
cisco Live!
Let's go
#CiscoLive

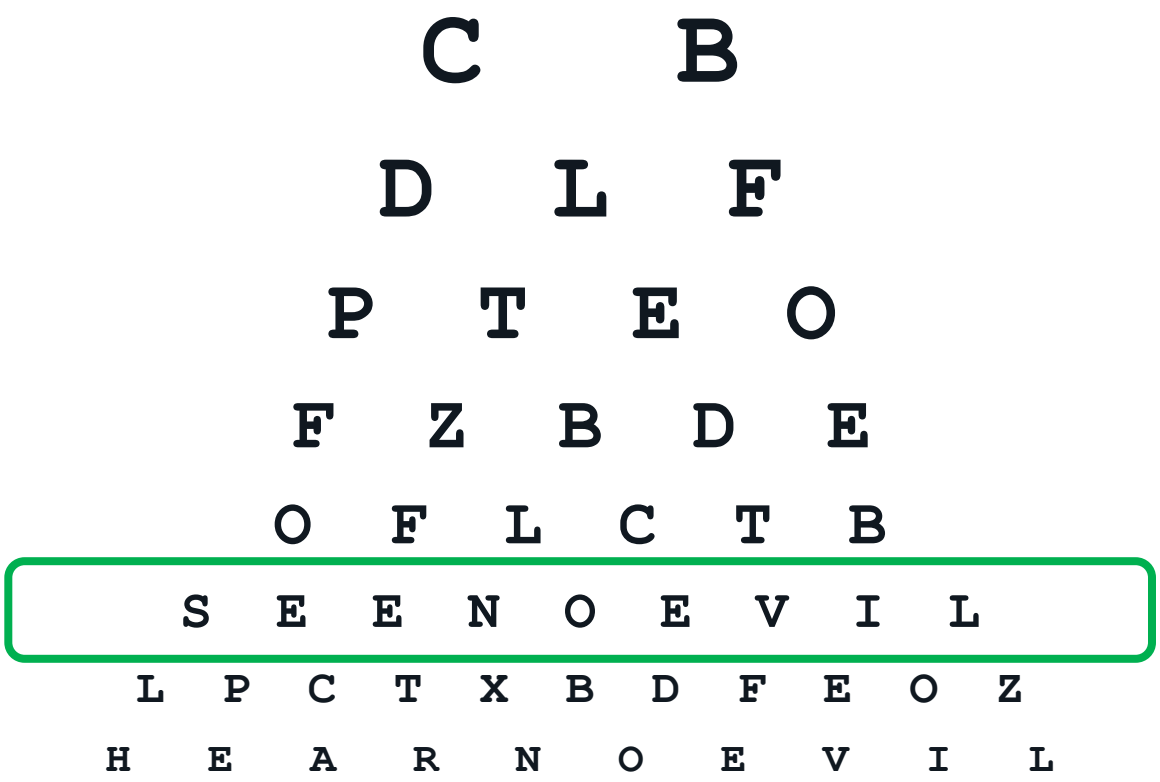
The bridge to possible

Seeing is Believing

Improving XDR Outcomes with Visibility

Mike McPhee, Multi-Domain Cybersecurity Architect

BRKSEC-2084



Cisco Webex App

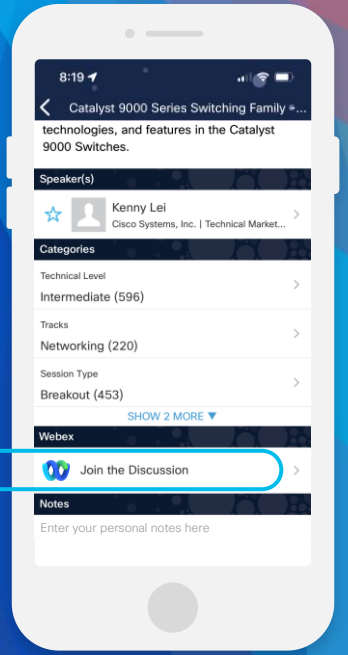
Questions?

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 9, 2023.



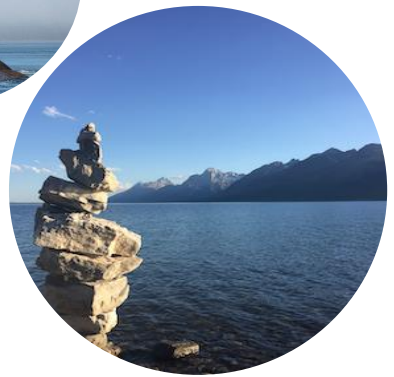
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2084

About me

- Rochester NY (Garbage Plates and Kristen Wig!!!)
- 10 years with Cisco
- 12+ years designing C2 systems
- 6 years in US Navy – “Bubblehead”
- GSE #339 & SANS MSISE
- CCIE 41663 (R&S, Sec) & CCDE 20180018
- homebrewer, woodworker







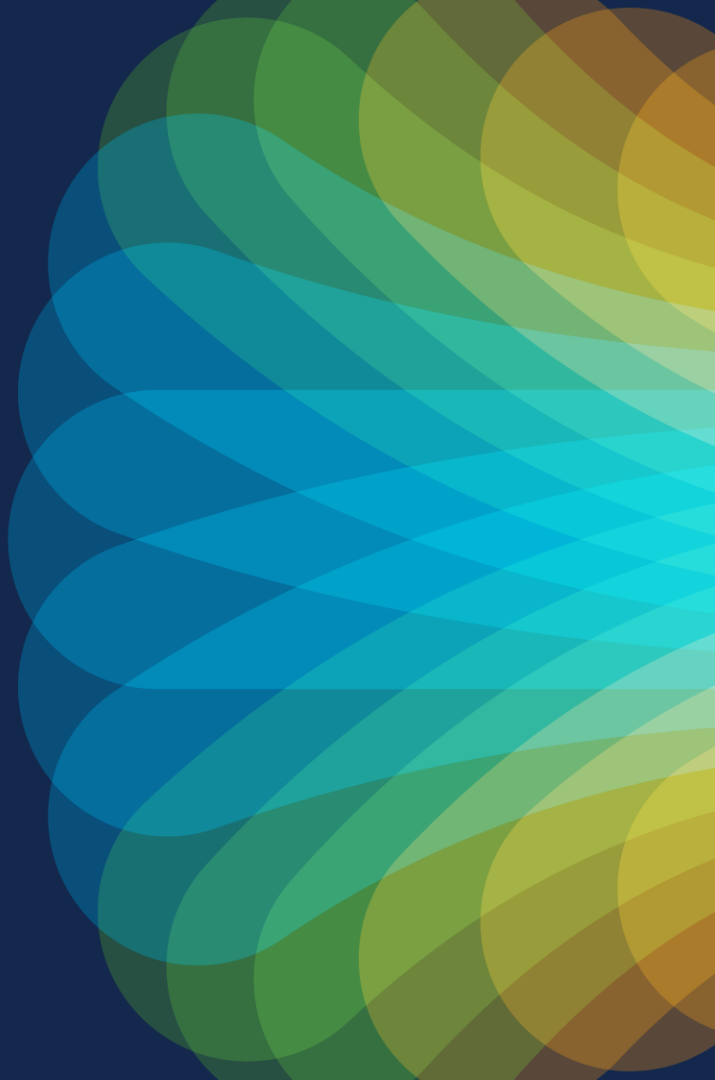
What is this session about?

- Background:
  - Breaches are accelerating
  - Defenders seem to be falling behind
- Problem:
  - We don't truly understand what our environments are doing, because…
  - We've all focused on the wrong part of the equation
- Solution:
  - Well, we're going to have to wait and see on that ;)

Agenda

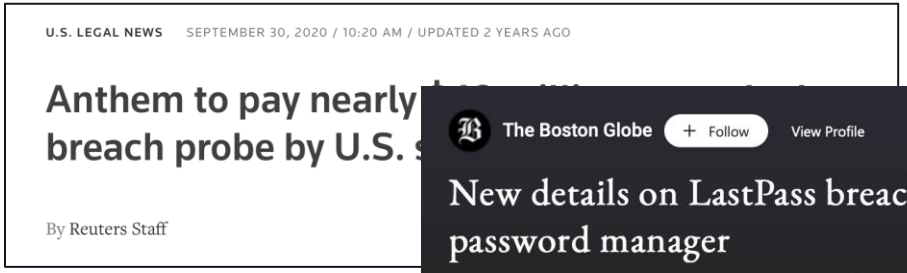
- Why are we in pain?
- Where did we go wrong?
- What can we do about it?
- How can visibility help?

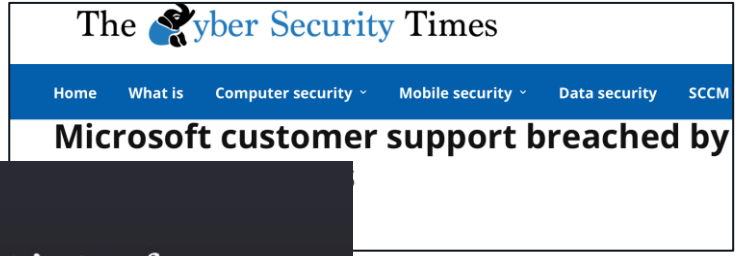
Why are we in pain?

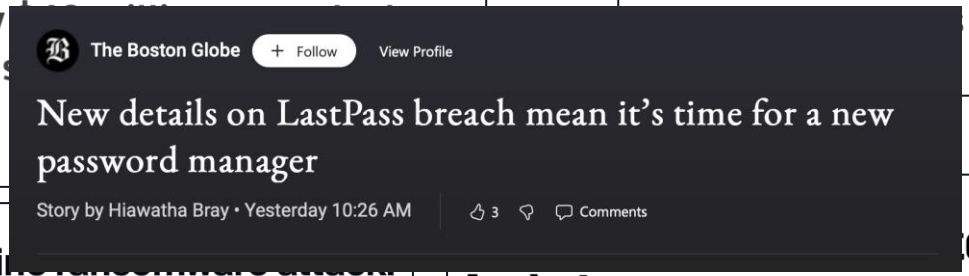


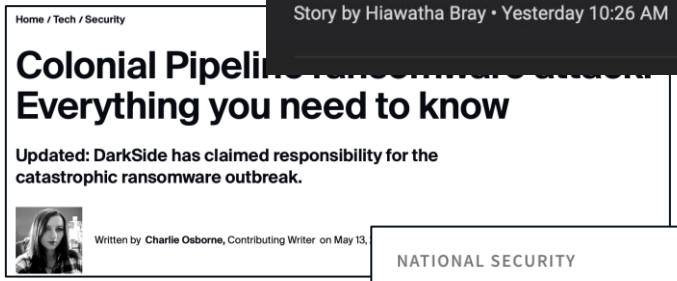
Breaking news!!!

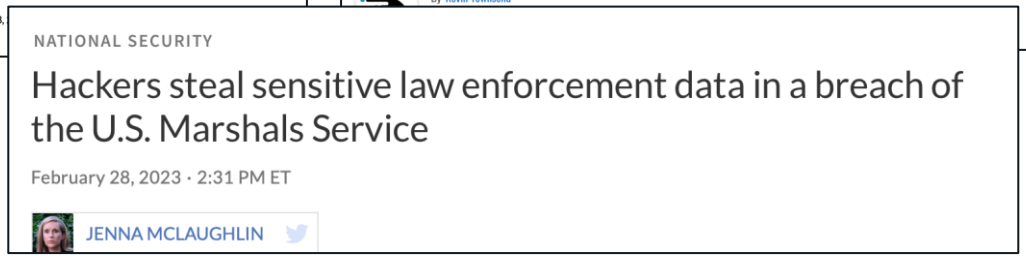
BLUF: Cybersecurity is a mess out there







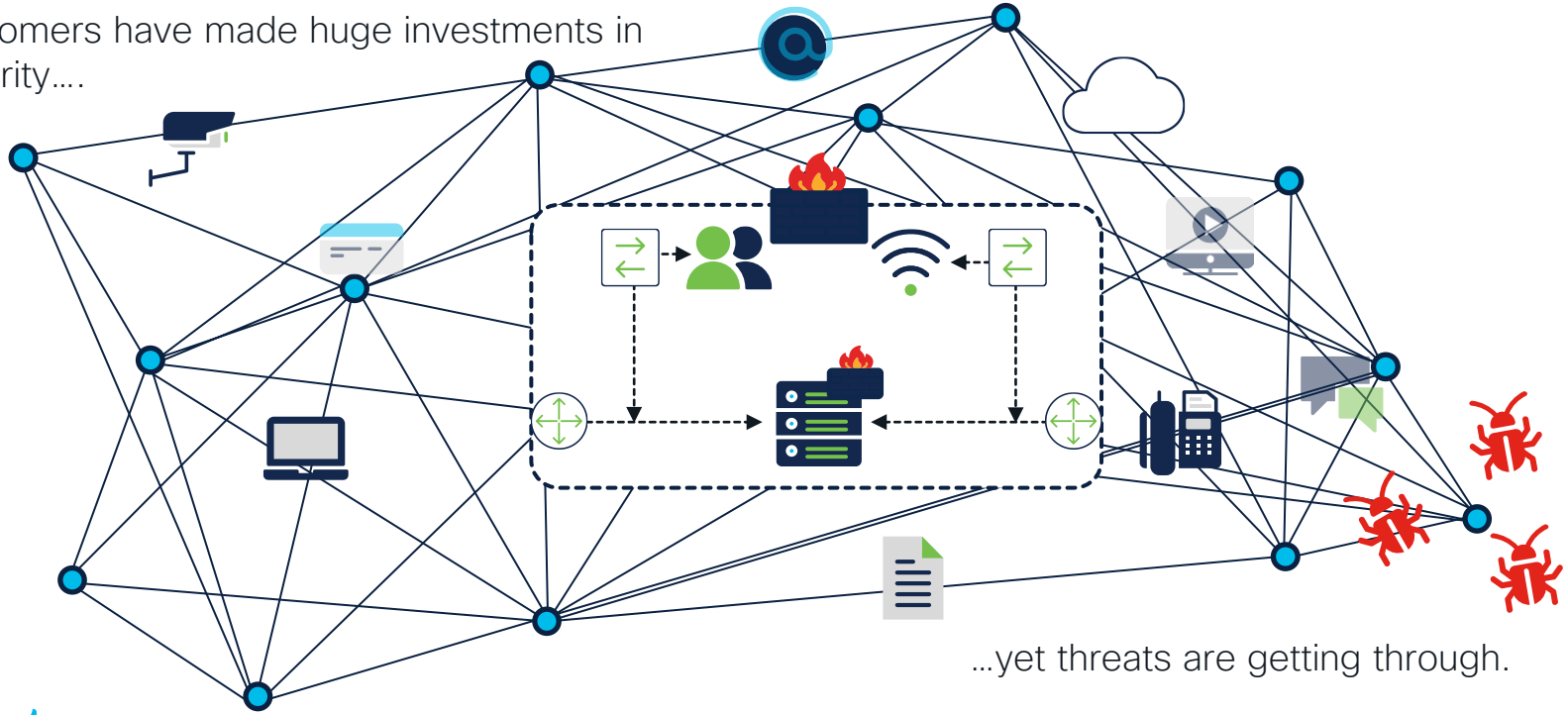




Have you been compromised?

How and when would you know?

Customers have made huge investments in security….



…yet threats are getting through.

Who gets the blame

The only thing getting more efficient is identifying scapegoats

- Tenure of a CISO: ~*2 years* (CIOs 4.3, CEOs 8.1)
- Solutions in security stack: *50-60* (medium-sized companies)
- Unfilled security roles in US: *>715,000*

- Leading investment areas: (Expect ~$1.75T by 2025 vs. $10.5T loss)
    1. Services: 50%, or almost $900B
        ... 18. Cyber Insurance: ~$15B
            ... Last: Security Awareness Training: $8B

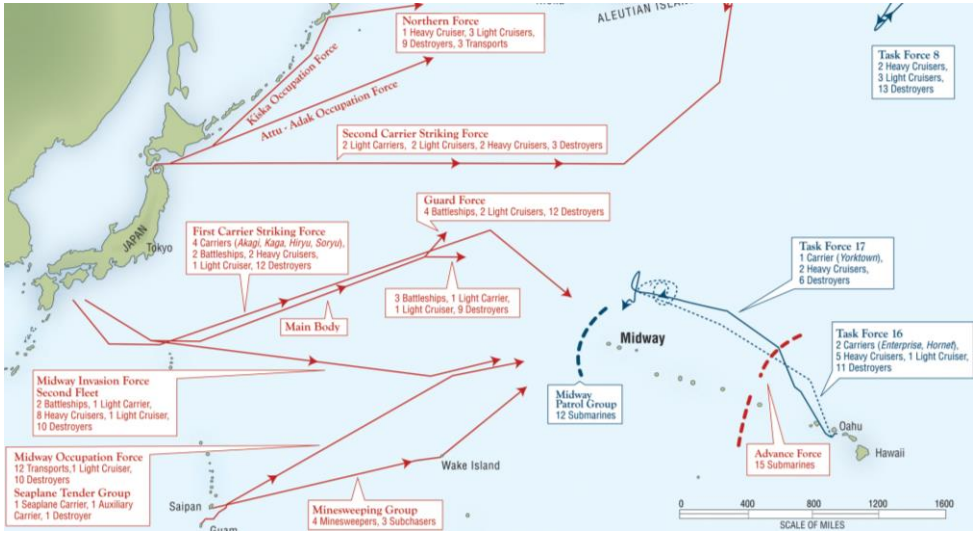
1: https://www.forbes.com/sites/forbestechcouncil/2020/02/10/the-ciso-job-and-its-short-tenure/
2: https://biztechmagazine.com/article/2019/03/rsa-2019-most-organizations-use-too-many-cybersecurity-tools
3: https://fortune.com/education/articles/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/
4: https://cybersecurityventures.com/cybersecurity-almanac-2022/

Where did we go wrong?

Security and Network folks share similar scars and war stories!

- Pay for the mistakes and decisions of others
- Complexity of domains lacks or obscures critical information
- Forced to be reactive and work under significant pressure
- Target of frustration, fury, or panic
- Nebulous workload and scope of responsibilities – “utility players”

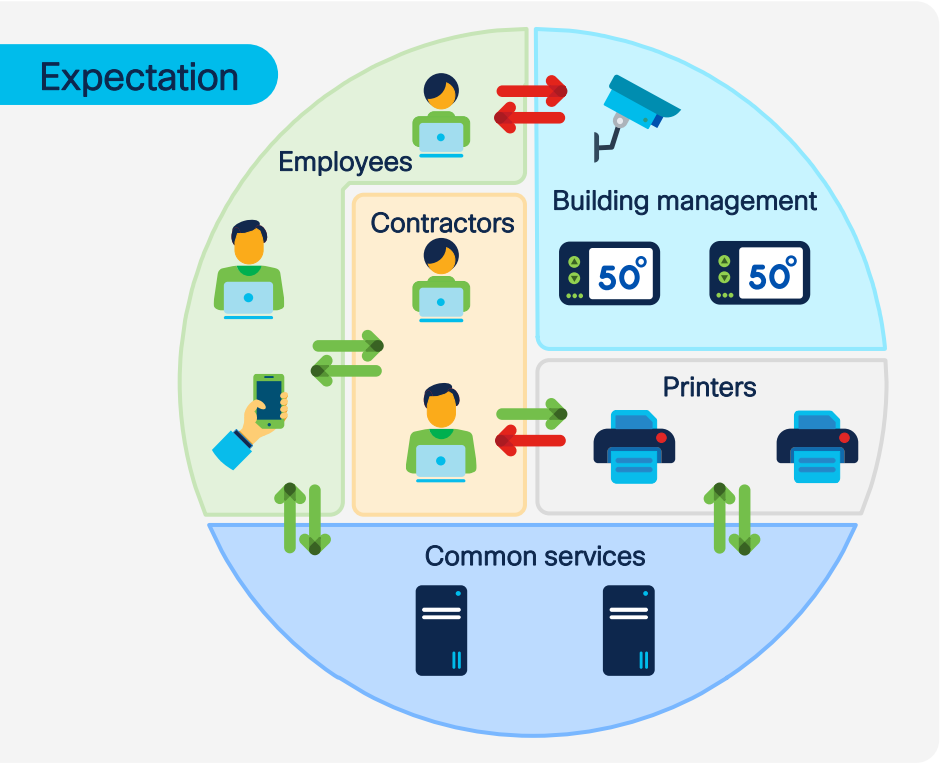
Is there a root problem?

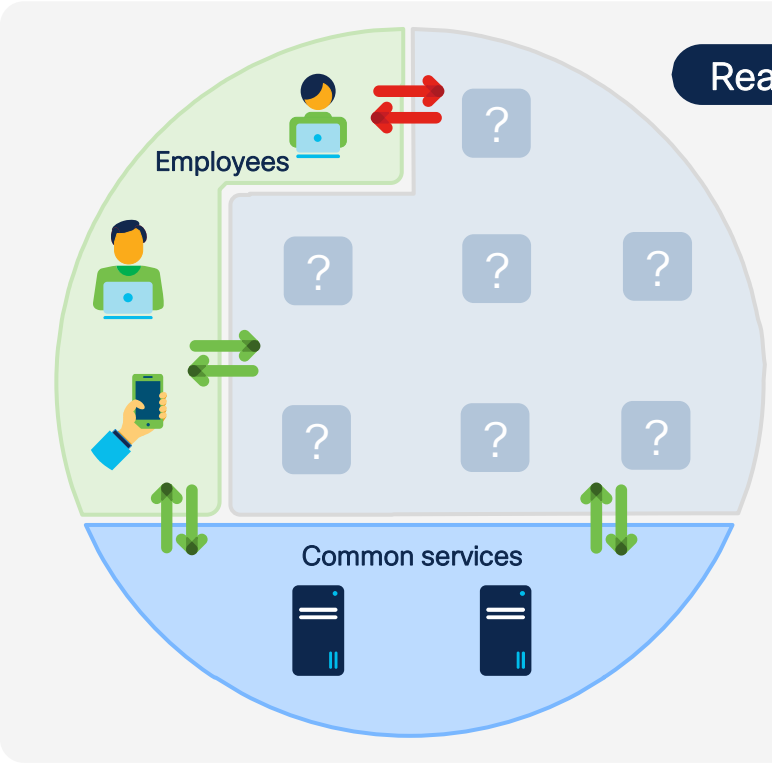


Events leading to and during the Battle of Midway 4-7 June 1942

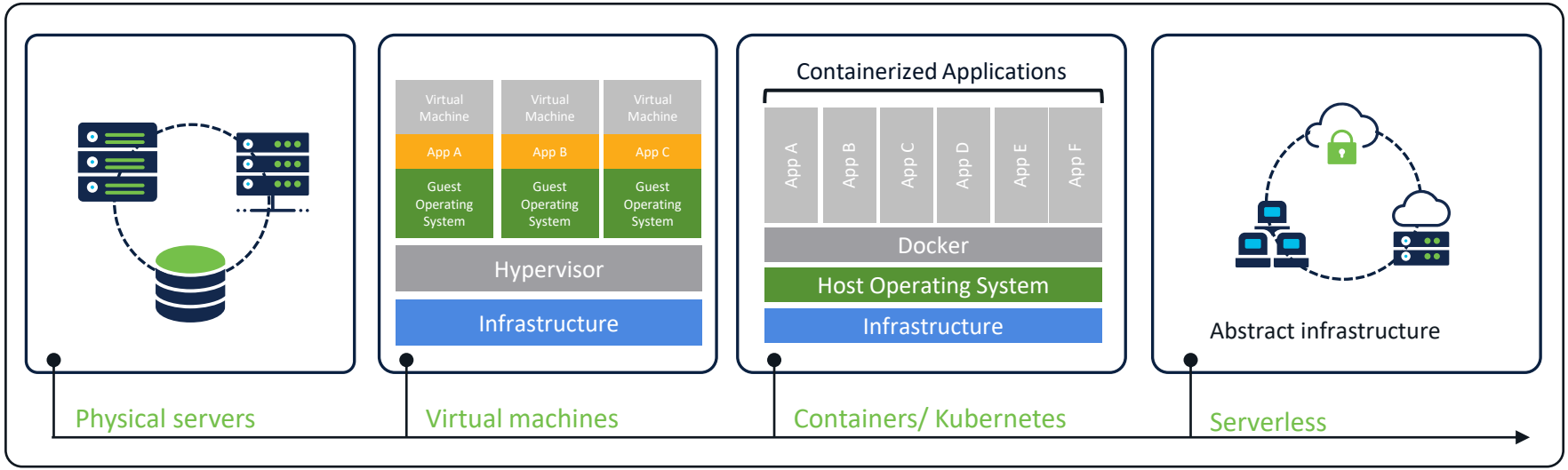
- Fog of War == massive drain and slow response
- Can't defend against unseen threats (just ask Yamamoto!)
- Technology stacks add to this
  - Getting 100% of what you pay for?
  - Staff to operate the stack effectively?
  - Fuse information? Or confuse Ops?
- Lack of visibility → slowed or impaired response
  - Fixes happen later, if at all
  - Uncovered by law enforcement (😨)

How can you segment without context & visibility?





Data Center trends render traditional detection & segmentation approaches moot



Threat actors are getting smarter

Motivated and targeted adversaries

- State sponsored
- Financial/espionage motives
- $1T cybercrime market

Insider Threats

- Compromised credentials
- Disgruntled employees
- Admin/privileged accounts

Increased attack sophistication

- Advanced persistent threats
- Encrypted malware
- Zero-day exploits

207 DAYS Industry average detection time for a breach → **73 DAYS** Industry average time to contain a breach → **$3.86M** Average cost of a data breach

Source: Ponemon 2020 Cost of a Data Breach Study

The Fallacy of Recent Security Strategies

"You must prevent everything!" or "I bought plenty of visibility!"

- $t_P > t_D + t_R$, where
  - P = Time prevention offers you
  - D = Time to detect the attack
  - R = Time to respond and mitigate
- Prevention != permanent
- Prevention buys time for D&R to occur
- Attackers will persist and overcome
- Eventually, we must detect and respond

And you can't protect what you don't see

Ignorance is *not* bliss, it turns out!

- We're not using what we've purchased
  - Infrastructure offers significant visibility features
  - Lack of standards within org makes every part unique
- We act without awareness
  - Teams don't know what normal is
  - Actions mask adversary's behavior or alert them
  - Can taint or ruin forensic evidence
  - May open additional vectors for exploit
- We've focused too long on Protection and Policy at expense of Visibility

What can we do about it?

Use what you've got!

Baked-in visibility throughout architecture enables security outcomes

- Network infrastructure
  - Flexible Netflow, ETA & IPFIX
  - AAA Events
  - Device fingerprinting
- Basic services
  - DHCP & DNS logs & activity
  - User mappings (login/logoff events)
- Integrate solutions and collect logs
- Maybe consider an XDR???

Effective security depends on total visibility

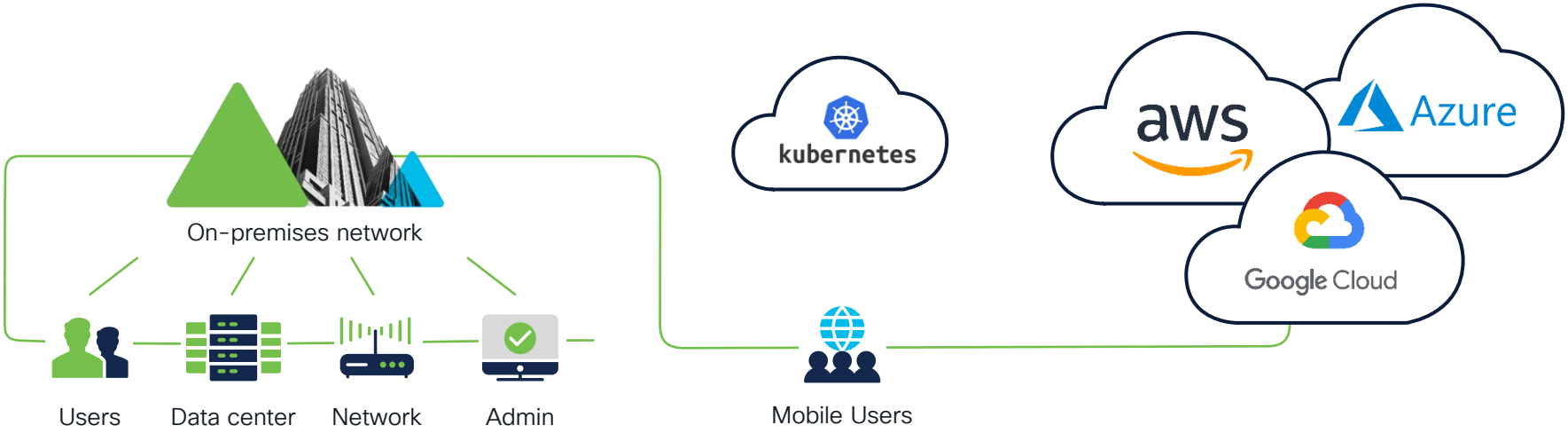
Know
every entity

See
every conversation

Understand what
is normal

Be alerted to
change

Respond to
threats quickly



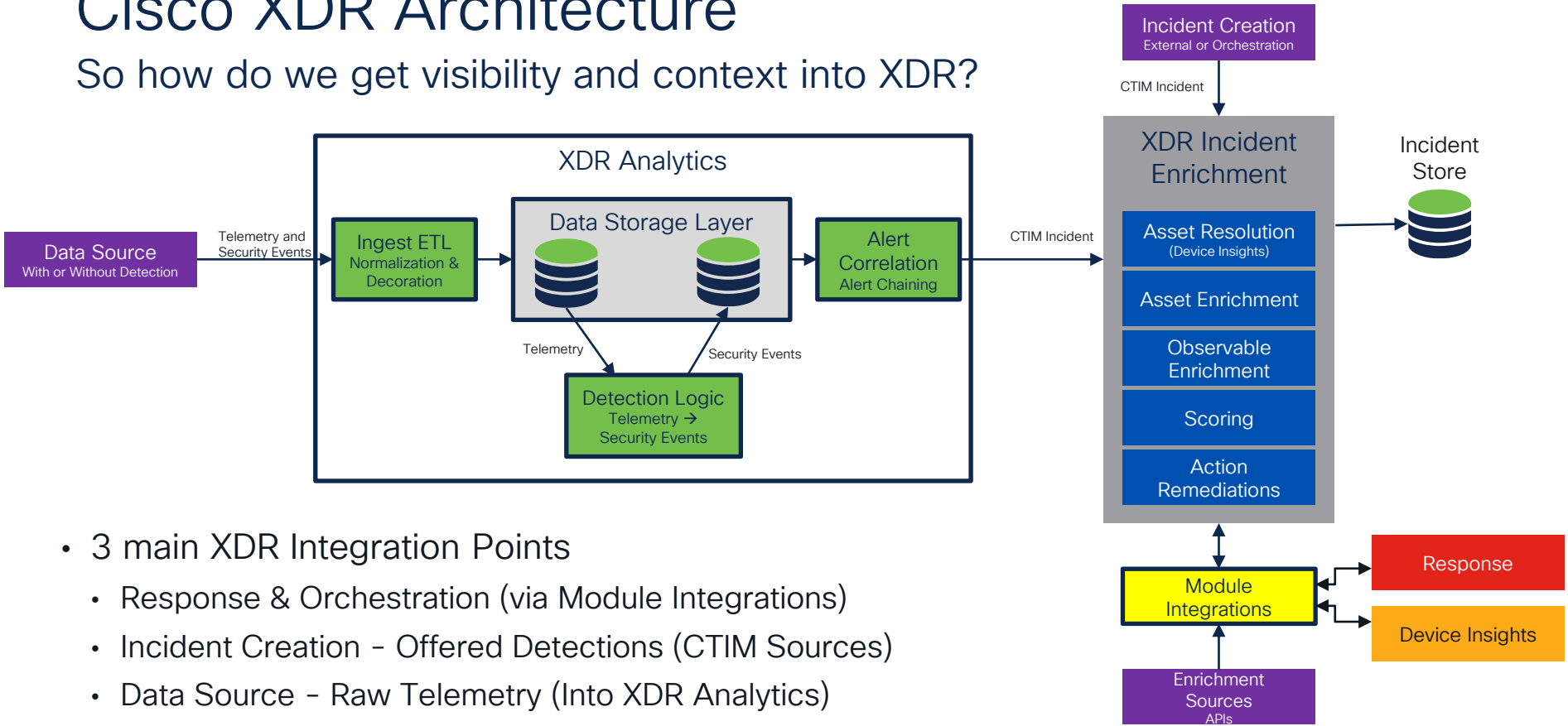
What does visibility have to do with XDR?

A real XDR uses visibility and context to simplify security operations

- Many definitions of XDR, but in general, they help answer:
  - What really happened?
  - Why should we care?
  - What should we do about it?
- All of these questions require true situational awareness
  - Visibility = discern which behaviors are normal vs. anomalous
  - Context = understand concern and priority
- XDR should only consume data that can immediately improve detections, add context, or guide response

Cisco XDR Architecture

So how do we get visibility and context into XDR?



- 3 main XDR Integration Points
  - Response & Orchestration (via Module Integrations)
  - Incident Creation – Offered Detections (CTIM Sources)
  - Data Source – Raw Telemetry (Into XDR Analytics)

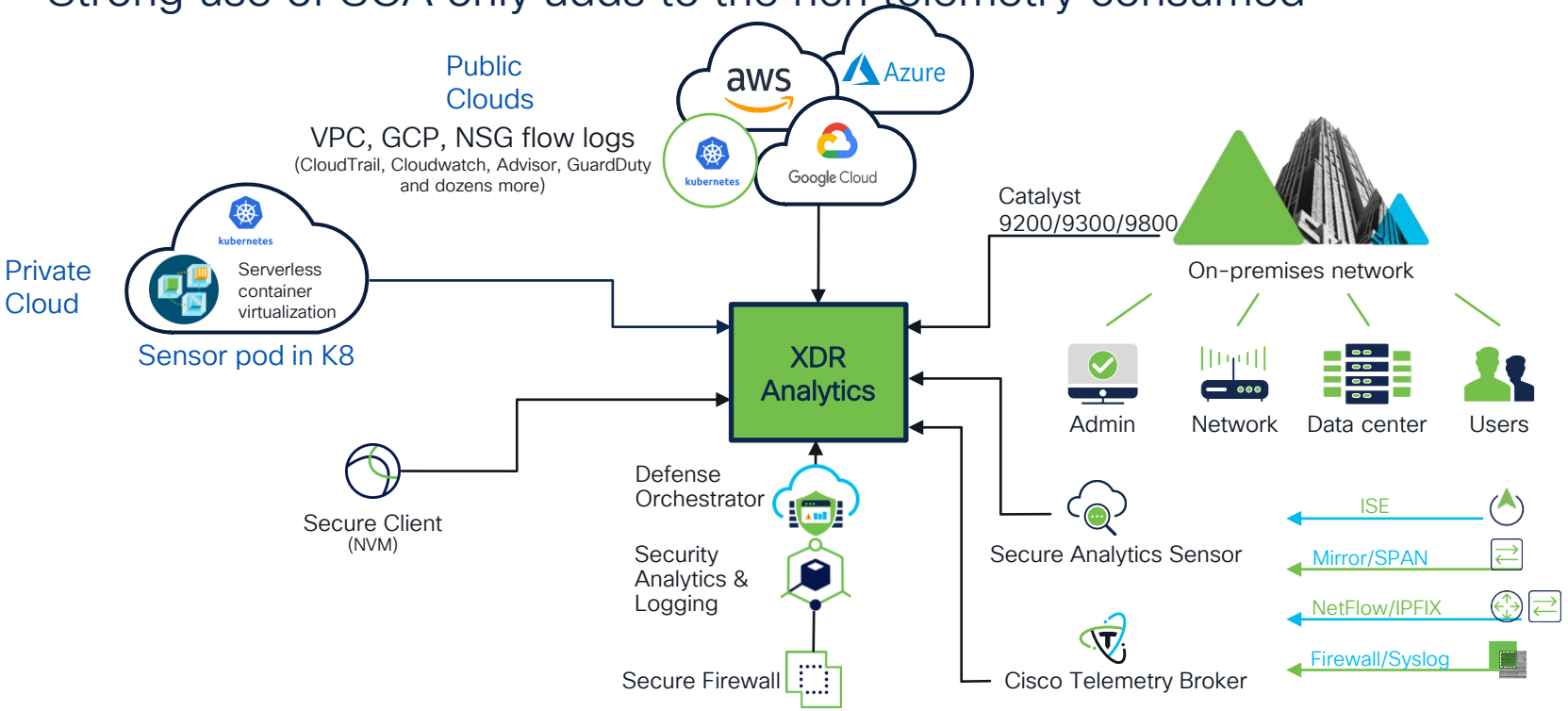
A quick primer on semantics

We're dealing with varying levels of visibility here

- Telemetry: Raw flow or events, usually comes from willing sources
  - XDR applies analytics and provides new detections
  - End goal for entire Cisco portfolio
- Incidents: Pre-detected and escalated events gathered from other sources
  - XDR can still enrich these events
  - Most likely approach for 3rd party integrations
- Enrichment: Data that brings color to the above
  - Some sources can serve multiple roles
  - Additional context enhances situational awareness and improves confidence

Most telemetry directly attaches to XDR Analytics

Strong use of SCA only adds to the rich telemetry consumed



Third Party Integrations offering visibility to Cisco XDR

- EDR:
  - CrowdStrike Falcon® Insight
  - Sentinel Endpoint Security
  - Microsoft Defender
  - Trend Micro Vision One
  - Cybereason Endpoint Security
  - Palo Alto Networks Cortex EDR
- Email:
  - Proofpoint Email Protection
  - Microsoft MS365
- Cloud Logs:
  - AWS
  - Microsoft Azure
  - Google Cloud Platform
- NGFW:
  - Checkpoint Security Gateway & Management
  - Fortinet FortiGate
  - Palo Alto Networks Next-Generation Firewall
- NDR:
  - Darktrace Respond
  - ExtraHop Reveal
- SIEM:
  - Microsoft Sentinel
- Application & Identity:
  - Microsoft Azure AD

Module integrations offer response & enrichment through Automation

Cisco Security Technical Alliance has cultivated a large variety of integrations that enrich the telemetry received further upstream.

Third-party security

Operational tools, intelligence sources, infrastructure protections and visibility

Cisco infrastructure

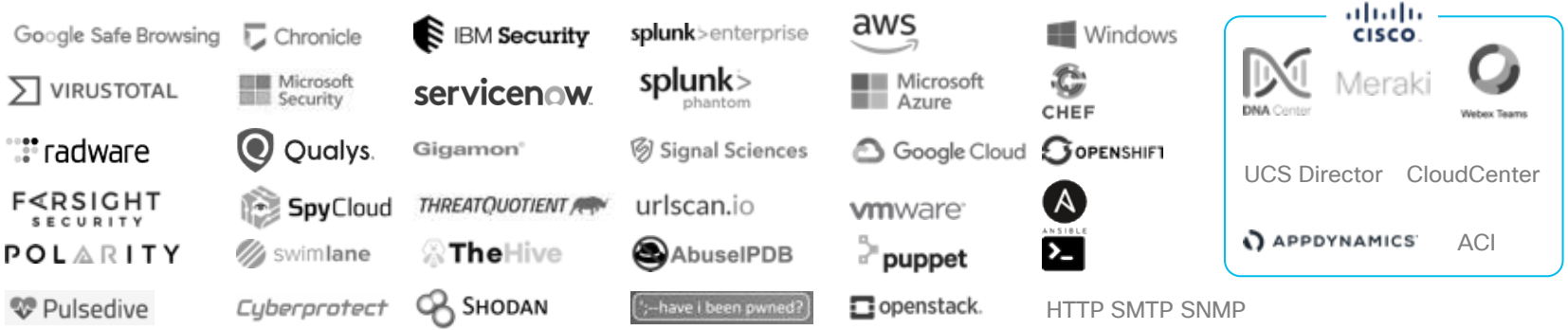
Networking, collaboration, server/app, and multicloud management platforms

Third-party infrastructure

IT service management, and cloud/virtual and DevOp platforms

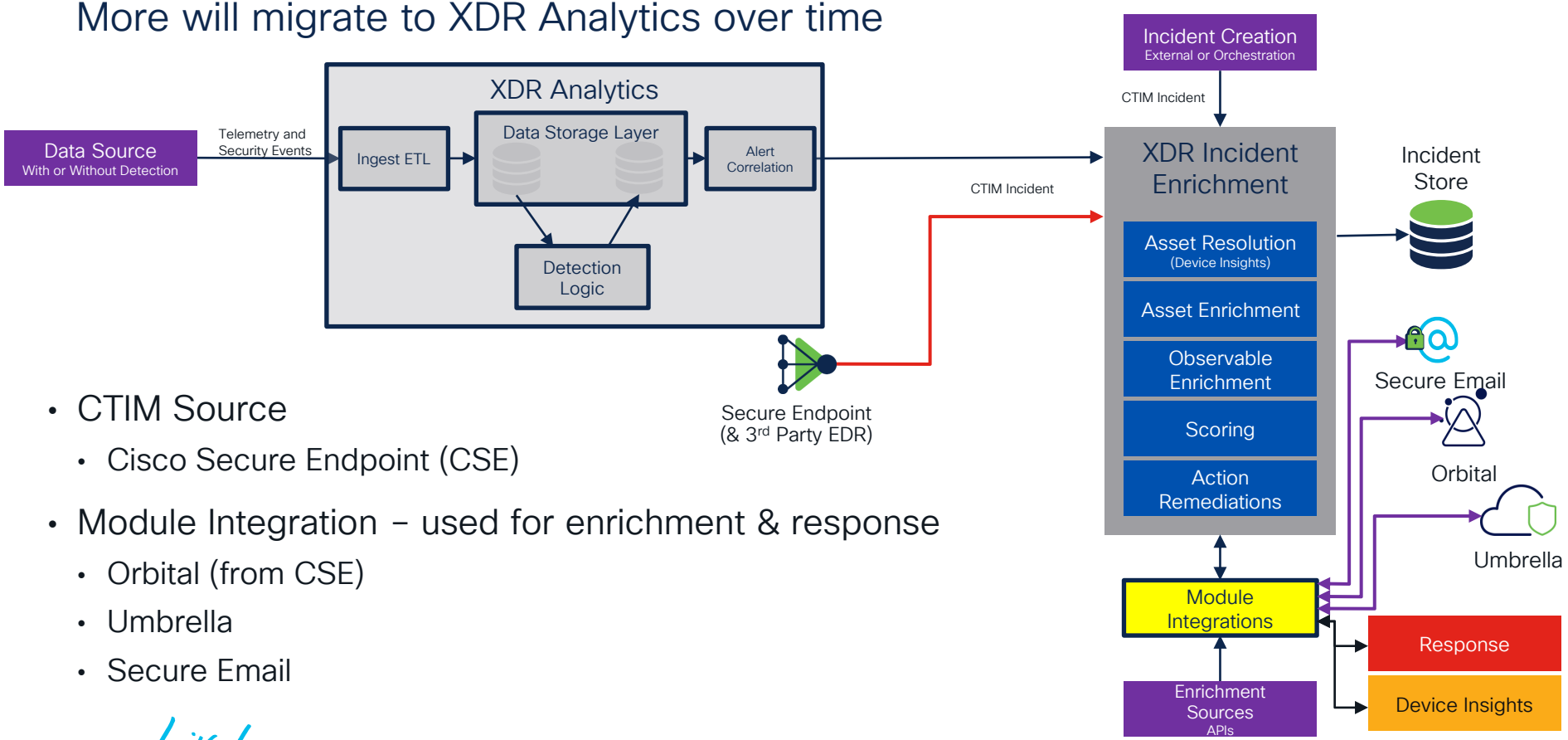
General infrastructure

Scripting/dev tools, system interfaces, data exchanges, and messaging protocols



Some potential sources come in elsewhere

More will migrate to XDR Analytics over time



- CTIM Source
  - Cisco Secure Endpoint (CSE)
- Module Integration – used for enrichment & response
  - Orbital (from CSE)
  - Umbrella
  - Secure Email

Individual Integrations

Automatic Integrations

Some integrations automatically configured as XDR tenant is created

- Activation of Cisco XDR will automatically create integrations with core capabilities:
  - Core XDR to XDR Analytics (formerly Secure Cloud Analytics)
  - Device Insights
  - Secure Client
  - Secure Endpoint to XDR Incident Enrichment (skips XDR Analytics)
- Integrations in Cisco SecureX will also carry over
  - Module Integrations (in SecureX Integrations tab)
  - Pre-existing SCA integrations (Public cloud, webhooks, etc.)
  - Pre-existing Device Insights integrations
  - Cisco Secure Client profiles

Public Cloud Integrations

Network Traffic data ingested via direct integrations

AWS:

1. Create IAM Role
2. Add credentials
3. Configure VPC Flow Logs
4. Configure S3 Bucket
5. Add Flow Logs to XDR

Details:
http://cs.co/9002OlORq

Azure:

1. Retrieve Azure AD URL
2. Create Azure AD Application
3. Grant Access to Application
4. Grant Storage Access
5. Enable Azure Network Watcher
6. Register Insights Provider
7. Enable Azure NSG Flow Logs
8. Configure in XDR Analytics

Details:

http://cs.co/9001OlORU

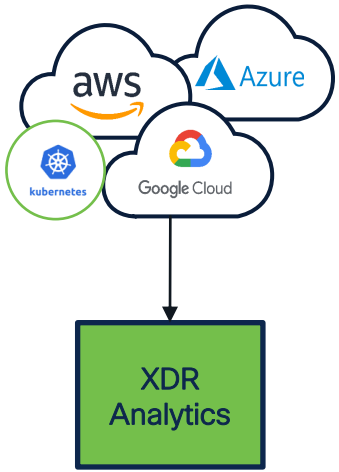
GCP:

1. Configure Service Account
2. Configure GCP to generate VPC Flow Logs
3. Enable Stackdriver Monitoring API
4. Upload Credentials to XDR Analytics

Details:
http://cs.co/9003OlORS

Kubernetes (non-GCP):

1. Create Service Account
2. Create DaemonSet
3. Verify Integration

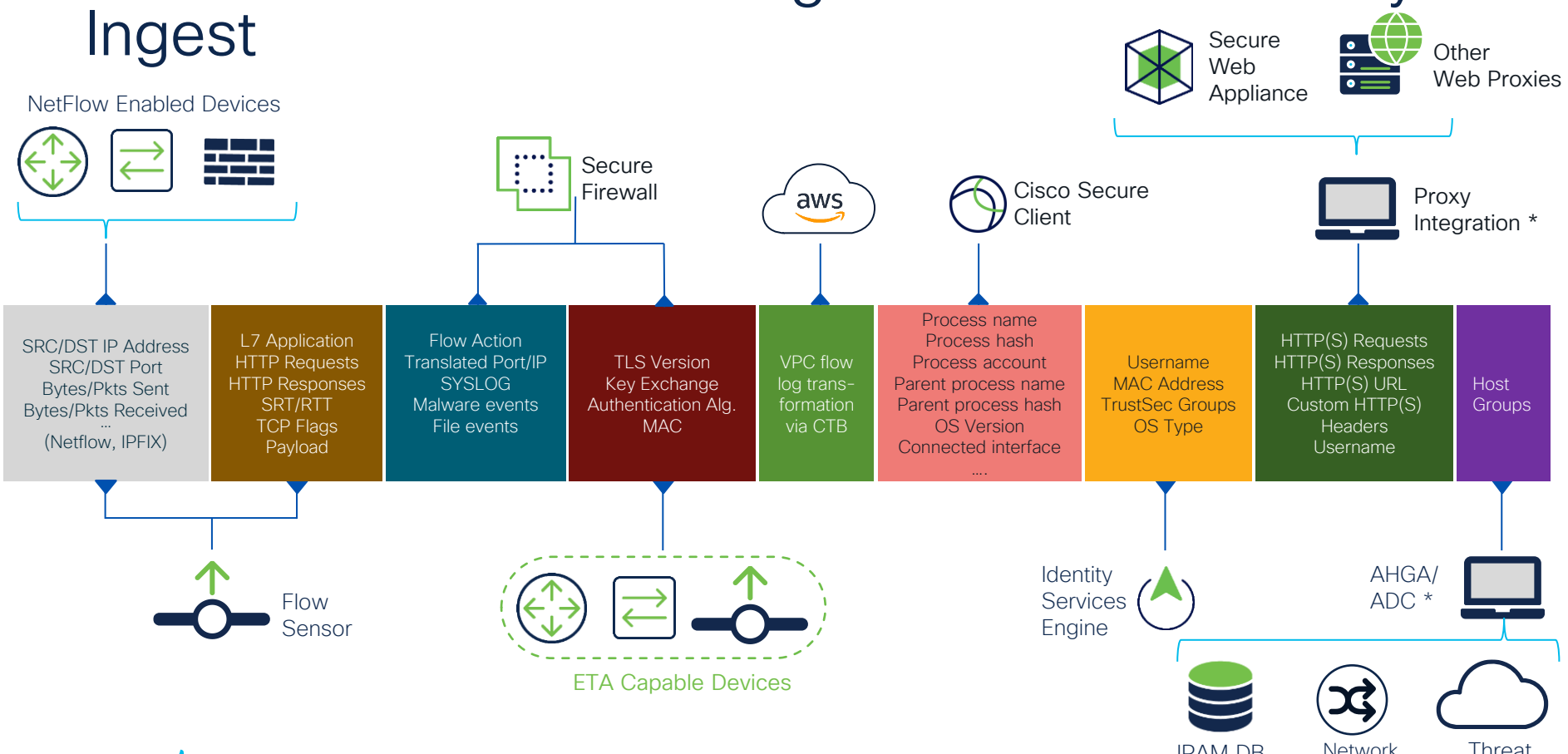


Bringing On-Premises NDR Telemetry

On-premises NDR can ship flows to XDR Analytics

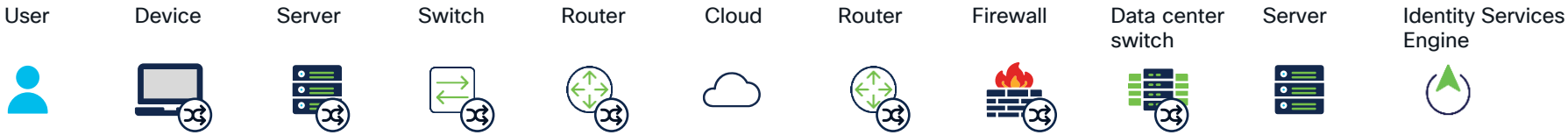
- For Cisco Secure Network Analytics (SNA)
  - Recommend Cisco Telemetry Broker (CTB)
    - Scales best
    - Entitlement included with XDR
    - Offers increasing transform and filter capabilities
  - May also use SNA Flow Collector (FC), SCA Private Network Monitor (PNM) or Observable Network Appliance (ONA)
    - Eventually CTB will offer the superset of features.
- Darktrace and Extrahop NDR integrations
  - Flow forwarding directly from their FC equivalents or via CTB as relay

SNA still critical in offering Extensive Telemetry Ingest



* Delivered through Advanced Services

Building an end-to-end visibility infrastructure involves using what you have wisely



NetFlow Export is available across the Cisco portfolio

Switch
Catalyst 2960-X (v9/IPFIX)
Catalyst 3650/3850 (v9/IPFIX)
Catalyst 4500E (v9/IPFIX)
Catalyst 6500E (v9/IPFIX)
Catalyst 6800 (v9/IPFIX)
Catalyst 9200 (v9/IPFIX)
Catalyst 9300/9400 (v9/IPFIX ETA)
Catalyst 9500 (v9/IPFIX)
Catalyst 9600 (v9/IPFIX)
IE3000 (v9/IPFIX)
IE4000 (v9/IPFIX)
IE5000 (v9/IPFIX)

Router
Cisco ISR 4000 (v9/IPFIX ETA)
Cisco CSR 1000v (v9/IPFIX ETA)
Cisco ASR 1000 (v9/IPFIX ETA)
Cisco ASR 9000 (v9/IPFIX)
Cisco WLC 5520, 8510, 8540 (v9 Enhanced)
Catalyst 9800 (v9/IPFIX ETA)

Firewall
ASA 5500-X (NSEL)
FTD (NSEL,Syslog)
Meraki MX/Z (v9 Enhanced v14.5)

Data center switch
Nexus 1000v (v9/IPFIX)
Nexus 3000 (sFlow)
Nexus 7000 (M Series modules – (v9/IPFIX)
Nexus 7000 (F Series modules – (v9/IPFIX sampled)
Nexus 9000 Series (sFlow)
Nexus 9000 Series EX/FX (v9)

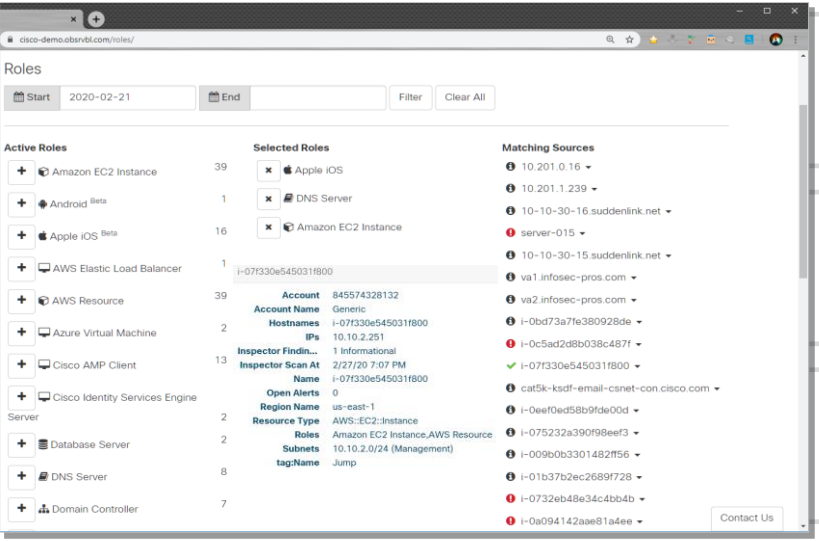
Servers, software
SNA Flow Sensor (v9/IPFIX ETA)
Cisco UCS VIC (v9/IPFIX)

Cloud
AWS
Azure
(VPC Flow Logs via CTB)

Endpoint
AnyConnect (IPFIX)

The above is a non-exhaustive list of Cisco exporters.
For individual platform features, reference the Cisco feature navigator: http://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/index.jsp

NDR analytics dynamically maps entities by role, benefitting other detectors in environment



Type based modeling

Functional modeling

Cloud specific modeling

Roles include:

Android	Web server
VoIP client	Mail server
Medical imaging client	Citrix PVS server
Apple iOS	Remote desktop server
Windows workstation	AWS lambda
Wireless LAN controller	Azure virtual machine
Domain controller	GCP compute instance
DNS server	Kerberos node

...over 70+ entity roles are supported !

Portals report all observed device types as wells as device types not seen for a comprehensive view of environments

Host investigation in SNA contributes to the Cisco XDR's awareness of on-premises entities

Host summary

10.201.3.18

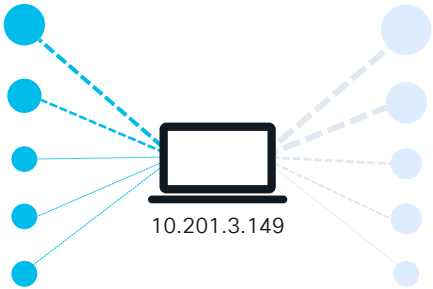
Flows | History

Hostname:	dhcp-atl-4-71.acme.com
Host group:	Desktops, Sales
Location:	Atlanta, GA
First Seen:	1/25/20 1:52 AM
Last Seen:	6/1/21 8:31 AM
Policies:	Insider Threat Event, Client IP Policy

Quarantine | Unquarantine

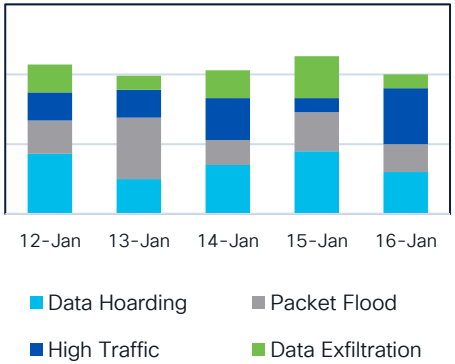
Summary of aggregated host information

Traffic by peer host group



Observed communication patterns

Alarms by Type



Historical alarming behavior

Role mapping allows entity modeling to baseline behavior and detect anomalies

Collect input

- IP Telemetry
- Enhanced NetFlow
- Identity Services Engine user data
- DNS Snooping
- External threat intel
- Endpoint metadata
- System/Account logs

Perform analysis

Dynamic entity modeling

- Role
- Group
- Consistency
- Rules
- Forecast

Draw conclusions

What is the role of the device?
Is its behavior consistent with that type of role?

What ports/protocols does the device continually access? Do other similar roles do the same?

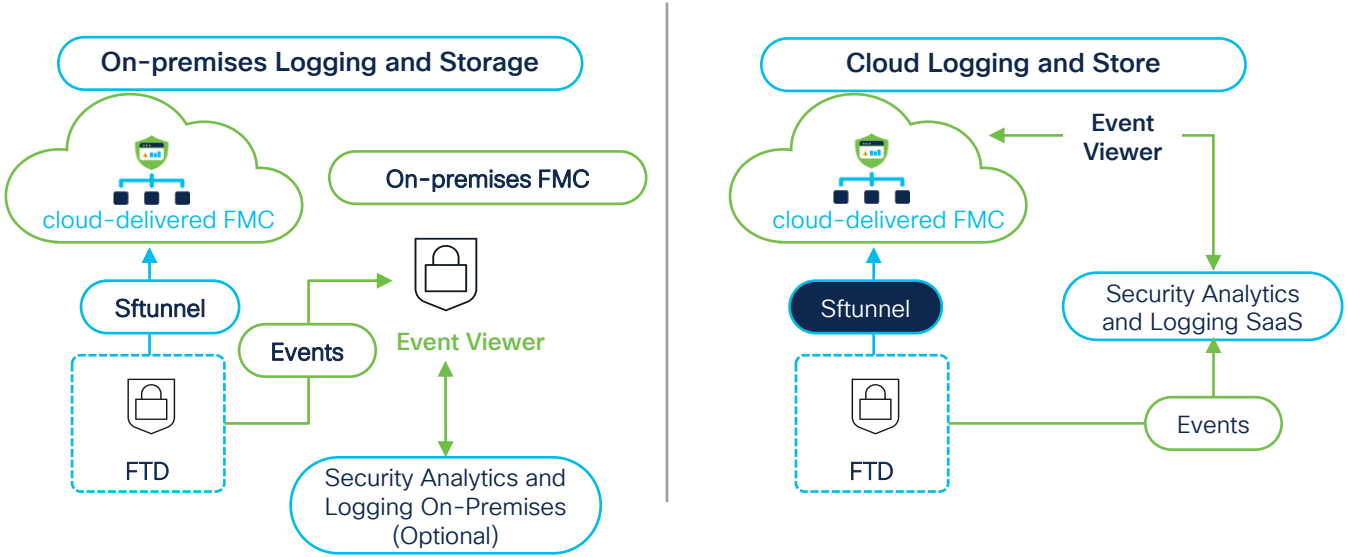
What connections does it continually make?
What is the reputation of the IPs it connects to?

Does it communicate internally only?
What geographies does it normally talk to?

How much data does the device normally send/receive? Is it consistent with expectations?

Security Analytics and Logging Options

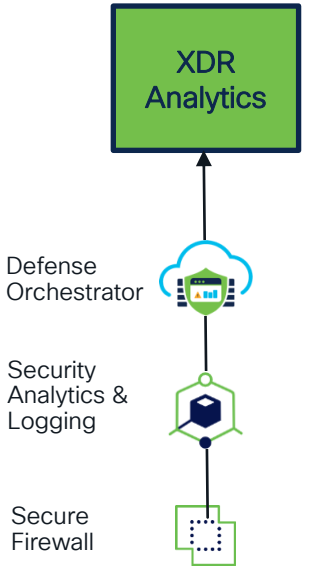
SaaS-delivered SAL offers quickest NGFW telemetry integration



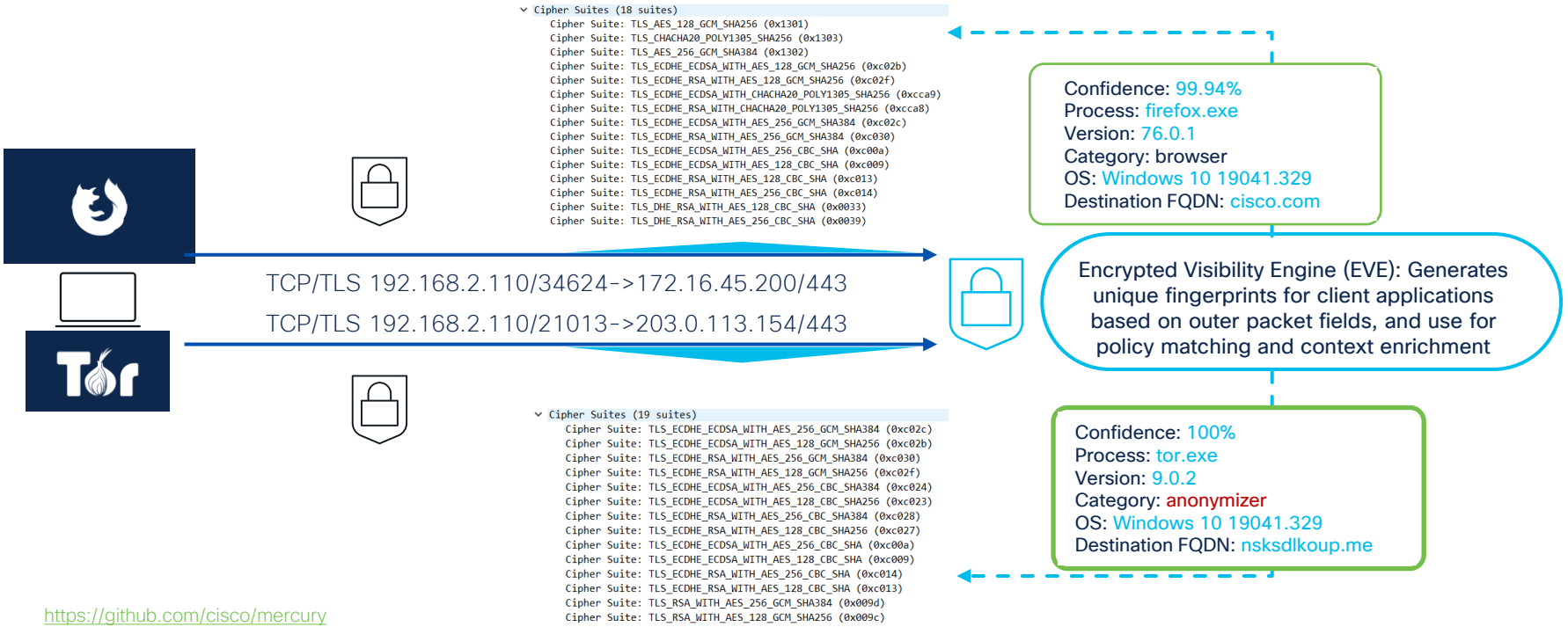
- On-premises SAL not yet integrated
- Detections in Cisco XDR leverage SCA roots

Bridging NGFW Telemetry with CDO & SAL

- Currently supports SaaS-delivered SAL
- Secure Firewall (FTD) sends events via Secure Services Exchange (SSX, formerly SSE)
- SAL connection to XDR Analytics currently requires Cisco Defense Orchestrator (CDO)
- https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/sal-cloud/fmc-and-sal-saas-integration-guide.html



Firewalls can now offer visibility without decryption, with Encrypted Visibility Engine (EVE)

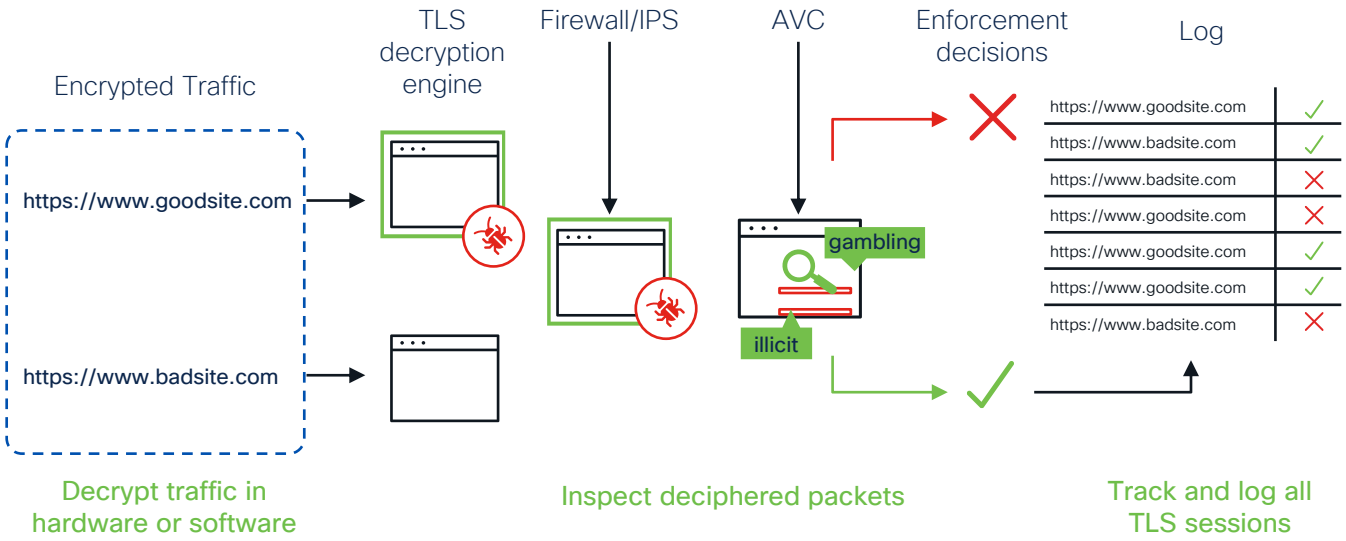


https://github.com/cisco/mercury

They can also implement TLS 1.3 Decryption

This upstream Visibility in NGFW Benefits the entire XDR Ecosystem

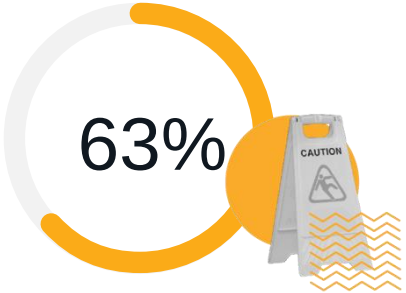
- TLS hardware acceleration delivers high-performance encrypted traffic inspection
- Centralized TLS policies enforcement
- Examples: Blocking self-signed encrypted traffic, exclusions for banking, health care, etc., reputation-based rules



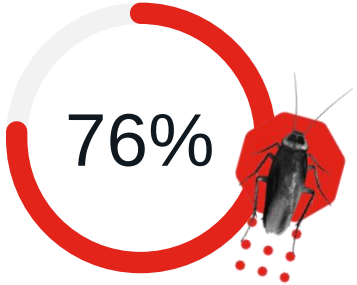
The importance of visibility in encrypted traffic

Cisco's ETA (Secure Analytics) and EVE (Secure Firewall) have you covered

- Threat detections discovered in encrypted traffic were directly proportional to the customer's encrypted traffic analytics coverage.
- That is, the higher the coverage, the more threat detections were found.



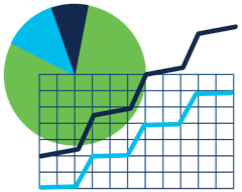
63% of all threat detections were discovered in encrypted traffic



76% of critical or high-risk threats were discovered in encrypted traffic

This baseline in entity modeling helps detect abnormal activity

30+ detections active on day zero



130+ available alerts

IP address detected

Communicates with set of IPs

Classify roles
Dynamically assign roles to entities

Database server identified

Data stays within environment

36 day baseline
monitor and model behavior

Data access from regular location

Existing IP accesses database server

New external connection osbservation

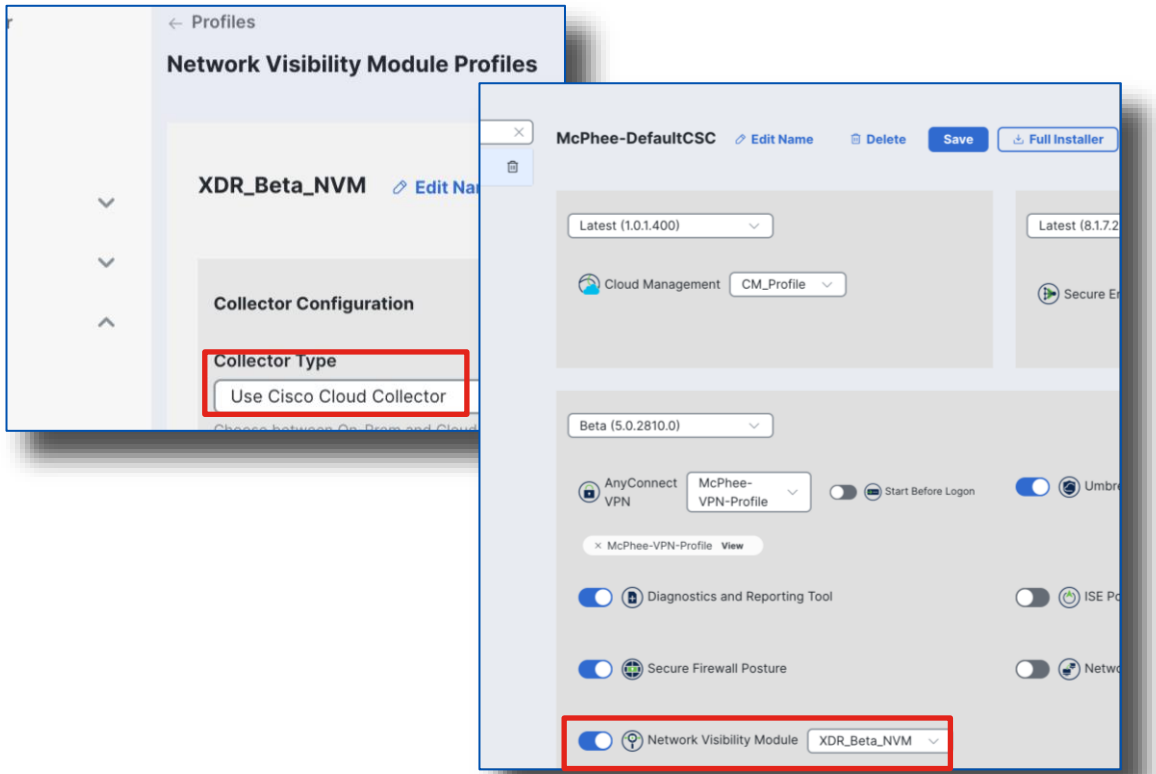
New high throughput connection

Alert triggers
for database exfiltration

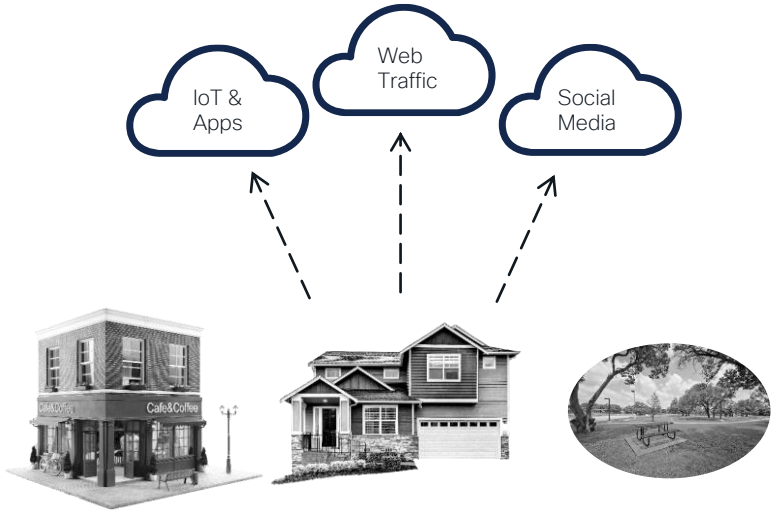
NVM Telemetry sheds light into of-premises or non-NDR covered events

A critical link between what happens in the box and over the network

- Re-invented for XDR, with more fields, easily extended records, etc.
- Ingest via Cisco Security Cloud NVM Broker
- Subscribed to by XDR Analytics
- Viewable in XDR Analytics Event Viewer



Complete and continuous remote worker visibility



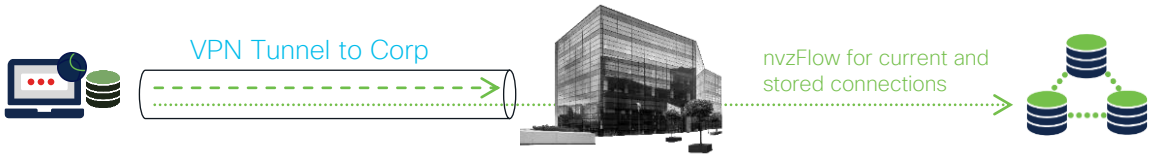
Endpoint and Remote worker visibility

- Discover and monitor remote worker traffic
- Identify unwanted application
- Detect threats and malicious processes
- Identify assets and applications running on the network

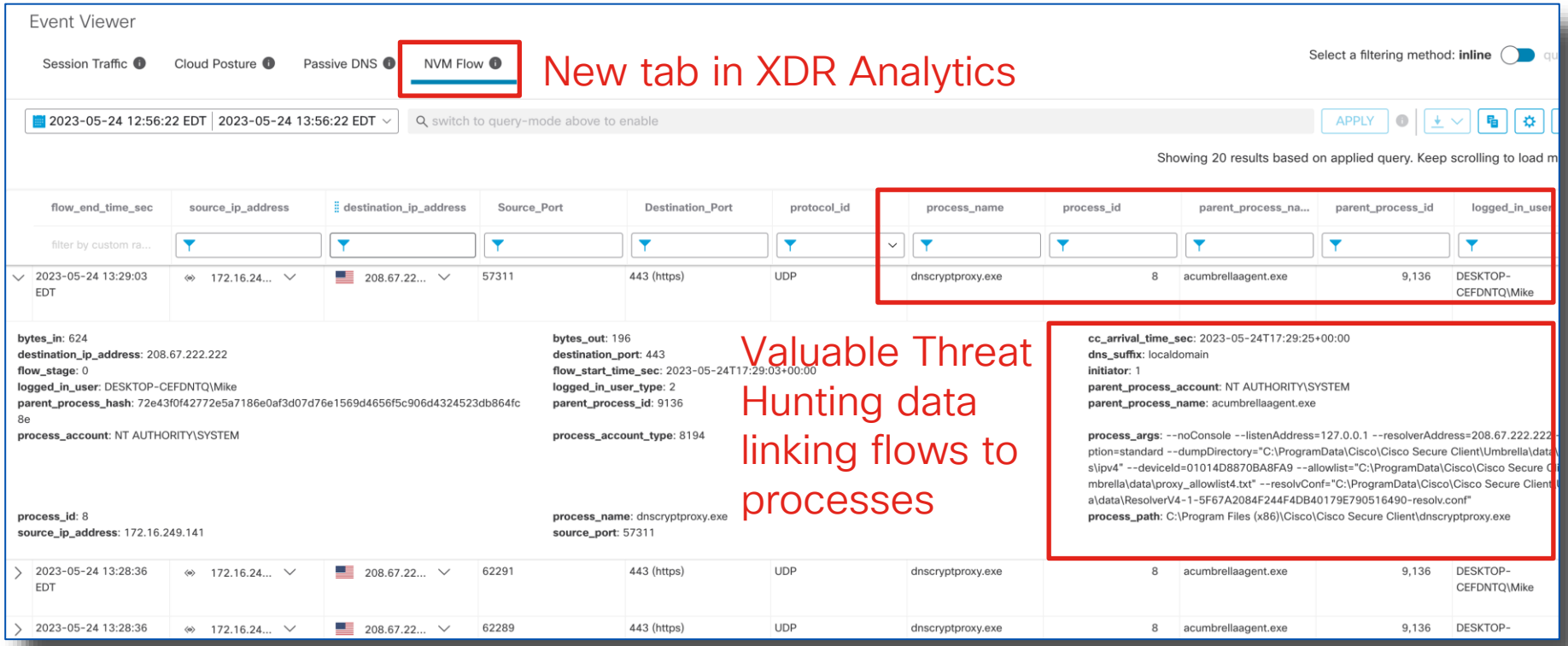
Visibility Independent of location

- working on-network, full tunnel
- on & off-network, split tunnel
- off-network, without VPN

Non-VPN flow telemetry is stored



NVM links highly detailed endpoint information with highly trusted network behaviors

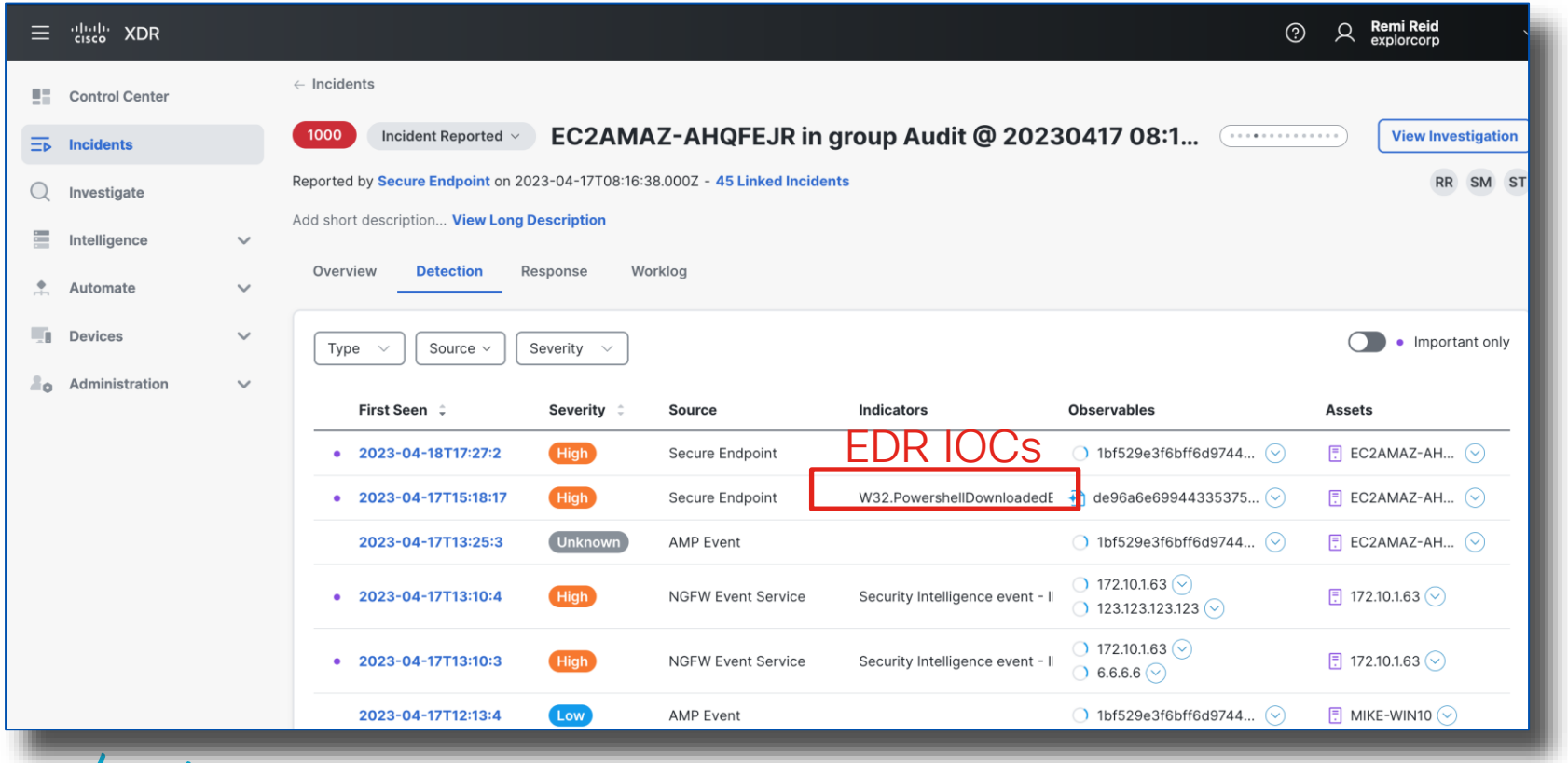


EDR Telemetry is treated as a CTIM source

EDR-created incidents can then be enriched by EDR

- Secure Endpoint integration is automatic
- 3rd Party EDR is via Module Integration
  - CrowdStrike Falcon® Insight
  - Sentinel Endpoint Security
  - Microsoft Defender
  - Trend Micro Vision One
  - Cybereason Endpoint Security
  - Palo Alto Networks Cortex EDR

EDR still offers the best malware-focused visibility, whether file, script, or memory

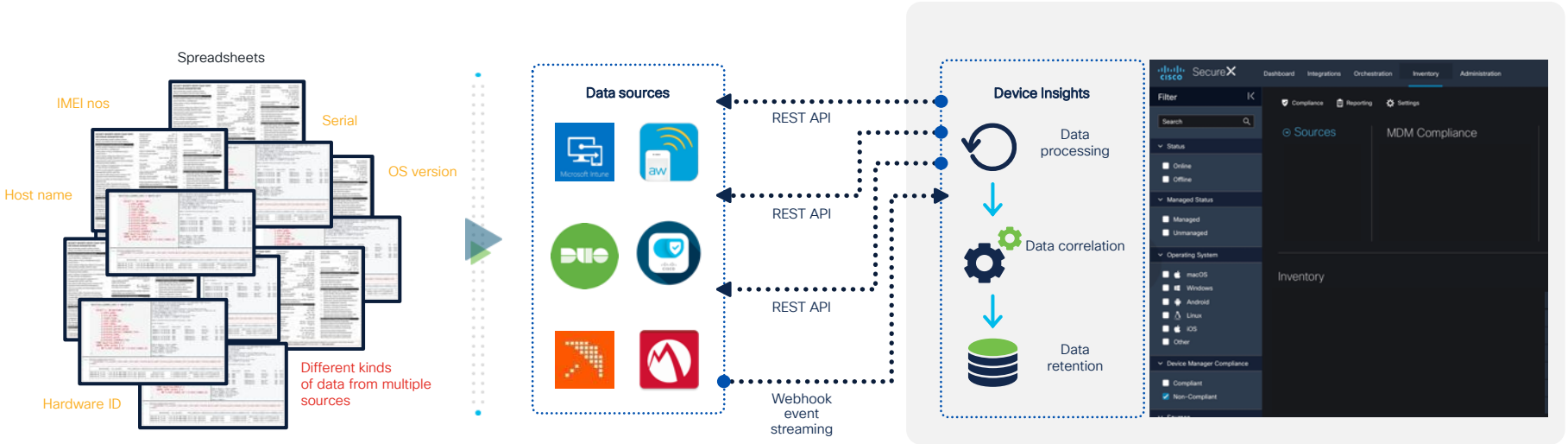


Visibility can extend to contextual insights into devices

Before:
Multiple spreadsheets, no combined view of the denominator

Solution:
Comprehensive device inventory all in one place!

After:
Gain unified visibility and contextual awareness to help you act on potential threats faster!

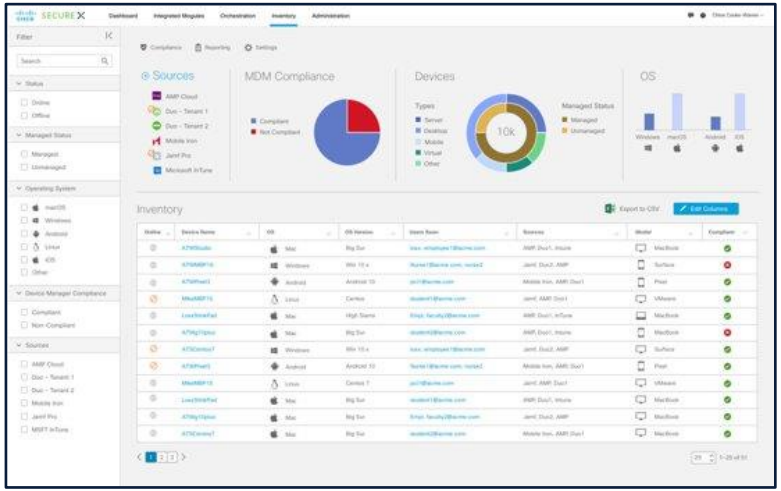


What is Device Insights?

Device Insights is a feature in Cisco XDR that unifies multiple device managers, endpoint detection and response tools, AV, and other endpoint security products and then brings the details those tools and solutions provide into a unified view within Cisco XDR.

With Device Insights, you'll be able to answer these all-important questions:

- What types of devices are connected to our network?
- What users have been accessing those devices?
- Where are those devices located?
- What vulnerabilities are associated with those devices?
- Which security agents are installed?
- Is our security software up to date?
- What context do we have from technologies beyond the endpoint?



The power of User & Device Context

- Brings a ton of context:
  - Users using the endpoint
  - Location(s) the endpoint was seen
  - IP Addresses (both Local and Global)
  - MAC Addresses (seen per NIC)
  - Windows Security Center Status
  - Vulnerabilities (as fed by applicable Products)
- Best covered by Aaron Woland's awesome BRKSEC-2754
  - https://www.ciscolive.com/on-demand/on-demand-library.html?search=BRKSEC-2754#/session/1675722393870001tdlm


Duo Access
Duo Beyond


Secure Endpoint


Umbrella (DNS)
Win / macOS only

Meraki SM


Secure Client


Orbital


Microsoft InTune


Mobile Iron

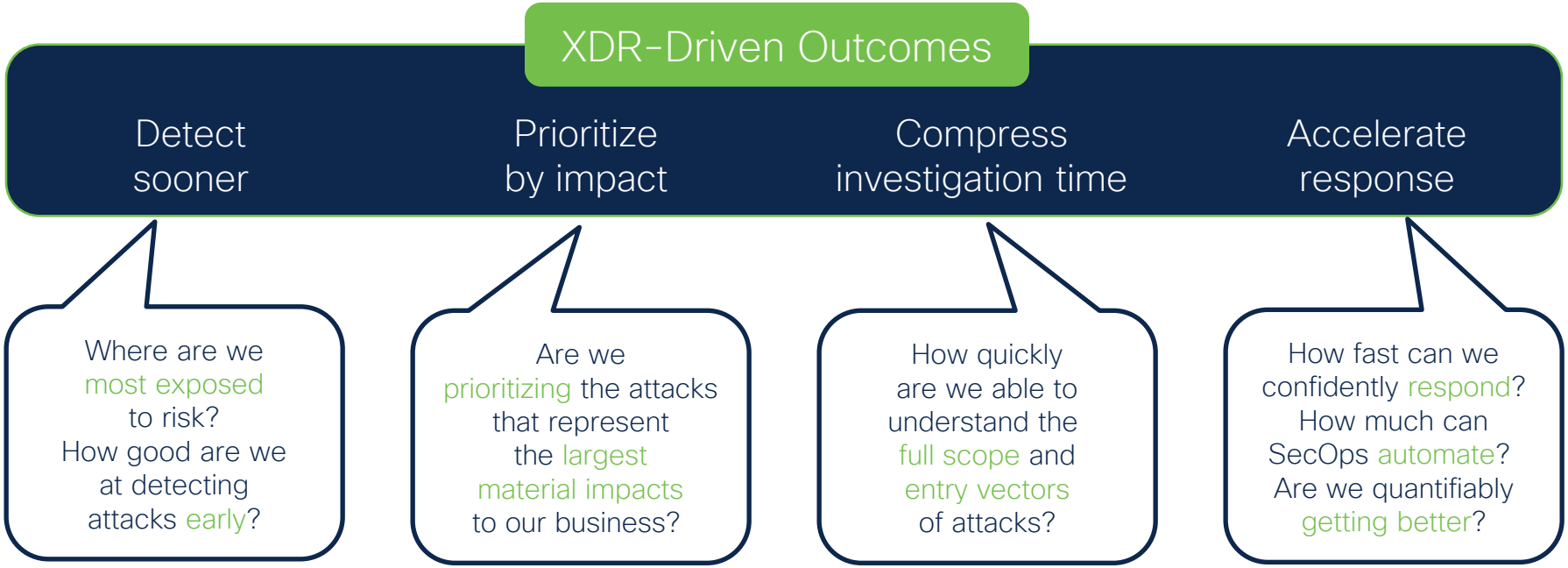

Airwatch


Custom CSVs


Jamf Pro

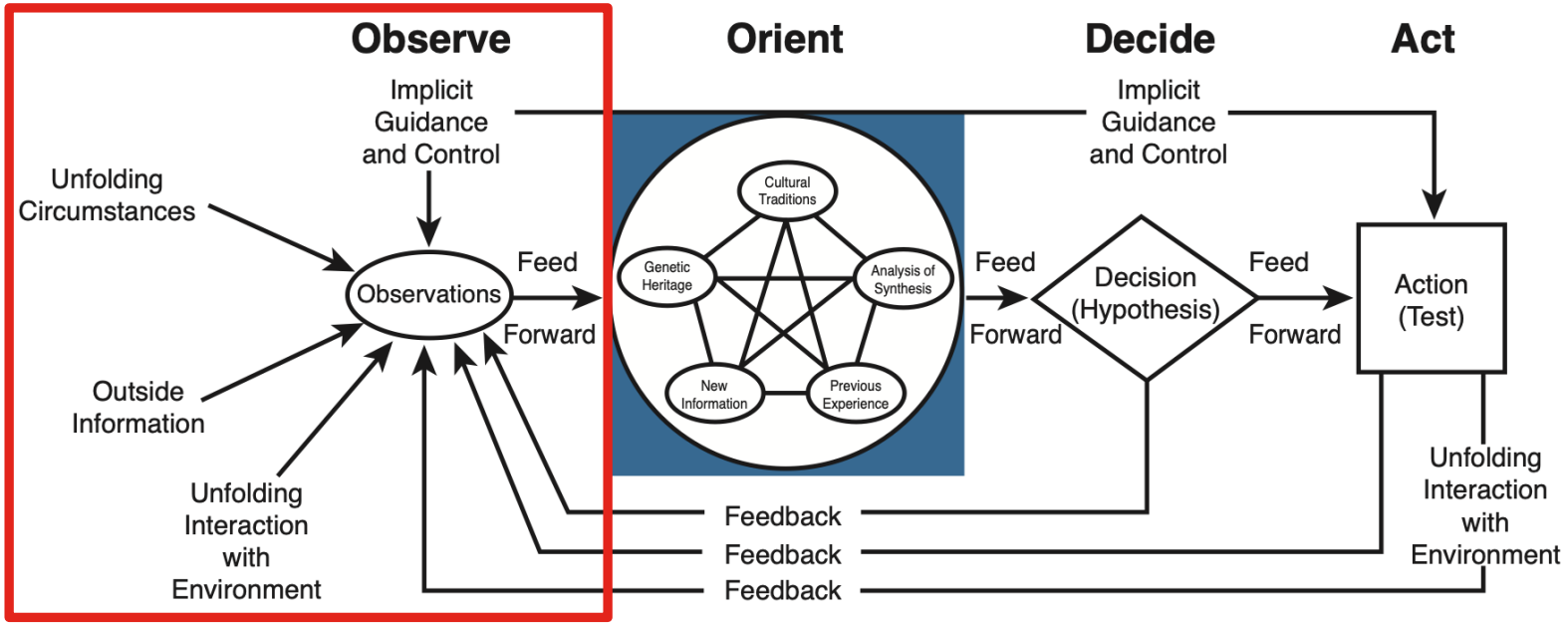
How can visibility help?

Cisco XDR shifts the architecture's focus to outcomes, not just latent capability



How do we accelerate detection, improve awareness, and reduce alert fatigue

Visibility & context lead to richer and more complete observations, accelerating the OODA Loop's execution & reducing iterations

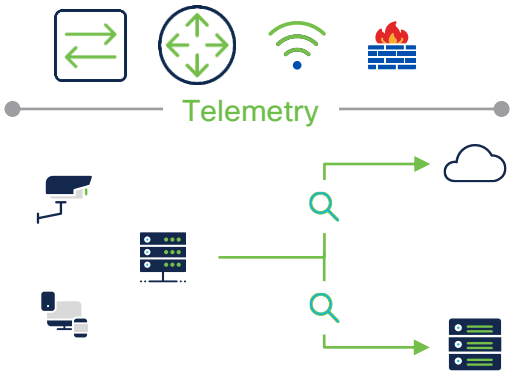


John Boyd's OODA Loop

Visibility is key to understanding the network's normal behavior and validating endpoint sources

Traffic visibility

Telemetry from the network and cloud provides up to layer 4 traffic visibility



Endpoint attribution

Who is behind the discovered IP? What device are they using? Where are they located?

Who: User

What: Device type

When: Login time

Where: Location

How: Security posture

Process: Endpoint process

Traffic indication

What type of traffic an IP is sending? What layer 7 app is used? Which URL is accessed?

Application: Layer 7 App

Web: URL identification

NAT: NAT information

Crypto: TLS version

Traffic Status : Firewall block

Intrusion : Malware or File event

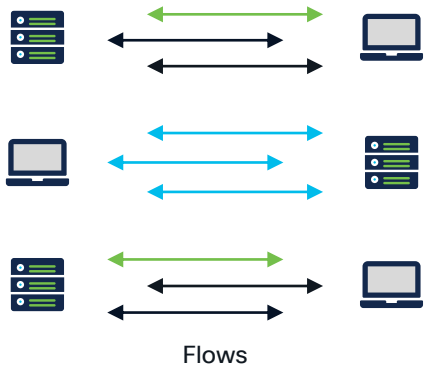
Communication Visibility | Identity | Context

Enriched Telemetry

Cisco detection-enabled solutions perform anomaly detection using behavioral modeling

Collect and analyze telemetry

Comprehensive data set optimized to remove redundancies



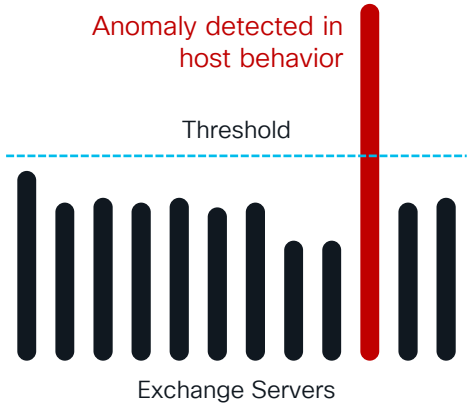
Create a baseline of normal behavior

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

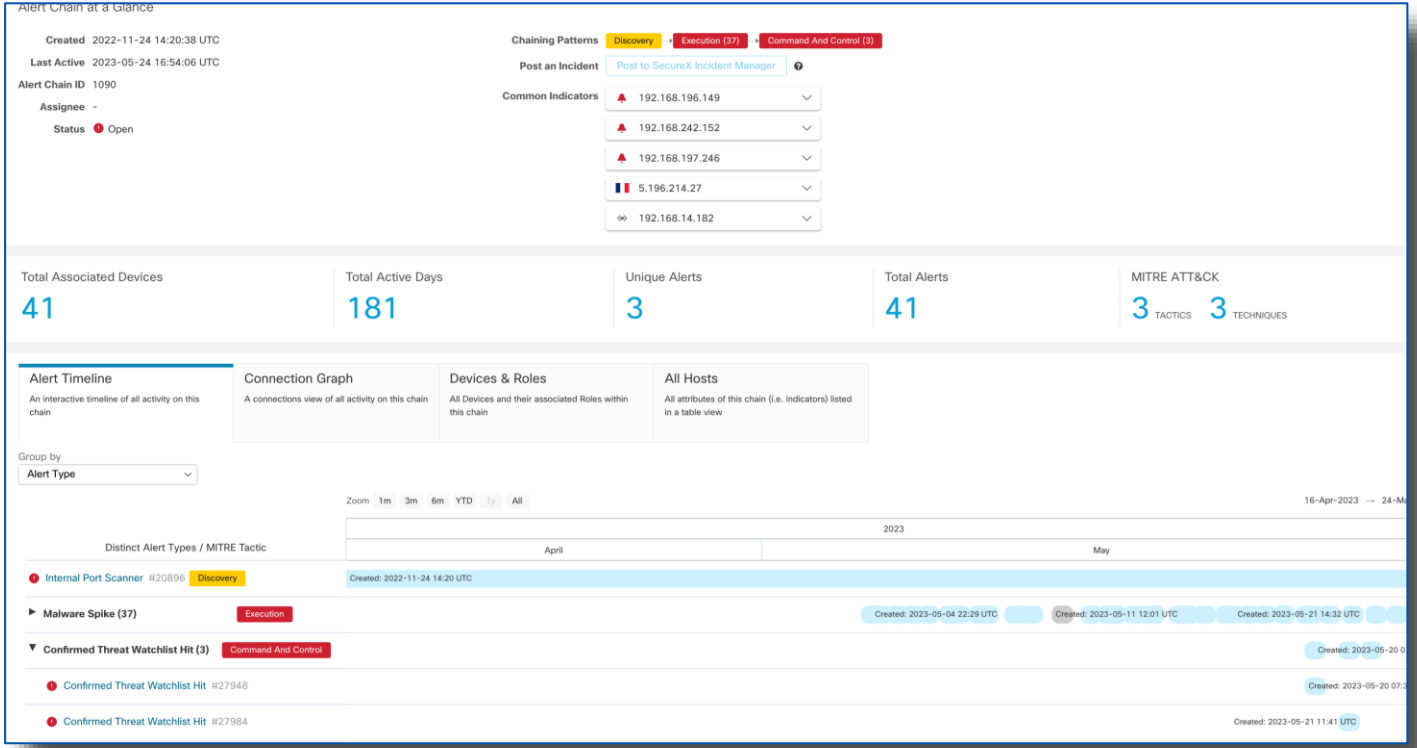
Alarm on anomalies and behavioral changes

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

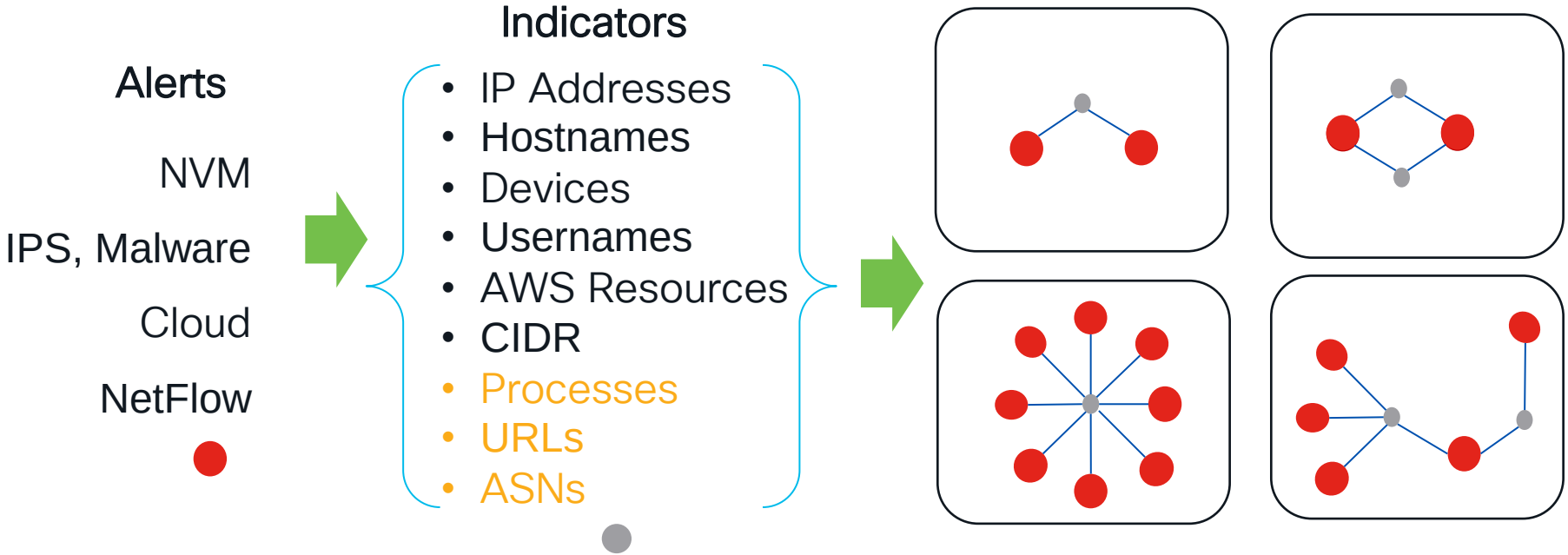


By correlating alerts and events into incidents, Alert Chains focus the investigation

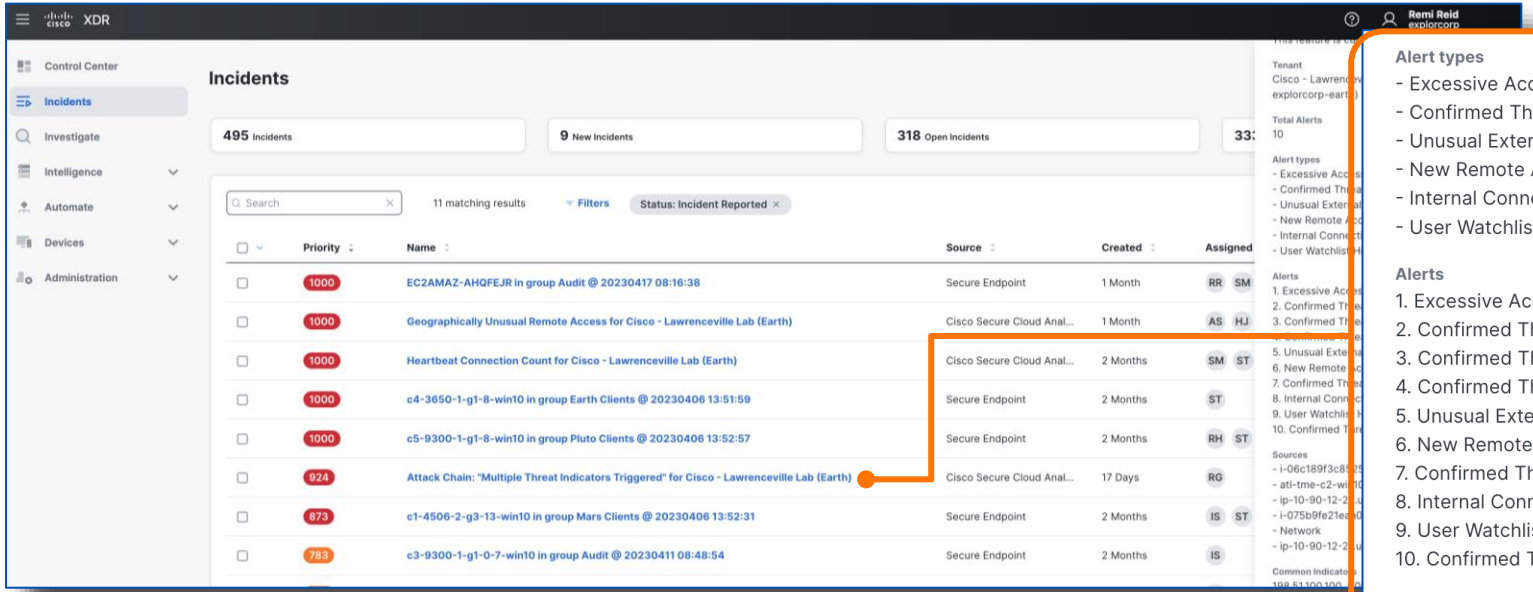
- Correlated events arranged as a tactically-oriented timeline
- Brings clarity to IR
- Weighs telemetry with context.



Alert Chaining correlates using an increasing list of Common Indicators



XDR combines available telemetry to create richer situational awareness

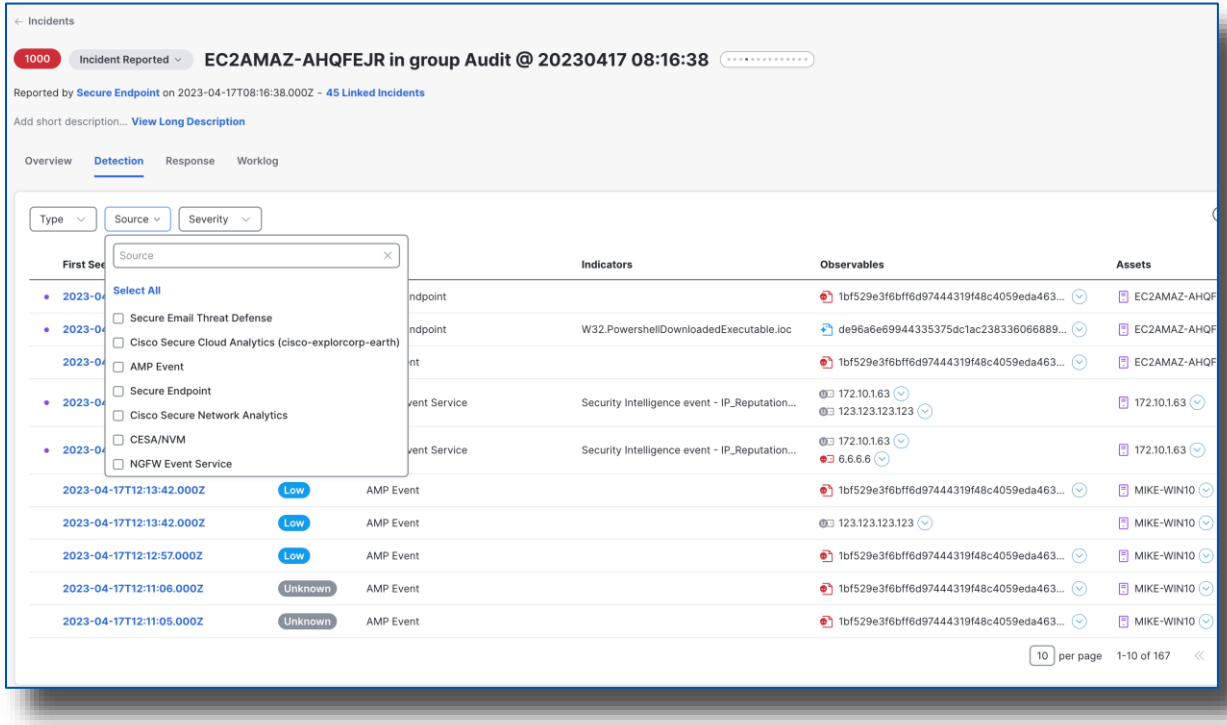


- Helps corollate, ID behaviors, and recommend response
- Sources tracked, used to spur further enrichment and Alert Chaining

After XDR Analytics or another CTIM source escalates, enrichment completes the picture

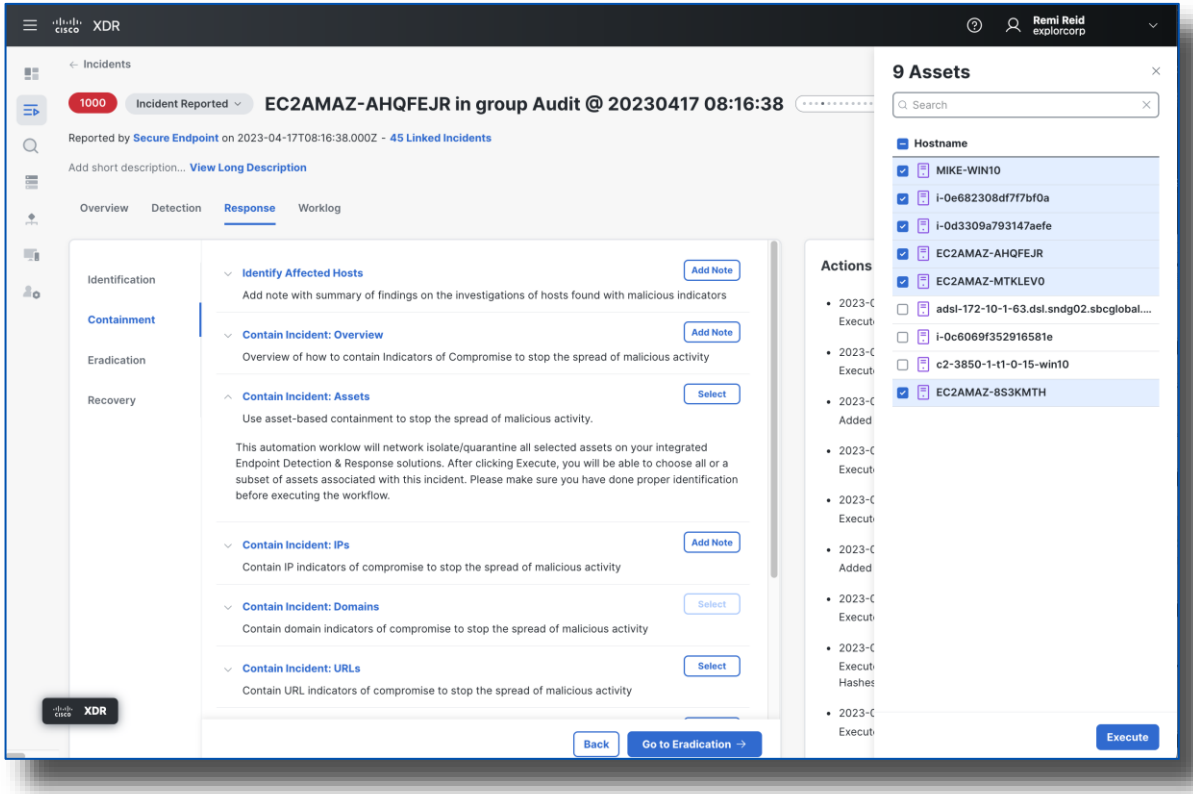
CTI, Device/User insights, other integrated modules enhance observations

- Ensure the impact and scale are clear
- CTI sources help categorize external actors
- User & Device context help assess risk and urgency

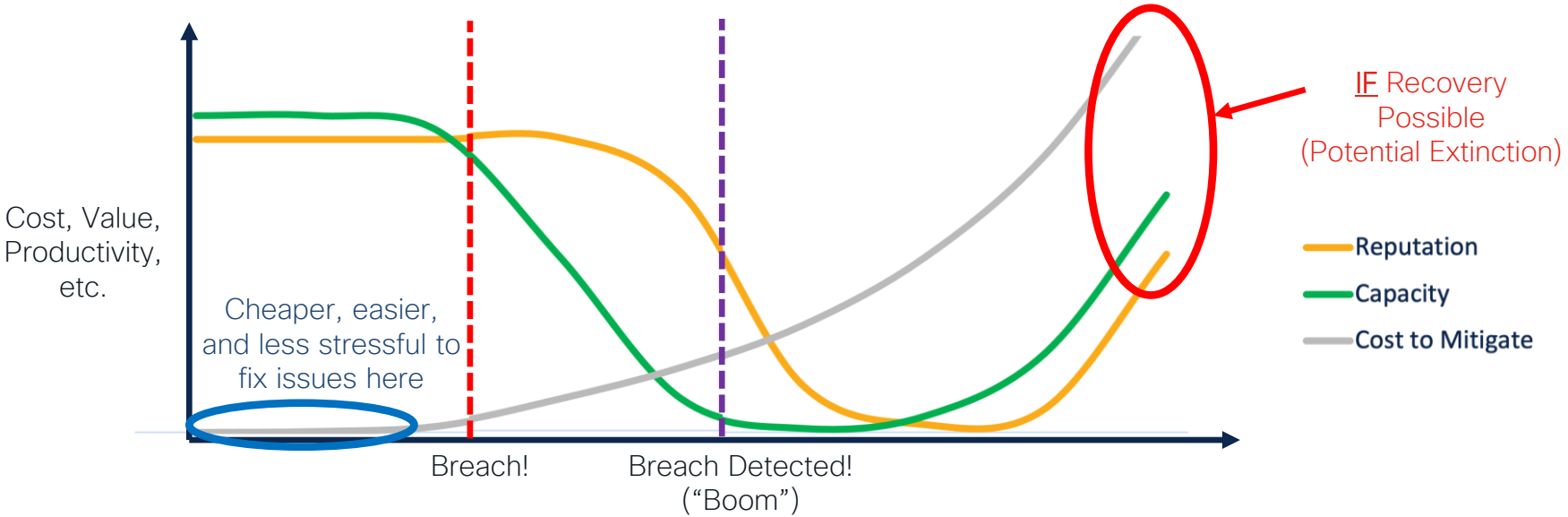


Visibility is used by Cisco XDR to guide and simplify response plans

- Visibility used to select MDR/CX/IR-recommended response actions
- SANS “PICERL” IR Framework guides response
- Enriched telemetry also delivered to Automation playbooks as needed



Earlier, more accurate Detection == Cheaper Mitigation



- Better to be "left of boom" – tackle problems before becoming acute!
- Earlier & effective controls = better performance, lower pressure/cost, preserved reputation
- Intel & Visibility relieves pressure! Not just for Global corporations/governments…we all need it!

The Cisco approach to XDR

Detect more, act faster, elevate productivity, build resilience

Detect the most sophisticated threats

- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimized for multi-vendor environments

Act on what *truly* matters, faster

- Prioritize threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations

Elevate productivity

- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks

Build resilience

- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, everyday with continuous, quantifiable improvement

The value of getting XDR right

50%
Decreased risk and cost of data breach

90%
Reduction of analyst effort per incident

90%
Increase in SecOps efficiency

85%
Reduction of attack dwell times

Better Security

Higher Performance

Faster Response

Better Detection

"It will make things easier, faster, and we will see much more going on in our environment than ever before."

– Michael Degroote, Mohawk Industries

Source: TEI (Total Economic Impact) study of Cisco's integrated security platform

Putting it all together!

- Unlock the telemetry you already own!
  - Netflow/IPFIX, NBAR/AVC, device tracking, packet captures, etc.
  - Team with NetOps: same efforts can improve network outcomes
  - Security context helps shed light on endpoints, users, and applications
- Latent visibility is critical to seeing many XDR focus areas:
  - Exfiltration, Command & Control
  - Insider Threat
  - DoS/DDoS
- Cisco XDR's focus on visibility closes the OODA loop and enhances remediation
- Cybersecurity is risk-reduction → why not actually focus on reducing risk rather than addressing impact?

Learning more – High Level

- Cisco XDR Main Page: https://www.cisco.com/go/xdr
- Cisco XDR Primer: https://www.cisco.com/c/en/us/products/collateral/security/xdr/xdr-primer-simplifying-security-operations.html
- Cisco XDR Webinars, Blogs, etc.: https://www.cisco.com/site/us/en/products/security/xdr/resources.html
- RSA Conference 2023 XDR Product Launch Keynote: https://www.youtube.com/watch?v=1NTm7vM_e8Y
- Click-Thru Demo of Cisco XDR: https://cs.co/xdr-product-tour
- Cisco XDR At-A-Glance: https://www.cisco.com/c/dam/en/us/products/collateral/security/xdr/xdr-aag.pdf
- Cisco XDR Security Operations Simplified E-Book: https://www.cisco.com/c/en/us/products/security/cisco-xdr-security-operations-simplified-ebook.html

Learning more – Related Training & References

- References:
  - MITRE's 11 Strategies of a World-Class SOC: https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
- Related Training:
  - Cisco Secure Analytics Training portal (mostly free!): https://learnsecureanalytics.cisco.com/
  - Cisco SecureX Training Portal (much of the integrations, orchestration & automation content will still apply!): https://learnsecurex.cisco.com/
- Integrations:
  - Cisco Security Technical Alliance (CSTA): https://www.cisco.com/go/csta
  - Legacy SecureX Code Exchange repository (much of it should carry over!): https://developer.cisco.com/codeexchange/search/?categories=Security&products=SecureX

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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

The bridge to possible

Thank you

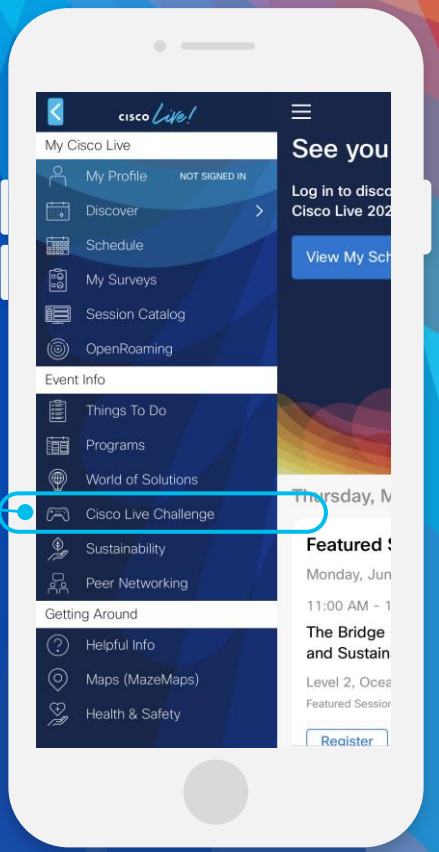
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!


cisco Live!
Let's go
#CiscoLive