Cisco live! Secure Endpoint en SecureX-sessies

Inhoud

Inleiding

Cisco live! Las Vegas is een van de belangrijkste industrie evenementen met meer dan 1100 sessies momenteel gepland 4-8 juni in het Mandalay Bay Convention Center. Met zo'n grote cursuscatalogus wilden we ervoor zorgen dat onze Secure Endpoint-klanten zich bewust waren van de onderwijsmogelijkheden om onze producten en diensten effectief te gebruiken. We benadrukken slechts een kleine selectie van de 129 beschikbare Labs, Breakout Sessions en Besprekingen rond het onderwerp Security beschikbaar dit jaar in Las Vegas, hopen dat u zult overwegen om zich bij ons aan te sluiten als we helpen om de wereld veiliger te maken.

Labs onder leiding van een instructeur

Cisco Secure Endpoint: naar rechts gaan door naar links te schuiven - LTRSEC-1114

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

Endpoint Security is de laatste verdedigingsmuur in het zich ontwikkelende landschap voor cybercriminaliteit en Cisco Secure Endpoint kan uw organisatie veilig houden als deze correct is geconfigureerd. In deze sessie hebt u praktische toegang tot de Secure Endpoint Console terwijl u implementatieconfiguraties en -praktijken leert voor de beste beveiligingspositie van een Engineering Team dat al meer dan tien jaar met Secure Endpoint (FKA AMP) heeft gewerkt. Je leert de mogelijkheden en functionaliteit van elke motor en welke omgevingen ze optimaal kunnen worden gebruikt. U weet hoe u waarschuwingen en automatiseringen kunt instellen om een aanval in uitvoering te beperken, zodat uw organisatie niet de volgende grote breuk hoeft te zijn.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: Instructor-led Lab
Technisch niveau: Inleiding
Technologie: beveiliging
Track: beveiliging

De evolutie van e-mailbeveiliging van beveiligde e-mailgateways naar API-gebaseerde platforms - LTRSEC-2011

Een e-mail diepe duik die integratie van SecureX behandelt om het meeste uit uw plaatsing van XDR te krijgen.

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

Deze laboratoriumsessie geeft een overzicht van de nieuwste functies van het Cisco Secure Email portfolio. De sessie zal zich richten op best practices om deelnemers in staat te stellen om het meeste uit hun e-mailplatform te halen. Onderwerpen voor gateway zijn onder meer het gebruik van SecureX Cisco Threat Response Private Intelligence, configuratie van op domeinen gebaseerde berichtenverificatie, rapportage en conformiteit (DMARC), geavanceerde vastlegging, API-gebruik en meer. Deelnemers zullen ook leren om de gateway te integreren in de nieuwere cloud met Cisco Secure Email Threat Defence. Het lab zal de software als een service bieden om te zoeken naar bedreigingen zoals zakelijke e-mail compromis dat traditionele indicatoren van het ontbreken van compromissen en onderzoek mogelijk gecompromitteerde accounts.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: Instructor-led Lab
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Secure Firewall - Problemen oplossen bij Threat Defense Data-Path (een praktisch handenlab) - LTRSEC-3880

John Groetzinger, technisch leider, Cisco Systems, Inc
Foster Lipkey, hoofdingenieur, Cisco Systems, Inc. - vooraanstaande luidspreker
Vidhi Mujumdar, leider, levering aan klanten, Cisco Systems

Een veel voorkomende zorg voor gebruikers van de Cisco Firepower-oplossing is wat ze moeten doen in het geval van een netwerkonderbreking of -degradatie die lijkt te zijn gerelateerd aan de Firepower-oplossing. In dit laboratorium zullen deelnemers methoden voor probleemoplossing leren voor het evalueren van datapad problemen binnen het Firepower platform, waaronder Firepower Series 3 NGIP's, ASA met Firepower Services, Firepower Threat Defence (FTD) en FXOS. Deze sessie biedt de deelnemers een kader om vast te stellen welk deel van de Firepower diensten bijdraagt aan het probleem en hoe de vastgestelde problemen snel kunnen worden opgelost. Dit framework zal de gehele datapad beslaan, vanaf het moment van pakkettoegang tot de deep packet inspection, inclusief de snortregel en preprocessorprestaties. Dit laboratorium zal zowel Snort 2.9 als Snort 3 en de verschillen tussen hen behandelen. Dit laboratorium zal probleemoplossing scenario's met behulp van Virtual Firepower Threat Defence (vFTD) bevatten om het probleemoplossing framework te implementeren. Bovendien zal dit lab kort de Secure Firewall-integratie van SecureX aanraken.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: Instructor-led Lab
Technisch niveau: geavanceerde
Technologie: beveiliging
Track: beveiliging

Workshop over cyberveerkracht - LTRSEC-1113

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

Is uw team voorbereid op de volgende aanval in de toeleveringsketen of de volgende nuldag? Reality check! We worden allemaal aangevallen, elke dag en uiteindelijk zullen we allemaal gecompromitteerd worden! Daarom moet uw organisatie Cyber Resilient zijn. Cyberveerkracht verwijst naar het vermogen van een organisatie om snel te herkennen, te reageren en te herstellen van een IT-beveiligingsincident. Het opbouwen van cyberveerkracht omvat het maken van een risicogericht plan dat ervan uitgaat dat het bedrijf op een bepaald moment te maken zal krijgen met een breuk of een aanval. In dit lab, zult u cyber security aanvallen ervaren in een enterprise lab omgeving waar u aanvaller en verdediger spelen en leren, uit de eerste hand, waarom u zeer geïntegreerde security oplossingen en CyberOps vaardigheden nodig hebt om Cyber Resilient te zijn.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: Instructor-led Lab
Technisch niveau: Inleiding
Technologie: SecureX, Beveiliging
Track: beveiliging

Uitbraken

Problemen met probleemoplossing en isolatie van prestaties als gevolg van beveiligde endpoints (Windows, Linux en MAC) - BRKSEC-2072

Vibhor Amrodia, technisch leider, Cisco Systems, Inc

U verlaat deze sessie met ideeën om u te helpen snel en effectief prestatiekwesties te isoleren met Secure Endpoints geïnstalleerd. Dit is een diepgaande sessie over hoe we prestatiekwesties op uw endpoints (Windows, Linux en MAC) kunnen analyseren en isoleren met behulp van enkele van de logbestanden die beschikbaar zijn met Secure Endpoint en ook door gebruik te maken van enkele van de OS-specifieke hulpprogramma's en tools. De focusgebieden voor deze sessie zijn: Windows CPU en RAM Utilisation Detectie en Isolation Linux CPU en RAM Utilisation Detectie en Isolation MAC CPU en RAM Utilisation Detectie en Isolation

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: beveiliging
Track: beveiliging

Cisco Unified Agent: Cisco Secure-client. AMP, AnyConnect, orbitaal en paraplu samenbrengen - BRKSEC-2834

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

We hebben allemaal de klachten gehoord of de klachten zelf gedaan: "Cisco heeft te veel agents".

Kom te weten van Aaron Woland, CCIE #20113 en Cisco Live Distinguished Speaker Hall of Fame Elite; hij toont je dat Cisco naar de klachten heeft geluisterd en de eerste herhaling van een Unified security agent heeft geleverd: Cisco Secure Client.

Cisco Secure Client (CSC) biedt een modulair kader waarmee AnyConnect VPN, Cisco Secure Endpoint (voorheen AMP voor endpoints), Network Visibility Module, Umbrella Cloud Security, ISE Posture, Secure Firewall Posture (voorheen Hostscan) en Network Access Module (NAM) allemaal samen kunnen bestaan; met een modern cloudgebaseerd beheer dat afkomstig is van SecureX - nauw verbonden met SecureX-apparaatinzichten.

In deze sessie gaan we in op de technologie achter de Secure Client, hoe dingen echt werken en hoe ze niet werken. We zullen implementatiemodellen vanuit de cloud en met behulp van uw eigen software-implementatiemechanismen behandelen. We zullen alle informatie over de naadloze upgradestromen van bestaande AnyConnect- en Secure Endpoint-agents (AMP) leren. We zullen het hebben over scenario's waarin het zinvol is om te upgraden naar CSC en scenario's waar het echt voordelig voor u is om te blijven met de bestaande AnyConnect en Secure Endpoint (AMP) agents - op zijn minst voor nu.

Kom wat tijd doorbrengen met Aaron & worden vermaakt terwijl u alles leert over deze spannende ontwikkeling van Cisco Security.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Van schip tot kust: integraties, samenwerking en (veilig) controle over de beveiligde e-mailgateway van Cisco - BRKSEC-2288

Robert Sherwin, technisch leider, Cisco Systems, Inc. - eminent spreker

Cisco Secure Email integreert buiten zijn eigen e-mailgateway. Beveiliging, vastlegging, API & configuratie en SecureX - we zullen u laten zien hoe e-mail zich uitstrekt tot buiten de gateway en u het beste uit uw omgeving haalt, groot of klein!

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Cisco's Malware Defense Cloud en Secure Malware Analytics-integraties - BRKSEC-2242

Bill Yazji, Technisch beveiligingsarchitect, Cisco Systems - Distinguished Speaker

U kunt het als "AMP Cloud and Threat Grid" gekend hebben, maar ze zijn omgedoopt in de Malware Defense Cloud en Secure Malware Analytics. Tijdens deze sessie wordt uitgebreid gekeken naar het aanbod van Malware Defense Cloud en Malware Analytics en worden hun integraties met Cisco-beveiligingsarchitecturen besproken, inclusief Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella en Meraki. Deze producten werken samen, en we zullen de Malware Defence Architecture behandelen en demonstreren hoe alle stukken bij elkaar passen om de industrie te verstrekken die de Geavanceerde Architectuur van de Bedreiging leidt. Deze sessie is perfect voor klanten die nieuwer zijn dan de Cisco Security Suite, en voor klanten die een of meer producten bezitten en dieper willen gaan in de manier waarop ze samenwerken.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Cisco XDR met firewall - BRKSEC-2090

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

SecureX, Cisco's XDR, is het breedste geïntegreerde platform ter wereld. In deze sessie zullen deelnemers de kracht van Firewall en SecureX integratie zien. Dit omvat firewallincidenten in SecureX, firewallverrijking aan onderzoeken van de bedreigingsreactie, en orkestratie SecureX die Firewall API's gebruiken. Deelnemers moeten beschikken over een basiskennis van Cisco Secure Firewall. Deelnemers vereisen geen kennis van SecureX.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging

Track: beveiliging

Versnel uw SOC met Cisco SecureX - BRKSEC-1023

Matt Vander Horst, Technisch Leider, Cisco - Distinguished Speaker

Wist u dat het XDR-platform SecureX van Cisco kan versnellen hoe uw organisatie incidenten onderzoekt en erop reageert? SecureX combineert een reeks functies die u in staat stellen om beveiligingsincidenten op te lossen, een betere zichtbaarheid te verkrijgen over een brede portfolio van producten en automatisering te gebruiken om te onderzoeken en te reageren op machinesnelheid. In deze sessie krijgt u een inleiding tot SecureX en leert u de basis van de verschillende functies, waaronder: het SecureX-dashboard, bedreigingsrespons, incidentmanager, orkestratie, apparaatinzichten en beveiligde client. We delen ook een lijst met andere sessies die u kunt bijwonen voor dieper duiken in deze functies en meer.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Inleiding
Technologie: SecureX, Beveiliging
Track: beveiliging

Cisco XDR met e-mail: Bescherm, analyseer en evolueer het SMTP-gesprek - BRKSEC-2095

Robert Sherwin, technisch leider, Cisco Systems, Inc. - vooraanstaand spreker

E-mail staat bekend als de zwakste schakel in een bedrijfsnetwerk en in minder dan twee minuten biedt hackers en actoren een open deur die leidt tot een compromis of breuk. E-mail is een primaire vector voor malware-infectie, omdat het moeiteloos kwaadaardige payloads voor de gebruiker plaatst en is slechts één klik verwijderd van exploitatie. Behalve alleen het leveren van malware, zijn de aanvallers geavanceerder dan ooit in het ontwerpen en genereren van phishing links die lijken op de diensten die ze imiteren. Cisco Secure Email is aan het evolueren hoe uitgebreide detectie en respons zich richt op deze bedreigingen en uw SMTP-gesprekken veilig stelt.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Uitgebreide detectie met Cisco XDR: beveiligingsanalyses voor de hele onderneming - BRKSEC-2178

Matthew Robertson, eminent technisch marketing engineer, Cisco Systems, Inc. - eminent spreker

Extended Detection and Response (XDR) is vandaag de dag een populair modewoord. Bij deze sessie wordt het onderwerp gedemystificeerd en worden de uitgebreide detectie- en analysemogelijkheden van Cisco XDR onderzocht met specifieke aandacht voor het uitbreiden van uw detectiemogelijkheden en het versnellen van uw respons. Deze sessie bestrijkt meerdere detectietechnologieën, waaronder endpoint, netwerk analyse en firewall en onderzoekt hoe analyses deze detecties bij elkaar kunnen brengen en de XDR-doelstelling kunnen realiseren.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak

Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Cisco IT-beveiliging vanuit A-Z. Advanced Malware Protection to Zero Trust - BRKCOC-2620

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

Het onmogelijke doen: Cisco heeft de beveiliging vergroot en de ervaring verbeterd, in één beweging, door Zero Trust voor de werknemers te introduceren. Deze sessie zal duiken in de details van de beveiligde Zero Trust authenticatie stroom, hoe we profiteerden van het uitlijnen van de nieuwe stroom met een betere ervaring, en hoe we hebben ontwikkeld endpoint configuraties om Zero Trust te ondersteunen met behulp van Jamf Pro, InTune/SCCM, en Meraki Systems Manager.
Deze sessie gaat ook dieper in op de manier waarop Cisco IT Cisco Secure Endpoint implementeert en onderhoudt in zijn vloot van 200k+ apparaten.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: hybride werk, beveiliging
Track: Cisco op Cisco

Cisco SecureX XDR - De betekenis van alle onderdelen - BRKSEC-2113

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

XDR (Extended Detection and Response) is een van de heetste beveiligingstechnologieën op de markt en het wordt steeds populairder. Gezien de brede waaier van wat kan-zijn, zou-moeten, en in een XDR-oplossing wordt gedaan, is er natuurlijk veel ingewikkeldheid die tot verwarring kan leiden over hoe/wat achter de schermen gebeurt. Deze sessie zal licht werpen op de interne werking van de ongelooflijk capabele XDR-oplossing van Cisco, met Network Detection & Response, Endpoint Detection & Response, Email Threat Defence, Malware Analytics, Unified Security Agent; en hoe al deze onderdelen en onderdelen bij elkaar komen om de verwachte uitkomst van een XDR te produceren.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Leveraging Ciscoâ€™s XDR-oplossing met IT Service Management (ITSM) en SIEM Systems voor incidentonderzoek - BRKSEC-2122

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

In deze sessie zullen we laten zien hoe het XDR-platform (eXtended Detection and Response), SecureX, de beveiligingsbewerkingen kan verbeteren om een beter resultaat te leveren zonder extra complexiteit te creëren. We zullen de volgende gebruikscases bekijken: het inzetten van context van IT Service Management (ITSM) en SIEM in bedreigingsjacht, het toevoegen van geconsolideerde zichtbaarheid van bedreigingen voor ITSM-incidenten en SIEM-waarschuwingen, het formaliseren van incidentresponsprocedures door gebruik te maken van automatisering en orkestratie. Bijna de helft van de

sessie zullen demonstraties zijn. De oplossingen van ITSM en SIEM die hieronder vallen, zijn onder andere ServiceNow, Jira en Splunk, en deelnemers lopen weg met klaar om te gebruiken workflows.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: automatisering en orkestratie, beveiliging
Track: beveiliging

Integratie van opensourcegereek en Cisco XDR - BRKSEC-2075

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

XDR-oplossingen (Extended Detection and Response) bieden de mogelijkheid om organisaties te beschermen tegen gebeurtenissen in verband met cyberbeveiliging door sneller te detecteren en te reageren en risico's en blootstelling te verminderen. Een XDR moet integraties van derden bevatten om extra detectiemotoren te kunnen leveren. Deze sessie introduceert open source Zeek en biedt uitvoerbare details over hoe u kunt integreren in Cisco XDR om de resultaten van de klantbeveiliging te verbeteren.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

De kracht van GreySkull! Adversarial Emulation - BRKSEC-2180

Jason Maynard, Veld CTO Cybersecurity Canada, CSS

In deze sessie zullen we leren over wedijver op tegenstanders en hoe zowel rode als blauwe teams er voordeel uit kunnen halen. We leren over de tools die we tot onze beschikking hebben en bouwen vervolgens een operatie uit waarbij Caldera gebruikt wordt zonder preventieve mogelijkheden. Vervolgens zullen we de resultaten op tegenspraak bekijken, inclusief het bekijken van de resultaten op ons passief geïmplementeerde Cisco Security-portfolio. De verkregen kennis zorgt ervoor dat defensieve teams de mogelijkheid begrijpen om onze verdediging te vergroten. Vervolgens zetten we onze preventieve functies in op een groot aantal Cisco-beveiligingstechnologieën en voeren we de test opnieuw uit om de resultaten te bekijken. Begrijpen hoe tegenstanders hun slachtoffer benaderen en hoe verdedigers in staat zijn de verdediging op zich te nemen is een recept voor succes.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Een inleiding tot op risico gebaseerd kwetsbaarheidsbeheer - BRKSEC-1639

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

Risicogebaseerd kwetsbaarheidsbeheer (RBVM) omvat meer dan u waarschijnlijk denkt. In deze onderhoudende en informatieve talk, zullen we diep duiken in de fundamentele concepten en de theorieën van het kwantificeren van risico's onderstrepen en dan delen hoe praktische RBVM-programma's essentieel zijn om het moderne netwerk te beveiligen. We zullen vervolgens bespreken hoe Kenna RBVM aan een breed scala aan Cisco-producten en -producten brengt.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: uitbraak
Technisch niveau: Inleiding
Technologie: SecureX, Beveiliging
Track: beveiliging

Interactieve doorbraak

Leveraging SecureX met Cisco Talos-incidentrespons - IBOSEC-2011

Joe Schumacher, incidentcommandant, Cisco Systems, Inc.

De deelnemers zullen rechtstreeks van ons team van de Reactie van het Incident van Cisco Talos (Talos IR) op hoe te hefboomwerking SecureX leren om reactieinspanningen tijdens een veiligheidsincident te versnellen. Ze krijgen inzicht in hoe SecureX kan worden gebruikt, of ze nu werken met een extern incidentresponsbedrijf zoals Talos IR of een interne onderzoeksreactie uitvoeren. De sessie wordt opgebouwd rond een gefaseerd telefoongesprek in de Talos IR-hotline door een fictieve klant van de containerserver met meerdere Cisco-beveiligingsproducten. Het team van Talos IR zal zich inzetten om doelstellingen inzake respons vast te stellen en achtergrondinformatie te verzamelen alvorens over te gaan tot noodreactieactiviteiten, waaronder het gebruik van SecureX samen met andere beveiligingsproducten tot het incident is ingedamd.
Het doel van de bijeenkomst zal zijn om de deelnemer op de volgende gebieden te informeren:
SecureX inbouwen om observables voor de teams te verbinden om samen te werken en te werken tijdens het onderzoek
Integratie van SecureX met beveiligingsproducten voor een tijdige en effectieve respons

Sessietype: interactieve uitbraak
Technisch niveau: Inleiding
Technologie: SecureX, Beveiliging
Track: beveiliging

IBOSEC-2005 - IBOSEC-2005

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

Ontdek en uitwisselt ideeën over het gebruik van SecureX met Cisco Security en tools van derden in een interactieve sessie waar we de opbouw en verbinding van verschillende services bespreken. Breng uw ideeën en vragen mee of leer van anderen die hun SecureX-reis al zijn begonnen.

Sessietype: interactieve uitbraak
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

inlooplaboratoria

Cisco Secure Client en SecureX-apparaatinzichten - beter samen - LABSEC-2776

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

De Cisco Secure Client is een nieuwe Unified client die de meeste Cisco-endpointclients onder één paraplu

brengt. Cisco Secure Client bestaat uit standaard AnyConnect-modules en security clients zoals AMP (AKA Cisco Secure Endpoint) en Orbital. Als deel van dit LAB leert u hoe u Cisco Secure Client kunt implementeren en beheren vanuit de SecureX-cloud. Het gedeelte dat is gewijd aan SecureX-apparaatinzichten toont aan hoe Cisco Secure Client en de modules ervan kunnen worden gebruikt voor bedrijfsmiddelenbeheer en onderzoek van beveiligingsincidenten.

Sessietype: Walk-in Lab
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Technische seminars

Cisco Secure-client: van AnyConnect naar uitgebreide clientbeveiliging! - TECSEC-2780.

Hacke Nohre, Architect voor Technische Oplossingen, Cisco - Distinguished Speaker
Thorsten Schranz, Technical Marketing Engineer, Cisco Systems, Inc. - Distinguished Speaker
Valeria Scribanti, Specialist voor technische oplossingen, Cisco Systems, Inc. - Distinguished Speaker

De nieuwe hybride werknemers, complexe aanvalsscenario's, snelle cloudadoptie en de alomtegenwoordigheid van encryptie op het internet hebben cliëntbeveiliging belangrijker dan ooit gemaakt!

In deze sessie van 4 uur laten we zien hoe we AnyConnect (VPN) kunnen uitbreiden naar een volledig uitgeruste Endpoint Security. We zullen ons richten op de technische aspecten van Cisco Secure Client-modules, waaronder:
EDR/EPP (Secure Endpoint)
Endpoint Network Telemetry (netwerkzichtbaarheidsmodule)
DNS-/webbeveiliging (Umbrella)
Endpoint posture (ISE/Secure-firewall)
en de resultaten van het uitvoeren van één client die centraal wordt beheerd in Cisco SecureX (XDR).
De bedoelde doelgroep zijn Network and Security Engineers en Architects die geïnteresseerd zijn in endpointbeveiliging. Enige kennis van endpointbeveiliging, besturingssystemen en gemeenschappelijke aanvalsvectoren wordt verondersteld.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: technisch seminar
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

Uitgebreide detectie en respons met Cisco Secure - TECSEC-2004

Matthew Robertson, eminent technisch marketing engineer, Cisco Systems, Inc. - eminent spreker

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

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

Matt Vander Horst, Technisch Leider, Cisco - Distinguished Speaker

Beginnend met diepgaand duiken in Cisco's Extended Detection and Response-aanbod, biedt deze sessie een volledige analyse van de implementatie en werking van de verschillende productcomponenten, inclusief

Cisco Secure Endpoint, Secure Cloud Analytics, Umbrella, Meraki en Email Threat Defence en hun werking in Cisco XDR. Hieronder vallen ook operationele best practices en implementatiedetails in de werking van de responsmachine en de integratie van Cisco XDR met niet-Cisco-producten zoals CrowdStrike Falcon.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: technisch seminar
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: beveiliging

DevNet

Security Automation: ontwikkelen met SecureX - DEVNET-1083

Matt Vander Horst, Technisch Leider, Cisco - Distinguished Speaker

Wist u dat het XDR-platform van Cisco meerdere manieren heeft waarop u uw beveiligingsbewerkingen kunt automatiseren en krachtige integraties kunt bouwen? Met SecureX-integratiemodules kunt u gegevens van andere platforms in uw onderzoeken opnemen, met SecureX Threat Response API's kunt u automatiseren hoe u bedreigingen onderzoekt en erop reageert, en met SecureX-orkestratie kunt u krachtige workflows bouwen met een no-to-low-codelezer. Stop bij deze sessie om meer te weten te komen over elk van deze drie facetten van SecureX en hoe u deze kunt gebruiken om uw beveiligingsoperaties te overladen.

Sessietype: DevNet
Technisch niveau: Inleiding
Technologie: SecureX, Beveiliging

Track: DevNet

Automatisering van Cyber Hygiene Operations met SecureX en Kenna Security - DEVLIT-1355

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

De IT-werkzaamheden zijn nog steeds zeer handmatig. Klanten worden altijd uitgedaagd om hun systeemgezondheid te behouden en de online beveiliging te verbeteren. In deze snelle sessie tonen we aan hoe Cisco SecureX-orkestratie en Kenna Security kunnen worden gebruikt om kwetsbaarheidsbeheer te automatiseren.

Sessietype: DevNet
Technisch niveau: Intermediate
Technologie: automatisering en orkestratie, beveiliging
Track: DevNet

SecureX-orkestratie gebruiken voor automatisering van openbare cloudincidentrespons - DEVWKS-2240

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

Wanneer werkbelastingen worden verplaatst naar publieke cloudproviders zoals AWS, Azure of GCP, kunnen incidentrespons en herstel moeilijker worden en zullen verschillende tools nodig zijn. Deze sessie zal u begeleiden door het creëren van SecureX-orkestratieworkflows die het proces van identificatie van bedreigingen automatiseren en vereenvoudigen, reactieprocedures vereenvoudigen en secops teams

gemoedsrust geven bij het beveiligen van resources in multi-cloud of hybride-cloud omgevingen.
Nieuw dit jaar DevNet werkplaats zitplaatsen zijn vooraf geregistreerde deelnemers zitten eerst. Er zijn slechts 12 laptops beschikbaar voor deze sessie. Dit is een hands-on DevNet Workshop waar je samen met een instructeur programmeert. Breng uw eigen 3,5 mm aux-connector hoofdtelefoons mee om de presentator te horen of neem een koptelefoon op bij het DevNet Command Center.
Door deze DevNet Workshop bij te wonen, kom je in aanmerking om Cisco Continuing Education (CE) Credits te verdienen. Vind meer informatie op: https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: DevNet
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: DevNet

Hybride cloudworkflows schalen met SecureX Orchestrator en Remote Connector - DEVNET-2109

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

Mogelijk hebt u gehoord van SecureX Orchestration (SXO) in de context van security orchestration. We zullen je laten zien dat het veel meer kan doen en een basis kan zijn voor het creëren van effectieve hybride cloud-operatietools. Deze sessie begint met een overzicht van de architectuur op hoog niveau, gevolgd door een doorloop van de voorbeeldoplossing van het massaal implementeren van Cisco Umbrella, waarin wordt uitgelegd hoe de componenten in elkaar passen en welke uitdagingen ze oplossen. U verlaat deze sessie met een begrip van hoe u zeer schaalbare hybride cloud workflows kunt bouwen door gebruik te maken van het zijwaartse patroon, en vertrouwdheid met voorbeeldcode die u kunt wijzigen om uw eigen oplossingen te bouwen.

Sessietype: DevNet
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging
Track: DevNet

De R-telling verdubbelen in XDR: Hoe uw beveiligingsbewerkingen (SecOps) te automatiseren binnen 10 klikken in Cisco SecureX (zonder enige coderegel te schrijven) - DEVNET-2214

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

Deze sessie zal laten zien hoe de kracht van automatisering kan worden benut via SecureX Orchestration zonder enige code te schrijven. Hierdoor kunnen organisaties de R-telling in Cisco XDR (uitgebreide detectie en respons) verdubbelen. We zullen door een paar zeer eenvoudig te installeren voorbeelden die u de grond raken lopen. We gebruiken de hoeveelheid klikken die nodig zijn in de console als metriek, om u te bewijzen hoe u toegang tot krachtige automatisering zonder al te veel haasje kunt krijgen. Uiteindelijk leer je ook hoe je dit een stap verder kunt zetten en langzaam een meester wordt in de automatisering van je beveiligingsoperaties. Daarna krijgt u al het materiaal om zelf aan de slag te gaan. Deze sessie is bedoeld voor incidentresponders, beveiligingsanalisten, SOC-managers of iedereen die geïnteresseerd is in automatisering en beveiliging.

Sessietype: DevNet
Technisch niveau: Intermediate
Technologie: SecureX, Beveiliging

Track: DevNet

Integreren met Microsoft Graph API: Python en SecureX gebruiken - DEVWKS-3260

Hacke Nohre, Architect voor Technische Oplossingen, Cisco - Distinguished Speaker

In deze workshop bespreken we hoe de Microsoft Graph API kan worden geïntegreerd in typische Cisco-omgevingen.
We zullen een overzicht op hoog niveau van de Microsoft Graph API met enige focus op Oauth2-verificatie en autorisatie naar Azure AD.
Vervolgens tonen we hoe we toegang kunnen krijgen tot deze API via zowel python-scripts als SecureX om toegang te krijgen tot informatie over de Azure AD-groepen en -rollen voor een specifieke gebruiker toegang tot informatie over beveiligingsgebeurtenissen vanuit de Microsoft-omgeving
De deelnemers kunnen proberen om de stappen in de workshop te volgen vanuit de labomgevingen tijdens de workshop, of ze kunnen de stappen later voltooien. We zullen aanwijzingen geven voor lab-instellingen die deelnemers in staat stellen om de workshoptaken zelf te voltooien, zonder dat ze een eigen Azure- of SecureX-account nodig hebben.

Kwalificaties voor Cisco-tegoed voor voortgezet onderwijs: ja
Sessietype: DevNet
Technisch niveau: geavanceerde
Technologie: DevNet, Beveiliging
Track: DevNet

Automatiseer en vereenvoudig uw Ransomware Defence met SecureX - DEVNET-1456

Elia Maracani, System Engineer, Cisco Systems, Inc.

Ransomware-aanvallen richten zich steeds meer op back-ups. Bescherming, evenals snel en gemakkelijk herstellen van de back-up van uw bedrijf, wordt zo de beste en belangrijkste stap in de verdediging tegen slopende ransomware aanvallen. Met behulp van een demo, zullen we de veelzijdigheid en de aanpassing benadrukken die SecureX kan bieden via zijn orkestratie-engine. Dankzij de integratie die Cisco SecureX biedt met zowel 1e (Cisco Umbrella, Cisco Secure Endpoint) als 3e-partij oplossingen (Cohesity Helios), kunt u de tijd en complexiteit van ransomware detectie, onderzoek en herstel drastisch verminderen.

Sessietype: DevNet
Technisch niveau: Inleiding
Technologie: SecureX, Beveiliging
Track: DevNet

Productoverzicht of strategieoverzicht

Cisco XDR: gebouw voor het Security Operations Center van morgen - PSOSEC-1007

Sana Sana Yousuf, productmarketingmanager, Cisco Systems, Inc.

Beveiligingsteams worden geconfronteerd met een zich uitbreidend bedreigingslandschap en een complexe omgeving die security efficiëntie steeds moeilijker maakt. De armoedegrens voor cyberveiligheid wordt breder, en kwaadaardige actoren maken gebruik van dit gapende gat om aanhoudende aanvallen te ontketenen. Wij geloven dat alleen een effectieve 'Extended Detection and Response' oplossing geavanceerde tegenstanders zoals Turla, Wannacry en NotPetya in uw omgeving kan detecteren en herstellen. Leer meer over de ontwrichtende waarde van XDR in het hybride, multi-leverancier, multi-vector

universum. Luister naar mij pleiten voor een voortdurend groeiend ecosysteem van multi-leverancierstechnologie integraties als basis voor de beveiliging van de toekomst. En hoe XDR een krachtmultiplier kan worden voor je SOC?

Sessietype: Productoverzicht
Technisch niveau: Algemeen
Technologie: SecureX, hybride cloud, security
Track: beveiliging

Hoe u uw beveiligingsveerkracht proactief kunt versterken - PSOCX-2000

Varun Dhingra, sr.Director, beveiliging en samenwerking voor productbeheer, Cisco Systems, Inc.
Mark Hammond, Director productbeheer, Cisco Systems, Inc

Je moet niet alleen de cyberveiligheid beheren, maar je staat ook onder echte druk om regelgeving aan te nemen die is gebaseerd op dataprivacy. Hoe ontwerp je een cyberbeveiligingsprogramma dat voldoet aan de voortdurend veranderende eisen van risico, regelgeving, bedrijfsdoelstellingen en operationele impact? In deze sessie leert u hoe u een op de industrie afgestemd kader voor gegevensbeveiliging en privacy kunt ontwerpen om tegemoet te komen aan de behoeften van belanghebbenden en oplossingen te ontwikkelen die zakelijke flexibiliteit mogelijk maken. Het raamwerk is ontworpen om de gewenste activiteiten en resultaten op het gebied van cyberbeveiliging te volgen die intuïtief zijn om eenvoudige, niet-technische communicatie tussen multidisciplinaire teams mogelijk te maken.

Sessietype: Productoverzicht
Technisch niveau: Intermediate
Technologie: Customer Experience, SecureX, Security

Aanvullende kansen

Samen met de vele sessietypes hierboven vermeld, Live! heeft veel innovatie en inspiratie direct op de conferentievloer. Ontmoet de engineers, Capture the Flag, of neem de uitdaging, live! blijft demonstreren hoe Cisco de brug naar mogelijk is. Bekijk de volledige catalogus en meer details op Ciscolive.com.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.