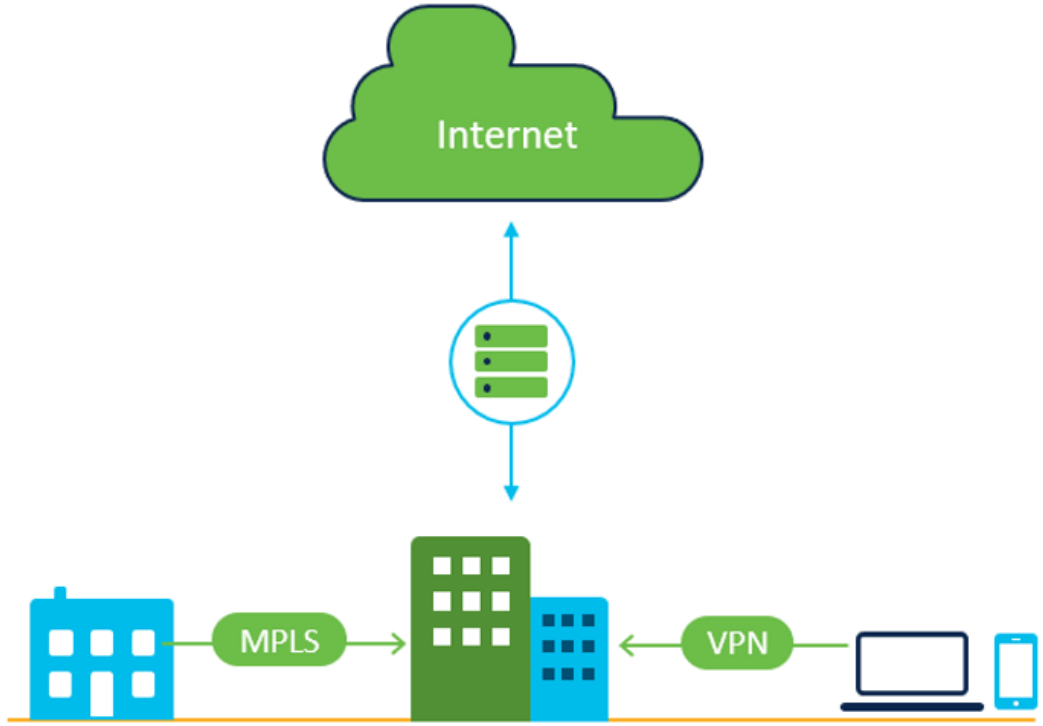
Cisco XDR

- технологічна досконаліть та фінансова ефективність

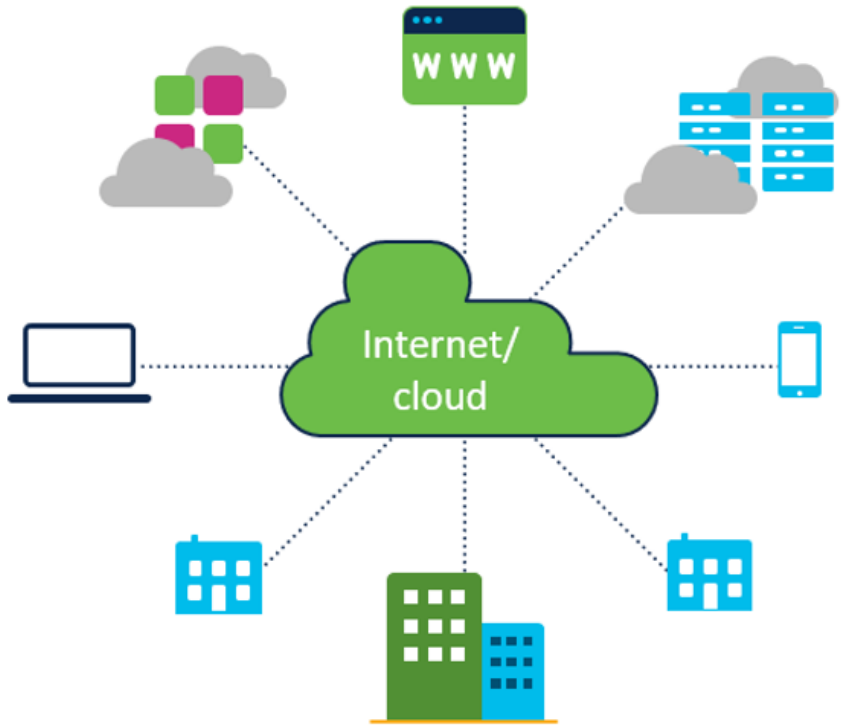
IT.Integrator | cisco Partner

Передумови XDR: Network & Security transformation

Centralized



Decentralized



Poor Application Performance
Poor User Experience
Complex

Expensive
No scalability
Insecure

Simple, Agile,
Flexible Performance
Exceptional User Experience
State of the Art Cyber Security
Reduced Total Cost of Ownership (TCO)

IT.Integrator | cisco Partner

Периметр організації тепер виглядає інакше, ніж раніше

> *The enterprise perimeter is no longer a location; it is a set of dynamic **edge** capabilities delivered when needed as a **service** from the cloud.*

Gartner: The Future of Network **Security** is in the Cloud,
Neil MacDonald, Lawrence Orans, Joe Skorupa, 2019

IT.Integrator | cisco Partner

Cisco Security Reference Architecture

IT.Integrator | cisco Partner

Enter XDR

Gartner defines Extended Detection and Response (XDR) as a unified incident detection and response platform that automatically collects and correlates data from multiple proprietary security components.

First, it must centralize collections of historic and real-time event data in common formats and make it available for fast indexed searches.

Second, it must use multiple machine learning techniques to analyze huge amounts of telemetry data from multiple products to detect subtle malicious activity.

Lastly, it must offer automation capabilities to take care of routine tasks that accelerate response — or even proactively improve protection and posture.

IT.Integrator | cisco Partner

Don’t Trust Everything Labeled XDR

- The concept of XDR **sounds simple**, but it is **difficult to execute** in practice
- **Unifying data sets** in meaningful ways is the central **challenge** of building an effective XDR platform
- **Security solutions** are often built **standalone** and generally **lack APIs**, compatible **database** structures, and data **normalization**
- **EDR or NDR** form partnerships to make XDR claims, but due to the **loose**, non-native **integrations**, they can’t deliver on the promise of XDR

A Cisco's Interpretation of XDR

We believe a robust XDR solution should:

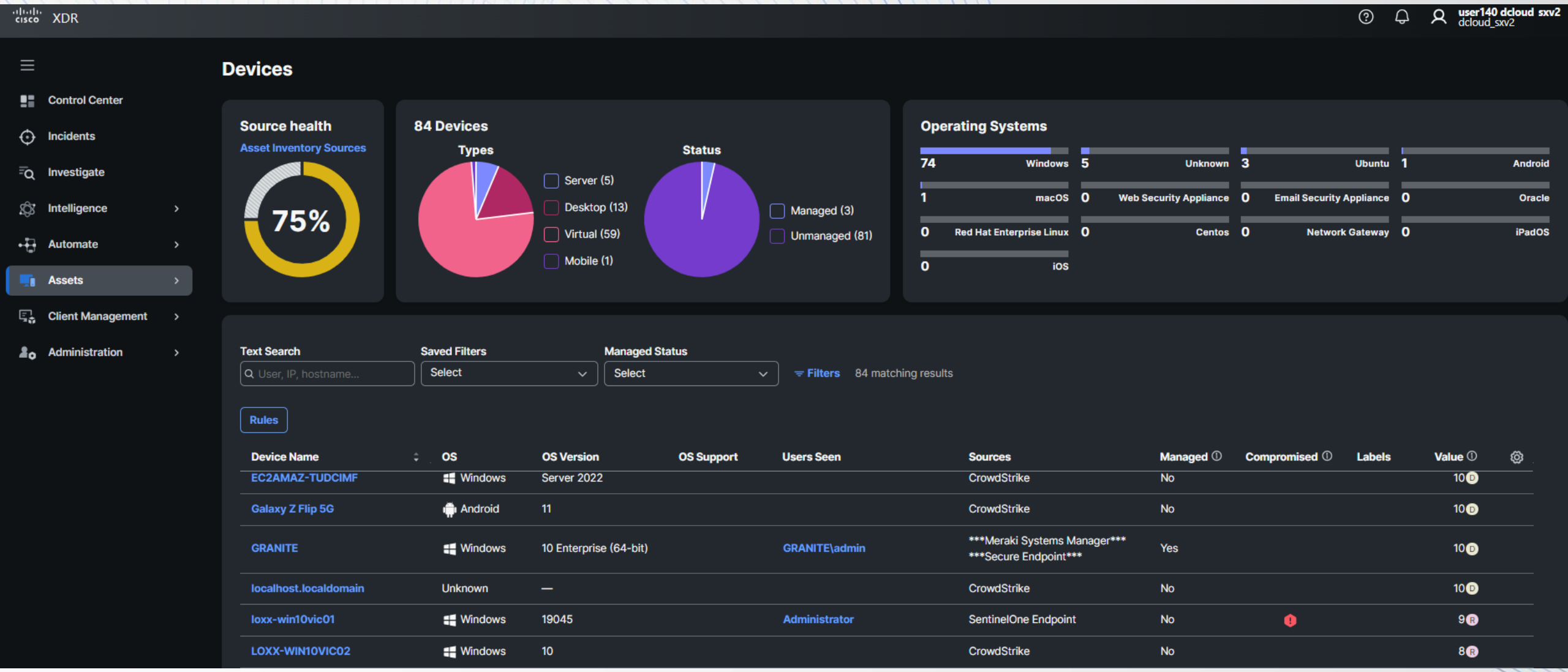
- Bring together **many different** control points and data sources – "**X**"
- Make detection smarter and faster with **machine learning**-enhanced analytics – "**D**"
- Reduce dwell times through easier **investigations**, faster **responses**, and more **automation** - "**R**"

A Cisco’s Interpretation of XDR

X + D R

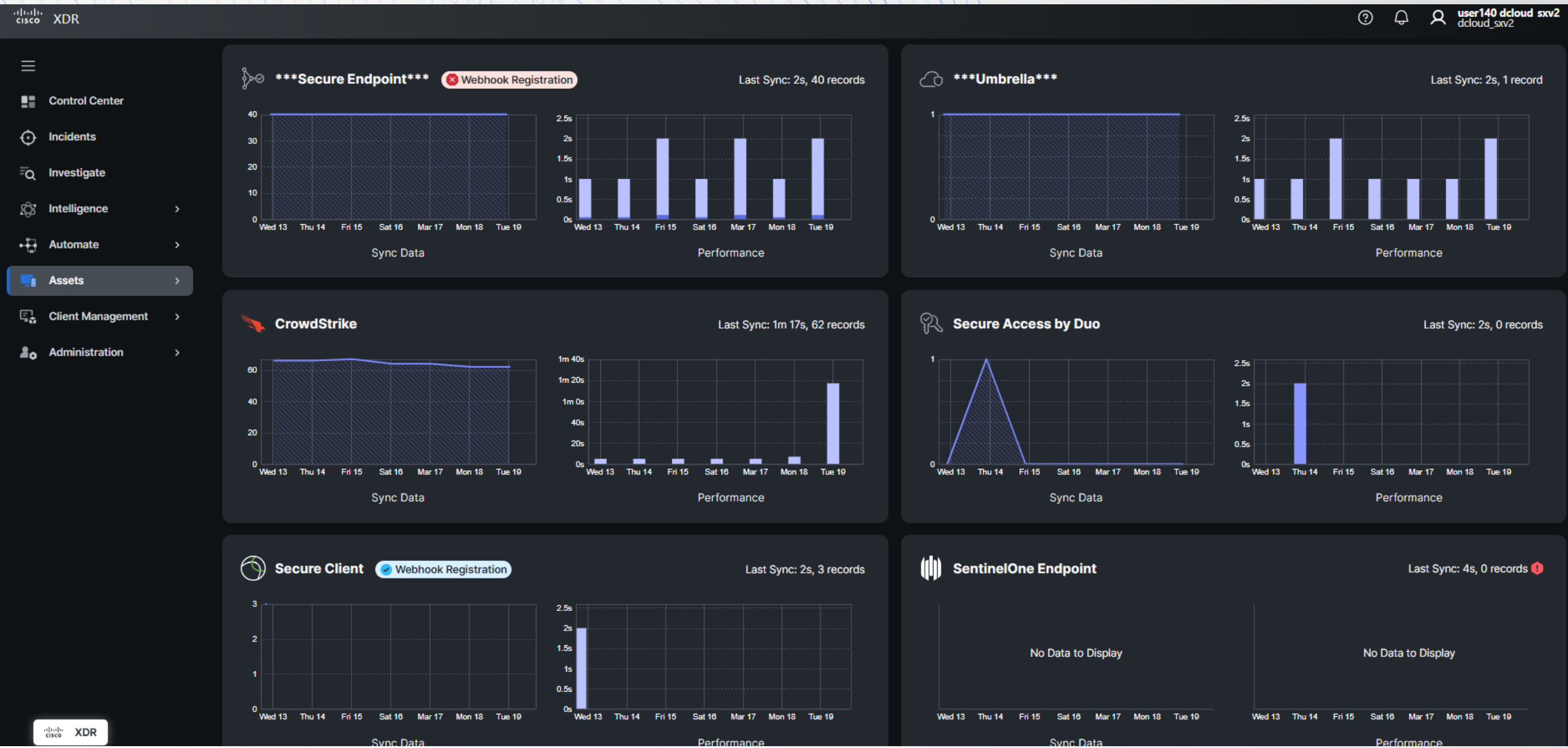
IT.Integrator | cisco Partner

Cisco XDR. Активи: Пристрої



IT.Integrator | cisco Partner

Cisco XDR. Активи: Джерела

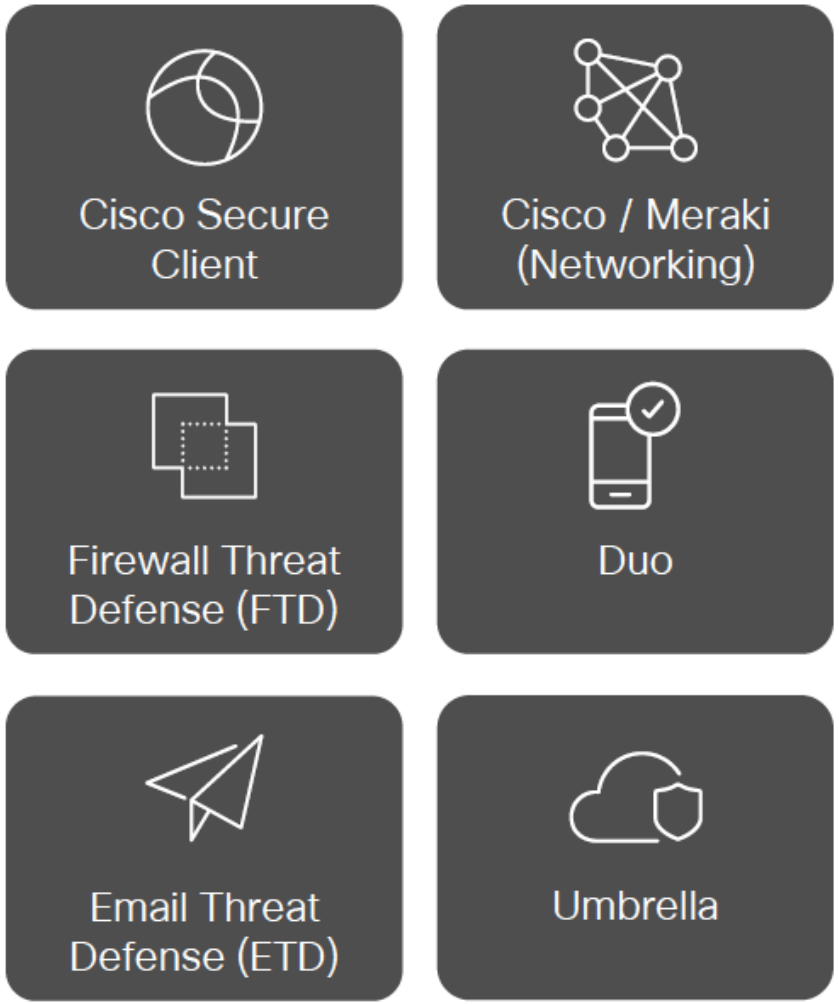


IT.Integrator | cisco Partner

Ефективний XDR: **Джерела телеметрії**

The top six data sources that customers believe are essential for an XDR are 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%

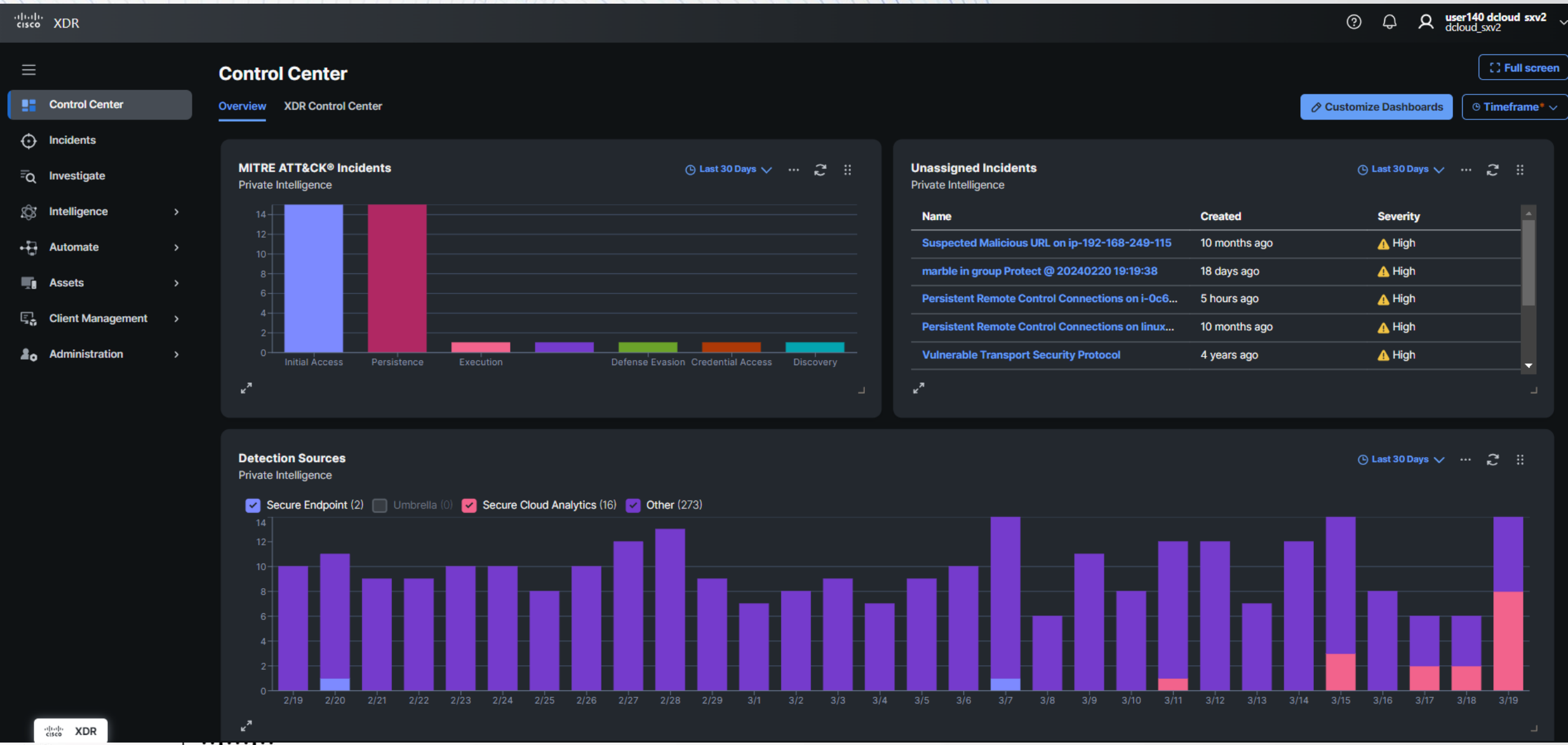


A Cisco’s Interpretation of XDR

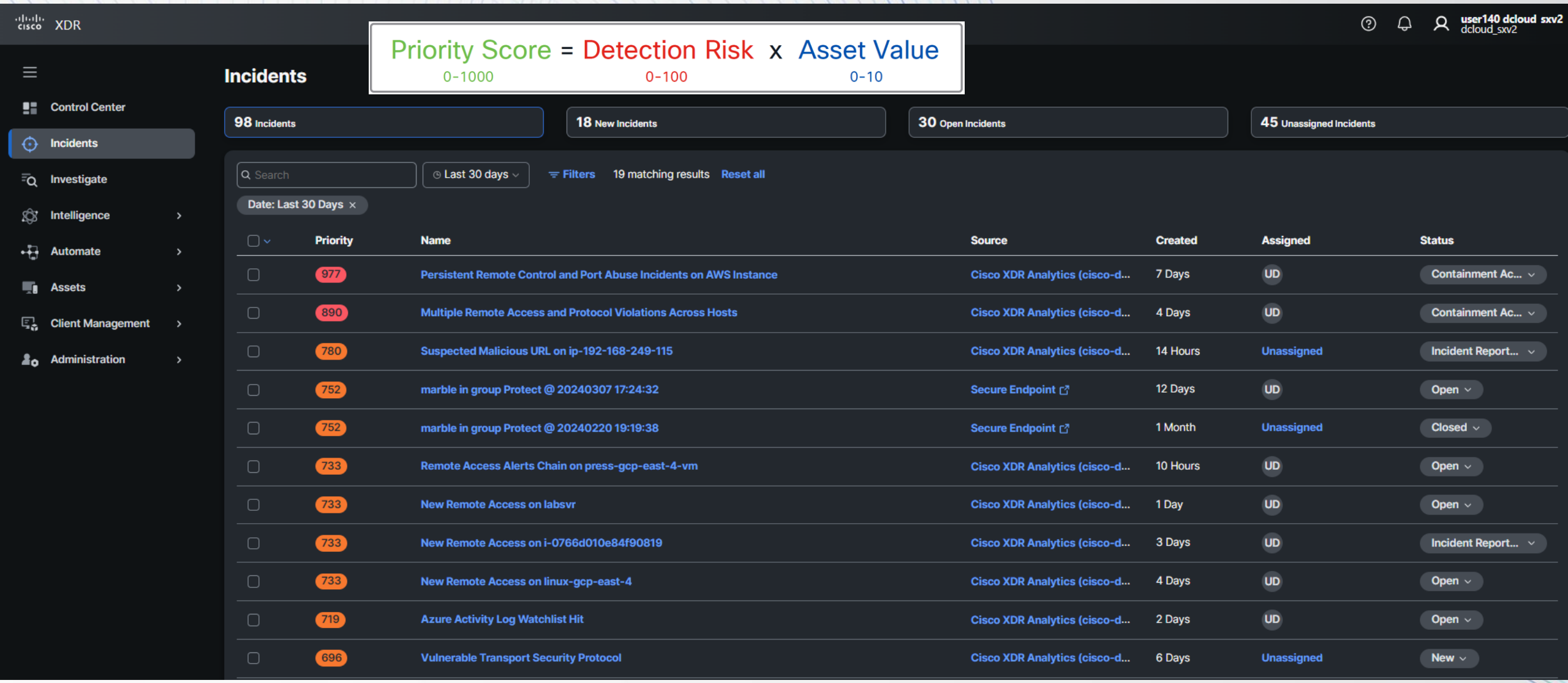
XDR

IT.Integrator | cisco Partner

Cisco XDR. Центр керування

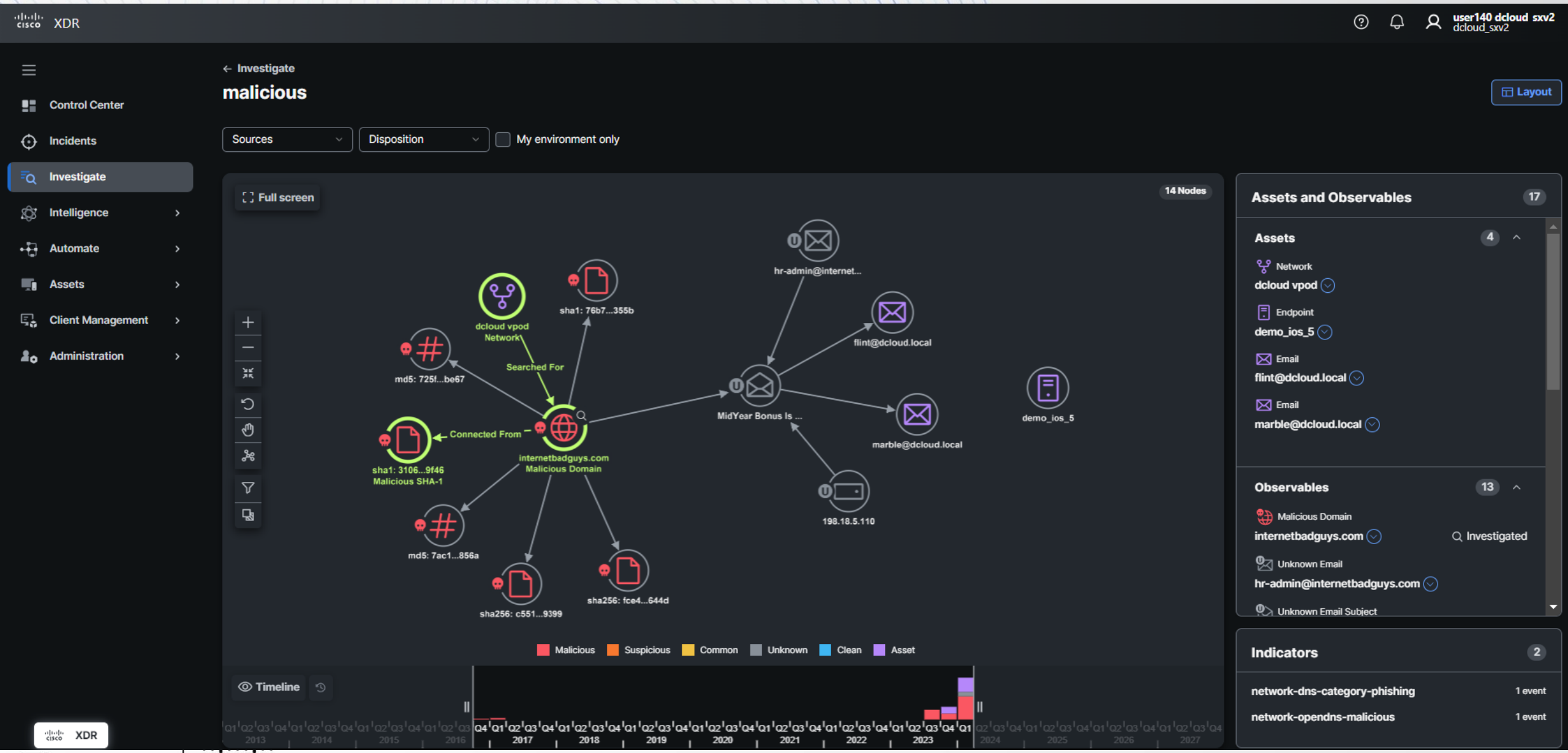


Cisco XDR. Пріоритезація інцидентів

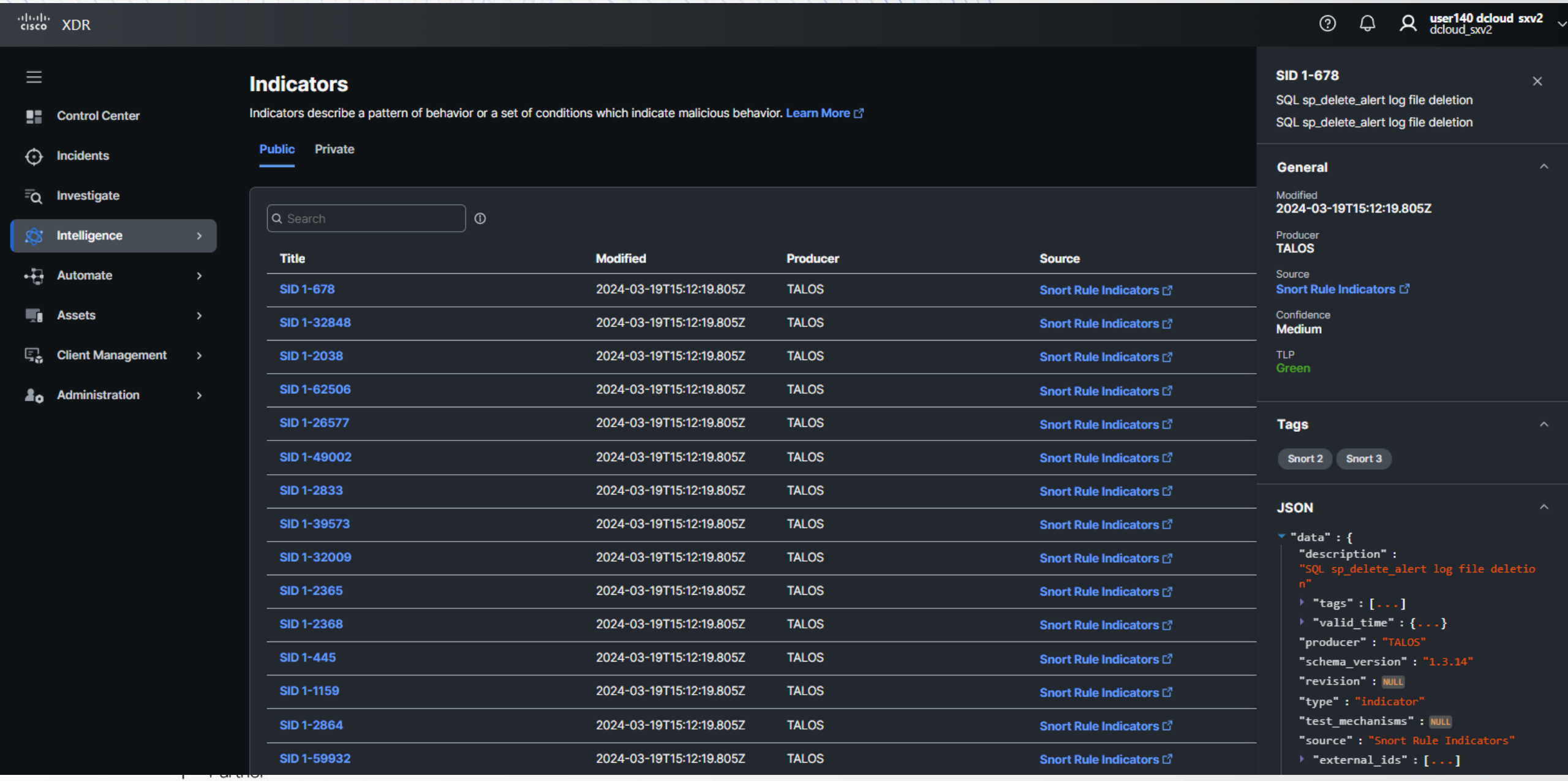


IT.Integrator | cisco Partner

Cisco XDR. Розслідування



Cisco XDR. Розвідка

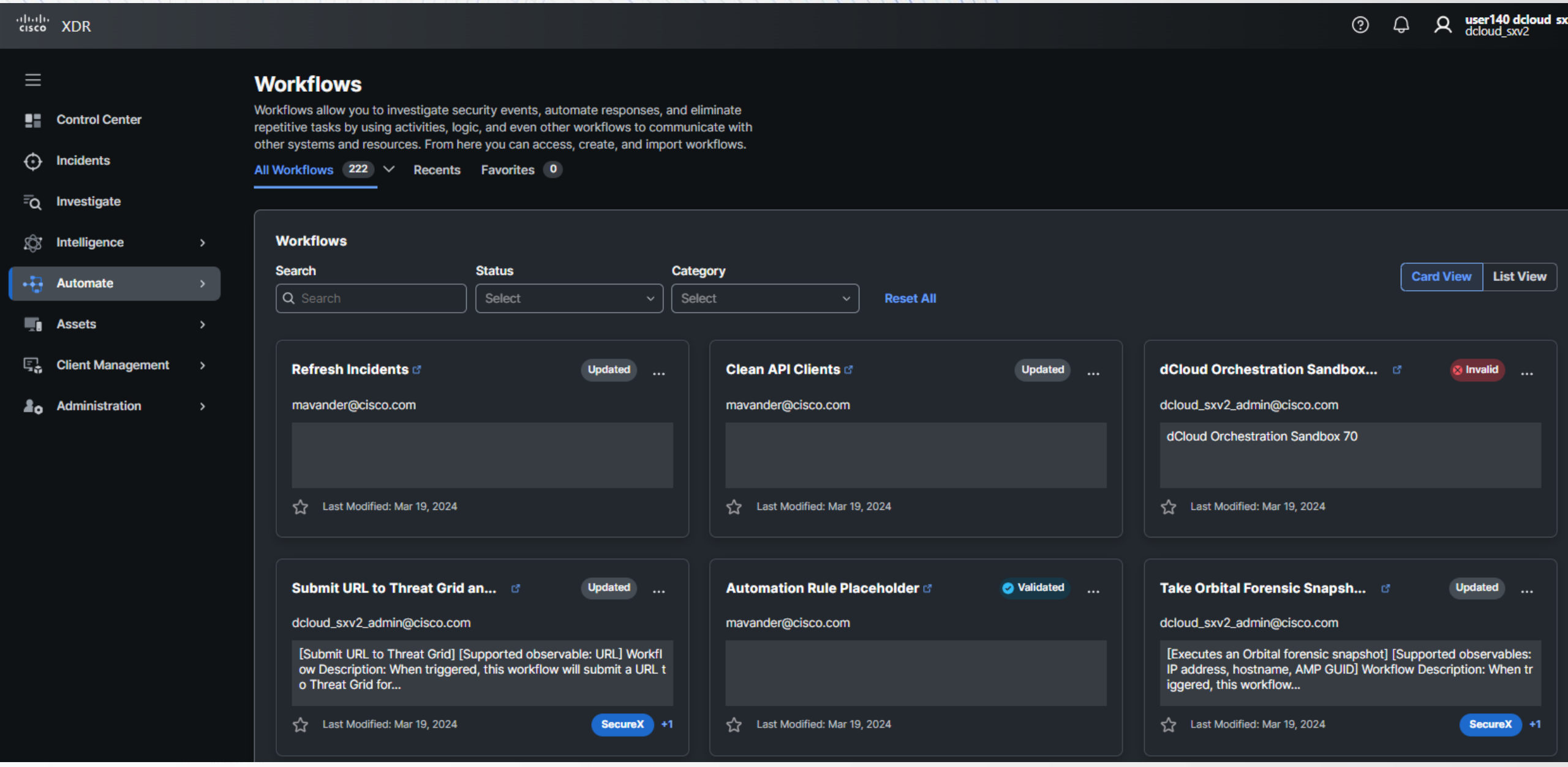


A Cisco’s Interpretation of XDR

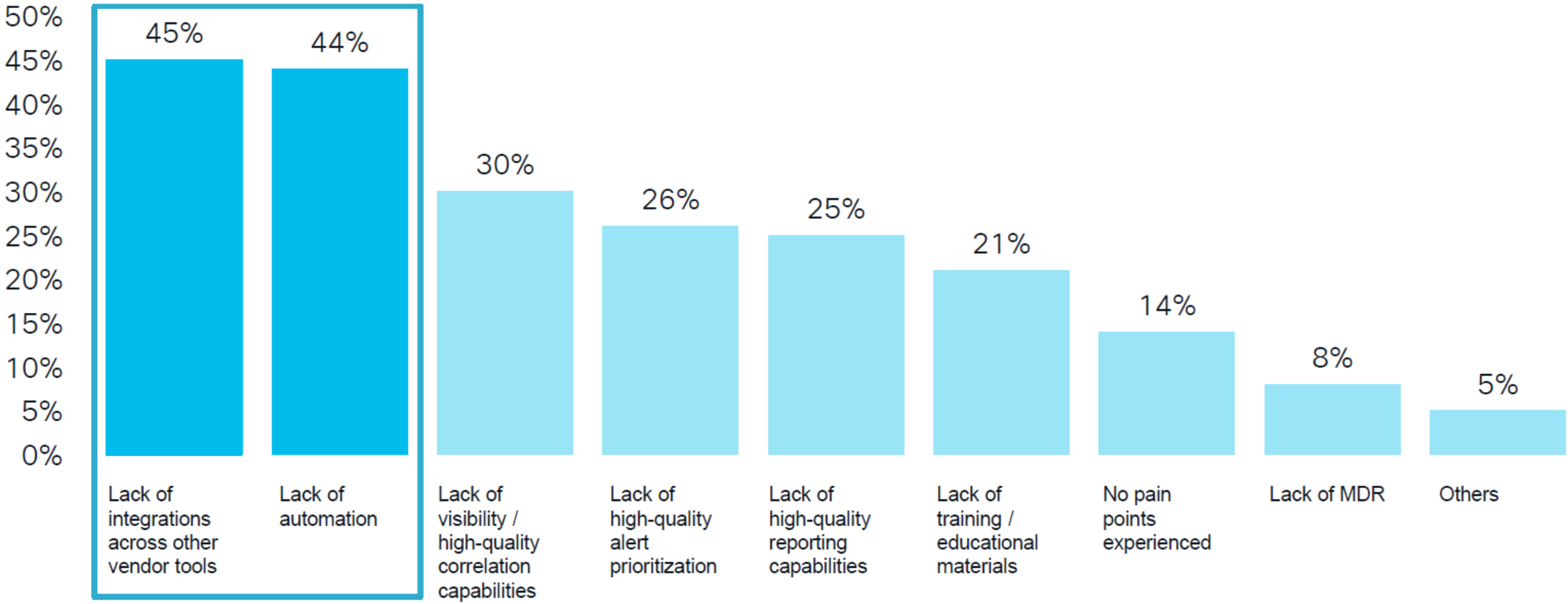
XDR

IT.Integrator | cisco Partner

Cisco XDR. Автоматизація та оркестрація



Ефективний XDR: **Функціонал**



IT.Integrator | cisco Partner

Our XDR solution focuses on the important tasks

Simplicity

Integrate technology together with true turnkey interoperability

Visibility

Accelerate time to detect and investigate threats and maintain contextual awareness

Efficiency

Accelerate time to remediate and automate workflows to lower costs and strengthen security

IT.Integrator | cisco Partner

Easy to buy tiers for Cisco XDR

Cisco XDR Essentials

Full-featured XDR
+
Native integration of the full Cisco security portfolio
+
Talos and third-party threat intelligence enrichment

Cisco XDR Advantage

All features in Essentials
+
Integrations with extensive list of third-party tools

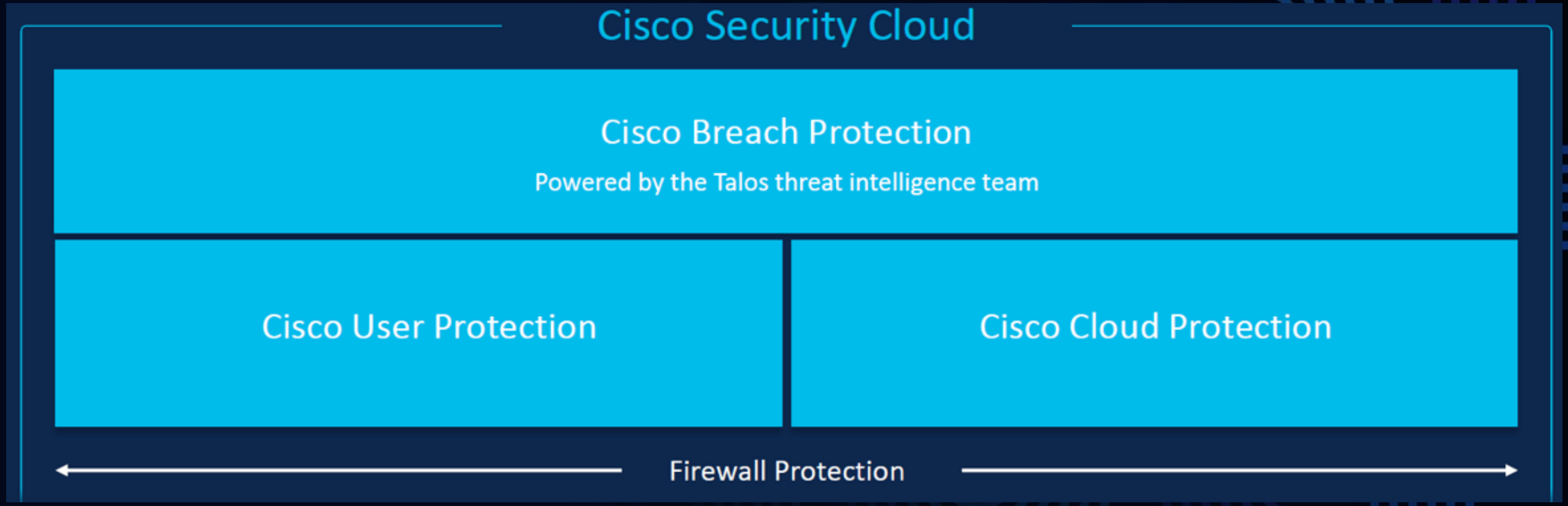
Cisco XDR Premier

All features in Advantage
+
Managed extended detection & response (MXDR) delivered by Cisco CX

Buy a la carte or as a part of the new Breach Protection Suite.

IT.Integrator | cisco Partner

Introducing security only Cisco can deliver



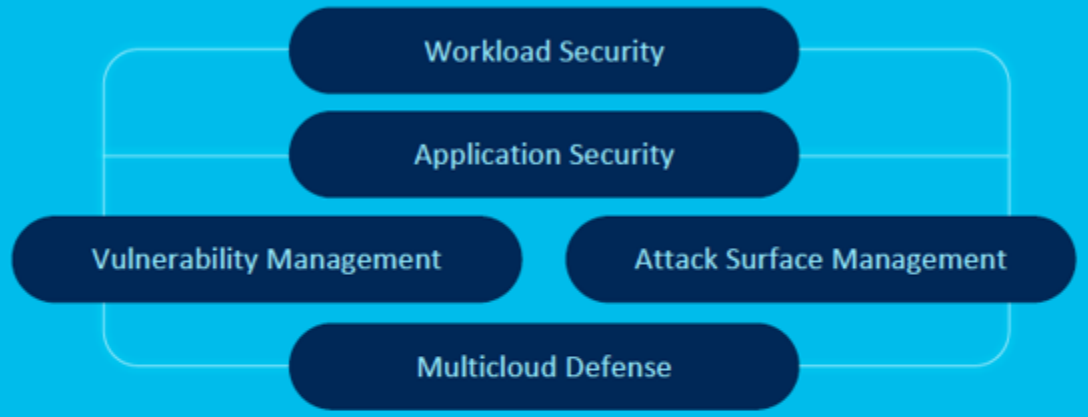
IT.Integrator | cisco Partner

Introducing security only Cisco can deliver

IT.Integrator | cisco Partner

Introducing security only Cisco can deliver

Cisco Cloud Protection Suite



* Global General Availability Coming Soon

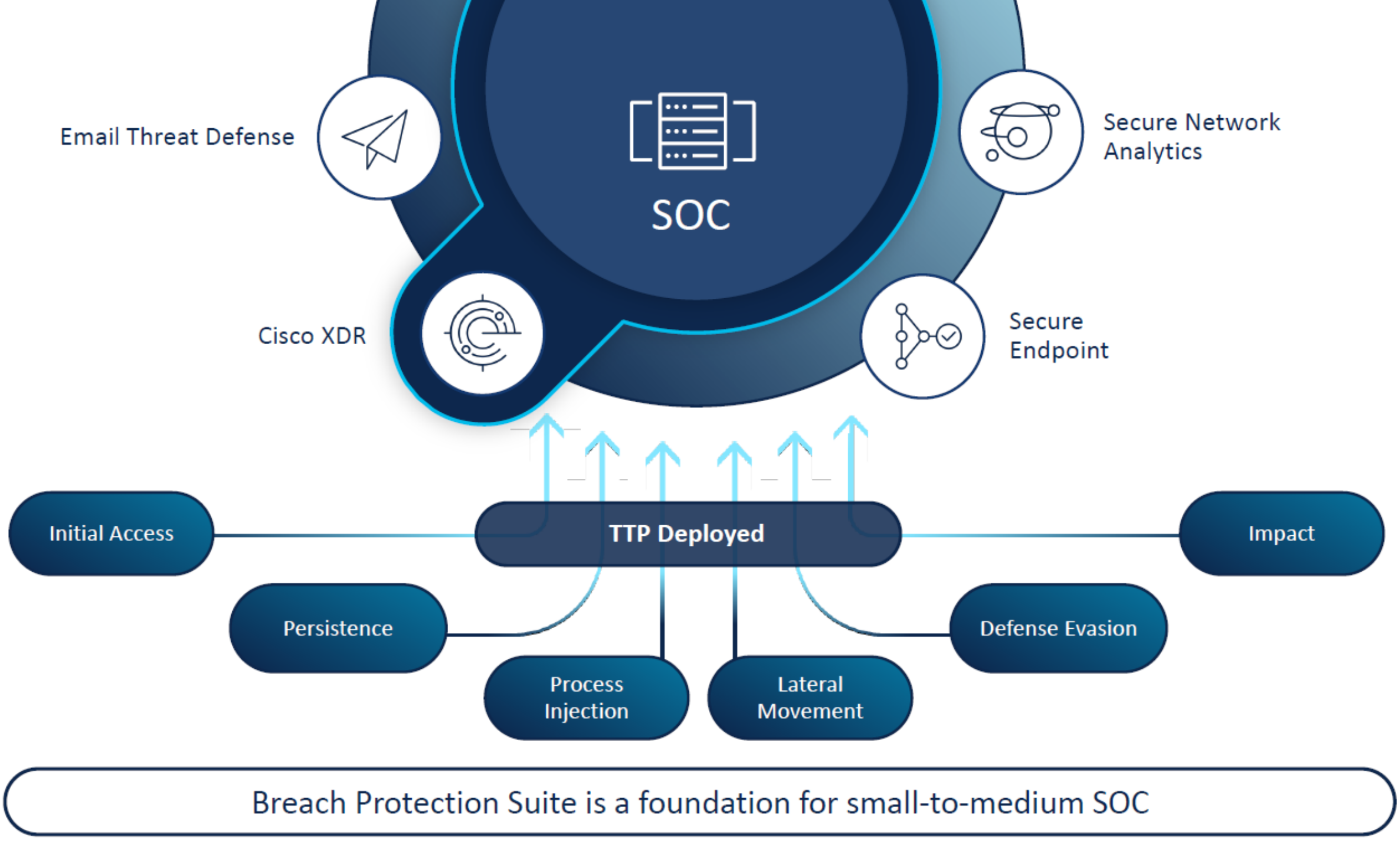
Cisco Multicloud Defense

Cisco Vulnerability Management

Cisco Secure Workload

Cisco Attack Surface Management

Cisco Cloud Application Security



Breach Protection Suite is a foundation for small-to-medium SOC

IT.Integrator | cisco Partner

Наступні кроки: **проектування та впровадження**

Власник / Інвестор
Стратегія

Ефективність бізнесу
(CIA)
+
Фінансова
ефективність
(TCO, ROI)

IT / ІБ Дирекція
Цілі

Простота, Видимість,
Ефективність
+
Інтеграція,
Автоматизація
+
Кадрове
забезпечення

Виконавці
Завдання

Джерела
(EDR, NDR, FW, Identity,
e-mail, DNS, Ckoud)
+
Виробники
(Cisco, 3th party)
+
Функціонал
(реалізація цілей)

Повний цикл системної інтеграції: Проектування, Впровадження, Підтримка експлуатації

Additional Resources

- Where can you learn more about Cisco XDR?
- Cisco XDR At a Glance
- Cisco XDR Overview Video
- An XDR Primer: The Promise of Simplifying Security Operations Position Paper
- Cisco XDR: Security Operations Simplified eBook
- Five Ways to Experience XDR eBook
- XDR Buyer's Guide

Cisco XDR on Cisco.com

IT.Integrator | cisco Partner

Дякую за увагу!