

CISCO *Live!*



#CiscoLive



The bridge to possible

Visibility, Detection and Response

With Cisco Secure Network Analytics

Matt Robertson
@mrobertson25
BRKSEC-3019



#CiscoLive

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, Lancopé
- Canadian eh
- Known beer hoser: <http://www.beerhoser.ca>



So, What are Analytics?

Designing algorithms directed at achieving some outcome.

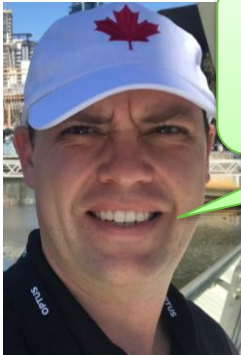
Machine Learning:

“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

SecureX

Cisco Secure Network Analytics
(Stealthwatch on-prem)

Cisco Secure Cloud Analytics
(Stealthwatch Cloud)

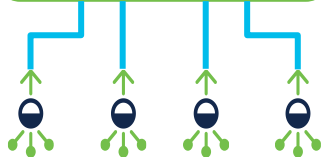
Manager



Data
Nodes



Flow
Collectors



Secure
Cloud Analytics
SaaS Adapter

Premises network data
(flow, DNS, ISE, etc.)



Native cloud telemetry



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

Custom Security Events

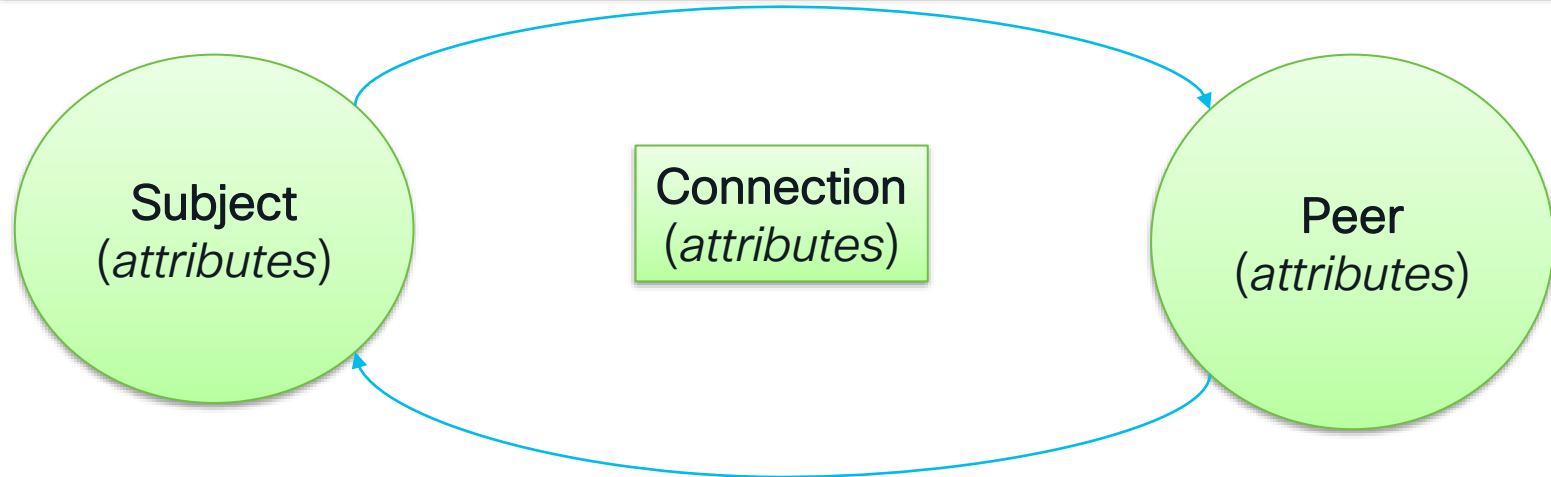
Custom Security Events

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

Matt's Note:

When implanted these are often the most immediately actionable events

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

Custom Events (9) **Relationship Events (412)** Core Events (438) [Create New Policy](#)

EVENT	POLICY NAME	MAP OR DIAGRAM NAME	HOST GROUPS	TRAFFIC BY SERVICES	TRAFFIC BY APPLICATIONS	STATUS
Ex. Relationship High Traffic	Filter Policy Name	Filter Map or Diagram Name	Ex. "Inside Hosts"	Ex. "https"	Ex. "Corporate Email"	Ex. "On"
Relationship High Total Traffic	Inside Hosts <-> Outside Hosts / ID: 0	Internet Usage	Inside Hosts ↔ Outside Hosts	--	--	<input type="checkbox"/> Off

Description

☒ Behavioral and Threshold

This event indicates that the total traffic between the two host groups in the relationship exceeds the threshold. The alarm is raised if the alarm condition exists for longer than a user-specified duration.

☐ Threshold Only

Tolerance / 100

Never trigger alarm when less than: bytes in 24 hours

Always trigger alarm when greater than: bytes in 24 hours

Trigger alarm when duration greater than: minutes

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.

Event	Event Type	Policy Name	Policy Type	Hosts	When Host Is Source	When Host Is Target
Suspect Data Hoarding	Ex. C...	Inside Hosts	Ex. Role	Ex. Network Scanners	Ex. On + Alarm	Ex. On + Alarm
Suspect Data Hoarding	Security	Inside Hosts	Default	Inside Hosts	On	On

Description
The source host has downloaded an unusual amount of data from one or more hosts.

☒ Behavioral and Threshold
☐ Threshold Only

Tolerance / 100

Never trigger alarm when less than: downloaded payload bytes in 24 hrs

Always trigger alarm when greater than: downloaded payload bytes in 24 hrs

Analytics Node

Matt's Note:
New innovation is happening here.

Welcome to Analytics

Analytics provides additional detection and modeling capabilities as well as new interface features that enable you to review, prioritize, and address any security concerns.

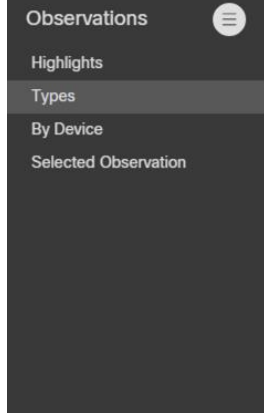
Beginning with v7.3.2, Analytics provides:

- Automated role detection
- Additional alerting capabilities
- Experimental alert dashboard
- Supporting device report

New!

“Analytics” Node

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



Types

Observations

Anomalous Profile Observation (0)

Device(s) used a profile for the first time which differs from typical behaviors seen in the network (e.g., an abnormally high number of devices using the profile for the first time, sending anomalous traffic)

Telemetry: [Netflow](#)

Bad Protocol Observation (0)

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

Detected Threats

Threats that we detected on your network

Malicious file execution

Execution of file with malicious name or other characteristics

Last seen: 6 hours ago
Affected Assets: 1
Alerts: 1
Category: Attack Pattern - unknown

High Severity ▼

[Threat Detail](#)

DoS attack

This may indicate a Denial-of-service (DoS) attack or non-stealthy scanning activity

Last seen: 21 days ago
Affected Assets: 1
Alerts: 1
Category: Attack Pattern - unknown

High Severity ▼

[Threat Detail](#)

Cryptocurrency miner

Software that uses your computing resources to mine cryptocurrencies

Last seen: 6 hours ago
Affected Assets: 3
Alerts: 2
Category: Tool - crypto miner

High Severity ▼

[Threat Detail](#)

Tor

Free software and network for enabling anonymous communication

Last seen: 14 hours ago
Affected Assets: 5
Alerts: 3
Category: Tool - anonymization

Medium Severity ▼

[Threat Detail](#)

The Thing about Behaviour



There exist conditions that make the observation malicious



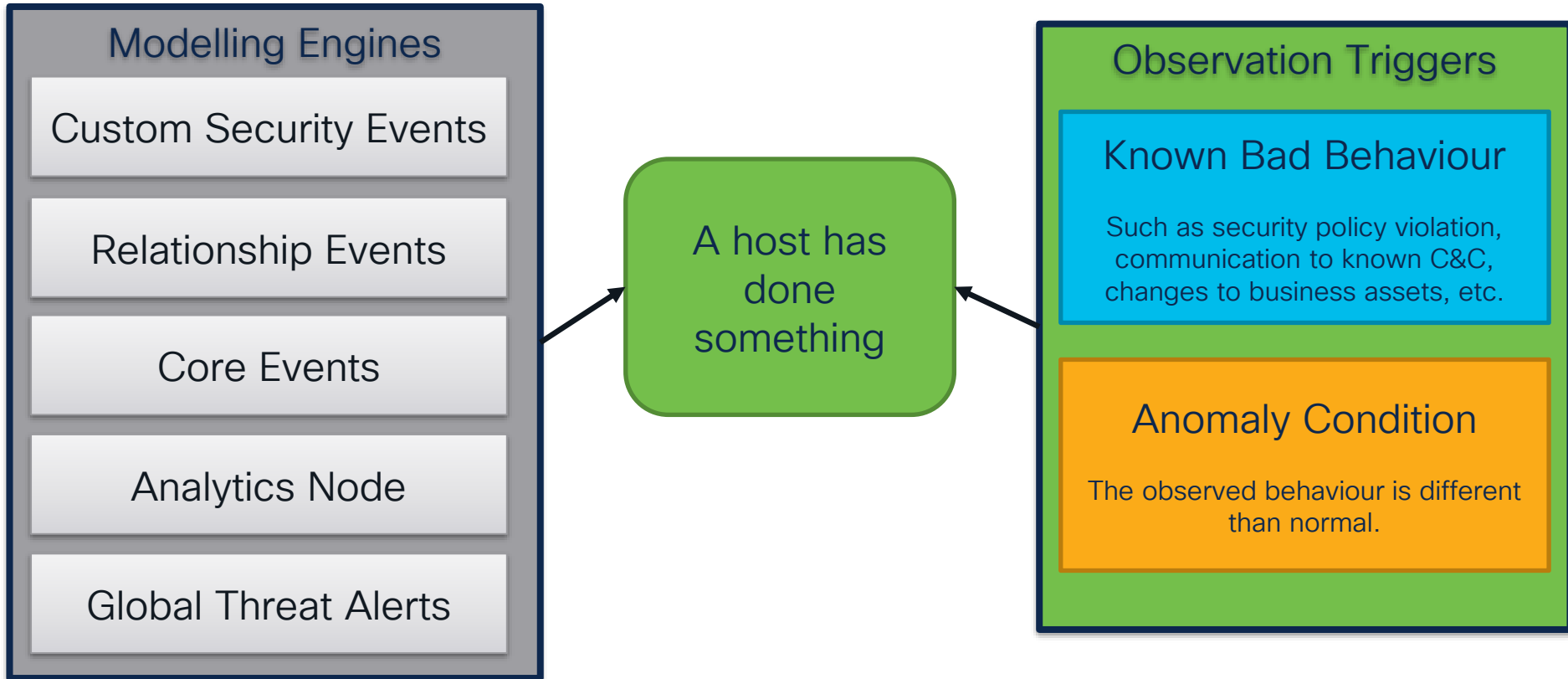
Observation:
This man drinks beer

Some observations are just
“different than normal”

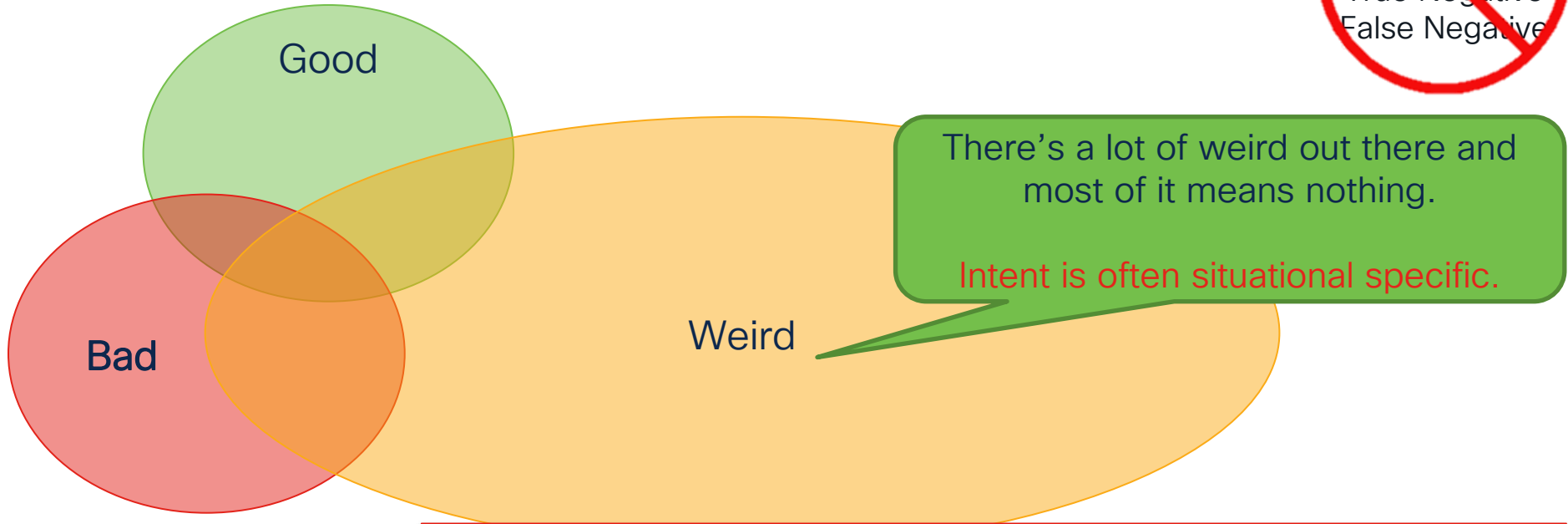


Key Idea:
Behaviour events are an observation

Behaviour events are an observation



The Thing about Behaviour



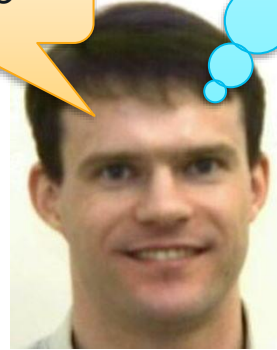
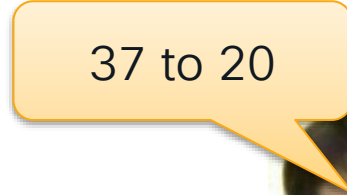
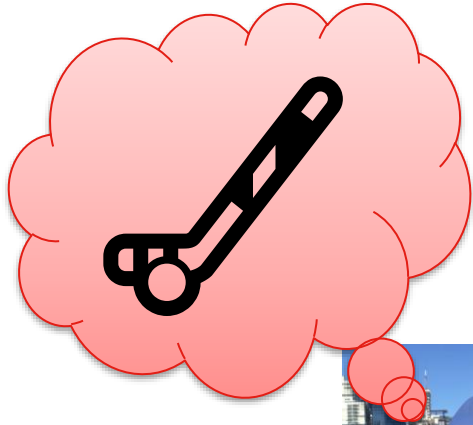
Intent requires business relevant language:
10.10.10.10 just uploaded a large amount of data to 128.107.78.10
versus
The PCI server just uploaded a large amount of data to an external server

Demo



Extended Detection and Response

Making the Alarms Business Relevant



What matters to one organization might not matter to another

Making the Alarms Business Relevant

Input

Enhance data input
to the Analytics
Engines with
additional telemetry

Accurate
observations!

Analyze

Tune/Prioritise the
alarms in the
context of the
business

Relevant
observations!

Export

Extend the alarm
with data from
other systems
using SecureX

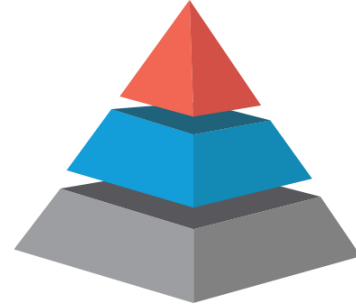
Tighten up
the OODA
Loop!

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

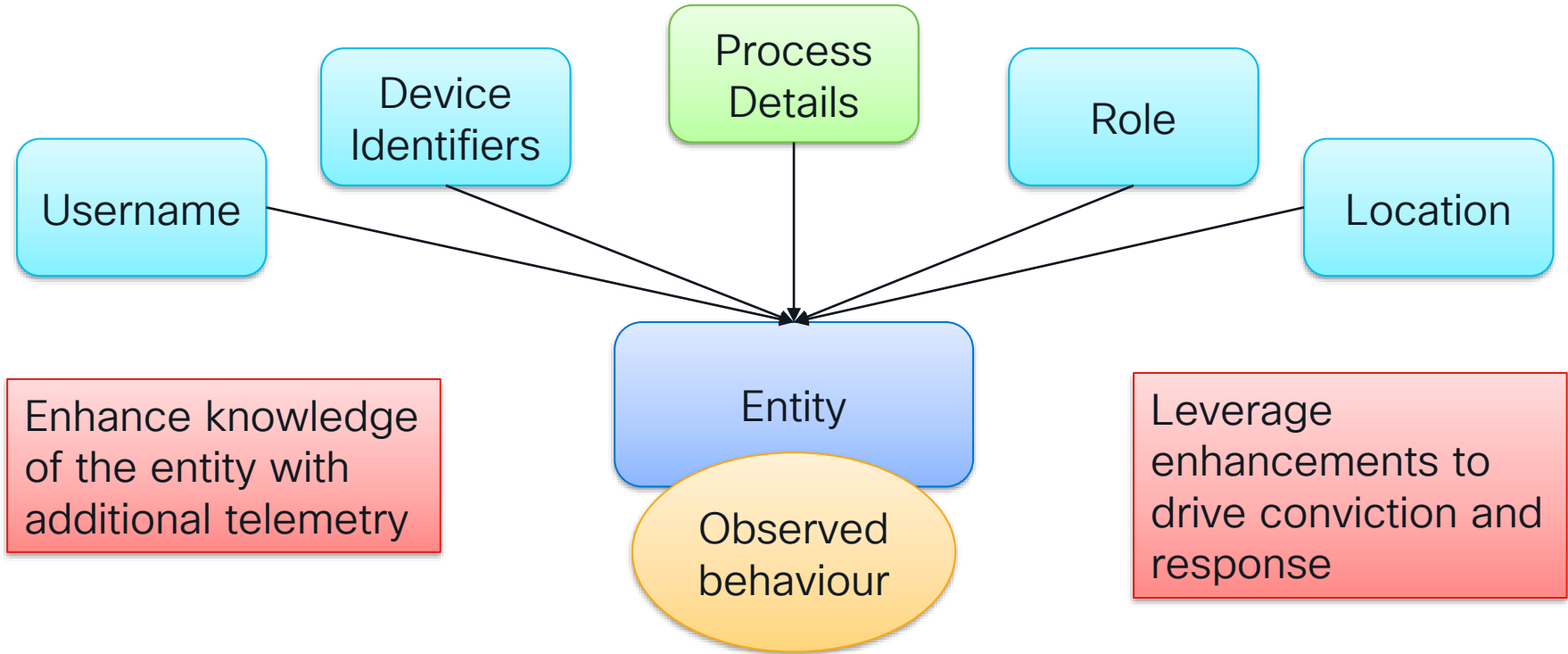


Alarm prioritization with Tiered Alarms:

- 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

Secure Network Analytics MITRE Mappings

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

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

Initial Access	Privilege Escalation	Discovery	Command and Control
<ul style="list-style-type: none">Drive-by CompromiseExploit Public-Facing ApplicationExternal Remote ServicesSpearphishing AttachmentSpearphishing LinkTrusted RelationshipValid Accounts	<ul style="list-style-type: none">Valid Accounts	<ul style="list-style-type: none">Account DiscoveryApplication Window DiscoveryFile and Directory DiscoveryNetwork Service ScanningNetwork Share DiscoveryNetwork SniffingPassword Policy DiscoveryRemote System DiscoverySystem Information DiscoverySystem Network Connections DiscoverySystem Service Discovery	<ul style="list-style-type: none">Commonly Used PortCommunication Through Removable MediaConnection ProxyCustom Cryptographic ProtocolData EncodingData ObfuscationDomain FrontingDomain Generation AlgorithmsFallback ChannelsMulti-Stage ChannelsMulti-hop ProxyMultiband CommunicationMultilayer EncryptionPort KnockingRemote Access ToolsRemote File CopyStandard Application Layer ProtocolStandard Cryptographic ProtocolStandard Non-Application Layer ProtocolUncommonly Used PortWeb Service
Execution	Defense Evasion	Lateral Movement	Impact
<ul style="list-style-type: none">Dynamic Data ExchangeExploitation for Client ExecutionPowerShellScheduled TaskWindows ManagementInstrumentationWindows Remote Management	<ul style="list-style-type: none">BITS JobsDCShadowDeobfuscate/Decode Files or InformationDisabling Security ToolsPort KnockingRedundant AccessSIP and Trust Provider HijackingValid AccountsWeb Service	<ul style="list-style-type: none">Application Deployment SoftwareExploitation of Remote ServicesRemote Desktop ProtocolRemote File CopyRemote ServicesWindows Admin SharesWindows Remote Management	<ul style="list-style-type: none">Network Denial of ServiceResource Hijacking
Exfiltration	Credential Access	Persistence	
<ul style="list-style-type: none">Automated ExfiltrationData CompressedData EncryptedData Transfer Size LimitsExfiltration Over Alternative ProtocolExfiltration Over Command and Control ChannelExfiltration Over Other Network MediumScheduled Transfer	<ul style="list-style-type: none">Account ManipulationBrute ForceForced AuthenticationLLMNR/NBT-NS Poisoning and RelayNetwork Sniffing	<ul style="list-style-type: none">Account ManipulationBITS JobsExternal Remote ServicesPort KnockingRedundant AccessSIP and Trust Provider HijackingScheduled TaskValid Accounts	
	Collection		
	<ul style="list-style-type: none">Data StagedData from Information RepositoriesData from Network Shared DriveEmail Collection		

To learn more about Stealthwatch, please visit [cisco.com/go/stealthwatch](https://www.cisco.com/go/stealthwatch)
Sign up for a free 2-week visibility assessment [here](#)

Tuning the Corpus

Event	Event Type	Policy Name	Policy Type	Hosts	When Host Is Source	When Host Is Target
Suspect Data Hoarding	Ex. C...	Inside Hosts	Default	Ex. Network Scanners	Ex. On + Alarm	Ex. On + Alarm
Suspect Data Hoarding	Security	Inside Hosts	Default	Inside Hosts	On Off On On + Alarm	On

Description

The source host has downloaded an unusual amount of data from one or more hosts.

☒ Behavioral and Threshold
☐ Threshold Only

Tolerance / 100

Never trigger alarm when less than: downloaded payload bytes in 24 hrs

Always trigger alarm when greater than: downloaded payload bytes in 24 hrs

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

Alarm Severity	
Alarm Type ↑	Alarm Severity
<input type="text"/>	<input type="text"/>
Suspect Data Hoarding	Major
Suspect Data Loss	Critical
Suspect Long Flow	Major
Suspect Quiet Long Flow	Minor
	Trivial
	Informational

Export: alarm response rules & actions

Response Management

Rules Actions Syslog Formats

Rules

Add New Rule

Name ↑	Type	Description	Enabled	Actions
Priority A: Severity Critical	Host Alarm	These are well-tuned, well-understood, and typically low-volume alarms. The chance of a false positive is generally quite low. Security teams should be well versed on what actions to take when these alarms arrive. If you want to use tiered alarms, refer to the Response Management online help topic.	<input checked="" type="checkbox"/>	...
Priority B: Severity Major	Host Alarm	These alarms are of interest and are tuned, observed, and documented. When these alarms have been tuned to a point that a security organization is comfortable with it and believes it to be a valuable source of intelligence, an alarm can be migrated from Priority B to Priority A. This can be done by modifying the alarm severity from Major to Critical. You can modify the alarm severity on the Alarm Severity page (click Configure > Alarms from the main menu). If you want to use tiered alarms, refer to the Response Management online help topic.	<input type="checkbox"/>	...
Priority C: Severity Minor	Host Alarm	These are your catch-all alarms that do not meet the requirements of the higher-priority categories. These alarms may or may not be tuned or be of interest. They may be useful for a general correlation of network events. For example, if you have had relatively few Priority C "high traffic" alarms, and one day there are suddenly dozens or hundreds of them, that may indicate something occurring on the network. As alarms in Priority C are identified to be of interest, they can be moved into Priority B, (or directly into Priority A, though this is not advised) by modifying the alarm severity from Minor to Major. You can modify the alarm severity on the Alarm Severity page (click Configure > Alarms from the main menu). If you want to use tiered alarms, refer to the Response Management online help topic.	<input type="checkbox"/>	...
CTA	Host Alarm		<input checked="" type="checkbox"/>	...

- 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

Response Management

Rules Actions Syslog Formats

Actions

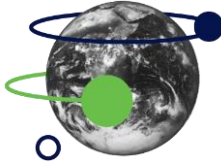
Add New Action

Name ↑	Type	Description	Used By Rules		
Create Threat Response Incident	Threat Response Incident				
CTA	Syslog Message				
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.			
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input type="checkbox"/>	...

Syslog Message
Email
SNMP Trap
ISE ANC Policy
Webhook
Threat Response Incident

Extended Detection and Response with SecureX

Secure
Network
Analytics



Create incidents automatically in
Incident Manager as an alarm action

SECURE X



Incident
Manager

Response Management

Rules Actions Syslog Formats

Threat Response Incident Action

Name: Create Threat Response Incident Description:

☐ Enabled Disabled actions are not performed for any associated rules.

Incident Confidence Level: High

☒ Create a new Target entity in SecureX Threat Response for alarms processed by this action.

☒ Create targets in Threat Response for internal hosts only.

☐ Create targets in Threat Response for internal and external hosts.

Use host details from the alarm data: Source and Target Hosts

Incidents

New Incident

Search...

> Assigned to me - Open (0)

> Assigned to me - New (0)

> Assigned to others - (5,300)

CSE: Employees to Bottling Line

Cisco Stealthwatch Enterprise Oct 07, 2021

CSE: Employees to Bottling Line

Cisco Stealthwatch Enterprise Oct 05, 2021

CSE: Employees to Bottling Line

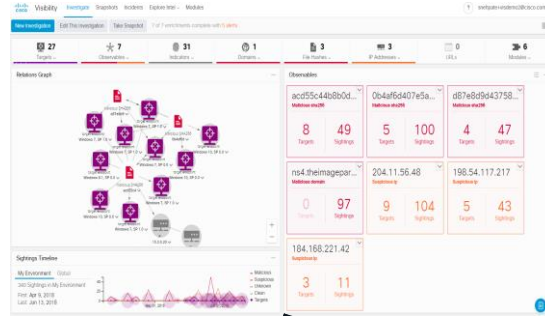
Add short description...

New · Created By Cisco Stealthwatch Enterprise on 2021-10-07 04:00:01 UTC

Summary Observables Timeline Sightings Linked References (1)

Incident Title	CSE: Employees to Bottling Line
Confidence	High
Severity	High
Start Active Time	2021-10-07T04:00:01Z
Device ID	smc-01

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 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**

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

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Threat Protection | Secure Access Control | Managed Remote Access

Reliable | Scalable | Flexible



SDWAN



On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

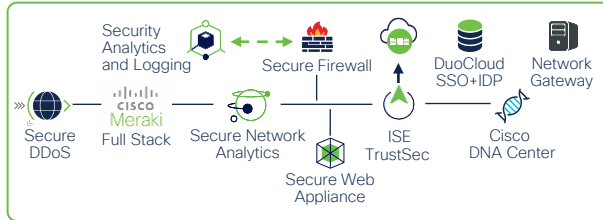


IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



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



Application Security

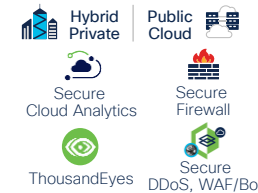
ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack



App Observability | Detection | Response

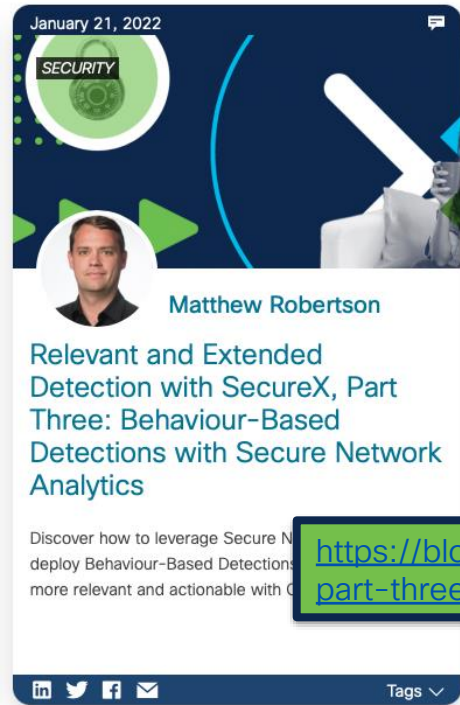


Some awesome related sessions!

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>

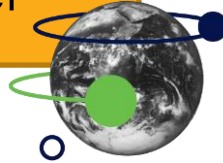
Technical Session Surveys

- 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.





The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive