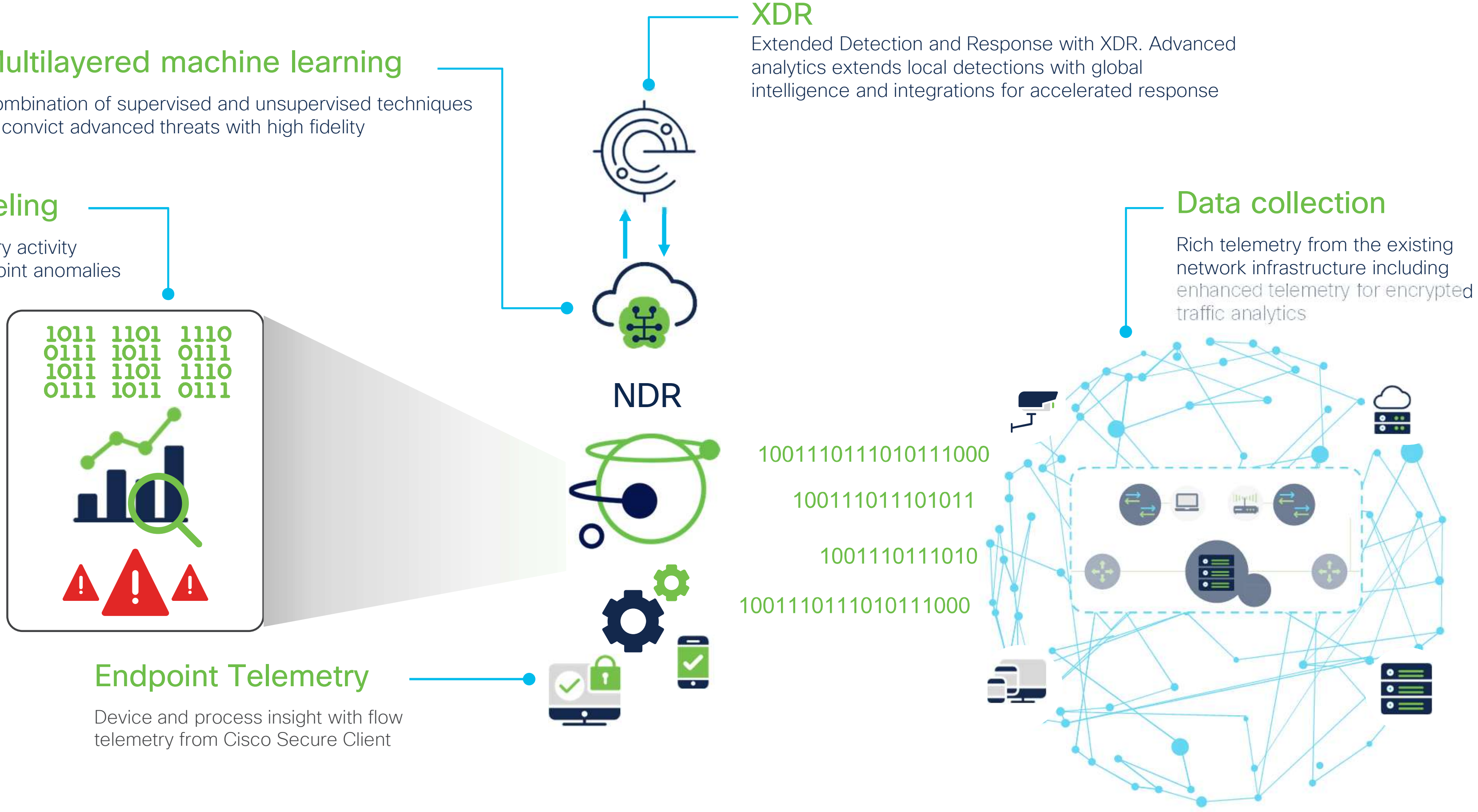
PREČO XDR POTREBUJE NDR

KRITICKÁ ÚLOHA SIETE V DETEKCII A REAKCII NA HROZBY

Tomáš Ondovčík

13.5.2025

Network Detection and Response System



XDR

Extended Detection and Response with XDR. Advanced analytics extends local detections with global intelligence and integrations for accelerated response

Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

Data collection

Rich telemetry from the existing network infrastructure including enhanced telemetry for encrypted traffic analytics

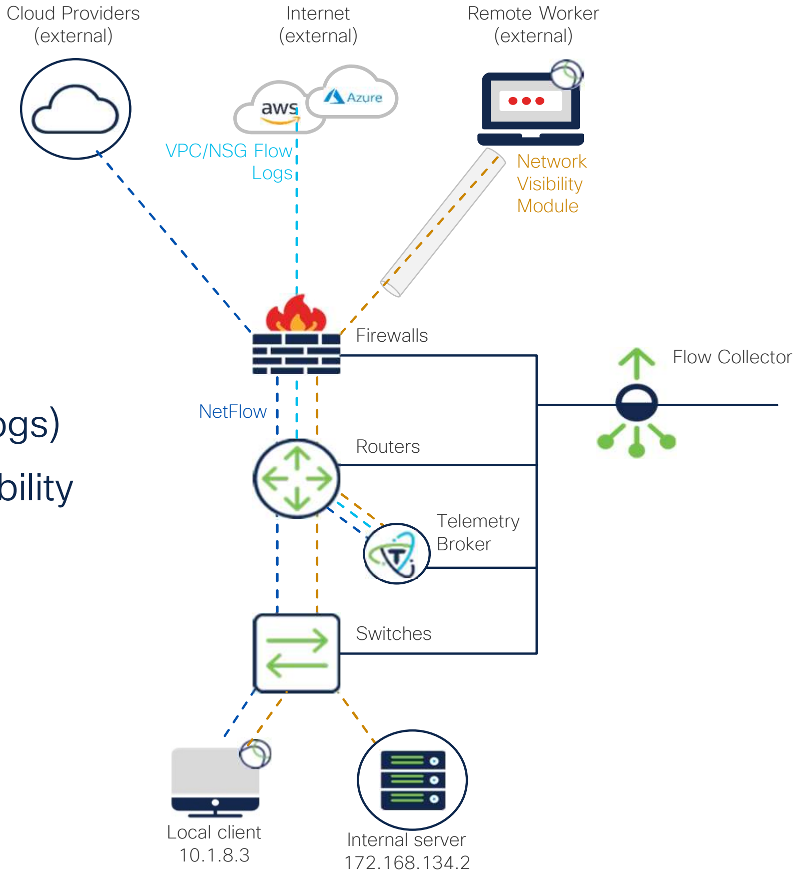
Endpoint Telemetry

Device and process insight with flow telemetry from Cisco Secure Client

The network is the source of truth

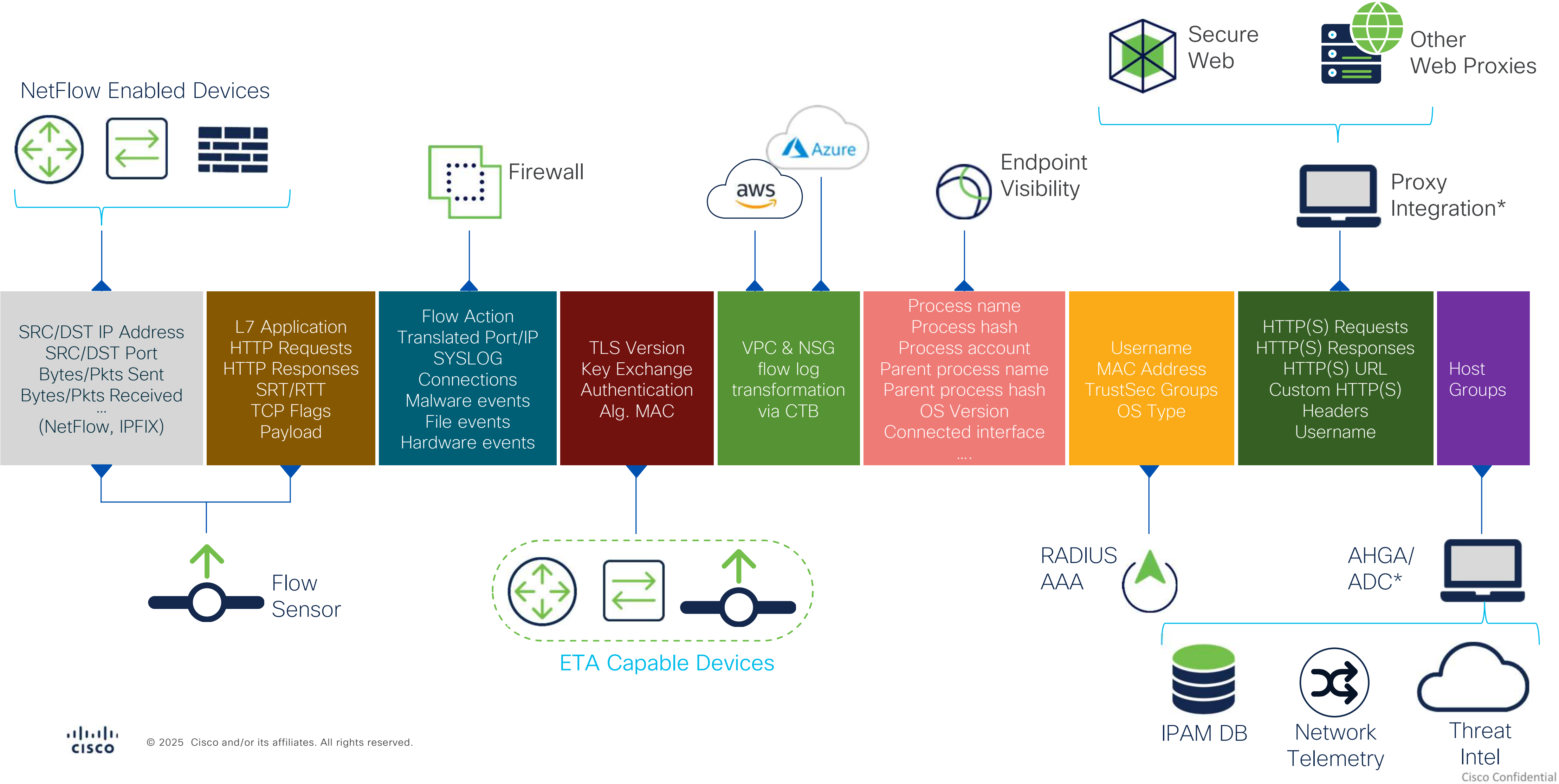
See it ALL!

- A trace of every conversation
- Agentless information collection
- Remote worker endpoint data collection
- Cloud Telemetry ingest (Flow Logs)
- East to west and north south visibility (FW logs)
- Light meta data collection using the existing infrastructure
- Capture enhanced NetFlow



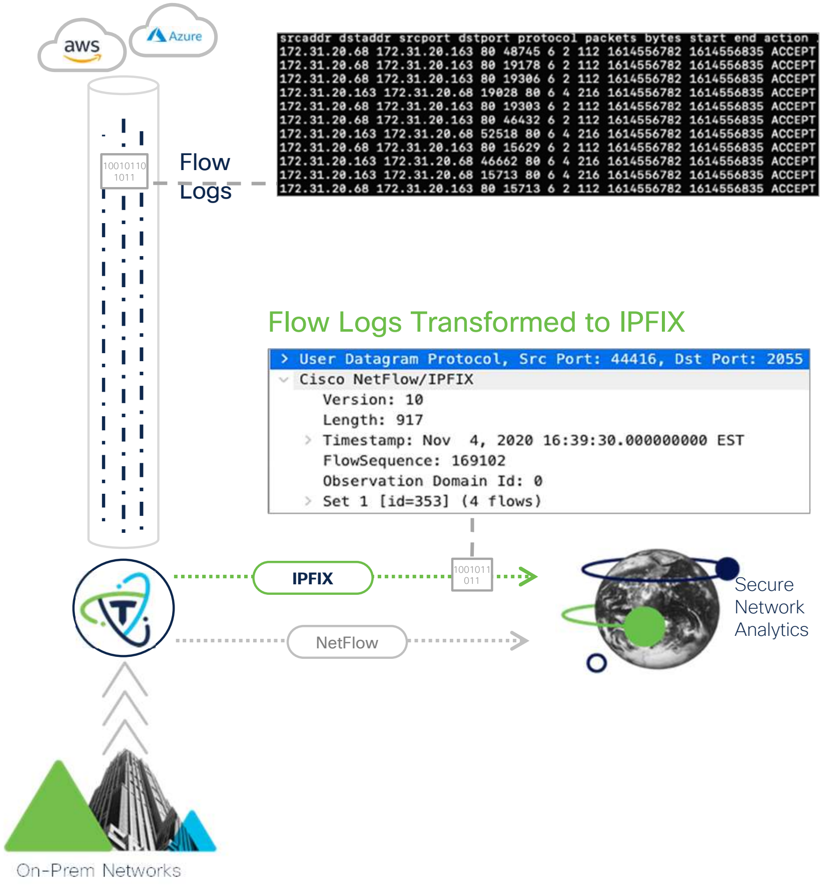
Flow information	Packets
Source address	10.1.8.3
Destination address	172.168.134.2
Source port	47321
Destination port	443
Interface	Gi0/0/1
IP TOS	0x00
IP protocol	6
Next hop	172.168.25.1
TCP flags	0x1A
Source SGT	100
:	:
ETA meta data	IDP | SPLT
Application name	NBAR SECURE-HTTP
Process Name	chrome.exe
Process Account User	Acme/john

Extensible Telemetry Ingest



Monitor your hybrid cloud environment

- Cloud Flow Logs from AWS and Azure provide insight into the activities of hosts residing within cloud environments
- Metadata from Flow Logs centers around the network activity, similar to NetFlow/IPFIX
  - There are 25 total fields provided in Flow Logs
- CTB pulls Flow Logs from AWS S3 buckets and Azure BLOB storage via secure HTTPS connections and transforms the telemetry to IPFIX
  - Once the VPC flow is transformed it is then forwarded to consumers



```
srcaddr dstaddr srcport dstport protocol packets bytes start end action
172.31.20.68 172.31.20.163 80 48745 6 2 112 1614556782 1614556835 ACCEPT
172.31.20.68 172.31.20.163 80 19178 6 2 112 1614556782 1614556835 ACCEPT
172.31.20.68 172.31.20.163 80 19306 6 2 112 1614556782 1614556835 ACCEPT
172.31.20.163 172.31.20.68 19028 80 6 4 216 1614556782 1614556835 ACCEPT
172.31.20.68 172.31.20.163 80 19303 6 2 112 1614556782 1614556835 ACCEPT
172.31.20.68 172.31.20.163 80 46432 6 2 112 1614556782 1614556835 ACCEPT
172.31.20.163 172.31.20.68 52518 80 6 4 216 1614556782 1614556835 ACCEPT
172.31.20.68 172.31.20.163 80 15629 6 2 112 1614556782 1614556835 ACCEPT
172.31.20.163 172.31.20.68 46662 80 6 4 216 1614556782 1614556835 ACCEPT
172.31.20.163 172.31.20.68 15713 80 6 4 216 1614556782 1614556835 ACCEPT
172.31.20.68 172.31.20.163 80 15713 6 2 112 1614556782 1614556835 ACCEPT
```

Flow Logs Transformed to IPFIX

```
> User Datagram Protocol, Src Port: 44416, Dst Port: 2055
v Cisco NetFlow/IPFIX
    Version: 10
    Length: 917
  > Timestamp: Nov  4, 2020 16:39:30.000000000 EST
    FlowSequence: 169102
    Observation Domain Id: 0
  > Set 1 [id=353] (4 flows)
```

NDR the De-Duplicator

Challenge: Network Telemetry

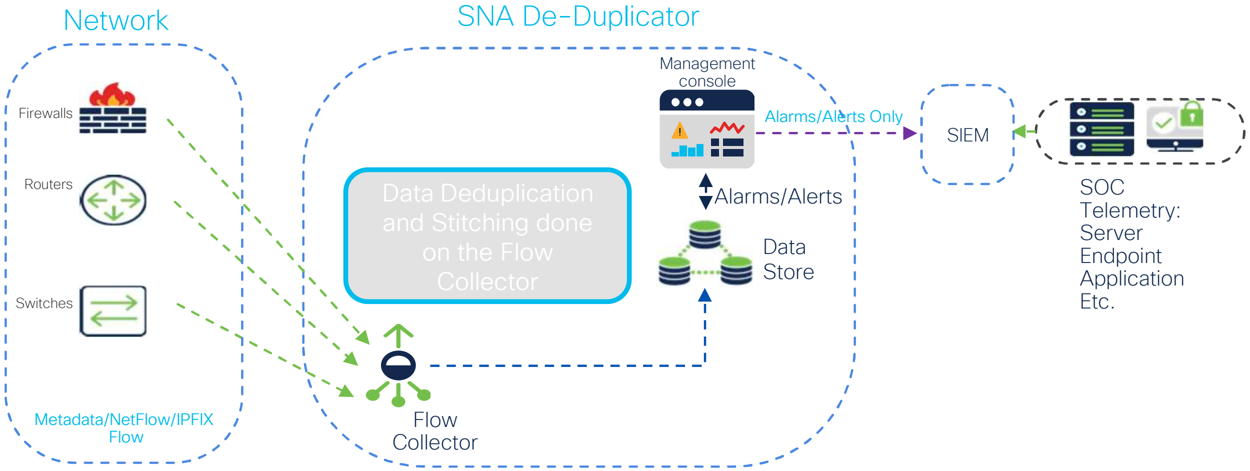
- High volume of metadata/flow data
- Multiple hops (5-6 typical) creates duplicate records
- Bi-directional sessions double the data
- Aggregated export every 60 seconds

Solution: NDR

- Acts as a de-duplicator between telemetry exporters and SIEM
- Stitches and de-duplicates telemetry sets
- Achieves 6:1 reduction (83.5% fewer flows)

Benefits

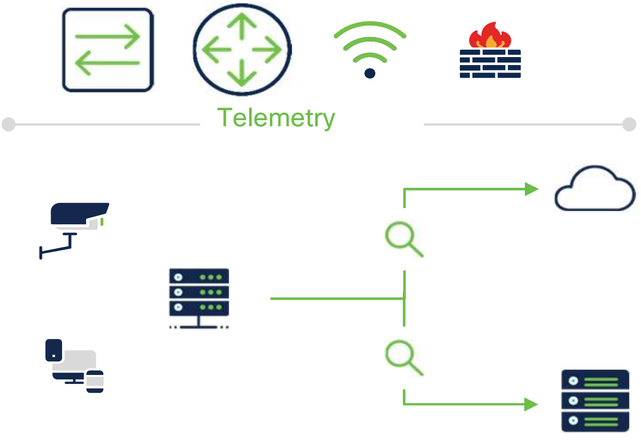
- Symmetric and asymmetric flow stitching
- Converts data into an end-to-end session record
- Enables efficient storage of data
- Improves host-level reporting accuracy
- Preserves all unique data elements



Enriched Telemetry

Traffic visibility

Telemetry from the network and cloud provides up to layer 4 traffic visibility



Communication Visibility

Endpoint attribution

Who is behind the discovered IP? What device are they using? Where are they located?

Who: User

What: Device type

When: Login time

Where: Location

How: Security posture

Process: Endpoint process

Identity

Traffic indication

What type of traffic an IP is sending? What layer 7 app is used? Which URL is accessed?

Application: Layer 7 App

Web: URL identification

NAT: NAT information

Crypto: TLS version

Traffic Status : Firewall block

Intrusion : Malware or File event

Context

Contextual actionable intelligence

Session Data | 100% network accountability

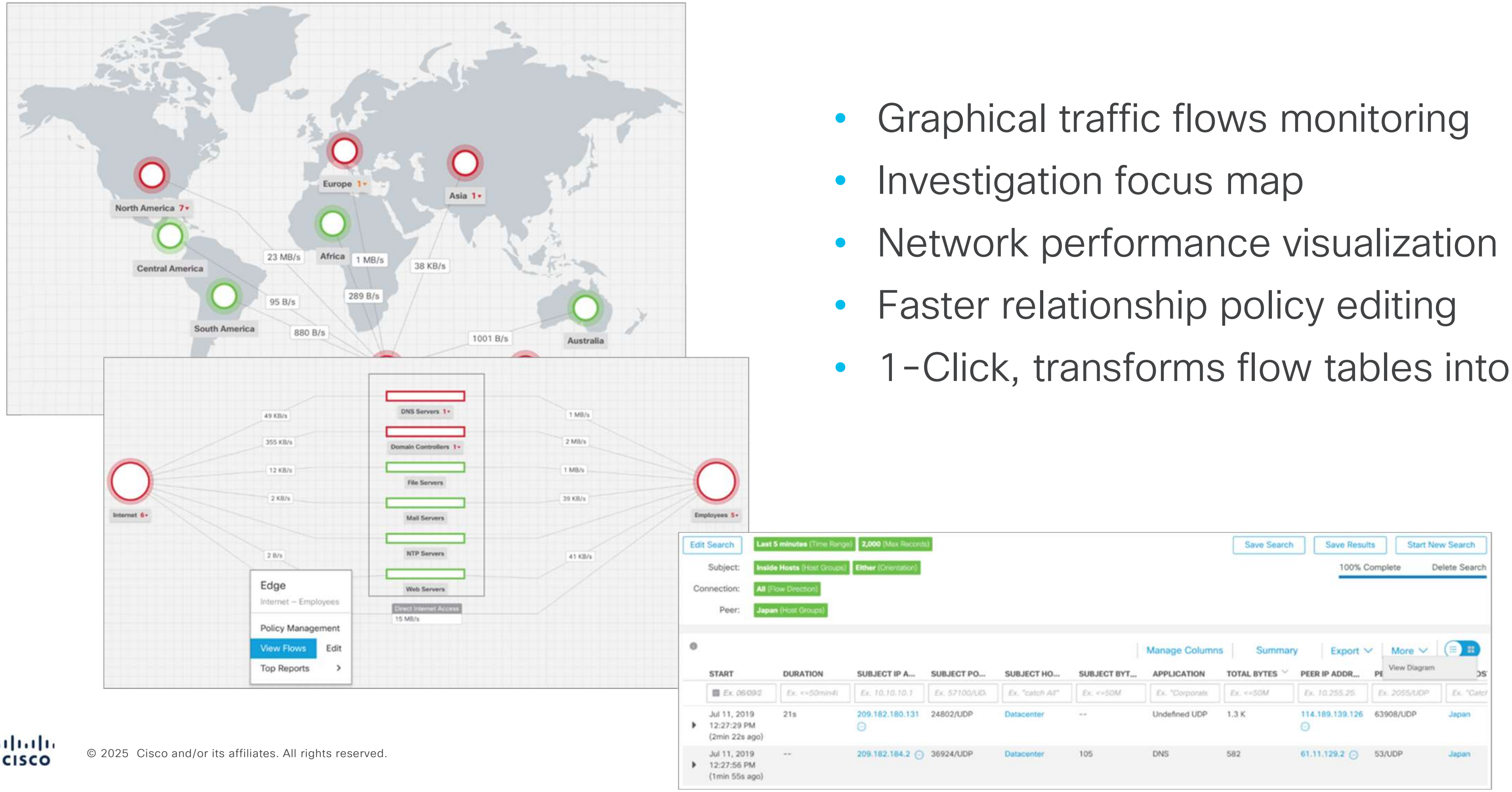
Client	Server	Translation	Service	User	Application	Process #	Traffic	Group	Mac	SGT	Encryption TLS/SSL version
1.1.1.1	2.2.2.2	3.3.3.3	80/tcp	Doug	http	beab09fe3 45ac3217d d80fd46c...	20M	location	00:2b:1f	10	TLS 1.2

Visibility

- User information
- Group/ segment
- Network telemetry
- NAT/proxy
- Interface information
- Layer 7
- Policy information
- Endpoint
- Firewall Security Events
- Threat intelligence
- Cloud
- Encrypted traffic analytics

Visualize traffic flows

- Graphical traffic flows monitoring
- Investigation focus map
- Network performance visualization
- Faster relationship policy editing
- 1-Click, transforms flow tables into maps



Last 5 minutes (Time Range) 2,000 (Max Records)

Subject: Inside Hosts (Host Groups) Either (Orientation)

Connection: All (Flow Direction)

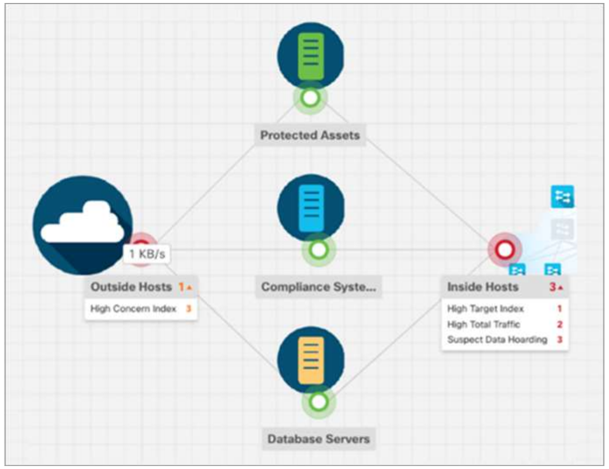
Peer: Japan (Host Groups)

100% Complete Delete Search

START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PE	OS
Ex. 06/09/2	Ex. <=50min4i	Ex. 10.10.10.1	Ex. 57100/UD	Ex. "catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 10.255.25	Ex. 2055/UDP	Ex. "Catc
Jul 11, 2019 12:27:29 PM (2min 22s ago)	21s	209.182.180.131	24802/UDP	Datacenter	--	Undefined UDP	1.3 K	114.189.139.126	63908/UDP	Japan
Jul 11, 2019 12:27:56 PM (1min 55s ago)	--	209.182.184.2	36924/UDP	Datacenter	105	DNS	582	61.11.129.2	53/UDP	Japan

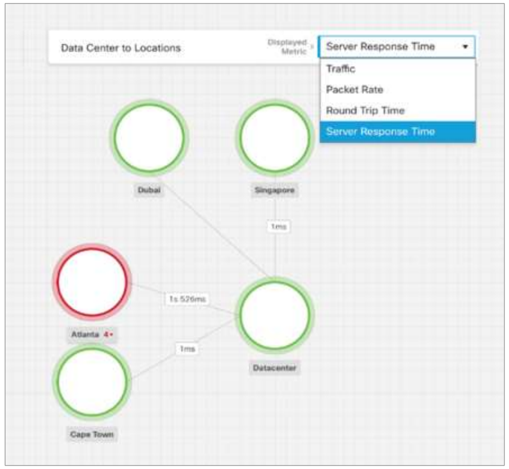
Build maps to focus on critical metrics

Triggered alarms



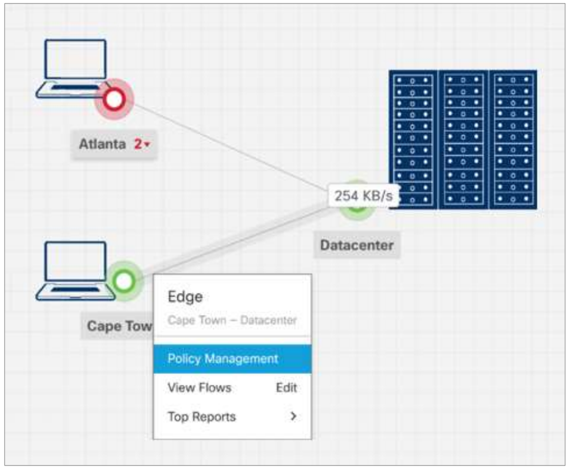
- View triggered alarms brief per host groups
- Drill down into alarms triggered per host group

Network performance



- Visualize network performance metrics
  - RTT, SRT, packet rate and traffic bandwidth

Relationship policy

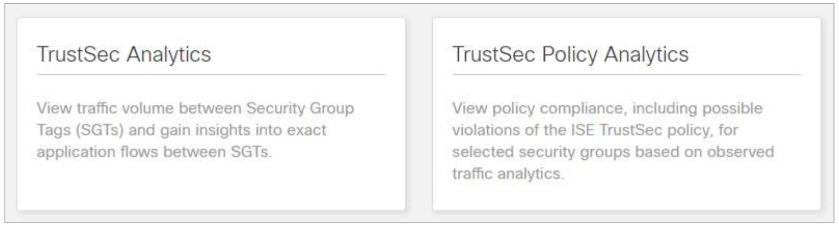


- Relationship policy creation based on graphical representation
- Monitor Segmented network traffic
- Detect abnormal flows faster

Visualize group communications between SGTs

- Report on all observed SGT group communications
- Quickly see which SGTs are communicating
- Click on any cell to display the amount of data transmitted
- View up to 300 SGTs

⬜	No traffic seen
🟩	Traffic seen, default policy allows IP traffic
🟥	Traffic seen, policy allows some traffic and has default Deny IP
🟦	Traffic seen, policy is complex,



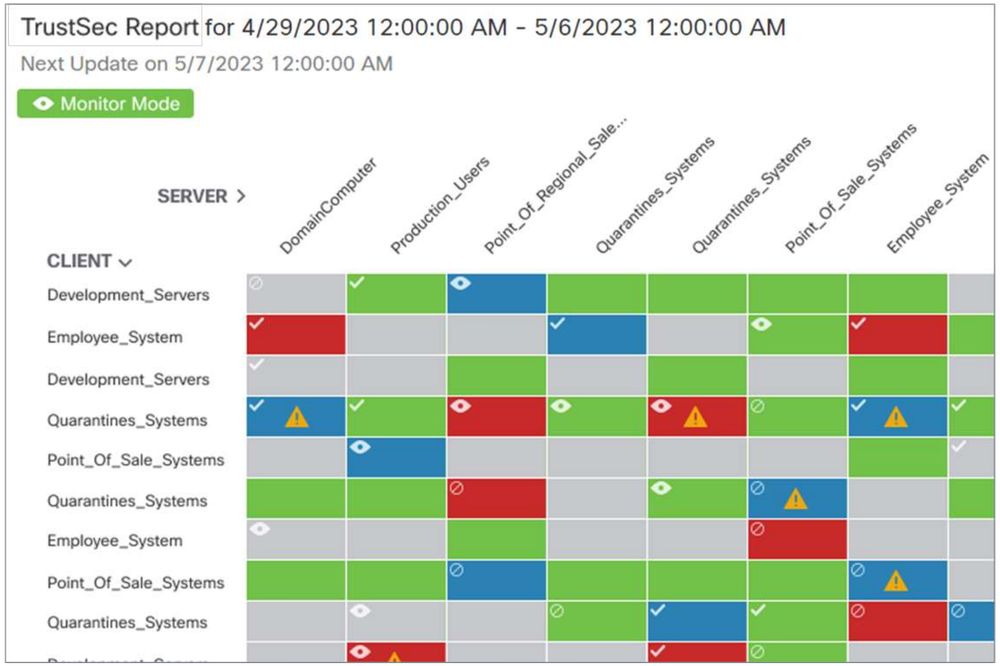
TrustSec Analytics

View traffic volume between Security Group Tags (SGTs) and gain insights into exact application flows between SGTs.

TrustSec Policy Analytics

View policy compliance, including possible violations of the ISE TrustSec policy, for selected security groups based on observed traffic analytics.

90 days of historical policy data

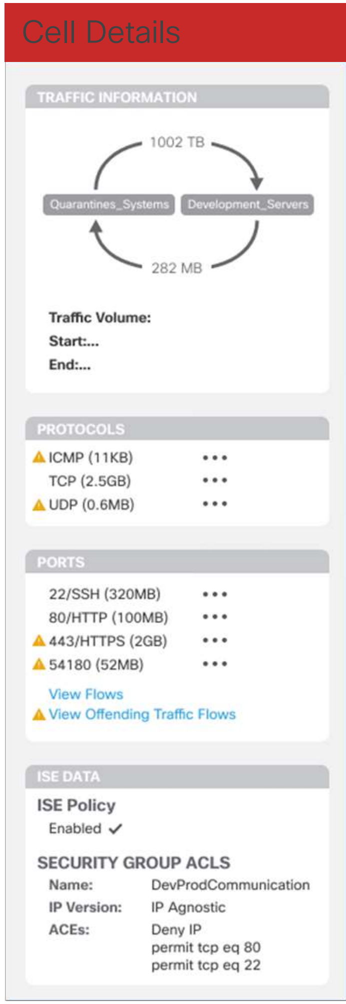


TrustSec Report for 4/29/2023 12:00:00 AM - 5/6/2023 12:00:00 AM

Next Update on 5/7/2023 12:00:00 AM

Monitor Mode

CLIENT ⌄ \ SERVER ›	DomainComputer	Production_Users	Point_Of_Regional_Sale...	Quarantines_Systems	Quarantines_Systems	Point_Of_Sale_Systems	Employee_System	
Development_Servers	⬜ ⊘	🟩 ✓	🟦 👁	🟩	🟩	🟩	🟩	⬜
Employee_System	🟥 ✓	⬜	⬜	🟦 ✓	⬜	🟩 👁	🟥 ✓	🟩
Development_Servers	⬜ ✓	⬜	🟩	⬜	🟩	⬜	🟩	⬜
Quarantines_Systems	🟦 ✓ ⚠	🟩 ✓	🟥 👁	🟩 👁	🟥 👁 ⚠	🟩 ⊘	🟦 ✓ ⚠	🟩 ✓
Point_Of_Sale_Systems	⬜	🟦 👁	⬜	⬜	⬜	⬜	🟩	⬜ ✓
Quarantines_Systems	🟩	🟩	🟥 ⊘	⬜	🟩 👁	🟦 ⊘ ⚠	⬜	🟩
Employee_System	⬜ 👁	⬜	🟩	⬜	⬜	🟥 ⊘	⬜	⬜
Point_Of_Sale_Systems	🟩	🟩	🟦 ⊘	🟩	🟩	🟩	🟦 ⊘ ⚠	⬜
Quarantines_Systems	⬜	⬜ 👁	⬜	🟩 ⊘	🟦 ✓	🟩 ✓	🟥 ⊘	🟦 ⊘
Development_Servers	⬜	🟥 👁 ⚠	⬜	⬜	🟥 ✓	🟩 ⊘	⬜	⬜



Cell Details

TRAFFIC INFORMATION

Traffic Volume:
Start:...
End:...

PROTOCOLS

⚠ ICMP (11KB)	•••
TCP (2.5GB)	•••
⚠ UDP (0.6MB)	•••

PORTS

22/SSH (320MB)	•••
80/HTTP (100MB)	•••
⚠ 443/HTTPS (2GB)	•••
⚠ 54180 (52MB)	•••

View Flows
⚠ View Offending Traffic Flows

ISE DATA

ISE Policy
Enabled ✓

SECURITY GROUP ACLS

Name:	DevProdCommunication
IP Version:	IP Agnostic
ACEs:	Deny IP permit tcp eq 80 permit tcp eq 22

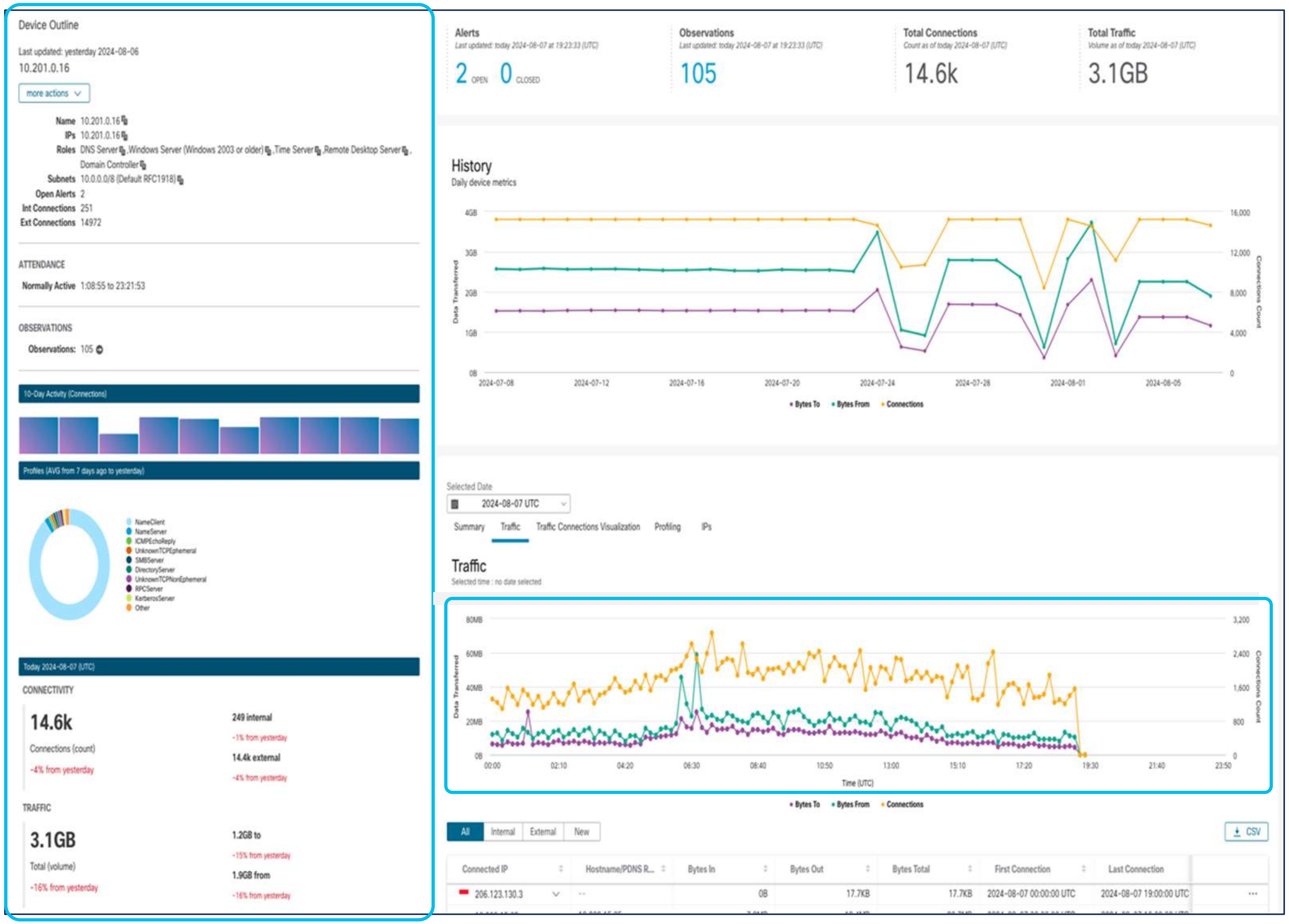
Naturally extend investigations with device context and trends

Device Outline provides:

- Name, IP, roles, subnet, open Alerts, internal and external connections for the device
- Normally active period displayed
- Observations for the device
- 10 Day Activity Connections Graph
- Connectivity and traffic activity seen for the device for the current day

Traffic Report provides:

- Select any time on the traffic statistics graph and see results dynamically filtered in the flow table
- Accelerates investigation of traffic anomalies
- Immediately correlates chart events with actual flows attributing to the event



Device Outline

Last updated: yesterday 2024-08-06

10.201.0.16

Name	10.201.0.16
IPs	10.201.0.16
Roles	DNS Server, Windows Server (Windows 2003 or older), Time Server, Remote Desktop Server, Domain Controller
Subnets	10.0.0.0/8 (Default RFC1918)
Open Alerts	2
Int Connections	251
Ext Connections	14972

ATTENDANCE

Normally Active 1:08:55 to 23:21:53

OBSERVATIONS

Observations: 105

Today 2024-08-07 (UTC)

CONNECTIVITY

14.6k Connections (count) -4% from yesterday

249 internal -1% from yesterday

14.4k external -4% from yesterday

TRAFFIC

3.1GB Total (volume) -16% from yesterday

1.2GB to -15% from yesterday

1.9GB from -16% from yesterday

Alerts
Last updated: today 2024-08-07 at 19:23:33 (UTC)
2 OPEN 0 CLOSED

Observations
Last updated: today 2024-08-07 at 19:23:33 (UTC)
105

Total Connections
Count as of today 2024-08-07 (UTC)
14.6k

Total Traffic
Volume as of today 2024-08-07 (UTC)
3.1GB

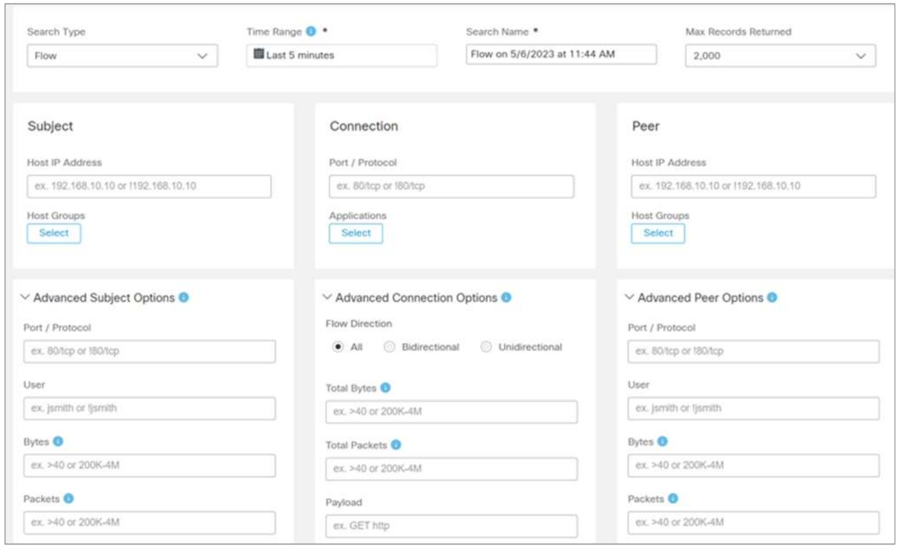
History
Daily device metrics

Selected Date
2024-08-07 UTC

Traffic
Selected time : no date selected

Connected IP	Hostname/PDNS R...	Bytes In	Bytes Out	Bytes Total	First Connection	Last Connection
206.123.130.3	--	0B	17.7KB	17.7KB	2024-08-07 00:00:00 UTC	2024-08-07 19:00:00 UTC

Investigate with flow searches and host reports



Search Type: Flow

Time Range *: Last 5 minutes

Search Name *: Flow on 5/6/2023 at 11:44 AM

Max Records Returned: 2,000

Subject

Host IP Address: ex. 192.168.10.10 or !192.168.10.10

Host Groups: Select

Connection

Port / Protocol: ex. 80/tcp or !80/tcp

Applications: Select

Peer

Host IP Address: ex. 192.168.10.10 or !192.168.10.10

Host Groups: Select

Advanced Subject Options

Port / Protocol: ex. 80/tcp or !80/tcp

User: ex. jsmith or !jsmith

Bytes: ex. >40 or 200K-4M

Packets: ex. >40 or 200K-4M

Advanced Connection Options

Flow Direction: ● All ○ Bidirectional ○ Unidirectional

Total Bytes: ex. >40 or 200K-4M

Total Packets: ex. >40 or 200K-4M

Payload: ex. GET http

Advanced Peer Options

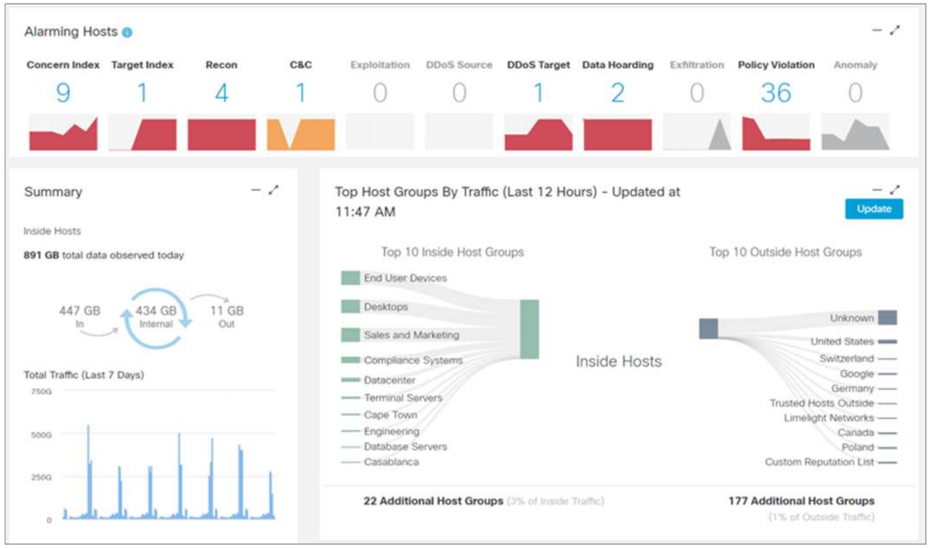
Port / Protocol: ex. 80/tcp or !80/tcp

User: ex. jsmith or !jsmith

Bytes: ex. >40 or 200K-4M

Packets: ex. >40 or 200K-4M

- Common search parameters via Basic search
- Search parameters are organized by subject, host and peer within Advanced search
- Identify/search based on user, device, segmentation identity



Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
9	1	4	1	0	0	1	2	0	36	0

Summary

Inside Hosts

891 GB total data observed today

Top Host Groups By Traffic (Last 12 Hours) - Updated at 11:47 AM

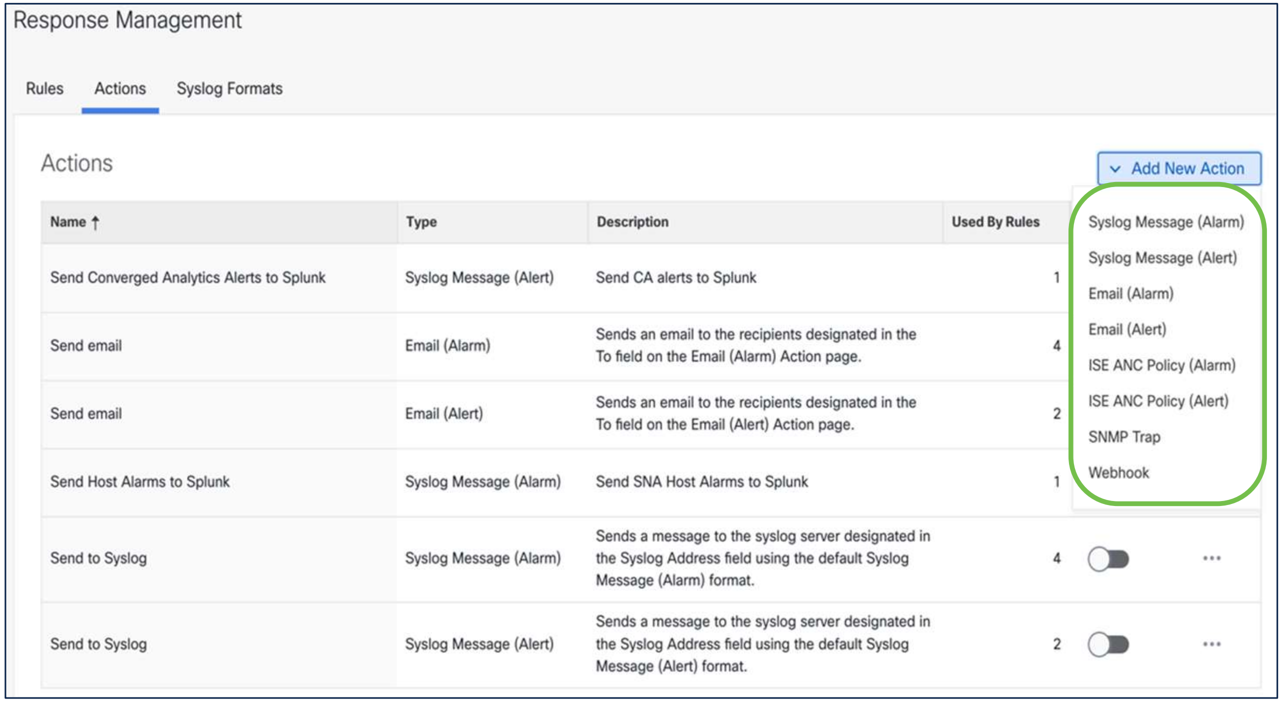
22 Additional Host Groups (3% of Inside Traffic)

177 Additional Host Groups (1% of Outside Traffic)

- Focus investigation on top host alarming severity throughout the kill chain
- Visualize groups communications throughout organization
- Understand why alarms are triggered and see violated policies and threshold values

Native response automation and alert sharing

- Use webhooks to enhance data-sharing with third-party tools adding unparalleled flexibility in response management
- Send malware detections to XDR furthering forensic investigations
- Limit an endpoint’s network access as detections occur combining Adaptive Network Control (ANC) and Identity Services.
- Send detections to SIEMs



Response Management

Actions

Name ↑	Type	Description	Used By Rules
Send Converged Analytics Alerts to Splunk	Syslog Message (Alert)	Send CA alerts to Splunk	1
Send email	Email (Alarm)	Sends an email to the recipients designated in the To field on the Email (Alarm) Action page.	4
Send email	Email (Alert)	Sends an email to the recipients designated in the To field on the Email (Alert) Action page.	2
Send Host Alarms to Splunk	Syslog Message (Alarm)	Send SNA Host Alarms to Splunk	1
Send to Syslog	Syslog Message (Alarm)	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message (Alarm) format.	4
Send to Syslog	Syslog Message (Alert)	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message (Alert) format.	2

Fully Automated Responses

Identity Services

XDR

SIEMs

Integration NDR with XDR

Cross correlation of data

Correlation of NDR findings with other detections mechanisms including EDR based detections, email and others

Impact Analysis

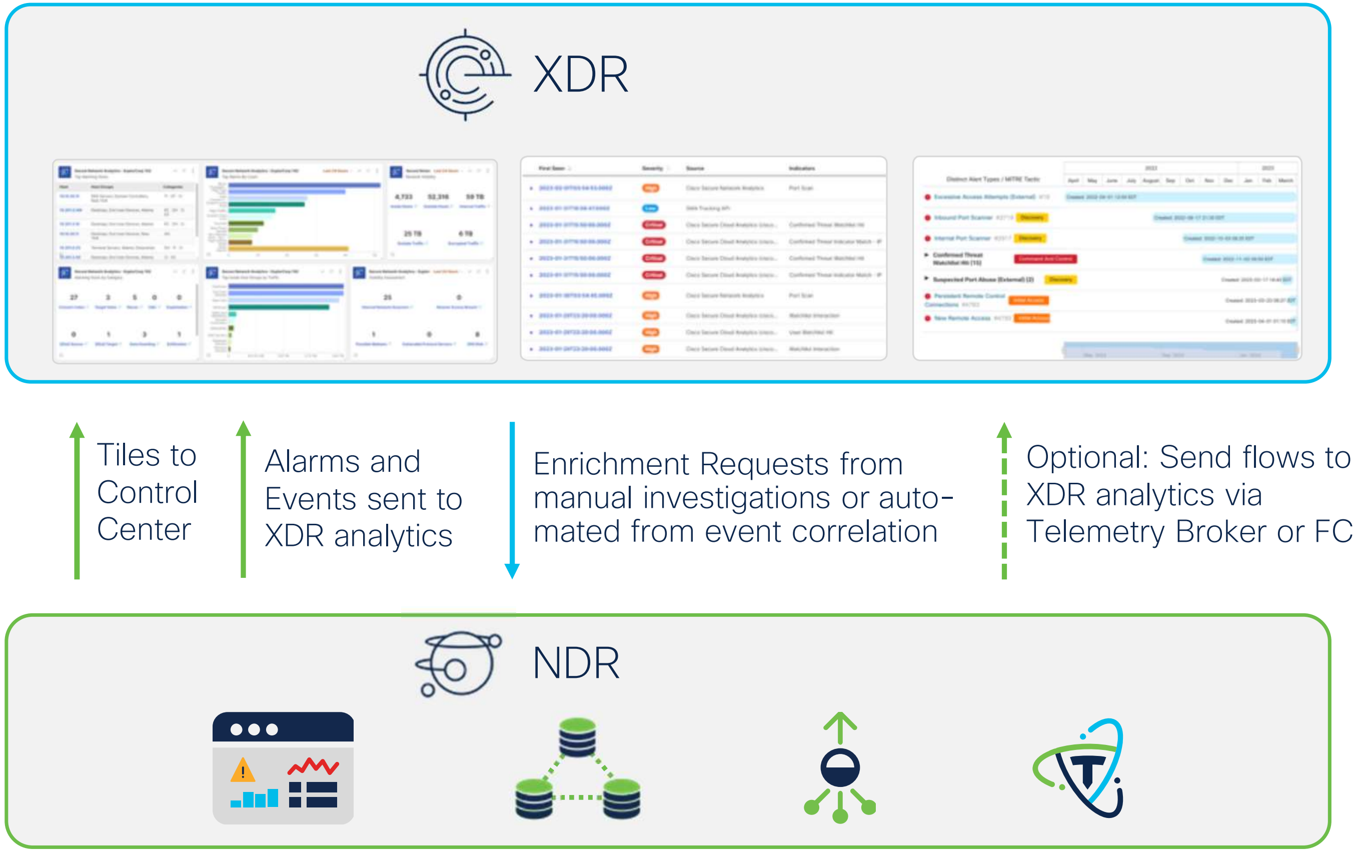
Understand the Impact of an incident leveraging XDR incident Manager

Reduce the time to respond

Reducing the time to response leveraging XDR automation and the multi responses capabilities

Extend response capability

Expand NDR response capabilities with multiple technologies through XDR integrations

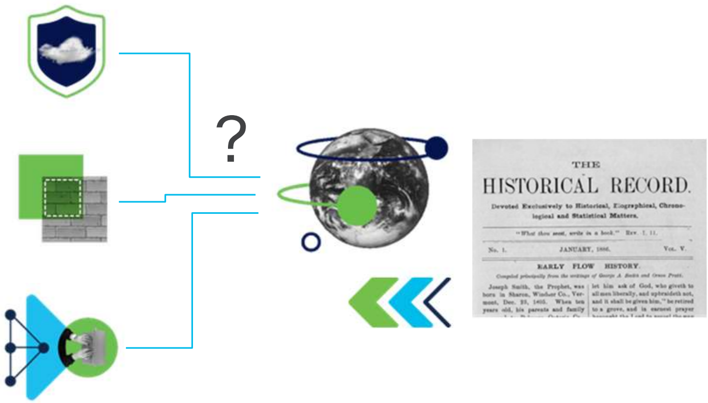


XDR
Tiles to Control Center
Alarms and Events sent to XDR analytics
Enrichment Requests from manual investigations or auto-mated from event correlation
Optional: Send flows to XDR analytics via Telemetry Broker or FC
NDR

NDR Capabilities needed for XDR Outcomes

- Response & Automation
  - Respond to a threat using pre-configured actions.
  - Provide manual and automated actions for blocking C&C communication across all your environment
  - Isolate infect system to prevent additional malware spreading

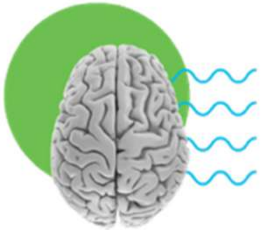
- Historical Investigations
  - Find historical communication with bad destinations prior to conviction
  - Gather a device communication trends before during and after an infection to identify additional artifacts and indicators
  - Detect malware lateral movement by looking at historical communication



NDR Network Detection and Response system recap

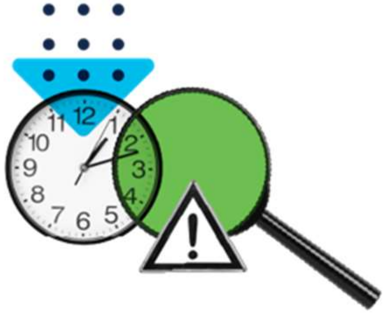
Contextual network-wide visibility

Agentless, using existing network and cloud infrastructure, even in encrypted traffic



Predictive threat analytics

Combination of behavioral modeling, machine learning analytics



Automated detection and response

High-fidelity alerts prioritized by threat severity with ability to conduct forensic analysis