cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Meraki & Secure Network and Cloud Analytics

Threat Detection for the Rest of Us

Alex Burger
Matt Robertson

BRKMER-2003

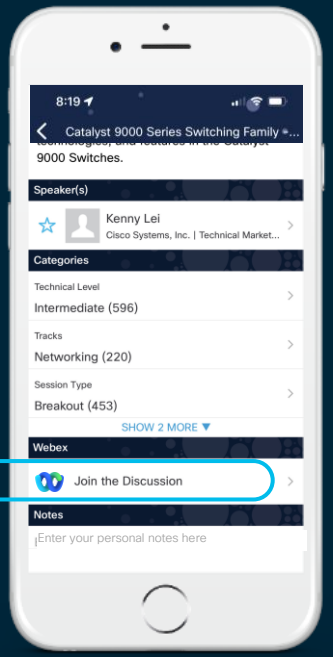
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

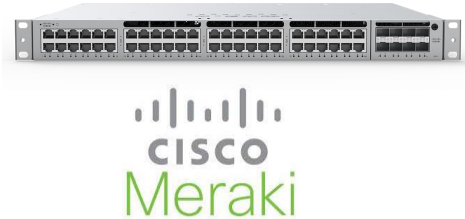
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKMER-2003

Webex spaces will be moderated by the speaker until June 17, 2022.

Agenda



Agenda:

- Introduction
- Secure Network/Cloud Analytics
- Telemetry from the Meraki Network
- Some analytical outcomes
- Summary

Watch out for this guy!

About Us

Matt Robertson
Principal Engineer

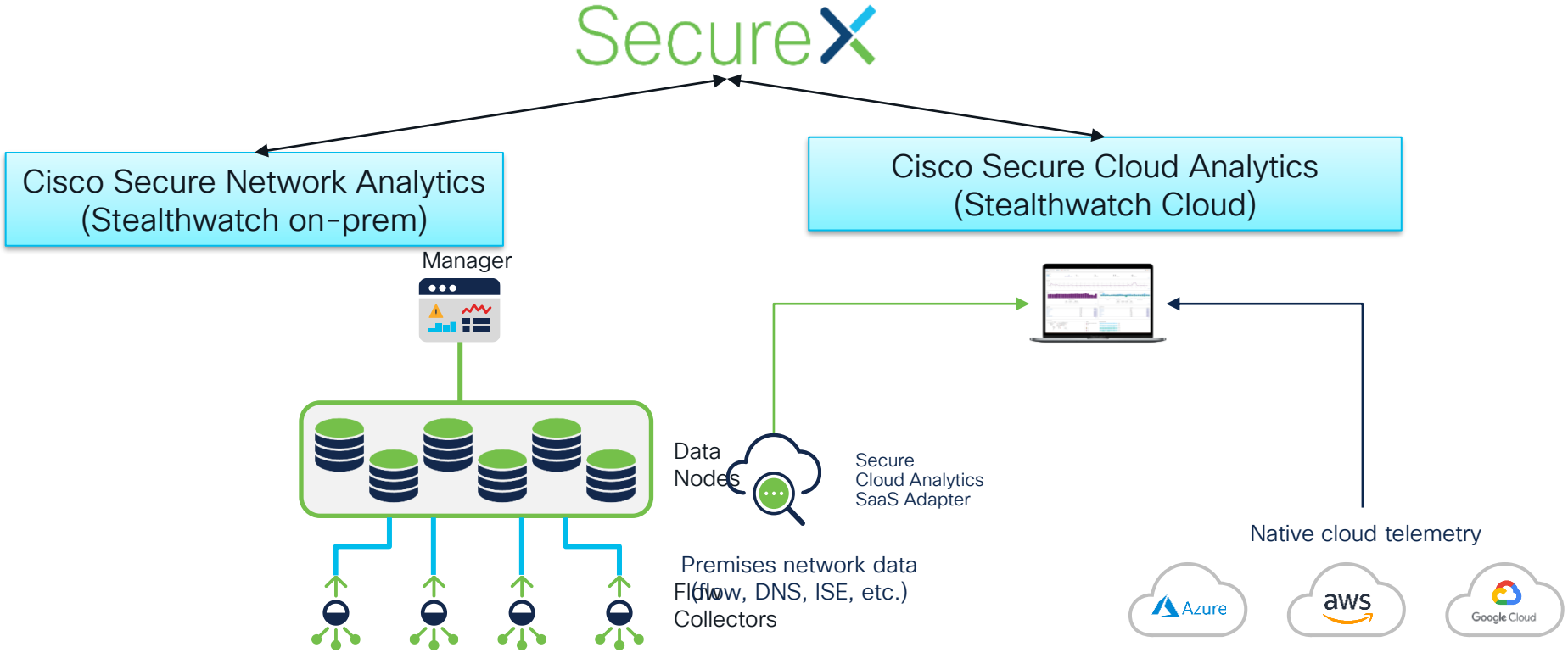
CISCO SECURE

Alex Burger
Sr. Technical Marketing Engineer

CISCO Meraki

Cisco Secure Network & Cloud Analytics

Cisco Secure Network Analytics Portfolio



Secure Network Analytics is a collector and aggregator of telemetry for the purposes of security analysis and monitoring

Security Analytics: Outcomes

Automating Security Operations

Automating or Augmenting these functions:

- Incident Responder
- Security Analyst
- Security Operations
- Threat Hunter
- Compliance and Policy
- Business Continuity
- Cybercrime fighting
- Etc.

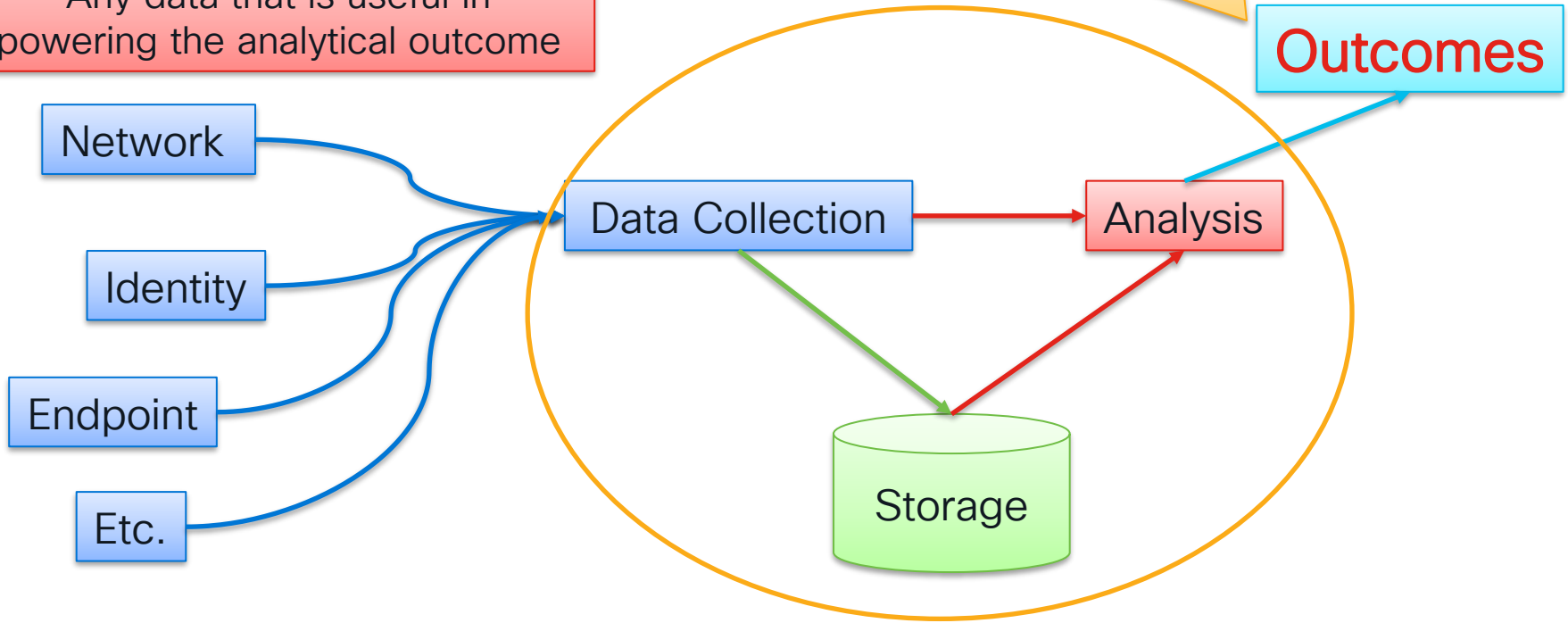
Automating implies an algorithmic approach, which could be a diverse set of methods to accomplish the outcome:

- Entity Modelling
- Statistical Analysis
- Predictive Analysis
- Machine Learning
- Unsupervised Learning
- Supervised Learning
- Reinforced Learning
- Artificial Intelligence
- Etc.

Powering Analytics with Telemetry

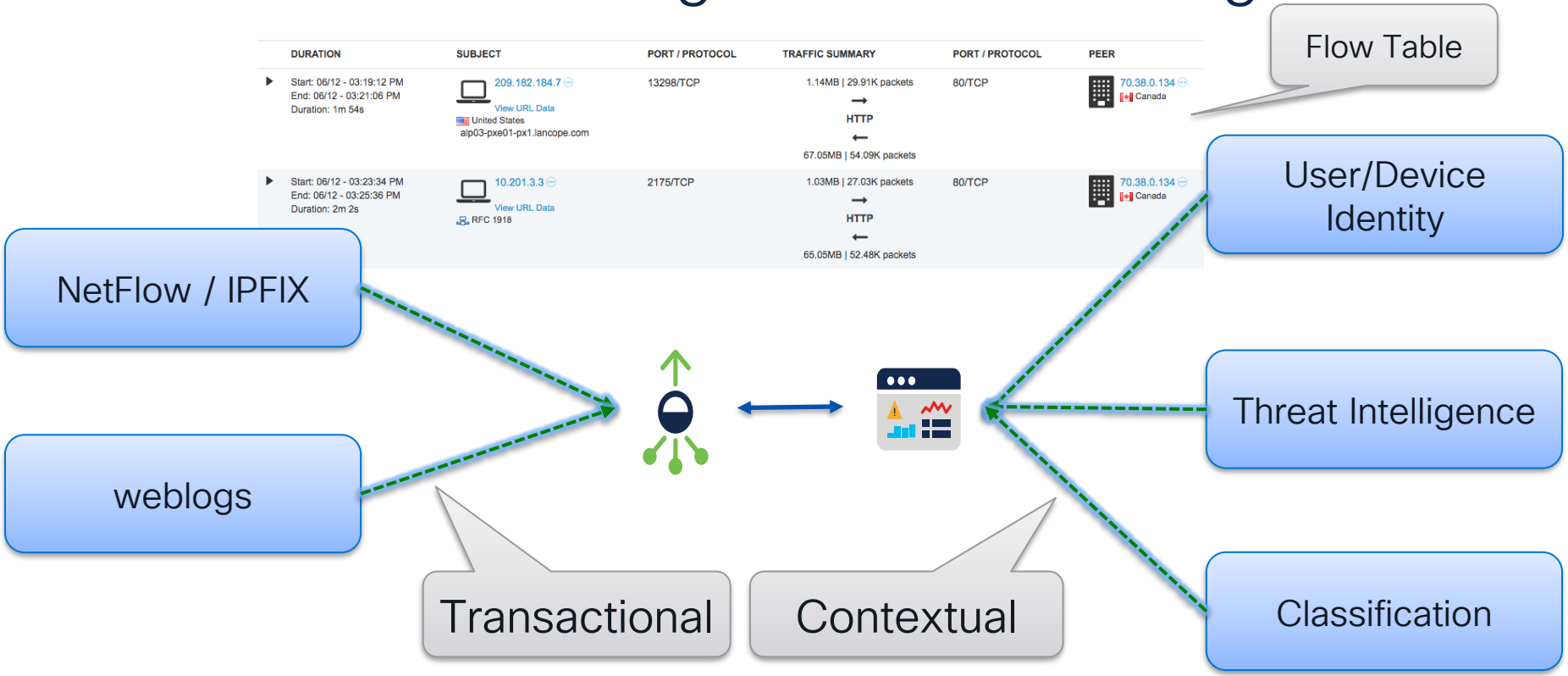
Telemetry:
Any data that is useful in powering the analytical outcome

This is what's important.



Stealthwatch: Building the “General Ledger”

DURATION	SUBJECT	PORT / PROTOCOL	TRAFFIC SUMMARY	PORT / PROTOCOL	PEER
Start: 06/12 - 03:19:12 PM End: 06/12 - 03:21:06 PM Duration: 1m 54s	209.182.184.7 View URL Data United States alp03-pxe01-px1.lancope.com	13298/TCP	1.14MB | 29.91K packets → HTTP ← 67.05MB | 54.09K packets	80/TCP	70.38.0.134 Canada
Start: 06/12 - 03:23:34 PM End: 06/12 - 03:25:36 PM Duration: 2m 2s	10.201.3.3 View URL Data RFC 1918	2175/TCP	1.03MB | 27.03K packets → HTTP ← 65.05MB | 52.48K packets	80/TCP	70.38.0.134 Canada



Secure Network Analytics: The “Bi-Flow”

A single database entry representing a logical bi-directional network flow between two network entities

DURATION	SUBJECT	SUBJECT PORT/PROTOCOL	TRAFFIC SUMMARY	PEER PORT/PROTOCOL	PEER	ACTIONS
Start: Jun 5, 2019 2:37:24 PM End: Jun 5, 2019 2:37:59 PM Duration: 35seconds	10.90.90.100 View URL Data RFC 1918 darrin 00:50:56:b6:e7:c2	50323/TCP	5.97 KB | 40 packets → Cloud storage & computing services ← 7.09 KB | 36 packets	80/TCP	52.95.145.35 Canada s3-website.ca-central-1.amazonaws.com	

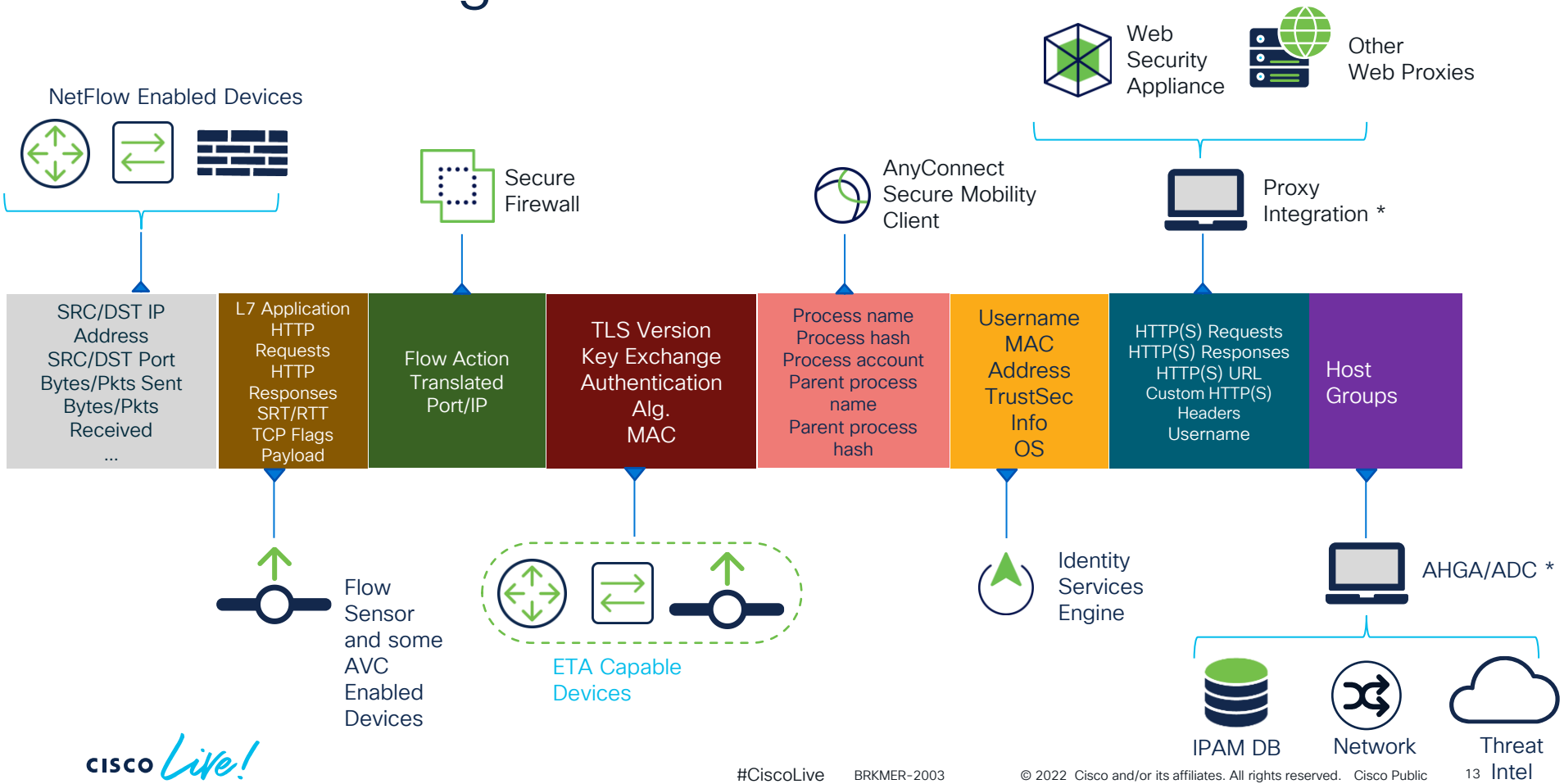
General

View URL Data

Subject		Totals		Peer	
Packets:	40	Packets:	76	Packets:	36
Packet Rate:	1.14 pps	Packet Rate:	2.17 pps	Packet Rate:	1.03 pps
Bytes:	5.97 KB	Bytes:	13.06 KB	Bytes:	7.09 KB
Byte Rate:	174.63 bps	Byte Rate:	382.06 bps	Byte Rate:	207.43 bps
Percent Transfer:	45.71%	Subject Byte Ratio:	45.71%	Percent Transfer:	54.29%
Host Groups:	End User Devices, Main Campus Building 2	RTT:	0seconds	Host Groups:	Canada
Payload:	GET http://beerhoser.ca/beerhoser_main.png	SRT:	0seconds	Payload:	304 304 Not Modified

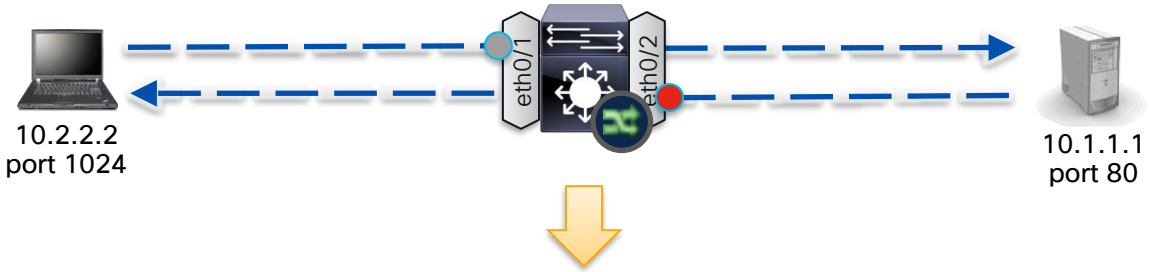
Telemetry from multiple sources synthesised and compressed into this single entry

Understanding Bi-Flow Enrichment



Telemetry from the Meraki Network

Transactional Telemetry with NetFlow



Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT	TCP Flags
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010	SYN,ACK,PSH
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100	SYN,ACK,FIN

NetFlow is a protocol. The **Metadata** is what's important.

Meraki NetFlow Exporters

Meraki MX

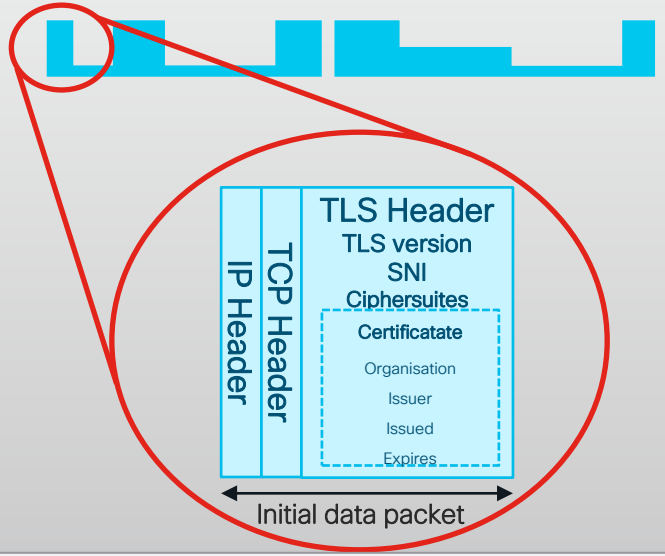
NetFlow v9

Meraki MS390 & C9300-M

IPFIX enriched with Application and ETA

Enhanced Telemetry for Encrypted Traffic Analytics

Initial Data Packet



First application layer message.

In **TLS** this is the **Client Hello** and **Server Hello**

Sequence of Packet Lengths and Time (SPLT)

Size and timing of the first packets of a flow

Useful in identifying application, data types and characterising the source

The Meraki MS390 & C9300-M

Cisco Hardware

+

Meraki Cloud Management

Modular Uplinks
8 x 10G
2 x 40G

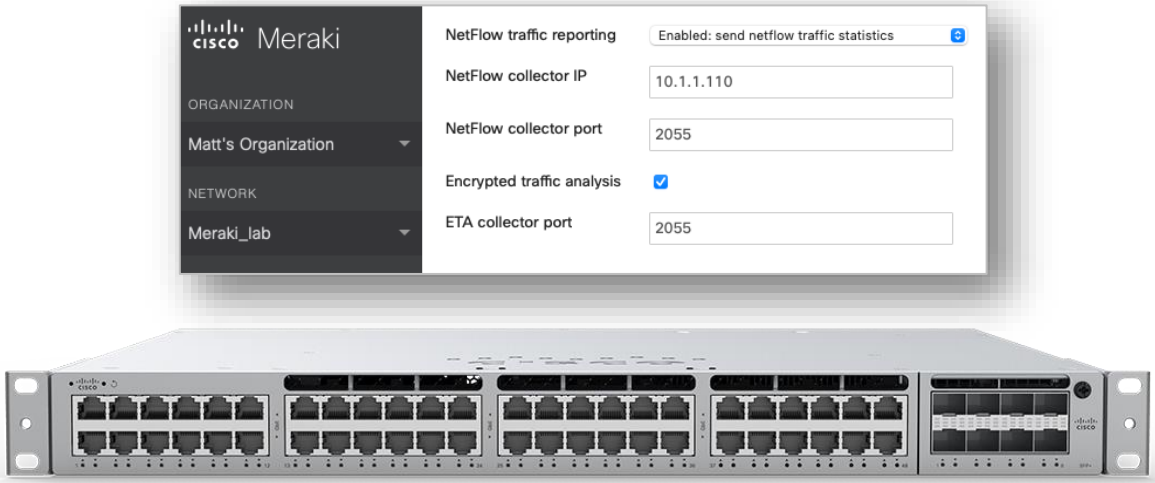
Stacking
480Gbps

mGig
24 x 10Gbps
48 x 5Gbps

PoE
24/48 port
802.3bt

Redundancy
Stack Power
Hot-Swap fans

The Meraki MS390 & C9300-M: What's new



Validated NetFlow export to SNA or SCA

Rapid, one-click, config & deployment

NetFlow & Encrypted Traffic Analytics

NetFlow v10 (IPFIX) with IPv4 / IPv6 / Adaptive Policy / NBAR / ETA

AVC NetFlow*

IPv4 and v6 records built for Cisco Secure Analytics (Network and Cloud)

NetFlow and ETA

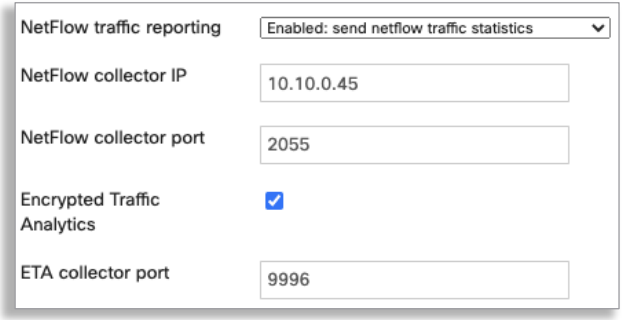
on every port on every supported switch in the network

Encrypted Traffic Analytics

for in-depth analysis of traffic without MiTM decryption

Adaptive Policy**

Export of Source Security Group Tags (SGTs)

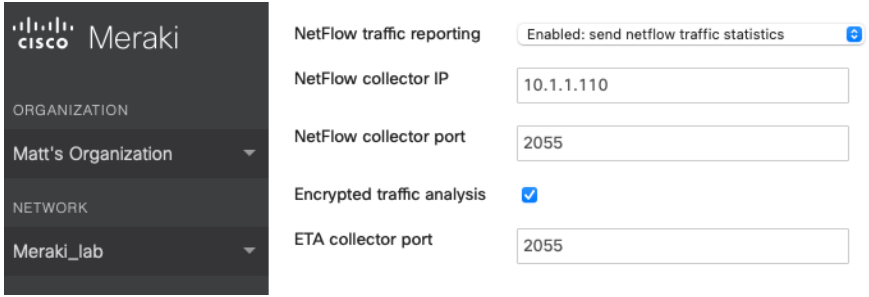


MS390/C9300-M Flow Config:

MS NetFlow and Encrypted Traffic Analytics

Last updated: Sep 16, 2021

https://documentation.meraki.com/MS/Meraki_MS_Beta/MS_Netflow_and_ETA



MATCH	COLLECT
NBAR application	connection client counter bytes network long
interface input	connection client counter packets long
source address	connection client ip address
destination address	connection client transport port
protocol	connection initiator
version	connection new-connections
transport source port	connection server counter bytes network long
transport destination port	connection server counter packets long
	connection server ipv4 address
	connection server transport port
	counter bytes long
	counter packets long
	adaptive policy source group-tag
	dot1q vlan input
	destination mac address
	source mac address
	flow direction
	flow observation point
	interface output
	timestamp absolute first
	timestamp absolute last
	transport tcp flags

One click deployment to all ports on all MS390's in a network
Unprecedented ease of deployment!

+ETA enabled on all ports

MS390 & C9300-M is an ideal SNA telemetry source

- Line rate, hardware supported telemetry
- Deep packet inspection enables application recognition
- Telemetry for advanced encrypted traffic analytics
- One click deployment to all devices

Duration	Subject IP Address	Subject Proces...	Application	Application (NBAR)	Total Bytes	Encryption TLS...	Encryption Key...	Encryption Aut...	Encryption Alg...	Encryption MAC	Peer IP Address	Peer Port/Prot...
Ex. <=50min4	Ex. 10.10.10.10	chrome	Ex. "Corporate	Ex. netbios	Ex. <=50M	Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. SHA384	Ex. 10.255.25	Ex. 2055/UDP
1min 48s	10.90.90.201	chrome.exe	HTTPS	ssl	9.33 K	TLS 1.2	RSA	RSA	AES_128_GCM/128	SHA256	146.112.61.110	443/TCP
6min 9s	10.90.90.201	chrome.exe	Web	google-services	47.21 K	TLS 1.3	PSK_ECDHE	--	AES_128_GCM/128	SHA256	142.251.41.67	443/TCP

Application (NBAR) data

ETA “Encryption fields”

Dashboard Demo

Some Outcomes

You can do a lot of things with analytics

https://cisco.bravais.com/s/lnmF3Eowwg51t7Rj9DtD

cisco

Stealthwatch Value Use Case Menu

This limited collection of use cases highlights the capabilities of Stealthwatch

Threat Detection

- Detecting Beaconing
- Detecting Bogon Traffic
- Detecting Command and Control Traffic Using the Threat Intelligence License
- Detecting Fake Applications
- Detecting Fileless Malware - PowerShell Attacks
- Detecting Internal Brute Force Attacks
- Detecting Lateral Movement
- Detecting Man in the Middle Attacks
- Detecting Password Spray Attacks
- Detecting Rogue DHCP Servers
- Detecting TOR Traffic
- Detecting Rogue DNS Traffic
- Detecting Fragmentation Attacks
- Detecting Targeted Attacks
- Detecting ATM Attacks
- Detecting WannaCry Malware
- Reducing Mean Time To Know
- Detecting Browser-Based Attacks
- Detecting Cryptomining Attacks
- Using Cognitive Intelligence
- Using Cognitive Intelligence and AMP for Network Security
- Detecting Malware in Encrypted Traffic

Compliance

- Identifying Medical Asset Types on the Network
- Managing Stealthwatch Users
- Monitoring Trusted Third Party Users
- Using Bi-Directional Policies
- Using the ETA Cryptographic Audit Application
- Using the Visibility Assessment Application
- Verifying Change Control Management
- Detecting Obsolete Encryption Protocols
- Detecting Insecure Protocols
- Detecting Torrent or File Sharing Traffic
- Monitoring Vendor Activity
- Monitoring High Priority Host Groups
- Detecting Fake Applications
- Detecting Rogue and New Devices
- Defining Business Applications
- Detecting Application Access Policy Violation
- Identifying Applications on the Network
- Monitoring Remote Access Users
- Using Custom Security Events to Monitor Firewalls
- Using Encryption Auditing

Incident Response

Network Visibility

- Identifying a Virtual Machine Generating Excessive Traffic
- Investigating NTP Reflection DDoS
- Investigating Unidirectional Traffic
- Using the Host Classifier Application
- Using the Interface Status Report in the SMC Web UI for Network Operations
- Using the SMC Web UI for Network Usage Accounting
- Using Stealthwatch for Network Segmentation and Policy Development

Forensic Investigation

- Reporting Internet URL Access
- Using the Interface Status Report for Security Operations
- Using the Security Event Workflow
- Using Top Reports
- Obtaining Historical Conversations for Unauthorized Data Transfer

Alarm Categories

- Alarm Category: Command and Control
- Alarm Category: Anomaly

Example Behavioural Analytic Outcomes

BRKSEC-2267

Security Policy:

Analyse network behaviour to design, implement and validate security policy

Threat Detection:

Analyse network behaviour to infer the presence of a threat actor

BRKSEC-3019

And there are many, many more available outcomes …

Layers of Detection in SNA

New!

Custom Security Events

- User Defined Policy
- Generate an alarm based on flow attributes

Core Events

- Runs on each flow collector
- 98+ tunable behavioural algorithms:
  - Statistical anomaly detection
  - Policy based detection
- Some threat Intelligence powered alarms

Relationship Events

- Interaction between host groups that violate a policy setting
- Directly created or automatically created from network diagram

“Analytics” Node

- Runs on Manager
- Requires central data store
- Common analytics with Secure Cloud Analytics

Global Threat Alerts (Cognitive Intelligence)

- Cloud Hosted
- Multi-layer Machine Learning
- Malware classification

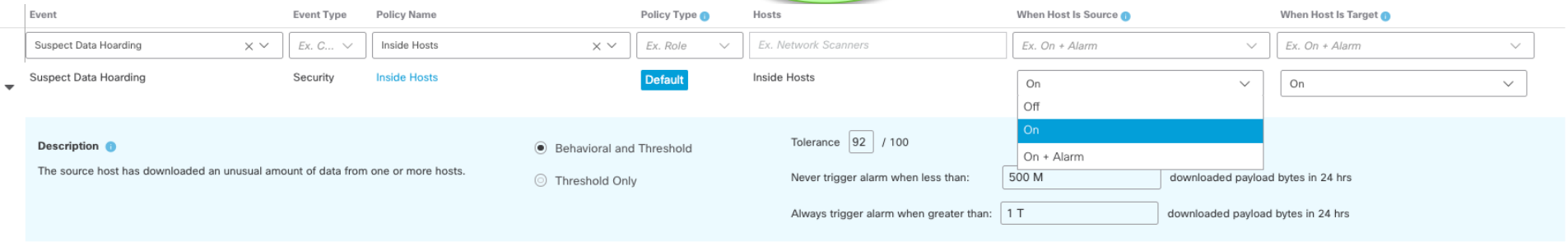
Network Behavioral Threat Detection

Core Events

- Runs on each flow collector
- 98+ tunable behavioural algorithms:
  - Statistical anomaly detection
  - Policy based detection
- Some threat Intelligence powered alarms

Entity
(IP Address, Host Group)

For every algorithm, maintain historical model of entity's behaviour. Generate an event when conditions are met.



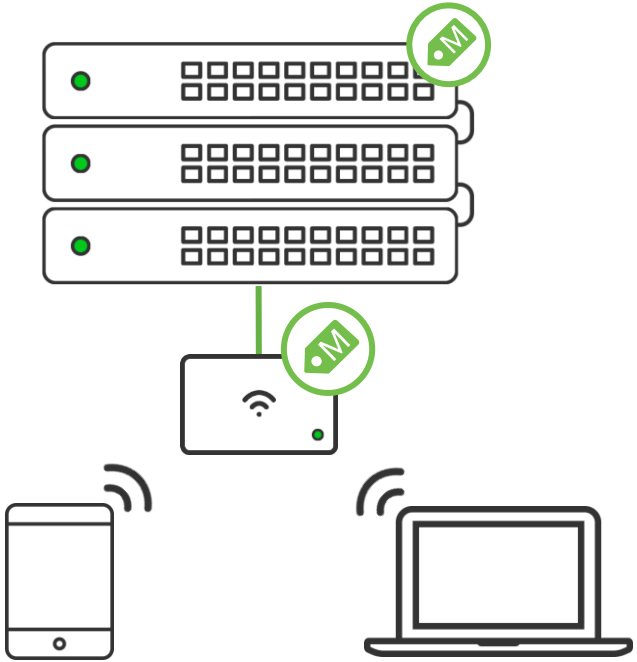
Adaptive Policy

Micro-Segmentation and Context with Security Group Tags

Organization-Wide intent-based **policy**

Utilizing inline **Security Group Tags** (SGTs)

Context shared over the data-plane providing **identical policy** for **wired** and **wireless** access



Flexible Group Assignment

Static port assignment

Fixed wired devices without a supplicant

Static SSID assignment

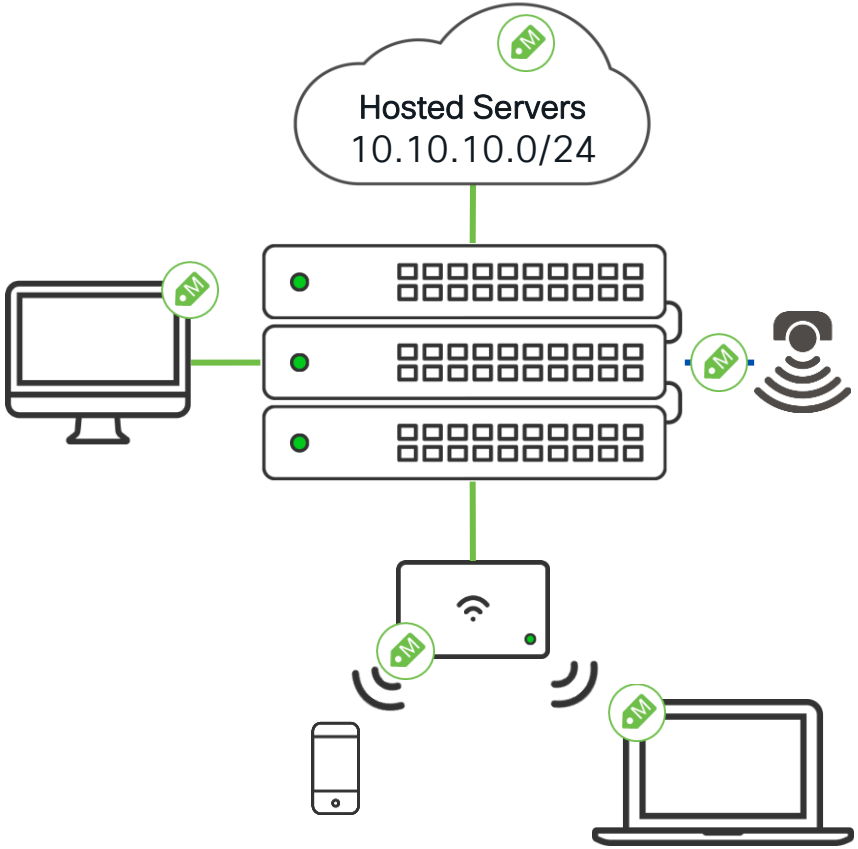
Single-use SSIDs like guest

Dynamic via RADIUS

Wired and Wireless MAB/802.1X & iPSK w/RADIUS

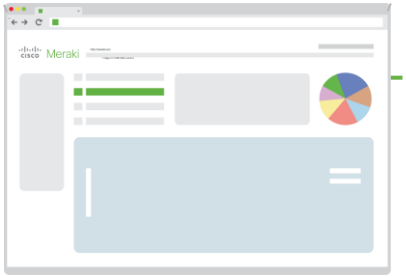
IP Prefix to SGT Map

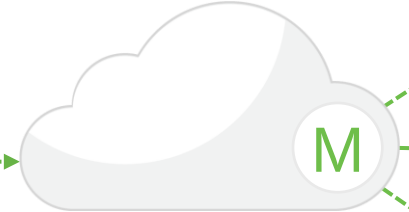
Last resort traffic match based on IP/Subnet



One Consistent Policy Across Networks

SRC | DST	Employee	IoT	IoT Server
Employee	✔	✘	✔
IoT	✘	✘	✔
IoT Server	✔	✔	✔





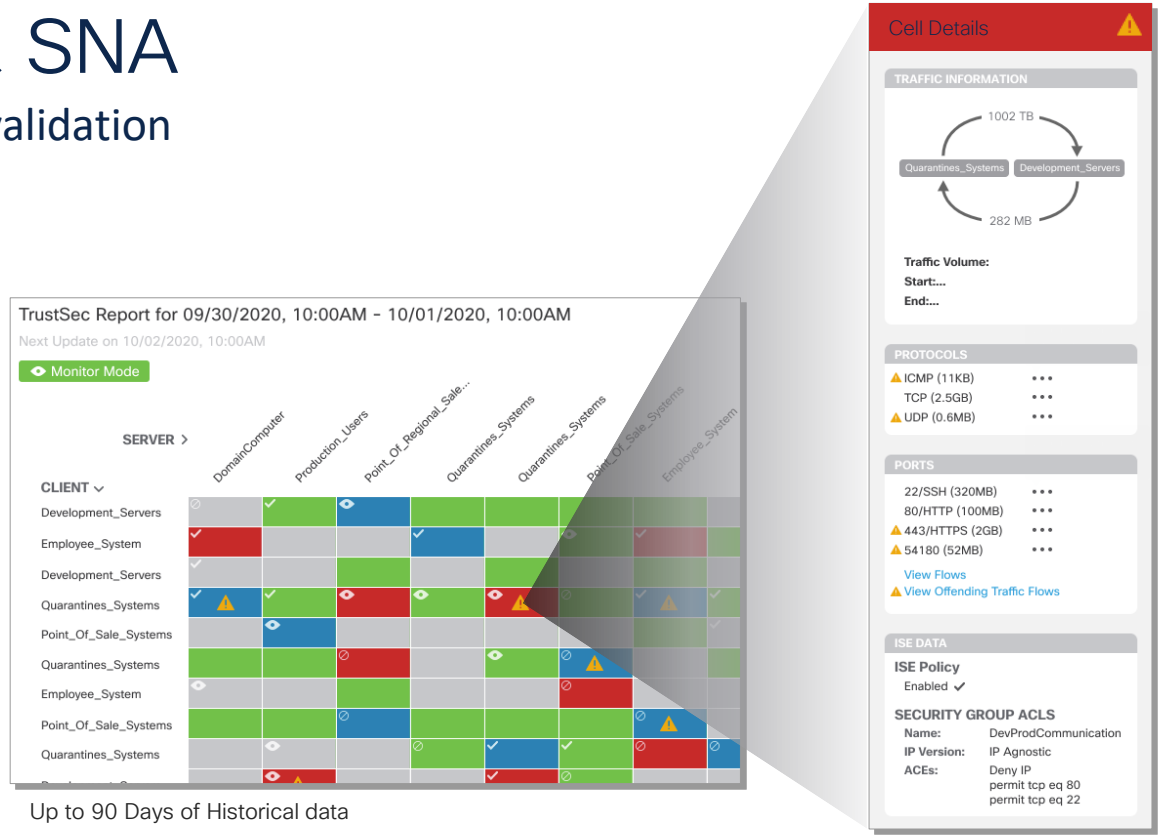
Policy & Groups are configured in dashboard and pushed to Adaptive Policy nodes like any other Meraki configuration change

Adaptive Policy & SNA

Informed policy creation and validation

Global flow **visibility** and **context**

Group based policy and traffic **flow tracking**



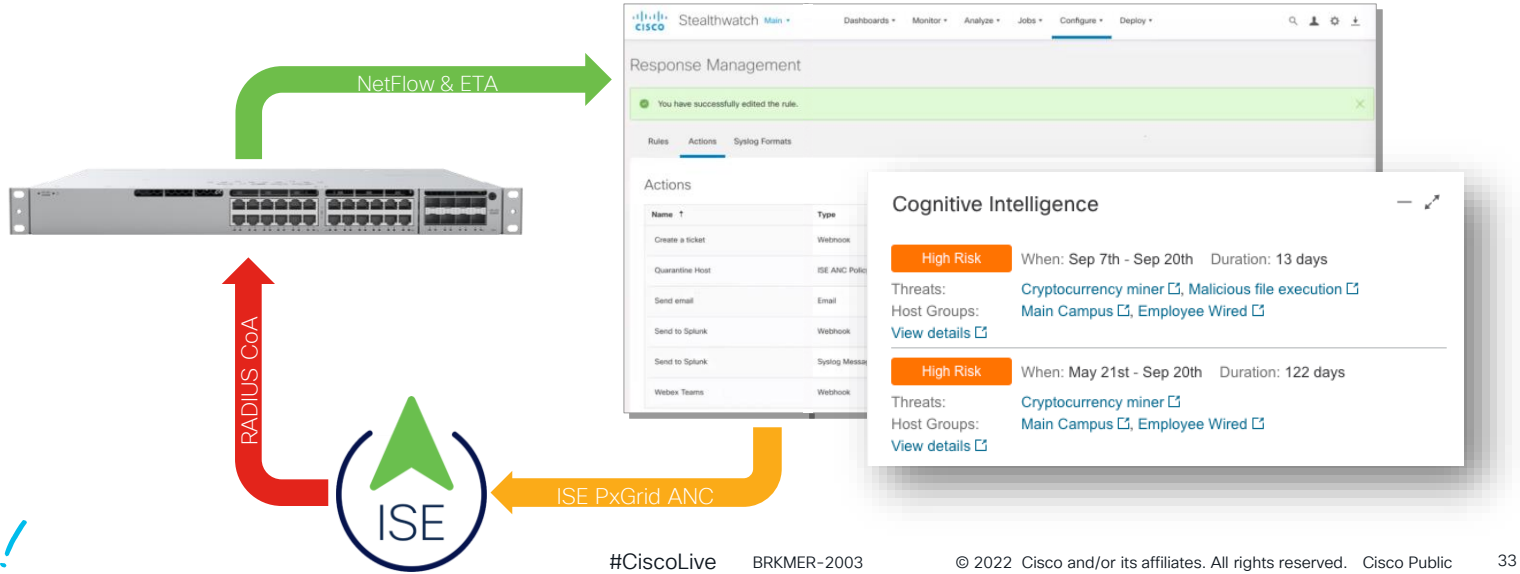
Up to 90 Days of Historical data

Threat Detection and Response

Telemetry provided by **MS390/C9300-M** to SNA

Flexible outcomes: Policy Violation

Trigger **CoA** via ISE



Demo

Summary

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Some awesome related sessions!

Session ID	Title	When
BRKSEC-2267	Building Network Security Policy Through Data Intelligence	Tuesday at 2:30 PM
BRKSEC-3019	Visibility, Detection and Response with Cisco Secure Network Analytics	Wednesday at 4:00 PM
BRKMER-2003	Meraki & Secure Network and Cloud Analytics: Threat Detection for the Rest of Us	Thursday at 9:30 AM
BRKSEC-2053	Zero Trust: Securing the Evolving Workplace	Monday at 4:00 PM

Technical Session Surveys

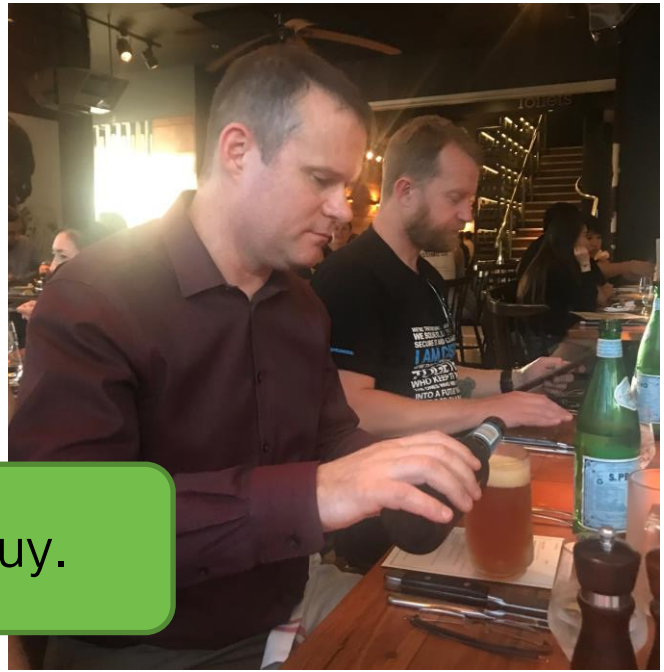
- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Parting Thoughts

Data analytics are a critical component of the modern network/security operations center

Meraki MS390/C9300-M is an ideal telemetry source for Cisco Secure Network/Cloud Analytics

Watch out for this guy.



Thank you

cisco Live!

ALL IN

#CiscoLive