Cisco Live! Endpoint seguro e sessões SecureX

Contents

Como fortalecer proativamente sua resiliência de segurança - PSOCX-2000
Oportunidades adicionais

Introduction

Cisco Live! Las Vegas é um dos principais eventos do setor, com mais de 1.100 sessões programadas para 4 a 8 de junho no Mandalay Bay Convention Center. Com um catálogo de cursos tão grande, queríamos ter certeza de que nossos clientes de endpoint seguro estavam cientes das oportunidades de educação para utilizar nossos produtos e serviços de forma eficaz. Destacando apenas uma pequena seleção dos 129 Laboratórios, Sessões de breakout e Discussões disponíveis em torno do tópico de Segurança, disponíveis este ano em Las Vegas, esperamos que você considere a possibilidade de se juntar a nós, pois ajudamos a tornar o mundo um lugar mais seguro.

Laboratórios ministrados por instrutor

Ponto de extremidade seguro da Cisco: fazendo certo mudando para a esquerda - LTRSEC-1114

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

A segurança de endpoint é a última barreira de defesa no cenário de crimes cibernéticos em evolução e, quando configurada corretamente, o Cisco Secure Endpoint pode manter sua empresa segura. Nesta sessão, você terá acesso prático ao Secure Endpoint Console enquanto aprende configurações e práticas de implantação para a melhor postura de segurança de uma equipe de engenharia que trabalhou com o Secure Endpoint (FKA AMP) por uma década. Você aprenderá os recursos e a funcionalidade de cada mecanismo e em quais ambientes eles podem ser utilizados de forma ideal. Você saberá como definir alertas e automatizações para mitigar um ataque em andamento para que sua empresa não tenha que ser a próxima grande violação.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de sessão: Laboratório ministrado por instrutor
Nível técnico: introdutório
Tecnologia: segurança
Opção: Segurança

Cobrindo a evolução da segurança de e-mail de gateways de e-mail seguros para plataformas baseadas em API - LTRSEC-2011

Um aprofundamento de e-mail que aborda a integração do SecureX para aproveitar ao máximo sua implantação XDR.

Alberto Torralba, arquiteto de soluções técnicas.Sales, Cisco Systems, Inc.
Greg Barnes, engenheiro técnico de marketing da Cisco Systems, Inc.

Esta sessão de laboratório apresentará uma visão geral dos mais novos recursos do portfólio Cisco Secure Email. A sessão se concentrará nas práticas recomendadas para permitir que os participantes aproveitem ao máximo sua plataforma de e-mail. Os tópicos para gateway incluirão o uso da inteligência privada do SecureX Cisco Threat Response, a configuração da Autenticação de Mensagens Baseada em Domínio, Relatórios e Conformidade (DMARC), registro avançado, uso de API e muito mais. Os participantes também aprenderão a integrar o gateway à nova nuvem, oferecendo o Cisco Secure Email Threat Defense. O laboratório vai apresentar o software como uma oferta de serviço para procurar ameaças, como

comprometimento de e-mail comercial, que não possuem indicadores tradicionais de comprometimento e investigar contas potencialmente comprometidas.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de sessão: Laboratório ministrado por instrutor
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Firewall seguro - Solução de problemas de caminho de dados do Threat Defense (um laboratório prático) - LTRSEC-3880

John Groetzinger, Líder técnico, Cisco Systems, Inc
Foster Lipkey, Engenheiro Principal, Cisco Systems, Inc. - Palestrante Distinto
Vidhi Mujumdar, Líder, Entrega ao cliente, Cisco Systems

Uma preocupação comum dos usuários da solução Cisco Firepower é o que fazer no caso de uma interrupção ou degradação da rede que pareça estar relacionada à solução Firepower. Neste laboratório, os participantes aprenderão metodologias de solução de problemas para avaliar problemas de caminho de dados na plataforma Firepower, incluindo NGIPs Firepower Series 3, ASA com Firepower Services, Firepower Threat Defense (FTD) e FXOS. Essa sessão fornecerá aos participantes uma estrutura para identificar qual parte dos serviços Firepower está contribuindo para o problema e como atenuar rapidamente os problemas identificados. Essa estrutura cobrirá todo o caminho de dados desde a entrada de pacotes até a inspeção profunda de pacotes, incluindo a regra Snort e o desempenho do pré-processador. Este laboratório cobrirá o Snort 2.9 e o Snort 3 e as diferenças entre eles. Este laboratório conterá cenários de solução de problemas usando o Virtual Firepower Threat Defense (vFTD) para implementar a estrutura de solução de problemas. Além disso, este laboratório abordará brevemente a integração do SecureX Secure Firewall.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de sessão: Laboratório ministrado por instrutor
Nível técnico: Avançado
Tecnologia: segurança
Opção: Segurança

Workshop sobre resiliência digital - LTRSEC-1113

Ron Taylor, Sr. Macaco de teste do laboratório de segurança, Cisco Systems, Inc.
Leo Cruz, arquiteto de soluções técnicas, Cisco Systems, Inc.

Sua equipe está preparada para o próximo ataque à cadeia de suprimentos ou para o próximo dia zero? Verificação da realidade! Estamos todos sob ataque, todos os dias e todos acabaremos por ser comprometidos! Por esse motivo, sua empresa precisa ser resiliente ao ciberespaço. A resiliência cibernética se refere à capacidade de uma empresa de identificar, responder e se recuperar rapidamente de um incidente de segurança de TI. O desenvolvimento da resiliência cibernética inclui a elaboração de um plano focado no risco que pressupõe que, em algum momento, a empresa enfrentará uma violação ou um ataque. Neste laboratório, você terá ataques de segurança cibernética em um ambiente de laboratório empresarial, no qual você atua como invasor e defensor e aprende, em primeira mão, por que precisa de soluções de segurança altamente integradas e habilidades de CyberOps para ser resiliente ao cibernético.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de sessão: Laboratório ministrado por instrutor
Nível técnico: introdutório
Tecnologia: SecureX, segurança
Opção: Segurança

Debates

Solução de problemas e isolamento de problemas de desempenho devido a endpoints seguros (Windows, Linux e MAC) - BRKSEC-2072

Vibhor Amrodia, Líder técnico, Cisco Systems, Inc

Você sairá desta sessão com ideias para ajudá-lo a isolar de forma rápida e eficaz os problemas de desempenho com os endpoints seguros instalados. Esta é uma sessão aprofundada sobre como podemos analisar e isolar problemas de desempenho em seus endpoints (Windows, Linux e MAC) usando alguns dos registros disponíveis com o Secure Endpoint e também usando alguns utilitários e ferramentas específicos do SO. As áreas de foco desta sessão seriam: Detecção de utilização de CPU e RAM do Windows e Isolamento Detecção de utilização de CPU e RAM do Linux e Isolamento Detecção e Isolamento de utilização de CPU e RAM do MAC

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: segurança
Opção: Segurança

Agente unificado da Cisco: Cisco Secure Client. Reunindo AMP, AnyConnect, Orbital e Umbrella - BRKSEC-2834

Aaron Woland, engenheiro renomado, Cisco Systems, Inc. - palestrante renomado

Todos nós ouvimos as reclamações ou fizemos as reclamações: "A Cisco tem muitos agentes".

Aprenda com Aaron Woland, CCIE #20113 e Cisco Live Distinguished Speaker Hall of Fame Elite; enquanto ele mostra que a Cisco ouviu as reclamações e forneceu a primeira iteração de um agente de segurança unificado: o Cisco Secure Client.

O Cisco Secure Client (CSC) fornece uma estrutura modular que permite que o AnyConnect VPN, o Cisco Secure Endpoint (antigo AMP para Endpoints), o Network Visibility Module, o Umbrella Cloud Security, o ISE Posture, o Secure Firewall Posture (antigo Hostscan) e o Network Access Module (NAM) coexistam; com um gerenciamento moderno baseado em nuvem proveniente do SecureX - conectado intimamente com informações do dispositivo SecureX.

Nesta sessão, vamos nos aprofundar na tecnologia por trás do Secure Client, como as coisas realmente funcionam e como não funcionam. Abordaremos modelos de implantação a partir da nuvem e usando seus próprios mecanismos de implantação de software. Aprenderemos tudo sobre os fluxos de atualização contínuos dos agentes atuais do AnyConnect e do Secure Endpoint (AMP). Falaremos sobre cenários em que faz sentido atualizar para o CSC e cenários em que realmente beneficia você para ficar com os agentes atuais do AnyConnect e do Secure Endpoint (AMP) - pelo menos por enquanto.

Venha passar algum tempo com Aaron e divirta-se enquanto aprende tudo sobre esse desenvolvimento interessante do Cisco Security.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Do envio para a costa: integrações, colaboração e controle (com segurança) além do Cisco Secure Email Gateway - BRKSEC-2288

Robert Sherwin, Líder Técnico, Cisco Systems, Inc. - Palestrante distinto

O Cisco Secure Email integra-se fora de ser seu próprio gateway de e-mail. Segurança, registro, API e configuração e SecureX - nós o guiaremos através de como o e-mail se estende além do gateway e aproveita ao máximo seu ambiente, grande ou pequeno!

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Integrações da Cisco com Malware Defense Cloud e Secure Malware Analytics - BRKSEC-2242

Bill Yazji, arquiteto de segurança técnica, Cisco Systems - palestrante renomado

Você pode tê-lo conhecido como "AMP Cloud and Threat Grid", mas eles foram renomeados como Malware Defense Cloud e Secure Malware Analytics. Esta sessão analisará e analisará detalhadamente as ofertas de Malware Defense Cloud e Malware Analytics enquanto cobre suas integrações com as arquiteturas de segurança da Cisco, incluindo Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella e Meraki. Esses produtos funcionam em conjunto e abordaremos a Malware Defense Architecture e demonstraremos como todas as peças se encaixam para oferecer a Advanced Threat Architecture líder do setor. Esta sessão é perfeita para aqueles que são mais recentes no Cisco Security Suite, bem como para aqueles clientes que possuem um ou mais produtos e desejam aprofundar em como eles trabalham juntos.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Cisco XDR com firewall - BRKSEC-2090

Eric Kostlan, Engenheiro Técnico de Marketing, Cisco Systems, Inc. - Palestrante renomado
Adi Sankar, engenheiro técnico de marketing, Cisco Systems, Inc.

O SecureX, o XDR da Cisco, é a plataforma mais ampla e integrada do mundo. Nesta sessão, os participantes verão o poder da integração do Firewall com o SecureX. Isso inclui incidentes de firewall no SecureX, enriquecimento de firewall para investigações de resposta a ameaças e orquestração do SecureX usando APIs de firewall. Os participantes devem ter uma compreensão básica do Cisco Secure Firewall. Os participantes não precisam conhecer o SecureX.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Acelere seu SOC com o Cisco SecureX - BRKSEC-1023

Matt Vander Horst, Líder Técnico, Cisco - Palestrante Destacado

Você sabia que a plataforma XDR da Cisco SecureX pode acelerar a forma como sua empresa investiga e responde a incidentes? O SecureX combina um conjunto de recursos que permitem que você assuma o controle de incidentes de segurança, obtenha melhor visibilidade em um amplo portfólio de produtos e use a automação para investigar e responder na velocidade da máquina. Nesta sessão, você obterá uma introdução ao SecureX e aprenderá os fundamentos de seus vários recursos, incluindo: painel SecureX, resposta a ameaças, gerenciador de incidentes, orquestração, insights de dispositivos e cliente seguro. Também compartilharemos uma lista de outras sessões que você pode participar para aprofundar-se nesses recursos e muito mais.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: introdutório
Tecnologia: SecureX, segurança
Opção: Segurança

Cisco XDR com e-mail: proteja, analise e desenvolva a conversa SMTP - BRKSEC-2095

Robert Sherwin, Líder Técnico, Cisco Systems, Inc. - Palestrante renomado

O e-mail é conhecido como o elo mais fraco em uma rede empresarial e em menos de dois minutos fornece aos hackers e agentes uma porta aberta que leva a um comprometimento ou violação. O e-mail é o principal vetor de infecção por malware, pois ele coloca facilmente payloads mal-intencionadas na frente do usuário e está a apenas um clique de distância da exploração. Além de apenas distribuir malware, os invasores estão mais sofisticados do que nunca em criar e gerar links de phishing que se parecem com os serviços que estão representando. O Cisco Secure Email está evoluindo na forma como a eXtended Detection and Response tem como alvo esses vetores de ameaças e protege suas conversas de SMTP.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Detecção estendida com Cisco XDR: análise de segurança em toda a empresa - BRKSEC-2178

Matthew Robertson, engenheiro técnico de marketing renomado, Cisco Systems, Inc. - palestrante renomado

O Extended Detection and Response (XDR) é um termo popular atualmente. Desmistificando o tópico, esta sessão explorará os recursos estendidos de detecção e análise do XDR da Cisco com foco específico em como ampliar seus recursos de detecção e acelerar sua resposta. Abordando várias tecnologias de detecção, incluindo endpoint, análise de rede e firewall, esta sessão explorará como a análise pode reunir essas detecções e atingir o objetivo XDR.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança

Opção: Segurança

Cisco IT Security de A a Z. Proteção avançada contra malware para confiança zero - BRKCOC-2620

Steve Vida, arquiteto de segurança digital, Cisco Systems, Inc.
Gil Daudistel, GERENTE.SEGURANÇA DA INFORMAÇÃO, Cisco Systems, Inc.

Fazer o impossível: a Cisco aumentou a segurança e melhorou a experiência, em um movimento, introduzindo o Zero Trust for the Workforce. Esta sessão analisará os detalhes do fluxo de autenticação seguro do Zero Trust, como nos beneficiamos do alinhamento do novo fluxo com uma experiência melhor e como implantamos configurações de endpoint para oferecer suporte ao Zero Trust usando o Jamf Pro, o InTune/SCCM e o Meraki Systems Manager.
Esta sessão também analisará como a TI da Cisco implementa e mantém o Cisco Secure Endpoint em sua frota de mais de 200.000 dispositivos.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: trabalho híbrido, segurança
Track: Cisco na Cisco

Cisco SecureX XDR - Compreendendo todas as peças - BRKSEC-2113

Aaron Woland, engenheiro renomado, Cisco Systems, Inc. - palestrante renomado

O eXtended Detection and Response (XDR) é uma das tecnologias de segurança mais avançadas do mercado e está observando um enorme crescimento na sua adoção. Dada a ampla gama do que pode ser, deve ser e é feito em uma solução XDR, há naturalmente muita complexidade que pode levar à confusão sobre como/o que está acontecendo nos bastidores. Esta sessão irá esclarecer o funcionamento interno da solução XDR incrivelmente eficiente da Cisco, com Detecção e resposta de rede, Detecção e resposta de endpoint, Defesa contra ameaças por e-mail, Análise de malware, Agente de segurança unificado; e como todas essas partes e peças se unem para produzir o resultado esperado de um XDR.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Aproveitando a solução XDR da Cisco com gerenciamento de serviços de TI (ITSM) e sistemas SIEM para investigação de incidentes - BRKSEC-2122

Oxana Sannikova, Arquiteta de soluções técnicas, Cisco Systems, Inc.

Nesta sessão, mostraremos como a plataforma XDR (eXtended Detection and Response), SecureX, pode aumentar as operações de segurança para oferecer um resultado melhor sem criar complexidade adicional. Examinaremos os seguintes casos de uso: aproveitamento do contexto do IT Service Management (ITSM) e do SIEM na busca de ameaças, adição de visibilidade consolidada de ameaças a incidentes de ITSM e alertas de SIEM, formalização de procedimentos de resposta a incidentes com o aproveitamento da automação e orquestração. Quase metade da sessão será constituída por manifestações. As soluções ITSM e SIEM abordadas incluirão ServiceNow, Jira e Splunk, e os participantes sairão com fluxos de trabalho prontos para uso.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: automação e orquestração, segurança
Opção: Segurança

Integração do Open Source Zeek com o Cisco XDR - BRKSEC-2075

King Mark Stephens, arquiteto de segurança cibernética global, CISCO Richfield, Ohio

As soluções de XDR (Extended Detection and Response, detecção e resposta estendidas) oferecem o potencial de proteger as empresas de eventos de segurança cibernética, detectando e respondendo mais rapidamente e reduzindo o risco e a exposição. Um XDR deve incluir integrações de terceiros para fornecer mecanismos de detecção adicionais. Esta sessão apresentará o código aberto Zeek e fornecerá detalhes acionáveis de como integrar-se ao Cisco XDR para melhorar os resultados de segurança do cliente.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

O poder do GraySkull! Emulação de Adversário - BRKSEC-2180

Jason Maynard, CTO de campo de segurança digital do Canadá, CSS

Nesta sessão, aprenderemos sobre emulação adversária e como as equipes vermelha e azul podem se beneficiar com seu uso. Aprendemos sobre as ferramentas disponíveis para nós e depois criamos uma operação utilizando a Caldera sem capacidades preventivas. Em seguida, analisaremos os resultados contraditórios, o que inclui a análise dos resultados em nosso portfólio de segurança da Cisco implantado passivamente. O conhecimento adquirido garante que as equipes defensivas entendam a oportunidade de aumentar nossas defesas. Em seguida, ativaremos nossos recursos preventivos em uma variedade de tecnologias de segurança da Cisco e executaremos o teste novamente analisando os resultados. Entender como o adversário aborda a vítima e a capacidade dos defensores de criar camadas de defesa é uma receita para o sucesso.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de Sessão: Reunião à Parte
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Uma introdução ao gerenciamento de vulnerabilidades baseado em risco - BRKSEC-1639

David Brothers, arquiteto de soluções técnicas, Cisco Systems, Inc.

O RBVM (Risk-Based Vulnerability Management, gerenciamento de vulnerabilidades baseado em risco) abrange mais do que você provavelmente imagina. Nesta palestra divertida e informativa, vamos nos aprofundar nos conceitos fundamentais e nas teorias de sublinhar a quantificação do risco e, em seguida, compartilhar como os programas práticos de RBVM são essenciais para garantir a rede moderna. Em seguida, discutiremos como a Kenna leva a RBVM a uma grande variedade de produtos e ofertas da Cisco.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim

Tipo de Sessão: Reunião à Parte
Nível técnico: introdutório
Tecnologia: SecureX, segurança
Opção: Segurança

Reunião Interativa à Parte

Aproveitando o SecureX com a resposta a incidentes do Cisco Talos - IBOSEC-2011

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

Os participantes aprenderão diretamente com nossa equipe de resposta a incidentes do Cisco Talos (Talos IR) sobre como utilizar o SecureX para acelerar os esforços de resposta durante um incidente de segurança. Eles terão uma ideia de como o SecureX pode ser utilizado, seja trabalhando com uma empresa externa de resposta a incidentes, como a Talos IR, ou conduzindo uma resposta investigativa interna. A sessão será construída em torno de uma chamada telefônica em etapas na linha direta IR do Talos por um cliente fictício com vários produtos de segurança da Cisco. A equipe de IR da Talos se comprometerá a estabelecer objetivos de resposta e obter informações de apoio antes de iniciar as atividades de resposta de emergência, que incluirão o uso do SecureX juntamente com outros produtos de segurança até que o incidente seja contido.
Os objetivos da sessão serão informar esse participante nas seguintes áreas:
Incorporar o SecureX para conectar observáveis para que as equipes colaborem e trabalhem durante a investigação
Integrar o SecureX com produtos de segurança para orquestrar uma resposta oportuna e eficaz

Tipo de sessão: breakout interativo
Nível técnico: introdutório
Tecnologia: SecureX, segurança
Opção: Segurança

Conheça o SecureX Idea Exchange - IBOSEC-2005

Josh Bordelon, arquiteto de segurança corporativa global, Cisco Systems, Inc.

Explore e troque ideias sobre a utilização do SecureX com as ferramentas de segurança da Cisco e de terceiros em uma sessão interativa onde discutimos a criação e a conexão de vários serviços. Traga suas ideias e perguntas ou aprenda com outras pessoas que já iniciaram a jornada do SecureX.

Tipo de sessão: breakout interativo
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Laboratórios para visitas

Cisco Secure Client e SecureX Device Insights - melhor juntos - LABSEC-2776

Paul Carco, ENGENHEIRO.MARKETING TÉCNICO, Cisco Systems, Inc.
Serhii Kucherenko, Engenheiro de Escalações de Clientes, Cisco Systems, Inc.

O Cisco Secure Client é um novo cliente unificado que reúne a maioria dos clientes de endpoint da Cisco. O Cisco Secure Client compreende os módulos padrão do AnyConnect e clientes de segurança, como o AMP

(conhecido como Cisco Secure Endpoint) e Orbital. Como parte deste LABORATÓRIO, você aprenderá como implantar e gerenciar o Cisco Secure Client a partir da SecureX Cloud. A parte dedicada ao SecureX Devices Insights demonstrará como o Cisco Secure Client e seus módulos podem ser usados para gerenciamento de ativos de nível empresarial e investigação de incidentes de segurança.

Tipo de sessão: Laboratório com orientações
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Seminários técnicos

Cisco Secure Client: do AnyConnect à segurança abrangente do cliente! - TECSEC-2780

Hacke Nohre, arquiteto de soluções técnicas, Cisco - palestrante renomado
Thorsten Schranz, Engenheiro Técnico de Marketing, Cisco Systems, Inc. - Palestrante renomado
Valeria Scribanti, Especialista em soluções técnicas, Cisco Systems, Inc. - Palestrante renomado

A nova força de trabalho híbrida, cenários de ataque complexos, a adoção rápida da nuvem e a difusão da criptografia na Internet tornaram a segurança do cliente mais importante do que nunca!
Nesta sessão de 4 horas, mostraremos como podemos expandir o AnyConnect (VPN) para uma segurança de endpoint com todos os recursos. Vamos nos aprofundar nos aspectos técnicos dos módulos do Cisco Secure Client, incluindo:
EDR/EPP (endpoint seguro)
Telemetria de rede de endpoint (Módulo de visibilidade de rede)
Proteção de DNS/Web (Umbrella)
Postura de endpoint (ISE/firewall seguro)
e nos resultados da execução de um único cliente gerenciado centralmente no Cisco SecureX (XDR).
O público-alvo são os engenheiros e arquitetos de rede e segurança com interesse em segurança de endpoint. Presume-se que haja algum conhecimento de segurança de endpoint, sistemas operacionais e vetores de ataque comuns.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de sessão: Seminário técnico
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

Detecção e resposta estendidas com o Cisco Secure - TECSEC-2004

Matthew Robertson, engenheiro técnico de marketing renomado, Cisco Systems, Inc. - palestrante renomado

Hanna Jabbour, engenheira de marketing técnico líder, Cisco Systems, Inc. - Palestrante renomado

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

Matt Vander Horst, Líder Técnico, Cisco - Palestrante Destacado

Começando com o aprofundamento da oferta de detecção e resposta estendida da Cisco, esta sessão fornecerá uma visão completa da implementação e da operação dos vários componentes do produto, incluindo Cisco Secure Endpoint, Secure Cloud Analytics, Umbrella, Meraki e Email Threat Defense e sua operação no Cisco XDR. Também serão incluídas as melhores práticas operacionais e os detalhes de

implementação na operação do mecanismo de resposta, bem como a integração do Cisco XDR com produtos que não sejam da Cisco, como o Crowdstrike Falcon.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de sessão: Seminário técnico
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: Segurança

DevNet

Automação de segurança: Desenvolvendo com SecureX - DEVNET-1083

Matt Vander Horst, Líder Técnico, Cisco - Palestrante Destacado

Você sabia que a plataforma XDR da Cisco tem várias maneiras de automatizar suas operações de segurança e criar integrações poderosas? Os módulos de integração do SecureX permitem que você traga dados de outras plataformas para suas investigações, as APIs do SecureX Threat Response permitem automatizar a forma como você investiga e responde a ameaças, e a orquestração do SecureX permite que você crie fluxos de trabalho poderosos usando um editor de arrastar e soltar códigos, sem restrições. Passe por esta sessão para saber mais sobre cada uma dessas três facetas do SecureX e como você pode usá-las para sobrecarregar suas operações de segurança.

Tipo de sessão: DevNet
Nível técnico: introdutório
Tecnologia: SecureX, segurança

Opção: DevNet

Automatização de operações de ciberhigiene com SecureX e segurança Kenna - DEVLIT-1355

Oxana Sannikova, Arquiteta de soluções técnicas, Cisco Systems, Inc.

As operações de TI ainda são muito manuais hoje. Os clientes são sempre desafiados a manter a integridade do sistema e melhorar a segurança on-line. Nesta rápida sessão, demonstraremos como a orquestração do Cisco SecureX e a Kenna Security podem ser utilizadas para automatizar o gerenciamento de vulnerabilidades.

Tipo de sessão: DevNet
Nível técnico: intermediário
Tecnologia: automação e orquestração, segurança
Opção: DevNet

Usando a orquestração SecureX para automatizar a resposta a incidentes de nuvem pública - DEVWKS-2240

Brian Sak, arquiteto de soluções técnicas, Cisco Systems, Inc. - palestrante renomado

Quando as cargas de trabalho são transferidas para provedores de nuvem pública como AWS, Azure ou GCP, a resposta a incidentes e a correção podem se tornar mais difíceis e exigirão ferramentas diferentes. Esta sessão o guiará pela criação de fluxos de trabalho de orquestração do SecureX que automatizam e simplificam o processo de identificação de ameaças, simplificam procedimentos de resposta e proporcionam

tranquilidade às equipes de secops ao proteger recursos em ambientes de várias nuvens ou de nuvem híbrida. Novo este ano, o lugar do workshop DevNet é o lugar dos participantes pré-registrados. Há apenas 12 laptops disponíveis para esta sessão. Este é um workshop prático do DevNet no qual você escreve códigos junto com um instrutor. Traga seus próprios fones de ouvido com conector auxiliar de 3,5 mm para ouvir o apresentador ou pegue um par de fones de ouvido no Centro de Comando DevNet.
Ao participar deste Workshop DevNet, você estará qualificado para receber créditos do Cisco Continuing Education (CE). Encontre detalhes em: https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de sessão: DevNet
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: DevNet

Dimensionamento de fluxos de trabalho de nuvem híbrida com SecureX Orchestrator e conector remoto - DEVNET-2109

Steve McNutt, arquiteto de soluções técnicas, Cisco Systems, Inc.

Você já deve ter ouvido falar da SecureX Orchestration (SXO) no contexto da orquestração de segurança. Mostraremos que ele pode fazer muito mais e ser a base para a criação de ferramentas eficientes de operações de nuvem híbrida. Esta sessão começa com uma visão geral arquitetônica de alto nível seguida por um passo a passo do exemplo de solução de implantação em massa do Cisco Umbrella, explicando como os componentes se encaixam e os desafios que eles resolvem. Você sairá desta sessão com uma compreensão de como criar fluxos de trabalho de nuvem híbrida altamente escaláveis aproveitando o padrão sidecar e a familiaridade com o código de exemplo que você pode modificar para criar suas próprias soluções.

Tipo de sessão: DevNet
Nível técnico: intermediário
Tecnologia: SecureX, segurança
Opção: DevNet

Fazendo com que o R conte duas vezes no XDR: Como automatizar suas operações de segurança (SecOps) em 10 cliques no Cisco SecureX (sem escrever nenhuma linha de código) - DEVNET-2214

Christopher Van Der Made, Gerente de Produtos de Engenharia, Cisco Systems, Inc. - Palestrante renomado

Esta sessão mostrará como o poder da automação pode ser aproveitado através da SecureX Orchestration sem escrever qualquer código. Isso permitirá que as organizações façam a contagem de R dobrar no XDR (eXtended Detection and Response) da Cisco. Vamos falar sobre alguns exemplos extremamente simples de instalar que farão você chegar ao fim. Usaremos a quantidade de cliques necessários no console como métrica para provar como você pode obter acesso à automação avançada sem muita confusão. No final, você também aprenderá a dar um passo à frente e lentamente tornar-se um mestre na automação de suas operações de segurança. Você terá todo o material depois para começar você mesmo. Essa sessão destina-se a atendentes de incidentes, analistas de segurança, gerentes de SOC ou qualquer pessoa com interesse em automação e segurança.

Tipo de sessão: DevNet
Nível técnico: intermediário
Tecnologia: SecureX, segurança

Opção: DevNet

Integração com a API do Microsoft Graph: usando Python e SecureX - DEVWKS-3260

Hacke Nohre, arquiteto de soluções técnicas, Cisco - palestrante renomado

Neste workshop, discutiremos como a API do Microsoft Graph pode ser integrada em ambientes típicos da Cisco.
Abordaremos uma visão geral de alto nível da API do Microsoft Graph com algum foco na autenticação e autorização do Oauth2 para o Azure AD.
Em seguida, mostraremos como podemos acessar essa API por meio de scripts python e SecureX para acessar informações sobre os grupos e funções do Azure AD para um usuário específico
acessar informações sobre eventos de segurança no ambiente da Microsoft
Os participantes podem tentar seguir as etapas do workshop a partir dos ambientes de laboratório durante o workshop ou podem concluir as etapas posteriormente. Forneceremos ponteiros para configurações de laboratório que permitem que os participantes concluam as tarefas do workshop por conta própria, sem a necessidade de sua própria conta do Azure ou SecureX.

Qualificado para o Crédito de Educação Contínua da Cisco: Sim
Tipo de sessão: DevNet
Nível técnico: Avançado
Tecnologia: DevNet, segurança
Opção: DevNet

Automatize e simplifique sua defesa contra ransomware com o SecureX - DEVNET-1456

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

Os ataques de ransomware estão se concentrando cada vez mais em backups. A proteção, assim como a recuperação rápida e fácil do backup da sua empresa, está se tornando a melhor e mais importante etapa na defesa contra ataques de ransomware debilitantes. Com a ajuda de uma demonstração, realçaremos a versatilidade e a personalização que o SecureX é capaz de fornecer através de seu mecanismo de orquestração. Graças à integração que o Cisco SecureX oferece com soluções de primeira (Cisco Umbrella, Cisco Secure Endpoint) e de terceiros (Cohesity Helios), você poderá reduzir drasticamente o tempo e a complexidade da detecção, investigação e recuperação de ransomware.

Tipo de sessão: DevNet
Nível técnico: introdutório
Tecnologia: SecureX, segurança
Opção: DevNet

Visão geral do produto ou da estratégia

Cisco XDR: prédio para o centro de operações de segurança do futuro - PSOSEC-1007

Sana Sana Yousuf, gerente de marketing de produtos, Cisco Systems, Inc.

As equipes de segurança enfrentam um cenário de ameaças em expansão e um ambiente complexo, o que torna a eficácia da segurança cada vez mais evasiva. A linha de pobreza da segurança digital está se ampliando, e os agentes mal-intencionados estão aproveitando essa brecha para desencadear ataques

persistentes. Acreditamos que apenas uma solução eficaz de "detecção e resposta estendida" pode detectar e corrigir criminosos sofisticados como Turla, Wannacry e NotPetya em seu ambiente. Saiba mais sobre o valor disruptivo do XDR no universo híbrido, de vários fornecedores e vetores. Ouça-me defender um ecossistema em constante crescimento de integrações de tecnologia de vários fornecedores como base para a criação de operações de segurança futuras. E como o XDR pode se tornar um multiplicador de força para seu SOC?

Tipo de sessão: visão geral do produto ou da estratégia
Nível Técnico: Geral
Tecnologia: SecureX, nuvem híbrida, segurança
Opção: Segurança

Como fortalecer proativamente sua resiliência de segurança - PSOCX-2000

Varun Dhingra, Diretor sênior, Gerenciamento de produtos, Segurança e colaboração, Cisco Systems, Inc.
Mark Hammond, diretor de gerenciamento de produtos, Cisco Systems, Inc

Você não só precisa gerenciar a segurança cibernética, mas também enfrenta uma pressão real para adotar regulamentos baseados na privacidade de dados. Como você projeta um programa de segurança digital que atenda aos requisitos em constante mudança de risco, regulamentação, objetivos de negócios e impacto operacional? Nesta sessão, você aprenderá a arquitetar uma estrutura de privacidade e segurança de dados alinhada com o setor para atender às necessidades das partes interessadas e produzir soluções que permitam agilidade comercial. A estrutura foi projetada para rastrear as atividades e os resultados desejados de segurança digital que são intuitivos para permitir uma comunicação simples e não técnica entre equipes multidisciplinares.

Tipo de sessão: visão geral do produto ou da estratégia
Nível técnico: intermediário
Tecnologia: experiência do cliente, SecureX, segurança

Oportunidades adicionais

Junto com os muitos tipos de sessão listados acima, o Live! tem muita inovação e inspiração bem no chão da conferência. Conheça os engenheiros, capture a bandeira ou participe do Desafio, ao vivo! continua a demonstrar como a Cisco é a ponte para o possível. Confira o catálogo completo e mais detalhes em Ciscolive.com.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.