Cisco Live Terminales seguros y sesiones SecureX

Contenido

Introducción

Cisco Live Las Vegas es uno de los principales eventos de la industria con más de 1100 sesiones programadas actualmente del 4 al 8 de junio en el Centro de Convenciones de Mandalay Bay. Con un catálogo de cursos tan amplio, queríamos asegurarnos de que nuestros clientes de terminales seguros eran conscientes de las oportunidades educativas para utilizar nuestros productos y servicios de forma eficaz. Al destacar solo una pequeña selección de los 129 laboratorios disponibles, sesiones introductorias y debates sobre el tema de la seguridad disponibles este año en Las Vegas, esperamos que considere la posibilidad de unirse a nosotros para ayudar a hacer del mundo un lugar más seguro.

Laboratorios impartidos por un instructor

Terminal seguro de Cisco: hacerlo bien cambiando a la izquierda - LTRSEC-1114

Caly Hess, Security PrincessX, Cisco Systems, Inc.
Pedro Medina, Ingeniero de software, Cisco Systems, Inc.

Endpoint Security es la última barrera de defensa en el cambiante panorama de la ciberdelincuencia y, si se configura correctamente, Cisco Secure Endpoint puede mantener su organización segura. En esta sesión, tendrá acceso práctico a Secure Endpoint Console mientras aprende las configuraciones y prácticas de implementación para obtener la mejor condición en materia de seguridad de un equipo de ingeniería que ha trabajado con Secure Endpoint (FKA AMP) durante la mayor parte de una década. Aprenderá las capacidades y la funcionalidad de cada motor y en qué entornos se pueden utilizar de forma óptima. Sabrá cómo establecer alertas y automatizaciones para mitigar un ataque en curso, de modo que su organización no tenga que ser la siguiente brecha importante.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: laboratorio impartido por un instructor
Nivel técnico: Introductorio
Tecnología: seguridad
Opción: Seguridad

Cubre la evolución de la seguridad del correo electrónico desde gateways de correo electrónico seguros a plataformas basadas en API - LTRSEC-2011

Un análisis en profundidad por correo electrónico sobre la integración de SecureX para sacar el máximo partido a su implementación de XDR.

Alberto Torralba, Arquitecto de soluciones técnicas.Ventas, Cisco Systems, Inc.
Greg Barnes, Ingeniero técnico de marketing, Cisco Systems, Inc.

En esta sesión de laboratorio se describirán las funciones más recientes de la cartera de Cisco Secure Email. La sesión se centrará en las prácticas recomendadas para que los participantes puedan sacar el máximo partido de su plataforma de correo electrónico. Entre los temas del gateway se incluyen el uso de la inteligencia privada SecureX Cisco Threat Response, la configuración de la autenticación de mensajes basada en dominio, la generación de informes y el cumplimiento (DMARC), el registro avanzado, el uso de la API y mucho más. Los participantes también aprenderán a integrar el gateway en la nueva nube que ofrece Cisco Secure Email Threat Defence. El laboratorio describirá el software como una oferta de servicio

para buscar amenazas como el riesgo del correo electrónico empresarial que carecen de indicadores tradicionales de riesgo e investigar las cuentas potencialmente comprometidas.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: laboratorio impartido por un instructor
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Firewall seguro: solución de problemas de ruta de datos de Threat Defence (práctica práctica en laboratorio) - LTRSEC-3880

John Groetzinger, Director técnico, Cisco Systems, Inc
Foster Lipkey, Ingeniero principal, Cisco Systems, Inc. - Orador distinguido
Vidhi Mujumdar, Líder, Prestación de servicios al cliente, Cisco Systems

Una preocupación habitual de los usuarios de la solución Cisco Firepower es qué deben hacer en caso de que se produzca una degradación o interrupción de la red que parezca estar relacionada con la solución Firepower. En este laboratorio, los participantes aprenderán metodologías de resolución de problemas para evaluar los problemas de ruta de datos en la plataforma Firepower, incluidos los NGIP Firepower serie 3, ASA con Firepower Services, Firepower Threat Defense (FTD) y FXOS. Esta sesión proporcionará a los participantes un marco para identificar qué parte de Firepower Services está contribuyendo al problema y cómo mitigar rápidamente los problemas identificados. Este marco cubrirá la totalidad de la ruta de datos desde el ingreso de paquetes hasta la inspección profunda de paquetes, incluida la regla Snort y el rendimiento del preprocesador. En este laboratorio se analizarán tanto Snort 2.9 como Snort 3 y las diferencias entre ellos. Este laboratorio contendrá situaciones de solución de problemas mediante Virtual Firepower Threat Defence (vFTD) para implementar el marco de solución de problemas. Además, este laboratorio abordará brevemente la integración de SecureX Secure Firewall.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: laboratorio impartido por un instructor
Nivel técnico: Avanzado
Tecnología: seguridad
Opción: Seguridad

Taller de resistencia cibernética - LTRSEC-1113

Ron Taylor, Sr. Security Lab Test Monkey, Cisco Systems, Inc.
Leo Cruz, Arquitecto de soluciones técnicas, Cisco Systems, Inc.

¿Está su equipo preparado para el próximo ataque a la cadena de suministros o para el próximo día cero? Comprobación de la realidad! Todos estamos bajo ataque, todos los días y todos estaremos eventualmente comprometidos! Por este motivo, su organización debe ser ciberresistente. La resistencia cibernética hace referencia a la capacidad de una organización para identificar, responder y recuperarse rápidamente de un incidente de seguridad de TI. La creación de resistencia cibernética incluye la realización de un plan centrado en los riesgos que asume que la empresa se enfrentará en algún momento a una brecha o a un ataque. En este laboratorio, experimentará ataques de ciberseguridad en un entorno de laboratorio empresarial en el que se juega a ser atacante y defensor y aprenderá de primera mano por qué necesita soluciones de seguridad altamente integradas y habilidades de CyberOps para ser resistente a las amenazas cibernéticas.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: laboratorio impartido por un instructor
Nivel técnico: Introductorio

Tecnología: SecureX, seguridad
Opción: Seguridad

Desgloses

Resolución de problemas de rendimiento y aislamiento debido a terminales seguros (Windows, Linux y MAC) - BRKSEC-2072

Vibhor Amrodia, Director técnico, Cisco Systems, Inc

Esta sesión le ofrecerá ideas que le ayudarán a aislar de forma rápida y eficaz los problemas de rendimiento con los terminales seguros instalados. Esta es una sesión en profundidad sobre cómo podemos analizar y aislar los problemas de rendimiento en sus terminales (Windows, Linux y MAC) utilizando algunos de los registros disponibles con Secure Endpoint y también algunas de las herramientas y utilidades específicas del sistema operativo. Las áreas de interés para esta sesión serían: Detección y aislamiento de la utilización de CPU y RAM en Windows CPU y RAM en Linux Detección y aislamiento de la utilización de CPU y RAM en MAC Detección y aislamiento de la utilización de CPU y RAM

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: seguridad
Opción: Seguridad

Agente unificado de Cisco: Cisco Secure Client. Combinación de AMP, AnyConnect, Orbital y Umbrella - BRKSEC-2834

Aaron Woland, Ingeniero distinguido, Cisco Systems, Inc. - Orador distinguido

Todos hemos oído las quejas o hemos hecho nosotros mismos las quejas: "Cisco tiene demasiados agentes".

Aaron Woland, CCIE #20113 y la prestigiosa sala de la fama de Cisco Live le enseñan que Cisco ha escuchado las quejas y ha presentado la primera iteración de un agente de seguridad unificado: Cisco Secure Client.

Cisco Secure Client (CSC) proporciona un marco modular que permite que AnyConnect VPN, Cisco Secure Endpoint (anteriormente AMP para terminales), Network Visibility Module, Umbrella Cloud Security, ISE Posture, Secure Firewall Posture (anteriormente Hostscan) y Network Access Module (NAM) existan todos juntos; con una moderna gestión basada en la nube procedente de SecureX, íntimamente conectada con información de dispositivos SecureX.

En esta sesión, profundizaremos en la tecnología subyacente a Secure Client, cómo funcionan realmente las cosas y cómo no. Trataremos los modelos de implementación desde la nube y utilizaremos sus propios mecanismos de implementación de software. Aprenderemos todo sobre los flujos de actualización integrales de los agentes existentes de AnyConnect y Secure Endpoint (AMP). Hablaremos de situaciones en las que tiene sentido actualizar a CSC y situaciones en las que realmente le beneficie permanecer con los agentes de AnyConnect y Secure Endpoint (AMP) existentes, al menos por ahora.

Venga a pasar algún tiempo con Aaron y diviértase mientras aprende todo sobre este interesante desarrollo de Cisco Security.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout

Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Desde la nave hasta la costa: integraciones, colaboración y (de forma segura) toma de control más allá de Cisco Secure Email Gateway - BRKSEC-2288

Robert Sherwin, Director técnico, Cisco Systems, Inc. - Altavoz distinguido

Cisco Secure Email se integra fuera de ser su propia gateway de correo electrónico. Seguridad, registro, API y configuración, y SecureX: le guiaremos por el modo en que el correo electrónico se extiende más allá del gateway y es posible sacar el máximo partido de su entorno, ya sea grande o pequeño.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Nube de defensa frente a malware de Cisco e integraciones de análisis de malware seguro - BRKSEC-2242

Bill Yazji, Arquitecto de seguridad técnica, Cisco Systems, orador distinguido

Puede que lo haya conocido como "AMP Cloud and Threat Grid", pero se les ha rebautizado como Malware Defense Cloud and Secure Malware Analytics. En esta sesión se revisarán y profundizarán en las ofertas de Malware Defence Cloud y Malware Analytics, al tiempo que se abordan sus integraciones con las arquitecturas de seguridad de Cisco, entre las que se incluyen Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella y Meraki. Estos productos funcionan en conjunto y hablaremos sobre la arquitectura de defensa frente a malware y demostraremos cómo todas las piezas encajan para ofrecer la arquitectura de amenazas avanzadas líder del sector. Esta sesión es perfecta para aquellos que son nuevos en Cisco Security Suite, así como para aquellos clientes que poseen uno o más productos y desean profundizar en cómo trabajan juntos.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Cisco XDR con firewall - BRKSEC-2090

Eric Kostlan, Ingeniero Técnico De Marketing, Cisco Systems, Inc., Ponente Destacado
Adi Sankar, Ingeniero técnico de marketing, Cisco Systems, Inc.

SecureX, el XDR de Cisco, es la plataforma más amplia e integrada del mundo. En esta sesión, los asistentes verán el poder del firewall y la integración de SecureX. Esto incluye los incidentes de firewall en SecureX, el enriquecimiento del firewall en investigaciones de respuesta ante amenazas y la orquestación de SecureX mediante API de firewall. Los asistentes deben tener conocimientos básicos de Cisco Secure Firewall. Los asistentes no necesitan conocer SecureX.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Acelere su SOC con Cisco SecureX - BRKSEC-1023

Matt Vander Horst, Líder Técnico, Cisco - Orador distinguido

¿Sabía que la plataforma SecureX XDR de Cisco puede acelerar la forma en que su organización investiga y responde a los incidentes? SecureX combina un conjunto de funciones que le permiten hacerse cargo de los incidentes de seguridad, obtener una mejor visibilidad de una amplia cartera de productos y utilizar la automatización para investigar y responder a la velocidad de la máquina. En esta sesión, obtendrá una introducción a SecureX y aprenderá los aspectos básicos de sus diversas funciones, entre las que se incluyen: el panel de SecureX, la respuesta ante amenazas, el administrador de incidentes, la orquestación, la información de los dispositivos y el cliente seguro. También compartiremos una lista de otras sesiones a las que puede asistir para profundizar en estas funciones y mucho más.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: Introductorio
Tecnología: SecureX, seguridad
Opción: Seguridad

Cisco XDR con correo electrónico: protección, análisis y evolución de la conversación SMTP - BRKSEC-2095

Robert Sherwin, Líder Técnico, Cisco Systems, Inc. - Orador distinguido

El correo electrónico se conoce como el eslabón más débil de una red empresarial y, en menos de dos minutos, proporciona a los hackers y a los atacantes una puerta abierta que conduce a un riesgo o a una brecha. El correo electrónico es un vector principal de la infección de malware, ya que coloca sin esfuerzo cargas maliciosas delante del usuario y solo está a un clic de la explotación. Más allá de la mera distribución de malware, los atacantes son más sofisticados que nunca a la hora de crear y generar enlaces de phishing que se parecen a los servicios que están suplantando. Cisco Secure Email está desarrollando la forma en que la detección y respuesta extendidas se dirige a estos vectores de amenazas y protege sus conversaciones SMTP.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Detección ampliada con Cisco XDR: análisis de seguridad en toda la empresa - BRKSEC-2178

Matthew Robertson, Ingeniero distinguido de marketing técnico de Cisco Systems, Inc. (orador distinguido)

Detección y respuesta ampliadas (XDR) es una palabra de moda muy conocida en la actualidad. Si se desmitifica el tema, en esta sesión se explorarán las capacidades de detección y análisis ampliadas del XDR de Cisco, con especial atención a cómo ampliar las capacidades de detección y acelerar la respuesta. En esta

sesión, que abarca varias tecnologías de detección, como los análisis de terminales, redes y firewalls, se explorará cómo los análisis pueden aunar estas detecciones y cumplir el objetivo del XDR.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Cisco IT Security de la A a la Z. Protección frente a malware avanzado sin confianza: BRKCOC-2620

Steve Vida, Arquitecto de ciberseguridad, Cisco Systems, Inc.
Gil Daudistel, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, Cisco Systems, Inc.

Hacer lo imposible: Cisco aumentó la seguridad y mejoró la experiencia en un solo movimiento gracias a la introducción de la confianza cero para el personal. Esta sesión profundizará en los detalles del flujo de autenticación segura Zero Trust, cómo nos beneficiamos de alinear el nuevo flujo con una mejor experiencia y cómo implementamos configuraciones de terminales para admitir Zero Trust con Jamf Pro, InTune/SCCM y Meraki Systems Manager.
En esta sesión también se hablará sobre cómo Cisco IT implementa y mantiene Cisco Secure Endpoint en su flota de más de 200 000 dispositivos.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: trabajo híbrido, seguridad
Opción: Cisco sobre Cisco

Cisco SecureX XDR: todas las piezas y piezas tienen sentido - BRKSEC-2113

Aaron Woland, Ingeniero distinguido, Cisco Systems, Inc. - Orador distinguido

La detección y respuesta extendidas (XDR) es una de las tecnologías de seguridad más novedosas del mercado, y está experimentando un tremendo crecimiento en su adopción. Dada la amplia gama de lo que se puede, se debe y se hace en una solución XDR, es natural que haya una gran complejidad que puede generar confusión sobre cómo y qué sucede entre bastidores. Esta sesión arrojará luz sobre el funcionamiento interno de la increíblemente capaz solución XDR de Cisco, con Network Detection & Response, Endpoint Detection & Response, Email Threat Defense, Malware Analytics, Unified Security Agent; y cómo todas estas partes y piezas se unen para producir el resultado esperado de un XDR.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Aprovechamiento de la solución XDR de Cisco con gestión de servicios de TI (ITSM) y sistemas SIEM para la investigación de incidentes - BRKSEC-2122

Oxana Sannikova, arquitecta de soluciones técnicas, Cisco Systems, Inc.

En esta sesión demostraremos cómo la plataforma XDR (detección y respuesta extendidas) SecureX puede

aumentar las operaciones de seguridad para ofrecer mejores resultados sin crear complejidad adicional. Analizaremos los siguientes casos prácticos: aprovechar el contexto de IT Service Management (ITSM) y SIEM en la búsqueda de amenazas, añadir visibilidad de amenazas consolidada a los incidentes de ITSM y las alertas de SIEM, formalizar los procedimientos de respuesta ante incidentes aprovechando la automatización y la orquestación. Casi la mitad de la sesión serán manifestaciones. Las soluciones ITSM y SIEM tratadas incluirán ServiceNow, Jira y Splunk, y los asistentes se marcharán con flujos de trabajo listos para usar.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: automatización y orquestación, seguridad
Opción: Seguridad

Integración de Open Source Zeek y Cisco XDR - BRKSEC-2075

King Mark Stephens, Arquitecto de ciberseguridad global, CISCO Richfield, Ohio

Las soluciones de detección y respuesta ampliadas (XDR) ofrecen la posibilidad de proteger a las organizaciones frente a los eventos de ciberseguridad, ya que detectan y responden con mayor rapidez y reducen el riesgo y la exposición. Un XDR debe incluir integraciones de terceros para proporcionar motores de detección adicionales. En esta sesión se presentará Zeek de código abierto y se proporcionarán detalles sobre cómo realizar la integración en Cisco XDR para mejorar los resultados de seguridad de los clientes.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

¡El poder de GreySkull! Emulación adversarial: BRKSEC-2180

Jason Maynard, CTO de campo de ciberseguridad de Canadá, CSS

En esta sesión aprenderemos sobre la emulación contradictoria y cómo los equipos rojos y azules pueden beneficiarse de su uso. Aprendemos acerca de las herramientas disponibles para nosotros y luego construimos una operación aprovechando Caldera sin capacidades preventivas. A continuación, revisaremos los resultados contradictorios, que incluyen la revisión de los resultados de nuestra cartera de soluciones de seguridad de Cisco implementadas de forma pasiva. El conocimiento adquirido garantiza que los equipos de defensa entiendan la oportunidad de aumentar nuestras defensas. A continuación, activaremos nuestras capacidades preventivas en una variedad de tecnologías de seguridad de Cisco y volveremos a realizar la prueba revisando los resultados. Entender cómo el adversario aborda la capacidad de sus víctimas y defensores para defenderse por capas es una receta para el éxito.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Introducción a la gestión de vulnerabilidades basada en riesgos - BRKSEC-1639

David Brothers, Arquitecto de soluciones técnicas, Cisco Systems, Inc.

La gestión de vulnerabilidades basada en riesgos (RBVM) abarca más de lo que probablemente cree. En esta entretenida e informativa charla, profundizaremos en los conceptos básicos y subrayaremos las teorías de cuantificación del riesgo y luego compartiremos cómo los programas prácticos de RBVM son esenciales para asegurar la red moderna. A continuación, hablaremos sobre cómo Kenna aporta RBVM a una amplia gama de productos y ofertas de Cisco.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Breakout
Nivel técnico: Introductorio
Tecnología: SecureX, seguridad
Opción: Seguridad

Desglose interactivo

Aprovechamiento de SecureX con Cisco Talos Incident Response - IBOSEC-2011

Joe Schumacher, Comandante de incidentes, Cisco Systems, Inc.

Los participantes aprenderán directamente de nuestro equipo de respuesta ante incidentes de Cisco Talos (Talos IR) sobre cómo aprovechar SecureX para acelerar los esfuerzos de respuesta durante un incidente de seguridad. Obtendrán información sobre cómo utilizar SecureX, tanto si trabajan con una empresa externa de respuesta a incidentes como Talos IR como si llevan a cabo una respuesta de investigación interna. La sesión se desarrollará en torno a una llamada telefónica organizada en la línea directa de infrarrojos de Talos por parte de un cliente de retención ficticio con varios productos de seguridad de Cisco. El equipo de infrarrojos de Talos se encargará de establecer objetivos sobre la respuesta y de obtener información general antes de pasar a las actividades de respuesta ante emergencias, que incluirán el uso de SecureX junto con otros productos de seguridad hasta que se haya contenido el incidente.
Los objetivos del período de sesiones serán informar a los participantes en las siguientes esferas:
Incorporación de SecureX para conectar elementos observables para que los equipos colaboren y trabajen durante la investigación
Integración de SecureX con los productos de seguridad para organizar una respuesta eficaz y puntual

Tipo de sesión: Interactive Breakout
Nivel técnico: Introductorio
Tecnología: SecureX, seguridad
Opción: Seguridad

Profundice en el intercambio de ideas de SecureX - IBOSEC-2005

Josh Bordelon, Arquitecto de seguridad empresarial global de Cisco Systems, Inc.

Explore e intercambie ideas sobre la utilización de SecureX con Cisco Security y herramientas de terceros en una sesión interactiva en la que trataremos la creación y conexión de diversos servicios. Traiga sus ideas y preguntas o aprenda de otras personas que ya han iniciado su viaje a SecureX.

Tipo de sesión: Interactive Breakout
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Laboratorios de entrada

Cisco Secure Client y SecureX Device Insights: mejor juntos - LABSEC-2776

Paul Carco, INGENIERO DE MARKETING TÉCNICO, Cisco Systems, Inc.
Serhii Kucherenko, ingeniero de escalado de clientes de Cisco Systems, Inc.

Cisco Secure Client es un nuevo cliente unificado que reúne a la mayoría de los clientes de terminales de Cisco en un mismo marco. Cisco Secure Client consta de módulos AnyConnect estándar y clientes de seguridad como AMP (también conocido como Cisco Secure Endpoint) y Orbital. Como parte de este LABORATORIO, aprenderá a implementar y administrar Cisco Secure Client desde SecureX Cloud. La parte dedicada a SecureX Devices Insights demostrará cómo Cisco Secure Client y sus módulos se pueden utilizar para la gestión de activos a nivel empresarial y la investigación de incidentes de seguridad.

Tipo de sesión: Walk-in Lab
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Seminarios técnicos

Cisco Secure Client: desde AnyConnect hasta la completa seguridad del cliente - TECSEC-2780

Hacke Nohre, Arquitecto de soluciones técnicas, Cisco - Ponente destacado
Thorsten Schranz, Ingeniero Técnico De Marketing, Cisco Systems, Inc., Destacado Ponente
Valeria Scribanti, Especialista en soluciones técnicas, Cisco Systems, Inc. - Oradora distinguida

El nuevo personal híbrido, los complejos escenarios de ataque, la rápida adopción de la nube y la omnipresencia del cifrado en Internet han hecho que la seguridad de los clientes sea más importante que nunca.
En esta sesión de 4 horas, mostraremos cómo podemos ampliar AnyConnect (VPN) para ofrecer una seguridad completa para terminales. Profundizaremos en los aspectos técnicos de los módulos de Cisco Secure Client, entre los que se incluyen:
EDR/EPP (terminal seguro)
Telemetría de red de terminales (Network Visibility Module)
Protección de DNS/Web (Umbrella)
Estado del terminal (ISE/Secure Firewall)
y en los resultados de la ejecución de un único cliente gestionado de forma centralizada en Cisco SecureX (XDR).
El público objetivo son los ingenieros y arquitectos de redes y seguridad interesados en la seguridad de los terminales. Se supone que se dispone de cierto conocimiento de la seguridad de los terminales, los sistemas operativos y los vectores de ataque habituales.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Seminario técnico
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

Detección y respuesta ampliadas con Cisco Secure - TECSEC-2004

Matthew Robertson, Ingeniero distinguido de marketing técnico de Cisco Systems, Inc. (orador distinguido)

Hanna Jabbour, Ingeniera Líder En Marketing Técnico, Cisco Systems, Inc., Oradora Destacada

Adi Sankar, Ingeniero técnico de marketing, Cisco Systems, Inc.

Matt Vander Horst, Líder Técnico, Cisco - Orador distinguido

Esta sesión, que comienza con una profundización en la oferta Extended Detection and Response de Cisco, proporcionará un recorrido completo por la implementación y el funcionamiento de los diversos componentes del producto, incluidos Cisco Secure Endpoint, Secure Cloud Analytics, Umbrella, Meraki y Email Threat Defence, así como su funcionamiento en Cisco XDR. También se incluirán prácticas recomendadas operativas y detalles de implementación en el funcionamiento del motor de respuesta, así como la integración de Cisco XDR con productos que no son de Cisco, como Crowdstrike Falcon.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: Seminario técnico
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: Seguridad

DevNet

Automatización de la seguridad: desarrollo con SecureX - DEVNET-1083

Matt Vander Horst, Líder Técnico, Cisco - Orador distinguido

¿Sabía que la plataforma XDR de Cisco cuenta con varias formas de automatizar sus operaciones de seguridad y crear potentes integraciones? Los módulos de integración de SecureX le permiten incorporar datos de otras plataformas a sus investigaciones, las API de respuesta ante amenazas de SecureX le permiten automatizar la forma en que investiga y responde a las amenazas, y la orquestación de SecureX le permite crear flujos de trabajo potentes utilizando un editor de arrastrar y soltar de código no-a-bajo. Pase por esta sesión para obtener más información sobre cada una de estas tres facetas de SecureX y cómo puede utilizarlas para impulsar sus operaciones de seguridad.

Tipo de sesión: DevNet
Nivel técnico: Introductorio
Tecnología: SecureX, seguridad

Opción: DevNet

Automatización de las operaciones de ciberhigiene con SecureX y seguridad Kenna - DEVLIT-1355

Oxana Sannikova, arquitecta de soluciones técnicas, Cisco Systems, Inc.

Las operaciones de TI siguen siendo muy manuales en la actualidad. Los clientes se enfrentan siempre al reto de mantener el buen estado del sistema y mejorar la seguridad online. En esta sesión rápida demostraremos cómo se puede aprovechar la orquestación de Cisco SecureX y Kenna Security para automatizar la gestión de vulnerabilidades.

Tipo de sesión: DevNet
Nivel técnico: intermedio
Tecnología: automatización y orquestación, seguridad
Opción: DevNet

Uso de la orquestación SecureX para automatizar la respuesta a incidentes de la nube

pública - DEVWKS-2240

Brian Sak, Arquitecto de soluciones técnicas, Cisco Systems, Inc. - Ponente distinguido

Cuando las cargas de trabajo se trasladan a proveedores de nube pública como AWS, Azure o GCP, la respuesta a incidentes y la remediación pueden volverse más difíciles y requerirán herramientas diferentes. Esta sesión le guiará en la creación de flujos de trabajo de orquestación de SecureX que automatizan y simplifican el proceso de identificación de amenazas, simplifican los procedimientos de respuesta y proporcionan a los equipos de seguridad tranquilidad a la hora de proteger los recursos en entornos de nubes múltiples o híbridas.
La novedad de este año en el taller DevNet es que los asistentes registrados previamente se sientan en primer lugar. Solo hay 12 portátiles disponibles para esta sesión. Este es un taller práctico de DevNet en el que se codifica junto con un instructor. Traiga sus propios auriculares de 3,5 mm con conector auxiliar para escuchar al presentador o tome un par de auriculares en el Centro de Comando DevNet.
Al asistir a este taller de DevNet, podrá obtener créditos de Cisco Continuing Education (CE). Encontrará más información en: https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: DevNet
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: DevNet

Ampliación de flujos de trabajo de nube híbrida con SecureX Orchestrator y conector remoto - DEVNET-2109

Steve McNutt, Arquitecto de soluciones técnicas, Cisco Systems, Inc.

Puede que haya oído hablar de SecureX Orchestration (SXO) en el contexto de la orquestación de la seguridad. Le demostraremos que puede hacer mucho más y que es la base para crear herramientas eficaces de operaciones en la nube híbrida. Esta sesión comienza con una descripción general de la arquitectura de alto nivel seguida de un recorrido por la solución de ejemplo de implementación masiva de Cisco Umbrella, en la que se explica cómo encajan los componentes y los retos que resuelven. En esta sesión aprenderá a crear flujos de trabajo de nube híbrida altamente escalables aprovechando el modelo de sidecar y estará familiarizado con el código de ejemplo que puede modificar para crear sus propias soluciones.

Tipo de sesión: DevNet
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: DevNet

Cómo duplicar la cuenta R en XDR: Cómo automatizar sus operaciones de seguridad (SecOps) con 10 clics en Cisco SecureX (sin escribir ninguna línea de código) - DEVNET-2214

Christopher Van Der Made, Director de productos de ingeniería, Cisco Systems, Inc., destacado ponente

En esta sesión se mostrará cómo aprovechar el poder de la automatización a través de SecureX Orchestration sin escribir ningún código. Esto permitirá a las organizaciones duplicar el recuento de R en XDR (detección y respuesta ampliadas) de Cisco. Vamos a caminar a través de un par de ejemplos muy simples de instalar que le hará golpear el suelo corriendo. Utilizaremos la cantidad de clics que se necesitan en la consola como métrica, para demostrarle cómo puede obtener acceso a una potente automatización sin

demasiadas molestias. Al final, también aprenderá cómo llevar esto un paso más allá y lentamente convertirse en un maestro en la automatización de sus operaciones de seguridad. Obtendrá todos los materiales después para comenzar usted mismo. Esta sesión está dirigida a los responsables de la respuesta ante incidentes, analistas de seguridad, directores de SOC o cualquier persona interesada en la automatización y la seguridad.

Tipo de sesión: DevNet
Nivel técnico: intermedio
Tecnología: SecureX, seguridad
Opción: DevNet

Integración con la API de Microsoft Graph: uso de Python y SecureX - DEVWKS-3260

Hacke Nohre, Arquitecto de soluciones técnicas, Cisco - Ponente destacado

En este taller explicaremos cómo se puede integrar la API de Microsoft Graph en entornos típicos de Cisco. Trataremos una descripción general de alto nivel de la API de Microsoft Graph con un poco de énfasis en la autenticación y autorización de Oauth2 para Azure AD.
A continuación, mostraremos cómo podemos acceder a esta API a través de scripts python y SecureX para acceder a la información sobre los grupos y roles de Azure AD para un usuario específico
obtener acceso a información sobre eventos de seguridad del entorno de Microsoft
Los asistentes pueden intentar seguir los pasos del taller desde los entornos de laboratorio durante el taller o pueden completar los pasos más tarde. Proporcionaremos indicaciones a las configuraciones de laboratorio que permiten a los asistentes completar las tareas del taller por su cuenta, sin necesidad de tener su propia cuenta de Azure o SecureX.

Califica para el crédito de educación continua de Cisco: Sí
Tipo de sesión: DevNet
Nivel técnico: Avanzado
Tecnología: DevNet, seguridad
Opción: DevNet

Automatice y simplifique su defensa contra el ransomware con SecureX - DEVNET-1456

Elia Maracani, ingeniera de sistemas de Cisco Systems, Inc.

Los ataques de ransomware se centran cada vez más en las copias de seguridad. Proteger, así como recuperar rápida y fácilmente la copia de seguridad de su empresa, se está convirtiendo en el mejor y más importante paso en la defensa contra los ataques de ransomware debilitantes. Con la ayuda de una demostración, destacaremos la versatilidad y personalización que SecureX puede proporcionar a través de su motor de orquestación. Gracias a la integración que Cisco SecureX proporciona con las soluciones de primera (Cisco Umbrella, Cisco Secure Endpoint) y de terceros (Cohesity Helios), podrá reducir drásticamente el tiempo y la complejidad de la detección, investigación y recuperación de ransomware.

Tipo de sesión: DevNet
Nivel técnico: Introductorio
Tecnología: SecureX, seguridad
Opción: DevNet

Descripción general del producto o estrategia

Cisco XDR: la base del centro de operaciones de seguridad del mañana - PSOSEC-1007

Sana Sana Yousuf, Gerente de marketing de productos, Cisco Systems, Inc.

Los equipos de seguridad se enfrentan a un panorama de amenazas en expansión y a una eficacia de la seguridad compleja que hace que el entorno sea cada vez más esquiva. La línea de pobreza de la ciberseguridad se está ampliando y los sujetos malintencionados están aprovechando este enorme agujero para desencadenar ataques persistentes. Creemos que solo una solución eficaz de "detección y respuesta ampliadas" puede detectar y remediar a adversarios sofisticados como Turla, Wannacry y NotPetya en su entorno. Descubra el valor disruptivo del XDR en el universo híbrido, multivectorial y multivectorial. Escuche cómo defiendo un ecosistema en continuo crecimiento de integraciones tecnológicas de varios proveedores como base para crear las operaciones de seguridad del futuro. ¿Y cómo XDR puede convertirse en un multiplicador de fuerza para su SOC?

Tipo de sesión: descripción general del producto o la estrategia
Nivel técnico: General
Tecnología: SecureX, nube híbrida, seguridad
Opción: Seguridad

Cómo reforzar de forma proactiva su resistencia de seguridad - PSOCX-2000

Varun Dhingra, Director, Gestión De Productos, Seguridad Y Colaboración, Cisco Systems, Inc.
Mark Hammond, Director de gestión de productos de Cisco Systems, Inc

No solo tiene que gestionar la ciberseguridad, sino que también se enfrenta a una presión real para adoptar normativas basadas en la privacidad de los datos. ¿Cómo diseña un programa de ciberseguridad que cumpla los requisitos en constante cambio de riesgo, regulación, objetivos empresariales e impacto operativo? En esta sesión, aprenderá a diseñar un marco de privacidad y seguridad de datos alineado con el sector para satisfacer las necesidades de las partes interesadas y generar soluciones que permitan la agilidad empresarial. El marco está diseñado para realizar un seguimiento de las actividades y los resultados de ciberseguridad que se desean de forma intuitiva para permitir una comunicación sencilla y no técnica entre equipos multidisciplinares.

Tipo de sesión: descripción general del producto o la estrategia
Nivel técnico: intermedio
Tecnología: experiencia del cliente, SecureX, seguridad

Oportunidades adicionales

Además de los numerosos tipos de sesiones que se han mencionado anteriormente, Live! cuenta con mucha innovación e inspiración en la sala de conferencias. Meet the Engineers, Capture the Flag o Take the Challenge, Live! sigue demostrando que Cisco es el puente hacia lo posible. Consulte el catálogo completo y más información en Ciscolive.com.


cisco Live!
Let's go

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).