

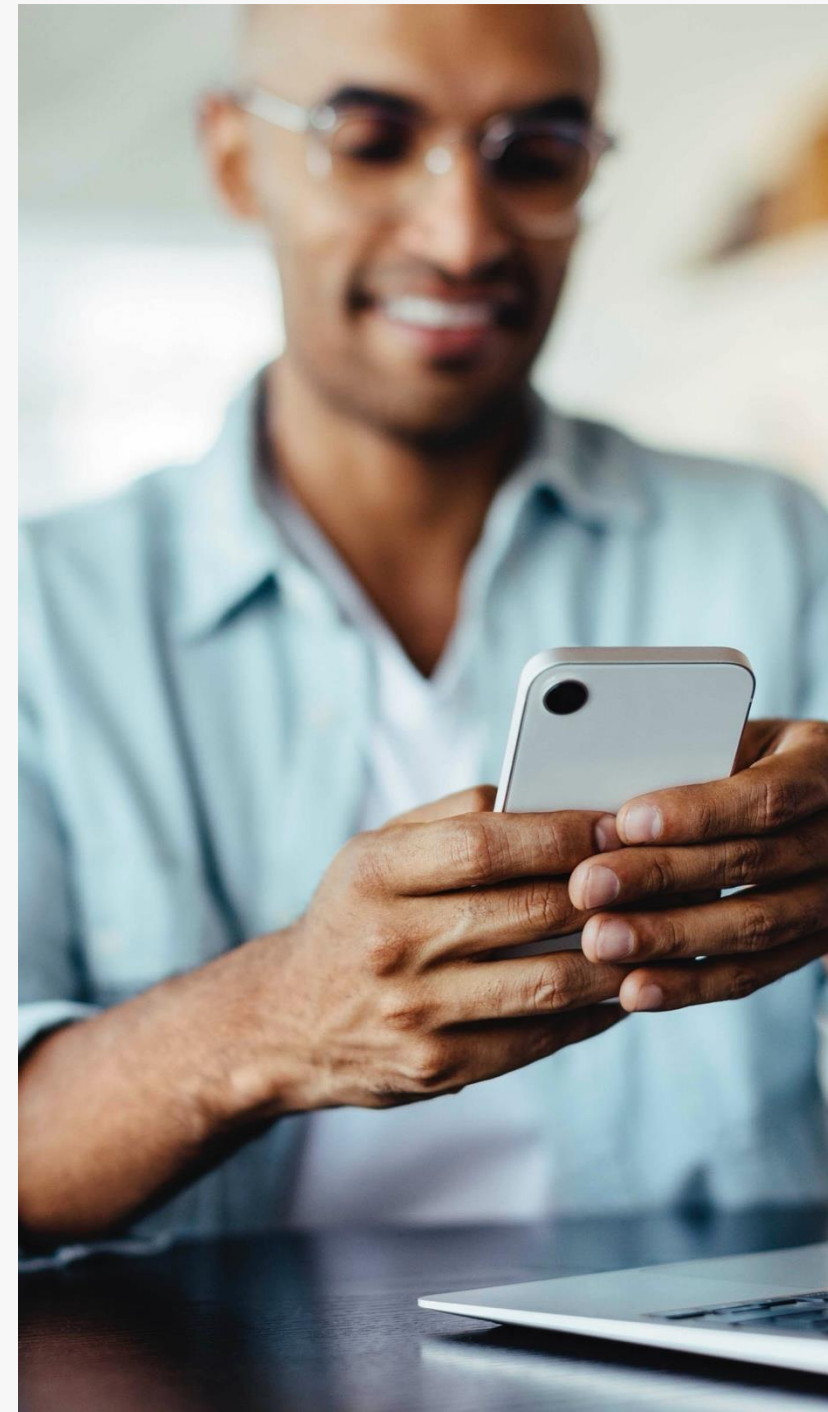


Secure Network Analytics

Tech Club

Vlastimil Menčík (vmencik@cisco.com)
Software Engineering Technical Leader

15.10.2024



Agenda

- 1 Overview
- 2 Network
- 3 Detections
- 4 Investigate & Respond
- 5 Secure Network Analytics and Splunk

Overview



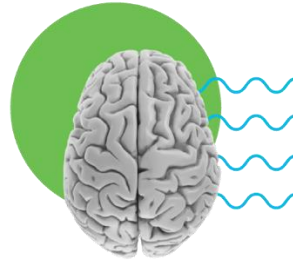
Cisco Secure Network Analytics

Network Detection and Response



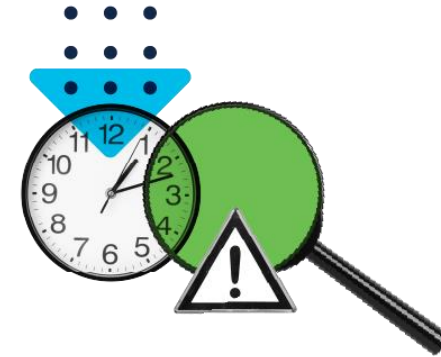
Contextual network-wide visibility

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



Predictive threat analytics

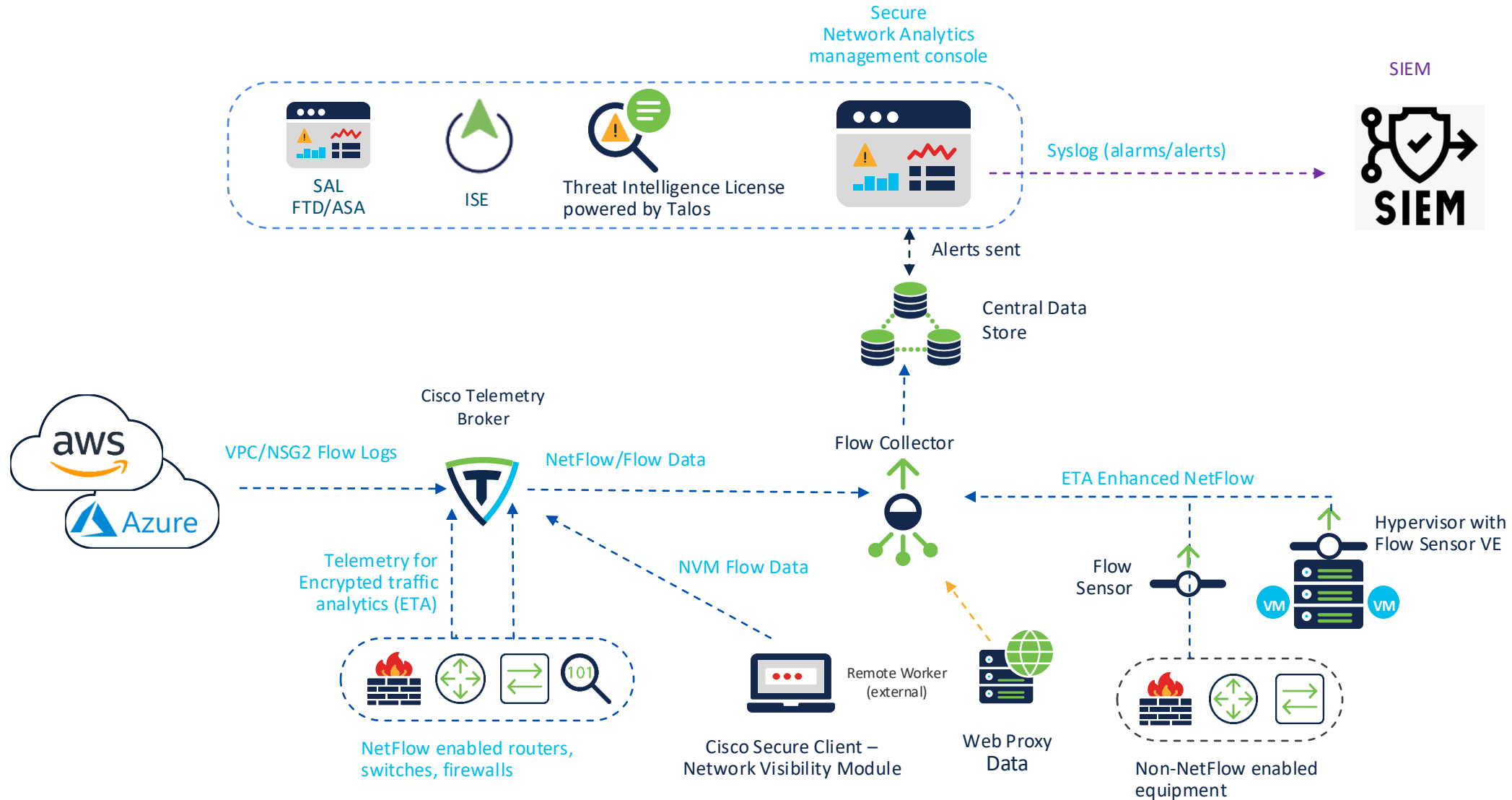
Combination of behavioral modeling, machine learning and global threat intelligence



Automated detection and response

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

Secure Network Analytics Architecture



Required core components

Secure Network Analytics manager

- A physical or virtual appliance that aggregates, organizes, and presents analysis from flow collectors
- Central management for all Secure Network Analytics devices
- User interface to Secure Network Analytics
- Maximum 2 per deployment

Flow collector (FC)

- A physical or virtual appliance that aggregates, normalizes and analyze telemetry and application data collected from exporters such as routers, switches, and firewalls
- High performance NetFlow/SFlow/IPFIX collector
- Maximum 25 per deployment

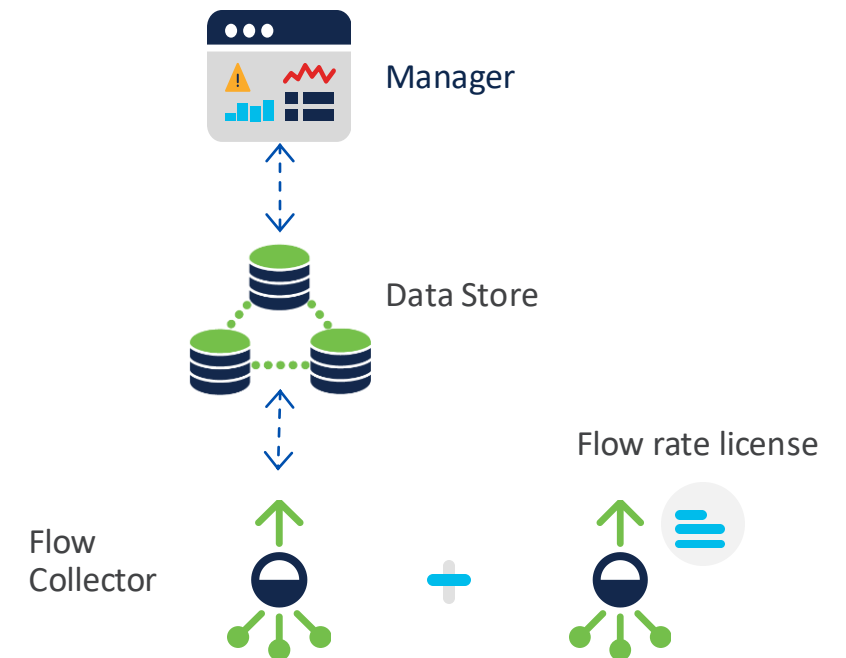
Data Store (DS)

- A physical or virtual appliance that store data in a scalable, resilient way.
- Maximum of 36 data nodes.

Flow rate license

- Collection, management, and analysis of telemetry by Secure Network Analytics
- The flow rate license is simply determined by the number/type of switches, routers, firewalls and probes present on the network
- FPS estimation Tool: <https://apps.cisco.com/cfgon/public/app/lancope/fpsestimator.jsp#/add-items>

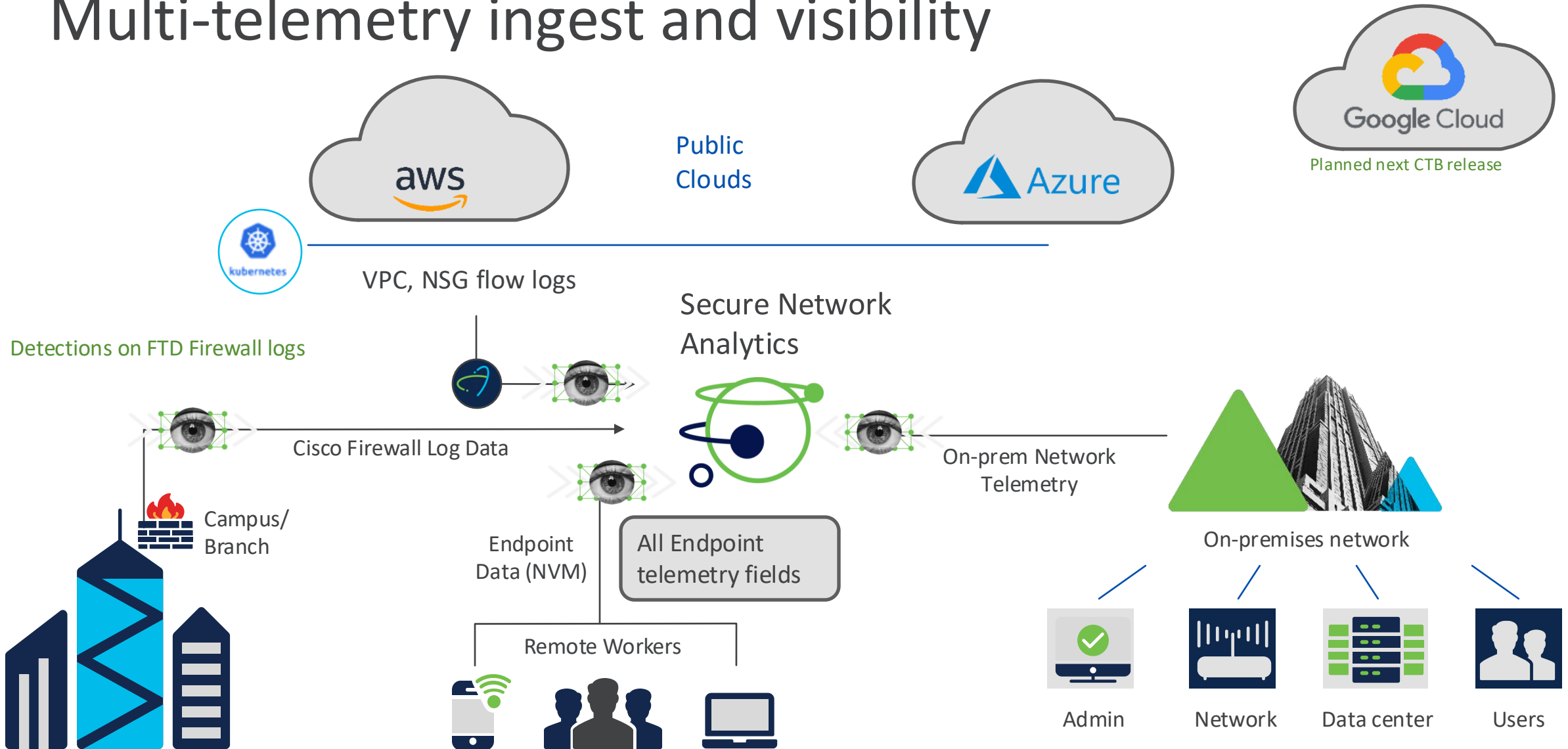
Secure Network Analytics Deployment



Network-wide visibility

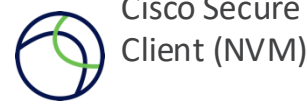


Multi-telemetry ingest and visibility



Extensible Telemetry Ingest

NetFlow Enabled Devices



SRC/DST IP Address
SRC/DST Port
Bytes/Pkts Sent
Bytes/Pkts Received
...
(NetFlow, IPFIX)

L7 Application
HTTP Requests
HTTP Responses
SRT/RTT
TCP Flags
Payload

Flow Action
Translated Port/IP
SYSLOG
Connections
Malware events
File events
Hardware events

TLS Version
Key Exchange
Authentication
Alg. MAC

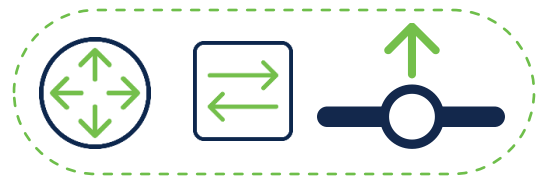
VPC & NSG
flow log
transformation
via CTB

Process name
Process hash
Process account
Parent process name
Parent process hash
OS Version
Connected interface
...

Username
MAC Address
TrustSec Groups
OS Type

HTTP(S) Requests
HTTP(S) Responses
HTTP(S) URL
Custom HTTP(S)
Headers
Username

Host
Groups



Identity
Services
Engine



AHGA/
ADC*



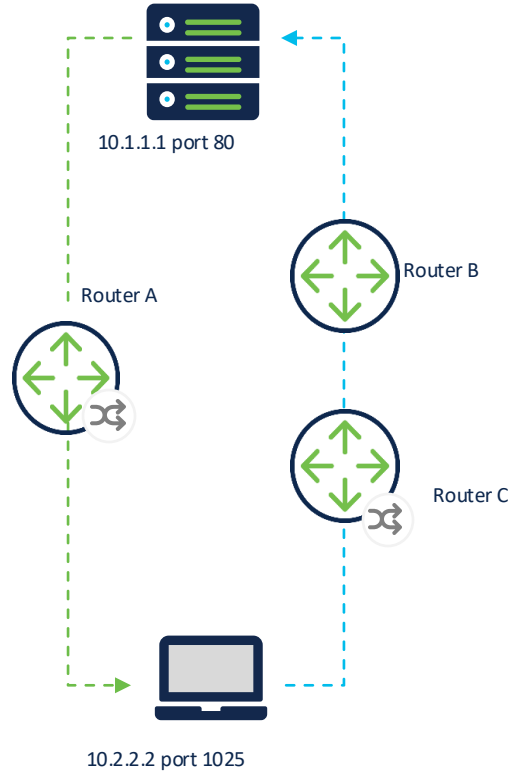
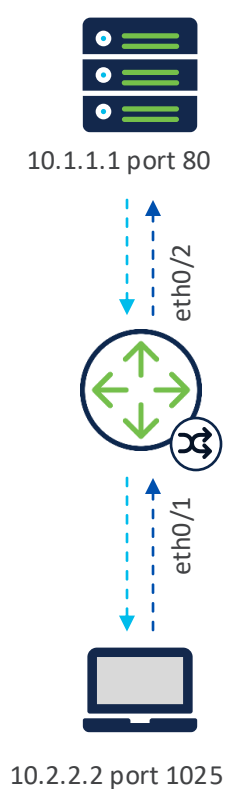
IPAM DB

Network
Telemetry

Threat
Intel



Telemetry processing: end-to-end sessions



Data Deduplication and Stitching

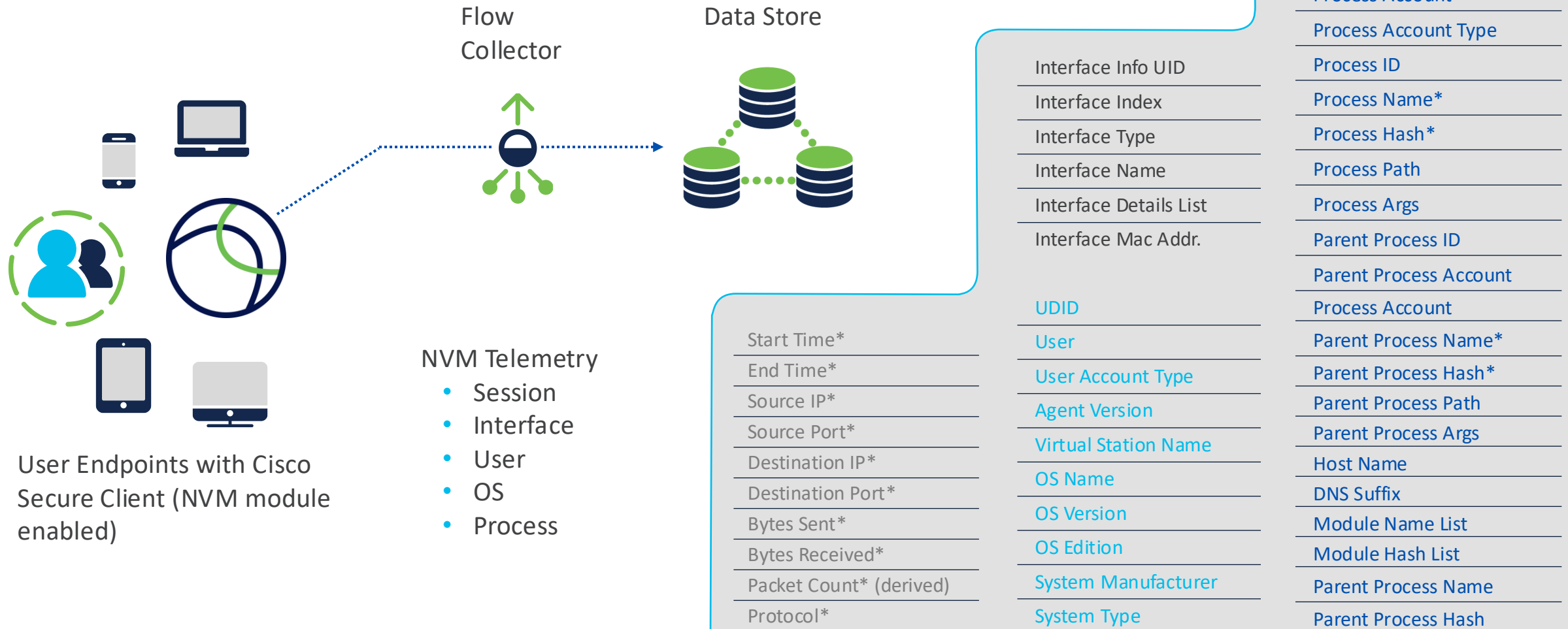
- Symmetric and Asymmetric flow stitching
- From Data to Session information
- Enable efficient storage of telemetry data
- Necessary for accurate host-level reporting
- No data is discarded:
Unique data elements are written into the data base

Bidirectional telemetry record

Start time	Client IP	Client port	Server IP	Server port	Proto	Client bytes	Client Pkts	Server bytes	Server Pkts	Interfaces
10:20:12.221	10.2.2.2	1025	10.1.1.1	80	TCP	2027	5	28712	17	eth0/1 eth0/2

Endpoint Network: NVM telemetry records retained

**No longer need to purchase an Endpoint license for NVM telemetry starting with 7.5.1. NVM traffic is now included along with NetFlow when calculating Flow Rate (FPS) licensing requirements.



* NVM telemetry records available within non-Data Store deployments

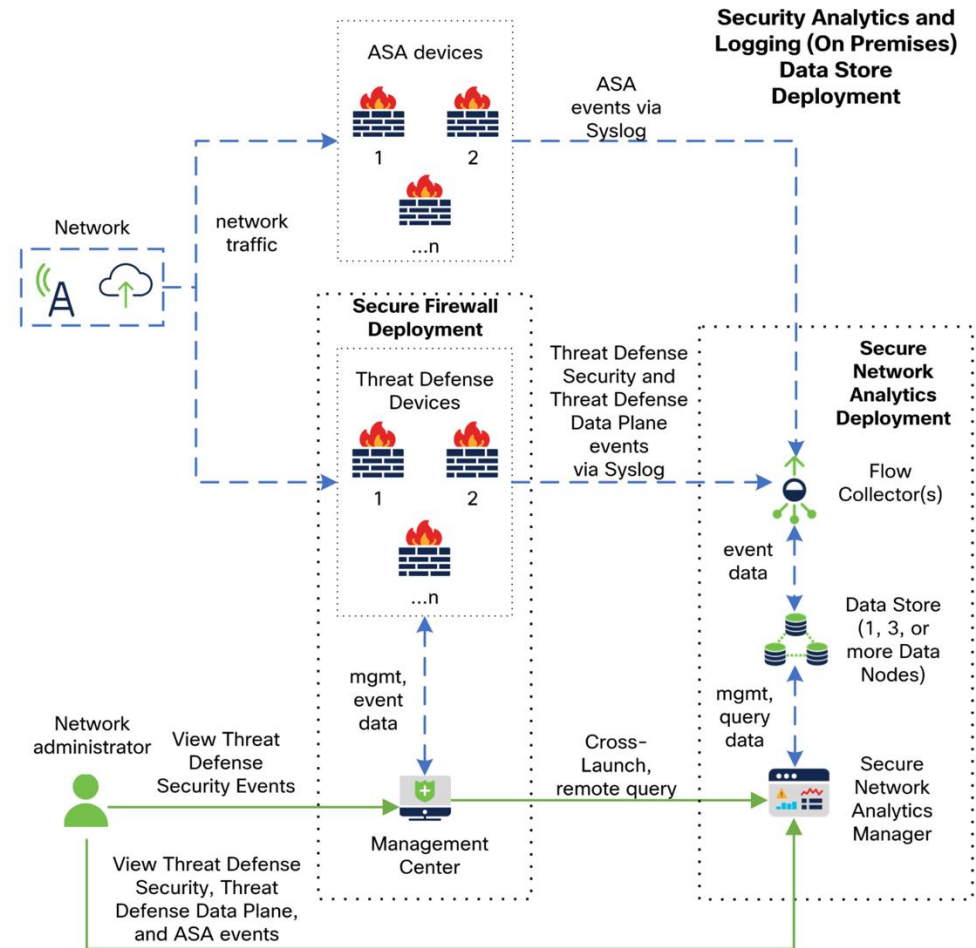
FMC logging integration with Secure Network Analytics

Longer Event Retention and increased scale

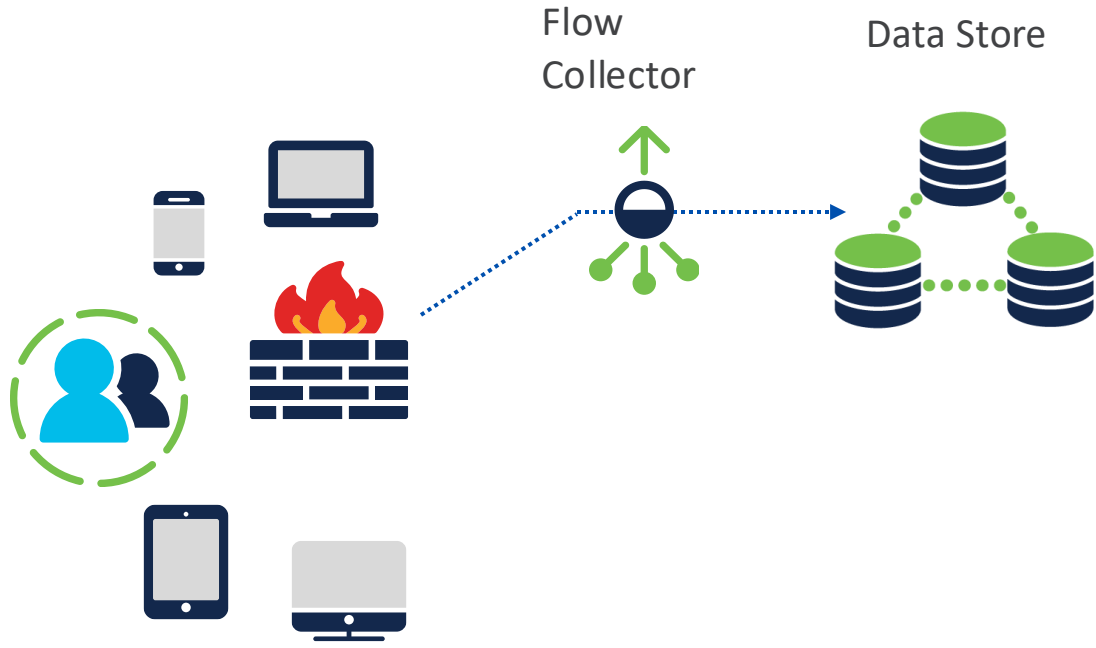
- External Storage via Secure Network Analytics
- Auto select event source or manually specify
- Multiple Flow Collectors as event destinations

Easy button for setup

- Setup FMC analytics direct launch links to the Secure Analytics console
- Setup remote query credentials from Secure Analytics datastore



Additional Firewall Fields Retained



31 New fields ingested, stored & visible in 7.5.1

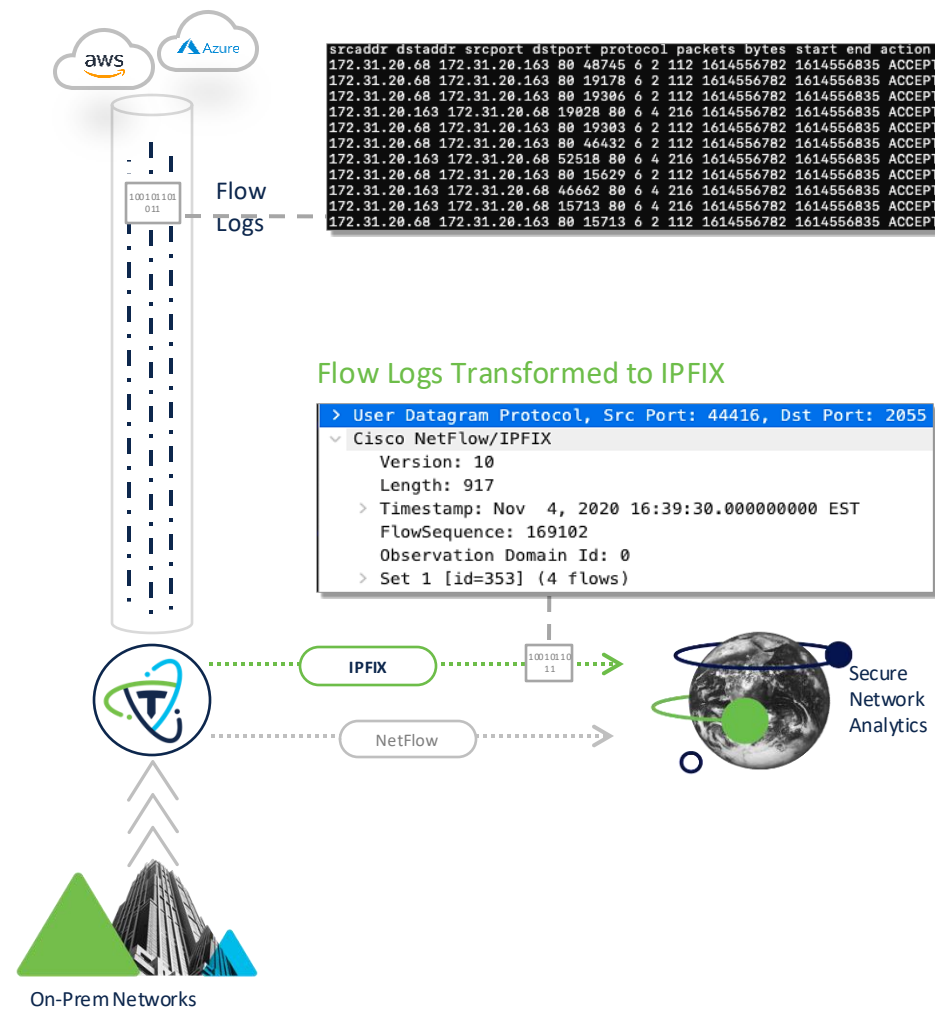
The screenshot shows the 'Investigate' section of the Cisco Secure Network Analytics interface. The left sidebar contains navigation options: ExplorCorp, Monitor, Investigate (highlighted with a blue box), Report, Configure, and Apps. The main content area lists several search and management options: Flow Search, Host Search, Copyright Infringement, Security Analytics and Logging (OnPrem) (highlighted with a blue box and a checkmark), Search Management, Job Management, Saved Searches, Saved Results, Assets, Hosts, and Host Groups.

The 'Show/Hide Columns' window displays a list of 31 fields, each with a checked checkbox. A red box highlights the first 31 items in the list. A blue line connects the 'Security Analytics and Logging (OnPrem)' option in the main interface to this list.

- Authentication Source
- Client App Detector
- Decrypt Peer IP
- Encrypt Peer IP
- Enrichment Data Json
- EVE Process Confidence Score
- EVE Process Name
- EVE Threat Confidence
- EVE Threat Confidence Score
- HTTP Hostname
- HTTP URI
- Mitre Attack Groups
- Mitre Enrichment
- NAT Initiator IP
- NAT Initiator Port
- NAT Responder IP
- NAT Responder Port
- Original Client Source IP
- Other Enrichment
- SMTP Attachments
- SMTP From
- SMTP Headers
- SMTP To
- Snort Rule Groups
- Threat Name
- TLS SNI
- User Name
- VPN Action
- Zero Trust Application
- Zero Trust Application Group
- Zero Trust Application Policy

Monitoring 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



Functional network segmentation by groups

Inside



DNS servers



Employee



Web servers



Guest wireless



Anti virus servers



Printers

Outside



Cloud



Partners



Internet

A host group is grouping of hosts that share attributes and policies

Host group are monitored to establish baseline behavior and thresholds

Alerts are sent when hosts behave outside the group behavior

Three Ways to Segment

1. Manual Host Group Creation
2. APIs using IPAM, IND, Threat Intelligence data
3. Host Group Automation Service

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 45ac3217dd8 0fd46c...	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

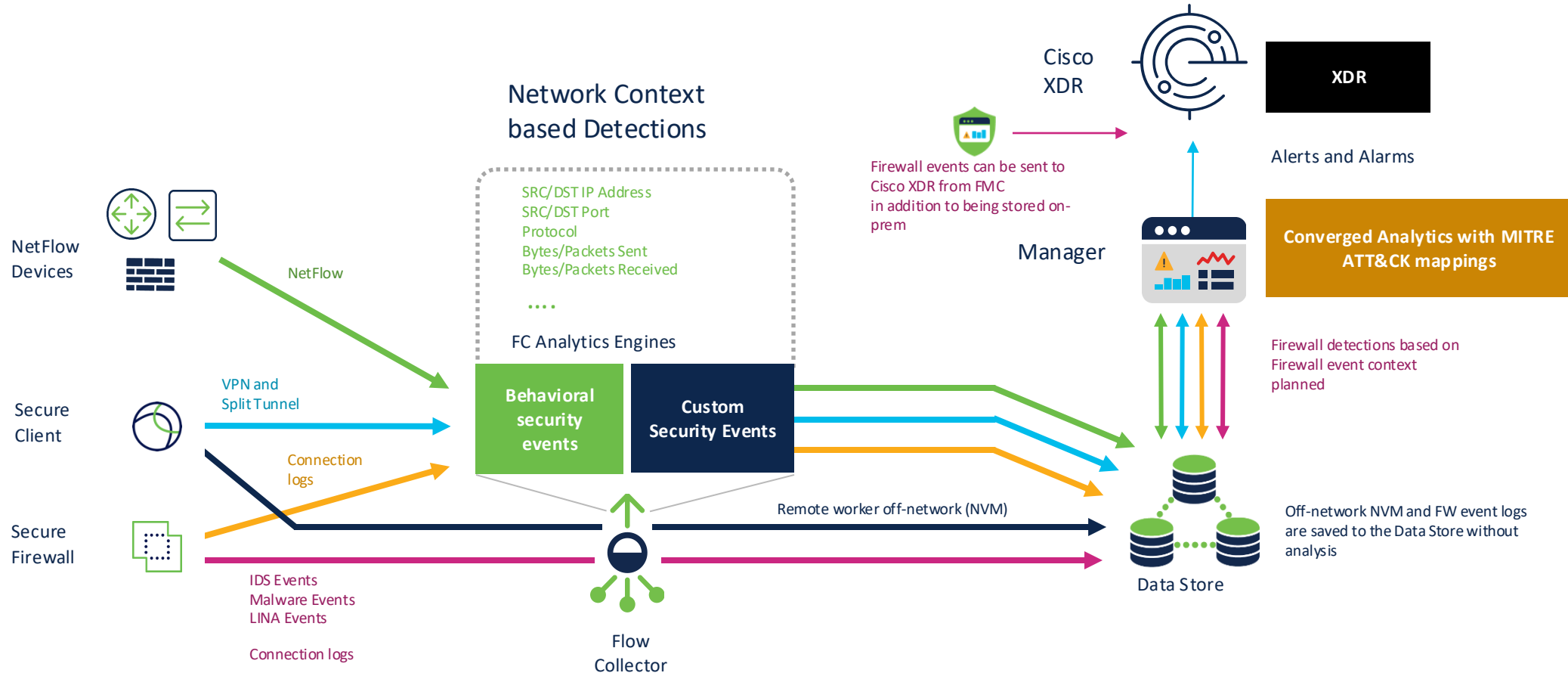


Encrypted traffic analytics

Detections



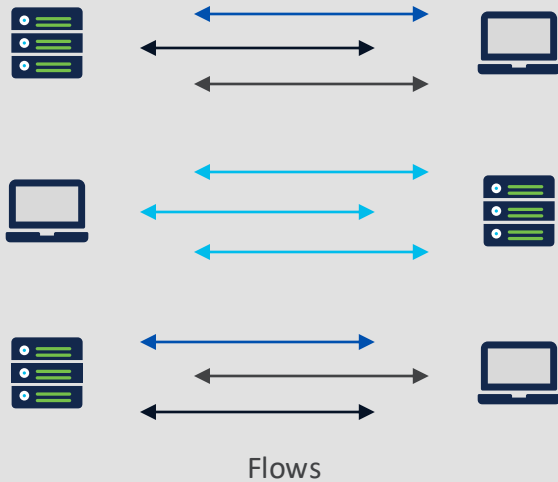
Secure Network Analytics Data Store detection architecture



Anomaly detection using behavioral modeling

Collect and analyze telemetry

Comprehensive data set optimized to remove redundancies



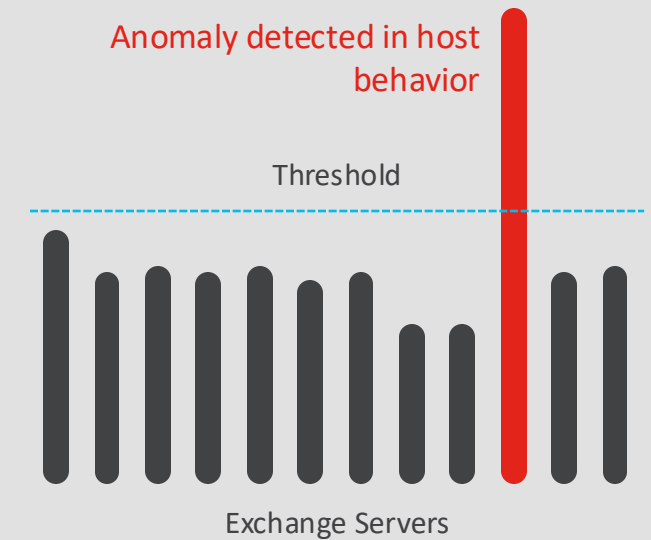
Create a baseline of normal behavior

Security events to detect anomalies and known bad behavior

Security Observations		
Number of concurrent flows	New flows created	Number of SYNs received
Packet per second	Number of SYNs sent	Rate of connection resets
Bits per second	Time of day	Duration of the flow

Alarm on anomalies and behavioral changes

Alarm categories for high-risk, low-noise alerts for faster response



Logical alarms based on suspicious events

Source or target of malicious behavior

Every event contribute to a source and target scores that increase to detect slow and repeated attacks

Reconnaissance

Scanning and network reconnaissance-based detection

Command and Control

URL and IP based detection of communication with C&C Botnet and Tor network

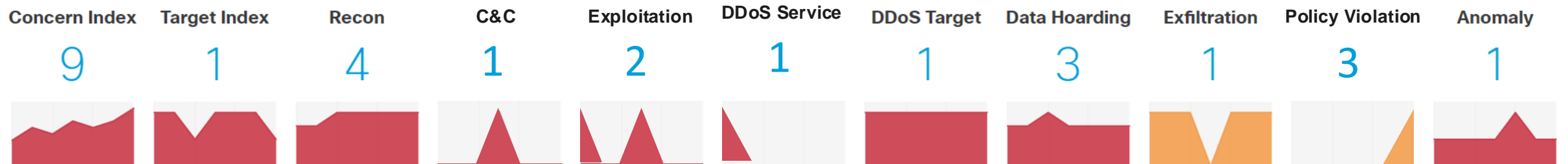
DDoS Activity

Statistical DDoS detection based on baselined traffic analysis

Insider threats

Data movement-based detections laterally and vertically in a network

Alarming Hosts ⓘ



Automated learning & detection with Converged Analytics

48 Network based alerts

- New Remote Access
- LDAP Connection Spike
- Outbound LDAP Spike
- Protocol Forgery
- Repeated Umbrella Sinkhole Communication

2 Telemetry sources

- NetFlow
- Endpoint Network Visibility Module

Alerts mapped to MITRE Tactics and Techniques

Alert Type	MITRE ATT&CK Ta...	MITRE ATT&CK Te...	Observation Types	Telemetry ?
Outbound LDAP Connection Spike Device is communicating with a large number of external hosts using an LDAP port. This may indicate a possible infected host or an internally-initiated port scan.	Reconnaissance	Active Scanning	• IP Scanner	Netflow North-South
Persistent Remote Control Connections Device is receiving persistent connections from a new host on a remote control protocol like Remote Desktop or SSH. This may indicate that a firewall rule or ACL is overly permissive.	Initial Access	External Remote Ser...	• New External Server • Persistent External Server	Netflow North-South
Potential Database Exfiltration A statistically unusual amount of data was transferred from a database server to a client. This may indicate data exfiltration.	Exfiltration	Exfiltration Over Alte...	• New High Throughput Connection	Netflow North-South
Potential Data Exfiltration Device downloaded data from an internal device that it doesn't communicate with regularly. Shortly after that, the device uploaded a similar amount of data to an external device. This may indicate that sensitive data is compromised.	Exfiltration	Automated Exfiltration	• Potential Data Forwarding	East-West Netflow North-South
Protocol Forgery Device was observed running a potentially restricted service (such as SSH) on a non-standard port. This may indicate an evasion of security controls.	Command and Cont...	Non-Standard Port	• Bad Protocol	ETA Netflow North-South

Unlocking the power of MITRE focused cloud first detection development within on-prem deployments

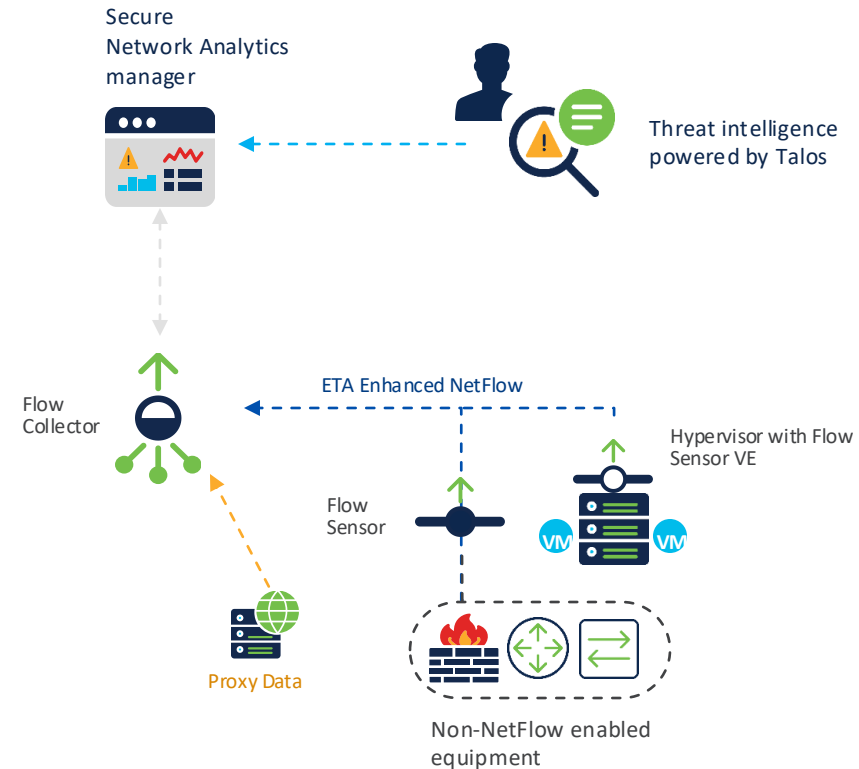
Threat intelligence license powered by



Global threat intelligence

Detects connections to:

- Bogons
- Known C&C
- Tor entry & exit nodes
- Talos IP block list (once a day)
- Automatic periodic updates from Cisco Cloud
- Polls every half hour



Investigate and Respond



Detected Alarms tied to entities

Quick snapshot of malicious activity

Suspicious behavior linked to logical alarms

Risks prioritized to take immediate action

Alarming Hosts i

Concern Index

4

Target Index

2

Recon

4

Top Alarming Hosts

Host	Category
10.201.3.149 ... End User Devices	<div style="display: flex; flex-wrap: wrap; gap: 5px;"> DH CI RC AN EX </div>
10.10.30.11 ... End User Devices	<div style="display: flex; flex-wrap: wrap; gap: 5px;"> AN </div>
10.201.3.18 ... End User Devices	<div style="display: flex; flex-wrap: wrap; gap: 5px;"> DH RC CI AN </div>

The screenshot shows the 'Security Insight Dashboard | Inside Hosts' interface. At the top, there's a navigation bar with 'Host' search and 'Admin User' profile. Below the dashboard title, there's a 'Alarming Hosts' section with a row of metrics: Concern Index (4), Target Index (2), Recon (4), C&C (0), Exploitation (3), DDoS Source (0), DDoS Target (1), Data Hoarding (3), Exfiltration (1), Policy Violation (0), and Anomaly (5). Each metric has a small bar chart. Below this is a 'Top Alarming Hosts' table with columns for Host and Category. The table lists several hosts with their categories (e.g., End User Devices, Terminal Servers). To the right, there are two charts: 'Alarms by Type' (a stacked bar chart showing event counts over time) and 'Today's Alarms' (a donut chart showing the distribution of various alarm types like Packet Flood, High Volume Email, etc.).

Host Report

Host Summary

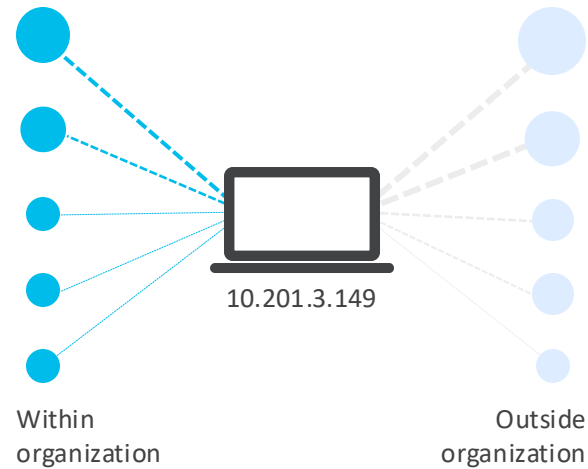


Flows Classify History

Status: Active
Hostname: --
Host Groups: End User Devices,Desktops,Atlanta,Sales and Marketing
Location: RFC 1918
First Seen: 6/7/24 9:34 AM
Last Seen: 8/16/24 9:34 AM
Policies: Insider Threat Event (10.201.3.149),Client IP Policy,Inside
MAC Address: --

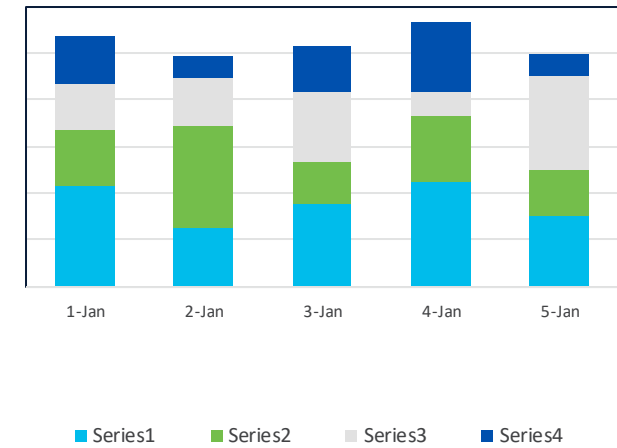
Summary of aggregated host information

Traffic by peer host group



Observed communication patterns

Alarms by Type

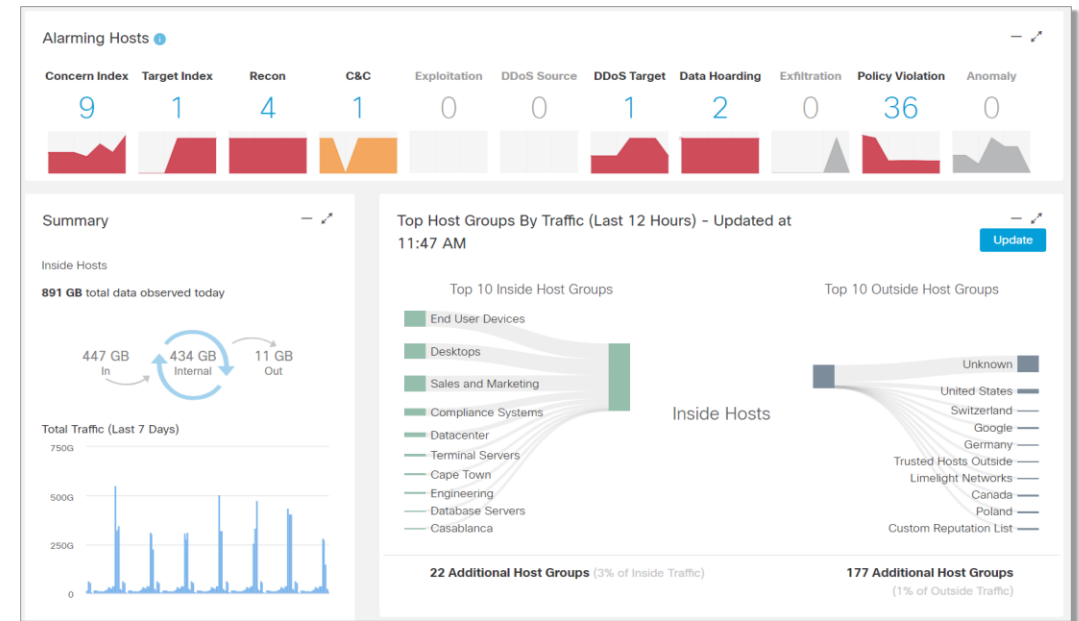


Historical alarming behavior

Investigate with Flow searches and Host Group reports

The screenshot displays the Cisco Flow search interface. At the top, there are search parameters: Search Type (Flow), Time Range (Last 5 minutes), Search Name (Flow on 5/6/2023 at 11:44 AM), and Max Records Returned (2,000). Below this, the interface is organized into three main sections: Subject, Connection, and Peer. Each section has a basic search field and an advanced search section. The Subject section includes Host IP Address, Host Groups, and Advanced Subject Options (Port / Protocol, User, Bytes, Packets). The Connection section includes Port / Protocol, Applications, Flow Direction (All, Bidirectional, Unidirectional), Total Bytes, Total Packets, and Payload. The Peer section includes Host IP Address, Host Groups, and Advanced Peer Options (Port / Protocol, User, Bytes, Packets).

- 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



- 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
- Limit an endpoint's network access as detections occur combining Adaptive Network Control (ANC) and Cisco ISE.
- Send detections to SIEMs using configurable Syslog messages.

Response Management

Rules Actions Syslog Formats

Actions

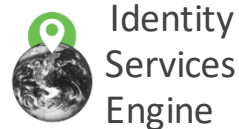
[Add New Action](#)

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	<input type="checkbox"/> ...
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	<input type="checkbox"/> ...

▼ Add New Action

- Syslog Message (Alarm)
- Syslog Message (Alert)
- Email (Alarm)
- Email (Alert)
- ISE ANC Policy (Alarm)
- ISE ANC Policy (Alert)
- SNMP Trap
- Webhook

Fully Automated Responses



Cisco XDR

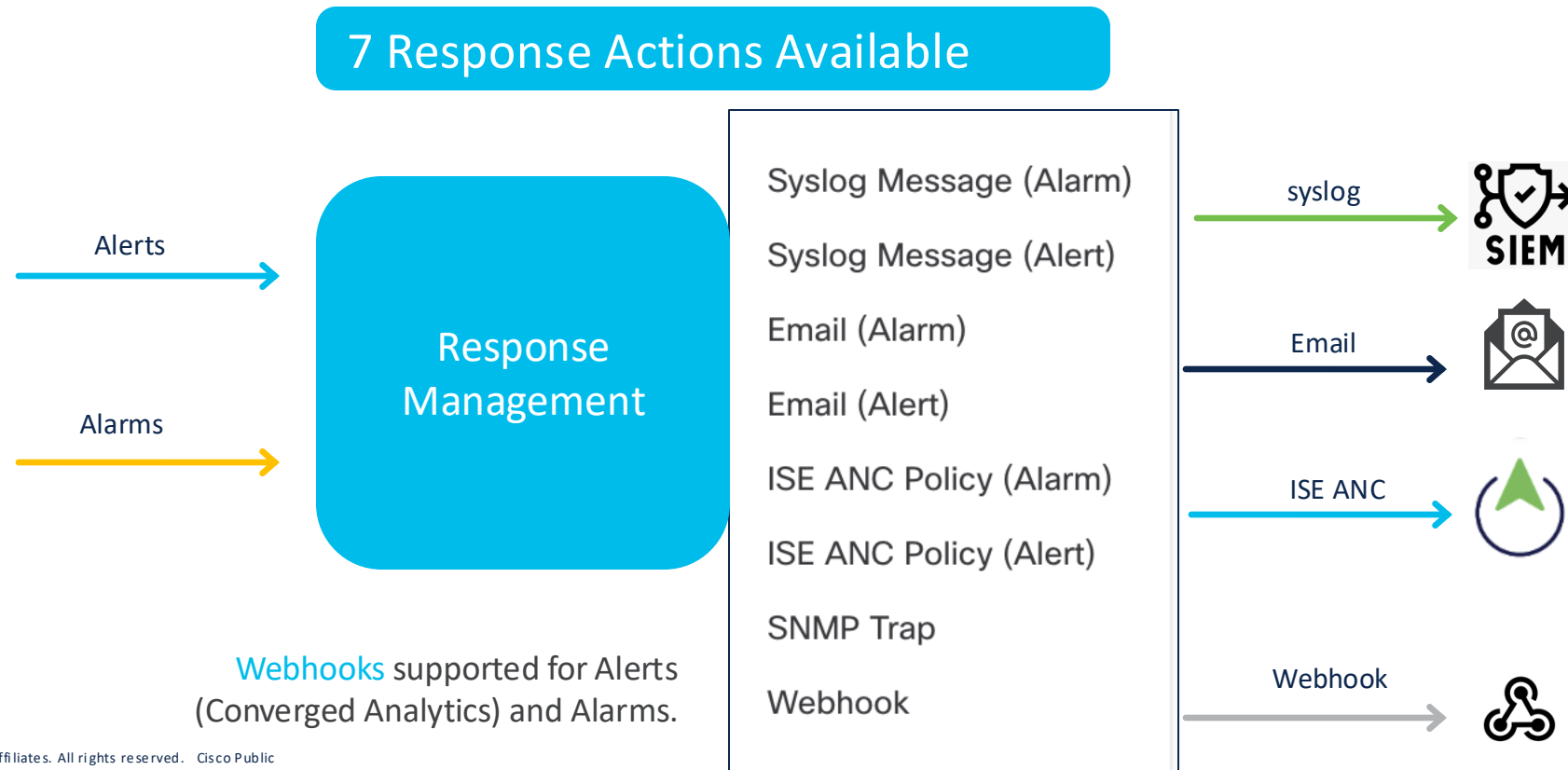


servicenow™

SIEMs

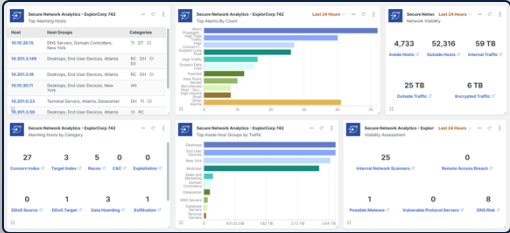
Response Automation Actions

- Response Management is one of the key functions within SNA to share Alerts and Alarms with third-party tools adding unparalleled flexibility in response management.
- You can configure several Response Management Actions for Converged Analytics Alerts and Behavioral analytics Alarms.

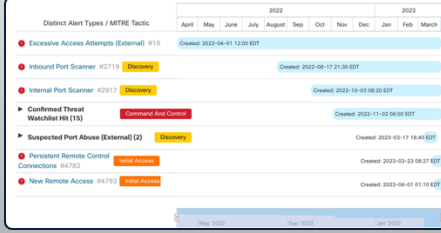


Improving on-prem NDR with Cisco XDR





First Seen	Severity	Source	Indicators
2023-02-01T03:54:53.000Z	Info	Cisco Secure Network Analytics	Port Scan
2023-01-31T16:08:47.000Z	Info	SMA Tracking API	
2023-01-31T15:50:00.000Z	Critical	Cisco Secure Cloud Analytics (Cisco...	Confirmed Threat Watchlist Hit
2023-01-31T15:50:00.000Z	Critical	Cisco Secure Cloud Analytics (Cisco...	Confirmed Threat Indicator Match - IP
2023-01-31T15:50:00.000Z	Critical	Cisco Secure Cloud Analytics (Cisco...	Confirmed Threat Watchlist Hit
2023-01-31T15:50:00.000Z	Critical	Cisco Secure Cloud Analytics (Cisco...	Confirmed Threat Indicator Match - IP
2023-01-30T03:54:45.000Z	Info	Cisco Secure Network Analytics	Port Scan
2023-01-29T23:20:00.000Z	Info	Cisco Secure Cloud Analytics (Cisco...	Watchlist Interaction
2023-01-29T23:20:00.000Z	Info	Cisco Secure Cloud Analytics (Cisco...	User Watchlist Hit
2023-01-29T23:20:00.000Z	Info	Cisco Secure Cloud Analytics (Cisco...	Watchlist Interaction




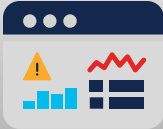



↑ Tiles to Control Center

↑ 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 CTB



Secure Network Analytics + Splunk



SNA and Splunk – Current Use Cases

NDR Detections

SNA detections accessible in Splunk

- NDR detection outcomes published to Splunk via Syslog or Webhooks
- Detections indexed in Splunk for additional investigation and correlation
- Pivot back to NDR for deep investigation
- Configurable sending rules via SNA Response Management
- Reduction in cost vs full log storage in Splunk
- Pivot from NDR (External Lookup) to Splunk for further investigation

SNA Splunk App

SNA Dashboard deployed as an App in Splunk

- Views into NDR data and outcomes from within Splunk
- Uses Splunk Dashboard language
- API based lookups (No Splunk data storage cost)

Data Integration

SNA bi-flow data sent to Splunk

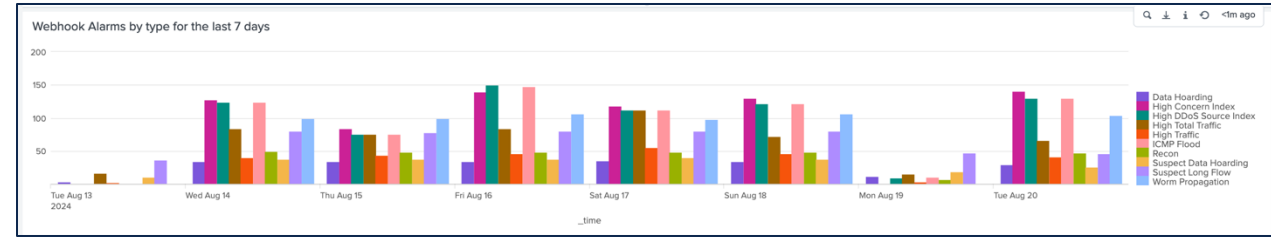
- Stitched and Deduped data provides increased visibility over raw data
- Bi-flow used for Hunting, Investigations, Audit, etc.
- Reduction in Splunk storage cost over direct storage
- Integration via Services-built adaptor or self-built both using FCs Flow Forwarder
- Service adaptor provides filterability of data pre-send and conversion of our protobuf output into a more Splunk acceptable Syslog format.

NDR Detections Use Case - Webhook

NDR Response Configuration in SNA

SNA Alarm Dashboards in Splunk

The screenshot shows the 'Response Management' section in Cisco SNA. Under the 'Actions' tab, a 'Webhook Action' is being configured. The 'Name' is 'Splunk webhook' and the 'Description' is 'WH'. The 'Webhook HTTPS URL' is 'https://10.90.15.230:8088/services/collector'. The 'Basic Authentication' checkbox is checked, with the 'Username' set to 'SNA' and an 'Authentication Password' field. A 'Test Action' button is visible at the bottom right.



NDR Detections in Splunk

The screenshot shows a Splunk search results page for an event. The event details are as follows:

- Time:** 8/20/24 3:36:01000 PM
- Event:** [-]
- Host:** host 1
- Source:** source 1
- Source Type:** source type 1
- Alarm Category:** High Traffic
- Alarm ID:** 80-KW-AJZY-55Y6-B
- Alarm Severity:** Minor
- Alarm Status:** INACTIVE
- Alarm Type Description:** The host traffic rate averaged over a 5-minute period has exceeded the limit of the acceptable traffic values.
- Alarm Type Name:** High Traffic
- Alarm ID:** 30
- Details:** Observed 65,028 bps. Policy maximum allows up to 5M bps.
- Device Hostname:** atl-tse-pdu-atlb.cisco.com
- Device ID:** 301
- Device IP:** 10.90.15.237
- Device Name:** atl-tse-fcds751
- Domain ID:** 301
- Domain Name:** ExplorCorp
- End Active Time:** 2024-08-20T20:25:00Z
- End Active Time Local:** 2024-08-20T20:25:00 (UTC)
- Policy Description:** DDoS Target Event (10.10.30.15)
- Policy ID:** 162
- Policy Name:** 10.10.30.15
- Policy Type:** Host
- Src IP:** 10.90.15.235
- Source Country Code:** XR
- Source Country Name:** RFC 1918
- Source Host Group ID:** 37
- Source Host Group Names:** DNS Servers
- Source Host Group Paths:** Inside Hosts -> By Function -> Servers -> DNS Servers
- Source IP:** 10.10.30.15

Additional Investigation

The screenshot shows the 'Presets' menu in Splunk, which allows users to quickly apply predefined search and visualization configurations. The menu is organized into sections: REAL-TIME, RELATIVE, and OTHER. The 'Relative' section is expanded, showing options like '30 second window', '1 minute window', '5 minute window', '30 minute window', '1 hour window', and 'All time (real-time)'. The 'Date Range' section is also visible, with options like 'Week to date', 'Month to date', and 'Year to date'.

NDR Splunk App Use Case

App for Splunk on splunkbase
<https://splunkbase.splunk.com/app/6398>

App displaying Alarms from SNA in the splunk>enterprise UI

The screenshot shows the Splunkbase app page for the Cisco Secure Network Analytics (Stealthwatch) App for Splunk Enterprise. The page includes a search bar, a 'Submit an App' button, and a 'Log In' button. The main content area features the app title, a description, and a 'Login to Download' button. Below this, there are sections for 'Latest Version 2.0.3' (February 14, 2023), 'Compatibility' (Splunk Enterprise Platform Version: 9.2, 9.1, 9.0, 8.2, 8.1, 8.0), 'Rating' (5 stars), and 'Support' (Developer Supported App). The page also has tabs for 'Summary', 'Details', 'Installation', 'Troubleshooting', 'Contact', and 'Version History'. A blue arrow points from this page towards the right.

The screenshot shows the Splunk Enterprise Alarms interface. The top navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. The main content area is titled 'Alarms' and includes a search bar for 'IP Address' and a dropdown for 'Alarm Type' set to 'All'. Below this, there are two summary charts: a 'Daily Alarm Summary' pie chart and a 'Weekly Alarm Summary' bar chart. The pie chart shows the distribution of alarm types, with 'other (19)' being the largest category. The bar chart shows the number of alarms per day from 08/16/2024 to 08/22/2024. A table below the charts lists individual alarms with columns for 'First Active', 'Alarm', 'Status', 'Source IP', 'Source Hostname', 'Source Username', 'Source Host Group(s)', 'Target IP', 'Target Hostname', and 'Target Username'.

First Active	Alarm	Status	Source IP	Source Hostname	Source Username	Source Host Group(s)	Target IP	Target Hostname	Target Username
2024-08-20 14:35:00 CDT	High Total Traffic	Active	10.201.0.23			Inside Hosts/By Function/Servers/Terminal Servers Inside Hosts/By Location/Atlanta Inside Hosts/By Location/Datacenter			
2024-08-20 14:35:00 CDT	High File Sharing Index	Active	10.201.3.20	nov23minssongrcdnlabtask680-1.cisco.com		Inside Hosts/By Function/Client IP Ranges (DHCP Range)/End User Devices Inside Hosts/By Function/Users/Desktops Inside Hosts/By Location/Atlanta Inside Hosts/Business Units/Sales and Marketing			
2024-08-20 12:40:00 CDT	High Total Traffic	Active	10.10.30.55			Inside Hosts/By Function/Client IP Ranges (DHCP Range)/End User Devices Inside Hosts/By Function/Users/Desktops Inside Hosts/By Location/New York Inside Hosts/By Function/Servers/Domain Controllers			

Data Integration Use Case – 1

Forwarder/DEX – Feature on the Flow Collector

Customer can enable FC to send bi-flow data from a specific FC somewhere else.

- Build into FC using protobuf
- Sends over a websocket
- Proves a ~6x reduction in data vs. directly sending Netflow to Splunk

Limitations

- This is specific to a single FC
- There are limitations to data volumes
- This is not specifically for Splunk

On DEVNET

<https://developer.cisco.com/docs/stealthwatch-data-exporter/stealthwatch-data-exporter/#overview>

Data Integration Use Case - 2

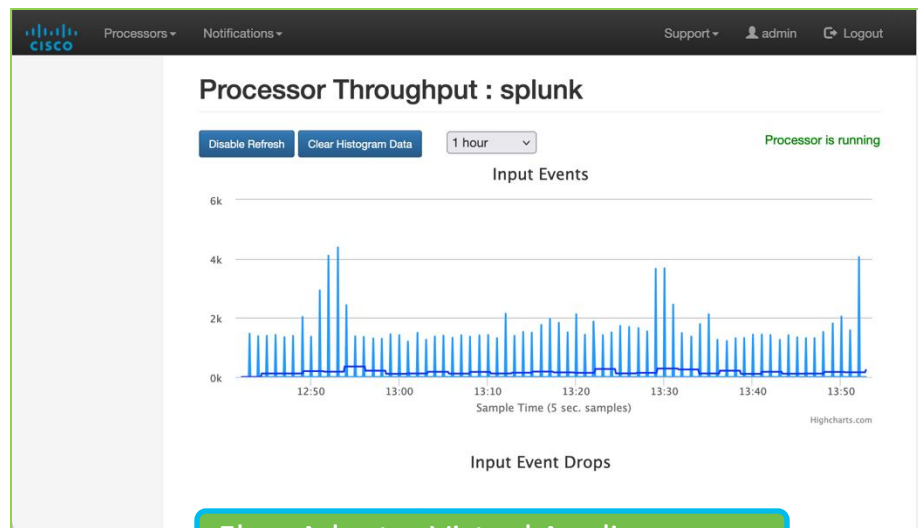
Flow Adaptor - SIEM Service to convert flow export to syslog

Customer can purchase a service that will integrate you FC with your SIEM.

- Uses the FC Flow Forwarder
- Requires a VM with a Flow Adaptor application
- Does the conversion to a Splunk friendly syslog format
- Can filter traffic to eliminate columns reducing size of data

Limitations

- Complicated to deploy, requires maintenance and updates
- Does not scale - 2 FC to 1 Flow Adaptor
50-60k FPS combined total
- Requires a VM outside of SNA per every 2 FCs (One customer has 23 Flow Adaptors running)

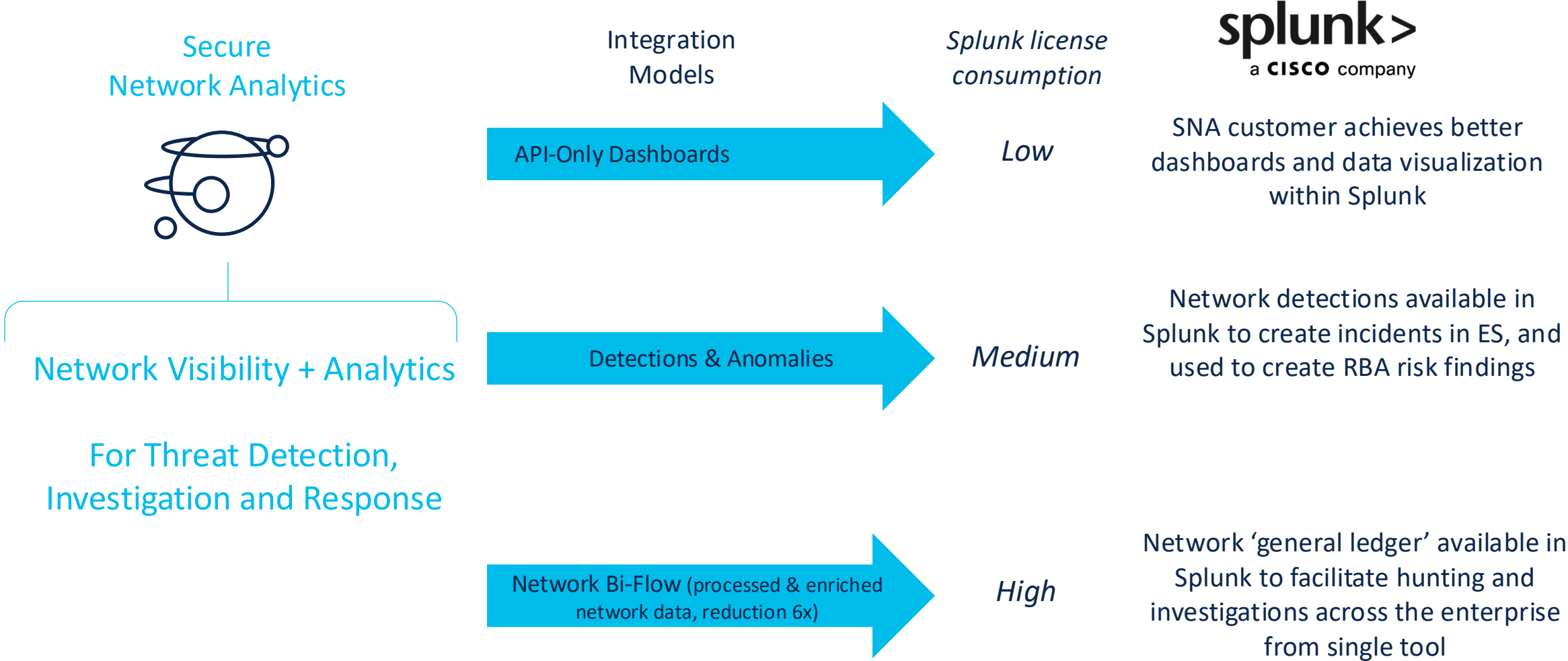


```
> 8/15/24 Aug 15 09:35:59 10.90.15.229 Aug 15 14:36:00 atl-tme-CSDP-FADA-2.2 client=209.182.185.222,server=208.93.140.90,flow_id=144655904,start_active_usec=1723732371000000,last_active_usec=1723732499000000,service_port=80,,protocol=6,service_id=0,,app_id=0,flow_sensor_app_id=23,packetshaper_app_id=0,nbar_app_id=0,palo_alto_app_id=,username=vlan_id=0,mpls_label=0,connections=2,retransmits=0,rtt=0,srt=0,sequence_num=224328595,fc_ip=10.90.15.237,selected_cipher_suite=b'',netflow_count=0,client_port=34053,client_port_max=0,client_xlate_ip=0.0.0.0,client_xlate_port=0,client_mac=,client_asn=0,client_payload=b'',client_payload_ex=b'GET http://alerts.conduit-services.com/root/1528270/1523533/US/',client_group_list=[50031,43,1],client_num_bytes=0,client_num_packets=4,client_syn_packets=0,client_syn_ack_packets=0,client_rst_packets=0,client_fin_packets=0,client_sgt_id=0,client_sgt_name=,client_total_bytes=0,client_process_name=,client_process_hash=,client_process_username=,client_parent_process_name=,client_parent_process_name=,client_id=b'',client_byte_distribution=[],client_tls_version=,client_tls_session_id=b'',client_payload_binary=b'',client_payload_ex_binary=b'GET http://alerts.conduit-services.com/root/1528270/1523533/US/',server_port=80,server_port_max=0,server_xlate_ip=0.0.0.0,server_xlate_port=0,server_mac=,server_asn=0,server_payload=b'',server_payload_ex=b'304 Not Modified',server_group_list=[61758,61452,60000,0],server_num_bytes=0,server_num_packets=4,server_syn_packets=0,server_syn_ack_packets=0,server_rst_packets=0,server_fn_packets=0,server_fn_packets=0,server_sgt_id=0,server_sgt_name=,server_total_bytes=0,server_total_packets=0,server_process_name=,server_process_hash=,server_process_username=,server_parent_process_name=,server_parent_process_hash=,server_payload_ex_binary=b'304 Not Modified',server_payload_binary=b''
```

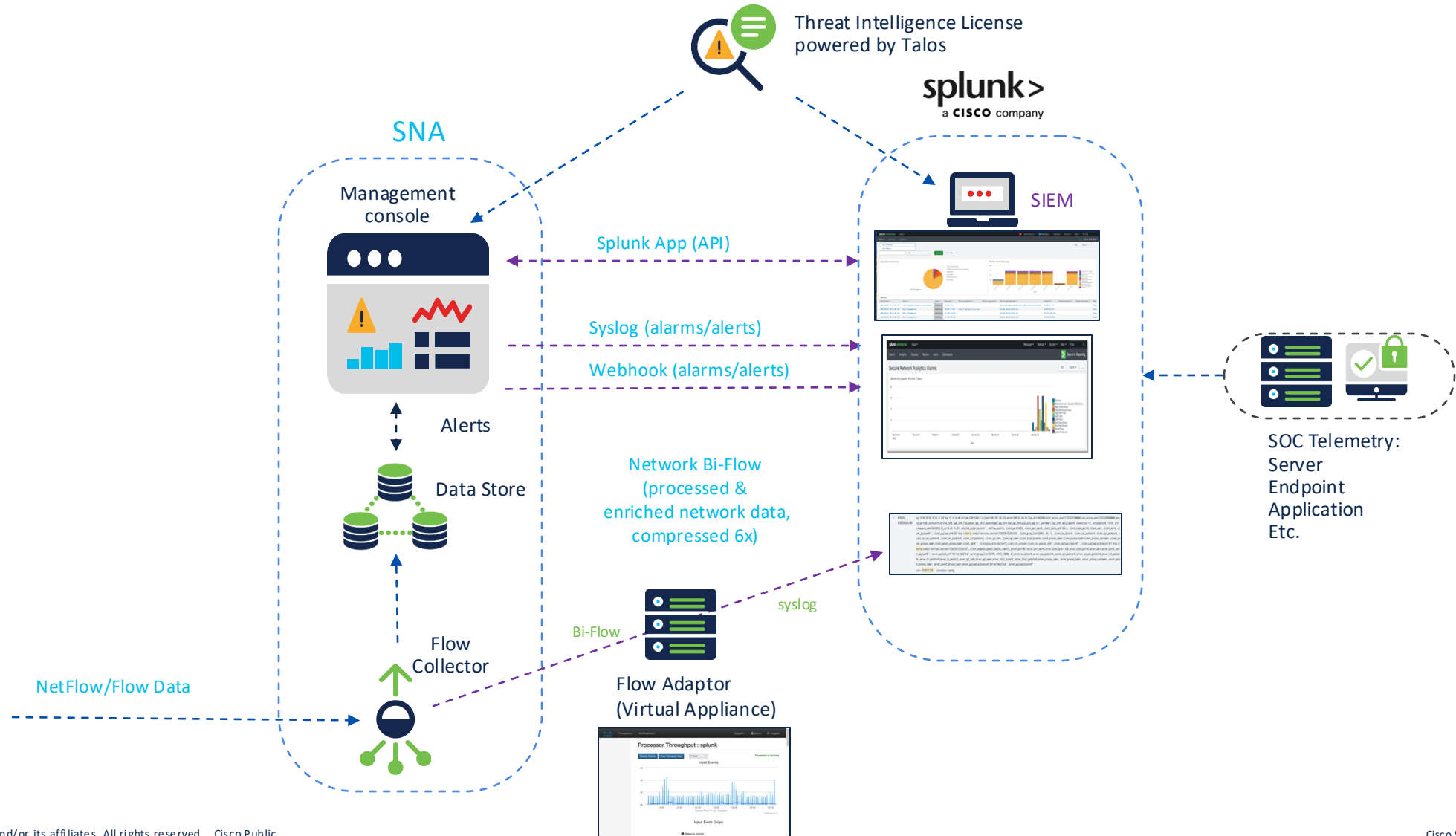
host = 10.90.15.229 sourcetype = syslog

Example of converted flow data sent as syslog to Splunk

Secure Network Analytics (SNA) + Splunk Current Integration Options



SNA & Splunk Architecture



Secure Network Analytics Resources

- **Secure** Analytics Videos

<http://cs.co/SecureAnalyticsVideos>

- **Detection** demo series

- Showcase alerting through product demonstration of real-world attacks
- Comprehensive package covering a specific alert lifecycle and expert insights
- Available in the [Secure Analytics Detections Demo playlist](#) on



Secure Network Analytics Click Through Demo

[SNA 7.5 Click Through Demo](#)

Cisco Secure Network Analytics 7.5.1 - Instant Demo (dCloud)

[Cisco Secure Network Analytics 7.5.1 - Instant Demo](#)

Cisco Secure Network Analytics Customer Test Drive 7.4.2 (dCloud)

[Cisco Secure Network Analytics Customer Test Drive 7.4.2](#)

[Cisco Security Analytics White Paper](#)

Video Title	Duration	Views	Posted
Introduction to this Detections Demo Series	5:53	54 views	1 month ago
AWS Detector Modified	3:56	50 views	1 month ago
Azure OAuth Bypass	4:01	32 views	1 month ago
New Internal Device Alert Demo	4:43	91 views	2 months ago

Q&A



