Cisco Live!安全终端和SecureX会话

目录

简介

Cisco Live!拉斯维加斯是重要的行业活动之一，目前有1100多个会议安排在6月4日至8日的曼德勒湾会议中心。鉴于课程目录如此庞大，我们希望确保我们的安全终端客户了解可有效利用我们的产品和服务的教育机会。 今年在拉斯维加斯，我们重点介绍围绕安全主题的129个可用实验、分组讨论以及讨论中的一小部分，希望您能与我们一起，帮助我们让世界更安全。

教师指导实验

思科安全终端：向左移动，实现正确操作 — LTRSEC-1114

Caly Hess，Security PrincessX，思科系统公司
Pedro Medina，思科系统公司软件工程师

端点安全是不断发展的网络犯罪形势下的最后一堵防线，如果配置正确，思科安全端点可以保证您的组织的安全。在此会话中，您将拥有对安全终端控制台的实际访问权限，同时可以从与安全终端(FKA AMP)合作了近十年的工程团队学习部署配置和实践以实现最佳安全状态。您将了解每个引擎的功能和功能，以及可以在哪些环境中优化利用它们。您将了解如何设置警报和自动化以缓解正在进行的攻击，这样您的组织就不必成为下一个重大漏洞。

有资格获得思科继续教育学分：是
会话类型：教师指导实验
技术级别：介绍
技术：安全
路径：安全

涵盖从安全邮件网关到基于API的平台的邮件安全演变 — LTRSEC-2011

有关集成SecureX以充分利用XDR部署的电邮深入探讨。

Alberto Torralba，Cisco Systems， Inc.技术解决方案架构师销售
Greg Barnes，思科系统公司技术营销工程师

本实验课程将概述思科安全电邮产品组合的最新功能。本课程将重点介绍最佳实践，使学员能够充分利用其电邮平台。网关主题将包括：使用SecureX思科威胁响应专用智能、配置基于域的消息身份验证、报告和一致性(DMARC)、高级日志记录、API使用情况等。学员还将学习如何将网关集成到思科安全电邮威胁防御的较新云产品。本实验将概述软件即服务产品，以查找缺乏传统危害指标的商业电子邮件危害等威胁，并调查可能受到危害的客户。

有资格获得思科继续教育学分：是
会话类型：教师指导实验

技术级别：中级
技术：SecureX、安全
路径：安全

安全防火墙 — 威胁防御数据路径故障排除（实验操作实用）— LTRSEC-3880

John Groetzinger，思科系统公司技术主管
Foster Lipkey，思科系统公司首席工程师 — 杰出发言人
Vidhi Mujumdar，思科系统公司客户交付主管

Cisco Firepower解决方案的用户普遍关心的一个问题是，当出现似乎与Firepower解决方案相关的网络中断或性能下降时，该如何处理。在本实验中，学员将学习用于评估Firepower平台(包括Firepower系列3 NGIP、具备Firepower服务的ASA、Firepower威胁防御(FTD)和FXOS)中的数据路径问题的故障排除方法。此会议将为与会者提供一个框架，以确定哪部分Firepower服务导致了问题，以及如何快速缓解已发现的问题。此框架将涵盖从数据包入口到深度数据包检测（包括Snort规则和预处理器性能）的整个数据路径。本实验将介绍Snort 2.9和Snort 3以及它们之间的差异。本实验将包含使用虚拟Firepower威胁防御(vFTD)实施故障排除框架的故障排除场景。此外，本实验将简要介绍SecureX安全防火墙集成。

有资格获得思科继续教育学分：是
会话类型：教师指导实验
技术水平：高级
技术：安全
路径：安全

网络恢复能力研讨会 — LTRSEC-1113

Ron Taylor，Cisco Systems， Inc.高级安全实验室Test Monkey
Leo Cruz，思科系统公司技术解决方案架构师

您的团队准备好应对下一次供应链攻击还是下一个零日攻击？现实检查！我们每个人每天都遭受攻击，我们最终都会被攻陷！因此，您的组织需要具备网络恢复能力。网络恢复能力是指组织能够迅速识别、响应和从IT安全事件中恢复。建立网络恢复能力包括制定以风险为中心的计划，假定业务在某个时候将面临漏洞或攻击。在本实验中，您将在企业实验室环境中体验网络安全攻击，在这种环境中，您将扮演攻击者和防御者，并第一手了解为何您需要高度集成的安全解决方案和网络运营技能才能实现网络弹性。

有资格获得思科继续教育学分：是
会话类型：教师指导实验
技术级别：介绍
技术：SecureX、安全
路径：安全

分流

排除和隔离由安全终端（Windows、Linux和MAC）引起的性能问题 — BRKSEC-

2072

Vibhor Amrodia，思科系统公司技术主管

在本次培训中，您将了解一些想法，帮助您快速有效地隔离已安装安全终端的性能问题。这是一个深入的会话，介绍我们如何使用安全终端提供的某些日志以及使用一些操作系统特定的实用程序和工具来分析和隔离终端（Windows、Linux和MAC）上的性能问题。此会话的重点区域为：Windows CPU和RAM使用率检测和隔离Linux CPU和RAM使用率检测和隔离MAC CPU和RAM使用率检测和隔离

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：安全
路径：安全

Cisco Unified Agent:Cisco Secure Client。将AMP、AnyConnect、Orbital和Umbrella融为一体 — BRKSEC-2834

Aaron Woland，思科系统公司杰出工程师 — 杰出发言人

我们都听到过这些抱怨，也有人抱怨过：“思科的座席太多”。

了解Aaron Woland、CCIE #20113和Cisco Live Distinguished Speaker Hall of Fame Elite；同时他向您展示思科倾听了投诉，并提供了统一安全代理的第一个版本：Cisco Secure Client。

思科安全客户端(CSC)提供模块化框架，允许AnyConnect VPN、思科安全终端（以前称为面向终端的AMP）、网络可视性模块、Umbrella云安全、ISE终端安全评估、安全防火墙终端安全评估（以前称为Hostscan）和网络访问模块(NAM)一起存在；同时提供来自SecureX的现代基于云的管理 — 与SecureX设备见解紧密相连。

在本次培训中，我们将深入探讨安全客户端背后的技术、实际工作原理以及实际工作原理与不足之处。我们将介绍来自云的部署模式，并使用您自己的软件部署机制。我们将详细了解现有AnyConnect和安全终端(AMP)代理的无缝升级流程。我们将讨论哪些场景适合升级到CSC，以及哪些场景能让您真正受益于现有的AnyConnect和安全终端(AMP)代理（至少目前如此）。

请花些时间与Aaron一起娱乐，同时从思科安全了解这一激动人心的开发成果。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

从发货到岸：集成、协作和（安全）控制思科安全电邮网关 — BRKSEC-2288

Robert Sherwin，Cisco Systems， Inc.技术主管 — 杰出发言人

Cisco Secure Email集成在其自身邮件网关之外。安全、日志记录、API和配置以及SecureX — 我们将带您了解电邮如何扩展到网关之外，以及如何切实地充分利用您的环境，无论规模大小！

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

思科的恶意软件防御云和安全恶意软件分析集成 — BRKSEC-2242

Bill Yazji，思科系统公司技术安全架构师 — 杰出发言人

您可能已将其称为“AMP云和威胁网格”，但它们已被重新命名为“恶意软件防御云和安全恶意软件分析”。此会议将回顾并深入探讨恶意软件防御云和恶意软件分析产品，同时介绍其与思科安全架构的集成，包括安全邮件、安全Web、安全防火墙、安全终端、Umbrella和Meraki。这些产品协同工作，我们将涵盖恶意软件防御架构，并展示如何将所有组件结合在一起，提供行业领先的高级威胁架构。本课程非常适合新接触思科安全套件的客户，以及拥有一个或多个产品并希望更深入地了解其合作方式的客户。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

带防火墙的Cisco XDR - BRKSEC-2090

Eric Kostlan，思科系统公司技术营销工程师 — 著名演讲人
Adi Sankar，思科系统公司技术营销工程师

SecureX是思科的XDR，是世界上最广泛的集成平台。在此会议中，与会者将看到防火墙与SecureX集成的强大功能。这包括SecureX中的防火墙事件、针对威胁响应调查的防火墙丰富功能，以及使用防火墙API的SecureX协调。与会者应基本了解思科安全防火墙。与会者不需要了解SecureX。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

通过Cisco SecureX - BRKSEC-1023加速SOC

Matt Vander Horst，思科技术主管 — 杰出演讲人

您是否知道，思科的XDR平台SecureX可以加快您的组织调查和响应事故的方式？SecureX结合了一系列功能，允许您处理安全事件，获得更全面产品组合的可视性，并使用自动化来调查和以机器速度响应。在本次培训中，您将了解SecureX的简介并了解其基本功能，包括：SecureX控制面板、威胁响应、事件管理器、协调、设备见解和安全客户端。我们还将分享您可以参加的其他会话的列表，以便更深入地了解这些功能以及更多内容。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：介绍
技术：SecureX、安全
路径：安全

带电子邮件的Cisco XDR：保护、分析和发展SMTP会话 — BRKSEC-2095

Robert Sherwin，Cisco Systems， Inc.技术主管 — 杰出发言人

电子邮件被认为是企业网络中最薄弱的环节，在不到两分钟的时间内，黑客和攻击者就打开了通往威胁或漏洞的大门。电子邮件是恶意软件感染的主要媒介，因为它可以轻松地将恶意负载置于用户面前，并且只需点击一下鼠标即可防止恶意软件攻击。除了传递恶意软件，攻击者比以往任何时候都更善于制作和生成类似于他们所模拟的服务的网络钓鱼链接。思科安全电邮不断发展扩展检测和响应如何针对这些威胁媒介并保护您的SMTP会话。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

使用Cisco XDR的扩展检测：整个企业的安全分析 — BRKSEC-2178

Matthew Robertson，思科系统公司杰出技术营销工程师 — 杰出发言人

扩展检测和响应(XDR)是当今流行的流行术语。此会议将深入探讨思科XDR的扩展检测和分析功能，重点探讨如何扩展检测功能并加快响应速度。此会议涵盖多种检测技术，包括终端、网络分析和防火墙，将探讨分析如何将这些检测结合到一起，实现XDR目标。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

A-Z提供的思科IT安全。零信任高级恶意软件防护 — BRKCOC-2620

Steve Vida，思科系统公司网络安全架构师
Gil Daudistel，思科系统公司信息安全经理

做不可能的事情：思科通过引入员工零信任机制，通过一次移动提高安全性和改善体验。此会议将

深入介绍安全零信任身份验证流程的详细信息、我们如何从使新流程与更好的体验协调中获益，以及我们如何使用Jamf Pro、InTune/SCCM和Meraki Systems Manager部署终端配置以支持零信任。
此会议还将深入探讨思科IT如何在其超过20万台设备群中实施和维护思科安全终端。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：混合工作、安全
路径：思科现身说法

Cisco SecureX XDR — 理解所有部件和部件 — BRKSEC-2113

Aaron Woland，思科系统公司杰出工程师 — 杰出发言人

扩展检测和响应(XDR)是市场上最热门的安全技术之一，其采用率正在快速增长。由于XDR解决方案中能够执行的和应该执行的操作范围广泛，因此自然会出现许多复杂性，导致对幕后如何/发生什么的困惑。此专题讨论将深入介绍思科功能强大的XDR解决方案的内部工作方式，包括网络检测和响应、终端检测和响应、邮件威胁防御、恶意软件分析、统一安全代理；以及所有这些组件和组件如何一起产生预期的XDR结果。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

将思科的XDR解决方案与IT服务管理(ITSM)和SIEM系统相结合，用于事故调查 — BRKSEC-2122

Oxana Sannikova，思科系统公司技术解决方案架构师

在本次培训中，我们将展示扩展检测和响应(XDR)平台SecureX如何增强安全操作，从而在不增加复杂性的情况下提供更好的结果。我们将了解以下使用案例：在威胁搜寻中利用IT服务管理(ITSM)和SIEM的情景，为ITSM事件和SIEM警报添加整合的威胁可视性，通过利用自动化和协调来正式制定事件响应程序。会议将近一半的时间将进行演示。涵盖的ITSM和SIEM解决方案将包括ServiceNow、Jira和Splunk，参与者将带着随时可用的工作流程离开。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：自动化和协调、安全
路径：安全

集成开源Zeek和思科XDR - BRKSEC-2075

King Mark Stephens，俄亥俄州思科里奇菲尔德全球网络安全架构师

扩展检测和响应(XDR)解决方案通过更快速地检测和响应以及降低风险和暴露，为组织提供保护以防范网络安全事件的潜力。XDR必须包括第三方集成，以提供额外的检测引擎。此会议将介绍开源Zeek，并提供有关如何集成到Cisco XDR以改善客户安全成果的可操作详情。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

灰头骨的力量！对抗仿真 — BRKSEC-2180

Jason Maynard，CSS加拿大网络安全现场首席技术官

在本次培训中，我们将了解对抗仿真，以及红色和蓝色团队如何从中受益。我们了解可供我们使用的工具，然后利用Caldera构建一个没有预防功能的运营。然后，我们将审查对抗性成果，包括审查被动部署的思科安全产品组合的成果。获得的知识可确保防御团队了解增强防御能力的机会。然后，我们将启用我们针对各种思科安全技术的防御功能，并再次执行测试，查看测试结果。了解攻击者如何接近其受害者和防御者进行分层防御的能力是成功的秘诀。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：中级
技术：SecureX、安全
路径：安全

基于风险的漏洞管理简介 — BRKSEC-1639

David Brothers，思科系统公司技术解决方案架构师

基于风险的漏洞管理(RBVM)所涵盖的内容可能超出您的想象。在这个有趣且内容丰富的演讲中，我们将深入探讨量化风险的基本概念和理论，然后分享实用RBVM程序对于保护现代网络的重要性。然后，我们将讨论Kenna如何将RBVM引入到各种思科产品和服务中。

有资格获得思科继续教育学分：是
会话类型：分支
技术级别：介绍
技术：SecureX、安全
路径：安全

互动式分组讨论

利用SecureX和Cisco Talos事件响应 — IBOSEC-2011

Joe Schumacher，思科系统公司事故指挥员

学员将直接从思科Talos事件响应(Talos IR)团队了解如何在安全事件期间利用SecureX加快响应速

度。他们将深入了解如何利用SecureX，无论是与Talos IR等外部事件响应公司合作，还是执行内部调查响应。此会话将围绕一个虚拟的注册客户通过多个思科安全产品拨打分步电话拨入Talos IR热线。Talos IR团队将参与制定响应目标并获取背景信息，然后进入应急响应活动，其中将包括使用SecureX和其他安全产品，直到事件得到控制。
会议的目标是在以下方面告知与会者：
结合SecureX来连接可观察信息，以便团队协作并完成调查
将SecureX与安全产品集成，以协调及时有效的响应

会话类型：交互式分支
技术级别：介绍
技术：SecureX、安全
路径：安全

深入了解SecureX Idea Exchange - IBOSEC-2005

Josh Bordelon，思科系统公司全球企业安全架构师

在互动会话中，探讨和交流有关使用思科安全和第三方工具的SecureX的想法，在此次互动会话中，我们将讨论构建和连接各种服务。带上您的想法和问题，或者向已经开始SecureX之旅的其他人学习。

会话类型：交互式分支
技术级别：中级
技术：SecureX、安全
路径：安全

步入式实验室

Cisco Secure Client和SecureX Device Insights — 更好地结合 — LABSEC-2776

Paul Carco，思科系统公司技术营销工程师
Serhii Kucherenko，思科系统公司客户升级工程师

Cisco Secure Client是一种新的统一客户端，将大多数思科终端客户端置于一个保护伞下。思科安全客户端包括标准AnyConnect模块和安全客户端，例如AMP（也称为思科安全终端）和Orbital。作为本实验的一部分，您将学习如何从SecureX云部署和管理Cisco安全客户端。SecureX Device Insights专用的部分将演示Cisco Secure Client及其模块如何用于企业级资产管理和安全事故调查。

会话类型：步入式实验
技术级别：中级
技术：SecureX、安全
路径：安全

技术研讨会

思科安全客户端：从AnyConnect到全面的客户端安全！- TECSEC-2780

Hacke Nohre，思科技术解决方案架构师 — 杰出演讲人
Thorsten Schranz，Cisco Systems， Inc.技术营销工程师 — 杰出发言人
Valeria Scribanti，Cisco Systems， Inc.技术解决方案专家 — 杰出发言人

新的混合型员工队伍、复杂的攻击场景、云的快速采用以及互联网上无处不在的加密，使客户端安全变得比以往任何时候都更重要！
在这个4小时的课程中，我们将展示我们如何将AnyConnect(VPN)扩展到功能齐全的终端安全。我们将深入了解思科安全客户端模块的技术方面，包括：
EDR/EPP（安全终端）
终端网络遥测（网络可视性模块）
DNS/Web保护(Umbrella)
终端安全评估（ISE/安全防火墙）
以及运行在Cisco SecureX(XDR)中集中管理的单个客户端的结果。
目标受众是对终端安全感兴趣的网络和安全工程师和架构师。假设对终端安全、操作系统和常见攻击媒介有一定的了解。

有资格获得思科继续教育学分：是
会议类型：技术研讨会
技术级别：中级
技术：SecureX、安全
路径：安全

使用Cisco Secure - TECSEC-2004扩展检测和响应

Matthew Robertson，思科系统公司杰出技术营销工程师 — 杰出发言人

Hanna Jabbour，Cisco Systems， Inc.首席技术营销工程师 — 杰出演讲人

Adi Sankar，思科系统公司技术营销工程师

Matt Vander Horst，思科技术主管 — 杰出演讲人

从深入了解思科的扩展检测和响应产品开始，此会议将全面介绍各种产品组件的实施和操作，包括思科安全终端、安全云分析、Umbrella、Meraki和邮件威胁防御及其在Cisco XDR中的操作。其中还包括操作最佳实践和响应引擎运行中的实施细节，以及Cisco XDR与非思科产品（如Crowdstrike Falcon）的集成。

有资格获得思科继续教育学分：是
会议类型：技术研讨会
技术级别：中级
技术：SecureX、安全
路径：安全

DevNet

安全自动化：使用SecureX开发 — DEVNET-1083

Matt Vander Horst，思科技术主管 — 杰出演讲人

您是否知道，思科的XDR平台具有多种方式，可以自动执行安全操作并构建强大的集成？通过SecureX集成模块，您可以将来自其他平台的数据纳入到调查中；通过SecureX威胁响应API，您可以自动执行调查和应对威胁的方式；通过SecureX协调，您可以使用自下而上的代码拖放编辑器构建强大的工作流程。通过此会话了解有关SecureX这三个方面的详细信息，以及如何使用这些信息增强您的安全操作。

会话类型：DevNet
技术级别：介绍
技术：SecureX、安全

路径：DevNet

通过SecureX和Kenna Security实现网络卫生操作自动化 — DEVLIT-1355

Oxana Sannikova，思科系统公司技术解决方案架构师

如今，IT操作仍需要大量手动操作。客户始终面临保持系统正常运行和提高在线安全性的挑战。在此快速课程中，我们将演示如何利用Cisco SecureX协调和Kenna Security来自动化漏洞管理。

会话类型：DevNet
技术级别：中级
技术：自动化和协调、安全
路径：DevNet

使用SecureX协调自动化公共云事件响应 — DEVWKS-2240

Brian Sak，Cisco Systems， Inc.技术解决方案架构师 — 杰出演讲人

当工作负载迁移到AWS、Azure或GCP等公共云提供商时，事件响应和补救会变得更加困难，并且需要不同的工具。此会议将指导您创建SecureX协调工作流程，这些工作流程可自动化和简化威胁识别流程、简化响应程序，并在多云或混合云环境中保护资源时让安全团队高枕无忧。
今年新推出的DevNet研讨会座位是预先注册的与会者首先就座。此会话只有12台笔记本电脑。这是一个动手的DevNet研讨会，您可在其中与讲师一起进行编码。在DevNet命令中心自带3.5毫米辅助连接器耳机以聆听演示者或拿起一对耳机。
通过参加此DevNet研讨会，您将有资格获得思科继续教育(CE)学分。有关详细信息，请访问 :https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

有资格获得思科继续教育学分：是
会话类型：DevNet
技术级别：中级
技术：SecureX、安全
路径：DevNet

使用SecureX Orchestrator和远程连接器扩展混合云工作流程 — DEVNET-2109

Steve McNutt，思科系统公司技术解决方案架构师

您可能听说过安全协调环境中的SecureX Orchestration(SXO)。我们将向您展示it可以做更多的事情，并成为创建高效混合云运营工具的基础。此会议首先从高级架构概述开始，然后是大规模部署Cisco Umbrella的示例解决方案的逐步介绍，说明这些组件如何配合使用以及它们如何解决挑战。在离开此会议时，您将了解如何利用侧板模式构建高度可扩展的混合云工作流程，并熟悉可以修改以构建您自己的解决方案的示例代码。

会话类型：DevNet
技术级别：中级
技术：SecureX、安全
路径：DevNet

在XDR中使R计数翻倍：如何在Cisco SecureX中单击10次后自动执行安全操作(SecOps)（无需编写任何代码行） — DEVNET-2214

Christopher Van Der Made，思科系统公司工程产品经理 — 杰出发言人

此会议将说明如何在不编写任何代码的情况下通过SecureX协调来利用自动化的强大功能。这将使组织能够在思科的XDR（扩展检测和响应）中将R计数加倍。我们将介绍几个非常简单的安装示例，这些示例将让您顺利地投入使用。我们将使用控制台中需要的点击量作为指标，来证明您如何能够在不太费力的情况下获得强大的自动化功能。最后，您还将学习如何更进一步，逐步成为安全运营自动化的专家。所有材料你以后就可以自己开始了。本课程面向突发事件响应人员、安全分析师、SOC经理或对自动化和安全感兴趣的任何人。

会话类型：DevNet
技术级别：中级
技术：SecureX、安全
路径：DevNet

与Microsoft Graph API集成：使用Python和SecureX - DEVWKS-3260

Hacke Nohre，思科技术解决方案架构师 — 杰出演讲人

在本研讨会中，我们将讨论如何将Microsoft Graph API集成到典型的思科环境中。
我们将简要介绍Microsoft Graph API，重点介绍Oauth2身份验证和Azure AD授权。
然后，我们将展示如何通过python脚本和SecureX访问此API，以获取有关特定用户的Azure AD组和角色的信息
从Microsoft环境访问有关安全事件的信息
参与者可以在研讨会期间尝试从实验室环境中执行研讨会中的步骤，也可以在稍后完成步骤。我们将提供实验设置的指针，使参与者无需拥有自己的Azure或SecureX帐户即可自行完成研讨会任务。

有资格获得思科继续教育学分：是
会话类型：DevNet
技术水平：高级
技术：DevNet、安全

路径：DevNet

使用SecureX自动化和简化勒索软件防御 — DEVNET-1456

Elia Maracani，思科系统公司系统工程师

勒索软件攻击越来越侧重于备份。因此，保护，以及快速轻松地恢复公司的备份，是防御勒索软件攻击的最佳且最重要的步骤。在演示的帮助下，我们将重点介绍SecureX通过其协调引擎提供的通用性和定制功能。由于Cisco SecureX与第一（Cisco Umbrella、思科安全终端）和第三方解决方案(Cohesity Helios)的集成，您将能够显着减少勒索软件检测、调查和恢复的时间和复杂性。

会话类型：DevNet
技术级别：介绍
技术：SecureX、安全
路径：DevNet

产品或战略概述

Cisco XDR：为未来安全运营中心构建 — PSOSEC-1007

Sana Sana Yousuf，思科系统公司产品营销经理

安全团队面临着不断扩大的威胁形势，以及日益难以发挥的复杂环境安全效力。网络安全贫困线正在扩大，恶意攻击者正在利用这一巨大漏洞发动持续攻击。我们相信，只有有效的“扩展检测和响应”解决方案才能检测并补救您环境中的复杂攻击者，如Turla、Wannacry和NotPetya。了解XDR在混合、多供应商、多矢量世界中的颠覆性价值。听我说明，多供应商技术集成的生态系统在不断发展，是构建未来安全运营的基础。XDR如何成为您的SOC的力量倍增器？

会话类型：产品或策略概述
技术水平：一般
技术：SecureX、混合云、安全
路径：安全

如何主动增强您的安全恢复能力 — PSOCX-2000

Varun Dhingra，思科系统公司产品管理安全与协作高级总监
Mark Hammond，思科系统公司产品管理总监

您不仅必须管理网络安全，而且还要面临基于数据隐私制定法规的切实压力。您如何设计一个网络安全计划，以满足风险、监管、业务目标和运营影响等不断变化的要求？在本次培训中，您将学习如何构建行业一致的数据安全和隐私框架，以满足利益相关方的需求并生成可实现业务灵活性的解决方案。该框架旨在跟踪所需的网络安全活动和结果，这些活动和结果直观，可在多学科团队之间实现简单的非技术沟通。

会话类型：产品或策略概述
技术级别：中级
技术：客户体验、SecureX、安全

其他商机

与上面列出的许多会话类型一样，Live！在会议楼上有许多创新和灵感。 与工程师会面、捕捉旗帜或参加挑战赛，现场直播！继续演示思科如何成为通向成功的桥梁。 请访问Ciscolive.com查看完整目录和更多详细信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。