シスコライブ！セキュアなエンドポイントとSecureXセッション

内容

はじめに

シスコライブ！ラスベガスは、6月4日から8日にかけてマンダレー・ベイ・コンベンション・センターで開催される1100セッションを含む業界有数のイベントです。このような大規模なコースカタログを使用して、シスコの製品とサービスを効果的に利用するための教育機会について、セキュアエンドポイントのお客様に確実に認識していただきたいと考えました。 今年ラスベガスで提供されるセキュリティに関する129のラボ、ブレークアウトセッション、ディスカッションのほんの一部に焦点を当て、世界をより安全な場所にするためにシスコの参加をご検討ください。

インストラクターによる実習

Cisco Secure Endpoint：左にシフトして右に進む – LTRSEC-1114

シスコセキュリティプリンセスXキャリー・ヘス
シスコ、ソフトウェアエンジニア、ペドロ・メディナ

エンドポイントセキュリティは、進化するサイバー犯罪の状況における最後の防御壁であり、適切に設定すると、Cisco Secure Endpointによって組織の安全性を維持できます。このセッションでは、Secure Endpoint Consoleに実際にアクセスしながら、10年以上にわたってSecure Endpoint(FKA AMP)を使用して作業してきたエンジニアリングチームから、導入の構成と最適なセキュリティポスチャのためのプラクティスを学びます。各エンジンの機能と機能、および最適に利用できる環境について学習します。進行中の攻撃を軽減するためにアラートと自動化を設定し、組織が次の大規模なセキュリティ侵害を受ける必要がないようにする方法を習得できます。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：インストラクターによる実習
技術レベル：導入部
テクノロジー：セキュリティ
トラック：セキュリティ

セキュアなEメールゲートウェイからAPIベースのプラットフォームへのEメールセキュリティの進化について説明する – LTRSEC-2011

XDR導入を最大限に活用するためのSecureXの統合に関するEメールによる詳細な説明。

シスコテクニカルソリューションアーキテクト、アルベルト・トラルバ氏
グレッグ・バーンズ氏（Cisco Systems, Inc.、テクニカルマーケティングエンジニア）

このラボセッションでは、Cisco Secure Emailポートフォリオの最新機能の概要を説明します。このセッションでは、Eメールプラットフォームを最大限に活用するためのベストプラクティスに焦点を当てます。ゲートウェイに関するトピックには、SecureX Cisco Threat Responseプライベートインテリジェンスの使用、ドメインベースのメッセージ認証、レポートと適合性(DMARC)の設定、高度なロギング、APIの使用などが含まれます。また、Cisco Secure Email Threat Defenseを提供する新しいクラウドにゲートウェイを統合する方法についても学習します。このラボでは、Software as a Serviceの概要を示して、従来のセキュリティ侵害の指標がないビジネス電子メールの侵害などの脅威を探し、潜在的に侵害されているアカウントを調査します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：インストラクターによる実習
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

セキュアファイアウォール – 脅威対策データパスのトラブルシューティング（実用的な実習）– LTRSEC-3880

ジョン・グロッツィンガー氏（Cisco Systems, Inc、テクニカルリーダー）
フォスター・リプキー（シスコプリンシパルエンジニア）– 講演要人
Vidhi Mujumdar、シスコカスタマーデリバリリーダー

シスコのFirepowerソリューションを使用するユーザに共通の懸念事項の1つは、Firepowerソリューションに関連すると思われるネットワークの中断または機能低下が発生した場合に何をすべきかということです。この実習では、Firepowerシリーズ3 NGIP、ASAとFirepowerサービス、Firepower脅威対策(FTD)、FXOSなど、Firepowerプラットフォーム内のデータパスの問題を評価するためのトラブルシューティング手法を学習します。このセッションでは、Firepowerサービスのどの部分が問題に寄与しているかを特定するための枠組みと、特定された問題を迅速に軽減する方法を参加者に提供します。このフレームワークは、パケット入力からディープパケットインスペクション（Snortルールやプリプロセッサパフォーマンスなど）までのデータパス全体をカバーします。この実習では、Snort 2.9とSnort 3の両方と、その違いについて説明します。この実習には、仮想Firepower脅威対策(vFTD)を使用してトラブルシューティングフレームワークを実装するトラブルシューティングシナリオが含まれます。また、この実習では、SecureXセキュアファイアウォールの統合についても簡単に触れます。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：インストラクターによる実習
技術レベル：上級
テクノロジー：セキュリティ
トラック：セキュリティ

サイバーレジリエンスワークショップ – LTRSEC-1113

シスコセキュリティラボテストモンキーSr Security Lab, Inc.、ロン・テイラー
レオ・クルス氏（シスコ、テクニカルソリューションアーキテクト）

御社のチームは、次のサプライチェーン攻撃または次のゼロデイに備えていますか？リアリティチェック！私たちは毎日攻撃を受けており、最終的には全員が危険にさらされます。このため、組織はサイバー復元力を備えている必要があります。サイバーレジリエンスとは、ITセキュリティインシデントを特定し、対応し、迅速に回復する組織の能力を指します。サイバー復元力の構築には、ある時点でビジネスが侵害または攻撃に直面すると想定した、リスクに焦点を当てた計画の作成が含まれます。このラボ演習では、エンタープライズラボ環境でサイバーセキュリティ攻撃を体験します。この環境では、攻撃者と防御者を演じながら、サイバー復元力を得るために高度に統合されたセキュリティソリューションとCyberOpsスキルが必要な理由を直接学習します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：インストラクターによる実習
技術レベル：導入部
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

サブ会議

セキュアエンドポイント（Windows、Linux、およびMAC）によるパフォーマンスの問題のトラブルシューティングと切り分け – BRKSEC-2072

Vibhor Amrodia（シスコテクニカルリーダー）

このセッションでは、Secure Endpointsをインストールした状態でパフォーマンスの問題を迅速かつ効果的に切り分けるために役立つアイデアについて説明します。このセッションでは、Secure Endpointで利用可能なログの一部と、OS固有のユーティリティおよびツールを使用して、エンドポイント（Windows、Linux、およびMAC）のパフォーマンスの問題を分析および切り分ける方法について詳しく説明します。このセッションの重点領域は、次のとおりです。Windows CPUおよびRAM使用率の検出と分離Linux CPUおよびRAM使用率の検出と分離MAC CPUおよびRAM使用率の検出と分離

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：セキュリティ
トラック：セキュリティ

シスコの統合エージェント：Cisco Secure ClientAMP、AnyConnect、Orbital、Umbrellaを統合 – BRKSEC-2834

シスコディスティングイッシュドエンジニア、アーロン・ウォランド – ディスティングイッシュ

ドスピーカー

私たちは皆、苦情を聞いたことがあるか、「シスコにはエージェントが多すぎます」という苦情を自分たちで受け止めました。

Aaron Woland、CCIE #20113、Cisco Live Distinguished Speaker Hall of Fame Eliteが、シスコが苦情に耳を傾け、ユニファイドセキュリティエージェントの最初のイテレーションであるCisco Secure Clientを提供したことを紹介します。

Cisco Secure Client(CSC)は、AnyConnect VPN、Cisco Secure Endpoint（以前のAMP for Endpoints）、Network Visibility Module、Umbrella Cloud Security、ISE Posture、Secure Firewall Posture（以前のHostscan）、およびNetwork Access Module(NAM)をすべて統合できるモジュラフレームワークを提供します。SecureXから提供される最新のクラウドベースの管理は、SecureXのデバイスインサイトと密接に接続しています。

このセッションでは、Secure Clientの背後にあるテクノロジーについて詳しく説明し、実際の動作とその動作について説明します。クラウドからの導入モデルと、独自のソフトウェア導入メカニズムを使用した導入モデルについて説明します。既存のAnyConnectおよびセキュアエンドポイント(AMP)エージェントからのシームレスなアップグレードフローについて詳しく説明します。CSCにアップグレードするのが適切なシナリオと、少なくとも現時点では、既存のAnyConnectおよびセキュアエンドポイント(AMP)エージェントを使用し続けることが本当に役立つシナリオについて説明します。

Aaronと一緒に時間を過ごし、シスコのセキュリティからのこのエキサイティングな開発について学びながら楽しんでください。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

艦船から陸上：統合、コラボレーション、（安全に）Cisco Secure Email Gatewayを超えた制御 – BRKSEC-2288

シスコテクニカルリーダー、ロバート・シャーウィン – 講演者

Cisco Secure Emailは、独自のメールゲートウェイの外部と統合できます。セキュリティ、ロギング、APIと設定、およびSecureX – 電子メールがゲートウェイを越えて拡大し、大小を問わず環境を最大限に活用する方法について説明します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

シスコのマルウェア防御クラウドとセキュアなマルウェア分析の統合 – BRKSEC-2242

ビル・ヤジ（シスコテクニカルセキュリティアーキテクト）– 上級スピーカー

「AMPクラウドと脅威グリッド」という名称で知られているかもしれませんが、マルウェア防御クラウドおよびセキュアなマルウェア分析というブランドに変更されました。このセッションでは、Malware Defenseクラウドとマルウェア分析サービスについて詳しく説明し、Secure Email、Secure Web、Secure Firewall、Secure Endpoint、Umbrella、Merakiなどのシスコのセキュリティアーキテクチャとの統合について取り上げます。これらの製品は連携して動作します。ここでは、マルウェア防御アーキテクチャについて取り上げ、これらの要素がどのように組み合わさり、業界をリードする高度な脅威アーキテクチャを提供するかを示します。このセッションは、Cisco Security Suiteの新しい製品を使用するお客様や、1つ以上の製品を所有し、それらの製品がどのように連動するかを詳しく知りたいと考えているお客様に最適です。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

ファイアウォール付きCisco XDR - BRKSEC-2090

Eric Kostlan、テクニカルマーケティングエンジニア、シスコシステムズ – 講演者
アディ・サンカー氏（シスコシステムズ、テクニカルマーケティングエンジニア）

シスコのXDRであるSecureXは、世界で最も広範な統合プラットフォームです。このセッションでは、ファイアウォールとSecureXの統合の効果について説明します。これには、SecureXのファイアウォールインシデント、脅威対応調査に対するファイアウォールの強化、ファイアウォールAPIを使用したSecureXオーケストレーションが含まれます。参加者は、Cisco Secure Firewallに関する基本的な知識を持っている必要があります。参加者はSecureXの知識は必要ありません。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

Cisco SecureXでSOCを加速 – BRKSEC-1023

マット・バンダー・ホルスト、テクニカルリーダー、シスコ – 上級スピーカー

シスコのXDRプラットフォームであるSecureXによって、組織での調査やインシデントへの対応が迅速化されることをご存知でしたか？SecureXは、一連の機能を組み合わせて、セキュリティ事故を管理し、幅広い製品ポートフォリオの可視性を高め、自動化を使用して調査を行い、マシ

ン速度で対応します。このセッションでは、SecureXの概要を説明し、SecureXダッシュボード、脅威応答、インシデントマネージャ、オーケストレーション、デバイスの洞察、セキュアなクライアントなど、SecureXのさまざまな機能の基礎を学びます。また、これらの機能の詳細な調査などのために参加できる他のセッションのリストも共有します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：導入部
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

Eメールを使用したCisco XDR:SMTPカンバセーションの保護、分析、および進化 – BRKSEC-2095

シスコテクニカルリーダー、ロバート・シャーウィン – 講演者

電子メールはビジネスネットワークの中で最も弱いリンクとして知られており、わずか2分でハッカーや攻撃者に侵入や侵害につながる開かれた扉を提供します。電子メールは、悪意のあるペイロードをユーザの目の前に簡単に配置し、不正利用から1クリックしか離れないため、マルウェア感染の主要な媒介となります。単にマルウェアを配信するだけではなく、攻撃者は、偽装しているサービスと同じようにフィッシングリンクを作成して生成するという点で、かつてないほど高度な技術を持っています。Cisco Secure Emailは、Extended Detection and Response(XDR)がこのような脅威ベクトルをターゲットにし、SMTP通信を保護する方法を進化させています。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

Cisco XDRによる検出の拡張：企業全体のセキュリティ分析 – BRKSEC-2178

マシュー・ロバートソン、ディスティングイッシュドテクニカルマーケティングエンジニア、シスコシステムズ、ディスティングイッシュドスピーカー

Extended Detection and Response(XDR)は、現在広く使用されている流行語です。このセッションでは、トピックを解説しながら、シスコのXDRの広範な検出および分析機能について考察します。特に、検出機能を拡張して対応を迅速化する方法について重点的に説明します。このセッションでは、エンドポイント、ネットワーク分析、ファイアウォールなど、複数の検出テクノロジーを取り上げ、分析によってこれらの検出を統合し、XDRの目的を達成する方法について説明します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

シスコITセキュリティの概要ゼロトラストへの高度なマルウェア防御 – BRKCOC-2620

スティーブ・ビダ氏（シスコサイバーセキュリティアーキテクト）
ギル・ダウディステル氏（シスコ、情報セキュリティ担当マネージャ）

不可能を可能にする：シスコは、従業員に対するゼロ信頼を導入することで、セキュリティを強化し、エクスペリエンスを向上させました。このセッションでは、安全なゼロトラスト認証フローの詳細、新しいフローを適切なエクスペリエンスに合わせて調整することで得られる利点、Jamf Pro、InTune/SCCM、およびMeraki Systems Managerを使用してゼロトラストをサポートするためのエンドポイント構成を展開した方法について説明します。
このセッションでは、シスコITが200,000台以上のデバイスでCisco Secure Endpointを実装および維持する方法についても説明します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：ハイブリッドワーク、セキュリティ
トラック：Cisco on Cisco

Cisco SecureX XDR – すべてのパーツと部品を理解する – BRKSEC-2113

シスコディスティングイッシュドエンジニア、アーロン・ウォランド – ディスティングイッシュドスピーカー

Extended Detection and Response(XDR)は、市場で最もホットなセキュリティテクノロジーの1つであり、導入が急増しています。XDRソリューションで何ができるか、何をすべきか、何を行うかについて幅広い範囲を考えると、当然のことながら、舞台裏でどのように何が起こっているのかについて混乱を招く可能性のある多くの複雑さがあります。このセッションでは、ネットワークの検出と応答、エンドポイントの検出と応答、Eメール脅威に対する防御、マルウェア分析、Unified Security Agentなど、シスコの非常に優れたXDRソリューションの仕組み、およびこれらの要素がどのように組み合わさり、XDRに期待される結果が生み出されるかについて説明します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

シスコのXDRソリューションとIT Service Management(ITSM)およびSIEMシステムを活用したインシデント調査 – BRKSEC-2122

シスコテクニカルソリューションアーキテクト、Oxana Sannikova

このセッションでは、Extended Detection and Response(XDR)プラットフォームであるSecureXが、複雑さを増すことなくセキュリティ運用を強化し、より良い結果を生み出す方法に

ついて説明します。ここでは、次のユースケースについて説明します。IT Service Management(ITSM)およびSIEMのコンテキストを脅威追跡で活用し、ITSMインシデントおよびSIEMアラートに統合された脅威の可視性を追加し、自動化およびオーケストレーションを活用してインシデント対応手順を形式化します。セッションの約半分はデモです。ITSMおよびSIEMソリューションには、ServiceNow、Jira、およびSplunkが含まれ、参加者はワークフローをすぐに使用できます。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：自動化とオーケストレーション、セキュリティ
トラック：セキュリティ

オープンソースZeekとCisco XDRの統合 – BRKSEC-2075

キング・マーク・スティーブンス氏（オハイオ州シスコリッチフィールド、グローバルサイバーセキュリティアーキテクト）

Extended Detection and Response(XDR)ソリューションは、検出と対応を高速化し、リスクと脅威を軽減することで、サイバーセキュリティイベントから組織を保護する可能性を提供します。XDRには、追加の検出エンジンを提供するためのサードパーティ統合が含まれている必要があります。このセッションでは、オープンソースのZeekについて紹介し、お客様のセキュリティ成果を向上させるためにCisco XDRに統合する方法について実用的な詳細を説明します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

グレイスカルのパワー！Adversarial Emulation(BRKSEC-2180)

ジェイソン・メイナード氏（CSS、フィールドCTO、サイバーセキュリティカナダ）

このセッションでは、敵対的なエミュレーションと、赤と青の両方のチームがその使用からどのように利益を得ることができるかについて学びます。私たちは利用可能なツールについて学び、予防機能なしでCalderaを活用したオペレーションを構築します。次に、シスコのセキュリティ製品の受動的な展開に関する成果のレビューを含め、敵対的な成果をレビューします。得られた知識によって、防御チームは防御を強化する機会を理解できます。その後、シスコのさまざまなセキュリティテクノロジーに対する予防機能をオンにし、結果を確認しながらテストを再実行します。攻撃者が被害者にどのようにアプローチし、防御者の防御力を強化するかを理解することが、成功の秘訣です。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ

トラック：セキュリティ

リスクベースの脆弱性管理の概要 – BRKSEC-1639

デビッド・ブラザーズ氏 (シスコ、テクニカルソリューションアーキテクト)

リスクベースの脆弱性管理(RBVM)は、お客様が考える以上のものを含んでいます。この楽しく有益なトークでは、基本的な概念に深く掘り下げ、リスクを定量化する理論を強調し、現代のネットワークを保護するために実用的なRBVMプログラムがいかに不可欠であるかを共有します。その後、KennaがRBVMをシスコのさまざまな製品やサービスにもたらす方法について説明します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：ブレイクアウト
技術レベル：導入部
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

対話型ブレークアウト

SecureXとCisco Talosインシデント対応の活用 – IBOSEC-2011

ジョー・シューマッハ氏 (シスコ、インシデントコマンダー)

参加者は、Cisco Talos Incident Response(Talos IR)チームから、セキュリティインシデント発生時にSecureXを活用して対応を迅速化する方法について直接学習します。Talos IRのような外部のインシデント対応企業と連携するか、内部の調査対応を行うかに関係なく、SecureXをどのように利用できるかについて理解を深めることができます。このセッションは、複数のシスコセキュリティ製品を所有する架空の保持ユーザによって、ターロスIRホットラインへの段階的な電話コールを中心に構築されます。Talos IRチームは、緊急対応活動に移る前に、対応に関する目標を設定し、背景情報を入手します。この活動には、インシデントが封じ込められるまで、SecureXを他のセキュリティ製品とともに使用することが含まれます。
セッションの目標は、次の領域の参加者に通知することです。
SecureXを組み込んでチームがコラボレーションし、調査を通じて作業できるように監視可能なものを接続
SecureXとセキュリティ製品を統合して、タイムリーで効果的な対応を調整する

セッションタイプ：インタラクティブブレークアウト
技術レベル：導入部
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

SecureX Idea Exchangeの詳細 – IBOSEC-2005

シスコ、グローバルエンタープライズセキュリティアーキテクト、ジョシュ・ボルデロン

さまざまなサービスの構築と接続について話し合うインタラクティブなセッションで、

SecureXとシスコのセキュリティおよびサードパーティ製ツールの利用に関するアイデアを探り、交換します。アイデアや質問を持ち込んだり、すでにSecureXへの移行を開始している他の人から学んだりしてください。

セッションタイプ：インタラクティブブレークアウト
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

ウォークインラボ

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

シスコテクニカルマーケティング担当エンジニア、Paul Carco
シスコカスタマーエスカレーションエンジニア、Serhii Kucherenko

Cisco Secure Clientは、シスコのほとんどのエンドポイントクライアントを1つのシステムにまとめた新しい統合クライアントです。Cisco Secure Clientは、標準のAnyConnectモジュールと、AMP（別名Cisco Secure Endpoint）やOrbitalなどのセキュリティクライアントで構成されています。この実習では、SecureXクラウドからCisco Secure Clientを導入および管理する方法を学習します。SecureX Device Insights専用のパートでは、Cisco Secure Clientとそのモジュールを使用して、エンタープライズレベルの資産管理とセキュリティインシデントの調査を行う方法について説明します。

セッションタイプ：ウォークインラボ
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

テクニカルセミナー

Cisco Secure Client:AnyConnectから包括的なクライアントセキュリティ- TECSEC-2780

Hacke Nohre、テクニカルソリューションアーキテクト、シスコ – 上級スピーカー
Thorsten Schranz、テクニカルマーケティングエンジニア、シスコシステムズ – 講演者
Valeria Scribanti、Technical Solutions Specialist、シスコ – 講演者

新しいハイブリッドワークフォース、複雑な攻撃シナリオ、急速なクラウドの導入、インターネットでの暗号化の普及により、クライアントのセキュリティはこれまで以上に重要になっています。
この4時間のセッションでは、AnyConnect(VPN)をフル機能のエンドポイントセキュリティに拡張する方法について説明します。Cisco Secure Clientモジュールの次の技術面について詳しく説明します。
EDR/EPP（セキュアエンドポイント）
エンドポイントネットワークテレメトリ(Network Visibility Module)

DNS/Web保護(Umbrella)
エンドポイントポスチャ（ISE/セキュアファイアウォール）
Cisco SecureX(XDR)で一元管理される単一のクライアントを実行した結果を確認します。
対象者は、エンドポイントセキュリティに関心を持つネットワークおよびセキュリティエンジニアとアーキテクトです。エンドポイントセキュリティ、オペレーティングシステム、一般的な攻撃ベクトルに関する知識が前提となります。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：テクニカルセミナー
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

Cisco Secureによる検出と応答の拡張 – TECSEC-2004

マシュー・ロバートソン、ディスティングイッシュドテクニカルマーケティングエンジニア、シスコシステムズ、ディスティングイッシュドスピーカー

シスコテクニカルマーケティングエンジニア、ハンナ・ジャバウアー氏（上級スピーカー）

アディ・サンカー氏（シスコシステムズ、テクニカルマーケティングエンジニア）

マット・バンダー・ホルスト、テクニカルリーダー、シスコ – 上級スピーカー

このセッションでは、シスコの広範な検出と対応のオファーの詳細な説明から始め、さまざまな製品コンポーネント（Cisco Secure Endpoint、Secure Cloud Analytics、Umbrella、Meraki、Email Threat Defenseなど）の実装と運用、およびCisco XDRでのそれらの運用について詳しく説明します。また、Cisco XDRとCrowdstrike Falconなどのシスコ以外の製品との統合だけでなく、応答エンジンの運用における運用のベストプラクティスと実装の詳細についても説明します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：テクニカルセミナー
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：セキュリティ

DevNet

セキュリティ自動化：SecureXを使用した開発 – DEVNET-1083

マット・バンダー・ホルスト、テクニカルリーダー、シスコ – 上級スピーカー

シスコのXDRプラットフォームには、セキュリティ運用を自動化し、強力な統合を構築するための複数の方法があることをご存知でしたか？SecureX統合モジュールを使用すると、他のプラットフォームのデータを調査に取り込むことができます。また、SecureX Threat Response APIを使用すると、脅威の調査および対処方法を自動化できます。また、SecureXオーケストレーションを使用すると、低負荷なコードのドラッグアンドドロップエディタを使用して強力なワークフ

ローを構築できます。このセッションでは、SecureXの3つの側面の詳細と、それらを使用してセキュリティ運用を強化する方法について説明します。

セッションタイプ：DevNet
技術レベル：導入部
テクノロジー：SecureX、セキュリティ

トラック：DevNet

SecureXとKenna Securityによるサイバー衛生業務の自動化 – DEVLIT-1355

シスコテクニカルソリューションアーキテクト、Oxana Sannikova

IT運用は現在でも非常に手動で行われています。お客様は常に、システムの健全性を維持し、オンラインセキュリティを改善するという課題に直面しています。このクイックセッションでは、Cisco SecureXオーケストレーションとKenna Securityを活用して脆弱性管理を自動化する方法について説明します。

セッションタイプ：DevNet
技術レベル：中級
テクノロジー：自動化とオーケストレーション、セキュリティ
トラック：DevNet

SecureXオーケストレーションを使用したパブリッククラウドのインシデント対応の自動化 – DEVWKS-2240

Brian Sak、テクニカルソリューションアーキテクト、シスコシステムズ – 講演者

ワークロードがAWS、Azure、GCPなどのパブリッククラウドプロバイダーに移行すると、インシデントの対応と修復がより困難になり、異なるツールが必要になります。このセッションでは、SecureXオーケストレーションワークフローの作成について説明します。このワークフローにより、脅威の特定プロセスの自動化と簡素化、対応手順の簡素化が実現し、セキュリティチームがマルチクラウドまたはハイブリッドクラウド環境でリソースを保護する際の安心感が得られます。
今年の新しいDevNetワークショップの席は、事前に登録された参加者が最初に着席します。このセッションで使用できるノートPCは12台のみです。これは、インストラクターと一緒にコーディングする実践的なDevNetワークショップです。独自の3.5mm AUXコネクタヘッドフォンを持ち込んでプレゼンターの声を聞いたり、DevNet Command Centerでヘッドフォンを取り上げたりしてください。
このDevNetワークショップに参加すると、シスコの継続的な教育(CE)クレジットを取得できます。詳細については、https://www.cisco.com/c/en/us/training-events/training-certifications/training/continuing-education-program.html#~qualifying-optionsを参照してください。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：DevNet
技術レベル：中級

テクノロジー：SecureX、セキュリティ
トラック：DevNet

SecureX Orchestratorとリモートコネクタを使用したハイブリッドクラウドワークフローの拡張 – DEVNET-2109

スティーブ・マクナット氏（シスコテクニカルソリューションアーキテクト）

SecureXオーケストレーション(SXO)は、セキュリティオーケストレーションのコンテキストで使用されます。さらに多くのことを実現し、効果的なハイブリッドクラウド運用ツールを作成するための基盤となることを示します。このセッションでは、まずアーキテクチャの概要を説明し、次にCisco Umbrellaの大量導入ソリューションの例を紹介し、コンポーネントの組み合わせとそのソリューションで解決できる課題について説明します。このセッションでは、サイドカーパターンを活用して高度にスケーラブルなハイブリッドクラウドワークフローを構築する方法を理解し、独自のソリューションを構築するために変更できるサンプルコードに精通していることを確認します。

セッションタイプ：DevNet
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：DevNet

XDRでのRカウントを2倍にする：Cisco SecureXで10クリック以内にセキュリティ運用(SecOps)を自動化する方法（コード行を記述しない）- DEVNET-2214

クリストファー・ヴァン・デル・マード氏（シスコ、エンジニアリングプロダクトマネージャ）– 講演要人

このセッションでは、コードを記述することなく、SecureXオーケストレーションを通じて自動化の力を活用する方法について説明します。これにより、組織はシスコのXDR(eXtended Detection and Response)でRカウントを2倍にすることができます。私たちは、あなたが実行して地面に当たるようにするいくつかの非常に簡単な例をインストールします。コンソールで必要なクリック数をメトリックとして使用し、急ぎすぎることなく強力な自動化にアクセスする方法を実証します。最後に、これを一歩進めて、セキュリティ運用を自動化するマスターになる方法も学びます。その後、すべての資料を入手して、自分で始めます。このセッションは、インシデント対応担当者、セキュリティアナリスト、SOCマネージャ、または自動化とセキュリティに関心のあるすべての人を対象としています。

セッションタイプ：DevNet
技術レベル：中級
テクノロジー：SecureX、セキュリティ
トラック：DevNet

Microsoft Graph APIとの統合：PythonおよびSecureXの使用 – DEVWKS-3260

Hacke Nohre、テクニカルソリューションアーキテクト、シスコ – 上級スピーカー

このワークショップでは、一般的なシスコ環境にMicrosoft Graph APIを統合する方法について説明します。
ここでは、Microsoft Graph APIの概要を説明し、Oauth2認証とAzure ADへの承認に焦点を当てます。
次に、PythonスクリプトとSecureXの両方からこのAPIにアクセスして、特定のユーザーのAzure ADグループとロールに関する情報にアクセスする方法を示します
microsoft環境からセキュリティイベントに関する情報にアクセスする
参加者は、ワークショップ中にラボ環境からワークショップの手順に従うことも、後で手順を完了することもできます。独自のAzureまたはSecureXアカウントがなくても、参加者が自分でワークショップタスクを完了できるラボのセットアップへのポインタを提供します。

シスコの継続的な教育クレジットの認定：はい
セッションタイプ：DevNet
技術レベル：上級
テクノロジー：DevNet、セキュリティ
トラック：DevNet

SecureXでランサムウェア防御を自動化およびシンプル化 – DEVNET-1456

Elia Maracani、システムエンジニア、シスコシステムズ社

ランサムウェアの攻撃は、バックアップにますます重点を置くようになっています。企業のバックアップを迅速かつ容易に回復するだけでなく、保護することが、ランサムウェア攻撃を防ぐ上で最善かつ最も重要なステップになります。デモを通じて、SecureXがオーケストレーションエンジンを通じて提供できる汎用性とカスタマイズについて説明します。Cisco SecureXが第1のソリューション(Cisco Umbrella、Cisco Secure Endpoint)とサードパーティのソリューション(Cohesity Helios)の両方に統合されているため、ランサムウェアの検出、調査、および回復にかかる時間と複雑さを大幅に削減できます。

セッションタイプ：DevNet
技術レベル：導入部
テクノロジー：SecureX、セキュリティ
トラック：DevNet

製品または戦略の概要

Cisco XDR：将来のセキュリティオペレーションセンターのための構築 – PSOSEC-1007

サナ・サナ・ユースフ氏（シスコ、プロダクトマーケティングマネージャ）

セキュリティチームは、拡大する脅威の状況と複雑な環境に直面しているため、セキュリティの有効性はますます見えにくくなっています。サイバーセキュリティの貧困線は拡大し、悪意のある攻撃者はこの穴を利用して執拗な攻撃を放っています。お客様の環境でTurla、Wannacry、NotPetyaなどの高度な攻撃者を検出して修復できるのは、効果的な「拡張された検出および対応

」ソリューションだけであると考えています。ハイブリッド、マルチベンダー、マルチベクトルの世界におけるXDRの破壊的な価値について説明します。将来のセキュリティ運用を構築するための基盤として、マルチベンダーのテクノロジー統合エコシステムが継続的に成長を続けていることを説明します。また、XDRはSOCのフォースマルチプライヤーになりうるのでしょうか。

セッションタイプ：製品または戦略の概要
技術レベル：一般
テクノロジー：SecureX、ハイブリッドクラウド、セキュリティ
トラック：セキュリティ

セキュリティの復元力を積極的に強化する方法 – PSOCX-2000

Varun Dhingra (シスコシステムズ社、プロダクトマネジメントセキュリティ&コラボレーション担当シニアディレクタ)
シスコシステムズプロダクトマネジメントディレクター、マーク・ハモンド

サイバーセキュリティを管理する必要があるだけでなく、データプライバシーに基づく規制を採用しなければならないという現実の圧力にも直面しています。リスク、規制、ビジネス目標、および運用への影響という絶え間なく変化する要件を満たすサイバーセキュリティプログラムをどのように設計しますか。このセッションでは、関係者のニーズを満たし、ビジネスの俊敏性を実現するソリューションを作成するために、業界向けのデータセキュリティおよびプライバシーフレームワークを設計する方法について学習します。このフレームワークは、目的とするサイバーセキュリティ活動と成果を追跡するように設計されており、直感的に複数の専門分野にまたがるチーム間で技術的でないシンプルなコミュニケーションを可能にします。

セッションタイプ：製品または戦略の概要
技術レベル：中級
テクノロジー：カスタマーエクスペリエンス、SecureX、セキュリティ

その他の機会

上記の多くのセッションタイプに加えて、ライブ！は会議フロアで多くのイノベーションとインスピレーションを持っています。 エンジニアとのミーティング、旗の獲得、チャレンジのライブを通じて、シスコが実現できる架け橋であることを継続的にデモンストレーションします。 詳細については、Ciscolive.comを参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。