Cisco Live!安全終端和SecureX會話

目錄

簡介

Cisco Live!拉斯維加斯是重要的行業活動之一，目前有超過1100場活動安排在6月4日至8日在曼德勒灣會展中心。面對如此龐大的課程目錄，我們希望確保我們的安全終端客戶能夠認識到我們有機會有效地利用產品和服務。 今年在拉斯維加斯，我們提供了129個可用的實驗、分組討論和有關安全主題的討論，作為其中的一小部分，我們希望您能考慮加入我們的行列，因為我們將幫助世界變得更加安全。

教師指導實驗

思科安全端點：通過左移實現右移 — LTRSEC-1114

Caly Hess，Security PrincessX，思科系統公司
Pedro Medina，Cisco Systems， Inc.軟體工程師

端點安全是不斷變化的網路犯罪形勢的最後一道防線，如果配置得當，思科安全端點可以保證您組織的安全。在此會話中，您將擁有對安全終端控制檯的實際訪問許可權，同時可以從與安全終端(FKA AMP)合作了十年的大部分時間的工程團隊學習部署配置和實踐以獲得最佳安全狀態。您將瞭解每個引擎的功能和功能，以及可以在哪些環境中最佳化利用它們。您將知道如何設定警報和自動化以緩解正在進行的攻擊，從而使您的組織不必成為下一個重大漏洞。

有資格獲得思科繼續教育學分：是
課程型別：教師指導實驗
技術級別：介紹
技術：安全性
途徑：安全性

涵蓋從安全電子郵件網關到基於API的平台的郵件安全演變 — LTRSEC-2011

有關整合SecureX以充分利用XDR部署的電子郵件深入分析。

Alberto Torralba，Cisco Systems， Inc.技術解決方案架構師銷售
Greg Barnes，思科系統公司技術行銷工程師

本實驗課程將概述思科安全電子郵件產品組合的最新功能。本課程將重點介紹使參與者能夠充分利用其電子郵件平台的最佳做法。網關主題包括使用SecureX思科威脅響應專用智慧、配置基於域的消息身份驗證、報告和一致性(DMARC)、高級日誌記錄、API使用等。參與者還將學習如何將該網關整合到思科安全郵件威脅防禦服務這一較新的雲產品中。該實驗室將概述軟體即服務產品，以發現缺乏傳統危害指標的商業電子郵件危害等威脅，並調查可能受到危害的客戶。

有資格獲得思科繼續教育學分：是

課程型別：教師指導實驗
技術級別：中級
技術：SecureX、安全
途徑：安全性

安全防火牆 — 威脅防禦資料路徑故障排除（實驗操作） — LTRSEC-3880

John Groetzinger，思科系統公司技術主管
Foster Lipkey，Cisco Systems， Inc.首席工程師 — 傑出演講人
Vidhi Mujumdar，思科系統公司客戶交付部負責人

思科Firepower解決方案的使用者普遍關心的一個問題是，當出現似乎與Firepower解決方案相關的網路中斷或降級時，該怎麼做。在本實驗中，學員將學習用於評估Firepower平台中資料路徑問題的故障排除方法，包括Firepower系列3 NGIP、具備Firepower服務的ASA、Firepower威脅防禦(FTD)和FXOS。此會議將為參與者提供一個框架，以確定哪部分Firepower服務導致了問題，以及如何快速緩解已發現的問題。此框架將涵蓋從封包輸入到深度封包檢查（包括Snort規則和前處理器效能）的整個資料路徑。本實驗將介紹Snort 2.9和Snort 3以及它們之間的區別。本實驗將包含使用虛擬Firepower威脅防禦(vFTD)實施故障排除框架的故障排除方案。此外，本實驗還將簡要介紹SecureX安全防火牆整合。

有資格獲得思科繼續教育學分：是
課程型別：教師指導實驗
技術級別：高級
技術：安全性
途徑：安全性

網路恢復力研討會 — LTRSEC-1113

Ron Taylor， Cisco Systems， Inc.高級安全實驗室Test Monkey
Leo Cruz，思科系統公司技術解決方案架構師

您的團隊準備好應對下一次供應鏈攻擊或下一次零日攻擊了嗎？現實檢查！我們每天都受到攻擊、我們最終都會被攻陷！因此，您的組織需要具備網路恢復能力。網路恢復能力是指組織能夠迅速識別、響應和從IT安全事件中恢復。建立網路復原能力包括制定以風險為中心的計畫，假定業務在某個時候將面臨漏洞或攻擊。在本實驗中，您將在企業實驗室環境中體驗網路安全攻擊，在這種環境中，您扮演攻擊者和防禦者，並第一手瞭解為什麼您需要高度整合的安全解決方案和網路操作技能才能實現網路彈性。

有資格獲得思科繼續教育學分：是
課程型別：教師指導實驗
技術級別：介紹
技術：SecureX、安全
途徑：安全性

分支

排除和隔離由安全終端（Windows、Linux和MAC）引起的效能問題 — BRKSEC-2072

Vibhor Amrodia，Cisco Systems， Inc.技術主管

在結束此會議時，您將瞭解到如何幫助您快速有效地隔離安裝了安全端點的效能問題。這是一個深入的課程，介紹我們如何使用安全終端上的一些可用日誌以及一些作業系統特定的實用程式和工具來分析和隔離終端（Windows、Linux和MAC）上的效能問題。此會話的重點領域為：Windows CPU和RAM使用率檢測和隔離Linux CPU和RAM使用率檢測和隔離MAC CPU和RAM使用率檢測和隔離

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：安全性
途徑：安全性

思科統一代理：思科安全客戶端。將AMP、AnyConnect、Orbital和Umbrella結合在一起 — BRKSEC-2834

Aaron Woland，思科系統公司傑出工程師 — 傑出發言人

我們都聽過抱怨，或者自己也抱怨過：「思科的代理人太多了」。

瞭解Aaron Woland、CCIE #20113和Cisco Live Distinguished Speaker Hall of Fame Elite；同時他向您展示思科傾聽了投訴，並提供了統一安全代理的第一個版本：思科安全客戶端。

思科安全客戶端(CSC)提供模組化框架，允許AnyConnect VPN、思科安全終端（以前稱為終端的AMP）、網路可視性模組、Umbrella雲安全、ISE安全狀態、安全防火牆狀態（以前稱為Hostscan）和網路訪問模組(NAM)一起存在；以及來自SecureX的現代基於雲的管理 — 與SecureX裝置見解緊密連線。

在本次會議中，我們將深入探討安全客戶端背後的技術、實際工作方式以及不工作方式。我們將使用您自己的軟體部署機制，從雲覆蓋部署模式。我們將從現有AnyConnect和安全終端(AMP)代理處瞭解無縫升級流程的所有資訊。我們將討論升級到CSC的合理方案，以及您繼續使用現有AnyConnect和安全終端(AMP)代理的真正優勢方案 — 至少目前如此。

來與Aaron一起玩一會，同時從思科安全部瞭解這一令人振奮的發展。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

從發貨到岸上：整合、合作和（安全）控制思科安全郵件網關以外的業務 — BRKSEC-2288

Robert Sherwin，Cisco Systems， Inc.技術主管 — 傑出發言人

Cisco Secure Email整合在其自身的郵件網關之外。安全、日誌記錄、API和配置以及SecureX — 我們將帶您瞭解電子郵件是如何超越網關並切實地充分利用您的環境（無論規模大小）！

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

思科的惡意軟體防禦雲和安全惡意軟體分析整合 — BRKSEC-2242

Bill Yazji，思科系統公司技術安全架構師 — 傑出發言人

您可能將其稱為「AMP雲和威脅網格」，但它們已被重新命名為「惡意軟體防禦雲和安全惡意軟體分析」。此會議將回顧並深入研究惡意軟體防禦雲和惡意軟體分析產品，同時涵蓋其與思科安全架構的整合，包括安全電子郵件、安全Web、安全防火牆、安全終端、Umbrella和Meraki。這些產品協同工作，我們將覆蓋惡意軟體防禦架構，並展示如何將所有元件結合在一起，以提供業界領先的高級威脅架構。本課程非常適合於那些新接觸思科安全套件的人以及擁有一個或多個產品，並希望更深入地瞭解這些產品如何協同工作的客戶。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

含防火牆的Cisco XDR - BRKSEC-2090

Eric Kostlan，Cisco Systems， Inc.技術行銷工程師 — 傑出演講人
Adi Sankar，思科系統公司技術行銷工程師

SecureX是思科的XDR，是世界上最廣泛的整合平台。在此會議中，與會者將看到防火牆與SecureX整合的強大功能。這包括SecureX中的防火牆事件、針對威脅響應調查的防火牆增強功能，以及使用防火牆API的SecureX協調。與會者應具備思科安全防火牆的基本知識。與會者不需要瞭解SecureX。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

使用Cisco SecureX加速SOC - BRKSEC-1023

Matt Vander Horst，思科技術主管 — 傑出發言人

您是否知道，思科的XDR平台SecureX可以加快您的組織調查和響應事故的方式？SecureX結合了一系列功能，允許您負責安全事件、跨廣泛的產品組合獲得更好的可視性，以及使用自動化來調查和以機器速度做出響應。在此會議中，您將瞭解SecureX的簡介並瞭解其各種功能的基礎知識，包括SecureX控制面板、威脅響應、事件管理器、協調、裝置洞察和安全客戶端。我們還將分享您可以參加的其他會話的清單，以便更深入地瞭解這些功能以及更多內容。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：介紹
技術：SecureX、安全
途徑：安全性

帶電子郵件的Cisco XDR：保護、分析和發展SMTP會話 — BRKSEC-2095

Robert Sherwin，Cisco Systems， Inc.技術主管 — 傑出發言人

電子郵件被認為是企業網路中最薄弱的環節，在不到兩分鐘的時間內，駭客和攻擊者就開啟了一扇門，可導致危害或洩露。電子郵件是惡意軟體感染的主要媒介，因為它可以毫不費力地將惡意負載置於使用者面前，並且只需按一下一下即可被利用。除了傳遞惡意軟體，攻擊者比以往更善於製作和生成類似於他們所模擬的服務的網路釣魚連結。Cisco Secure Email正在改進擴展檢測和響應如何針對這些威脅媒介並保護您的SMTP對話。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

使用Cisco XDR的擴展檢測：整個企業的安全分析 — BRKSEC-2178

Matthew Robertson，思科系統公司傑出技術行銷工程師 — 傑出發言人

擴展檢測和響應(XDR)是當今流行的流行詞。本課程將深入探討思科XDR的擴展檢測和分析功能，重點探討如何擴展檢測功能和加快響應速度。涵蓋終端、網路分析和防火牆等多種檢測技術。本課程將探討分析如何將這些檢測結合起來，實現XDR目標。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

A-Z提供的思科IT安全。實現零信任的高級惡意軟體防護 — BRKCOC-2620

Steve Vida，思科系統公司網路安全架構師
Gil Daudistel，思科系統公司資訊保安經理

做不可能的事：思科通過引入員工零信任機制，通過一次行動提高安全性和改善體驗。此會議將深入瞭解安全的零信任身份驗證流的詳細資訊、我們如何從使新流與更好的體驗協調中受益，以及我們如何使用Jamf Pro、InTune/SCCM和Meraki Systems Manager部署終端配置以支援零信任。此會議還將深入探討思科IT如何在其超過20萬台裝置群中實施和維護思科安全終端。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：混合工作、安全
路徑：思科在思科

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

Aaron Woland，思科系統公司傑出工程師 — 傑出發言人

擴展檢測和響應(XDR)是市場上最熱門的安全技術之一，其採用率正在快速增長。鑑於在XDR解決方案中可以執行的和應該執行的操作的範圍很廣，自然會出現很多複雜性，導致對幕後如何/正在發生什麼的困惑。此會議將介紹思科功能強大的XDR解決方案的內部運作，包括網路檢測和響應、端點檢測和響應、電子郵件威脅防禦、惡意軟體分析、統一安全代理；以及所有這些部分和部分如何結合起來產生預期的XDR結果。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

利用思科的XDR解決方案與IT服務管理(ITSM)和SIEM系統進行事件調查 — BRKSEC-2122

Cisco Systems， Inc.技術解決方案架構師Oxana Sannikova

在本節中，我們將展示擴展檢測和響應(XDR)平台SecureX如何增強安全操作，從而在不增加複雜性的情況下提供更好的結果。我們將檢視以下使用案例：在威脅搜尋中利用IT服務管理(ITSM)和SIEM的情景，為ITSM事件和SIEM警報新增整合的威脅可視性，通過利用自動化和協調來正式化事件響應程式。會議將近一半的時間將進行演示。涵蓋的ITSM和SIEM解決方案將包括ServiceNow、Jira和Splunk，參與者將隨身攜帶使用工作流程。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：自動化和協調、安全
途徑：安全性

整合開源Zeek和Cisco XDR - BRKSEC-2075

King Mark Stephens，Cisco Richfield， Ohio全球網路安全架構師

擴展檢測和響應(XDR)解決方案通過更快地檢測和響應以及降低風險和暴露提供了保護組織免受網路安全事件影響的潛力。XDR必須包含第三方整合以提供其他檢測引擎。此會議將介紹開源Zeek並提供有關如何整合到Cisco XDR以改善客戶安全成果的可操作詳情。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

灰頭骨的力量！對抗模擬 — BRKSEC-2180

Jason Maynard，CSS網路安全加拿大現場技術長

在本課程中，我們將學習對抗模擬以及如何使用紅藍兩色團隊。我們瞭解可用的工具，然後利用Caldera構建一個沒有預防功能的操作。然後，我們將審查對抗性結果，包括審查被動部署的思科安全產品組合的結果。獲得的知識確保防禦團隊瞭解加強防禦的機會。然後，我們將啟用我們針對各種思科安全技術的預防性功能，並再次執行測試，檢視測試結果。瞭解對抗方如何接近其受害者以及防禦方部署防禦的能力是成功的秘訣。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

基於風險的漏洞管理簡介 — BRKSEC-1639

David Brothers，Cisco Systems， Inc.技術解決方案架構師

基於風險的漏洞管理(RBVM)所涵蓋的範圍超出了您的想象。在這個有趣且內容豐富的演講中，我們將深入探討量化風險的基本概念和理論，然後分享RBVM程式對於確保現代網路安全的重要性。然後，我們將討論Kenna如何將RBVM引入到各種思科產品和服務中。

有資格獲得思科繼續教育學分：是
會話型別：分支
技術級別：介紹
技術：SecureX、安全
途徑：安全性

互動式分組討論

利用SecureX和Cisco Talos事件響應 — IBOSEC-2011

Joe Schumacher，思科系統公司事故指揮官

參與者將直接從思科Talos事件響應(Talos IR)團隊瞭解如何在安全事件期間利用SecureX加快響應

速度。他們將深入瞭解如何利用SecureX，無論是與Talos IR這樣的外部事件響應公司合作，還是執行內部調查響應。此會話將圍繞一個虛擬的保留客戶通過分步電話撥打多種Cisco安全產品的Talos IR熱線建立。Talos IR團隊將參與制定響應目標並獲取背景資訊，然後進入應急響應活動，其中將包括使用SecureX和其他安全產品，直到事件得到控制。
會議的目標是在下列領域向與會者通報情況：
將SecureX合併為連線可觀察資料，以便團隊合作並完成調查
將SecureX與安全產品整合，以協調及時有效的響應

會話型別：互動式分支
技術級別：介紹
技術：SecureX、安全
途徑：安全性

深入瞭解SecureX Idea Exchange - IBOSEC-2005

Josh Bordelon，思科系統公司全球企業安全架構師

在互動式會議中，探討和交流有關使用SecureX和思科安全以及第三方工具的想法，在此會議中，我們將討論構建和連線各種服務。提出您的想法和問題，或者向已經開始SecureX之旅的其他人學習。

會話型別：互動式分支
技術級別：中級
技術：SecureX、安全
途徑：安全性

步入式實驗室

思科安全客戶端和SecureX裝置洞察 — 更好地結合 — LABSEC-2776

Paul Carco，Cisco Systems， Inc.技術行銷工程師
Serhii Kucherenko，思科系統公司客戶升級工程師

思科安全客戶端是一種新的統一客戶端，將大多數思科終端客戶端集中到一個保護傘下。思科安全客戶端包括標準AnyConnect模組和安全客戶端，例如AMP（又稱為思科安全終端）和Orbital。作為本實驗的一部分，您將學習如何從SecureX雲部署和管理Cisco Secure Client。SecureX Device Insights專用的部分將演示Cisco Secure Client及其模組如何用於企業級資產管理和安全事件調查。

會話型別：步入式實驗
技術級別：中級
技術：SecureX、安全
途徑：安全性

技術研討會

思科安全客戶端：從AnyConnect到全面的客戶端安全！- TECSEC-2780

Hacke Nohre，思科技術解決方案架構師 — 傑出演講者
Thorsten Schranz，Cisco Systems， Inc.技術行銷工程師 — 傑出演講者
Valeria Scribanti，Cisco Systems， Inc.技術解決方案專家 — 卓越演講者

新的混合型員工、複雜的攻擊場景、雲的快速採用以及網際網路上無處不在的加密技術，使客戶端安全變得比以往任何時候都更重要！
在這個4小時的課程中，我們將展示如何將AnyConnect(VPN)擴展到功能全面的終端安全中。我們將深入瞭解思科安全客戶端模組的技術方面，包括：
EDR/EPP（安全端點）
終端網路遙測（網路可視性模組）
DNS/Web保護(Umbrella)
終端狀態（ISE/安全防火牆）
以及運行在Cisco SecureX(XDR)中集中管理的單個客戶端的結果。
目標受眾是對終端安全感興趣的網路和安全工程師和架構師。假設對終端安全、作業系統和常見攻擊媒介有一定的瞭解。

有資格獲得思科繼續教育學分：是
會議型別：技術研討會
技術級別：中級
技術：SecureX、安全
途徑：安全性

使用Cisco Secure的擴展檢測和響應 — TECSEC-2004

Matthew Robertson，思科系統公司傑出技術行銷工程師 — 傑出發言人

Hanna Jabbour，Cisco Systems， Inc.首席技術行銷工程師 — 傑出演講人

Adi Sankar，思科系統公司技術行銷工程師

Matt Vander Horst，思科技術主管 — 傑出發言人

從深入瞭解思科的擴展檢測和響應服務開始，此會議將全面瞭解各種產品元件的實施和操作，包括思科安全終端、安全雲分析、Umbrella、Meraki和電子郵件威脅防禦及其在Cisco XDR中的操作。還包括操作最佳實踐和響應引擎運行中的實施細節，以及思科XDR與非思科產品（如Crowdstrike Falcon）的整合。

有資格獲得思科繼續教育學分：是
會議型別：技術研討會
技術級別：中級
技術：SecureX、安全
途徑：安全性

DevNet

安全自動化：使用SecureX開發 — DEVNET-1083

Matt Vander Horst，思科技術主管 — 傑出發言人

您是否知道，思科的XDR平台具有多種方法，可以自動執行您的安全操作並構建強大的整合？SecureX整合模組允許您將資料從其他平台帶到您的調查中，SecureX威脅響應API允許您自動執行調查和應對威脅的方式，而SecureX協調允許您使用自下而上的代碼拖放編輯器構建強大的工作流。通過此會話稍作瞭解有關SecureX的這三個方面的詳細資訊，以及如何使用這些資訊來增強您的安全操作。

會話型別：DevNet
技術級別：介紹
技術：SecureX、安全

途徑：DevNet

通過SecureX和Kenna Security實現網路衛生操作自動化 — DEVLIT-1355

Cisco Systems， Inc.技術解決方案架構師Oxana Sannikova

如今，IT操作仍需要大量手動操作。客戶始終面臨保持系統健康並提高線上安全性的挑戰。在此快速會議中，我們將演示如何利用Cisco SecureX協調和Kenna Security來自動化漏洞管理。

會話型別：DevNet
技術級別：中級
技術：自動化和協調、安全
途徑：DevNet

使用SecureX協調自動執行公共雲事件響應 — DEVWKS-2240

Brian Sak，Cisco Systems， Inc.技術解決方案架構師 — 傑出演講者

當工作負載遷移到AWS、Azure或GCP等公共雲提供商時，事件響應和補救會變得更加困難，並且需要不同的工具。此會議將指導您建立SecureX協調工作流程，這些工作流程可自動化和簡化威脅識別流程、簡化響應程式，以及在多雲或混合雲環境中保護資源時讓安全團隊高枕無憂。
今年新推出的DevNet研討會座位是預先註冊的與會人員首先就座。此會話只有12檯筆記型電腦可用。這是一次動手的DevNet研討會，您可以在此與講師一起進行編碼。在DevNet命令中心自帶一個3.5毫米輔助聯結器耳機，以聽取講演者的聲音或拿起一對耳機。
通過參加此DevNet研討會，您將有資格獲得思科繼續教育(CE)學分。有關詳細資訊，請訪問:https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-options

有資格獲得思科繼續教育學分：是
會話型別：DevNet
技術級別：中級
技術：SecureX、安全
途徑：DevNet

使用SecureX Orchestrator和遠端聯結器擴展混合雲工作流 — DEVNET-2109

Steve McNutt，Cisco Systems， Inc.技術解決方案架構師

您可能聽說過安全協調環境中的SecureX Orchestration(SXO)。我們將向您展示，它可以做更多的事情，並成為建立高效混合雲運營工具的基礎。本課程首先從高級架構概述開始，然後逐步介紹大規模部署Cisco Umbrella的示例解決方案，解釋這些元件如何搭配在一起，以及它們如何解決挑戰。在結束此會議後，您將瞭解如何利用側板模式構建高度可擴展的混合雲工作流程，並熟悉可以修改以構建您自己的解決方案的示例代碼。

會話型別：DevNet
技術級別：中級
技術：SecureX、安全
途徑：DevNet

在XDR中使R計數翻倍：如何在Cisco SecureX中按一下10次即可自動執行安全操作(SecOps)（無需編寫任何代碼行） — DEVNET-2214

Christopher Van Der Made，思科系統公司工程產品經理 — 傑出演講人

此會議將顯示如何在不編寫任何代碼的情況下通過SecureX協調來利用自動化的力量。這將使組織能夠在思科的XDR（擴展檢測和響應）中將R計數加倍。我們將介紹幾個非常簡單的安裝示例，它們將讓您順利地投入使用。我們將使用控制檯中需要的點選量作為指標，來證明您如何能夠訪問強大的自動化而沒有太多麻煩。最後，您還將學習如何更進一步，逐步成為您的安全操作自動化的高手。所有材料你準備後自己動手做。本課程面向突發事件響應人員、安全分析師、SOC經理或對自動化和安全性感興趣的任何人。

會話型別：DevNet
技術級別：中級
技術：SecureX、安全
途徑：DevNet

與Microsoft Graph API整合：使用Python和SecureX - DEVWKS-3260

Hacke Nohre，思科技術解決方案架構師 — 傑出演講者

在本研討會中，我們將討論如何在典型的思科環境中整合Microsoft Graph API。
我們將簡要概述Microsoft Graph API，重點介紹Oauth2身份驗證和Azure AD授權。
然後，我們將展示如何通過python指令碼和SecureX訪問此API，以訪問特定使用者的Azure AD組和角色的相關資訊
從Microsoft環境訪問有關安全事件的資訊
在研討會期間，與會者可以嘗試從實驗室環境中執行研討會中的步驟，也可以稍後完成步驟。我們將提供實驗設定的指標，讓參與者無需擁有自己的Azure或SecureX帳戶，即可自行完成研討會任務。

有資格獲得思科繼續教育學分：是
會話型別：DevNet
技術級別：高級

技術：DevNet、安全
途徑：DevNet

使用SecureX自動化和簡化勒索軟體防禦 — DEVNET-1456

Elia Maracani，思科系統公司系統工程師

勒索軟體攻擊越來越側重於備份。因此，保護，以及快速輕鬆地恢復公司的備份，是防禦破壞性的勒索軟體攻擊的最佳且最重要的步驟。在演示的幫助下，我們將重點介紹SecureX通過其協調引擎提供的通用性和定製功能。藉助Cisco SecureX提供的第一方（Cisco Umbrella、思科安全終端）和第三方解決方案(Cohesity Helios)的整合，您將能夠顯著減少勒索軟體檢測、調查和恢復的時間和複雜性。

會話型別：DevNet
技術級別：介紹
技術：SecureX、安全
途徑：DevNet

產品或策略概述

Cisco XDR：為未來安全運營中心構建 — PSOSEC-1007

Sana Sana Yousuf，思科系統公司產品行銷經理

安全團隊面臨著不斷擴大的威脅形勢和日益難以實現的複雜環境安全效力。網路安全貧困線正在擴大，惡意行為者正在利用這一巨大漏洞發動持續攻擊。我們相信，只有有效的「擴展檢測和響應」解決方案才能檢測並補救您環境中的複雜對手，如Turla、Wannacry和NotPetya。瞭解XDR在混合、多供應商、多向量世界中的破壞性價值。請聽我講一個案例，說明一個不斷增長的多供應商技術整合生態系統，以此作為構建未來安全運營的基礎。XDR如何成為您的SOC的力倍增器？

會話型別：產品或策略概述
技術級別：一般
技術：SecureX、混合雲、安全
途徑：安全性

如何主動加強您的安全恢復能力 — PSOCX-2000

Varun Dhingra，Cisco Systems， Inc.產品管理安全與合作高級總監
Mark Hammond，思科系統公司產品管理總監

您不僅需要管理網路安全，而且還面臨著制定基於資料隱私的法規的切實壓力。您如何設計一個網路安全計畫，以滿足風險、法規、業務目標和運營影響等不斷變化的要求？在此會議中，您將學習如何構建行業一致的資料安全和隱私框架，以滿足利益相關方的需求並生成可實現業務靈活性的解決方案。該框架旨在跟蹤所需的網路安全活動和結果，這些活動和結果直觀，可實現多學科團隊之間的簡單非技術溝通。

會話型別：產品或策略概述

技術級別：中級
技術：客戶體驗、SecureX、安全

其他商機

除了上面列出的許多會議型別，「直播！有大量的創新和靈感。」 與工程師會面、捕捉旗幟或參加挑戰，現場觀看！繼續展示思科如何成為實現目標的橋樑。 請檢視Ciscolive.com上的完整目錄和更多詳細資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。