Universidad Cenfotec

Maestría en Ciberseguridad

Documento final del Proyecto de Investigación Aplicada 2

Propuesta de una solución enfocada en seguridad de cloud computing para el registro y monitoreo de servicios de cloud services.

Berny Cordero Quirós

Abril 2018

Carta de Autorización para la Divulgación de la Tesis

Presente

Datos Generales

Nombre del Alumno: Berny Cordero Quirós

Título de tesis: Propuesta de una solución enfocada en seguridad de cloud computing para el registro y monitoreo de servicios de cloud services.

E-mail: bernycq@gmail.com Teléfono: 88947686

Consentimiento:

SI [X] NO [ ]

Autorizando la consulta y uso con fines exclusivos académicos a través de este medio a la Universidad CENFOTEC, de la versión física y digital de mi tesis titulada "Propuesta de una solución enfocada en seguridad de cloud computing para el registro y monitoreo de servicios de cloud services".

Fecha: 04/24/2018

BERNY CORDERO QUIROS (FIRMA)

Digitally signed by BERNY CORDERO QUIROS (FIRMA)
DN: serialNumber=CPF-01-1240-0306, sn=CORDERO QUIROS, givenName=BERNY, c=CR, o=PERSONA FISICA, ou=CIUDADANO, cn=BERNY CORDERO QUIROS (FIRMA)
Date: 2018.04.25 11:49:11 -06'00'

Firma: _____

Dedicatoria

Este trabajo de tesis está dedicado a mi madre, Floralia, quien ha sido una constante fuente de apoyo y aliento para afrontar los obstáculos, estoy realmente agradecido por tenerla en mi vida. Este trabajo está también dedicado a mis hermanos, Osvaldo y Priscila, quienes siempre me han amado incondicionalmente y cuyos buenos ejemplos me han enseñado a trabajar duro para las metas que aspiro a lograr.

Agradecimientos

Agradezco profundamente al profesor Luis Carlos Naranjo, por el apoyo en el desarrollo del presente trabajo de graduación, por la orientación brindada y el seguimiento al logro de los objetivos planteados mediante sus recomendaciones. Igualmente, expreso mi gratitud al Sr. Roy Martinez y la Srta. Yuliana Leitón por los comentarios y retroalimentación emitidos durante la elaboración de este.

Tabla de Contenidos.

Figuras.

Tablas.

Abstract

A los usuarios finales de la computación en la nube, a quienes les ha cambiado la forma de realizar sus actividades diarias, mejorando en la mayoría de los casos y permitiéndoles colaborar de una manera distinta con otros usuarios en diferentes lugares, tener acceso a las aplicaciones que requieren desde su navegador web y prácticamente desde cualquier equipo, incluso desde sus dispositivos móviles como teléfonos celulares o tabletas. Si bien es cierto que la computación en la nube es una tecnología que ya se utiliza desde hace algunos años, aún falta que sea completamente absorbida como una tendencia central en las organizaciones.

Sin embargo, la computación en nube es un arma de doble filo desde el punto de vista de seguridad y privacidad. A pesar de su potencial para proporcionar una garantía de bajo costo, las organizaciones pueden aumentar los riesgos de almacenar datos sensibles en la nube. En este trabajo, se analiza cómo las características de esta tecnología, tales como la novedad, la naturaleza de la arquitectura, y el atractivo y vulnerabilidad como un objetivo ciberdelincuencia están estrechamente ligada a la privacidad y la seguridad. Berny Cordero también investigo cómo los contextos proporcionados por las

instituciones formales e informales afectan a la privacidad y los problemas de seguridad en la nube.

Capítulo 1 Introducción

1.1 Generalidades

De acuerdo a T. Ambika, del departamento de ciencia de la universidad de Periyar, India, que durante años la Internet ha sido en diagramas de red representado por un símbolo de la nube hasta 2008, cuando una variedad de nuevos servicios comenzó a emerger que los recursos de computación autorizados a acceder a través de Internet denominan computación en la nube. La computación en nube abarca actividades tales como: el uso de sitios de redes sociales y otras formas de computación interpersonal; Sin embargo, la mayoría del tiempo con la computación en nube, se está interesado que acceden a las aplicaciones de software en línea, almacenamiento de datos y capacidad de procesamiento. La computación en nube es una manera de aumentar la capacidad o añadir capacidades dinámicamente sin tener que invertir en nuevas infraestructuras, formación de nuevo personal, o licencia de software nuevo. Se extiende de Tecnología de la Información (IT) de las capacidades existentes. (T.Ambika, 2014)

Adicionalmente como menciona (T.Ambika, 2014), en los últimos años, la computación en nube ha pasado de ser un concepto prometedor negocio a uno de los segmentos de rápido crecimiento de la industria de TI. Pero a medida que más y más información sobre las personas y empresas se colocan en la nube, están empezando a crecer Las preocupaciones acerca de lo seguro que es un entorno. A pesar de todo el entorno que rodea la nube, los clientes siguen siendo reacios a desplegar sus negocios en la nube. Los problemas de

seguridad en la computación en nube han jugado un papel importante en el retraso de su aceptación, la seguridad se manifiesta como el mayor desafío para la adopción de la computación en nube.

La realización de este proyecto se basa en el SIEM (Security Information and Event Management) que es el resultado de la Información de seguridad y administración de los eventos en lo que vamos analizar y elaboraremos la creación de las alertas.

1.2 Antecedentes del Problema

De acuerdo al estudio realizado por (K.Kavitha, 2015) Profesor del Colegio de Ingeniería de Adhiparasakthi, se han identificado siete problemas de seguridad que deben abordarse ante las empresas a considerar el cambio del modelo de computación en la nube, los cuales, son los siguientes:

1. El acceso de usuarios privilegiados: La información transmitida desde el cliente a través de Internet plantea un cierto grado de riesgo, debido a problemas de propiedad de los datos; las empresas deben dedicar tiempo a conocer sus proveedores y sus regulaciones tanto como sea posible antes de asignar algunas aplicaciones triviales.
2. Cumplimiento de la normativa: Los clientes son responsables de la seguridad de su solución, ya que pueden elegir entre los proveedores que permiten ser controladas por terceros y por otra parte organizaciones que comprueban los niveles de seguridad y los proveedores que no lo hacen.
3. Ubicación de los datos en función: En los contratos, algunos clientes podrían no saber qué país o jurisdicción se encuentran sus datos.

4. La segregación de datos: La información cifrada de varias compañías puede almacenarse en el mismo disco duro, por lo que un mecanismo para separar datos debería ser desplegado por el proveedor.
5. La recuperación: Cada proveedor debe tener un protocolo de recuperación de desastres para proteger los datos de usuario.
6. Investigación apoyo: Si un cliente sospecha que la actividad defectuosa del proveedor, él no debe de tener muchas formas legales para iniciar una investigación.
7. Viabilidad a largo plazo: Se refiere a la capacidad de cancelar un contrato y recuperar todos datos si el proveedor actual es comprado por otra empresa.

1.3 Definición y Descripción del Problema

En la presente investigación se analizan sistemáticamente las vulnerabilidades y amenazas de seguridad de la computación en la nube existentes. Para cada vulnerabilidad y amenaza, identificamos qué modelo o modelos de servicio en la nube se ven afectados por estos problemas de seguridad.

Basándose en el artículo "*Benefits, risks and recommendations for information security",* (European Network and Information Security Agency (ENISA), 2009), se establece un análisis de vulnerabilidades en computación en la nube. Este análisis ofrece una breve descripción de las vulnerabilidades, e indica qué modelos de servicios de la nube pueden ser afectados por ellos. Para este análisis, nos centramos principalmente en las vulnerabilidades conocidas

basadas en la tecnología. Sin embargo, hay otras vulnerabilidades que son comunes a cualquier organización, pero tienen que ser tomadas en consideración, ya que pueden afectar negativamente a la seguridad de la nube y su plataforma subyacente. Algunas de estas vulnerabilidades son los siguientes:

1. La falta de selección de empleados y pobres prácticas de contratación, de algunos proveedores de la nube no se pueden llevar a cabo la investigación de de sus empleados o proveedores. Los usuarios privilegiados como los administradores de la nube por lo general tienen acceso ilimitado a los datos de ella.
2. La falta de verificación de antecedentes del cliente, la mayoría de los proveedores de la nube no comprueban los antecedentes personales de sus clientes, y casi cualquier persona puede abrir una cuenta con una tarjeta de crédito válida y correo electrónico. Relatos apócrifos pueden dejar que los atacantes realicen las actividades maliciosas sin ser identificados.
3. La falta de educación de seguridad, la gente seguirá siendo un punto débil en la seguridad de la información. Esto es cierto en cualquier tipo de organización; sin embargo, en la nube, que tiene un impacto más grande porque hay más personas que interactúan con ella: los proveedores de nube, los proveedores de terceros, proveedores, clientes de la organización, y los usuarios finales.

Computación en la nube aprovecha muchas de las tecnologías existentes, tales como servicios web, navegadores web, y la virtualización, lo que contribuye a la evolución de los entornos de nube. Por lo tanto, cualquier vulnerabilidad asociada a estas tecnologías también afectan a la nube, e incluso puede tener

un impacto significativo. (European Network and Information Security Agency (ENISA), 2009)

1.4 Justificación

Una reciente encuesta realizada por Cloud Security Alliance (CSA) y IEEE indica que las empresas de todos los sectores están dispuestos a adoptar la computación en nube, pero que la seguridad se necesita tanto para acelerar la adopción de nubes a gran escala y para responder a los conductores de regulación. También detalla que la computación en la nube está dando forma al futuro de las TI, pero la ausencia de un entorno de cumplimiento está teniendo impacto dramático en el crecimiento de la computación en la nube varios son los estudios que se han realizado en relación con las cuestiones de seguridad en la nube, pero este trabajo presenta un análisis detallado de los problemas y desafíos de seguridad de computación en nube se centra en los tipos de implementación de computación en la nube y los tipos de prestación de servicios.

1.5 Viabilidad

1.5.1 Punto de Vista Técnico

"En pocos años, nadie tendrá en cuenta el grado de seguridad de computación en nube es porque habrá pocas alternativas." Estas palabras proféticas vienen de gurú de la computación en la nube Nick Marshall, director general de Redes Mundiales Giacom en el Reino Unido. Haciendo que el movimiento inicial de la computación en la nube este todavía a un gran paso, sin embargo, no puede tomarse a la ligera. La seguridad es un tema clave,

especialmente para las organizaciones que deben cumplir con las diversas normas de cumplimiento de normativas como PCI DSS y HIPAA / HITECH.

Por ahora, la computación en la nube es una opción viable para las empresas que buscan simplificar y reducir los gastos de capital para implementar, mantener y los software de acceso, plataformas e infraestructuras. Y si bien la consolidación y la virtualización pueden hacer para un entorno de TI más manejable, estos dos pilares en que se sostiene en la nube podrían plantear un objetivo más grande para la ingeniería social y otras formas de ataques.

Lo que es más, con todos sus beneficios, la computación en la nube significa que algunas funciones de muchas organizaciones están acostumbrados a la manipulación son asumidas por los vendedores, por lo que puede ser una proposición difícil "la entrega de llaves." (Team, 2012)

1.5.2 Punto de Vista Operativo

Antes de empezar a ingresar una organización a la nube, es importante determinar cómo su organización puede salir. Eso significa que el desarrollo de una estrategia de salida para su separación de un proveedor de servicios como parte de los planes de continuidad de negocio y recuperación de desastres. Por ejemplo, ¿cómo recuperar los datos del proveedor, especialmente cuando sus sistemas estén en problemas?

Incluso si el lector no sabe dónde están sus datos en cualquier momento dado, un proveedor de servicio en la nube debe ser capaz de decirle lo que sucederá con sus datos y servicio en caso de un desastre. Preguntar al vendedor si se tiene la capacidad de realizar una restauración completa, y si es así, ¿cuánto tiempo se tardaría.

Por este medio obtenemos visibilidad de los eventos relacionados con la seguridad en medio de los servidores, el sistema de monitoreo y el archivador de los eventos.

1.5.3 Punto de Vista Económico

Basados en el análisis de negocios económicos, podemos decir que la computación en nube permitirá a las empresas de alquiler de software y almacenamiento de datos de forma remota en una medida que sea necesario. Esto debería reducir los costes fijos en las empresas cuando entran en un nuevo mercado o iniciar la producción de un bien. (Etro, 2009)

Otros beneficios de economía de la computación en nube incluyen:

1. Actualizaciones de software rápidas y facilidad de modificación del software.
2. El costo compartido entre los consumidores.
3. Capacidad computacional variable y una mayor eficiencia.
4. El ahorro de energía como servidores se mueve a climas fríos.

A medida que las empresas se vuelven más baratas para iniciar y operar, se puede esperar ver varios cientos de miles de clientes nuevos.

La computación en nube también podría resultar en precios más bajos para los consumidores, el aumento de la competencia entre las empresas, y un

aumento en el crecimiento del producto por varias décimas de un punto porcentual. Esto es significativo.

Las ganancias en el corto plazo serán mucho mayores si los gobiernos miembros apoyan la adopción a través de incentivos financieros, promoción general y de acuerdos para reducir las barreras a la transmisión de datos a través de fronteras. (Etro, 2009)

1.6 Objetivos

1.6.1 Objetivo General

Proponer una solución enfocada en seguridad de cloud computing para el registro y monitoreo de cloud services, basada en el resultado de la información de seguridad y administración de eventos.

1.6.2 Objetivos Específicos

1.1 Definir fuentes selectas de logs en el entorno de nube cruzada del SIEM existente.

2.1 Identificar las amenazas en el entorno del cloud computing.

3.1 Crear las reglas en el SIEM con el fin de monitorear y tratar los eventos recibidos.

4.1 Confeccionar una guía con las reglas creadas para identificar las amenazas de forma proactiva recibidas en el SIEM.

1.7 Alcances y Limitaciones

1.7.1 Alcances

1. Entregar la lista de logs usados para la creación de las alertas definiendo su tipo de dato dependiendo de la empresa que distribuye en este caso AZURE y AWS, todo esto en una base de un sistema de Información de seguridad y administración de eventos (SIEM) ya definido.
2. Enumerar unas lista de las amenazas mas comunes a nivel de cloud computing relacionadas en un ambiente de PyMES, con la idea de conocer sus vulnerabilidades mas comunes.
3. Creación de las alertas de cloud computing para nuestro sistema de Información de seguridad y administración de eventos (SIEM), basadas en AZURE y AWS.
4. Basados en las alertas creadas realizar una serie de instrucciones para ayudar en el análisis y acciones finales al usuario final. Estas están basadas en donde se obtuvieron los logs y una breve explicación demostrada con un ejemplo.

1.7.2 Limitaciones

1. El tiempo de inactividad: Esta puede ser una de las peores desventajas de la computación en nube. Ningún proveedor de nube, la mejor, podría reclamar inmunidad a las interrupciones del servicio. Sistemas de computación en la nube se basan en la Internet, lo que significa que su acceso es totalmente dependiente de su conexión a este. Y, al igual que cualquier hardware,

plataformas de nube a sí mismos pueden fallar por cualquiera de las mil razones.

2. La seguridad y la privacidad: Cualquier dato de discusión que involucra debe abordar la seguridad y la privacidad, especialmente cuando se trata de gestionar los datos sensibles. No hay que olvidar espacio de código y lo que ocurrió a él después de su consola AWS EC2 fue vulnerado y sus datos finalmente eliminada, lo que obligó a la empresa a cerrar puertas para siempre. Mediante el aprovechamiento de una infraestructura basada en la nube a distancia, una empresa externaliza básicamente todo lo que tiene.
3. La vulnerabilidad a los ataques: En la computación en nube, cada componente es potencialmente accesible desde Internet. Por supuesto, no hay nada conectado a Internet es perfectamente seguro e incluso los mejores equipos sufren ataques graves y violaciones de seguridad. Pero dado que la computación en nube se construye como un servicio público y que es fácil de ejecutar antes de aprender a caminar, nadie en AWS comprueba sus habilidades de administración antes de otorgarle una cuenta: todo lo que necesita para empezar es una tarjeta de crédito válida.
4. Control limitado y flexibilidad: En diversos grados (dependiendo del servicio particular) usuarios de la nube tienen un control limitado sobre la función y la ejecución de su infraestructura de alojamiento. Las políticas de gestión podrían imponer límites a lo que los clientes pueden hacer con sus despliegues. Los clientes también se limitan al control y la gestión de sus aplicaciones, los datos y servicios, pero no la infraestructura. Por supuesto,

nada de esto será normalmente un problema, pero debe ser tenido en cuenta.

5. Dependencias plataforma de computación en la nube: La dependencia implícita, también conocido como "los proveedores de tecnología" es otra de las desventajas de la computación en nube. Diferencias muy arraigadas entre los sistemas del proveedor a veces puede hacer que sea imposible migrar de una plataforma en la nube a otra. No sólo puede ser complejo y costoso volver a configurar sus aplicaciones para satisfacer las exigencias de un nuevo huésped, pero la migración también podría exponer sus datos de vulnerabilidades de seguridad y privacidad adicionales.
6. Costos de computación en nube. La computación en nube, especialmente en una pequeña escala y para los proyectos a corto plazo, puede ser caro. A pesar de que puede permitirle reducir los gastos de personal y de hardware, la etiqueta general de precios podría terminar siendo más alta de lo esperado. Hasta que esté seguro de lo que funciona mejor para usted, es una buena idea experimentar con una variedad de ofertas. Usted también puede hacer uso de las calculadoras de costos proporcionados por proveedores como AWS de Amazon y GCP de Google.
7. A nivel investigativo solo se van a confeccionar 14 reglas que según la industria son las más comunes a nivel SIEM de cloud computing.

1.8 Estado de la Cuestión

El investigador decidió orientar la investigación sobre la seguridad en la computación en la nube debido a que, en los últimos años, todos nos hemos

vuelto usuarios en estas tecnologías sin darnos cuenta sobre las repercusiones y riesgos que conlleva el uso de estos servicios. Debido a esto se procedió a investigar el estado de la cuestión de este tema, así como si existe algún tipo de marco que sirva como base para su implementación.

La computación en la nube en su concepto central no es una idea nueva, conceptos similares como por ejemplo Application Service Provider (ASP) han existido por varios años. Sin embargo, lo que ha ocurrido recientemente es que las posibilidades de creación de redes y virtualización han aumentado considerablemente, permitiendo un uso nuevo y más amplio del concepto. Al igual que con ASP, la computación en nube gira en torno a la utilización y la combinación de servicios para ofrecer funcionalidad que admita valores empresariales, en lugar de un producto entregado. Esto ha dado lugar a que muchas nuevas e innovadoras soluciones de cloud computing estén disponibles para empresas y clientes privados de todo el mundo.

Por lo tanto, esta tesis apunta tanto a los departamentos de TI que buscan Informática como una alternativa a un recurso sobre el terreno, así como una audiencia que investiga la adopción del cloud computing. Las conclusiones serán de interés para la mayoría de los departamentos de TI interesados en mejorar potencialmente su flexibilidad y eficiencia. La tesis también presenta alternativas de servicio en la nube, directrices y un método de trabajo que podría ser de interés para una comunidad académica más amplia y personal de TI como administradores, arquitectos y diseñadores, con respecto a los servicios en la nube y los recursos en las instalaciones.

El siguiente estado de la cuestión recorre una selección de diferentes autores expertos en computación en la nube, los cuales han publicado sus artículos referentes a este tema y de los cuales su calificación se ha verificado en la fuente scholar.google.com

Inicialmente, para realizar el sondeo del estado de la cuestión de este tema se utilizó Google Académico (scholar.google.com) en donde se aplicaron los siguientes criterios de búsqueda.

Inicialmente se utilizaron los criterios:

+cloud +computing +governance

Lo cual nos regresó un total de 42300 resultados.

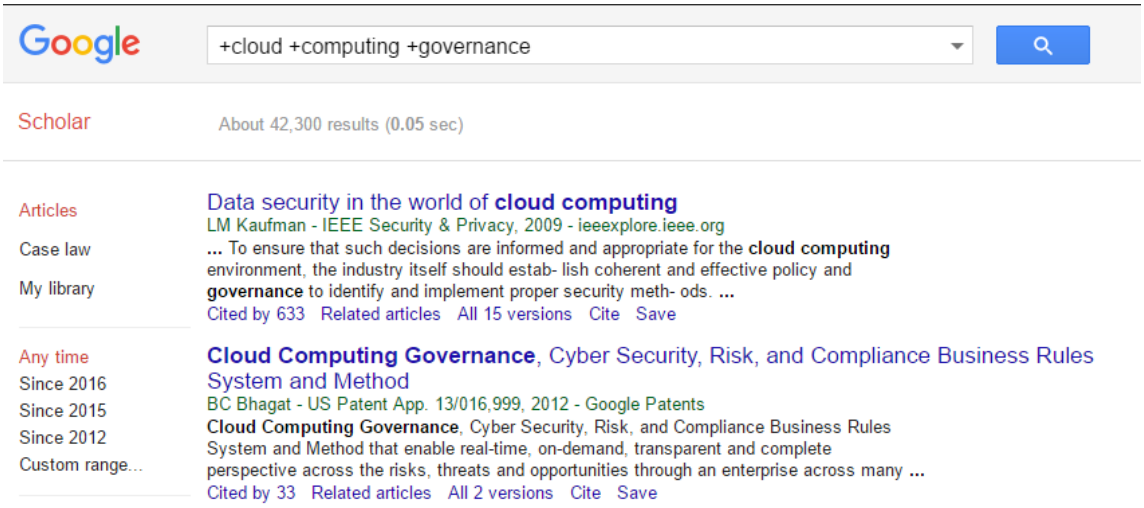

FIGURA 1: RESULTADOS DE SCHOLAR DE GOOGLE

Refinando la búsqueda, se llegó a la siguiente consulta que mostró 5810 resultados:

+cloud +computing +governance +iaas

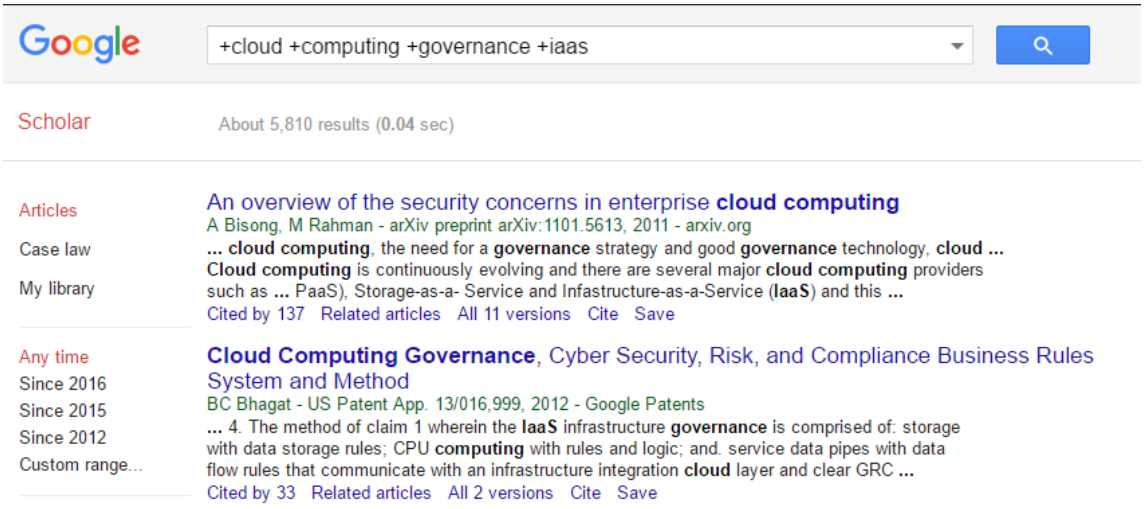

FIGURA 2: RESULTADOS DE SCHOLAR DE GOOGLE CON FILTROS EXTRAS

Se agregó más parámetros a la búsqueda y se obtuvieron 53 resultados.

+cloud +computing +governance +iaas +27018

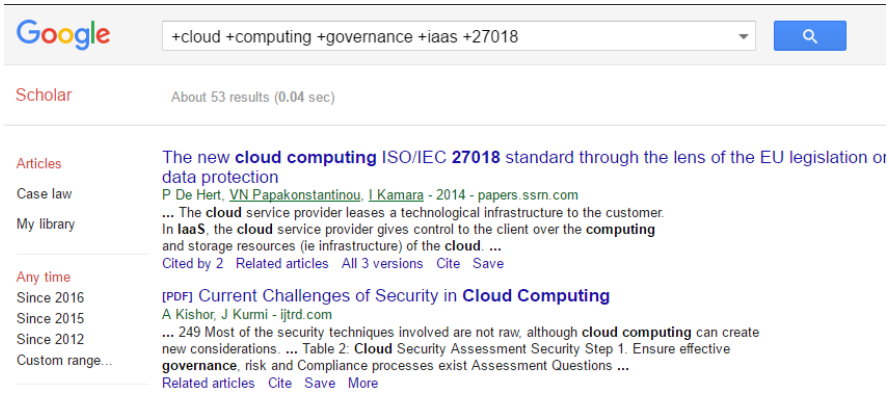

FIGURA 3: RESULTADOS DE SCHOLAR DE GOOGLE CON PARÁMETROS EXTRAS

Luego se procedió a eliminar los resultados de años anteriores al 2015, lo cual disminuyó los resultados a 18.

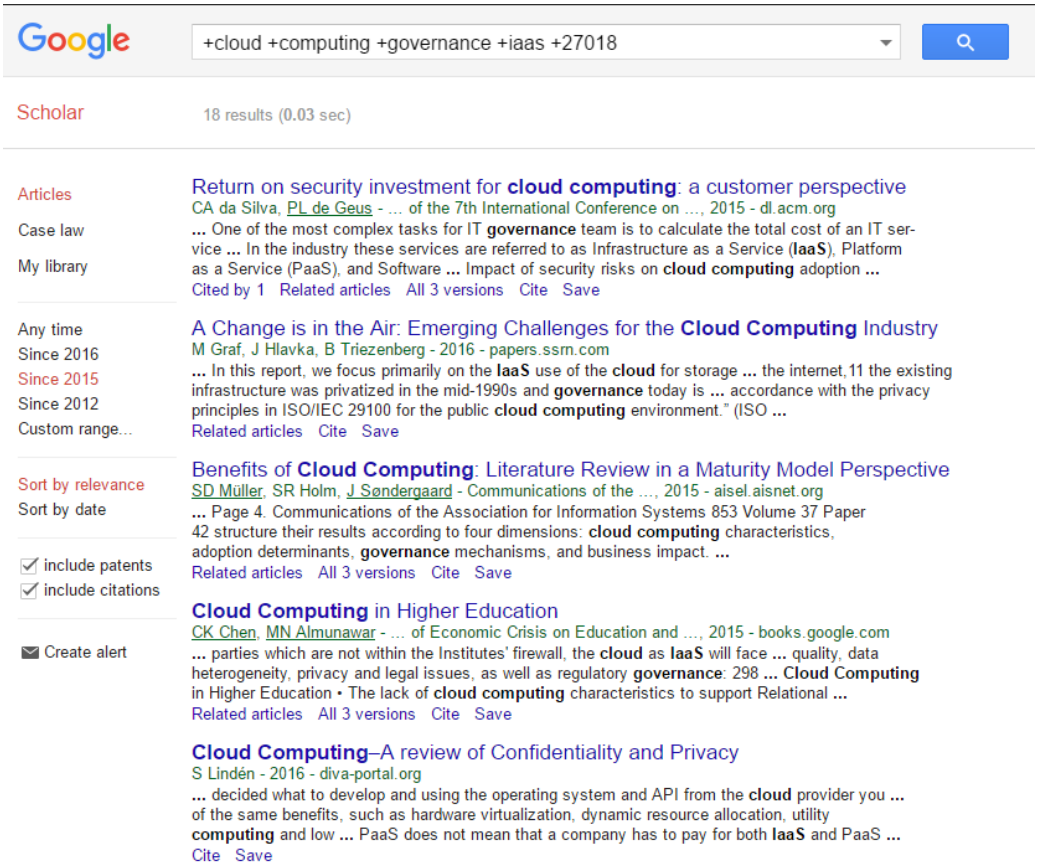

FIGURA 4: RESULTADOS DE SCHOLAR DE GOOGLE CON PARÁMETROS Y FILTROS EXTRAS

Con los resultados obtenidos de la búsqueda anterior, se estudian la selección de publicaciones con el fin de evaluar la revolución tecnológica conocida como computación en la nube, los riesgos que conlleva y las mejores prácticas de cómo asegurarla.

Como paradigma de esta revolución encontramos el cambio que se da en el universo digital basado en la información y como dichos datos son compartidos a través de la insegura red conocida como internet.

Justamente, debido a este cambio que comienza a darse dentro de la sociedad, es que es necesario detenerse a pensar en lo que está sucediendo,

tanto en la vida de las personas, así como en funcionamiento de las empresas en esta era de la información y su integración a la computación en la nube.

Esta investigación se centra, entonces, en el análisis de uno de los mayores cambios de paradigma que se dan en el centro de la transformación tecnológica del presente siglo en el mundo informático, que se da gracias a la implementación de la computación en la nube. Esta transformación se caracteriza por la nueva relación que se da entre la información y la manera que se tiene para acceder a ella.

Por último, adicionalmente se procederá a analizar tanto los aspectos positivos (disponibilidad y omnipresencia de la información), como los negativos (peligros en la seguridad y control, tanto de la información, así como del acceso a ella), a los que nos enfrentamos cuando comenzamos a vivir en la nube y nos volvemos cada vez más ciudadanos del mundo digital.

Ahora bien, basados en la lectura de los artículos leídos, se procede a la definición del objetivo general y los objetivos específicos que guiarán esta investigación.

Capítulo 2 Marco Conceptual

FIGURA 5: NUBE DE PALABRAS PARA VISUALIZAR LA FRECUENCIA DE LAS PALABRAS DEL CAPÍTULO 2

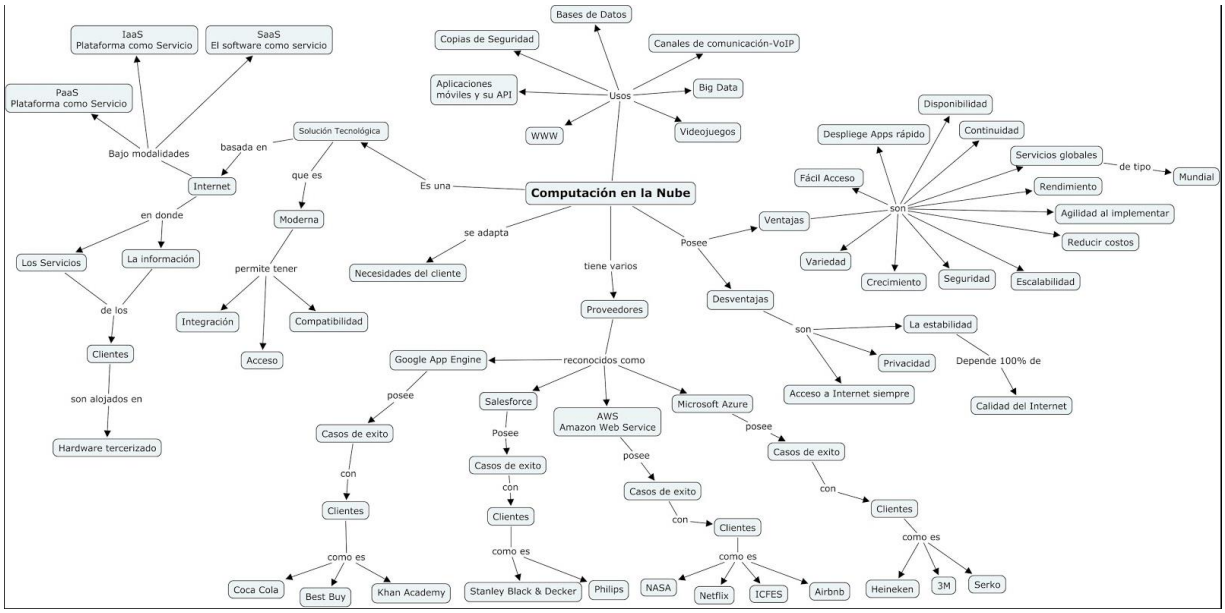

FIGURA 6: MODELO JERÁRQUICO DE PALABRAS CLAVES DEL CAPÍTULO 2 MARCO CONCEPTUAL.

2.1 Servicios en la nube

En lugar de ejecutar una aplicación para proporcionar una funcionalidad específica, se podría acceder a esa funcionalidad como un servicio. Estos servicios se pueden combinar fácilmente con otros servicios, tanto internos como externos, para proporcionar funcionalidad adicional.

Un servicio debe tener funcionalidad autónoma, es decir, debe proporcionar la misma funcionalidad independientemente de otros. Esta funcionalidad debe proporcionarse directamente desde el servicio sin necesidad de acceso a través de otros. Un servicio también debe estar ligeramente acoplado. Esto significa que el servicio podría ser visto como una caja negra, donde el usuario no necesita saber cómo se realiza el cómputo, sino sólo qué información se debe proporcionar y devolver. Esto es importante ya que un servicio poco acoplado puede escalarse y mantenerse fácilmente. Juntos, estos

principios permiten que los servicios se conviertan en componentes del sistema reutilizables (Sanders, J. A. Hamilton et al., 2008).

2.2 La historia y el desarrollo de la computación en la nube

Cloud computing y otros servicios basados en Internet continúan desarrollándose rápidamente, aunque no ha sido exactamente un camino directo para llegar a donde está ahora. El estado actual de la industria puede parecer obvio e inevitable cuando miramos hacia atrás, pero hace poco tiempo habría sido difícil adivinar que aquí es donde las cosas iban realmente.

La historia de la computación en nube ha pasado por una serie de cambios importantes que lo han hecho más accesible y asequible. Como muchas otras cosas, sin embargo, es importante entender dónde ha estado para adivinar a dónde va.

El estado actual de la computación en la nube se basa en una columna vertebral de Internet fuerte, pero no es así como comenzó o dónde termina. La nube privada es ahora una parte importante de muchas infraestructuras de TI de negocios, haciendo que elementos como la virtualización y la arquitectura orientada a servicios sean aún más importantes. Si nos fijamos en el desarrollo de la nube en los últimos años, es más fácil ver por qué la nube es un componente integral de las soluciones de TI modernas.

2.3 Que es la computación en la nube (Cloud Computing)

Cloud Computing utiliza servicios para proporcionar funcionalidades específicas a través de Internet. Es básicamente un par de servidores

conectados a Internet, ubicados juntos o distribuidos en varias ubicaciones, que proporciona aplicaciones y datos para los usuarios del cliente. Estos servidores pueden ser computadoras virtualizadas que se proveen dinámicamente y se presentan como uno o más recursos de computación unificados basados en acuerdos de nivel de servicio establecidos a través de la negociación entre el proveedor de servicios y los consumidores. La idea principal es que el cliente es agnóstico respecto al hardware subyacente (Buyya, Yeo et al., 2008; Leavitt 2009).

Para el usuario hay principalmente tres aspectos que son nuevos con la computación en nube, en comparación con un recurso en el local. Primero hay la apariencia de una cantidad infinita de potencia de computación y soporte de hardware. El segundo es la eliminación del costo inicial del nuevo hardware y el tercero es la posibilidad de pagar por la cantidad de recursos que realmente se utiliza (Michael Armbrust 2010). Básicamente un servicio con funcionalidad comparable se ofrece en lugar de un producto entregado. Los servicios no son procesos mecanizados; De hecho, suelen recurrirse a otros servicios con los seres humanos, cuidando el mantenimiento y administrando las relaciones proveedor-consumidor. Este es un modelo relativamente nuevo dentro de la industria del software (Bennett, Layzell et al., 2000).

Para que algo sea realmente un servicio en la nube tiene que ser entregado a través de la red de telecomunicaciones. El usuario se basa en los servicios de procesamiento y acceso a los datos, que también tiene que estar bajo su control legal del usuario. Dado que algunos de los recursos en los que dependen los servicios están virtualizados, el cliente no necesita saber qué

servidor ejecuta el servicio o dónde se encuentra. Esto junto con un contrato muy flexible crea el entorno muy dinámico y escalable que permiten los servicios en la nube (Clarke 2010). Este entorno promueve el uso de clientes gruesos y delgados, ya que todas las capacidades están disponibles a través de la red y el acceso a través de mecanismos estándar (GICTF 2010).

2.4 Los Principios de la Computación en Nube

Las imágenes de la informática seria en los años 50 y 60 de fila tras fila de máquinas de cinta magnética son en realidad un presagio de una estructura de cloud computing. En otras palabras, las empresas ya estaban utilizando una gran cantidad de máquinas para proporcionar más potencia de lo que una sola unidad podría y, además, permitir que más de un usuario acceda a los mismos activos.

En la década de los 50, esas gigantescas computadoras centrales se instalaban en escuelas, organizaciones gubernamentales y grandes corporaciones porque eran los únicos lugares que posiblemente podrían albergar todas esas máquinas. Incluso entonces, varias instancias del mainframe serían inconcebibles, por lo que se convirtió en práctica normal para desarrollar "terminales mudo" que permitió a varias personas para acceder a los recursos necesarios. Este es el mismo principio que la virtualización moderna, que nos sitúa en el camino hacia la computación en la nube.

2.5 Historia Temprana - Máquinas Virtuales

La implementación real de máquinas virtuales se produjo en los años 70 cuando IBM lanzó un sistema operativo llamado VM. Esto permitió que varias computadoras distintas residieran en el mismo entorno de procesamiento, lo que daría lugar al tipo de interacciones que conocemos como virtualización de llamadas. En términos básicos, significa que cada usuario individual tendría una máquina con su propia memoria, procesador y otros componentes de hardware, pero muchos de los recursos serían compartidos por otros.

Este tipo de "grupo de computación" mostró a las empresas que podrían comenzar a agregar soluciones de red sin aumentar su infraestructura de hardware. Todo se trataba de aprovisionar los recursos que ya tenían, cambiar el tráfico cuando era necesario y equilibrar la carga en la red y el ancho de banda para proporcionar mejores servicios a sus clientes.

2.6 La Edad Media - El potencial de Internet

Las soluciones de telecomunicaciones eran una parte integral del desarrollo de la nube, y esto fue posible con la comercialización de Internet. La red en la que se basa, sin embargo, se remonta a los años 60 cuando J.C.R. Lickliker permitió el desarrollo de ARPANET (Red de Agencias de Proyectos Avanzados de Investigación). Esto eventualmente se convertiría en el precursor de la Internet moderna.

La idea de conectar a personas de todo el mundo para acceder a programas y datos de diferentes lugares se convirtió en una posibilidad real. En los años 70, la gente estaba realmente profundizando en el potencial sugerido

por los primeros experimentos en los años 60. En 1971, por ejemplo, se envió el primer correo electrónico y el Departamento de Defensa de los Estados Unidos siguió desarrollando ARPANET en Internet.

En 1979, tanto CompuServe Information Services como The Source se pusieron en línea, mostrando que era posible que los proveedores de servicios comerciales alojaran servicios de Internet. Sin embargo, no fue hasta 1993 que el navegador Mosaic hizo el Internet mucho más gráfico algo que el usuario promedio podría manejar. Fue poco después de que cuando Netscape lanzó, y luego, en 1995, tanto Amazon y eBay apareció.

2.7 Revolución Industrial - Computación asequible

Parte de la razón de la brecha entre 1979 y 1993 fue que las computadoras todavía no eran asequibles o lo suficientemente compactas como para que las personas tuvieran en sus hogares o para que las compañías equiparan a todo su personal. Los años 80 vieron el boom más grande en las computadoras, con IBM que pone hacia fuera una gama de computadoras personales asequibles y Microsoft que empuja su sistema de funcionamiento hacia afuera en una escala grande.

Luego, en los años 90, finalmente había suficiente ancho de banda disponible para poner realmente el Internet a disposición de las masas, lo que significaba que todas aquellas empresas que habían equipado a su personal con computadoras ahora tenían una forma válida de conectarlos a todos. Sin este tipo de ancho de banda de alta velocidad e interoperabilidad de software, este tipo de computación conectada nunca hubiera funcionado.

2.8 Historia Moderna - Arquitectura Orientada a Servicios (IaaS)

El surgimiento de redes comerciales no fue fácil, y una vez que estalló la primera burbuja en 2000, las empresas tuvieron que empezar a replantear sus modelos de negocio. La lección aprendida fue que no importa cuánto dinero los inversionistas arrojaron a usted, todavía necesita un sólido plan de negocios para sobrevivir a largo plazo.

En la búsqueda de nuevas maneras de monetizar el Internet, muchas compañías comenzaron a realizar un modelo de servicio para entregar soluciones y recursos utilizables. Salesforce.com fue la empresa que realmente comenzó esta tendencia al ser pionera en el concepto de ofrecer aplicaciones de clase empresarial a través de un simple sitio web.

Luego, en 2002, Amazon se incorporó a la tendencia con Amazon Web Services. Esto dio a los usuarios la posibilidad de acceder a soluciones de almacenamiento, computación y otras aplicaciones a través de Internet. En 2006 avanzaron con la nube Elastic Compute (EC2), que básicamente permite a los desarrolladores alquilar espacio en sus computadoras para almacenar y ejecutar sus propias aplicaciones. Era toda una infraestructura que entregaban como un servicio.

En 2009, la mayoría de los influyentes de la industria estaban a bordo, con empresas como Microsoft y Google entregando aplicaciones para el consumidor medio, así como las empresas en forma de servicios sencillos y accesibles.

2.9 Poseer tu nube personal y sus posibilidades

La ubicuidad del cloud computing ha llevado a un entorno en el que las empresas no tienen que ir a terceros para aprovechar este recurso. La tecnología se ha desarrollado hasta el punto de que las organizaciones pueden desplegar efectivamente sus propias nubes privadas o híbridas, en lugar de confiar en las nubes públicas. Esto puede potencialmente aumentar el rendimiento y disminuir ciertos costos en esta área.

Más importante aún, un despliegue de nube privada le da al equipo de TI más visibilidad en el back-end de su sistema, lo que es particularmente útil para empresas que están extremadamente conscientes de la seguridad y requieren supervisión directa de todos sus activos.

Las implementaciones de la nube privada son cada vez más frecuentes, ya que ofrecen una gran cantidad de los mismos costos y ventajas de conveniencia, y soportan varias plataformas, permitiendo a la organización mantener un mayor control. El camino para llegar a este punto ha sido largo, y aunque puede ser difícil predecir exactamente lo que depara el futuro, actualmente hay muchos beneficios al aprovisionar recursos a través de una red privada segura y segura.

2.10 Seguridad y la Nube

En la primera parte de este escrito, los autores, explican cuestiones básicas sobre la computación en la nube, historia, su evolución, ventajas y desventajas. En la segunda parte se explora la situación actual de esta

tecnología desde el punto de vista de la seguridad y sus implementaciones en Costa Rica.

Para el adecuado desarrollo de esta investigación, es adecuado aclarar algunos conceptos comunes en el campo de la nube que son claramente definidos por (Delgado, 2014).

2.10.1 Computación en la nube:

Es el término más importante, puerta de entrada a este mundo. Entiéndase por Computación en la nube el proceso de llevar los datos, procesamiento y desarrollo de soluciones IT fuera de la empresa, a un lugar centralizado en plataformas seguras remotas. Es decir, el poder de cómputo de una compañía se deja en manos de un tercero encargado del mantenimiento y la disponibilidad del recurso.

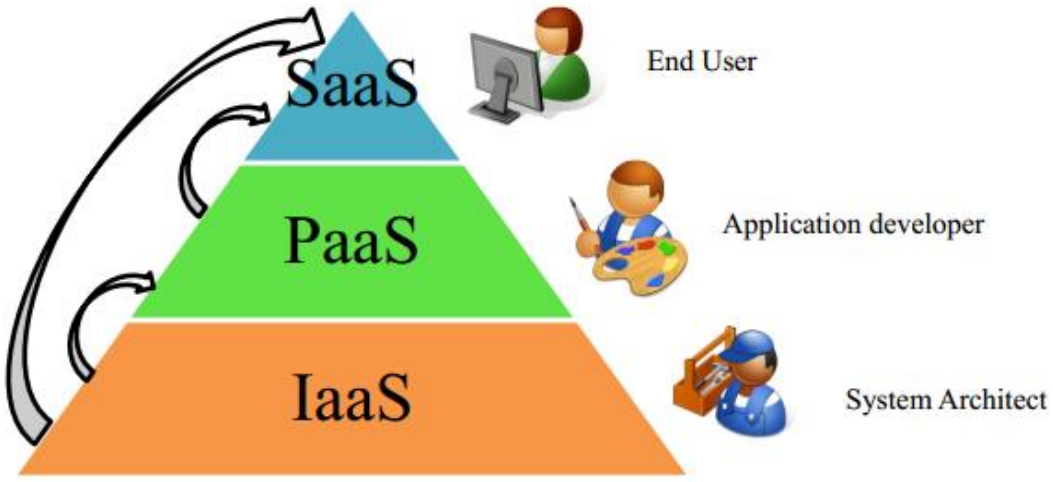

FIGURA 7: MODELOS DE SERVICIOS DE CLOUD COMPUTING

2.10.2 SaaS, Software como servicio:

Con este modelo las empresas dejan de adquirir costosas licencias de software pasando a un modo de suscripción mensual adaptado a las necesidades de las compañías. Además, se obtienen actualizaciones de software manteniendo a las compañías en paralelo con el desarrollo de la industria. Uno de los ejemplos es Adobe Creative Cloud, que ha dejado de vender sus productos para ofrecer planes o suscripciones que dan derecho a los usuarios a usar la aplicación a cambio de pago mensual. Como beneficio, mantiene durante el tiempo de suscripción las aplicaciones actualizadas a la última versión sin incurrir en gastos adicionales. Otro claro ejemplo es Office 365, que ofrece su suite de ofimática en un modelo de pagos mensuales con la posibilidad de descarga de herramientas de escritorio. SaaS son aplicaciones que se ejecutan en los servidores de la nube en lugar de en los equipos o servidores del cliente. Esto permite al cliente ejecutar la aplicación en su navegador web sin necesidad de instalación (Leavitt 2009, Marston, Li et al., 2010).

Estos servicios a menudo se ejecutan como aplicaciones web y son generalmente muy escalables junto con una alta disponibilidad que los hace muy fáciles de adoptar (Michael Armbrust 2010). Muchas soluciones SaaS permiten al cliente comenzar a utilizarlas tan pronto como el pago es recibido por el proveedor, lo que resulta en un rápido proceso de inicio (Pattabhiram y D'Anna 2010)

2.10.3 IaaS, Infraestructura como servicio:

Gracias a esto se pone fin a las costosas inversiones, implementación y mantenimiento de hardware en las compañías. En el modelo tradicional tener un listado operativo de servidores le cuesta a la compañía una buena cantidad de dinero en gastos ocultos como la energía, el aire acondicionado, las licencias, el ingeniero de soporte especializado, etc. Con la infraestructura como servicio todo esto es cosa del pasado ya que todo se resume en un pago mensual a un tercero quien es el que se tiene que preocupar por la vitalidad y disponibilidad de las máquinas que ofrece. Gracias a esto el recurso humano de TI en las compañías se puede dedicar a pensar en estrategias en pro del negocio y no en cómo mantener unos servidores funcionando. IaaS el usuario obtiene acceso a las partes centrales del servidor (Leavitt 2009, Marston, Li et al., 2010). Estas instancias se parecen mucho al hardware físico y dan a los usuarios el control de casi todo el software desde el núcleo y hacia arriba (Michael Armbrust 2010). Esto se utiliza principalmente para el almacenamiento y capacidades computacionales, y suele estar diseñado para desarrolladores y arquitectos de sistemas (Marston, Li et al., 2010). Un ejemplo de un servicio de infraestructura disponible es Amazon Elastic Compute Cloud (EC2) (Amazon.com 2011), donde los usuarios pueden asignar servidores virtuales y administrarlos como si fueran hardware real.

2.10.4 PaaS, Plataforma como servicio:

Está enfocado a empresas desarrolladoras de software y se utiliza para construir, probar y lanzar aplicaciones sin necesidad de comprar una sólida infraestructura de hardware y software. Está enfocado al desarrollo de

aplicaciones, con PaaS, no es necesario adquirir licencias de lenguajes de programación, menos infraestructura de desarrollo o pruebas. PaaS ofrece todos los elementos necesarios para que los desarrolladores de software escriban sus programas, los prueben y los lleven posteriormente a ambientes productivos. PaaS ofrece a los usuarios más libertad para desarrollar sus propias aplicaciones y programas en el entorno cloud de un proveedor y ejecutar todo desde allí. Esto puede eliminar efectivamente la necesidad de costosas herramientas de desarrollo y recursos internos. A PaaS se puede ver como acceso desde el sistema operativo y hacia arriba (Leavitt 2009, Marston, Li et al., 2010). Microsoft Windows Azure (2011) es un ejemplo de una plataforma donde los usuarios pueden desarrollar, cargar y administrar sus propias aplicaciones.

2.10.5 Utility Computing:

Lo más probable es que en un modelo tradicional cuando una empresa compra un servidor, no use todos los recursos disponibles con el hardware. Lo normal es ver empresas con servidores sobredimensionados que no usan su capacidad al 100%, con un servicio basado en cloud. A las compañías se les da el denominado modelo de Utility Computing, o sistema pay-as-you-go, donde la empresa solo paga por los recursos que necesita en un determinado periodo de tiempo. Este uso es calculado y facturado en términos de ancho de banda utilizado y niveles de almacenamiento de datos. Amazon es una de las empresas pioneras en este servicio, ofreciendo infraestructura por demanda y facturando por lo que usa. Por ejemplo, si contrata un servidor con dos gigas en

RAM por un valor de un dólar la hora, puede aumentar la memoria del servidor y esta acción se verá reflejada en su factura.

2.10.6 Nube Privada:

Como su misma palabra lo indica, se trata de una nube en donde sólo la compañía comparte recursos para sí misma, los empleados pueden acceder a ellos siempre y cuando estén dentro del ámbito privado de la compañía, las personas ajenas no tienen acceso a la información. En contraste con la nube pública está la nube privada, que se gestiona y se hospeda desde dentro de la organización. Beneficia de muchos de los efectos positivos de una nube pública, como ser elástica y basada en servicios, pero también proporciona un mayor control sobre la información crítica de la organización que la nube pública (Marston, Li et al., 2010).

Una solución de nube privada tiene que ser muy grande para obtener las ventajas de la escala asociados con los servicios de nube pública. Si la capacidad de los servidores no es lo suficientemente grande el usuario puede no obtener la percepción esperada de una cantidad casi interminable de poder de computación y soporte de hardware. Esto significa que debemos tener cuidado al nombrar a un centro de datos privado o a una granja de servidores una nube privada, ya que éstos pueden no tener todas las ventajas que asignamos al cloud computing (Armbrust, Fox et al., 2010)

2.10.7 Nube Pública:

La nuble publica es la que ofrece servicios usando los mismos recursos de servidor atendiendo a varias partes de manera simultánea. Al contrario de las redes privadas que restringen el servicio a personas ajenas, las públicas están alineadas con el objetivo de brindar servicios unificados abiertos. Una nube pública está disponible de un proveedor de servicios de terceros a través de Internet. En una nube pública, todos los datos y cálculos se almacenan y se realizan en los servidores del proveedor. Esto significa que los usuarios interactúan con los servidores del proveedor en lugar de los propios.

La nube pública suele ser una forma cómoda y rápida para que las organizaciones desplieguen sus soluciones de TI en comparación con invertir e instalar hardware en las instalaciones. Esto reduce efectivamente los costos iniciales de hardware y mantenimiento. Por otra parte, esta implementación obliga a los clientes a depender del proveedor. Las principales características de habilitación de las nubes públicas son la escala y disponibilidad de los centros de datos y las granjas de servidores de los proveedores de nube. Esto significa que el usuario percibe una cantidad casi interminable de poder de computación y soporte de hardware (Marston, Li et al., 2010).

2.10.8 Cloud Híbrida:

Se trata de la combinación de nube privada y pública, se usa para incrementar el rendimiendo de aplicaciones altamente transaccionales en donde subir a una nube externa podría impactar la operación de la organización. Se define entonces como una combinación entre lo privado y lo público para

garantizar niveles de tráfico balanceados. La nube hibrida es una combinación de estas dos implementaciones de nube.

Esto significa que la información crítica se mantiene dentro de la organización, mientras que la no crítica se subcontrata a los proveedores externos de las nubes públicas. Esto significa que partes de la nube están alojadas internamente dentro de la organización y manejan la información crítica, mientras que el resto de la funcionalidad se accede a través de proveedores públicos. La parte interna de la nube no tiene que ser capaz de soportar todas las necesidades del negocio, sino sólo las que manejan la información crítica. Las compañías pueden aprovechar las ventajas de la computación en la nube sin sacrificar el control de su información crítica (Marston, Li et al., 2010).

2.10.9 Data Center:

Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo en Latinoamérica, o centro de cálculo en Europa o centro de datos. Es en este lugar en donde se concentra todo el recurso de cómputo ofrecido en las nubes públicas, privadas o híbridas. Al final todas residen en un centro de datos o Data Center.

2.11 Logs y la Nube

Los logs son una de las piezas más importantes de los datos analíticos en una infraestructura de servicios basada en la nube. En cualquier momento, Los

propietarios de servicios y los operadores deben entender el estado de cada componente de infraestructura para el monitoreo de fallas, para evaluar el uso de las funciones y para supervisar los procesos empresariales.

Los desarrolladores de aplicaciones, así como el personal de seguridad, necesitan acceso a la información histórica para la depuración y las investigaciones forenses. Se discute un marco de logs y directrices que proporcionan un enfoque proactivo a la tala para asegurar que los datos necesarios para las investigaciones forenses se han generado y recogido. El marco estandarizado elimina la necesidad de que las partes interesadas en la tala reinventen sus propios estándares.

Estas directrices aseguran que la información crítica asociado con la infraestructura de nube y el software como servicio (SaaS) los casos de uso se recogen como parte de una defensa de la estrategia. Además, se aseguran de que los consumidores de logs pueden analizar, procesar y correlacionar de manera efectiva y sencilla.

La computación en nube se utiliza cada vez más para implementar y ejecutar servicios de usuario, también conocidos como software como servicio (SaaS). La ejecución de cualquier aplicación requiere información sobre cada capa de infraestructura por razones técnicas, de seguridad y comerciales. En esta sección se describen algunos de estos problemas y casos de uso que pueden beneficiarse del análisis y la gestión del registro. Si se observa el ciclo de vida de desarrollo de software, los casos de uso se presentan en el siguiente orden:

- Depuración y forense

- Supervisión de fallos
- Solución de problemas
- Uso de funciones
- Supervisión del rendimiento
- Detección de seguridad / incidentes
- Cumplimiento normativo

Cada uno de estos casos de uso puede aprovechar el análisis de log para resolver completamente o al menos ayudar a acelerar drásticamente y simplificar la solución al caso de uso.

2.11.1 Log Tuning

Los datos de logs están ahora centralizados y se tienen que ajustar las fuentes de los logs para asegurarse de que obtengamos el tipo correcto de ellos y los detalles correctos. Cada componente de logs debe ser visitado y tuneado basado en los casos de uso. Algunas preguntas en que debemos considerar de dónde recolectar los logs individuales, qué logs almacenar en el mismo lugar, y si se deben recopilar ciertos logs. Por ejemplo, si está ejecutando un servidor Web Apache, recolecta todos los logs en el mismo archivo; todos los accesos a los archivos multimedia, los errores y los accesos regulares, o se van a pasar por alto algunos logs de registro.

Dependiendo de los casos de uso, es posible que necesite logs detalles en los logs de registro. Por ejemplo, en Apache es posible registrar el tiempo de procesamiento para cada solicitud. De esa manera, es posible identificar las

degradaciones del rendimiento supervisando cuánto tarda Apache en procesar una solicitud.

Un proceso de mejora continúa para asegurar que los desencadenadores de eventos están produciendo el mayor número posible de alertas válidas mientras se reducen activamente los FPA. Ocasionalmente, las reglas de SIEM (Información de seguridad y administración de eventos) pueden producir alertas positivas falsas (FPA). Este es el resultado de un evento que coincide con un desencadenador de correlación dado, al demostrar el mismo patrón de comportamiento que un exploit conocido, pero se considera benigno: un evento válido justificado por un negocio que no es de naturaleza malintencionada. Éstos ocurren como acontecimientos anómalos de una sola vez o en una manera bastante infrecuente para ser explicados simplemente en incidencias cerradas.

Otras veces se nota que el mismo evento desencadena con bastante frecuencia que se abren y se cierran varios incidentes para el mismo o similar evento (s). Múltiples alertas FPA que ocurren reducen la productividad de los analistas y proporcionan "ruido" innecesario en nuestra infraestructura y en nuestras herramientas de monitoreo.

Tales eventos frecuentes y verificados deben ser excluidos de nuestras reglas correlacionadas. Hay varias formas de hacerlo: se puede modificar un dispositivo cliente para eliminar el problema que causa la coincidencia de correlación, ya que no debemos examinar nuestros propios controles para excluir estas alertas. Otros elementos como los dispositivos de red (DC, Proxy, switches, ID’s de nube) simplemente están conduciendo el tráfico que no genera y debe ser eliminado.

Algunas opciones incluyen agregarlos a filtros de exclusión existentes, modificar los propios disparadores de correlación, modificar la configuración de los dispositivos de infraestructura. El proceso mediante el cual se hace esto se conoce como " Tuning". Tuning hace posible enfocarse en alertas positivas verdaderas (TPA) mientras que elimina el ruido (FPA) de nuestro sistema de detección de la intrusión (IDS), al igual que afinar una estación de radio para conseguir la alimentación más clara posible sin estática.

2.11.2 Desafíos análisis de los Log

La computación en nube se utiliza cada vez más para implementar y ejecutar servicios de usuario, también conocidos como software como servicio (SaaS).

La ejecución de cualquier aplicación requiere información sobre cada capa de infraestructura por razones técnicas, de seguridad y comerciales. En esta sección se describen algunos de estos problemas y casos de uso que pueden beneficiarse del análisis y la gestión del registro. Si observamos el ciclo de vida de desarrollo de software, los casos de uso se presentan en el siguiente orden:

• Depuración y forense

• Supervisión de fallos

• Solución de problemas

• Uso de funciones

• Supervisión del rendimiento

• Detección de seguridad / incidentes

• Cumplimiento normativo y normativo

Cada uno de estos casos de uso puede aprovechar el análisis de log para resolver completamente o al menos ayudar a acelerar drásticamente y simplificar la solución al caso de uso.

2.11.3 Administración de Log

La resolución de los problemas de registro de la nube descritos en la última sección requiere una solución o arquitectura de administración de registros para admitir la siguiente lista de características:

• Centralización de todos los registros

• Almacenamiento de registros escalable

• Rápido acceso y recuperación de datos

• Soporte para cualquier formato de registro

• Ejecución de trabajos de análisis de datos

• Retención de registros de registro

• Archivado de troncos antiguos y restauración bajo demanda

• Acceso a datos segregados mediante control de acceso

• Preservación de la integridad del registro

• Rastro de auditoría para el acceso a registros

Estos requisitos coinciden con los desafíos definidos en la última sección. Sin embargo, no abordan los últimos tres desafíos de los registros de registro no identificados y no normalizados.

2.11.4 Directrices de log

Para abordar los desafíos relacionados con la información en los registros de registro, se necesita establecer un conjunto de directrices y tener las propias aplicaciones instrumentadas para seguir estas pautas. Estas directrices se desarrollaron sobre la base de las normas existentes de explotación y la investigación realizada en varias empresas de gestión de registros.

Cuándo registrar ¿Cuándo las aplicaciones generan registros? Tomar la decisión de cuándo escribir registros de registro debe ser impulsado por los casos de uso. Estos casos de uso en aplicaciones de nube surgen en cuatro áreas:

- Registro pertinente de negocios
- Registro basado en operaciones
- Registro relacionado con la seguridad (forense)
- Mandatos reglamentarios y normativos

Como regla general, en cada llamada de retorno en una aplicación, el estado se debe registrar, si fue exitoso o fue un fracaso. De esta manera se registran los errores y se puede rastrear la actividad en toda la aplicación.

2.11.4.1 Negocios

El registro relevante de negocios cubre las características utilizadas y las métricas de negocio que se están siguiendo. Las funciones de seguimiento en una aplicación en la nube son cruciales para la gestión de productos. Ayuda no sólo a determinar qué características se utilizan actualmente, sino que también

se puede utilizar para tomar decisiones informadas sobre la dirección futura del producto. Se describen otras métricas empresariales que se desean al iniciar sesión en una aplicación en la nube. Los acuerdos se deben de dar a nivel de servicio de supervisión (SLA)

Aunque algunas de las métricas son más de origen operacional, como latencias de aplicaciones.

2.11.4.2 Operacionales

El registro operacional debe implementarse para las siguientes instancias:

- Los errores son problemas que afectan a un solo usuario de aplicación y no a toda la plataforma.
- Las condiciones críticas son situaciones que afectan a todos los usuarios de la aplicación. Exigen atención inmediata.
- El sistema y la aplicación inician, detienen y reinician. Cada uno de estos eventos podría indicar un posible problema. Siempre hay una razón por la que una máquina se detuvo o se reinició.
- Cambios en los problemas de seguimiento de objetos y cambios de atributos en una actividad. Los objetos son entidades en la aplicación, como usuarios, facturas o mercancías. Otros ejemplos de cambios que deben registrarse son:

  - Instalación de una nueva aplicación (generalmente registrada en el nivel del sistema operativo).
  - Cambio de configuración.

- Las actualizaciones de código de programa de registro permiten la atribución de cambios a los desarrolladores.
- Las ejecuciones de copia de seguridad deben registrarse para auditar copias de seguridad con éxito o fallidas.
- Auditoría del acceso al registro (especialmente los intentos de cambio).

2.11.4.3 Seguridad

El registro de seguridad en la aplicación en la nube se refiere a la autenticación y autorización, así como al soporte forense. Además de estos tres casos, las herramientas de seguridad (por ejemplo, el sistema de detección o prevención de intrusiones o las herramientas antivirus) registrarán todo tipo de otros problemas relacionados con la seguridad, como intentos de ataques o la detección de virus en un sistema.

Las aplicaciones en la nube deben centrarse en los siguientes casos de uso:

- Inicio de sesión / cierre de sesión (local y remoto)
- Cambios de contraseña / cambios de autorización
- Acceso de recursos fallido (autorización denegada)
- Toda la actividad ejecutada por una cuenta privilegiada

Las cuentas privilegiadas, administradores o usuarios root son los que tienen control de un sistema o aplicación. Tienen privilegios para cambiar la mayoría de los parámetros en la aplicación. Por lo tanto, es crucial para fines de seguridad para supervisar muy de cerca lo que estas cuentas están haciendo.

2.11.4.4 Cumplimiento

El cumplimiento y las demandas regulatorias son un grupo más de casos de uso que demandan. La diferencia de los otros casos de uso es que a menudo es requerido por la ley o por socios de negocios para cumplir con estas regulaciones. Por ejemplo, el estándar de seguridad de datos de la industria de tarjetas de pago exige un conjunto de acciones con respecto al registro. La parte interesante sobre él es que exige que alguien revise los registros y no sólo que se generen. Tenga en cuenta que la mayoría de los reglamentos y normas cubrirán los casos de uso. Por ejemplo, la actividad privilegiada de registro es una parte central de cualquier esfuerzo de registro reglamentario.

2.11.5 Que hacer con los registros

Ahora dejando los casos de uso de alto nivel y la configuración de la infraestructura para en los registros individuales. ¿Qué se debe tener un registro individual?

Como mínimo, los siguientes campos deben estar presentes en cada registro: Timestamp, Application, User, Session ID, Severity, Reason, Categorization. Estos campos ayudan a responder a las preguntas: cuándo, qué, quién, y por qué. Además, son responsables de proporcionar toda la información exigida por nuestros casos de uso.

Una marca de tiempo es necesaria para identificar cuándo ocurrió un registro de registro o el evento registrado. Las marcas de tiempo se registran en

un formato estándar. El campo de aplicación identifica al productor de la entrada de registro. Un campo de usuario es necesario para identificar qué usuario ha activado una actividad. Utilice nombres de usuario o ID únicos para distinguirlos a los usuarios entre sí. Un identificador de sesión ayuda a rastrear una sola solicitud en diferentes aplicaciones y niveles. El desafío es compartir el mismo ID en todos los componentes. Se registra una gravedad para filtrar registros en función de su importancia. Es necesario establecer un sistema de gravedad, por ejemplo: depuración, información, advertencia, error y criterio. El mismo esquema debe utilizarse en todas las aplicaciones y niveles. Una razón es a menudo necesaria para identificar por qué algo ha sucedido. Por ejemplo, se denegó el acceso debido a privilegios insuficientes o una contraseña incorrecta. La razón identifica por qué. Como un último conjunto de campos obligatorios de campo, categoría o taxonomía deben ser registradas.

La categorización es un método comúnmente utilizado para aumentar la información en los registros de registros para permitir el abordaje de eventos similares de una manera común. Esto es muy útil en por ejemplo, en la presentación de informes. Piense en un informe que muestre todos los inicios de sesión fallidos. Se podría intentar construir un patrón de búsqueda realmente complicado que encuentre sucesos de inicio de sesión fallidos en todo tipo de aplicaciones diferentes o se podría usar un campo de categoría común para tratar todos esos registros.

2.12 SIEM (Información de seguridad y administración de eventos)

En los entornos de red de computadoras de hoy se producen enormes cantidades de datos de registro de seguridad. Para manejar estos datos y proporcionar un mayor nivel de seguridad de la información y administración y análisis de registros centralizados, se pueden utilizar sistemas de información de seguridad y gestión de eventos (o SIEMs). Los SIEMs pueden ayudar a organizaciones a luchar con las diversas regulaciones de cumplimiento que existen y reducir el riesgo de intrusiones en la red. Los SIEM recogen y agregan datos de registro de dispositivos y aplicaciones a través de software llamados agentes, filtran datos poco interesantes y normalizan a un formato propietario, analizan mediante correlación utilizando información contextual y alertan a los administradores en caso de ataque. Los datos de registro se almacenan utilizando mecanismos de seguridad especiales en los llamados medios de escritura una vez leídos, por razones de cumplimiento. Se presta especial atención a la seguridad en la fuente del registro.

Una visión general del mercado se detalla cómo son las sugerencias sobre cómo organizar el entorno en torno a la SIEM y qué datos de registro son dignos de análisis. Se pronostica que el cumplimiento continuará siendo el motivador más importante para la adquisición de SIEM. Se prevé que la usabilidad y la escalabilidad aumentarán a medida que el mercado continúe creciendo rápidamente y la normalización se convertirá en un factor clave. Se prestará más atención a la incorporación de información contextual en el proceso de análisis, especialmente para la gestión de la identidad y el acceso. Los tipos de fuentes de registro admitidos aumentarán en número y

desarrollarán capacidades de respuesta automatizadas orientadas a las políticas.

Los sistemas de información de seguridad y gestión de eventos son sistemas que proporcionan un manejo centralizado de registros, mediante la recolección de registros (principalmente los relacionados con la seguridad) de diversos dispositivos y aplicaciones de una red, así como el análisis y almacenamiento de estos registros. Si el sistema detecta un ataque, puede reaccionar a través de sus canales de gestión de incidentes, que incluyen alertar al personal e incluso iniciar medidas contrarias. Un SIEM también puede ayudar a una organización a cumplir con las regulaciones relativas a la retención de datos y este último puede ser útil en casos de re-descubrimiento y forense. El sistema también puede, en cierta medida, ayudar con el diagnóstico de red. Otros casos de uso incluyen monitoreo de usuarios y políticas y administración de identidades.

2.12.1 Funcionamiento de los SIEM’s

Por supuesto, es importante entender cómo funcionan los SIEM. Naturalmente hay diferencias entre diferentes SIEM de diferentes proveedores, pero hay algunas partes / conceptos generales que siguen siendo los mismos. Las partes fundamentales de un SIEM se describen por recogida, análisis / agregación y retención. Los datos de registro se recopilan de las diversas fuentes y, puesto que hay tantos formatos diferentes de los datos, primero se agregan (de los varios dispositivos) y después normalizan generalmente en un formato propietario. Este proceso se conoce como consolidación. Los datos se

analizan mediante la agregación de datos de los diferentes dispositivos y se correlacionan mediante la agrupación de diferentes partes de un ataque en una imagen completa. En esta etapa, la información contextual sobre el entorno de red y las amenazas comunes es muy útil. Las alertas y los informes se generan como una salida del análisis. Por lo general, los datos de registro se almacenan en línea en el SIEM durante unas pocas horas después de lo cual se trasladan a un archivo, por ejemplo, para cumplir con las normativas y para guardar datos que pueden ser importantes para la detección forense. Esta funcionalidad también puede expresarse como "cinco Cs":

- Colección
- Consolidación
- Correlación
- Comunicación
- Control

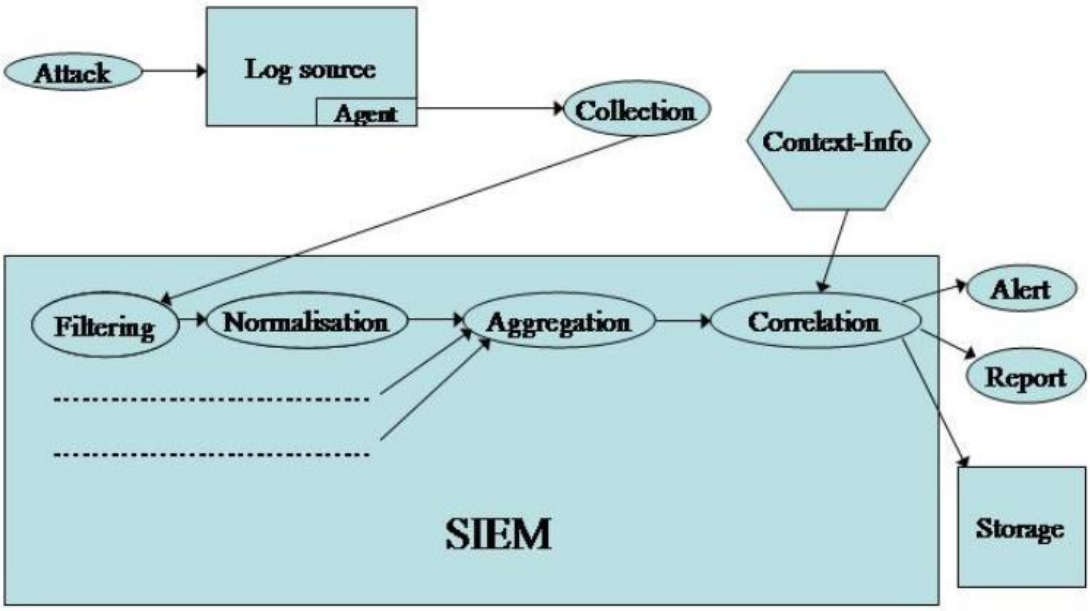

FIGURA 8: FUNCIONAMIENTO Y RECOLECCIÓN DE LOGS DE UN SIEM

2.12.2 Colección

Los SIEM recogen datos de registro de una gran cantidad (típicamente docenas o cientos) de diferentes tipos de dispositivos. El transporte de la fuente del registro al SIEM puede ser necesario para ser confidencial, autenticado (para proteger contra registros falsos) y confiable. Los protocolos diferentes para la colección incluyen syslog (existen versiones confiables y encriptadas y no seguras), SNMP, SFTP, IDXP y OPSEC (un estándar Checkpoint). Para fuentes de registro que no admiten estos protocolos de colección estándar o relacionada. Se trata de una pieza de software instalada en la fuente de registro que traduce (normaliza) los datos de registro de origen a un formato que el SIEM entiende. El uso de agentes suele significar tiempos de despliegue más largos para el producto, aunque también podrían usarse para la normalización y otros

pretratamientos para distribuir el trabajo. La mayoría de los productos necesitan usar agentes para los registros de eventos de Windows y uno de los agentes más utilizados es Snare (anteriormente conocido como Backlog) por Intersect Alliance, que se traduce en syslog y se utiliza incluso en los productos SIEM por los competidores de Snare.

Existen dos enfoques diferentes para la recolección el SIEM decide cuándo debe ocurrir la recolección o el sistema de origen. El primero, denominado pull, significa que el SIEM inicia sesión en el dispositivo o agente fuente y extrae los registros mientras que el último, llamado push, tiene la fuente / agente a transferir los registros al SIEM a su conveniencia. Por supuesto "pull" significa que el SIEM está más en control (y de hecho tiene algún tipo de acceso a cada dispositivo de registro) y por lo tanto más importante. Por supuesto, el enfoque centralizado significa que se necesita más poder de procesamiento en el SIEM. Cuando los datos de registro se deben recopilar depende de si el análisis en tiempo real y las alertas son necesarias. Si no, entonces la mejor idea puede ser transmitir sólo cuando la red no está demasiado ocupado.

Dependiendo de lo que el SIEM se va a utilizar para que no puede ser esencial para recoger todos los datos de registro. En su lugar, algunos datos "poco interesantes" pueden ser filtrados cuando se recopilan (o de hecho no se generan en absoluto) para reducir las demandas de ancho de banda de red, almacenamiento y potencia de procesamiento SIEM. Esto significa un menor costo (de hecho, los dos indicadores de precios más importantes son el número de dispositivos para recopilar y el número de eventos por segundo o EPS) y menos riesgo de ataques de denegación de servicio. Por supuesto, no siempre

es obvio en ese momento lo que constituye datos interesantes y poco interesante ya que estos últimos pueden parecer de repente muy interesantes después de los procesos de agregación y correlación.

Si el SIEM se utiliza para adherirse a ciertas regulaciones o leyes no puede ser una opción para no recoger todos los datos e incluso si ninguna regla actual lo exige. Normalmente hay algunas restricciones sobre las fuentes de registro con las que el SIEM se comunicará, para evitar que los atacantes agreguen entradas de registro falsas (por ejemplo, un atacante agrega un dispositivo que genera registros que el SIEM recopilará), lo cual podría ser problemático por varias razones (por ejemplo, introducir cifras fiscales defectuosas, etc.), algunos SIEM impiden el registro de dispositivos conectados sin un procedimiento especial. Por supuesto, esto puede ser un problema en el caso de dispositivos "benevolentes" extraíbles como discos USB y dispositivos DHCP (que reciben direcciones IP dinámicamente y por lo tanto parecen ser dispositivos diferentes para SIEMs que asignan identidad en una base IP) que a menudo se desconectan y vuelven a conectar.

2.12.3 Consolidación o normalización y agregación

Con muchos tipos de formatos de registro, la mayoría de los SIEM normalizan los datos a un formato propietario. Para problemas de interoperabilidad idealmente este es un formato estándar, pero normalmente no es este el caso. Por lo general, la diversidad de los formatos de origen significa que una gran cantidad de datos normalizados se incluirán en un encabezado general como un etiquetado algo como "misceláneo" o "cadena", que puede no

ser muy útil para fines de búsqueda. Es importante tener en cuenta que para el cumplimiento puede ser importante almacenar los datos en su forma original. Si bien es importante normalizar, entre otras cosas, la fecha y la hora de los datos de registro, también es vital asegurarse de que el tiempo es correcto en relación con un reloj común. Normalmente, la normalización temporal de este tipo utiliza un método como el proporcionado por el Network Time Protocol o NTP.

Después de la normalización, el proceso de agregación comienza. Su propósito es reunir diferentes eventos que son del mismo tipo para ayudar a ver los datos de registro como menos separados y más relacionados. Esto es similar a la correlación que sin embargo reúne diferentes piezas (diferentes tipos de eventos) de un ataque. Dado que los procesos son bastante parecidos, existe cierta confusión sobre la terminología correcta en la literatura. Las definiciones utilizadas aquí son como el término de "colación" en la importancia de la agregación que se ilustra mejor con un ejemplo: Hay varios mensajes de registro que pueden ser indicadores de intentos de intrusión y / u otros problemas de seguridad. Por ejemplo, es una buena idea supervisar los inicios de sesión que tienen lugar muy temprano en la mañana o tarde en la noche o los fines de semana, cuando normalmente nadie estaría conectado. Además, un agregado de mensajes puede mostrar cosas que las distintas no pueden. Por ejemplo, un atacante malicioso que intenta acceder a la cuenta de un usuario específico puede intentar adivinar la contraseña. Dado que los inicios de sesión fallidos son normales (la falta de ortografía de la contraseña es común ya que las contraseñas correctas contienen muchos caracteres especiales y caracteres mixtos), los mensajes de registro no son suficientes por separado. En su lugar,

muchos intentos fallidos de inicio de sesión en rápida sucesión tienen más probabilidades de ser intentos de intrusión. Por supuesto expertos atacantes saben todo esto y tratarán de extender sus intentos lo suficiente para engañar a los mecanismos de detección de intrusiones en su lugar. Como siempre hay una batalla constante y hay que tener en cuenta que la seguridad es un proceso y no un producto.

2.12.4 Correlación e información contextual

En el proceso de correlación se juntan diferentes eventos de registro (de diferentes tipos) para formar un ataque o incidente (a veces la entrada de palabra se utiliza para una pieza no correlacionada de datos de registro mientras que el evento se reserva para datos correlacionados). Este proceso es muy avanzado y requiere un procesamiento intensivo, ya que debe entender qué ataque n es (y no es) lo que normalmente se logra mediante la descarga de información de amenazas de bases de datos en línea y el uso de información contextual (una base de conocimientos) para entender el entorno de red específico a una menor o mayor extensión. Esta información puede incluir directorios de usuario y prioridad y ubicación del dispositivo (lógica o incluso física). Esto se puede utilizar potencialmente para asignar dispositivos para mediar el problema de DHCP como se describió anteriormente. Idealmente el SIEM también puede aprender de los eventos en los que recibe datos y actualizar la información contextual. Por supuesto, esto significa más sobrecarga computacional. Idealmente debería incorporarse al SIEM y actualizarse

automáticamente cuando, por ejemplo, se haya realizado una nueva exploración de vulnerabilidades.

Hay varias maneras de juzgar si algo constituye un ataque o no y cuán grave es. Dos enfoques comúnmente utilizados en IDSs son la detección basada en anomalías (ABD) de un ataque y la detección de mal uso (o firma) (MBD). El primero reacciona en cualquier cosa que no se especifica como comportamiento "bueno" mientras que el último reacciona cuando ocurre algo conocido para ser malo. ABD obviamente requiere mucha escritura de política y, por lo tanto, muy probablemente reaccionará en algún buen comportamiento (porque ese tipo de comportamiento se olvidó al escribir la política). Sin embargo, puede detectar el abuso de privilegios, las desviaciones de los patrones de uso normales y los ataques internos (los internos tienen más acceso y conocimiento y por lo tanto, no requieren vulnerabilidades de "firma" bien conocidas en su ataque) y es realmente el modo más duro de seguridad default deny.

2.12.5 Comunicación o Alerta / Reporte

Hay tres maneras en que los administradores son informados por el SIEM que los ataques o comportamiento extraño están tomando o han tenido lugar. El SIEM envía una alerta tan pronto como se da cuenta de que algo está mal, o envía un informe en un tiempo predeterminado. La tercera opción es, por supuesto, que el administrador esté monitoreando activamente el SIEM en tiempo real (normalmente a través de una interfaz gráfica de usuario basada en web que admita diferentes funciones de cuenta de usuario). Puede parecer extraño que las alertas de ataques (es decir, intrusiones) no se dejan a los IDSs,

pero un SIEM es obviamente más inteligente, dando una menor tasa de falsos positivos, y puede capturar las cosas que un IDS no (y ya que los registros son generados por otros tipos De los dispositivos también el SIEM también atrapará algo que un IDS simplemente no puede). Por supuesto, las alertas deben contener la información necesaria para acciones ulteriores o corren el riesgo de ser simplemente ignoradas.

Algunos productos SIEM pueden incluso tomar acciones protectoras (reactivas) (como eliminar software malicioso, cerrar puertos) a través de los dispositivos conectados. Por supuesto, esto requiere que el SIEM esté en control de los dispositivos y no sólo un dispositivo de escucha pasivo, lo que significa que es un nodo aún más importante en la arquitectura. Esto también significa que no es sólo un producto de seguridad sino también una gestión de red. Este tipo de remediación aún no está muy bien implementado en SIEMs.

Los informes suelen ser programados para ser generados regularmente, pero también se pueden hacer sobre la marcha. Normalmente hay cientos de informes de plantillas para las necesidades estándar que aceleran enormemente el despliegue del SIEM. Un informe típico detalla la actividad de inicio de sesión de la noche anterior (cuando es probable que no haya mucha actividad) y la mayoría de los productos SIEM proporcionan visualizaciones de estadísticas comunes. Estos tipos de informes son ideales para una visión general rápida para un administrador y perfecto para la gestión.

De acuerdo con algunos investigadores SIEMs no son muy útiles si no son constantemente monitoreados, aunque con productos en evolución (tienen más casos de uso que simplemente monitoreo de eventos en tiempo real) estas

opiniones pueden cambiar. Aunque se tiene razón de que todavía tenemos problemas con virus a pesar de software anti-virus sin duda tendríamos muchos más sin él y lo mismo es cierto para SIEMs. Dado que la supervisión en tiempo real "requiere cinco empleados a tiempo completo" o incluso más, lo más probable es que no sea rentable utilizar SIEMs. También significa que la externalización del monitoreo del SIEM sería una decisión acertada, pero esto es dudoso, ya que la información del contexto (como el conocimiento específico de la empresa) se extrañaría. También se pide herramientas más simples, una llamada que parece haber sido oída por los vendedores de estos sistemas.

2.12.6 Control o almacenamiento

Mientras se analiza, los datos se almacenan normalmente en línea y cuando ya no se necesitan, normalmente se archivan. Los datos pueden ser almacenados normalizados (y agregados) para acelerar las cosas cuando se utiliza de nuevo, pero debe ser almacenado en forma más o menos original (datos en bruto) si se utiliza como prueba legal o cumplimiento. Por lo general, los datos se almacenan en forma comprimida y posiblemente encriptada, pero ya que esto significa un poco menos de seguridad (las claves de cifrado se pueden perder, la compresión de corrupción). Por lo general, el almacenamiento de los aparatos SIEM está en el rango TB, permitiendo el almacenamiento de hasta miles de millones de eventos de acuerdo con netForensics, un proveedor SIEM. Uno podría optar por mantener datos más interesantes en línea más de datos menos interesantes. Dado que enormes cantidades de datos suelen estar

involucrados, es muy importante utilizar una buena indexación y administración para el almacenamiento en línea.

2.13 Riesgos del Cloud Computing

El proceso de crear y administrar un espacio de nube seguro es una tarea más desafiante que crear un entorno de TI clásico y seguro. Dada la inmadurez de esta tecnología, los nuevos recursos y la reasignación de los tradicionales no están totalmente probados y vienen con nuevos riesgos que aún están bajo investigación. Los principales riesgos de la adopción de cloud computing identificados en esta propuesta se explican a continuación:

2.13.1 Malentendido con las políticas y responsabilidades.

En el escenario de cloud computing, las responsabilidades se dividen entre los dos actores: el proveedor de la nube y el cliente. Existe un tremendo potencial para decisiones equivocadas de gestión de riesgos si los proveedores de la nube no revelan hasta qué punto se implementan los controles de seguridad y el consumidor sabe qué controles son necesarios para ser adoptados. Diferentes tipos de servicios en la nube adoptados significan diferentes responsabilidades para el proveedor de servicios y el cliente.

Si se adopta un modelo de servicio IaaS, el proveedor es responsable de la seguridad física, la seguridad del entorno y la seguridad del software de virtualización, mientras que el consumidor es responsable de asegurar todo lo demás por encima de esta capa, incluyendo el sistema operativo, las aplicaciones y los datos.

Sin embargo, en un modelo de servicio en la nube SaaS, el proveedor es responsable no sólo de la seguridad física y ambiental sino también de todos los servicios de software que utiliza para proporcionar ese servicio de particular al cliente. En este caso, las responsabilidades del consumidor en el ámbito de la seguridad se reducen mucho.

2.13.2 Seguridad de los datos y problemas de confidencialidad

Una de las mayores preocupaciones de seguridad que tiene la gente al pasar a la nube está relacionada con el problema de mantener los datos seguros y confidenciales. A este respecto, surgen algunos problemas particulares: quién puede crear datos, dónde se almacenan los datos, quién puede acceder y modificar datos, qué sucede cuando se borran los datos, cómo se realiza la copia de seguridad, cómo se realiza la transferencia de datos, etc. Todo esto se conoce como ciclo de vida de seguridad de datos.

Este ciclo de vida existe también en la arquitectura clásica, pero en un entorno de nube, sus etapas son mucho más complejas, lo que plantea mayores riesgos de seguridad y requiere una gestión más cuidadosa. Vale la pena recordar a este respecto que es mucho más difícil para el cliente de nube, para comprobar eficazmente las prácticas de manejo de datos del proveedor de la nube y, por tanto, hay que asegurarse de que los datos se manejan de una manera adecuada.

Para contrarrestar este riesgo, se proponen a los clientes estrategias como encriptación de datos, infraestructura particular de clave pública,

dispersión de datos, estandarización de API, etc. como medidas de seguridad para crear un entorno de confianza y seguro.

2.13.3 Falta de normas

La inmadurez de esta tecnología dificulta el desarrollo de un conjunto completo y comúnmente aceptado de estándares. Como resultado, se establecieron muchas organizaciones de desarrollo estándar para investigar y desarrollar las especificaciones. Organizaciones como Cloud Security Alliance, Agencia Europea de Seguridad de Redes y de Información, Cloud Standards Customer Council, etc. han desarrollado normas y recomendaciones sobre mejores prácticas. Otros establecimientos, como el Grupo de Trabajo de Gestión Distribuida, el Instituto Europeo de Normas de Telecomunicaciones, el Open Grid Forum, el Open Cloud Consortium, el Instituto Nacional de Estándares y Tecnología, la Asociación de la Industria de Redes de Almacenamiento, etc. centraron su actividad en el desarrollo de normas de trabajo para diferentes aspectos de la tecnología de la nube.

La emoción en torno a la nube ha creado una ráfaga de estándares y la actividad de código abierto que conduce a la confusión del mercado. Es por eso que ciertos grupos de trabajo como Cloud Standards Coordination, TM Forum, etc. actúan para mejorar la colaboración, la coordinación, la información y el intercambio de recursos entre las organizaciones que actúan en este campo de investigación.

2.13.4 Problemas de interoperabilidad

La tecnología de cloud computing ofrece un grado de escalabilidad de recursos que nunca se ha alcanzado antes. Las empresas pueden beneficiarse de necesidades computacionales adicionales, espacio de almacenamiento, asignación de ancho de banda, etc. siempre que lo necesiten y sin grandes inversiones para soportar demandas de pico de carga. Si la demanda cae, la capacidad adicional se puede cerrar tan rápidamente como se amplió sin ningún equipo de hardware sentado inactivo.

Esta gran ventaja también tiene un inconveniente importante. Viene junto con el riesgo de administrar datos en un entorno compartido (computación, almacenamiento y red) con otros clientes de la nube. Además, al mismo tiempo una empresa puede tener múltiples proveedores de nube para diferentes servicios que tienen que ser interoperables. Con el tiempo, por diferentes razones, las empresas pueden decidir trasladar sus servicios a otra nube y, en tal caso, la falta de interoperabilidad puede bloquear o plantear grandes obstáculos a tal proceso.

Los proveedores de la nube pueden encontrar atractivo el sistema de bloqueo del cliente, pero para los clientes los problemas de interoperabilidad significan que son vulnerables a los aumentos de precios, la calidad de los servicios que no satisfacen sus necesidades, el cierre de uno o más servicios en la nube, con el proveedor de la misma.

2.13.5 Fallas de fiabilidad

Otro aspecto importante del cloud computing es la confiabilidad o disponibilidad de servicios. El desglose de un servicio esencial que opera en una nube tiene un impacto en muchos clientes. Por ejemplo, en abril de 2012 hubo una interrupción de Gmail que hizo que los servicios de Gmail no estuvieran disponibles durante casi 1 hora. La empresa dijo por primera vez que afectó a menos del 2% de sus clientes, luego se actualizó al 10%, lo que suma alrededor de 35 millones de clientes de un total de 350 millones de usuarios.

Estos incidentes no son raros y evidencian la falta de control del cliente sobre sus datos. La ironía es que, en términos de fiabilidad, los proveedores de la nube han establecido altos estándares que rara vez se logran en un entorno interno. Sin embargo, debido a que estas interrupciones afectan a un gran número de consumidores, lanzan dudas en la mente de los responsables de TI sobre la viabilidad de reemplazar la funcionalidad de escritorio con la funcionalidad ofrecida por la nube.

Además, en esta industria, las empresas líderes han establecido algunos servicios de calidad de alto nivel. Esos niveles no son fáciles de alcanzar por los otros proveedores de servicios en la nube que no cuentan con una infraestructura tan bien desarrollada.

Desafortunadamente para los clientes estos servicios de calidad pueden llegar a costos más altos y a veces los tomadores de decisiones, atraídos por los servicios más baratos, serán renuentes a colaborar con tal proveedor.

2.13.6 Intruso malicioso

Una persona malintencionada es una persona motivada para crear un impacto negativo en la misión de la organización al tomar medidas que comprometen la confidencialidad, integridad y / o disponibilidad de la información. Cuando los datos sensibles se procesan fuera de la empresa, los gerentes de la organización son menos conscientes de la naturaleza y el nivel de riesgo y no poseen capacidad rápida y directa para controlar y contrarrestar estos riesgos.

Expertos en seguridad están muy conscientes de la relación inversa entre lealtad y riesgo. Incluso si los empleados de la empresa de confianza pueden cometer errores o cometer fraude y los forasteros no son automáticamente menos éticos que ellos, es prudente invertir en los empleados a largo plazo de la empresa con mayor confianza.

Las actividades maliciosas de un miembro de la red podrían tener un impacto en: la confidencialidad, integridad y disponibilidad de todo tipo de datos y servicios con impacto en las actividades internas, la reputación de la organización y la confianza del cliente. Esto es especialmente importante en el caso del cloud computing debido al hecho de que las arquitecturas en la nube requieren ciertas funciones, como los administradores de la nube, los auditores de la nube, el personal de seguridad de la nube, que son extremadamente de alto riesgo.

Capítulo 3 Marco Metodológico

3.1 Tipo de Investigación

La investigación que se llevó a cabo es de tipo evaluativo, ya que brinda una visión general de tipo aproximativo, respecto a una determinada realidad en las tecnologías de la nube existentes, así como de las implementaciones existentes, por tanto, no se requiere la formulación de una hipótesis.

Durante el desarrollo de esta investigación se describirán de manera profunda las tecnologías de la nube, sus aplicaciones prácticas, sus ventajas y desventajas, así como el tipo de que se utiliza para proteger la información de los usuarios de dicho servicio, basados plenamente con la descripción de sistemas a terceros para realizar satisfactoriamente la obtención de los logs y pos su consiguiente monitoreo.

3.2 Alcance Investigativo

El alcance investigativo de este documento combina las fases de exploración y descripción de las tecnologías de la computación en la nube, en donde se procederá a agrupar conocimiento para facilitar el cumplimiento de los objetivos.

Según muchos analistas en el área de tecnologías de la información, la seguridad y la computación en nube son temas candentes para la mayoría de las empresas. Las empresas necesitan el almacenamiento de datos, el software de procesamiento, la infraestructura y el marco bajo demanda y sin grandes inversiones en hardware / software. Cada organización quiere obtener más beneficios de esta nueva forma de entregar los recursos informáticos. Muchas

empresas, principalmente pequeñas y medianas empresas (PYME), están considerando migrar a servicios de cloud computing.

La computación en nube es un concepto que se ha vuelto cada vez más popular en los últimos años a través de un aumento en las capacidades de conexión a Internet, posibilidades de virtualización y éxito comercial. Ofrece funcionalidades a través de la red de telecomunicaciones en forma de servicios y no como un producto entregado. Esto en combinación con que el usuario es agnóstico a la tecnología subyacente ofrece ventajas como el aumento de flexibilidad en la solución técnica y el modelo de pago, robustez y disponibilidad, así como la seguridad en tamaño. La desventaja del cloud computing es que tenga dependencia de la conexión a internet, la pérdida de control sobre los datos y el riesgo de bloqueo del proveedor.

Estas ventajas y desventajas hacen que la decisión entre un recurso on-premise y un servicio de cloud computing sea compleja. Esta investigación de acción basada en casos tiene como objetivo proporcionar a los investigadores y personal de TI, como administradores, arquitectos y diseñadores, herramientas y directrices para reducir la complejidad de la decisión. Se realiza mediante una presentación de una solución arquitectónica que tiene la facultad de potenciar los beneficios de la computación en nube, la construcción de una tarjeta de evaluación que indica si un sistema es adecuado para cloud computing o no y mediante la identificación de posibles alternativas de cloud computing a los sistemas indicados.

A través de un estudio de literatura se muestra cómo los principios de Service Oriented Arquitectura (SOA) pueden mejorar la integración y fortalecer los

beneficios de la Informática. El estudio de la literatura junto con entrevistas cualitativas y discusiones con la empresa cliente también produce pautas junto con requisitos para sistemas de computación en nube alternativos.

Capítulo 4 Análisis del Diagnostico

4.1 Análisis para definir las fuentes de los logs en la nube cruzada.

La colección de los registros es el corazón y el alma de un SIEM. Cuantas más fuentes de registro envíen registros al SIEM, más se puede lograr con el SIEM. Su red genera grandes cantidades de datos de registro por ejemplo la infraestructura de una empresa puede generar un aproximado de 10 Terabytes de datos de registro de texto sin formato por mes y usted, como analista, puede quejarse de esta realidad, ya que es demasiada información.

Los registros son la clave para entender "¿Quién nos está atacando hoy?" Y "¿Cómo obtuvieron acceso a todos nuestros secretos empresariales?". Aunque pensamos que los controles de seguridad contienen toda la información que necesitamos para garantizar la seguridad, solo contienen las cosas que han detectado, no hay un contexto de "antes y después del evento" dentro de ellas. Sin embargo, este contexto suele ser vital para permitirle separar los falsos positivos de la detección verdadera. El contexto es la diferencia entre detectar un ataque real, en lugar de perseguir un sistema meramente desconfigurado.

Los ataques exitosos contra los sistemas informáticos rara vez se ven como ataques reales, excepto en retrospectiva: si este no fuera el caso, podríamos automatizar todas las defensas de seguridad y no requerir analistas humanos. Además, los atacantes pueden intentar eliminar y falsificar entradas

de registro para cubrir sus pistas. Por esta razón, tener una fuente protegida de información de registro en la que se pueda confiar es vital para cualquier procedimiento legal por uso incorrecto de la computadora.

Se necesitaran los registros de los componentes críticos de su red y su empresa. Seguramente se necesitarán los registros de tu firewall. También necesitarán registros de sus servidores de claves, especialmente su servidor de Active Directory y su aplicación clave y servidores de base de datos. También los registros de tu IDS y antivirus.

Se debe pensar cuáles son los elementos clave de su red, desde el punto de vista comercial. Piense en las partes de su infraestructura que son cruciales para el funcionamiento del negocio. Los registros que esos componentes generan son las claves para mantener su red activa y la empresa en funcionamiento.

Especialmente para una compañía pequeña / mediana, es importante decidir qué es importante que esté observando, ya que es probable que tenga recursos limitados asignados a la tarea de monitoreo de seguridad. No se puede contratar suficientes personas para leer cada línea de esos registros en busca de cosas malas. Incluso si se tuviera éxito, los analistas estarían tan aburridos que nunca verían nada, aunque estuviera justo frente a su cara.

Así que aquí están los registros que debe tener en cuenta para su inclusión en su situación:

1- Registros de sus controles de seguridad:

- IDS

- Endpoint Security (Antivirus, antimalware)
- Prevención de pérdida de datos
- Concentradores VPN
- Filtros web
- Honeypots
- Firewalls

2- Registros desde su infraestructura de red:

- Routers
- Switches
- Domain Controllers
- Wireless Access Points
- Application Servers
- Databases
- Intranet Applications

3- Información de infraestructura no registrada

- Configuration
- Locations
- Owners
- Network Maps
- Vulnerability Reports
- Software Inventory

4- Mapeos de procesos de negocios

- Business Process Mappings

- Points of Contact
- Partner Information

Sería de mucha ayuda que cada sistema operativo y cada aplicación en el mundo grabaran sus eventos de registro en el mismo formato. Por desgracia, no lo hacen. La mayoría de los registros están escritos para ser legibles para los humanos, no para las computadoras. Por lo tanto, cuando escuchemos hablar sobre un SIEM sobre "cuántos dispositivos admite", están hablando sobre cuántos dispositivos puede analizar y normalizar. Esto lleva los registros de lo humano a lo comprensible, a lo que se entiende por máquina, por lo que el SIEM puede entender y trabajar con los registros de muchas fuentes dispares.

Desglosar esos registros de muchas fuentes en sus componentes, o normalizarlos, es lo que permite al SIEM buscar entre los registros de múltiples dispositivos y correlacionar los eventos entre ellos. Una vez que hemos normalizado los registros en una tabla de base de datos, podemos hacer búsquedas de estilo de base de datos.

Esto, a su vez, permite que el SIEM realice la correlación automatizada de estos eventos, como la coincidencia de campos entre eventos de registro, a lo largo de períodos de tiempo y entre tipos de dispositivos:

"Si un único host no puede iniciar sesión en tres servidores separados usando las mismas credenciales dentro de un intervalo de tiempo de 6 segundos, envíe una alerta"

Esto es obviamente útil, a diferencia de los registros nativos con los que se comienza. Además, la normalización de eventos permite la creación de resúmenes de informes de nuestra información de registro, tales como:

"¿Qué cuentas de usuario han accedido al mayor número de hosts distintos en el último mes?"

"¿Qué subred genera la mayor cantidad de intentos de inicio de sesión fallidos por día, promediados en 6 meses?"

Armado con esta comprensión de lo que es un SIEM, y cómo se relacionan los archivos de registro.

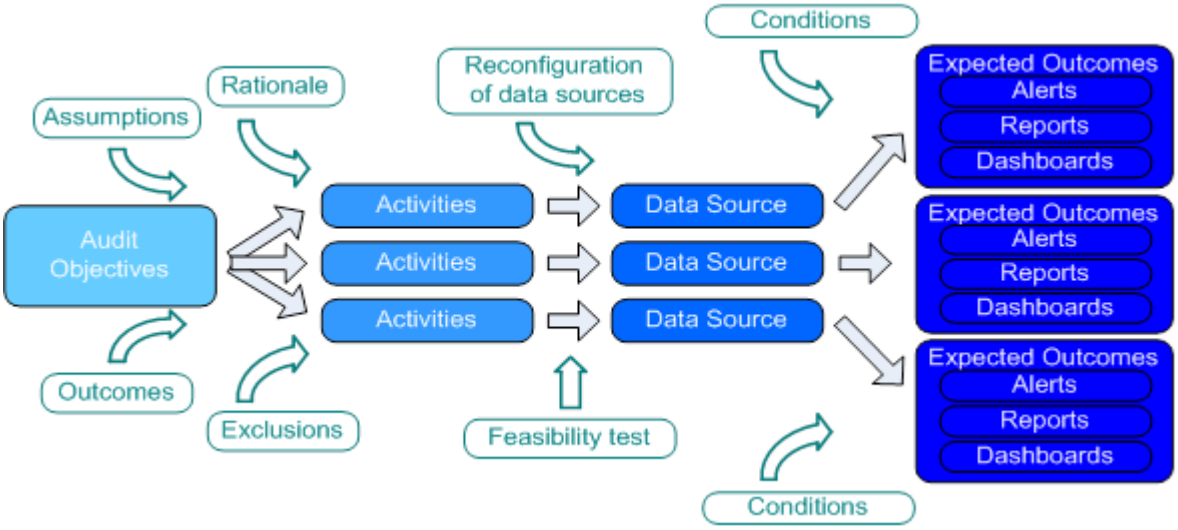

FIGURA 9: SIEM Y LA RELACIÓN DE LOS ARCHIVOS Y LOS LOGS

4.2 Análisis para Identificar las amenazas en el entorno del cloud computing.

La seguridad informática en la nube (o seguridad en la nube) es un subdominio de la seguridad de la información. La seguridad en la nube debe abordar problemas como la protección de la identidad, el mantenimiento de la privacidad y el control del acceso. También debe garantizar la continuidad del

negocio y las opciones de recuperación de desastres con copias de seguridad continuas y en la nube en caso de incumplimiento o desastre.

Las infracciones a la nube vienen de muchas maneras. Los servidores del proveedor de servicios en la nube podrían fallar debido a la falta de seguridad, por ejemplo, los hackers o clientes infelices pueden atacar los recursos de la nube. Puede haber problemas de disponibilidad y confiabilidad, problemas legales y regulatorios, interfaces de programación de aplicaciones inseguras, pérdida / fuga de datos, información privilegiada maliciosa, y secuestro de tráfico y servicios, por nombrar algunas fuentes de infracciones.

Con tantas formas de vulnerar un entorno de nube, se necesita un enfoque estructurado para evitar posibles infracciones. Esto se hace en tres pasos: identificación de activos, identificación de amenazas e identificación de contramedidas.

Primero, se deben identificar qué activos está tratando de proteger y qué propiedades de esos activos se deben mantener. Identificar qué ataques se pueden montar y si hay otras amenazas, como desastres naturales. Por último, se debe identificar cómo se pueden contrarrestar esas amenazas.

La información privilegiada malintencionada es uno de los beneficios de la computación en la nube, las organizaciones no necesitan conocer los detalles técnicos de cómo se prestan los servicios. Los procedimientos del proveedor, el acceso físico a los sistemas, el monitoreo de los empleados y los problemas relacionados con el cumplimiento son transparentes para el cliente. Sin un conocimiento y control completo, su organización puede estar en riesgo.

Pérdida y fuga de datos con los recursos de infraestructura compartida, las organizaciones deberían preocuparse por los sistemas de autenticación de servicios que otorgan acceso a los datos. Las organizaciones también deberían preguntar sobre el cifrado, los procedimientos de eliminación de datos y la continuidad del negocio.

Un secuestro de cuenta de los sistemas sencillos de registro de Internet, el fraude electrónico y los esquemas de fraude pueden permitir que un pirata informático tome el control de su cuenta. Además, el phishing, el fraude y la explotación de las vulnerabilidades del software podrían comprometer sus credenciales. Si sus credenciales se ven comprometidas, los atacantes podrían obtener acceso a su (s) cuenta (s) de servicio de computación en la nube. Esto comprometerá aún más la confidencialidad, integridad y disponibilidad de esos servicios.

Por múltiples razones se deben prevenir estas violaciones de seguridad, ya que las infracciones de seguridad son costosas y pueden quitar una gran parte del presupuesto de TI, destruir marcas y eventualmente conducir a una pérdida de negocios. Entonces, ¿cómo previene las violaciones de datos? Esto puede sonar difícil, ¡pero en realidad es muy fácil! Se debe de investigar antes de elegir un proveedor de servicios. Se debe preguntar acerca de la administración de claves de cifrado. ¿Quién va a administrar las llaves? ¿Quién tiene acceso a las llaves? Elegir las propias claves de encriptación y auto gestionadas. No permitir que su proveedor de servicios controle sus llaves. Además, evitar el riesgo del secuestro de las cuentas.

El uso de la computación en la nube ha crecido en los últimos años, y dicho crecimiento definitivamente ha contribuido a aumentar las amenazas a la seguridad a medida que los hackers continúan experimentando con nuevas formas de ataque. Como resultado, las amenazas de seguridad se están convirtiendo en algo cotidiano. El compromiso de datos podría pasarle a cualquiera, desde una gran corporación a un individuo. Sin embargo TI han respondido vigorosamente implementando tecnologías para mitigar los riesgos, educando a los interesados para que inviertan en herramientas de evaluación de riesgos para la protección de datos, mediante la encriptación, eligiendo cuidadosamente la infraestructura segura y adquiriendo certificaciones de cumplimiento. Como resultado, las numerosas amenazas en las infracciones de datos en la nube, la pérdida de datos, los ataques internos maliciosos y el secuestro estarán bajo control.

4.3 Análisis de la de la creación de las reglas para un SIEM.

Las reglas son el ingrediente básico para cualquier herramienta o tecnología de SIEM. Una regla no es más que un conjunto de instrucciones lógicas que debe seguir un sistema antes de determinar qué hacer y qué no hacer. Como se sabe, SIEM es un sistema pasivo. Todo lo que hace es una coincidencia de patrones de los registros recibidos y sigue las instrucciones sobre qué hacer (desencadenar) y qué no hacer (no desencadenar). Este patrón de coincidencia también se denomina Reglas de correlación o Reglas de tiempo real. Estas Reglas de Correlación no son más que "su visualización de cómo se vería un ataque en una Infraestructura de TI".

Se debe de seguir una serie de pasos antes de empezar con el análisis de la creación de estas reglas.

- Fase de requisitos: en esta fase, el autor de la regla debe recopilar los requisitos exactos para establecer una regla. Estos requisitos deben indicar cuál es el "Intento" de la regla y también capturan la respuesta que provocaría un disparador de regla. Es en esta fase de requisitos, donde realmente comienza la "visualización".

- Fase de diseño: en la fase de diseño, realiza el diseño esquelético bruto de la regla en sí. Se buscan respuestas a preguntas como,

  ¿Qué registros usar para crear esta regla específica?

  ¿Qué atributo de registro es más adecuado para activar la regla?

  ¿Cuáles son los diversos atributos para recopilar / representar?

  ¿Qué tipo de regla escribir?

  ¿Qué tipo de alerta se configurará? (Leer correo electrónico, capturas SNMP, disparador del tablero de instrumentos, acción de respuesta, etc.)

  Esta es la fase más crucial. Cuando se trata de seleccionar tipos de reglas, se necesita saber cuáles son todas las características disponibles de su herramienta SIEM o tecnología. En general, como una guía para todo uso, clasifica ampliamente las reglas para cualquier herramienta o tecnología de SIEM en lo siguiente:

  1. Regla de evento único: si la condición 1, 2, 3 hasta N coincide, dispara. Tipo de regla típicamente utilizado, ya que es una coincidencia directa de patrones de tipo de evento, ID de evento, IP, etc.

2. Reglas de uno a uno o de uno a muchos: si una condición coincide con una fuente, varios objetivos o un objetivo, varios escenarios de fuentes están en juego

3. Reglas de causa y efecto o "Seguido de" Reglas o reglas secuenciales: si la condición A coincide y conduce a la condición B. Esto normalmente será un escenario de "Escaneo seguido con un exploit", "error de adivinación de contraseña seguido de inicio de sesión exitoso" tipo escenarios, etc.

4. Reglas transitorias o reglas de seguimiento: si la condición A coincide con el atacante a la máquina A y dentro de un tiempo, la máquina A se convierte en atacante de la máquina B (una vez más se corresponde con la condición A). Esto se usa típicamente en escenarios de infección de gusanos / malware. Aquí, el objetivo en el primer evento se convierte en la fuente en el segundo evento.

5. Reglas de tendencias: estas reglas son el seguimiento de varias condiciones durante un período de tiempo, en función de los umbrales. Esto sucede en escenarios DoS o DDoS.

- Fase de desarrollo: Aquí es donde se escribe la regla. Recuerde, una vez que la comprensión lógica está ahí para las condiciones requeridas para coincidir (generalmente usando operadores booleanos), escribir una regla es muy simple y directo (por supuesto, necesita conocer los menús de la herramienta SIEM para hacerlo)
- Fase de prueba y la fase de despliegue. Las pruebas son críticas para validar la lógica involucrada en la regla. Simular las condiciones de la regla en el entorno de desarrollo / entorno de prueba ayudará a resolver las grietas en la regla.

- Fase de implementación posterior: una vez que se implementa la regla, debemos gestionarla. Garantizar que la regla se ajusta según los comentarios de Security Analysts. Esto puede implicar agregar condiciones adicionales a la regla, listas blancas, ajustes de umbral, etc. Esto es lo que hace que la regla sea mejor y más eficiente para lograr el "INTENTO". Básicamente es un "Modelo de cascada" en el que se vuelve a la regla una y otra vez para ajustarla de acuerdo con las necesidades exactas.

Capítulo 5 Propuesta a la Solución

5.1 Fuentes de logs recomendadas para el registro y el monitoreo – Priorización

Según la industria proporcionada por el cuadrante de Gartner los líderes de la industria referente a tecnologías y soluciones de cloud computing son Amazon Web Services y Microsoft (Azure).

FIGURA 10: CUADRANTE DE GARTNER REFERENTE A CLOUD COMPUTING. FUENTE: HTTPS://WWW.GARTNER.COM

Por lo tanto, la siguiente es la base de las fuentes de recursos recomendadas para los logs y el monitoreo. La fuente de datos de seguridad relacionadas con la nube (AWS & Azure) para logs y monitoreo en el entorno de la infraestructura, se estableció el siguiente enfoque:

Los tipos de logs se clasifican en las tres categorías siguientes:

1. Prioridad # 1: Incluye logs de prioridad máxima que son necesarios para llevar a cabo investigaciones de seguridad (respuesta a incidentes).
2. Prioridad # 2: Incluye logs de prioridad media que agregan información contextual a las investigaciones de seguridad.
3. Prioridad # 3: Incluye los logs de menor prioridad que son útiles para optimizar la seguridad y el funcionamiento del entorno / aplicación de nube cruzada.

5.1.1 Tipos de Logs Prioridad#1

Tipo de Log	Descripcion	Punto de Integración/Localización del Log	Categoría	Servicio	Prioridad	Gratis/Pago de Suscripción	Comentarios
CloudTrail	Graba API de AWS solicita cuenta y entrega archivos de registro. Cloudtrail captura información que incluye la identidad de un Llamada de API, el tiempo de una llamada de API, la dirección IP de origen de una API los parámetros de petición, y los elementos de respuesta devuelto por el servicio AWS.	S3 Buckets	SBI & Logging	AWS	1	Pago por Servicio y S3 almacenamiento.	38 servicios son compatibles por el rastro de la nube. Los registros que son la máxima prioridad y relacionados con incidente respuesta se utilizará tales como EC2, IAM y etc.
VPC FlowLogs	Monitorear el tráfico que fluye a través de Virtual Private Clouds (VPCs), registros de firewall. Captura tráfico IP para una interfaz de red, subred o VPC especificada	CloudWatch/s3	Red	AWS	1	Servicio gratuito, pago por almacenamiento y servicio de streaming (Cloudwatch / Kinesis)	
Config	Proporciona un inventario detallado de los recursos de AWS y sus configuración, y registra continuamente los cambios de estos recursos. (por ejemplo, reglas de entrada / salida de grupos de seguridad, Reglas de ACL de red para VPC y el valor de las etiquetas en Amazon EC2 instancias)	SNS/S3 Buckets	Descubrimiento	AWS	1	$ 0.003 por configuración y elementos registrados	
Azure AD Reports	Proporciona una variedad de informes de actividad, seguridad y auditoría.	REST API	Identificación y Control de Acceso	Azure	1	Tarifas gratuitas, asociadas cuando se almacenan en una cuenta de almacenamiento.	Si se integran y se amplían desde las instalaciones, no es necesario.
Azure Security Center Alerts	Azure Security Center ofrece recomendaciones de seguridad enfocadas y un rápido despliegue de tecnologías de socios integrados. Utiliza análisis de comportamiento y aprendizaje automático para una detección eficaz de amenazas y le ayuda a crear una línea de tiempo de ataque para una remediación más rápida.	Azure Log Integración	SBI & Logging	Azure	1	Libre / suscripción para Advanced "ATA"	
Activity Log/Audit Log/Operational Logs	Operaciones de administración (Crear / Actualizar / Eliminar llamadas de la API por Azure) El registro de actividad de Azure es un registro que proporciona las operaciones que se realizaron en los recursos de su suscripción. Registro de actividades, ayuda a determinar el "qué, quién y cuando "para cualquier operación de escritura (PUT, POST, DELETE) tomada en los recursos de la suscripción.	Cuenta de almacenamiento (debe ser un propósito general cuenta de almacenamiento), Hub de eventos, Azure Log Integración, Almacenamiento Servicios REST API	Identificación y Control de Acceso	Azure	1	Cuotas gratuitas y asociadas cuando se almacenan en una cuenta de almacenamiento	
Network Security Logs(NSG)	Un grupo de seguridad de red (NSG) contiene una lista de control de acceso list (ACL) que permiten o niegan el tráfico de red a VM instancias en una red virtual. Los NSG pueden asociarse con subnets o instancias de VM individuales dentro de esa subred.		Red	Azure	1		
Linux OS security Log	Registros de actividades del SO desde un servidor Linux / VM	Con agente, Sin agente	Calcular	AWS/Azure	1		
Windows OS security Log	Registros de actividades del SO desde un servidor Windows / VM	Con agente, Sin agente	Calcular	AWS/Azure	1		
WAF	Un firewall de aplicaciones web (WAF) es un firewall de aplicaciones para Aplicaciones HTTP.		Aplicación	Herramienta de Seguridad	1		
Firewall(Virtual)	Proporciona información detallada sobre el tráfico de la red.	Syslog	Red	Herramienta de Seguridad	1		
Cloud Passage	Detectar las violaciones de seguridad y cumplimiento y las amenazas en la infraestructura de la nube	API	Calcular	Herramienta de Seguridad	1		
Antivirus Security Epo	Recopila información de antivirus y informes de análisis de vulnerabilidades.	Base de Dato	Calcular	Herramienta de Seguridad	1		
VSE(Windows Only)	Recopila información de antivirus y informes de análisis de vulnerabilidades.	Base de Dato	Calcular	Herramienta de Seguridad	1		

TABLA 1: TIPO DE LOGS DE PRIORIDAD#1 FUENTE: ELABORACIÓN PROPIA.

5.1.2 Tipos de Logs Prioridad#2

Tipo de Log	Descripcion	Punto de Integración/Localización del Log	Categoría	Servicio	Prioridad	Gratis/Pago de Suscripción	Comentarios
ELB Access Logs	ELB proporciona registros de acceso que capturan información detallada sobre solicitudes o conexiones enviadas al equilibrador de carga.	S3 Buckets	Red	AWS	2	Servicio gratuito, pago por almacenamiento S3	
S3 Access Log	Los registros de acceso S3 registran cada acceso desde los buckets S3. Las operaciones de usuarios pueden ser una de las siguientes: cargar, descargar, compartir, acceso y publicación de contenidos.	S3 Buckets	Identificación y Control de Acceso	AWS	2	Servicio gratuito, pago por almacenamiento S3	
Azure SQL Database Auditing	Rastrea eventos de base de datos y escribe eventos auditados en un registro de auditoría en su cuenta de almacenamiento de Azure.	Servicios de Almecenamiento REST API	SBI & Logging	Azure	2	Tarifas gratuitas, asociadas cuando se almacenan en una cuenta de almacenamiento.	
WhiteHat web scanning	Plataforma de exploración de aplicaciones. Permite a los negocios rápidamente implementar un programa escalable de seguridad de aplicaciones en todo el desarrollo de software (SDLC).	API	Aplicación	Herramienta de Seguridad	2		

TABLA 2: TIPO DE LOGS DE PRIORIDAD#2 FUENTE: ELABORACIÓN PROPIA.

5.1.3 Tipos de Logs Prioridad#3

Tipo de Log	Descripcion	Punto de Integración/Localización del Log	Categoría	Servicio	Prioridad	Gratis/Pago de Suscripción	Comentarios
Config Rules	Detalles de cumplimiento, resumen de cumplimiento y estado de evaluación de las reglas de configuración de AWS		Conformidad	AWS	3	$ 2 por regla activa por mes	
Inspector	Inspector es un servicio automatizado de evaluación de seguridad que mejorar la seguridad y el cumplimiento de las aplicaciones desplegadas AWS. Durante la ejecución de la evaluación, la red, el sistema de la actividad del proceso dentro de la meta especificada, y una amplio conjunto de datos de actividad y de configuración. La información que aquí se presentan son los resultados de las evaluaciones y hallazgos de Servicio de Inspector de Amazon.	API	Conformidad	AWS	3	Pagar por el servicio (prueba gratuita disponible)	
CloudWatch	Amazon CloudWatch es un servicio de supervisión para los recursos de nube de AWS y para las aplicaciones que ejecuta en AWS. Puede utilizar Amazon CloudWatch para recopilar y rastrear métricas, recopilar y supervisar archivos de registro, establecer alarmas y reaccionar automáticamente a los cambios en los recursos de AWS	S3 Buckets	SBI & Logging	AWS	3	El monitoreo básico (5min) es gratuito. Se realiza monitoreo detallado (1min) y métricas personalizadas.	Cloudwatch es una monitorización y puede utilizarse para el punto de recogida de registros. Algunas herramientas SIEM podrían utilizarlo como un punto de integración.
Trusted Advisor	Mejorar la seguridad de las aplicaciones mediante el cierre de vacíos, AWS, y examinar los permisos.		Descubrimiento	AWS	3	% del uso mensual de AWS	Trusted Advisor no produce ningún registro, sino que genera recomendaciones (datos) que pueden ser consumidas por algunas herramientas de terceros.
Azure Storage Analytics	Captura lo siguiente: • Proporciona registros (trazas de solicitudes ejecutadas de blobs, tablas y colas) y métricas (resumen de capacidades clave y estadísticas de solicitud). • ¿Cuántas solicitudes anónimas es mi aplicación viendo desde un rango determinado de direcciones IP? • ¿A qué contenedores se accede más? • ¿Cuántas veces se está accediendo a una URL SAS específica y cómo? • ¿Quién emitió la solicitud para eliminar un contenedor?	Servicios de Almecenamiento REST API	SBI & Logging	Azure	3	Cuotas gratuitas y asociadas cuando se almacenan en una cuenta de almacenamiento	
Cloud Checker	CloudCheckr ofrece una plataforma unificada de gestión de costes y seguridad para la gestión de costes, el inventario AWS, la seguridad continua y la auditoría de conformidad en toda la inversión de AWS. transforma los datos de AWS en conocimientos prácticos mediante informes, alertas, análisis y automatización del entorno	API	SBI & Logging	Herramienta de Seguridad	3		
SkyHigh	Skyhigh descubre todos los servicios en la nube en uso por los empleados tanto dentro como fuera de la red, incluyendo miles de servicios en la nube sin categoría de firewalls y proxies web. Puede reportar amenazas basadas en la nube para SIEM.	Syslog o API	Descubrimiento	Herramienta de Seguridad	3		Skyhigh Cloud Access Security para o shadow IT

TABLA 3: TIPO DE LOGS DE PRIORIDAD#3 FUENTE: ELABORACIÓN PROPIA.

5.1.4 Fuentes recomendadas de Logs – Análisis

Después de revisar la tabla con la lista provista, se llega a la conclusión y se recomienda que se incluyan las siguientes fuentes de registro, debido a que son los logs principales a nivel investigativo que ayudarán al análisis y respuesta de incidentes.

- AWS CloudTrail
- AWS VPC FlowLogs
- Azure NSG
- Azure Activity Logs
- Linux OS security log
- Windows OS security log

- AWS S3 Access Logs

5.1.5 Casos de uso recomendados

La siguiente tabla incluye la lista de Casos de Uso recomendados, basados en las 7 fuentes de datos principales para este propósito: CloudTrail, registros de Sistemas Operativos, Flowlogs de VPC, NSG de Azure, registros de acceso de S3 y registros de actividad de Azure.

Casos de Uso	Descripcion	Fuende de Datos	Comentarios
Se detectó una cuenta de corta duración	Detecta cuándo se crea una cuenta o credencial y se elimina poco después. Esto puede ser una indicación de actividades maliciosas	CloudTrail, OS Security Logs	Se eliminaron los registros de actividad de Azure como fuente de datos, ya que la administración de usuarios de Azure se controla mediante AD local (en premisa).
Actividad anormal - Una política de auditoría fue cambiado	Esta alerta captura eventos relacionados con la política de auditoría cambios.	Windows OS Security Logs	
Se detectó un evento sospechoso - detección de puertos. Se detectó un ataque de barrido de evento sospechoso.	Esta regla se activa cuando se detecta un número excesivo de exploraciones de puertos en una interfaz especificada. Esta regla se activa cuando se detecta un número excesivo de exploraciones de direcciones IP en la red.	VPC FlowLogs, NSG	Estos son dos casos de uso separados, pero serán tratados como uno solo. (12 total de casos de uso)
Se detectó un ataque de Fuerza Bruta (AWS) Iniciar sesión después de varios inicios de sesión fallidos)	Detecta el número excesivo de intentos fallidos de inicio de sesión junto con un intento exitoso (esto podría indicar un ataque de fuerza bruta exitoso).	CloudTrail, OS Security Logs	Se eliminaron los registros de actividad de Azure como fuente de datos, ya que la administración de usuarios de Azure se controla mediante AD local (en premisa).
El permiso del usuario ha cambiado	Activa una alerta cuando el permiso de usuario cambia y podría indicar la escalada de privilegios.	CloudTrail, Activity logs	Cambios de permisos de usuario de IAM de AWS y cambios de roles de usuario en recursos de Azure
Error de autenticación	Detecta la autenticación de usuario fallida en AWS	CloudTrail	Se eliminaron los registros de actividad de Azure como fuente de datos, ya que la administración de usuarios de Azure se controla mediante AD local (en premisa). También se puede obtener la creación y eliminación de cuentas a través de Office365.
Creación de nuevos usuarios de fuentes anomalas.	Detecta cuando se crean usuarios de AWS y la IP de origen proviene de fuentes desconocidas.	CloudTraill	Se eliminaron los registros de actividad de Azure como fuente de datos, ya que la administración de usuarios de Azure se controla mediante AD local (en premisa).
Proceso prohibido / servicios detectados (PowerShell)	Alertas cuando se ejecuta un proceso anómalo a través de PowerShell	Windows OS Security Logs	
Tráfico saliente sospechoso	Esta regla detecta una anomalía en el patrón de tráfico con un tráfico saliente incrementado en un puerto / dirección negado por una fuente interna.	VPC Flowlogs, NSG	
Usuario sospechoso - Solicitud de acceso satisfactoria por un solo usuario que accede a varios buckets S3	Detecta varios buckets S3 que son accesados por un solo usuario. Esto podría indicar actividades maliciosas.	S3 Access Logs	
Autenticación exitosa de fuentes anómalas	Detecta la autenticación exitosa en recursos AWS de fuentes desconocidas.	CloudTraill	Los registros de actividad de Azure no se incluyen porque la administración de usuarios de Azure está controlada por AD locales (en premisa).

TABLA 4: CASOS DE USO RECOMENDADOS. FUENTE: ELABORACIÓN PROPIA.

5.2 Identificación de amenazas de la nube cruzada.

La seguridad en la nube se logra, en parte, a través de controles y garantías de terceros como en tradicionales de outsourcing. Pero como no existe un estándar común de seguridad para la computación en nube, hay desafíos

adicionales asociados con esto. Muchos proveedores de cloud implementan sus propios normas y tecnologías de seguridad, e implementar diferentes modelos de seguridad, que deben ser evaluados por sus propios méritos. En un modelo de nube de proveedores, la última instancia, es la adopción de clientes para garantizar que la seguridad en la nube cumpla con sus propias políticas de seguridad a través del proveedor de recopilación de requisitos evaluación de riesgos, diligencia debida y actividades de aseguramiento (CPNI Security Briefing, 2010).

Por lo tanto, los desafíos de seguridad que enfrentan las organizaciones que desean utilizar servicios en la nube no son radicalmente diferentes de los que dependen de sus propias empresas administradas internamente. Las amenazas externas están presentes y requieren la mitigación del riesgo o la aceptación del riesgo. A continuación se examinan los desafíos de seguridad de la información que las organizaciones adoptivas deberán considerar, ya sea actividades de aseguramiento en el proveedor o proveedores de nube pública o directamente, a través del diseño e implementando el control de seguridad en una nube de propiedad privada. En particular, examinamos las siguientes cuestiones:

- El tratamiento contra los activos de información que residen en entornos de cloud computing.
- Los tipos de atacantes y su capacidad de atacar la nube.
- Los riesgos de seguridad asociados con la nube
- Nuevos riesgos de seguridad en la nube.

- Algunos ejemplos de incidentes de seguridad en la nube.

5.2.1 Amenazas de Cloud Computing

Las amenazas a los activos de información que residen en la nube pueden variar según los modelos de entrega en la nube utilizada por las organizaciones de usuarios de la misma. Existen varios tipos de amenazas de seguridad a las que se es vulnerable. La siguiente recopilación ofrece una visión general de las amenazas para los clientes de la nube clasificadas confidencialidad, integridad y disponibilidad (CIA) y su relevancia para cada una de las nubes modelo de prestación de servicios.

Casos de Uso	Descripción
Confidencialidad	
Amenazas de los usuarios iniciados: • Usuario del proveedor de la nube malintencionada • Usuario de cliente malicioso de la nube • Usuario de terceros malintencionado (Apoyo ya sea el proveedor de la nube o el cliente organizaciones)	La amenaza de que los usuarios internos tengan acceso a los de adentro de la nube es mayor ya que cada uno de los modelos pueden introducir la necesidad de múltiples usuarios: SaaS - administradores de clientes y proveedores de cloud PaaS- desarrolladores de aplicaciones y entorno de prueba gerentes IaaS - consultores de plataformas de terceros
Amenazas de los atacantes externos: • Ataque de software remoto de la nube infraestructura • Ataque de software remoto de la nube aplicaciones • Ataque de hardware remoto contra la nube • Software remoto y ataque de hardware contra el punto final de las organizaciones de usuarios de la nube software y hardware • Ingeniería social de los usuarios de cloud computing, y los usuarios de los clientes de la nube.	La amenaza de los atacantes externos puede percibirse para aplicar más a la Internet pública frente a las nubes, Sin embargo, todos los tipos de modelos de entrega en la nube son afectados por atacantes externos, particularmente en nubes donde los puntos finales del usuario pueden ser dirigidos. Nube proveedores con grandes almacenes de datos con tarjeta de crédito datos personales, información personal y gobierno o propiedad intelectual, serán sometidos a ataques de grupos, con recursos significativos, intentando recuperar datos. Esto incluye la

	amenaza de ataque de hardware, ingeniería social y cadena de suministro ataques de atacantes dedicados.
Fuga de datos: • El incumplimiento de los derechos de varios dominios • Falta de transporte electrónico y físico sistemas para datos y copias de seguridad en la nube	Una amenaza de fuga generalizada de datos entre muchas organizaciones potencialmente competidoras, proveedor de la misma nube podría ser causada por error humano o hardware defectuoso que conduzca a comprometer la información.
Integridad	
Segregación de datos: • Perímetro de seguridad definido incorrectamente • Configuración incorrecta de máquinas virtuales y hypervisors	La integridad de los datos dentro del cloud hosting ambientes como SaaS configurado para compartir recurso de computación entre los clientes una amenaza contra la integridad de los datos si los recursos se segregan efectivamente.
Acceso de usuario: • Mala gestión de identidad y acceso procedimientos	Implementación de procedimientos de control de acceso deficientes crea muchas oportunidades de amenaza, por descontentos ex empleados del proveedor de la nube las organizaciones mantienen acceso remoto para administrar servicios cloud de clientes y puede causar daños a sus fuentes de datos.
Calidad de los datos: • Introducción de una aplicación defectuosa o componentes de la infraestructura	La amenaza del impacto de la calidad de los datos los proveedores de cloud aloja muchos datos de clientes, la introducción de un componente defectuoso o mal configurado requerido por otro usuario de la nube podría afectar la integridad de los datos para otros usuarios de la nube compartida en la infraestructura.
Disponibilidad	

Gestión del cambio: • Pruebas de penetración de clientes que impactan otros clientes de la nube • Cambios de infraestructura en la nube proveedores, clientes y sistemas de terceros afectando a los clientes de la nube	Como el proveedor de la nube tiene una responsabilidad creciente para la gestión del cambio dentro de la entrega de nubes modelos, existe la amenaza de que los cambios efectos negativos. Estos podrían ser causados por software o cambios de hardware en los servicios existentes en la nube.
Peligro de denegación de servicio: • Denegación distribuida de ancho de banda de red de servicio • Denegación de servicio DNS de red • Denegación de servicio de aplicaciones y datos	La amenaza de la denegación de servicio contra los recursos disponibles de cloud computing es generalmente una amenaza externa contra los servicios públicos en la nube. Sin embargo, la amenaza puede todos los modelos de servicios en la nube como los agentes de amenaza interna podrían introducir componentes de hardware que causan una denegación de servicio.
Interrupción física:• Interrupción de los servicios de TI del proveedor de la nube mediante acceso físico• Interrupción de los servicios de TI del cliente en la nube mediante acceso físico• Interrupción de proveedores de WAN de terceros servicios	La amenaza de interrupción de los servicios en la nube el acceso físico es diferente entre las grandes nubes proveedores de servicios y sus clientes. Los proveedores deben tener experiencia en los centros de datos y han considerado la capacidad de entre otras estrategias de disponibilidad. Hay una amenaza que la infraestructura de usuario de la nube puede estar físicamente más fácilmente, ya sea por parte de externamente donde los entornos de oficina menos el trabajo a distancia es la práctica estándar.
Aprovechando los procedimientos de recuperación débiles: • Invocación de una recuperación de desastres inadecuada o procesos de continuidad del negocio	La amenaza de una recuperación inadecuada y de los procedimientos de gestión que se están iniciando cuando los usuarios de la nube consideran la recuperación de su propia en paralelo con los gestionados por proveedores de servicios en la nube de terceros. Si estos procedimientos no se prueban, entonces el impacto el tiempo de recuperación puede ser significativo.

TABLA 5: AMENAZAS DE CLOUD COMPUTING FUENTE: ELABORACIÓN PROPIA.

5.2.2 Tipos de atacantes en Cloud Computing

Muchas de las amenazas y desafíos de seguridad en la computación en la nube serán familiares para las organizaciones, la gestión de la infraestructura interna y los que participan en los modelos tradicionales de outsourcing. Cada una de las amenazas de los modelos de servicios informáticos resulta de los atacantes, que se pueden dividir en dos grupos como se muestra a continuación:

Ataques Internos	Un atacante interno tiene las siguientes características: • Es empleado por el proveedor de servicios en la nube, el cliente u otro tercero proveedor de servicios de apoyo a la operación de un servicio en la nube • Puede tener acceso autorizado a servicios en la nube, datos de clientes o infraestructuras y aplicaciones de apoyo, en función de sus papeles. • Utiliza los privilegios existentes para obtener mayor acceso o apoyo a terceros en ataques contra la integridad de la confidencialidad y la disponibilidad de información dentro del servicio de la nube.
Ataques Externos	Un atacante externo tiene las siguientes características: • No es empleado por el proveedor de servicios en la nube, el cliente u otro tercero proveedor de servicios de apoyo a la operación de un servicio en la nube • No tiene acceso autorizado a servicios en la nube, datos de clientes o infraestructura y aplicaciones • Explota vulnerabilidades técnicas, operativas, de procesos y de ingeniería social para atacar a un proveedor de servicios en la nube, al cliente o a una organización de apoyo de terceros acceso a propagar ataques contra la confidencialidad, la integridad y la y la disponibilidad de información dentro del servicio en la nube.

TABLA 6: TIPOS DE ATACANTES EN CLOUD COMPUTING FUENTE: ELABORACIÓN PROPIA.

Aunque los atacantes internos y externos pueden ser claramente diferenciados, su capacidad para ejecutar el éxito de los ataques es lo que los diferencia como una, amenaza tanto para los clientes como para los vendedores.

En el entorno de la nube, los atacantes pueden clasificarse en cuatro tipos: aleatorio, débil, fuerte y sustancial (CPNI Security Briefing, 2010). Cada una de estas categorías se basa en la capacidad de ataque exitoso, en lugar del tipo de amenaza que presentan (es decir, criminal, espionaje o terrorismo):

• Aleatorio: el tipo más común de atacante utiliza herramientas y técnicas simples. El atacante puede escanear aleatoriamente Internet tratando de encontrar componentes vulnerables. Desplegarán conocidas herramientas o técnicas que deben ser fácilmente detectados.

• Débil - Los atacantes semicualificados que apuntan a servidores / proveedores de nube específicos al personalizar herramientas públicamente disponibles u objetivos específicos. Sus métodos son más avanzados cuando intentan personalizar sus ataques utilizando herramientas de exploit disponibles.

• Fuerte - Grupos organizados, bien financiados y calificados de atacantes con una jerarquía interna especializada en la orientación de aplicaciones particulares y usuarios de la nube. Generalmente este grupo del crimen organizado especializado en ataques a gran escala.

• Substancial - Motivados, atacantes fuertes que no son fácilmente detectados por las organizaciones que atacan, o incluso por las organizaciones competentes de aplicación de la ley y de investigación especializadas en crímenes o la seguridad cibernética. Para mitigar esta amenaza se requiere mayor inteligencia sobre los ataques y recursos en respuesta a la detección de un incidente o amenaza.

5.2.3 Riesgos de seguridad en la nube

Los riesgos de seguridad asociados con cada modelo de entrega en la nube varían y dependen de una amplia gama de factores como la sensibilidad de los activos de información, las arquitecturas en nube y el control de un entorno de nube particular. A continuación se exponen estos riesgos en un contexto general, excepto cuando se hace una referencia específica al modelo de entrega en la nube. En la siguiente tabla se resumen los riesgos de seguridad de la computación en la nube.

Riesgo	Descripción
Acceso privilegiado al usuario	Los proveedores de nube generalmente tienen acceso ilimitado a los datos de usuario, se necesitan controles para abordar el riesgo de acceso de usuario que lleva a datos de clientes comprometidos.
Ubicación y segregación de datos	Es posible que los clientes no sepan dónde se almacenan sus datos y puede haber un riesgo de que los datos se almacenen junto a información de otros clientes.
Eliminación de datos	La eliminación de datos en la nube es un riesgo, donde el hardware se emite dinámicamente a clientes basados en sus necesidades. El riesgo de que los datos no se eliminen de los datos tiendas, copias de seguridad y medios físicos durante la clausura se mejora dentro de la nube.
e-investigaciones y monitoreo de protección	La capacidad de los clientes de la nube para invocar sus propios procedimientos de investigaciones electrónicas dentro de la nube puede limitarse por el modelo de suministro en uso, y el acceso y complejidad de la arquitectura en nube. Los clientes no pueden implementar sistemas de monitoreo en infraestructura que ellos no poseen; deben confiar en los sistemas en uso por el proveedor de servicios en la nube para apoyar las investigaciones.

Asegurar la seguridad en la nube	Los clientes no pueden asegurar fácilmente la seguridad que no controlan directamente sin utilizar SLAs y tener derecho a auditar controles de seguridad dentro de sus acuerdos.

TABLA 7: RIESGOS DE SEGURIDAD EN LA NUBE FUENTE: ELABORACIÓN PROPIA.

5.3 Reglas propuestas para el monitoreo y Guía para identificar las amenazas de formar proactiva

Dado los datos obtenidos y requerimientos se proponen las siguientes reglas para el SIEM con el fin de monitorear los eventos recibidos, además se proponen una lista de instrucciones para identificar de mejor manera las amenazas de forma proactiva recibidas en el SIEM.

- Compromised Asset - Successful Brute Force Attack Detected
- Policy Violation - User Permission Changes
- Compromised Asset - SSH-RDP Inbound Ports Open
- Compromised Asset - Brute Force Login Attempt
- Compromised Asset - Compromised Core System
- Compromised Asset - Root User Compromised
- Denial of Service - SYN Flood Attack
- Malware - Prohibited Process Executed in PowerShell
- Malware - Malware Outbreak Detected
- Malware - High Number of Infected Hosts
- Compromised Asset - Suspicious Outbound Traffic
- Hacking - Suspicious Event - Port Scan
- Hacking - Suspicious Event - Address Sweep Attack Detected
- Compromised Asset - Excessive Traffic to Known Bad IP Address

5.3.1 Compromised Asset - Successful Brute Force Attack Detected

El propósito de esta alerta es identificar un intento exitoso de fuerza bruta realizado en AWS Console utilizando la fuente de datos CloudTrail. Un intento exitoso de inicio de sesión de fuerza bruta se define como al menos 5 intentos fallidos y, a continuación, un evento de inicio de sesión correcto en un corto período de tiempo. Esto puede ayudar a indicar si el evento ocurrido es malicioso y puede llevar a un compromiso de cuentas, activos y / o datos en el entorno de AWS. Toda la actividad de autenticación de la consola AWS debe proceder de la red, esta alerta buscará intentos de inicio de sesión de direcciones IP externas, lo que podría indicar un posible compromiso o fallo de Cloud para acceder a recursos de la red interna.

Debido a la naturaleza del entorno de la nube, es importante verificar la dirección de origen con el inquilino de la nube afectado para identificar si se pueden vincular a la dirección IP desconocida debido al acceso a recursos fuera de la red de o si se está produciendo un ataque.

5.3.1.1 Recursos de datos:

SIEM Campos	AWS CloudTrail Campos específicos del dispositivo	Descripción
deviceVendor	"AWS"	
deviceProduct	"CloudTrail"	
Name	Event Name	Nombre del evento que ocurrió en AWS
Start Time	eventTime	Hora de inicio del evento
Source Address	sourceIPAddress	Dirección que se utilizó para iniciar sesión en AWS Console y realizar los cambios de permiso
Source User ID	userIdentity->Accountid	ID de cuenta de AWS

Source User Name	UserIdentity->UserName	Nombre de usuario que realizó las acciones
Source Process Name	<Not Found in SIEM CloudTrail Documentation>	Nombre de proceso que proporciona un nombre de usuario al final del registro, útil si el Nombre de usuario de origen no está disponible
Source Service Name	<Not Found in SIEM CloudTrail Documentation>	Identifica que la acción realizada fue a través de AWS IAM
Source User Privileges	<Not Found in SIEM CloudTrail Documentation>	El tipo de rol que tenía la cuenta cuando la acción tuvo lugar, puede ser el rol de IAM o el rol Asumido
Request Url	<Not Found in SIEM CloudTrail Documentation>	Una cadena que identifica todas las acciones tomadas para el cambio de permiso. El final del registro de sucesos identifica la política afectada y proporciona información adicional
Request Method :	<Not Found in SIEM CloudTrail Documentation>	Muestra el ID de cuenta AWS y el nombre de usuario responsable de las acciones
Request Client Application	userAgent	console.amazonaws.com

TABLA 8: RECURSO DE DATOS COMPROMISED ASSET - SUCCESSFUL BRUTE FORCE ATTACK DETECTED FUENTE: ELABORACIÓN PROPIA.

5.3.1.2 Ejemplo de la alerta:

Esta alerta se dispara porque la cuenta berny.cordero ha tenido una acción de fallar varios inicios de sesión al menos 5 veces en 1 minuto y luego iniciar sesión con éxito en la consola AWS desde 165.165.165.165, lo que indica un potencial ataque de fuerza bruta desde una dirección IP externa. Investigue esta alerta buscando el ID de cuenta de AWS: 123456789 y poniéndose en contacto con el administrador. Pregúnteles dónde están ubicados y si se conectan al intento de acceso a AWS Console desde fuera del Proxy. Si han verificado su actividad, notifique al usuario que no son compatibles accediendo a recursos internos fuera de un Proxy y si la actividad continúa, se notificará a su gerente. Si es necesario, póngase en contacto con el administrador del usuario para verificar su trabajo. Resuelva esta alerta una vez que haya confirmado que

el administrador es responsable de los inicios de sesión y la autenticación fallidos o la contraseña de la cuenta se ha restablecido.

5.3.1.3 Entrevista Usuarios Finales - Identificar si la actividad proviene del usuario

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo y que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Está el usuario consciente de las autenticaciones fallidas y de la conexión correcta de las cuentas de usuario?

Sí –

a. Identificar si el usuario es responsable de estas acciones.

b. Si la actividad se identifica como legítima, puede ser validada por el usuario, pero no procede del proxy interno, notificar al usuario que debe tener acceso a sus recursos a través del proxy interno. Si no lo hace, se producirá una escalada en su gerente.

c. Si la actividad se identifica como legítima, puede ser validada por el usuario y procede del proxy interno, recibir la aprobación para trabajar con los desarrolladores de contenido del SIEM para resolver el falso positivo.

2. No -

a. Pida al usuario que restablezca las credenciales de la cuenta de AWS. Si no pueden restablecer las credenciales, se debe de escalar el problema al administrador con acceso para restablecer las credenciales de la cuenta de AWS.

b. ¿Cuál es el propósito de su cuenta AWS? ¿Qué tipo de sistemas hay en la cuenta? c. ¿Funciona la cuenta AWS con datos confidenciales?

d. ¿Puede acceder a otras cuentas, sistemas o datos confidenciales de AWS?

e. Si la cuenta AWS identificada puede acceder a otras cuentas o sistemas de AWS, recopile información sobre esas cuentas AWS y / o hosts para su posible aislamiento junto con el host original identificado en la alerta. Notificar a los propietarios de cuenta AWS identificados que se ven afectados.

f. Confirme que las credenciales de la cuenta se han restablecido y que el administrador de AWS tiene el control de su cuenta de AWS.

5.3.2 Policy Violation - User Permission Changes

El propósito de esta alerta es identificar los cambios de permisos realizados en AWS Console o Azure Portal desde una conexión hecha desde direcciones IP fuera de la red interna. Esta alerta puede ayudar a identificar posibles violaciones de políticas debido a cambios de permisos incorrectos por parte de los empleados o identificar diferentes tipos de incidentes debido a la actividad realizada por un usuario malintencionado y desconocido.

Debido a la naturaleza del entorno de la nube, es importante verificar la dirección de origen de la nube afectado para identificar que se pueden vincular a

la dirección IP desconocida debido al acceso a recursos fuera de la red interna o si se está produciendo un ataque.

5.3.2.1 Recursos de datos:

SIEM Campos	Campos específicos del dispositivo de registro de actividad de Azure	Descripción
deviceVendor	"Microsoft"	
deviceProduct	"Azure Activity Logs"	
sourceUserName	caller	Dirección de correo electrónico del usuario que ha realizado la operación, reclamación UPN o reclamación SPN según disponibilidad.
sourceUserId	claims_name	Uno de los valores siguientes: "Admin", "Operación"
deviceCustomString1	correlationId	Generalmente un GUID en el formato de cadena. Los eventos que comparten un correlationId pertenecen a la misma uber acción.
deviceCustomString2	description	Descripción de texto estático de un evento.
flexString1	eventDataId	Identificador único de un evento.
deviceAction	eventName_value	Solicitud final
deviceEventCategory	category_value	Administrativo
sourceAddress	httpRequest_clientIpAddress	Dirección IP origen
deviceCustomString3	httpRequest_method	Blob que describe la Solicitud Http. Normalmente incluye "clientRequestId", "clientIpAddress" y "method" (método HTTP, por ejemplo, PUT).
deviceEventClassId	id	/subscriptions/3f29717f-22fb-4402-8079-d0403513ff64/resourcegroups/Default-SQL-WestUS/deployments/Microsoft.SQL.NewDatabase/events/7507dd97-238c-4dce-84c0-c59fe27a662c/ticks/635918094947984086
deviceSeverity	level	Nivel del evento. Uno de los siguientes valores: "Crítico", "Error", "Advertencia", "Informativo" y "Verboso"
deviceCustomString4	resourceGroupName	Nombre del grupo de recursos para el recurso afectado.
deviceCustomString5	resourceProviderName_value	Nombre del proveedor de recursos para el recurso afectado

deviceCustomString6	resourceType_value	Microsoft.Resources/deployments
name	operationName_value	Nombre de la operación.
	properties	Conjunto de pares <Key, Value> (es decir, un diccionario) que describe los detalles del evento.
eventOutcome	Status_value	Cadena que describe el estado de la operación. Algunos valores comunes son: Iniciado, En progreso, Sucedido, Fallido, Activo, Resuelto.
requestMethod	subStatus_localizedValue	Normalmente el código de estado HTTP de la llamada REST correspondiente, pero también puede incluir otras cadenas que describan un subestado, como estos valores comunes: OK (Código de estado HTTP: 200), Creado (Código de estado HTTP: 201), Aceptado (Código de estado HTTP : Código de estado HTTP: 404), Conflicto (Código de estado HTTP: 409), Error interno del servidor (Código de estado HTTP) : 500), servicio no disponible (código de estado HTTP: 503), tiempo de espera de puerta de enlace (código de estado HTTP: 504).
event.deviceReceiptTime	eventTimestamp	Timestamp cuando el evento fue generado por el servicio Azure procesando la solicitud correspondiente al evento.
deviceExternalId	subscriptionId	Azure Subscription Id.
externalId	eventId	Fichero de continuación para obtener el siguiente conjunto de resultados cuando se dividen en múltiples respuestas. Normalmente es necesario cuando hay más de 200 registros.

TABLA 9: RECURSO DE DATOS POLICY VIOLATION - USER PERMISSION CHANGES FUENTE: ELABORACIÓN PROPIA.

5.3.2.2 Ejemplo de la alerta:

Esta alerta se activa porque los cambios de permisos de registro de actividad de Azure interactuaron con 40.78.109.106 de esta manera, lo cual es sospechoso porque esta actividad se realizó fuera del Proxy y podría indicar una

escalada de privilegios de usuario en una cuenta Azure comprometida. Investigue esta alerta buscando la suscripción Azure: 55e0b8cc-87f2-4cac-bc19-6eb6bcf8f72c, poniéndose en contacto con el administrador y preguntándoles si están al tanto de los cambios realizados en una función o cuenta en su suscripción Azure. Identifique cómo se conectan a su suscripción Azure y si están accediendo a ella a través de la red interna. Si es necesario, póngase en contacto con el administrador del usuario para verificar su trabajo. Resuelva esta alerta una vez que haya confirmado que los cambios en la cuenta eran válidos y la fuente de los cambios procedía del administrador. Notificar al usuario que debe acceder a su Portal Azure a través de la red interna.

5.3.2.3 Entreviste al usuario final para identificar si se ha producido una infracción de la política

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Está el usuario enterado de los cambios que se hicieron en su cuenta de AWS o suscripción de Azure?

1. Sí -

a. Identificar si el usuario es responsable de estas acciones.

b. Si la actividad se identifica como realizada por el usuario, pero no hay justificación para los cambios de permiso, notifique al administrador de usuarios. Esto se considera una violación de la política, notifique al administrador.
c. Si la actividad es identificada como legítima, puede ser validada por el usuario, tiene una justificación de negocio, pero no viene del proxy interno, notificar al usuario que debe tener acceso a sus recursos internos a través del proxy. Si no lo hace, se producirá una escalada en su gerente.
d. Si la actividad se identifica como legítima, puede ser validada por el usuario y procede del proxy interno, resolver como falso positivo.

2. No -

a. Esto no se considera una violación de la política y el tipo de incidente debe ser determinado. Una vez determinado, continúe con la investigación referenciando al incidente identificado.
b. Pida al usuario que restablezca las credenciales de cuenta de AWS / Azure. Si no pueden restablecer las credenciales, escalar el problema al administrador con acceso para restablecer las credenciales de cuenta de AWS / Azure.
c. ¿Cuál es el propósito de su cuenta AWS / Azure? ¿Qué tipo de sistemas hay en la cuenta? ¿Funciona la cuenta AWS / Azure con datos confidenciales?
d. ¿Puede acceder a otras cuentas, sistemas o datos confidenciales de AWS / Azure?
e. Si la cuenta AWS / Azure identificada puede acceder a otras cuentas o sistemas de AWS / Azure, recopile información sobre esas cuentas y / o hosts de AWS / Azure para su posible aislamiento junto con el host original identificado

en la alerta. Notificar a los propietarios de cuentas AWS / Azure identificados que están afectados.

f. Confirme que las credenciales de la cuenta se han restablecido y que el administrador de AWS / Azure tiene el control de su cuenta de AWS / Azure.

g. Confirme que la actividad sospechosa ha sido detenida.

5.3.3 Compromised Asset - SSH-RDP Inbound Ports Open

El propósito de esta alerta es identificar el tráfico SSH / RDP aceptado que ingresa a los recursos de AWS / Azure desde direcciones IP fuera de la red interna. Esta alerta puede ayudar a identificar activos potencialmente comprometidos debido a conexiones remotas aceptadas desde direcciones IP desconocidas que pueden ser el resultado de una amenaza externa. Debido a la naturaleza del entorno de la nube, es importante verificar la dirección de origen con el usuario de la nube afectado para identificar si se pueden vincular a la dirección IP desconocida debido al acceso a recursos fuera de la red interna o si se está produciendo un ataque.

5.3.3.1 Recursos de datos:

SIEM Campos	VPC Flowlogs Campos específicos del dispositivo	Descripción
deviceVendor	"AWS"	
deviceProduct	“VPC Flowlogs”	
message	status	El estado de registro del registro de flujo: OK: Los datos se registran normalmente en los registros de CloudWatch.

		NODATA: No hubo tráfico de red hacia o desde la interfaz de red durante la ventana de captura. SKIPDATA: Algunos registros de registro de flujo se omitieron durante la ventana de captura. Esto puede deberse a una restricción de capacidad interna oa un error interno.
deviceVersion	logversion	La versión de los registros de flujo VPC.
deviceExternalId	Account-id	El ID de cuenta de AWS para el registro de flujo.
deviceOutboundInterface	Interface-id	ID de la interfaz de red para la que se aplica el flujo de registro.
startTime	start	La hora, en segundos Unix, del inicio de la ventana de captura.
endTime	end	La hora, en segundos Unix, del final de la ventana de captura.
sourceAddress	srcaddr	La dirección IPv4 o IPv6 de origen. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
destinationAddress	dstaddr	La dirección IPv4 o IPv6 de destino. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
sourcePort	srcport	El puerto de origen del tráfico.
destinationPort	dstport	El puerto de destino del tráfico..
transportProtocol	protocol	El número de protocolo IANA del tráfico. Para obtener más información, vaya a Asigned Internet Protocol Numbers.
fileSize	packets	Número de paquetes transferidos durante la ventana de captura.
bytesOut	bytes	El número de bytes transferidos durante la ventana de captura.
deviceAction	action	La acción asociada con el tráfico: ACEPTAR: El tráfico registrado fue permitido por los grupos de seguridad o ACL de red. REJECT: El tráfico registrado no fue permitido por los grupos de seguridad o ACL de red.

TABLA 10: RECURSO DE DATOS COMPROMISED ASSET - SSH-RDP INBOUND PORTS OPEN VPC FUENTE: ELABORACIÓN PROPIA.

SIEM Campos	Azure Flowlogs Campos específicos de dispositivos	Descripción
deviceVendor	"Microsoft"	
deviceProduct	“Azure NSG Flowlogs”	
event.deviceCustomString1	systemId	Id de recurso de grupo de seguridad de red
event.deviceCustomString2	rule	Regla para la cual se enumeran los flujos
event.deviceCustomString3	resourceid	El Id de recurso del NSG - proporciona el ID de suscripción para Azure
event.deviceCustomString4	mac	La dirección MAC de la NIC para la VM donde se recogió el flujo
event.message	flowTuples	Una cadena que contiene varias propiedades para la tupla de flujo en formato separado por comas
event.transportProtocol	Protocol	El protocolo del flujo. Los valores válidos son T para TCP y U para UDP
event.deviceReceiptTime	Time Stamp	Este valor es la marca de tiempo de cuando el flujo se produjo en el formato EPIX de UNIX
event.deviceAction	Traffic	Si se permitió o se negó el tránsito. Los valores válidos son A para permitido y D para negado
event.sourcePort	Source Port	El puerto de origen
event.destinationAddress	Destination IP	El IP de destino
event.deviceCustomString5	Traffic Flow	La dirección del flujo de tráfico. Los valores válidos son I para entrada y O para salida
event.sourceAddress	Source IP	El IP de origen
event.destinationPort	Destination Port	El puerto de destino

TABLA 11: RECURSO DE DATOS COMPROMISED ASSET - SSH-RDP INBOUND PORTS OPEN AZURE

5.3.3.2 Ejemplo de la alerta:

Esta alerta se activa porque se ha realizado una conexión satisfactoria a

10.0.0.46 en Puerto: 22 desde 116.255.200.34 lo que indica una conexión

remota exitosa desde una dirección IP no identificada y un posible compromiso del host. Investigue esta alerta buscando el ID de cuenta de AWS: 180093952737 y poniéndose en contacto con el administrador. Pregúnteles dónde están ubicados y si se conectan al 10.0.0.46 desde fuera del Proxy. Si han verificado su actividad, notifique al usuario que no es seguro acceder a recursos fuera de un Proxy interno y si la actividad continúa, se notificará a su gerente. Si es necesario, póngase en contacto con el administrador del usuario para verificar su trabajo. Resuelva esta alerta una vez que haya confirmado que el usuario ha sido autorizado para acceder a este host desde el exterior de la red.

5.3.3.3 Entrevista Usuarios Finales - Identificar si la actividad proviene del usuario

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Es consciente el usuario de la autenticación y las acciones realizadas recientemente en el sistema de destino?

1. Sí -

a. Identificar si el usuario es responsable de estas acciones.
b. Verifique con el usuario que se les permite acceder a estos sistemas y realizar las acciones identificadas. Si el usuario no puede justificar o justificar sus

acciones, póngase en contacto con el administrador del usuario para verificación y escalamiento de sus actividades.

c. El host está autorizado para realizar la autenticación fuera del proxy interno.
d. Si la actividad se identifica como legítima, puede ser validada por el usuario, pero no tiene autorización para conectarse desde fuera del proxy, notificar al usuario que debe tener acceso a sus recursos a través del proxy interno. Si no lo hace, se producirá una escalada en su gerente.
e. Si la actividad se identifica como legítima, puede ser validada por el usuario y tiene autorización para conectarse desde fuera del proxy, resolver como falso positivo.
f. Si la actividad se identifica como legítima, puede ser validada por el usuario y procede del proxy interno, resolver como falso positivo.

2. No -

a. Pida al usuario que restablezca las credenciales de la cuenta. Si no pueden restablecer las credenciales, escalar el problema al administrador con acceso para restablecer las credenciales de la cuenta.
b. ¿Puede el usuario encontrar la (s) fuente (s) afectada (s) en su entorno?
c. ¿Puede el usuario cambiar grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.
d. ¿Cuál es el propósito del sistema objetivo?
e. ¿Qué acciones puede realizar la cuenta? ¿Puede acceder a otros sistemas o datos sensibles?

f. Si la cuenta identificada puede acceder a otros sistemas, recopile información sobre esos hosts para su posible aislamiento junto con el host original identificado en la alerta.

g. Confirme que las credenciales de la cuenta se han restablecido y que el administrador de AWS / Azure tiene el control de la cuenta.

5.3.8 Malware - Prohibited Process Executed in PowerShell

El propósito de esta alerta es identificar e investigar cualquier actividad maliciosa potencial que pueda haber sido identificada a partir de un proceso anómalo de PowerShell que puede indicar una instancia de AWS o Azure infectada. Debido a la naturaleza del entorno de la nube, es importante recopilar el ID de la cuenta de AWS o el ID de la suscripción de Azure junto con el nombre del host del dispositivo (si corresponde) así como la dirección IP de destino para ayudar al usuario a buscar el recurso en su entorno cloud.

5.3.8.1 Recursos de los datos:

Campos compartidos para Linux y Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
name	name	Nombre del evento LIDS que ocurrió
message	message	Mensaje de evento que identifica el SO, la identificación de la cuenta de AWS / Azure (si está disponible), el ID de la instancia (si está disponible), así como el nombre de la política de LIDS
deviceCustomString1	server_platform	Plataforma OS (Windows o Linux)
sourceHostName	server_hostname	Nombre de host del activo AWS / Azure

deviceCustomString2	server_group_name	Versión del sistema operativo
deviceHostName	ec2_instance_id	ID del elemento AWS / Azure
deviceCustomString3	ec2_account_id	Etiqueta del servidor: por lo general, el ID de cuenta de AWS o el ID de suscripción de Azure
deviceCustomString4	policy_name	Nombre de la política de LIDS
devicecustomString5	rule_name	Nombre de la regla que se llevó a cabo, identificando el evento
flexString2	original_log_entry	Entrada de registro crudo desde Linux o Windows - ayudará a identificar información adicional que no se puede asignar

TABLA 12: RECURSO DE DATOS MALWARE - PROHIBITED PROCESS EXECUTED IN POWERSHELL LINUX/WINDOWS FUENTE: ELABORACIÓN PROPIA.

Campos Linux:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	Id	Identificador de evento LIDS
event.Outcome	type	Resultado de la regla de LIDS que desencadenó
name	name	Nombre de los eventos LIDS
deviceReceiptTime	created_at	Hora en que ocurrió el evento
sourceHostName	server_hostname	Nombre de host que se encuentra en AWS o Azure
sourceAddress	server_ip_address	Dirección IP pública del elemento AWS o Azure
sourceDnsDomain	server_reported_fqdn	FQDN del servidor - puede contener la dirección IP privada en el nombre de AWS o Azure activo
sourceTranslatedAddress	server_primary_ip_address	Dirección IP privada del elemento AWS o Azure

TABLA 13: RECURSO DE DATOS MALWARE - PROHIBITED PROCESS EXECUTED IN POWERSHELL LINUX FUENTE: ELABORACIÓN PROPIA.

Campos Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	<EventID>4625</EventID>	ID de evento de Windows

deviceReceiptTime	<TimeCreated SystemTime='2017-06-13T20:56:18.796455500Z'/>	Hora en que ocurrió el evento
deviceEventCategory	<Channel>Security</Channel>	Tipo de evento de Windows
flexString1	<Computer>VA-EPO-01.EIP-VA.DEMO</Computer>	Nombre de host en el que se ha producido el evento
sourceUserName	<Data Name='SubjectUserName'>-</Data>	Nombre de usuario de origen vinculado al evento
deviceNtDomain	<Data Name='SubjectDomainName'>-</Data>	El dominio del host
destinationUserId	<Data Name='SubjectLogonId'>0x0</Data>	ID de inicio de sesión en Windows
destinationUserName	<Data Name='TargetUserName'>ADMINISTRATOR</Data>	Nombre de usuario específico para el evento
destinationNtDomain	<Data Name='TargetDomainName'></Data>	Nombre de dominio segmentado para el evento
reason	<Data Name='FailureReason'>%%2313</Data>	Código de razón de fallo de Windows
deviceCustomNumber1	<Data Name='LogonType'>3</Data>	Tipo de inicio de sesión de Windows
destinationProcessName	<Data Name='LogonProcessName'>NtLmSsp </Data>	Nombre de proceso de inicio de sesión de Windows
deviceCustomString6	<Data Name='AuthenticationPackageName'>NTLM</Data>	Nombre del paquete de

		autenticación de Windows
sourceHostName	<Data Name='WorkstationName'></Data>	Nombre de la estación de trabajo fuente del evento
sourceProcessId	<Data Name='ProcessId'>0x0</Data>	ID de proceso de Windows
sourceProcessName	<Data Name='ProcessName'>-</Data>	Nombre del proceso de Windows
sourceAddress	<Data Name='IpAddress'>-</Data>	Dirección IP de origen del evento
sourcePort	<Data Name='IpPort'>-</Data>	Puerto de origen del host para el evento

TABLA 14: RECURSO DE DATOS MALWARE - PROHIBITED PROCESS EXECUTED IN POWERSHELL WINDOWS FUENTE: ELABORACIÓN PROPIA.

5.3.8.2 Ejemplo de la alerta:

Esta alerta se activa cuando se ejecuta un comando potencialmente malicioso de PowerShell en la instancia i-e638637a en el entorno de la nube Azure o AWS. Para investigar esta alerta, revise el bloque PowerShell Script ubicado en el campo Flex String 2. Se deben revisar eventos adicionales para i-e638637a para comprender mejor todas las actividades realizadas en la instancia y los comandos adicionales ejecutados. Comuníquese con el administrador de la cuenta 668107645782. Resuelva esta alerta una vez que el propósito de los comandos ejecutados se haya entendido y se determine que no es malicioso.

5.3.8.3 Entrevista a los usuarios finales: identificar el comando potencialmente malicioso de PowerShell ejecutado.

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿El usuario ejecutó el comando para iniciar este proceso anómalo?

1. Sí -

a. Identificar el propósito del usuario para ejecutar el comando, ¿cuál es el propósito del proceso?

b. ¿Tienen un caso de negocio para ejecutar este proceso de PowerShell?

c. ¿Cuál es el propósito de la máquina en la que ejecutan este proceso de PowerShell en su entorno de nube?

d. ¿Cuál es el propósito del servidor o punto final? ¿Contiene información sensible? Esto ayudará a identificar la urgencia y el impacto de los eventos que tienen lugar.

e. ¿Son recursos de producción o desarrollo?

f. Si el usuario no puede justificar o justificar sus acciones, póngase en contacto con el administrador del usuario para verificación y escalamiento de sus actividades.

2. No -

a. Continúe la verificación identificando malware.

5.3.4 Compromised Asset - Brute Force Login Attempt

El propósito de esta alerta es identificar un host AWS / Azure potencialmente mal configurado o vulnerable como resultado de varios intentos de inicio de sesión de fuerza bruta. La alerta busca varios eventos de inicio de sesión fallidos en un corto período de tiempo contra el mismo host de destino. Esta alerta puede ayudar a indicar si hay posibles configuraciones erróneas para los activos de AWS / Azure, ya que sus configuraciones pueden potencialmente dejarlo expuesto a los atacantes. Esta alerta también puede indicar que un activo específico está siendo dirigido y potencialmente puede verse comprometido en algún momento si no se toman medidas. Debido a la naturaleza del entorno de la nube, es importante recopilar el ID de la cuenta de AWS o el ID de la suscripción de Azure junto con el nombre del host del dispositivo (si corresponde) así como la dirección IP de destino para ayudar al usuario a buscar el recurso en su entorno cloud.

5.3.4.1 Recurso de datos

Campos compartidos para Linux y Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
name	name	Nombre del evento LIDS que ocurrió
message	message	Mensaje de evento que identifica el SO, la identificación de la cuenta de AWS / Azure (si está disponible), el ID de la instancia (si está disponible), así como el nombre de la política de LIDS
deviceCustomString1	server_platform	Plataforma OS (Windows o Linux)

sourceHostName	server_hostname	Nombre de host del activo AWS / Azure
deviceCustomString2	server_group_name	Versión del sistema operativo
deviceHostName	ec2_instance_id	ID del elemento AWS / Azure
deviceCustomString3	ec2_account_id	Etiqueta del servidor: por lo general, el ID de cuenta de AWS o el ID de suscripción de Azure
deviceCustomString4	policy_name	Nombre de la política de LIDS
devicecustomString5	rule_name	Nombre de la regla que se llevó a cabo, identificando el evento
flexString2	original_log_entry	Entrada de registro crudo desde Linux o Windows - ayudará a identificar información adicional que no se puede asignar

TABLA 15: RECURSO DE DATOS COMPROMISED ASSET - BRUTE FORCE LOGIN ATTEMPT LINUX/WINDOWS FUENTE: ELABORACIÓN PROPIA.

Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	<EventID>4625</EventID>	ID de evento de Windows
deviceReceiptTime	<TimeCreated SystemTime='2017-06-13T20:56:18.796455500Z'/>	Hora en que ocurrió el evento
deviceEventCategory	<Channel>Security</Channel>	Tipo de evento de Windows
flexString1	<Computer>VA-EPO-01.EIP-VA.DEMO</Computer>	Nombre de host en el que se ha producido el evento
sourceUserName	<Data Name='SubjectUserName'>-</Data>	Nombre de usuario de origen vinculado al evento
deviceNtDomain	<Data Name='SubjectDomainName'>-</Data>	El dominio del host
destinationUserId	<Data Name='SubjectLogonId'>0x0</Data>	ID de inicio de sesión en Windows

destinationUserName	<Data Name='TargetUserName'>ADMINISTRATOR</Data>	Nombre de usuario específico para el evento
destinationNtDomain	<Data Name='TargetDomainName'></Data>	Nombre de dominio segmentado para el evento
reason	<Data Name='FailureReason'>%%2313</Data>	Código de razón de fallo de Windows
deviceCustomNumber1	<Data Name='LogonType'>3</Data>	Tipo de inicio de sesión de Windows
destinationProcessName	<Data Name='LogonProcessName'>NtLmSsp </Data>	Nombre de proceso de inicio de sesión de Windows
deviceCustomString6	<Data Name='AuthenticationPackageName'>NTLM</Data>	Nombre del paquete de autenticación de Windows
sourceHostName	<Data Name='WorkstationName'></Data>	Nombre de la estación de trabajo fuente del evento
sourceProcessId	<Data Name='ProcessId'>0x0</Data>	ID de proceso de Windows
sourceProcessName	<Data Name='ProcessName'>-</Data>	Nombre del proceso de Windows
sourceAddress	<Data Name='IpAddress'>-</Data>	Dirección IP de origen del evento
sourcePort	<Data Name='IpPort'>-</Data>	Puerto de origen del host para el evento

TABLA 16: RECURSO DE DATOS COMPROMISED ASSET - BRUTE FORCE LOGIN ATTEMPT WINDOWS FUENTE: ELABORACIÓN PROPIA.

Linux:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	Id	Identificador de evento LIDS
event.Outcome	type	Resultado de la regla de LIDS que desencadenó
name	name	Nombre de los eventos LIDS
deviceReceiptTime	created_at	Hora en que ocurrió el evento
sourceHostName	server_hostname	Nombre de host que se encuentra en AWS o Azure
sourceAddress	server_ip_address	Dirección IP pública del elemento AWS o Azure
sourceDnsDomain	server_reported_fqdn	FQDN del servidor - puede contener la dirección IP privada en el nombre de AWS o Azure activo
sourceTranslatedAddress	server_primary_ip_address	Dirección IP privada del elemento AWS o Azure

TABLA 17: RECURSO DE DATOS COMPROMISED ASSET - BRUTE FORCE LOGIN ATTEMPT LINUX
FUENTE: ELABORACIÓN PROPIA.

5.3.4.2 Ejemplo de la alerta:

Esta alerta se activa porque se ha producido un ataque de fuerza bruta en un sistema Linux en el entorno de nube de AWS. Los ataques de fuerza bruta NO deberían ser posibles contra los sistemas debidamente configurados. Para investigar esta alerta, póngase en contacto con el administrador de la instancia: server.domain.com en la siguiente cuenta: 1234123412341234. Pregunte al administrador si recientemente se han producido cambios en el sistema. Las causas potenciales pueden configurarse incorrectamente los ajustes del grupo de seguridad o la contraseña de la cuenta de servicio ha caducado. Resolver esta alerta una vez que el administrador ha detenido el ataque de ocurrir en su sistema.

5.3.4.3 Entrevista Usuarios Finales - Identificar si la actividad proviene del usuario

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o requerirá más investigación necesaria.

¿Es consciente el usuario de las autenticaciones fallidas en su sistema?

1. Sí –

a. Identificar si el usuario es responsable de estas acciones.

b. Si la actividad se identifica como legítima, puede ser validada por el usuario, pero no procede del proxy, notificar al usuario que debe tener acceso a sus recursos locales a través del proxy. Si no lo hace, se producirá una escalada en su gerente.

c. Si la actividad se identifica como legítima, puede ser validada por el usuario y procede del proxy, resolver como falso positivo.

2. No -

a. Identificar si el usuario tiene una razón para que sus sistemas estén orientados a Internet.

b. ¿Puede el usuario encontrar otras fuentes afectadas en su entorno?

c. ¿Puede el usuario cambiar grupos de seguridad / grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.

d. ¿Cuál es el propósito del sistema que está siendo dirigido?

e. ¿El sistema contiene datos confidenciales? ¿Tiene una razón para estar frente a internet y abierto al ataque?

f. Si procede, confirme que se han cambiado los ajustes de red del sistema para evitar que se envíe de nuevo esta alerta.

5.3.5 Compromised Asset - Compromised Core System

El propósito de esta alerta es identificar un activo básico potencialmente comprometido de AWS o Azure que ha experimentado varios inicios de sesión fallidos y, una continuación, un intento de inicio de sesión exitoso para hosts de Windows. Un activo básico puede ser un anfitrión que puede ofrecer acceso a otros sistemas, contener aplicaciones críticas de negocio o software, o puede contener los datos sensibles que los actores maliciosos están apuntando. Debido a la naturaleza del entorno del nube, es importante recopilar el ID de la cuenta de AWS o el ID de la suscripción de Azure con el nombre de anfitrión del dispositivo (si corresponda) así como la dirección IP de destino para ayudar al buscar un recurso en su entorno cloud.

5.3.5.1 Recurso de los datos:

Campos compartidos para Linux y Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
name	name	Nombre del evento LIDS que ocurrió

message	message	Mensaje de evento que identifica el SO, la identificación de la cuenta de AWS / Azure (si está disponible), el ID de la instancia (si está disponible), así como el nombre de la política de LIDS
deviceCustomString1	server_platform	Plataforma OS (Windows o Linux)
sourceHostName	server_hostname	Nombre de host del activo AWS / Azure
deviceCustomString2	server_group_name	Versión del sistema operativo
deviceHostName	ec2_instance_id	ID del elemento AWS / Azure
deviceCustomString3	ec2_account_id	Etiqueta del servidor: por lo general, el ID de cuenta de AWS o el ID de suscripción de Azure
deviceCustomString4	policy_name	Nombre de la política de LIDS
devicecustomString5	rule_name	Nombre de la regla que se llevó a cabo, identificando el evento
flexString2	original_log_entry	Entrada de registro crudo desde Linux o Windows - ayudará a identificar información adicional que no se puede asignar

TABLA 18: RECURSO DE DATOS COMPROMISED ASSET - COMPROMISED CORE SYSTEM LINUX/WINDOWS FUENTE: ELABORACIÓN PROPIA.

Campos Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	<EventID>4625</EventID>	ID de evento de Windows
deviceReceiptTime	<TimeCreated SystemTime='2017-06-13T20:56:18.796455500Z'/>	Hora en que ocurrió el evento
deviceEventCategory	<Channel>Security</Channel>	Tipo de evento de Windows
flexString1	<Computer>VA-EPO-01.EIP-VA.DEMO</Computer>	Nombre de host en el que se ha producido el evento
sourceUserName	<Data Name='SubjectUserName'>-</Data>	Nombre de usuario de origen

		vinculado al evento
deviceNtDomain	<Data Name='SubjectDomainName'>-</Data>	El dominio del host
destinationUserId	<Data Name='SubjectLogonId'>0x0</Data>	ID de inicio de sesión en Windows
destinationUserName	<Data Name='TargetUserName'>ADMINISTRATOR</Data>	Nombre de usuario específico para el evento
destinationNtDomain	<Data Name='TargetDomainName'></Data>	Nombre de dominio segmentado para el evento
reason	<Data Name='FailureReason'>%%2313</Data>	Código de razón de fallo de Windows
deviceCustomNumber1	<Data Name='LogonType'>3</Data>	Tipo de inicio de sesión de Windows
destinationProcessName	<Data Name='LogonProcessName'>NtLmSsp </Data>	Nombre de proceso de inicio de sesión de Windows
deviceCustomString6	<Data Name='AuthenticationPackageName'>NTLM</Data>	Nombre del paquete de autenticación de Windows
sourceHostName	<Data Name='WorkstationName'></Data>	Nombre de la estación de trabajo fuente del evento
sourceProcessId	<Data Name='ProcessId'>0x0</Data>	ID de proceso de Windows
sourceProcessName	<Data Name='ProcessName'>-</Data>	Nombre del proceso de Windows

sourceAddress	<Data Name='IpAddress'>-</Data>	Dirección IP de origen del evento
sourcePort	<Data Name='IpPort'>-</Data>	Puerto de origen del host para el evento

TABLA 19: RECURSO DE DATOS COMPROMISED ASSET - COMPROMISED CORE SYSTEM WINDOWS FUENTE: ELABORACIÓN PROPIA.

Campos Linux:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	Id	Identificador de evento LIDS
event.Outcome	type	Resultado de la regla de LIDS que desencadenó
name	name	Nombre de los eventos LIDS
deviceReceiptTime	created_at	Hora en que ocurrió el evento
sourceHostName	server_hostname	Nombre de host que se encuentra en AWS o Azure
sourceAddress	server_ip_address	Dirección IP pública del elemento AWS o Azure
sourceDnsDomain	server_reported_fqdn	FQDN del servidor - puede contener la dirección IP privada en el nombre de AWS o Azure activo
sourceTranslatedAddress	server_primary_ip_address	Dirección IP privada del elemento AWS o Azure

TABLA 20: *RECURSO DE DATOS COMPROMISED ASSET - COMPROMISED CORE SYSTEM LINUX FUENTE: ELABORACIÓN PROPIA.*

5.3.5.2 Ejemplo de la alerta:

Esta alerta se activó porque se ha producido un ataque exitoso de fuerza bruta en un sistema Windows en el entorno de Azure o AWS. Para investigar esta alerta, póngase en contacto con el administrador de la cuenta o suscripción 123412341234 y notifíquelos que server.domain.com ha sido potencialmente comprometida. El ataque se produjo desde la siguiente dirección IP: 123.123.123.123. Resuelva esta alerta una vez que haya confirmado que la

actividad era legítima o si está comprometida, asegúrese de que se han restablecido las credenciales del sistema comprometido. El sistema puede necesitar ser puesto en cuarentena para una investigación más profunda y para asegurarse de que no ha ocurrido ninguna otra actividad maliciosa. Trabaje con el administrador para garantizar que no se produzcan futuros ataques contra sus sistemas revisando los estándares de configuración para el entorno de la nube.

5.3.5.3 Entrevista Usuarios Finales - Identificar si la actividad proviene del usuario

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Es consciente el usuario de la autenticación y las acciones realizadas con éxito en el sistema principal de destino?

1. Sí -

a. Identificar si el usuario es responsable de estas acciones.

b. Verifique con el usuario que se les permite acceder a estos sistemas y realizar las acciones identificadas. Si el usuario no puede justificar o justificar sus acciones, póngase en contacto con el administrador del usuario para verificación y escalamiento de sus actividades.

c. Si la actividad se identifica como legítima, puede ser validada por el usuario, pero no procede del proxy, notificar al usuario que debe tener acceso a sus

recursos internos a través del proxy. Si no lo hace, se producirá una escalada en su gerente.

d. Si la actividad se identifica como legítima, puede ser validada por el usuario y procede del proxy interno, resolver como falso positivo.

2. No -

a. Pida al usuario que restablezca las credenciales de la cuenta. Si no pueden restablecer las credenciales, escalar el problema al administrador con acceso para restablecer las credenciales de la cuenta.

b. ¿Puede el usuario encontrar otras fuentes afectadas en su entorno?

c. ¿Puede el usuario cambiar grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.

d. ¿Cuál es el propósito del sistema u objetivo?

e. ¿Qué acciones puede realizar la cuenta? ¿Puede acceder a otros sistemas o datos sensibles?

f. Si la cuenta identificada puede acceder a otros sistemas, recopile información sobre esos hosts para su posible aislamiento junto con el host original identificado en la alerta.

g. Confirme que las credenciales de la cuenta se han restablecido y que el administrador de AWS / Azure tiene el control de la cuenta.

5.3.6 Compromised Asset - Root User Compromised

El propósito de esta alerta es identificar una cuenta de usuario raíz potencialmente comprometida en sistemas basados en Linux. La alerta busca varios eventos de inicio de sesión fallidos alrededor de la cuenta raíz y se generará después de que se haya identificado un inicio de sesión satisfactorio en un corto período de tiempo de los intentos fallidos de autenticación. Una cuenta de usuario raíz comprometida tendrá acceso completo al sistema al que ha iniciado sesión y puede dar lugar a activos comprometidos adicionales, eventos de ex filtración de datos e intentos de eliminar archivos maliciosos en los sistemas de destino. Debido a la naturaleza del entorno de la nube, es importante recopilar el ID de la cuenta de AWS o el ID de la suscripción de Azure junto con el nombre de host del dispositivo (si corresponde) así como la dirección IP de destino para ayudar al usuario a buscar el recurso en su entorno cloud.

5.3.6.1 Recurso de los datos

Campos compartidos para Linux y Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
name	name	Nombre del evento LIDS que ocurrió
message	message	Mensaje de evento que identifica el SO, la identificación de la cuenta de AWS / Azure (si está disponible), el ID de la instancia (si está disponible), así como el nombre de la política de LIDS
deviceCustomString1	server_platform	Plataforma OS (Windows o Linux)
sourceHostName	server_hostname	Nombre de host del activo AWS / Azure

deviceCustomString2	server_group_name	Versión del sistema operativo
deviceHostName	ec2_instance_id	ID del elemento AWS / Azure
deviceCustomString3	ec2_account_id	Etiqueta del servidor: por lo general, el ID de cuenta de AWS o el ID de suscripción de Azure
deviceCustomString4	policy_name	Nombre de la política de LIDS
devicecustomString5	rule_name	Nombre de la regla que se llevó a cabo, identificando el evento
flexString2	original_log_entry	Entrada de registro crudo desde Linux o Windows - ayudará a identificar información adicional que no se puede asignar

TABLA 21: RECURSO DE DATOS COMPROMISED ASSET - ROOT USER COMPROMISED LINUX/WINDOWS FUENTE: ELABORACIÓN PROPIA.

Campos Linux:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	Id	Identificador de evento LIDS
event.Outcome	type	Resultado de la regla de LIDS que desencadenó
name	name	Nombre de los eventos LIDS
deviceReceiptTime	created_at	Hora en que ocurrió el evento
sourceHostName	server_hostname	Nombre de host que se encuentra en AWS o Azure
sourceAddress	server_ip_address	Dirección IP pública del elemento AWS o Azure
sourceDnsDomain	server_reported_fqdn	FQDN del servidor - puede contener la dirección IP privada en el nombre de AWS o Azure activo
sourceTranslatedAddress	server_primary_ip_address	Dirección IP privada del elemento AWS o Azure

TABLA 22: RECURSO DE DATOS COMPROMISED ASSET - ROOT USER COMPROMISED LINUX FUENTE: ELABORACIÓN PROPIA.

Campos Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	<EventID>4625</EventID>	ID de evento de Windows

deviceReceiptTime	<TimeCreated SystemTime='2017-06-13T20:56:18.796455500Z'/>	Hora en que ocurrió el evento
deviceEventCategory	<Channel>Security</Channel>	Tipo de evento de Windows
flexString1	<Computer>VA-EPO-01.EIP-VA.DEMO</Computer>	Nombre de host en el que se ha producido el evento
sourceUserName	<Data Name='SubjectUserName'>-</Data>	Nombre de usuario de origen vinculado al evento
deviceNtDomain	<Data Name='SubjectDomainName'>-</Data>	El dominio del host
destinationUserId	<Data Name='SubjectLogonId'>0x0</Data>	ID de inicio de sesión en Windows
destinationUserName	<Data Name='TargetUserName'>ADMINISTRATOR</Data>	Nombre de usuario específico para el evento
destinationNtDomain	<Data Name='TargetDomainName'></Data>	Nombre de dominio segmentado para el evento
reason	<Data Name='FailureReason'>%%2313</Data>	Código de razón de fallo de Windows
deviceCustomNumber1	<Data Name='LogonType'>3</Data>	Tipo de inicio de sesión de Windows
destinationProcessName	<Data Name='LogonProcessName'>NtLmSsp </Data>	Nombre de proceso de inicio de sesión de Windows
deviceCustomString6	<Data Name='AuthenticationPackageName'>NTLM</Data>	Nombre del paquete de

		autenticación de Windows
sourceHostName	<Data Name='WorkstationName'></Data>	Nombre de la estación de trabajo fuente del evento
sourceProcessId	<Data Name='ProcessId'>0x0</Data>	ID de proceso de Windows
sourceProcessName	<Data Name='ProcessName'>-</Data>	Nombre del proceso de Windows
sourceAddress	<Data Name='IpAddress'>-</Data>	Dirección IP de origen del evento
sourcePort	<Data Name='IpPort'>-</Data>	Puerto de origen del host para el evento

TABLA 23: RECURSO DE DATOS COMPROMISED ASSET - ROOT USER COMPROMISED WINDOWS
FUENTE: ELABORACIÓN PROPIA.

5.3.6.2 Ejemplo de la alerta:

Esta alerta se activa porque se ha producido un ataque exitoso de fuerza bruta en un sistema Linux en el entorno de Azure o AWS que implica una cuenta de usuario root. Para investigar esta alerta, póngase en contacto con el administrador de la cuenta 1234123412341234 y notifíquelos que server.domain.com se ha visto potencialmente comprometido. El ataque se produjo desde la siguiente dirección IP: 10.3.23.13. Resuelva esta alerta una vez que haya confirmado que la actividad era legítima o si está comprometida, asegúrese de que se han restablecido las credenciales del sistema comprometido. El sistema puede necesitar ser puesto en cuarentena para una investigación más profunda y para asegurarse de que no ha ocurrido ninguna otra actividad maliciosa. Trabaje con el administrador del inquilino para

garantizar que no se produzcan futuros ataques contra sus sistemas revisando los estándares de configuración para el entorno de la nube.

5.3.6.3 Entrevista Usuarios Finales - Identificar si la actividad proviene del usuario

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Es consciente el usuario de la autenticación y de las acciones realizadas recientemente por la cuenta de usuario root?

1. Sí -

a. Identificar si el usuario es responsable de estas acciones.

b. Compruebe con el usuario en qué host se registró la cuenta raíz y las acciones realizadas.

c. Si la actividad se identifica como legítima, puede ser validada por el usuario, pero no procede del proxy interno, notificar al usuario que debe tener acceso a sus recursos a través del proxy interno. Si no lo hace, se producirá una escalada en su gerente.

d. Si la actividad se identifica como legítima, puede ser validada por el usuario y procede del proxy, resolver como falso positivo.

2. No -

a. Pida al usuario que restablezca las credenciales de la cuenta. Si no pueden restablecer las credenciales, escalar el problema al administrador con acceso para restablecer las credenciales de la cuenta.

b. ¿Puede el usuario encontrar otras fuentes afectadas en su entorno?

c. ¿Puede el usuario cambiar grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.

d. ¿Qué acciones puede realizar la cuenta? ¿Puede acceder a otros sistemas o datos sensibles?

e. Si la cuenta identificada puede acceder a otros sistemas, recopile información sobre esos hosts para su posible aislamiento junto con el host original identificado en la alerta.

f. Confirme que las credenciales de la cuenta se han restablecido y que el administrador del inquilino de AWS / Azure tiene el control de la cuenta.

5.3.7 Denial of Service - SYN Flood Attack

El propósito de esta alerta es identificar un posible ataque de Denegación de Servicio contra los recursos de AWS / Azure a través de un ataque de SYN Flood. Esta alerta puede ayudar a identificar potenciales actividades maliciosas con la intención de eliminar los recursos AWS / Azure enviando tráfico excesivo a través de paquetes SYN.

5.3.7.1 Recursos de los datos:

Campos compartidos para Linux y Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
name	name	Nombre del evento LIDS que ocurrió
message	message	Mensaje de evento que identifica el SO, la identificación de la cuenta de AWS / Azure (si está disponible), el ID de la instancia (si está disponible), así como el nombre de la política de LIDS
deviceCustomString1	server_platform	Plataforma OS (Windows o Linux)
sourceHostName	server_hostname	Nombre de host del activo AWS / Azure
deviceCustomString2	server_group_name	Versión del sistema operativo
deviceHostName	ec2_instance_id	ID del elemento AWS / Azure
deviceCustomString3	ec2_account_id	Etiqueta del servidor: por lo general, el ID de cuenta de AWS o el ID de suscripción de Azure
deviceCustomString4	policy_name	Nombre de la política de LIDS
devicecustomString5	rule_name	Nombre de la regla que se llevó a cabo, identificando el evento
flexString2	original_log_entry	Entrada de registro crudo desde Linux o Windows - ayudará a identificar información adicional que no se puede asignar

TABLA 24: RECURSO DE DATOS DENIAL OF SERVICE - SYN FLOOD ATTACK LINUX/WINDOWS
FUENTE: ELABORACIÓN PROPIA.

Campos Linux:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	Id	Identificador de evento LIDS
event.Outcome	type	Resultado de la regla de LIDS que desencadenó
name	name	Nombre de los eventos LIDS
deviceReceiptTime	created_at	Hora en que ocurrió el evento
sourceHostName	server_hostname	Nombre de host que se encuentra en AWS o Azure
sourceAddress	server_ip_address	Dirección IP pública del elemento AWS o Azure
sourceDnsDomain	server_reported_fqdn	FQDN del servidor - puede contener la dirección IP privada

		en el nombre de AWS o Azure activo
sourceTranslatedAddress	server_primary_ip_address	Dirección IP privada del elemento AWS o Azure

TABLA 25: RECURSO DE DATOS DENIAL OF SERVICE - SYN FLOOD ATTACK LINUX FUENTE: ELABORACIÓN PROPIA.

Campos Windows:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
eventId	<EventID>4625</EventID>	ID de evento de Windows
deviceReceiptTime	<TimeCreated SystemTime='2017-06-13T20:56:18.796455500Z'/>	Hora en que ocurrió el evento
deviceEventCategory	<Channel>Security</Channel>	Tipo de evento de Windows
flexString1	<Computer>VA-EPO-01.EIP-VA.DEMO</Computer>	Nombre de host en el que se ha producido el evento
sourceUserName	<Data Name='SubjectUserName'>-</Data>	Nombre de usuario de origen vinculado al evento
deviceNtDomain	<Data Name='SubjectDomainName'>-</Data>	El dominio del host
destinationUserId	<Data Name='SubjectLogonId'>0x0</Data>	ID de inicio de sesión en Windows
destinationUserName	<Data Name='TargetUserName'>ADMINISTRATOR</Data>	Nombre de usuario específico para el evento
destinationNtDomain	<Data Name='TargetDomainName'></Data>	Nombre de dominio segmentado para el evento

reason	<Data Name='FailureReason'>%%2313</Data>	Código de razón de fallo de Windows
deviceCustomNumber1	<Data Name='LogonType'>3</Data>	Tipo de inicio de sesión de Windows
destinationProcessName	<Data Name='LogonProcessName'>NtLmSsp </Data>	Nombre de proceso de inicio de sesión de Windows
deviceCustomString6	<Data Name='AuthenticationPackageName'>NTLM</Data>	Nombre del paquete de autenticación de Windows
sourceHostName	<Data Name='WorkstationName'></Data>	Nombre de la estación de trabajo fuente del evento
sourceProcessId	<Data Name='ProcessId'>0x0</Data>	ID de proceso de Windows
sourceProcessName	<Data Name='ProcessName'>-</Data>	Nombre del proceso de Windows
sourceAddress	<Data Name='IpAddress'>-</Data>	Dirección IP de origen del evento
sourcePort	<Data Name='IpPort'>-</Data>	Puerto de origen del host para el evento

TABLA 26: RECURSO DE DATOS DENIAL OF SERVICE - SYN FLOOD ATTACK WINDOWS FUENTE: ELABORACIÓN PROPIA.

5.3.7.2 Ejemplo de la alerta:

Esta alerta se activa cuando un ataque de SYN Flood se ha producido en un sistema Linux (en contra: $ destinationAddress desde la siguiente dirección: $ sourceAddress). Para investigar esta alerta, póngase en contacto con el administrador del sistema atacado. Pida al administrador que confirme que su

configuración de grupo de seguridad de AWS está configurada correctamente y si ha realizado cambios recientes. Esta alerta se puede resolver una vez que la dirección IP ofensiva ya no está causando una posible denegación de servicio.

5.3.7.3 Validar y categorizar el ataque

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Es consciente el usuario del excesivo tráfico de entrada a sus recursos?

1. Sí -

a. ¿Es el usuario responsable de este tráfico?

b. Si es así, ¿cuál es la razón por la que están generando este tráfico? ¿Tienen una razón de negocio y aprobación para realizar esta actividad?

c. ¿Cuál es el propósito de la (s) máquina (s) que está siendo objeto de esta actividad?

d. Si el usuario es responsable, puede proporcionar justificación y tiene la aprobación para realizar esta actividad en su entorno cloud, esta alerta puede ser procesada como un falso positivo.

e. Asesorar al usuario que están generando cantidades excesivas de tráfico de red contra sus recursos que pueden conducir a una denegación de servicio en su entorno, así como llevar a ramificaciones legales con el proveedor de cloud.

f. Si el usuario no detiene la actividad, escalar el caso a su administrador para una acción adicional.

2. No -

a. Proporcione al usuario los detalles del host de origen que se ve afectado por este tráfico. ¿Puede el usuario encontrar la fuente en su entorno y detener el tráfico?

b. ¿Puede el usuario cambiar grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.

c. Confirme que se ha detenido el tráfico excesivo a su (s) recurso (s).

5.3.9 Malware - Malware Outbreak Detected

El propósito de esta alerta es identificar un outbreak de malware tanto para activos locales como para activos de AWS / Azure. Una alerta de outbreak de malware se activa cuando al menos 10 activos (en las instalaciones y / o en la nube) se identifican como infectados con el mismo virus en un plazo de 4 horas y el antivirus lo identifica. Debido a la naturaleza del entorno en la nube, es importante recopilar el ID de cuenta de AWS o el ID de suscripción de Azure junto con el nombre de host de destino (si corresponde) así como la dirección IP de destino para ayudar al usuario a localizar el recurso en su entorno de nube.

5.3.9.1 Recurso de datos:

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
deviceVendor	"Antivirus Vendor"	Antivirus Vendor
deviceProduct		Producto
endTime		Tiempo de ocurrencia
deviceEventCategory	threatcateg	Categoría de amenaza

deviceAction	ActionName	Acción que tomó el antivirus
deviceReceiptTime	datetime	Archivo de tiempo infectado fue descubierto
deviceHostName	serverhostname	Nombre de host del dispositivo infectado
deviceAddress	serveripaddress	Dirección IP del dispositivo infectado
fileName	filename	Nombre del archivo infectado (incluye ruta de acceso)
filePath		Ubicación del archivo infectado (incluye nombre)
deviceCustomDate1.DetectTime	detecttime	Se ha detectado el archivo infectado con el tiempo
deviceCustomString1.VirusName	virusname	Nombre del virus
deviceCustomString2.VirusType	virustype	Muestra el tipo de virus, por ejemplo: Troyano
flexString2		Información de operación y estación de trabajo

TABLA 27: RECURSO DE DATOS MALWARE - MALWARE OUTBREAK DETECTED FUENTE: ELABORACIÓN PROPIA.

5.3.9.2 Ejemplo de la alerta

Esta alerta se dispara porque el antivirus descubrió un Artemis! 4605A5935796 se encontró en 10 máquinas en menos de 4 horas. Esto puede indicar que el malware se está propagando rápidamente en todo el entorno. Investigue esta alerta investigando Artemis! 4605A5935796. Comuníquese con los administradores de los sistemas infectados y, si es posible, determine la causa de la infección o si se produce alguna actividad inusual. Si es posible, poner en cuarentena los sistemas infectados y detener la propagación del virus. Resuelva esta alerta una vez que haya confirmado que la infección ya no se está extendiendo y que los administradores han sido notificados.

5.3.9.3 Entrevista Usuarios finales

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

a. Discuta con el usuario el evento que ocurrió, en qué host ocurrió y confirme el número de cuenta de AWS o el ID de suscripción de Azure.

b. ¿El malware ya estaba en cuarentena?

c. Utilizando las herramientas disponibles, trabaje con el usuario para identificar si el malware ya estaba en cuarentena por las capacidades actuales de AV. Si el malware se ha puesto en cuarentena, se trata de un falso positivo.

d. Si el malware no se puso en cuarentena, trabaje con el usuario para identificar lo siguiente para ayudarlo a analizar más a fondo y comprender cómo ocurrió este evento:

1. ¿Está identificado el malware en un servidor o host final? ¿Son recursos de producción o desarrollo?

2. ¿Cuál es el propósito del servidor o punto final? ¿Contiene información sensible? Esto ayudará a identificar la urgencia y el impacto del outbreak de malware.

3. ¿Ha habido alguna otra actividad inusual en sus otros recursos de la nube?

4. Identificar información adicional sobre la causa de este malware y los comportamientos que aparecen en el host infectado.

5.3.10 Malware - High Number of Infected Hosts

El propósito de esta alerta es identificar un gran número de hosts infectados tanto para activos locales como para activos AWS / Azure. Un alto número de alertas de hosts infectados se activa cuando se identifica que al menos 30 activos (en las instalaciones y / o en la nube) han sido infectados en un plazo de 8 horas y el antivirus lo identifica. Cada activo puede contener diferentes programas maliciosos. Debido a la naturaleza del entorno en la nube, es importante recopilar el ID de cuenta de AWS o el ID de suscripción de Azure junto con el nombre de host de destino (si corresponde) así como la dirección IP de destino para ayudar al inquilino a localizar el recurso en su entorno de nube.

5.3.10.1 Recurso de datos

SIEM Campos	Campos específicos del dispositivo CloudPassage LIDS	Descripción
deviceVendor	"Antivirus Vendor"	Antivirus Vendor
deviceProduct		Producto
endTime		Tiempo de ocurrencia
deviceEventCategory	threatcateg	Categoría de amenaza
deviceAction	ActionName	Acción que tomó el antivirus
deviceReceiptTime	datetime	Archivo de tiempo infectado fue descubierto
deviceHostName	serverhostname	Nombre de host del dispositivo infectado
deviceAddress	serveripaddress	Dirección IP del dispositivo infectado
fileName	filename	Nombre del archivo infectado (incluye ruta de acceso)
filePath		Ubicación del archivo infectado (incluye nombre)
deviceCustomDate1.DetectTime	detecttime	Se ha detectado el archivo infectado con el tiempo
deviceCustomString1.VirusName	virusname	Nombre del virus

deviceCustomString2.VirusType	virustype	Muestra el tipo de virus, por ejemplo: Troyano
flexString2		Información de operación y estación de trabajo

TABLA 28: RECURSO DE DATOS MALWARE - HIGH NUMBER OF INFECTED HOSTS FUENTE: ELABORACIÓN PROPIA.

5.3.10.2 Ejemplo de la alerta.

Esta alerta se activa porque los archivos infectados se encontraron en 30 máquinas en menos de 8 horas. Esto puede indicar que el malware se está propagando rápidamente en todo el entorno. Investigue esta alerta determinando el tipo de virus en los sistemas infectados y si las infecciones están relacionadas. Comuníquese con los administradores de los sistemas infectados y, si es posible, determine la causa de la infección o si se produce alguna actividad inusual que haya ocurrido recientemente. Si es posible, poner en cuarentena los sistemas infectados y detener la propagación del virus. Resolver esta alerta una vez que la propagación de la infección se ha detenido y los propietarios contactados.

5.3.10.3 Entrevista usuarios finales

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

a. Discuta con el usuario el evento que ocurrió, en qué host ocurrió y confirme el número de cuenta de AWS o el ID de suscripción de Azure.

b. ¿El malware ya estaba en cuarentena?

c. Utilizando las herramientas disponibles, trabaje con el usuario para identificar si el malware ya estaba en cuarentena por las capacidades actuales de AV. Si el malware se ha puesto en cuarentena, se trata de un falso positivo.

d. Si el malware no se puso en cuarentena, trabaje con el usuario para identificar lo siguiente para ayudarlo a analizar más a fondo y comprender cómo ocurrió este evento:

1. ¿Está identificado el malware en un servidor o host final? ¿Son recursos de producción o desarrollo?

2. ¿Cuál es el propósito del servidor o punto final? ¿Contiene información sensible? Esto ayudará a identificar la urgencia y el impacto del outbreak de malware.

3. ¿Ha habido alguna otra actividad inusual en sus otros recursos de la nube?

4. Identificar información adicional sobre la causa de este malware y los comportamientos que aparecen en el host infectado.

5.3.11 Compromised Asset - Suspicious Outbound Traffic

El propósito de esta alerta es identificar el mayor tráfico negado entre dos hosts. El aumento del tráfico en el puerto / dirección denegado se puede atribuir a errores de configuración, malware u otra actividad maliciosa de un activo de AWS / Azure. El aumento del tráfico se identifica como un aumento en tráfico anómalo negado por intervalos 10 eventos que comienzan con 20 eventos en 6 minutos todo el camino hasta 60 eventos en 6 minutos. Debido a la naturaleza del entorno de la nube, es importante verificar la dirección de origen con el usuario de la nube afectado para identificar si se pueden vincular a la dirección

IP desconocida debido al acceso a recursos fuera de la red o si se está produciendo un ataque.

5.3.11.1 Recurso de datos

SIEM Campos	VPC Flowlogs Campos específicos del dispositivo	Descripción
deviceVendor	"AWS"	
deviceProduct	“VPC Flowlogs”	
message	status	El estado de registro del registro de flujo: OK: Los datos se registran normalmente en los registros de CloudWatch. NODATA: No hubo tráfico de red hacia o desde la interfaz de red durante la ventana de captura. SKIPDATA: Algunos registros de registro de flujo se omitieron durante la ventana de captura. Esto puede deberse a una restricción de capacidad interna oa un error interno.
deviceVersion	logversion	La versión de los registros de flujo VPC.
deviceExternalId	Account-id	El ID de cuenta de AWS para el registro de flujo.
deviceOutboundInterface	Interface-id	ID de la interfaz de red para la que se aplica el flujo de registro.
startTime	start	La hora, en segundos Unix, del inicio de la ventana de captura.
endTime	end	La hora, en segundos Unix, del final de la ventana de captura.
sourceAddress	srcaddr	La dirección IPv4 o IPv6 de origen. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
destinationAddress	dstaddr	La dirección IPv4 o IPv6 de destino. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
sourcePort	srcport	El puerto de origen del tráfico.
destinationPort	dstport	El puerto de destino del tráfico..
transportProtocol	protocol	El número de protocolo IANA del tráfico. Para obtener más

		información, vaya a Asigned Internet Protocol Numbers.
fileSize	packets	Número de paquetes transferidos durante la ventana de captura.
bytesOut	bytes	El número de bytes transferidos durante la ventana de captura.
deviceAction	action	La acción asociada con el tráfico: ACEPTAR: El tráfico registrado fue permitido por los grupos de seguridad o ACL de red. REJECT: El tráfico registrado no fue permitido por los grupos de seguridad o ACL de red.

TABLA 29: RECURSO DE DATOS COMPROMISED ASSET - SUSPICIOUS OUTBOUND TRAFFIC VPC
FUENTE: ELABORACIÓN PROPIA.

SIEM Campos	Azure Flowlogs Campos específicos de dispositivos	Descripción
deviceVendor	"Microsoft"	
deviceProduct	“Azure NSG Flowlogs”	
event.deviceCustomString1	systemId	Id de recurso de grupo de seguridad de red
event.deviceCustomString2	rule	Regla para la cual se enumeran los flujos
event.deviceCustomString3	resourceid	El Id de recurso del NSG - proporciona el ID de suscripción para Azure
event.deviceCustomString4	mac	La dirección MAC de la NIC para la VM donde se recogió el flujo
event.message	flowTuples	Una cadena que contiene varias propiedades para la tupla de flujo en formato separado por comas
event.transportProtocol	Protocol	El protocolo del flujo. Los valores válidos son T para TCP y U para UDP
event.deviceReceiptTime	Time Stamp	Este valor es la marca de tiempo de cuando el flujo se produjo en el formato EPIX de UNIX
event.deviceAction	Traffic	Si se permitió o se negó el tránsito. Los valores válidos

		son A para permitido y D para negado
event.sourcePort	Source Port	El puerto de origen
event.destinationAddress	Destination IP	El IP de destino
event.deviceCustomString5	Traffic Flow	La dirección del flujo de tráfico. Los valores válidos son I para entrada y O para salida
event.sourceAddress	Source IP	El IP de origen
event.destinationPort	Destination Port	El puerto de destino

TABLA 30: RECURSO DE DATOS COMPROMISED ASSET - SUSPICIOUS OUTBOUND TRAFFIC AZURE FUENTE: ELABORACIÓN PROPIA.

5.3.11.2 Ejemplo de la alerta

Esta alerta se activó porque 31.7.241.253 ha incrementado el tráfico denegado a 10.0.0.46. El aumento del tráfico en la dirección / puerto denegado puede atribuirse a errores de configuración, malware u otra actividad maliciosa. Para investigar esta alerta revise la actividad adicional que está realizando la instancia, y póngase en contacto con el administrador del sistema. Si es posible determinar la causa del aumento del tráfico y detener la actividad. Esta alerta puede resolverse una vez que se ha solucionado el tráfico de salida sospechoso.

5.3.11.3 Entrevistar Usuarios Finales - Identificar si la actividad es legítima o maliciosa

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Es consciente el usuario del tráfico saliente?

1. Sí -

a. Identifique el propósito del usuario para el tráfico de salida identificado.

b. ¿Tienen un caso de negocio para apoyar su justificación del tráfico saliente?

c. ¿Cuál es el propósito de la (s) máquina (es) que está generando esta actividad? ¿Maneja datos sensibles?

d. ¿Qué tipo de tráfico se envía? ¿Se ha identificado algún dato importante o sensible como parte de este tráfico saliente?

e. ¿Cuál es el propósito de la fuente de destino? ¿Por qué se envía este tráfico a la (s) fuente (es)?

f. ¿Son recursos de producción o desarrollo que generan esta actividad?

g. Si el usuario no puede justificar o justificar sus acciones, póngase en contacto con el administrador del usuario para verificación y escalamiento de sus actividades.

h. Si la actividad es identificada como legítima y puede ser validada por el usuario y su gerente, resolver como falso positivo.

2. No -

a. Proporcione al usuario los detalles del host de origen que envía el tráfico recopilado anteriormente. ¿Puede el usuario encontrar la fuente en su entorno y detener el tráfico?

b. ¿Puede el usuario cambiar grupos de seguridad / grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.

c. Confirme que se ha detenido la actividad de salida sospechosa.

5.3.12 Hacking - Suspicious Event - Port Scan

El propósito de esta alerta es identificar un escaneo de puertos que se está produciendo contra activos de AWS / Azure seleccionados. Esta alerta puede ayudar a identificar si un atacante está realizando un reconocimiento en el entorno de la nube y generará actividad si hay al menos 20 eventos desde la misma dirección IP de origen a la misma dirección IP de destino en un período de 5 minutos. Debido a la naturaleza del entorno de la nube, es importante verificar la dirección de origen con el inquilino de la nube afectado para identificar si se pueden vincular a la dirección IP desconocida debido al acceso a recursos fuera de la red o si se está produciendo un ataque.

5.3.12.1 Recurso de datos

SIEM Campos	VPC Flowlogs Campos específicos del dispositivo	Descripción
deviceVendor	"AWS"	
deviceProduct	“VPC Flowlogs”	
message	status	El estado de registro del registro de flujo: OK: Los datos se registran normalmente en los registros de CloudWatch. NODATA: No hubo tráfico de red hacia o desde la interfaz de red durante la ventana de captura. SKIPDATA: Algunos registros de registro de flujo se omitieron durante la ventana de captura. Esto puede deberse a una restricción de capacidad interna oa un error interno.
deviceVersion	logversion	La versión de los registros de flujo VPC.
deviceExternalId	Account-id	El ID de cuenta de AWS para el registro de flujo.
deviceOutboundInterface	Interface-id	ID de la interfaz de red para la que se aplica el flujo de registro.

startTime	start	La hora, en segundos Unix, del inicio de la ventana de captura.
endTime	end	La hora, en segundos Unix, del final de la ventana de captura.
sourceAddress	srcaddr	La dirección IPv4 o IPv6 de origen. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
destinationAddress	dstaddr	La dirección IPv4 o IPv6 de destino. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
sourcePort	srcport	El puerto de origen del tráfico.
destinationPort	dstport	El puerto de destino del tráfico..
transportProtocol	protocol	El número de protocolo IANA del tráfico. Para obtener más información, vaya a Asigned Internet Protocol Numbers.
fileSize	packets	Número de paquetes transferidos durante la ventana de captura.
bytesOut	bytes	El número de bytes transferidos durante la ventana de captura.
deviceAction	action	La acción asociada con el tráfico: ACEPTAR: El tráfico registrado fue permitido por los grupos de seguridad o ACL de red. REJECT: El tráfico registrado no fue permitido por los grupos de seguridad o ACL de red.

TABLA 31: RECURSO DE DATOS HACKING - SUSPICIOUS EVENT - PORT SCAN VPC FUENTE: ELABORACIÓN PROPIA.

SIEM Campos	Azure Flowlogs Campos específicos de dispositivos	Descripción
deviceVendor	"Microsoft"	
deviceProduct	“Azure NSG Flowlogs”	
event.deviceCustomString1	systemId	Id de recurso de grupo de seguridad de red
event.deviceCustomString2	rule	Regla para la cual se enumeran los flujos
event.deviceCustomString3	resourceid	El Id de recurso del NSG - proporciona el ID de suscripción para Azure

event.deviceCustomString4	mac	La dirección MAC de la NIC para la VM donde se recogió el flujo
event.message	flowTuples	Una cadena que contiene varias propiedades para la tupla de flujo en formato separado por comas
event.transportProtocol	Protocol	El protocolo del flujo. Los valores válidos son T para TCP y U para UDP
event.deviceReceiptTime	Time Stamp	Este valor es la marca de tiempo de cuando el flujo se produjo en el formato EPIX de UNIX
event.deviceAction	Traffic	Si se permitió o se negó el tránsito. Los valores válidos son A para permitido y D para negado
event.sourcePort	Source Port	El puerto de origen
event.destinationAddress	Destination IP	El IP de destino
event.deviceCustomString5	Traffic Flow	La dirección del flujo de tráfico. Los valores válidos son I para entrada y O para salida
event.sourceAddress	Source IP	El IP de origen
event.destinationPort	Destination Port	El puerto de destino

TABLA 32: RECURSO DE DATOS RECURSO DE DATOS HACKING - SUSPICIOUS EVENT - PORT SCAN AZURE FUENTE: ELABORACIÓN PROPIA.

5.3.12.2 Ejemplo de la alerta

Esta alerta se activó porque se detectó una exploración de puerto potencial. 91.211.3.106 se ha comunicado más de 20 veces en 5 minutos con 10.0.0.18 en el entorno de cloud del SIEM. Esta actividad podría ser un atacante que realiza reconocimientos sobre el medio ambiente. Para investigar esta alerta, comience por ver el tráfico adicional desde 91.211.3.106. El administrador del SIEM debe ser notificado de la actividad. Para obtener más información sobre el propietario del activo revise los campos: ID externo del dispositivo (para AWS), para Azure la suscripción se puede encontrar en la siguiente cadena:

deviceCustomString3. Determine si se está produciendo el escaneo de puertos debido a la configuración incorrecta del grupo de seguridad (si se trata de una cuenta AWS) o a un grupo de seguridad de red incorrecto (cuenta Azure). Si es posible, determine si 91.211.3.106 es un activo propiedad del usuario y póngase en contacto con el propietario para determinar si la actividad es maliciosa. Resuelva esta alerta una vez que la actividad se ha detenido al reconfigurar las configuraciones de grupo de seguridad o NSG.

5.3.12.3 Entrevistar Usuarios Finales - Identificar si la actividad es legítima o maliciosa

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Es consciente el usuario del tráfico entrante sospechoso contra sus hosts?

1. Sí -

a. ¿Es el usuario responsable de este tráfico?

b. Si es así, ¿cuál es la razón por la que están generando este tráfico? ¿Tienen un permiso de negocio u aprobación para realizar esta actividad?

c. ¿Cuál es el propósito de la (s) máquina (s) que está siendo objeto de esta actividad?

d. Si el usuario es responsable, puede proporcionar justificación y tiene la aprobación para realizar esta actividad en su entorno cloud, esta alerta puede ser procesada como un Falso Positivo.

e. Asesorar al usuario que están generando cantidades excesivas de tráfico de red contra sus recursos que pueden conducir a una denegación de servicio en su entorno, así como llevar a ramificaciones legales con el proveedor de cloud.

f. Si el usuario no detiene la actividad, escalar el caso a su administrador para la acción adicional.

2. No -

a. Proporcione al usuario los detalles del host de origen que envía el tráfico recopilado anteriormente. ¿Puede el usuario encontrar la fuente en su entorno y detener el tráfico?

c. ¿Puede el usuario cambiar grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.

d. Confirme que la actividad sospechosa ha sido detenida.

5.3.13 Hacking - Suspicious Event - Address Sweep Attack Detected

El propósito de esta alerta es identificar un ataque de barrido de direcciones que está ocurriendo contra los activos de AWS / Azure. Esta alerta puede ayudar a identificar si un atacante realiza un reconocimiento en el entorno de la nube y generará actividad si hay al menos 20 eventos desde la misma dirección IP de origen a la misma dirección IP de destino en un período de 1 minuto. Debido a la naturaleza del entorno de la nube, es importante verificar la dirección de origen con el usuario de la nube afectado para identificar si se

pueden vincular a la dirección IP desconocida debido al acceso a recursos fuera de la red o si se está produciendo un ataque.

5.3.13.1 Recurso de datos

SIEM Campos	VPC Flowlogs Campos específicos del dispositivo	Descripción
deviceVendor	"AWS"	
deviceProduct	“VPC Flowlogs”	
message	status	El estado de registro del registro de flujo: OK: Los datos se registran normalmente en los registros de CloudWatch. NODATA: No hubo tráfico de red hacia o desde la interfaz de red durante la ventana de captura. SKIPDATA: Algunos registros de registro de flujo se omitieron durante la ventana de captura. Esto puede deberse a una restricción de capacidad interna oa un error interno.
deviceVersion	logversion	La versión de los registros de flujo VPC.
deviceExternalId	Account-id	El ID de cuenta de AWS para el registro de flujo.
deviceOutboundInterface	Interface-id	ID de la interfaz de red para la que se aplica el flujo de registro.
startTime	start	La hora, en segundos Unix, del inicio de la ventana de captura.
endTime	end	La hora, en segundos Unix, del final de la ventana de captura.
sourceAddress	srcaddr	La dirección IPv4 o IPv6 de origen. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
destinationAddress	dstaddr	La dirección IPv4 o IPv6 de destino. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
sourcePort	srcport	El puerto de origen del tráfico.
destinationPort	dstport	El puerto de destino del tráfico..
transportProtocol	protocol	El número de protocolo IANA del tráfico. Para obtener más

		información, vaya a Asigned Internet Protocol Numbers.
fileSize	packets	Número de paquetes transferidos durante la ventana de captura.
bytesOut	bytes	El número de bytes transferidos durante la ventana de captura.
deviceAction	action	La acción asociada con el tráfico: ACEPTAR: El tráfico registrado fue permitido por los grupos de seguridad o ACL de red. REJECT: El tráfico registrado no fue permitido por los grupos de seguridad o ACL de red.

TABLA 33: RECURSO DE DATOS HACKING - SUSPICIOUS EVENT - ADDRESS SWEEP ATTACK DETECTED VPC FUENTE: ELABORACIÓN PROPIA.

SIEM Campos	Azure Flowlogs Campos específicos de dispositivos	Descripción
deviceVendor	"Microsoft"	
deviceProduct	“Azure NSG Flowlogs”	
event.deviceCustomString1	systemId	Id de recurso de grupo de seguridad de red
event.deviceCustomString2	rule	Regla para la cual se enumeran los flujos
event.deviceCustomString3	resourceid	El Id de recurso del NSG - proporciona el ID de suscripción para Azure
event.deviceCustomString4	mac	La dirección MAC de la NIC para la VM donde se recogió el flujo
event.message	flowTuples	Una cadena que contiene varias propiedades para la tupla de flujo en formato separado por comas
event.transportProtocol	Protocol	El protocolo del flujo. Los valores válidos son T para TCP y U para UDP
event.deviceReceiptTime	Time Stamp	Este valor es la marca de tiempo de cuando el flujo se produjo en el formato EPIX de UNIX
event.deviceAction	Traffic	Si se permitió o se negó el tránsito. Los valores válidos

		son A para permitido y D para negado
event.sourcePort	Source Port	El puerto de origen
event.destinationAddress	Destination IP	El IP de destino
event.deviceCustomString5	Traffic Flow	La dirección del flujo de tráfico. Los valores válidos son I para entrada y O para salida
event.sourceAddress	Source IP	El IP de origen
event.destinationPort	Destination Port	El puerto de destino

TABLA 34: RECURSO DE DATOS HACKING - SUSPICIOUS EVENT - ADDRESS SWEEP ATTACK DETECTED AZURE FUENTE: ELABORACIÓN PROPIA.

5.3.13.2 Ejemplo de la alerta

Esta alerta se activó porque se detectó un potencial ataque de barrido de direcciones. 81.30.144.118 se ha comunicado más de 20 veces en 1 minuto con varios sistemas en el entorno de la nube. Esta actividad podría ser un atacante que realiza reconocimientos sobre el medio ambiente. Para investigar esta alerta, comience por observar el tráfico adicional desde 81.30.144.118 y determinar si hay actividad adicional en instancias de la misma cuenta mirando los campos: Device External ID (AWS) o DeviceCustomString3 (Azure). El administrador debe ser notificado de la actividad. Determine si la actividad de ataque de barrido se está produciendo debido a configuraciones incorrectas de grupos de seguridad (si se trata de cuentas AWS) o a configuraciones de grupos de seguridad de red (si se trata de una suscripción Azure). Si es posible, determine si el 81.30.144.118 es un activo propiedad del usuario y contacte al propietario para investigar la causa de la actividad. Resuelva esta alerta una vez que la actividad se ha detenido al reconfigurar las configuraciones de grupo de seguridad o NSG.

5.3.12.3 Entrevistar Usuarios Finales - Identificar si la actividad es legítima o maliciosa

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Es consciente el usuario del tráfico entrante sospechoso contra sus hosts?

1. Sí -

a. ¿Es el usuario responsable de este tráfico?

b. Si es así, ¿cuál es la razón por la que están generando este tráfico? ¿Tienen un permiso de negocio u aprobación para realizar esta actividad?

c. ¿Cuál es el propósito de la (s) máquina (s) que está siendo objeto de esta actividad?

d. Si el usuario es responsable, puede proporcionar justificación y tiene la aprobación para realizar esta actividad en su entorno cloud, esta alerta puede ser procesada como un Falso Positivo.

e. Asesorar al usuario que están generando cantidades excesivas de tráfico de red contra sus recursos que pueden conducir a una denegación de servicio en su entorno, así como llevar a ramificaciones legales con el proveedor de cloud.

f. Si el usuario no detiene la actividad, escalar el caso a su administrador para la acción adicional.

2. No -

a. Proporcione al usuario los detalles del host de origen que envía el tráfico recopilado anteriormente. ¿Puede el usuario encontrar la fuente en su entorno y detener el tráfico?

c. ¿Puede el usuario cambiar grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.

d. Confirme que la actividad sospechosa ha sido detenida.

5.3.14 Compromised Asset - Excessive Traffic to Known Bad IP Address

El propósito de esta alerta es identificar el tráfico excesivo que se envía desde un activo AWS / Azure a una dirección IP defectuosa conocida. Una dirección IP defectuosa conocida se deriva de la lista de de amenazas que contiene direcciones IP malintencionadas conocidas. Esta alerta puede ayudar a identificar un host potencialmente comprometido debido al tráfico que se está enviando a este destino malicioso. Esta alerta también puede ayudar a identificar las configuraciones erróneas en los activos de AWS / Azure que el usuario de la nube debe corregir. Debido a la naturaleza del entorno de la nube, es importante verificar la dirección de origen con el usuario de la nube afectado para identificar si se pueden vincular a la dirección IP desconocida debido al acceso a recursos fuera de la red o si se está produciendo un ataque.

5.3.14.1 Recurso de datos

SIEM Campos	VPC Flowlogs Campos específicos del dispositivo	Descripción
deviceVendor	"AWS"	
deviceProduct	“VPC Flowlogs”	

message	status	El estado de registro del registro de flujo: OK: Los datos se registran normalmente en los registros de CloudWatch. NODATA: No hubo tráfico de red hacia o desde la interfaz de red durante la ventana de captura. SKIPDATA: Algunos registros de registro de flujo se omitieron durante la ventana de captura. Esto puede deberse a una restricción de capacidad interna oa un error interno.
deviceVersion	logversion	La versión de los registros de flujo VPC.
deviceExternalId	Account-id	El ID de cuenta de AWS para el registro de flujo.
deviceOutboundInterface	Interface-id	ID de la interfaz de red para la que se aplica el flujo de registro.
startTime	start	La hora, en segundos Unix, del inicio de la ventana de captura.
endTime	end	La hora, en segundos Unix, del final de la ventana de captura.
sourceAddress	srcaddr	La dirección IPv4 o IPv6 de origen. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
destinationAddress	dstaddr	La dirección IPv4 o IPv6 de destino. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada.
sourcePort	srcport	El puerto de origen del tráfico.
destinationPort	dstport	El puerto de destino del tráfico..
transportProtocol	protocol	El número de protocolo IANA del tráfico. Para obtener más información, vaya a Asigned Internet Protocol Numbers.
fileSize	packets	Número de paquetes transferidos durante la ventana de captura.
bytesOut	bytes	El número de bytes transferidos durante la ventana de captura.
deviceAction	action	La acción asociada con el tráfico:

		ACEPTAR: El tráfico registrado fue permitido por los grupos de seguridad o ACL de red. REJECT: El tráfico registrado no fue permitido por los grupos de seguridad o ACL de red.

TABLA 35: RECURSO DE DATOS COMPROMISED ASSET - EXCESSIVE TRAFFIC TO KNOWN BAD IP ADDRESS VPC FUENTE: ELABORACIÓN PROPIA.

SIEM Campos	Azure Flowlogs Campos específicos de dispositivos	Descripción
deviceVendor	"Microsoft"	
deviceProduct	“Azure NSG Flowlogs”	
event.deviceCustomString1	systemId	Id de recurso de grupo de seguridad de red
event.deviceCustomString2	rule	Regla para la cual se enumeran los flujos
event.deviceCustomString3	resourceid	El Id de recurso del NSG - proporciona el ID de suscripción para Azure
event.deviceCustomString4	mac	La dirección MAC de la NIC para la VM donde se recogió el flujo
event.message	flowTuples	Una cadena que contiene varias propiedades para la tupla de flujo en formato separado por comas
event.transportProtocol	Protocol	El protocolo del flujo. Los valores válidos son T para TCP y U para UDP
event.deviceReceiptTime	Time Stamp	Este valor es la marca de tiempo de cuando el flujo se produjo en el formato EPIX de UNIX
event.deviceAction	Traffic	Si se permitió o se negó el tránsito. Los valores válidos son A para permitido y D para negado
event.sourcePort	Source Port	El puerto de origen
event.destinationAddress	Destination IP	El IP de destino
event.deviceCustomString5	Traffic Flow	La dirección del flujo de tráfico. Los valores válidos son I para entrada y O para salida
event.sourceAddress	Source IP	El IP de origen
event.destinationPort	Destination Port	El puerto de destino

TABLA 36: RECURSO DE DATOS COMPROMISED ASSET - EXCESSIVE TRAFFIC TO KNOWN BAD IP ADDRESS AZURE FUENTE: ELABORACIÓN PROPIA.

5.3.14.2 Ejemplo de la alerta

Esta alerta se activó porque una instancia (69.195.159.158) ha interactuado con una dirección IP defectuosa conocida: (10.0.0.38). La dirección 10.0.0.38 se ha encontrado en la lista de inteligencia de amenazas local que contiene direcciones IP defectuosas conocidas o una lista de méritos similares. El tráfico a esta dirección IP podría revelar que el 69.195.159.158 (cuenta externa de AWS Device External ID) (Azure Subscription: deviceCustomString3) está infectado con malware, está siendo utilizado para actividades malintencionadas, está mal configurado o tiene otros problemas. Para investigar esta alerta, determine el tipo de tráfico, la cantidad, los tamaños de paquetes y otra información encontrada en eventos similares de la Instancia. Póngase en contacto con el administrador local del sistema SIEM e infórmele del problema. Resuelva esta alerta una vez que haya confirmado la causa del tráfico y se ha detenido.

5.3.14.3 Entrevistar Usuarios Finales - Identificar si la actividad es legítima o maliciosa

Entrevistar al usuario final y discutir los eventos que han tenido lugar en su entorno, hacer preguntas para entender la actividad que se llevó a cabo que ayudará a identificar si las acciones pueden ser justificadas o más investigación es necesaria.

¿Es consciente el usuario del tráfico excesivo a la dirección IP incorrecta identificada?

1. Sí -

a. Identifique el propósito del usuario para el tráfico de salida identificado.

b. ¿Tienen un caso de negocio para apoyar su justificación del tráfico saliente?

d. ¿Cuál es el propósito de la (s) máquina (es) que está generando esta actividad? ¿Maneja datos sensibles?

e. ¿Qué tipo de tráfico se envía? ¿Se ha identificado algún dato importante o sensible como parte de este tráfico saliente?

f. ¿Cuál es el propósito de la fuente de destino? ¿Por qué se envía este tráfico a la (s) fuente (es)?

g. ¿Son recursos de producción o desarrollo que generan esta actividad?

h. Si el usuario no puede justificar o justificar sus acciones, póngase en contacto con el administrador del usuario para verificación y escalamiento de sus actividades.

i. Si la actividad es identificada como legítima y puede ser validada por el usuario y su gerente, resolver estas alertas como falsas positivas.

2. No -

a. Proporcione al usuario los detalles del host de origen que envía el tráfico. ¿Puede el usuario encontrar la fuente en su entorno y detener el tráfico?

b. ¿Puede el usuario cambiar grupos de seguridad de red o resolver a nivel de sistema? Si no, escalar el problema al administrador con acceso para bloquear el acceso a la red.

c. Confirme que se ha detenido la actividad de salida sospechosa.

Capítulo 6 Conclusiones

La presente tesis tuvo como objetivo proponer una solución centralizada de administración de registros (logs) y amenazas que proporciona visibilidad en el entorno de nube cruzada de la infraestructura basada en el resultado del SIEM (Información de seguridad y administración de eventos) para el registro y monitoreo de todo su entorno de nube. Esto con el objetivo de ayudar al análisis, administración y monitoreo del entorno del cloud computing para defender a las empresas, ya sean medianas o grandes al control de lo que entra o sale en el entorno de la nube cruzada a través de la infraestructura de internet, además sirve como una manera de referencia o idea para quienes quieran implementar estos métodos para el futuro del cloud computing enfocado en la ciberseguridad.

Uno de los objetivos necesarios para el desarrollo de esta tesis es definir las fuentes selectas de logs en el entorno de nube cruzada del SIEM existente, para demostrar esto según el Capítulo 4.1, donde se definen las bases de lo que se desea y necesita analizar, colectando unas serie de logs que nos ayudarán con el análisis de las alertas además de la creación de las mismas, normalmente en este tipo de sistemas de nube cruzadas existen miles de datos, sin embargo haciendo una selección de los más importantes para identificar amenazas lograremos la creación de las alertas necesarias indispensable para el análisis de las mismas. Cabe destacar que es muy importante, según se demostró en la presente tesis, hacer un listado de las prioridades de los logs dividiendo estos por prioridad máxima, media y menos indispensables para llevar a cabo las respuesta a incidentes, información contextual para las investigaciones de

seguridad, además para optimizar la seguridad y el funcionamiento del entorno / aplicación.

Además, se debía de demostrar según múltiples escenarios la identificación de las amenazas más comunes dentro de la nube cruzada, dentro del Capítulo 4.2 se enlistó una serie de amenazas a los activos de información que residen en la nube y sus posibles vulnerabilidades. Además se debe de identificar el tipo de información que se pude ver amenazada si entra en categorías de la confidencialidad, integridad y disponibilidad. Parte de la investigación referente a esta tesis es identificar qué tipo de atacantes son las que vulneran los activos y la infraestructura existente en este caso los dividimos entre internos y externos. Las vulnerabilidades existieron mucho antes de que la computación en nube se pusiera de moda, además ante el crecimiento de la economía, es sumamente importante resolver cualquier problema que pueda causar bloqueos en este nuevo paradigma de la informática como lo es cloud computing, por lo tanto es importante mantener controles estrictos sobre estos para evitar estas amenazas y vulnerabilidades.

Seguidamente con base en las amenazas expuestas realizamos una exploración para exponer un conjunto de reglas en el SIEM con el fin de monitorear y tratar los eventos recibidos, según se explica detalladamente en el Capítulo 4.3, además se proponen una lista de instrucciones para identificar de mejor manera las amenazas de forma proactiva recibidas en el SIEM. Con estas alertas tenemos la oportunidad de erradicar un problema que requiere una acción inmediata aparte de proactivamente, tenemos la oportunidad de realizar una mejora en los procesos y en el accionar de cada analista, además es

importante recalcar que se puede erradicar una debilidad en la infraestructura existente.

Referencias

Glosario Cloud Computing 2017, Revista Cloud Computing – Glosario Cloud Computing. (2017). Extraido en el 2017 de, https://www.revistacloudcomputing.com/glosario-cloud-computing.

Glosario Cloud Computing 2016, Cloudlatam – Glosario del Cloud Computing. (2016). Extraido en el 2016 de, http://www.cloudlatam.com/glosario-del-cloud-computing.

Servidor Cloud Glosario 2015, Estudio del Cloud Computing Retos y Oportunidades. (2015) Extraido en el 2015 de, https://www.arsys.es/microsites/servidor-cloud/glosario.

Glosario sobre tecgnologia en la nube 2016, Ontsi (2016). Extraido en el 2016 de, http://www.ontsi.red.es/ontsi/sites/default/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf

Incibe – Instituto nacional de cibersuguridad 2016 – Glosario. (2016). Extraido en el 2016 de, https://www.incibe.es/glossary/Formacion/Glosario.

Australian Goverment - Department of Finance 2014. *Australian Government Cloud.* (2014). Extraido de de, http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf

Los 10 terminos claves de la computacion en la nube 2014. Delgado, A. (2014). Extraido el 23 de Marzo de 2014, http://www.vanguardia.com/actualidad/tecnologia/252327-los-10-terminos-claves-de-la-computacion-en-la-nube

The History of Cloud Computing 2013. ECI. (2013). Extraido en el 2013 de, http://www.eci.com/cloudforum/cloud-computing-history.html

Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe 2009. Etro, F. (2009). Extraido en el 2009 de, http://www.techpolicy.com/Articles/E/Economic-Impact-of-Cloud-Computing-on-Business-Cre.aspx

European Network and Information Security Agency 2009 (ENISA). (2009). (varios, Ed.) Extraido en el 2009 de, *https://www.enisa.europa.eu/*.

Study on Cloud Computing Model and its Benefits, *Challenges 2015.* K.Kavitha. (2015). Extraido de http://www.rroij.com/: http://www.rroij.com/open-access/study-on-cloud-computing-model-and-itsbenefits-challenges.php?aid=44804

El análisis de información y las investigaciones cuantitativa y cualitativa 2007. Sarduy Domínguez, Y. (2007). Extraido en el 2007 de, http://bvs.sld.cu/revistas/spu/vol33_3_07/spu20207.htm

Security Issues and challenges in Cloud Computing 2014. T.Ambika. (2014). Extraido el 12 de Diciembre del 2014 de, http://ijarcet.org/wp-content/uploads/IJARCET-VOL-3-ISSUE-12-4343-4348.pdf

Cloud Computing – A Viable Option? 2012. Team, P. M. (2012). Extraido en el 2012 de, https://www.pondurance.com/cloud-computing-a-viable-option/

Cloud Computing Policy 2010. U.S. Department of Commerce. (2010). Extraido en el 2010 de, http://ocio.os.doc.gov/ITPolicyandPrograms/Policy___Standards/PROD01_009505

Gartner confirms what we all know: AWS and Microsoft are the cloud leaders, by a fair way 2017, Gartner. (2017). Extraido el19 Junio 2017. *https://www.theregister.co.uk/2017/06/19/gartner_confirms_what_we_all_know_aws_and_microsoft_are_the_cloud_leaders_by_a_fair_way/*

SIEM/Log Management Security Log Management - Security Intelligence 2016. E*vercom. (2016), Extraido en el 2016 de, http://evercom.controlcloud.com.au/SIEMLogManagement*

Glosario

Abreviaturas Cloud Computing

Fuente (Revista Cloud Computing Glosario Cloud Computing)

API: “Application Programming Interface”. Es una interfaz que permite a las aplicaciones de terceros, solicitar datos y tenerlos de vuelta en un formato predefinido y de acuerdo a normas específicas. Constituye el mecanismo más utilizado de comunicación entre aplicaciones.

App: “Application software”. Es el término utilizado comúnmente como abreviatura de aplicación informática, la cual se define como un programa informático diseñado para ayudar al usuario a realizar una serie de tareas específicas. Además, las aplicaciones pueden ser estándar o desarrollados a medida para cubrir las necesidades particulares de un usuario en concreto.

BaaS: “Backend as a Service”. También conocida como MBaaS (Mobile Backend as a Service), básicamente se refiere a la conexión entre aplicaciones móviles y servicios en la nube.

Backup: Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en una computadora con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados. Los dispositivos más empleados para llevar a cabo la técnica de backup pueden ser cintas magnéticas, DVD, discos duros, discos ópticos, USB o hasta incluso la implementación de un servicio remoto de copia de seguridad.

BPM: “Business Process Management”. Gestión de Procesos de Negocio, el BPM se refiere al tipo de gestión empresarial consistente en la integración de los procesos, las personas y los sistemas tecnológicos de la compañía, en aras de facilitar el desarrollo de las estrategias de negocio de la entidad.

Cloud Computing: Es un nuevo concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos no están en el PC o equipos del usuario, sino que están ubicado en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente a través “la Nube” de Internet, de una forma sencilla y cómoda.

Clúster: Conjunto de servidores que trabajan como una única máquina mejorando el desempeño de las transacciones y operaciones implantadas en este sistema.

Colocation: Servicio ofrecido por las empresas que proveen centros de datos en sus instalaciones donde se instalan servidores y sistemas de conectividad para proveer un área de procesamiento o almacenamiento fuera de las instalaciones del negocio.

CPD: Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.

CRM: “Customer Retationship Management”. Gestión de la relación con el cliente, son herramientas informáticas dedicadas a la gestión integrada de información sobre clientes. Estas aplicaciones permiten, desde almacenar y organizar esta información, hasta integrar, procesar y analizar la misma.

DaaS: “Datacenter as a Service. ”Modelo tecnológico por el que un proveedor ofrece una plataforma virtual que engloba una solución de centro de datos completo para el cliente. Son soluciones normalmente adaptadas a grandes empresas que precisan vastos modelos de computación.

DaaS: “Desktop as a Service”. Modelo de negocio en el que el proveedor facilita una solución de escritorio remoto. Esto permite a cada usuario disponer del mismo escritorio sea cual sea el terminal utilizado, y permite reducir la cantidad de licencias necesarias para mantener distintos dispositivos (PC, portátil, PC en casa,…), e incorpora las medidas de seguridad necesarias para que el acceso a este tipo de entornos sea seguro.

Data Center: Un centro de almacenaje de datos y que provee servicios de negocio que entrega de forma segura aplicaciones y datos a usuarios remotos a través de Internet.

End to End: extremo a extremo, se trata de soluciones cloud basadas en el principio del end-to-end, el cual establece que las funciones específicas de las aplicaciones deben residir en el host final de una red y no en los nodos intermedios, siempre y cuando puedan ser implementadas completa y correctamente en dicho host final.

Grid Computing: Tecnología que permite la coordinación de todo tipo de recursos heterogéneos (cómputo, almacenamiento, aplicaciones, etc., de diferentes arquitecturas), trabajando de forma descentralizada. Supone el uso integrado de equipamiento de alto rendimiento, redes, y bases de datos ubicadas en distintas instituciones. Suele utilizarse este modelo por universidades o laboratorios de investigación, que se asocian, obteniendo así resultados sinérgicos.

IaaS: “Infraestracture as a Service” o “Infraestructura como Servicio”. Con una Infraestructura como servicio (Iaas) lo que se tiene es una solución basada en

virtualización en la que se paga por consumo de recursos: espacio en disco utilizado, tiempo de CPU, espacio en base de datos y transferencia de datos.

ISO27001: Estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la metodología del Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).

ITIL: “Information Technology Infrastructure Library”, es una recopilación de las mejores prácticas en la industria de las tecnologías de la información, en cuanto a los procesos referentes a la provisión de servicios de tecnología de información a las empresas y organizaciones.

Mainframe: Computadora de gran capacidad de cómputo y costosa, utilizada principalmente en empresas que necesitan procesar gran cantidad de datos o soportar gran cantidad de usuarios. Puede funcionar durante largos períodos de tiempo sin ninguna interrupción, pudiéndose reparar en funcionamiento.

Máquina Virtual: Computadora que está construido utilizando recursos virtualizados. Este sistema se comporta a nivel lógico de manera idéntica a la de un computador físico, de modo que el Sistema Operativo o aplicaciones que corren sobre él no detectan la diferencia.

Multitenancy: Uso común entre todos los clientes y usuarios de los servicios de computación en la nube desde la misma plataforma tecnológica del proveedor contratado.

Nube Pública: Hace referencia al modelo estándar de Cloud Computing, en donde el prestador de estos servicios pone a disposición de cualquier usuario en Internet su infraestructura.

Nube Privada: Empleando los mismos preceptos que el Cloud Computing tradicional, ofrece los mismos servicios pero en la propia infraestructura del cliente.

Nube Híbrida: Es una combinación de las mejores características de los modelos de Cloud Privado y Público.

On-demand: Término referido al concepto de —bajo demanda. Dentro del ámbito tecnológico se utiliza para expresar la flexibilidad de los productos cloud, basados en un modelo de pago por uso y en los cuales el proveedor pone a disposición del cliente todos sus recursos, pudiéndolos usar bajo petición previa.

On-premise: Modelo referido al esquema tradicional de licenciamiento, es decir la empresa adquiere las licencias que le otorgan derecho de uso de los sistemas del proveedor, los integra en sus propias instalaciones y mantiene sus datos dentro de su propia infraestructura de tecnología.

OpenNebula: Software de código abierto enfocado a la virtualización de centros de datos y sistemas en la Nube, por medio de esta herramienta se pueden construir nubes ya sean públicas, privadas o híbridas.

Open Source: El software libre no debe ser confundido con el software gratuito o freeware. El software libre no tiene por qué ser gratuito, sino que adquiere su denominación por el hecho de que el código fuente es “Código Abierto” (Open Source). Los programas bajo licencia GPL (“General Public License”), una vez adquiridos, pueden ser usados, copiados, modificados y redistribuidos libremente, salvo determinados casos en los que se indiquen ciertas restricciones, como la obligación de distribuir el software con la misma licencia.

PaaS: “Platform as a Service” o “Plataforma como Servicio”. Es el resultado de la aplicación al desarrollo de Software del modelo SaaS . El modelo PaaS abarca el ciclo completo para desarrollar e implantar aplicaciones desde Internet.

RaaS: “Robot as a Service”, Robot como Servicio, es la entrega como un servicio, de un software que permite a un usuario dar de alta a un robot para realizar ciertas acciones. La utilización de este tipo de servicios cloud se centra en su uso para dar asistencia médica, para el control remoto de equipos de minería, para unidades militares autónomas, para líneas de fabricación industrial, para exploración espacial, etc.

SaaS: “Software as a Service” o “Software como Servicio”. Es aquella aplicación ofrecida por su creador a través de Internet para su utilización por varios clientes manteniendo la privacidad de sus datos y la personalización de la aplicación.

SLA: “Service Level Agreement” o “Acuerdo de Nivel de Servicio”. Es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a hacerlo bajo determinadas condiciones y con unas prestaciones mínimas.

Storage: En un computador, el storage es el lugar donde los datos son guardados para acceder a ellos de forma electromagnética u óptica por el procesador de la computadora.

TI o IT: Tecnologías de la Información.

TIC o ICT: Tecnologías de la Información y la Comunicación.

Vblock: Los paquetes de infraestructura Vblock son plataformas validadas de infraestructuras integradas y desarrolladas por Cisco, EMC y VMware, que ofrecen capacidades de virtualización.

Virtualización: Es el concepto que describe cómo en un solo computador físico se coordina el uso de los recursos para que varios sistemas operativos puedan funcionar al mismo tiempo de forma independiente y sin que ellos (los SO) sepan que están compartiendo recursos con otros sistemas operativos.

VMWare: Es el nombre que lleva el software de virtualización de servidores (Virtual Machine), por extensión de la marca de la empresa que lo facilita. Se trata de un sistema de virtualización por software, en el que se emula un sistema físico (computadora) con unas características de hardware determinadas. VMWare permite ejecutar varios sistemas operativos de forma independiente sobre una infraestructura física.

VPN: “Virtual Private Network”, Red Privada Virtual, son configuraciones de redes informáticas que incluyen equipos que no pueden estar físicamente conectados a la red por motivos geográficos, posibilitando mediante el acceso en remoto y a través de Internet, que el personal de la compañía pueda acceder a la información que necesiten de su empresa, aunque ésta sea de carácter privado.