ManageEngine
Log360

La inteligencia de amenazas y las ventajas de la SIEM

Por qué las soluciones SIEM son la opción ideal para obtener funciones de inteligencia de amenazas.

www.manageengine.com/latam/log-management

Introducción

La inteligencia de amenazas (TI) es el arma no tan secreta que el sector de la ciberseguridad está utilizando para fortalecer su lucha contra los ataques. Aunque existe desde hace tiempo, hasta hace poco la inteligencia de amenazas logró un amplio reconocimiento. Según la Encuesta sobre Inteligencia de Amenazas Cibernéticas de SANS 2018, el 81 por ciento de los profesionales de la seguridad creen que invertir en funciones de inteligencia de amenazas ayudó a mejorar la postura de seguridad de su organización, en comparación con el 64 por ciento en 2016.

Sin embargo, a pesar del creciente interés, también hay mucho debate en torno a este tema. ¿Qué implica exactamente la inteligencia de amenazas? ¿Qué funciones son necesarias para que una organización pueda afirmar que cuenta con un sistema de inteligencia de amenazas maduro? ¿Cuáles son las mejores herramientas para proporcionar estas funciones?

En este documento técnico discutiremos:

- La inteligencia de amenazas y sus diversos aspectos.
- Cómo se incorpora la inteligencia de amenazas al marco de seguridad de una organización.
- Las ventajas de utilizar una solución SIEM para implementar un sistema integral de inteligencia de amenazas en su organización.
- Casos de uso empresariales.

Desmitificando la inteligencia de amenazas

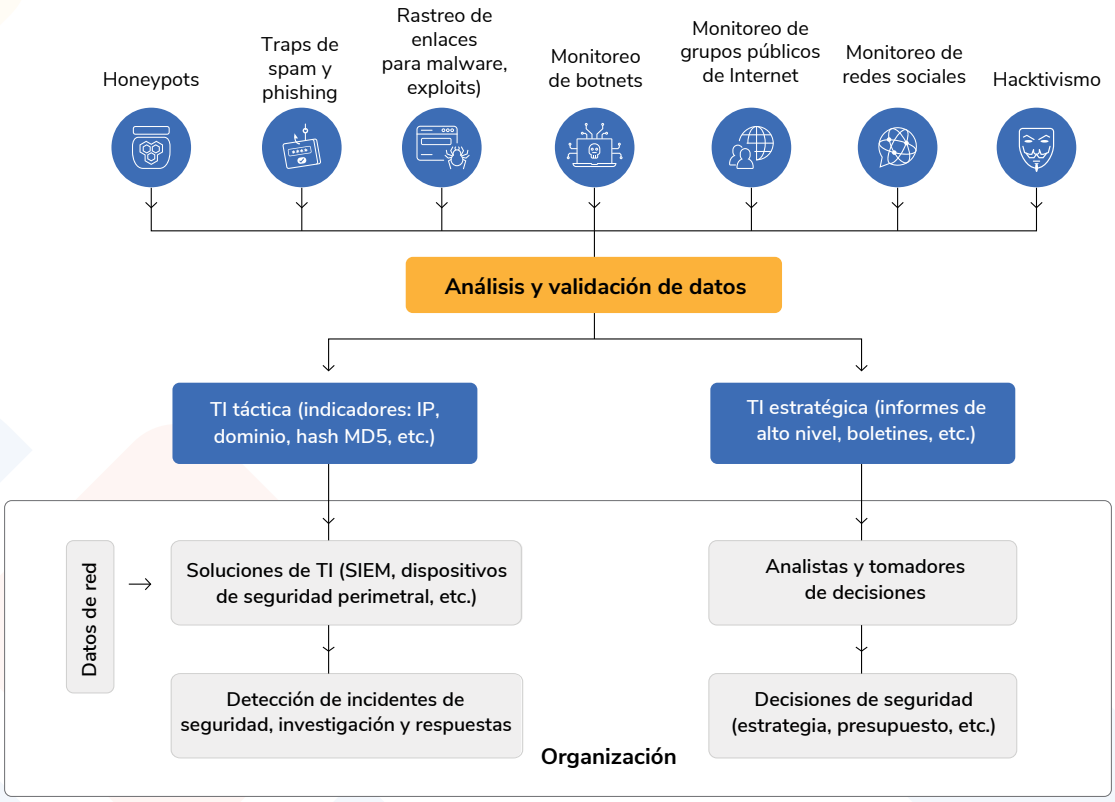
Gartner, la principal empresa de investigación y asesoramiento del mundo, define la inteligencia de amenazas como "un conocimiento basado en pruebas que incluye el contexto, los mecanismos, los indicadores, las implicaciones y los consejos procesables sobre una amenaza o un peligro existente o emergente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

Esta definición nos ayuda a observar los siguientes aspectos de la inteligencia de amenazas

- Basada en un enfoque de "mal conocido", la inteligencia de amenazas ayuda a las organizaciones a detectar amenazas con base en lo que se ha observado en otras partes del mundo.
- La inteligencia de amenazas no sólo es una lista de IP maliciosas. También incluye perfiles detallados de atacantes, mecanismos de ataque e instrucciones sobre cómo responder a una amenaza.
- Está en constante evolución y proporciona información sobre las amenazas existentes y emergentes.
- Su principal objetivo es equipar mejor a las organizaciones para luchar contra las amenazas globales.

El ciclo de la inteligencia de amenazas

La definición de inteligencia de amenazas nos ayuda a apreciar lo que es; sin embargo, todavía no aborda dos preocupaciones importantes: ¿De dónde viene? ¿Y cómo se incorpora en el contexto de la seguridad de la red de una organización? El siguiente diagrama puede ayudarnos a visualizar las respuestas a estas preguntas:



Los datos de inteligencia de amenazas se recopilan de todo Internet mediante una combinación de técnicas automatizadas y manuales. Luego, los equipos de investigación especializados procesan estos datos, analizando y validando la información antes de publicarla en forma de inteligencia de amenazas estratégica o táctica.

La inteligencia de amenazas estratégica está pensada principalmente para el consumo humano, y orienta las decisiones estratégicas de seguridad, como decidir en qué áreas de la ciberseguridad hay que centrarse, lanzar programas de concienciación de empleados sobre las amenazas más recientes, etc.

La inteligencia de amenazas táctica normalmente se publica en forma de fuentes contra amenazas, y generalmente es leída 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 Symantec Deepsight.

Las ventajas de la SIEM

Entre la amplia gama de soluciones de seguridad disponibles actualmente que ofrecen funciones de inteligencia de amenazas, ninguna es tan completa como las que ofrecen las soluciones SIEM. De hecho, las soluciones SIEM son la opción más popular entre quienes desean desarrollar funciones de inteligencia de amenazas. Cuando se trata de inteligencia de amenazas, los siguientes factores suponen una ventaja para las soluciones SIEM:

Calidad de la inteligencia de amenazas

Las alertas de seguridad son tan buenas como la información en la que se basan. Como se mostró en el diagrama anterior, el procesamiento de los datos sobre amenazas implica un gran esfuerzo humano. Esto significa que la calidad de la información sobre amenazas puede variar mucho entre los distintos proveedores.

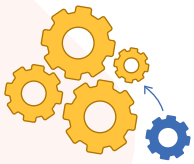
Las soluciones SIEM procesan inteligencia de amenazas de fuentes de confianza, y algunas incluso le dan la opción de añadir fuentes personalizadas a las que su organización se suscribe de forma independiente. Dado que muchas fuentes contra amenazas son específicas de un sector o de ciertos tipos de amenazas, su organización debería utilizar fuentes personalizadas.

Visión global de su red

El conocimiento de las amenazas globales no le sirve de nada si no puede utilizarlo en el contexto de su propia red. Gracias a la visión global de todos los dispositivos y aplicaciones de su red, las soluciones SIEM pueden notificarle si se detectan entidades maliciosas en cualquier sistema de su red.

Las soluciones SIEM utilizan los resultados de los datos de la red para clasificar las alertas de forma más eficaz. Pueden reducir los falsos positivos al emitir una alerta sólo si el atacante detectado tiene patrones de actividad específicos y sospechosos.

Menos integraciones requeridas

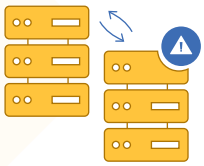


En última instancia, el objetivo de la inteligencia de amenazas es hacer que el ciclo de detección y respuesta a incidentes sea lo más eficiente y rápido posible. Si estas funciones se distribuyen entre varias soluciones que no se integran bien, esto frustra el objetivo de la inteligencia de amenazas.

Las soluciones SIEM superan este problema al proporcionar la mayoría de las funciones necesarias desde una única consola que permite realizar integraciones de manera eficiente cuando sea necesario. Una vez que se detecta, se puede investigar, gestionar y responder al incidente de seguridad. Esto ayuda a acelerar el proceso de resolución de incidentes, garantizando que su organización permanezca protegida frente a cualquier amenaza.

Inteligencia de amenazas y SIEM en acción: Casos de uso empresariales

Comunicación con los servidores de retro llamada



A veces, si un sistema de su red se infecta, puede quedar bajo el control de un servidor externo, también conocido como servidor de retro llamada (callback) o de comando y control. Este servidor de retro llamada puede utilizar este sistema para extraer datos sensibles o infectar otros servidores críticos de su red.

Las soluciones SIEM analizan constantemente los logs de tráfico saliente de su red y registran las comunicaciones que se envían a este tipo de servidores. Luego 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 de retro llamada.

Intentos de inyección de SQL desde fuentes maliciosas

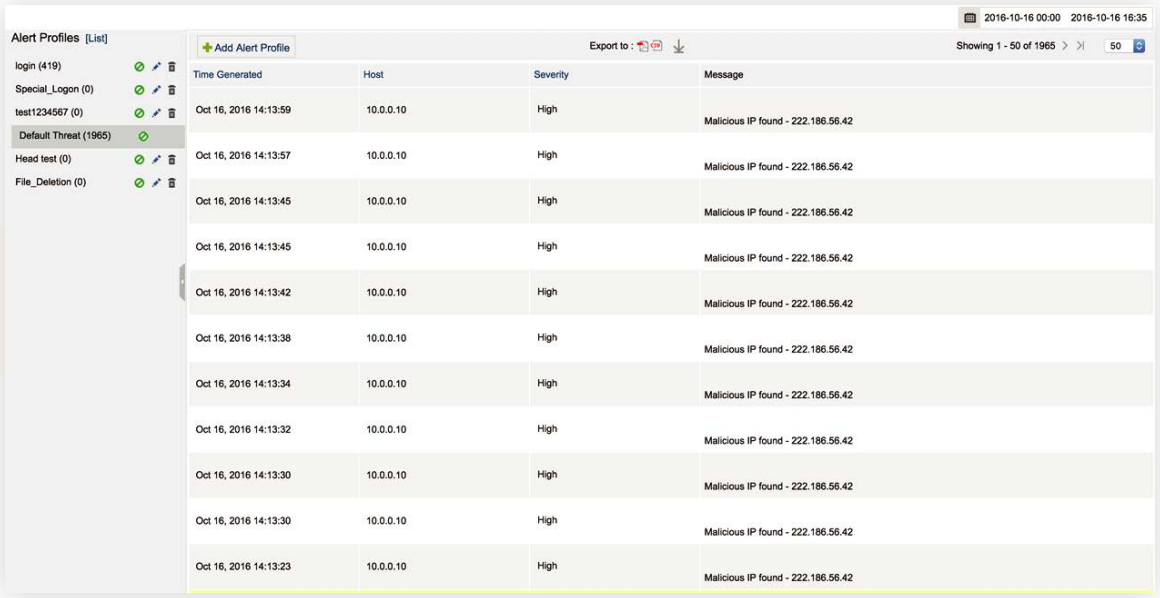
Los atacantes pueden explotar las vulnerabilidades de su servidor web e inyectar código SQL malicioso para recuperar registros comerciales confidenciales de sus bases de datos. Para evitar este tipo de infracciones de datos, las soluciones SIEM controlan todas las conexiones entrantes a sus servidores web y detectan cualquier IP o dominio malicioso. Esto le permite contener la pérdida de datos importantes e identificar y corregir las vulnerabilidades de su servidor web.

Potenciales descargas de malware

Los atacantes siempre están buscando nuevas formas de infiltrarse en su red y descargar malware en sus sistemas. Dado que el malware no se distingue fácilmente del software normal, hay que estar atento a los indicadores que sugieren la existencia de un software problemático.

Por ejemplo, si un atacante conocido se conecta remotamente a su red tras un ataque de fuerza bruta a la VPN de su organización, accede a un sistema de la red y descarga software en él, lo más probable es que se trate de un ataque de malware. Las soluciones SIEM utilizan módulos de correlación que pueden buscar patrones de actividad como éste, lo que le permite detectar ataques con gran precisión y reducir las alertas de falsos positivos.

Funciones destacadas: El módulo de inteligencia de amenazas de Log360



El módulo de inteligencia de amenazas de ManageEngine Log360 ofrece estas ventajas:

- **Actualizaciones dinámicas:** El procesador de fuentes contra amenazas de la solución recupera automáticamente la inteligencia de amenazas más reciente de fuentes de código abierto altamente fiables.
- **No requiere configuraciones:** El perfil de alerta de las fuentes contra amenazas está preconfigurado. Log360 comienza a analizar su red en busca de amenazas tan pronto añade fuentes de log para el monitoreo.
- **Posibilidad de añadir fuentes personalizadas:** Añada fácilmente fuentes contra amenazas personalizadas basadas en STIX/TAXII para compararlas con los logs de su red.

- **Generador de reglas de correlación:** Cree reglas de correlación personalizadas que detectan las actividades sospechosas de un atacante y activan alarmas.
- **Potente motor de búsqueda:** Busque en millones de logs en segundos y cree un rastro de log de cualquier actividad de actores maliciosos en su red.
- **Gestión de incidentes:** Supervise el estado de las alertas de amenazas con la consola de gestión de tickets integrada en la solución, o reenvíe las alertas a consolas de mesa de ayuda externas.
- **Respuesta automática:** Asigne scripts personalizados para que se activen automáticamente cuando se produzca una alerta de amenaza.

Conclusión

La inteligencia de amenazas realmente revoluciona la lucha contra el creciente número de ciberataques a los que se enfrentan las organizaciones. Se trata de un esfuerzo global y de colaboración por parte de la industria de la ciberseguridad, y cuando se utiliza correctamente, ayuda a las organizaciones a detectar y frustrar las amenazas en el momento de su detección.

Gracias a sus completas funciones de seguridad, las soluciones SIEM son la opción ideal para implementar sistemas de inteligencia de amenazas en las empresas. Y con las alertas de amenazas efectivas, podrá proteger a su organización en todo momento.