cisco Live!

ALL IN

#CiscoLive

The bridge to possible

Building Network Security Policy Through Data Intelligence

Matt Robertson
@mrobertson25

BRKSEC-2267

Cisco Webex App

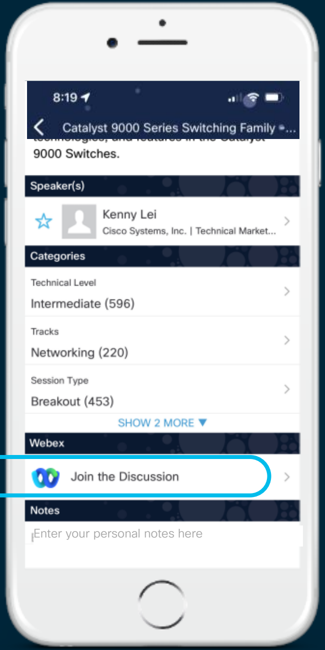
Questions?

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

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



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2267

About This Session:

Policy Analytics:
Design, validate and verify policy through data analytics

Agenda:

- Designing Policy
- Validating Policy
- Verifying Policy
- Summary

Examples using ISE, TrustSec and Secure Network Analytics

BRKSEC-2026

Vs.

The Great Canadian Bacon Debate

About Me

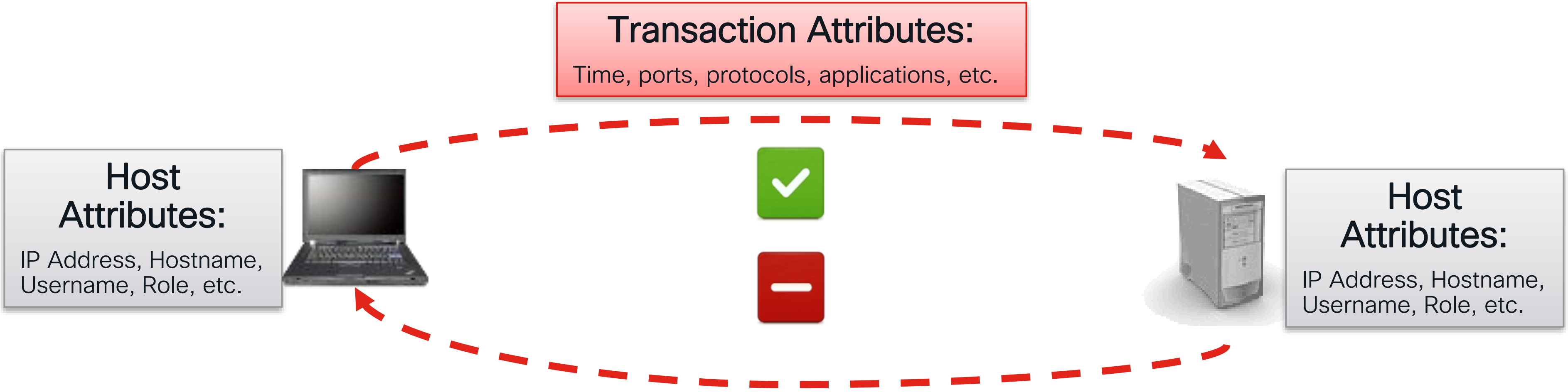
Matt Robertson

- Principal Technical Marketing Engineer
- Security Analytics and Advanced Threat
- Cisco Live Distinguished Speaker
- 14 years at Cisco: Development, TME, Lancope
- Canadian eh
- Known beer hoser: http://www.beerhoser.ca

Designing Policy

Segmentation & Network Security Policy

Security policy should dictate a hierarchy of access permissions; that is, grant users access only to what is necessary for the completion of their work
https://en.wikipedia.org/wiki/Network_security_policy



Transaction Attributes:

Time, ports, protocols, applications, etc.

Host Attributes:

IP Address, Hostname, Username, Role, etc.

Host Attributes:

IP Address, Hostname, Username, Role, etc.

Segmentaion Policy is Hard

CISO: How do I deploy segmentation without getting fired?

Bear downs 36 beers, passes out at campground

Rainier, not Busch, the beverage of choice for thirsty black bear

http://www.nbcnews.com/id/5756809/ns/us_news-weird_news/t/bear-downs-beers-passes-out-campground

Boozy feral pig steals beer, gets drunk and starts fight with a cow

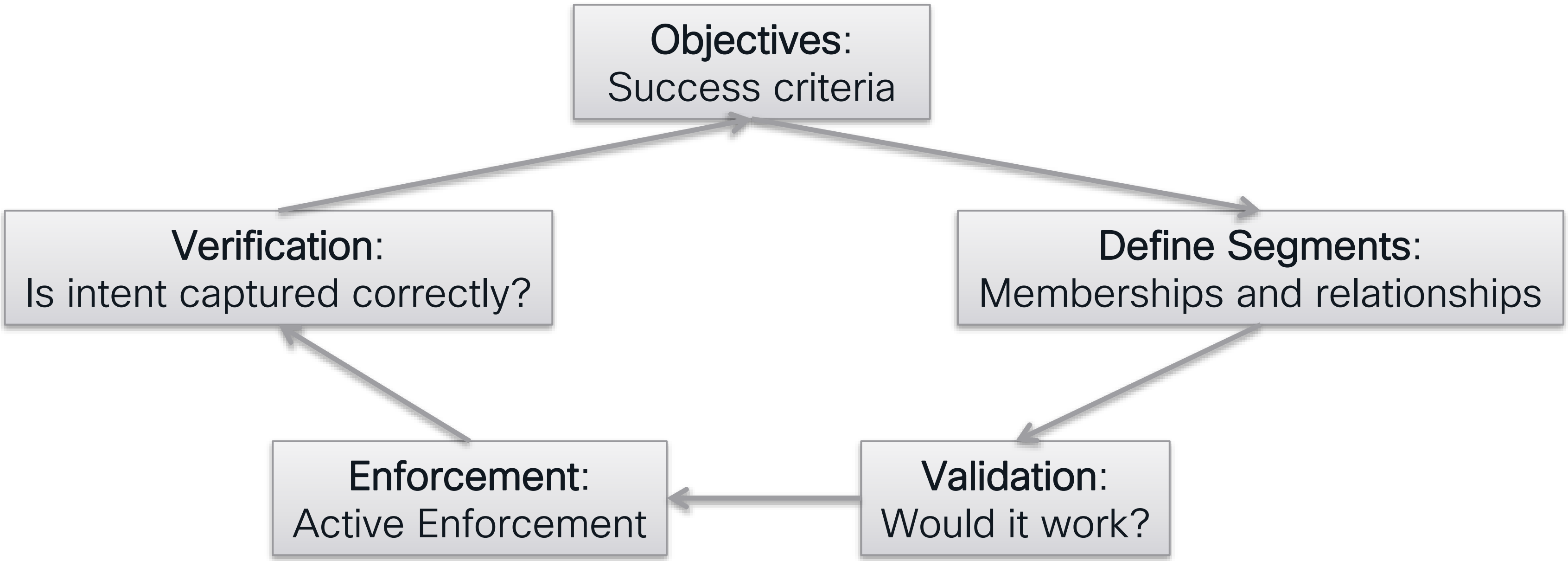
Belligerent porker went on bender after drinking three six-packs of beer

https://www.independent.co.uk/news/world/australasia/boozy-feral-pig-steals-beer-gets-drunk-and-starts-fight-with-a-cow-8805312.html

MOLSON
CANADIAN
BIÈRE LAGER BEER

We all know we want it but we're not sure how to do it effectively

Policy and Segmentation is a Process



Objectives:
Success criteria

Define Segments:
Memberships and relationships

Validation:
Would it work?

Enforcement:
Active Enforcement

Verification:
Is intent captured correctly?

Defining Objectives and Success

Example Objective:
Regulatory compliance and reduced threat surface

Who is the audience that measures the results against that goal?

Even if segmentation is working as intended, if the auditor isn't happy you're not done.

Starting a Design

Best Practice:
Start Small, you don't have to do everything at once

Identify assets to protect

PCI Data, Production Systems, Intellectual Property, Etc

Methods of Classification

- Static
- Dynamic
- Etc.

Policy Enforcement Points

- Firewall
- Umbrella
- Route/Switch via DNAC/ISE and TrustSec
- Etc.

Propagation Methods

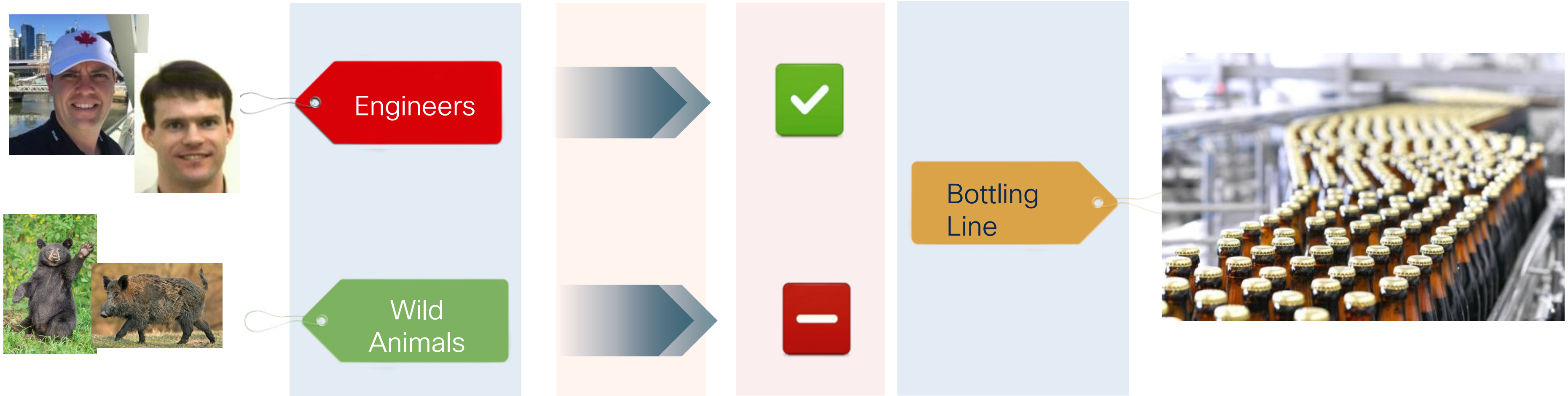
- Inline Tagging
- Out of band overlay
- Implied
- Etc.

Business Centric Segmentation

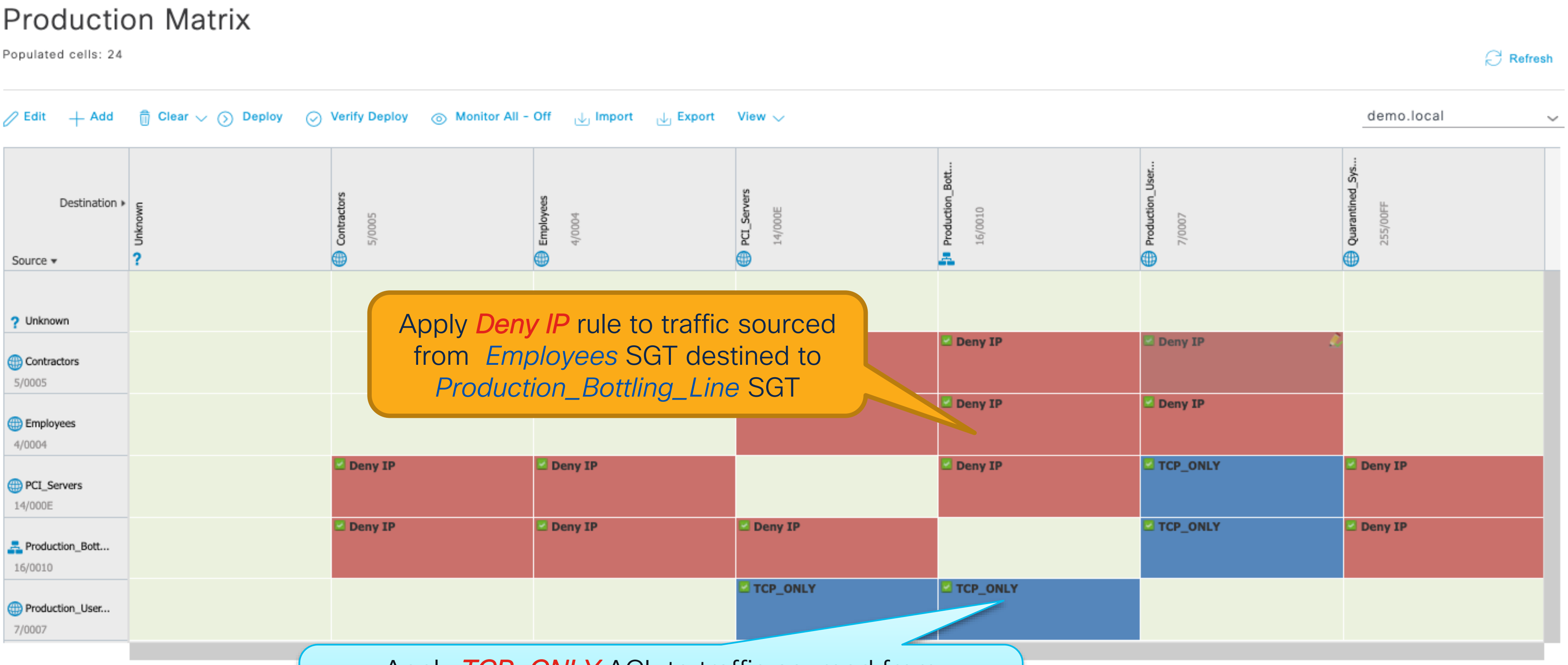
Business-based groups and memberships

Business-centric relationships between groups

Business-based groups and memberships



Example ISE TrustSec Policy Matrix



Production Matrix

Populated cells: 24

Destination ▸ Source ▾	Unknown	Contractors 5/0005	Employees 4/0004	PCI_Servers 14/000E	Production_Bott... 16/0010	Production_User... 7/0007	Quarantined_Sys... 255/00FF
Unknown							
Contractors 5/0005					Deny IP	Deny IP	
Employees 4/0004					Deny IP	Deny IP	
PCI_Servers 14/000E		Deny IP	Deny IP		Deny IP	TCP_ONLY	Deny IP
Production_Bott... 16/0010		Deny IP	Deny IP	Deny IP		TCP_ONLY	Deny IP
Production_User... 7/0007				TCP_ONLY	TCP_ONLY		

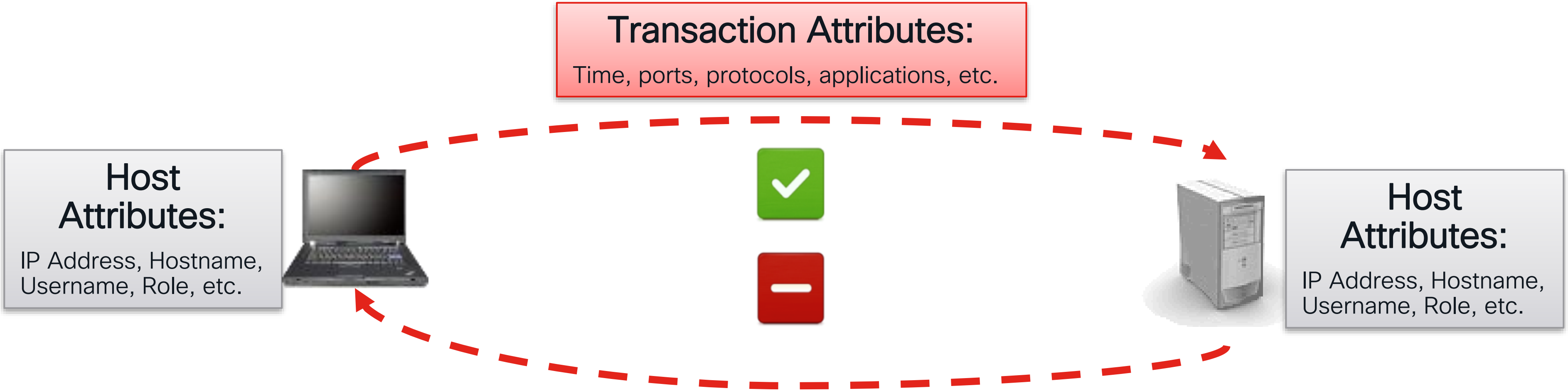
Apply *Deny IP* rule to traffic sourced from *Employees* SGT destined to *Production_Bottling_Line* SGT

Apply *TCP_ONLY* ACL to traffic sourced from *Production_Users* SGT destined to *Production_Bottling_Line* SGT

Validating Policy

Validating Policy Objective

How do I know that my policies are correct and won’t disrupt operations?



Transaction Attributes:

Time, ports, protocols, applications, etc.

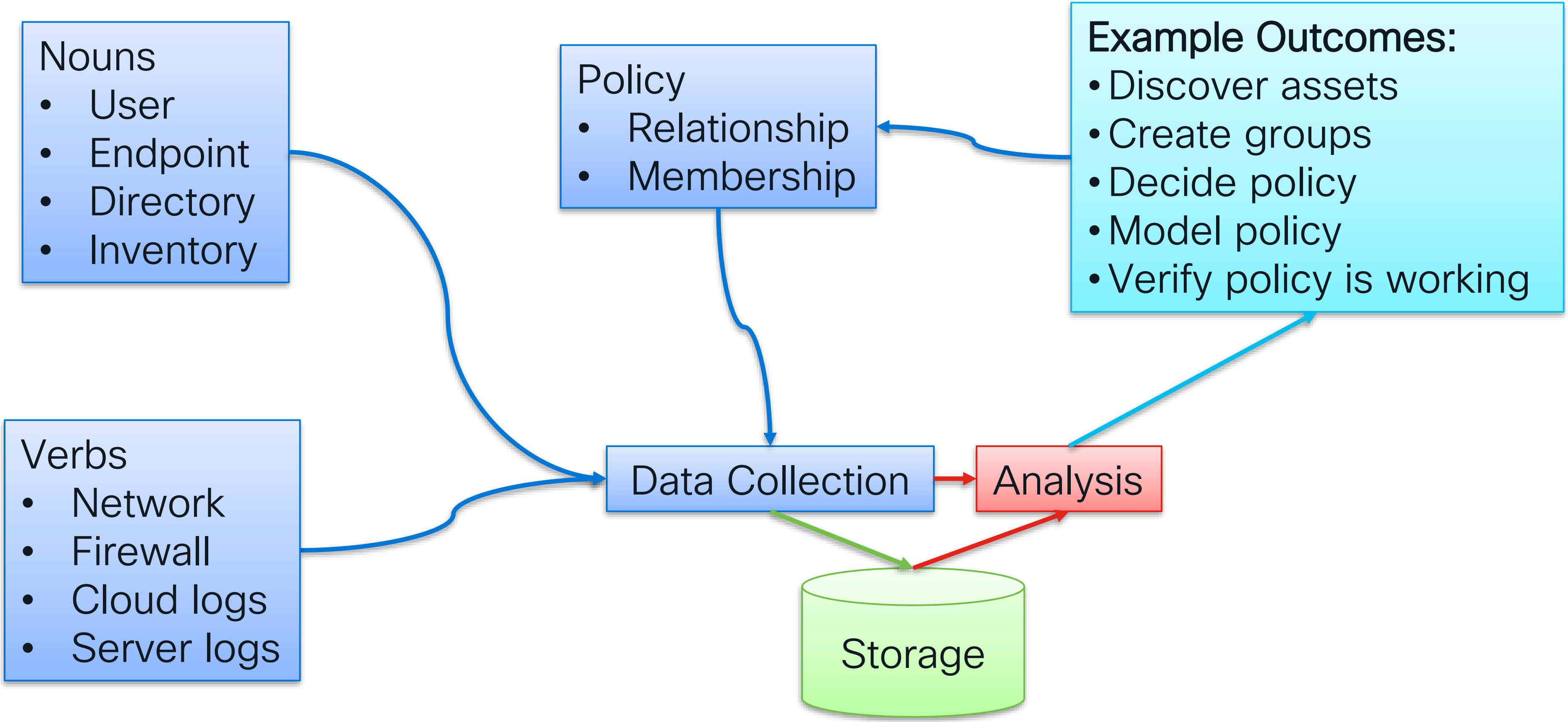
Host Attributes:

IP Address, Hostname,
Username, Role, etc.

Host Attributes:

IP Address, Hostname,
Username, Role, etc.

Data for Policy Analytical Outcomes



Nouns

- User
- Endpoint
- Directory
- Inventory

Verbs

- Network
- Firewall
- Cloud logs
- Server logs

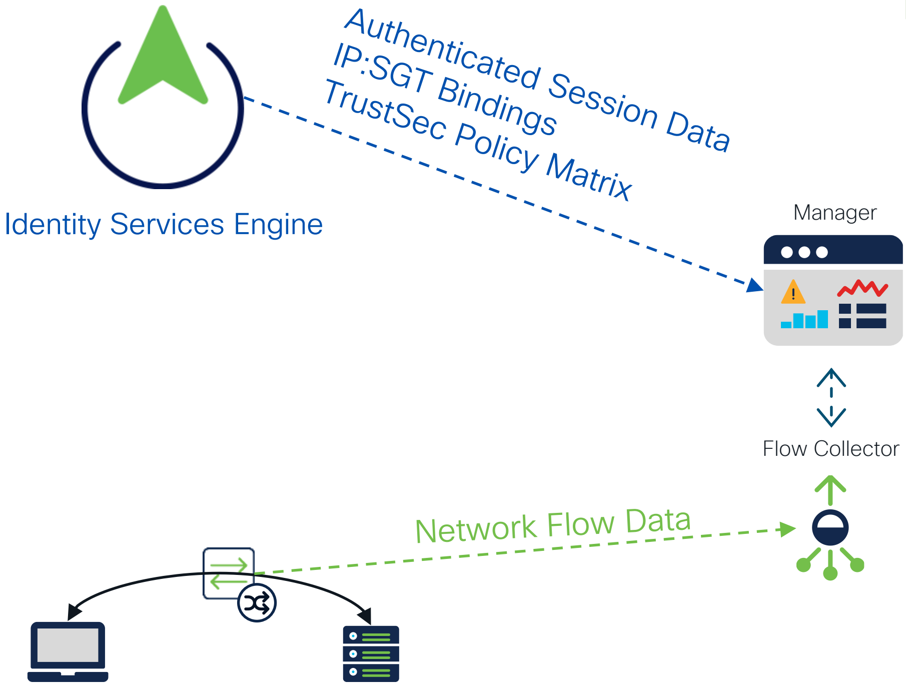
Policy

- Relationship
- Membership

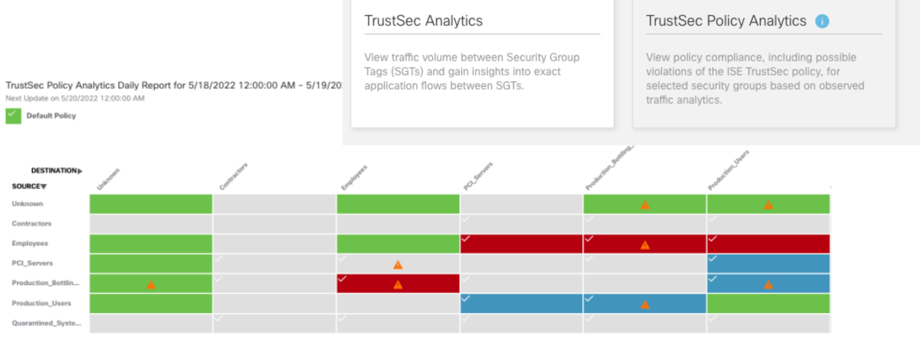
Example Outcomes:

- Discover assets
- Create groups
- Decide policy
- Model policy
- Verify policy is working

Policy Analytics with Secure Network Analytics



1. TrustSec Analytics Reports



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.

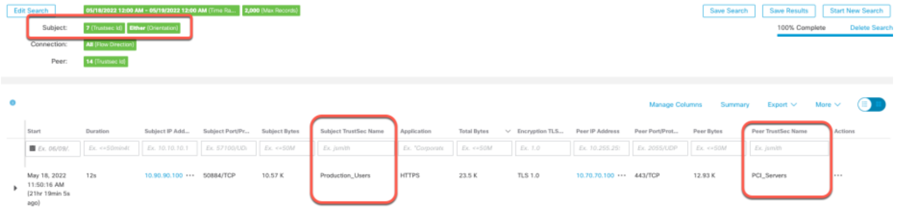
TrustSec Policy Analytics Daily Report for 5/18/2022 12:00:00 AM - 5/19/20

Next Update on 5/20/2022 12:00:00 AM

🟩 Default Policy

DESTINATION▶ SOURCE▼	Unknown	Contractors	Employees	PCI_Servers	Production_Bottling...	Production_Users
Unknown	🟩		🟩		🟩 ▲	🟩 ▲
Contractors				✓	✓	✓
Employees	🟩		🟩	🟥 ✓	🟥 ✓ ▲	🟥 ✓
PCI_Servers	🟩	✓	✓ ▲		✓	🟦 ✓
Production_Bottlin...	🟩 ▲	✓	🟥 ✓ ▲	✓		🟦 ✓ ▲
Production_Users	🟩			🟦 ✓	🟦 ✓ ▲	🟩
Quarantined_Syste...		✓	✓	✓	✓	✓

2. Direct flow analysis leveraging SGT & DGT in Flow Table
3. Custom Security Events



05/18/2022 12:00 AM - 05/19/2022 12:00 AM (Time Ra... 2,000 (Max Records)

Subject: 7 (Trustsec Id) Either (Orientation)

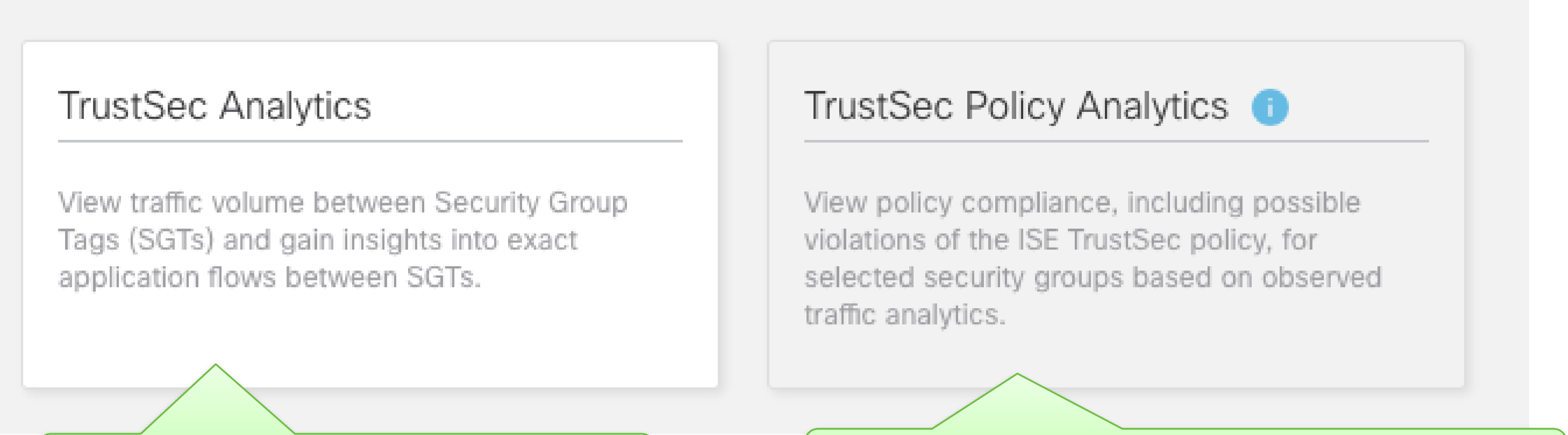
Connection: All (Flow Direction)

Peer: 14 (Trustsec Id)

Start	Duration	Subject IP Add...	Subject Port/Pr...	Subject Bytes	Subject TrustSec Name	Application	Total Bytes	Encryption TLS...	Peer IP Address	Peer Port/Prot...	Peer Bytes	Peer TrustSec Name	Actions
Ex. 06/09/.	Ex. <=50min4t	Ex. 10.10.10.1	Ex. 57100/UDi	Ex. <=50M	Ex. jsmith	Ex. "Corporate	Ex. <=50M	Ex. 1.0	Ex. 10.255.25:	Ex. 2055/UDP	Ex. <=50M	Ex. jsmith	
May 18, 2022 11:50:16 AM (21hr 19min 5s ago)	12s	10.90.90.100 •••	50884/TCP	10.57 K	Production_Users	HTTPS	23.5 K	TLS 1.0	10.70.70.100 •••	443/TCP	12.93 K	PCI_Servers	•••

TrustSec Policy Analytics

Two report types introduced in Secure Network Analytics v7.3.1



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.

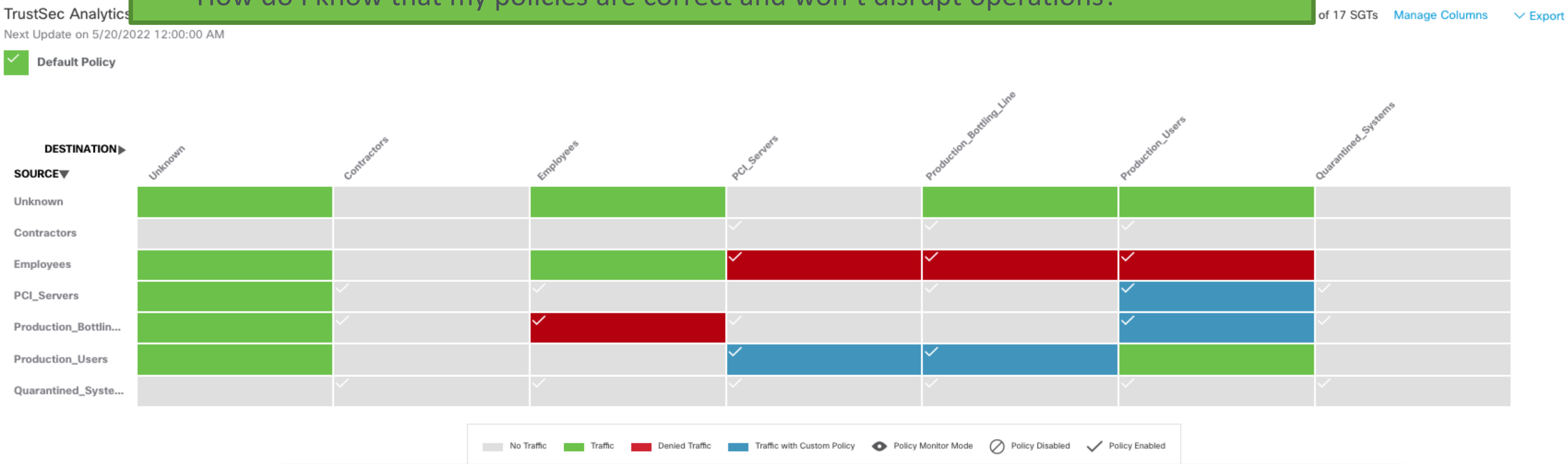
Multiple Reports of this type allowed

One report of this type allowed per deployment

TrustSec Analytics Report

Designed to provide visibility into SGT traffic:

- How do I decide what policies should exist between my groups?
- How do I know that my policies are correct and won't disrupt operations?



TrustSec Analytics

of 17 SGTs

Manage Columns

Export

Next Update on 5/20/2022 12:00:00 AM

🟩 Default Policy

DESTINATION ▶ / SOURCE ▼	Unknown	Contractors	Employees	PCI_Servers	Production_Bottling_Line	Production_Users	Quarantined_Systems
Unknown	🟩	⬜	🟩	⬜	🟩	🟩	⬜
Contractors	⬜	⬜	⬜	⬜ ✓	⬜ ✓	⬜ ✓	⬜
Employees	🟩	⬜	🟩	🟥 ✓	🟥 ✓	🟥 ✓	⬜
PCI_Servers	🟩	⬜ ✓	⬜ ✓	⬜	⬜ ✓	🟦 ✓	⬜ ✓
Production_Bottlin...	🟩	⬜ ✓	🟥 ✓	⬜ ✓	⬜	🟦 ✓	⬜ ✓
Production_Users	🟩	⬜	⬜	🟦 ✓	🟦 ✓	🟩	⬜
Quarantined_Syste...	⬜	⬜ ✓	⬜ ✓	⬜ ✓	⬜ ✓	⬜ ✓	⬜ ✓

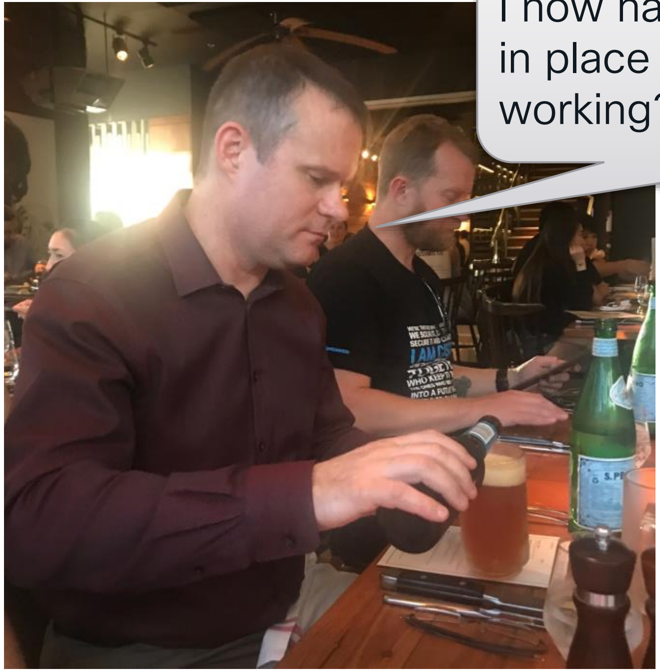
⬜ No Traffic 🟩 Traffic 🟥 Denied Traffic 🟦 Traffic with Custom Policy 👁 Policy Monitor Mode ⊘ Policy Disabled ✓ Policy Enabled

- Gray – no traffic
- Green – there is traffic and a *permit IP* ACL exists
- Red – there is traffic and a *deny IP* ACL exists
- Blue – there is traffic and an ACL other than *permit IP* or *deny IP* exists

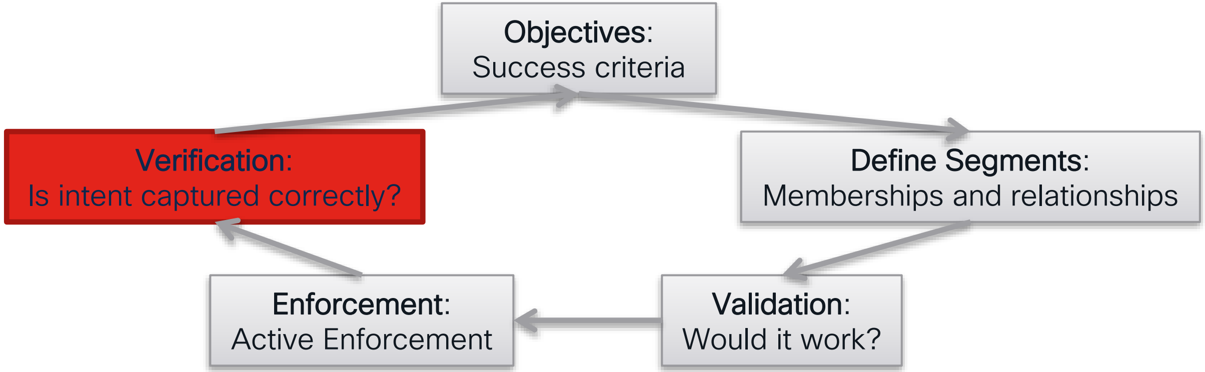
Demo

Verifying Policy

Verifying Policy: Is intent captured correctly?



I now have classifications and policy in place – How do I verify that its working?



Objectives: Success criteria

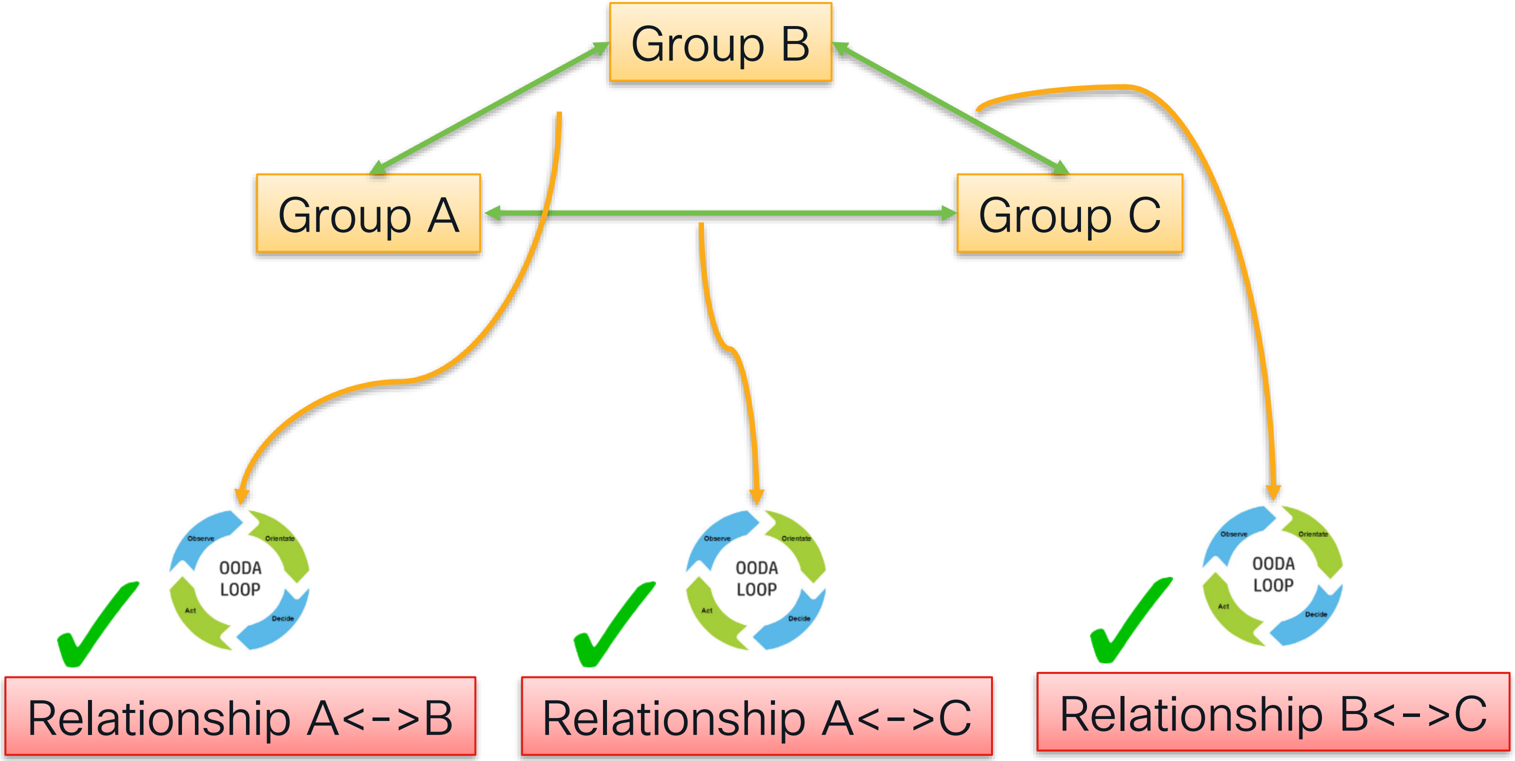
Define Segments: Memberships and relationships

Validation: Would it work?

Enforcement: Active Enforcement

Verification: Is intent captured correctly?

Examine and Refine Relationships

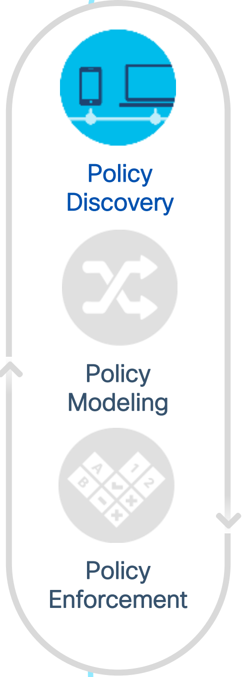


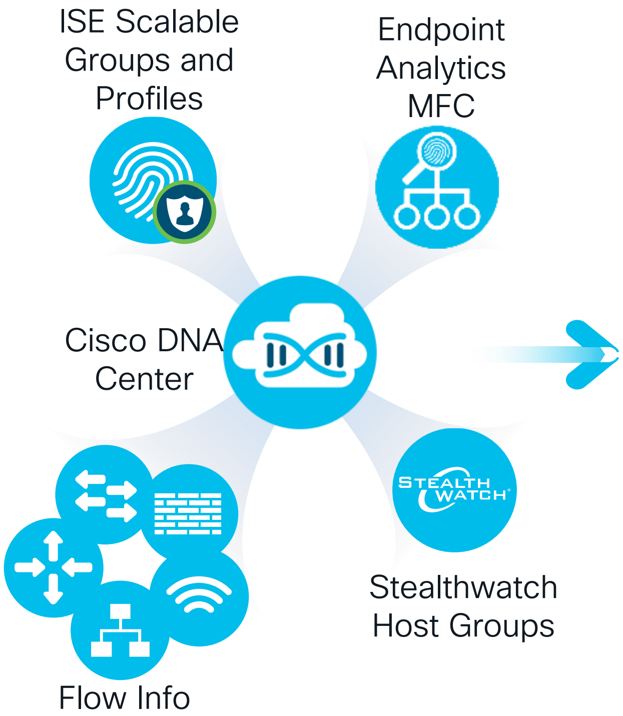
✓ Relationship A<-->B

✓ Relationship A<-->C

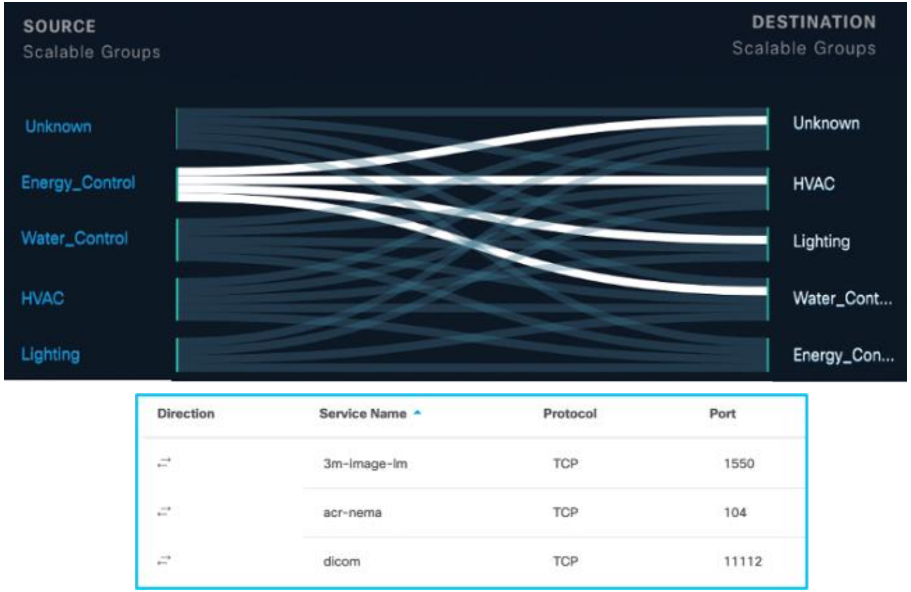
✓ Relationship B<-->C

Aside: Group-Based Policy Analytics on DNAC





Group-Group Activity

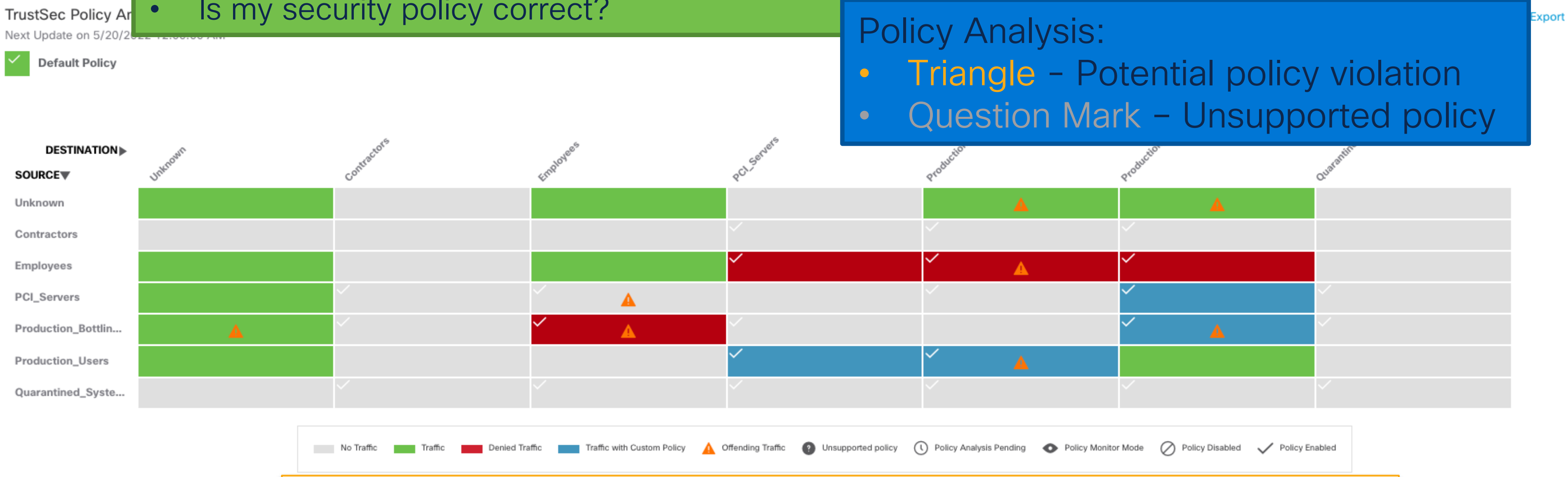


Direction	Service Name ▲	Protocol	Port
⇄	3m-image-lm	TCP	1550
⇄	acr-nema	TCP	104
⇄	dicom	TCP	11112

SNA: TrustSec Policy Analytics Report

Designed to help verify correctness and adherence to TrustSec policy:

- Is my security policy being enforced as intended?
- Is my security policy correct?



TrustSec Policy Ar

Next Update on 5/20/2

Export

✓ Default Policy

DESTINATION ▶ / SOURCE ▼	Unknown	Contractors	Employees	PCI_Servers	Productio	Productio	Quarantin
Unknown	🟩	⬜	🟩	⬜	🟩 ⚠	🟩 ⚠	⬜
Contractors	⬜	⬜	⬜	⬜ ✓	⬜ ✓	⬜ ✓	⬜
Employees	🟩	⬜	🟩	🟥 ✓	🟥 ✓ ⚠	🟥 ✓	⬜
PCI_Servers	🟩	⬜ ✓	⬜ ✓ ⚠	⬜	⬜ ✓	🟦 ✓	⬜ ✓
Production_Bottlin...	🟩 ⚠	⬜ ✓	🟥 ✓ ⚠	⬜ ✓	⬜	🟦 ✓ ⚠	⬜ ✓
Production_Users	🟩	⬜	⬜	🟦 ✓	🟦 ✓ ⚠	🟩	⬜
Quarantined_Syste...	⬜	⬜ ✓	⬜ ✓	⬜ ✓	⬜ ✓	⬜ ✓	⬜ ✓

⬜ No Traffic 🟩 Traffic 🟥 Denied Traffic 🟦 Traffic with Custom Policy ⚠ Offending Traffic ? Unsupported policy 🕓 Policy Analysis Pending 👁 Policy Monitor Mode ⊘ Policy Disabled ✓ Policy Enabled

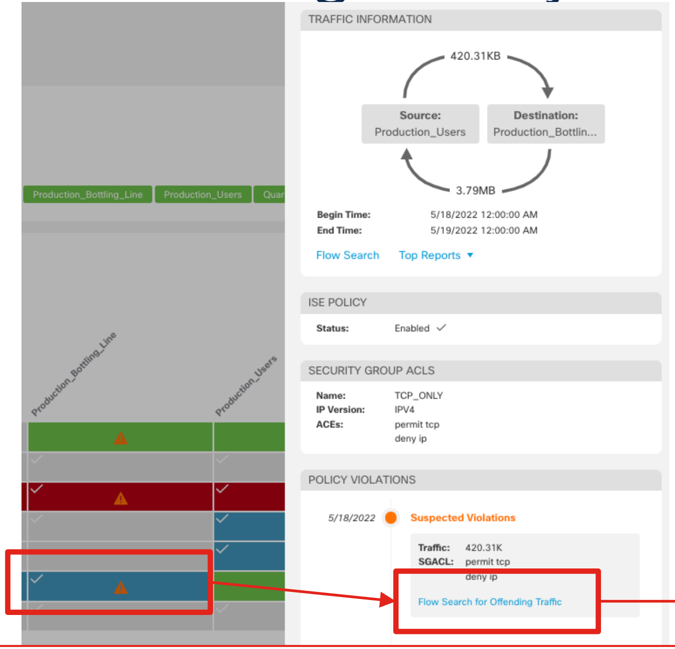
Policy Analysis:

- Triangle – Potential policy violation
- Question Mark – Unsupported policy

- Gray – no traffic
- Green – there is traffic and a *permit IP* ACL exists
- Red – there is traffic and a *deny IP* ACL exists
- Blue – there is traffic and an ACL other than *permit IP* or *deny IP* exists

Demo

Evaluating Policy



TRAFFIC INFORMATION

420.31KB

Source: Production_Users

Destination: Production_Bottlin...

3.79MB

Begin Time: 5/18/2022 12:00:00 AM
End Time: 5/19/2022 12:00:00 AM

Flow Search   Top Reports ▾

ISE POLICY

Status: Enabled ✓

SECURITY GROUP ACLS

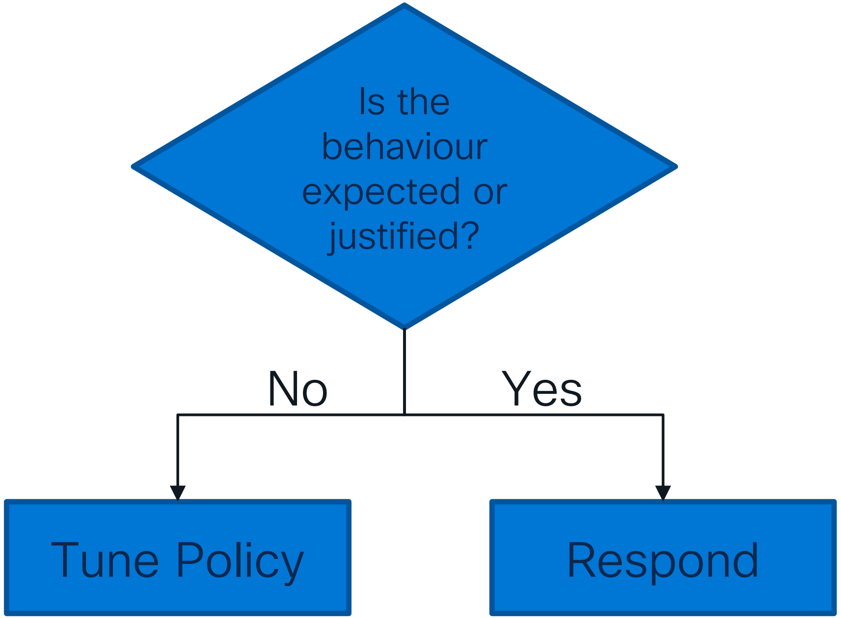
Name: TCP_ONLY
IP Version: IPV4
ACEs: permit tcp
deny ip

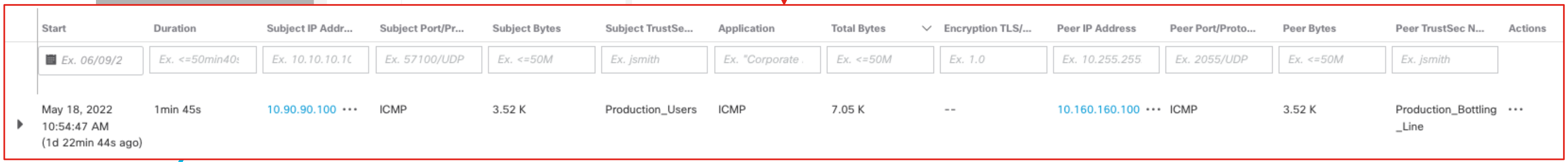
POLICY VIOLATIONS

5/18/2022 ● Suspected Violations

Traffic: 420.31K
SGACL: permit tcp
deny ip

Flow Search for Offending Traffic





Start	Duration	Subject IP Addr...	Subject Port/Pr...	Subject Bytes	Subject TrustSe...	Application	Total Bytes	Encryption TLS/...	Peer IP Address	Peer Port/Proto...	Peer Bytes	Peer TrustSec N...	Actions
Ex. 06/09/2	Ex. <=50min40s	Ex. 10.10.10.1(	Ex. 57100/UDP	Ex. <=50M	Ex. jsmith	Ex. "Corporate	Ex. <=50M	Ex. 1.0	Ex. 10.255.255	Ex. 2055/UDP	Ex. <=50M	Ex. jsmith	
May 18, 2022 10:54:47 AM (1d 22min 44s ago)	1min 45s	10.90.90.100 •••	ICMP	3.52 K	Production_Users	ICMP	7.05 K	--	10.160.160.100 •••	ICMP	3.52 K	Production_Bottling _Line	•••

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 Live!

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

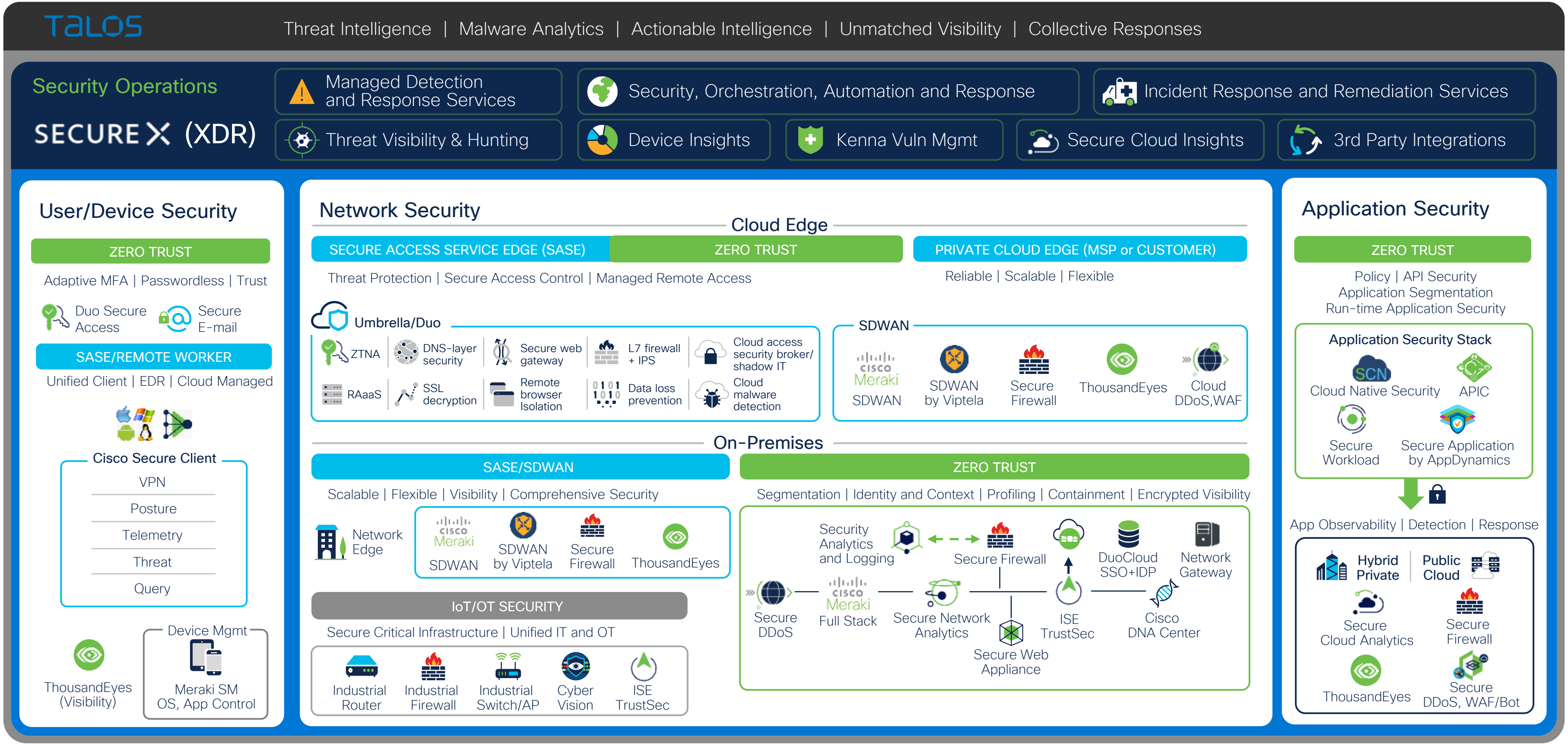
Cisco Guided Study Groups
180-day certification prep program with learning and support

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**

CISCO SECURE

Security Reference Architecture



TALOS

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECUREX (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt

Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- CISCO Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- CISCO Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- CISCO Meraki Full Stack
- Secure Network Analytics
- ISE TrustSec
- Cisco DNA Center
- Secure Web Appliance

Application Security

ZERO TRUST

Policy | API Security

Application Segmentation

Run-time Application Security

Application Security Stack

- SCN Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

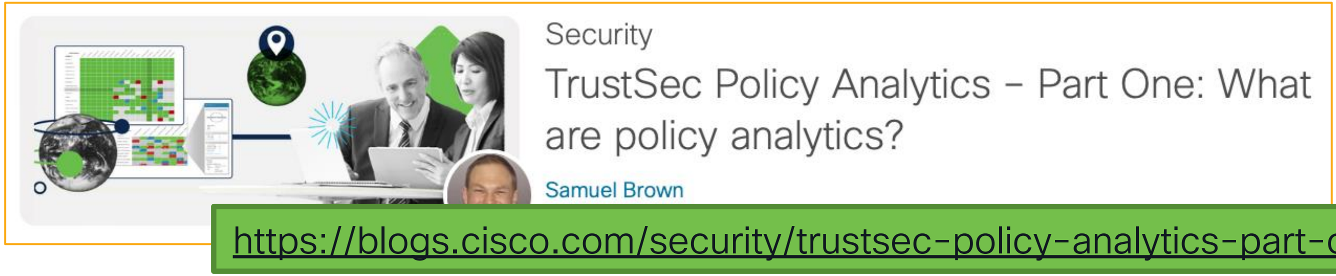
App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Some awesome related sessions!

Session ID	Title	When
BRKSEC-2053	Zero Trust: Securing the Evolving Workplace	Monday at 4:00 PM
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

Reading: TrustSec Policy Analytics Blog Series

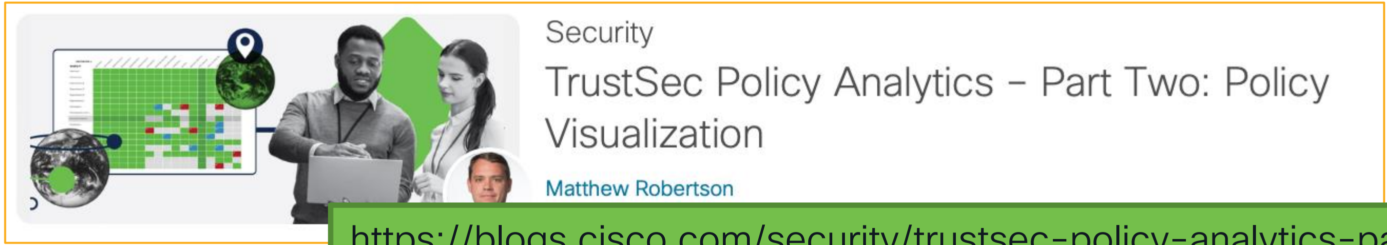


Security

TrustSec Policy Analytics – Part One: What are policy analytics?

Samuel Brown

https://blogs.cisco.com/security/trustsec-policy-analytics-part-one-what-are-policy-analytics

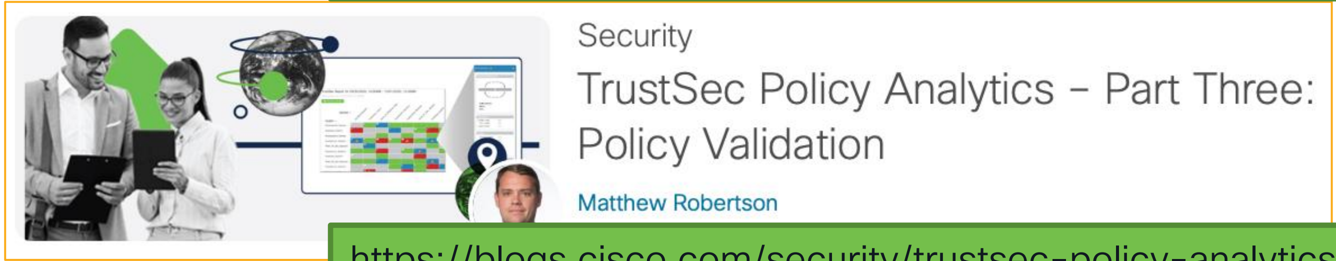


Security

TrustSec Policy Analytics – Part Two: Policy Visualization

Matthew Robertson

https://blogs.cisco.com/security/trustsec-policy-analytics-part-two-policy-visualization



Security

TrustSec Policy Analytics – Part Three: Policy Validation

Matthew Robertson

https://blogs.cisco.com/security/trustsec-policy-analytics-part-three-policy-validation

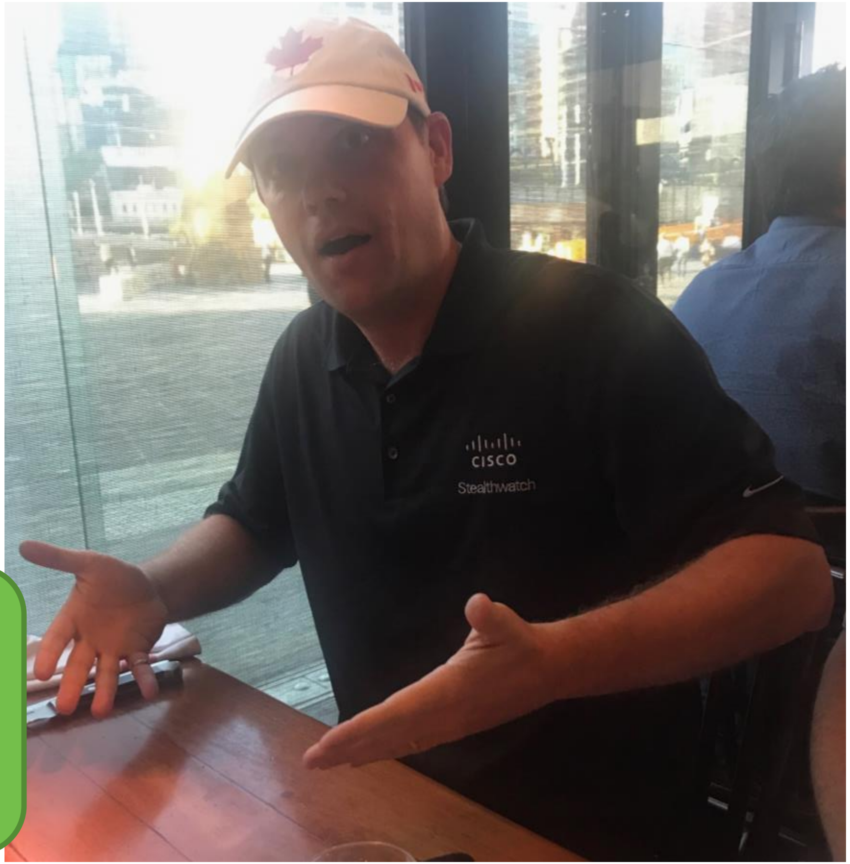
Technical Session Surveys

- 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

Network security policy can be effectively designed, verified and validated with data analytics

Keep your eyes open
and
don’t have your beer stolen.



CISCO The bridge to possible

Thank you

CISCO Live!

#CiscoLive

cisco Live!

#CiscoLive