The bridge to possible

Cisco XDR

Сенс рішення

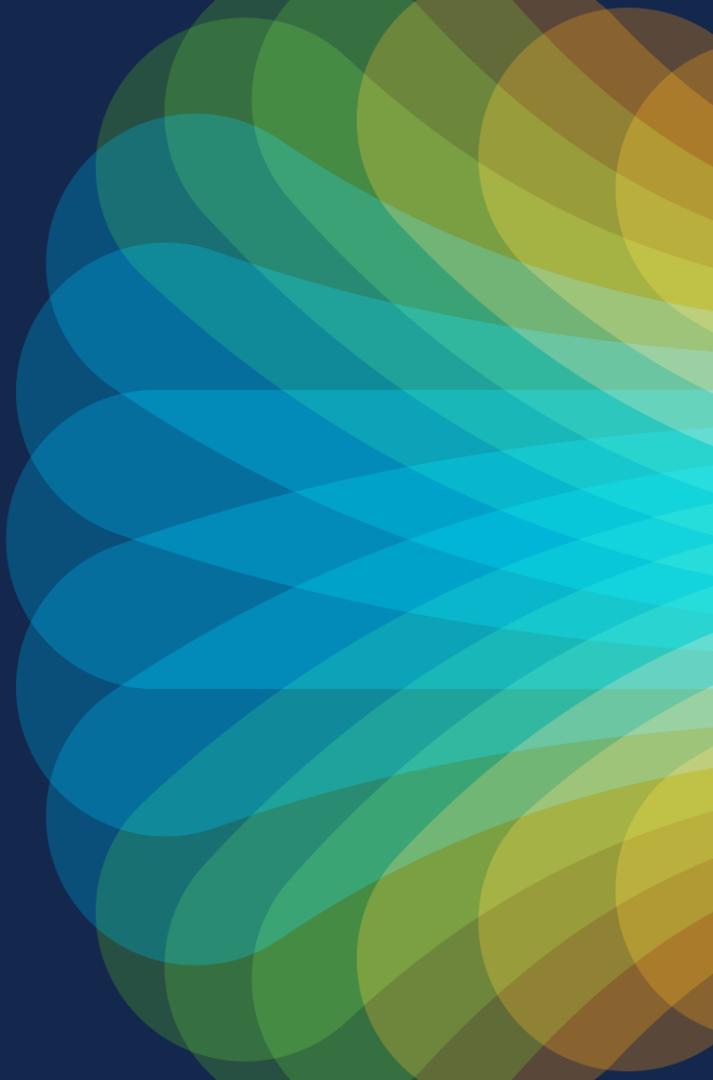
Павло Родіонов, CCIE 11155, CISSP, GREM
Solutions Engineer, рішення Cisco Security
prodiono@cisco.com

cisco Live!

Agenda

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

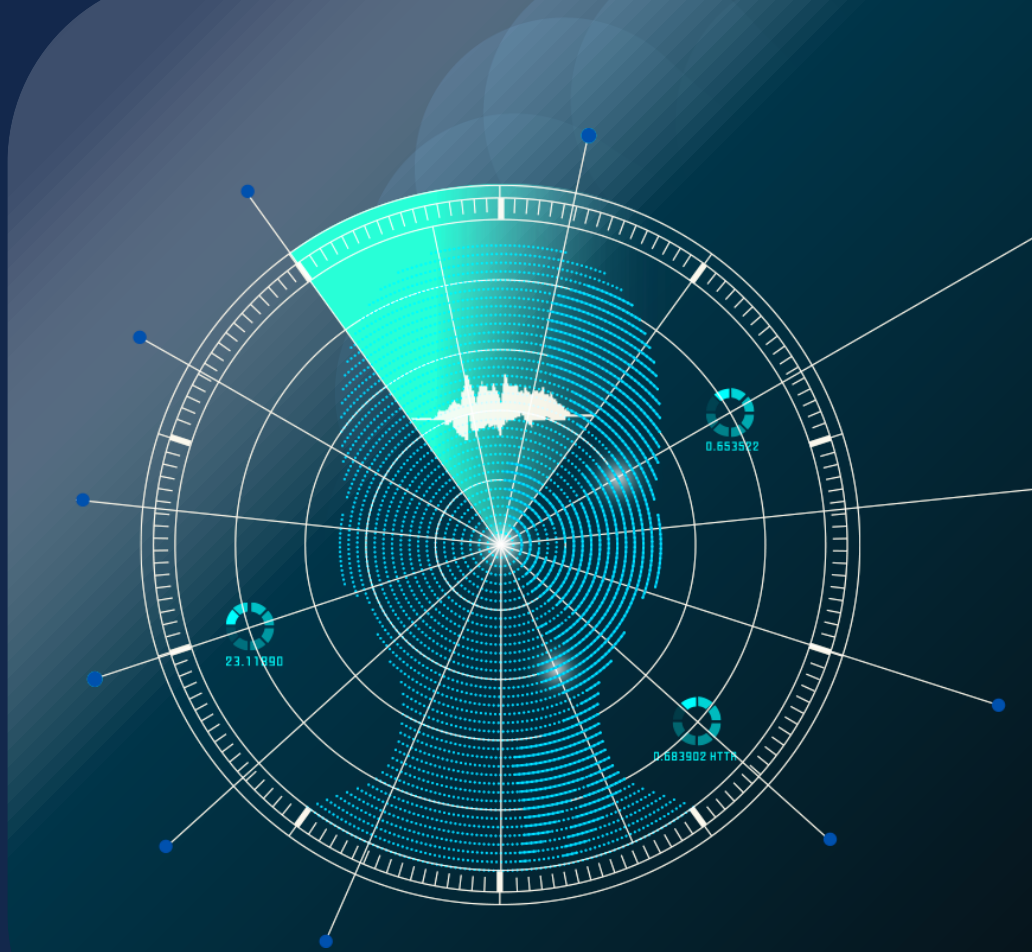
Невеликий урок історії



Ще у 2017 році

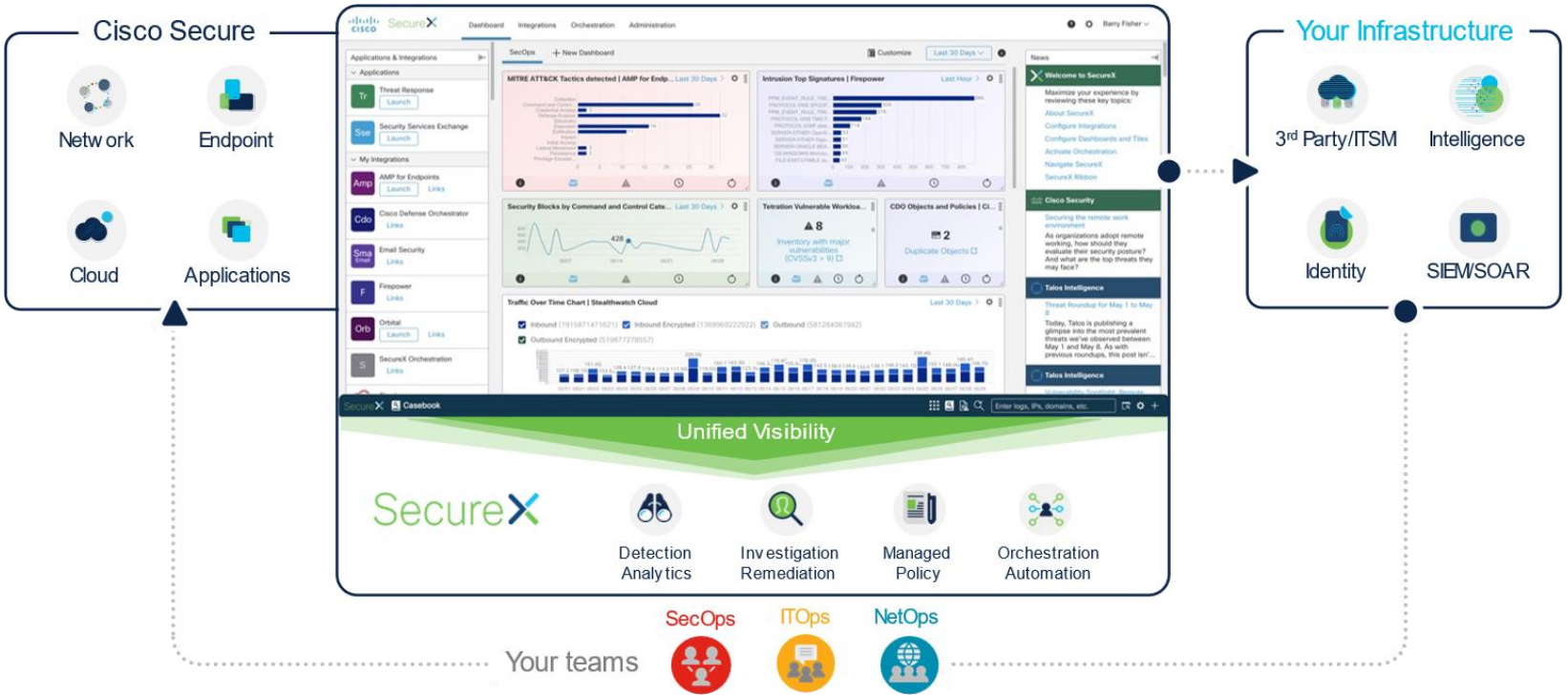
- Улюблений проєкт Security Leadership: «visibility»
  - Перейменований на Cisco Threat Response (2018)
    - На основі історії виконання incident response
    - Продукція процесу, якого вони дотримувалися як практики
    - Шукайте ”observables", і він збагачується з усіх інтегрованих джерел (через API)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

Потім в 2020...



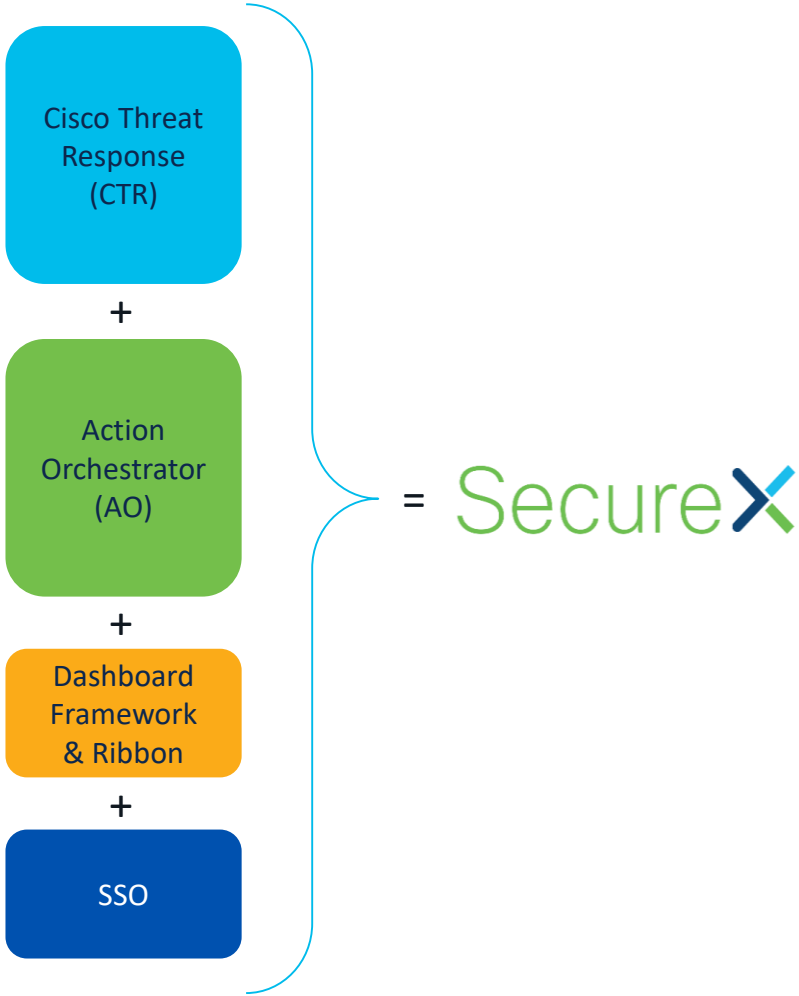
Представлено SecureX у травні 2020 року

Хмарна **вбудована** платформа в нашому портфоліо

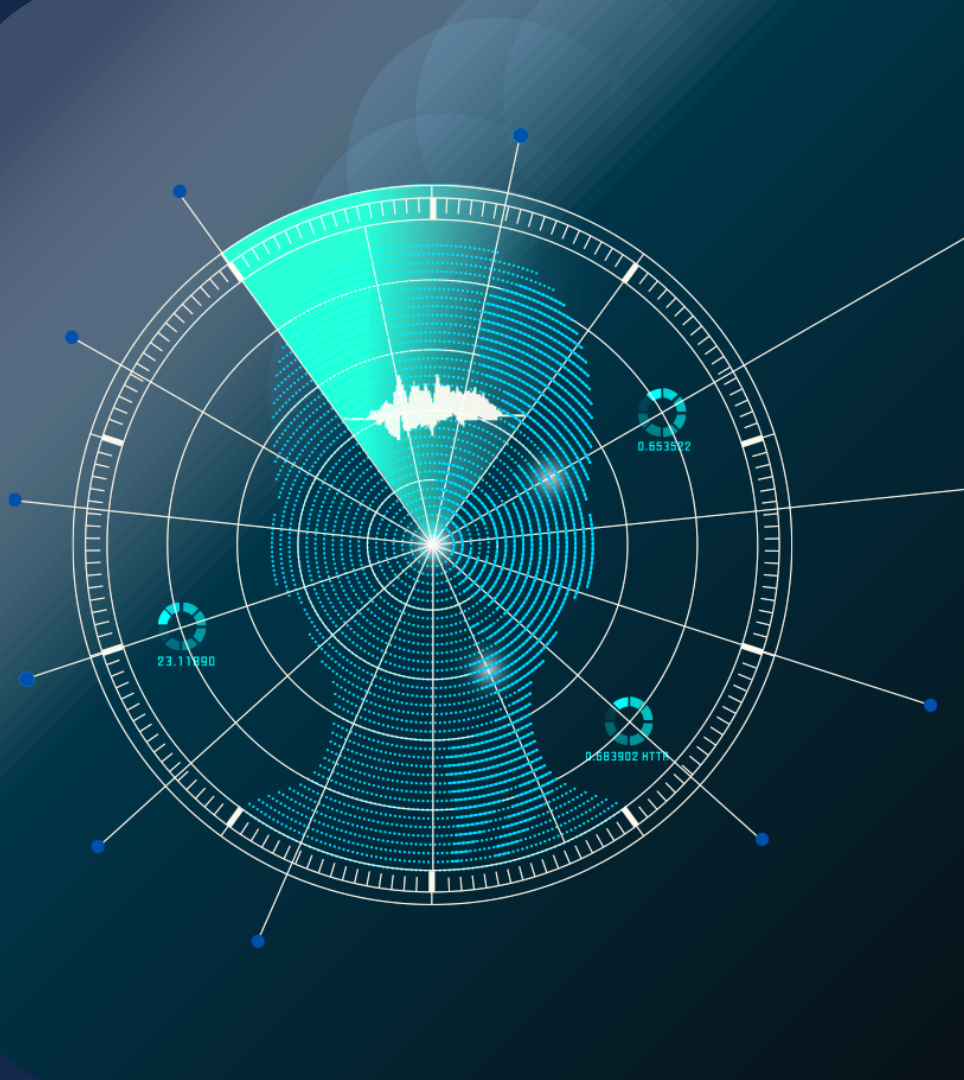


SecureX мав стати платформою

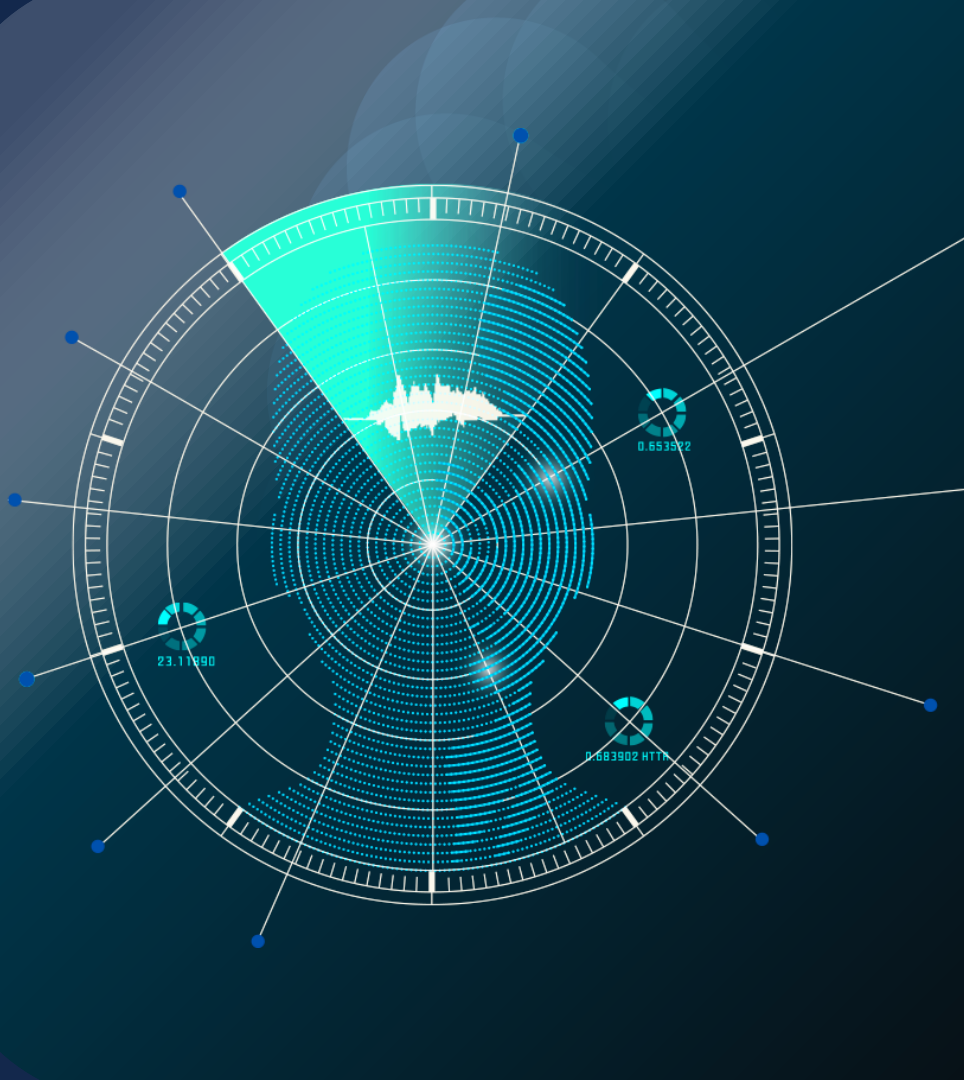
- Cisco Secure [function]
  - X мав стати центральним місцем
  - X використовував Cisco Threat Response для інтеграції всіх продуктів Cisco разом
  - X додає повний механізм автоматизації, який ми «придбали» у хмарного підрозділу
  - X надав досвід єдиного входу для безпеки Cisco
  - Усі майбутні інтерфейси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



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



Cisco повністю прийняла концепцію XDR; розглядаючі 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**

Значні внутрішні інвестиції 2

Розширення наших команд User Experience та Interface

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

3 **Прямі та дотичні опитування**

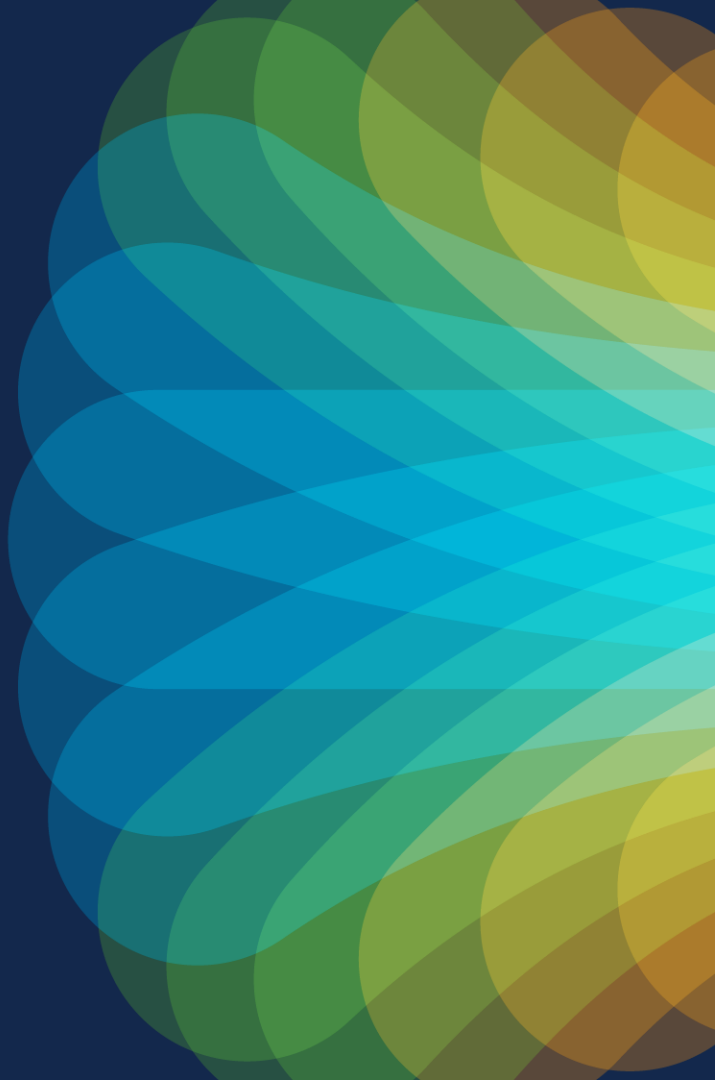
Широкий найм експертів 4

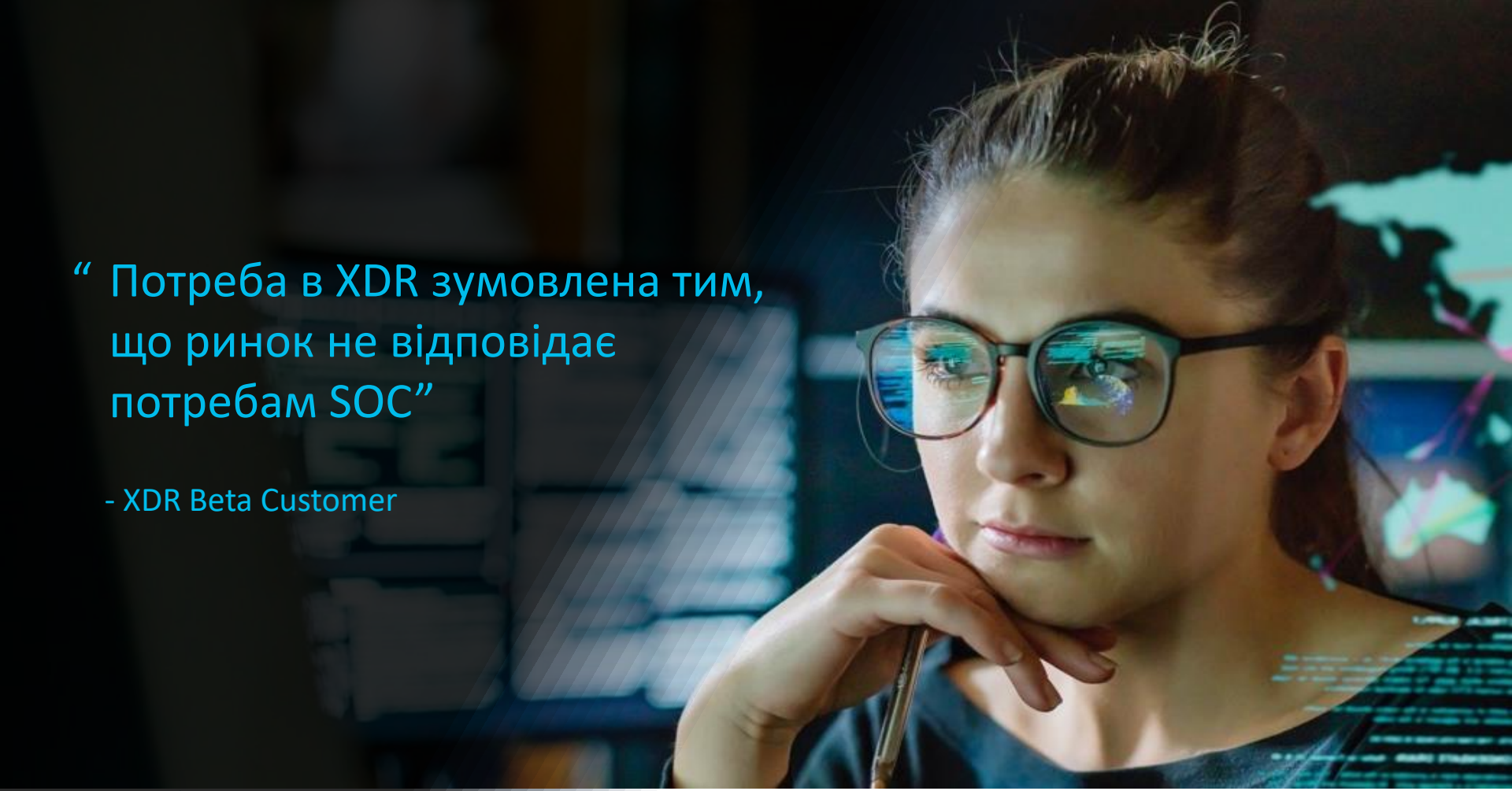
Залучили головних інженерів у ключових місцях з величезним досвідом управління інцидентами / SOC

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

5 **Реструктуризація наших продуктів**

Що це дало?





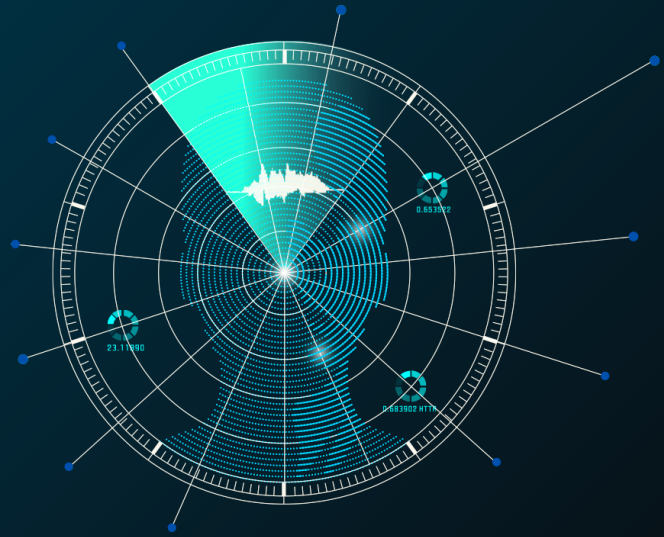
Bopor
Turla

// Nickname

Snake,
Venomous Bear,
Uroburos,
Group 88,
Waterbug

Супротивник: що відомо?

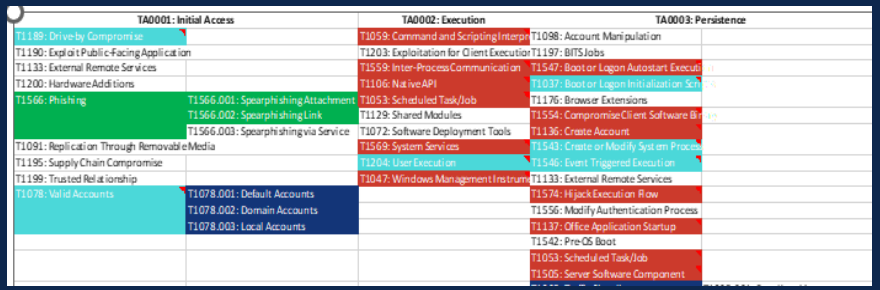
- Естонські спецслужби пов'язують це угруповання з Федеральною службою безпеки Росії (ФСБ).
- НЕ розгортає розширені інструменти, якщо це не необхідно для компрометації цілі

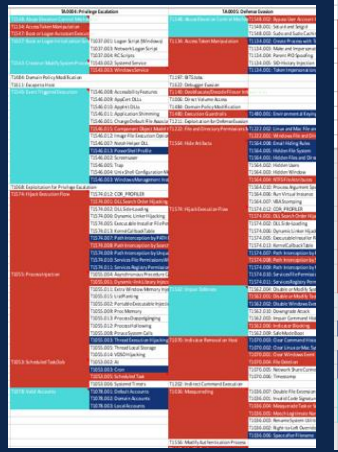


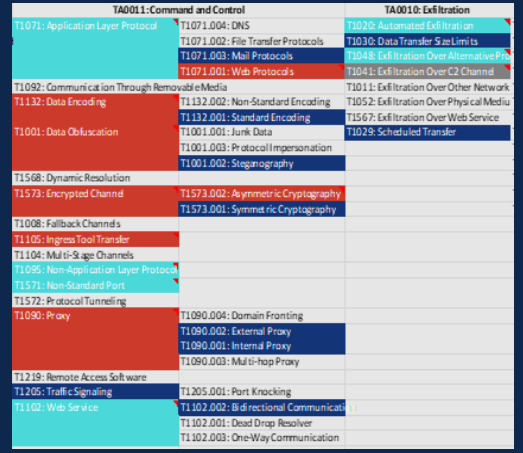
Метод:

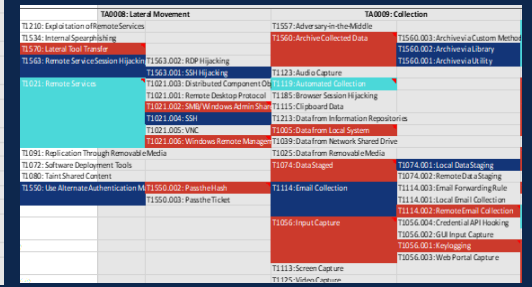
- Віддає перевагу водопоям і соціальній інженерії для маніпулювання жертвами
- Виготовлені приманки ретельно пристосовані до своїх цілей
- Теми-експлойти, пов'язані з поточними подіями
- Шкідливе програмне забезпечення першого етапу зазвичай діє як фільтр

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





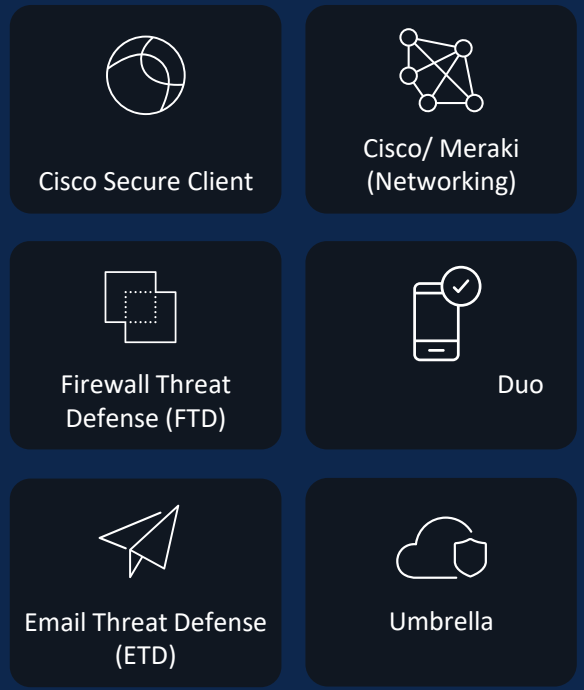




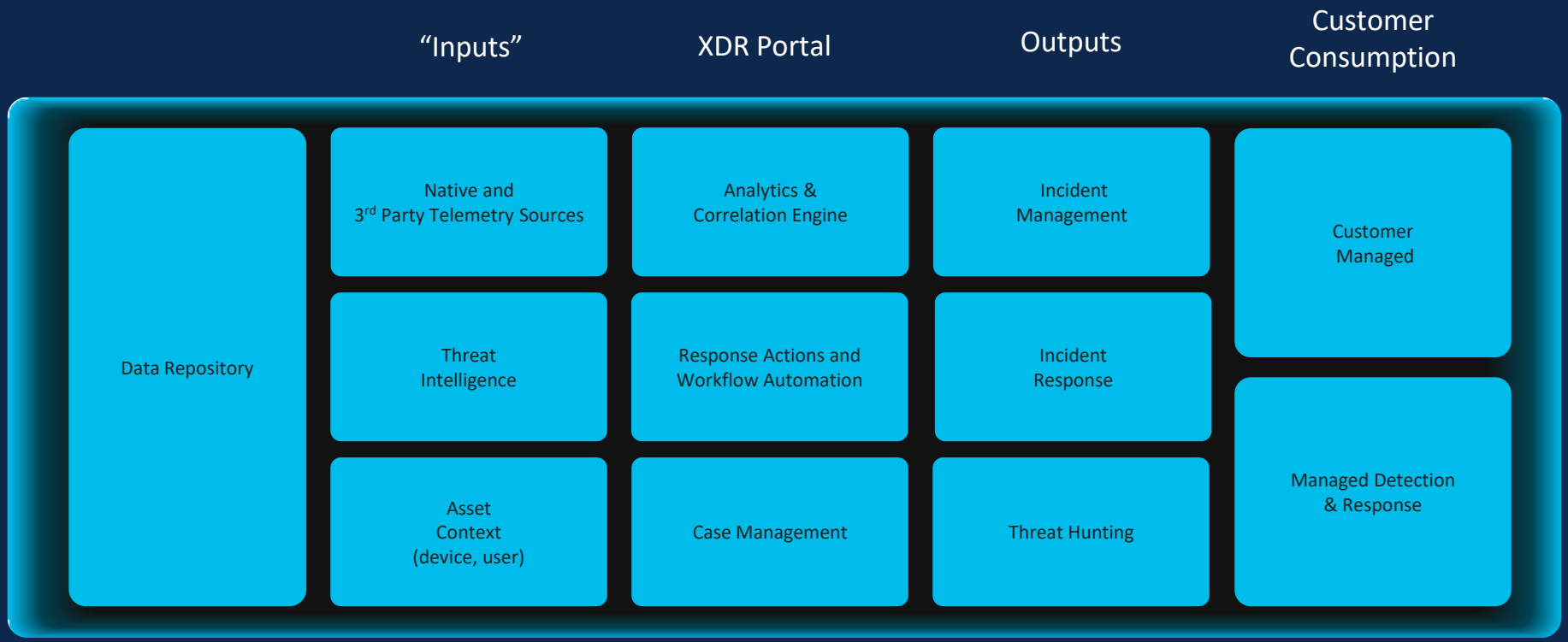
Важливість джерела телеметричних даних

Шість основних джерел даних, які, на думку клієнтів, є важливими для XDR:
Endpoint, Network, Firewall, Identity, Email and DNS

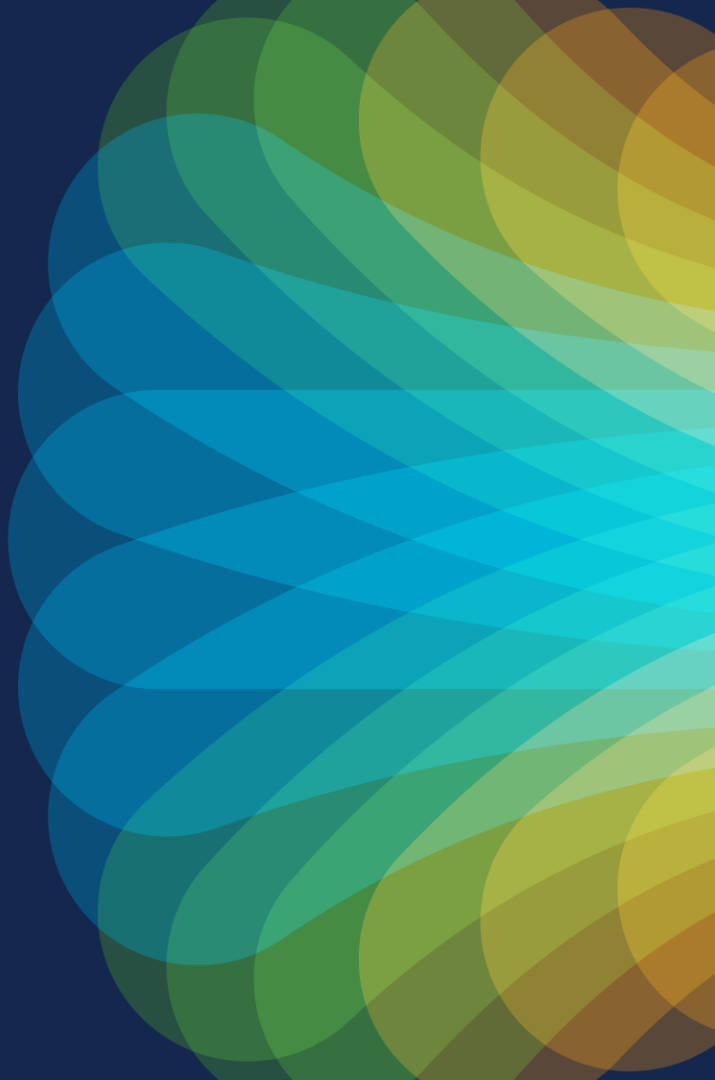
	Essential	
	Count	Share
Endpoint	255	85.0%
Network	226	75.3%
Firewall	207	69.0%
Identity	191	63.7%
Email	179	59.7%
DNS	140	46.7%
Public Cloud	137	45.7%
Non-Security Sources	36	12.0%



З яких складових блоків складається ідеальне рішення XDR?



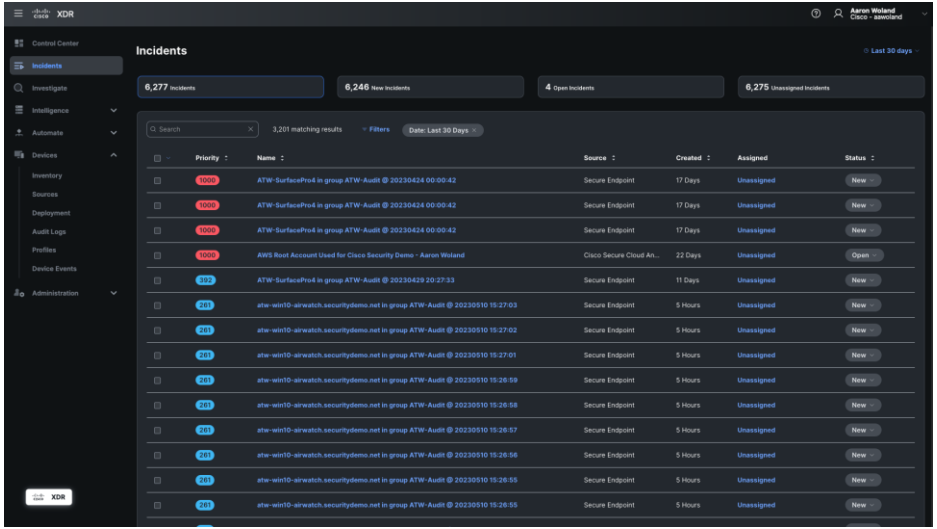
Як ми цього досягаємо?



Еволюція

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

soon plus



“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

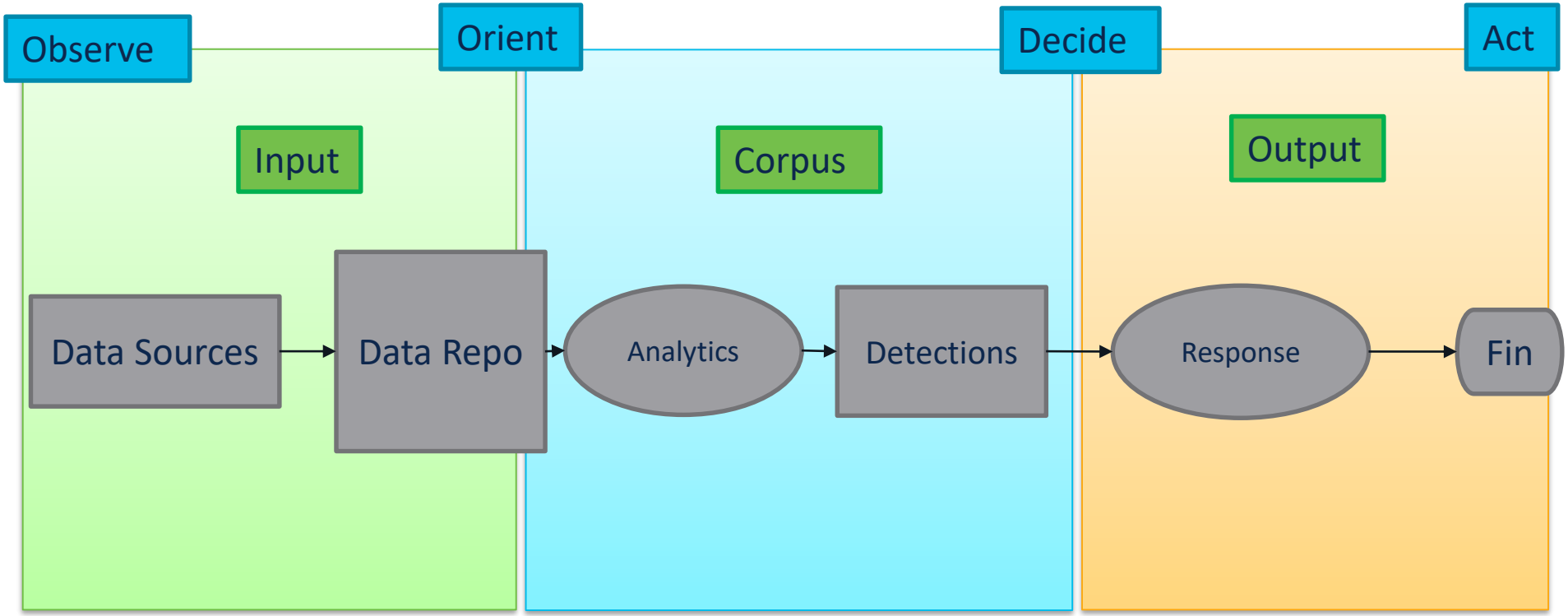
Tier 2 (Sr/Lead):

- Сповіщення IDS/IPS
- Шахраї-користувачі
- DNS Sinkholing домени
- Блокування IP/VPN
- DDoS
- Ескалація до CTI/CTA/CTD/IR
- 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

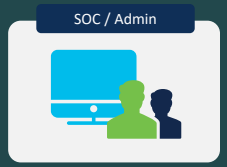
XDR прискорює цикл OODA



Аналітики будують хронологію.

XDR **автоматизує створення** хронології

Хронологія розслідування – що сталося і коли?



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/TTP?

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.

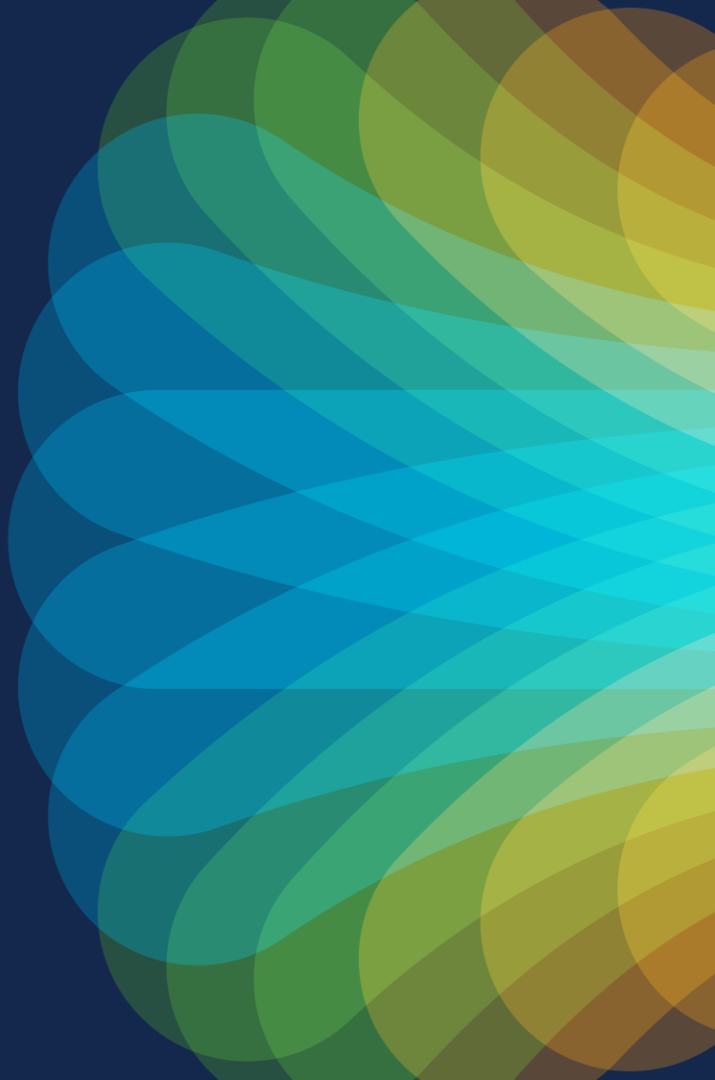
Зовнішнє збагачення

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



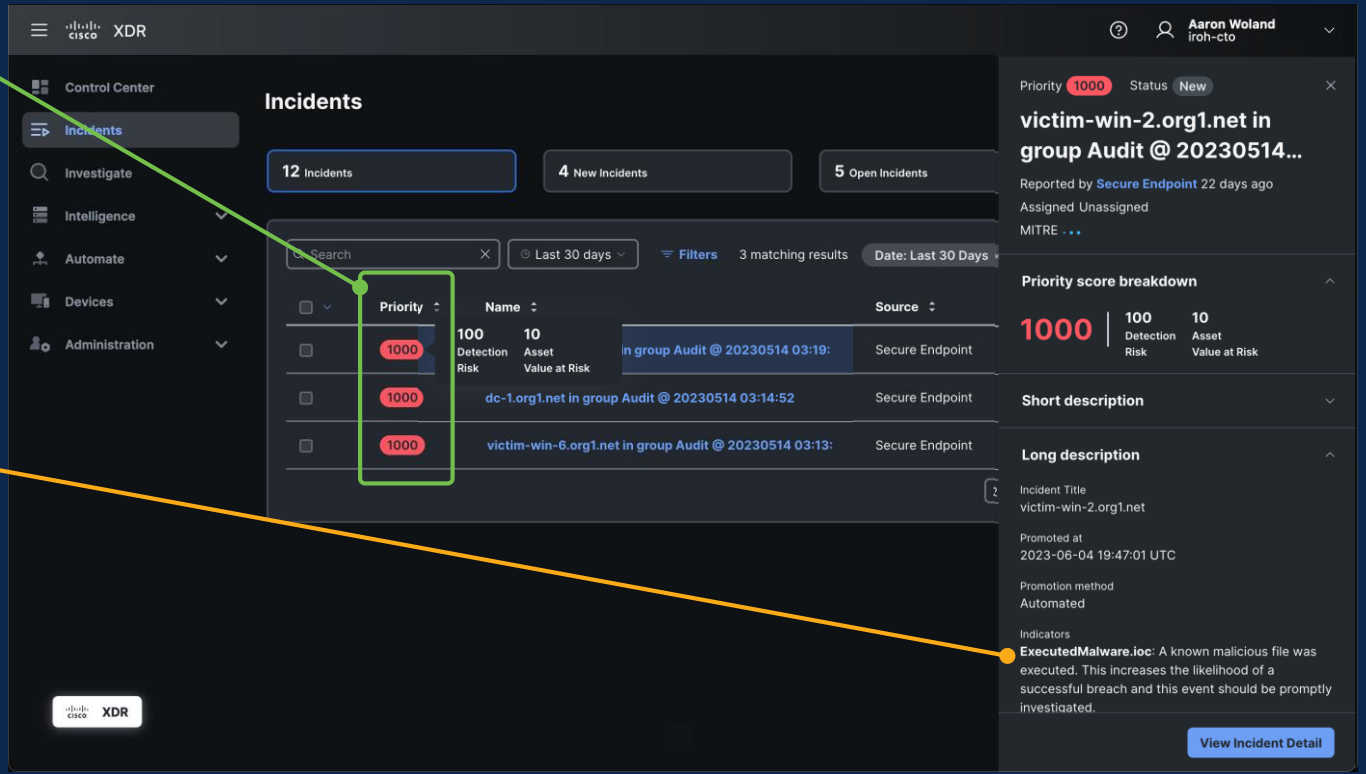
Cisco XDR – Incident Manager

Пріоритетна черга

Використовує (запатентований) Алгоритм від Kenna 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



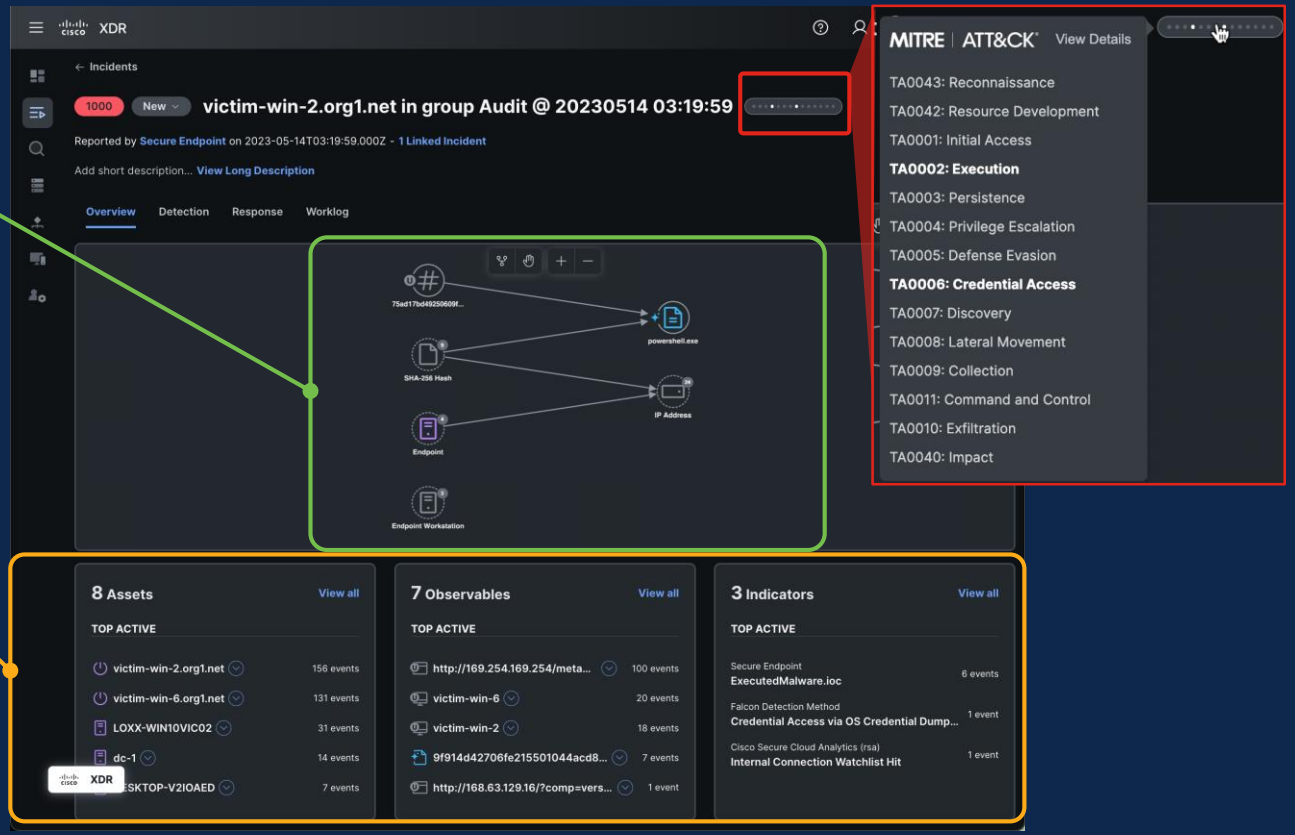
Cisco XDR – Диспетчер інцидентів / Огляд

Огляд

Схема для узагальнення інциденту. Не детальна схема розслідування.

Активи / Спостережуваний об'єкт та індикатори

Найактивніший список із загальною кількістю, зазначеною вгорі.



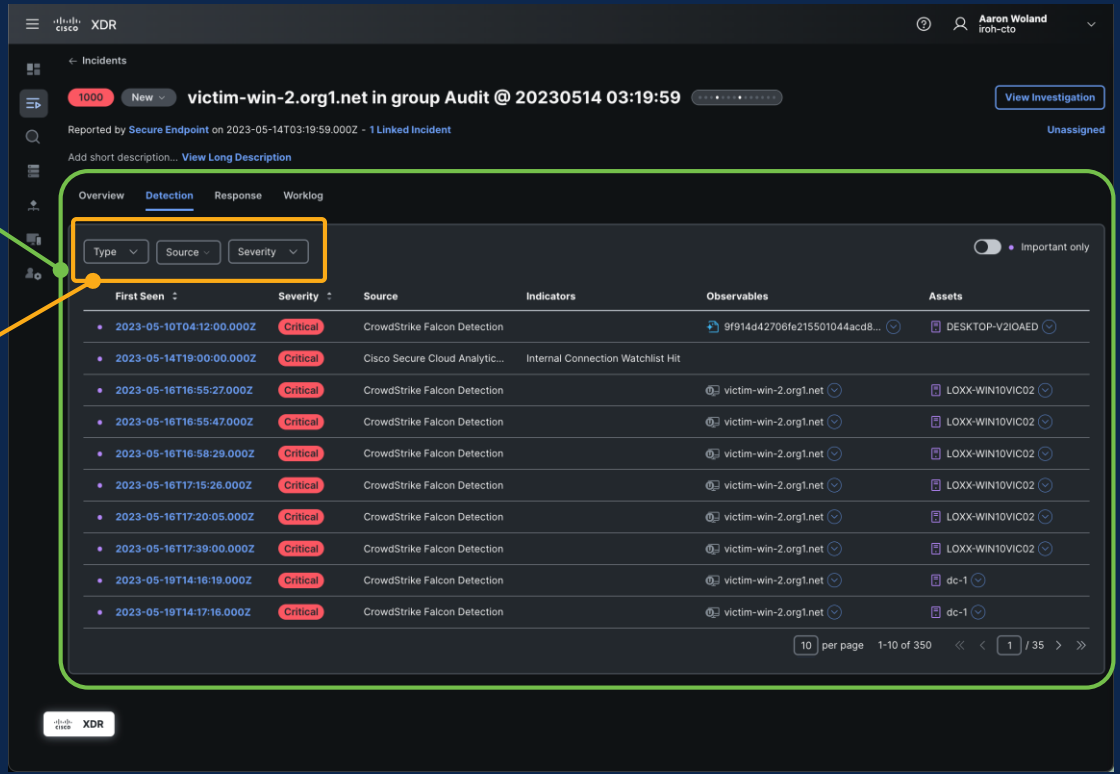
Cisco XDR – Диспетчер інцидентів / Виявлення

Виявлення

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

Типи подій

Оригінал: сповіщення надіслано до XDR
Досліджено: корельовані події



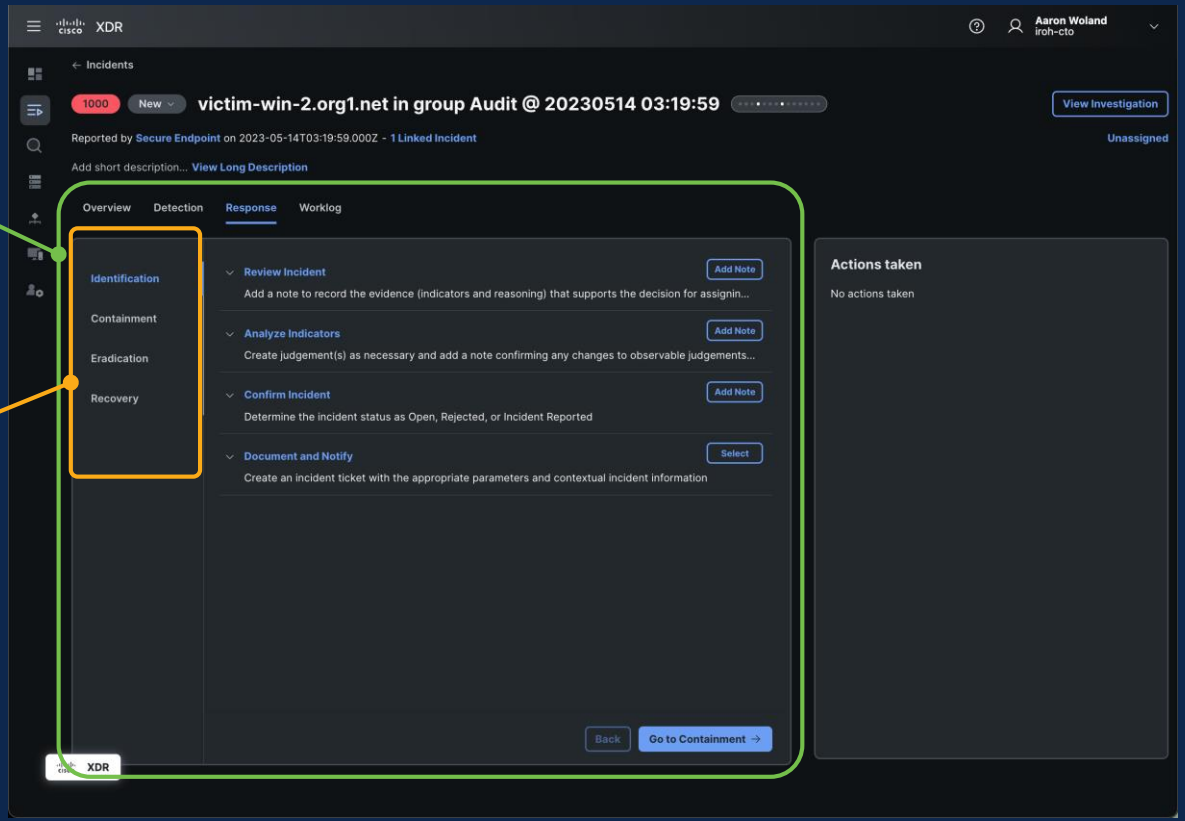
Cisco XDR – менеджер інцидентів / реагування

Відповіді

Контент, специфічний для TTP в інциденті

Крок через

Identification -> Containment -> Eradication -> Recovery



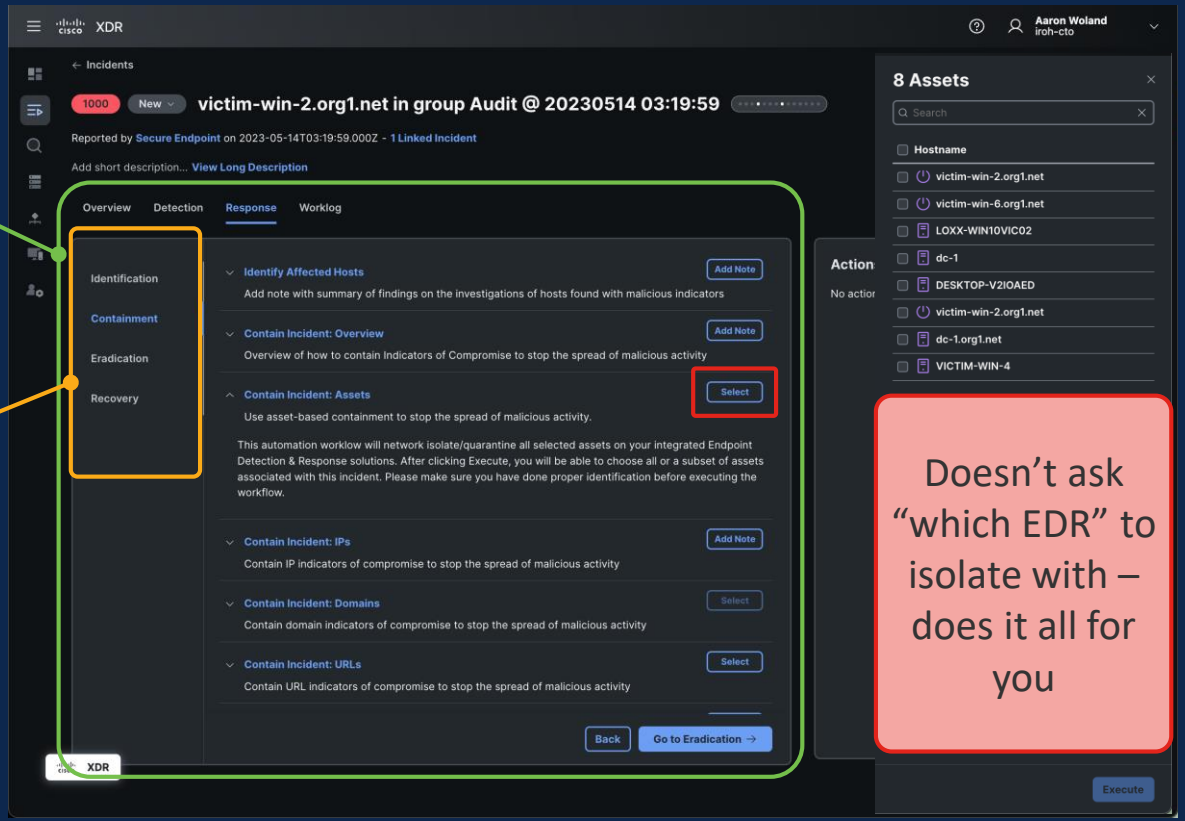
Cisco XDR – менеджер інцидентів / реагування

Відповіді

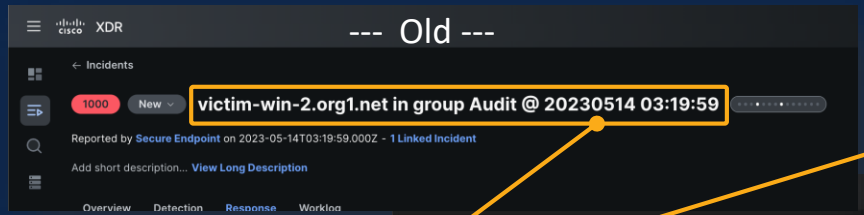
Контент, специфічний для TTP в інциденті

Крок через

Identification -> Containment -> Eradication -> Recovery



Cisco XDR – AI який допомагає аналітику

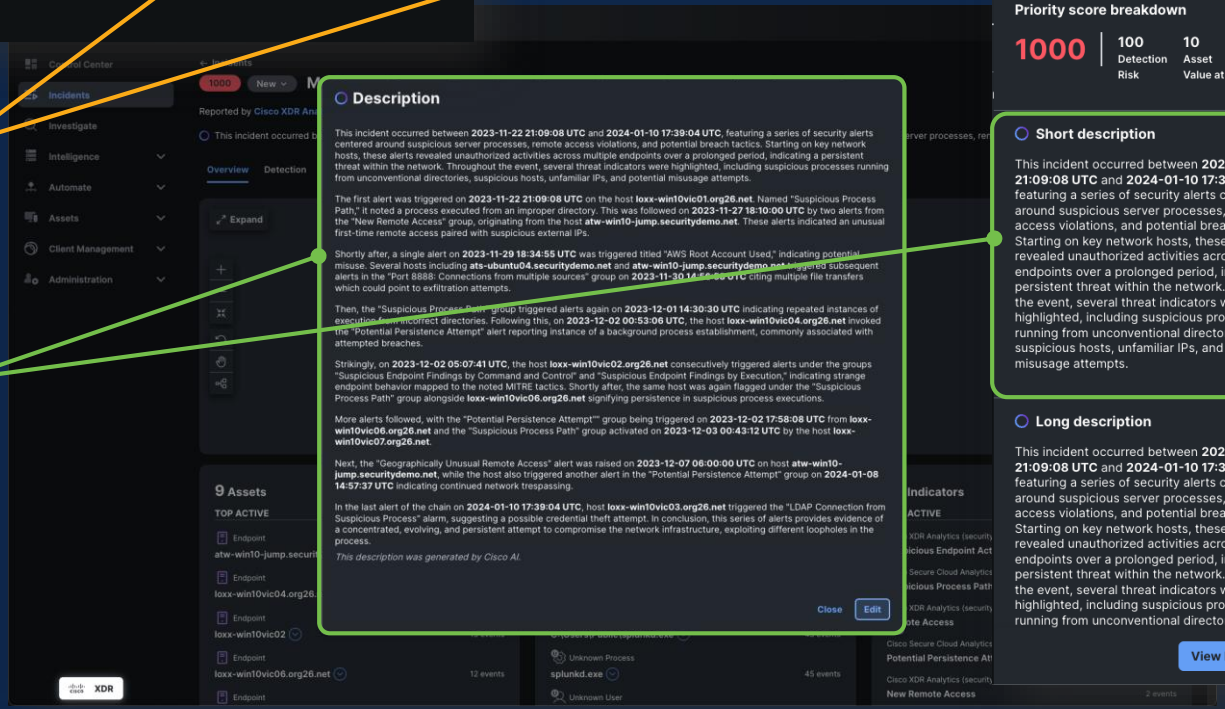


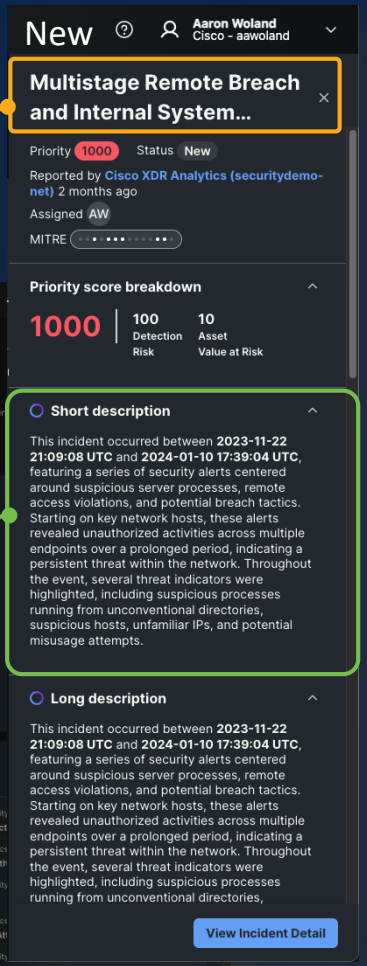
Назви інцидентів

Тепер генерується AI, що робить їх набагато зрозумілішими.

Описи

Короткі та довгі описи тепер також генеруються AI
Значно зменшуються зусилля аналітика

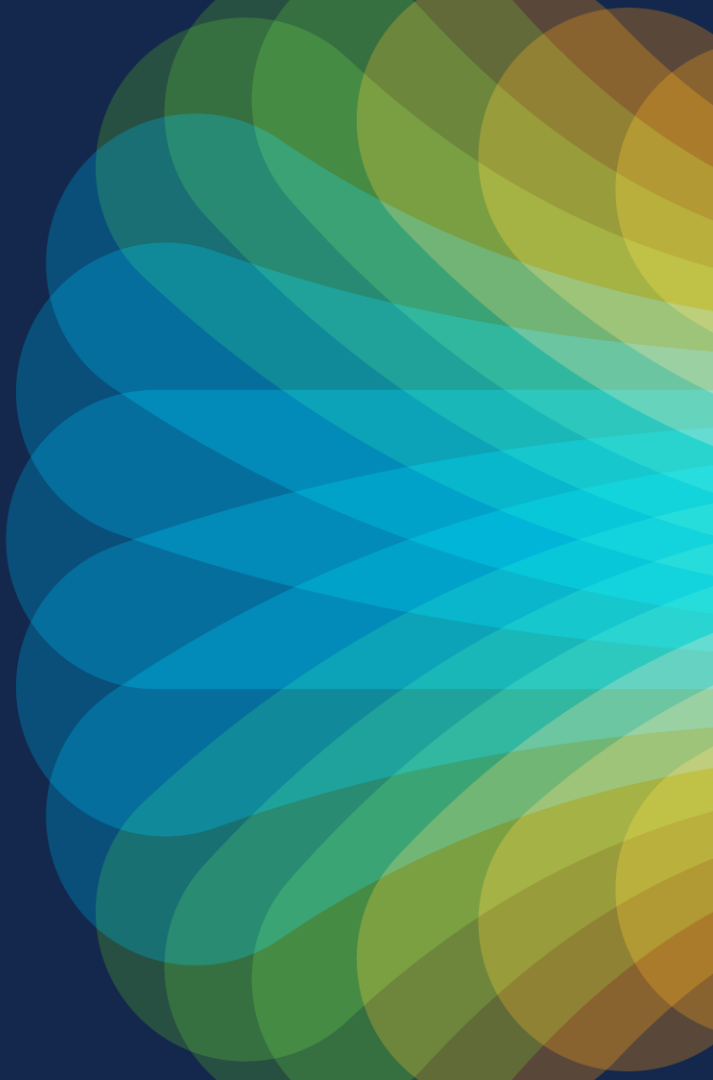




Agenda

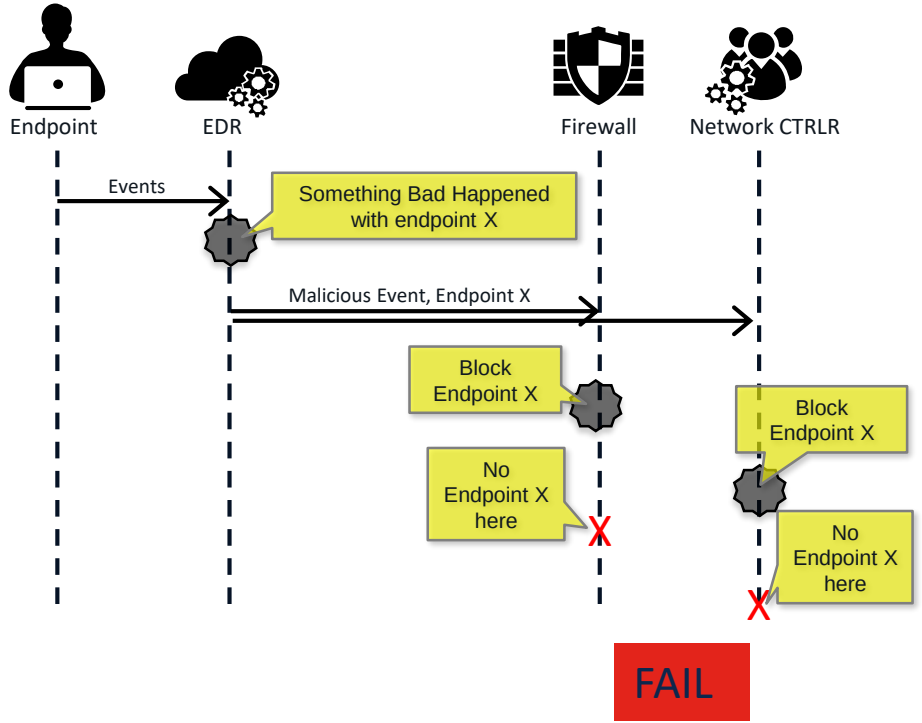
- Урок історії
- Еволюція
- Керування інцидентами і процеси
- Інтеграція та реагування
- Ключова телеметрія XDR
- Це все!

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

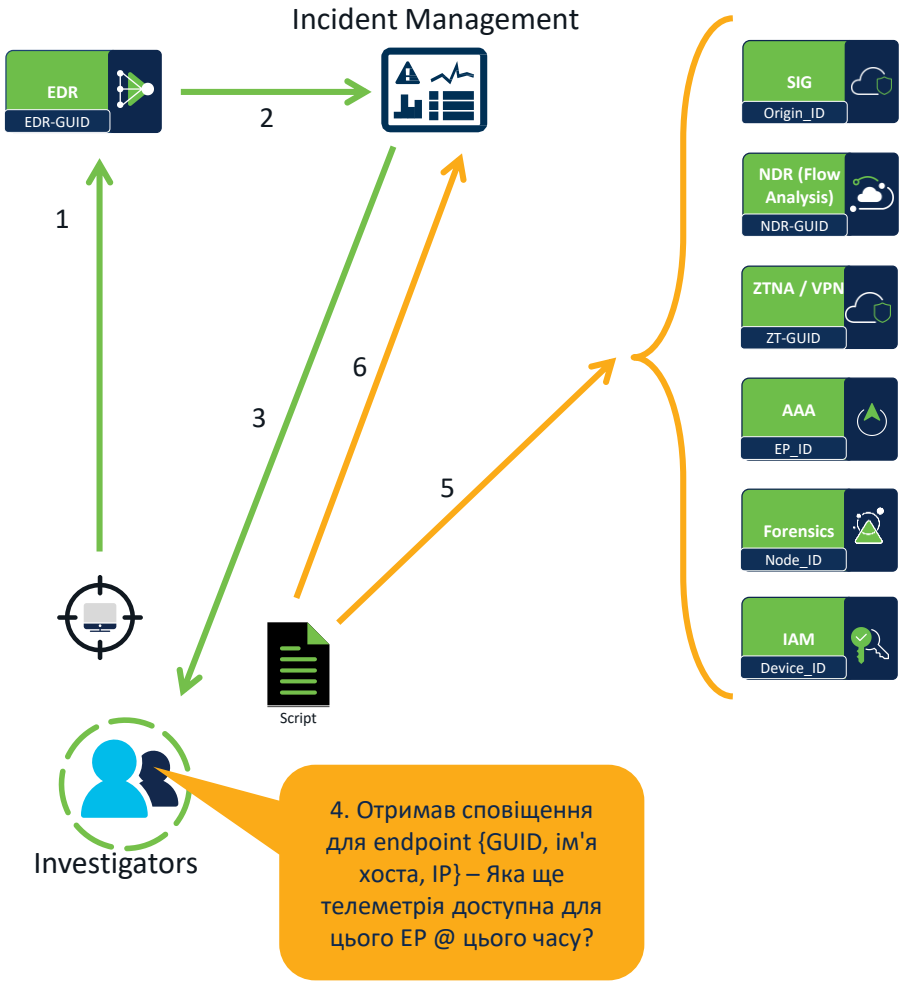


Нам потрібен спільний кінцевий об'єкт

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

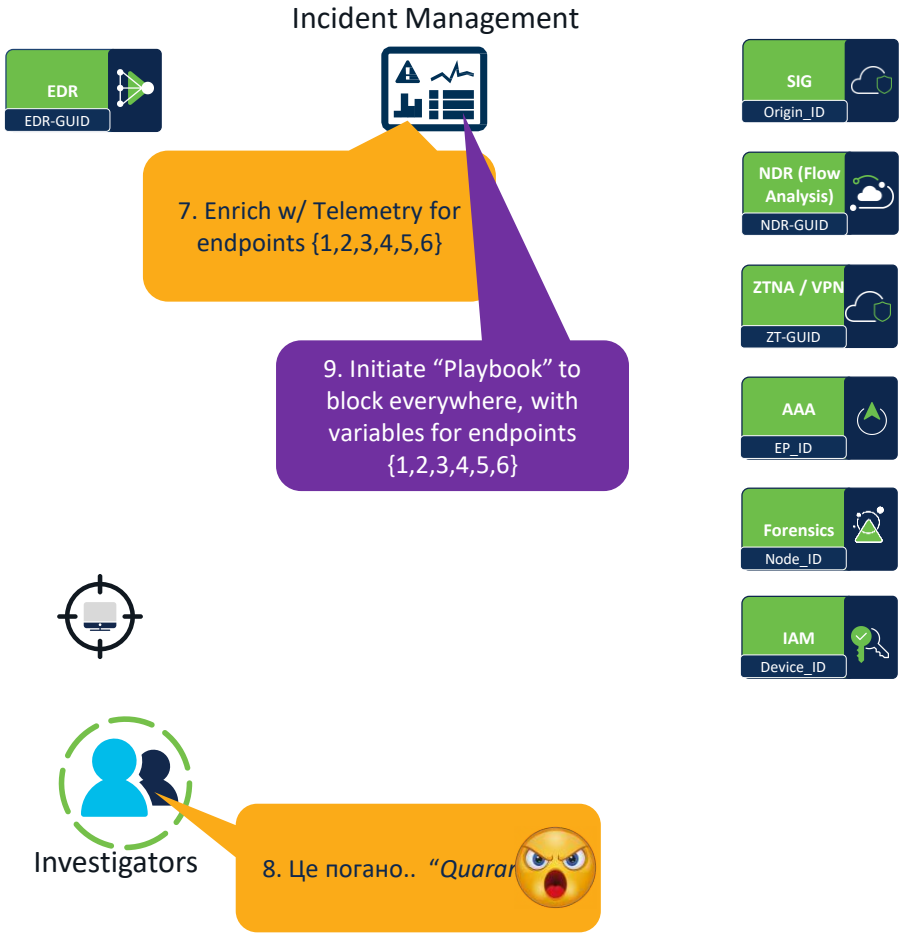


Хід розслідувань SOC

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 «всемогутнього» карантину
9. Інструменти управління інцидентами ініціюють playbook для реагування в усіх пунктах використання

**Комусь потрібно було побудувати ці процеси



Хід розслідувань SOC

Примітка: це загальний приклад:

a) Playbook ініціює ізоляцію за допомогою EDR-GUID

b) Playbook блокує домен на SIG

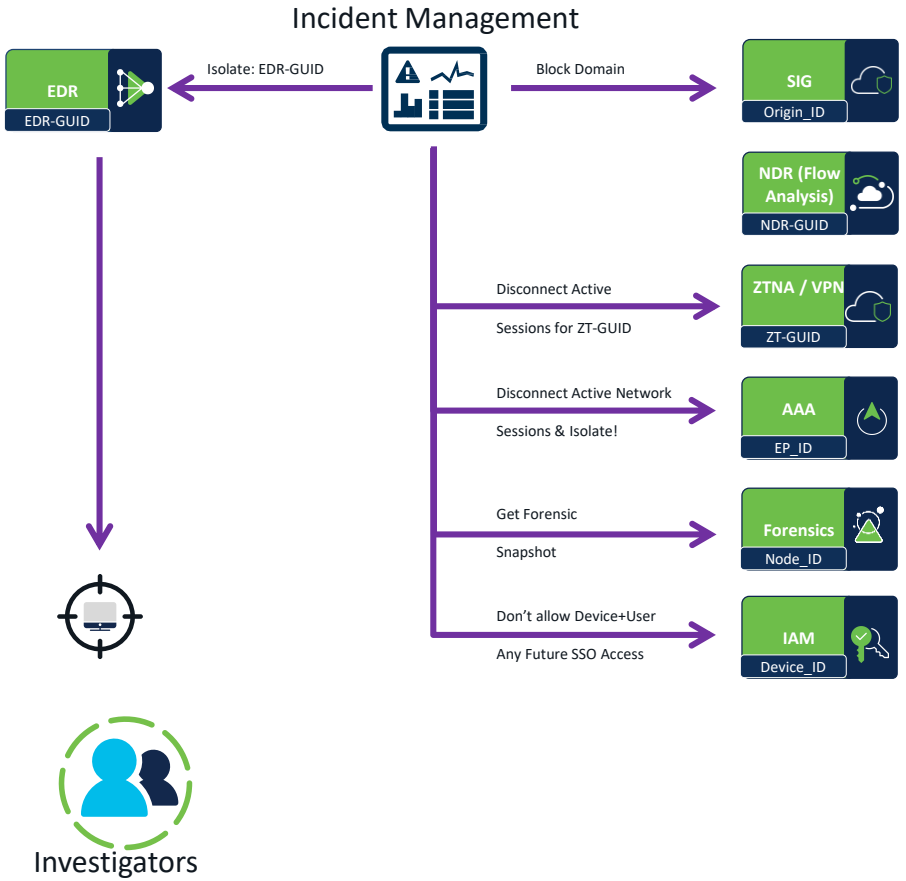
c) Playbook відключає активні сеанси для сеансів ZTNA/VPN і AAA

d) Playbook ізолює кінцеву точку, коли починається новий сеанс AAA

e) Playbook ініціює новий forensics знімок зараженого хоста

f) Playbook інформує рішення IAM, щоб відхилити будь-які подальші спроби комбінації Користувач+Пристрій

**Комусь потрібно було побудувати ці процеси



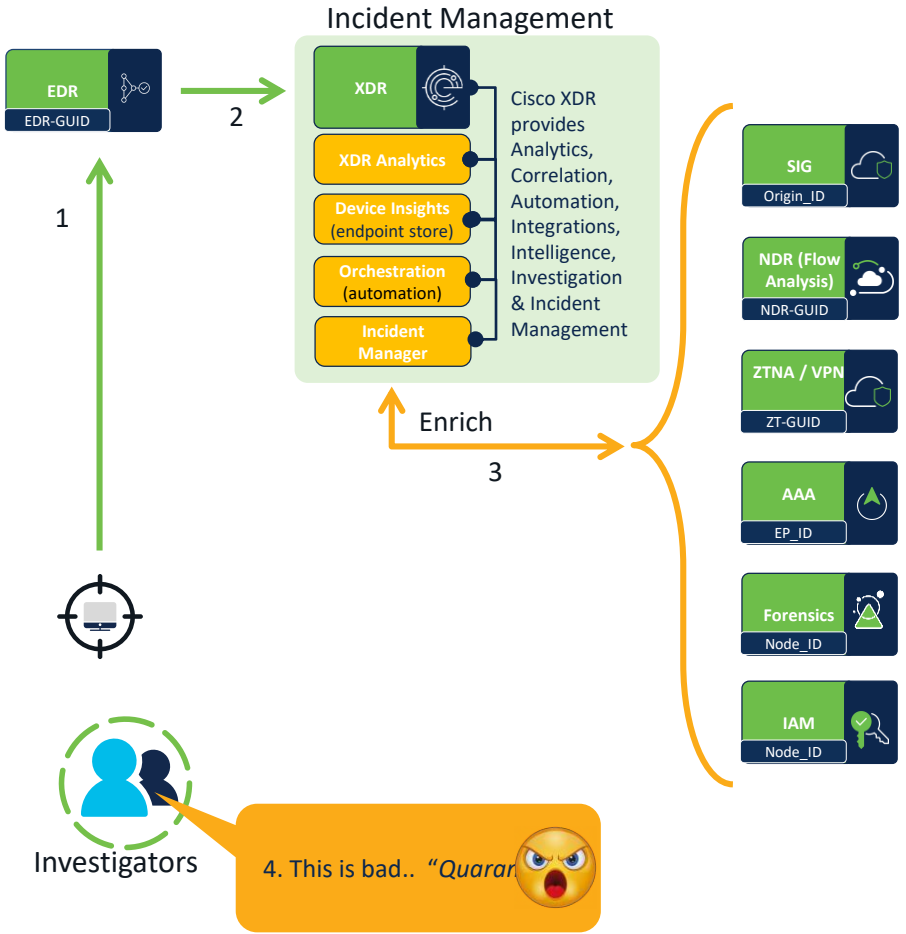
Хід розслідувань SOC

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



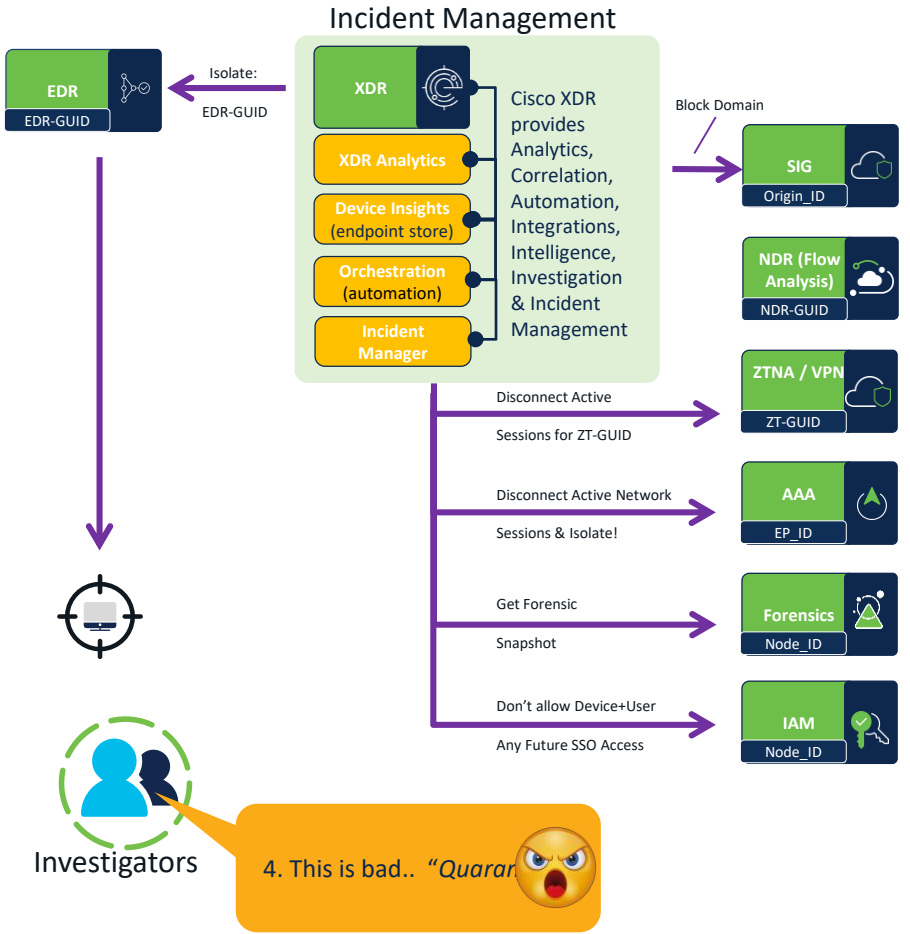
Хід розслідувань SOC

З Cisco XDR:

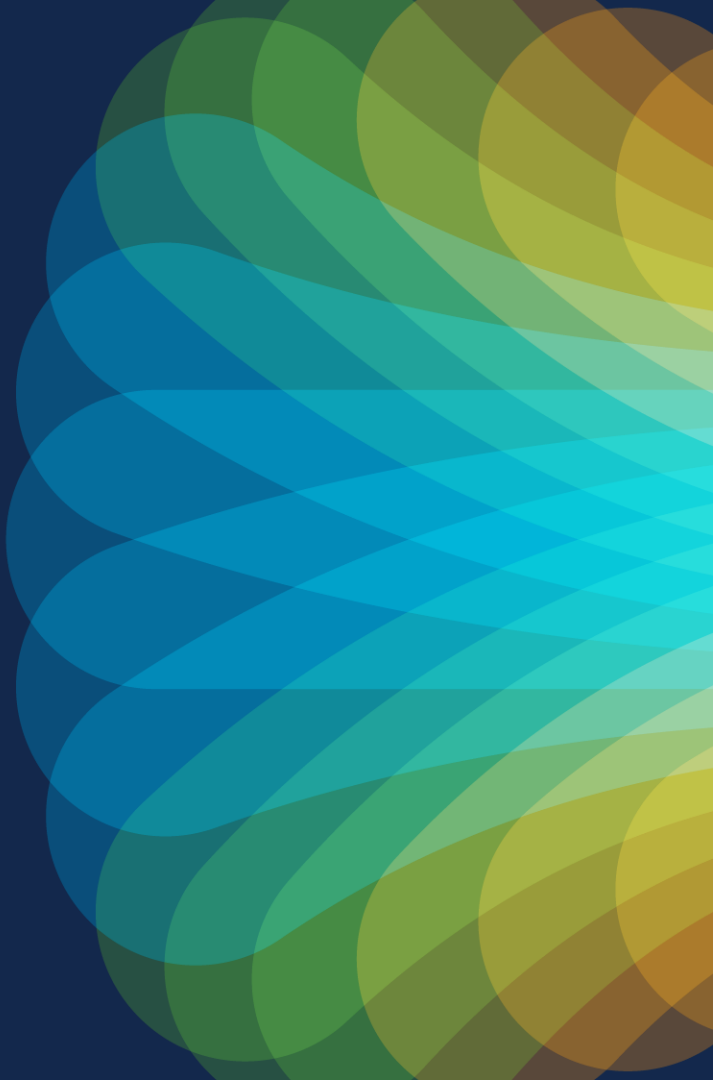
1. EDR виявляє зловмисну активність
2. Сповіщення надіслано до Cisco XDR

   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,?

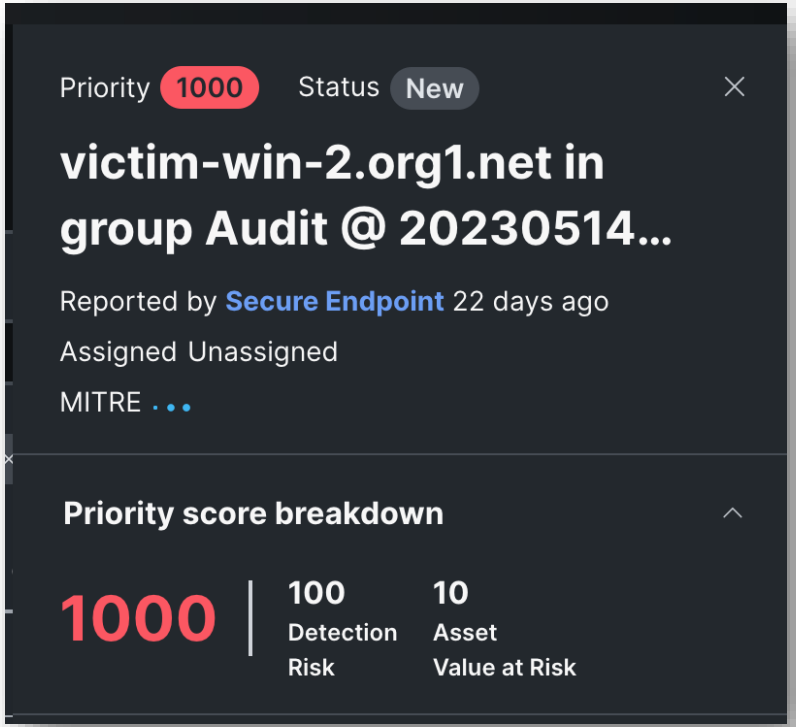


Пріоритет інцидентів

- За своєю суттю: це комбінація:

  Detection Risk
  +
  Asset Value

- Звідки беруться ці значення?



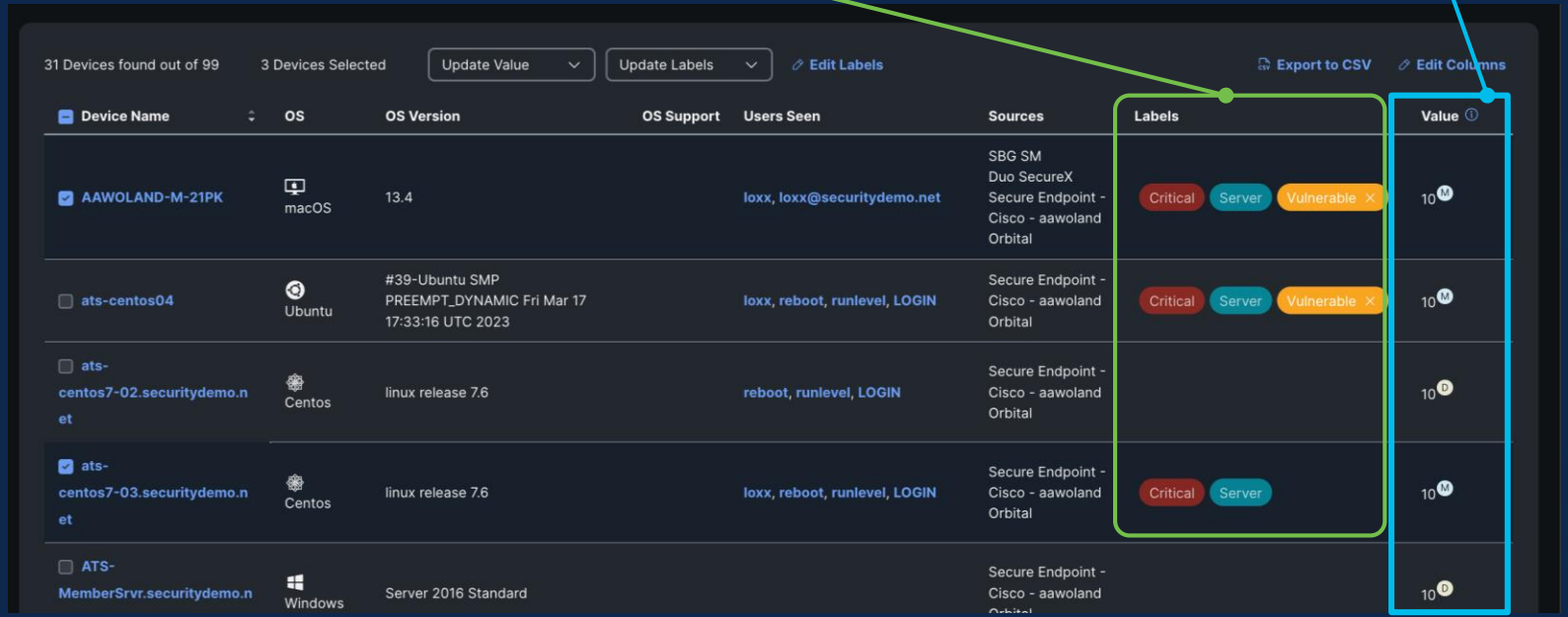
Device Insights у XDR додає деякі нові речі

Етикетки

Опис/групування пристроїв – вручну та програмно

Значення пристрою

Значення 1-10.
1 = найменш цінні
10 = Найцінніший



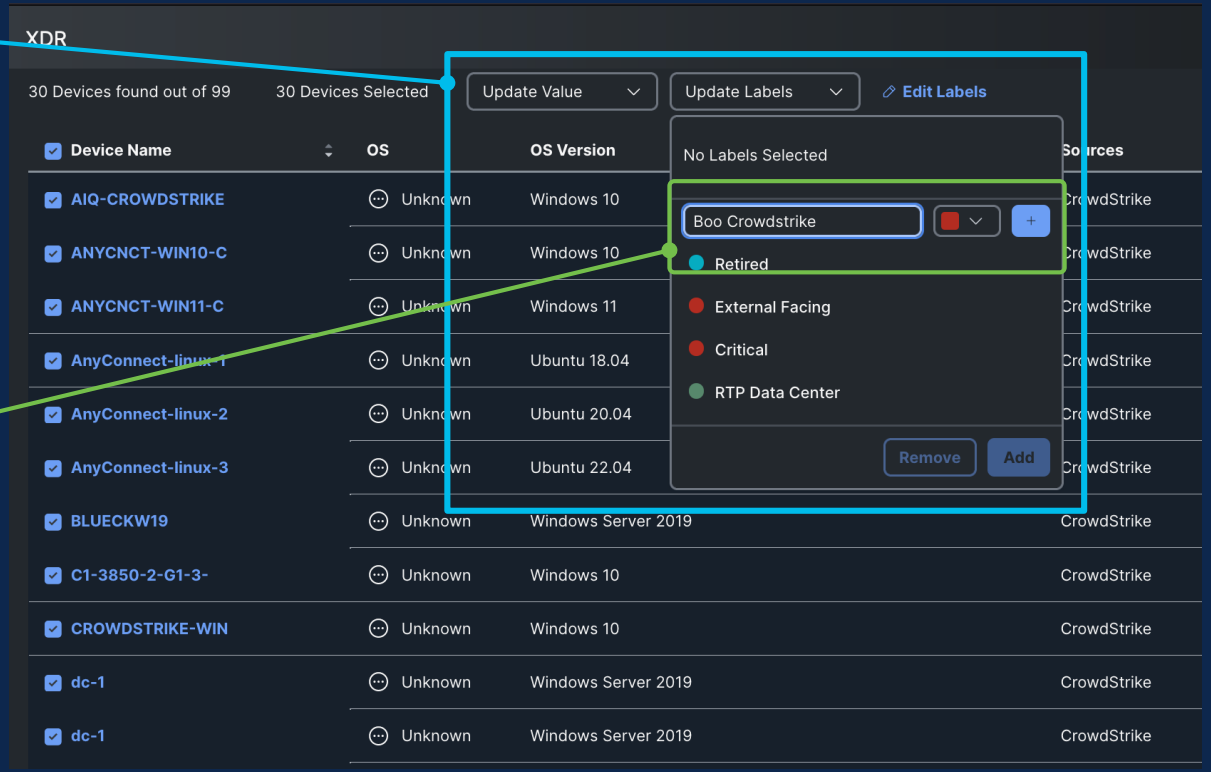
Device Insights у XDR додає деякі нові речі

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



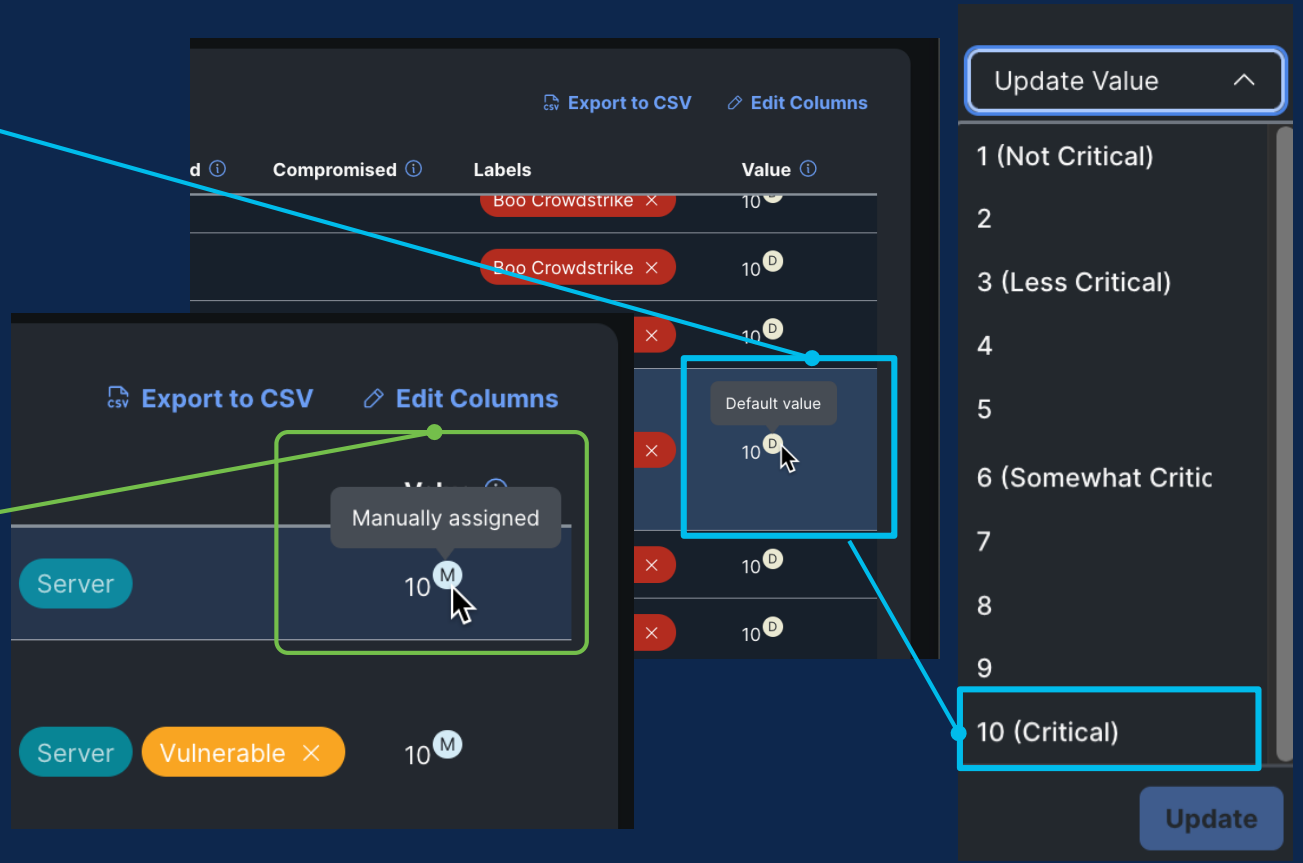
Device Insights у XDR додає деякі нові речі

Масове оновлення

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

Створення в режимі реального часу

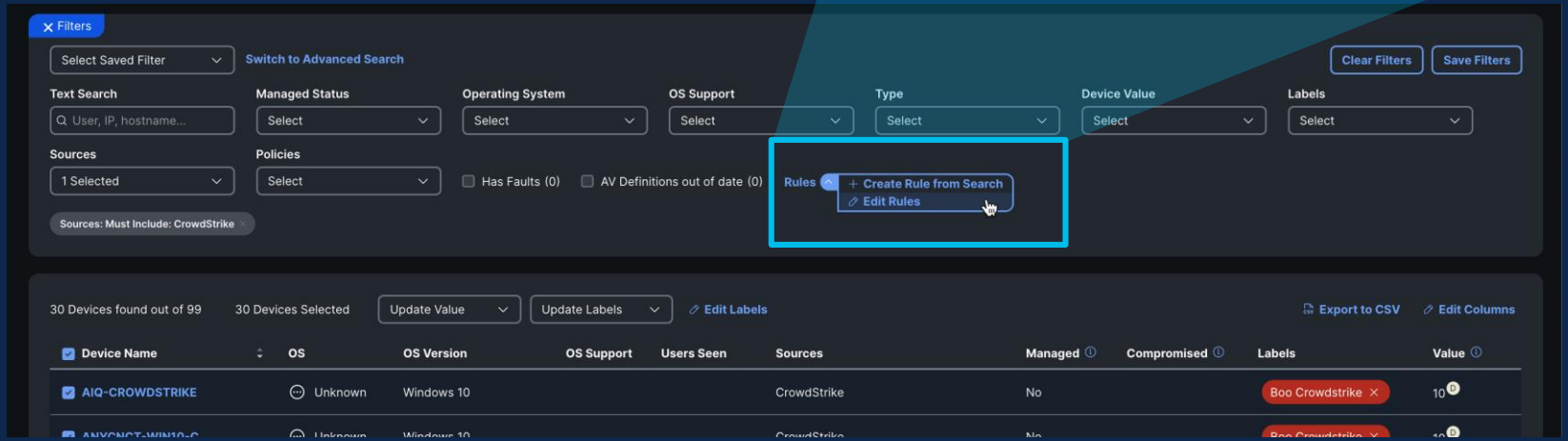
Може навіть створювати та застосовувати нові мітки в рядку



Device Insights у XDR додає деякі нові речі

Правила роботи

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



Device Insights у XDR додає деякі нові речі

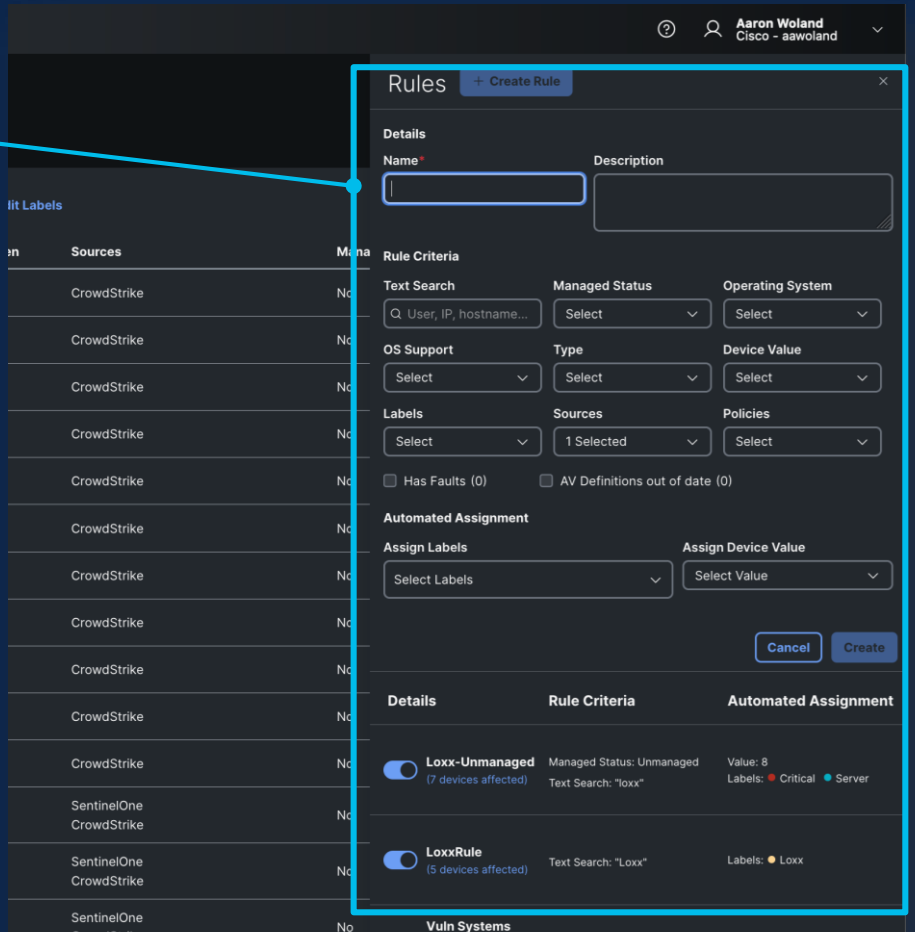
Rules Engine

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

Може вмикати / вимикати правила

Може змінити або видалити їх

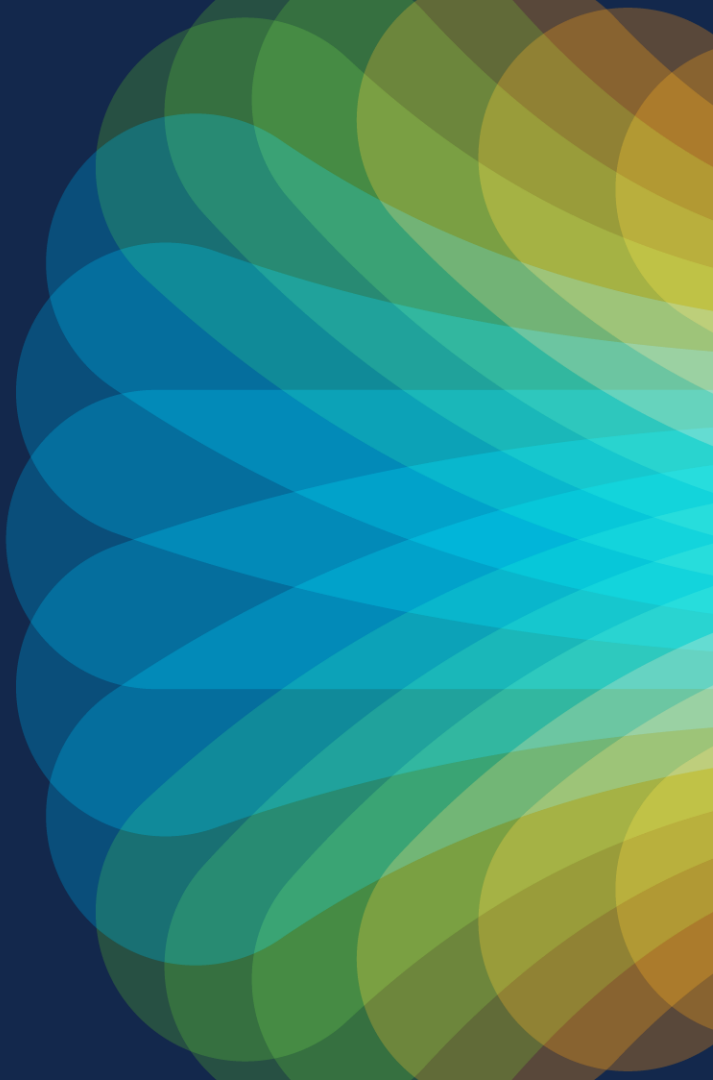
Можна скористатися наявними пошуковими запитами або створити новий пошук у редакторі правил.



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

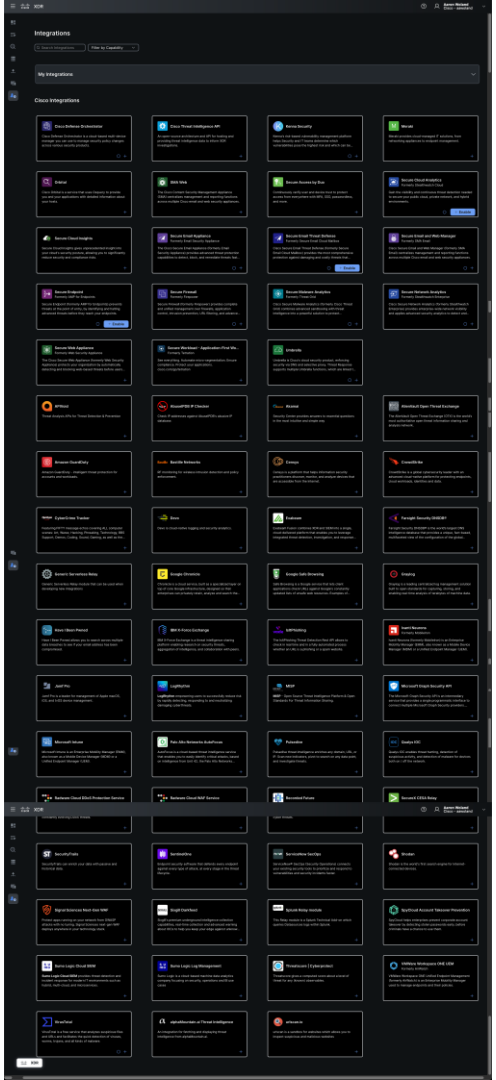
Email Threat Defense (ETD)

Umbrella

Також 3-тя сторона

- EDR:
  - Crowstrike
  - Sentinel One
  - MSFT Defender
- NDR:
  - Dark Trace
  - ExtraHop

… Та інші джерела інформації



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

-Tom Gillis, SVP & GM – Cisco Secure

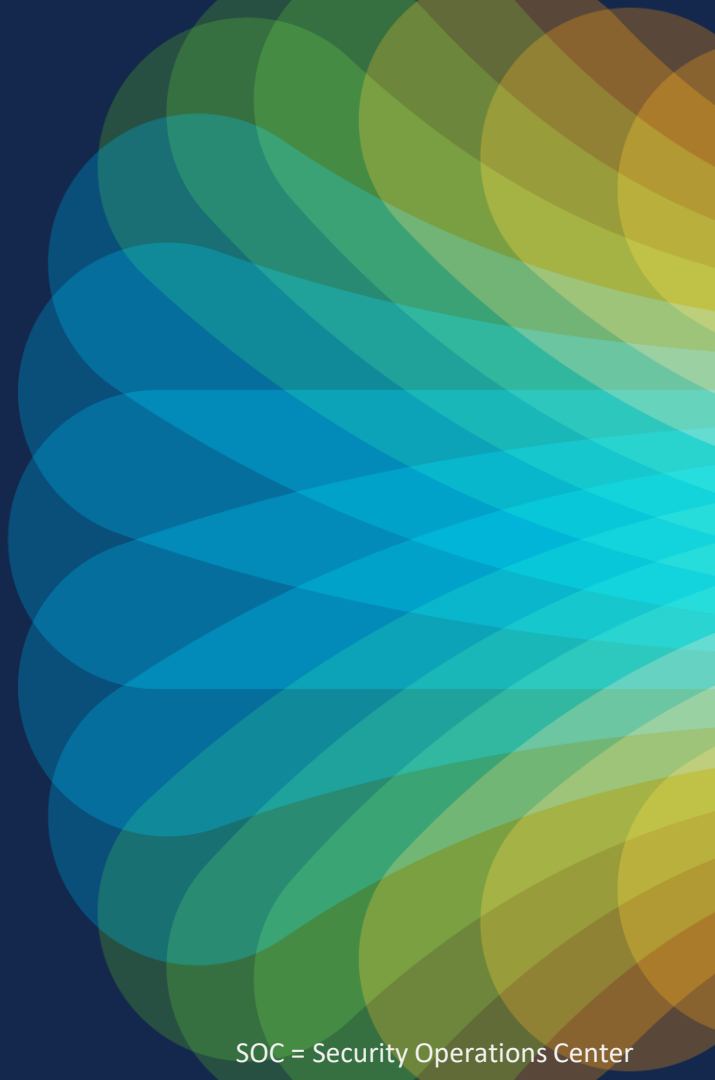
~250 мільйонів endpoints надають найбільший набір сервісів безпеки для більш ніж

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?



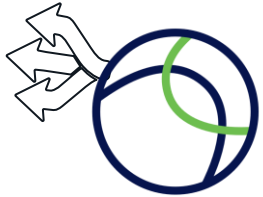
cisco Live!

SOC = Security Operations Center

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

- SANS Instructor
SEC530: Defensible Network Architectures

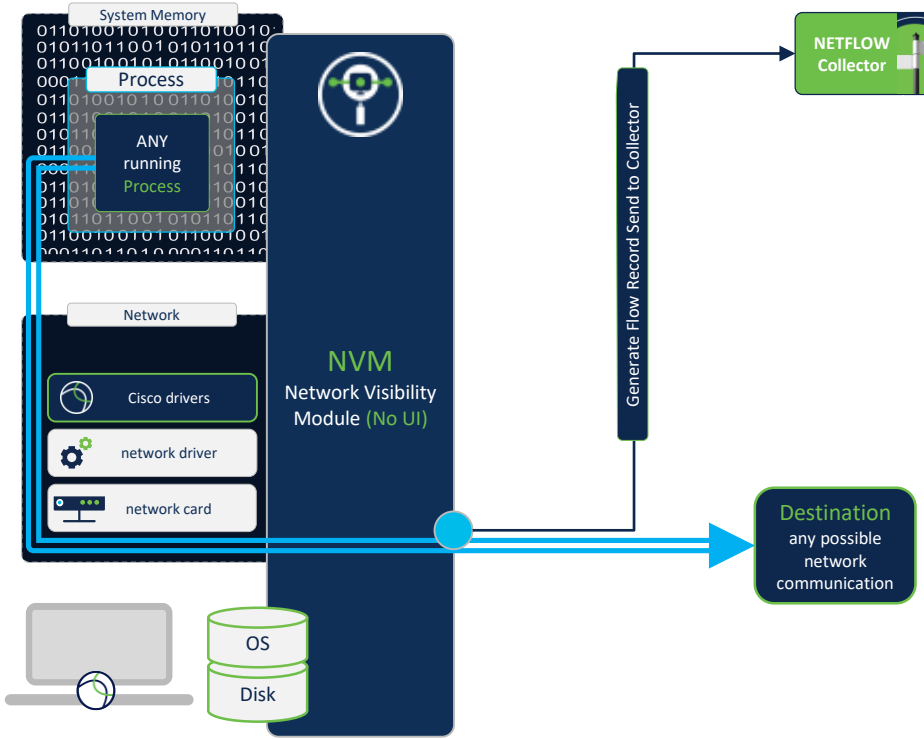
Network Visibility Module (NVM)

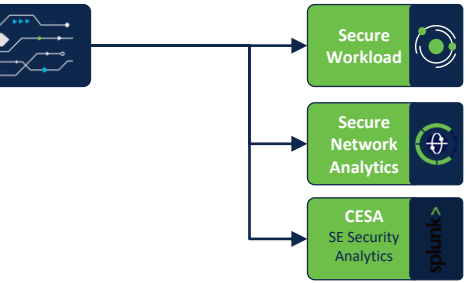


- Створює запис потоку кожного мережевого підключення з endpoint
  - User, Process, Machine Info, etc.
  - Працює On та Off Prem
  - Надсилає дані в IPFIX (NetFlow) на основі "nvzFlow".

Conceived by Vinny Parla back in 2011
Been a product almost since then!

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)
- Потокові 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

NVM (IPFIX Formatted)

- Source IP
- Destination IP
- Source Port
- Destination Port
- Bytes Sent
- Bytes Received
- **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**

Справжня атрибуція пристрою,
Не просто "IP-адреса"

Глибока видимість endpoint

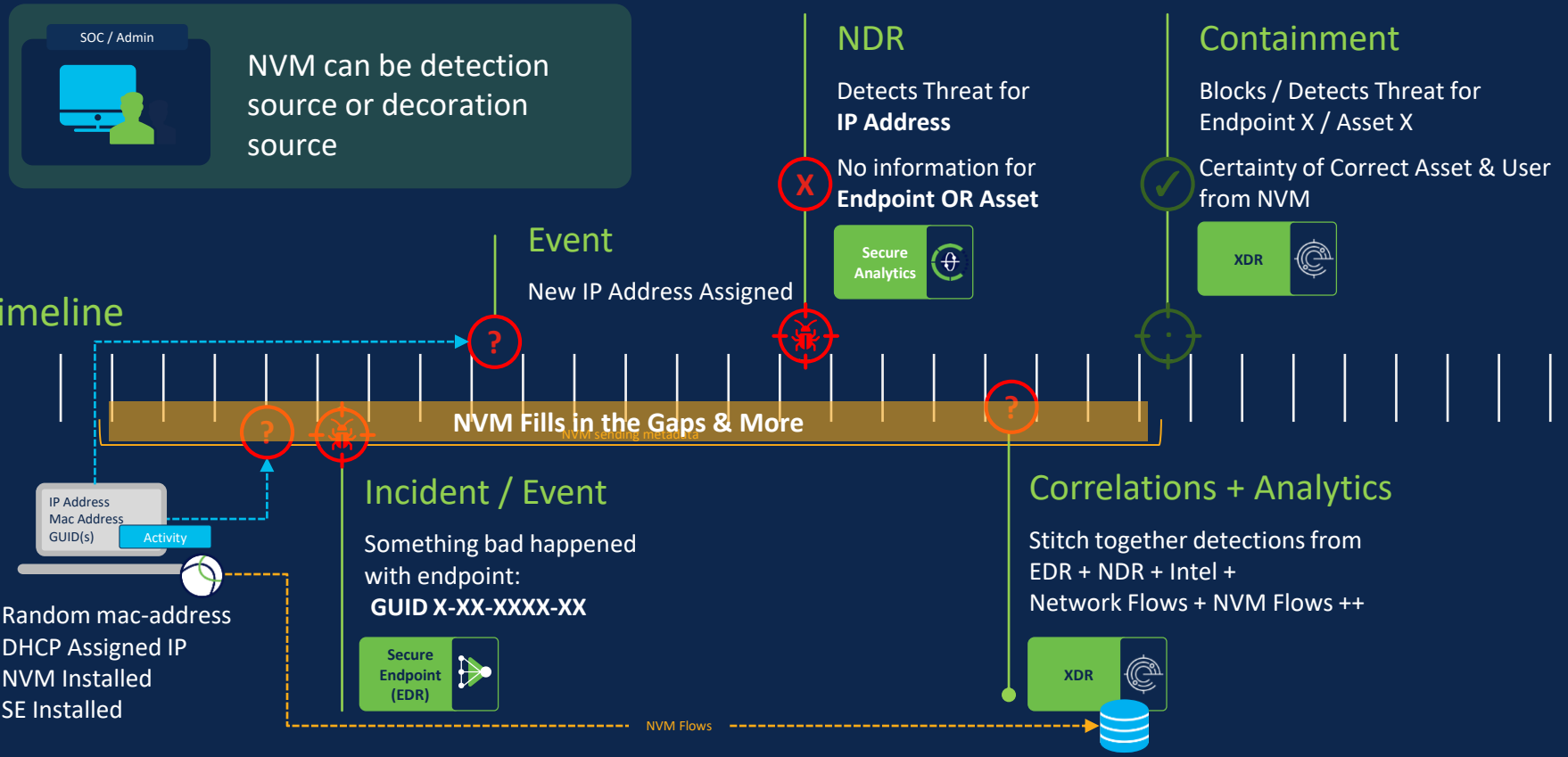
User
Traffic Stats
Processes
Applications
SaaS Used
Accounts
Destinations
Machine Details

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

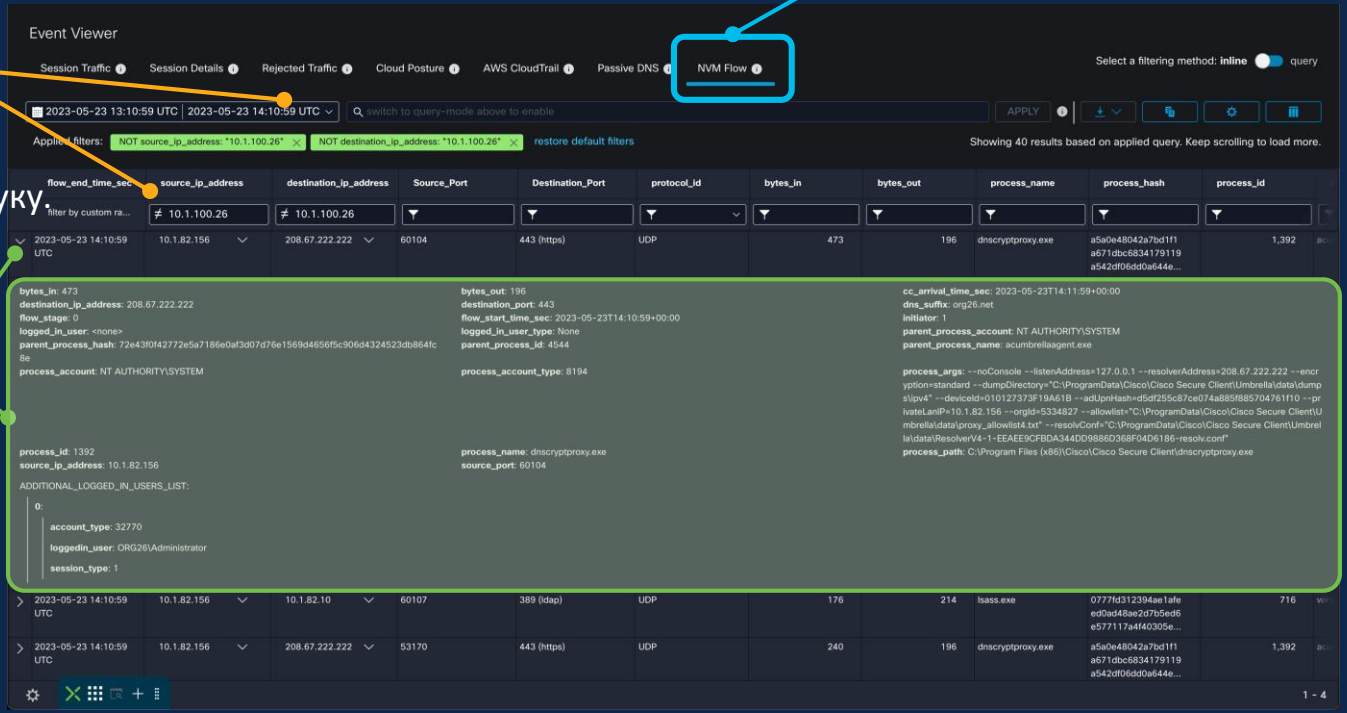
New NVM Flows Tab

МИТТЄВІ ФІЛЬТРИ

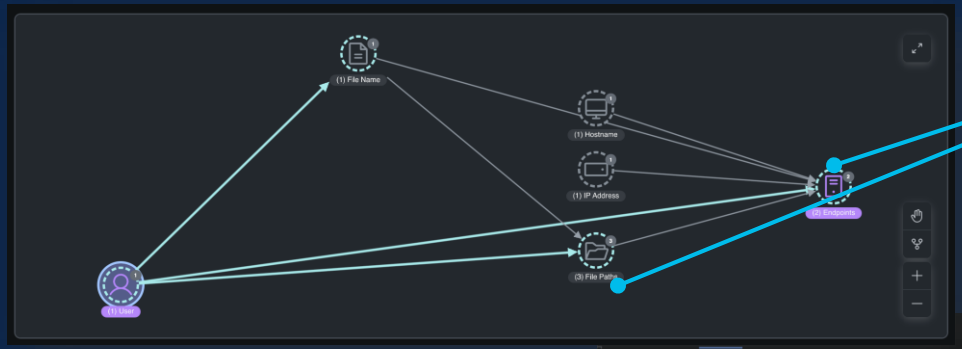
Пошукова активність за атрибутом або багато за допомогою розширеного пошуку.

Подробиці телеметрії

Перегляньте детальну телеметрію, зібрану з потоку



NVM забезпечує виявлення та показ

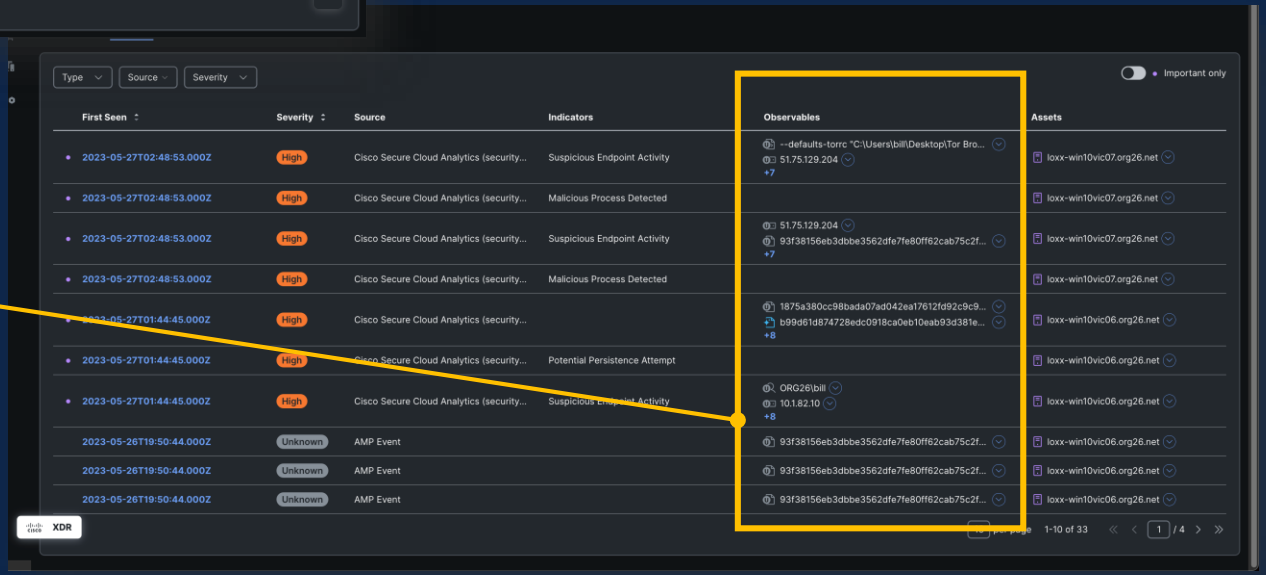


Відображає бічний рух

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

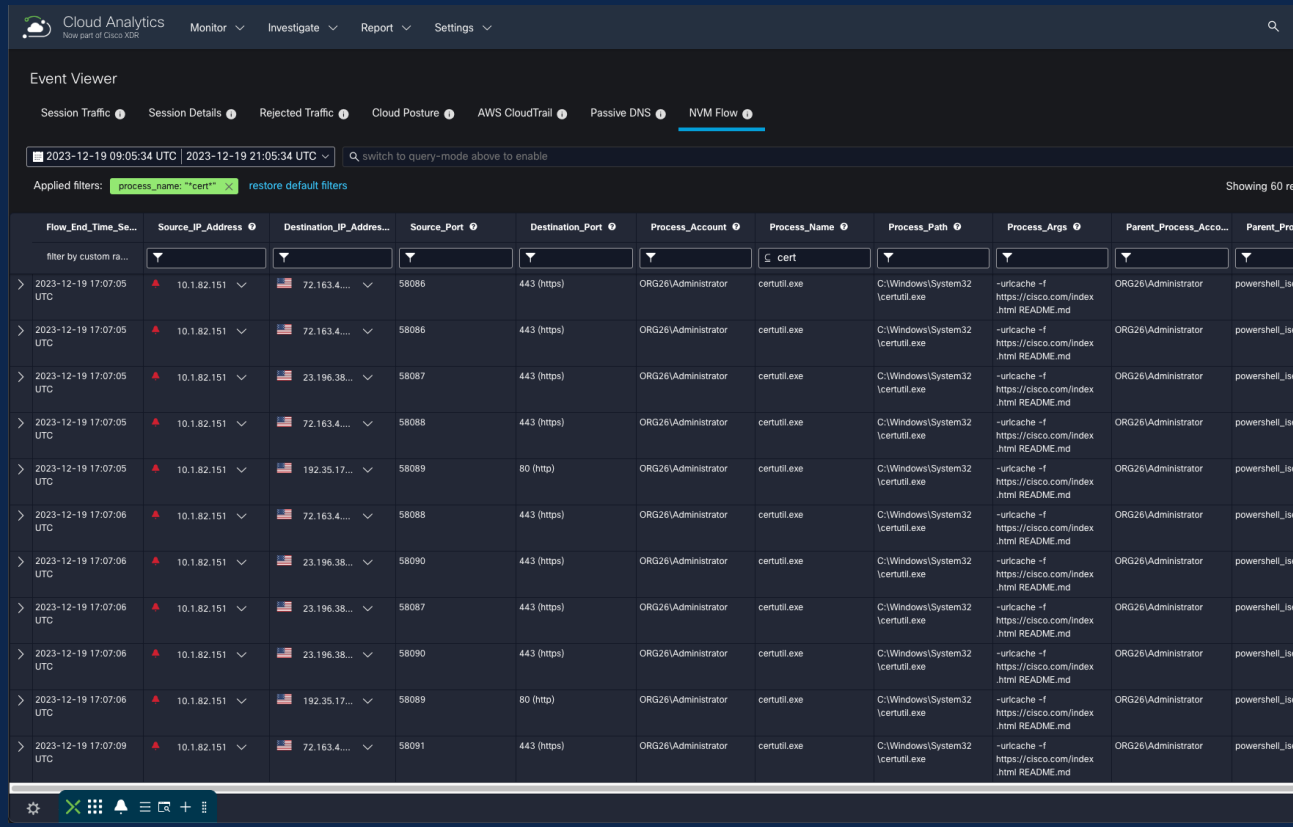
Безпосереднє джерело спостережуваних об'єктів

Для нових виявлених об'єктів у XDR Analytics



NVM у порівнянні з SYSMON та журналами мережевих подій

- 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)

Assets > Users

“inventory”користувачів це підмножина категорії “Assets”

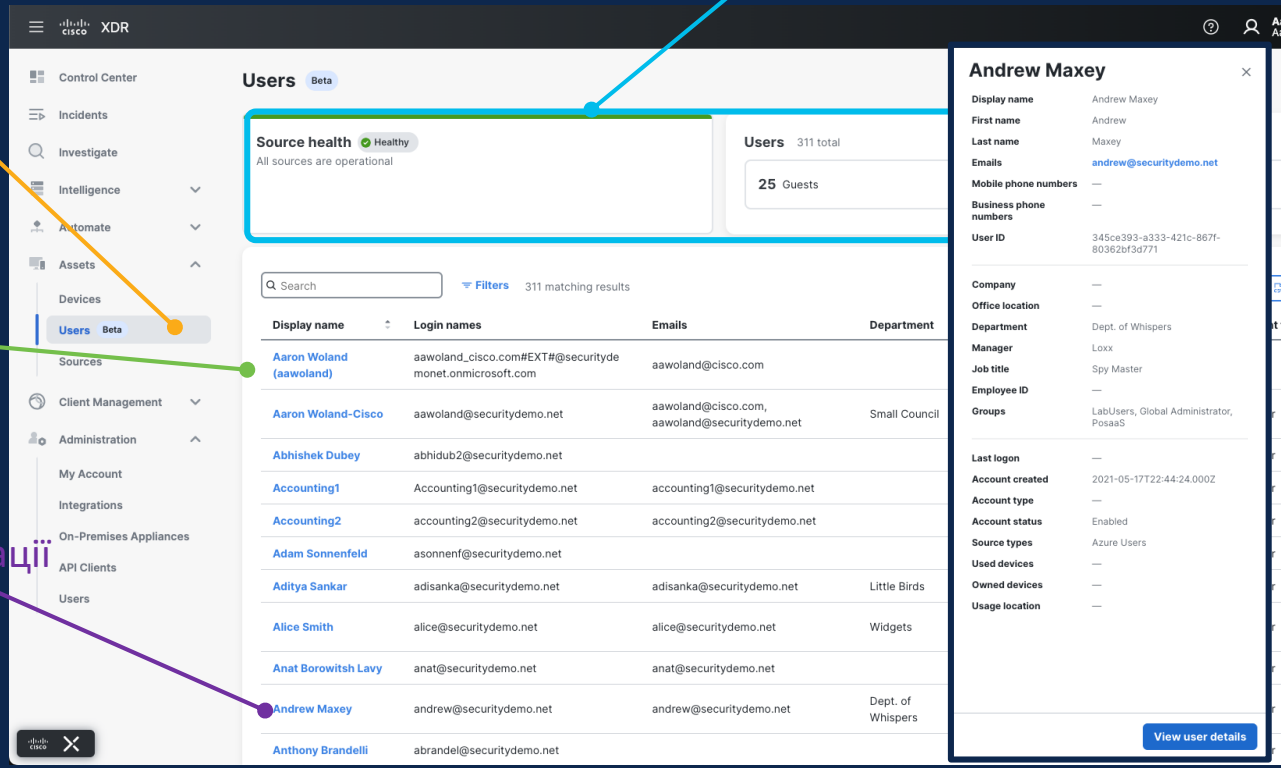
Об'єднаний інвентар

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.

Ключові показники, що відображаються



Сторінка відомостей про користувача

Найпопулярніші пристрої, що використовуються / належать

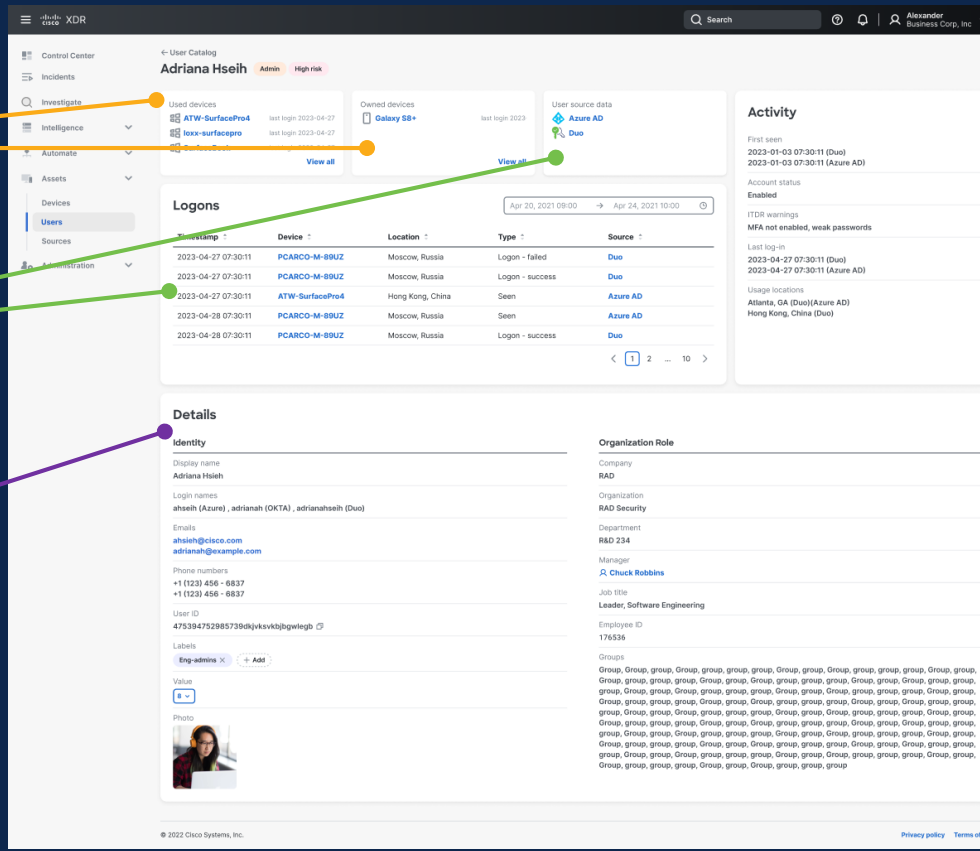
Натисніть «Переглянути всі», щоб переглянути список усіх пристроїв

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



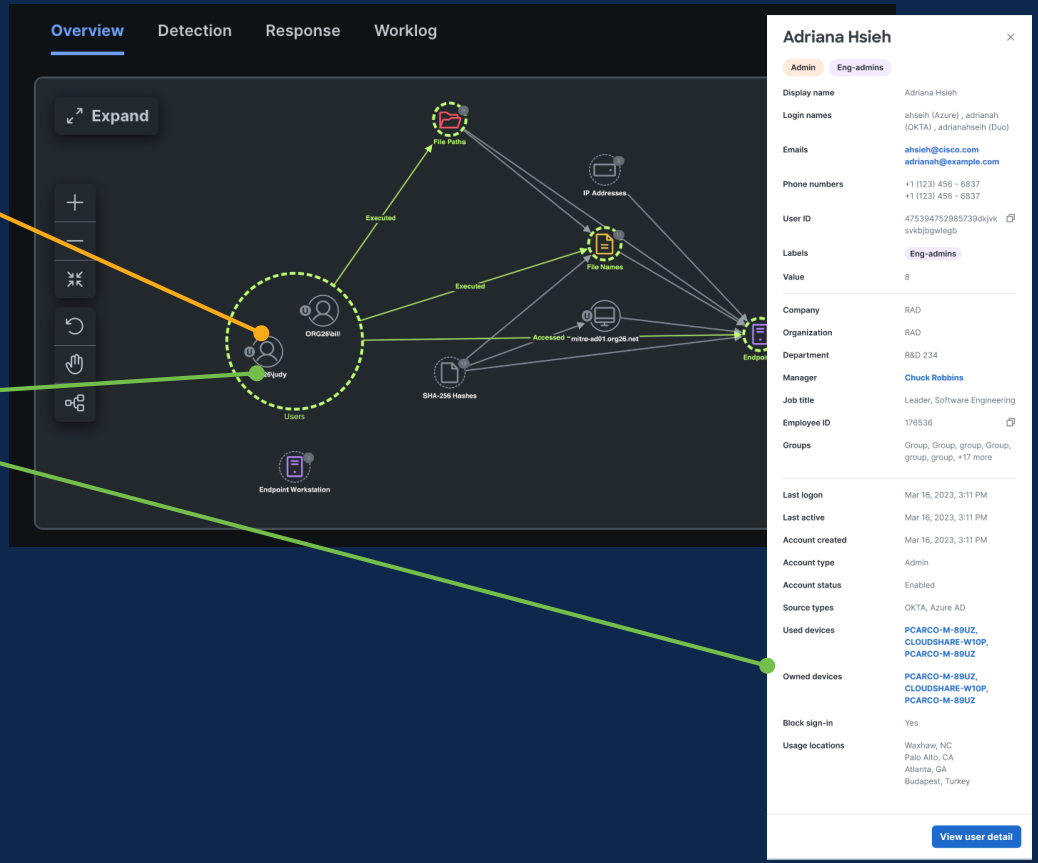
Контекст користувача в розслідуванні / управлінні інцидентами

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»



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

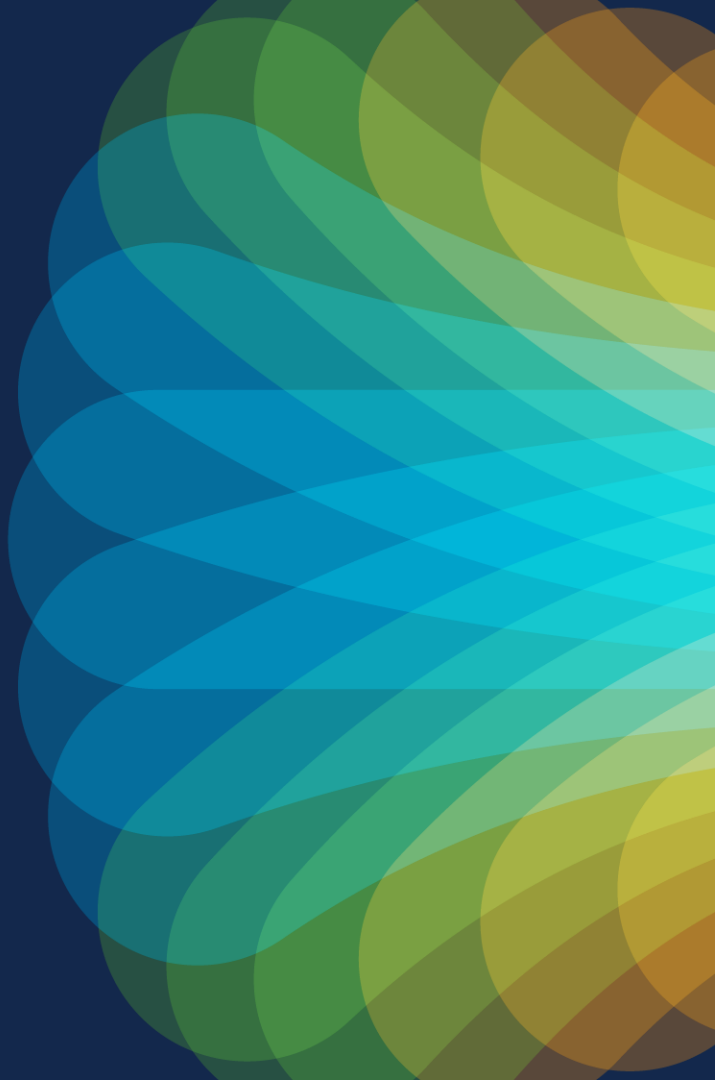
Cisco Identity Intelligence

Чому OORT?

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

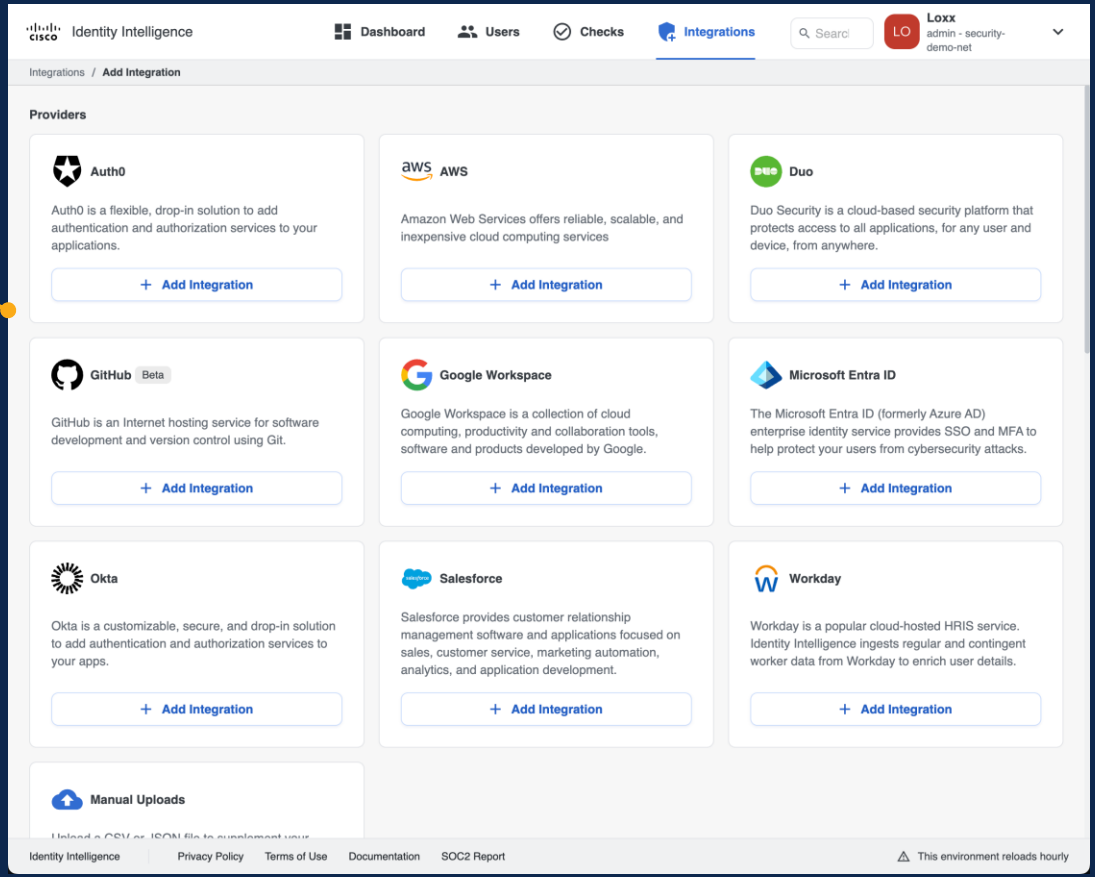
- Лідер на ринку ITDR
- Великий інфлюенсер / радник з Identity Security з провідними аналітиками
- Data Scientists / Команда інженерів з лідерами в галузі безпеки ідентифікаційних даних

Примітка: ці екрани з оригінального інтерфейсу Oort UI



Інтеграція!!

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

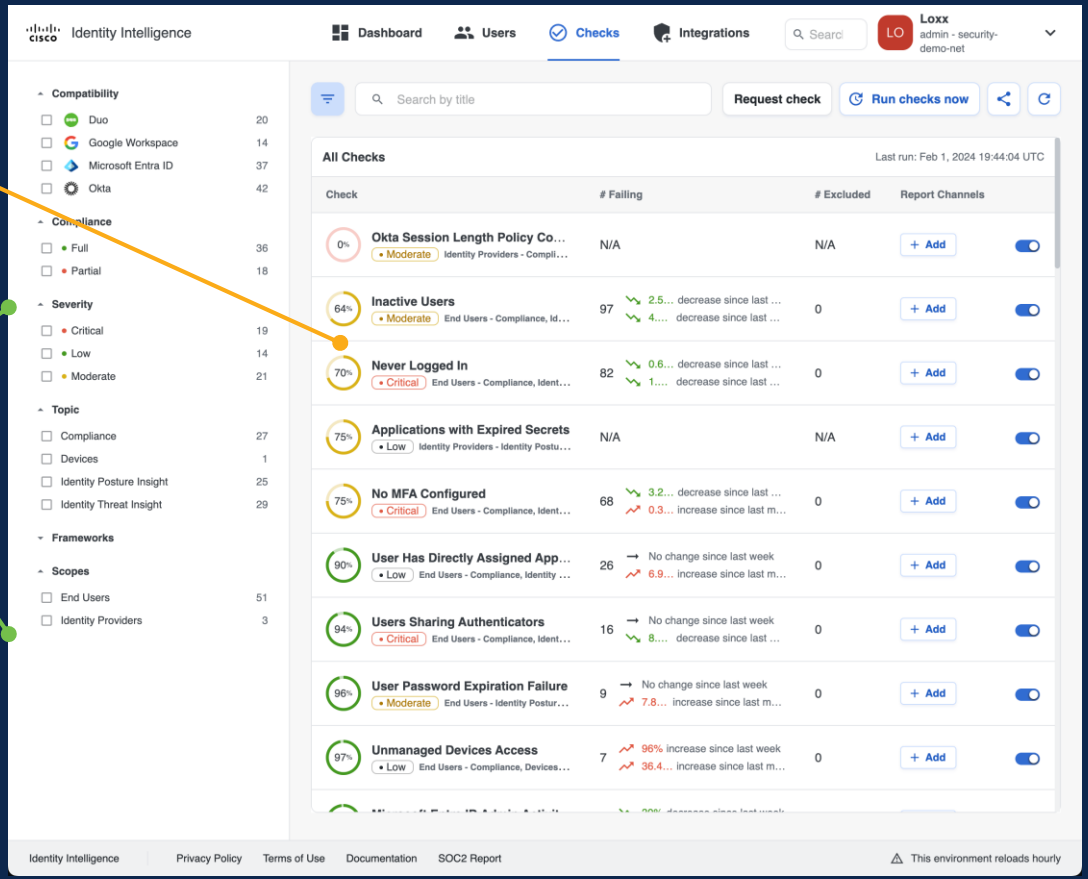


Перевіряє

АКА: сигнатури для виявлень

Піддається фільтруванню

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

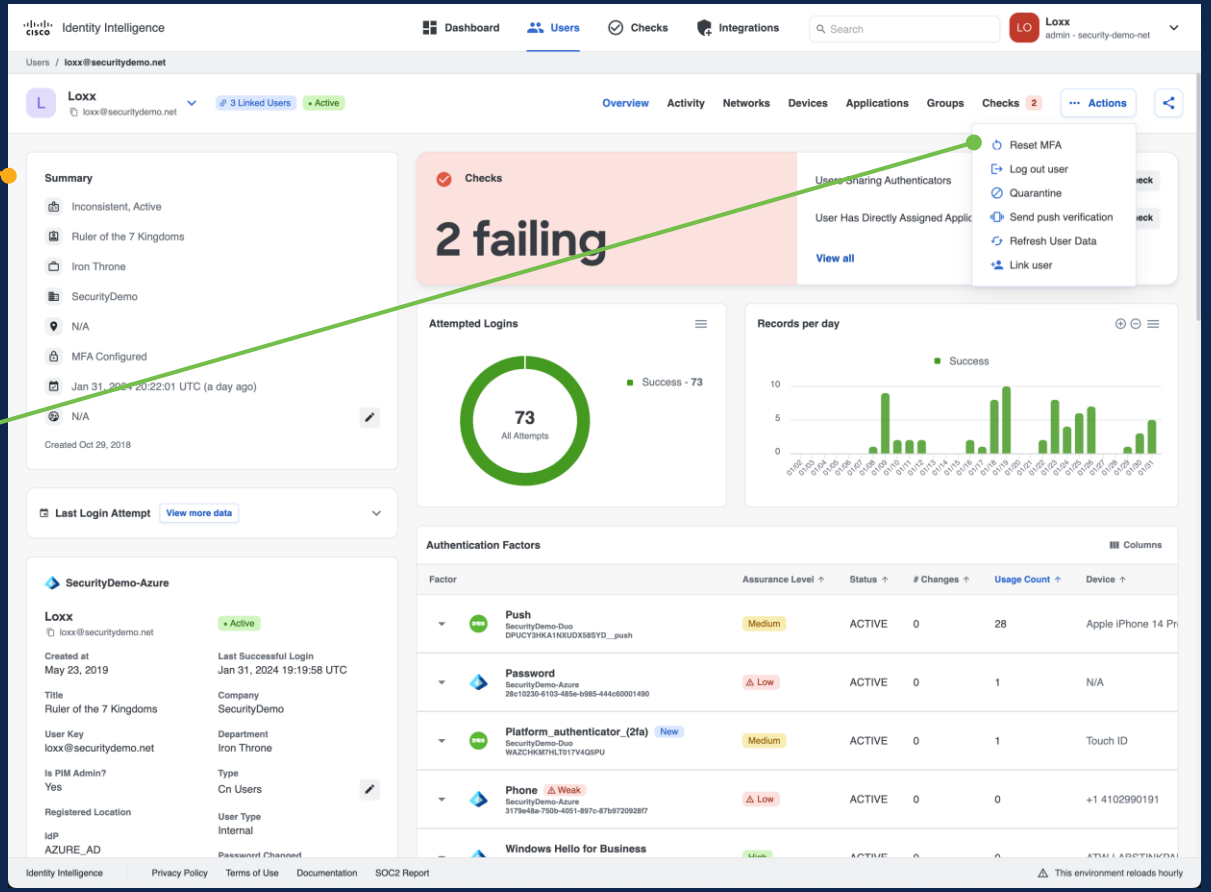


Інформація про користувача

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

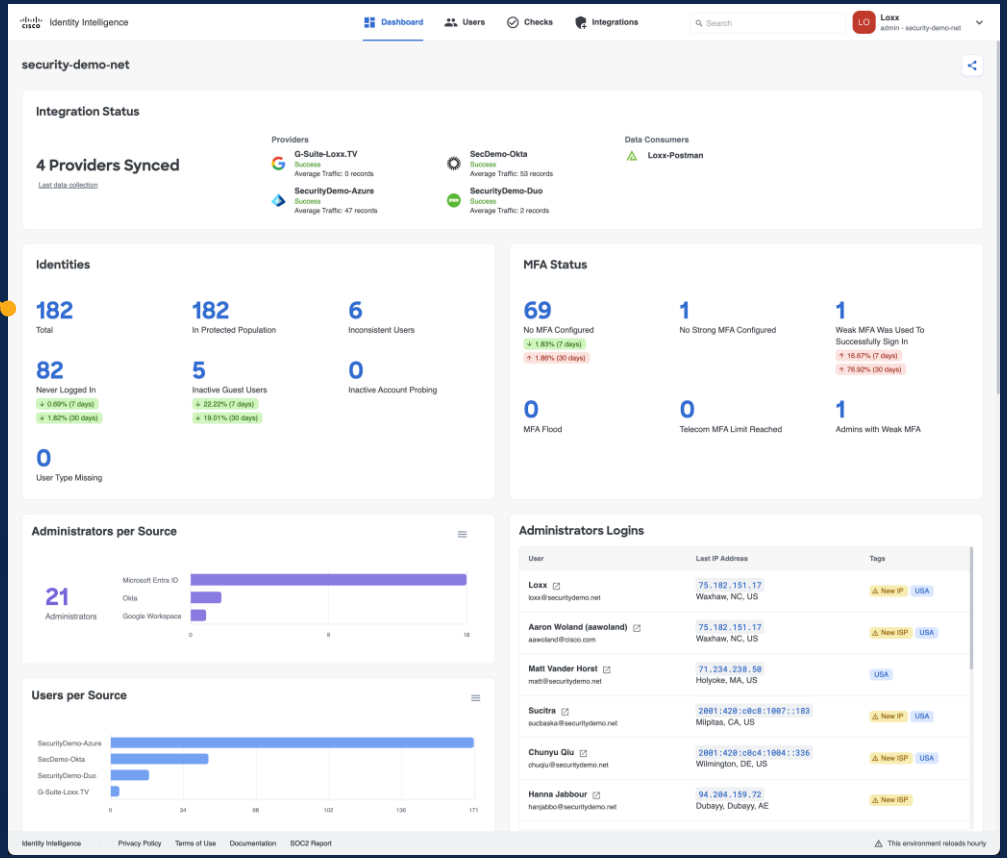
Відповідь

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



Розуміння

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



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 багатофакторна 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


cisco
The bridge to possible
Thank you
cisco Live!