Cisco Live ! Sessions Secure Endpoint et SecureX

Table des matières

Introduction

Cisco Live ! Las Vegas est l'un des événements majeurs de l'industrie avec plus de 1100 sessions actuellement prévues du 4 au 8 juin au Centre de Convention de Mandalay Bay. Avec un catalogue de cours aussi vaste, nous souhaitions nous assurer que nos clients Secure Endpoint connaissaient les opportunités de formation pour utiliser efficacement nos produits et services. Nous vous présentons une petite sélection des 129 ateliers, sessions en petits groupes et discussions sur la sécurité disponibles cette année à Las Vegas. Nous espérons que vous envisagerez de vous joindre à nous pour contribuer à rendre le monde plus sûr.

Travaux Pratiques Dirigés Par Un Instructeur

Terminaux sécurisés Cisco : faire le bon choix en déplaçant vers la gauche - LTRSEC-1114

Caly Hess, Security PrincessX, Cisco Systems, Inc.
Pedro Medina, Ingénieur logiciel, Cisco Systems, Inc.

La sécurité des terminaux est le dernier rempart dans le paysage de la cybercriminalité en pleine évolution et, lorsqu'elle est correctement configurée, la solution Cisco Secure Endpoint peut protéger votre entreprise. Au cours de cette session, vous aurez un accès pratique à la console Secure Endpoint tout en découvrant les configurations et les pratiques de déploiement pour la meilleure position de sécurité d'une équipe d'ingénierie qui a travaillé avec Secure Endpoint (FKA AMP) pendant près de dix ans. Vous apprendrez les capacités et les fonctionnalités de chaque moteur et les environnements dans lesquels ils peuvent être utilisés de manière optimale. Vous saurez comment définir des alertes et des automatismes pour limiter les risques d'attaque en cours, afin que votre entreprise ne soit pas obligée d'être la prochaine attaque majeure.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : travaux pratiques dirigés par un instructeur
Niveau technique : Introduction
Technologie : sécurité

Piste : sécurité

Couvrant l'évolution de la sécurité de la messagerie électronique des passerelles de messagerie sécurisées vers les plates-formes basées sur API - LTRSEC-2011

Un e-mail détaillé sur l'intégration de SecureX pour tirer le meilleur parti de votre déploiement XDR.

Alberto Torralba, architecte de solutions techniques.Ventes, Cisco Systems, Inc.
Greg Barnes, Ingénieur marketing technique, Cisco Systems, Inc.

Cette session de travaux pratiques présente les toutes dernières fonctionnalités de la gamme Cisco Secure Email. La session sera axée sur les meilleures pratiques pour permettre aux participants de tirer le meilleur parti de leur plate-forme de messagerie. Les sujets relatifs à la passerelle incluent l'utilisation de l'intelligence privée SecureX Cisco Threat Response, la configuration de l'authentification des messages basée sur le domaine, le reporting et la conformité (DMARC), la journalisation avancée, l'utilisation de l'API et bien plus encore. Les participants apprendront également à intégrer la passerelle dans le nouveau cloud Cisco Secure Email Threat Defense. Ces travaux pratiques présentent le logiciel en tant qu'offre de service pour rechercher les menaces telles que les compromissions de la messagerie professionnelle qui ne présentent pas d'indicateurs classiques de compromission et pour étudier les comptes potentiellement compromis.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : travaux pratiques dirigés par un instructeur
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Pare-feu sécurisé - Dépannage du chemin de données de défense contre les menaces (travaux pratiques) - LTRSEC-3880

John Groetzinger, responsable technique, Cisco Systems, Inc
Foster Lipkey, Ingénieur principal, Cisco Systems, Inc. - Intervenant émérite
Vidhi Mujumdar, responsable, livraison client, Cisco Systems

Une préoccupation commune pour les utilisateurs de la solution Cisco Firepower est de savoir quoi faire en cas d'interruption ou de dégradation du réseau qui semble être liée à la solution Firepower. Au cours de ces travaux pratiques, les participants apprendront les méthodologies de dépannage permettant d'évaluer les problèmes de chemin de données au sein de la plate-forme Firepower, notamment les réseaux NGIP Firepower série 3, l'ASA avec les services Firepower, Firepower Threat Defense (FTD) et FXOS. Cette session fournira aux participants un cadre permettant d'identifier la partie des services Firepower qui contribue au problème et la manière de résoudre rapidement les problèmes identifiés. Ce cadre couvrira l'intégralité du chemin de données depuis l'entrée des paquets jusqu'à l'inspection approfondie des paquets, y compris la règle Snort et les performances du préprocesseur. Ce TP porte à la fois sur Snort 2.9 et Snort 3 et sur leurs différences. Ces travaux pratiques contiennent des scénarios de dépannage utilisant

Virtual Firepower Threat Defense (vFTD) pour mettre en oeuvre la structure de dépannage. En outre, ces travaux pratiques aborderont brièvement l'intégration du pare-feu sécurisé SecureX.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : travaux pratiques dirigés par un instructeur
Niveau technique : Avancé
Technologie : sécurité
Piste : sécurité

Atelier sur la cyberrésilience - LTRSEC-1113

Ron Taylor, Sr Security Lab Test Monkey, Cisco Systems, Inc.
Leo Cruz, architecte de solutions techniques, Cisco Systems, Inc.

Votre équipe est-elle préparée à la prochaine attaque de la chaîne d'approvisionnement ou au jour zéro suivant ? La réalité ! Nous sommes tous attaqués, chaque jour, et nous finirons tous par être compromis ! Pour cette raison, votre entreprise doit être cyber-résiliente. La cyberrésilience fait référence à la capacité d'une entreprise à identifier un incident de sécurité informatique, à y répondre et à s'en remettre rapidement. Pour renforcer la cyberrésilience, il faut élaborer un plan axé sur les risques qui suppose que l'entreprise sera confrontée à un moment donné à une attaque ou à une brèche. Au cours de ces travaux pratiques, vous découvrirez les attaques de cybersécurité dans un environnement de laboratoire d'entreprise où vous jouerez le rôle d'attaquant et de défenseur et apprendrez par vous-même pourquoi vous avez besoin de solutions de sécurité hautement intégrées et de compétences en cyberopérations pour être résilient.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : travaux pratiques dirigés par un instructeur
Niveau technique : Introduction
Technologie : SecureX, sécurité
Piste : sécurité

Séances

Dépannage et isolation des problèmes de performances dus aux terminaux sécurisés (Windows, Linux et MAC) - BRKSEC-2072

Vibhor Amrodia, responsable technique, Cisco Systems, Inc

Vous allez terminer cette session avec des idées pour vous aider à isoler rapidement et efficacement les problèmes de performances avec Secure Endpoints installé. Il s'agit d'une session approfondie sur la façon dont nous pouvons analyser et isoler les problèmes de performances sur vos terminaux (Windows, Linux et MAC) à l'aide de certains journaux disponibles avec Secure Endpoint et également à l'aide de certains utilitaires et outils spécifiques au système d'exploitation. Les domaines d'intérêt de cette session sont les suivants : Détection et isolation de l'utilisation du processeur et de la mémoire vive Windows Détection et isolation de l'utilisation du processeur et de la mémoire vive Linux Détection et isolation de l'utilisation du

processeur et de la mémoire vive MAC

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : sécurité
Piste : sécurité

Cisco Unified Agent : Cisco Secure Client. Rassembler AMP, AnyConnect, Orbital et Umbrella - BRKSEC-2834

Aaron Woland, Ingénieur distingué, Cisco Systems, Inc. - Intervenant distingué

Nous avons tous entendu les plaintes ou nous-mêmes porté plainte : « Cisco a trop d'agents ».

Venez découvrir Aaron Woland, CCIE #20113 et Cisco Live Distinguished Speaker Hall of Fame Elite. Il vous montrera que Cisco a écouté les plaintes et a livré la première version d'un agent de sécurité unifié : Cisco Secure Client.

Cisco Secure Client (CSC) fournit une structure modulaire permettant à AnyConnect VPN, Cisco Secure Endpoint (anciennement AMP for Endpoints), Network Visibility Module, Umbrella Cloud Security, ISE Posture, Secure Firewall Posture (anciennement Hostscan) et Network Access Module (NAM) d'exister ensemble ; avec une gestion moderne basée sur le cloud provenant de SecureX - connectée intimement avec SecureX device insights.

Au cours de cette session, nous étudierons la technologie sous-jacente au client sécurisé, la manière dont les choses fonctionnent réellement et la manière dont elles ne fonctionnent pas. Nous couvrirons les modèles de déploiement à partir du cloud et en utilisant vos propres mécanismes de déploiement de logiciels. Nous allons tout savoir sur les flux de mise à niveau transparents des agents AnyConnect et AMP (Secure Endpoint) existants. Nous aborderons des scénarios dans lesquels il est judicieux d'effectuer une mise à niveau vers CSC et des scénarios dans lesquels il est réellement avantageux pour vous de rester avec les agents AnyConnect et AMP (Secure Endpoint) existants, du moins pour l'instant.

Venez passer un peu de temps avec Aaron et vous divertir tout en apprenant tout sur ce développement passionnant de Cisco Security.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

De l'expédition à la terre : intégrations, collaboration et prise de contrôle (sécurisée) au-delà de la passerelle de messagerie sécurisée Cisco - BRKSEC-2288

Robert Sherwin, responsable technique, Cisco Systems, Inc. - Intervenant émérite

Cisco Secure Email s'intègre bien au-delà de sa propre passerelle de messagerie. Sécurité, journalisation, API et configuration, et SecureX : nous vous expliquerons comment les e-mails vont au-delà de la passerelle et comment tirer le meilleur parti de votre environnement, grand ou petit !

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Intégrations de Cisco Malware Defense Cloud et Secure Malware Analytics - BRKSEC-2242

Bill Yazji, architecte de la sécurité technique, Cisco Systems - conférencier émérite

Vous l'avez peut-être appelé « AMP Cloud and Threat Grid », mais ils ont été rebaptisés « Malware Defense Cloud and Secure Malware Analytics ». Cette session examinera et approfondira les offres de solutions de protection contre les programmes malveillants et d'analyse des programmes malveillants tout en abordant leurs intégrations avec les architectures de sécurité Cisco, notamment Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella et Meraki. Ces produits fonctionnent ensemble et nous allons couvrir l'architecture de défense contre les programmes malveillants et démontrer comment tous les éléments s'intègrent pour fournir la meilleure architecture de protection avancée du secteur. Cette session est idéale pour les nouveaux utilisateurs de la suite de sécurité Cisco, ainsi que pour les clients qui possèdent un ou plusieurs produits et souhaitent approfondir leur collaboration.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Cisco XDR avec pare-feu - BRKSEC-2090

Eric Kostlan, Ingénieur marketing technique, Cisco Systems, Inc. - Intervenant émérite
Adi Sankar, Ingénieur marketing technique, Cisco Systems, Inc.

SecureX, le routeur XDR de Cisco, est la plate-forme la plus large et la plus intégrée au monde. Au cours de cette session, les participants découvriront la puissance de l'intégration du pare-feu et de SecureX. Cela inclut les incidents de pare-feu dans SecureX, l'enrichissement du pare-feu pour les enquêtes de réponse aux menaces et l'orchestration SecureX à l'aide des API de pare-feu. Les participants doivent avoir une compréhension de base de Cisco Secure Firewall. Les participants n'ont pas besoin de connaître SecureX.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Accélérez votre SOC avec Cisco SecureX - BRKSEC-1023

Matt Vander Horst, responsable technique, Cisco - Intervenant émérite

Saviez-vous que la plate-forme Cisco XDR SecureX peut accélérer la façon dont votre entreprise enquête et répond aux incidents ? SecureX combine une suite de fonctionnalités qui vous permettent de prendre en charge les incidents de sécurité, d'obtenir une meilleure visibilité sur une large gamme de produits et d'utiliser l'automatisation pour enquêter et répondre à la vitesse de la machine. Au cours de cette session, vous découvrirez SecureX et découvrirez les bases de ses diverses fonctionnalités, notamment le tableau de bord SecureX, la réponse aux menaces, le gestionnaire d'incidents, l'orchestration, les informations sur les périphériques et le client sécurisé. Nous partagerons également une liste d'autres sessions auxquelles vous pouvez assister pour approfondir ces fonctions et bien plus encore.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : Introduction
Technologie : SecureX, sécurité
Piste : sécurité

Cisco XDR avec e-mail : protéger, analyser et faire évoluer la conversation SMTP - BRKSEC-2095

Robert Sherwin, responsable technique, Cisco Systems, Inc. - Intervenant émérite

Les e-mails sont considérés comme le maillon le plus faible d'un réseau d'entreprise. En moins de deux minutes, les hackers et les acteurs peuvent accéder à un réseau de compromission ou de faille de sécurité. Les e-mails sont le principal vecteur d'infection par les programmes malveillants, car ils mettent sans effort les charges utiles malveillantes devant l'utilisateur et ne sont qu'à un clic de l'exploitation. Au-delà de la simple diffusion de programmes malveillants, les pirates sont plus que jamais à la pointe de la technologie pour créer et générer des liens d'hameçonnage qui ressemblent exactement aux services qu'ils utilisent. La solution de sécurisation de la messagerie électronique de Cisco évolue dans la manière dont eXtended Detection and Response cible ces vecteurs de menace et sécurise vos conversations SMTP.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Détection étendue avec Cisco XDR : analyses de sécurité dans toute l'entreprise - BRKSEC-2178

Matthew Robertson, Ingénieur marketing technique distingué, Cisco Systems, Inc. - Intervenant distingué

Détection étendue et réponse (XDR) est un mot à la mode populaire aujourd'hui. Démystifiant le sujet, cette session explorera les fonctionnalités de détection et d'analyse étendues du routeur XDR de Cisco, avec un accent particulier sur la manière d'étendre vos capacités de détection et d'accélérer votre réponse. Cette session couvre plusieurs technologies de détection, notamment les terminaux, l'analyse du réseau et le pare-feu. Elle explique comment l'analyse peut combiner ces détections et atteindre l'objectif XDR.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Sécurité informatique Cisco de A à Z. Protection avancée contre les programmes malveillants - Zero Trust - BRKCOC-2620

Steve Vida, architecte de la cybersécurité, Cisco Systems, Inc.
Gil Daudistel, RESPONSABLE.SÉCURITÉ DES INFORMATIONS, Cisco Systems, Inc.

Faire l'impossible : Cisco a amélioré la sécurité et l'expérience, en un seul mouvement, en introduisant Zero Trust for the Workforce. Cette session abordera en détail le flux sécurisé d'authentification Zero Trust, les avantages que nous avons tirés de l'alignement du nouveau flux avec une meilleure expérience et la manière dont nous avons déployé les configurations de terminaux pour prendre en charge Zero Trust à l'aide de Jamf Pro, InTune/SCCM et Meraki Systems Manager.
Cette session abordera également la manière dont Cisco IT met en oeuvre et gère les terminaux sécurisés Cisco dans son parc de plus de 200 000 périphériques.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : travail hybride, sécurité
Suivi : Cisco sur Cisco

Cisco SecureX XDR - Compréhension de toutes les pièces - BRKSEC-2113

Aaron Woland, Ingénieur distingué, Cisco Systems, Inc. - Intervenant distingué

XDR (eXtended Detection and Response, détection et réponse étendues) est l'une des technologies de sécurité les plus prisées du marché et son adoption connaît une croissance fulgurante. Étant donné le large éventail de ce qui peut être, ce qui devrait être et ce qui est fait

dans une solution XDR, il y a naturellement beaucoup de complexité qui peut mener à la confusion sur comment / ce qui se passe en coulisse. Cette session mettra en lumière les rouages internes de la solution XDR de Cisco, incroyablement performante, avec les fonctions de détection et de réponse du réseau, de détection et de réponse des terminaux, de défense contre les menaces de messagerie, d'analyse des programmes malveillants, d'agent de sécurité unifié et la façon dont toutes ces parties et parties s'assemblent pour produire le résultat attendu d'un XDR.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Exploitation de la solution XDR de Cisco avec les systèmes de gestion des services informatiques (ITSM) et SIEM pour l'investigation des incidents - BRKSEC-2122

Oxana Sannikova, architecte de solutions techniques, Cisco Systems, Inc.

Au cours de cette session, nous allons vous montrer comment la plate-forme SecureX (eXtended Detection and Response) peut augmenter les opérations de sécurité afin d'obtenir de meilleurs résultats sans générer de complexité supplémentaire. Nous étudierons les cas d'utilisation suivants : exploitation du contexte de la gestion des services informatiques (ITSM) et du SIEM dans la recherche de menaces, ajout d'une visibilité consolidée sur les menaces aux incidents ITSM et aux alertes SIEM, formalisation des procédures de réponse aux incidents en exploitant l'automatisation et l'orchestration. Près de la moitié de la session sera consacrée à des démonstrations. Les solutions ITSM et SIEM couvertes comprendront ServiceNow, Jira et Splunk, et les participants repartiront avec des workflows prêts à l'emploi.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : automatisation et orchestration, sécurité
Piste : sécurité

Intégration de Open Source Zeek et Cisco XDR - BRKSEC-2075

King Mark Stephens, architecte de la cybersécurité mondiale, CISCO Richfield, Ohio

Les solutions XDR (Extended Detection and Response) offrent la possibilité de protéger les entreprises contre les événements de cybersécurité en détectant et en réagissant plus rapidement, tout en réduisant les risques et l'exposition. Un XDR doit inclure des intégrations tierces pour fournir des moteurs de détection supplémentaires. Cette session présentera Zeek open source et fournira des détails exploitables sur la manière d'intégrer dans Cisco XDR pour améliorer les résultats en matière de sécurité des clients.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée

Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Le pouvoir de GreySkull ! Émulation d'adversaire - BRKSEC-2180

Jason Maynard, directeur technique, Cybersécurité Canada, CSS

Au cours de cette session, nous étudierons l'émulation antagoniste et la manière dont les équipes rouges et bleues peuvent en tirer parti. Nous découvrons les outils à notre disposition, puis nous élaborons une opération en tirant parti de Caldera sans capacités préventives. Nous passerons ensuite en revue les résultats de la confrontation, notamment ceux de notre gamme de solutions de sécurité Cisco déployées de manière passive. Les connaissances acquises permettent aux équipes de défense de comprendre l'opportunité d'augmenter nos défenses. Nous allons ensuite activer nos fonctionnalités de prévention sur diverses technologies de sécurité Cisco et effectuer à nouveau le test en examinant les résultats. Comprendre comment l'adversaire aborde sa victime et la capacité des acteurs de la défense à mettre en place une défense est la clé du succès.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Introduction à la gestion des vulnérabilités basée sur le risque - BRKSEC-1639

David Brothers, architecte de solutions techniques, Cisco Systems, Inc.

La gestion des vulnérabilités basée sur les risques (RBVM) englobe bien plus que vous ne le pensez. Au cours de cette présentation divertissante et instructive, nous allons approfondir les concepts fondamentaux et souligner les théories de quantification des risques, puis expliquer comment des programmes RBVM pratiques sont essentiels pour sécuriser le réseau moderne. Nous verrons ensuite comment Kenna apporte RBVM à un large éventail de produits et d'offres Cisco.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : séparée
Niveau technique : Introduction
Technologie : SecureX, sécurité
Piste : sécurité

Séance interactive

Utilisation de SecureX avec Cisco Talos Incident Response - IBOSEC-2011

Joe Schumacher, responsable des incidents, Cisco Systems, Inc.

Les participants apprendront directement auprès de notre équipe Cisco Talos Incident Response (Talos IR) comment exploiter SecureX pour accélérer les efforts de réponse lors d'un incident de sécurité. Ils pourront ainsi mieux comprendre comment SecureX peut être utilisé, qu'il s'agisse d'une collaboration avec une société externe de gestion des incidents telle que Talos IR ou d'une enquête interne. La session s'articulera autour d'un appel téléphonique par étapes vers la ligne d'assistance Talos IR par un client fictif avec plusieurs produits de sécurité Cisco. L'équipe Talos IR s'engage à établir des objectifs en matière d'intervention et à obtenir des informations de base avant de passer aux activités d'intervention d'urgence, qui comprendront l'utilisation de SecureX avec d'autres produits de sécurité jusqu'à ce que l'incident ait été maîtrisé.
Les objectifs de la séance seront d'informer le participant dans les domaines suivants :
L'intégration de SecureX pour connecter les éléments observables afin que les équipes puissent collaborer et travailler tout au long de l'enquête
Intégration de SecureX aux produits de sécurité pour orchestrer une réponse rapide et efficace

Type de session : session séparée interactive
Niveau technique : Introduction
Technologie : SecureX, sécurité
Piste : sécurité

Découverte de SecureX Idea Exchange - IBOSEC-2005

Josh Bordelon, architecte de sécurité d'entreprise mondial, Cisco Systems, Inc.

Explorez et échangez des idées sur l'utilisation de SecureX avec Cisco Security et des outils tiers dans une session interactive où nous discutons de la création et de la connexion de divers services. Apportez vos idées et vos questions ou apprenez des autres qui ont déjà commencé leur transition vers SecureX.

Type de session : session séparée interactive
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Laboratoires sans rendez-vous

Cisco Secure Client et SecureX Device Insights - mieux ensemble - LABSEC-2776

Paul Carco, INGÉNIEUR.MARKETING TECHNIQUE, Cisco Systems, Inc.
Serhii Kucherenko, Ingénieur des escalades client, Cisco Systems, Inc.

Le client sécurisé Cisco est un nouveau client unifié qui regroupe la plupart des clients de terminaux Cisco sous un même toit. Cisco Secure Client comprend des modules AnyConnect standard et des clients de sécurité tels qu'AMP (alias Cisco Secure Endpoint) et Orbital. Dans le cadre de ces travaux pratiques, vous apprendrez à déployer et à gérer Cisco Secure Client à partir du cloud SecureX. La partie consacrée à SecureX Devices Insights explique comment Cisco Secure Client et ses modules peuvent être utilisés pour la gestion des ressources d'entreprise et les enquêtes sur les incidents de sécurité.

Type de session : atelier pratique
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Séminaires techniques

Cisco Secure Client : d'AnyConnect à la sécurité client complète ! - TECSEC-2780

Hacke Nohre, architecte de solutions techniques, Cisco - conférencier émérite
Thorsten Schranz, Ingénieur marketing technique, Cisco Systems, Inc. - Intervenant émérite
Valeria Scribanti, Spécialiste des solutions techniques, Cisco Systems, Inc. - Intervenante émérite

La nouvelle main-d'oeuvre hybride, les scénarios d'attaque complexes, l'adoption rapide du cloud et l'omniprésence du cryptage sur Internet ont rendu la sécurité des clients plus importante que jamais !
Au cours de cette session de 4 heures, nous vous montrerons comment nous pouvons étendre AnyConnect (VPN) à la sécurité complète des terminaux. Nous aborderons les aspects techniques des modules Cisco Secure Client, notamment :
EDR/EPP (point d'extrémité sécurisé)
Télémétrie réseau des terminaux (module de visibilité réseau)
Protection DNS/Web (Umbrella)
Posture des terminaux (ISE/pare-feu sécurisé)
et les résultats de l'exécution d'un client unique géré de manière centralisée dans Cisco SecureX (XDR).
Le public ciblé est constitué d'ingénieurs et d'architectes réseau et de sécurité qui s'intéressent à la sécurité des terminaux. Une certaine connaissance de la sécurité des terminaux, des systèmes d'exploitation et des vecteurs d'attaque courants est supposée.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : Séminaire technique
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

Détection et réponse étendues avec Cisco Secure - TECSEC-2004

Matthew Robertson, Ingénieur marketing technique distingué, Cisco Systems, Inc. - Intervenant distingué

Hanna Jabbour, Ingénieur Marketing Technique Leader, Cisco Systems, Inc. - Intervenante émérite

Adi Sankar, Ingénieur marketing technique, Cisco Systems, Inc.

Matt Vander Horst, responsable technique, Cisco - Intervenant émérite

Cette session, qui débute par un approfondissement de l'offre de détection et de réponse étendues de Cisco, fournit une présentation complète de la mise en oeuvre et du fonctionnement des différents composants du produit, notamment Cisco Secure Endpoint, Secure Cloud Analytics, Umbrella, Meraki et Email Threat Defense et de leur fonctionnement dans Cisco XDR. Les meilleures pratiques opérationnelles et les détails de mise en oeuvre du moteur de réponse seront également inclus, ainsi que l'intégration de Cisco XDR à des produits non Cisco tels que Crowdstrike Falcon.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : Séminaire technique
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Piste : sécurité

DevNet

Automatisation de la sécurité : développement avec SecureX - DEVNET-1083

Matt Vander Horst, responsable technique, Cisco - Intervenant émérite

Saviez-vous que la plate-forme XDR de Cisco offre plusieurs moyens d'automatiser vos opérations de sécurité et de créer de puissantes intégrations ? Les modules d'intégration SecureX vous permettent d'intégrer des données provenant d'autres plates-formes dans vos investigations, les API de réponse aux menaces SecureX vous permettent d'automatiser la manière dont vous enquêtez et répondez aux menaces, et l'orchestration SecureX vous permet de créer des flux de travail puissants à l'aide d'un éditeur de glisser-déplacer de code « no-to-low ». Passez à cette session pour en savoir plus sur chacune de ces trois facettes de SecureX et sur la façon dont vous pouvez les utiliser pour optimiser vos opérations de sécurité.

Type de session : DevNet
Niveau technique : Introduction
Technologie : SecureX, sécurité

Suivi : DevNet

Automatisation des opérations de cyberhygiène avec SecureX et Kenna Security - DEVLIT-1355

Oxana Sannikova, architecte de solutions techniques, Cisco Systems, Inc.

Les opérations informatiques sont encore très manuelles aujourd'hui. Les clients sont toujours confrontés au défi de maintenir l'intégrité du système et d'améliorer la sécurité en ligne. Au cours de cette session rapide, nous allons démontrer comment l'orchestration Cisco SecureX et Kenna Security peuvent être exploitées pour automatiser la gestion des vulnérabilités.

Type de session : DevNet
Niveau technique : intermédiaire

Technologie : automatisation et orchestration, sécurité
Suivi : DevNet

Utilisation de l'orchestration SecureX pour automatiser la réponse aux incidents de cloud public - DEVWKS-2240

Brian Sak, architecte de solutions techniques, Cisco Systems, Inc. - Intervenant émérite

Lorsque les charges de travail sont transférées vers des fournisseurs de cloud public tels qu'AWS, Azure ou GCP, la réponse et la résolution des incidents peuvent devenir plus difficiles et nécessitent des outils différents. Cette session vous guidera tout au long de la création de workflows d'orchestration SecureX qui automatisent et simplifient le processus d'identification des menaces, simplifient les procédures de réponse et offrent aux équipes secops la tranquillité d'esprit lors de la sécurisation des ressources dans des environnements multicloud ou de cloud hybride.
Nouveauté cette année, les participants à l'atelier DevNet sont inscrits en premier. Seuls 12 ordinateurs portables sont disponibles pour cette session. Il s'agit d'un atelier DevNet pratique où vous codez avec un instructeur. Apportez vos propres écouteurs à connecteur auxiliaire de 3,5 mm pour écouter le présentateur ou prendre une paire d'écouteurs au Centre de commande DevNet.
En participant à cet atelier DevNet, vous pourrez obtenir des crédits Cisco pour la formation continue (CE). Pour plus d'informations, consultez le site : https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : DevNet
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Suivi : DevNet

Évolutivité des flux de travail du cloud hybride avec SecureX Orchestrator et un connecteur distant - DEVNET-2109

Steve McNutt, architecte de solutions techniques, Cisco Systems, Inc.

Vous avez peut-être entendu parler de SecureX Orchestration (SXO) dans le contexte de l'orchestration de la sécurité. Nous vous montrerons qu'il peut faire beaucoup plus et servir de base à la création d'outils d'exploitation de cloud hybride efficaces. Cette session commence par une présentation générale de l'architecture, suivie d'une présentation de la solution type de déploiement de masse Cisco Umbrella, expliquant comment les composants s'intègrent et les défis qu'ils représentent. Vous quitterez cette session avec une compréhension de la manière de créer des workflows de cloud hybride hautement évolutifs en tirant parti du modèle de carte de profil, et une connaissance du code d'exemple que vous pouvez modifier pour créer vos propres solutions.

Type de session : DevNet
Niveau technique : intermédiaire

Technologie : SecureX, sécurité
Suivi : DevNet

Doublement du nombre de R dans XDR : Comment automatiser vos opérations de sécurité (SecOps) en 10 clics dans Cisco SecureX (sans écrire de ligne de code) - DEVNET-2214

Christopher Van Der Made, Responsable produits d'ingénierie, Cisco Systems, Inc. - Intervenant émérite

Cette session vous montrera comment la puissance de l'automatisation peut être exploitée via SecureX Orchestration sans écrire de code. Cela permettra aux entreprises de doubler le nombre de R dans le XDR (eXtended Detection and Response) de Cisco. Nous allons passer en revue quelques exemples d'installation extrêmement simples qui vous permettront d'atteindre le point de départ. Nous utiliserons le nombre de clics nécessaires dans la console comme mesure, pour vous prouver comment vous pouvez accéder à une automatisation puissante sans trop de tracas. À la fin, vous apprendrez également à aller encore plus loin et à maîtriser l'automatisation de vos opérations de sécurité. Vous recevrez tous les documents par la suite pour commencer vous-même. Cette session s'adresse aux intervenants en cas d'incident, aux analystes de sécurité, aux responsables SOC ou à toute personne intéressée par l'automatisation et la sécurité.

Type de session : DevNet
Niveau technique : intermédiaire
Technologie : SecureX, sécurité
Suivi : DevNet

Intégration à l'API Microsoft Graph : utilisation de Python et SecureX - DEVWKS-3260

Hacke Nohre, architecte de solutions techniques, Cisco - conférencier émérite

Au cours de cet atelier, nous discuterons de la manière dont l'API Microsoft Graph peut être intégrée dans des environnements Cisco classiques.
Nous aborderons une présentation de haut niveau de l'API Microsoft Graph, en mettant l'accent sur l'authentification Oauth2 et l'autorisation d'Azure AD.
Nous verrons ensuite comment accéder à cette API via des scripts python et SecureX pour accéder aux informations sur les groupes et les rôles Azure AD pour un utilisateur spécifique accéder aux informations sur les événements de sécurité de l'environnement Microsoft
Les participants peuvent essayer de suivre les étapes de l'atelier à partir des environnements de laboratoire pendant l'atelier, ou ils peuvent effectuer les étapes plus tard. Nous vous fournirons des pointeurs vers les configurations des travaux pratiques qui permettent aux participants d'effectuer les tâches de l'atelier par eux-mêmes, sans avoir besoin de leur propre compte Azure ou SecureX.

Peut bénéficier du crédit de formation continue Cisco : Oui
Type de session : DevNet

Niveau technique : Avancé
Technologie : DevNet, sécurité
Suivi : DevNet

Automatisez et simplifiez votre défense contre les ransomwares avec SecureX - DEVNET-1456

Elia Maracani, Ingénieur système, Cisco Systems, Inc.

Les attaques par ransomware se concentrent de plus en plus sur les sauvegardes. La protection, ainsi que la récupération rapide et facile de la sauvegarde de votre entreprise, deviennent ainsi la meilleure et la plus importante étape de la défense contre les attaques de ransomware débilitantes. À l'aide d'une démonstration, nous mettrons en avant la polyvalence et la personnalisation que SecureX est en mesure d'offrir via son moteur d'orchestration. Grâce à l'intégration de Cisco SecureX aux solutions 1er (Cisco Umbrella, Cisco Secure Endpoint) et tierces (Cohesity Helios), vous pourrez réduire considérablement le temps et la complexité de détection, d'investigation et de récupération des ransomwares.

Type de session : DevNet
Niveau technique : Introduction
Technologie : SecureX, sécurité
Suivi : DevNet

Présentation du produit ou de la stratégie

Cisco XDR : Bâtiment pour le centre des opérations de sécurité de demain - PSOSEC-1007

Sana Sana Yousuf, responsable marketing produits, Cisco Systems, Inc.

Les équipes chargées de la sécurité sont confrontées à un paysage de menaces en pleine expansion et à un environnement complexe qui rend la sécurité de plus en plus difficile à atteindre. Le seuil de pauvreté en matière de cybersécurité s'élargit et des acteurs malveillants profitent de cette lacune béante pour lancer des attaques persistantes. Nous pensons que seule une solution de « détection et de réponse étendues » efficace peut détecter et éliminer les hackers sophistiqués tels que Turla, Wannacry et NotPetya dans votre environnement. Découvrez la valeur révolutionnaire de XDR dans l'univers hybride, multifournisseur et multivecteur. Écoutez-moi vous présenter l'intérêt d'un écosystème toujours plus vaste d'intégrations technologiques multifournisseurs, qui servira de base à la mise en place des opérations de sécurité de demain. Et comment XDR peut devenir un multiplicateur de force pour votre SOC ?

Type de session : présentation du produit ou de la stratégie
Niveau technique : Général
Technologie : SecureX, cloud hybride, sécurité
Piste : sécurité

[Comment renforcer de manière proactive votre résilience en matière de sécurité - PSOCX-2000]

Varun Dhingra, Directeur senior, Gestion des produits, Sécurité et collaboration, Cisco Systems, Inc.
Mark Hammond, Directeur de la gestion des produits, Cisco Systems, Inc

Non seulement vous devez gérer la cybersécurité, mais vous devez également faire face à une réelle pression pour adopter des réglementations basées sur la confidentialité des données. Comment concevez-vous un programme de cybersécurité qui réponde aux exigences en constante évolution des risques, de la réglementation, des objectifs commerciaux et de l'impact opérationnel ? Au cours de cette session, vous apprendrez à concevoir un cadre de sécurité et de confidentialité des données aligné sur le secteur afin de répondre aux besoins des parties prenantes et de produire des solutions qui favorisent l'agilité de l'entreprise. Le cadre est conçu pour suivre les activités et les résultats de cybersécurité souhaités qui sont intuitifs pour permettre une communication simple et non technique entre des équipes multidisciplinaires.

Type de session : présentation du produit ou de la stratégie
Niveau technique : intermédiaire
Technologie : expérience client, SecureX, sécurité

Opportunités supplémentaires

En plus des nombreux types de sessions répertoriés ci-dessus, Live ! a beaucoup d'innovation et d'inspiration directement sur le plancher de la conférence. Rencontrez les ingénieurs, saisissez le drapeau ou relevez le défi, en direct ! continue de démontrer comment Cisco est la passerelle vers le possible. Consultez le catalogue complet et plus de détails à l'adresse Ciscolive.com.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.