Cisco Stealthwatch

Análisis de seguridad y visibilidad escalable

¿Se ha visto comprometido? ¿Cómo lo sabe?

Ya ha realizado una gran inversión en la infraestructura de TI y la seguridad de su organización. Sin embargo, los ataques llegan a su objetivo y los agentes internos hostiles actúan con impunidad. Además, se tarda meses o incluso años en detectar las amenazas[1]. Esta falta de visibilidad de las amenazas es una característica de la complejidad creciente de la red, así como de los ataques en constante evolución. Así mismo, los equipos de seguridad, con sus recursos limitados y herramientas inconexas, hacen lo que pueden. ¿Cómo sabe si sus controles de seguridad actuales están funcionando, se gestionan y se configuran correctamente? ¿Y cómo sabe que estas herramientas hacen el trabajo para el que las necesita?

La solución: red + seguridad

Los metadatos de los paquetes de red pueden proporcionar información útil sobre quién se conecta a la organización y cuál es su intención. Todo entra en contacto con la red, por lo que esta información puede abarcar desde la central a la sucursal, la nube pública y los centros de datos privados, hasta los usuarios en itinerancia e incluso el Internet of Things (IoT). Analizar estos datos puede ayudar a detectar amenazas que puedan haber encontrado la forma de superar los controles existentes antes de que tengan un impacto significativo. También puede detectar comportamientos cuestionables de personal interno hostil. También cabe destacar que el análisis que funciona correctamente puede disminuir la carga del equipo de seguridad y proporcionarle más oportunidades para concentrarse en las amenazas de alta probabilidad. Este enfoque para la detección avanzada de amenazas es:

Se integra
con su infraestructura actual

Sin agente
sin la necesidad de instalar sensores en todas partes

Flexible
en términos de implementación y opciones de consumo: en las instalaciones o en la nube, appliance de hardware/virtual o SaaS

Gane confianza en la efectividad de su seguridad

Cisco Stealthwatch proporciona visibilidad de toda la empresa, desde la red privada a la nube pública y aplica análisis de seguridad avanzado para detectar y responder a las amenazas en tiempo real. Analiza continuamente las actividades de la red y crea una línea de base del comportamiento de red normal para, a continuación, utilizarla junto con algoritmos de machine learning avanzados para detectar anomalías. Sin embargo, no todas las cosas *raras* son maliciosas y Stealthwatch puede correlacionar de forma rápida y con gran confianza las anomalías con las amenazas como ataques de comando y control, ransomware, ataques de denegación de servicios, criptominería ilícita, malware desconocido, así como amenazas internas. Con una solución única sin agentes, obtendrá supervisión de amenazas completa del centro de datos, las sucursales, los terminales y la nube, independientemente de la presencia de cifrado en la red.

Ventajas

Se conoce a todos los hosts. Se ven todas las conversaciones.

Entiende lo que es normal. Se reciben alertas sobre los cambios.

Se responde rápidamente a las amenazas.

- **Supervisa y detecta de forma continua** las amenazas avanzadas que han superado los controles de seguridad existentes o que se originan desde el interior
- **Se centra en los incidentes críticos, sin distracciones,** con alarmas contextuales de alta fiabilidad priorizadas por gravedad de la amenaza
- **Respuesta rápida y efectiva** con un conocimiento completo de la actividad de la amenaza, seguimientos de auditoría de la red para las investigaciones forenses e integración con los controles de seguridad existentes
- **Aprovecha las inversiones existentes** en la infraestructura de TI y utiliza la completa telemetría de la red para una mayor seguridad
- **La seguridad se amplía a medida que crecen las necesidades empresariales,** tanto si añade una nueva sucursal o centro de datos como si trasladan cargas de trabajo a la nube o, simplemente, se añaden más dispositivos
- **Garantiza el cumplimiento** con alarmas que informan del incumplimiento de las políticas y que se pueden adaptar a la lógica empresarial

1. El tiempo medio de detección de una brecha es de 197 días según el informe Ponemon 2018.

“Cisco Stealthwatch nos ha ayudado a obtener visibilidad del tráfico interno en un 100 %, lo que ha dado como resultado la identificación de amenazas que eran muy difíciles de detectar previamente”.

Arquitecto de TI, empresa de gran tamaño
Empresa de fabricación industrial

Siguientes pasos

Si desea obtener más información, visite https://www.cisco.com/c/es_es/products/collateral/security/stealthwatch/datasheet-c78-739398.html o póngase en contacto con el representante de su cuenta en Cisco.

C45-736510-05 11/18

Visibilidad contextual de toda la red

Stealthwatch proporciona **visibilidad de toda la empresa sin agentes** en las instalaciones, así como en todos los entornos de nube pública. Con el conocimiento de quién se encuentra en la red y qué están haciendo, también ayuda a las organizaciones a implementar una **segmentación más inteligente** personalizada según la lógica empresarial. Y proporciona **inteligencia accionable** enriquecida con contexto como el usuario, dispositivo, ubicación, marca de tiempo, aplicación, etc.

Análisis predictivos de amenazas

Stealthwatch usa un canal de técnicas analíticas para detectar amenazas avanzadas antes de que se conviertan en una brecha. Mediante el uso del **análisis del comportamiento de la red,** puede señalar anomalías, que se analizan más a fondo mediante una combinación de **machine learning supervisado y no supervisado** para una detección de amenazas de alta fidelidad. Esto permite que su equipo de seguridad se centre en las amenazas más graves. El motor de análisis de seguridad de Stealthwatch también funciona con la **inteligencia de amenazas de Cisco Talos,** líder del sector y que cuenta con la información más actualizada para la correlación de amenazas locales y globales.

Detección y respuesta automatizadas

La combinación de esta visibilidad de toda la empresa basada en el contexto y la aplicación de técnicas analíticas avanzadas ayuda a las organizaciones a detectar amenazas como el **malware desconocido o cifrado, las amenazas internas, los incumplimientos de la política** y cualquier cosa relacionada con la red. Los equipos de seguridad pueden ver las **alarmas, cuya prioridad se ordena por gravedad de la amenaza,** y disponen de información adicional para emprender acciones de forma fácil. Stealthwatch también tiene la capacidad para almacenar la telemetría a escala y proporciona seguimientos de auditoría de la red para **investigaciones forenses** de eventos pasados y para la **supervisión del cumplimiento.** Por último, se integra con sus controles de seguridad existentes para responder a la amenaza, sin paradas en la actividad empresarial.

Análisis del tráfico cifrado para una mayor seguridad

El rápido aumento de tráfico cifrado está cambiando el panorama de las amenazas. Aunque el cifrado es estupendo para la seguridad y privacidad de los datos, también se ha convertido en una oportunidad para que los cibercriminales escondan malware y eviten la detección. Gartner predice que, para el año 2019, el 80 % de todo el tráfico web estará cifrado y el 70 % de los ataques utilizarán cifrado. No es viable para descifrar y analizar el tráfico cifrado y pronto, con la aparición de TLS 1.3, no será ni siquiera posible. Cisco ha introducido una tecnología revolucionaria, **Encrypted Traffic Analytics (ETA),** respaldada por la red de Cisco y Stealthwatch de última generación, para analizar el tráfico cifrado sin ningún descifrado. Esto permite a las organizaciones 1) detectar amenazas en el tráfico cifrado y 2) realizar el cumplimiento criptográfico para saber qué porcentaje de su negocio digital utiliza un cifrado sólido y auditar en busca de incumplimientos de la política. Para obtener más información, vaya a https://www.cisco.com/go/eta