Cisco Live! 보안 엔드포인트 및 SecureX 세션

목차

소개

Cisco Live! 라스베이거스는 만달레이 베이 컨벤션 센터에서 오는 6월 4일부터 8일까지 1100여 개 세션이 예정된 업계 최고의 행사 중 하나입니다. 이러한 대규모 교육 과정 카탈로그를 통해 Cisco의 Secure Endpoint 고객이 Cisco 제품과 서비스를 효과적으로 활용할 수 있는 교육 기회를 인지하고 있는지 확인하고자 했습니다. Las Vegas에서 올해 사용할 수 있는 보안 주제를 둘러싼 129개 랩, 브레이크아웃 세션 및 토론 중에서 몇 가지만 강조하면서, Cisco가 세상을 더 안전한 곳으로 만드는 데 도움을 주므로 여러분도 함께 참여해 주시기 바랍니다.

강의식 랩

Cisco Secure Endpoint: Doing it Right by Shifting Left - LTRSEC-114

Caly Hess, Security PrincessX, Cisco Systems, Inc.
Pedro Medina, 소프트웨어 엔지니어, Cisco Systems, Inc.

엔드포인트 보안은 진화하는 사이버 범죄 환경의 마지막 방어벽입니다. Cisco Secure Endpoint를 적절히 구성하면 조직을 안전하게 지킬 수 있습니다. 이 세션에서는 FKA AMP(Secure Endpoint)와 10년 동안 협업한 엔지니어링 팀에서 Secure Endpoint Console에 대한 실습 및 구축 컨피그레이션을 익히고 최상의 보안 상태에 대한 사례를 학습합니다. 각 엔진의 기능과 각 엔진을 최적의 상태로 활용할 수 있는 환경에 대해 알아봅니다. 조직이 다음 주요 보안 침해가 될 필요가 없도록 진행 중인 공격을 완화할 수 있도록 경고와 자동화를 설정하는 방법을 알고 있을 것입니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 강의식 랩
기술 수준: 소개
기술: 보안
트랙: 보안

보안 이메일 게이트웨이에서 API 기반 플랫폼으로의 이메일 보안 발전 소개 - LTRSEC-2011

XDR 구축을 최대한 활용하기 위해 SecureX의 통합을 다룬 이메일 심층 분석

Alberto Torralba, Technical Solutions Architect.Sales, Cisco Systems, Inc.
Greg Barnes, Cisco Systems, Inc. 기술 마케팅 엔지니어

이 실습 세션에서는 Cisco Secure Email 포트폴리오의 최신 기능을 개괄적으로 살펴봅니다. 이 세

션에서는 참가자가 이메일 플랫폼을 최대한 활용할 수 있도록 하는 모범 사례에 초점을 둡니다. 게이트웨이에 대한 항목에는 SecureX Cisco Threat Response 프라이빗 인텔리전스 사용, 도메인 기반 DMARC(Message Authentication, Reporting & Conformance) 구성, 고급 로깅, API 사용 등이 포함됩니다. 또한 참가자는 Cisco Secure Email Threat Defense를 제공하는 최신 클라우드에 게이트웨이를 통합하는 방법을 배웁니다. 이 랩에서는 SaaS(Software as a Service) 솔루션을 개괄적으로 살펴보면서 기존의 보안 침해 지표가 없는 비즈니스 이메일 보안 침해와 같은 위협을 추적하고 보안 침해 가능성이 있는 계정을 조사합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 강의식 랩
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

보안 방화벽 - Threat Defense 데이터 경로 문제 해결(실습 랩) - LTRSEC-3880

John Groetzinger, 기술 리더, Cisco Systems, Inc
Foster Lipkey, Cisco Systems, Inc. 수석 엔지니어 - Distinguished Speaker
Vidhi Mujumdar, Cisco Systems, 고객 딜리버리 리더

Cisco Firepower 솔루션 사용자의 공통적인 관심사 중 하나는 Firepower 솔루션과 관련된 것으로 보이는 네트워크 중단 또는 성능 저하 시 수행할 작업입니다. 이 실습에서는 Firepower Series 3 NGIP, ASA with Firepower Firepower Services, FTD(Domain Threat Defense) 및 FXOS를 비롯한 Firepower 플랫폼 내에서 데이터 경로 문제를 평가하기 위한 문제 해결 방법을 학습합니다. 이 세션에서는 Firepower 서비스의 어떤 부분이 문제에 기여하고 있는지 파악하고 확인된 문제를 신속하게 완화하는 방법을 제시하는 프레임워크를 참가자에게 제공합니다. 이 프레임워크는 패킷 인그레스(ingress)부터 Snort 규칙 및 프리프로세서 성능을 비롯한 심층 패킷 검사까지 데이터 경로 전체를 다룹니다. 이 Lab에서는 Snort 2.9와 Snort 3의 차이점을 모두 다룹니다. 이 실습에는 트러블슈팅 프레임워크를 구현하기 위해 vFTD(Virtual Firepower Threat Defense)를 사용하는 트러블슈팅 시나리오가 포함됩니다. 또한 이 실습에서는 SecureX Secure Firewall 통합에 대해 간단히 설명합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 강의식 랩
기술 레벨: 고급
기술: 보안
트랙: 보안

Cyber Resilience 워크숍 - LTRSEC-1113

Ron Taylor, Sr Security Lab Test Monkey, Cisco Systems, Inc.
Leo Cruz, Cisco Systems, Inc. 기술 솔루션 설계자

여러분의 팀은 다음 공급망 공격 또는 다음 제로데이 공격에 대비하고 있습니까? 현실 확인! 우리 모두는 매일 공격을 받고 있으며 결국 모두 피해를 입게 됩니다! 이러한 이유로 인해 여러분의 조직은 사이버 레질리언스가 필요합니다. Cyber resilience는 IT 보안 사고를 신속하게 식별, 대응, 복구할 수 있는 조직의 능력을 의미합니다. 사이버 레질리언스를 구축하려면 어떤 시점에서는 보안 침해 또는 공격에 직면할 것으로 가정한 위험 중심의 계획을 수립해야 합니다. 이 실습에서는 공격자

와 방어자 역할을 수행하는 엔터프라이즈 실습 환경에서 사이버 보안 공격을 경험하며, Cyber Resilient를 위해 고도로 통합된 보안 솔루션과 CyberOps 기술이 필요한 이유를 직접 학습합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 강의식 랩
기술 수준: 소개
기술: SecureX, 보안
트랙: 보안

브레이크아웃

보안 엔드포인트로 인한 성능 문제 해결 및 격리(Windows, Linux 및 MAC) - BRKSEC-2072

Vibhor Amrodia, 기술 리더, Cisco Systems, Inc

이 세션에서는 Secure Endpoints가 설치된 상태에서 성능 문제를 신속하고 효과적으로 격리하는 데 도움이 되는 아이디어를 제공합니다. 이 세션에서는 Secure Endpoint에서 사용할 수 있는 로그 중 일부와 OS 관련 유틸리티 및 툴을 사용하여 엔드포인트(Windows, Linux, MAC)의 성능 문제를 분석하고 격리하는 방법에 대해 심층적으로 설명합니다. 이 세션의 중점 영역은 다음과 같습니다. Windows CPU 및 RAM 사용률 탐지 및 격리 Linux CPU 및 RAM 사용률 탐지 및 격리 MAC CPU 및 RAM 사용률 탐지 및 격리

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: 보안
트랙: 보안

Cisco Unified Agent: Cisco Secure Client. AMP, AnyConnect, Orbital 및 Umbrella 결합 - BRKSEC-2834

Aaron Woland, Cisco Systems, Inc. - Distinguished Speaker

우리는 모두 불만을 들었거나 스스로 불만을 제기했습니다. "Cisco는 상담원이 너무 많다."

CCIE #20113 및 Cisco Live Distinguished Speaker Hall of Fame Elite인 Aaron Woland에게 Cisco가 불만 사항을 듣고 통합 보안 에이전트의 첫 번째 버전인 Cisco Secure Client를 제공했음을 알려드립니다.

Cisco Secure Client(CSC)는 AnyConnect VPN, Cisco Secure Endpoint(이전 AMP for Endpoints), Network Visibility Module, Umbrella Cloud Security, ISE Posture, Secure Firewall Posture(이전 Hostscan) 및 Network Access Module(NAM)을 지원하는 모듈형 프레임워크를 제공하며, SecureX에서 제공하는 최신 클라우드 기반 관리 기능과 SecureX 장치 인사이트를 통해 긴밀하게 연결됩니다.

이 세션에서는 Secure Client의 이면에 있는 기술, 실제 작동 방식 및 작동 방식에 대해 자세히 살펴

보겠습니다. 클라우드의 구축 모델과 자체 소프트웨어 구축 메커니즘을 사용하는 방법에 대해 살펴보겠습니다. 기존 AnyConnect 및 AMP(Secure Endpoint) 에이전트의 원활한 업그레이드 흐름에 대한 모든 내용을 알아보겠습니다. CSC로 업그레이드하는 것이 적절한 시나리오와 적어도 현재로서는 기존 AnyConnect 및 AMP(Secure Endpoint) 에이전트를 유지하는 것이 진정으로 도움이 되는 시나리오에 대해 설명하겠습니다.

Aaron과 함께 시간을 보내고 Cisco Security에서 이러한 흥미로운 개발에 대해 모두 알아보며 즐거움을 만끽하십시오.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

From Ship to Shore: Cisco Secure Email Gateway - BRKSEC-2288을 뛰어넘는 통합, 협업 및 (안전한) 제어

Robert Sherwin, 기술 리더, Cisco Systems, Inc. - 뛰어난 연사

Cisco Secure Email은 자체 메일 게이트웨이가 아닌 통합됩니다. 보안, 로깅, API 및 컨피그레이션, SecureX - 이메일이 게이트웨이를 넘어 확장되고 규모와 상관없이 귀사의 환경을 최대한 활용하는 방법을 안내해 드립니다!

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

Cisco의 Malware Defense 클라우드 및 보안 악성코드 분석 통합 - BRKSEC-2242

Bill Yazji, Cisco Systems 기술 보안 설계자 - DSE

"AMP Cloud and Threat Grid"로 알고 있을 수 있지만 Malware Defense Cloud and Secure Malware Analytics로 다시 브랜드화되었습니다. 이 세션에서는 Secure Email, Secure Web, Secure Firewall, Secure Endpoint, Umbrella 및 Meraki를 비롯한 Cisco 보안 아키텍처와의 통합에 대해 살펴보면서 Malware Defense 클라우드 및 Malware Analytics 제품을 심층적으로 살펴봅니다. 이 제품들은 함께 작동하며, Cisco는 Malware Defense Architecture를 다루며 이 모든 요소가 어떻게 조화를 이루는지 시연하여 업계 최고의 지능형 위협 아키텍처를 제공할 것입니다. 이 세션은 Cisco Security Suite를 처음 사용하는 고객과 하나 이상의 제품을 보유하고 있으며 함께 일하는 방식에 대해 자세히 살펴보고자 하는 고객에게 적합합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간

기술: SecureX, 보안
트랙: 보안

Cisco XDR with Firewall - BRKSEC-2090

Eric Kostlan, Cisco Systems, Inc. 기술 마케팅 엔지니어 - 발표자
Adi Sankar, Cisco Systems, Inc. 기술 마케팅 엔지니어

Cisco의 XDR인 SecureX는 세계에서 가장 광범위한 통합 플랫폼입니다. 이 세션에서는 방화벽 및 SecureX 통합의 장점을 살펴봅니다. 여기에는 SecureX에서의 방화벽 사고, 위협 대응 조사에 대한 방화벽 강화, 방화벽 API를 사용한 SecureX 오케스트레이션 등이 포함됩니다. 참석자는 Cisco Secure Firewall에 대해 기본적으로 알고 있어야 합니다. 참석자는 SecureX에 대한 지식이 필요하지 않습니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

Cisco SecureX - BRKSEC-1023으로 SOC 가속화

Matt Vander Horst, 기술 리더, Cisco - Distinguished Speaker

Cisco의 XDR 플랫폼 SecureX를 통해 더 신속하게 사고를 조사하고 대응할 수 있다는 사실을 알고 계십니까? SecureX는 보안 사고를 담당하고, 광범위한 제품 포트폴리오에 더 나은 가시성을 확보하고, 자동화를 사용하여 시스템 속도로 조사하고 대응할 수 있는 일련의 기능을 통합합니다. 이 세션에서는 SecureX에 대해 소개하고 SecureX 대시보드, 위협 대응, 인시던트 관리자, 오케스트레이션, 장치 인사이트, 보안 클라이언트 등 다양한 기능의 기초를 학습합니다. 또한 이러한 기능에 대한 자세한 내용을 살펴보기 위해 참석하실 수 있는 다른 세션 목록도 공유해 드리겠습니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 수준: 소개
기술: SecureX, 보안
트랙: 보안

Cisco XDR with Email: SMTP 대화 보호, 분석 및 발전 - BRKSEC-2095

Robert Sherwin, 기술 리더, Cisco Systems, Inc. - 뛰어난 연사

이메일은 비즈니스 네트워크에서 가장 취약한 링크로 알려져 있으며, 2분 이내에 해커와 공격자에게 보안 침해 또는 보안 침해로 이어질 수 있는 열린 문을 제공합니다. 이메일은 사용자 앞에 악성 페이로드를 쉽게 전달하며 익스플로잇에서 단 한 번의 클릭만으로 벗어나기 때문에 악성코드 감염의 주요 벡터입니다. 공격자는 단순히 악성코드를 전달하는 수준을 넘어 모방 서비스처럼 보이는 피싱 링크를 만들고 생성하는 방법을 그 어느 때보다도 교묘하게 사용하고 있습니다. Cisco Secure

Email은 eExtend Detection and Response가 이러한 위협 벡터를 대상으로 하고 SMTP 대화를 보호하는 방식을 발전시키고 있습니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

Cisco XDR을 통한 확장 감지: 기업 전체의 보안 분석 - BRKSEC-2178

Matthew Robertson, Cisco Systems, Inc. - Distinguished Speaker

XDR(Extended Detection and Response)은 오늘날 널리 사용되는 유행어입니다. 이 세션에서는 이 주제를 명확하게 설명하면서 탐지 기능을 확장하고 대응 속도를 높이는 방법에 초점을 맞추어 Cisco XDR의 확장된 탐지 및 분석 기능을 살펴봅니다. 이 세션에서는 엔드포인트, 네트워크 분석 및 방화벽을 비롯한 여러 탐지 기술을 다루면서 분석을 통해 이러한 탐지 기술을 통합하고 XDR 목표를 실현하는 방법을 살펴봅니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

A-Z의 Cisco IT 보안 Advanced Malware Protection을 통한 제로 트러스트(Zero Trust) - BRKCOC-2620

Steve Vida, Cisco Systems, Inc. 사이버 보안 설계자
Gil Daudistel, Cisco Systems, Inc. 정보 보안 매니저

불가능한 일 처리: Cisco는 Zero Trust for the Workforce를 도입하여 보안과 경험을 한 단계 향상시켰습니다. 이 세션에서는 안전한 Zero Trust 인증 플로우에 대한 세부 사항, 더 나은 환경과 새로운 플로우를 연결함으로써 어떤 이점을 얻었는지, Jamf Pro, InTune/SCCM 및 Meraki Systems Manager를 사용하여 Zero Trust를 지원하기 위해 엔드포인트 컨피그레이션을 롤아웃한 방법에 대해 살펴봅니다.
또한 이 세션에서는 Cisco IT가 20만 대 이상의 장치에서 Cisco Secure Endpoint를 구현하고 유지 관리하는 방법에 대해 자세히 살펴봅니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: 하이브리드 업무, 보안
트랙: Cisco on Cisco

Cisco SecureX XDR - 모든 부품과 요소를 이해합니다 - BRKSEC-2113

Aaron Woland, Cisco Systems, Inc. - Distinguished Speaker

XDR(eExtended Detection and Response)은 시장에서 가장 주목받는 보안 기술 중 하나이며, 도입이 폭발적으로 증가하고 있습니다. 무엇이 될 수 있고, 있어야 하며, XDR 솔루션으로 수행되는 광범위한 범위를 고려하면 당연히 복잡성이 커져 배후에서 어떻게/무엇이 일어나고 있는지에 대한 혼란이 생길 수 있습니다. 이 세션에서는 네트워크 탐지 및 대응, 엔드포인트 탐지 및 대응, 이메일 위협 방어, 악성코드 분석, Unified Security Agent를 비롯한 Cisco의 뛰어난 기능을 갖춘 XDR 솔루션의 내적 기능과 이러한 모든 요소와 요소를 결합하여 XDR의 결과를 어떻게 생성할지 조명합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

Cisco의 XDR 솔루션과 ITSM(IT Service Management) 및 SIEM Systems를 활용하여 사고 조사 - BRKSEC-2122

Oxana Sannikova, 기술 솔루션 설계자, Cisco Systems, Inc.

이 세션에서는 XDR(eXtended Detection and Response) 플랫폼인 SecureX가 어떻게 보안 운영을 강화하여 복잡성을 늘리지 않으면서 더 나은 결과를 제공하는지 살펴봅니다. ITSM(IT Service Management) 및 SIEM의 컨텍스트를 위협 헌팅에 활용하고, ITSM 사고 및 SIEM 알림에 통합된 위협 가시성을 추가하고, 자동화 및 오케스트레이션을 활용하여 사고 대응 절차를 공식화하는 사용 사례를 살펴보겠습니다. 세션의 거의 절반이 데모가 될 것이다. 지원되는 ITSM 및 SIEM 솔루션에는 ServiceNow, Jira 및 Splunk가 포함되며, 참석자는 즉시 사용 가능한 워크플로우를 사용할 수 있습니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: 자동화 및 오케스트레이션, 보안
트랙: 보안

오픈 소스 Zeek 및 Cisco XDR 통합 - BRKSEC-2075

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

XDR(Extended Detection and Response) 솔루션은 더 신속하게 탐지하고 대응하며 위험과 노출을 줄여 사이버 보안 사건으로부터 조직을 보호할 수 있는 잠재력을 제공합니다. XDR에는 추가 탐지 엔진을 제공하기 위해 서드파티 통합이 포함되어야 합니다. 이 세션에서는 오픈 소스 Zeek를 소개하고 Cisco XDR에 통합하여 고객 보안 성과를 개선하는 방법에 대한 실행 가능한 세부 정보를 제공합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간

기술: SecureX, 보안
트랙: 보안

그레이 스컬의 힘! 대립적 에뮬레이션 - BRKSEC-2180

Jason Maynard, Field CTO Cybersecurity 캐나다, CSS

이 세션에서는 공격자 에뮬레이션에 대해 알아보고 레드 팀과 블루 팀 모두 어떻게 이를 활용할 수 있는지 알아봅니다. Cisco에서 사용 가능한 툴에 대해 알아본 다음 예방 기능 없이 Caldera를 활용하여 운영을 구축합니다. 그런 다음 수동으로 배포된 Cisco 보안 포트폴리오에 대한 결과를 검토하는 등 적대적 결과를 검토합니다. 이렇게 얻은 지식은 방어 팀이 Cisco 방어 체계를 강화할 수 있는 기회를 제대로 이해하도록 보장합니다. 그런 다음 다양한 Cisco 보안 기술에 대한 예방 기능을 켜고 결과를 다시 검토하여 테스트를 다시 수행합니다. 공격자가 피해자에게 어떻게 접근하고 방어자들이 방어막을 치는 능력을 이해하는 것이 성공의 지름길입니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

위험 기반 취약성 관리 소개 - BRKSEC-1639

David Brothers, Cisco Systems, Inc. 기술 솔루션 설계자

RBVM(Risk-Based Vulnerability Management)은 여러분이 생각하는 것 이상을 포괄합니다. 이 유익하고 유익한 강연에서는 리스크를 수량화하는 기본 개념과 기본 이론을 심층적으로 살펴본 다음 RBVM 프로그램이 현대 네트워크를 보호하는 데 얼마나 중요한 역할을 하는지 공유합니다. 그런 다음 Kenna가 다양한 Cisco 제품 및 오퍼링에 RBVM을 구현하는 방법에 대해 설명합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 분할
기술 수준: 소개
기술: SecureX, 보안
트랙: 보안

대화형 분할

Cisco Talos를 통한 SecureX 활용 사고 대응 - IBOSEC-2011

Joe Schumacher, 사고 사령관, Cisco Systems, Inc.

참가자는 Cisco Talos IR(Talos Incident Response) 팀으로부터 보안 사고 발생 시 SecureX를 활용하여 대응 노력을 가속화하는 방법에 대해 직접 배우게 됩니다. Talos IR과 같은 외부 사고 대응 회사와 협력하거나 내부 조사 대응을 수행하든 SecureX를 어떻게 활용할 수 있는지 파악할 수 있습니다. 이 세션은 여러 Cisco 보안 제품을 보유한 가상의 보유자 고객이 Talos IR 핫라인으로 거는 단계적 전화 통화를 기반으로 구성됩니다. Talos IR 팀은 긴급 대응 활동으로 전환하기 전에 대응 목표

를 설정하고 배경 정보를 얻기 위해 참여합니다. 이 활동에는 사고가 억제될 때까지 SecureX를 다른 보안 제품과 함께 사용하는 것이 포함됩니다.
이 세션의 목표는 다음 분야의 참가자에게 알리는 것입니다.
SecureX를 통합하여 팀이 조사를 통해 협업하고 작업할 수 있도록 관찰 가능 요소를 연결
SecureX를 보안 제품과 통합하여 적시에 효과적인 대응

세션 유형: Interactive Breakout
기술 수준: 소개
기술: SecureX, 보안
트랙: 보안

SecureX Idea Exchange에 대해 자세히 알아보기 - IBOSEC-2005

Josh Borderon, Cisco Systems, Inc. 글로벌 엔터프라이즈 보안 아키텍트

다양한 서비스 구축 및 연결에 대해 논의하는 대화형 세션에서 SecureX를 Cisco Security 및 타사 툴과 함께 활용하는 방법을 알아보고 아이디어를 교환하십시오. 아이디어와 질문을 제시하거나 이미 SecureX 여정을 시작한 다른 파트너로부터 정보를 얻으십시오.

세션 유형: Interactive Breakout
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

워크인 랩

Cisco Secure Client 및 SecureX Device Insights - 효과적인 통합 - LABSEC-2776

Paul Carco, 엔지니어.TECHNICAL MARKETING, Cisco Systems, Inc.
Serhii Kucherenko, 고객 에스컬레이션 엔지니어, Cisco Systems, Inc.

Cisco Secure Client는 대부분의 Cisco 엔드포인트 클라이언트를 하나의 우산으로 제공하는 새로운 통합 클라이언트입니다. Cisco Secure Client는 표준 AnyConnect 모듈과 AMP(Cisco Secure Endpoint) 및 Orbital과 같은 보안 클라이언트로 구성됩니다. 이 실습에서는 SecureX Cloud에서 Cisco Secure Client를 구축하고 관리하는 방법을 학습합니다. SecureX Device Insights 전담 부서는 Cisco Secure Client 및 해당 모듈을 어떻게 기업 수준의 자산 관리 및 보안 사고 조사에 활용할 수 있는지 시연합니다.

세션 유형: 실습
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

기술 세미나

Cisco Secure Client: AnyConnect에서 포괄적인 클라이언트 보안으로! - TECSEC-

2780

Hacke Nohre, 기술 솔루션 설계자, Cisco - Distinguished Speaker
Thorsten Schranz, 기술 마케팅 엔지니어, Cisco Systems, Inc. - Distinguished Speaker
Valeria Scribanti, Technical Solutions Specialist, Cisco Systems, Inc. - Distinguished Speaker

새로운 하이브리드 인력, 복잡한 공격 시나리오, 빠른 클라우드 도입 및 인터넷상의 암호화 보급으로 클라이언트 보안이 그 어느 때보다 중요해졌습니다!
이 4시간 세션에서는 AnyConnect(VPN)를 모든 기능을 갖춘 엔드포인트 보안으로 확장하는 방법을 보여 드리겠습니다. 다음을 비롯한 Cisco Secure Client 모듈의 기술적 측면을 자세히 살펴보겠습니다.
EDR/EPP(보안 엔드포인트)
엔드포인트 네트워크 텔레메트리(Network Visibility Module)
DNS/웹 보호(Umbrella)
엔드포인트 상태(ISE/보안 방화벽)
단일 클라이언트를 실행하여 Cisco SecureX(XDR)에서 중앙 집중식으로 관리할 수 있습니다.
대상은 엔드포인트 보안에 관심이 있는 네트워크 및 보안 엔지니어와 설계자입니다. 엔드포인트 보안, 운영 체제 및 일반적인 공격 벡터에 대한 몇 가지 지식이 있는 것으로 가정합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 기술 세미나
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

Cisco Secure - TECSEC-2004를 통한 확장된 탐지 및 대응

Matthew Robertson, Cisco Systems, Inc. - Distinguished Speaker

Hanna Jabbour, Cisco Systems, Inc. 수석 기술 마케팅 엔지니어 - 발표자

Adi Sankar, Cisco Systems, Inc. 기술 마케팅 엔지니어

Matt Vander Horst, 기술 리더, Cisco - Distinguished Speaker

이 세션에서는 Cisco의 확장 탐지 및 대응 솔루션에 대한 심층적인 분석을 시작으로 Cisco Secure Endpoint, Secure Cloud Analytics, Umbrella, Meraki 및 Email Threat Defense와 Cisco XDR에서의 작업을 비롯한 다양한 제품 구성 요소의 구현 및 작업에 대한 완벽한 설명을 제공합니다. 또한 응답 엔진 운영에 있어 운영 모범 사례 및 구현 세부 사항과 Cisco XDR과 Crowdstrike Falcon과 같은 타사 제품의 통합도 포함됩니다.

Cisco Continuing Education 크레딧: 예
세션 유형: 기술 세미나
기술 레벨: 중간
기술: SecureX, 보안
트랙: 보안

DevNet

보안 자동화: SecureX로 개발 - DEVNET-1083

Matt Vander Horst, 기술 리더, Cisco - Distinguished Speaker

Cisco의 XDR 플랫폼에는 보안 운영을 자동화하고 강력한 통합을 구축할 수 있는 여러 가지 방법이 있다는 사실을 알고 계십니까? SecureX 통합 모듈을 사용하면 다른 플랫폼의 데이터를 조사 단계로 가져올 수 있으며, SecureX Threat Response API를 사용하면 위협을 조사하고 대응하는 방법을 자동화할 수 있으며, SecureX 오케스트레이션을 사용하면 코드 끌어서 놓기 편집기를 사용하여 강력한 워크플로를 구축할 수 있습니다. 이 세션에 들러 SecureX의 세 가지 면 각각에 대해 자세히 알아보고 이를 사용하여 보안 운영을 감독하는 방법을 알아보십시오.

세션 유형: DevNet
기술 수준: 소개
기술: SecureX, 보안

트랙: DevNet

SecureX 및 Kenna Security로 사이버 위생 운영 자동화 - DEVLIT-1355

Oxana Sannikova, 기술 솔루션 설계자, Cisco Systems, Inc.

오늘날 IT 운영은 여전히 매우 수작업으로 이루어지고 있습니다. 고객은 시스템 상태를 유지하고 온라인 보안을 강화해야 하는 과제에 항상 직면해 있습니다. 이 빠른 세션에서는 Cisco SecureX 오케스트레이션 및 Kenna Security를 활용하여 취약점 관리를 자동화하는 방법을 시연하겠습니다.

세션 유형: DevNet
기술 레벨: 중간
기술: 자동화 및 오케스트레이션, 보안
트랙: DevNet

퍼블릭 클라우드 사고 대응을 자동화하기 위한 SecureX 오케스트레이션 사용 - DEVWKS-2240

Brian Sak, Cisco Systems, Inc. 기술 솔루션 설계자 - 발표자

워크로드가 AWS, Azure 또는 GCP와 같은 퍼블릭 클라우드 공급자로 이동할 경우 사고 대응 및 교정이 더욱 어려워질 수 있으며 다양한 도구가 필요합니다. 이 세션에서는 위협 식별 프로세스를 자동화 및 간소화하고, 대응 절차를 간소화하며, 멀티 클라우드 또는 하이브리드 클라우드 환경에서 리소스를 보호할 때 보안 담당 팀이 안심할 수 있도록 하는 SecureX 오케스트레이션 워크플로를 생성하는 방법을 안내합니다.
올해 DevNet 워크숍 좌석은 사전 등록된 참석자가 먼저 앉습니다. 이 세션에는 12대의 노트북만 사용할 수 있습니다. 이 실습형 DevNet 워크샵에서는 강사와 함께 코드를 작성할 수 있습니다. 직접 3.5mm aux 커넥터 헤드폰을 가져와서 발표자 소리를 듣거나 DevNet Command Center에서 헤드폰을 들어 보십시오.
이 DevNet Workshop에 참가하면 Cisco Continuing Education(CE) 크레딧을 받을 수 있습니다. 자

세한 내용은 다음을 참조하십시오. https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

Cisco Continuing Education 크레딧: 예
세션 유형: DevNet
기술 레벨: 중간
기술: SecureX, 보안
트랙: DevNet

SecureX Orchestrator 및 원격 커넥터로 하이브리드 클라우드 워크플로 확장 - DEVNET-2109

Steve McNutt, Cisco Systems, Inc. 기술 솔루션 설계자

보안 오케스트레이션의 맥락에서 SXO(SecureX Orchestration)에 대해 들어보셨을 것입니다. Cisco는 이 솔루션이 더 많은 것을 할 수 있으며 효과적인 하이브리드 클라우드 운영 툴을 만드는 기반이 될 수 있음을 보여 드리겠습니다. 이 세션은 아키텍처 개요로 시작하고, Cisco Umbrella를 대량 배포하는 예제 솔루션을 단계별로 살펴보면서 구성 요소가 서로 어떻게 부합하는지, 그리고 어떻게 해결하는지 설명합니다. 이 세션에서는 사이드카 패턴을 활용하여 확장성이 뛰어난 하이브리드 클라우드 워크플로를 구축하는 방법에 대한 이해와 자체 솔루션을 구축하기 위해 수정할 수 있는 예제 코드를 숙지하는 방법을 다룹니다.

세션 유형: DevNet
기술 레벨: 중간
기술: SecureX, 보안
트랙: DevNet

XDR에서 R 수를 두 배로 늘리기: Cisco SecureX에서 10번의 클릭으로 보안 작업(SecOps)을 자동화하는 방법(코드 라인 작성 없이) - DEVNET-2214

Christopher Van Der Made, Cisco Systems, Inc. 엔지니어링 제품 관리자 - DSE

이 세션에서는 코드를 작성하지 않고도 SecureX Orchestration을 통해 자동화의 기능을 활용할 수 있는 방법을 보여 줍니다. 이를 통해 조직은 Cisco의 XDR(eExtended Detection and Response)에서 R 카운트를 두 배로 늘릴 수 있습니다. 우리는 당신이 지면을 뛰게 만들 몇 가지 매우 간단한 예를 설치하는 방법을 자세히 살펴볼 것입니다. 콘솔에 필요한 클릭 수를 메트릭으로 사용하여, 너무 많은 시간 없이 강력한 자동화에 액세스할 수 있는 방법을 증명합니다. 또한 이 과정을 한 단계 더 발전시켜 보안 운영 자동화의 마스터가 되는 방법도 배우게 됩니다. 나중에 모든 자료를 준비해서 직접 시작하세요. 이 세션은 사고 대응자, 보안 분석가, SOC 관리자 또는 자동화 및 보안에 관심이 있는 모든 사람을 대상으로 합니다.

세션 유형: DevNet
기술 레벨: 중간
기술: SecureX, 보안
트랙: DevNet

Microsoft Graph API와 통합: Python 및 SecureX 사용 - DEVWKS-3260

Hacke Nohre, 기술 솔루션 설계자, Cisco - Distinguished Speaker

이 워크숍에서는 Microsoft Graph API를 일반적인 Cisco 환경에 통합하는 방법을 설명합니다. Azure AD에 대한 Oauth2 인증 및 권한 부여에 중점을 두고 Microsoft Graph API에 대한 개괄적인 개요를 다룹니다.
그런 다음 파이썬 스크립트와 SecureX를 통해 이 API에 액세스하여 특정 사용자에 대한 Azure AD 그룹 및 역할에 대한 정보에 액세스하는 방법을 보여 줍니다
Microsoft 환경의 보안 이벤트에 대한 정보 액세스
참석자는 워크숍 중에 랩 환경에서 워크샵의 단계를 따르거나 나중에 단계를 완료할 수 있습니다. 참석자가 Azure 또는 SecureX 계정이 없어도 스스로 워크숍 작업을 완료할 수 있도록 하는 랩 설정에 대한 포인터를 제공합니다.

Cisco Continuing Education 크레딧: 예
세션 유형: DevNet
기술 레벨: 고급
기술: DevNet, 보안
트랙: DevNet

SecureX로 랜섬웨어 방어 자동화 및 간소화 - DEVNET-1456

Elia Maracani, 시스템 엔지니어, Cisco Systems, Inc.

랜섬웨어 공격은 갈수록 백업에 치중하고 있습니다. 회사의 백업을 빠르고 쉽게 복구할 뿐만 아니라 보호하는 것은 랜섬웨어 공격을 방어하는 데 있어 가장 중요하고 최고의 단계가 되고 있습니다. 데모를 통해 SecureX가 오케스트레이션 엔진을 통해 제공할 수 있는 다기능성 및 사용자 정의를 강조할 것입니다. Cisco SecureX가 1차(Cisco Umbrella, Cisco Secure Endpoint) 및 타사 솔루션(Cohesity Helios)과 통합됨에 따라 랜섬웨어 탐지, 조사 및 복구에 소요되는 시간과 복잡성을 대폭 줄일 수 있습니다.

세션 유형: DevNet
기술 수준: 소개
기술: SecureX, 보안
트랙: DevNet

제품 또는 전략 개요

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

Sana Sana Yousuf, Cisco Systems, Inc. 제품 마케팅 매니저

보안 팀은 위협 환경이 확장되고 복잡한 환경에 직면하여 보안 실효성이 점점 더 어려워지고 있습니다. 사이버 보안 빈곤선이 더욱 확대되고 있으며, 악의적인 공격자들은 이러한 틈새를 이용해 지속적인 공격을 감행하고 있습니다. Cisco는 효과적인 '확장 탐지 및 대응' 솔루션만이 귀사의 환경에서 Turla, Wannacry, NotPetya와 같은 정교한 공격자를 탐지하고 치료할 수 있다고 믿습니다. 하이브리드 멀티벤더 멀티벡터 세계에서의 XDR의 파괴적 가치에 대해 알아보십시오. 미래의 보안 운영

을 구축하기 위한 기반으로서 지속적으로 성장하는 멀티벤더 기술 통합 에코시스템에 대한 사례를 들어보십시오. XDR을 어떻게 SOC의 승수가 될 수 있을까요?

세션 유형: 제품 또는 전략 개요
기술 수준: 일반
기술: SecureX, 하이브리드 클라우드, 보안
트랙: 보안

보안 복원력을 사전 대응적으로 강화하는 방법 - PSOCX-2000

Varun Dhingra, Cisco Systems, Inc. 제품 관리 보안 및 협업 담당 수석 이사
Mark Hammond, Cisco Systems, Inc. 제품 관리 이사

사이버 보안을 관리해야 할 뿐만 아니라 데이터 프라이버시에 기반한 규정을 도입해야 하는 실질적인 압박에 직면하고 있습니다. 끊임없이 변화하는 위험, 규제, 비즈니스 목표 및 운영 영향의 요구 사항을 충족하는 사이버 보안 프로그램을 어떻게 설계하고 계십니까? 이 세션에서는 이해 관계자의 요구 사항을 충족하고 비즈니스 민첩성을 지원하는 솔루션을 생성하기 위해 업계에 맞게 조정된 데이터 보안 및 개인 정보 보호 프레임워크를 구축하는 방법을 학습합니다. 이 프레임워크는 원하는 사이버 보안 활동과 결과를 추적하도록 설계되었으며, 이를 통해 다양한 분야의 팀 간에 간단하고 비기술적인 커뮤니케이션이 가능합니다.

세션 유형: 제품 또는 전략 개요
기술 레벨: 중간
기술: 고객 경험, SecureX, 보안

추가 기회

위에 나열된 많은 세션 유형과 함께 Live!는 회의장에서 많은 혁신과 영감을 제공합니다. 엔지니어를 만나고, 깃발을 잡아내고, 챌린지에 참여하십시오. Live! 는 Cisco가 어떻게 가능성을 실현해 왔는지를 지속적으로 보여줍니다. 전체 카탈로그 및 자세한 내용은 Ciscolive.com을 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.