Cisco Live! Sessioni Secure Endpoint e SecureX

Sommario

Introduzione

Cisco Live! Las Vegas è uno degli eventi più importanti del settore, con oltre 1100 sessioni attualmente in programma dal 4 all'8 giugno al Mandalay Bay Convention Center. Con un catalogo di corsi così ampio, volevamo essere sicuri che i nostri clienti Secure Endpoint fossero a conoscenza delle opportunità formative per utilizzare i nostri prodotti e servizi in modo efficace. Evidenziando solo una piccola selezione dei 129 laboratori disponibili, Breakout Sessions e Discussioni che riguardano il tema della sicurezza disponibile quest'anno a Las Vegas, speriamo che prenderete in considerazione di unirvi a noi come aiutiamo a rendere il mondo un luogo più sicuro.

Laboratori con istruttore

Cisco Secure Endpoint: spostamento a destra con il tasto sinistro - LTRSEC-1114

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

La sicurezza degli endpoint è l'ultimo muro di difesa nell'evoluzione del crimine informatico e, se configurato correttamente, Cisco Secure Endpoint può garantire la sicurezza dell'organizzazione. In questa sessione si avrà accesso pratico a Secure Endpoint Console e al tempo stesso si apprenderanno le configurazioni e le procedure di installazione per la migliore postura di sicurezza da parte di un team di tecnici che ha lavorato con Secure Endpoint (FKA AMP) per la maggior parte di un decennio. Verranno illustrate le funzionalità e le caratteristiche di ogni motore e gli ambienti in cui è possibile utilizzarli in modo ottimale. L'utente saprà come impostare avvisi e automazioni per ridurre un attacco in corso in modo che l'organizzazione non debba essere la prossima violazione importante.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: laboratorio con istruttore
Livello tecnico: Introduttivo
Tecnologia: sicurezza
Brano: Sicurezza

Copertura dell'evoluzione della sicurezza della posta elettronica dai gateway di posta elettronica sicuri alle piattaforme basate su API - LTRSEC-2011

Un approfondimento e-mail sull'integrazione di SecureX per ottenere il massimo dall'implementazione di XDR.

Alberto Torralba, Technical Solutions Architect.Sales, Cisco Systems, Inc.
Greg Barnes, tecnico marketing, Cisco Systems, Inc.

In questa sessione introduttiva verranno presentate le funzionalità più recenti del portafoglio di prodotti Cisco Secure Email. La sessione sarà incentrata sulle best practice per consentire ai partecipanti di ottenere il massimo dalla loro piattaforma e-mail. Gli argomenti relativi al gateway includono l'utilizzo dell'intelligence privata SecureX Cisco Threat Response, la configurazione di DMARC (Domain-based Message Authentication, Reporting & Conformance), la registrazione avanzata, l'utilizzo dell'API e altro ancora. I partecipanti apprenderanno inoltre a integrare il gateway nel nuovo cloud che offre Cisco Secure Email Threat Defense. Il laboratorio presenterà il software come un'offerta di servizio per la ricerca di minacce quali compromessi di posta elettronica aziendali che mancano dei tradizionali indicatori di compromissione e analizzerà gli account potenzialmente compromessi.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: laboratorio con istruttore
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Secure Firewall - Risoluzione dei problemi relativi ai percorsi di dati per la difesa dalle minacce (un pratico laboratorio) - LTRSEC-3880

John Groetzinger, Technical Leader, Cisco Systems, Inc
Foster Lipkey, Principal Engineer, Cisco Systems, Inc. - Diffusore
Vidhi Mujumdar, Leader, Customer Delivery, Cisco Systems

Un problema comune per gli utenti della soluzione Cisco Firepower è quello che devono fare in caso di interruzione o deterioramento della rete che sembra essere correlato alla soluzione Firepower. In questa esercitazione i partecipanti apprenderanno le metodologie di risoluzione dei problemi per la valutazione dei problemi dei percorsi dati all'interno della piattaforma Firepower, inclusi i NGIP Firepower serie 3, l'ASA con servizi Firepower, Firepower Threat Defense (FTD) e FXOS. Questa sessione fornirà ai partecipanti una struttura per identificare quale parte dei servizi Firepower sta contribuendo al problema e come attenuare rapidamente i problemi identificati. Questa struttura coprirà l'intero percorso dei dati, dall'ingresso dei pacchetti all'ispezione approfondita dei pacchetti, incluse le regole Snort e le prestazioni del preprocessore. Questa esercitazione illustrerà sia Snort 2.9 che Snort 3 e le differenze tra di essi. Questa esercitazione conterrà gli scenari di risoluzione dei problemi utilizzando Virtual Firepower Threat Defense (vFTD) per implementare il framework di risoluzione dei problemi. Inoltre, questa esercitazione tratterà brevemente dell'integrazione SecureX Secure Firewall.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: laboratorio con istruttore
Livello tecnico: avanzato
Tecnologia: sicurezza
Brano: Sicurezza

Workshop sulla resilienza informatica - LTRSEC-1113

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

Il team è preparato per il prossimo attacco alla catena di fornitura o per il giorno zero successivo? Controllo della realtà! Siamo tutti sotto attacco, ogni giorno, e alla fine saremo tutti compromessi! Per questo motivo, la vostra organizzazione deve essere Cyber Resilient. La sicurezza informatica si riferisce alla capacità di un'organizzazione di identificare, rispondere e ripristinare rapidamente un sistema in seguito a un problema di sicurezza IT. Per sviluppare la capacità di recupero informatico occorre elaborare un piano incentrato sui rischi che preveda che l'azienda dovrà prima o poi affrontare una violazione o un attacco. In questo laboratorio, si sperimenteranno attacchi alla sicurezza informatica in un ambiente di laboratorio aziendale in cui si gioca a attaccante e difensore e si imparerà, in prima persona, perché è necessario soluzioni di sicurezza altamente integrate e competenze CyberOps per essere Cyber Resilient.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: laboratorio con istruttore
Livello tecnico: Introduttivo
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Eventi

Risoluzione dei problemi e isolamento dei problemi di prestazioni dovuti agli endpoint sicuri (Windows, Linux e MAC) - BRKSEC-2072

Vibhor Amrodia, Technical Leader, Cisco Systems, Inc

In questa sessione verranno lasciate alcune idee per isolare in modo rapido ed efficace i problemi di prestazioni con gli endpoint sicuri installati. Questa è una sessione di approfondimento su come analizzare e isolare i problemi di prestazioni degli endpoint (Windows, Linux e MAC) utilizzando alcuni dei log disponibili con Secure Endpoint e alcuni strumenti e utilità specifici del sistema operativo. Le aree di interesse per questa sessione sono: Rilevamento dell'utilizzo della CPU e della RAM di Windows e Isolamento Rilevamento dell'utilizzo della CPU e della RAM di Linux e Isolamento dell'utilizzo della CPU e della RAM MAC Rilevamento e isolamento della CPU e della RAM

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout

Livello tecnico: Intermedio
Tecnologia: sicurezza
Brano: Sicurezza

Cisco Unified Agent: Cisco Secure Client. Unione di AMP, AnyConnect, Orbital e Umbrella - BRKSEC-2834

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

Abbiamo tutti sentito le lamentele o lo abbiamo fatto noi stessi: "Cisco ha troppi agenti".

Vieni a conoscere Aaron Woland, CCIE #2013 e Cisco Live Distinguished Speaker Hall of Fame Elite; mentre ti mostra che Cisco ha ascoltato le lamentele e ha consegnato la prima iterazione di un agente di sicurezza unificato: Cisco Secure Client.

Cisco Secure Client (CSC) offre una struttura modulare che permette a AnyConnect VPN, Cisco Secure Endpoint (in precedenza AMP for Endpoints), Network Visibility Module, Umbrella Cloud Security, ISE Posture, Secure Firewall Posture (in precedenza Hostscan) e Network Access Module (NAM) di coesistere; con una gestione moderna basata su cloud fornita da SecureX, e una connessione perfetta con le informazioni dettagliate sui dispositivi SecureX.

In questa sessione, esamineremo la tecnologia alla base di Secure Client, il funzionamento reale delle cose e come non funzionano. Verranno illustrati i modelli di installazione dal cloud e l'utilizzo dei propri meccanismi di installazione del software. Verranno fornite tutte le informazioni sui flussi di aggiornamento degli agenti AnyConnect e Secure Endpoint (AMP) esistenti. Parleremo di scenari dove ha senso effettuare l'aggiornamento a CSC e di scenari in cui vantaggi davvero mantenere gli agenti AnyConnect e Secure Endpoint (AMP) esistenti - almeno per il momento.

Vieni a trascorrere un po' di tempo con Aaron e divertiti a scoprire tutto questo fantastico sviluppo di Cisco Security.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Da nave a terra: integrazione, collaborazione e (in modo sicuro) controllo oltre Cisco Secure Email Gateway - BRKSEC-2288

Robert Sherwin, Technical Leader, Cisco Systems, Inc. - Relatore speciale

Cisco Secure Email si integra al di fuori di essere un proprio gateway di posta. Sicurezza, registrazione, API e configurazione e SecureX: vi guideremo attraverso il modo in cui l'e-mail si estende oltre il gateway e in cui è possibile sfruttare al massimo il vostro ambiente, grande o piccolo!

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Integrazioni di Cisco Malware Defense Cloud e Secure Malware Analytics - BRKSEC-2242

Bill Yazji, Technical Security Architect, Cisco Systems - Relatore distinto

È possibile che tu l'abbia conosciuta come "AMP Cloud and Threat Grid", ma sono stati rinominati come Malware Defense Cloud e Secure Malware Analytics. In questa sessione verranno analizzati e approfonditi i prodotti Malware Defense Cloud e Malware Analytics e ne verranno illustrate le integrazioni con le architetture di sicurezza Cisco, tra cui Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella e Meraki. Questi prodotti funzionano insieme e verrà illustrata l'architettura di difesa da malware e verrà dimostrato come tutti i componenti interagiscono per fornire l'architettura di minaccia avanzata leader del settore. Questa sessione è perfetta per coloro che sono più recenti rispetto a Cisco Security Suite, nonché per i clienti che possiedono uno o più prodotti e desiderano approfondire la loro collaborazione.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Cisco XDR con firewall - BRKSEC-2090

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

SecureX, XDR di Cisco, è la piattaforma più integrata al mondo. In questa sessione i partecipanti potranno vedere la potenza dell'integrazione di Firewall e SecureX. tra cui gli incidenti del firewall in SecureX, l'arricchimento del firewall per le indagini di risposta alle minacce e l'orchestrazione di SecureX tramite le API del firewall. I partecipanti devono avere una conoscenza di base di Cisco Secure Firewall. I partecipanti non devono conoscere SecureX.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Accelerate il vostro SOC con Cisco SecureX - BRKSEC-1023

Matt Vander Horst, Direttore tecnico, Cisco - Relatore speciale

Lo sapevate che la piattaforma Cisco XDR SecureX può accelerare il modo in cui la vostra organizzazione indaga e risponde agli incidenti? SecureX combina una suite di funzionalità che consentono di gestire gli incidenti relativi alla sicurezza, ottenere una migliore visibilità su un'ampia gamma di prodotti e utilizzare l'automazione per analizzare e rispondere alla velocità della macchina. In questa sessione verrà fornita un'introduzione a SecureX e verranno illustrate le caratteristiche di base delle varie funzionalità, tra cui il dashboard SecureX, la risposta alle minacce, la gestione degli incidenti, l'orchestrazione, le informazioni dettagliate sui dispositivi e il client sicuro. Verrà inoltre condiviso un elenco di altre sessioni a cui è possibile partecipare per approfondire queste e altre funzionalità.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Introduttivo
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Cisco XDR con e-mail: protezione, analisi ed evoluzione della conversazione SMTP - BRKSEC-2095

Robert Sherwin, Technical Leader, Cisco Systems, Inc. - Relatore speciale

L'e-mail è nota come il collegamento più debole in una rete aziendale e in meno di due minuti fornisce a hacker e attori una porta aperta che porta a un compromesso o a una violazione. La posta elettronica è un vettore primario per l'infezione da malware perché mette senza sforzo payload dannosi davanti all'utente ed è solo un clic lontano dallo sfruttamento. Oltre a distribuire malware, gli aggressori sono più sofisticati che mai nel creare e generare link di phishing che assomigliano proprio ai servizi che stanno impersonando. Cisco Secure Email sta sviluppando il modo in cui eXtended Detection and Response individua questi vettori di minaccia e protegge le conversazioni SMTP.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Extended Detection con Cisco XDR: analisi della sicurezza a livello aziendale - BRKSEC-2178

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

La funzionalità Extended Detection and Response (XDR) è una parola d'ordine molto diffusa al giorno d'oggi. Demistificando l'argomento, questa sessione esplorerà le funzionalità estese di rilevamento e analisi del Cisco XDR con un'attenzione specifica su come estendere le funzionalità di rilevamento e accelerare la risposta. In questa sessione verranno illustrate le funzionalità di più

tecnologie di rilevamento, inclusi endpoint, analisi di rete e firewall, che consentono all'analisi di riunire i rilevamenti e ottenere risultati per l'obiettivo XDR.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Cisco IT Security dalla A-Z. Protezione avanzata da malware a zero trust - BRKCOC-2620

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

Fare l'impossibile: Cisco ha aumentato la sicurezza e ha migliorato l'esperienza in un unico movimento, introducendo la fiducia zero per la forza lavoro. In questa sessione verranno approfonditi i dettagli del flusso di autenticazione sicuro Zero Trust, i vantaggi derivanti dall'allineamento del nuovo flusso con un'esperienza migliore e l'implementazione di configurazioni degli endpoint per supportare Zero Trust con Jamf Pro, InTune/SCCM e Meraki Systems Manager.
In questa sessione verrà approfondito anche il modo in cui Cisco IT implementa e gestisce Cisco Secure Endpoint nel suo parco di dispositivi con capacità superiore a 200.000 rpm.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: lavoro ibrido, sicurezza
Brano: Cisco su Cisco

Cisco SecureX XDR - Il senso di tutte le parti e i pezzi - BRKSEC-2113

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

La tecnologia XDR (eXtended Detection and Response) è una delle tecnologie di sicurezza più avanzate sul mercato e sta registrando una crescita notevole in termini di adozione. Data l'ampia gamma di ciò che può, dovrebbe e viene realizzato in una soluzione XDR, esiste naturalmente una grande complessità che può generare confusione su come/cosa sta accadendo dietro le quinte. Questa sessione chiarirà il funzionamento interno della soluzione XDR incredibilmente efficiente di Cisco, con Network Detection & Response, Endpoint Detection & Response, Email Threat Defense, Malware Analytics, Unified Security Agent; e il modo in cui tutte queste parti e pezzi si uniscono per produrre il risultato previsto di un XDR.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza

Brano: Sicurezza

Sfruttare la soluzione XDR di Cisco con IT Service Management (ITSM) e SIEM Systems for Incident Investigation - BRKSEC-2122

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

In questa sessione verrà illustrato in che modo la piattaforma eXtended Detection and Response (XDR), SecureX, può aumentare le operazioni di sicurezza per offrire risultati migliori senza creare ulteriore complessità. Verranno esaminati i seguenti casi di utilizzo: utilizzo del contesto di IT Service Management (ITSM) e SIEM nella ricerca di minacce, aggiunta di visibilità consolidata delle minacce agli incidenti ITSM e agli avvisi SIEM, formalizzazione delle procedure di risposta agli incidenti mediante automazione e orchestrazione. Quasi la metà della sessione sarà dedicata alle manifestazioni. Le soluzioni ITSM e SIEM illustrate includono ServiceNow, Jira e Splunk, mentre i partecipanti si allontanano con flussi di lavoro pronti all'uso.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: Automazione e orchestrazione, sicurezza
Brano: Sicurezza

Integrazione di Open Source Zeek e Cisco XDR - BRKSEC-2075

King Mark Stephens, architetto della sicurezza informatica globale, CISCO Richfield, Ohio

Le soluzioni XDR (Extended Detection and Response) offrono la possibilità di proteggere le organizzazioni da eventi di sicurezza informatica grazie alla possibilità di rilevare e rispondere più rapidamente e ridurre i rischi e l'esposizione. Un XDR deve includere integrazioni di terze parti per fornire motori di rilevamento aggiuntivi. Questa sessione introdurrà il software Zeek open source e fornirà dettagli pratici su come integrarlo in Cisco XDR per migliorare i risultati sulla sicurezza dei clienti.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Il potere di GreySkull! Emulazione avversa - BRKSEC-2180

Jason Maynard, CTO Field Cybersecurity Canada, CSS

In questa sessione impareremo a conoscere l'emulazione avversaria e come i team rosso e blu possono trarre beneficio da esso uso. Apprendiamo gli strumenti a nostra disposizione e quindi costruiamo un'operazione che sfrutta Caldera senza capacità preventive. Esamineremo quindi i risultati avversari, che includono la revisione dei risultati sul nostro portafoglio di prodotti Cisco

Security implementati passivamente. Le conoscenze acquisite assicurano che i team di difesa comprendano l'opportunità di aumentare le difese. Quindi, attiveremo le nostre capacità preventive su una varietà di tecnologie di sicurezza Cisco ed eseguiremo nuovamente il test rivedendo i risultati. Comprendere come l'avversario affronta la sua vittima e la capacità dei difensori di proteggere la difesa è una ricetta per il successo.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Introduzione alla gestione delle vulnerabilità basata sui rischi - BRKSEC-1639

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

La gestione delle vulnerabilità basata sui rischi (RBVM, Risk-Based Vulnerability Management) include molto di più di quanto si pensi. In questo discorso divertente e istruttivo, approfondiremo i concetti di base e le teorie di quantificazione del rischio e condivideremo l'importanza dei programmi RBVM per proteggere la rete moderna. In seguito parleremo di come Kenna apporti RBVM a una vasta gamma di prodotti e offerte Cisco.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: Breakout
Livello tecnico: Introduttivo
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Breakout interattivo

Sfruttamento di SecureX con Cisco Talos Incident Response - IBOSEC-2011

Joe Schumacher, Incident Commander, Cisco Systems, Inc.

I partecipanti apprenderanno direttamente dal team Cisco Talos Incident Response (Talos IR) come utilizzare SecureX per accelerare le operazioni di risposta in caso di problemi relativi alla sicurezza. Approfondiranno il modo in cui SecureX può essere utilizzato, sia collaborando con una società esterna di risposta agli incidenti, come Talos IR, sia conducendo una risposta investigativa interna. La sessione sarà costruita intorno a una telefonata di prova nella hotline IR di Talos da parte di un cliente fittizio con diversi prodotti di sicurezza Cisco. Il team di IR Talos si impegnerà a stabilire obiettivi di risposta e a ottenere informazioni generali prima di passare alle attività di risposta alle emergenze, che includeranno l'utilizzo di SecureX insieme ad altri prodotti di sicurezza fino a quando l'incidente non sarà stato contenuto.
L'obiettivo della sessione sarà quello di informare il partecipante nei seguenti settori:
Integrazione di SecureX per collegare gli osservatori affinché i team collaborino e lavorino durante l'indagine
Integrazione di SecureX con i prodotti per la sicurezza per coordinare una risposta tempestiva ed

efficace

Tipo di sessione: Interactive Breakout
Livello tecnico: Introduttivo
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Scambio di idee SecureX - IBOSEC-2005

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

Esplora e scambia idee sull'utilizzo di SecureX con Cisco Security e strumenti di terze parti in una sessione interattiva in cui discutiamo della creazione e della connessione di vari servizi. Porta le tue idee e domande o impara da altri che hanno già iniziato il loro viaggio SecureX.

Tipo di sessione: Interactive Breakout
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Esercitazioni pratiche

Cisco Secure Client e SecureX Device Insights - una combinazione ottimale - LABSEC-2776

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

Cisco Secure Client è un nuovo client unificato che riunisce la maggior parte dei client endpoint Cisco. Cisco Secure Client comprende moduli AnyConnect standard e client di sicurezza come AMP (alias Cisco Secure Endpoint) e Orbital. Come parte di questo laboratorio, imparerai come distribuire e gestire Cisco Secure Client dal cloud SecureX. La parte dedicata a SecureX Devices Insights dimostrerà come Cisco Secure Client e i suoi moduli possono essere utilizzati per la gestione delle risorse a livello enterprise e l'analisi degli incidenti relativi alla sicurezza.

Tipo di sessione: Walk-in Lab
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Seminari tecnici

Cisco Secure Client: da AnyConnect alla sicurezza completa dei client - TECSEC-2780

Hacke Nohre, Technical Solutions Architect, Cisco - Relatore

Thorsten Schranz, Technical Marketing Engineer, Cisco Systems, Inc. - Diffusore
Valeria Scribanti, Specialista in soluzioni tecniche, Cisco Systems, Inc. - Relatore distinto

La nuova forza lavoro ibrida, i complessi scenari di attacco, la rapida adozione del cloud e la diffusione della crittografia su Internet hanno reso la sicurezza dei client più importante che mai! In questa sessione di 4 ore verrà spiegato come espandere AnyConnect (VPN) in modo da ottenere la sicurezza degli endpoint completa di tutte le funzionalità. Esamineremo gli aspetti tecnici dei moduli Cisco Secure Client, tra cui:
EDR/EPP (Secure Endpoint)
Telemetria di rete dell'endpoint (Network Visibility Module)
Protezione DNS/Web (Umbrella)
Postura degli endpoint (ISE/Secure Firewall)
e sui risultati dell'esecuzione di un singolo client gestito centralmente in Cisco SecureX (XDR).
I destinatari sono i tecnici e gli architetti della rete e della sicurezza interessati alla sicurezza degli endpoint. Si presuppone una certa conoscenza della sicurezza degli endpoint, dei sistemi operativi e dei vettori di attacco comuni.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: seminario tecnico
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

Extended Detection and Response con Cisco Secure - TECSEC-2004

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

Hanna Jabbour, responsabile tecnico marketing, Cisco Systems, Inc. - Relatore

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

Matt Vander Horst, Direttore tecnico, Cisco - Relatore speciale

A partire da un approfondimento dell'offerta Extended Detection and Response di Cisco, questa sessione fornirà una panoramica completa dell'implementazione e del funzionamento dei diversi componenti del prodotto, tra cui Cisco Secure Endpoint, Secure Cloud Analytics, Umbrella, Meraki and Email Threat Defense e il loro funzionamento in Cisco XDR. Sono inoltre incluse best practice operative e dettagli sull'implementazione nel funzionamento del motore di risposta, nonché l'integrazione di Cisco XDR con prodotti di terze parti, ad esempio Crowdstrike Falcon.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: seminario tecnico
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: Sicurezza

DevNet

Automazione della sicurezza: sviluppo con SecureX - DEVNET-1083

Matt Vander Horst, Direttore tecnico, Cisco - Relatore speciale

Lo sapevate che la piattaforma Cisco XDR consente di automatizzare le operazioni di sicurezza e realizzare potenti integrazioni? I moduli di integrazione SecureX consentono di importare nelle ricerche dati provenienti da altre piattaforme, le API SecureX Threat Response consentono di automatizzare le ricerche e le risposte alle minacce e l'orchestrazione SecureX consente di creare flussi di lavoro potenti utilizzando un editor di trascinamento codice di livello minimo. Interrompere questa sessione per ulteriori informazioni su ognuno di questi tre aspetti di SecureX e su come utilizzarli per potenziare le operazioni di sicurezza.

Tipo di sessione: DevNet
Livello tecnico: Introduttivo
Tecnologia: SecureX, sicurezza

Brano: DevNet

Automazione delle operazioni di Cyber Hygiene con SecureX e Kenna Security - DEVLIT-1355

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

Oggi le operazioni IT sono ancora molto manuali. I clienti si trovano sempre a dover affrontare sfide che richiedono di preservare lo stato del sistema e di migliorare la sicurezza online. In questa rapida sessione verrà illustrato come utilizzare l'orchestrazione Cisco SecureX e Kenna Security per automatizzare la gestione delle vulnerabilità.

Tipo di sessione: DevNet
Livello tecnico: Intermedio
Tecnologia: Automazione e orchestrazione, sicurezza
Brano: DevNet

Utilizzo dell'orchestrazione SecureX per l'automazione della risposta a incidenti nel cloud pubblico - DEVWKS-2240

Brian Sak, Technical Solutions Architect, Cisco Systems, Inc. - Diffusore

Quando i carichi di lavoro vengono spostati nei provider di cloud pubblici come AWS, Azure o GCP, la risposta e il monitoraggio e l'aggiornamento degli incidenti possono diventare più difficili e richiederanno strumenti diversi. Questa sessione guiderà l'utente nella creazione di workflow di orchestrazione SecureX che automatizzano e semplificano il processo di identificazione delle minacce, semplificano le procedure di risposta e offrono ai team di settore la massima tranquillità nella protezione delle risorse in ambienti multi-cloud o hybrid-cloud.
Novità di quest'anno I partecipanti preregistrati al workshop DevNet saranno i primi a sedersi. Per questa sessione sono disponibili solo 12 notebook. Si tratta di un workshop pratico su DevNet in cui si programma con un istruttore. È possibile utilizzare le cuffie con connettore AUX da 3,5 mm

per ascoltare il presentatore o utilizzare un paio di cuffie nel centro di comando DevNet. Partecipando a questo workshop DevNet, potrai ottenere i crediti CE (Cisco Continuing Education). Ulteriori informazioni sono disponibili all'indirizzo: https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: DevNet
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: DevNet

Scalabilità dei flussi di lavoro Hybrid Cloud con SecureX Orchestrator e connettore remoto - DEVNET-2109

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

È possibile che si sia sentito parlare di SXO (SecureX Orchestration) nel contesto dell'orchestrazione della sicurezza. Vi dimostreremo che può fare molto di più e costituire una base per la creazione di strumenti operativi ibridi efficaci. Questa sessione inizia con una panoramica dell'architettura di alto livello seguita da una presentazione della soluzione di esempio dell'installazione di massa di Cisco Umbrella, in cui viene illustrato come i componenti si integrano e le sfide che risolvono. In questa sessione verranno fornite informazioni su come creare flussi di lavoro ibridi altamente scalabili sfruttando il modello sidecar e la familiarità con il codice di esempio che è possibile modificare per creare soluzioni personalizzate.

Tipo di sessione: DevNet
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: DevNet

Come raddoppiare il numero di R in XDR: come automatizzare le operazioni di sicurezza (SecOps) entro 10 clic in Cisco SecureX (senza scrivere alcuna riga di codice) - DEVNET-2214

Christopher Van Der Made, Engineering Product Manager, Cisco Systems, Inc. - Relatore speciale

In questa sessione verrà illustrato come sfruttare la potenza dell'automazione tramite l'orchestrazione SecureX senza scrivere alcun codice. Ciò consentirà alle organizzazioni di raddoppiare il numero di R in XDR (eXtended Detection and Response) di Cisco. Vi presenteremo un paio di esempi estremamente semplici da installare che vi faranno andare a fondo. La quantità di clic necessari nella console verrà utilizzata come metrica per dimostrare come sia possibile accedere a una potente automazione senza troppi problemi. Alla fine, imparerete anche come fare un passo avanti e diventare lentamente un maestro nell'automazione delle operazioni di sicurezza. In seguito riceverai tutto il materiale per iniziare da solo. Questa sessione è destinata a coloro che hanno risposto a un incidente, analisti di sicurezza, manager SOC o a chiunque abbia un

interesse per l'automazione e la sicurezza.

Tipo di sessione: DevNet
Livello tecnico: Intermedio
Tecnologia: SecureX, sicurezza
Brano: DevNet

Integrazione con l'API di Microsoft Graph: utilizzo di Python e SecureX - DEVWKS-3260

Hacke Nohre, Technical Solutions Architect, Cisco - Relatore

In questo workshop verrà illustrato come integrare l'API di Microsoft Graph in ambienti Cisco tipici. Verrà fornita una panoramica di alto livello dell'API di Microsoft Graph con particolare attenzione all'autenticazione e all'autorizzazione Oauth2 per Azure AD.
Verrà quindi illustrato come accedere a questa API tramite script Python e SecureX per accedere alle informazioni sui gruppi e i ruoli di Azure AD per un utente specifico
accedere alle informazioni sugli eventi di protezione dall'ambiente Microsoft
I partecipanti possono tentare di seguire i passaggi del workshop dagli ambienti di laboratorio durante il workshop oppure possono completare i passaggi in un secondo momento. Verranno forniti i puntatori alle impostazioni di laboratorio che consentono ai partecipanti di completare le attività del workshop autonomamente, senza la necessità di un account Azure o SecureX.

Qualifica per il credito Cisco per l'istruzione continua: Sì
Tipo di sessione: DevNet
Livello tecnico: avanzato
Tecnologia: DevNet, Sicurezza
Brano: DevNet

Automazione e semplificazione della difesa ransomware con SecureX - DEVNET-1456

Elia Maracani, System Engineer, Cisco Systems, Inc.

Gli attacchi ransomware sono sempre più concentrati sui backup. Proteggere, oltre a recuperare rapidamente e facilmente il backup della vostra azienda, sta diventando così il passo migliore e più importante nella difesa contro attacchi ransomware debilitanti. Con l'aiuto di una demo, metteremo in evidenza la versatilità e la personalizzazione che SecureX è in grado di fornire tramite il suo motore di orchestrazione. Grazie all'integrazione fornita da Cisco SecureX con le soluzioni di prima (Cisco Umbrella, Cisco Secure Endpoint) e di terze parti (Cohesity Helios), sarà possibile ridurre drasticamente il tempo e la complessità del rilevamento, dell'indagine e del ripristino dei ransomware.

Tipo di sessione: DevNet
Livello tecnico: Introduttivo
Tecnologia: SecureX, sicurezza

Brano: DevNet

Panoramica del prodotto o della strategia

Cisco XDR: Building for the Security Operations Center of Tomorrow - PSOSEC-1007 (Costruzione per il centro operazioni di sicurezza del futuro)

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

I team addetti alla sicurezza devono far fronte a un panorama di minacce in espansione e a un ambiente complesso che rende sempre più difficile l'efficienza della sicurezza. La soglia di povertà della cibersicurezza si sta allargando e gli attori malintenzionati stanno approfittando di questa lacuna per scatenare attacchi persistenti. Riteniamo che solo una soluzione efficace di 'Extended Detection and Response' sia in grado di rilevare e correggere avversari sofisticati come Turla, Wannacry e NotPetya nel vostro ambiente. Scopri il valore di interruzione delle attività di XDR nell'universo ibrido, multivendor e multivettore. Ascoltate le mie argomentazioni a favore di un ecosistema in continua crescita di integrazioni di tecnologie multifornitore come base per la creazione di operazioni di sicurezza future. E come XDR può diventare un moltiplicatore di forza per il vostro SOC?

Tipo di sessione: panoramica sul prodotto o sulla strategia
Livello tecnico: Generale
Tecnologia: SecureX, Hybrid Cloud, Sicurezza
Brano: Sicurezza

Come rafforzare in modo proattivo la resilienza della sicurezza - PSOCX-2000

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

Non solo è necessario gestire la sicurezza informatica, ma si deve anche affrontare una pressione reale per adottare normative basate sulla privacy dei dati. Come si progetta un programma di sicurezza informatica che soddisfi i requisiti in continua evoluzione in termini di rischio, regolamentazione, obiettivi aziendali e impatto operativo? In questa sessione imparerete a progettare un framework per la protezione e la privacy dei dati allineato al settore per soddisfare le esigenze dei soggetti interessati e produrre soluzioni che consentano la flessibilità aziendale. La struttura è progettata per tenere traccia delle attività e dei risultati di cibersicurezza desiderati che sono intuitivi per consentire una comunicazione semplice e non tecnica tra team multidisciplinari.

Tipo di sessione: panoramica sul prodotto o sulla strategia
Livello tecnico: Intermedio
Tecnologia: Customer Experience, SecureX, Security

Ulteriori opportunità

Oltre ai numerosi tipi di sessione elencati in precedenza, Live! è dotato di un'ampia gamma di

innovazioni e di ispirazione direttamente nella sala conferenze. Incontra gli ingegneri, acquisisci la bandiera o accetta la sfida, Live! continua a dimostrare come Cisco rappresenti il ponte verso il possibile. Il catalogo completo e ulteriori dettagli sono disponibili all'indirizzo Ciscolive.com.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).