Cisco Live! Secure Endpoint and SecureX Sessions

Contents

Introduction

Cisco Live! Las Vegas is one of premier industry events with over 1100 sessions currently scheduled June 4-8th at the Mandalay Bay Convention Center. With such a large course catalogue, we wanted to make sure our Secure Endpoint customers were aware of the education opportunities to utilize our products and services effectively. Highlighting just a small selection of the 129 available Labs, Breakout Sessions, and Discussions surrounding the topic of Security available this year in Las Vegas, we hope you will consider joining us as we help make the world a more secure place.

Instructor-Led Labs

Cisco Secure Endpoint: Doing it Right by Shifting Left - LTRSEC-1114

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

Endpoint Security is the last wall of defense in the evolving cyber crime landscape and, when configured properly, Cisco Secure Endpoint can keep your organization safe. In this session, you will have hands-on access to the Secure Endpoint Console while you learn deployment configurations and practices for the best security posture from an Engineering Team that has worked with Secure Endpoint (FKA AMP) for the better part of a decade. You will learn the capabilities and functionality of each engine and what environments they can be optimally utilized in. You will know how to set alerts and automations to mitigate an attack in progress so your organization doesn't have to be the next major breach.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Instructor-led Lab
Technical Level: Introductory
Technology: Security
Track: Security

Covering the evolution of email security from secure email gateways to API based platforms - LTRSEC-2011

An email deep dive covering integration of SecureX to get the most out of your XDR deployment.

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

This lab session will overview the newest features of the Cisco Secure Email portfolio. The session will focus on best practices to enable participants to get the most out of their Email platform. Topics for gateway will include using SecureX Cisco Threat Response private intelligence, configuration of Domain-based Message Authentication, Reporting & Conformance (DMARC), advanced logging, API usage and more. Participants will also learn to integrate the gateway into the newer cloud offering Cisco Secure Email Threat Defense. The lab will overview the software as a service offering to hunt for threats such as business email compromise that lack traditional indicators of compromise and investigate potentially compromised accounts.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Instructor-led Lab
Technical Level: Intermediate
Technology: SecureX, Security

Track: Security

Secure Firewall - Threat Defense Data-Path troubleshooting (a practical hands on lab) - LTRSEC-3880

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

One common concern for users of the Cisco Firepower solution is what to do in the event of a network interruption or degradation that appears to be related to the Firepower solution. In this lab participants will learn troubleshooting methodologies for evaluating data-path issues within the Firepower platform including Firepower Series 3 NGIPs, ASA with Firepower Services, Firepower Threat Defense (FTD), and FXOS. This session will provide the participants with a framework to identify which portion of Firepower services is contributing to the problem and how to quickly mitigate issues identified. This framework will cover the entirety of the data-path from packet ingress through deep packet inspection including Snort rule and preprocessor performance. This lab will cover both Snort 2.9 and Snort 3 and the differences between them. This lab will contain troubleshooting scenarios using Virtual Firepower Threat Defense (vFTD) to implement the troubleshooting framework. Additionally, this lab will briefly touch on the SecureX Secure Firewall integration.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Instructor-led Lab
Technical Level: Advanced
Technology: Security
Track: Security

Cyber Resilience Workshop - LTRSEC-1113

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

Is your team prepared for the next supply chain attack or the next zero day? Reality check! We are all under attack, every day and we will all eventually be compromised! For this reason, your organization needs to be Cyber Resilient. Cyber resilience refers to an organization's ability to identify, respond, and recover swiftly from an IT security incident. Building cyber resilience includes making a risk-focused plan that assumes the business will at some point face a breach or an attack. In this lab, you will experience cyber security attacks in an enterprise lab environment where you play attacker and defender and learn, first-hand, why you need highly integrated security solutions and CyberOps skills to be Cyber Resilient.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Instructor-led Lab
Technical Level: Introductory
Technology: SecureX, Security
Track: Security

Breakouts

Troubleshooting and Isolating Performance Issues due to Secure Endpoints(Windows, Linux and MAC) - BRKSEC-2072

Vibhor Amrodia, Technical Leader, Cisco Systems, Inc

Youâ€™ll leave this session with ideas to help you quickly and effectively isolate performance issues with Secure Endpoints installed. This is a deep-dive session on how we can analyze and isolate performance issues on your endpoints(Windows, Linux, and MAC) using some of the logs available with Secure Endpoint and also by using some of the OS-specific utilities and tools. Focus areas for this session would be: Windows CPU and RAM Utilization detection and Isolation Linux CPU and RAM Utilization detection and Isolation MAC CPU and RAM Utilization detection and Isolation

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: Security
Track: Security

Cisco's Unified Agent: Cisco Secure Client. Bringing AMP, AnyConnect, Orbital & Umbrella together - BRKSEC-2834

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

We have all heard the complaints or did the complaining ourselves: "Cisco has too many agents".

Come learn from Aaron Woland, CCIE #20113 and Cisco Live Distinguished Speaker Hall of Fame Elite; while he shows you that Cisco listened to the complaints and has delivered the first iteration of a unified security agent: Cisco Secure Client.

Cisco Secure Client (CSC) provides a modular framework allowing for AnyConnect VPN, Cisco Secure Endpoint (formerly AMP for Endpoints), Network Visibility Module, Umbrella Cloud Security, ISE Posture, Secure Firewall Posture (formerly Hostscan) and the Network Access Module (NAM) to all exist together; with a modern cloud-based management coming from SecureX - connected intimately with SecureX device insights.

In this session, we will dive into the technology behind the Secure Client, how things really work and how they do not. We will cover deployments models from the cloud and using your own software deployment mechanisms. We will learn all about the seamless upgrade flows from existing AnyConnect and Secure Endpoint (AMP) agents. We will talk about scenarios where it makes sense to upgrade to CSC and scenarios where it truly benefits you to stay with the existing AnyConnect and Secure Endpoint (AMP) agents - at least for now.

Come spend some time with Aaron & be entertained while learning all about this exciting development from Cisco Security.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

From Ship to Shore: Integrations, Collaboration, and (Securely) Taking Control Beyond the Cisco Secure Email Gateway - BRKSEC-2288

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

Cisco Secure Email integrates outside of being its own mail gateway. Security, logging, API & configuration, and SecureX - we will walk you through how email extends beyond the gateway and feasibly

making the most of your environment, large or small!

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Cisco's Malware Defense Cloud and Secure Malware Analytics Integrations - BRKSEC-2242

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

You may have known it as "AMP Cloud and Threat Grid", but they've been rebranded as the Malware Defense Cloud and Secure Malware Analytics. This session will review and take a dive deep into the Malware Defense Cloud and Malware Analytics offerings while covering their integrations with Cisco security architectures, including Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella and Meraki. These products work together, and we will be covering the Malware Defense Architecture and demonstrate how all of the pieces fit together to provide the industry leading Advanced Threat Architecture. This session is perfect for those who are newer to the Cisco Security Suite, as well as those customers who own one or more products and want to go deeper into how they work together.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Cisco XDR with Firewall - BRKSEC-2090

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

SecureX, Cisco's XDR, is the broadest most integrated platform in the world. In this session attendees will see the power of Firewall and SecureX integration. This includes Firewall incidents in SecureX, Firewall enrichment to threat response investigations, and SecureX orchestration using Firewall API's. Attendees should have a basic understanding of Cisco Secure Firewall. Attendees do not require knowledge of SecureX.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Accelerate your SOC with Cisco SecureX - BRKSEC-1023

Matt Vander Horst, Technical Leader, Cisco - Distinguished Speaker

Did you know that Cisco's XDR platform SecureX can accelerate how your organization investigates and responds to incidents? SecureX combines a suite of features that allow you to take charge of security incidents, gain better visibility across a wide portfolio of products, and use automation to investigate and respond at machine speed. In this session, you will get an introduction to SecureX and learn the basics of its

various features including: the SecureX dashboard, threat response, incident manager, orchestration, device insights, and secure client. We'll also share a list of other sessions you can attend for deeper dives into these features and more.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Introductory
Technology: SecureX, Security
Track: Security

Cisco XDR with Email: Protect, Analyze and Evolve the SMTP Conversation - BRKSEC-2095

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

Email is known as the weakest link in a business network and in less than two minutes provides hackers and actors an open door leading to a compromise or breach. Email is a primary vector for malware infection because it effortlessly puts malicious payloads in front of the user and is only one click away from exploitation. Beyond just delivering malware, attackers are more sophisticated than ever at crafting and generating phishing links that look just like the services they are impersonating. Cisco Secure Email is evolving how eXtended Detection and Response targets these threat vectors and secures your SMTP conversations.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Extended Detection with Cisco XDR: Security analytics across the enterprise - BRKSEC-2178

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

Extended Detection and Response (XDR) is a popular buzzword today. Demystifying the topic, this session will explore the extended detection and analytics capabilities of Cisco's XDR with specific focus on how to extend your detection capabilities and accelerate your response. Covering multiple detection technologies, including endpoint, network analytics and firewall this session will explore how analytics can bring these detections together and deliver on the XDR objective.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Cisco IT Security from A-Z. Advanced Malware Protection to Zero Trust - BRKCOC-2620

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

Doing the impossible: Cisco increased security and improved experience, in one movement, by introducing Zero Trust for the Workforce. This session will dive into the details of the secure Zero Trust authentication flow, how we benefited from aligning the new flow with a better experience, and how we rolled out endpoint configurations to support Zero Trust using Jamf Pro, InTune/SCCM, and Meraki Systems Manager.
This session will also dive into how Cisco IT implements and maintains Cisco Secure Endpoint in their fleet of 200k+ devices.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: Hybrid Work, Security
Track: Cisco on Cisco

Cisco SecureX XDR - Making sense of all the parts & pieces - BRKSEC-2113

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

eXtended Detection and Response (XDR) is one of the hottest security technologies in the market, and it is seeing tremendous growth in adoption. Given the broad range of what can-be, should-be, and is done in an XDR solution, there is naturally a lot of complexity which can lead to confusion about how/what is happening behind the scenes. This session will shed light into the inner-workings of Ciscoâ€™s incredibly capable XDR solution, with Network Detection & Response, Endpoint Detection & Response, Email Threat Defense, Malware Analytics, Unified Security Agent; and how all these parts and pieces come together to produce the outcome expected of an XDR.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Leveraging Cisco's XDR solution with IT Service Management (ITSM) and SIEM Systems for Incident Investigation - BRKSEC-2122

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

In this session we will show how eXtended Detection and Response (XDR) platform, SecureX, can augment security operations to deliver a better outcome without creating additional complexity. We will look at the following use cases: leveraging context from IT Service Management (ITSM) and SIEM in threat hunting, adding consolidated threat visibility to ITSM incidents and SIEM alerts, formalizing incident response procedures by leveraging automation and orchestration. Almost half of the session will be demonstrations. The ITSM and SIEM solutions covered will include ServiceNow, Jira and Splunk, and attendees will walk away with ready to use workflows.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: Automation & Orchestration, Security
Track: Security

Integrating Open Source Zeek and Cisco XDR - BRKSEC-2075

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

Extended Detection and Response (XDR) solutions offer the potential to protect organizations from cyber security events by detecting and responding faster and reducing risk and exposure. An XDR must include 3rd party integrations to provide additional detection engines. This session will introduce open source Zeek and provide actionable details of how to integrate into Cisco XDR to improve customer security outcomes.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

The Power of GraySkull! Adversarial Emulation - BRKSEC-2180

Jason Maynard, Field CTO Cybersecurity Canada, CSS

In this session we will learn about adversarial emulation and how both red and blue teams can benefit from it use. We learn about the tools available to us and then build out an operation leveraging Caldera without preventive capabilities. We will then review the adversarial outcomes which includes reviewing the outcomes on our passively deployed Cisco Security portfolio. The knowledge gained ensures defensive teams understand the opportunity to increase our defenses. We will then turn on our preventive capabilies across a variety of Cisco security technologies and perform the test again reviewing the results. Understanding how the adversarial approaches their victim and defendersâ€™ ability to layer defense is a recipe for success.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

An Introduction to Risk-Based Vulnerability Management - BRKSEC-1639

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

Risk-Based Vulnerability Management (RBVM) encompasses more than you probably think. In this entertaining and informative talk, we will deep dive into the foundational concepts and underlining theories of quantifying risk and then share how practical RBVM programs are essential to secure the modern network. We will then discuss how Kenna brings RBVM to a wide array of Cisco products and offerings.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Breakout
Technical Level: Introductory
Technology: SecureX, Security
Track: Security

Interactive Breakout

Leveraging SecureX with Cisco Talos Incident Response - IBOSEC-2011

Joe Schumacher, Incident Commander, Cisco Systems, Inc.

Participants will learn directly from our Cisco Talos Incident Response (Talos IR) team on how to leverage SecureX to accelerate response efforts during a security incident. They will gain insight on how SecureX can be utilized whether working with an outside incident response company like Talos IR or conducting an internal investigative response. The session will be constructed around a staged phone call into the Talos IR hotline by a fictitious retainer customer with multiple Cisco security products. The Talos IR team will engage to establish objectives on response and gain background information before moving into emergency response activities, which will include using SecureX along with other security products until the incident has been contained.
The goals for the session will be to inform that participant in the following areas:
Incorporating SecureX to connect observables for the teams to collaborate and work through the investigation
Integrating SecureX with security products to orchestrate a timely and effective response

Session Type: Interactive Breakout
Technical Level: Introductory
Technology: SecureX, Security
Track: Security

Dig Into SecureX Idea Exchange - IBOSEC-2005

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

Explore and exchange ideas on utilizing SecureX with Cisco Security and third party tools in an interactive session where we discuss building and connecting various services. Bring your ideas and questions or learn from others that have already begun their SecureX journey.

Session Type: Interactive Breakout
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Walk-In Labs

Cisco Secure Client and SecureX Device Insights - better together - LABSEC-2776

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

The Cisco Secure Client is a new unified client that brings most Cisco endpoint clients under one umbrella. Cisco Secure Client comprises standard AnyConnect modules and security clients such as AMP (AKA Cisco Secure Endpoint) and Orbital. As part of this LAB, you will learn how to deploy and manage Cisco Secure Client from the SecureX Cloud. The part dedicated to the SecureX Devicse Insights will demonstrate how Cisco Secure Client and its modules can be used for enterprise-level assets management and investigation of security incidents.

Session Type: Walk-in Lab
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Technical Seminars

Cisco Secure Client: from AnyConnect to comprehensive Client Security! - TECSEC-2780

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

The new hybrid workforce, complex attack scenarios, rapid cloud adoption and the pervasiveness of encryption on the internet has made client security more important than ever!
In this 4-hour session we will show how we can expand AnyConnect (VPN) into full featured Endpoint Security. We will drill down into technical aspects of Cisco Secure Client modules including:
EDR/EPP (Secure Endpoint)
Endpoint Network Telemetry (Network Visibility Module)
DNS/Web protection (Umbrella)
Endpoint Posture (ISE/Secure Firewall)
and into the outcomes of running a single client centrally managed in Cisco SecureX (XDR).
The intended audience are Network and Security Engineers and Architects with an interest in endpoint security. Some knowledge of endpoint security, operating systems and common attack vectors is assumed.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Technical Seminar
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

Extended Detection and Response with Cisco Secure - TECSEC-2004

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

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

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

Matt Vander Horst, Technical Leader, Cisco - Distinguished Speaker

Beginning with deep dive into Cisco's Extended Detection and Response offer this session will provide a complete walkthrough of the implementation and operation of the varying product components, including Cisco Secure Endpoint, Secure Cloud Analytics, Umbrella, Meraki and Email Threat Defence and their operation in Cisco XDR. Also included will be operational best practices and implementation details in the operation of the response engine as well as the integration of Cisco XDR with non Cisco products such as Crowdstrike Falcon.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: Technical Seminar
Technical Level: Intermediate
Technology: SecureX, Security
Track: Security

DevNet

Security Automation: Developing with SecureX - DEVNET-1083

Matt Vander Horst, Technical Leader, Cisco - Distinguished Speaker

Did you know that Cisco's XDR platform has multiple ways you can automate your security operations and build powerful integrations? SecureX integration modules allow you to bring data from other platforms into your investigations, SecureX Threat Response APIs allow you to automate how you investigate and respond to threats, and SecureX orchestration allows you to build powerful workflows using a no-to-low code drag and drop editor. Stop by this session to learn more about each of these three facets of SecureX and how you can use them to supercharge your security operations.

Session Type: DevNet
Technical Level: Introductory
Technology: SecureX, Security

Track: DevNet

Automating Cyber Hygiene Operations with SecureX and Kenna Security - DEVLIT-1355

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

IT operations are still very manual today. Customers are always challenged to maintain system health and improve online security. In this quick session we will demonstrate how Cisco SecureX orchestration and Kenna Security can be leveraged to automate vulnerability management.

Session Type: DevNet
Technical Level: Intermediate
Technology: Automation & Orchestration, Security
Track: DevNet

Using SecureX orchestration for Automating Public Cloud Incident Response - DEVWKS-2240

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

When workloads move into public cloud providers like AWS, Azure, or GCP, incident response and remediation can become more difficult and will require different tools. This session will guide you through creating SecureX orchestration workflows that automate and simplify the process of threat identification, simplify response procedures, and give secops teams peace of mind when securing resources in multi-cloud or hybrid-cloud environments.
New this year DevNet workshop seating is pre-registered attendees are seated first. There are only 12 laptops available for this session. This is a hands-on DevNet Workshop where you code along with an instructor. Bring your own 3.5mm aux connector headphones to hear the presenter or pick up a pair of headphones at the DevNet Command Center.
By attending this DevNet Workshop, you will be eligible to earn Cisco Continuing Education (CE) Credits. Find details at: https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: DevNet
Technical Level: Intermediate
Technology: SecureX, Security
Track: DevNet

Scaling Hybrid Cloud Workflows with SecureX Orchestrator and Remote Connector - DEVNET-2109

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

You may have heard of SecureX Orchestration (SXO) in the context of security orchestration. We will show you it can do a lot more, and be a foundation for creating effective hybrid cloud operations tools. This session starts with a high-level architectural overview followed by a walk-through of the example solution of mass deploying Cisco Umbrella, explaining how the components fit together and the challenges they solve. You'll leave this session with an understanding of how to build highly scalable hybrid cloud workflows by leveraging the sidecar pattern, and familiarity with example code that you can modify to build your own solutions.

Session Type: DevNet
Technical Level: Intermediate
Technology: SecureX, Security
Track: DevNet

Making the R count double in XDR: How to Automate your Security Operations (SecOps) within 10 Clicks in Cisco SecureX (without Writing any Line of Code) - DEVNET-2214

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

This session will show how the power of automation can be leveraged through SecureX Orchestration without writing any code. This will enable organizations to make the R count double in Cisco's XDR (eXtended Detection and Response). We will walk through a couple of extremely simple to install examples that will make you hit the ground running. We will use the amount of clicks that are needed in the console as metric, to prove you how you can get access to powerful automation without too much hasle. At the end, you will also learn how to take this a step further and slowly become a master at automation your security operations. You will get all of the materials afterwards to get started yourself. This session is meant for incident responders, security analysts, SOC managers, or anyone with interest in automation and security.

Session Type: DevNet
Technical Level: Intermediate
Technology: SecureX, Security
Track: DevNet

Integrating with Microsoft Graph API: Using Python and SecureX - DEVWKS-3260

Hacke Nohre, Technical Solutions Architect, Cisco - Distinguished Speaker

In this workshop we will discuss how the Microsoft Graph API can be integrated in typical Cisco environments.
We will cover a high-level overview of the Microsoft Graph API with some focus on Oauth2 authentication and authorization to Azure AD.
We will then show how we can access this API via both python scripts and SecureX to access information about the Azure AD groups and roles for a specific user
access information about security events from the Microsoft environment
The attendees can attempt to follow the steps in the workshop from the lab environments during the workshop, or they can complete the steops later. We will provide pointers to lab setups that allow attendees to complete the workshop tasks on their own, without the need for their own Azure or SecureX account.

Qualifies for Cisco Continuing Education Credit: Yes
Session Type: DevNet
Technical Level: Advanced
Technology: DevNet, Security
Track: DevNet

Automate and Simplify Your Ransomware Defense with SecureX - DEVNET-1456

Elia Maracani, System Engineer, Cisco Systems, Inc.

Ransomware attacks are increasingly focusing on backups. Protecting, as well as quickly and easily recovering your company's backup, is thus becoming the best and most important step in defending against debilitating ransomware attacks. With the help of a demo, we will be highlighting the versatility and customisation that SecureX is able to provide via its orchestration engine. Thanks to the integration that Cisco SecureX provides with both 1st (Cisco Umbrella, Cisco Secure Endpoint) and 3rd party solutions (Cohesity Helios) you will be able to drastically reduce the time and complexity of ransomware detection, investigation and recover.

Session Type: DevNet
Technical Level: Introductory
Technology: SecureX, Security
Track: DevNet

Product or Strategy Overview

Cisco XDR: Building for the Security Operations Center of Tomorrow - PSOSEC-1007

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

Security teams face an expanding threat landscape and a complex environment-making security efficacy increasingly elusive. The cybersecurity poverty line is widening, and malicious actors are taking advantage of this gaping hole to unleash persistent attacks. We believe that only an effective 'Extended Detection and Response' solution can detect and remediate sophisticated adversaries like Turla, Wannacry and NotPetya in your environment. Learn about the disruptive value of XDR in the hybrid, multi-vendor, multi-vector universe. Hear me make a case for a continually growing ecosystem of multivendor technology integrations as a foundation for building tomorrow's security operations. And how XDR can become a force multiplier for your SOC?

Session Type: Product or Strategy Overview
Technical Level: General
Technology: SecureX, Hybrid Cloud, Security
Track: Security

How to Proactively Strengthen Your Security Resilience - PSOCX-2000

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

You not only have to manage cybersecurity, but you also face real pressure to adopt regulations based on data privacy. How do you design a cybersecurity program that meets the ever changing requirements of risk, regulation, business objectives, and operational impact? In this session, youâ€™ll learn how to architect an industry-aligned data security and privacy framework to meet stakeholder needs and produce solutions that

enable business agility. The framework is designed to track desired cybersecurity activities and outcomes that are intuitive to enable simple, non-technical communication between multi-disciplinary teams.

Session Type: Product or Strategy Overview
Technical Level: Intermediate
Technology: Customer Experience, SecureX, Security

Additional Opportunities

Along with the many session types listed above, Live! has a lot of innovation and inspiration right on the conference floor. Meet the Engineers, Capture the Flag, or take the Challenge, Live! continues to demonstrate how Cisco is the bridge to possible. Check out the full catalogue and more details at Ciscolive.com.