ManageEngine

Log360

Usar indicadores para enfrentar los **ataques a la seguridad**

Tabla de contenidos

Introducción

Las brechas de seguridad y ataques sofisticados están en aumento, lo cual ha incitado mejoras continuas en el ámbito de gestión de eventos e información de seguridad (SIEM). Para combatir estos ataques avanzados, los proveedores han reforzado las plataformas y soluciones de inteligencia de seguridad.

Las mejoras en las técnicas de mitigación de ataques han generado varios parámetros nuevos que detectan los patrones de amenaza o ataque en una fase temprana. Las secciones de este documento técnico profundizan en estos dos parámetros –indicadores de compromiso (IoC) e indicadores de ataque (los IoA)– que ayudan a detectar ataques al instante, trazar la secuencia de un ataque e identificar un ataque antes de que se cause daños y mucho más.

Este documento técnico ayuda a los profesionales de seguridad a comprender las funciones únicas de estos indicadores, las diferencias entre ellos y los pasos para configurar una solución SIEM para detectar **IoC** e **IoA**.

Patrones de ataque y sus indicadores.

Las empresas no son inmunes a los ataques de seguridad, sin importar lo buenos que sean sus sistemas de seguridad. Los hackers siempre intentan explotar las vulnerabilidades y las brechas de seguridad de una red, normalmente para acceder a los recursos críticos de la red o para interrumpir los servicios de la empresa.

Así pues, los ataques a la seguridad se pueden clasificar en dos tipos:

- Ataques que interrumpen las operaciones comerciales, como los ataques DDoS destinados a interrumpir el servicio web de una empresa de comercio electrónico o de banca.
- Ataques que roban información confidencial.

Dependiendo del tipo de ataque, el patrón de aproximación será diferente. Por ejemplo, los ataques que intentan interrumpir las operaciones comerciales se enfocan en eludir los sistemas de seguridad de los endpoints e inundar los recursos con tráfico irrelevante. Por otro lado, los ataques que intentan robar datos se enfocan en adquirir información confidencial mediante el acceso no autorizado a recursos críticos.

Independientemente de su tipo, todo ataque dejará un rastro, que se conoce como indicador. Estos indicadores proporcionan detalles que ayudan a los profesionales de la seguridad a:

- Concluir si un evento sospechoso es una amenaza o un ataque en curso..
- Detectar las amenazas en su fase inicial, lo que ayuda a contener un ataque antes de que ocurra.
- Identificar si un ataque está en curso o si ya ha ocurrido antes.
- Acelerar el proceso de descubrimiento de ataques.
- Determinar el impacto total de un ataque una vez resuelto.

Hay dos indicadores principales que resultan útiles para los profesionales de la seguridad: IoC e IoA

IoCs

La mayoría de las empresas se basan en los IoC para contener un ataque en curso o para realizar un análisis forense para resolver un ataque o evaluar su impacto. Esencialmente, los IoC indican a los administradores que la red ha sido comprometida. Responden a las siguientes preguntas vitales: qué ha pasado, quién ha estado involucrado y cuándo ha ocurrido.

IoAs

Los IoA son eventos de seguridad sospechosos que podrían resultar ser una amenaza o ataque. Una vez detectados, los IoA se enriquecen con información contextual, como patrones de comportamiento de los usuarios, vulnerabilidades y datos de entrada de otras herramientas de seguridad. Todos estos detalles ayudan a determinar si un IoA es una amenaza potencial. Dado que los IoA identifican los ataques en una fase temprana, son muy importantes para prevenir ataques.

Explicación de los indicadores con un escenario de ataque.

La lucha contra los ataques a la seguridad es un proceso que involucra varios pasos. El primer paso en ese proceso es la recopilación de pistas, también conocidas como indicadores. Veamos un escenario de ataque para entender el proceso de identificación de indicadores.

Escenario de ataque

Supongamos que en este escenario hay un archivo malicioso de Microsoft Excel que se difunde por correo electrónico a los empleados de una organización. El correo electrónico está redactado con hilos de mensajes auténticos, por lo que muchos empleados descargan el archivo malicioso porque creen que es un mensaje de alguien conocido. Cuando un usuario abre ese archivo, se ejecuta automáticamente una macro. A continuación, esa macro intenta acceder a bases de datos críticas, copia información confidencial de los clientes de esas bases de datos, añade esos datos al archivo de Excel y luego sube el archivo de Excel modificado a un sitio en la nube.

Investigar el ataque

Los ataques se pueden evitar durante la etapa de intrusión siempre que se determine que el origen del ataque es sospechoso o malicioso. En este caso, el correo electrónico procede de una dirección IP no sospechosa y el mensaje parece auténtico, engañando así al filtro de spam. Por lo tanto, sería difícil detectar y contener este ataque en la etapa inicial.

El ataque se hace evidente en la etapa de compromiso, lo que permite detectarlo. Este tipo de ataques se puede detectar rápidamente configurando los perfiles de alerta adecuados para los siguientes IoC:

- Intentos de acceso no autorizados en bases de datos críticas.
- Acciones de copia no autorizada realizadas en una base de datos.
- Intentos de subir o transferir un archivo a un sitio en la nube no autorizado.

De nuevo, el éxito de este proceso de descubrimiento de ataques depende de la validación de cada uno de los IoC (con respecto al contexto del usuario) y del enriquecimiento de los eventos mediante su correlación con otros eventos relacionados. Los administradores de seguridad necesitan profundizar en este patrón de ataque específico e identificar los indicadores de este ataque. Una vez que lo hagan, podrán enfrentar de forma proactiva cualquier ataque que siga un patrón similar. Sin embargo, los ataques no siempre ocurren de la misma forma.

Teniendo en cuenta este escenario, es posible que cada vez que el atacante intente un ataque utilice una técnica de infiltración en la red distinta a un archivo Excel. Teniendo esto en cuenta, los administradores de seguridad deben establecer traps definiendo reglas de correlación que cubran todas las posibles acciones de un patrón de ataque.

Para este escenario, los administradores de seguridad pueden crear una regla de correlación personalizada que incluya las siguientes acciones:

Acciones de correlación	Razones para configurar la acción
Se instala un malware en el sistema o se ejecuta un archivo malicioso.	Es posible que un atacante utilice distintos vectores cada vez que intenta forzar el acceso a la red. Por lo tanto, configure una acción para detectar el malware en el sistema, ya sea en forma de un archivo malicioso o la ejecución de un script.
Un ataque de suplantación de IP se produce dentro de un firewall interno.	Tras la inyección de un archivo malicioso en la red, el atacante puede intentar encontrar la dirección IP de una base de datos o un servidor crítico para obtener acceso no autorizado. Por lo tanto, es crucial establecer una acción para detectar cualquier ataque de suplantación en los firewalls internos.
Varios intentos de acceso no autorizado a una base de datos o servidor crítico.	Después de que un atacante encuentre un servidor o una base de datos, su siguiente paso sería obtener acceso a estos recursos. Los atacantes con privilegios insuficientes intentarán saltarse el proceso de autenticación o acceder al sistema mediante un ataque con contraseña. En cualquiera de los casos, configurar una acción para un gran número de intentos de inicio de sesión fallidos ayudará a validar los eventos como una amenaza potencial.
Intentos de leer o copiar archivos de una base de datos de forma masiva.	Si hay un intento de lectura o copia de archivos de la base de datos de forma masiva, el evento se puede clasificar como un ataque en curso. Esta acción se puede utilizar para impedir que los hackers lean o copien archivos de la base de datos antes de que se filtren datos críticos.
Intentos sospechosos de transferir archivos a un sitio en la nube o a una dirección IP externa.	Incluso si los hackers ya han copiado datos de los recursos críticos, todavía hay una oportunidad de evitar que los datos salgan de las instalaciones al supervisar los eventos de transferencia de archivos dentro de la red. Configure acciones para los intentos de transferencia de archivos a un destino sospechoso (destino con IP maliciosa, destino ubicado en una región geográfica no relacionada, sitio de nube restringido, etc.) o durante horas no laborables para evitar la filtración de datos.

Este tipo de reglas de correlación cubren todos los escenarios posibles en los que se pueden producir patrones de ataque similares. Y más importante aún, estas reglas alertan a los administradores de seguridad en tiempo real, ayudándoles a evitar que las amenazas a la seguridad comprometan la seguridad y la reputación de su organización. Además, para ayudar a mitigar las amenazas, cada regla de correlación se puede enriquecer con información empresarial contextual específica de ese evento.

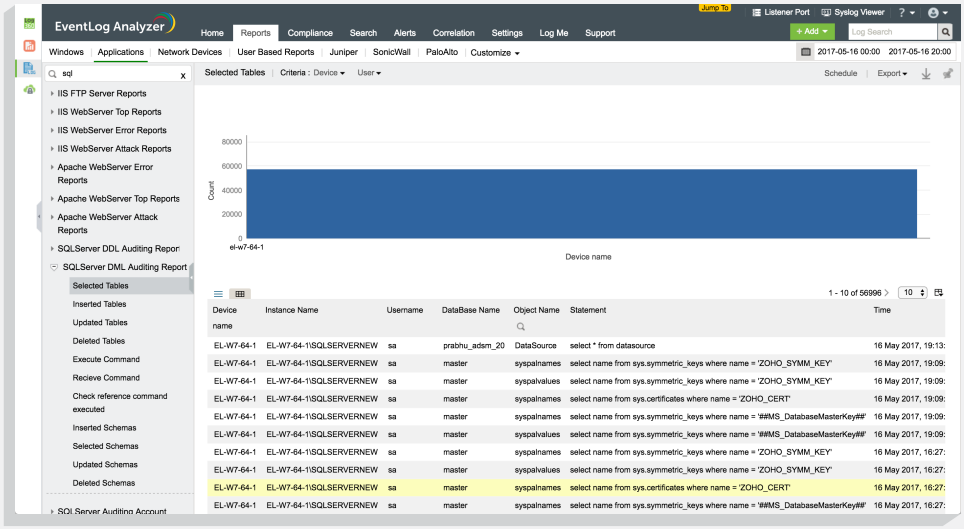
Detectar y enriquecer los IoC e IoA con Log360

Log360 incluye un sistema de respuesta a eventos en tiempo real que detecta IoC y un motor de correlación que ayuda a enriquecer los IoA.

Esta solución también cuenta con una base de datos global de amenazas IP integrada que contiene más de 600 millones de direcciones IP maliciosas. Cuando el tráfico de cualquiera de estas direcciones IP llegue a los recursos de la red, los administradores de seguridad recibirán una notificación en tiempo real y, con la solución, incluso podrán configurar un script personalizado para bloquear esta dirección IP de inmediato.

Sistema de respuesta a eventos en tiempo real: Log360 cuenta con más de 700 perfiles de alerta predefinidos que se basan en un estudio meticuloso de varios IoC. Los administradores de seguridad pueden optar por activar los perfiles de alerta que sean relevantes para su contexto empresarial para detectar los ataques al instante. Cada vez que se produzca un IoC, los administradores recibirán notificaciones en tiempo real por correo electrónico o SMS, así como un informe detallado sobre el evento, lo que acelera el proceso de mitigación de ataques. Además, para reducir el número de falsos positivos, Log360 incluye la posibilidad de crear perfiles de alerta para dispositivos específicos en función de la frecuencia de los eventos o del tiempo. Log360 también proporciona informes detallados sobre cada uno de los siguientes aspectos:

- **Intentos de acceso no autorizado a bases de datos críticas.**
  - Fallos de inicio de sesión inusuales: identifica quién intentó iniciar sesión, desde qué dirección IP, cuándo y si fue desde un host remoto.
  - Detalles de los fallos de inicio de sesión: enumera todos los fallos de inicio de sesión, incluida la razón por la que falló el inicio de sesión (por ejemplo, si se debió a una contraseña incorrecta o a un nombre de usuario incorrecto).
- **Copia no autorizada de información crítica.**
  - Auditoría detallada de DML: registra quién ejecutó una consulta de selección en la base de datos, desde dónde y cuándo.
  - Intentos de copia: determina quién intentó copiar datos, a dónde y desde cuál equipo se realizó el intento.



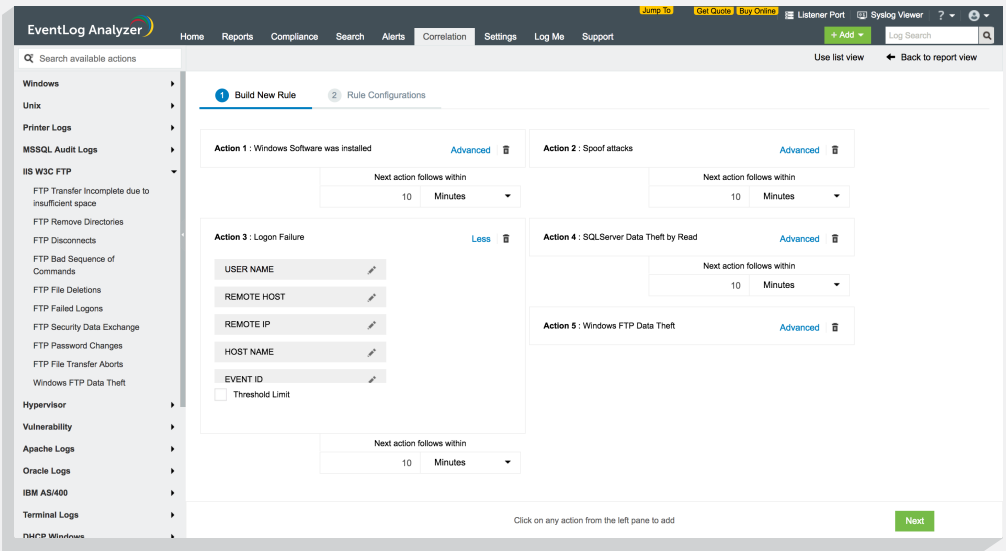
Análisis detallado de las actividades sospechosas en una base de datos

Estos detalles proporcionan a los usuarios de Log360 un contexto adicional, que les ayuda a validar los incidentes como una amenaza o un ataque.

El motor de correlación: Log360 permite correlacionar diferentes eventos en toda la red para recrear y detectar patrones de ataque conocidos.

En cuanto al escenario de violación de datos anterior, los administradores pueden utilizar Log360 para crear una regla de correlación personalizada y detectar ataques similares más rápidamente. Con el generador de reglas de correlación de arrastrar y soltar de Log360, los usuarios pueden simplemente seleccionar acciones predefinidas y crear una regla para cualquier patrón de ataque.

Además, los usuarios pueden establecer valores de umbral para cada una de las acciones para detectar con precisión los patrones de ataque y ahorrar tiempo evitando investigar falsos positivos.



Generador de reglas de Log360

IoA o IoC:
¿Cuál se debe utilizar?

No hay una única respuesta. Los ataques a la seguridad son dinámicos y cambian de patrón muy a menudo. Si bien algunos ataques se identifican en su fase inicial, muchos ataques sofisticados duran un largo periodo de tiempo y no se detectan hasta que el daño está hecho. Por eso, muchas veces las empresas se dan cuenta de que son víctimas de un ataque cuando ya es demasiado tarde. No hay una regla rápida y estricta sobre los indicadores que deben utilizar los centros de operaciones de seguridad.

Para proteger su red de los ataques, auditar las actividades que se producen en la red y detectar anomalías de manera efectiva, las organizaciones deben configurar su solución SIEM de modo que supervise todos los IoC conocidos, así como los IoA que se sincronizan con su estrategia de seguridad.

Acerca de ManageEngine

ManageEngine ofrece herramientas de gestión de TI en tiempo real que permiten a un equipo de TI satisfacer la necesidad de servicios y soporte en tiempo real de una organización. En todo el mundo, más de 60 000 empresas establecidas y emergentes – incluyendo más del 60 por ciento de las empresas en Fortune 500– confían en los productos de ManageEngine para garantizar el rendimiento óptimo de su infraestructura de TI crítica, incluyendo redes, servidores, aplicaciones, desktops y más. ManageEngine es una división de Zoho Corp. con oficinas en todo el mundo, incluyendo Estados Unidos, Reino Unido, India, Japón y China.

Log360 permite correlacionar diferentes eventos en toda la red para recrear y detectar patrones de ataque conocidos.

Acerca del autor

Subhalakshmi Ganapathy trabaja actualmente como analista senior de marketing de productos para soluciones de seguridad de TI en ManageEngine. Tiene un profundo conocimiento en la gestión de la seguridad de la información y el cumplimiento. Proporciona orientación estratégica a las empresas sobre la gestión de eventos e información de seguridad (SIEM), la seguridad de la red y la privacidad de los datos.

Contacte a Subha en subhalakshmi.g@manageengine.com.

Email:
log360-support@manageengine.com.

Or

Línea gratuita:

+1 925 924 9500 (Línea gratuita)

+1 408 916 9393 (Directo)

Or

Visite **www.manageengine.com/latam/log360** para obtener más información sobre la solución y todas sus funciones.