ManageEngine
Log360

CÓMO SACAR EL MÁXIMO PROVECHO A SU SIEM

EL MANUAL PARA LOS ANALISTAS DE SEGURIDAD

¡Incluye entrevistas con 3 profesionales de la seguridad informática!

Ram Vaidyanathan
& Tanya Austin

Índice

Introducción

Los ataques cibernéticos se han vuelto más sofisticados y selectivos en los últimos tiempos. Los adversarios están realizando su debida diligencia de antemano y adquiriendo la infraestructura adecuada, comprometiendo las cuentas de los usuarios pertinentes y desarrollando funciones específicas para derribar las organizaciones. En este contexto, los analistas de seguridad informática deben desempeñar un rol fundamental en la función de seguridad de sus organizaciones.

Para lograr este objetivo más amplio, los analistas de seguridad informática deben:

1. **Mantener las configuraciones estándar:**
   Un analista de seguridad informática debe garantizar que todos los recursos de la red estén configurados de forma segura y correcta de acuerdo con las políticas de seguridad de la organización y los mandatos de cumplimiento pertinentes.

2. **Evaluar el riesgo:**
   El analista debe realizar frecuentes evaluaciones de riesgo para conocer las amenazas y vulnerabilidades que existen en la red. También deben ser conscientes del impacto empresarial de un posible incidente de seguridad.

3. **Obtener visibilidad de todas las actividades de una red:**
   En cualquier momento, un analista de seguridad debe tener visibilidad de todas las actividades en la red. Deberían ser capaces de obtener los logs de seguridad pertinentes de toda la red para conseguir esta visibilidad.

4. **Monitorear las amenazas:**
   Deben monitorear las amenazas a la seguridad y los indicadores de peligro utilizando técnicas como la correlación de eventos, la inteligencia sobre amenazas, la detección de anomalías y las alertas.

5. **Realizar una investigación forense:**
   En caso de que se produzca un incidente, tienen que hacer una investigación forense para examinar detalladamente la causa raíz del problema.

6. **Responder a las amenazas:**
   Deben tomar las medidas adecuadas en caso de que se produzca una violación de seguridad. Esto puede implicar la configuración de flujos de trabajo de respuesta automatizados y la mejora de los controles de seguridad para garantizar que la violación de seguridad no se repita.

7. **Supervisar las métricas de seguridad importantes:**
   Muchos analistas de seguridad también hacen un seguimiento de las métricas importantes relacionadas con el centro de operaciones de seguridad para garantizar la mejora constante de la postura de seguridad de su organización.

Una solución de gestión de eventos e información de seguridad (SIEM) o de análisis de seguridad es la parte más importante del arsenal de un analista de seguridad cuando realiza estas tareas. La solución SIEM adecuada puede ayudar a detectar las amenazas y mitigar los incidentes. Este libro trata de cómo un analista de seguridad puede aprovechar al máximo las funciones de una solución SIEM.

¿Por qué debería leer este libro?

Hemos escrito este libro para ayudarle a entender las 10 funciones más importantes de una solución SIEM:

1. Obtención de logs
2. Análisis e informes de seguridad
3. Correlación de eventos en tiempo real
4. Detección de anomalías
5. Inteligencia sobre amenazas
6. Monitoreo de la nube
7. Aplicación de marcos de seguridad informática
8. Gestión de la conformidad
9. Análisis forense de los logs
10. Respuesta a incidentes

Si comprende estas funciones, podrá sacar más provecho de su implementación de SIEM. En el Capítulo 11, también compartimos consejos y trucos de tres analistas de seguridad a los que entrevistamos mientras escribíamos este libro. Esto puede darle algunos consejos prácticos que puede aplicar en su organización.

Capítulo 1: La criticidad de la obtención de logs

Su solución SIEM debe obtener e ingerir los logs de múltiples dispositivos de su red. A continuación, puede reunir estos logs e identificar patrones que indiquen una amenaza. Aquí hay nueve fuentes de log de las que su solución SIEM necesita ingerir logs:

Dispositivos de red:

Los routers, switches y puntos de acceso actúan como transportadores de información. Esto los hace vulnerables a los intentos de infiltración. Por ejemplo, en un ataque de inundación SYN, un servidor es incapaz de establecer una conexión con un cliente porque la dirección IP del cliente está amañada para ser inalcanzable. El servidor espera que el cliente le devuelva la confirmación, pero nunca lo hace. El servidor espera la confirmación durante un tiempo determinado antes de descartar la solicitud.

Este periodo de espera estrangula el ancho de banda del servidor. Las numerosas solicitudes falsas, seguidas del periodo de espera, conducen a una denegación de servicio de las solicitudes legítimas, ya que el servidor está saturado. Para entender los vectores de ataque en una situación así, se pueden consultar los logs de los routers y otros dispositivos de red. Puede comprobar sus logs para ver la dirección IP del servidor que envía las múltiples solicitudes. También puede comprobar el pico de tráfico y el lapso de tiempo durante el cual se produce para identificar un posible ataque SYN.

Servidores de autenticación:

La información de inicio de sesión de los usuarios de sus servidores de autenticación puede revelar posibles amenazas. Por ejemplo, un fallo en el inicio de sesión debido a una contraseña incorrecta podría parecer inofensivo, pero los múltiples fallos en el inicio de sesión podrían deberse a un ataque de fuerza bruta. La información de inicio de sesión de sus servidores de autenticación mostrará información como los paquetes de autenticación utilizados para autenticar a un usuario. Estos logs también revelarán por qué se produjo un fallo en el inicio de sesión, cuántas veces ocurrió y a qué hora ocurrió. A continuación, puede iniciar una investigación si es necesario.

Estaciones de trabajo:

Los logs de las estaciones de trabajo proporcionan datos más granulares sobre la información de inicio y cierre de sesión que la información presente en los controladores de dominio de su red. Por ejemplo, un fallo en el inicio de sesión se representará como "las credenciales del cliente están revocadas". Pero la razón por la que fueron revocados puede atribuirse a muchas razones que son difíciles de averiguar a partir de los logs del controlador de dominio o del servidor de autenticación. Los logs de las estaciones de trabajo pueden ofrecerle información más detallada, como por ejemplo, un fallo en el inicio de sesión debido a una cuenta deshabilitada o debido a un intento de inicio de sesión durante horas no autorizadas.

Active Directory:

El monitoreo de la información de Active Directory puede ayudarle a abordar la mayoría de sus problemas de amenazas internas. Estos logs revelarán si se ha creado algún nuevo usuario o si se ha alterado alguna configuración o permiso de GPO; esta información es esencial para mantener la seguridad de su red.

Aplicaciones de terceros:

El uso de aplicaciones de terceros a veces puede contribuir a las vulnerabilidades a las que se enfrenta su organización. Examine la aplicación de terceros con la que decida asociarse para comprobar si cumple sus estándares de seguridad. El registro de todas las interacciones con aplicaciones de terceros en su red puede ayudarle a averiguar si alguna configuración o acción relacionada está dando lugar a alertas.

Bases de datos:

Las organizaciones utilizan servidores de bases de datos para alojar información altamente sensible, como datos financieros, datos personales de los interesados y otra información empresarial confidencial. Es posible que estos almacenes de datos se corrompan debido a una mala gestión por parte de los empleados, y los valiosos datos que contienen los convierten en un objetivo principal para los hackers. Para combatir esto, es importante realizar un monitoreo de la actividad de la base de datos las 24 horas del día.

Servidores de archivos:

El registro de la información del servidor de archivos puede ayudarle a obtener información sobre quién ha accedido, creado, modificado, eliminado, cambiado nombres o copiado un archivo. También puede averiguar si alguien intentó acceder a un archivo y si se le denegó el acceso o si se cambiaron los permisos de acceso.

Dispositivos de seguridad:

El registro del tráfico de los firewalls y las soluciones IDS o IPS puede ayudar a controlar el tráfico bloqueado, los intentos de intrusión y cualquier comportamiento anómalo que pueda indicar un ataque externo.

Logs de la plataforma en la nube:

A medida que las empresas adoptan una infraestructura híbrida y multi-nube, se hace necesario que monitoree toda la actividad en la nube en la consola central de su SIEM.

Formateo de los logs para el análisis

Incluso la red más rudimentaria puede generar un número abrumador de logs. A menos que se formateen los logs en un formato utilizable, es difícil analizarlos. Para lograrlo, su solución SIEM debe añadir contexto y ser coherente con las etiquetas de los logs. También debe mostrar la gravedad para poder priorizar los logs correctos.

Añadiendo contexto:
Añadir información contextual sobre el evento puede ahorrarle varios pasos en el proceso de investigación. Por ejemplo, estudie estos dos formatos:

- Formato 1: 2020-07-15T23:00:27Z|WARN| AD object modified. (Objeto AD Modificado)
- Formato 2: 2020-07-15T23:00:27Z|WARN| "ABC" OU name changed. (Nombre de OU cambiado)

El formato 2 revela información clara sobre el evento y ayuda a acelerar la investigación.

Utilice formatos de datos y de tiempo coherentes: Dado que es importante saber cuándo se produjo un incidente, formatee sus logs para que muestren un formato de tiempo consistente en todos los lugares.

Mostrar la gravedad del evento: No todos los eventos son iguales en gravedad, lo que significa que diferentes eventos requieren diferentes enfoques. Algunos eventos de seguridad tienen que ser registrados como de baja prioridad, para que pueda identificar los incidentes que necesitan una acción inmediata.

Por ejemplo, **2020-07-15T23:00:27|ATTENTION| "ABC" OU name changed** podría registrarse como un incidente de menor prioridad en comparación con **2020-08-15T21:00:28|CRITICAL| "Access to File A denied"**, ya que el archivo "A" podría ser un archivo sensible al que una entidad no autorizada está intentando acceder.

Le recomendamos que clasifique sus eventos de seguridad como 1) Advertencia, 2) Atención y 3) Crítico, para poder responder primero a los incidentes críticos.

Este enfoque de formatear los logs permite mejorar la legibilidad, el contexto y la respuesta.

Obtención de logs mediante recopilación con agentes y sin agentes

Si tiene un poco de experiencia con la recopilación de logs, es probable que haya escuchado los términos "basado en agentes" y "sin agentes".

Recopilación de logs basada en agentes: Este método de recopilación de logs implica un agente - un software precursor que debe instalarse en los dispositivos- para garantizar que los logs se recopilan de ellos. Esta información se transfiere al servidor destinado a almacenar estos logs.

Estas son cuatro ventajas de la recopilación de logs basada en agentes:

1. **Una información detallada más profunda:**
   Obtendrá información granular sobre los procesos y logs de la red, lo que puede ayudarle a recibir una visión más profunda.

2. **Eficiencia del ancho de banda de la red:**
   Puede programar ciertos agentes para que filtren los datos de log no críticos y sólo envíen los datos útiles por la red para su análisis. Esto significa que se consume menos ancho de banda al enviar los datos filtrados por la red.

3. **Mayor seguridad:**
   Los agentes no requieren un acceso remoto permanente para la recopilación de logs, lo que resulta en una mayor seguridad. La seguridad de un agente puede reforzarse mediante firewalls, lo que lo hace más seguro que la recopilación de logs sin agente.

4. **Más fiabilidad:**
   Las soluciones basadas en agentes pueden monitorear los hosts incluso cuando están desconectados de la LAN.

Recopilación de logs sin agente:
La recopilación de logs sin agentes se basa en el software y las aplicaciones existentes instaladas en los dispositivos para recopilar datos de log. Esto significa que no hay ningún agente que haga de intermediario para la recopilación de logs de los dispositivos. Esto le ahorra la necesidad de tener que actualizar el agente y garantiza la recopilación de logs sin inconvenientes.

Estas son tres ventajas de la recopilación de logs sin agentes:

1. **Menos invasivo, fácil y rápido de implementar:**
   Como no hay ningún agente implementado, este método de recopilación de logs requiere una configuración mínima.

2. **Menor coste de mantenimiento:**
   No hay necesidad de actualizaciones frecuentes.

3. **Adecuado para la implementación de grandes nodos:**
   La recopilación sin agentes es más fácil de manejar para los nuevos administradores. Si utiliza herramientas de implementación rentables pero menos robustas, es preferible la recopilación de logs sin agentes.

Debería tener la opción de configurar tanto la recopilación de logs basada en agentes como la que no lo es, en función de sus necesidades.

Tres maneras de registrar bien los logs

Estas son tres maneras de garantizar que no se limita solamente a recopilar logs, sino que obtiene información útil de ellos.

1. **Obtención de logs:**
   En la sección anterior se habló de todas las fuentes desde las que se debe obtener logs. Aunque su organización puede tener sus propias necesidades de registros de logs, es muy importante que recopile los logs de estas fuentes de log cruciales para asegurarse de que esté controlando los recursos de red esenciales.

2. **Compruebe si hay manipulación de logs:**
   Los hackers pueden intentar evadir las defensas para que usted no pueda atraparlos. Su objetivo inmediato puede ser borrar sus logs de auditoría para que no pueda ver las actividades nefastas que han llevado a cabo. Busque el ID de evento 1102 en su solución de registro de logs. Este ID de evento se genera cuando se borran los logs de seguridad. Le sugerimos que establezca notificaciones cuando se produzca este evento. Su solución SIEM le proporcionará información sobre la cuenta de usuario que ha borrado los logs.

3. **Registro de logs de baja latencia:**
   Pruebe su mecanismo de ingesta de logs para ver si sus logs se están ingiriendo rápidamente para así monitorear los eventos en tiempo real.

Capítulo 2: Cómo hacer un buen análisis de seguridad

Después de que su solución SIEM obtenga los logs de su red y los introduzca en un formato utilizable, tiene que interpretar patrones significativos y comunicar información procesable. Para ello, debe tener en cuenta tanto los datos en tiempo real como los históricos. Debe saber qué usuario realizó qué actividad, en qué host y a qué hora. Debe ser capaz de lograr tanto la seguridad centrada en los datos como la seguridad centrada en el usuario.

Seguridad centrada en los datos y en el usuario

Con la seguridad centrada en los datos, puede vigilar de cerca todos los activos de datos críticos y asegurarse de que no caigan en las manos equivocadas.

Con la seguridad centrada en el usuario, se pueden controlar de cerca las actividades realizadas por los diferentes usuarios en la red. Cada vez que un usuario realiza una actividad sospechosa, usted puede recibir una notificación al respecto.

Desarrollar casos de uso como punto de partida

El mejor punto de partida para construir su análisis de seguridad es desarrollar casos de uso altamente efectivos. Estos casos de uso serían las respuestas a los retos de seguridad más urgentes a los que se enfrenta su organización.

Los casos de uso que desarrolle deben incluir tanto casos de uso esenciales como complejos. Mientras que los casos de uso esenciales implican los factores de higiene de seguridad básicos que casi todas las empresas necesitan, los casos de uso complejos implican desafíos únicos. La empresa de análisis Gartner describe varios casos de uso esenciales y complejos que puede construir dentro de su solución de análisis de seguridad.

Estos son algunos ejemplos de casos de uso esenciales:

- Monitoreo de amenazas como el ransomware y vulnerabilidad del correo electrónico.
- Cumplir con los mandatos normativos como PCI DSS, HIPAA, SOX y GDPR.
- Comprender sus riesgos de seguridad actuales utilizando marcos de seguridad informática como NIST y MITRE ATT&CK.

Estos son algunos ejemplos de casos de uso complejos:

- Defiéndase contra las amenazas en todas las zonas geográficas.
- Busque grandes volúmenes, velocidades y variedades de recopilación de datos.
- Busque las amenazas en los entornos de múltiples inquilinos.

Creación de valor a partir de la información y logs

Su SIEM debe proporcionar información e informes sobre cada caso de uso. Usted debe ser capaz de responder a las siguientes preguntas:

- ¿Qué actividad se ha realizado?
- ¿Quién ha realizado la actividad?
- ¿Dónde se realizó la actividad?
- ¿Cuándo se realizó la actividad?
- ¿Cómo se realizó la actividad?

Debería poder visualizar un informe que muestre toda la información importante de forma organizada. También debería poder examinar detalladamente cualquiera de los detalles proporcionados, elegir el intervalo de fechas específico que debe considerarse para el análisis y exportar el informe en diferentes formatos de archivo como CSV, PDF y HTML.

Capítulo 3: Encontrar patrones con la correlación de eventos

Un evento A que se produce por sí solo en una parte de la red puede ser malicioso o no. Un evento B que se produce por sí solo en otra parte de la red puede ser malicioso o no. Lo mismo ocurre con el evento C y el evento D.

Pero si estos cuatro eventos suceden uno tras otro en rápida sucesión, la historia podría ser algo siniestra. La capacidad de unir eventos aparentemente no relacionados como un solo incidente se denomina correlación de eventos.

Los ataques a la seguridad pueden ser complejos. Pero incluso los ataques más complejos utilizan los mismos fundamentos básicos. Tiene que haber un inicio de sesión por parte del atacante a través de algún tipo de vulneración de cuenta. O si se trata de una persona con información privilegiada maliciosa, sólo habría un inicio de sesión legítimo. Tras el inicio de sesión, el atacante podría recorrer la red accediendo a diferentes servidores, cambiando configuraciones, relajando las políticas de seguridad e incluso borrando archivos. Su trabajo consistiría en trazar el camino del atacante y descubrir que su secuencia de acciones es peligrosa.

La correlación de eventos puede detectar posibles ataques, así como proporcionarle la línea de tiempo de las acciones maliciosas realizadas. Para ello, examina los volúmenes de datos de log e identifica los patrones de actividad que pueden indicar una violación de seguridad inminente.

Por ejemplo, piense en un atacante que se cuela entre las defensas de su firewall, entra en un servidor Windows, accede a la aplicación del servidor de bases de datos instalada en él y borra los datos críticos. El rastro de log del atacante está repartido en múltiples ubicaciones. El poder de la correlación de eventos radica en el hecho de que puede trabajar con miles de logs de varios dispositivos, elegir esta secuencia específica de eventos de su firewall, servidor de Windows y servidor de base de datos, y alertarle en cuestión de segundos.

Su solución de análisis de seguridad debería ofrecer una lista de reglas de correlación predefinidas. Se trata de reglas integradas en la solución out-of-the-box por el proveedor y que incluyen los casos de uso más populares. Puede utilizar estas reglas de correlación predefinidas para protegerse de amenazas como la fuerza bruta, el criptojacking y las firmas conocidas de ransomware.

Aparte de las reglas predefinidas, también necesita la flexibilidad de construir sus propias reglas de correlación. Al fin y al cabo, cada organización es única y sería imposible adelantarse a todos los tipos de amenazas a los que podría enfrentarse cada organización. Usted es el que mejor conoce su organización; así que, dependiendo del riesgo al que se exponga su sector y su empresa, puede utilizar esta flexibilidad para crear sus propias reglas.

Capítulo 4: Detección de anomalías con el análisis del comportamiento de usuarios y entidades

Los atacantes sofisticados son plenamente conscientes de las diferentes formas en que las empresas intentan adelantarse a sus movimientos. Por lo tanto, se vuelven innovadores y buscan nuevas formas de conseguir un punto de apoyo inicial, moverse lateralmente, borrar sus huellas para evitar la detección, escalar privilegios y robar datos. Con la información sobre los ataques que se comparte abiertamente hoy en día, los delincuentes informáticos saben que tienen que ir cambiando su modus operandi para aumentar sus posibilidades de éxito. Para ello, utilizan técnicas como:

Ataques de día cero:

Los actores de las amenazas utilizan exploits relativamente desconocidos para comprometer una red. Como se conoce poca información sobre el exploit, será difícil detectarlo.

Ataques "Living off the land":

Esto ocurre cuando el atacante utiliza aplicaciones de confianza o de la lista blanca para promover su causa. Por ejemplo, PowerShell, una herramienta de confianza utilizada por los administradores de sistemas, puede utilizarse con fines maliciosos, como la enumeración de dominios, el reconocimiento e incluso la propagación de malware. Dado que PowerShell es una aplicación de confianza, es posible que no suene ninguna alarma y que el ataque pase desapercibido.

Amenaza persistente avanzada (APT):

En este ataque, el adversario accede a una red, permanece sin ser detectado durante mucho tiempo y roba lentamente la información. El delincuente informático puede conseguirlo al pasar desapercibido y escalando gradualmente los privilegios. Dado que las actividades se extienden a lo largo del tiempo, puede resultar difícil detectar una APT.

Si sólo utiliza un sistema de detección de amenazas basado en reglas, su red no estará protegida adecuadamente. Un sistema basado en reglas depende de que usted escriba las condiciones, y buscará los escenarios en los que se incumplen estas condiciones. Si se infringe una condición, recibirá una alerta. Hay tres problemas con este enfoque:

1. Es difícil predecir la cadena de muerte cibernética en cada posible ataque y escribir una regla para detectarlo. Un ataque podría seguir una secuencia de acciones completamente nueva que usted no podría haber previsto. Esto es lo que los actores de las amenazas aprovechan para llevar a cabo ataques de día cero, living-off-the-land y APT.
2. En redes grandes y complejas, el número de usuarios y hosts puede ser grande. En estos escenarios, es difícil escribir una regla basada en la actividad realizada por cada usuario o host.
3. Sólo se sabe de un ataque cuando ya ha comenzado.

Para protegerse de las amenazas más difíciles de detectar, debe utilizar el análisis del comportamiento de usuarios y entidades (UEBA) basado en el machine learning. Con UEBA, su solución de análisis de seguridad puede aprender lo que constituye un comportamiento normal para cada usuario y entidad en la red, y puede crear una línea de base de actividades regulares para cada usuario y entidad.

Una anomalía, por definición, es algo que se desvía de lo esperado. Cualquier actividad que se desvíe de esta línea de base se marca como una anomalía. Cada vez que un usuario o entidad registra una anomalía, la puntuación de riesgo aumenta. Cuando la puntuación de riesgo supere un determinado umbral, podrá investigar el problema.

Existen principalmente tres tipos de anomalías que se pueden analizar:

1. **Anomalía de tiempo:**
   Esto ocurre cuando una actividad ocurre en un momento que cae fuera de los buckets de tiempo esperados. Por ejemplo, un usuario podría mostrar una anomalía horaria al iniciar la sesión en el dominio a las 3 de la madrugada cuando normalmente lo hace entre las 8 y el mediodía.

2. **Anomalía de recuento:**
   Cuando el número de actividades realizadas por un usuario o en un host excede lo que se considera normal para un periodo de tiempo específico, se produce una anomalía de recuento. Por ejemplo, si el número de accesos a un archivo entre las 3 pm y las 4 pm supera lo que se considera normal para ese tiempo agregado de una hora, se activará una anomalía de recuento.

3. **Anomalía de patrón:**
   Esto es el resultado de una secuencia inesperada de eventos. Por ejemplo, un usuario llamado Steve se conecta a un host con la dirección IP 192.168.10.1 a las 7 pm. Aunque es normal que Steve se conecte a ese equipo, no es normal que esté conectado en ese momento. Esta secuencia activará una anomalía de patrón.

Medir el riesgo con precisión mediante el análisis de grupos de pares

El análisis de grupos de pares es una técnica para hacer más precisa su puntuación de riesgo. Con esta técnica, se pueden identificar usuarios o hosts con características o patrones de comportamiento similares y clasificarlos como un grupo. Se puede construir una mejor seguridad comparando el comportamiento observado de un usuario o host con el del grupo de pares correspondiente. La puntuación de riesgo del usuario o del host puede verse afectada positiva o negativamente en función del grupo de pares.

Figura 4-1: Agrupación de pares para mejorar la puntuación de riesgo

Hay muchas situaciones en las que la agrupación por pares puede ayudar a elaborar puntuaciones de riesgo más precisas. Estos son algunos ejemplos:

1. **Primera vez que un usuario accede a un recurso:**
   Un usuario accede por primera vez a un servidor de base de datos crítico. Sin el análisis del grupo de pares, esta actividad se consideraría arriesgada. Pero si el usuario pertenece al grupo de pares de los analistas de marketing que suelen acceder a este servidor de bases de datos, la actividad no se marcará.

2. **Anomalía en el tiempo de inicio de sesión de un usuario:**
   Un usuario se conecta a la red en un momento que se desvía mucho de su línea base de comportamiento esperado. Si no hay un análisis del grupo de pares, esto podría considerarse arriesgado. Pero si el usuario es miembro de un grupo de pares que muestra actividad de inicio de sesión en ese momento, la puntuación de riesgo será menor. En la Figura 4-2, a continuación, se muestra un ejemplo de Informe de Anomalías.

3. **Un administrador de TI instala un software inusual:**
   Un administrador de TI instala un software inusual en un host específico. Esto podría dar lugar a una anomalía en el patrón y la puntuación de riesgo del administrador de TI podría aumentar. Sin embargo, tras el análisis del grupo de pares, se descubre que este usuario forma parte del grupo de pares denominado "administradores de TI" y esta acción anómala no se desvía realmente del comportamiento promedio de ese grupo. Por lo tanto, la puntuación de riesgo no se eleva tanto.

4. **Hay un número anormal de lecturas de archivos en un host por parte de un usuario:**
   Un servidor sensible contiene numerosos archivos críticos para el negocio sobre marcas y hojas de ruta de productos. Un usuario lee algunos de estos archivos y se desvía de su comportamiento esperado. Sin el análisis del grupo de pares, la puntuación de riesgo del usuario de esta acción podría sugerir actividades alarmantes. Pero tras el análisis del grupo de pares, usted se da cuenta que este comportamiento es típico de un grupo que contiene otros 100 miembros. Por lo tanto, la puntuación de riesgo no se ve muy afectada.

5. **Treinta usuarios pertenecientes a diferentes departamentos acceden a una base de datos durante un fin de semana:**
   Una base de datos relacionada con la ingeniería a la que acceden 30 usuarios pertenecientes a departamentos como TI, preventa, ventas y gestión de productos. Sin el análisis del grupo de pares, esto parece una actividad arriesgada y la puntuación de riesgo de cada usuario aumentará. Sin embargo, con el análisis de grupos de pares, todos estos usuarios se clasifican en un solo grupo y la puntuación de riesgo no aumenta tanto.

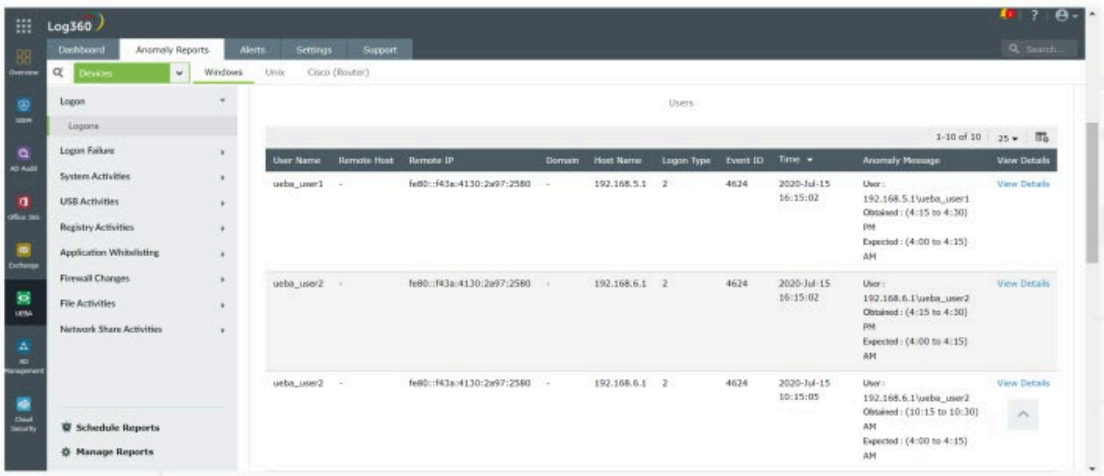

Figura 4-2: Análisis de las anomalías del tiempo de inicio de sesión en los dispositivos Windows en Log360

Utilizar la estacionalidad para mejorar la puntuación de riesgo

Numerosos productos, como los chocolates, la ropa de verano, la ropa de deporte y los disfraces de Halloween, pertenecen a los mercados de temporada. La demanda de estos productos suele alcanzar un pico durante unos días o meses, y luego disminuye. Dependiendo del mercado, las ventas atribuidas a la estacionalidad pueden variar. Por ejemplo, las ventas de ropa de invierno durante los meses de invierno pueden eclipsar las ventas del resto del año.

En la red de una organización, los usuarios y los hosts podrían exhibir un comportamiento estacional como:

1. Un servidor de bases de datos que es muy consultado el lunes de cada semana.

2. Un usuario que trabaja en sábados alternos.

3. Un usuario que accede a un determinado servidor de archivos sólo una vez al mes y, normalmente, el último día laborable del mes.

Estos tres ejemplos se refieren a sucesos raros de carácter estacional. Pero, ¿son anomalías? No, no lo son.

Estas tres actividades (y otras similares), aunque son raras y se desvían de lo esperado, no son anomalías. Como empiezan a aceptarse como normales después de que ocurran unas cuantas veces, se puntuarán como actividades normales que siguen una tendencia estacional.

Los algoritmos de machine learning utilizados para detectar anomalías deben ser capaces de tener en cuenta la estacionalidad. Deben comprender los efectos estacionales en el comportamiento de los usuarios y hosts, y ser capaces de identificar una actividad concreta como no anómala, aunque sea poco frecuente. Después de tener en cuenta la estacionalidad, no se levantarán indicadores y las puntuaciones de riesgo no deberían aumentar. ¿Y si la actividad hubiera ocurrido fuera de esta "ventana estacional"? Eso sería una anomalía, como lo ilustra el caso de uso que sigue.

Entender la estacionalidad con un ejemplo de la vida real

Su empresa de TI realiza actividades especiales el primer y tercer sábado de cada mes. El sábado por la mañana, su plataforma de análisis de seguridad detecta que un empleado se conecta a la red. Curiosamente, es el segundo sábado del mes. Un sistema menos capacitado lo aceptaría; después de todo, el empleado estuvo en línea el sábado anterior, así que ¿por qué no hoy? Pero un sistema bien capacitado detectará anomalías estacionales como ésta. Conoce la diferencia entre los distintos sábados de un mes. Se activa una alarma y aumenta la puntuación de riesgo del empleado.

Capítulo 5: Responder mejor con la inteligencia sobre amenazas

Gartner, una de las principales empresas de investigación y asesoramiento, define la inteligencia sobre amenazas como "un conocimiento basado en pruebas, que incluye el contexto, los mecanismos, los indicadores, las implicaciones y los consejos procesables, sobre una amenaza o un peligro existente o emergente para los activos que puede utilizarse para fundamentar las decisiones relativas a la respuesta del sujeto a esa amenaza o peligro".

Esta definición nos ayuda a comprender los siguientes aspectos de la inteligencia sobre amenazas:

1. La inteligencia sobre amenazas ayuda a las organizaciones a detectar las amenazas observadas en todo el mundo utilizando estrategias como el enfoque "malo conocido", que se centra en los signos que pueden detectarse para detener un ataque, incluido un hash o un indicador de compromiso.
2. La inteligencia sobre amenazas no es sólo una lista de IP malas. Incluye perfiles detallados de actores de amenazas, mecanismos de ataque e instrucciones sobre cómo responder a una amenaza.
3. Está en constante evolución y proporciona información sobre las amenazas existentes y emergentes.
4. Su principal objetivo es equipar mejor a las organizaciones en la lucha contra las amenazas globales.

Utilizando una combinación de técnicas automatizadas y manuales, los datos de inteligencia sobre amenazas se recogen de todo Internet. A continuación, estos datos son procesados por equipos de investigación especializados que analizan y validan la información antes de publicarla en forma de inteligencia estratégica o táctica sobre amenazas.

La inteligencia estratégica sobre amenazas está destinada principalmente al consumo humano, y orienta las decisiones estratégicas en materia de seguridad, como decidir en qué áreas de la seguridad informática hay que centrarse, y cómo lanzar programas de concienciación de los empleados sobre las últimas amenazas.

La inteligencia táctica sobre amenazas se publica normalmente en forma de fuentes contra amenazas, y generalmente es interpretada por una o más soluciones de seguridad. Es más útil en el día a día, ya que ayuda a las organizaciones a detectar y combatir los incidentes de seguridad en sus redes. Algunas fuentes contra amenazas populares son AlienVault OTX, FireEye iSIGHT Threat Intelligence y Webroot BrightCloud Threat Intelligence.
Una solución SIEM efectiva puede permitirle utilizar la inteligencia sobre amenazas de las siguientes maneras:

1. **Añadir fuentes contra amenazas personalizadas:**
Las soluciones SIEM procesan la información sobre amenazas procedente de fuentes de confianza, y algunas incluso le dan la opción de añadir fuentes personalizadas a las que su organización se suscribe de forma independiente. Dado que muchas fuentas contra amenazas son específicas de un sector o de ciertos tipos de amenazas, las fuentes personalizadas pueden tener más sentido para su organización.

2. **Ofrece una visión global de su red:**
El conocimiento de las amenazas globales no sirve de nada si no se puede utilizar en el contexto de su propia red. Con una visión completa de todos los dispositivos y aplicaciones de su red, un SIEM puede notificarle si se detectan entidades maliciosas en cualquier sistema de su red.

3. **Reducir el número de integraciones:**
Las soluciones SIEM proporcionan las funciones necesarias desde una única consola con opciones para una integración sin problemas cuando sea necesario. Una vez que se detecta un incidente de seguridad, se puede investigar a fondo, gestionar y responder a él. Esto ayuda a agilizar el proceso de resolución de incidentes, garantizando que su organización permanezca segura ante cualquier amenaza.

Detectar las amenazas de forma inteligente: Dos casos de uso

A continuación se presentan dos casos de uso en los que puede utilizar la inteligencia sobre amenazas en una solución SIEM para proteger a su organización de las mismas.

Caso de uso 1:

Comunicación con los servidores de retrollamada

A veces, un sistema infectado puede quedar bajo el control de un servidor externo, también conocido como servidor de comando y control (C2 o C&C). El servidor C2 puede entonces utilizar este sistema para extraer datos sensibles o infectar otros servidores críticos de su red.

Los SIEM que aprovechan la inteligencia sobre amenazas analizan constantemente los logs de tráfico saliente de su red y capturan las comunicaciones que se envían a este tipo de servidores. A continuación, puede iniciar una investigación para averiguar cómo y cuándo se infectó el sistema, y puede comprobar si hay otros sistemas potencialmente infectados que hayan tenido contacto con este servidor C2.

Caso de uso 2:

Intentos de inyección SQL desde fuentes maliciosas

aLos atacantes pueden aprovechar las vulnerabilidades de su servidor web e inyectar código SQL malicioso para recuperar registros comerciales confidenciales de sus bases de datos. Para evitar estas violaciones de datos, la función de inteligencia de amenazas de su SIEM le permite vigilar todas las conexiones entrantes a sus servidores web y marcar cualquier IP o dominio malicioso. De este modo, puede contener la pérdida de datos importantes, e identificar y corregir las vulnerabilidades de su servidor web.

Capítulo 6: Endurecimiento de la seguridad en la nube

La nube está sustituyendo rápidamente a los tradicionales centros de datos on-premises, pero la desventaja es que se depende mucho más de los proveedores de la nube para gestionar la seguridad de su hardware. Aun así, debido al modelo de responsabilidad compartida en la informática en la nube, no se puede dejar la gestión de la seguridad completamente en manos de los proveedores de la nube. Las empresas también tienen que tomar medidas proactivas contra los atacantes cibernéticos que atacan su red.

He aquí seis pasos sencillos pero efectivos para reforzar la seguridad de la infraestructura de la nube:

1. **Detectar errores de configuración de la nube:**
   Los errores de configuración de la nube son posiblemente la principal causa de las violaciones de datos que se producen en ella. Un error de configuración se produce cuando un administrador de seguridad establece los servicios en la nube de forma incorrecta o especifica ajustes que no proporcionan la seguridad adecuada para los datos almacenados en la nube. Por ejemplo, un error de configuración común de los bucket de S3 es hacerlos accesibles al público. Esto significa que otros usuarios en la web con cuentas de AWS pueden acceder a los datos sensibles almacenados en su bucket de S3. Un solo error de configuración como éste puede provocar una violación masiva de los datos y llevar al incumplimiento de la normativa. Las auditorías de seguridad periódicas y exhaustivas de la infraestructura de la nube ayudan a detectar los errores de configuración y a rectificarlos inmediatamente antes de que los adversarios los exploten.

2. **Realizar pruebas de penetración:**
   Siempre es mejor que te hackees a ti mismo antes de que un atacante lo haga por ti. Debe evaluar la seguridad de su infraestructura en la nube simulando un ataque cibernético. Esto puede revelar las vulnerabilidades y permitirle comprender la madurez de la seguridad de su organización. Una organización con un hacker ético en su equipo puede realizar estas simulaciones y probar el rendimiento de sus controles de seguridad. También se sabe que las empresas contratan a hackers éticos de forma puntual cuando quieren probar las configuraciones de seguridad.

3. **Obtenga visibilidad de toda la actividad en la nube:**
   La mayoría de las organizaciones de todo el mundo han adoptado una estrategia multi-nube en la que utilizan servicios en la nube de múltiples proveedores. Esto les permite distribuir sus activos, datos, aplicaciones y almacenamiento en varios entornos de alojamiento. Aunque una estrategia de múltiples nubes tiene sus ventajas, también hace más difícil monitorear lo que ocurre en la nube en cualquier momento. Es fundamental contar con una solución efectiva de gestión de eventos e información de seguridad (SIEM) que centralice la información obtenida de todas las plataformas en la nube y alerte a los analistas de seguridad en caso de que se produzca un percance. Las técnicas de detección de anomalías también deben utilizarse para observar cualquier actividad anormal realizada por los usuarios en cualquier host.

La Figura 6-1 muestra cómo una solución SIEM efectiva como ManageEngine Log360 puede proporcionarle información crítica sobre lo que está ocurriendo en su infraestructura en la nube.

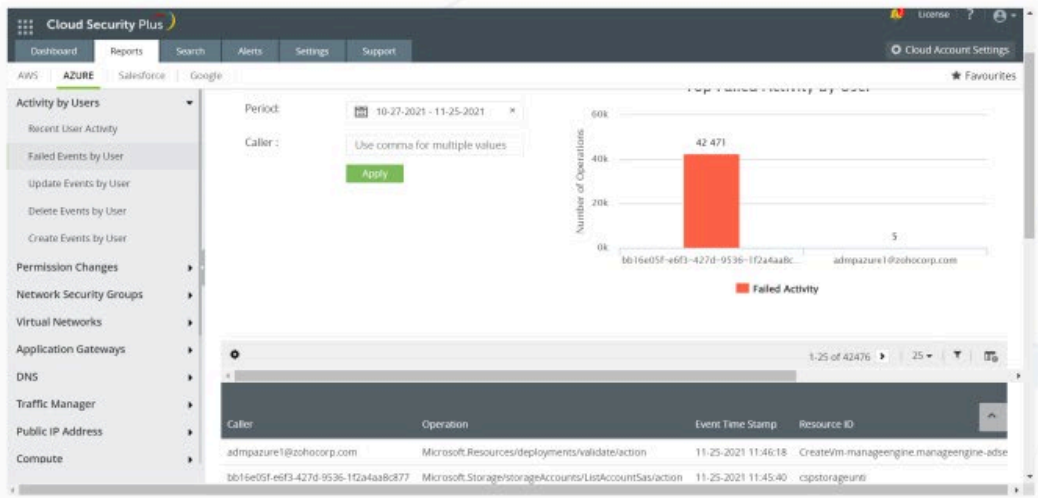

Figura 6-1: Monitoreo de las infraestructuras en la nube en una consola de su solución SIEM

4. **Minimice el riesgo con una autenticación y autorización sólidas:**

Implemente controles estrictos de gestión de accesos e identidades para garantizar que sólo las personas autorizadas tengan acceso a los recursos de la red. Hay que seguir el principio del mínimo privilegio y poner en práctica el modelo de seguridad "Zero Trust", que reconoce la confianza como una vulnerabilidad. El acceso justo, el acceso justo a tiempo y la autenticación multifactorial también deberían aplicarse para mejorar la seguridad.

La autenticación adaptativa es una novedad que funciona creando un perfil para cada usuario con un cálculo de su puntuación de riesgo. En función de la puntuación de riesgo, se puede exigir al usuario que proporcione credenciales adicionales o, por el contrario, permitirle utilizar menos credenciales. Esto permite una mayor seguridad. Por ejemplo, si un usuario se conecta desde un dispositivo no registrado o desde una nueva ubicación geográfica, su puntuación de riesgo aumenta automáticamente y se le presentan mecanismos de autenticación adicionales para demostrar su identidad.

5. **Introduzca un broker de seguridad de acceso a la nube:**

Un broker de seguridad de acceso a la nube (CASB) es un mecanismo de control de políticas y visibilidad de la nube que se sitúa entre los usuarios de los servicios en la nube y las aplicaciones en la nube. Este software monitorea todas las actividades que los usuarios realizan en la nube y también aplica las políticas de seguridad. El CASB puede ser una implementación on-premises o una aplicación SaaS. Un CASB puede ayudar a una empresa a monitorear toda la actividad de los usuarios en la nube. Cuando un CASB se integra con una solución SIEM, un analista de seguridad puede obtener un contexto más profundo en torno a la actividad de un usuario en la nube para una investigación.

6. **Capacite a sus empleados para que la seguridad sea una prioridad:**
   Los empleados deben ser capacitados regularmente para asegurarse de que no sean víctimas de una vulneración de la cuenta. Puede ser necesario capacitar a sus empleados al menos una vez cada seis meses.

Ventajas de una solución SIEM integrada en CASB

La empresa de análisis Gartner definió por primera vez la expresión "broker de seguridad de acceso a la nube", o CASB, en 2012. Se ha convertido en una tecnología bien conocida y adoptada para la defensa informática. Se puede pensar en ella como una solución que se sitúa entre los usuarios de una organización y los distintos servicios en la nube a los que acceden. Y como se encuentra allí, un CASB puede ayudarle a autenticar y autorizar a los usuarios cuando intentan acceder a la nube, y también puede permitirle identificar lo que entra y sale de la nube. Es posible que su centro de operaciones de seguridad dependa en gran medida de una solución SIEM en la actualidad; en los próximos dos años, deberá garantizar que su SIEM se integre de manera eficiente con un CASB externo o tenga funciones CASB integradas.

Un CASB debe formar parte de su SIEM por cinco razones principales: para hacer frente a la gran adopción de las aplicaciones en la nube, para correlacionar los eventos que se producen en diferentes partes de la red, para evitar las filtraciones de datos, para proporcionar visibilidad a la TI invisible y para ofrecer visibilidad a la gestión de accesos e identidades (IAM).

1. **Abordar la gran adopción de las aplicaciones en la nube:**

   El empleado promedio utiliza hasta 30 aplicaciones SaaS en la nube. Además, utilizan estas aplicaciones en sus propios dispositivos móviles. Por si fuera poco, la mayoría de las organizaciones utilizan hoy en día un entorno multi-nube con varios modelos de entrega PaaS e IaaS. Por lo tanto, es necesario contar con una solución SIEM habilitada para CASB que ofrezca visibilidad de las aplicaciones en uso y de cómo se están utilizando. Con una solución de este tipo, también puede ser consciente del nivel de riesgo que una aplicación concreta supone para su organización.

   Una herramienta SIEM sin una integración CASB no le dará esta visibilidad de las actividades en la nube. Y un CASB independiente carecerá del contexto de seguridad necesario que proporcionan los eventos de interés que se producen en otras partes de la red.

2. **Correlacionar los eventos que ocurren en diferentes partes de la red:**

   Los ataques cibernéticos se han vuelto sofisticados en los últimos tiempos; hay instancias de ataques de living-off-the-land, de malware en la nube con acceso inicial en un servidor on-premises, ransomware y disruptionware en la nube, y ataques internos. Necesita la capacidad de ver patrones y correlacionar eventos aparentemente no relacionados que ocurren en diferentes partes de la red, y agruparlos como un solo incidente de seguridad.

   Una solución SIEM integrada en CASB le permitirá ver las actividades maliciosas tanto en los entornos on-premises como en la nube.

3. **Prevención de la filtración de datos:** Con la llegada de las aplicaciones en la nube, existe un riesgo considerable de filtración de datos, tanto intencionada como no intencionada. Por ejemplo, un empleado del departamento de marketing puede utilizar una aplicación llamada Font Candy para crear una tipografía vibrante. Sin embargo, esta aplicación puede no estar autorizada dentro de la organización, y el empleado puede tener datos de contacto privados e información clasificada almacenada en ella. En un escenario así, se necesita la capacidad de gestionar las cargas no autorizadas de datos sensibles y evitar las filtraciones de datos. Con un CASB, también puede aplicar políticas y controles de seguridad en la nube para evitar que los datos se transfieran por Internet.

   Una herramienta SIEM integrada en CASB le permitirá ver toda esta información en la misma consola que el resto de la información de seguridad importante.

4. **Proporcionar visibilidad a la TI invisible:** Hoy en día, la mayoría de las organizaciones tienen una lista de aplicaciones en la nube autorizadas que los empleados pueden utilizar si lo desean. Estas aplicaciones podrían haber sido aprobadas después de que la organización las considerara seguras y efectivas para la productividad de los empleados. Las aplicaciones aprobadas son propiedad o están controladas por la organización. Por otro lado, también puede haber aplicaciones "invisibles" que estén fuera de la propiedad o el control de las organizaciones de TI. Las aplicaciones invisibles pueden tener vulnerabilidades y brechas que podrían ser explotadas por los atacantes.

   Un CASB le permitirá descubrir las aplicaciones invisibles y los principales usuarios que acceden a estas aplicaciones. Una herramienta SIEM integrada en CASB le permitirá ver esta información junto con otras actividades que el usuario pueda haber realizado en la red. De esta manera, se puede obtener una imagen completa de las posibles actividades maliciosas.

5. **Ofreciendo visibilidad en IAM:** Según Erik Wahlstrom, director de investigación de Gartner, "las organizaciones no deberían sustituir sus programas de IAM por los CASB, sino más bien combinar ambos para aumentar la gobernanza y el control de acceso de las aplicaciones en la nube." Un CASB puede proporcionar una mejor IAM a través de formas como la autenticación adaptativa y el análisis de riesgo basado en el usuario.

   Al incorporar esta función en el SIEM, podrá ver el comportamiento arriesgado de los usuarios en una sola consola y también utilizar libros de tácticas y flujos de trabajo para responder a estas amenazas.

Capítulo 7: Dominar la investigación forense informática

La investigación forense informática consiste en hacer un backtracking de un ataque para evaluar los daños y predecir si se pueden causar más. Este capítulo le guiará en la realización de una investigación forense informática.

Este es un ejemplo sencillo de cómo se puede utilizar el análisis forense de los logs para comprender las complejidades de lo que ocurrió durante un ataque. Suponga que su herramienta SIEM ha generado una alerta para informarle de que un usuario ha modificado un archivo importante. Como se trata de un archivo importante, se comprueba si el usuario tiene privilegios para realizar dicha acción. Lo que le resulta extraño es que, aunque el usuario tenga permiso para realizar dichas modificaciones, una persona con ese rol concreto no tiene ninguna función relacionada con el archivo que se ha modificado.

En este caso, podría preguntarse si el usuario ha sido añadido recientemente a la lista de control de acceso con los permisos necesarios. A continuación, busque los logs que indiquen el Evento con ID 4670, que corresponde a los permisos de un objeto que se ha modificado. Estos logs revelarán quién hizo cambios en la lista de control de acceso. Esta es una versión bastante simplificada de la ciencia forense de los logs.

Consulta de archivos de logs para eventos específicos

El análisis de los archivos de log es un proceso tedioso debido al gran volumen de logs generados por todos los dispositivos de la red. Incluso si ha configurado sus políticas de auditoría para eliminar el "ruido" durante la recopilación de logs, seguirá teniendo terabytes de datos que procesar. Así que el reto obvio es este: ¿Cómo se busca un evento de interés? Por mucho que sea un problema de aguja en el pajar, se puede hacer una consulta para buscar eventos concretos en los archivos de log. Puede especificar cómo quiere que se devuelvan los archivos de log y en qué orden quiere que se presenten.

Una buena manera de buscar eventos específicos en terabytes de datos de log es utilizar Elasticsearch. Esto le ofrece una manera fácil de buscar y analizar grandes volúmenes de datos. Una buena solución SIEM puede ayudarle a agregar sus datos de log y a buscar eventos específicos utilizando Elasticsearch. Log360 le permite agregar sus logs y utilizar Elasticsearch para recuperar eventos específicos, y utiliza efectos visuales intuitivos para mostrar los análisis. La Figura 7-1 muestra cómo se usa Elasticsearch en Log360.

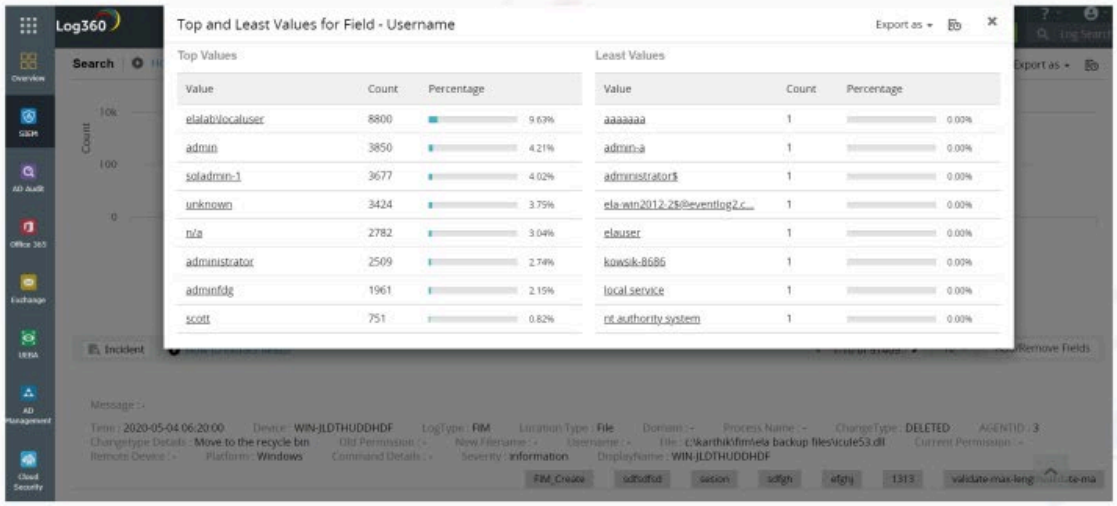

Figura 7-1: Motor de búsqueda de logs de Log360

Tres trucos para hacer bien el análisis forense de logs

1. **Compruebe la fuente de inteligencia sobre amenazas:** Puede complementar su análisis forense con fuentes de inteligencia sobre amenazas específicas del sector que agreguen contexto a las actividades de su red. Por ejemplo, puede obtener información de inteligencia sobre amenazas sobre una dirección IP maliciosa que haya intentado infiltrarse en su red. Su fuente de inteligencia sobre amenazas puede proporcionar contexto sobre la dirección IP con información histórica, como cualquier ataque anterior asociado a la dirección IP que se haya llevado a cabo en otras organizaciones de su sector. Esto puede ayudarle a entender lo que los atacantes podrían estar intentando hacer en su red.

2. **Diseño de plantillas de alerta:** Puede guardar una consulta de búsqueda para utilizarla en el futuro. También puede guardar sus búsquedas como alertas para recibir una notificación cada vez que se cumplan sus condiciones de búsqueda. Esto le ayudará a reducir las tareas repetitivas.

3. **Visualización de la causa raíz:** La representación visual de la secuencia de eventos que condujeron a una alerta facilita a cualquier analista la comprensión de todo el recorrido de un incidente de seguridad.

Capítulo 8: Cumplimiento de los mandatos normativos

Se realizan auditorías periódicas para garantizar el cumplimiento de los mandatos. Es importante que las empresas superen estas auditorías para evitar sanciones y otras consecuencias importantes que podrían interrumpir el negocio. Los mandatos de cumplimiento garantizan que las organizaciones cumplan los requisitos mínimos para protegerse de las amenazas a la seguridad.

Mandatos de cumplimiento populares

A continuación se presentan tres mandatos de cumplimiento populares que están en vigor en todo el mundo:

HIPAA:

Se trata de una ley federal estadounidense que constituye leyes de privacidad, leyes de notificación de violaciones de seguridad y leyes de seguridad que protegen la información de salud de los pacientes y les otorga el derecho a ser informados sobre la divulgación de su información a un tercero.

PCI:

La PCI DSS es un conjunto de leyes que regulan el modo en que se almacena, procesa y transmite la información de las tarjetas de crédito. Estas leyes reguladoras mejoran la seguridad de las cuentas en todo el proceso de las transacciones. Especifican los requisitos de cifrado de datos; los requisitos de protección de los datos de los titulares de las tarjetas; y los requisitos de mantenimiento de los firewalls, las soluciones antivirus y otras soluciones de seguridad.

GDPR:

El GDPR es un conjunto de normas cuyo objetivo es otorgar a los ciudadanos de la UE un mayor control sobre sus datos personales. El GDPR obliga a las empresas a recopilar información de forma legal y a disponer de la protección prescrita para evitar que la información se utilice de forma indebida.

Subvertir cualquiera de estos mandatos puede acarrear sanciones exorbitantes e incluso penas de cárcel. El incumplimiento del GDPR en el Reino Unido en 2018 se fijó en una multa máxima de 17,5 millones de libras esterlinas o el 4% de la facturación global anual de la organización -lo que sea mayor- por infracción. En caso de incumplimiento de la norma PCI DSS, las multas suelen oscilar entre 5.000 y 100.000 dólares al mes hasta que el comerciante logre el cumplimiento.

Es seguro decir que ninguna organización quiere gastar ingresos en pagar multas. Por ello, la gestión del cumplimiento es un asunto serio que requiere atención.

Antes de empezar a gestionar el cumplimiento de la normativa dentro de su organización, usted debe tener en cuenta:

1. El ámbito en el que funciona su organización y las leyes o mandatos que rigen ese sector.

2. El marco de seguridad de TI existente que tiene en su sitio y si es escalable a una organización en crecimiento.
3. Las complejidades tecnológicas de su red que afectarán a sus operaciones, como el acceso a los servidores o la ubicación de activos de red importantes.

También recomendamos una evaluación de riesgos exhaustiva, que es una buena manera de determinar los peligros a los que se enfrenta su organización. La evaluación de riesgos le ayudará a calcular los costes que podría tener que pagar en caso de un incidente de seguridad en su empresa, tanto en términos de sanciones como de pérdidas por interrupción de la actividad. Una evaluación de los riesgos también le ayudará a priorizar qué amenazas inmediatas y paralizantes necesitan más atención, para que pueda invertir en la solución de seguridad adecuada.

También debería invertir en una solución de gestión del cumplimiento que pueda hacer la mayor parte del trabajo por usted. La mayoría de las soluciones SIEM ofrecen una variedad de controles de seguridad de TI con informes detallados que se asignan a las leyes de cumplimiento que le corresponden.

Log360 ofrece informes en profundidad para comprobar y demostrar el cumplimiento del GDPR, PCI DSS, HIPAA, SOX, CCPA y más. Estos informes de cumplimiento pueden personalizarse para adaptarse a las necesidades internas de su empresa. Teniendo en cuenta el potencial de las futuras normativas de cumplimiento de las TI, la solución también ofrece informes de cumplimiento personalizados. La Figura 8-1 muestra los diferentes informes relacionados con el cumplimiento de la normativa disponibles en Log360.

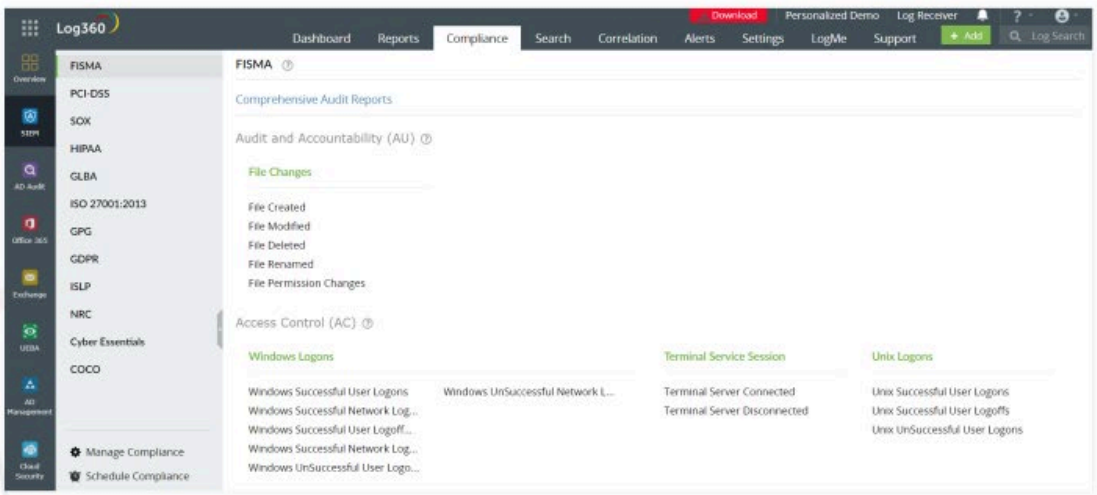

Figura 8-1: Análisis de la conformidad con Log360

Capítulo 9: Perfeccionar su respuesta a los incidentes

Así que ha recopilado sus logs y los ha centralizado. Ha establecido las fuentes contra amenazas y ha definido el tipo de eventos sobre los que quiere recibir alertas. ¿Qué sigue? Lógicamente, el siguiente paso es la respuesta a los incidentes. Su plan de respuesta a incidentes es aún mejor si está automatizado.

Automatización de la respuesta a incidentes

Un plan automatizado de respuesta a incidentes ayuda a contener los daños mientras se intenta averiguar los detalles de la amenaza y cómo mitigarla. La automatización de la respuesta a incidentes ayudará a reducir el tiempo medio de resolución (MTTR). Su MTTR mide el tiempo medio que se tarda en controlar y remediar una amenaza.

Establecer un MTTR bajo se traduce en menos daños que usted debe manejar a largo plazo. Cuando se permite que una amenaza o entidad maliciosa fermente dentro de su red durante un largo período, puede causar aún más daño a sus recursos de red y puede ser catastrófico.

Disminución del MTTR

A continuación se indican ocho pasos para configurar respuestas automatizadas a incidentes utilizando su solución SIEM. Seguir estas soluciones puede permitirle disminuir su MTTR.

1. **Log de eventos:** Establezca alertas en su solución SIEM para que se le notifiquen los indicadores de vulneración. Cada vez que un usuario realiza actividades que van en contra de sus reglas, usted debe recibir un correo electrónico o un SMS al respecto. Además, este evento también debería ser visible en su dashboard.

2. **Clasificar las alertas:** Cada alerta debe clasificarse como "Crítica", "Problema" o "Atención" y debe estar codificada por colores. Esto le ayudará a priorizar las alertas.

3. **Añadir alertas a un incidente:** En numerosas ocasiones, puede haber múltiples alertas; sin embargo, su análisis mostrará que estas alertas forman parte de un único ataque. En estos casos, debería poder añadir varias alertas en un solo incidente. Por ejemplo, es posible que desee tratar las ocurrencias de movimiento lateral y escalada de privilegios como un solo incidente.

4. **Asignar incidentes a los analistas:** Su solución SIEM debería permitirle hacer uso de reglas de asignación para asignar automáticamente el incidente a un analista de seguridad.

5. **Supervisar el estado del incidente:** Debería poder supervisar el estado del incidente en cualquier momento. Debe saber si el incidente está "abierto", "cerrado" o "en curso".

6. **Investigación y diagnóstico de incidentes:** Debería poder ver detalles como la hora de creación del incidente, la antigüedad del mismo, los hosts y usuarios implicados, los sospechosos del incidente y los procesos que se ejecutaron como parte del mismo. También debe poder cotejar todas las pruebas y notas sobre el incidente en un solo lugar para poder tomar decisiones informadas sobre cómo responder. Esto también le ayudará a colaborar con otros analistas y a realizar análisis forenses de los logs de forma más efectiva.

7. **Responder con flujos de trabajo automatizados:** Lo ideal es que no se retrase la acción después de recibir una notificación por correo electrónico o SMS. Aquí es donde los flujos de trabajo automatizados ayudarán. Estos servirán como primera respuesta antes de que usted intervenga para tomar otras medidas. Los flujos de trabajo automatizados pueden permitirle cerrar la sesión de un usuario, desactivar un usuario, apagar un sistema, ejecutar un script para cambiar una regla del firewall, etc.

8. **Integrar con los sistemas de tickets:** Su solución SIEM debe integrarse de manera eficiente con las herramientas de gestión de tickets de terceros más conocidas. A continuación, el incidente puede gestionarse en la consola de su herramienta de gestión de tickets.

Responder con flujos de trabajo

A continuación se presentan dos escenarios reales en los que puede utilizar los flujos de trabajo de respuesta.

Ejemplo 1:

Defiéndase contra las amenazas internas

Una persona con información privilegiada maliciosa puede acceder físicamente a un servidor crítico y extraer archivos en un dispositivo extraíble. Para mitigar esto, puede establecer una alerta para que le notifique cuando se conecte un dispositivo USB a este servidor durante las horas no laborables. Sin embargo, una alerta por sí sola puede no ser suficiente; después de todo, sólo se tarda unos minutos en copiar los archivos. Debería tener un flujo de trabajo integrado que pueda bloquear el puerto USB de este dispositivo y notificarle el estado. Con este flujo de trabajo en marcha, los empleados no podrán llevarse información confidencial y usted podrá investigar el incidente a su conveniencia.

Ejemplo 2:

Desactive los sistemas vulnerados en su red

Cuando se produce un incidente, el primer paso de la investigación es revisar los logs de sus dispositivos, ya que toda la actividad de la red deja un rastro de log. A veces, los atacantes consiguen entrar en una red vulnerando una cuenta de usuario legítima. A continuación, pueden borrar los logs de los equipos que violan para evitar ser detectados u ocultar su presencia continua en la red.

Puede establecer alertas para identificar cuándo se borran los logs de seguridad de un equipo. En estos casos, puede ser demasiado tarde para deshacer el daño ya hecho, pero puede prevenir cualquier otra actividad maliciosa. Cree un flujo de trabajo integrado para cerrar la sesión y desactivar la cuenta de usuario vulnerada, aislando efectivamente al atacante de su red.

Tres trucos para responder correctamente a los incidentes

1. No es necesario reflejar cada alerta como un incidente de seguridad independiente. Identifique las alertas relacionadas y agréguelas en un solo incidente de seguridad. Esto le ayudará a gestionar las amenazas de manera eficiente.
2. Almacene toda la información sobre un incidente de seguridad, ya que esta información podría ser necesaria para futuros análisis. La duración de su almacenamiento depende de las necesidades de su empresa.
3. Establezca informes avanzados para diferentes perfiles de trabajo. Puede empezar con:

   - **Informes de analistas:**
     Número de incidentes, tipos de incidentes y tiempo empleado en detectarlos y responder a ellos.

   - **Informe del director del SOC:**
     Número de incidentes gestionados por los analistas junto con el tiempo medio de detección y respuesta a las amenazas por parte de los analistas.

   - **Informe a nivel de CISO:**
     Análisis del impacto de los incidentes en la empresa; dónde se puede implementar más automatización.

Capítulo 10: Marcos de seguridad informática populares: ATT&CK y NIST

Dos marcos que lograron aclarar nuestra confusión en lo que respecta a la seguridad informática fueron ATT&CK y NIST. La base de datos de tácticas y técnicas de ATT&CK, combinada con el marco del NIST para evaluar la postura de seguridad, crea una formidable defensa contra las amenazas conocidas.

Contar con una solución SIEM que pueda asignar los eventos de su red a las tácticas o técnicas de ATT&CK e implementar los flujos de trabajo adecuados para hacerles frente le sitúa en un lugar en el que su equipo SOC puede defender su red con confianza. Si su solución SIEM puede asignar sus configuraciones de seguridad en función de los requisitos del NIST, podrá reforzar la seguridad de su organización.

Un resumen general de MITRE ATT&CK

La fascinante forma que tiene ATT&CK de trazar el objetivo y los métodos de un atacante y de relacionarlo con las estrategias de mitigación adecuadas hace que este marco sea pionero a la hora de ayudar a las empresas a entender la mentalidad del adversario. Hoy en día, ATT&CK ha sido adoptado universalmente por las empresas para conocer los ataques a los que se enfrentan y las vulnerabilidades que pueden existir en sus redes. A través de ATT&CK, también pueden deducir el tipo de soluciones de seguridad que podrían necesitar. El marco ATT&CK se basa en la investigación de acceso público sobre las técnicas de ataques cibernéticos, la información sobre amenazas y los informes sobre incidentes de seguridad.

El marco MITRE ATT&CK es una matriz que presenta las tácticas de un ataque cibernético, el "por qué" (filas de la matriz), y las técnicas de un ataque cibernético, el "cómo" (columnas de la matriz). Para cada técnica, también enumera subtécnicas. Las subtécnicas describen las técnicas de forma más explícita. Por último, el marco enumera procedimientos que son ejemplos de las técnicas y subtécnicas observadas en el mundo real.

Tácticas en el marco de MITRE ATT&CK Hay 12 tácticas en el marco. Estas son:

1. **Acceso inicial:**
   Conseguir la entrada en una red a través de técnicas comunes como el phishing o la explotación de servicios remotos externos.

2. **Ejecución:**
   Ejecución de código malicioso en el sistema de la víctima que permite al atacante controlar el sistema de forma remota.

3. **Persistencia:**
   Aprovechando la presencia de la entidad maliciosa y esforzándose por mantener su posición en la red, el atacante intenta aplicar técnicas como el cambio de configuraciones o credenciales para impedir que los usuarios legítimos tengan acceso a la red.

4. **Escalamiento de privilegios:**
   Obtención de permisos de nivel superior para escalar privilegios.

5. **Evasión de la defensa:**
   Obtener acceso al software de confianza y a las herramientas existentes en el sistema para enmascarar el malware que circula en el sistema y ocultar sus propias huellas.

6. **Acceso a las credenciales:**
   Utilizar herramientas ingeniosas como la captura de pulsaciones de teclas o el software de keylogging para robar las credenciales de los usuarios.

7. **Descubrimiento:**
   Descubrir puntos vulnerables en la red que puedan ser explotados. Esto podría implicar el descubrimiento de una lista de cuentas y su estado en el entorno, o el escrutinio de las relaciones de confianza entre múltiples dominios en la misma red que podrían ser explotados.

8. **Movimiento lateral:**
   Pasar por múltiples sistemas utilizando credenciales legítimas o explotando sesiones remotas existentes para moverse dentro de la red de la organización.

9. **Recopilación:**
   Recogida de datos de interés para el objetivo del adversario, como el acceso a datos en el almacenamiento en la nube.

10. **Mando y control (C&C):**
    Comunicarse con sistemas vulnerados en la red para ejecutar tareas maliciosas. El atacante podría utilizar los protocolos de la aplicación y de la web para mezclar los comandos maliciosos con el tráfico normal, dificultando la detección de la comunicación entre el atacante y el sistema de la víctima.

11. **Robo:**
    Robo de datos mediante procedimientos automatizados y empaquetado de los datos que se roban para evitar su detección. Estos datos suelen comprimirse, cifrarse y robarse a través de un protocolo alternativo en lugar del canal de C&C existente.

12. **Impacto:**
    Interrumpir la disponibilidad o comprometer la integridad de los datos mediante la manipulación de los procesos empresariales y operativos.

Técnicas
Cada táctica puede ser llevada a cabo por un adversario a través de un sinnúmero de formas, y éstas se denominan técnicas. Por ejemplo, el acceso inicial podría realizarse mediante 10 técnicas diferentes.

Subtécnicas
Las subtécnicas son una descripción más detallada de una técnica. Por ejemplo, la técnica de manipulación de cuentas tiene cuatro subtécnicas diferentes asociadas.

MITRE ATT&CK y SIEM

Si su solución SIEM es capaz de aprovechar el marco y la base de conocimientos de MITRE ATT&CK, hará que su defensa de la seguridad sea más estricta. Dentro de su solución SIEM, podrá ver las posibles ocurrencias de técnicas o tácticas ejecutadas por los adversarios. También puede recibir alertas si se observan técnicas específicas, y puede agregar estas alertas en un solo incidente para una gestión eficiente.

La Figura 10-1 muestra un ejemplo de un posible acceso inicial por parte de un adversario, tal y como informa el módulo ATT&CK de Log360.

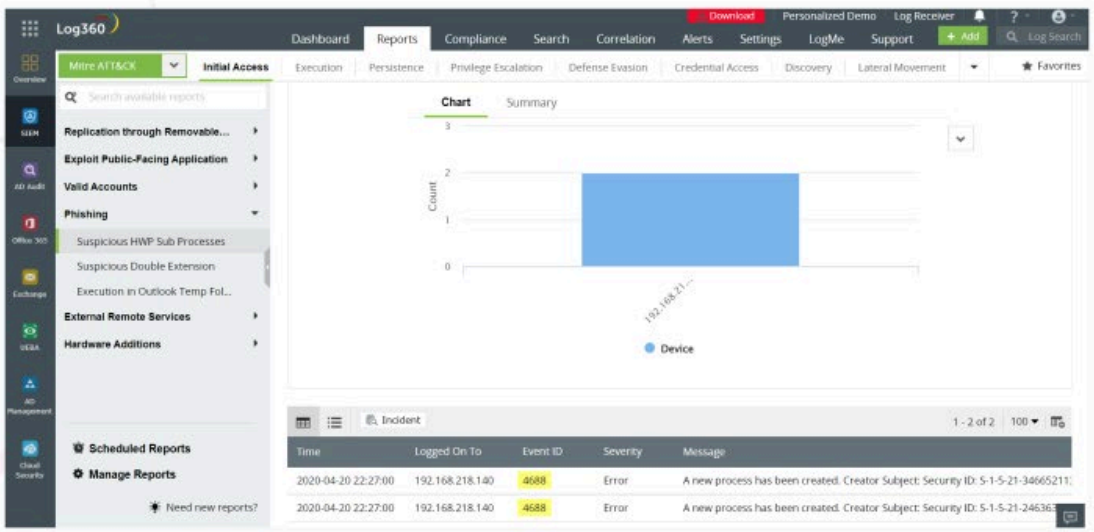

Figura 10-1: Detección del acceso inicial de la técnica de phishing con informes ATT&CK en Log360

El Marco de Seguridad Informática del NIST en resumen

El NIST pretende combinar las normas del sector (como la FISMA y la HIPAA) y las mejores prácticas (como las evaluaciones de riesgos y la identificación de activos) para ayudar a las organizaciones a reducir los riesgos de seguridad informática. Ayuda a las organizaciones a desarrollar una estrategia proactiva que categoriza los activos que necesitan ser protegidos y ayuda a reducir los riesgos de estos activos. También asesora a las organizaciones sobre las mejores formas de responder y recuperarse de los ataques cibernéticos en caso de que se produzcan.

Hay tres componentes en el Marco de Seguridad Informática del NIST:

1. **El centro del marco:** Este componente instruye sobre cómo aplicar técnicas de defensa uniformes y cumplir con las normas del sector.

2. **Niveles de aplicación del marco:**
Este componente del NIST ayuda a las organizaciones a evaluar su nivel de madurez en materia de seguridad, lo que se conoce como niveles de implementación, basándose en los siguientes factores:
i) ¿Qué tipo de actividades de seguridad informática realiza la organización para mitigar posibles riesgos?
ii)¿Se aplican las actividades de seguridad informática y las técnicas de defensa de manera uniforme en toda la organización?
iii) ¿Cómo participa y contribuye la organización al entorno general de la seguridad informática?

3. **Perfil del marco:**
Este componente ayuda a las organizaciones a definir y alinear sus resultados de seguridad, como las revisiones de la política de seguridad y las mejoras en el diseño de la seguridad, con los riesgos asociados (identificados en la etapa "central") y el nivel de madurez de seguridad en el que se encuentran actualmente (identificado en la etapa "nivel de implementación"). Las organizaciones pueden establecer esto como un "perfil actual" y luego crear "perfiles objetivo" para determinar los niveles de madurez a los que aspiran.

Hacer que ATT&CK y NIST trabajen para usted

Lo fundamental es recordar que una mezcla de estos dos marcos es lo que le ayudará a reforzar sus defensas informáticas. ATT&CK es más útil cuando su equipo SOC realiza simulaciones, pruebas de penetración en su red y desarrolla defensas en consecuencia. Este marco es el manual de referencia definitivo que necesitará para equipar a sus equipos rojos y azules. Seguir este plan ayudará a sus equipos SOC a entender qué vulnerabilidades deben corregir.

Los atributos del Marco de Seguridad Informática del NIST complementan la estrategia de defensa que ha empezado a construir con ATT&CK. Las directrices del NIST se presentan como una lista de control que puede utilizar para evaluar su postura de seguridad. Cuando esté construyendo una estrategia de defensa completa, puede empezar utilizando la lista de control de evaluación del NIST para evaluar su situación de seguridad y comprender los problemas de su red. A continuación, puede profundizar en la comprensión de cómo se pueden explotar las brechas de su red mediante el uso de ATT&CK.

Capítulo 11: Consejos de los analistas de seguridad

Mientras escribíamos este libro, hablamos con tres analistas de seguridad que empezaron su carrera en el ámbito de la seguridad informática en los últimos cinco años. Compartieron con nosotros su viaje junto con algunos consejos que podrían resultarle útiles. Se trata de una mezcla de consejos profesionales generales y consejos específicos sobre cómo sacar el máximo provecho a su solución SIEM.

Conversación con Sanjay Palanivel, analista de SOC en TATA Consultancy Services

1. **Cuéntenos cómo se inició en la seguridad informática.**
Me inicié en la seguridad informática aprendiendo sobre redes y obteniendo mi certificación CCNA.

2. **¿Cómo pueden los analistas de seguridad informática o los analistas de SOC al principio de su carrera ser más efectivos en su trabajo?**
Aprender el arte de identificar las alertas de falsos positivos y abordar los incidentes en función de la prioridad hace que un analista del SOC sea efectivo.

3. **¿Cuál es su rutina diaria como analista de seguridad?**
Mi rutina diaria consiste en analizar el comportamiento anormal de los usuarios, detectar las actividades en los endpoints y comprobar las nuevas amenazas del día. También tengo que comprobar mi solución SIEM y asegurarme de que esté obteniendo datos de todas las fuentes.

4. **¿Qué métricas son importantes para medir la efectividad de un SOC?**
Las métricas importantes del SOC efectivo son:

   - Mantener la salud de las infraestructuras.
   - Detección temprana y respuesta a la amenaza.
   - Mantener los acuerdos de nivel de servicio sin incumplimientos.

5. **¿Cómo prevé la evolución de las estrategias de la defensa informática?**
La automatización sustituye al monitoreo manual del monitoreo de la seguridad de los eventos y producirá un informe al respecto. Dirigirá las alertas al responsable del incidente. Además, veremos que incluso las startups empiezan a contratar analistas de SOC para su protección contra las amenazas cibernéticas.

Conversación con Nathersha S, analista de IAM en Vanguard Logistics Services

1. **Cuéntenos cómo se inició en la seguridad informática.**

Me inicié en la seguridad informática certificándome en CompTIA, CCNA, CEH e ITIL 4. También me parecieron valiosas las certificaciones gratuitas como Microsoft Azure Fundamentals y Aviatrix Certified Network Associate.

2. **¿Cómo pueden los analistas de seguridad informática o los analistas de SOC al principio de su carrera ser más efectivos en su trabajo?**

Como analista del SOC, no debes limitar tu aprendizaje al campo o al rol en la que te han colocado. Además de utilizar las herramientas SIEM como parte de su rol, usted debe explorar cada parte de cómo se produce el incidente. Para ello, debe tener una sólida base en los fundamentos de la red y la seguridad y una buena capacidad de resolución de problemas.

Siga aprendiendo sobre los nuevos vectores de ataque que lea en las noticias. Averigüe cómo se produjeron.

3. **¿Cuál es su rutina diaria como analista de seguridad?**

Mantener la infraestructura de TI general, las bases de datos de todos los empleados, los equipos, las impresoras y los dispositivos conectados a la red de la oficina.

Incorporar a los empleados con RACF, crear cuentas de buzón de correo y de Active Directory, y proporcionar acceso RDP y VPN. También tengo que proporcionar a los nuevos usuarios un acceso de mínimo privilegio y asegurarme de que tienen los privilegios necesarios para realizar su trabajo.

Desvincular a los empleados y revocar y eliminar su acceso a las cuentas, al correo electrónico y a las aplicaciones según la gestión de acceso basada en roles. También necesito hacer una auditoría manual de otras aplicaciones no sincronizadas.

4. **¿Puede dar sus comentarios sobre la seguridad de los datos?**

Me gustaría referirme aquí a la autenticación, la autorización y a la supervisión.

Autenticación: Hay que garantizar que cada persona tiene una identidad única para demostrar que es quien dice ser y que puede acceder a los datos solicitados. Para hacerla más robusta, podemos tener más de una forma de autenticación: autenticación multifactor o autenticación de triple factor para ser más seguros.

Autorización: Una vez que el usuario demuestra su identidad, hay que verificar si tiene el nivel de acceso requerido y si su rol le permite acceder y modificar la información requerida. El sistema y las políticas deben respetar el principio del mínimo privilegio. Una persona sólo debe tener acceso al conjunto de recursos que exige su rol. A un usuario no se le deben conceder privilegios de root o de administrador hasta que, y a menos que, la naturaleza de su rol lo exija. Esto garantiza que los datos sólo sean accesibles para la persona autentificada y autorizada y que otros intrusos no puedan reclamar el acceso falseando su identidad.

Supervisión: Deberá supervisar la actividad de cada empleado mientras accede a los recursos del sistema, los servicios de red y otras formas de servicios. Si un empleado introduce credenciales de inicio de sesión incorrectas durante un tiempo, el sistema debería detenerlo automáticamente y bloquear el inicio de sesión, ya que podría tratarse de un ataque de fuerza bruta. La organización siempre debe auditar y comprobar los registros de los empleados para asegurarse de que todo funciona según la política definida.

Los logs deben ser auditados con frecuencia para comprobar si hay un comportamiento anómalo del sistema o de los empleados.

5. **¿Cómo prevé la evolución de las estrategias de la defensa informática?**
Las organizaciones están invitando a los cazadores de bugs y recompensándolos con altas recompensas. Esto es seguridad proactiva.

Cada vez más organizaciones realizan pruebas de penetración. Creo que esto ocurre en un promedio de una vez cada seis meses. Sin embargo, debido al avance de los ataques, debemos estar más preparados para todos los posibles resultados y hacer esto una vez cada tres meses como mínimo.

Conversación con Logeshwaran, analista de seguridad de TI de Legato Health Services

1. **Cuéntenos cómo se inició en la seguridad informática.**
Empecé mi carrera como ingeniero de soporte de desktop. Pasé a ser ingeniero de sistemas y luego analista de seguridad.

2. **¿Qué habilidades tuvo que adquirir al iniciarse en la seguridad informática? ¿Cómo adquirió esas habilidades?**

Me inicié en la seguridad informática buscando e investigando en Google sobre la ingeniería social. Hablé con gente de seguridad informática de mi empresa para hacerme una idea de los fundamentos. La capacidad de análisis es esencial. Hay que preguntarse constantemente por qué y cómo ocurrió un incidente y seguir indagando.

3. **¿Cómo pueden los analistas de seguridad informática o los analistas de SOC al principio de su carrera ser más efectivos en su trabajo?**
Para ser más efectivo en seguridad informática, hay que:

- Aprender constantemente sobre las amenazas emergentes en sitios como bleepingcomputer.com, tryhackme.com y hackthebox.eu.
- Unirse a un foro o comunidad de seguridad y seguir lo que dicen los demás en ese ámbito.
- Nunca descartar las alertas aunque sean falsos positivos. Tiene que entender por qué se produjo la alerta. Con la experiencia aprenderá a identificar los falsos positivos.

¿Cuál es su rutina diaria como analista de seguridad?

Esta es mi rutina diaria:

1. Leer sobre las amenazas nuevas y emergentes.
2. Comprobar mi infraestructura para garantizar que no haya impacto de ninguna nueva amenaza.
3. Garantizar que no ejecutamos versiones anticuadas de software, ya que los exploits para las mismas estarán fácilmente disponibles en Internet.
4. Resolver cualquier duda de los desarrolladores, porque un código seguro significa menos trabajo.

Biografía de los autores

Tanya Austin: Tanya es una entusiasta de la seguridad informática que ha sido autora de múltiples e-books y artículos sobre seguridad informática. Le gusta investigar y escribir sobre las herramientas de detección de amenazas que potencian un centro de operaciones de seguridad, el análisis del comportamiento de usuarios y entidades, y marcos como MITRE ATT&CK que ayudan a reforzar la postura de seguridad de una organización.

Ram Vaidyanathan: Ram es un experto en seguridad informática y evangelista en ManageEngine, una división de Zoho Corporation. Como parte de su rol, se mantiene al día sobre las últimas técnicas que utilizan los atacantes para derribar organizaciones y sobre cómo éstas pueden defenderse con las soluciones de defensa adecuadas. Habla en varias conferencias y seminarios de seguridad, e interactúa con su público sobre Log360, una solución SIEM integral.

ManageEngine
Log360

Log360 es una solución SIEM unificada con funciones DLP y CASB integradas para detectar, investigar y responder a las amenazas de seguridad. Aporta inteligencia sobre amenazas, detección de anomalías basada en el machine learning, detección de ataques basada en reglas, correlación de eventos, análisis forense de logs, monitoreo de la seguridad en la nube y gestión de incidentes para hacer frente a los complejos casos de uso de la seguridad en las organizaciones. Log360 garantiza la seguridad de diferentes componentes de la red on-premises, híbrida y en la nube, como Active Directory, dispositivos perimetrales, estaciones de trabajo, bases de datos, aplicaciones críticas para el negocio, servicios en la nube, etc., mediante un monitoreo continuo.

La interfaz de usuario es sencilla de entender y utilizar. Con sus dashboards intuitivos y sus funciones de análisis de seguridad avanzadas, un analista de seguridad sabrá inmediatamente si una amenaza está al acecho en cualquier lugar de la red. Con alertas y respuestas contextuales, también pueden resolver el problema antes de que se convierta en un incidente de seguridad mayor.

Para más información sobre Log360, visite manageengie.com/latam/log-management.

Pruebe Log360 sin costo alguno durante 30 días

Puede probar Log360 sin costo alguno durante 30 días en su propio entorno de red y evaluar sus ventajas. ¡Esta es una forma libre de riesgo de probar Log360!

Descargar Log360 sin coste alguno