Cisco Live Sichere Endpunkt- und SecureX-Sitzungen

Inhalt

Einleitung

Cisco Live Las Vegas ist eines der bedeutendsten Branchenveranstaltungen mit über 1100 Sitzungen, die derzeit vom 4. bis 8. Juni im Mandalay Bay Convention Center geplant sind. Mit einem derart umfangreichen Kurskatalog wollten wir sicherstellen, dass unsere Secure Endpoint-Kunden die Bildungschancen zur effektiven Nutzung unserer Produkte und Services kennen. Wir möchten Ihnen die 129 verfügbaren Labs, Breakout Sessions und Diskussionen rund um das Thema Sicherheit vorstellen, die dieses Jahr in Las Vegas verfügbar sind. Wir hoffen, dass Sie sich uns anschließen werden, um die Welt sicherer zu machen.

Praktische Übungen mit Kursleiter

Cisco Secure Endpoint: Nach links verschieben - LTRSEC-1114

Caly Hess, Security PrincessX, Cisco Systems, Inc.
Pedro Medina, Software Engineer, Cisco Systems, Inc.

Endpoint Security ist die letzte Verteidigungslinie in der sich weiterentwickelnden Cyberkriminalität. Wenn Cisco Secure Endpoint richtig konfiguriert ist, kann Ihr Unternehmen sicher sein. In dieser Sitzung erhalten Sie praktischen Zugriff auf die Konsole für sichere Endgeräte und lernen Bereitstellungskonfigurationen und -verfahren für den besten Sicherheitsstatus von einem Technikerteam kennen, das seit mehr als einem Jahrzehnt mit sicheren Endgeräten (FKA AMP) zusammenarbeitet. Sie lernen die Fähigkeiten und Funktionen jeder Engine kennen und erfahren, in welchen Umgebungen sie optimal genutzt werden können. Sie wissen, wie Sie Warnmeldungen und Automatisierungen einrichten, um einen laufenden Angriff einzudämmen, damit Ihr Unternehmen nicht die nächste größere Sicherheitsverletzung sein muss.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Lab mit Kursleiter
Technische Ebene: Einführung
Technologie: Sicherheit
Kategorie: Sicherheit

Deckt die Entwicklung der E-Mail-Sicherheit von sicheren E-Mail-Gateways zu API-basierten Plattformen ab - LTRSEC-2011

Eine E-Mail mit detaillierten Informationen zur Integration von SecureX, um das Beste aus Ihrer XDR-Bereitstellung herauszuholen.

Alberto Torralba, Technical Solutions Architect.Vertrieb, Cisco Systems, Inc.
Greg Barnes, Technical Marketing Engineer, Cisco Systems, Inc.

In dieser Übung erhalten Sie einen Überblick über die neuesten Funktionen des Cisco Secure E-Mail-Portfolios. Der Schwerpunkt der Sitzung liegt auf Best Practices, damit die Teilnehmer ihre E-Mail-Plattform optimal nutzen können. Zu den Themen für Gateways gehören die Nutzung von SecureX Cisco Threat Response mit privaten Informationen, die Konfiguration von Domain-basierter Message Authentication, Reporting & Conformance (DMARC), erweiterte Protokollierung, API-Nutzung und vieles mehr. Die Teilnehmer lernen außerdem, wie sie das Gateway in die neuere Cloud integrieren können, indem

sie Cisco Secure Email Threat Defense anbieten. Im Rahmen der Übung wird ein Überblick über das Software-as-a-Service-Angebot gegeben, mit dem nach Bedrohungen wie geschäftlichen E-Mail-Kompromittierungen gesucht werden kann, bei denen es keine herkömmlichen Indications of Compromise gibt, und mögliche kompromittierte Konten untersucht werden können.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Lab mit Kursleiter
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Sichere Firewall - Fehlerbehebung im Datenpfad zum Schutz vor Bedrohungen (praktische praktische Übung) - LTRSEC-3880

John Groetzinger, Technischer Leiter, Cisco Systems, Inc
Foster Lipkey, Principal Engineer, Cisco Systems, Inc. - Distinguished Speaker
Vidhi Mujumdar, Leiter, Kundenbetreuung, Cisco Systems

Ein häufiges Problem für Benutzer der Cisco FirePOWER-Lösung ist, was im Fall einer Netzwerkunterbrechung oder -verschlechterung zu tun ist, die mit der FirePOWER-Lösung in Zusammenhang zu stehen scheint. In dieser Übung lernen die Teilnehmer Methoden zur Fehlerbehebung kennen, mit denen sich Datenpfad-Probleme innerhalb der Firepower-Plattform analysieren lassen, einschließlich Firepower Series 3 NGIPs, ASA mit Firepower Services, Firepower Threat Defense (FTD) und FXOS. In dieser Sitzung erhalten die Teilnehmer einen Rahmen, anhand dessen sie feststellen können, welcher Teil der FirePOWER-Services zu dem Problem beiträgt und wie sie die identifizierten Probleme schnell beheben können. Dieses Framework deckt den gesamten Datenpfad vom Paketeingang bis hin zur Deep Packet Inspection ab, einschließlich Snort-Regel und Präprozessorleistung. In dieser Übung werden sowohl Snort 2.9 als auch Snort 3 und die Unterschiede zwischen beiden behandelt. Diese Übung umfasst Szenarien zur Fehlerbehebung mithilfe von Virtual Firepower Threat Defense (vFTD) zur Implementierung des Frameworks für die Fehlerbehebung. Darüber hinaus wird in dieser Übung kurz die SecureX Secure Firewall-Integration behandelt.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Lab mit Kursleiter
Technische Stufe: Erweitert
Technologie: Sicherheit
Kategorie: Sicherheit

Workshop zur Cybersicherheit - LTRSEC-1113

Ron Taylor, Senior Security Lab Test Monkey, Cisco Systems, Inc.
Leo Cruz, Technical Solutions Architect, Cisco Systems, Inc.

Ist Ihr Team auf den nächsten Angriff auf die Lieferkette oder den nächsten Zero Day vorbereitet? Reality Check! Wir sind alle angegriffen, jeden Tag, und wir werden schließlich alle kompromittiert werden! Aus diesem Grund muss Ihr Unternehmen ausfallsicher sein. Cyber-Ausfallsicherheit bezieht sich auf die Fähigkeit eines Unternehmens, einen IT-Sicherheitsvorfall schnell zu identifizieren, darauf zu reagieren und sich davon zu erholen. Zur Erhöhung der Cyber-Ausfallsicherheit muss ein risikoorientierter Plan erstellt werden, der davon ausgeht, dass das Unternehmen irgendwann Opfer einer Sicherheitsverletzung oder eines Angriffs wird. In dieser Übung erleben Sie Cyber-Sicherheitsangriffe in einer Enterprise-Lab-Umgebung, in der Sie Angreifer und Verteidiger spielen und aus erster Hand erfahren, warum Sie hochintegrierte Sicherheitslösungen und CyberOps-Kenntnisse benötigen, um gegen Cyber-Angriffe gewappnet zu sein.

Qualifiziert für Cisco Continuing Education Credit: Ja

Sitzungstyp: Lab mit Kursleiter
Technische Ebene: Einführung
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Breakouts

Fehlerbehebung und Isolierung von Leistungsproblemen aufgrund von sicheren Endgeräten (Windows, Linux und MAC) - BRKSEC-2072

Vibhor Amrodia, Technical Leader, Cisco Systems, Inc

Sie verlassen diese Sitzung mit Ideen, wie Sie Leistungsprobleme bei installierten Secure Endpoints schnell und effektiv isolieren können. In diesem ausführlichen Webinar erfahren Sie, wie Sie Leistungsprobleme auf Ihren Endgeräten (Windows, Linux und MAC) analysieren und isolieren. Dabei werden einige der Protokolle von Secure Endpoint sowie betriebssystemspezifische Dienstprogramme und Tools verwendet. Schwerpunktbereiche für diese Sitzung sind: Erkennung der Windows-CPU- und RAM-Auslastung und Isolierung Erkennung und Isolierung der Linux-CPU- und RAM-Auslastung und Isolierung der MAC-CPU- und RAM-Auslastung

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: Sicherheit
Kategorie: Sicherheit

Cisco Unified Agent: Cisco Secure Client Verbinden von AMP, AnyConnect, Orbital und Umbrella - BRKSEC-2834

Aaron Woland, Distinguished Engineer, Cisco Systems, Inc. - Distinguished Speaker

Wir alle haben die Beschwerden gehört oder die Beschwerden selbst gemacht: "Cisco hat zu viele Agenten".

Lernen Sie von Aaron Woland, CCIE #20113 und Cisco Live Distinguished Speaker Hall of Fame Elite, während er Ihnen zeigt, dass Cisco den Beschwerden zugehört und die erste Version eines Unified Security Agents bereitgestellt hat: Cisco Secure Client.

Der Cisco Secure Client (CSC) bietet ein modulares Framework, mit dem AnyConnect VPN, Cisco Secure Endpoint (ehemals AMP für Endgeräte), Network Visibility Module, Umbrella Cloud Security, ISE Posture, Secure Firewall Posture (ehemals Hostscan) und das Network Access Module (NAM) gemeinsam genutzt werden können. Ein modernes Cloud-basiertes Management, das von SecureX bereitgestellt wird, ist eng mit SecureX-Gerätedaten verbunden.

In dieser Sitzung erfahren Sie mehr über die Technologie hinter dem Secure Client, wie Dinge wirklich funktionieren und wie nicht. Wir behandeln Bereitstellungsmodelle aus der Cloud und unter Verwendung Ihrer eigenen Software-Bereitstellungsmechanismen. Wir informieren uns über die nahtlosen Upgrade-Flows von vorhandenen AnyConnect- und Secure Endpoint (AMP)-Agenten. Wir werden über Szenarien sprechen, in denen ein Upgrade auf CSC sinnvoll ist, und Szenarien, in denen es wirklich von Vorteil ist, mit den vorhandenen AnyConnect und Secure Endpoint (AMP) Agenten zu bleiben - zumindest jetzt.

Kommen Sie und lassen Sie sich von Aaron unterhalten, während Sie sich mit Cisco Security über diese spannende Entwicklung informieren.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Vom Schiff zum Land: Integration, Zusammenarbeit und (sichere) Kontrolle - über das Cisco Secure Email Gateway hinaus - BRKSEC-2288

Robert Sherwin, Technical Leader, Cisco Systems, Inc. - Distinguished Speaker

Cisco Secure Email lässt sich außerhalb des eigenen Mail-Gateways integrieren. Sicherheit, Protokollierung, API und Konfiguration sowie SecureX: Wir erklären Ihnen, wie E-Mails über das Gateway hinausgehen und Ihre Umgebung - ob groß oder klein - optimal nutzen können.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Integration von Malware Defense Cloud und Secure Malware Analytics - BRKSEC-2242

Bill Yazji, Technical Security Architect, Cisco Systems - Distinguished Speaker

Sie kennen es vielleicht als "AMP Cloud and Threat Grid", aber die beiden wurden als "Malware Defense Cloud and Secure Malware Analytics" umbenannt. In dieser Sitzung werden die Cloud- und Malware Analytics-Angebote von Malware Defense vorgestellt und ihre Integration mit Cisco Sicherheitsarchitekturen wie Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella und Meraki näher besprochen. Diese Produkte arbeiten zusammen. In diesem Webinar beschäftigen wir uns mit der Malware Defense Architecture und zeigen, wie alle Komponenten zusammenpassen, um die branchenführende Advanced Threat Architecture bereitzustellen. Diese Schulung richtet sich an neuere Kunden der Cisco Security Suite sowie an Kunden, die ein oder mehrere Produkte besitzen und sich eingehender damit befassen möchten, wie diese zusammenarbeiten.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Cisco XDR mit Firewall - BRKSEC-2090

Eric Kostlan, Technical Marketing Engineer, Cisco Systems, Inc. - Distinguished Speaker
Adi Sankar, Technical Marketing Engineer, Cisco Systems, Inc.

SecureX, XDR von Cisco, ist die umfassendste integrierte Plattform der Welt. In dieser Sitzung erhalten die Teilnehmer einen Überblick über die Vorteile der Firewall- und SecureX-Integration. Dazu gehören Firewall-Vorfälle in SecureX, Firewall-Anreicherung zur Untersuchung von Bedrohungsreaktionen und SecureX-Orchestrierung mithilfe von Firewall-APIs. Die Teilnehmer sollten über grundlegende Kenntnisse der Cisco Secure Firewall verfügen. Die Teilnehmer benötigen keine Kenntnisse über SecureX.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Beschleunigen Sie Ihre SOC mit Cisco SecureX - BRKSEC-1023

Matt Vander Horst, Technical Leader, Cisco - Distinguished Speaker

Wussten Sie, dass die XDR-Plattform SecureX von Cisco die Art und Weise, wie Ihr Unternehmen Vorfälle untersucht und darauf reagiert, beschleunigen kann? SecureX vereint eine Reihe von Funktionen, mit denen Sie Sicherheitsvorfälle beheben, eine bessere Transparenz für ein breites Produktportfolio erzielen und dank Automatisierung mit hoher Maschinengeschwindigkeit ermitteln und reagieren können. In dieser Sitzung erhalten Sie eine Einführung in SecureX und lernen die Grundlagen der verschiedenen Funktionen kennen, darunter: SecureX Dashboard, Reaktion auf Bedrohungen, Incident-Manager, Orchestrierung, Geräteeinblicke und sicherer Client. Darüber hinaus stellen wir Ihnen eine Reihe weiterer Sessions zur Verfügung, in denen Sie mehr über diese Funktionen erfahren können.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Einführung
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Cisco XDR mit E-Mail: Schutz, Analyse und Weiterentwicklung des SMTP-Gesprächs - BRKSEC-2095

Robert Sherwin, Technical Leader, Cisco Systems, Inc. - Distinguished Speaker

E-Mails werden als das schwächste Glied in einem Unternehmensnetzwerk bezeichnet und bieten Hackern und Angreifern in weniger als zwei Minuten eine offene Tür, die zu einer Kompromittierung oder Sicherheitsverletzung führt. E-Mails sind ein wichtiger Angriffsvektor für Malware-Infektionen, da sie den Benutzer mühelos mit schädlichen Payloads konfrontieren und die Ausnutzung nur mit einem Klick verhindern. Über die reine Bereitstellung von Malware hinaus sind Angreifer raffinierter denn je darin, Phishing-Links zu erstellen, die genau wie die Dienste aussehen, die sie imitieren. Cisco Secure Email verbessert die Art und Weise, wie eXtended Detection and Response auf diese Bedrohungsvektoren abzielt und Ihre SMTP-Kommunikation schützt.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Erweiterte Erkennung mit Cisco XDR: Sicherheitsanalysen im gesamten Unternehmen - BRKSEC-2178

Matthew Robertson, Distinguished Technical Marketing Engineer, Cisco Systems, Inc. - Distinguished Speaker

Extended Detection and Response (XDR) ist heute ein beliebtes Schlagwort. Im Mittelpunkt dieser Sitzung stehen die erweiterten Erkennungs- und Analysefunktionen des Cisco XDR. Dabei geht es insbesondere darum, wie Sie Ihre Erkennungsfunktionen erweitern und Ihre Reaktionszeiten verkürzen können. In dieser Sitzung werden mehrere Erkennungstechnologien, einschließlich Endgeräte, Netzwerkanalysen und Firewall, behandelt. Es wird untersucht, wie Analysen diese Erkennungen zusammenführen und die XDR-Ziele erreichen können.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Cisco IT Security von A-Z. Erweiterter Malware-Schutz ohne Vertrauen - BRKCOC-2620

Steve Vida, Cybersicherheitsarchitekt, Cisco Systems, Inc.
Gil Daudistel, MANAGER.INFORMATION SECURITY, Cisco Systems, Inc.

Das Unmögliche tun: Cisco erhöhte die Sicherheit und verbesserte das Anwendererlebnis durch die Einführung von Zero Trust für die Mitarbeiter. In dieser Sitzung werden wir uns näher mit dem sicheren Zero Trust-Authentifizierungsablauf befassen, wie wir von der Abstimmung des neuen Ablaufs mit einer besseren Erfahrung profitiert haben und wie wir Endpunktkonfigurationen zur Unterstützung von Zero Trust mit Jamf Pro, InTune/SCCM und Meraki Systems Manager eingeführt haben.
In diesem Webinar erfahren Sie außerdem, wie Cisco IT Cisco Secure Endpoint in seinen über 200.000 Geräten implementiert und wartet.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: Hybrid-Arbeit, Sicherheit
Kategorie: Cisco on Cisco

Cisco SecureX XDR - Alle Teile verstehen - BRKSEC-2113

Aaron Woland, Distinguished Engineer, Cisco Systems, Inc. - Distinguished Speaker

Xtended Detection and Response (XDR) ist eine der am weitesten verbreiteten Sicherheitstechnologien und verzeichnet ein enormes Umsatzwachstum. Angesichts der großen Bandbreite dessen, was sein kann, sein sollte und was in einer XDR-Lösung gemacht wird, gibt es natürlich eine Menge Komplexität, die zu Verwirrung darüber führen kann, wie/was hinter den Kulissen passiert. In diesem Webinar erfahren Sie mehr über die Funktionsweise der leistungsstarken Cisco XDR-Lösung mit Netzwerkerkennung und -reaktion, Erkennung und Reaktion von Endgeräten, E-Mail-Bedrohungsabwehr, Malware-Analysen, Unified Security Agent und wie all diese Komponenten und Komponenten zusammenwirken, um das Ergebnis zu liefern, das für einen XDR erwartet wird.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Nutzung der XDR-Lösung von Cisco mit IT Service Management (ITSM) und SIEM-

Systemen zur Vorfalluntersuchung - BRKSEC-2122

Oxana Sannikova, Technical Solutions Architect, Cisco Systems, Inc.

In diesem Webinar erfahren Sie, wie die eXtended Detection and Response (XDR)-Plattform SecureX die Sicherheitsfunktionen optimieren kann, ohne die Komplexität zu erhöhen. Wir werden uns mit den folgenden Anwendungsfällen befassen: Nutzung des Kontexts von IT-Servicemanagement (ITSM) und SIEM bei der Verfolgung von Bedrohungen, Hinzufügen konsolidierter Bedrohungstransparenz zu ITSM-Incidents und SIEM-Warnungen, Formalisierung von Incident-Response-Verfahren durch Nutzung von Automatisierung und Orchestrierung. Fast die Hälfte der Tagung wird Demonstrationen sein. Zu den abgedeckten ITSM- und SIEM-Lösungen gehören ServiceNow, Jira und Splunk, und die Teilnehmer stellen fertige Workflows zur Verfügung.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: Automatisierung und Orchestrierung, Sicherheit
Kategorie: Sicherheit

Integration von Open Source Zeek und Cisco XDR - BRKSEC-2075

King Mark Stephens, Global Cyber Security Architect, CISCO Richfield, Ohio

XDR-Lösungen (Extended Detection and Response) bieten das Potenzial, Unternehmen vor Cyber-Sicherheitsvorfällen zu schützen, indem sie Bedrohungen schneller erkennen und darauf reagieren und Risiken und Risiken reduzieren. Ein XDR muss Drittanbieterintegrationen umfassen, um zusätzliche Erkennungs-Engines bereitzustellen. In dieser Sitzung wird Open Source Zeek vorgestellt. Außerdem erhalten Sie detaillierte Informationen zur Integration in Cisco XDR, mit denen sich die Sicherheitsfunktionen für Kunden verbessern lassen.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Die Macht von GreySkull! Adversariale Emulation - BRKSEC-2180

Jason Maynard, Field CTO Cybersecurity Kanada, CSS

In dieser Session erfahren Sie mehr über die Emulation von Angreifern und wie rote und blaue Teams davon profitieren können. Wir lernen die uns zur Verfügung stehenden Tools kennen und bauen dann eine Operation aus, bei der Caldera ohne vorbeugende Fähigkeiten eingesetzt wird. Anschließend überprüfen wir die Ergebnisse des Angriffs. Dazu gehören auch die Ergebnisse aus unserem passiv bereitgestellten Cisco Security-Portfolio. Dank des gewonnenen Wissens können Defensivteams die Möglichkeiten zur Verbesserung unserer Abwehrmechanismen verstehen. Anschließend aktivieren wir unsere vorbeugenden Funktionen für eine Vielzahl von Cisco Sicherheitstechnologien und führen den Test erneut durch, um die Ergebnisse zu überprüfen. Zu verstehen, wie die Angreifer auf ihre Opfer zugehen und wie die Verteidiger vorgehen, ist ein Erfolgsrezept.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit

Kategorie: Sicherheit

Einführung in das risikobasierte Vulnerability Management - BRKSEC-1639

David Brothers, Technical Solutions Architect, Cisco Systems, Inc.

Das risikobasierte Vulnerability Management (RBVM) umfasst mehr, als Sie wahrscheinlich denken. In diesem unterhaltsamen und informativen Vortrag werden wir uns eingehend mit den grundlegenden Konzepten und Theorien zur Quantifizierung von Risiken befassen und anschließend darüber sprechen, wie wichtig praktische RBVM-Programme für die Sicherung des modernen Netzwerks sind. Anschließend besprechen wir, wie Kenna RBVM zu einer breiten Palette von Produkten und Angeboten von Cisco bringt.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: Breakout
Technische Ebene: Einführung
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Interaktives Breakout

Nutzung von SecureX mit Cisco Talos Incident Response - IBOSEC-2011

Joe Schumacher, Incident Commander, Cisco Systems, Inc.

Die Teilnehmer lernen direkt von unserem Cisco Talos Incident Response (Talos IR) Team, wie sie SecureX nutzen können, um die Reaktionszeit bei einem Sicherheitsvorfall zu verkürzen. Sie erhalten Einblicke dazu, wie SecureX eingesetzt werden kann, unabhängig davon, ob sie mit einem externen Incident Response-Unternehmen wie Talos IR zusammenarbeiten oder eine interne Investigation durchführen. Die Sitzung wird von einem fiktiven Kunden mit mehreren Sicherheitsprodukten von Cisco um einen stufenweisen Telefonanruf in die IR-Hotline von Talos aufgebaut. Das IR-Team von Talos arbeitet zunächst an der Festlegung von Zielen für die Reaktion auf Notfälle und an der Gewinnung von Hintergrundinformationen, bevor es sich dann um Notfallmaßnahmen kümmert. Zu diesen Aktivitäten gehört die Verwendung von SecureX zusammen mit anderen Sicherheitsprodukten, bis der Vorfall eingedämmt ist.
Ziel der Sitzung ist es, den Teilnehmer über folgende Themen zu informieren:
Einbindung von SecureX zur Vernetzung von Observablen für die Zusammenarbeit und die Durchführung von Untersuchungen
Integration von SecureX in Sicherheitsprodukte für eine zeitnahe und effektive Reaktion

Sitzungstyp: Interaktives Breakout
Technische Ebene: Einführung
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Einblick in SecureX Ideenaustausch - IBOSEC-2005

Josh Bordelon, Global Enterprise Security Architect, Cisco Systems, Inc.

In einer interaktiven Sitzung, in der wir den Aufbau und die Verbindung verschiedener Services besprechen, können Sie SecureX mit Cisco Security-Lösungen und Tools von Drittanbietern nutzen und Ideen austauschen. Bringen Sie Ihre Ideen und Fragen mit, oder lernen Sie von anderen, die bereits den Weg zu SecureX eingeschlagen haben.

Sitzungstyp: Interaktives Breakout

Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Praktische Übungen

Cisco Secure Client und SecureX Device Insights - besser miteinander - LABSEC-2776

Paul Carco, ENGINEER.TECHNICAL MARKETING, Cisco Systems, Inc.
Serhi Kucherenko, Customer Escalations Engineer, Cisco Systems, Inc.

Der Cisco Secure Client ist ein neuer Unified Client, der die meisten Cisco Endgeräte-Clients unter einem Dach vereint. Cisco Secure Client umfasst standardmäßige AnyConnect-Module und -Sicherheitsclients wie AMP (auch bekannt als Cisco Secure Endpoint) und Orbital. In dieser Übung lernen Sie, wie Sie einen Cisco Secure Client über die SecureX Cloud bereitstellen und verwalten. Der Teil zu den Einblicken von SecureX Devices zeigt, wie der Cisco Secure Client und seine Module für das Ressourcenmanagement auf Unternehmensebene und die Untersuchung von Sicherheitsvorfällen eingesetzt werden können.

Sitzungstyp: Walk-in Lab
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Technische Seminare

Cisco Secure Client: von AnyConnect zu umfassender Client-Sicherheit! - TECSEC-2780

Hacke Nohre, Technical Solutions Architect, Cisco - Distinguished Speaker
Thorsten Schranz, Technical Marketing Engineer, Cisco Systems, Inc. - Distinguished Speaker
Valeria Scribanti, Technical Solutions Specialist, Cisco Systems, Inc. - Distinguished Speaker

Die neue Hybrid-Belegschaft, komplexe Angriffsszenarien, die schnelle Cloud-Einführung und die Verbreitung der Verschlüsselung im Internet haben die Client-Sicherheit wichtiger denn je gemacht!
In dieser 4-stündigen Session zeigen wir Ihnen, wie Sie AnyConnect (VPN) um Endpoint Security mit vollem Funktionsumfang erweitern können. Wir werden die technischen Aspekte der Cisco Secure Client-Module genauer untersuchen. Dazu gehören:
EDR/EPP (Secure Endpoint)
Netzwerktelemetrie für Endgeräte (Network Visibility Module)
DNS-/Webschutz (Umbrella)
Endgerätestatus (ISE/sichere Firewall)
und die Ergebnisse der Ausführung eines einzelnen Clients, der zentral in Cisco SecureX (XDR) verwaltet wird.
Die Zielgruppe sind Netzwerk- und Sicherheitstechniker sowie Architekten mit Interesse an Endpunktsicherheit. Es wird von einem gewissen Verständnis der Endpunktsicherheit, der Betriebssysteme und der gängigen Angriffsvektoren ausgegangen.

Qualifiziert für Cisco Continuing Education Credit: Ja
Art der Schulung: Technisches Seminar
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

Erweiterte Erkennung und Reaktion mit Cisco Secure - TECSEC-2004

Matthew Robertson, Distinguished Technical Marketing Engineer, Cisco Systems, Inc. - Distinguished Speaker

Hanna Jabbour, Leader Technical Marketing Engineer, Cisco Systems, Inc. - Distinguished Speaker

Adi Sankar, Technical Marketing Engineer, Cisco Systems, Inc.

Matt Vander Horst, Technical Leader, Cisco - Distinguished Speaker

Diese Sitzung beginnt mit ausführlichen Informationen zum Angebot Extended Detection and Response von Cisco und bietet eine umfassende Anleitung zur Implementierung und zum Betrieb der verschiedenen Produktkomponenten, einschließlich Cisco Secure Endpoint, Secure Cloud Analytics, Umbrella, Meraki und Email Threat Defense sowie deren Betrieb in Cisco XDR. Ebenfalls enthalten sind betriebliche Best Practices und Implementierungsdetails für den Betrieb der Response Engine sowie die Integration von Cisco XDR mit Produkten anderer Anbieter wie Crowdstreik Falcon.

Qualifiziert für Cisco Continuing Education Credit: Ja
Art der Schulung: Technisches Seminar
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Kategorie: Sicherheit

DevNet

Sicherheitsautomatisierung: Entwicklung mit SecureX - DEVNET-1083

Matt Vander Horst, Technical Leader, Cisco - Distinguished Speaker

Wussten Sie, dass die XDR-Plattform von Cisco mehrere Möglichkeiten zur Automatisierung Ihrer Sicherheitsabläufe und zum Aufbau leistungsstarker Integrationen bietet? SecureX-Integrationsmodule ermöglichen es Ihnen, Daten von anderen Plattformen in Ihre Untersuchungen einzubeziehen, SecureX Threat Response-APIs ermöglichen Ihnen, die Untersuchung von und die Reaktion auf Bedrohungen zu automatisieren, und SecureX-Orchestrierung ermöglicht Ihnen die Erstellung leistungsstarker Workflows mit einem Editor, der Code-Drag-and-Drop nicht zu niedrig definiert. Erfahren Sie in dieser Sitzung mehr über die drei Aspekte von SecureX und wie Sie diese nutzen können, um Ihre Sicherheitsmaßnahmen zu optimieren.

Sitzungstyp: DevNet
Technische Ebene: Einführung
Technologie: SecureX, Sicherheit

Nachverfolgung: DevNet

Automatisierung von Cyber-Hygienebetrieben mit SecureX und Kenna Security - DEVLIT-1355

Oxana Sannikova, Technical Solutions Architect, Cisco Systems, Inc.

Die IT-Abläufe sind auch heute noch sehr manuell. Kunden stehen immer vor der Herausforderung, den Systemzustand aufrechtzuerhalten und die Online-Sicherheit zu verbessern. In dieser kurzen Session zeigen wir Ihnen, wie Sie die Cisco SecureX-Orchestrierung und Kenna Security nutzen können, um das

Management von Sicherheitslücken zu automatisieren.

Sitzungstyp: DevNet
Technische Ebene: Erweiterte Grundlagen
Technologie: Automatisierung und Orchestrierung, Sicherheit
Nachverfolgung: DevNet

Verwenden der SecureX-Orchestrierung zur Automatisierung der Reaktion auf Vorfälle in der Public Cloud - DEVWKS-2240

Brian Sak, Technical Solutions Architect, Cisco Systems, Inc. - Distinguished Speaker

Wenn Workloads zu Public Cloud-Anbietern wie AWS, Azure oder GCP migriert werden, kann die Reaktion auf und Behebung von Vorfällen schwieriger werden und erfordert andere Tools. Diese Sitzung führt Sie durch die Erstellung von SecureX-Orchestrierungs-Workflows, die den Prozess der Bedrohungsidentifizierung automatisieren und vereinfachen, Reaktionsverfahren vereinfachen und sicherstellen, dass Seekops Teams beim Sichern von Ressourcen in Multi-Cloud- oder Hybrid-Cloud-Umgebungen sorgenfrei sind.
Neu in diesem Jahr DevNet Workshop Sitzplätze sind vorab registrierte Teilnehmer sitzen zuerst. Für diese Sitzung sind nur 12 Laptops verfügbar. Dies ist ein praktischer DevNet-Workshop, in dem Sie gemeinsam mit einem Kursleiter programmieren. Bringen Sie Ihren eigenen 3,5-mm-Kopfhörer mit Aux-Anschluss an, um den Moderator zu hören, oder nehmen Sie ein Paar Kopfhörer im DevNet Command Center mit. Durch die Teilnahme an diesem DevNet Workshop erhalten Sie Cisco Continuing Education (CE)-Gutschriften. Weitere Informationen finden Sie unter: https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: DevNet
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Nachverfolgung: DevNet

Skalierung von Hybrid Cloud-Workflows mit SecureX Orchestrator und Remote Connector - DEVNET-2109

Steve McNutt, Technical Solutions Architect, Cisco Systems, Inc.

Möglicherweise haben Sie bereits von SecureX Orchestration (SXO) im Zusammenhang mit der Sicherheitsorchestrierung gehört. Wir zeigen Ihnen, wie Sie mit dieser Lösung noch viel mehr erreichen und eine Grundlage für die Entwicklung effektiver Hybrid Cloud-Tools schaffen können. Diese Sitzung beginnt mit einem allgemeinen Überblick über die Architektur, gefolgt von einer Begehung der Beispiellösung für die Massenbereitstellung von Cisco Umbrella, in der erläutert wird, wie die Komponenten zusammenpassen und welche Herausforderungen sie lösen. Sie verlassen diese Sitzung mit einem Verständnis, wie man hochgradig skalierbare Hybrid Cloud-Workflows durch die Nutzung der Sidecar-Muster und Vertrautheit mit Beispiel-Code, die Sie ändern können, um Ihre eigenen Lösungen zu erstellen.

Sitzungstyp: DevNet
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Nachverfolgung: DevNet

Doppelt R zählen in XDR: So automatisieren Sie Ihre Sicherheitsabläufe (SecOps) innerhalb von 10 Klicks in Cisco SecureX (ohne jeden Code zu schreiben) - DEVNET-

2214

Christopher Van Der Made, Engineering Product Manager, Cisco Systems, Inc. - Distinguished Speaker

In dieser Sitzung wird gezeigt, wie die Leistungsfähigkeit der Automatisierung über SecureX Orchestration genutzt werden kann, ohne dass Code geschrieben werden muss. Damit können Organisationen die R-Anzahl im Cisco XDR verdoppeln (eXtended Detection and Response). Wir werden einige extrem einfach zu installierende Beispiele durchgehen, die Sie auf dem Boden laufen lassen. Wir verwenden die Anzahl der Klicks, die in der Konsole als Metrik benötigt werden, um Ihnen zu zeigen, wie Sie ohne großen Aufwand Zugang zu leistungsstarker Automatisierung erhalten können. Am Ende erfahren Sie auch, wie Sie diesen Schritt weiter gehen und langsam zum Meister bei der Automatisierung Ihrer Sicherheitsabläufe werden. Sie erhalten anschließend alle Materialien, um selbst damit zu beginnen. Diese Schulung richtet sich an Einsatzkräfte, Sicherheitsanalysten, SOC-Manager oder andere Personen, die sich für Automatisierung und Sicherheit interessieren.

Sitzungstyp: DevNet
Technische Ebene: Erweiterte Grundlagen
Technologie: SecureX, Sicherheit
Nachverfolgung: DevNet

Integration mit Microsoft Graph API: Verwenden von Python und SecureX - DEVWKS-3260

Hacke Nohre, Technical Solutions Architect, Cisco - Distinguished Speaker

In diesem Workshop wird erläutert, wie die Microsoft Graph API in typische Cisco Umgebungen integriert werden kann.
Wir werden einen allgemeinen Überblick über die Microsoft Graph-API geben, wobei der Schwerpunkt auf der Oauth2-Authentifizierung und -Autorisierung für Azure AD liegt.
Anschließend zeigen wir, wie wir über Python-Skripts und SecureX auf diese API zugreifen können, um auf Informationen zu den Azure AD-Gruppen und -Rollen für einen bestimmten Benutzer zuzugreifen.
Zugriff auf Informationen über Sicherheitsereignisse aus der Microsoft-Umgebung
Die Teilnehmer können während des Workshops versuchen, die Schritte im Workshop aus der Laborumgebung heraus zu verfolgen, oder sie können die Schritte später durchführen. Wir stellen Zeiger für Übungseinrichtungen bereit, mit denen die Teilnehmer die Workshop-Aufgaben selbstständig durchführen können, ohne ihr eigenes Azure- oder SecureX-Konto zu benötigen.

Qualifiziert für Cisco Continuing Education Credit: Ja
Sitzungstyp: DevNet
Technische Stufe: Erweitert
Technologie: DevNet, Sicherheit
Nachverfolgung: DevNet

Automatisieren und vereinfachen Sie Ihren Ransomware-Schutz mit SecureX - DEVNET-1456

Elia Maracani, System Engineer, Cisco Systems, Inc.

Ransomware-Angriffe konzentrieren sich zunehmend auf Backups. Der Schutz sowie die schnelle und einfache Wiederherstellung der Sicherung Ihres Unternehmens wird somit zum besten und wichtigsten Schritt bei der Abwehr von lähmenden Ransomware-Angriffen. In einer Demo zeigen wir die Vielseitigkeit und Anpassungsmöglichkeiten auf, die SecureX über seine Orchestrierungs-Engine bietet. Dank der

Integration von Cisco SecureX in Lösungen von Drittanbietern (Cisco Umbrella, Cisco Secure Endpoint) und anderen Anbietern (Cohesity Helios) können Sie den Zeitaufwand und die Komplexität bei der Erkennung, Untersuchung und Wiederherstellung von Ransomware erheblich reduzieren.

Sitzungstyp: DevNet
Technische Ebene: Einführung
Technologie: SecureX, Sicherheit
Nachverfolgung: DevNet

Produkt- oder Strategieübersicht

Cisco XDR: Gebäude für das Security Operations Center der Zukunft - PSOSEC-1007

Sana Sana Yousuf, Product Marketing Manager, Cisco Systems, Inc.

Sicherheitsteams sehen sich einer wachsenden Bedrohungslandschaft gegenüber und sehen sich komplexen Umgebungen gegenüber, in denen die Effektivität der Absicherung zunehmend an Bedeutung verliert. Die Armutsgrenze im Bereich der Cybersicherheit weitet sich aus, und böswillige Akteure nutzen dieses klaffende Loch, um dauerhafte Angriffe zu entfesseln. Wir glauben, dass nur eine effektive Lösung für erweiterte Erkennung und Reaktion komplexe Angreifer wie Turla, Wannacry und NotPetya in Ihrer Umgebung erkennen und beseitigen kann. Erfahren Sie mehr über den disruptiven Nutzen von XDR im hybriden, anbieterübergreifenden Multivektor-Universum. Hier können Sie sich für ein kontinuierlich wachsendes Ökosystem aus Technologien verschiedener Anbieter als Grundlage für zukünftige Sicherheitsmaßnahmen stark machen. Und wie kann XDR ein Kraftmultiplikator für Ihre SOC werden?

Sitzungstyp: Produkt- oder Strategieübersicht
Technische Stufe: Allgemein
Technologie: SecureX, Hybrid Cloud, Sicherheit
Kategorie: Sicherheit

Wie Sie Ihre Sicherheit proaktiv erhöhen - PSOCX-2000

Varun Dhingra, Sr.Director, Product Management Security & Collaboration, Cisco Systems, Inc.
Mark Hammond, Director Product Management, Cisco Systems, Inc

Sie müssen nicht nur die Cybersicherheit in den Griff bekommen, sondern stehen auch unter dem Druck, gesetzliche Bestimmungen einzuführen, die auf Datenschutz basieren. Wie gestalten Sie ein Cybersicherheitsprogramm, das den sich ständig ändernden Anforderungen hinsichtlich Risiko, Regulierung, Geschäftszielen und betrieblichen Auswirkungen gerecht wird? In dieser Session erfahren Sie, wie Sie ein branchenspezifisches Framework für Datensicherheit und Datenschutz entwickeln, um die Anforderungen von Interessengruppen zu erfüllen und Lösungen zu entwickeln, die geschäftliche Flexibilität ermöglichen. Das Framework ist darauf ausgelegt, gewünschte Aktivitäten und Ergebnisse im Bereich Cybersicherheit nachzuverfolgen, die intuitiv sind und eine einfache, nicht-technische Kommunikation zwischen fachübergreifenden Teams ermöglichen.

Sitzungstyp: Produkt- oder Strategieübersicht
Technische Ebene: Erweiterte Grundlagen
Technologie: Kundenerlebnis, SecureX, Sicherheit

Zusätzliche Möglichkeiten

Neben den vielen oben genannten Session-Typen hat Live! eine Menge Innovation und Inspiration direkt auf der Konferenzetage. Lernen Sie die Techniker kennen, erfassen Sie die Flagge, oder nehmen Sie an der

Challenge teil. Live! zeigt Ihnen weiterhin, wie Cisco die Brücke zum Möglichen baut. Den vollständigen Katalog und weitere Informationen finden Sie unter Ciscolive.com.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.