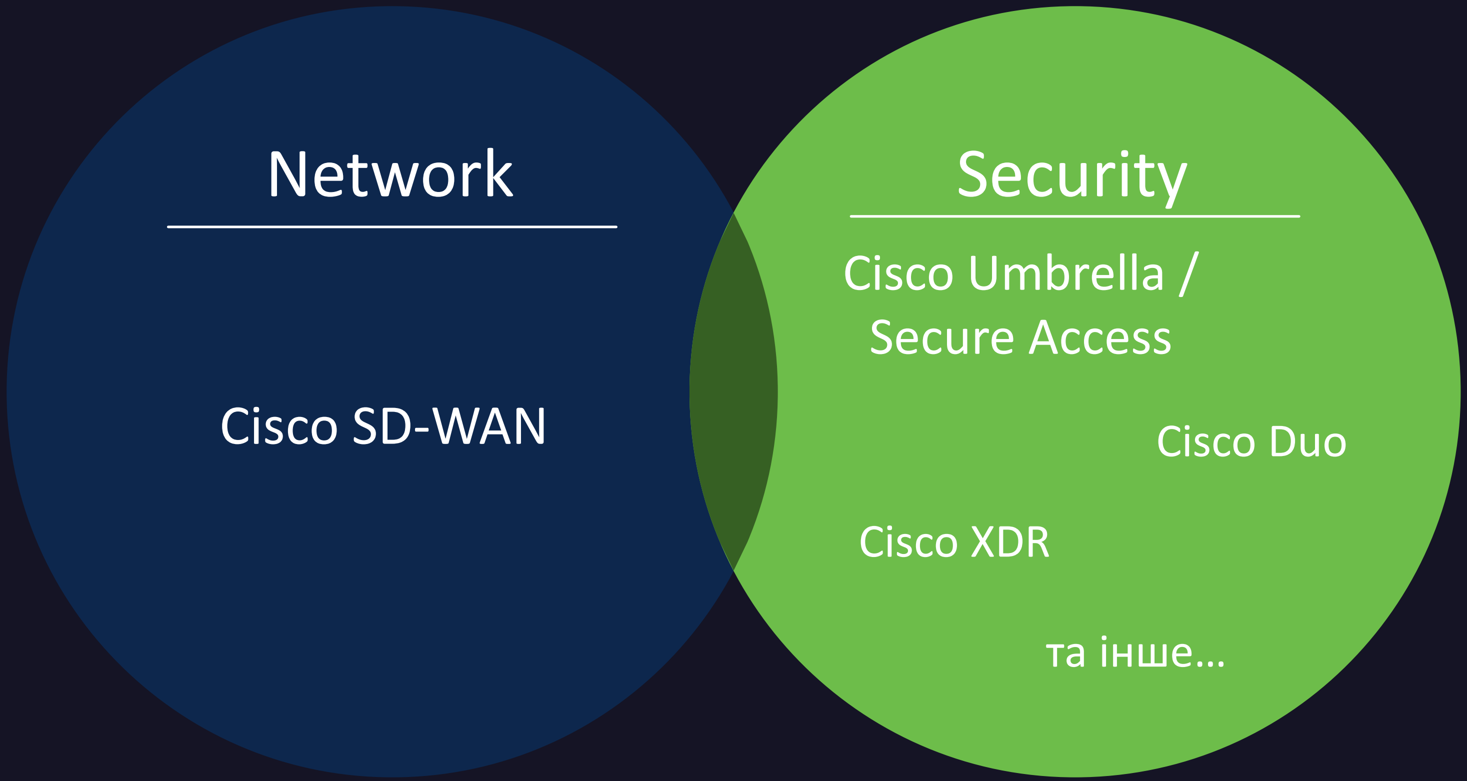
IT.Integrator | CISCO Partner

Основні компоненти Cisco SASE в частині кібербезпеки

Олексій Швачка

SSE or SASE ?



- The “Security Services Edge” category was first introduced by Gartner in the “2021 Roadmap for SASE Convergence” report in March of 2021

- SSE is the half of secure access service edge (SASE) focusing on the convergence of security services

- Networking convergence forms the other half of SASE

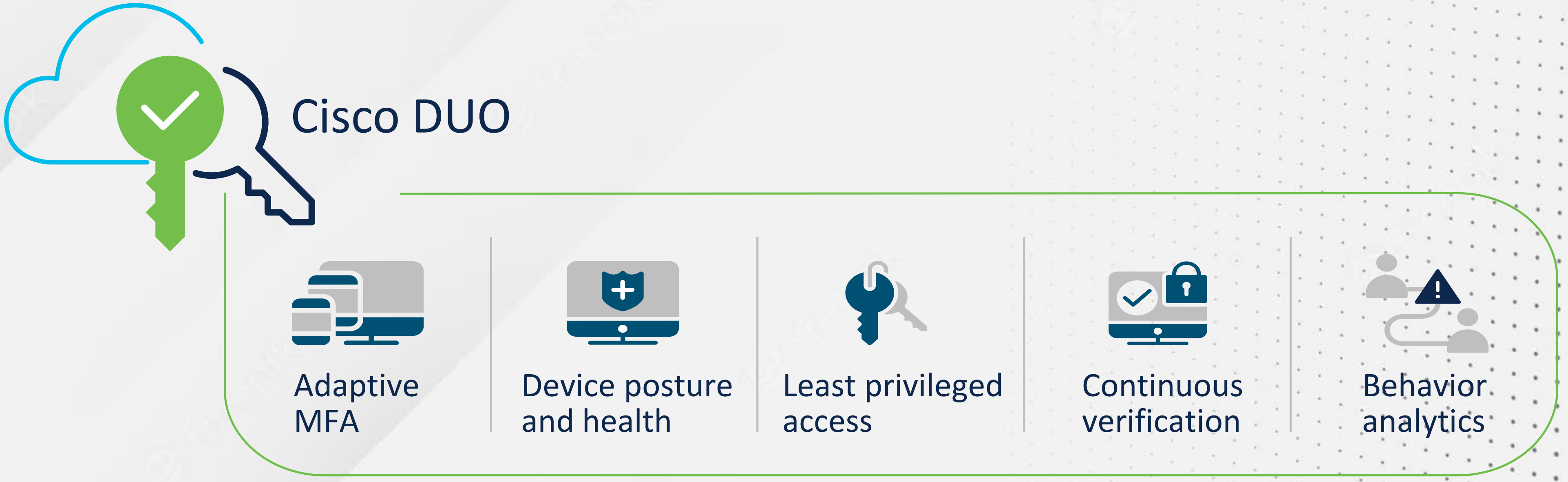
Agenda

- Cisco DUO
- Cisco Secure Access
- Cisco XDR

Agenda

- **Cisco DUO**
- Cisco Secure Access
- Cisco XDR

Cisco DUO



Cisco DUO

- Adaptive MFA
- Device posture and health
- Least privileged access
- Continuous verification
- Behavior analytics

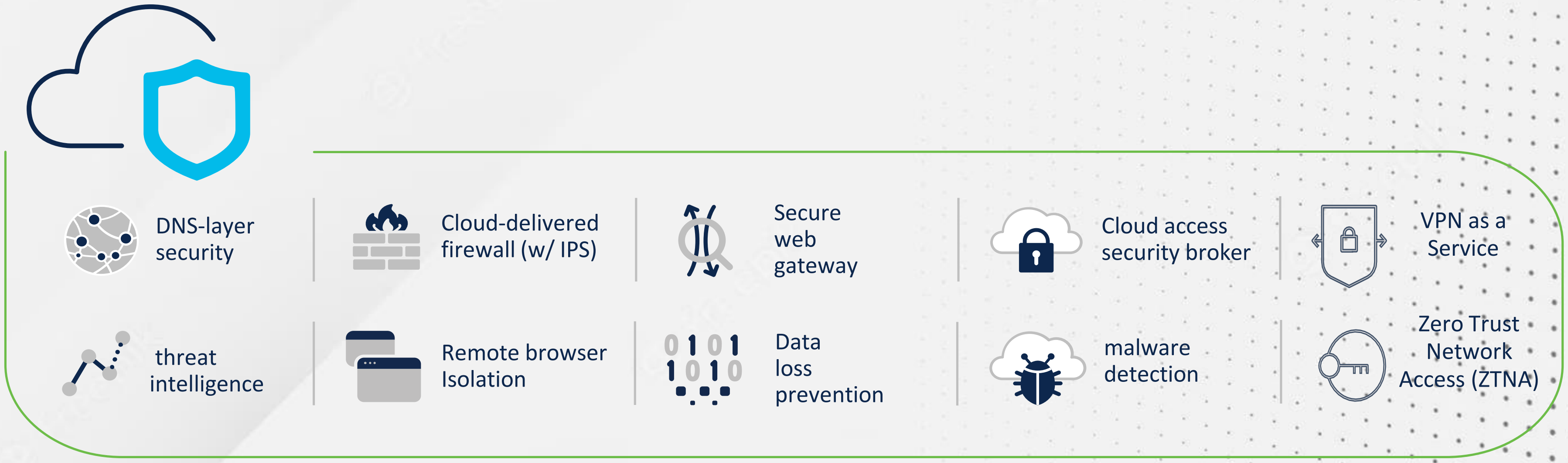
Verify the identity of all users and the trust of the devices before granting access to company-approved applications

Every user.
Every device.
Every application.

Agenda

- Cisco DUO
- **Cisco Secure Access**
- Cisco XDR

Cisco Secure Access



DNS-layer security

Cloud-delivered firewall (w/ IPS)

Secure web gateway

Cloud access security broker

VPN as a Service

threat intelligence

Remote browser Isolation

Data loss prevention

malware detection

Zero Trust Network Access (ZTNA)

Combines multiple security capabilities into one simple, effective, cloud-native service

Cloud-Native service with state-of-the-art cybersecurity capabilities delivered out of data centers worldwide, interconnected with private and public peerings to provide the fastest route and lower latency.

Cisco Secure Access

DNS-layer security

DNS-layer security

DNS-layer security

- DNS requests sent to SSE instead of the ISP's DNS server
- Statistical Models and Machine Learning
- The First Cyber Security Check

Cloud-Native to provide Quick Resolution with Unparallel Security

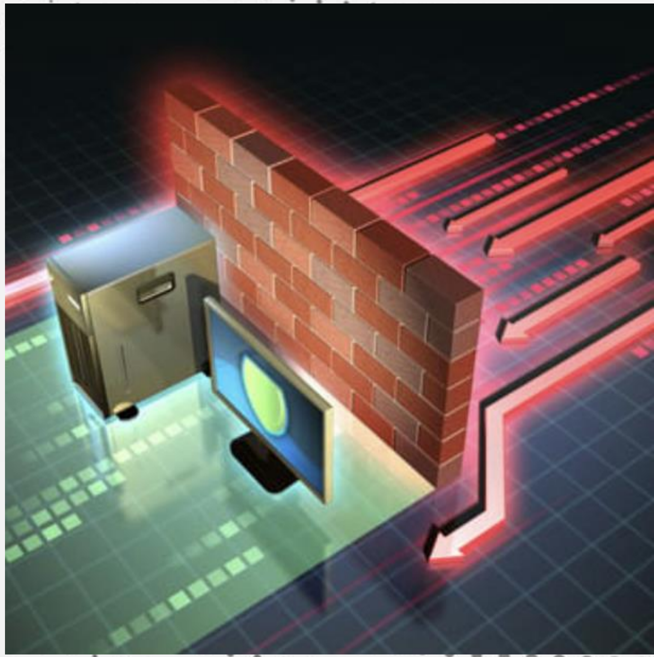
Cisco Secure Access

Cloud-delivered firewall with IPS

Cloud-delivered firewall (w/ IPS)

Cloud-delivered firewall with IPS

- Extends control to non-web, non-HTTP(S) traffic
- Enforces IP, port, and protocol policies
- IPS can do deep packet inspection with minimal latency impact



Cloud-Native to Stay ahead of the curve, secure and protect against advanced threats.

IT.Integrator | CISCO Partner

Cisco Secure Access

Secure Web Gateway

Secure web gateway

SWG for Safe Browsing

- URL Content Control
- Application Visibility and Control
- HTTPS Decryption

Cloud-Native to ensure that web-based applications and services are used in a secure manner.

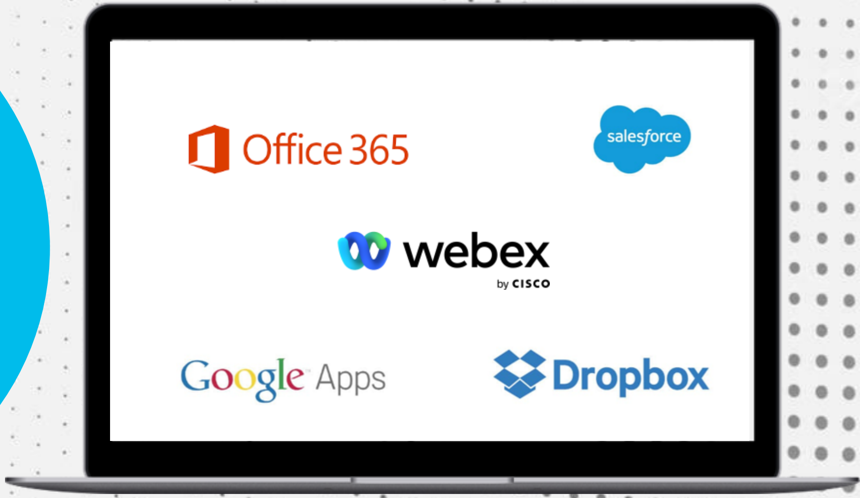
Cisco Secure Access

Cloud Access Security Broker

Cloud access security broker

CASB to protect SaaS apps

- Users,
- Data, and
- Applications.



Cloud-Native to provide visibility, data protection, compliance and threat protection over SaaS applications

IT.Integrator | cisco Partner

Cisco Secure Access

Malware Protection

Malware Protection

Malware Protection

- Detect and protect against malicious files.
- Unknown files sent to sandbox
- Malware in motion
- Malware at rest

Cloud-Native to provide up to date and enhanced protection against malware infections

Data Loss Prevention

Data loss prevention

Data Loss Prevention

- Minimize the risk of sharing confidential information
- Out-of-band DLP for SaaS apps through API
- Inline DLP supports all applications, sanctioned and unsanctioned

Cloud-Native to protect confidential information

IT.Integrator | cisco Partner

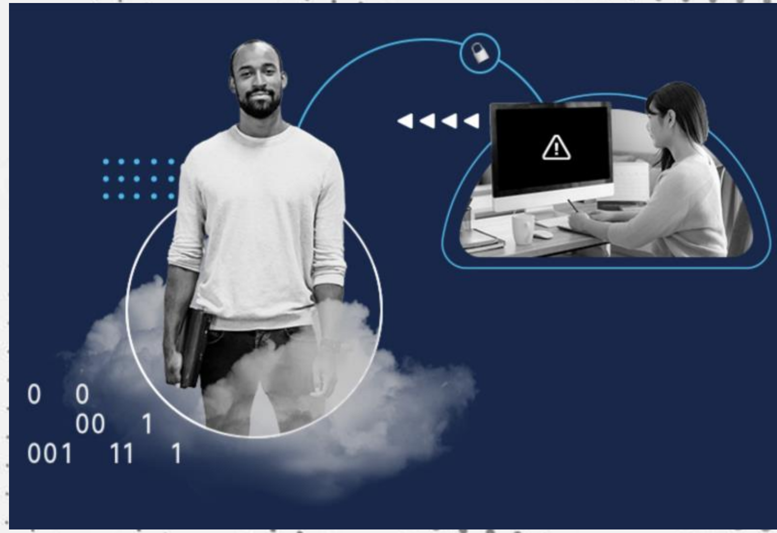
Cisco Secure Access

Remote Browser Isolation

Remote browser Isolation

Remote Browser Isolation

- protects against browser-based security threats by running websites on a safe, separate virtual environment.
- RBI moves the most dangerous part of browsing the internet away from the end user's machine and into the cloud.



Cloud-Native to provide a 70% reduction in attacks that compromise end-user systems, according to Gartner.

VPN as a Service (VPNaaS)

VPN as a Service

VPNaaS

- Deliver VPN capability as a cloud-based service
- No hardware to install, maintain, or update
- Easily connect users and things to any private app, any port, any protocol

Traditional VPN ✓

VPNaaS ✓

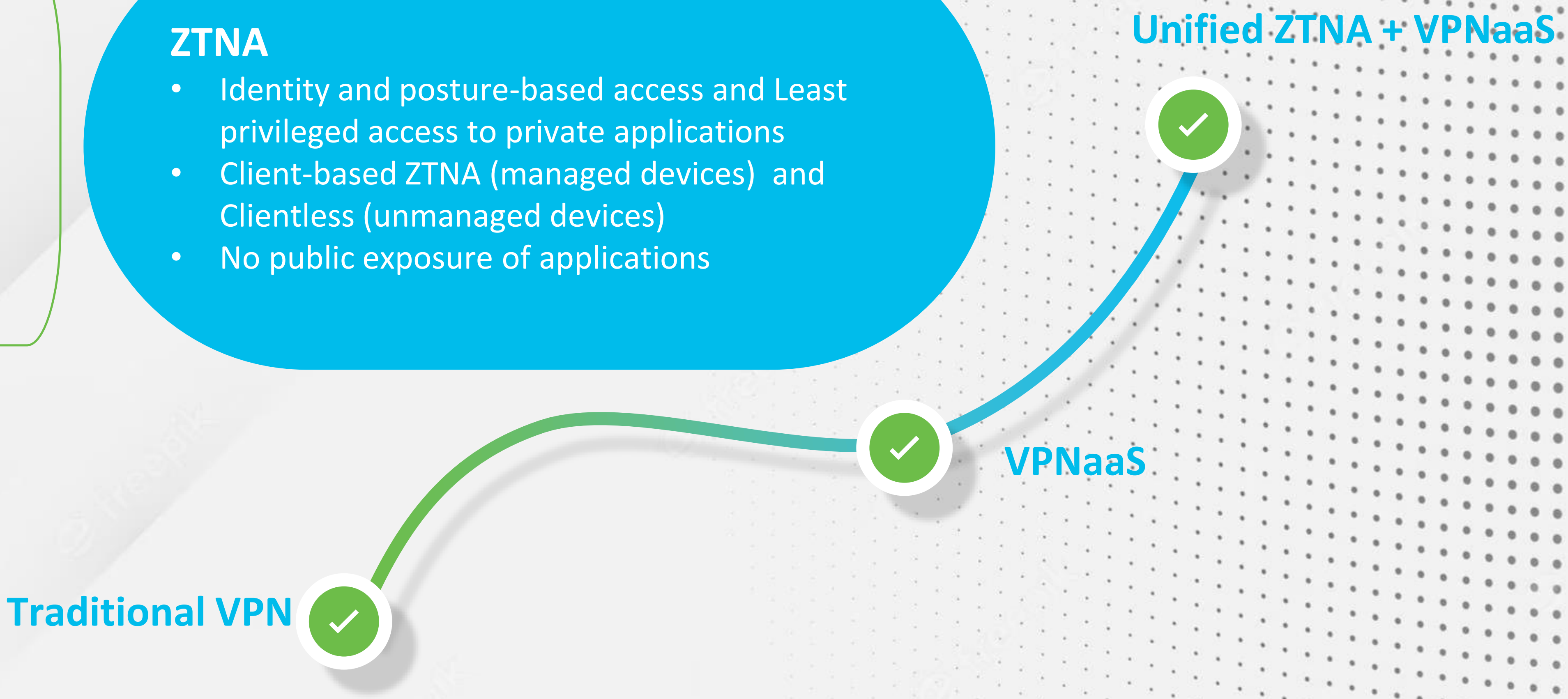
Cisco Secure Access

Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA)

ZTNA

- Identity and posture-based access and Least privileged access to private applications
- Client-based ZTNA (managed devices) and Clientless (unmanaged devices)
- No public exposure of applications



IT.Integrator | cisco Partner

Cisco Secure Access

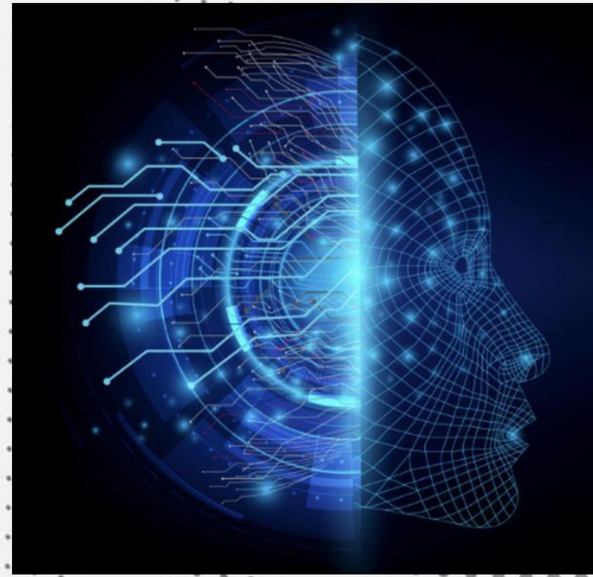
Threat Intelligence

Threat Intelligence

TALOS

Threat Intelligence

- Hundreds of full-time threat researchers and data scientists
- Artificial intelligence algorithms to detect abnormal behaviors

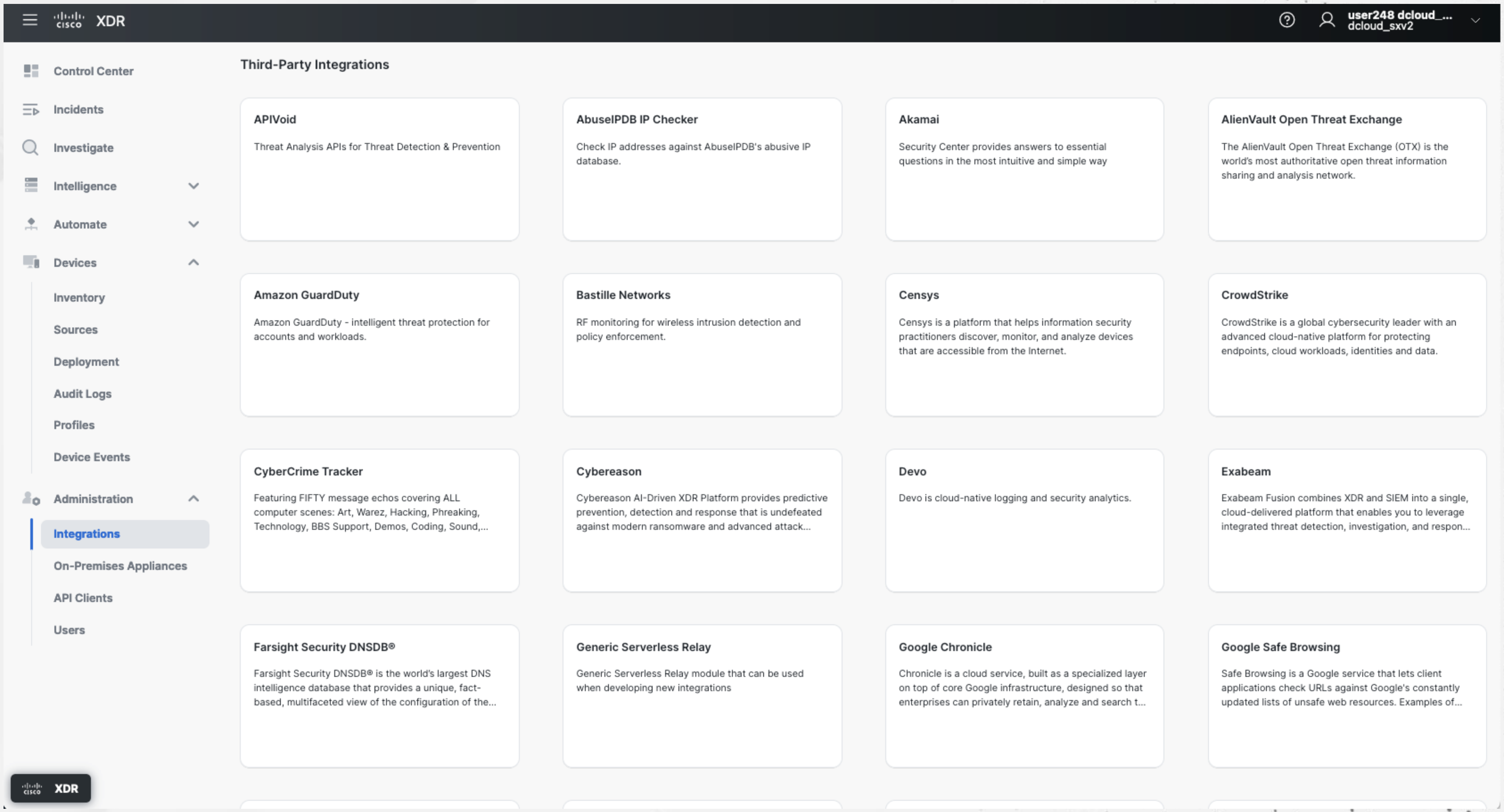


Agenda

- Cisco DUO
- Cisco Secure Access
- **Cisco XDR**

IT.Integrator | cisco Partner

Cisco XDR



Third-Party Integrations

APIVoid
Threat Analysis APIs for Threat Detection & Prevention

AbuseIPDB IP Checker
Check IP addresses against AbuseIPDB's abusive IP database.

Akamai
Security Center provides answers to essential questions in the most intuitive and simple way

AlienVault Open Threat Exchange
The AlienVault Open Threat Exchange (OTX) is the world's most authoritative open threat information sharing and analysis network.

Amazon GuardDuty
Amazon GuardDuty - intelligent threat protection for accounts and workloads.

Bastille Networks
RF monitoring for wireless intrusion detection and policy enforcement.

Censys
Censys is a platform that helps information security practitioners discover, monitor, and analyze devices that are accessible from the Internet.

CrowdStrike
CrowdStrike is a global cybersecurity leader with an advanced cloud-native platform for protecting endpoints, cloud workloads, identities and data.

CyberCrime Tracker
Featuring FIFTY message echos covering ALL computer scenes: Art, Warez, Hacking, Phreaking, Technology, BBS Support, Demos, Coding, Sound,...

Cybereason
Cybereason AI-Driven XDR Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack...

Devo
Devo is cloud-native logging and security analytics.

Exabeam
Exabeam Fusion combines XDR and SIEM into a single, cloud-delivered platform that enables you to leverage integrated threat detection, investigation, and respon...

Farsight Security DNSDB®
Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the...

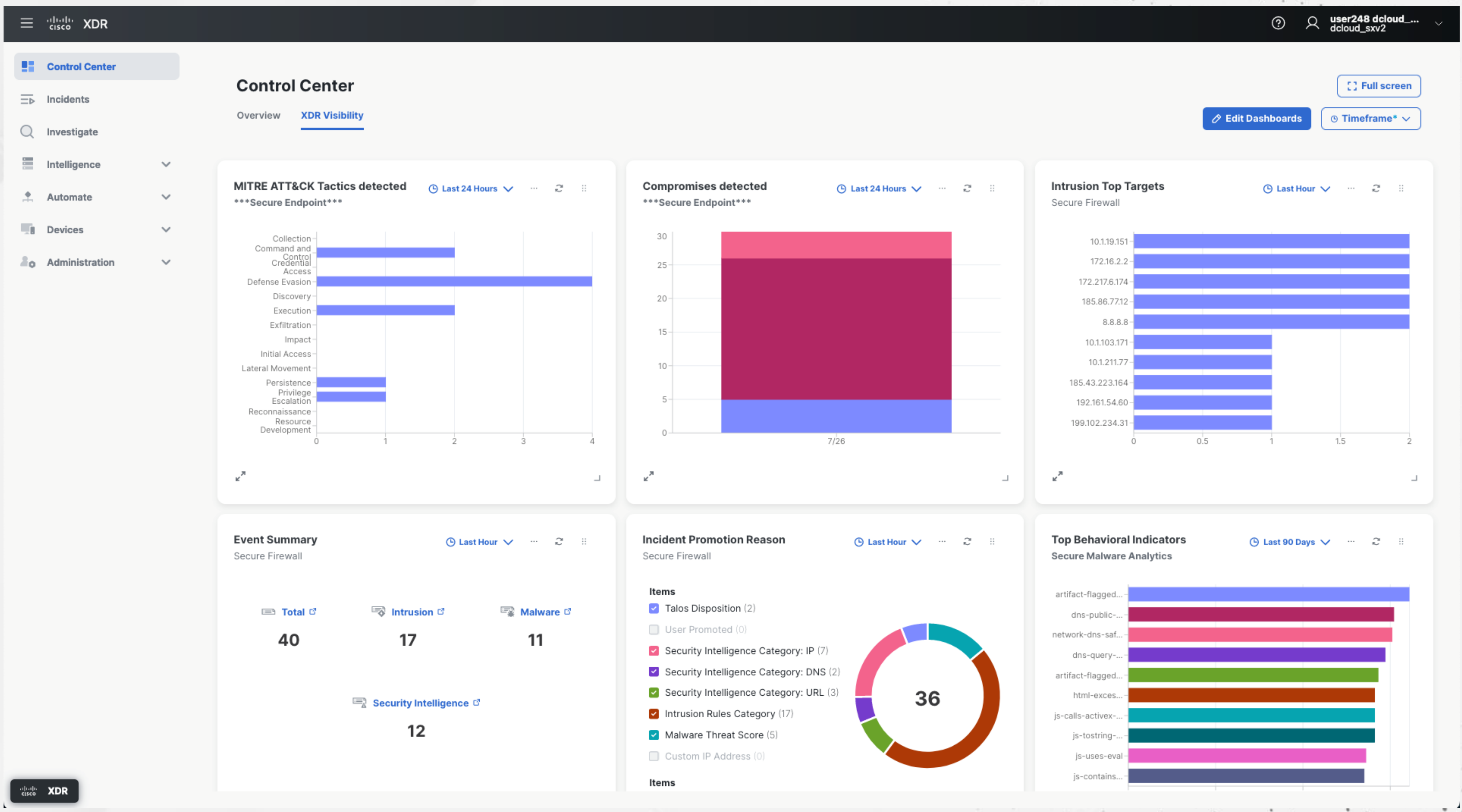
Generic Serverless Relay
Generic Serverless Relay module that can be used when developing new integrations

Google Chronicle
Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed so that enterprises can privately retain, analyze and search t...

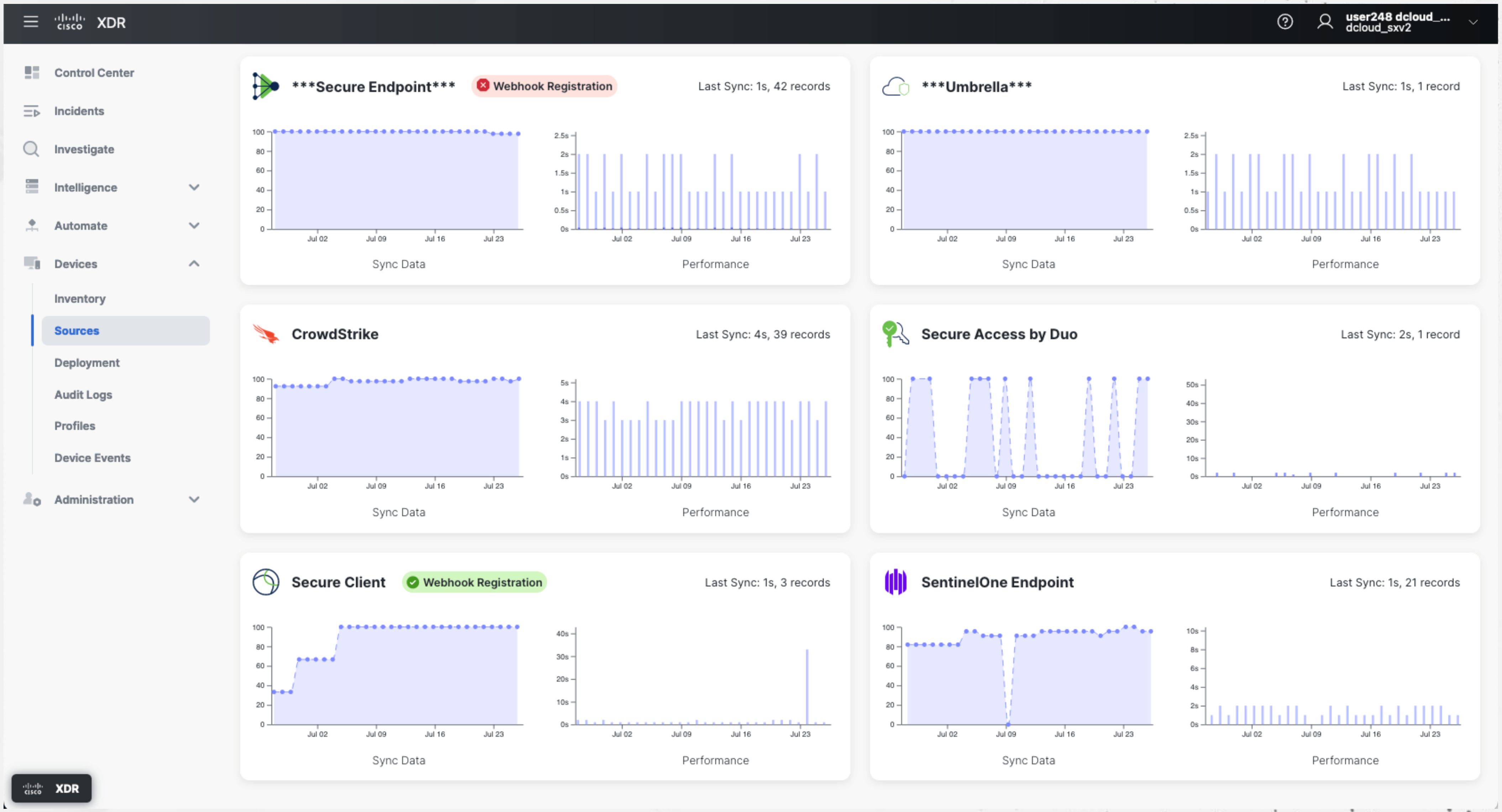
Google Safe Browsing
Safe Browsing is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources. Examples of...

IT.Integrator | cisco Partner

Cisco XDR



Cisco XDR



Secure Endpoint — Webhook Registration — Last Sync: 1s, 42 records

Umbrella — Last Sync: 1s, 1 record

CrowdStrike — Last Sync: 4s, 39 records

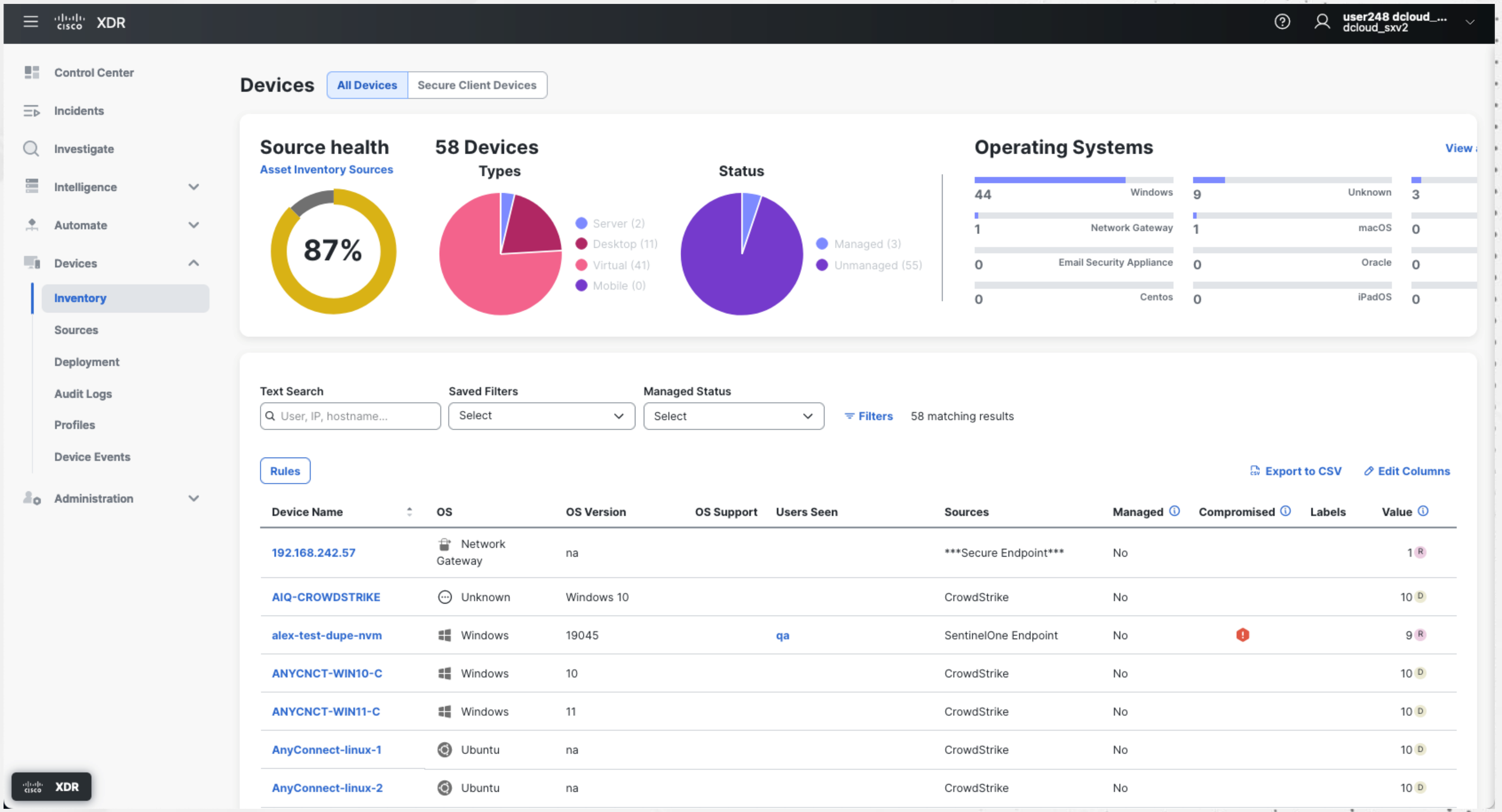
Secure Access by Duo — Last Sync: 2s, 1 record

Secure Client — Webhook Registration — Last Sync: 1s, 3 records

SentinelOne Endpoint — Last Sync: 1s, 21 records

IT.Integrator | cisco Partner

Cisco XDR



Devices

Source health

Asset Inventory Sources

87%

58 Devices

Types

- Server (2)
- Desktop (11)
- Virtual (41)
- Mobile (0)

Status

- Managed (3)
- Unmanaged (55)

Operating Systems

44	Windows	9	Unknown	3
1	Network Gateway	1	macOS	0
0	Email Security Appliance	0	Oracle	0
0	Centos	0	iPadOS	0

Text Search: User, IP, hostname...

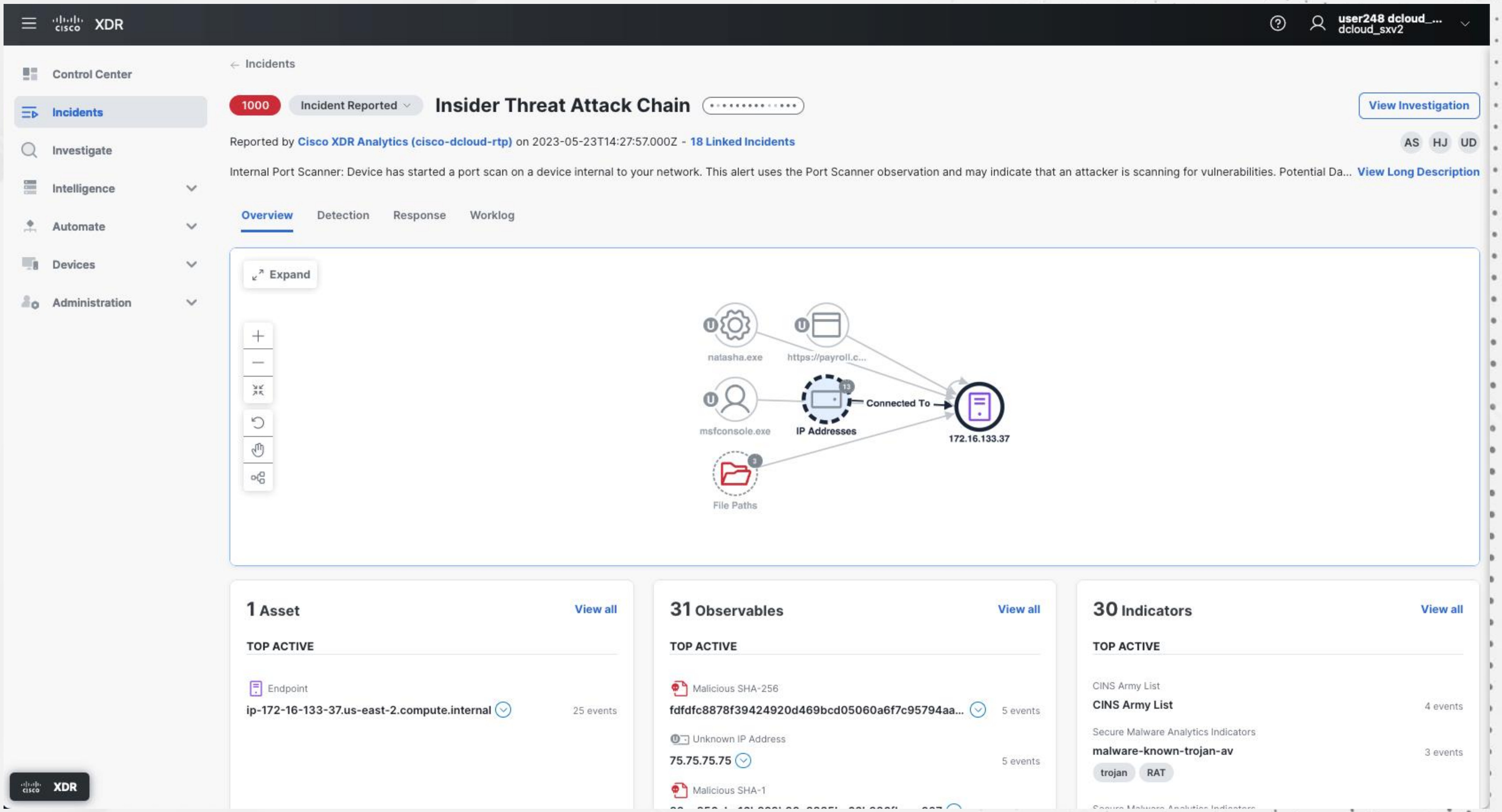
Saved Filters: Select

Managed Status: Select

58 matching results

Device Name	OS	OS Version	OS Support	Users Seen	Sources	Managed ⓘ	Compromised ⓘ	Labels	Value ⓘ
192.168.242.57	Network Gateway	na			***Secure Endpoint***	No			1 R
AIQ-CROWDSTRIKE	Unknown	Windows 10			CrowdStrike	No			10 D
alex-test-dupe-nvm	Windows	19045		qa	SentinelOne Endpoint	No	!		9 R
ANYCNCT-WIN10-C	Windows	10			CrowdStrike	No			10 D
ANYCNCT-WIN11-C	Windows	11			CrowdStrike	No			10 D
AnyConnect-linux-1	Ubuntu	na			CrowdStrike	No			10 D
AnyConnect-linux-2	Ubuntu	na			CrowdStrike	No			10 D

Cisco XDR



← Incidents

1000 Incident Reported

Insider Threat Attack Chain

Reported by Cisco XDR Analytics (cisco-dcloud-rtp) on 2023-05-23T14:27:57.000Z - 18 Linked Incidents

Internal Port Scanner: Device has started a port scan on a device internal to your network. This alert uses the Port Scanner observation and may indicate that an attacker is scanning for vulnerabilities. Potential Da... View Long Description

Overview | Detection | Response | Worklog

1 Asset View all

TOP ACTIVE

Endpoint
ip-172-16-133-37.us-east-2.compute.internal — 25 events

31 Observables View all

TOP ACTIVE

Malicious SHA-256
fdfdfc8878f39424920d469bcd05060a6f7c95794aa... — 5 events

Unknown IP Address
75.75.75.75 — 5 events

Malicious SHA-1

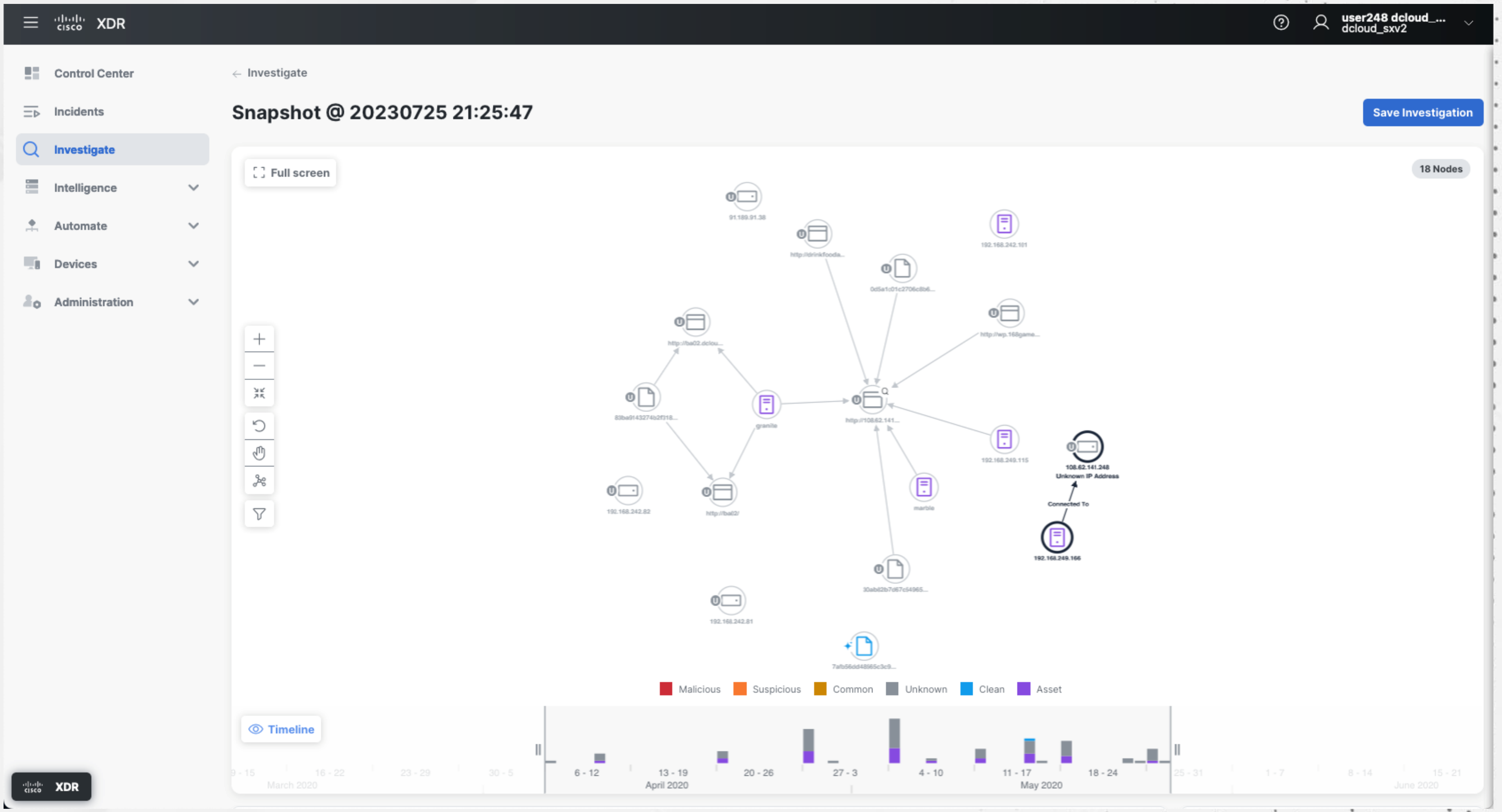
30 Indicators View all

TOP ACTIVE

CINS Army List
CINS Army List — 4 events

Secure Malware Analytics Indicators
malware-known-trojan-av — 3 events
trojan RAT

Cisco XDR



XDR

user248 dcloud_...
dcloud_sxv2

- Control Center
- Incidents
- Investigate
- Intelligence
- Automate
- Devices
- Administration

← Investigate

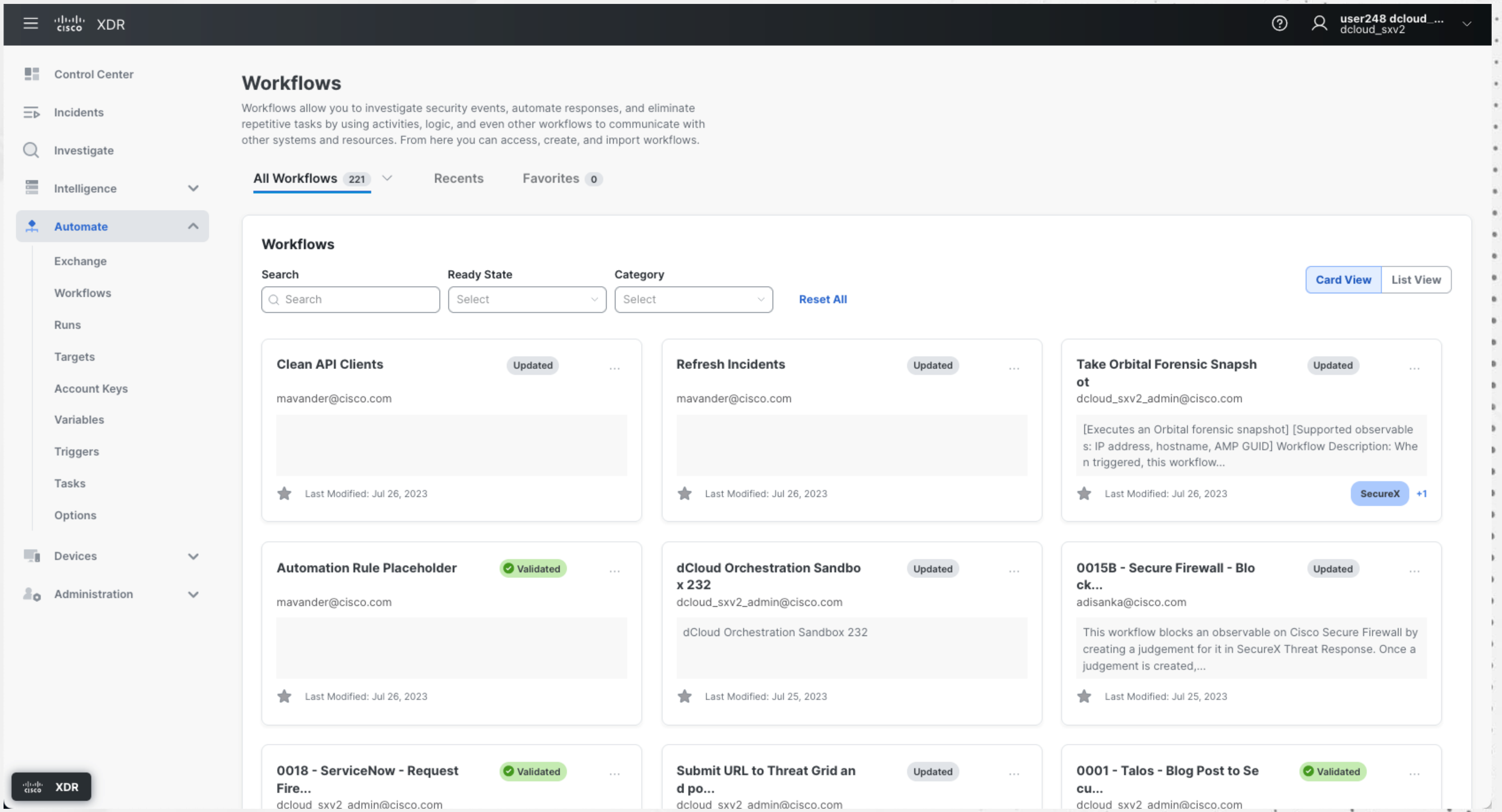
Snapshot @ 20230725 21:25:47

Save Investigation

Full screen

18 Nodes

Cisco XDR



Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 221 | Recents | Favorites 0

Workflows

Search: Search | Ready State: Select | Category: Select | Reset All | Card View | List View

Clean API Clients — Updated
mavander@cisco.com
Last Modified: Jul 26, 2023

Refresh Incidents — Updated
mavander@cisco.com
Last Modified: Jul 26, 2023

Take Orbital Forensic Snapshot — Updated
dcloud_sxv2_admin@cisco.com
[Executes an Orbital forensic snapshot] [Supported observables: IP address, hostname, AMP GUID] Workflow Description: When triggered, this workflow...
Last Modified: Jul 26, 2023 — SecureX +1

Automation Rule Placeholder — Validated
mavander@cisco.com
Last Modified: Jul 26, 2023

dCloud Orchestration Sandbox 232 — Updated
dcloud_sxv2_admin@cisco.com
dCloud Orchestration Sandbox 232
Last Modified: Jul 25, 2023

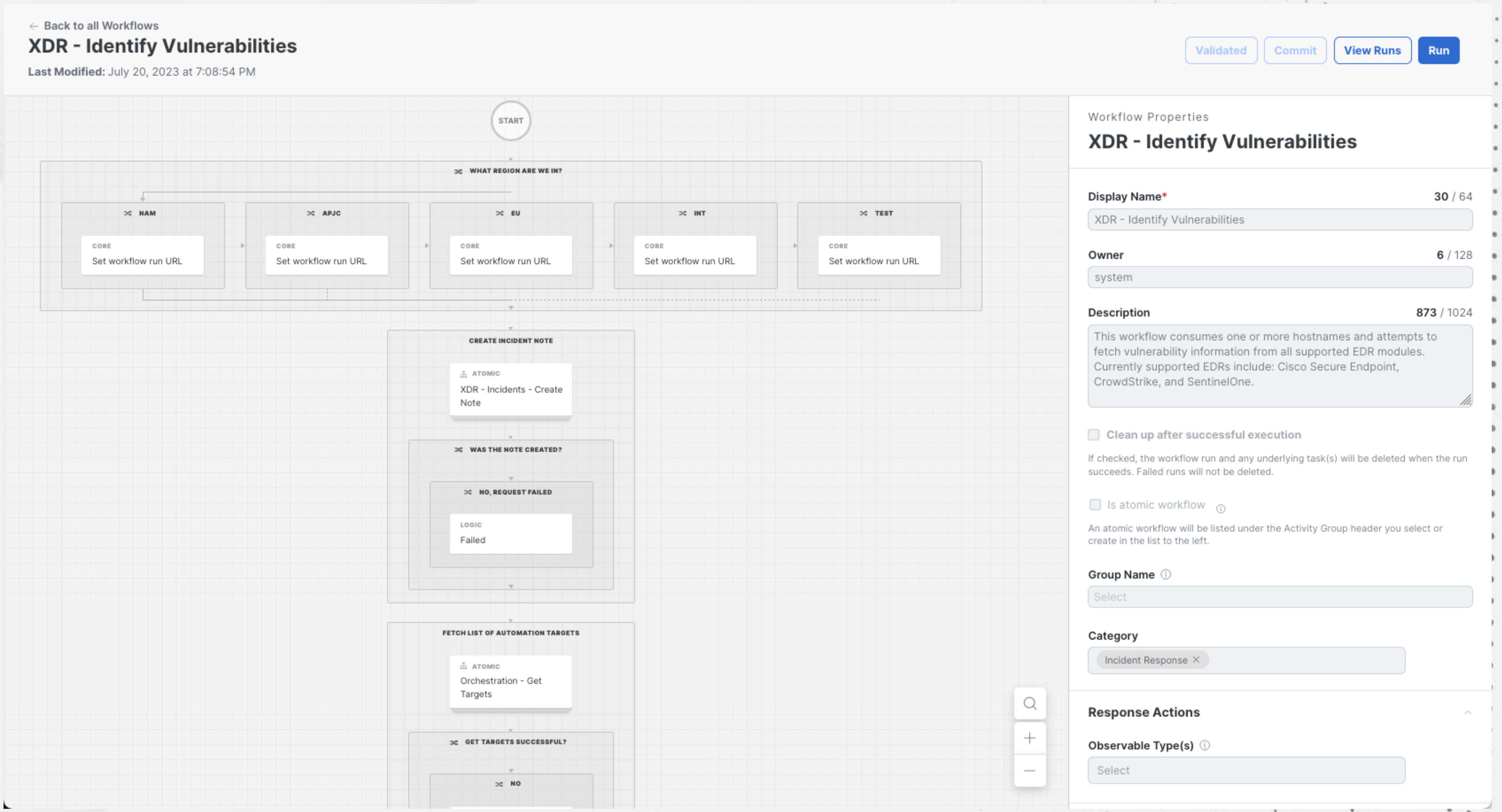
0015B - Secure Firewall - Block... — Updated
adisanka@cisco.com
This workflow blocks an observable on Cisco Secure Firewall by creating a judgement for it in SecureX Threat Response. Once a judgement is created,...
Last Modified: Jul 25, 2023

0018 - ServiceNow - Request Fire... — Validated
dcloud_sxv2_admin@cisco.com

Submit URL to Threat Grid and po... — Updated
dcloud_sxv2_admin@cisco.com

0001 - Talos - Blog Post to Secu... — Validated
dcloud_sxv2_admin@cisco.com

Cisco XDR



XDR - Identify Vulnerabilities

Last Modified: July 20, 2023 at 7:08:54 PM

Workflow Properties

XDR - Identify Vulnerabilities

Display Name* 30 / 64

XDR - Identify Vulnerabilities

Owner 6 / 128

system

Description 873 / 1024

This workflow consumes one or more hostnames and attempts to fetch vulnerability information from all supported EDR modules. Currently supported EDRs include: Cisco Secure Endpoint, CrowdStrike, and SentinelOne.

□ Clean up after successful execution

If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

□ Is atomic workflow

An atomic workflow will be listed under the Activity Group header you select or create in the list to the left.

Group Name

Select

Category

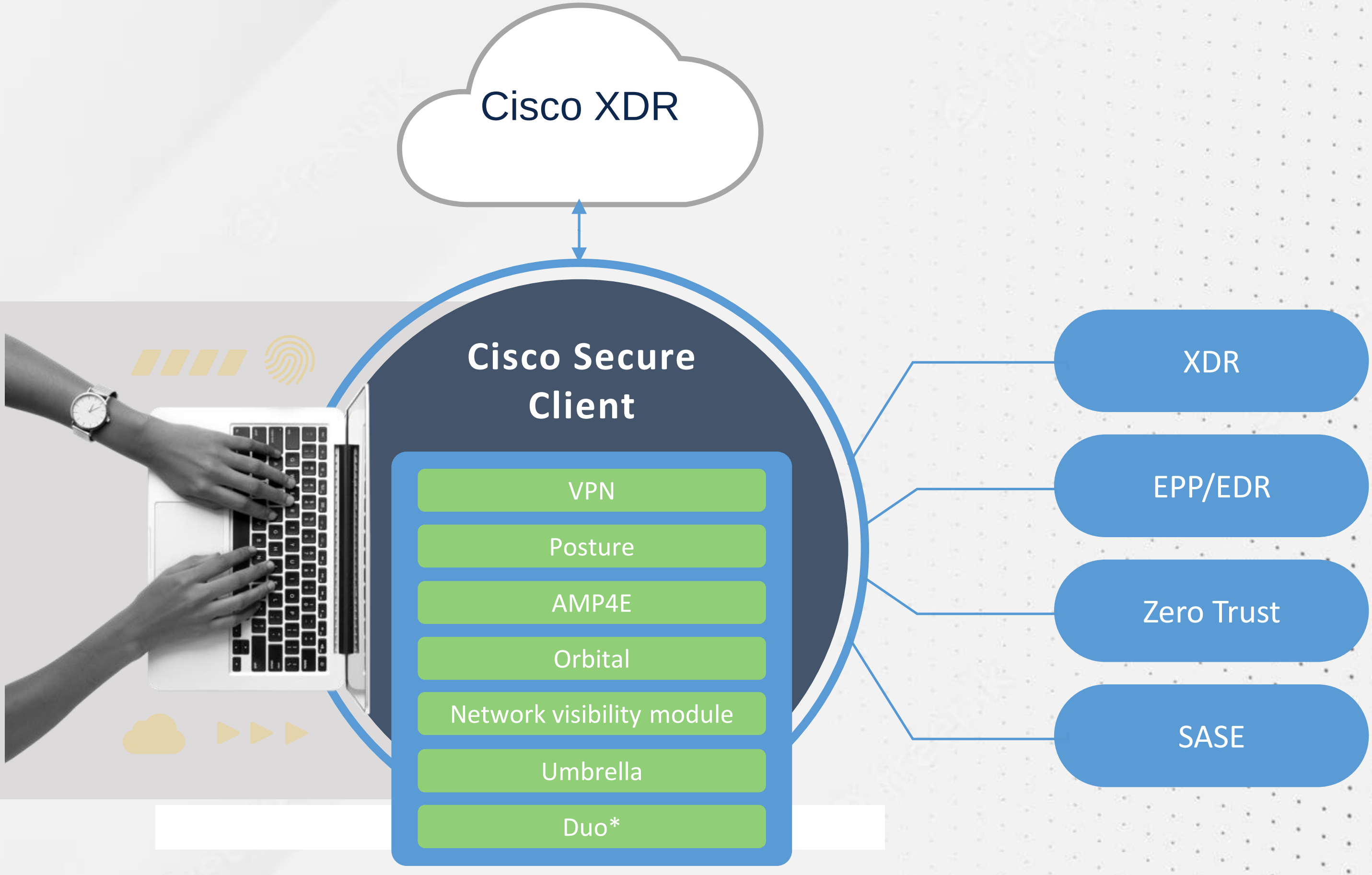
Incident Response ×

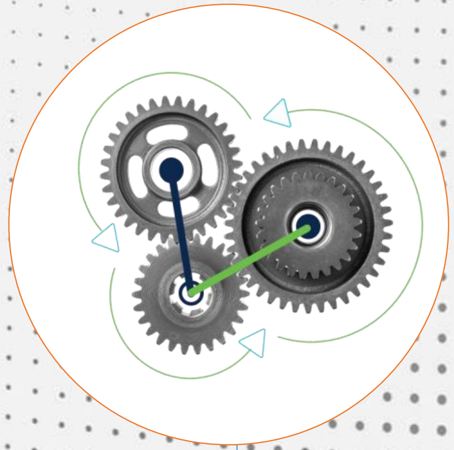
Response Actions

Observable Type(s)

Select

Cisco Secure Client





*Інтеграція DUO до Cisco Secure Client планується в майбутніх версіях

IT.Integrator | cisco Partner

DEMONSTRATION