



The bridge to possible

Cisco XDR

Сенс рішення

Павло Родіонов, CCIE 11155, CISSP, GREM
Solutions Engineer, рішення Cisco Security
prodiono@cisco.com

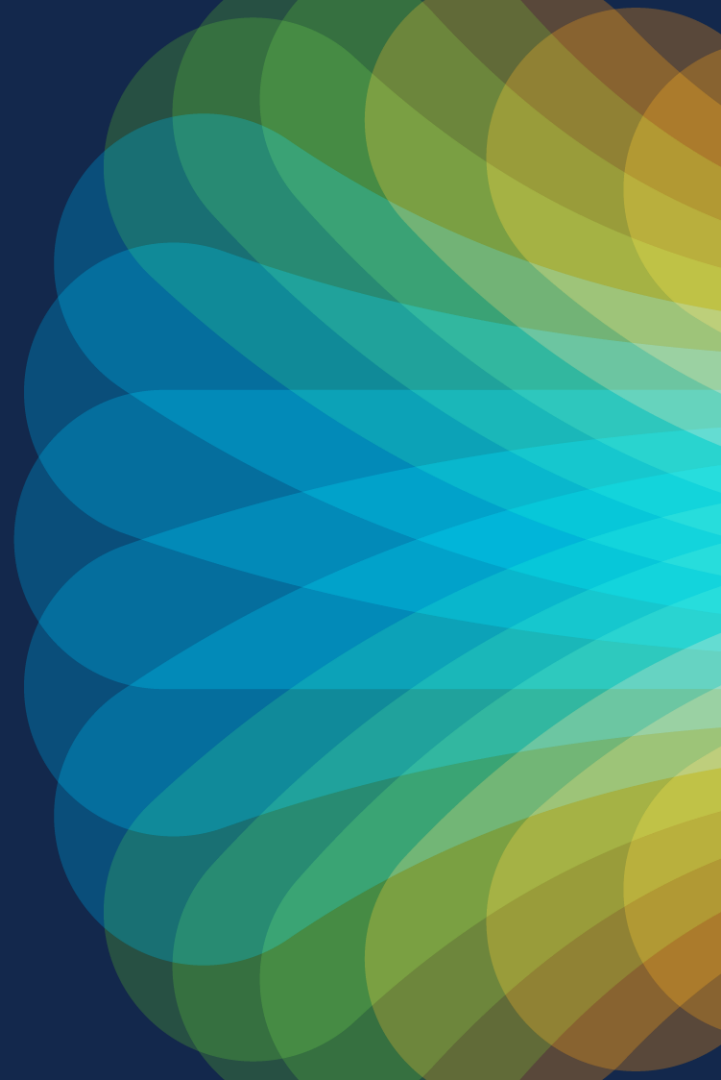
cisco Live!

BRKSEC-2113

Agenda

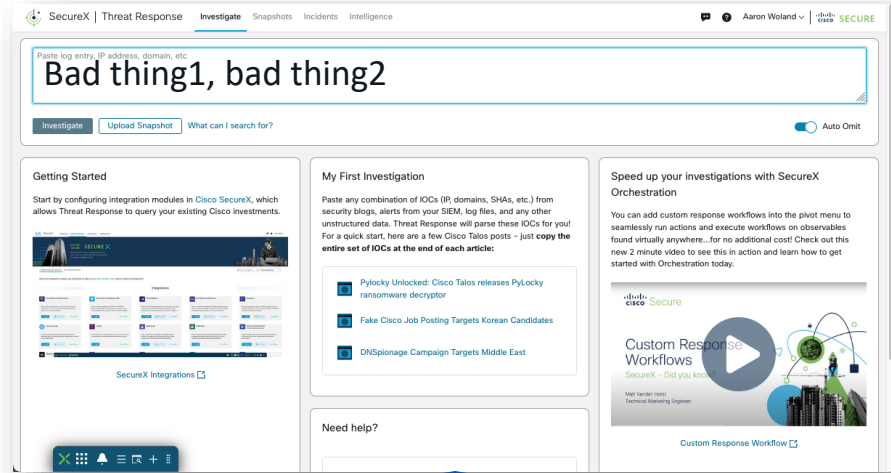
- Урок історії
- Еволюція
- Керування інцидентами і процеси
- Інтеграція та реагування
- Ключова телеметрія XDR
- Це все!

Невеликий урок історії



Ще у 2017 році

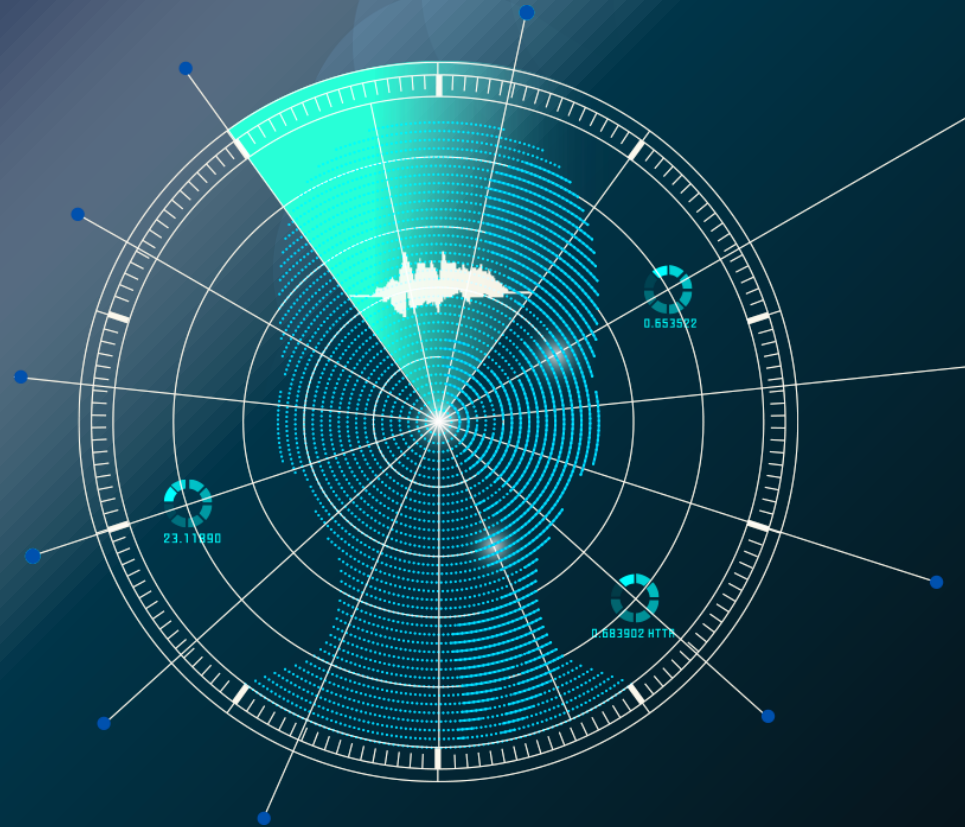
- Улюблений проєкт Security Leadership: «visibility»
- перейменованій на Cisco Threat Response (2018)
- На основі історії виконання incident response
- Продукція процесу, якого вони дотримувалися як практики
- Шукайте "observables", і він збагачується з усіх інтегрованих джерел (через API) "findings"
- Примітка: Cisco придбала Obsrvbl Networks в тому саме році



Ви бачили ознаки цих observables?

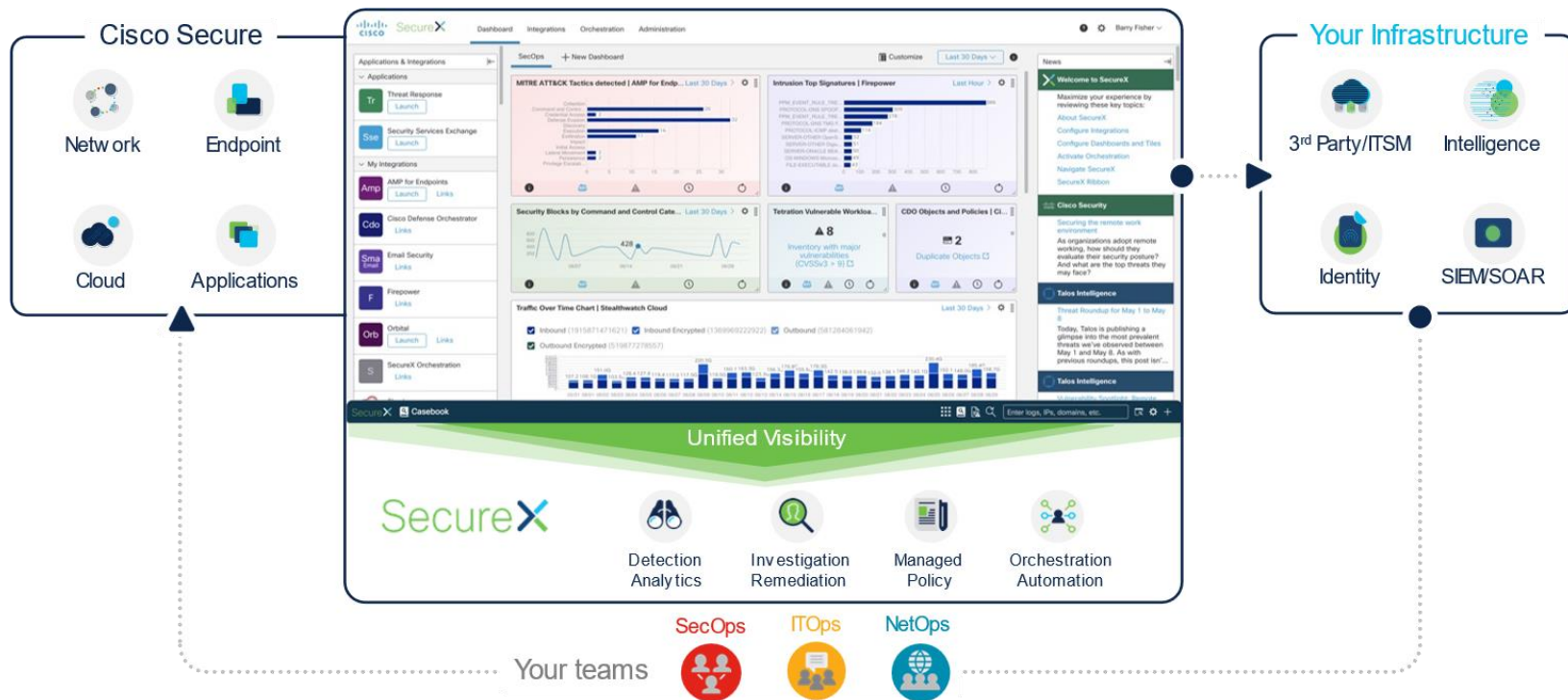


Потім в 2020...



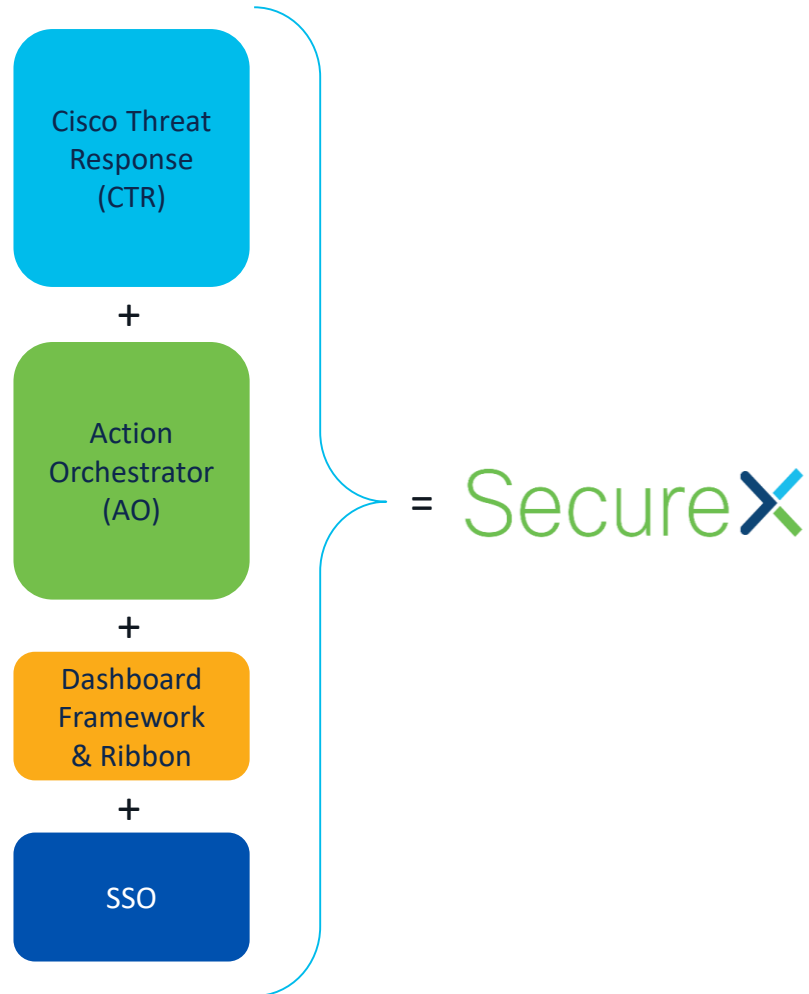
Представлено SecureX у травні 2020 року

Хмарна **вбудована** платформа в нашому портфоліо

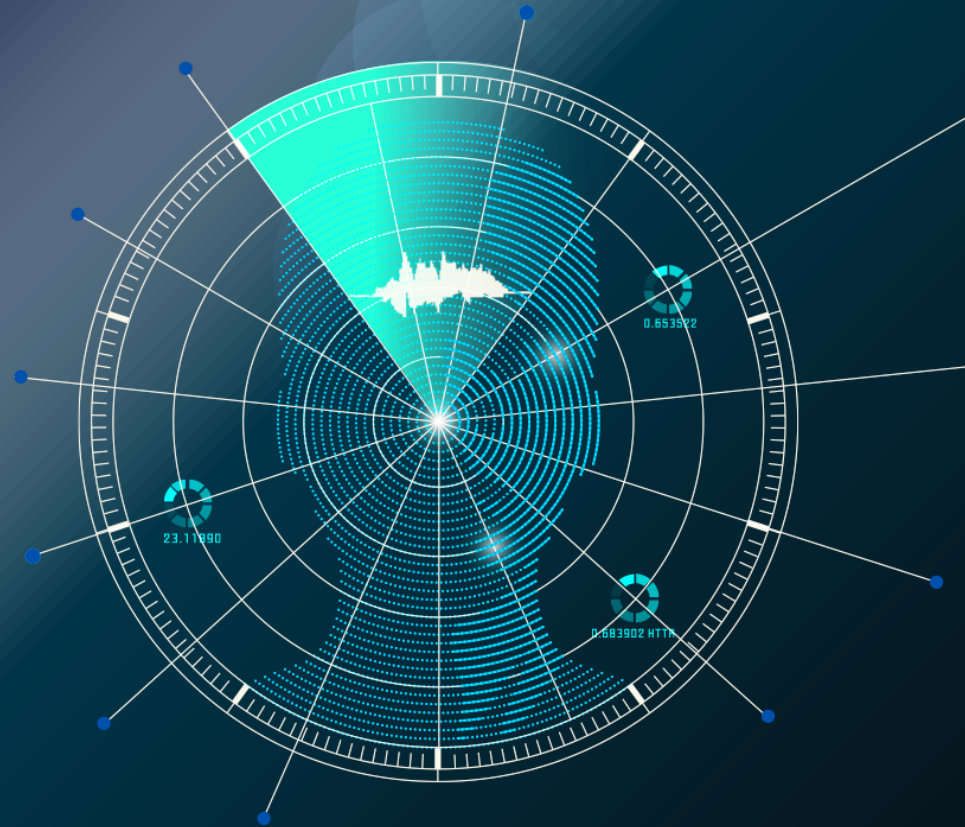


SecureX мав стати платформою

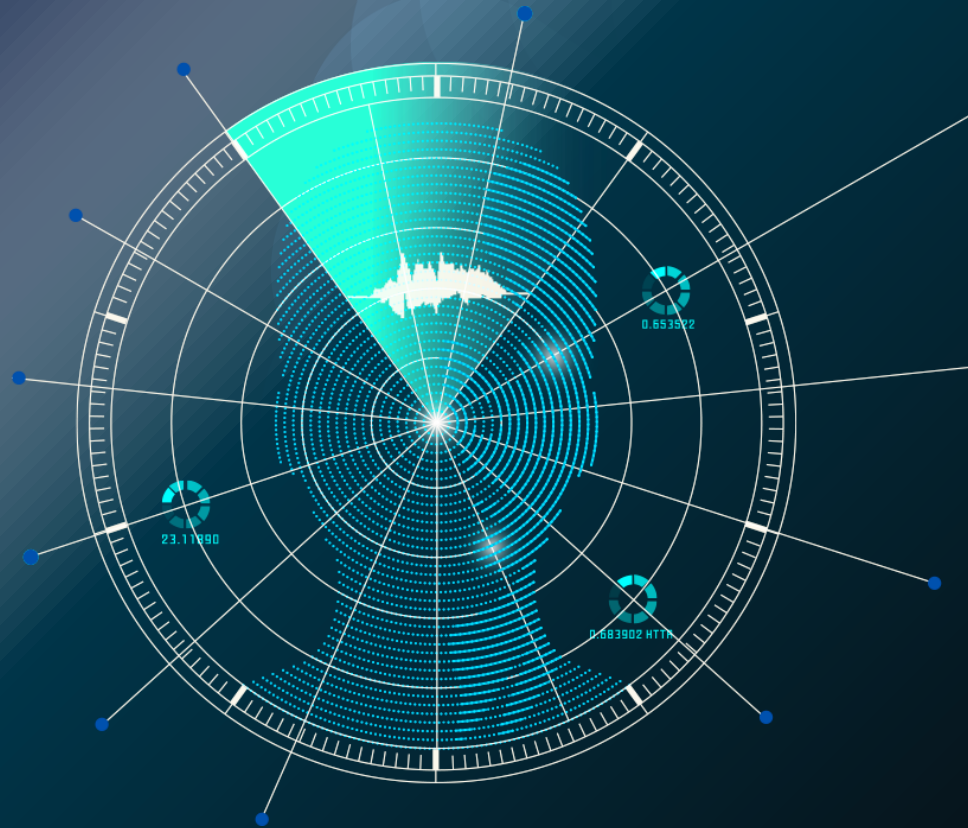
- Cisco Secure [function]
 - X мав стати центральним місцем
 - X використовував Cisco Threat Response для інтеграції всіх продуктів Cisco разом
 - X додає повний механізм автоматизації, який ми «придбали» у хмарного підрозділу
 - X надав досвід єдиного входу для безпеки Cisco
 - Усі майбутні інтерфейси користувача будуть побудовані на SecureX



У 2021 році аналітики створили нову ринкову категорію «eXtended detection & Response»



Сіско повністю
прийняла
концепцію XDR;
розглядаючи це як
ринковий перехід



Cisco з головою занурюється в простір XDR

Найняли зовнішню дослідницьку та дизайнерську компанію, щоб доповнити нас

1

Інвестує мільйони в дослідження

Клієнти навіть не знали, що спілкуються з Cisco (наосліп), а також наші власні відгуки клієнтів

3

Прямі та дотичні опитування

Використання НАЙКРАЩОЇ технології для досягнення визначеного досвіду, а не побудова досвіду на основі технології

5

Реструктуризація наших продуктів

Значні внутрішні інвестиції

2

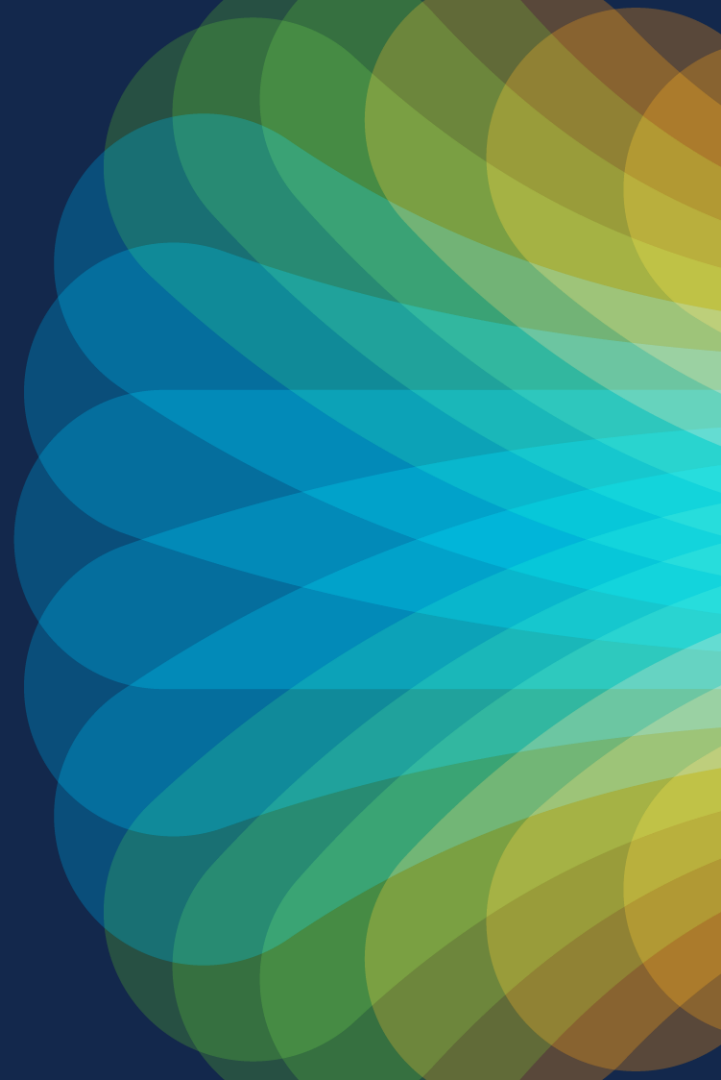
Розширення наших команд User Experience та Interface

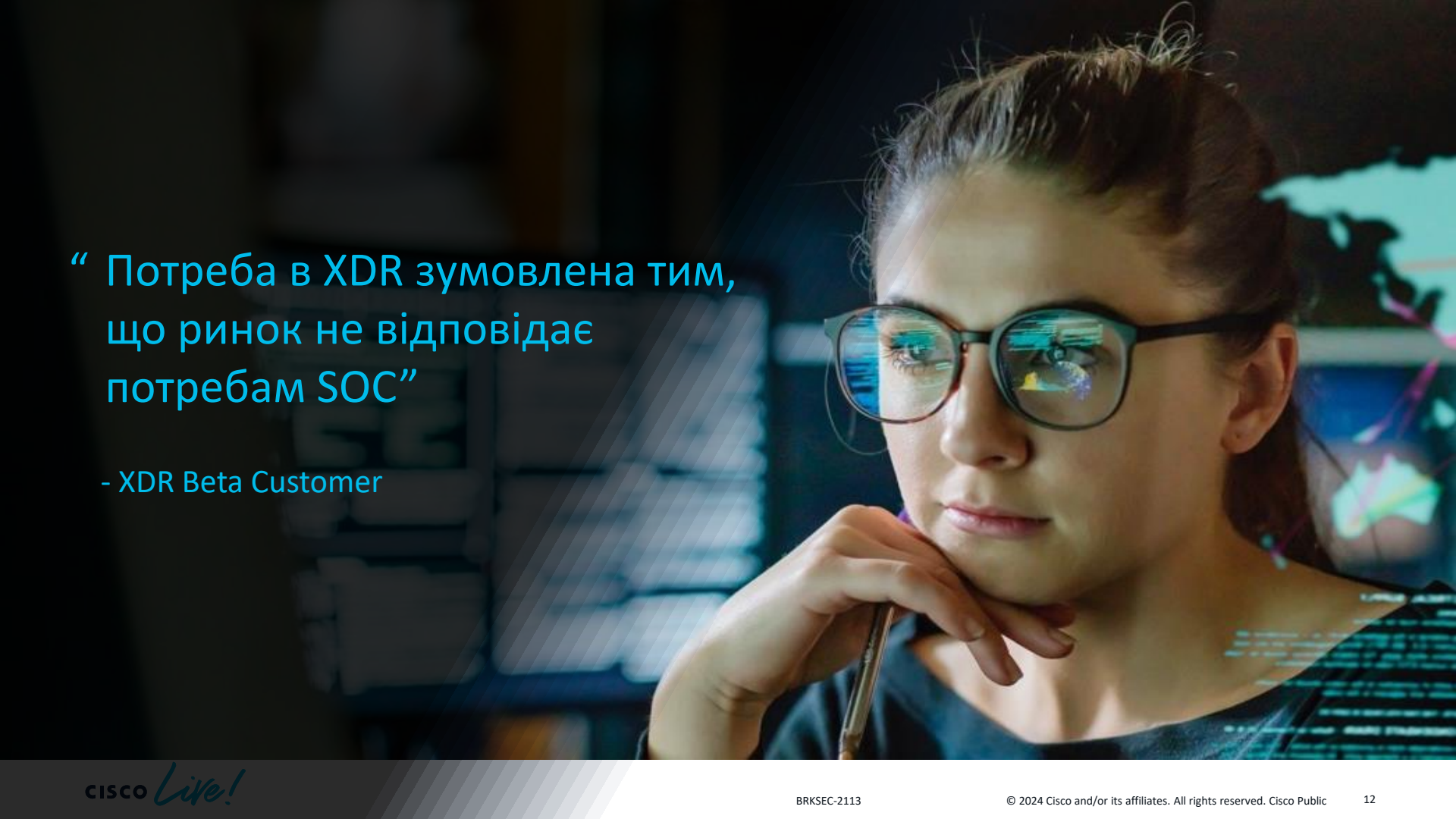
Широкий найм експертів

4

Залучили головних інженерів у ключових місцях з величезним досвідом управління інцидентами / SOC

Що це дало?



A woman with dark hair tied back, wearing glasses, is looking thoughtfully to the right. Her hand is resting on her chin. The background is a server room with racks of equipment and a glowing world map on a screen.

“ Потреба в XDR зумовлена тим,
що ринок не відповідає
потребам SOC”

- XDR Beta Customer



Bopor
Turla



// **Nickname**

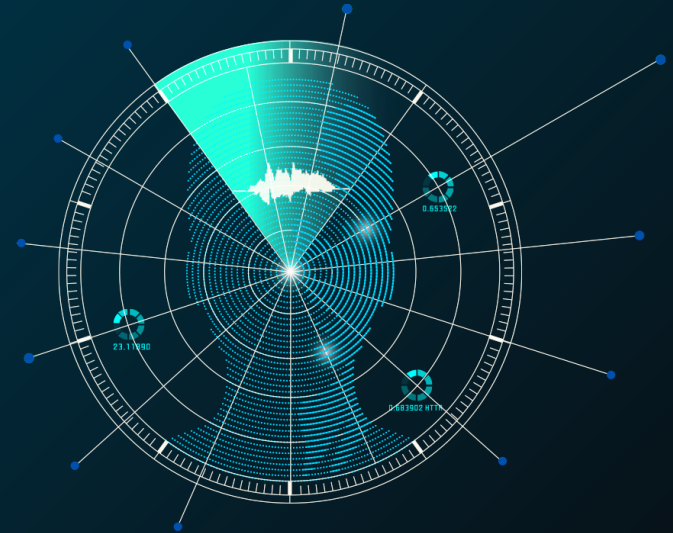
Snake,
Venomous Bear,
Uroburos,
Group 88,
Waterbug

Супротивник: що відомо?

- Естонські спецслужби пов'язують це угруповання з Федеральною службою безпеки Росії (ФСБ).
- НЕ розгортає розширені інструменти, якщо це не необхідно для компрометації цілі

Метод:

- Віддає перевагу водопоям і соціальній інженерії для маніпулювання жертвами
- Виготовлені приманки ретельно пристосовані до своїх цілей
- Теми-експлойти, пов'язані з поточними подіями
- Шкідливе програмне забезпечення першого етапу зазвичай діє як фільтр



Як без XDR ми можемо виявляти все це та реагувати на нього?

TA0001: Initial Access	TA0002: Execution	TA0003: Persistence
T1188: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1098: Account Manipulation
T1190: Exploit of Public-Facing Application	T1203: Exploitation for Client Execution	T1197: BITS Jobs
T1133: External Remote Services	T1529: Inter-Process Communication	T1547: Boot or Logon Autostart Execution
T1200: Hardware Additions	T1106: Native API	T1037: Boot or Logon Initialization Scripts
T1566: Phishing	T1566.001: Spearphishing Attachment	T1176: Browser Extensions
	T1566.002: Spearphishing Link	T1554: Compromise Client Software Binaries
	T1566.003: Spearphishing via Service	T1136: Create Account
T1091: Replication Through Removable Media	T1072: Software Deployment Tools	T1543: Create or Modify System Process
T1195: Supply Chain Compromise	T1569: System Services	T1546: Event Triggered Execution
T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1133: External Remote Services
		T1574: Hijack Execution Flow
		T1556: Modify Authentication Process
		T1137: Office Application Startup
		T1542: Pre-OS Boot
		T1053: Scheduled Task/Job
		T1055: Server Software Component

T1112: Modify Registry	T1027.001: Binary Padding
T1027: Obfuscated Files or Information	T1027.004: Compile After Delivery
	T1027.006: HTML Smuggling
	T1027.005: Inlet or Removal from Tool
	T1027.002: Software Packing
	T1027.003: Steganography
T1542: Pre-OS Boot	T1055.006: Asynchronous Procedure Call
T1055: Process Injection	T1055.001: Dynamic Link Library List
	T1055.011: Extra Random Memory Injection
	T1055.015: ListPaging
	T1055.005: Portable Executable Injection
	T1055.009: Proc Memory
	T1055.013: Process Doppelgänger
	T1055.012: Process Hollowing
	T1055.008: Process System Calls
	T1056.003: Thread Execution Hijacking
	T1055.025: Thread Local Storage
	T1055.014: VDSO Hijacking

TA0001: Command and Control	TA0010: Exfiltration
T1071: Application Layer Protocol	T1071.004: DNS
	T1071.002: File Transfer Protocols
	T1071.003: Mail Protocols
	T1071.001: Web Protocols
T1092: Communication Through Removable Media	T1132.002: Non-Standard Encoding
T1132: Data Encoding	T1132.001: Standard Encoding
	T1001.001: Junk Data
	T1001.003: Protocol Impersonation
	T1001.002: Steganography
T1568: Dynamic Resolution	T1573.002: Asymmetric Cryptography
T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
T1008: fallback Channels	
T1105: Ingress Tool Transfer	
T1104: Multi-Session Channels	
T1095: Non-Application Layer Protocols	
T1571: Non-Standard Path	
T1572: Protocol Tunneling	
T1090: Proxy	T1090.004: Domain Fronting
	T1090.002: Internal Proxy
	T1090.001: External Proxy
	T1090.003: Multi-Hop Proxy
T1219: Remote Access Software	
T1205: Traffic Signaling	T1205.001: Port Knocking
T1102: Web Service	T1102.002: Bi-directional Communication
	T1102.001: Dead Drop Resolver
	T1102.003: One-Way Communication

TA0006: Credential Access	TA0007: Discovery
T1557: Adversary-in-the-Middle	T1087: Account Discovery
T1180: Brute Force	T1180.004: Credential Stuffing
	T1180.002: Password Cracking
	T1180.001: Password Guessing
T1555: Credential Access from Password Store	T1010: Application Window Discovery
	T1217: Browser Bookmark Discovery
	T1227: Debugger Execution
	T1555.003: Credentials from Web Browsers
	T1555.005: Password Managers
	T1555.002: Secure Local Memory
	T1555.004: Windows Credential Manager
T1212: Exploitation for Credential Access	T1042: Debugger Evasion
T187: Forced Authentication	T1575: Network Shared Drive Discovery
T606: Forge Web Credentials	T1042: Network Sniffing
T056: Input Capture	T1056.004: Credential API Hooking
	T1056.002: GUI Input Capture
	T1056.001: Keylogging
	T1056.003: Web Portal Capture
T1556: Modify Authentication Process	T1057: Process Discovery
T111: Multi-Factor Authentication Interception	T1012: Query Registry
T021: Multi-Factor Authentication Request Generation	T1018: Network Service Discovery
	T1515: Software Discovery
T003: OS Credential Dumping	T1018.001: Security Software Discovery
	T1018.002: System Information Discovery
	T1018.004: System Location Discovery
	T1018.005: System Network Configuration
	T1018.001: System Network Connections Discovery
	T1018.001: System Owner/Discovery
	T1018.003: NTDS
	T1018.002: System Service Discovery
	T1018.004: Proc Filesystem
	T1124: System Time Discovery
	T1050.002: Security Account Manager
	T1497: Virtualization/Sandbox Evasion
T1538: Steal Web Session Cookies	
T1552: Unsecured Credentials	T1552.003: Bash History
	T1552.001: Credential Files
	T1552.002: Credential in Registry
	T1552.006: Group Policy Preferences
	T1552.004: Private Keys

T1028: Account Manipulation	T1190: Exploit of Public-Facing Application
T1028.001: Remote Account Hijacking	T1190.001: Exploit of Remote Services
T1028.002: Local Account Hijacking	T1190.002: Exploit of Local Services
T1028.003: Remote Shell	T1190.003: Exploit of Network Services
T1028.004: Local Shell	T1190.004: Exploit of Database Services
T1028.005: Remote Desktop Protocol	T1190.005: Exploit of Web Services
T1028.006: Remote Web Services	T1190.006: Exploit of Mobile Services
T1028.007: Remote Desktop Gateway	T1190.007: Exploit of VoIP Services
T1028.008: Remote Desktop Connection Broker	T1190.008: Exploit of Cloud Services
T1028.009: Remote Desktop Connection Gateway	T1190.009: Exploit of SaaS Services
T1028.010: Remote Desktop Connection Session	T1190.010: Exploit of PaaS Services
T1028.011: Remote Desktop Connection Host	T1190.011: Exploit of IaaS Services
T1028.012: Remote Desktop Connection Client	T1190.012: Exploit of SaaS Services
T1028.013: Remote Desktop Connection Gateway	T1190.013: Exploit of PaaS Services
T1028.014: Remote Desktop Connection Host	T1190.014: Exploit of IaaS Services
T1028.015: Remote Desktop Connection Client	T1190.015: Exploit of SaaS Services
T1028.016: Remote Desktop Connection Gateway	T1190.016: Exploit of PaaS Services
T1028.017: Remote Desktop Connection Host	T1190.017: Exploit of IaaS Services
T1028.018: Remote Desktop Connection Client	T1190.018: Exploit of SaaS Services
T1028.019: Remote Desktop Connection Gateway	T1190.019: Exploit of PaaS Services
T1028.020: Remote Desktop Connection Host	T1190.020: Exploit of IaaS Services
T1028.021: Remote Desktop Connection Client	T1190.021: Exploit of SaaS Services
T1028.022: Remote Desktop Connection Gateway	T1190.022: Exploit of PaaS Services
T1028.023: Remote Desktop Connection Host	T1190.023: Exploit of IaaS Services
T1028.024: Remote Desktop Connection Client	T1190.024: Exploit of SaaS Services
T1028.025: Remote Desktop Connection Gateway	T1190.025: Exploit of PaaS Services
T1028.026: Remote Desktop Connection Host	T1190.026: Exploit of IaaS Services

T1620: Reflective Code Loading	
T1207: Rogue Domain Controller	
T1014: Rookits	
T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1553.006: Code Signing Policy Modification
	T1553.004: Install Root Certificate
	T1553.005: Mark-of-the-Web Bypass
T1218: System Binary Proxy Execution	T1553.003: SIP and Trust Provider Hijacking
	T1218.003: COMET
	T1218.001: Compiled HTML File
	T1218.002: Control Panel
	T1218.004: InstallUI
	T1218.013: NavAgent
	T1218.014: MMC
	T1218.005: Mht
	T1218.007: Mixsec
	T1218.008: Odoocon
	T1218.009: Registry/Regasm
	T1218.010: Registry3
	T1218.011: Rand133
	T1218.012: Verclsid
T1216: System Script Proxy Execution	
T1221: Template Injection	
T1127: Trust of Developer Utilities Proxy Execution	
T1550: Use of Alternate Authentication Methods	T1550.002: Pass the Hash
	T1550.003: Pass the Ticket
T1078: Valid Accounts	T1078.001: Default Accounts
	T1078.002: Domain Accounts
	T1078.003: Local Accounts
T1497: Virtualization/Sandbox Evasion	
T1200: XSL Script Processing	









TA0008: Lateral Movement	TA0009: Collection
T1210: Exploitation of Remote Services	T1557: Adversary-in-the-Middle
T1534: Internal Spearphishing	T1560: Archive Collected Data
T1570: Lateral Tool Transfer	T1560.002: Archive via Library
T1558: Remote Service Session Hijacking	T1560.001: Archive via URL
	T1560.003: Archive via Custom Method
	T1560.004: Archive via Webhook
	T1560.005: Archive via FTP
	T1560.006: Archive via SFTP
	T1560.007: Archive via SMB
	T1560.008: Archive via WebDAV
	T1560.009: Archive via WebDAV
	T1560.010: Archive via WebDAV
	T1560.011: Archive via WebDAV
	T1560.012: Archive via WebDAV
	T1560.013: Archive via WebDAV
	T1560.014: Archive via WebDAV
	T1560.015: Archive via WebDAV
	T1560.016: Archive via WebDAV
	T1560.017: Archive via WebDAV
	T1560.018: Archive via WebDAV
	T1560.019: Archive via WebDAV
	T1560.020: Archive via WebDAV
	T1560.021: Archive via WebDAV
	T1560.022: Archive via WebDAV
	T1560.023: Archive via WebDAV
	T1560.024: Archive via WebDAV
	T1560.025: Archive via WebDAV
	T1560.026: Archive via WebDAV
	T1560.027: Archive via WebDAV
	T1560.028: Archive via WebDAV
	T1560.029: Archive via WebDAV
	T1560.030: Archive via WebDAV
	T1560.031: Archive via WebDAV
	T1560.032: Archive via WebDAV
	T1560.033: Archive via WebDAV
	T1560.034: Archive via WebDAV
	T1560.035: Archive via WebDAV
	T1560.036: Archive via WebDAV
	T1560.037: Archive via WebDAV
	T1560.038: Archive via WebDAV
	T1560.039: Archive via WebDAV
	T1560.040: Archive via WebDAV
	T1560.041: Archive via WebDAV
	T1560.042: Archive via WebDAV
	T1560.043: Archive via WebDAV
	T1560.044: Archive via WebDAV
	T1560.045: Archive via WebDAV
	T1560.046: Archive via WebDAV
	T1560.047: Archive via WebDAV
	T1560.048: Archive via WebDAV
	T1560.049: Archive via WebDAV
	T1560.050: Archive via WebDAV



Важливість джерела телеметричних даних

Шість основних джерел даних, які, на думку клієнтів, є важливими для XDR:

Endpoint, Network, Firewall, Identity, Email and DNS

Essential		
	Count	Share
 Endpoint	255	85.0%
 Network	226	75.3%
 Firewall	207	69.0%
 Identity	191	63.7%
 Email	179	59.7%
 DNS	140	46.7%
 Public Cloud	137	45.7%
 Non-Security Sources	36	12.0%



Cisco Secure Client



Cisco/ Meraki
(Networking)



Firewall Threat
Defense (FTD)



Duo

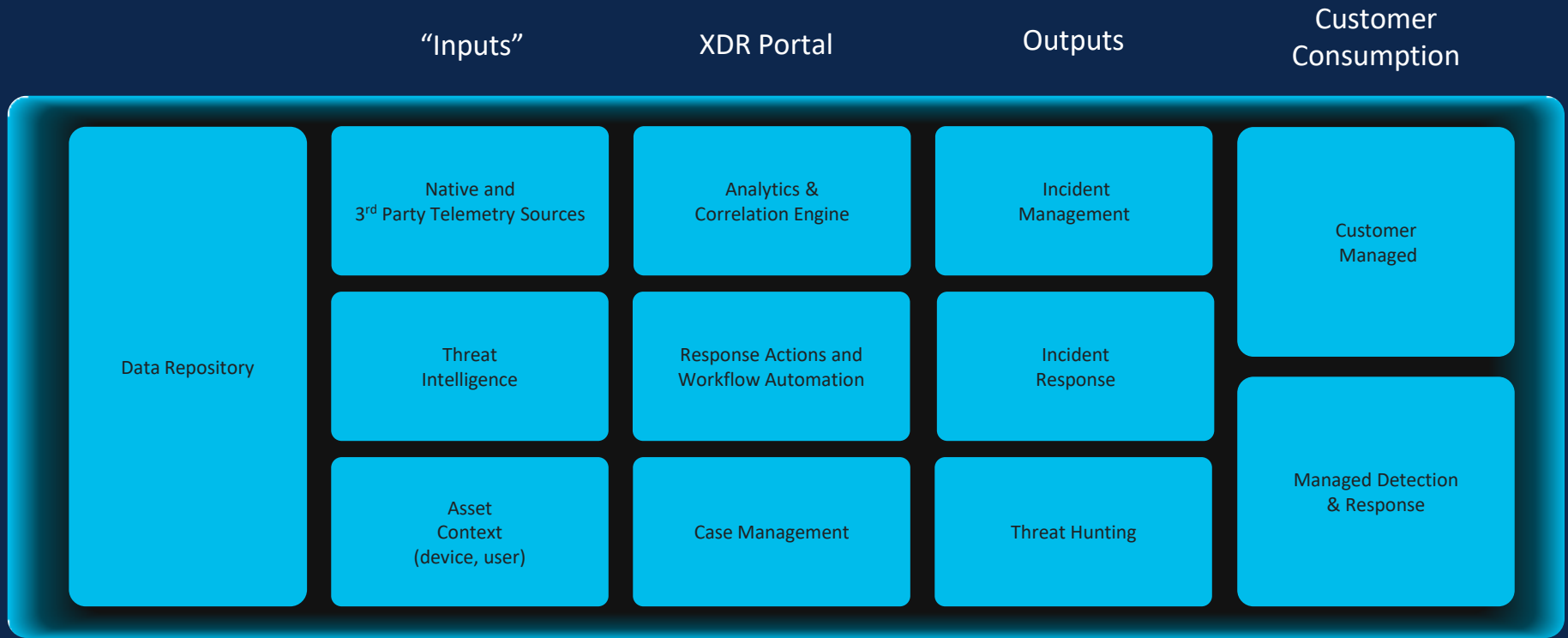


Email Threat Defense
(ETD)

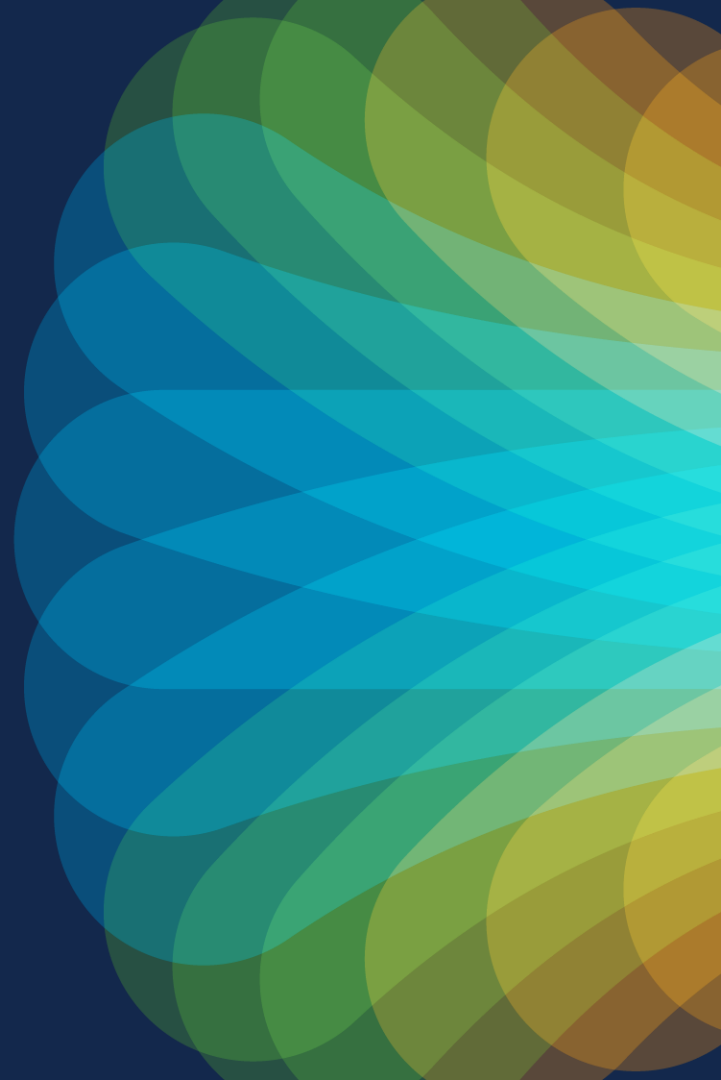


Umbrella

З яких складових блоків складається ідеальне рішення XDR?



Як ми цього
досягаємо?



Еволюція

- Частина SecureX
- *Плюс* Secure Cloud Analytics
- *Плюс* Kenna Intellectual Property
- *Плюс* нові технології
- *Дорівнює* Cisco XDR



Evolving Into

Cisco XDR

The screenshot shows the Cisco XDR 'Incidents' dashboard. It features a dark theme with a sidebar on the left containing navigation options like 'Incidents', 'Investigate', 'Intelligence', 'Automate', 'Devices', 'Inventory', 'Sources', 'Deployment', 'Audit Logs', 'Profiles', 'Device Events', and 'Administration'. The main area displays a table of incidents with columns for Priority, Name, Source, Created, Assigned, and Status. Summary statistics at the top show 6,277 Incidents, 6,246 New Incidents, 4 Open Incidents, and 6,275 Unassigned Incidents. A search bar and filters are also visible.

Priority	Name	Source	Created	Assigned	Status
1000	ATW - SurfacePro4 in group ATW - Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	ATW - SurfacePro4 in group ATW - Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	ATW - SurfacePro4 in group ATW - Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	AWS Root Account Used for Cisco Security Demo - Aaron Wieland	Cisco Secure Cloud An.	22 Days	Unassigned	Open
327	ATW - SurfacePro4 in group ATW - Audit @ 20230429 20:27:33	Secure Endpoint	11 Days	Unassigned	New
278	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:27:03	Secure Endpoint	5 Hours	Unassigned	New
263	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:27:02	Secure Endpoint	5 Hours	Unassigned	New
263	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:27:01	Secure Endpoint	5 Hours	Unassigned	New
263	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:26:59	Secure Endpoint	5 Hours	Unassigned	New
263	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:26:58	Secure Endpoint	5 Hours	Unassigned	New
263	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:26:57	Secure Endpoint	5 Hours	Unassigned	New
263	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:26:56	Secure Endpoint	5 Hours	Unassigned	New
263	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:26:55	Secure Endpoint	5 Hours	Unassigned	New
263	atw-win10-arwatch.securitydemo.net in group ATW - Audit @ 20230510 15:26:55	Secure Endpoint	5 Hours	Unassigned	New

CISCO *Live!*

soon plus

ORT
now part of CISCO

*“XDR – це інструмент підвищення
продуктивності операцій безпеки”*

- Me

Топ-3 обов'язки SOC

Моніторинг та реагування

- Безперервний моніторинг систем безпеки.
- Сортування, аналіз та реагування на інциденти.
- Координація зусиль з реагування та комунікація із зацікавленими сторонами.

Операції управління

- Пошук загроз, збір кібераналітики та оцінка ризиків.
- Проведення оцінки вразливостей та тестування на проникнення.
- Тонке налаштування інструментів і процесів безпеки для оптимальної продуктивності.

Відповідність, Освіта, та Стратегія

- Розробка політик, дотримання нормативних вимог та управління постачальниками.
- Навчання користувачів за допомогою навчальних та інформаційних програм.
- Інформування про нові загрози для формування стратегії безпеки.

Загальні обов'язки SOC

Tier 1 (Triage):

- Фішингові кампанії
- Аналіз фішингових файлів
- Аналіз IP/доменів
- Видалення мобільних пристроїв
- Розслідування email
- Звіти про вразливості третьої сторони – пошук загроз
- Ескалація до T2

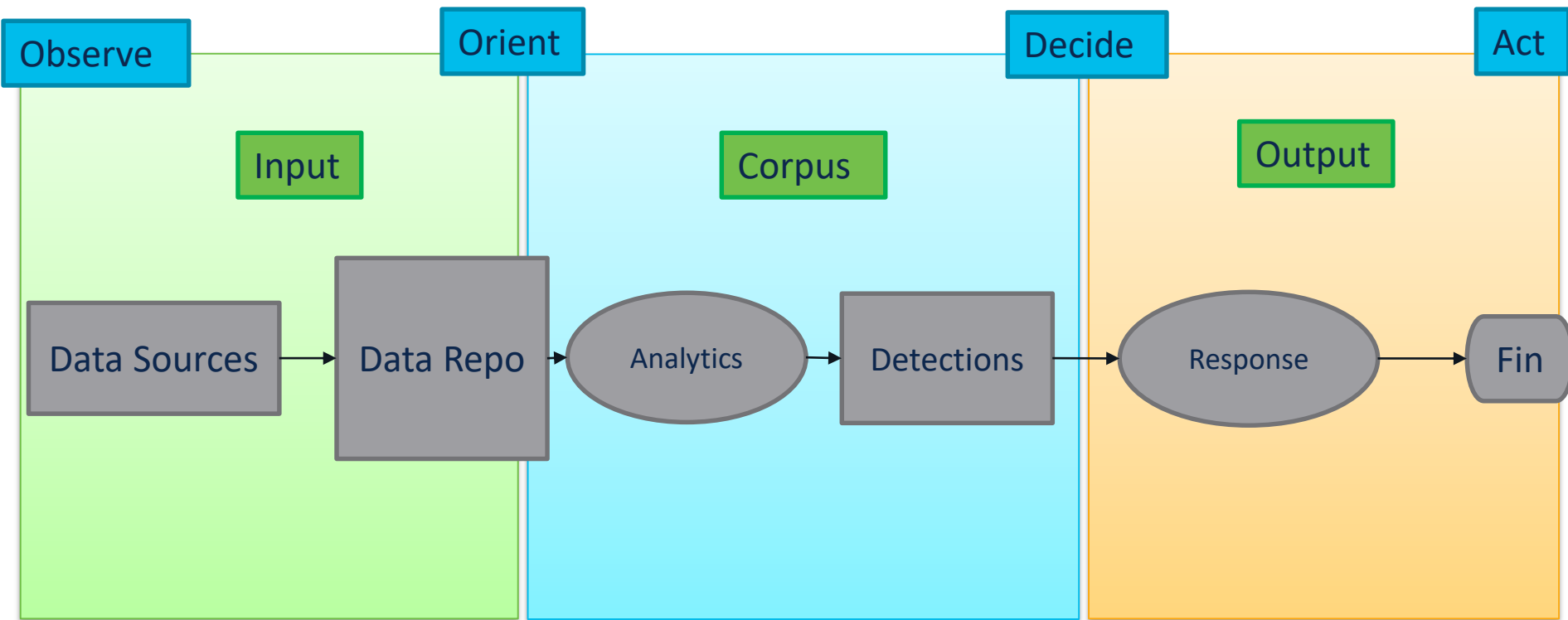
Tier 2 (Sr/Lead):

- Сповіщення IDS/IPS
- Шахраї-користувачі
- DNS Sinkholing домени
- Блокування IP/VPN
- DDoS
- Ескалація до СТІ/СТА/СТД/ІР
- Обліковий запис вимикається/стирає
- Збір forensics інформації

Shift Lead (Sr/T3):

- Створення та моніторинг dashboards
- Інструктаж співробітників
- Впевненість, що кожен виконує свою роботу
- Ситуативний перехід до інцидентів
- Керування чергою SOC
- Взаємодія з вендорами

XDR ускоряет цикл OODA




Аналітики будують
хронологію.

**XDR автоматизує
створення хронології**



Хронологія розслідування – що сталося і коли?

SOC / Admin



Розслідувач зазвичай будує часову шкалу під час розслідування



Починаючи звідси, дивіться вперед і назад для кореляції, щоб побудувати графік часової шкали / атаки «що сталося»

Отже, як ми можемо
змусити XDR працювати
з усіма цими
атаками/ТТР?

Нам потрібна аналітика та кореляція, а не лише спостереження

Obsrvbl Analytics Engine

Потужний механізм аналітики та кореляції SCA

SecureX & SCA інтеграція

Об'єднано фреймворки інтеграції з SecureX та Cloud Analytics для нової та вдосконаленої моделі інтеграції.

Зовнішнє збагачення

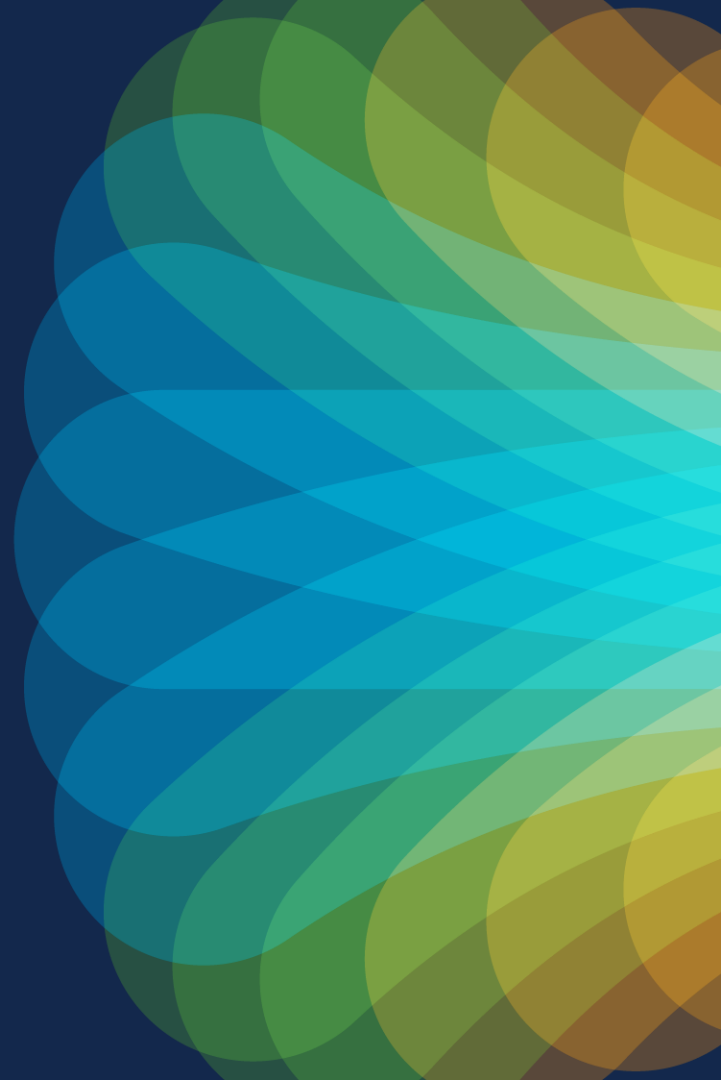
Протоколи збагачення від SecureX, не вимагаючи зберігання всіх даних в Data Repo (як це довелося б зробити SIEM).



Agenda

- Урок історії
- Еволюції
- Управління інцидентами та процесами
- Інтеграції та реагування
- Ключова телеметрія XDR
- Заключення!

Управління інцидентами та процесами



Cisco XDR – Incident Manager

Пріоритетна черга

Використовує (запатентований) Алгоритм від Кенна що базується на Asset Value + Risk of the TTPs

Короткий зміст інциденту

Поступове розкриття більш детальної інформації про інцидент – пріоритетні деталі, короткі / довгі описи, TTP

The screenshot displays the Cisco XDR Incident Manager interface. The main view shows a list of incidents with columns for Priority, Name, and Source. A green box highlights the 'Priority' column, which shows a score of 1000 for each incident. A yellow box highlights the 'Name' column, which shows the incident title: 'victim-win-2.org1.net in group Audit @ 20230514 03:19:'. The right-hand panel provides a detailed view of the selected incident, including its priority score breakdown (1000 total, 100 Detection Risk, 10 Asset Value at Risk), a short description, and a long description. The long description includes the incident title, promotion details, and indicators such as 'ExecutedMalware.ioc: A known malicious file was executed. This increases the likelihood of a successful breach and this event should be promptly investigated.'

Priority	Name	Source
1000	in group Audit @ 20230514 03:19:	Secure Endpoint
1000	dc-1.org1.net in group Audit @ 20230514 03:14:52	Secure Endpoint
1000	victim-win-6.org1.net in group Audit @ 20230514 03:13:	Secure Endpoint

Priority score breakdown

1000 | 100 Detection Risk | 10 Asset Value at Risk

Short description

Long description

Incident Title: victim-win-2.org1.net

Promoted at: 2023-06-04 19:47:01 UTC

Promotion method: Automated

Indicators: ExecutedMalware.ioc: A known malicious file was executed. This increases the likelihood of a successful breach and this event should be promptly investigated.

[View Incident Detail](#)

Cisco XDR – Диспетчер інцидентів / Огляд

Огляд

Схема для узагальнення інциденту. Не детальна схема розслідування.

Активи /
Спостережуваний об'єкт та індикатори

Найактивніший список із загальною кількістю, зазначеною вгорі.

The screenshot displays the Cisco XDR interface for an incident titled "victim-win-2.org1.net in group Audit @ 20230514 03:19:59". The interface is divided into several sections:

- Incident Overview:** Shows the incident title, reported by "Secure Endpoint" on "2023-05-14T03:19:59.000Z", and a "View Long Description" link.
- Network Diagram:** A central diagram showing relationships between entities. A green box highlights a flow from "75ed17bd4925660f..." to "powershell.exe", which then connects to "IP Address". Other entities include "SHA-256 Hash", "Endpoint", and "Endpoint Workstation".
- MITRE ATT&CK:** A dropdown menu on the right lists various MITRE ATT&CK techniques, including "TA0043: Reconnaissance", "TA0002: Execution", "TA0006: Credential Access", and "TA0007: Discovery".
- Assets and Observables:** A table at the bottom shows the most active assets and observables. The "Assets" section lists "victim-win-2.org1.net" (156 events), "victim-win-6.org1.net" (131 events), "LOXX-WIN10VIC02" (31 events), "dc-1" (14 events), and "SKTOP-V2IOAED" (7 events). The "Observables" section lists "http://169.254.169.254/meta..." (100 events), "victim-win-6" (20 events), "victim-win-2" (18 events), "9f914d42706fe215501044acd8..." (7 events), and "http://168.63.129.16/?comp=vers..." (1 event).
- Indicators:** A section showing "ExecutedMalware.ioc" (6 events) and "Internal Connection Watchlist Hit" (1 event).

Cisco XDR – Диспетчер інцидентів / Виявлення

Виявлення

Використовується для показу подій, які були пов'язані з цим інцидентом

Типи подій

Оригінал: сповіщення надіслано до XDR
Досліджено: корельовані події

The screenshot displays the Cisco XDR interface for an incident titled "victim-win-2.org1.net in group Audit @ 20230514 03:19:59". The interface includes a navigation menu, a search bar, and a "View Investigation" button. The incident is reported by "Secure Endpoint" on "2023-05-14T03:19:59.000Z" and is currently "Unassigned".

The "Detection" tab is active, showing a table of related events. The table has columns for "First Seen", "Severity", "Source", "Indicators", "Observables", and "Assets". A yellow box highlights the filter controls for "Type", "Source", and "Severity".

First Seen	Severity	Source	Indicators	Observables	Assets
2023-05-10T04:12:00.000Z	Critical	CrowdStrike Falcon Detection		9f914d42706fe215501044acd8...	DESKTOP-V2IOAED
2023-05-14T19:00:00.000Z	Critical	Cisco Secure Cloud Analytic...	Internal Connection Watchlist Hit		
2023-05-16T16:55:27.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN1DVIC02
2023-05-16T16:55:47.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN1DVIC02
2023-05-16T16:58:29.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN1DVIC02
2023-05-16T17:15:26.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN1DVIC02
2023-05-16T17:20:05.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN1DVIC02
2023-05-16T17:39:00.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN1DVIC02
2023-05-19T14:16:19.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	dc-1
2023-05-19T14:17:16.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	dc-1

At the bottom of the interface, there is a "10 per page" setting and a "1-10 of 350" indicator.

Cisco XDR – менеджер інцидентів / реагування

Відповіді

Контент, специфічний для TTP в інциденті

Крок через

Identification ->

Containment ->

Eradication -> Recovery

The screenshot displays the Cisco XDR interface for an incident titled "victim-win-2.org1.net in group Audit @ 20230514 03:19:59". The interface is divided into several sections:

- Incidents:** Shows the incident ID (1000), status (New), and a "View Investigation" button.
- Response Tab:** Contains a list of response actions:
 - Review Incident:** "Add a note to record the evidence (indicators and reasoning) that supports the decision for assignin..." with an "Add Note" button.
 - Analyze Indicators:** "Create judgement(s) as necessary and add a note confirming any changes to observable judgements..." with an "Add Note" button.
 - Confirm Incident:** "Determine the incident status as Open, Rejected, or Incident Reported" with an "Add Note" button.
 - Document and Notify:** "Create an incident ticket with the appropriate parameters and contextual incident information" with a "Select" button.
- Actions taken:** A section on the right stating "No actions taken".
- Navigation:** A "Back" button and a "Go to Containment ->" button at the bottom.

Annotations on the image include a green box around the "Response" tab and its content, and an orange box around the "Identification", "Containment", "Eradication", and "Recovery" options in the left sidebar.

Cisco XDR – менеджер інцидентів / реагування

Відповіді

Контент, специфічний для TTP в інциденті

Крок через

Identification ->

Containment ->

Eradication -> Recovery

The screenshot displays the Cisco XDR interface for an incident titled "victim-win-2.org1.net in group Audit @ 20230514 03:19:59". The interface is divided into several sections:

- Incidents:** Shows the incident title, ID (1000), and reporting details.
- Response Tab:** Contains a list of response actions:
 - Identify Affected Hosts:** Includes an "Add Note" button.
 - Contain Incident: Overview:** Includes an "Add Note" button.
 - Contain Incident: Assets:** Includes a "Select" button (highlighted with a red box).
 - Contain Incident: IPs:** Includes an "Add Note" button.
 - Contain Incident: Domains:** Includes a "Select" button.
 - Contain Incident: URLs:** Includes a "Select" button.
- Assets Panel (8 Assets):** Lists assets such as "victim-win-2.org1.net", "victim-win-6.org1.net", "LOXX-WIN10VIC02", "dc-1", "DESKTOP-V2IOAED", "victim-win-2.org1.net", "dc-1.org1.net", and "VICTIM-WIN-4".
- Action Panel:** Shows "No action" and an "Execute" button at the bottom right.

Annotations on the screenshot include a green box around the "Response" tab and its sub-items, and a yellow box around the "Identify Affected Hosts", "Contain Incident: Overview", and "Contain Incident: Assets" sections. A red box highlights the "Select" button for "Contain Incident: Assets".

Doesn't ask "which EDR" to isolate with – does it all for you

Cisco XDR – AI який допомагає аналітику

--- Old ---

1000 New victim-win-2.org1.net in group Audit @ 20230514 03:19:59

Reported by Secure Endpoint on 2023-05-14T03:19:59.000Z - 1 Linked Incident

Add short description... View Long Description

Overview Detection Response Worklog

Names of incidents

Now AI generates, which makes them much more understandable.

Descriptions

Short and long descriptions are now also generated by AI. Significantly reducing the effort of analysts.

Description

This incident occurred between 2023-11-22 21:09:08 UTC and 2024-01-10 17:39:04 UTC, featuring a series of security alerts centered around suspicious server processes, remote access violations, and potential breach tactics. Starting on key network hosts, these alerts revealed unauthorized activities across multiple endpoints over a prolonged period, indicating a persistent threat within the network. Throughout the event, several threat indicators were highlighted, including suspicious processes running from unconventional directories, suspicious hosts, unfamiliar IPs, and potential misusage attempts.

The first alert was triggered on 2023-11-22 21:09:08 UTC on the host loxx-win10vic01.org26.net. Named "Suspicious Process Path", it noted a process executed from an improper directory. This was followed on 2023-11-27 18:10:00 UTC by two alerts from the "New Remote Access" group, originating from the host atw-win10-jump.securitydemo.net. These alerts indicated an unusual first-time remote access paired with suspicious external IPs.

Shortly after, a single alert on 2023-11-29 18:34:55 UTC was triggered titled "AWS Root Account Used", indicating potential misuse. Several hosts including ats-subuntu04.securitydemo.net and atw-win10-jump.securitydemo.net triggered subsequent alerts in the "Port 8888: Connections from multiple sources" group on 2023-11-30 14:30:30 UTC, suggesting multiple file transfers which could point to exfiltration attempts.

Then, the "Suspicious Process Path" group triggered alerts again on 2023-12-01 14:30:30 UTC indicating repeated instances of execution from incorrect directories. Following this, on 2023-12-02 00:53:06 UTC, the host loxx-win10vic04.org26.net invoked the "Potential Persistence Attempt" alert reporting instance of a background process establishment, commonly associated with attempted breaches.

Strikingly, on 2023-12-02 05:07:41 UTC, the host loxx-win10vic02.org26.net consecutively triggered alerts under the groups "Suspicious Endpoint Findings by Command and Control" and "Suspicious Endpoint Findings by Execution", indicating strange endpoint behavior mapped to the noted MITRE tactics. Shortly after, the same host was again flagged under the "Suspicious Process Path" group alongside loxx-win10vic08.org26.net signifying persistence in suspicious process executions.

More alerts followed, with the "Potential Persistence Attempt" group being triggered on 2023-12-02 17:58:08 UTC from loxx-win10vic06.org26.net and the "Suspicious Process Path" group activated on 2023-12-03 00:43:12 UTC by the host loxx-win10vic07.org26.net.

Next, the "Geographically Unusual Remote Access" alert was raised on 2023-12-07 06:00:00 UTC on host atw-win10-jump.securitydemo.net, while the host also triggered another alert in the "Potential Persistence Attempt" group on 2024-01-08 14:57:37 UTC indicating continued network trespassing.

In the last alert of the chain on 2024-01-10 17:39:04 UTC, host loxx-win10vic03.org26.net triggered the "LDAP Connection from Suspicious Process" alarm, suggesting a possible credential theft attempt. In conclusion, this series of alerts provides evidence of a concentrated, evolving, and persistent attempt to compromise the network infrastructure, exploiting different loopholes in the process.

This description was generated by Cisco AI.

Short description

This incident occurred between 2023-11-22 21:09:08 UTC and 2024-01-10 17:39:04 UTC, featuring a series of security alerts centered around suspicious server processes, remote access violations, and potential breach tactics. Starting on key network hosts, these alerts revealed unauthorized activities across multiple endpoints over a prolonged period, indicating a persistent threat within the network. Throughout the event, several threat indicators were highlighted, including suspicious processes running from unconventional directories, suspicious hosts, unfamiliar IPs, and potential misusage attempts.

Long description

This incident occurred between 2023-11-22 21:09:08 UTC and 2024-01-10 17:39:04 UTC, featuring a series of security alerts centered around suspicious server processes, remote access violations, and potential breach tactics. Starting on key network hosts, these alerts revealed unauthorized activities across multiple endpoints over a prolonged period, indicating a persistent threat within the network. Throughout the event, several threat indicators were highlighted, including suspicious processes running from unconventional directories, suspicious hosts, unfamiliar IPs, and potential misusage attempts.

Priority 1000 Status New

Reported by Cisco XDR Analytics (securitydemo-net) 2 months ago

Assigned AW

MITRE

Priority score breakdown

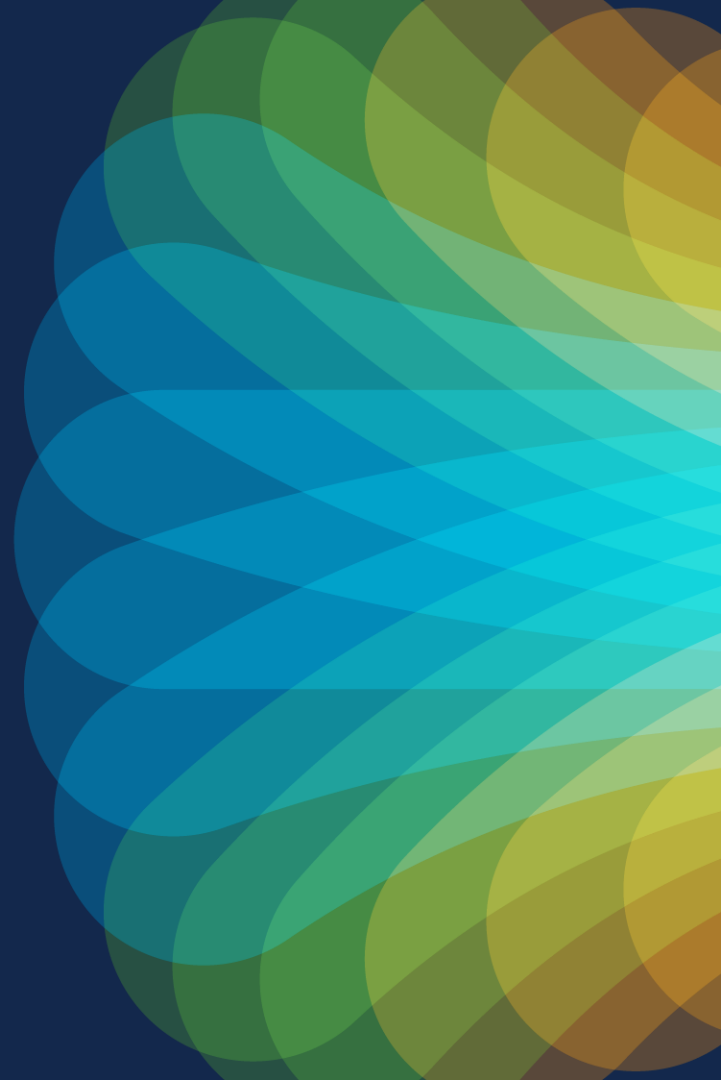
1000 | 100 Detection Risk | 10 Asset Value at Risk

View Incident Detail

Agenda

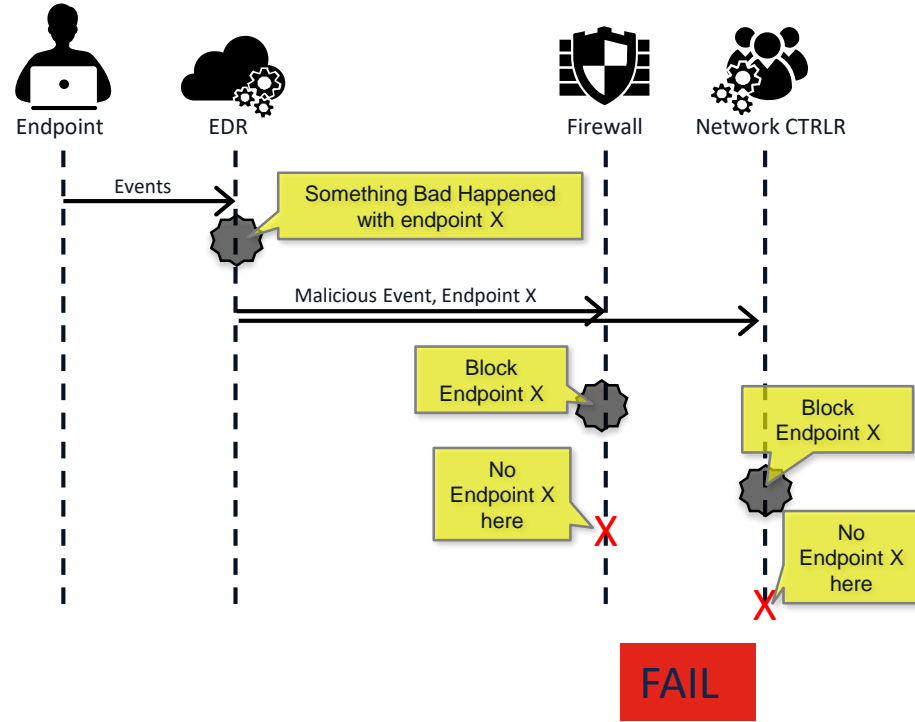
- Урок історії
- Еволюція
- Керування інцидентами і процеси
- Інтеграція та реагування
- Ключова телеметрія XDR
- Це все!

Інтеграції та реагування



Стан індустрії: немає спільних ідентичностей

- Ви бачите це на прикладі SIEM & SOAR
- Кожен продукт по-своєму дивиться на endpoint.
 - GUID (специфічний для продукту)
 - IP Address (ефемерний і постійно змінюється)
 - Mac Address (ефемерний, приватний, недоступний, дублюючий)
- Змусити продукти працювати разом – це складне завдання

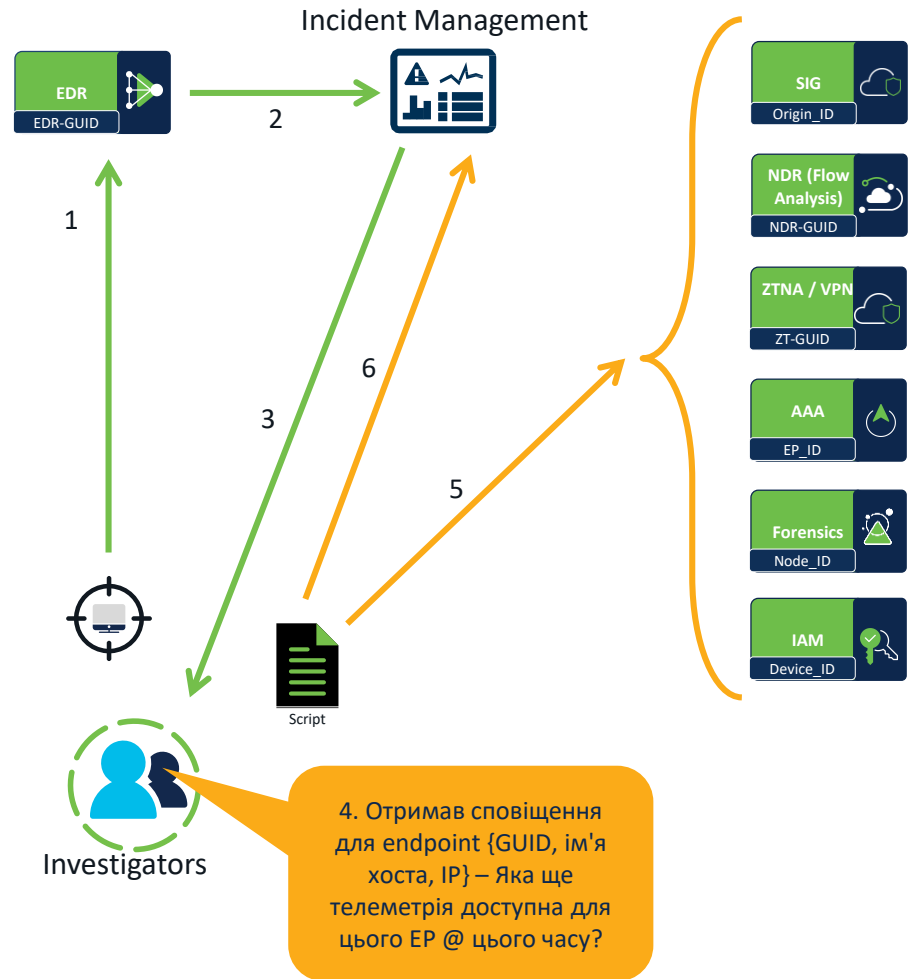


Нам потрібен спільний кінцевий об'єкт

Хід розслідувань SOC

Примітка: це загальний приклад:

1. EDR виявляє зловмисну активність
2. Сповіщення надходять до системи управління інцидентами
3. Про новий інцидент повідомили розслідування
4. Investigator бере дані про кінцеву точку з EDR і запускає скрипт
5. Скрипт отримує всі ідентифікатори з інших джерел телеметрії (жодне з них не є однаковим)
6. Скрипт оновлює диспетчер інцидентів новими спостережуваними елементами, щоб збагатити розслідування



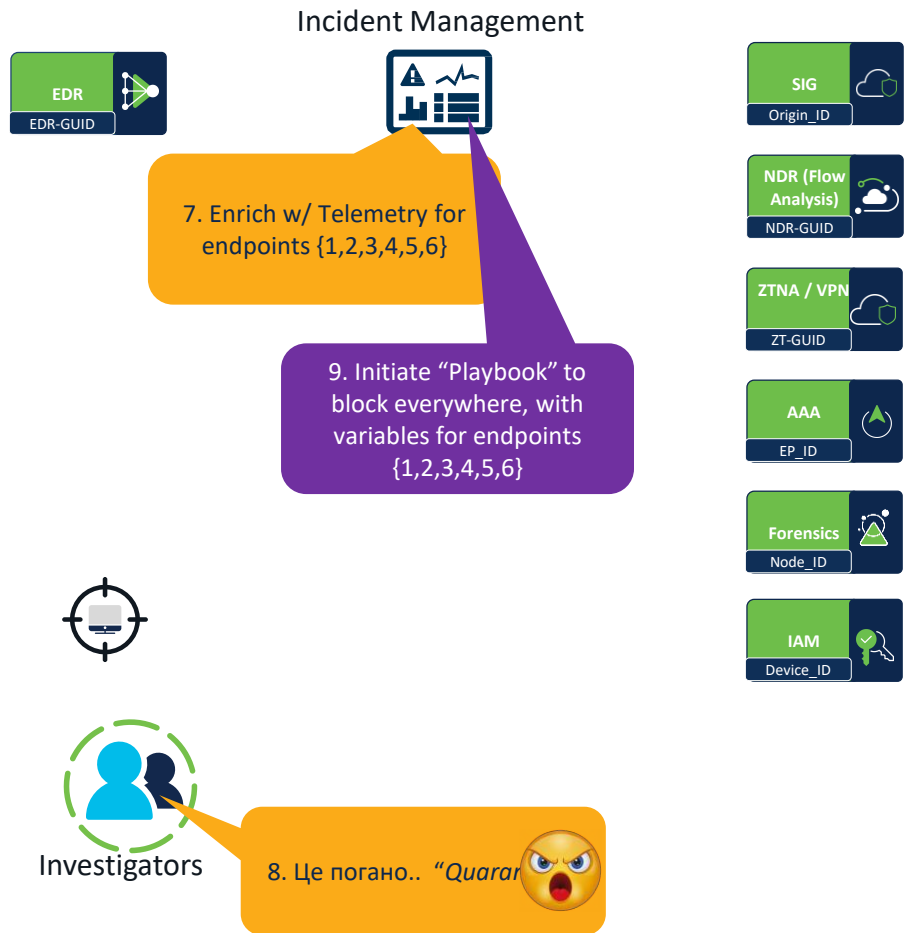
Хід розслідувань SOC

Примітка: це загальний приклад:

7. Диспетчер інцидентів використовує нову телеметрію з джерел для ідентифікаторів кінцевих точок
8. Investigator розуміє, що це погано, і ініціює опцію «всьогоутнього» карантину
9. Інструменти управління інцидентами ініціюють playbook для реагування в усіх пунктах використання

**Комусь потрібно було побудувати ці процеси

CISCO *Live!*

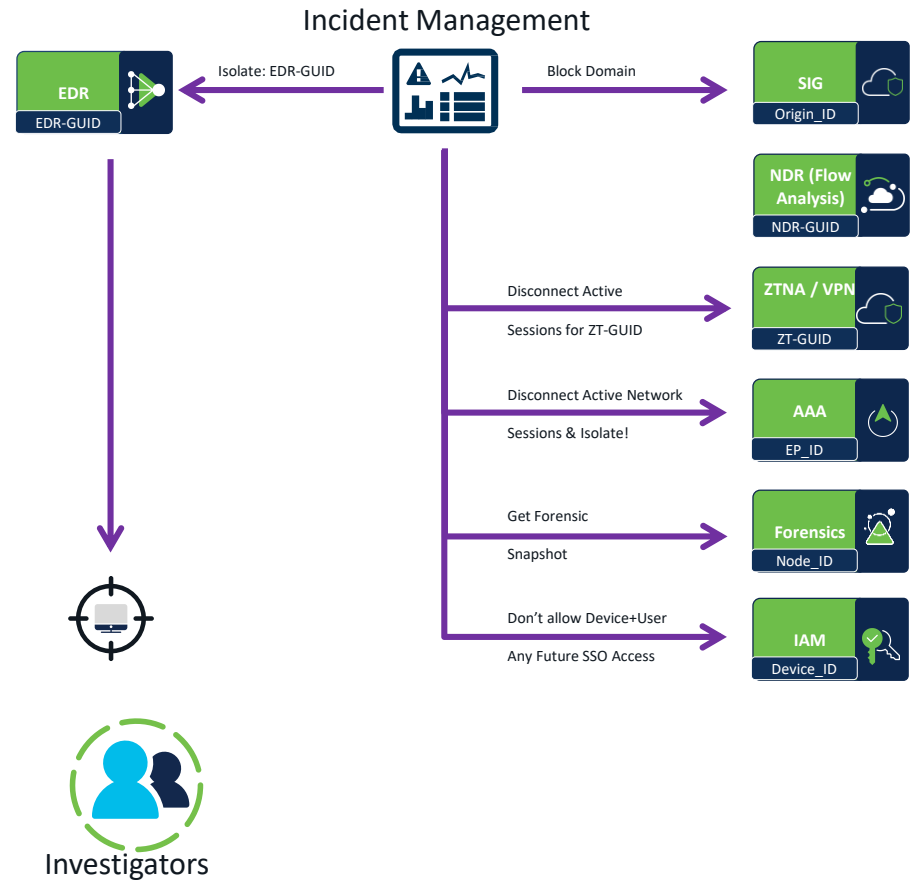



Хід розслідувань SOC

Примітка: це загальний приклад:

- Playbook ініціює ізоляцію за допомогою EDR-GUID
- Playbook блокує домен на SIG
- Playbook відключає активні сеанси для сеансів ZTNA/VPN і AAA
- Playbook ізолює кінцеву точку, коли починається новий сеанс AAA
- Playbook ініціює новий forensics знімок зараженого хоста
- Playbook інформує рішення IAM, щоб відхилити будь-які подальші спроби комбінації Користувач+Пристрій

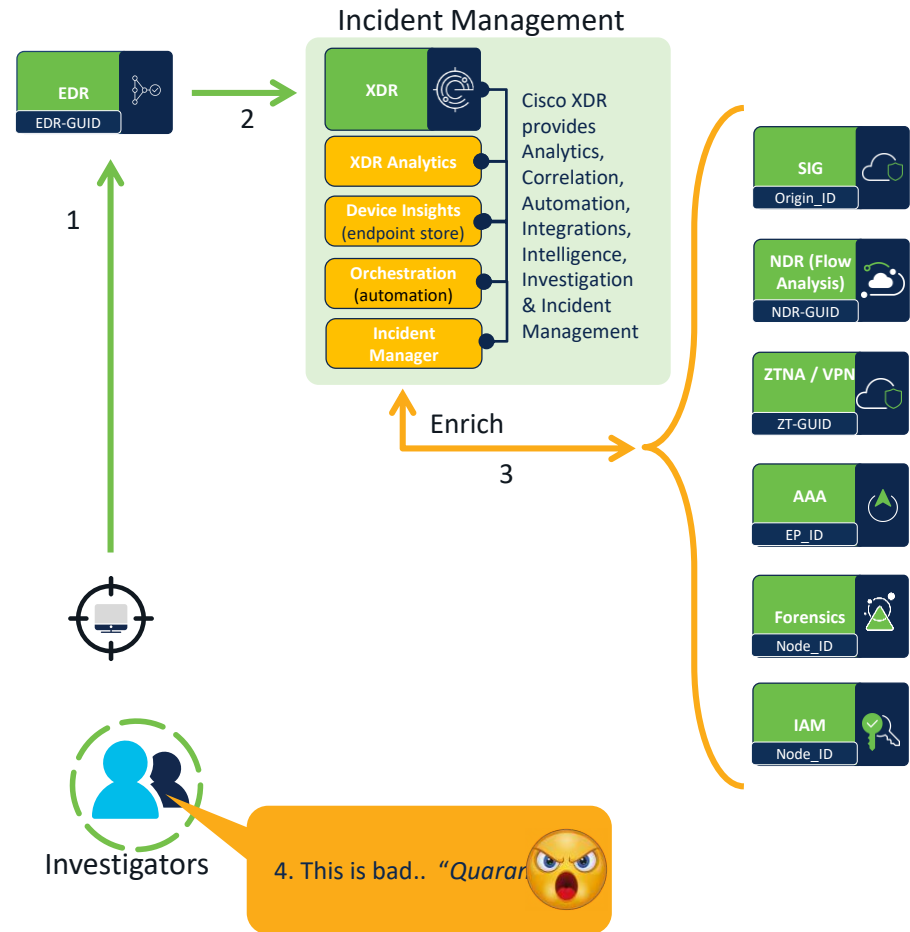
**Комуś потрібно було побудувати ці процеси



Хід розслідувань SOC

3 Cisco XDR:

1. EDR виявляє зловмисну активність
2. Сповіщення надіслано до Cisco XDR
Device Insights має всі унікальні ідентифікатори інтегрованих продуктів безпеки
3. Пріоритет оповіщення в XDR Analytics.
Інциденти, збагачені кожним інтегрованим продуктом безпеки та джерелом кібераналітики
4. Слідчий може все це побачити і вжити заходів
5. У відповіді використовується правильний ідентифікатор для кожного джерела



Хід розслідувань SOC

3 Cisco XDR:

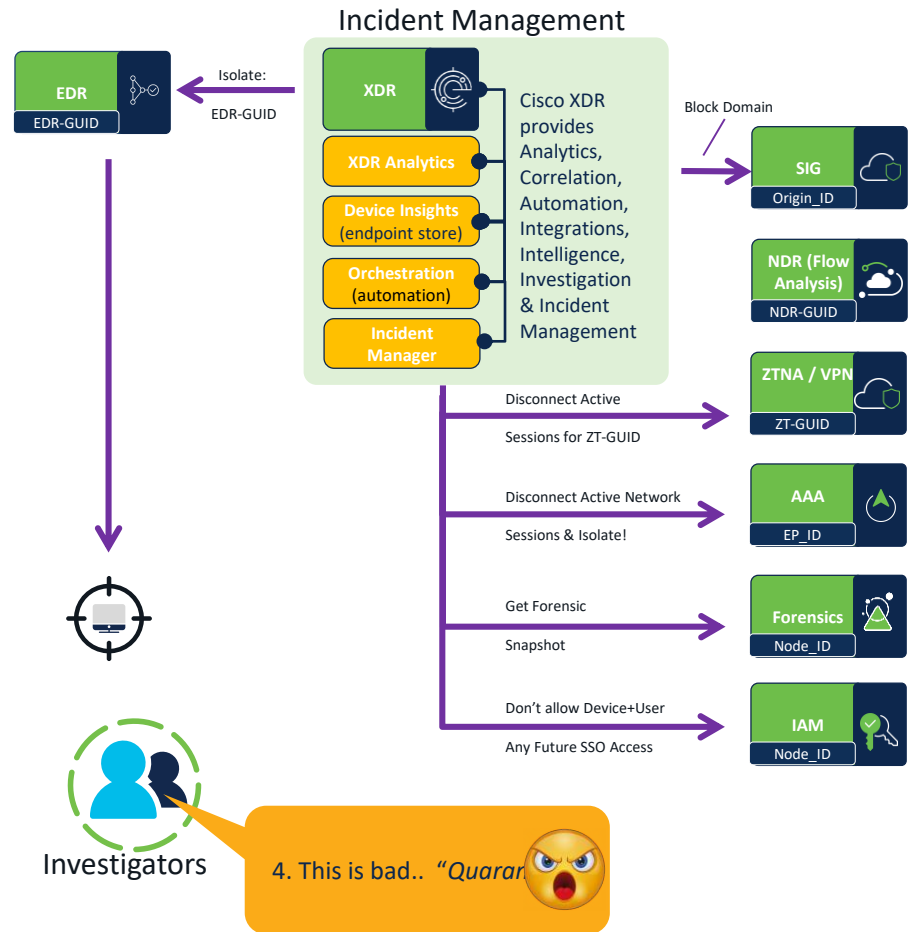
1. EDR виявляє зловмисну активність
2. Сповіщення надіслано до Cisco XDR

Device Insights має всі унікальні ідентифікатори інтегрованих продуктів безпеки

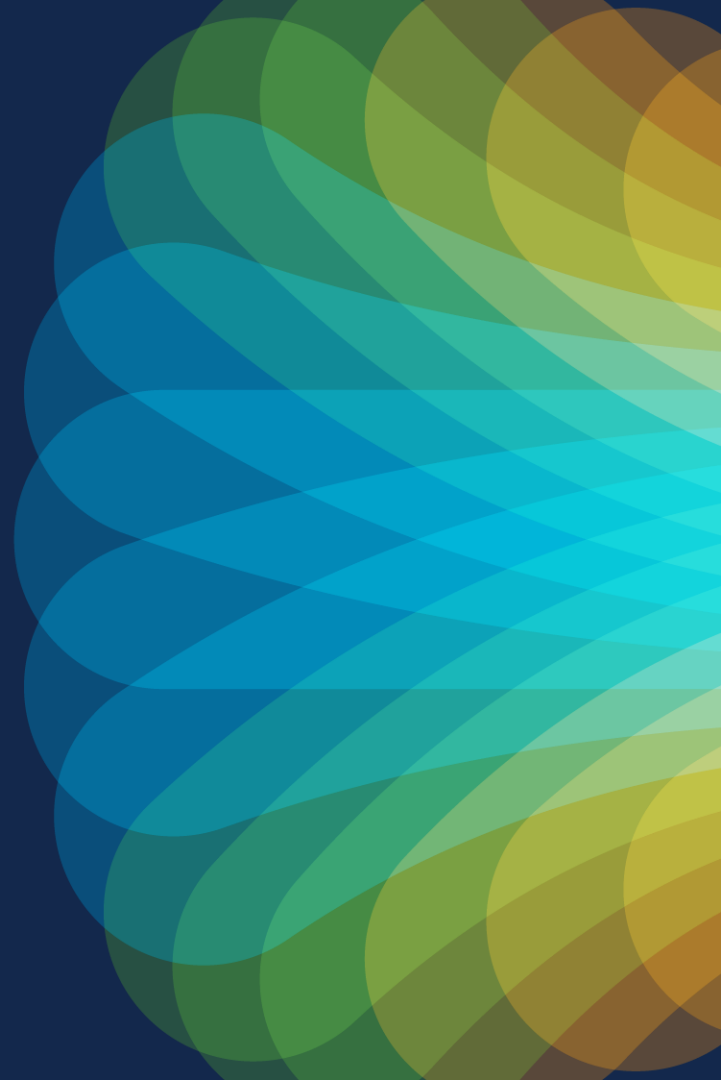
3. Пріоритет оповіщення в XDR Analytics.

Інциденти, збагачені кожним інтегрованим продуктом безпеки та джерелом кібераналітики

4. Слідчий може все це побачити і вжити заходів
5. У відповіді використовується правильний ідентифікатор для кожного джерела



Давайте поговоримо
про цю
пріоритезацію,?



Пріоритет інцидентів

- За своєю суттю: це комбінація:

Detection Risk

+

Asset Value

- Звідки беруться ці значення?

Priority **1000** Status **New** ×

victim-win-2.org1.net in group Audit @ 20230514...

Reported by **Secure Endpoint** 22 days ago

Assigned Unassigned

MITRE ...

Priority score breakdown ^

1000	100	10
	Detection Risk	Asset Value at Risk

Device Insights у XDR додає деякі нові речі

Етикетки

Опис/групування пристроїв – вручну та програмно

Значення пристрою

Значення 1-10.

1 = найменш цінні

10 = Найцінніший

Device Name	OS	OS Version	OS Support	Users Seen	Sources	Labels	Value
AAWOLAND-M-21PK	macOS	13.4		loxx, loxx@securitydemo.net	SBG SM Duo SecureX Secure Endpoint - Cisco - aawoland Orbital	Critical Server Vulnerable	10
ats-centos04	Ubuntu	#39-Ubuntu SMP PREEMPT_DYNAMIC Fri Mar 17 17:33:16 UTC 2023		loxx, reboot, runlevel, LOGIN	Secure Endpoint - Cisco - aawoland Orbital	Critical Server Vulnerable	10
ats-centos7-02.securitydemo.net	Centos	linux release 7.6		reboot, runlevel, LOGIN	Secure Endpoint - Cisco - aawoland Orbital		10
ats-centos7-03.securitydemo.net	Centos	linux release 7.6		loxx, reboot, runlevel, LOGIN	Secure Endpoint - Cisco - aawoland Orbital	Critical Server	10
ATS-MemberSrvr.securitydemo.net	Windows	Server 2016 Standard			Secure Endpoint - Cisco - aawoland Orbital		10

Device Insights у XDR додає деякі нові речі

Масове оновлення

Може масово оновлювати мітки та значення всіх вибраних об'єктів на екрані інвентаризації.

Створення в режимі реального часу

Може навіть створювати та застосовувати нові мітки в рядку

The screenshot displays the XDR interface with a table of 30 devices. A modal window is open for editing labels. The table has columns for Device Name, OS, OS Version, and Sources. The modal shows a list of labels, including 'Boo CrowdStrike', 'Retired', 'External Facing', 'Critical', and 'RTP Data Center'. The 'Retired' label is selected.

Device Name	OS	OS Version	Sources
AIQ-CROWDSTRIKE	Unknown	Windows 10	CrowdStrike
ANYCNET-WIN10-C	Unknown	Windows 10	CrowdStrike
ANYCNET-WIN11-C	Unknown	Windows 11	CrowdStrike
AnyConnect-linux-1	Unknown	Ubuntu 18.04	CrowdStrike
AnyConnect-linux-2	Unknown	Ubuntu 20.04	CrowdStrike
AnyConnect-linux-3	Unknown	Ubuntu 22.04	CrowdStrike
BLUECKW19	Unknown	Windows Server 2019	CrowdStrike
C1-3850-2-G1-3-	Unknown	Windows 10	CrowdStrike
CROWDSTRIKE-WIN	Unknown	Windows 10	CrowdStrike
dc-1	Unknown	Windows Server 2019	CrowdStrike
dc-1	Unknown	Windows Server 2019	CrowdStrike

Device Insights у XDR додає деякі нові речі

Масове оновлення

Може масово оновлювати мітки та значення всіх вибраних об'єктів на екрані інвентаризації.

Створення в режимі реального часу

Може навіть створювати та застосовувати нові мітки в рядку

The screenshot displays the Cisco XDR Device Insights interface. It features a table with columns for 'Compromised', 'Labels', and 'Value'. The 'Value' column shows a dropdown menu with a '10' value. A modal window is open, showing a 'Default value' dropdown with '10' selected and a 'Manually assigned' dropdown with 'M' selected. A 'Update Value' dropdown is also visible, showing a list of values from 1 to 10, with '10 (Critical)' highlighted. An 'Update' button is at the bottom right of the modal.

Compromised	Labels	Value
	Boo Crowdstrike	10
	Boo Crowdstrike	10
		10
		10
		10
		10
		10
		10
		10

Update Value



- 1 (Not Critical)
- 2
- 3 (Less Critical)
- 4
- 5
- 6 (Somewhat Critic
- 7
- 8
- 9
- 10 (Critical)

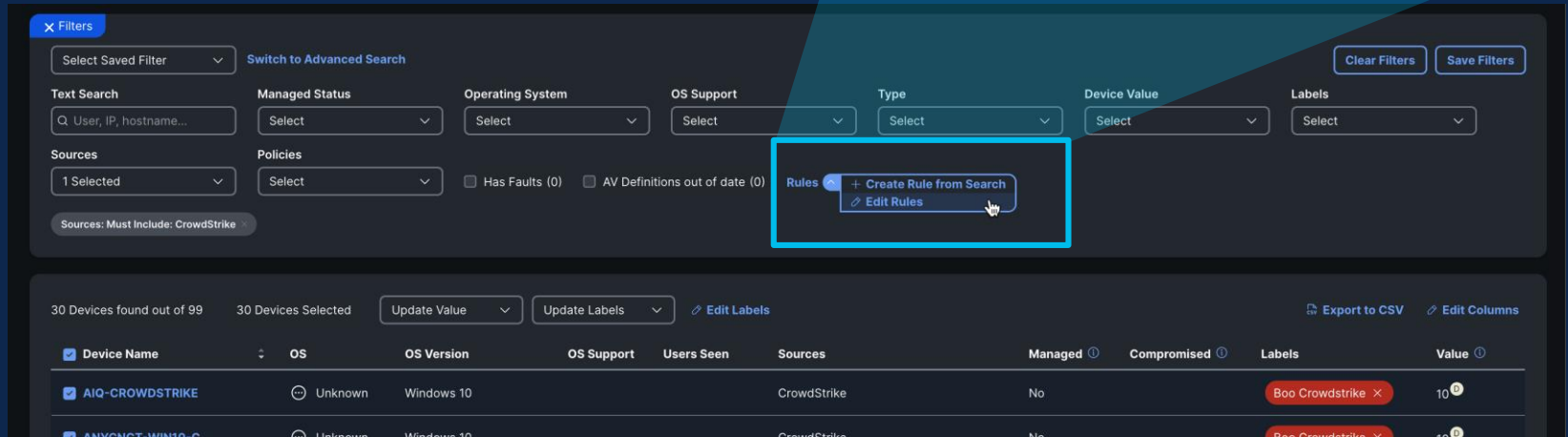
Update

Device Insights у XDR додає деякі нові речі

Правила роботи

На основі інсайтів «Пошук».
Застосування значень / міток,
коли виконуються правила.

Rules  + Create Rule from Search
 Edit Rules



The screenshot displays the Cisco XDR interface. At the top, there is a 'Filters' section with a 'Switch to Advanced Search' button. Below this are several filter categories: Text Search, Managed Status, Operating System, OS Support, Type, Device Value, and Labels. A 'Sources' section shows '1 Selected' and a 'Policies' section with checkboxes for 'Has Faults (0)' and 'AV Definitions out of date (0)'. A 'Rules' dropdown menu is highlighted with a red box, showing options for '+ Create Rule from Search' and 'Edit Rules'. Below the filters, a table shows 30 devices found out of 99. The table columns include Device Name, OS, OS Version, OS Support, Users Seen, Sources, Managed, Compromised, Labels, and Value. The first row shows a device named 'AIQ-CROWDSTRIKE' with OS 'Unknown', OS Version 'Windows 10', OS Support 'CrowdStrike', Users Seen 'No', Sources 'CrowdStrike', Managed 'No', Compromised 'No', Labels 'Boo CrowdStrike', and Value '10'.

Device Insights у XDR додає деякі нові речі

Rules Engine

На основі інсайтів «Пошук».
Застосовуйте значення / мітки, коли виконуються правила.

Може вмикати / вимикати правила

Може змінити або видалити їх

Можна скористатися наявними пошуковими запитами або створити новий пошук у редакторі правил.

The screenshot displays the Cisco XDR Rules Engine interface. A modal window titled "Rules" is open, showing the configuration for a rule. The modal is divided into several sections:

- Details:** Includes fields for "Name" and "Description".
- Rule Criteria:** Contains several criteria with dropdown menus:
 - Text Search:** A search input field with the placeholder "User, IP, hostname...".
 - Managed Status:** A dropdown menu with "Select" as the current value.
 - Operating System:** A dropdown menu with "Select" as the current value.
 - OS Support:** A dropdown menu with "Select" as the current value.
 - Type:** A dropdown menu with "Select" as the current value.
 - Device Value:** A dropdown menu with "Select" as the current value.
 - Labels:** A dropdown menu with "Select" as the current value.
 - Sources:** A dropdown menu with "1 Selected" as the current value.
 - Policies:** A dropdown menu with "Select" as the current value.
- Automated Assignment:** Includes checkboxes for "Has Faults (0)" and "AV Definitions out of date (0)".
- Assign Labels:** A dropdown menu with "Select Labels" as the current value.
- Assign Device Value:** A dropdown menu with "Select Value" as the current value.

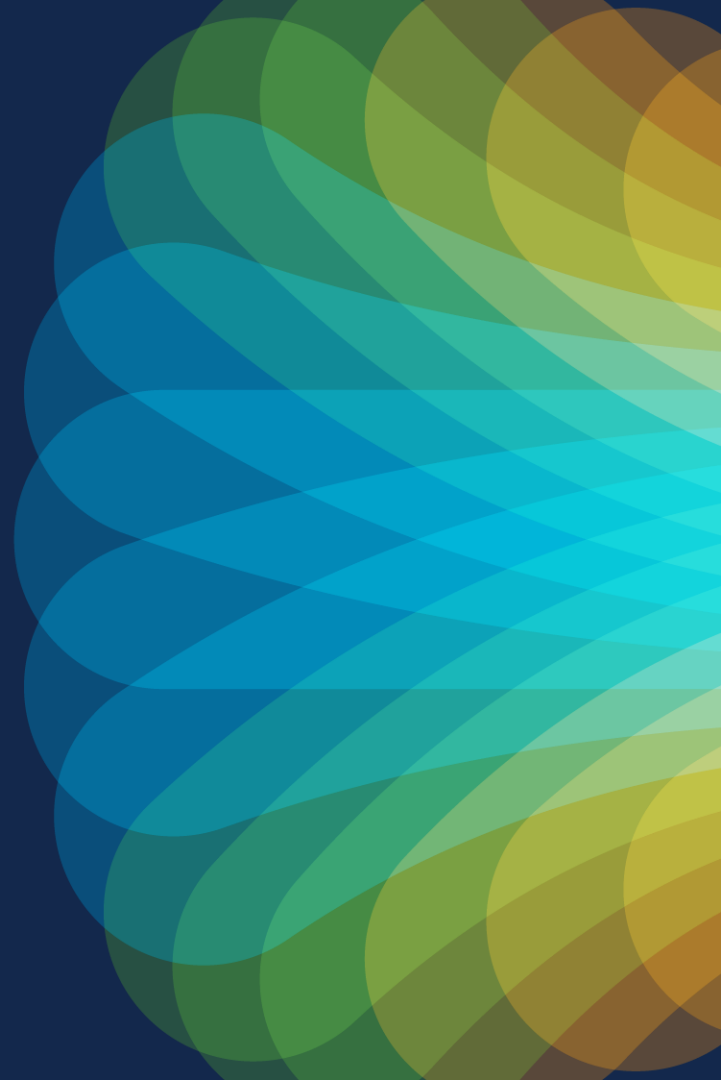
At the bottom of the modal, there are "Cancel" and "Create" buttons. Below the modal, a summary table is visible:

Details	Rule Criteria	Automated Assignment
<input checked="" type="checkbox"/> Loxx-Unmanaged (7 devices affected)	Managed Status: Unmanaged Text Search: "loxx"	Value: 8 Labels: ● Critical ● Server
<input checked="" type="checkbox"/> LoxxRule (5 devices affected)	Text Search: "Loxx"	Labels: ● Loxx

Agenda

- Урок історії
- Еволюція
- Керування інцидентами і процеси
- Інтеграція та реагування
- Ключова телеметрія XDR
- Це все!









Телеметрія, телеметрія та інше Телеметрія



Важливість джерела телеметричних даних

Шість основних джерел даних, які, на думку клієнтів, є важливими для XDR:

Endpoint, Network, Firewall, Identity, Email and DNS

Essential		
	Count	Share
 Endpoint	255	85.0%
 Network	226	75.3%
 Firewall	207	69.0%
 Identity	191	63.7%
 Email	179	59.7%
 DNS	140	46.7%
 Public Cloud	137	45.7%
 Non-Security Sources	36	12.0%



Cisco Secure
Endpoint



Cisco/ Meraki
(Networking)



Firewall Threat
Defense (FTD)



Duo



Email Threat Defense
(ETD)



Umbrella

Також 3-тя сторона

- EDR:



- Crowstrike



- Sentinel One



- MSFT Defender

- NDR:

- Dark Trace

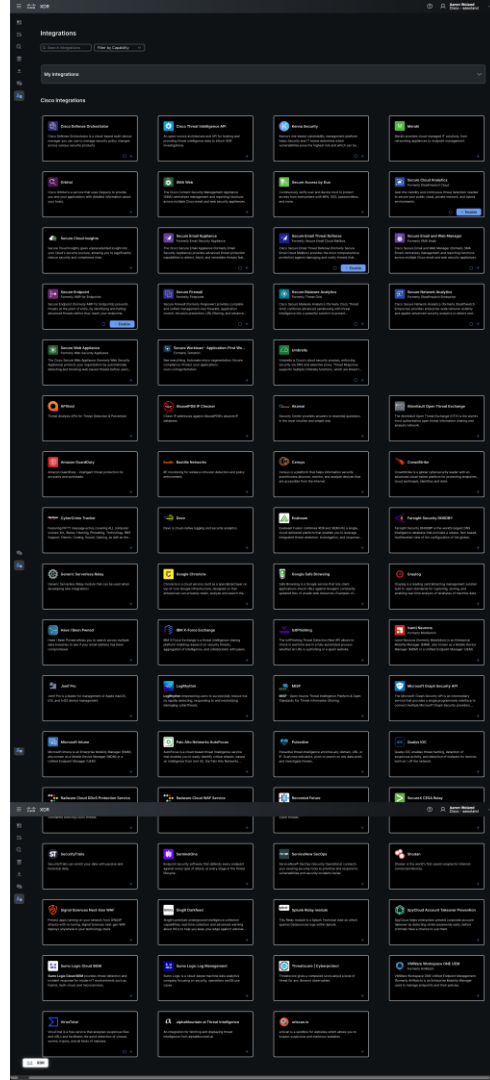


- ExtraHop



... Та інші джерела
інформації

CISCO *Live!*



“Я думаю, що NVM – це найкраще збережена секретна зброя Cisco”

-Tom Gillis, SVP & GM – Cisco Secure



A stylized world map in white and light blue on a dark blue background. The map is centered and serves as the background for the text.

~250

мільйонів endpoints надають найбільший набір
сервісів безпеки для більш ніж

80,000+

клієнтів по всьому світу

AnyConnect пройшов ребрендинг



AnyConnect

+



Cisco Secure
Endpoint (AMP)

=



Cisco Secure
Client

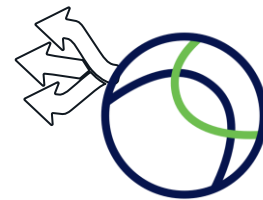
Чому це важливо для SOC, або для Cisco XDR?

“Мережева телеметрія має вирішальне значення для захищеної мережі. Шкода, що ми не можемо отримати NetFlow з endpoint”

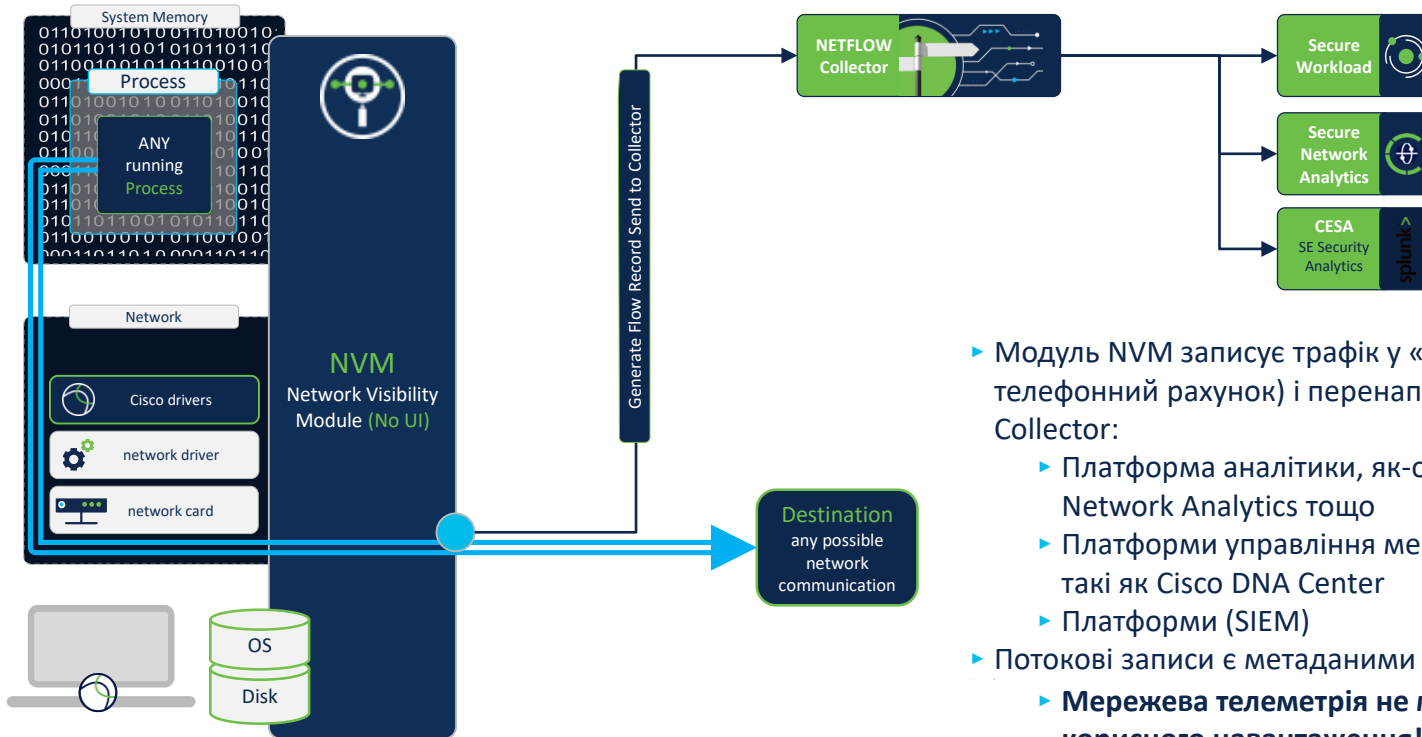
- SANS Instructor
SEC530: Defensible Network Architectures

Network Visibility Module (NVM)

- Створює запис потоку кожного мережевого підключення з endpoint
 - User, Process, Machine Info, etc.
 - Працює On та Off Prem
 - Надсилає дані в IPFIX (NetFlow) на основі "nvzFlow".



Network Visibility Module



- ▶ Модуль NVM записує трафік у «запис потоку» (як телефонний рахунок) і перенаправляє його до Netflow Collector:
 - ▶ Платформа аналітики, як-от Secure Workload, Secure Network Analytics тощо
 - ▶ Платформи управління мережею та автоматизації, такі як Cisco DNA Center
 - ▶ Платформи (SIEM)
- ▶ Потоківі записи є метаданими :
 - ▶ **Мережева телеметрія не містить жодного корисного навантаження!**

Видимість мережі + endpoint точок разом



Netflow/IPFIX

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received

NVM (IPFIX Formatted)

*Справжня атрибуція пристрою,
Не просто "IP-адреса"*



OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

Глибока видимість
endpoint

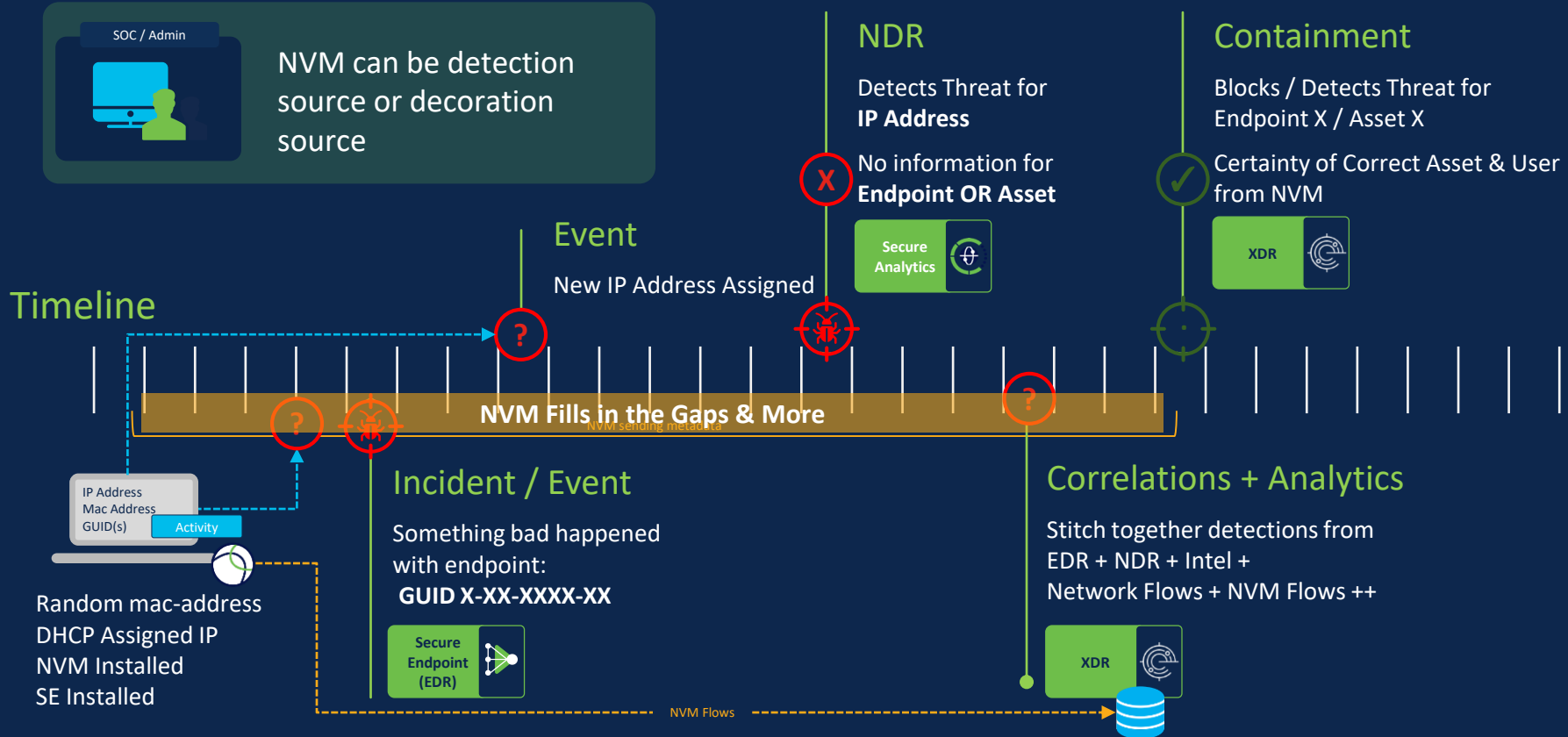
- User
- Traffic Stats
- Processes
- Applications
- SaaS Used
- Accounts
- Destinations
- Machine Details

Звичайно, це круто, але
чому це має вас
хвилювати?

“NVM каже: не тільки цей IP спілкується з цим IP на цих портах [...] Насправді у нього є ця програма, яка відкриває це з'єднання”

-Michael Scheck, Director Cisco CSIRT

Хронологія розслідування



NVM тепер є ключовим компонентом Cisco XDR

- Розгортання CSC за замовчуванням
 - Профіль CM за замовчуванням
 - Профіль NVM за замовчуванням – встановлено на XDR
- NVM надсилає безпосередньо в хмару
 - Потрібен керований хмарою CSC
 - Забезпечує ідентифікацію та безпечний транспорт
 - Може бути хмарним або onPrem, а не обома (сьогодні)

Переглядач подій NVM у XDR Analytics

New NVM Flows Tab

МИТТЄВІ ФІЛЬТРИ

Пошукова активність за атрибутом або багато за допомогою розширеного пошуку.

Подробиці телеметрії

Перегляньте детальну телеметрію, зібрану з потоку

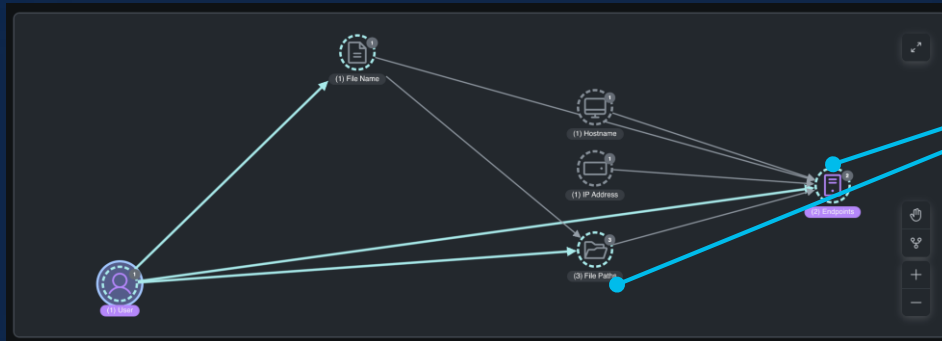
The screenshot displays the 'Event Viewer' interface with the 'NVM Flow' tab selected. The top navigation bar includes 'Session Traffic', 'Session Details', 'Rejected Traffic', 'Cloud Posture', 'AWS CloudTrail', 'Passive DNS', and 'NVM Flow'. A search bar shows filters: 'NOT source_ip_address: "10.1.100.26"' and 'NOT destination_ip_address: "10.1.100.26"'. The main table lists flow events with columns for time, IP addresses, ports, protocols, and bytes. A detailed view for a specific event shows the following data:

bytes_in	bytes_out	cc_arrival_time_sec
473	196	2023-05-23T14:11:59+00:00

Additional telemetry details include:

- destination_ip_address: 208.67.222.222
- flow_stage: 0
- logged_in_user: <none>
- parent_process_hash: 72e43f0f42772e5a7186e0af3d07d76e1569d4656f5c906d4324523db864fc
- process_account: NT AUTHORITY\SYSTEM
- process_account_type: 8194
- process_id: 1392
- source_ip_address: 10.1.82.156
- process_name: dnscryptproxy.exe
- source_port: 60104
- ADDITIONAL_LOGGED_IN_USERS_LIST: [{"account_type": 32770, "logged_in_user": "ORG26\Administrator", "session_type": 1}].

NVM забезпечує виявлення та показ



Відображає бічний рух

Забезпечує видимість і кореляцію між East-West та North-South

Безпосереднє джерело спостережуваних об'єктів

Для нових виявлених об'єктів у XDR Analytics

The screenshot shows the XDR Analytics interface with a table of security events. The table has columns for 'First Seen', 'Severity', 'Source', 'Indicators', 'Observables', and 'Assets'. A yellow box highlights the 'Observables' column, which contains various indicators and assets. The 'Observables' column is highlighted with a yellow box.

First Seen	Severity	Source	Indicators	Observables	Assets
2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Suspicious Endpoint Activity	51.75.129.204	loxx-win10vic07.org26.net
2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Malicious Process Detected	51.75.129.204	loxx-win10vic07.org26.net
2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Suspicious Endpoint Activity	93f38156eb3dbbe3562dfe7e80ff62cab75c2f...	loxx-win10vic07.org26.net
2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Malicious Process Detected	93f38156eb3dbbe3562dfe7e80ff62cab75c2f...	loxx-win10vic07.org26.net
2023-05-27T01:44:45.000Z	High	Cisco Secure Cloud Analytics (security...	Malicious Process Detected	1875a380cc98bada07ad042ea17612fd92c9c9...	loxx-win10vic06.org26.net
2023-05-27T01:44:45.000Z	High	Cisco Secure Cloud Analytics (security...	Malicious Process Detected	b99d61d874728edc0918ca0eb10ab93d381e...	loxx-win10vic06.org26.net
2023-05-27T01:44:45.000Z	High	Cisco Secure Cloud Analytics (security...	Potential Persistence Attempt	ORG26 bill	loxx-win10vic06.org26.net
2023-05-27T01:44:45.000Z	High	Cisco Secure Cloud Analytics (security...	Suspicious Endpoint Activity	10.1.82.10	loxx-win10vic06.org26.net
2023-05-26T19:50:44.000Z	Unknown	AMP Event		93f38156eb3dbbe3562dfe7e80ff62cab75c2f...	loxx-win10vic06.org26.net
2023-05-26T19:50:44.000Z	Unknown	AMP Event		93f38156eb3dbbe3562dfe7e80ff62cab75c2f...	loxx-win10vic06.org26.net
2023-05-26T19:50:44.000Z	Unknown	AMP Event		93f38156eb3dbbe3562dfe7e80ff62cab75c2f...	loxx-win10vic06.org26.net

NVM у порівнянні з SYSMON та журналами мережевих подій

Cloud Analytics
Now part of Cisco XDR

Monitor Investigate Report Settings

Event Viewer

Session Traffic Session Details Rejected Traffic Cloud Posture AWS CloudTrail Passive DNS **NVM Flow**

2023-12-19 09:05:34 UTC 2023-12-19 21:05:34 UTC

Applied filters: process_name:"cert" restore default filters

Flow_End_Time_Se...	Source_IP_Address	Destination_IP_Addres...	Source_Port	Destination_Port	Process_Account	Process_Name	Process_Path	Process_Args	Parent_Process_Acco...	Parent_Pro
2023-12-19 17:07:05 UTC	10.1.82.151	72.163.4....	58086	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:05 UTC	10.1.82.151	72.163.4....	58086	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:05 UTC	10.1.82.151	23.196.38...	58087	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:05 UTC	10.1.82.151	72.163.4....	58088	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:05 UTC	10.1.82.151	192.35.17...	58089	80 (http)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:06 UTC	10.1.82.151	72.163.4....	58088	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:06 UTC	10.1.82.151	23.196.38...	58090	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:06 UTC	10.1.82.151	23.196.38...	58087	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:06 UTC	10.1.82.151	23.196.38...	58090	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:06 UTC	10.1.82.151	192.35.17...	58089	80 (http)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...
2023-12-19 17:07:09 UTC	10.1.82.151	72.163.4....	58091	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32\certutil.exe	-urlcache -f https://cisco.com/index.html README.md	ORG26\Administrator	powershell_is...

- NVM Фіксує всі потоки.
- Sysmon знімає з першого разу і більше ніколи

Ідентичність є критично
важливим компонентом
будь-якого XDR

Ідентифікація в XDR

- Не тільки особистість людини (користувача)
 - Вже розглянули важливість ідентичності пристрою
 - Людська ідентичність також є важливим аспектом інциденту
 - Для контексту: хто брав участь
 - Для виявлення: атаки на основі ідентифікації

Сторінка інвентарю користувачів (у бета-версії)

Ключові показники, що відображаються

Assets > Users

“inventory” користувачів це підмножина категорії “Assets”

Об'єднаний інвентар

Фільтрований, сортований, зведений рівень об'єднаних облікових записів користувачів з усіх інтегрованих джерел.

Прогресивне розкриття інформації

Натисніть на User (Користувач) для "Drawer" відомостей про користувача. Натисніть на менеджера, щоб переглянути дані менеджера.

The screenshot displays the Cisco XDR interface for the 'Users' section. The left sidebar shows navigation options like 'Control Center', 'Incidents', 'Investigate', 'Intelligence', 'Automate', 'Assets', 'Devices', 'Sources', 'Client Management', 'Administration', 'My Account', 'Integrations', 'On-Premises Appliances', 'API Clients', and 'Users'. The main content area shows a 'Source health' indicator (Healthy), a 'Users' summary (311 total, 25 Guests), and a table of users. A 'Drawer' for 'Andrew Maxey' is open on the right, showing detailed information.

Display name	Login names	Emails	Department
Aaron Woland (aawoland)	aawoland_cisco.com#EXT#@securitydemo.net.onmicrosoft.com	aawoland@cisco.com	
Aaron Woland-Cisco	aawoland@securitydemo.net	aawoland@cisco.com, aawoland@securitydemo.net	Small Council
Abhishkek Dubey	abhidub2@securitydemo.net		
Accounting1	Accounting1@securitydemo.net	accounting1@securitydemo.net	
Accounting2	accounting2@securitydemo.net	accounting2@securitydemo.net	
Adam Sonnenfeld	asonnenf@securitydemo.net		
Aditya Sankar	adisanka@securitydemo.net	adisanka@securitydemo.net	Little Birds
Alice Smith	alice@securitydemo.net	alice@securitydemo.net	Widgets
Anat Borowitzh Lavy	anat@securitydemo.net	anat@securitydemo.net	
Andrew Maxey	andrew@securitydemo.net	andrew@securitydemo.net	Dept. of Whispers
Anthony Brandelli	abrandel@securitydemo.net		

Andrew Maxey

- Display name: Andrew Maxey
- First name: Andrew
- Last name: Maxey
- Emails: andrew@securitydemo.net
- Mobile phone numbers: —
- Business phone numbers: —
- User ID: 345ce393-a333-421c-867f-80362bf3d771
- Company: —
- Office location: —
- Department: Dept. of Whispers
- Manager: Loxx
- Job title: Spy Master
- Employee ID: —
- Groups: LabUsers, Global Administrator, PosaaS
- Last logon: —
- Account created: 2021-05-17T22:44:24.000Z
- Account type: —
- Account status: Enabled
- Source types: Azure Users
- Owned devices: —
- Owned devices: —
- Usage location: —

Сторінка відомостей про користувача

Найпопулярніші пристрої, що використовуються / належать

Натисніть «Переглянути всі», щоб переглянути список усіх пристроїв

Де бачили

Список усіх об'єднаних джерел для цього користувача та нещодавніх подій входу до системи для користувача

Детальніше

Усі властивості користувача: Членство в групі, Організаційна структура, Зображення (за наявності), усі адреси електронної пошти

Used devices

- ATW-SurfacePro4 (last login: 2023-04-27)
- loox-surfacepro (last login: 2023-04-27)

Owned devices

- Galaxy S8+ (last login: 2023)

Logons

Timestamp	Device	Location	Type	Source
2023-04-27 07:30:11	PCARCO-M-BRUZ	Moscow, Russia	Login - failed	Due
2023-04-27 07:30:11	PCARCO-M-BRUZ	Moscow, Russia	Login - success	Due
2023-04-27 07:30:11	ATW-SurfacePro4	Hong Kong, China	Seen	Azure AD
2023-04-28 07:30:11	PCARCO-M-BRUZ	Moscow, Russia	Seen	Azure AD
2023-04-28 07:30:11	PCARCO-M-BRUZ	Moscow, Russia	Login - success	Due

Details

Identity

Display name: Adriana Hsieh

Login names: ahseih (Azure), adrianah (OKTA), adrianahseih (Duo)

Emails: ahsieh@cisco.com, adrianah@example.com

Phone numbers: +1 (123) 456 - 6837, +1 (123) 456 - 6837

User ID: 475394732885793d61kxsvkqj@wqrlgh

Organization Role

Company: RAD

Organization: RAD Security

Department: R&D 234

Manager: Chuck Robbins

Job title: Leader, Software Engineering

Employee ID: 176536

Контекст користувача в розслідуванні / управлінні інцидентами

Реквізити для "Об'єктів" користувача

Стає об'єктом користувача – User Object, а не загальними даними

Прогресивне розкриття інформації

Якщо клацнути на позначенні користувача на графіку, у вікні з'явиться «висувна панель відомостей про користувача»

The screenshot displays a security dashboard with a navigation bar (Overview, Detection, Response, Worklog) and a main graph area. The graph shows a user node (Orco@all) connected to various system nodes like File Paths, File Names, IP Addresses, and SHA-256 Hashes. A detailed profile for Adriana Hsieh is shown on the right, including contact information, organizational details, and device usage.

Adriana Hsieh	
Admin	Eng-admins
Display name	Adriana Hsieh
Login names	ahsieh (Azure), adriana (OKTA), adrianahsieh (Duo)
Emails	ahsieh@csco.com, adriana.h@csco.com
Phone numbers	+1 (123) 456 - 6837, +1 (123) 456 - 6837
User ID	47539475298573adkjk, svkfbjgwieg
Labels	Eng-admins
Value	8
Company	RAD
Organization	RAD
Department	R&D 234
Manager	Chuck Robbins
Job title	Leader, Software Engineering
Employee ID	176536
Groups	Group, Group, group, group, group, +17 more
Last logon	Mar 18, 2023, 3:11 PM
Last active	Mar 18, 2023, 3:11 PM
Account created	Mar 18, 2023, 3:11 PM
Account type	Admin
Account status	Enabled
Source types	OKTA, Azure AD
Used devices	PCARCO-M-8BUZ, CLOUDSHARE-WYOP, PCARCO-M-8BUZ
Owned devices	PCARCO-M-8BUZ, CLOUDSHARE-WYOP, PCARCO-M-8BUZ
Block sign-in	Yes
Usage locations	Waxhaw, NC, Palo Alto, CA, Atlanta, GA, Budapest, Turkey

Ідентифікаційні дані призводять до виявлення та реагування на загрози ідентичності (ITDR)

- Кількість атак, заснованих на ідентифікаційних даних, зростає
- Зловмисники використовують «розростання ідентичності» від впровадження хмарних технологій і політик у стилі ZT
 - Ex: MFA Flooding / MFA Fatigue
- Використовуйте скомпрометовані облікові дані, користувачів із неналежними привілеями

The logo for DORT, featuring a stylized white flame-like shape to the left of the word "DORT" in a bold, white, sans-serif font.

now part of **CISCO**

Cisco Identity Intelligence

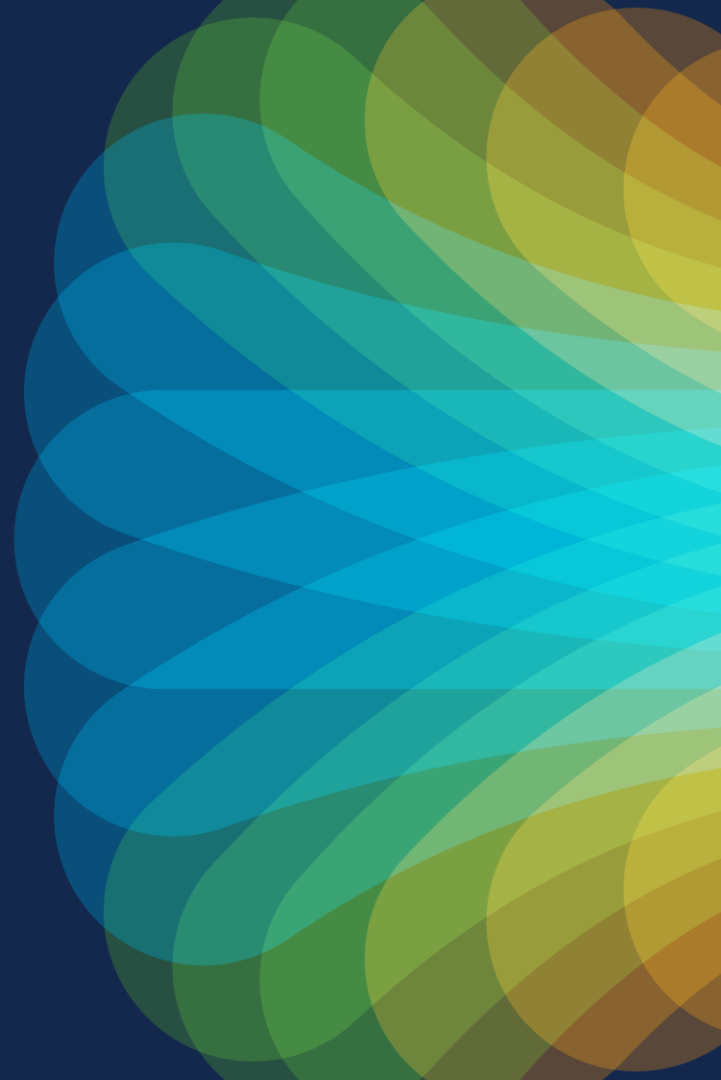
CISCO *Live!*

Чому OORT?

- Технології та залучення талантів
- Буквально команда, яка написала Device Insights – покинула Cisco і створила Oort
- Практично спеціально створений для цієї інтеграції

- Лідер на ринку ITDR
- Великий інфлюенсер / радник з Identity Security з провідними аналітиками
- Data Scientists / Команда інженерів з лідерами в галузі безпеки ідентифікаційних даних

Примітка: ці екрани з
оригінального
інтерфейсу Oort UI



Інтеграція!!

Cisco Identity Intelligence вже інтегрується з багатьма ключовими (хмарними) джерелами ідентифікаторів.

The screenshot displays the 'Add Integration' interface in Cisco Identity Intelligence. The top navigation bar includes 'Dashboard', 'Users', 'Checks', 'Integrations', and a search bar. The user is logged in as 'Loxx admin - security-demo-net'. The main content area is titled 'Integrations / Add Integration' and features a 'Providers' section with the following cards:

- Auth0:** Auth0 is a flexible, drop-in solution to add authentication and authorization services to your applications.
- AWS:** Amazon Web Services offers reliable, scalable, and inexpensive cloud computing services.
- Duo:** Duo Security is a cloud-based security platform that protects access to all applications, for any user and device, from anywhere.
- GitHub Beta:** GitHub is an Internet hosting service for software development and version control using Git.
- Google Workspace:** Google Workspace is a collection of cloud computing, productivity and collaboration tools, software and products developed by Google.
- Microsoft Entra ID:** The Microsoft Entra ID (formerly Azure AD) enterprise identity service provides SSO and MFA to help protect your users from cybersecurity attacks.
- Okta:** Okta is a customizable, secure, and drop-in solution to add authentication and authorization services to your apps.
- Salesforce:** Salesforce provides customer relationship management software and applications focused on sales, customer service, marketing automation, analytics, and application development.
- Workday:** Workday is a popular cloud-hosted HRIS service. Identity Intelligence ingests regular and contingent worker data from Workday to enrich user details.

At the bottom, there is a 'Manual Uploads' section with a '+ Add Integration' button. The footer contains links for 'Identity Intelligence', 'Privacy Policy', 'Terms of Use', 'Documentation', and 'SOC2 Report', along with a notice: 'This environment reloads hourly'.

Перевіряє

АКА: сигнатури для виявленнь

Піддається фільтруванню

Усі перевірки розподілено за категоріями, призначено відповідним джерелам ідентифікаторів і можна повністю фільтрувати

Identity Intelligence | Dashboard | Users | Checks | Integrations | Search | Loxx admin - security-demo-net

Search by title | Request check | Run checks now

Last run: Feb 1, 2024 19:44:04 UTC

Check	# Failing	# Excluded	Report Channels
0% Okta Session Length Policy Co... • Moderate Identity Providers - Compli...	N/A	N/A	+ Add <input checked="" type="checkbox"/>
64% Inactive Users • Moderate End Users - Compliance, Id...	97 2.5... decrease since last ... 4... decrease since last ...	0	+ Add <input checked="" type="checkbox"/>
70% Never Logged In • Critical End Users - Compliance, Ident...	82 0.6... decrease since last ... 1... decrease since last ...	0	+ Add <input checked="" type="checkbox"/>
75% Applications with Expired Secrets • Low Identity Providers - Identity Postu...	N/A	N/A	+ Add <input checked="" type="checkbox"/>
75% No MFA Configured • Critical End Users - Compliance, Ident...	68 3.2... decrease since last ... 0.3... increase since last m...	0	+ Add <input checked="" type="checkbox"/>
90% User Has Directly Assigned App... • Low End Users - Compliance, Identity ...	26 No change since last week 6.9... increase since last m...	0	+ Add <input checked="" type="checkbox"/>
94% Users Sharing Authenticators • Critical End Users - Compliance, Ident...	16 No change since last week 8... decrease since last ...	0	+ Add <input checked="" type="checkbox"/>
96% User Password Expiration Failure • Moderate End Users - Identity Postur...	9 No change since last week 7.8... increase since last m...	0	+ Add <input checked="" type="checkbox"/>
97% Unmanaged Devices Access • Low End Users - Compliance, Devices...	7 96% increase since last week 36.4... increase since last m...	0	+ Add <input checked="" type="checkbox"/>

Identity Intelligence | Privacy Policy | Terms of Use | Documentation | SOC2 Report | This environment reloads hourly

Інформація про користувача

Об'єднає ці дані в розділ "Статистика користувача" та відомості про користувача

Відповідь

OORT вже має мінімальні відповіді; що буде пов'язано з інцидентами та реагуванням на XDR.

The screenshot displays the Cisco Identity Intelligence user profile for 'Loxx' (loxx@securitydemo.net). The interface includes a navigation bar with 'Dashboard', 'Users', 'Checks', and 'Integrations'. The user profile is divided into several sections:

- Summary:** Lists user attributes such as 'Inconsistent, Active', 'Ruler of the 7 Kingdoms', 'Iron Throne', 'SecurityDemo', 'N/A', 'MFA Configured', and 'Jan 31, 2024 20:22:01 UTC (a day ago)'.
- Checks:** A prominent red box indicates '2 failing' checks. A dropdown menu shows actions like 'Reset MFA', 'Log out user', 'Quarantine', 'Send push verification', 'Refresh User Data', and 'Link user'.
- Attempted Logins:** A donut chart shows '73 All Attempts' with a 'Success - 73' percentage.
- Records per day:** A bar chart showing login success rates over time.
- Authentication Factors:** A table listing factors with their assurance levels and status.

Factor	Assurance Level	Status	# Changes	Usage Count	Device
Push SecurityDemo-Duo DFUCY3HKATXKUX885YD_push	Medium	ACTIVE	0	28	Apple iPhone 14 Pro
Password SecurityDemo-Azure 29c10220-6103-485e-b985-444c6001490	Low	ACTIVE	0	1	N/A
Platform_authenticator_(2fa) SecurityDemo-Duo WAZCHKM7HL191YV4QSPU	Medium	ACTIVE	0	1	Touch ID
Phone SecurityDemo-Azure 3179e48e-750b-4251-897c-87b97209287f	Low	ACTIVE	0	0	+1 4102990191
Windows Hello for Business	Medium	ACTIVE	0	0	ATM11AD32M10101

Розуміння

Надає детальну статистику щодо об'єднаних ідентичностей, статусу(ів) багатофакторної автентифікації, адміністративних логінів тощо.

Integration Status

4 Providers Synced

- Providers: G-Suite-Loxx.TV (Success, Average Traffic: 0 records), SecurityDemo-Azure (Success, Average Traffic: 47 records), SecDemo-Okta (Success, Average Traffic: 53 records), SecurityDemo-Duo (Success, Average Traffic: 2 records)
- Data Consumers: Loxx-Postman

Identities

- Total: 182
- In Protected Population: 182
- Inconsistent Users: 6
- Never Logged In: 82 (+0.69% (7 days), +1.82% (30 days))
- Inactive Guest Users: 5 (-22.22% (7 days), -19.01% (30 days))
- Inactive Account Probing: 0
- User Type Missing: 0

MFA Status

- No MFA Configured: 69 (+1.83% (7 days), +1.88% (30 days))
- No Strong MFA Configured: 1
- Weak MFA Was Used To Successfully Sign In: 1 (+16.67% (7 days), +76.92% (30 days))
- MFA Flood: 0
- Telecom MFA Limit Reached: 0
- Admins with Weak MFA: 1

Administrators per Source

21 Administrators

Source	Count
Microsoft Entra ID	18
Okta	2
Google Workspace	1

Users per Source

Source	Count
SecurityDemo-Azure	171
SecDemo-Okta	34
SecurityDemo-Duo	12
G-Suite-Loxx.TV	4

Administrators Logins

User	Last IP Address	Tags
Loxx loxx@securitydemo.net	75.182.151.17 Waxhaw, NC, US	New IP USA
Aaron Woland (aawoland) aawoland@cisoco	75.182.151.17 Waxhaw, NC, US	New ISP USA
Matt Vander Horst matt@securitydemo.net	71.234.238.58 Holyoke, MA, US	USA
Suecitra suecitra@securitydemo.net	2881.428:c8c4:1884::183 Milpitas, CA, US	New IP USA
Chunyu Qiu chuqiu@securitydemo.net	2881:428:c8c4:1884::336 Wilmington, DE, US	New ISP USA
Hanna Jabbour harrjaboo@securitydemo.net	94.284.159.72 Dubey, Dubey, AE	New ISP

Login Attempts from New Countries

Country	Success	Failure	Other
Bulgaria	23	6	0

Identity Security розділена на 2 окремі напрямки

Встановлення рівня

- Виявлення та реагування на загрози ідентифікації (ITDR)

- **РЕАКТИВНО**

- Використовує виявлені об'єкти та аналітику в усіх джерелах ідентифікації та автентифікації в організації
- Інтегрує загрози, пов'язані з ідентифікацією, в інциденти для повної картини
- Наприклад: атака MFA Flood або неможлива подорож у часі (ITT).

- Керування безпекою ідентифікаційних даних (ISPM)

- **ПРОАКТИВНА**

- Зосереджується на неправильних конфігураціях, порушеннях політики.
- Наприклад: Слабкий / не налаштований багатфакторна автентифікація

Інтеграція *Cisco Identity Intelligence* в *Cisco XDR & Duo Security* зараз в процесі

Keep an eye out!

Agenda

- Урок історії
- Еволюція
- Керування інцидентами і процеси
- Інтеграція та реагування
- Ключова телеметрія XDR
- Це все!

Так... Що відбувається зараз?

- XDR – це новий продукт, і Cisco бере за нього плату.
- SecureX може мігрувати на Cisco XDR.
- Secure Cloud Analytics став XDR.

- Всі існуючі інтеграції для SecureX і SCA продовжать працювати.
- Усі існуючі робочі процеси оркестрації працюватимуть і надалі.
- SecureX продовжить існувати для керування CSC та існуючих клієнтів, які не перейшли на XDR
- SecureX EoL у липні '24, заміна CSC Management незабаром



The bridge to possible

Thank you

CISCO *Live!*