Comparación de soluciones de análisis de seguridad

Descubra las características de Cisco Stealthwatch en comparación con otros productos de análisis de seguridad. Esta solución se amplía fácilmente, lo que le aporta visibilidad en toda la red. Stealthwatch puede detectar y responder a las amenazas avanzadas en tiempo real mediante machine learning y modelos de entidad.

See Stealthwatch

	Cisco Stealthwatch	Darktrace	Plixer
Detección			
Análisis y detección de malware en tráfico cifrado	✓ Utiliza Encrypted Traffic Analytics	✗ Análisis y detección de malware en tráfico cifrado	✗ Análisis y detección de malware en tráfico cifrado
Detección de acumulación de datos	✓ Los eventos se acumulan en el índice de acumulación de datos, que se mide mediante un límite absoluto o el comportamiento aprendido del host o los grupos.	Limitada Puede detectar una anomalía, pero no un evento específico de acumulación de datos	✗
Detección de movimientos laterales	✓ Ofrece detección de gusanos y seguimiento visual del malware a través de la red	Limitada Puede detectar una anomalía, pero no cuenta con una capacidad publicada para alertar específicamente sobre movimientos laterales	✗
Seguimiento de auditoría de toda la red	✓ Puede registrar todas las conversaciones en la red mediante recopiladores y sensores de flujo	Limitada Únicamente utiliza sensores, por lo que es probable que omita parte del tráfico	✓ Flujo de tráfico almacenado en la caja
Detección de reconocimiento	✓ Puede detectar análisis rápidos y lentos mediante un algoritmo exclusivo de gran sensibilidad a los eventos de velocidad de análisis muy reducida	Limitada Puede detectar el reconocimiento, pero es probable que no sea tan sensible como el algoritmo de análisis exclusivo de Stealthwatch	✓ Con análisis de flujo opcional
Machine learning	✓ Utiliza machine learning de varias capas para ofrecer una detección de alta fidelidad	✓	Limitada Cuenta con funciones limitadas para definir puntos de referencia en función de cálculos de tráfico amplios

	Cisco Stealthwatch	Darktrace	Plixer
Detección (continuación)			
Detección de fugas	✓ Genera una alarma de "sospecha de pérdida de datos" para los hosts que filtran más datos (incluidos datos cifrados) que uno normal	Limitada. Únicamente utiliza sensores en lugar de la telemetría del hardware de la red y la detección se limita a las ubicaciones de colocación de los sensores	✗
Detección de control y mando	✓ Puede detectar varios eventos de seguridad mediante análisis e inteligencia de amenazas para detectar pares de control y mando	Limitada. Únicamente utiliza sensores en lugar de la telemetría de la red y la detección se limita a las ubicaciones de colocación de los sensores	Limitada. Sin algoritmos específicos para control y mando
Detección de anomalías	✓ Cuenta con un sistema de detección de anomalías desarrollado y probado con más de 150 algoritmos	Limitada. Únicamente utiliza sensores en lugar de la telemetría de la red y la detección se limita a las ubicaciones de colocación de los sensores	Limitada. Con análisis de flujo opcional
Detección de malware	✓ Puede ofrecer una detección de vulnerabilidades de día cero	Limitada. Únicamente utiliza sensores en lugar de la telemetría de la red y la detección se limita a las ubicaciones de colocación de los sensores	Limitada. Con análisis de flujo opcional
Implementación			
Escalabilidad	✓ Puede ampliarse hasta 6 millones de flujos por segundo, gestionar 100 Mbps para conexiones de interfaz de 10 Gbps y picos en el tráfico superiores a los niveles nominales y recopilar la telemetría de miles de sensores	Limitada. Únicamente utiliza sensores en lugar de la telemetría de la red	Limitada. Es obligatorio realizar una personalización y configuración importantes para respaldar los mapas de flujo y la generación de informes consolidados en varios recopiladores de Plixer.
Almacenamiento de datos	✓ De media, el sistema puede almacenar 30-45 días de flujos de datos, y a menudo mucho más, para realizar una investigación forense en mayor profundidad.	Limitada. Sin informes de datos para confirmar la capacidad de almacenamiento	✓
Detección de vulnerabilidades de día cero	✓ Puede detectar malware nuevo o único para el que aún no existen firmas gracias a un método de comportamiento con más de 90 parámetros	✓ Únicamente utiliza sensores en lugar de la telemetría de la red y la detección se limita a las ubicaciones de colocación de los sensores	Limitada. Cuenta con funciones limitadas para definir puntos de referencia en función de cálculos de tráfico amplios

	Cisco Stealthwatch	Darktrace	Plixer
Implementación (continuación)			
Compresión de datos	✓ A medida que el recopilador recibe los flujos, se sintetizan en flujos bidireccionales residentes en la memoria. Esto reduce los falsos positivos y permite el almacenamiento eficiente de datos y la generación de informes precisos a nivel de host.	No es aplicable Únicamente utiliza sensores en lugar de la telemetría de la red.	Limitada Parte de la información se descarta
Modelo de implementación	Véase la nota No requiere la implementación de sensores o sondas caras. La telemetría puede activarse de manera sencilla desde los dispositivos de red para analizar el tráfico de la red.	Véase la nota Los clientes deben adquirir sensores y elegir enlaces que supervisar en lugar de simplemente activar la telemetría en los dispositivos de red y obtener todas las conversaciones; el modelo es caro y difícil de ampliar.	Véase la nota Puede consumir la mayoría de las fuentes de telemetría basada en flujos
Visibilidad de terminales	✓ Con Cisco AnyConnect 4.2 y versiones posteriores, la licencia de datos de terminales recopila la telemetría de los terminales mediante el protocolo Cisco Network Visibility Flow (nvzFlow).	✗	✗ Carece de características como contraseña de enable, preajustes de configuración para tipos de NAD y proxy TACACS+
Visibilidad de la nube	✓ Puede supervisar la nube pública a través de la solución basada en SaaS Stealthwatch Cloud	Limitada Utiliza sensores para supervisar la red de la nube privada y un conector de nube para aplicaciones de particulares	Limitada Consume registros de Amazon AWS, que son similares a los flujos e incluyen acciones de permiso y denegación
Exportación de datos	Véase la nota Cuenta con integraciones con sistemas de información de seguridad y ofrece API para la integración personalizada; también es compatible con la API REST y SOAP	Véase la nota Cuenta con un conector de Splunk que tomas los datos de syslog JSON de un appliance de Darktrace y muestra los incidentes de seguridad en Splunk; también los vincula con informes en el visualizador de amenazas de Darktrace	Véase la nota Es compatible con la API REST y los resultados de los registros
Notificaciones de alarma	Véase la nota Ofrece correo electrónico o exportación de syslog al sistema SIEM, Netcool, sistema de incidencias Remedy, etc., con notificaciones de correo electrónico, SNMP y syslog	Véase la nota Ofrece resultados con formato syslog	Véase la nota Ofrece registros y alertas salientes

	Cisco Stealthwatch	Darktrace	Plixer
investigación			
Flujos de trabajo de investigación de amplio alcance	✓ Puede investigar eventos de seguridad de ejecución larga. Genera alarmas basadas en el contexto y personalizadas, vincula el nombre de usuario con la dirección IP, supervisa el uso de la interfaz, realiza una inspección profunda de paquetes y registra todas las conversaciones de la red.	Limitada Clasifica la amenaza que detecta y la muestra en la interfaz del visualizador de amenazas	Limitada Carece de interfaces personalizables, de tendencias históricas rápidas, funciones automatizadas de remediación y herramientas de análisis del origen del problema
Eficacia para clientes de grandes empresas	✓ Simplifica la segmentación mediante modelos lógicos de grupo de hosts para organizar a los usuarios por ubicación, función, dirección IP, etc.; ofrece detalles de notificación personalizados y formatos con reconocimiento de alarmas	Limitada Únicamente utiliza sensores en lugar de la telemetría de la red, por lo que la ampliación a las empresas resulta difícil	Limitada Es obligatorio realizar una personalización y configuración importantes para respaldar los mapas de flujo y la generación de informes consolidados en varios recopiladores de Plixer.
Consulta flexible y sistema de filtrado	✓ Puede realizar consultas sobre todos los campos capturados. La búsqueda avanzada está disponible para el tráfico cifrado para el intercambio de claves de cifrado, el algoritmo de cifrado, la longitud de clave, la versión TLS/SSL, etc.	No es aplicable No hay información comparativa disponible en los materiales publicados	Limitada Carece de interfaces personalizables, de tendencias históricas rápidas, funciones automatizadas de remediación y herramientas de análisis del origen del problema.
Panel de ciberamenazas	Véase la nota Facilita información pertinente para el personal de operaciones de seguridad, como qué índices se completan con alertas, qué alarmas están activas, qué hosts tienen la mayoría de alarmas asociadas a ellos, etc. También ofrece la posibilidad de obtener más detalles y la telemetría asociada.	Véase la nota Principalmente una herramienta de seguridad y el espacio de trabajo se centra en las operaciones de seguridad	Véase la nota Seguridad y supervisión de la red basadas en el panel
Visualización y mapas	Véase la nota Genera mapas automáticos como rutas de propagación de gusanos y mapas de relaciones personalizados, lo que permite la visualización de cualquier conjunto de hosts y de cómo se comunican con cualquier otro conjunto	Véase la nota Muy orientada a los gráficos	Véase la nota Gráficos y diagramas sencillos
Investigación de incidentes	Véase la nota La interfaz de usuario se organiza en torno a flujos de trabajo basados en la persona, lo que lleva de inmediato a los administradores al origen de los problemas y a información adicional.	Véase la nota Cuenta con un visualizador de amenazas que permite la visibilidad y la gestión de las amenazas	Véase la nota Se ofrecen flujos de trabajo de investigación.

	Cisco Stealthwatch	Darktrace	Plixer
Contexto			
Riqueza de los datos contextuales	✓ Integración con Cisco Identity Services Engine (ISE). Permite la búsqueda de información de los hosts, como ID de usuario, dirección MAC, tipo de dispositivo y puerto de switch; no requiere una consulta independiente para buscar el usuario asociado debido a que se puede registrar el ID de usuario	Limitada Integración con Active Directory para los datos de usuario	Limitada Ofrece sensores centrados en una gran variedad de datos, incluidos el rendimiento de las aplicaciones y perspectivas en profundidad de DNS
Datos de identidad	✓ Integración con Cisco ISE, los productos Cisco ASA (NSEL), servidores DHCP/RADIUS y servidores de autenticación de Active Directory para la correl-ación de la identidad con la telemetría	Limitada Integración con Active Directory para los datos de usuario	Limitada Integración con Active Directory
Integración de proveedores de routing y switching	✓ Los routers, switches, firewalls y controladores inalámbricos son el principal origen de los datos. Puede analizar de manera nativa muchas versiones de telemetría y NetFlow de varios proveedores, como IPFIX y sFlow, además de otros protocolos de capa 7.	✗ Únicamente utiliza sensores en lugar de la telemetría de la red. Requiere SPAN o TAP para cada enlace supervisado y se limita a lo que incluye el enlace.	
Captura de datos de URL	See note Los sensores de flujo pueden extraer los datos de URL utilizados por los recopiladores de flujo y el centro de gestión. Se pueden consultar los datos de URL en función de los operadores. Además, se integra con Cisco Security Packet Analyzer, que puede descargar datagramas exactos que el flujo representa en formato PCAP.	See note Totalmente basada en sensores y cuenta con visibilidad de datos de paquetes	See note Puede capturar datos de URL mediante sensores

	Cisco Stealthwatch	Darktrace	Plixer
Contexto (continuación)			
Generación de NetFlow para entornos VMware	✓ Utiliza la función de exportación de NetFlow de switches virtuales o el sensor de flujo virtual	No es aplicable. No es aplicable ya que utiliza sensores para registrar el tráfico	✓ Puede consumir telemetría de NetFlow en VMware
Recopilación de datos de aplicaciones y flujos L7	✓ Mantiene el estado del flujo (activo, inactivo o continuo); genera NetFlow en función de la supervisión de puertos SPAN o TAP; cuenta con integración de proxy; ofrece la identidad de las aplicaciones de varios proveedores como Palo Alto Networks y L7 Defense, y utiliza NBAR y NBAR2 con el sensor de flujo	✓ Utiliza sondas que analizan estos datos directamente en paquetes sin procesar	Limitada. Puede recibir datos de firewalls, flujos de un SPAN con sensor e ID de aplicaciones de un sensor o firewall. Sin integración de proxy ni compatibilidad con NBAR.
Captura de paquetes completos	✓ Integración con Cisco Security Packet Analyzer, una herramienta que se instala en un SPAN o TAP que mantiene un búfer circular de datagramas en un segmento y ofrece la posibilidad de descargar datagramas exactos que la telemetría representa en formato PCAP e incluso los archivos contenidos en PCAP. También puede iniciar la decodificación de paquetes en lugar de descargar otra aplicación.	Desconocido. No hay información de comparación disponible en los materiales publicados	✗ Sin posibilidad de capturar paquetes completos
Análisis del tráfico cifrado	✓ Utiliza Encrypted Traffic Analytics o la telemetría mejorada de la red de Cisco para detectar malware y ayudar a garantizar el cumplimiento del cifrado. Stealthwatch analiza el tráfico cifrado mediante machine learning avanzado y inteligencia sobre amenazas globales.	Limitada. Podría detectar algunos comportamientos anómalos en el tráfico cifrado	✗ Sin posibilidad de analizar el tráfico cifrado
Puntuación de reputación de toda la empresa	✓ Crea puntuaciones basadas en índices para todos los hosts que calculan la actividad inusual de un host	Desconocido. El modelo de detección de anomalías podría utilizar un mecanismo de puntuación global	✗ Sin conceptos de índices de seguridad; únicamente activa alarmas y alertas generales

	Cisco Stealthwatch	Darktrace	Plixer
Inteligencia de amenazas			
Fuente de inteligencia de amenazas	✓ La licencia de inteligencia de amenazas de Stealthwatch y el mapa de riesgo global, con el respaldo de Talos, es una fuente de amenazas de una serie de fuentes que se actualiza al menos una vez cada hora. Su objetivo es ofrecer un conjunto de información con cero falsos positivos.	✓ Una fuente de amenazas que dispone de una lista de sitios maliciosos conocidos.	✗ Ninguna, aunque Plixer presenta un appliance centrado en DNS para la detección de problemas de DNS
Detección de vulnerabilidades	✓ Puede detectar amenazas internas como comunicaciones de control y mando y fuga de datos, además de ataques largos y lentos. Los eventos de seguridad aportan datos a los índices para activar alarmas por medio de algoritmos de comportamiento y límites absolutos que el operador puede definir.	✓ Se requiere la detección de una serie de vulnerabilidades, pero se desconoce el alcance.	✗
Intercambio de inteligencia de amenazas	✓ Cisco Talos utiliza los datos de inteligencia de amenazas de Stealthwatch y viceversa. Cisco comparte datos con cientos de partners, clientes y proveedores a través de los programas Aegis, Crete y Aspis, y es miembro fundador de la Alianza contra las Ciberamenazas.	✗	✗

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.