
cisco Live!
ALL IN

The bridge to possible

Visibility, Detection and Response

With Cisco Secure Network Analytics

Matt Robertson
@mrobertson25

BRKSEC-3019

Cisco Webex App

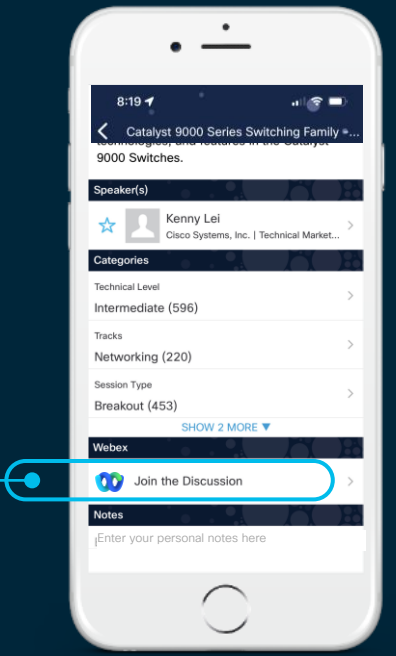
Questions?

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.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-3019

Agenda

Network Behaviour Analytics:
Understanding Secure Network Analytics Detections

Agenda:
- Introduction
- Threat Analytics with SNA
- Extended Detection and Response
- Summary

Extending detections with SecureX

About Me

Matt Robertson

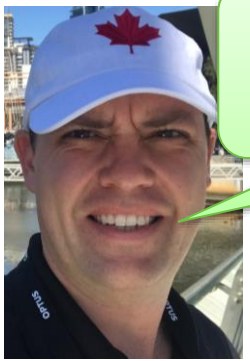
- Principal Technical Marketing Engineer
- Security Analytics and Advanced Threat
- Cisco Live Distinguished Speaker
- 14 years at Cisco: Development, TME, Lancope
- Canadian eh
- Known beer hoser: http://www.beerhoser.ca

So, What are Analytics?

Designing algorithms directed at achieving some outcome.

Machine Learning:
"Field of study that gives computers the ability to learn without being explicitly programmed."
– Arthur Samuel, 1959

Extremely useful in understanding domains that are constantly evolving with a large amount of variability



Key idea!
Analytics are not magic.

Two popular ML approaches:
- Supervised
- Unsupervised

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.

Example Behavioural Analytic Outcomes

BRKSEC-2267

Security Policy:

Analyse network behaviour to design, implement and validate security policy

Threat Detection:

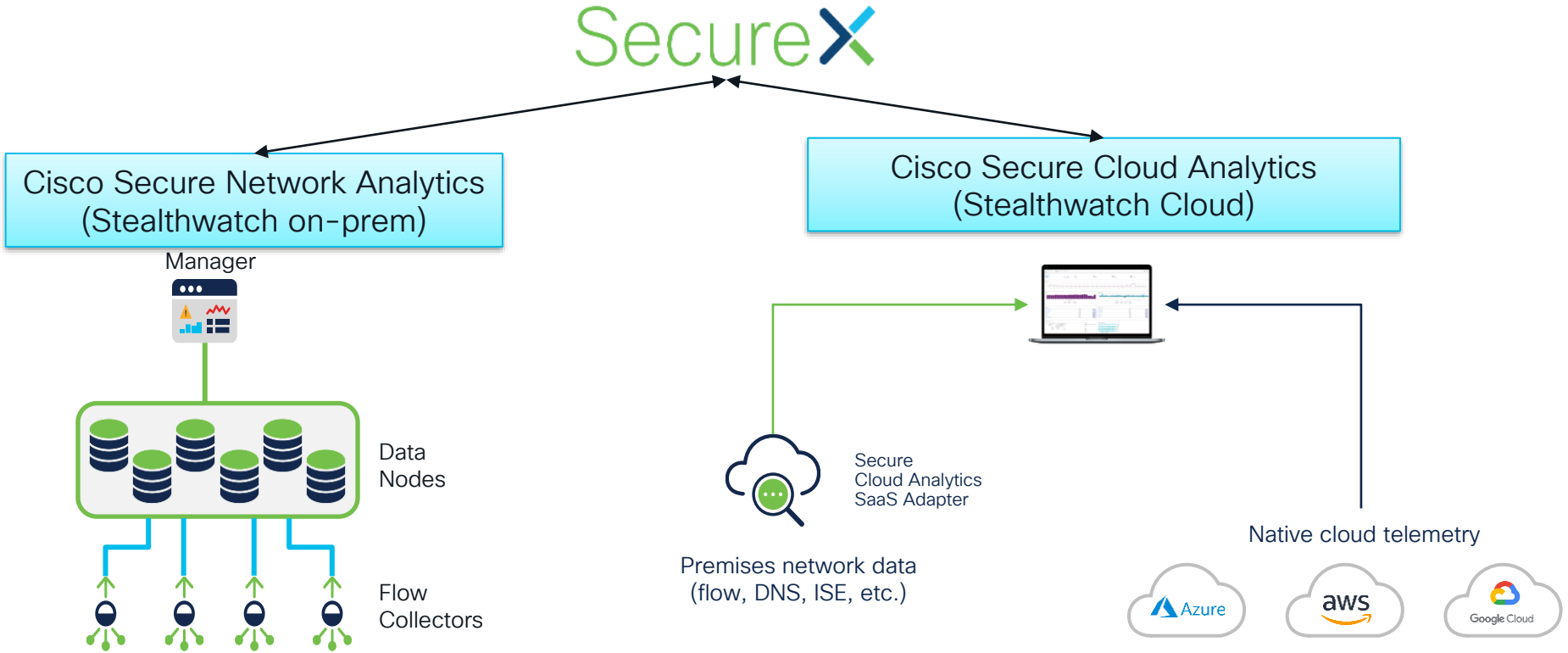
Analyse network behaviour to infer the presence of a threat actor

This Session!

And there are many, many more available outcomes ...

Threat Analytics with SNA

Cisco Secure Network Analytics Portfolio



Layers of Detection in SNA

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

Custom Security Events

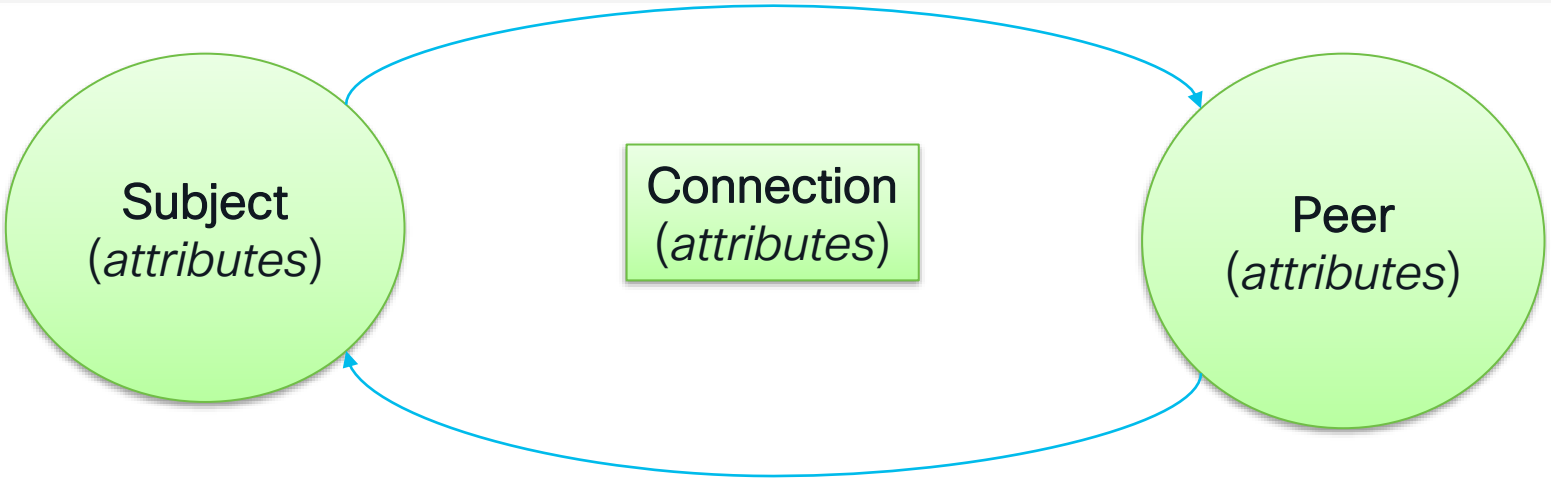
Matt's Note:

When implanted these are often the most immediately actionable events

Custom Security Events

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

Generate an action when a single flow matches the selected conditions

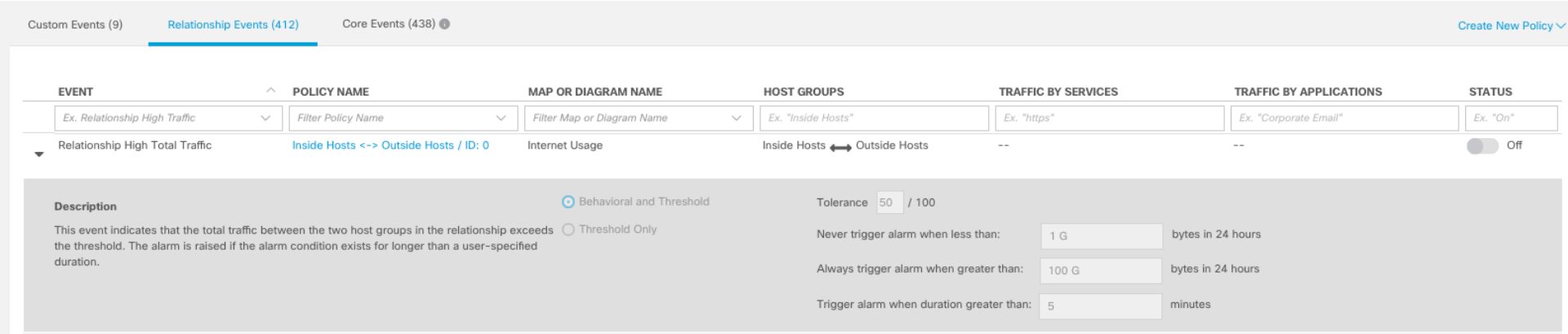


Relationship Events

Matt's Note:

Can be useful for traffic presence/absent notifications

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



Core Events

Core Events

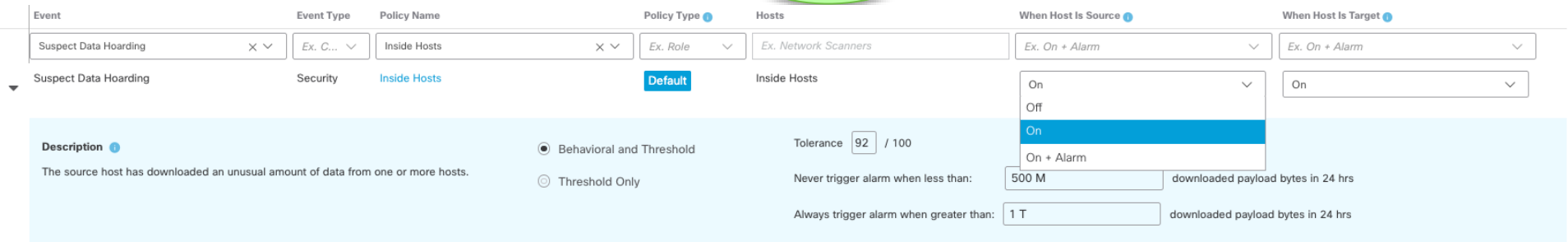
- Runs on each flow collector
- 98+ tunable behavioural algorithms:
  - Statistical anomaly detection
  - Policy based detection
- Some threat Intelligence powered alarms

Entity
(*IP Address, Host Group*)

Matt's Note:

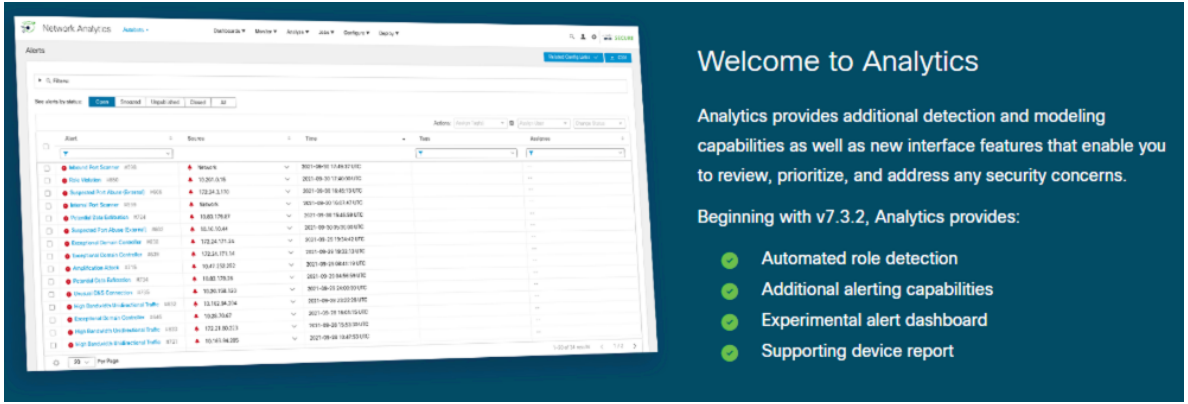
Not every algorithm needs to be used. Operationalising can take some thought, tuning and use of host groups.

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



Analytics Node

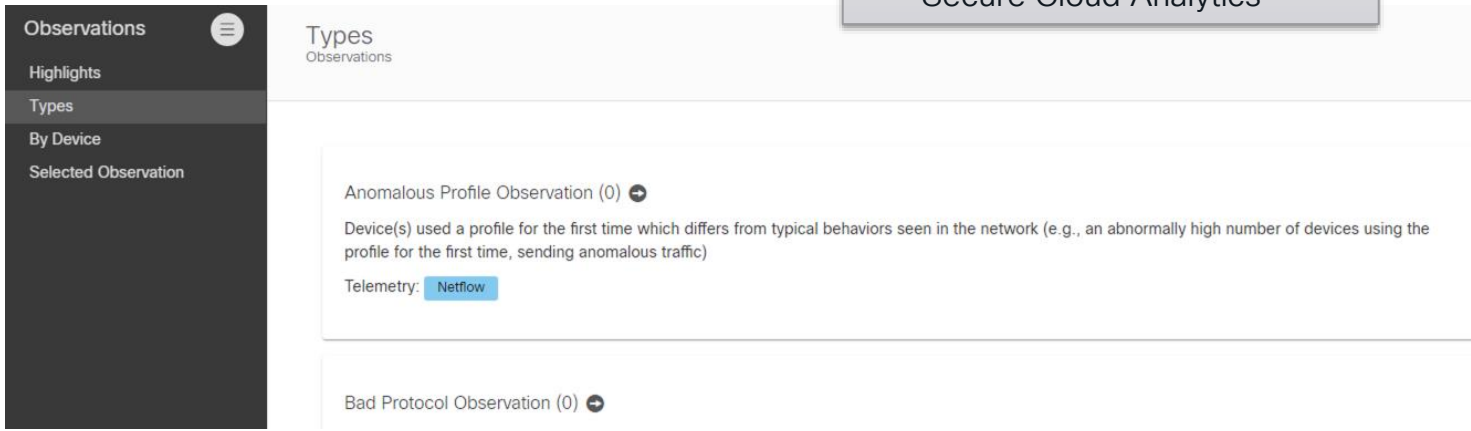
Matt's Note:
New innovation is happening here.



New!

"Analytics" Node

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



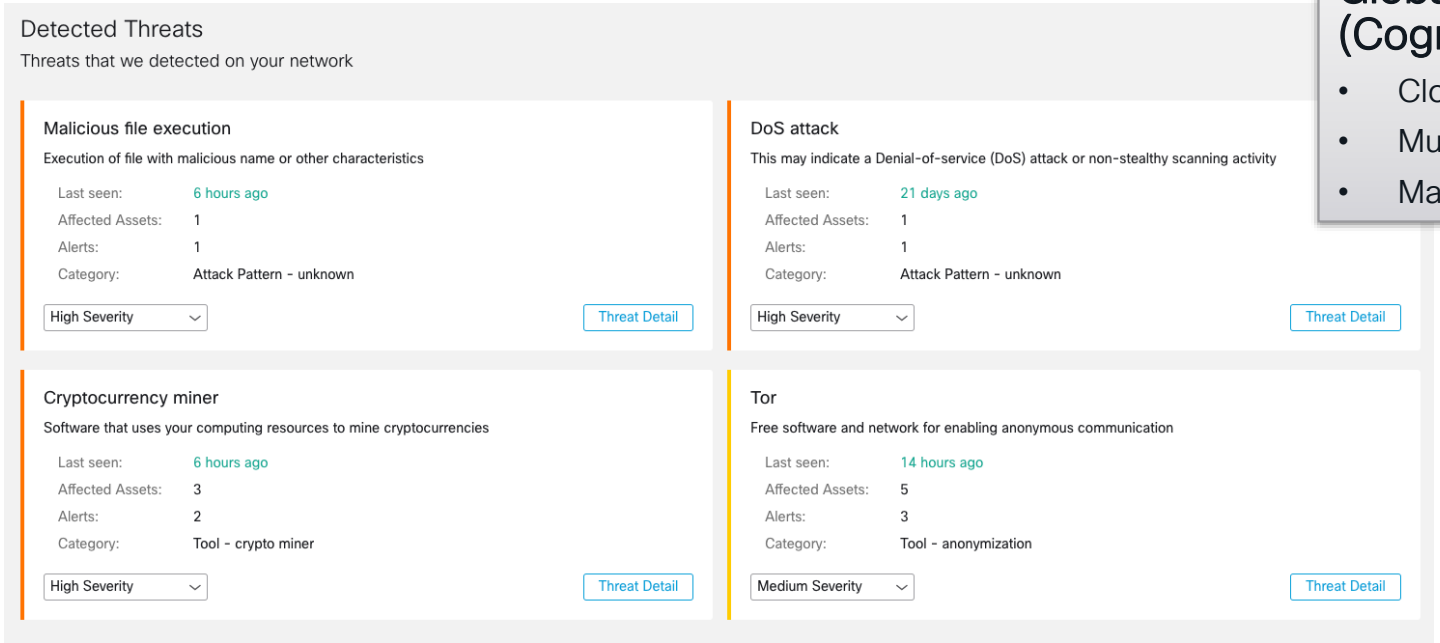
Global Threat Alerts

Matt's Note:

Useful in identifying presence of evasive threats

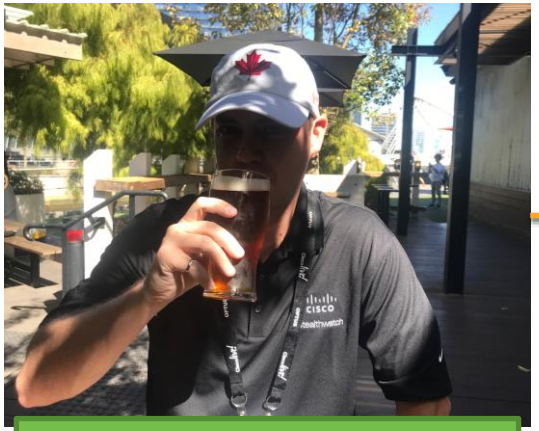
Global Threat Alerts (Cognitive Intelligence)

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



The Thing about Behaviour

There exist conditions that make the observation malicious

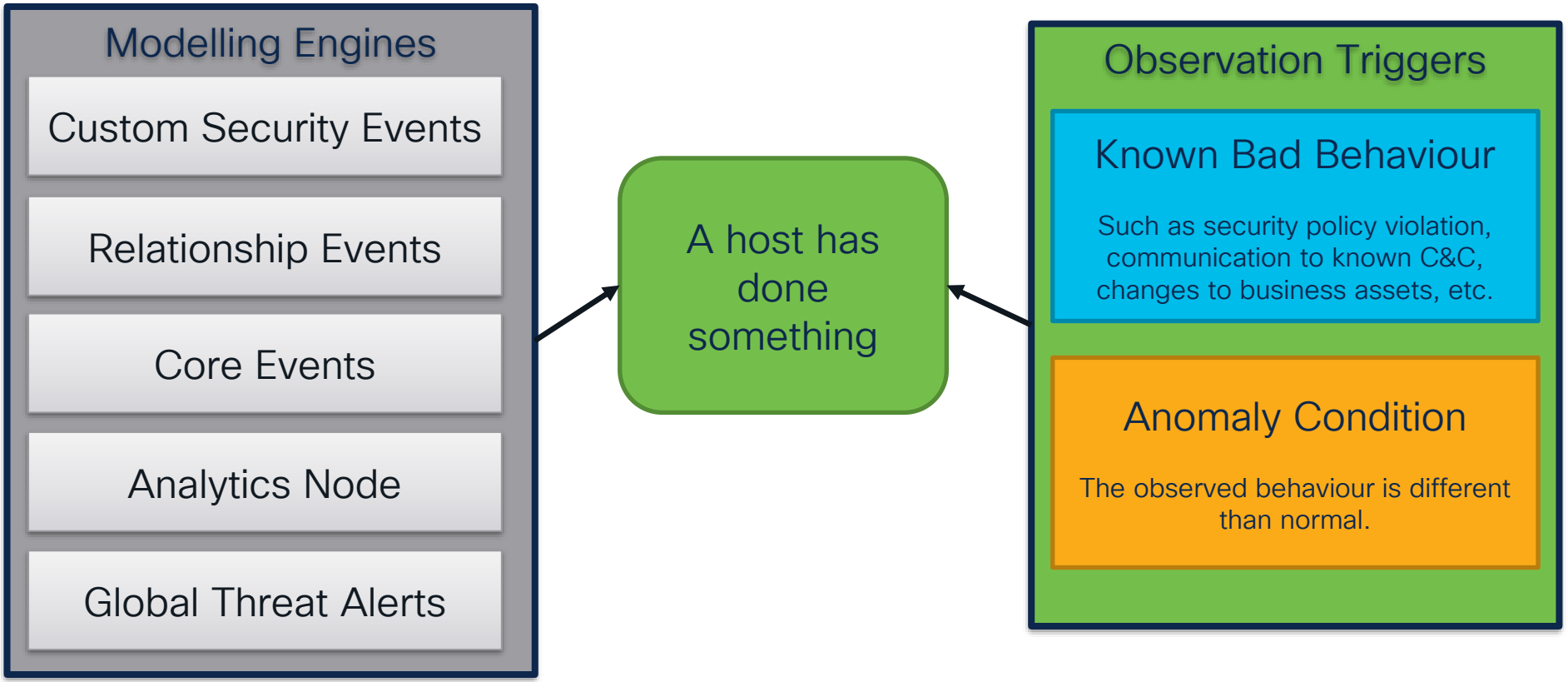


Observation:
This man drinks beer

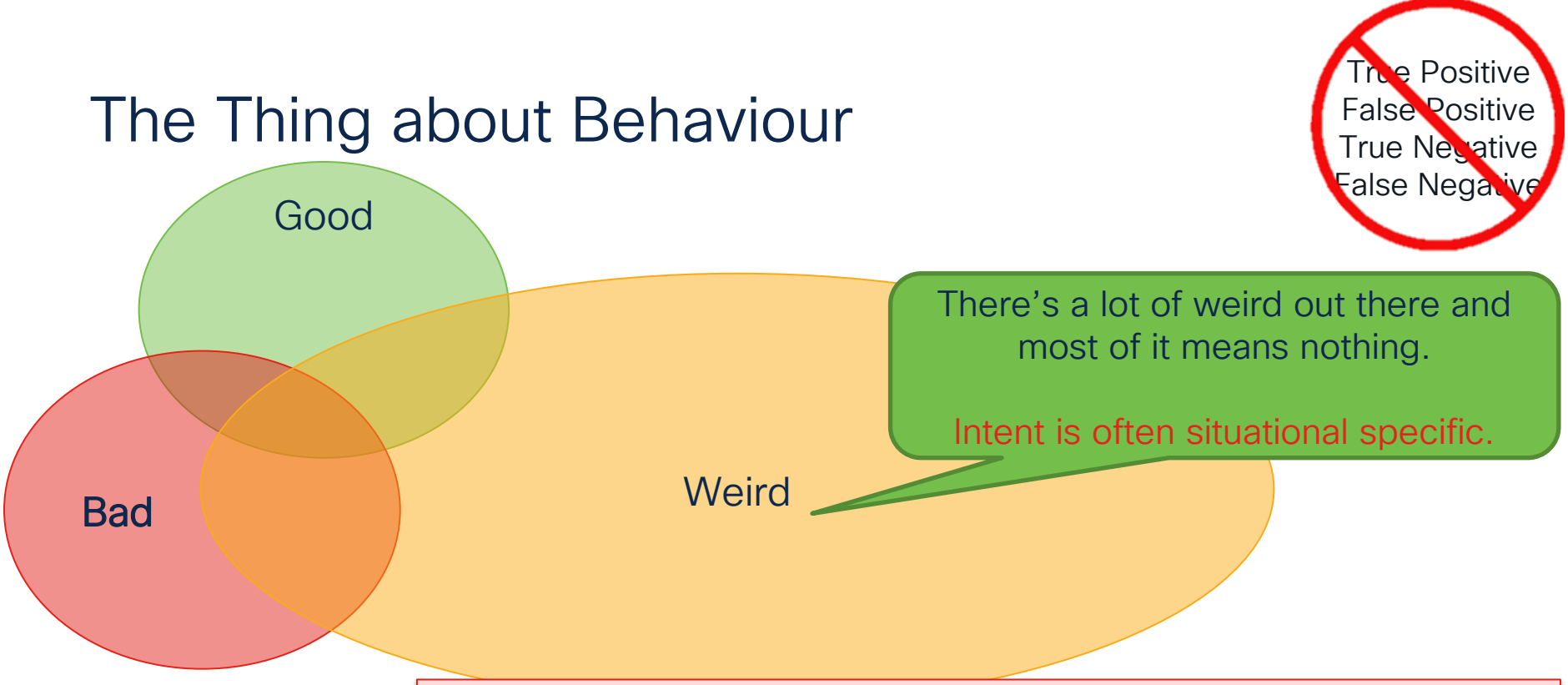
Some observations are just "different than normal"

Key Idea:
Behaviour events are an observation

Behaviour events are an observation



The Thing about Behaviour

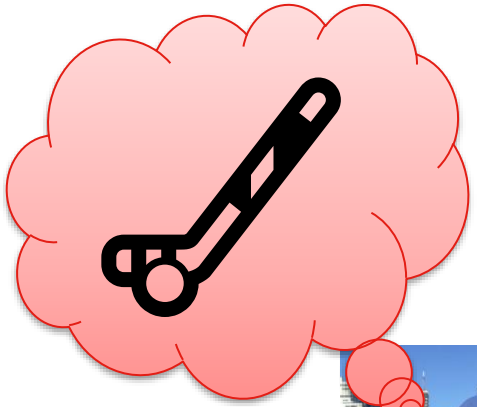


Intent requires business relevant language:
10.10.10.10 just uploaded a large amount of data to 128.107.78.10
versus
The PCI server just uploaded a large amount of data to an external server

Demo

Extended Detection and Response

Making the Alarms Business Relevant

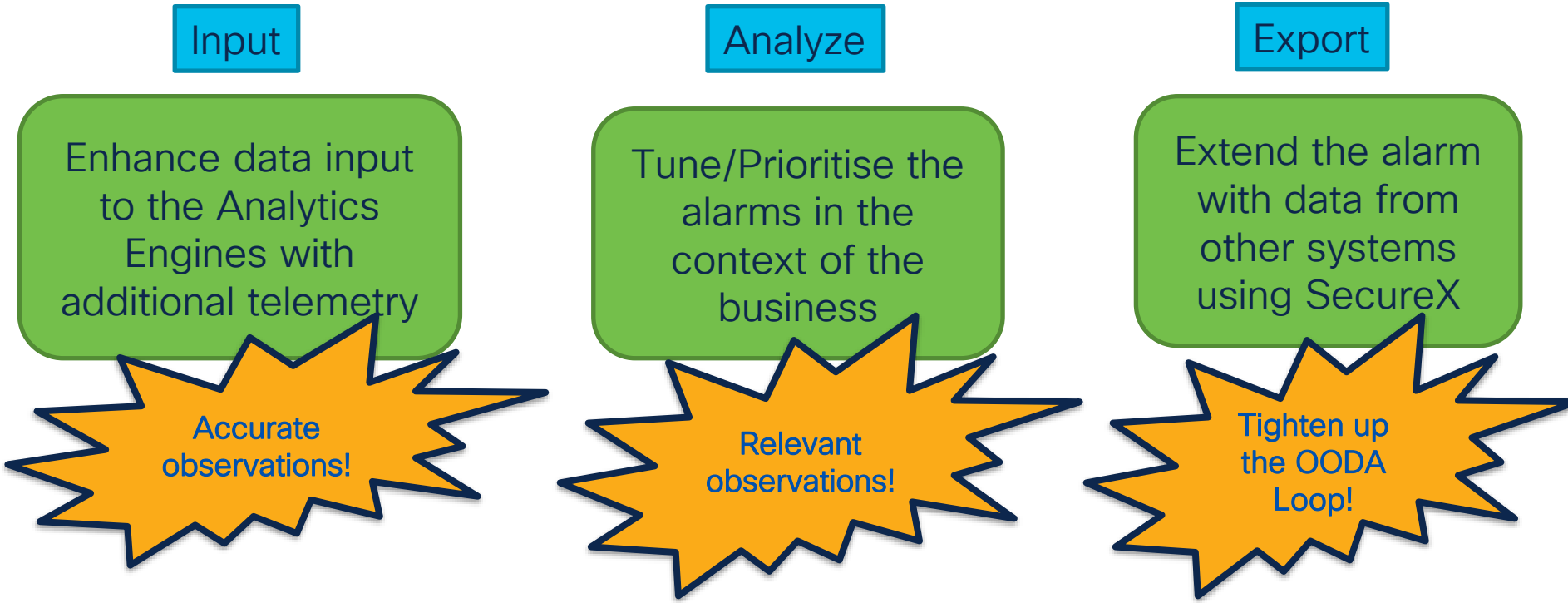


!

37 to 20

What matters to one organization might not matter to another

Making the Alarms Business Relevant



Making the Alarms Business Relevant

Six Phased Approach to Tuning:

1. Classify Inside: Bring RFC1918 and Public IP's Inside
2. Build Policy Groups Framework (Use By Function)
3. Classify Known Scanners
4. Classify Common Server Types
5. Classify Cloud Providers
6. Classify Undefined Applications

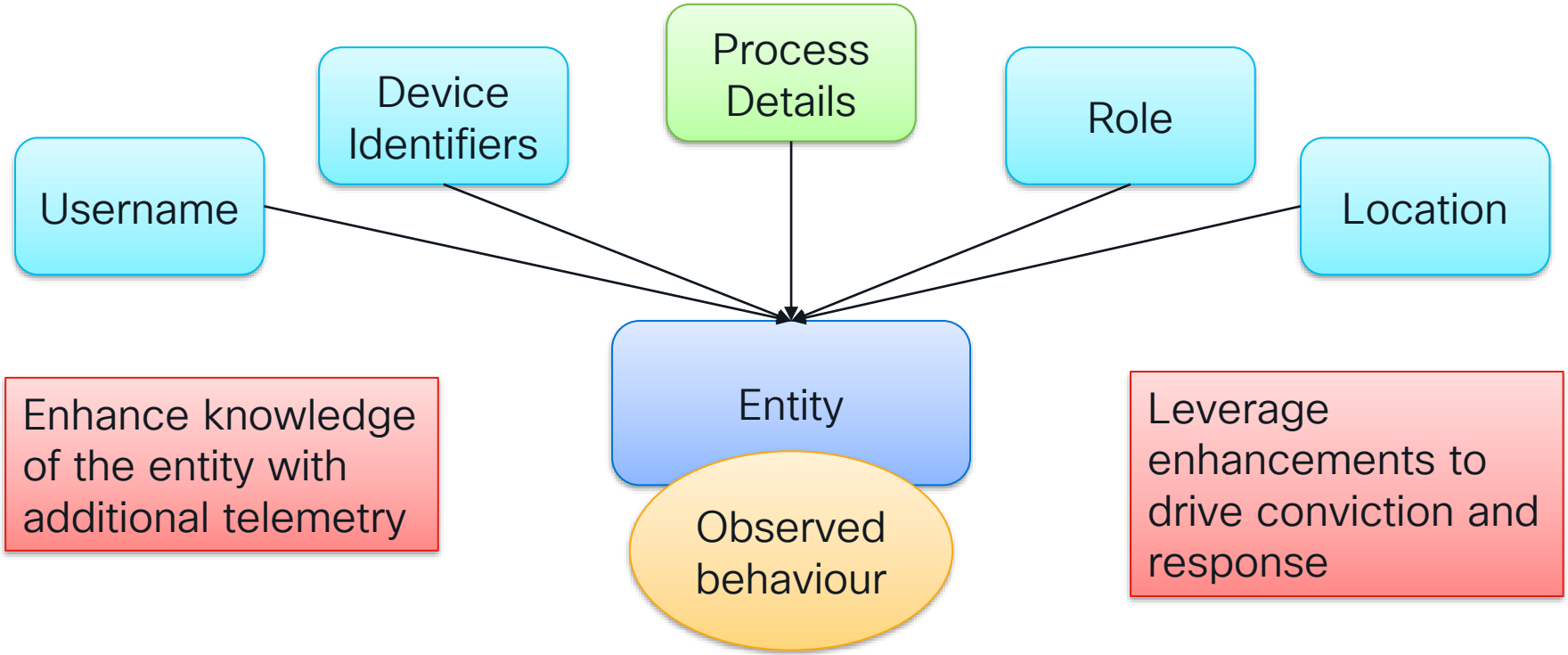
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/Cisco_Secure_Network_Analytics_Six_Phased_Approach_to_Tuning_DV_3_0.pdf

Alarm prioritization with Tiered Alarms:

- Priority A: Severity Critical
- Priority B: Severity Major
- Priority C: Severity Minor

http://b2bcontact.com/cisco-stealthwatch/tiered_alarms/

Input: Enhance the Detection



Prioritizing with MITRE ATT&CK

BRKSEC-2227 – Evaluating and Improving Defenses with MITRE ATT&CK

- Mike McPhee, Tuesday, June 14 1:00 PM – 1:45 PM

MITRE Mappings included in alert details from Global Threat Alerts and Analytics Node

Secure Network Analytics MITRE Mappings

https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-mitre-use-case.pdf

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Spearphishing Attachment
- Spearphishing Link
- Trusted Relationship
- Valid Accounts

Execution
- Dynamic Data Exchange
- Exploitation for Client Execution
- PowerShell
- Scheduled Task
- Windows Management
- Instrumentation
- Windows Remote Management

Exfiltration
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Scheduled Transfer

Privilege Escalation
- Scheduled Task
- Valid Accounts

Defense Evasion
- BITS Jobs
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- Port Knocking
- Redundant Access
- SIP and Trust Provider Hijacking
- Valid Accounts
- Web Service

Credential Access
- Account Manipulation
- Brute Force
- Forced Authentication
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing

Collection
- Data Staged
- Data from Information Repositories
- Data from Network Shared Drive
- Email Collection

Discovery
- Account Discovery
- Application Window Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Remote System Discovery
- System Information Discovery
- System Network Connections Discovery
- System Service Discovery

Lateral Movement
- Application Deployment Software
- Exploitation of Remote Services
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Windows Admin Shares
- Windows Remote Management

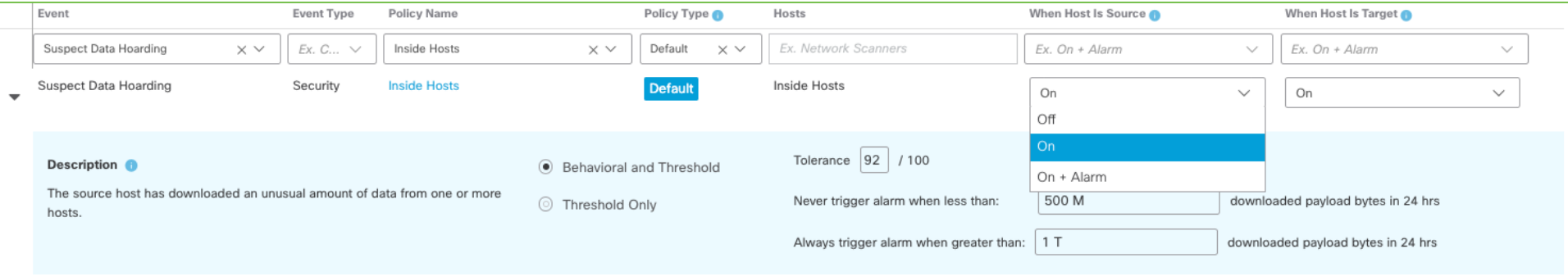
Persistence
- Account Manipulation
- BITS Jobs
- External Remote Services
- Port Knocking
- Redundant Access
- SIP and Trust Provider Hijacking
- Scheduled Task
- Valid Accounts

Command and Control
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-Stage Channels
- Multi-hop Proxy
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

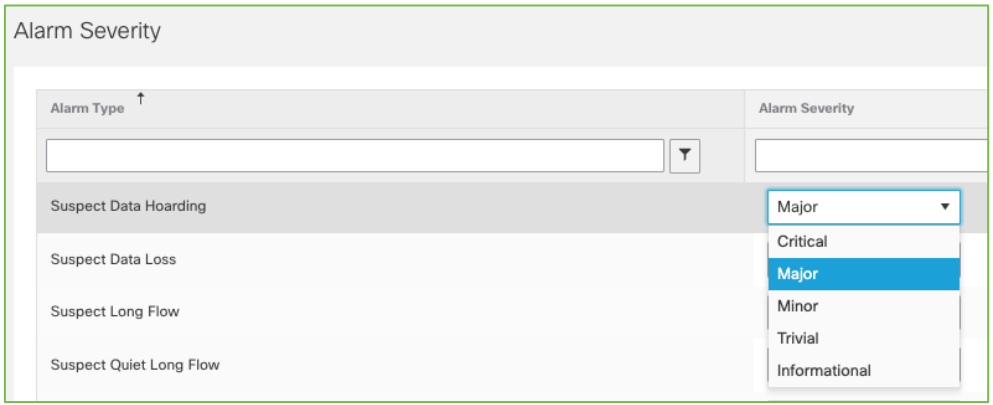
Impact
- Network Denial of Service
- Resource Hijacking

To learn more about Stealthwatch, please visit cisco.com/go/stealthwatch
Sign up for a free 2-week visibility assessment here

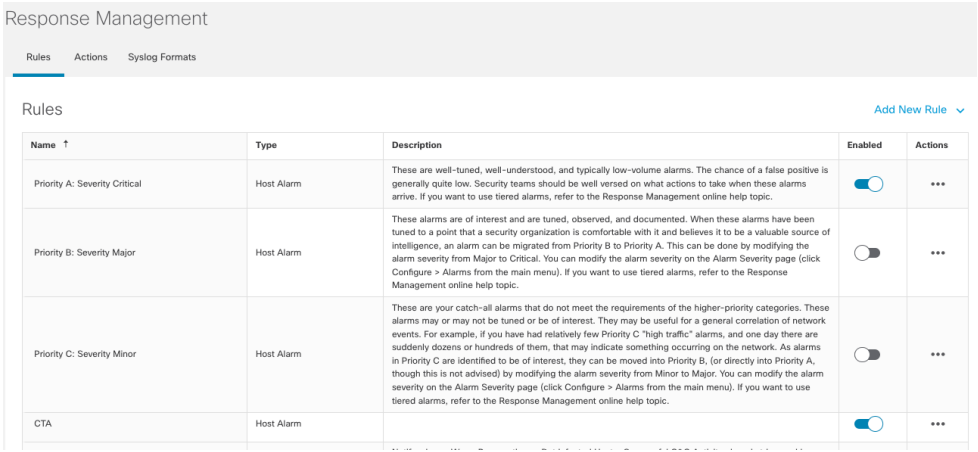
Tuning the Corpus



- Create custom security events
- Enable/Disable Alarms by type/role
- Tune thresholds
- Adjust Alarm severity (Tiered alarms)

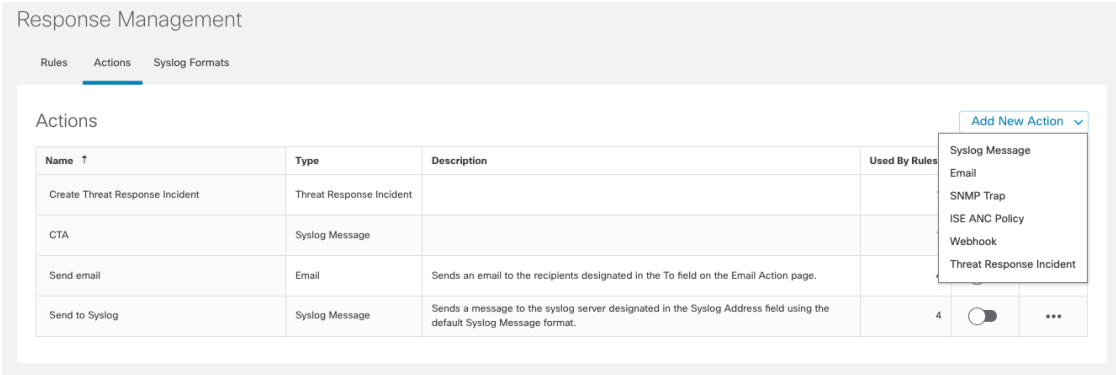


Export: alarm response rules & actions



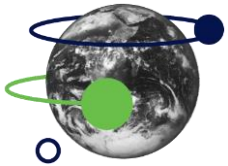
- Create rules to automate response/export on occurrence of an alarm
- Leverage built-in Tiered Alarm Severity rules

- Define automated actions when alarm rule is hit: ISE ANC, syslog, etc.
- Create SecureX Threat Response incident



Extended Detection and Response with SecureX

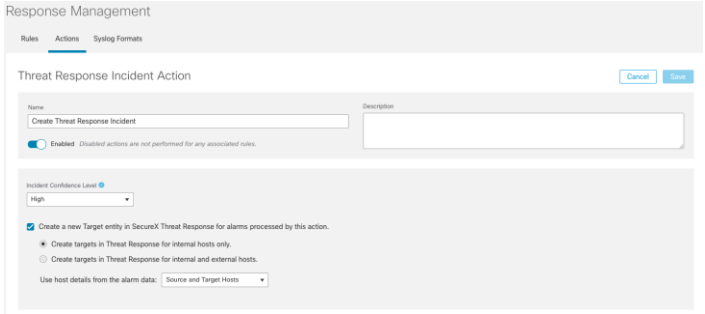
Secure Network Analytics

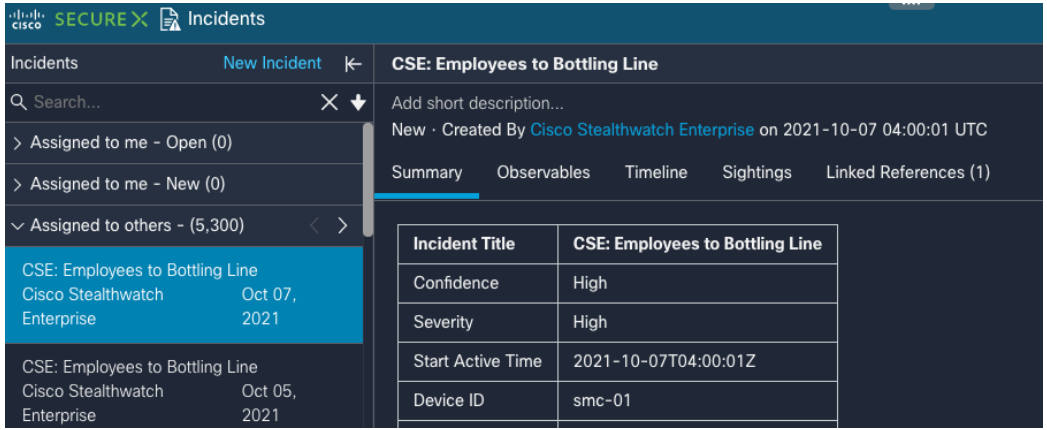


Create incidents automatically in Incident Manger as an alarm action

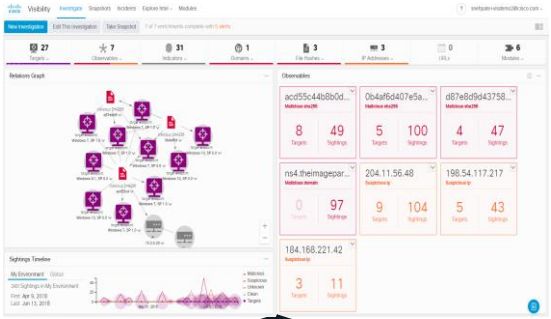
SECURE X

Incident Manager





SecureX Threat Response



Threat Response automatically queries integrated products via APIs to enrich investigation

Collect everything integrated products knows about the queried observables in one place for faster investigation

Virus Total | TALOS | SMA | ●●● | Endpoint | Umbrella | SNA | FTD | More ..

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 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

SECURE X (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

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

App Observability | Detection | Response

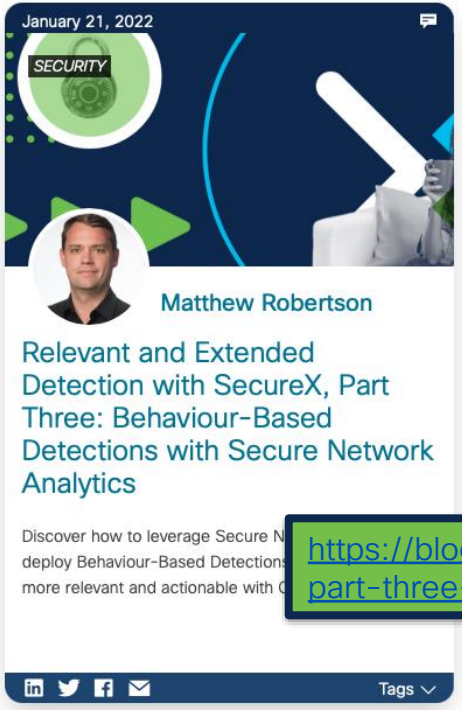
- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Some awesome related sessions!

Session ID	Title	When
BRKSEC-2227	Evaluating and Improving Defenses with MITRE ATT&CK	Tuesday at 1:00 PM
BRKSEC-2267	Building Network Security Policy Through Data Intelligence	Tuesday at 2:30 PM
BRKSEC-1483	SecureX All The Things	Thursday at 8:00 AM
BRKMER-2003	Meraki & Secure Network and Cloud Analytics: Threat Detection for the Rest of Us	Thursday at 9:30 AM
BRKSEC-2201	SecureX and Secure Firewall Better Together	Thursday at 10:30 AM

Reading: Relevant and Extended Detection with SecureX Blog Series

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-secureX



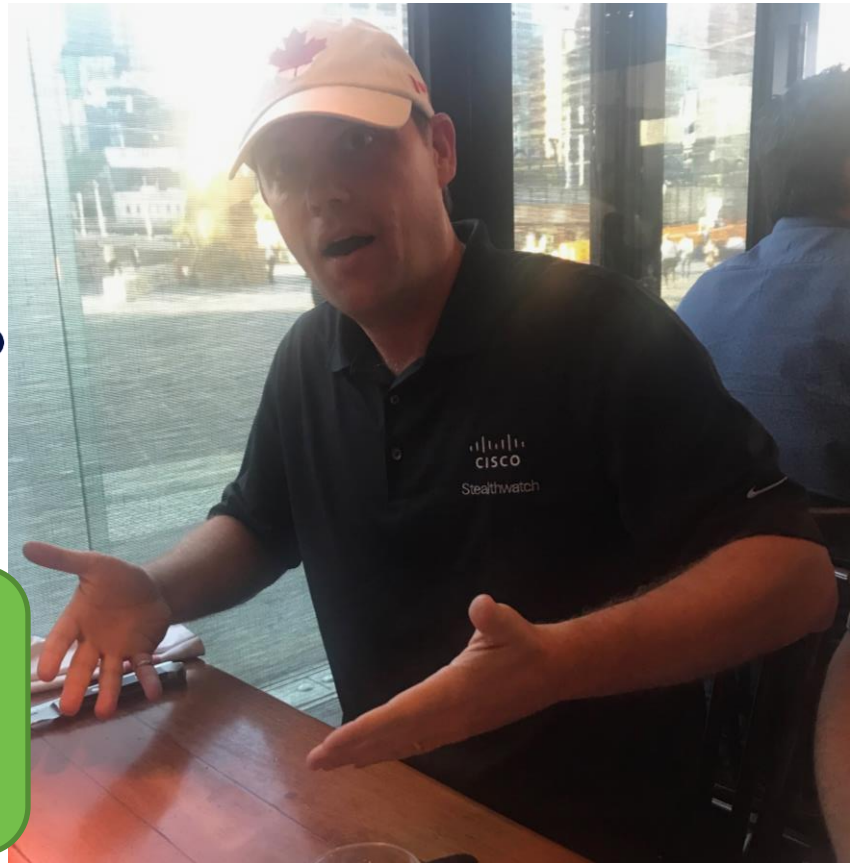
https://blogs.cisco.com/security/relevant-and-extended-detection-with-securex-part-three-behaviour-based-detections-with-secure-network-analytics

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

Behaviour-based detections are a critical component of the modern security operations center



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

Thank you


cisco Live!
ALL IN