DRAGOS

OT Threats Won’t Wait

Defend Critical Operations at Speed

Shaunna Hargrave
Sr. Industrial Responder

Mark Urban
Product, VP

Danielle Gauthier
Product, Intel/OT Watch

Agenda

1 OT SECURITY

- Baseline
- OT Threats
- Architect for MTTR

2 GAIN VISIBILITY: ASSETS & VULNS BASELINE

3 OPERATING AT SPEED, AT SCALE - WORKFLOWS

- Monitoring
- Detection
- Triage
- Investigation
- Resolution

4 DRAGOS PLATFORM

Exposed at Scale

Remote access & digital transformation introduce new risks. Common software elements across diverse systems create scalable attack opportunities.

IT Security Tools Struggle

IT tools don't understand OT systems & protocols, lack operational context, and often conflict with operations teams.

OPERATIONAL TECHNOLOGY (OT)

Automation systems that manage physical processes.

Business foundation for manufacturing, water & energy utilities, oil & gas, medical, logistics & transportation, building & data center management

Ransomware Groups & State-Sponsored Adversaries

Thousands of ransomware attacks on OT-reliant businesses; 23 dedicated threat groups; 9 ICS/OT-specific malware families.

Operational Blindness

Limited visibility into assets, networks, remote connections, threats, vulnerabilities, and misconfigurations. Complicates business continuity & compliance.

How Executing OT Intrusions Changed

Ransomware accelerates timelines, but that's not the whole story.


1171 Manufacturing


177 Industrial Control Systems


176 Transportation


44 Oil & Gas


41 Communications


30 Electric


20 Government


12 Water


11 Mining


7 Renewables


4 Data Centers

TOTAL: 1693 INCIDENTS

What adversaries leverage

- Public knowledge, off the shelf tooling
- Valid accounts & admin tools (LOTL)
- Ransomware economy rewards speed

Where friction dropped in OT

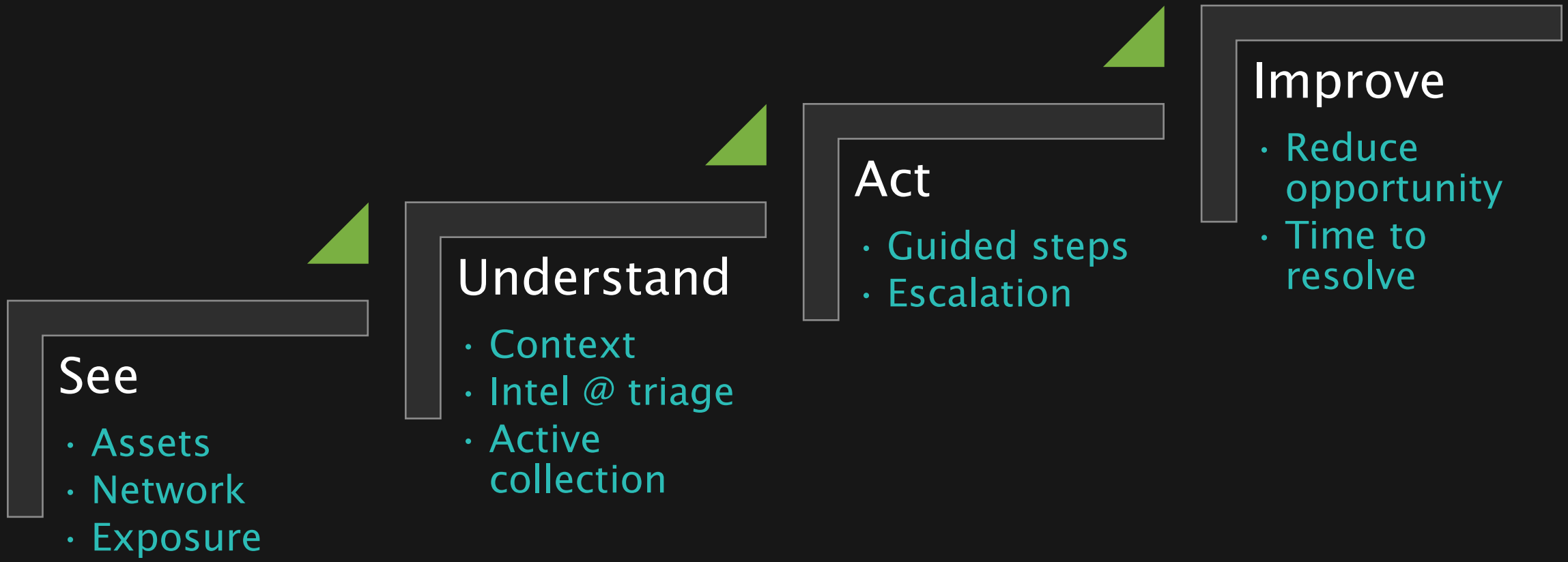
- Vendor/remote access
- Shared/reused credentials
- More reachable paths

How impact shows up

- Loss of view/control or safety stops
- Out-of-window maintenance changes
- Routine traffic until state change confirmed

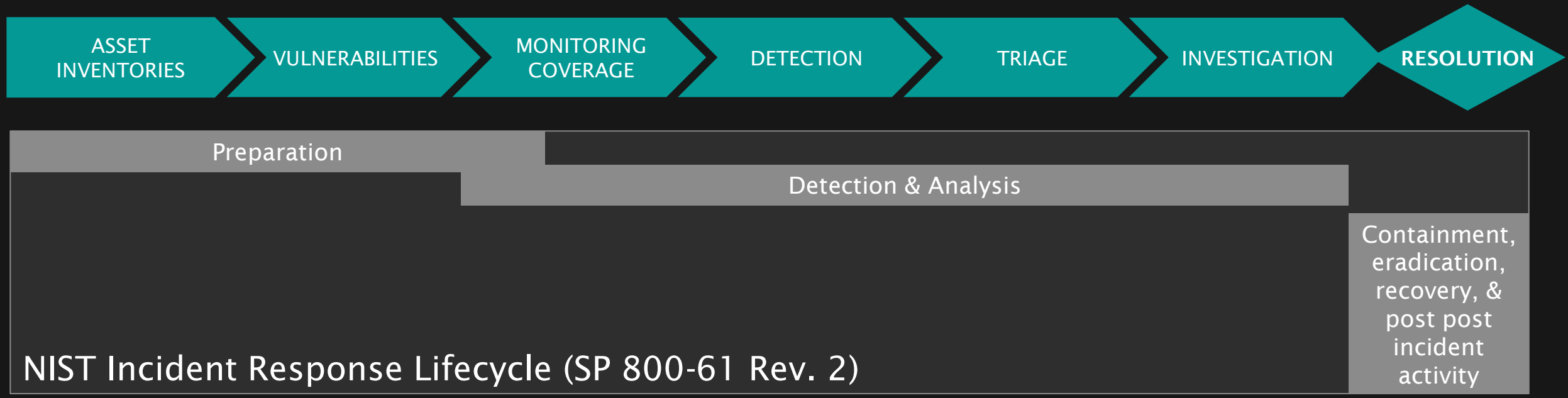
Why OT Visibility Matters

OT visibility is the pre-condition.



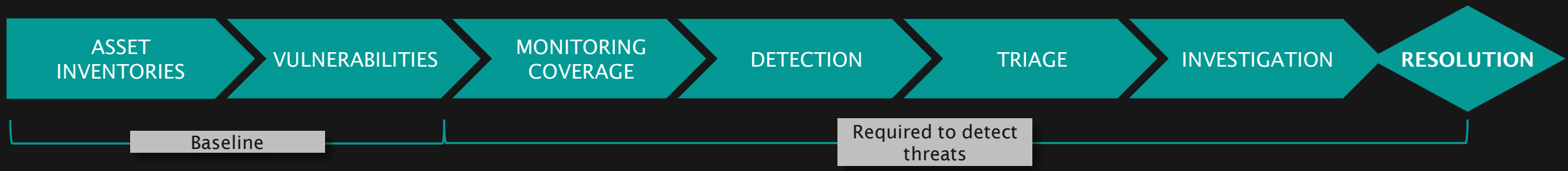
Architect for Fast Response & Resolution

Leverage Mean Time to Resolution (MTTR)



Architect for Fast Response & Resolution

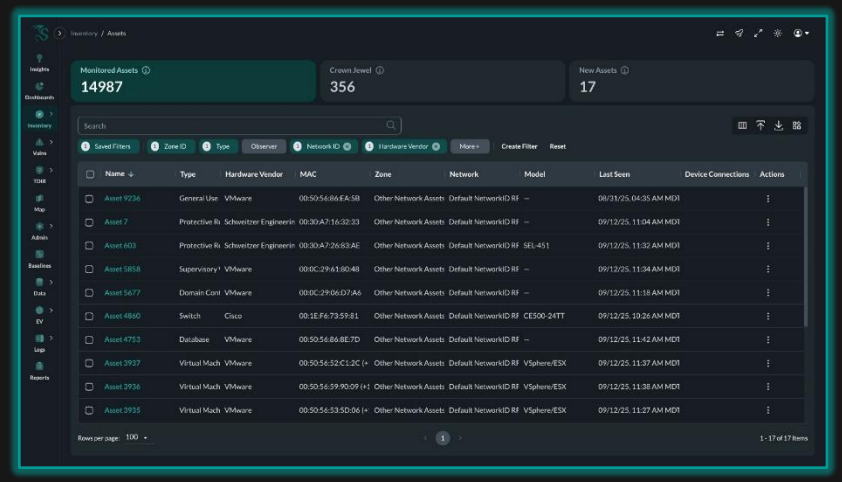
Challenges



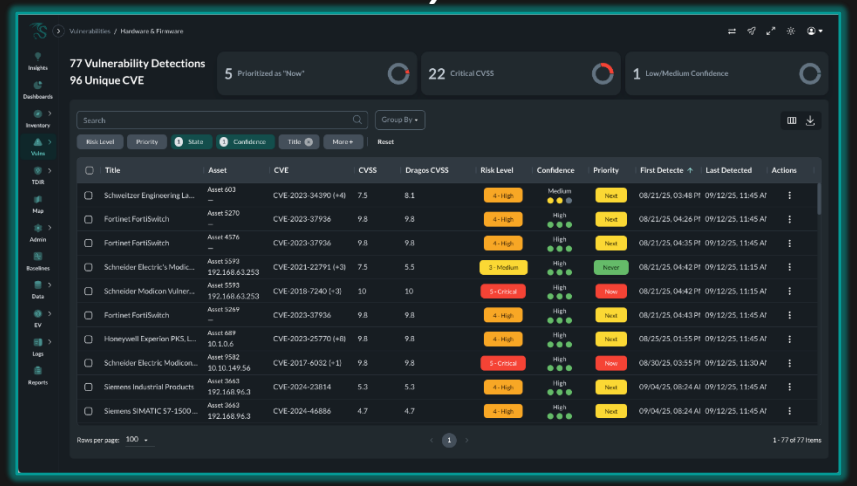
1. Stuck at "*Square one*" Batch-based asset uploads with no continuous asset discovery & monitoring,
2. IT-focused risk scores & mitigation
3. **Coverage** monitor crown jewels assets / core OT processes at critical sites
4. **Noise** Anomaly detection engines with little OT threat context create high alarm rates
5. **Prioritization** How to choose which alerts are important
6. **Lack of Guidance** What to do next?
7. **Lack of expertise** OT forensics, repair, restoration, reporting…

Gain Visibility: Assets & Vulns Baseline

Asset Inventory

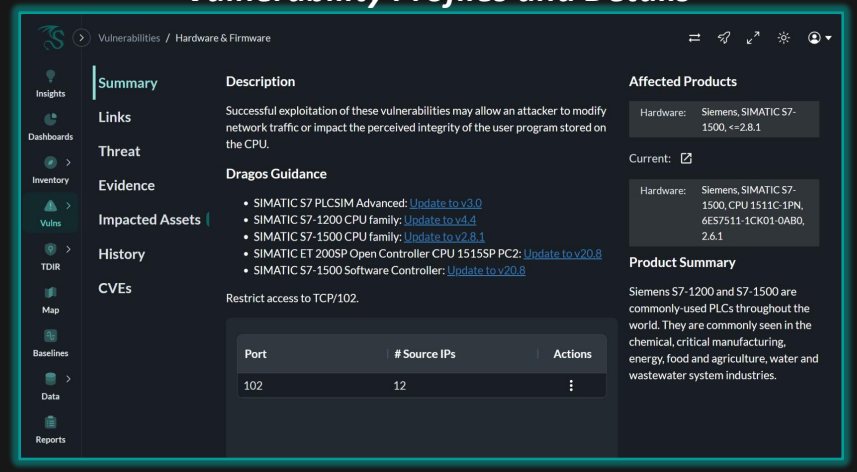


Vulnerability Dashboard



Zones and Comms

Vulnerability Proflies and Details



BUILDING EFFECTIVE OT CYBER PROGRAM

Mind the Gap

YOUR CYBER SECURITY RESOURCE & SKILL BASE (Probably IT Focused)	**DRAGOS** MANAGED PLATFORM SERVICE OT INCIDENT RESPONSE & ASSESSMENT SVCS & AI-ANALYST ASSIST TECH	OT CYBER SECURITY CAPABILITY

Operating at Speed, at Scale

Workflow Overview

1. Monitoring
2. Detection
3. Triage
4. Investigation
5. Resolution

Dragos DFIR Specialist

Dragos Managed Platform Service
OTWatch Complete

Insights
Dashboards
Inventory
Vulns
TDIR
Map
Baselines
Data
Reports

Welcome

Visibility

2 Sensors

- Paused 1/2
- Up to Date 2/2
- Ingest — Avg: 29.11 MB/s Last 7 days

Security

5,994 Internal Assets

- Unzoned Internal Assets
- Open Critical NOW Vulnerabilities
- New Sev. 4+ Alerts

Integrations

1 Service

- Active Integrations — Firewall

Recommendations

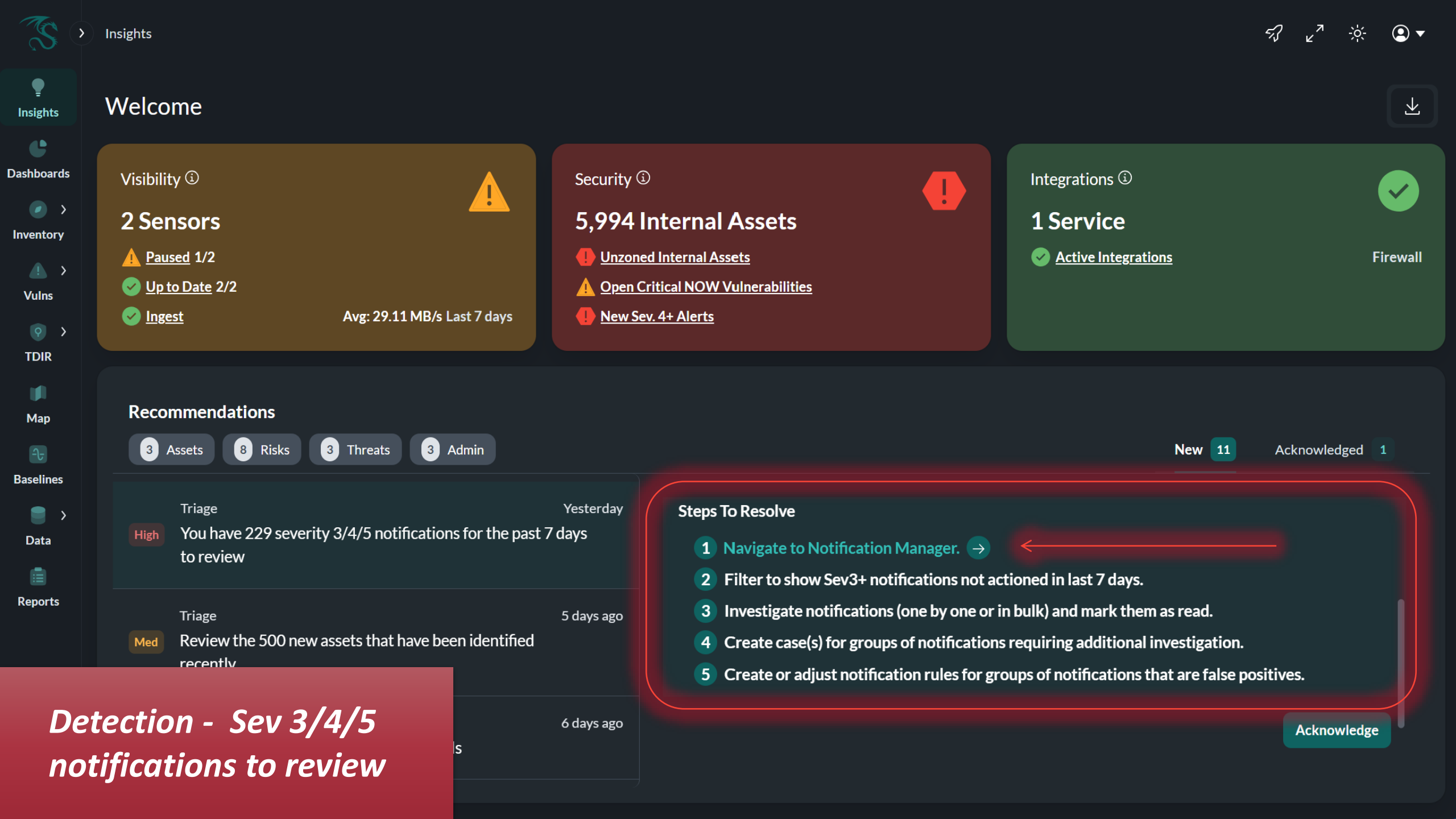
3 Assets | 8 Risks | 3 Threats | 3 Admin

New 11 | Acknowledged 1

High	Triage: You have 229 severity 3/4/5 notifications for the past 7 days to review	Yesterday
Med	Triage: Review the 500 new assets that have been identified recently	5 days ago
Med	Triage: 98 assets are using Clear Text Credentials	6 days ago

Select a recommendation to view details

Monitoring – One place to start (prioritized)


Insights
Insights
Dashboards
Inventory
Vulns
TDIR
Map
Baselines
Data
Reports
Welcome
Visibility
2 Sensors
Paused 1/2
Up to Date 2/2
Ingest
Avg: 29.11 MB/s Last 7 days
Security
5,994 Internal Assets
Unzoned Internal Assets
Open Critical NOW Vulnerabilities
New Sev. 4+ Alerts
Integrations
1 Service
Active Integrations
Firewall
Recommendations
3 Assets
8 Risks
3 Threats
3 Admin
New 11
Acknowledged 1
Triage
Yesterday
High
You have 229 severity 3/4/5 notifications for the past 7 days to review
Triage
5 days ago
Med
Review the 500 new assets that have been identified recently
6 days ago
Steps To Resolve
1 Navigate to Notification Manager.
2 Filter to show Sev3+ notifications not actioned in last 7 days.
3 Investigate notifications (one by one or in bulk) and mark them as read.
4 Create case(s) for groups of notifications requiring additional investigation.
5 Create or adjust notification rules for groups of notifications that are false positives.
Acknowledge
Detection - Sev 3/4/5 notifications to review

Insights
Dashboards
Inventory
Vulns
TDIR
Map
Baselines
Data
Reports

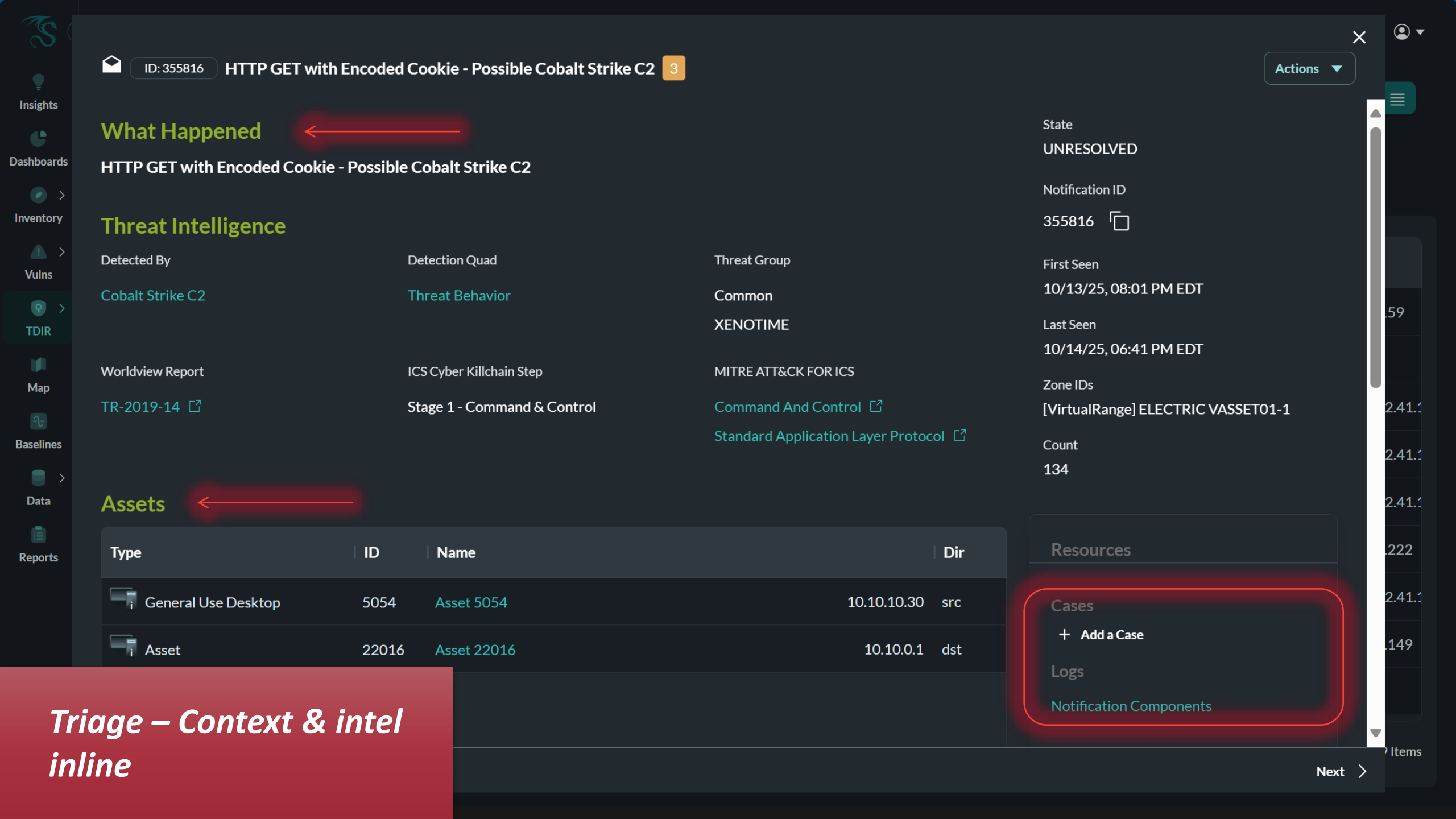
FILTERING | From 10/14/25, 02:43 AM EDT | To 10/16/25, 02:43 AM EDT | REFRESH | Auto-Refresh | Search

Severity >= 2 | Notification State == Unresolved | Show Only Baseline Summaries

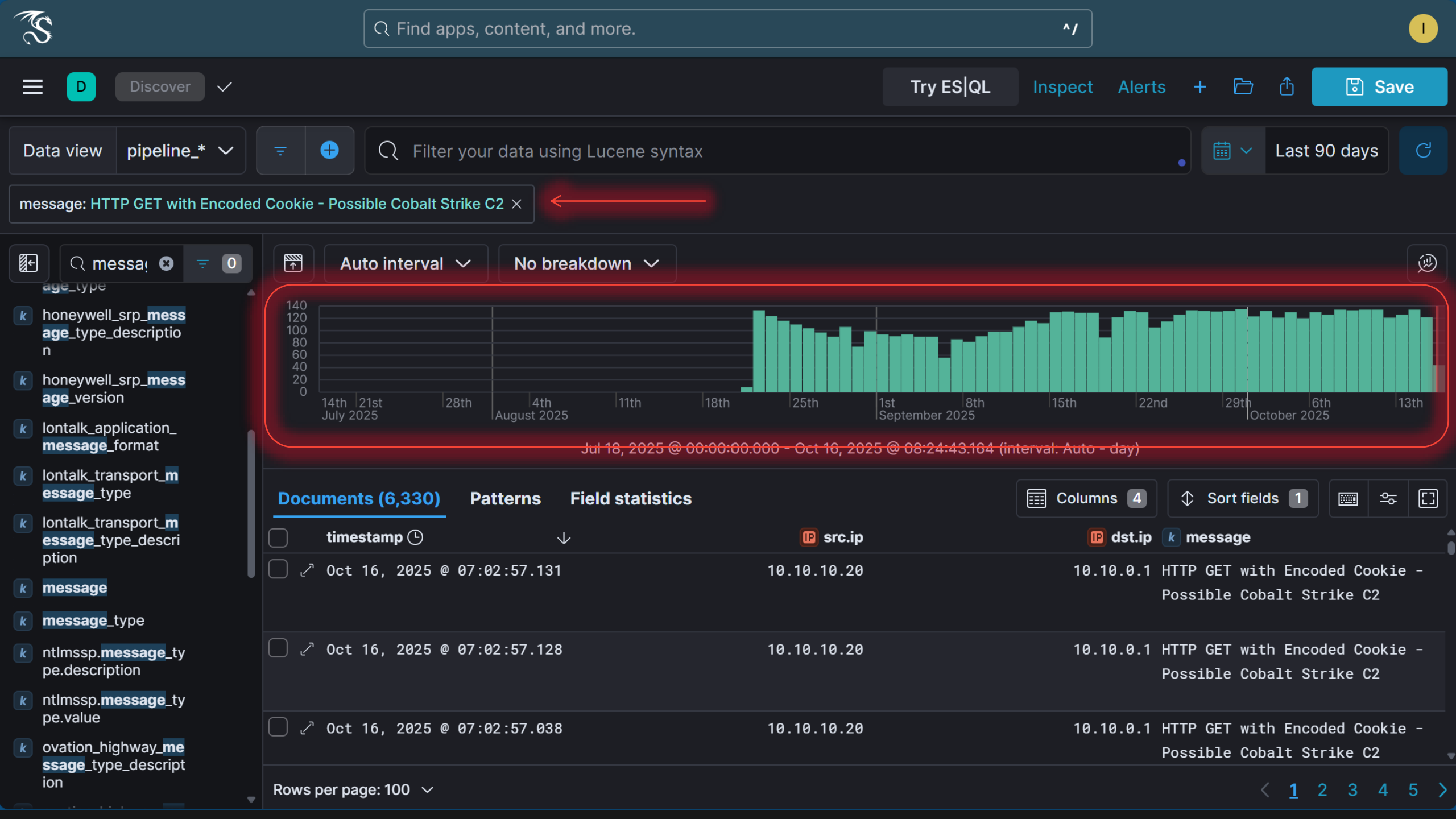
ID	Severity	Count	Last Seen	Summary	Src. IPv4	Dest. IPv4
356734	4	15	10/14/25, 07:02 PM	File Transfer Matched File Signature Rule	246.237.43.151	246.237.43.159
357315	4	29	10/14/25, 07:52 PM	DNP3 Stop Application Flood Detected	192.168.123.69	10.40.1.69
355814	3	106	10/14/25, 06:42 PM	HTTP POST with Encoded Payload - Possible Cobalt Strike C2	10.10.10.20	10.10.0.1, 192.41.:
355816	3	134	10/14/25, 06:41 PM	HTTP GET with Encoded Cookie - Possible Cobalt Strike C2	10.10.10.30	10.10.0.1, 192.41.:
356658	3	4	10/14/25, 07:22 AM	Cobalt Strike Behaviors	10.10.0.10, 192.16	10.10.0.1, 192.41.:
355805	2	286	10/14/25, 07:55 PM	RDP Auth Bypass Attempt Possible	192.168.193.10	192.168.211.222
355815	2	134	10/14/25, 06:41 PM	Cobalt Strike User-Agent + Cookie M2	10.10.10.30	10.10.0.1, 192.41.:
355819	2	170	10/14/25, 07:40 PM	HTTP Download Executable Smaller than 1 MB		

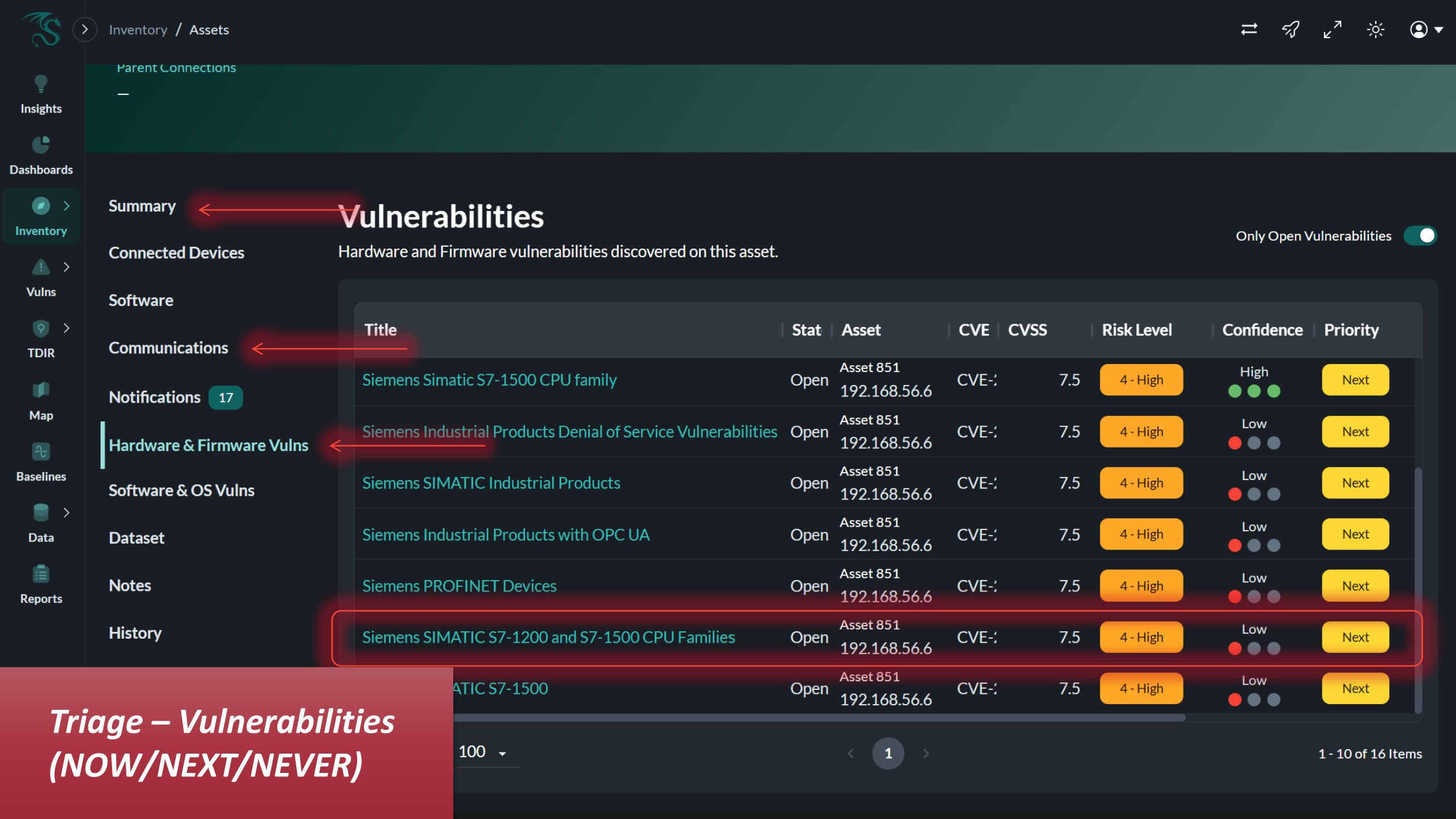
Rows per page: 100 | 1

Detection – Filter high-severity alerts

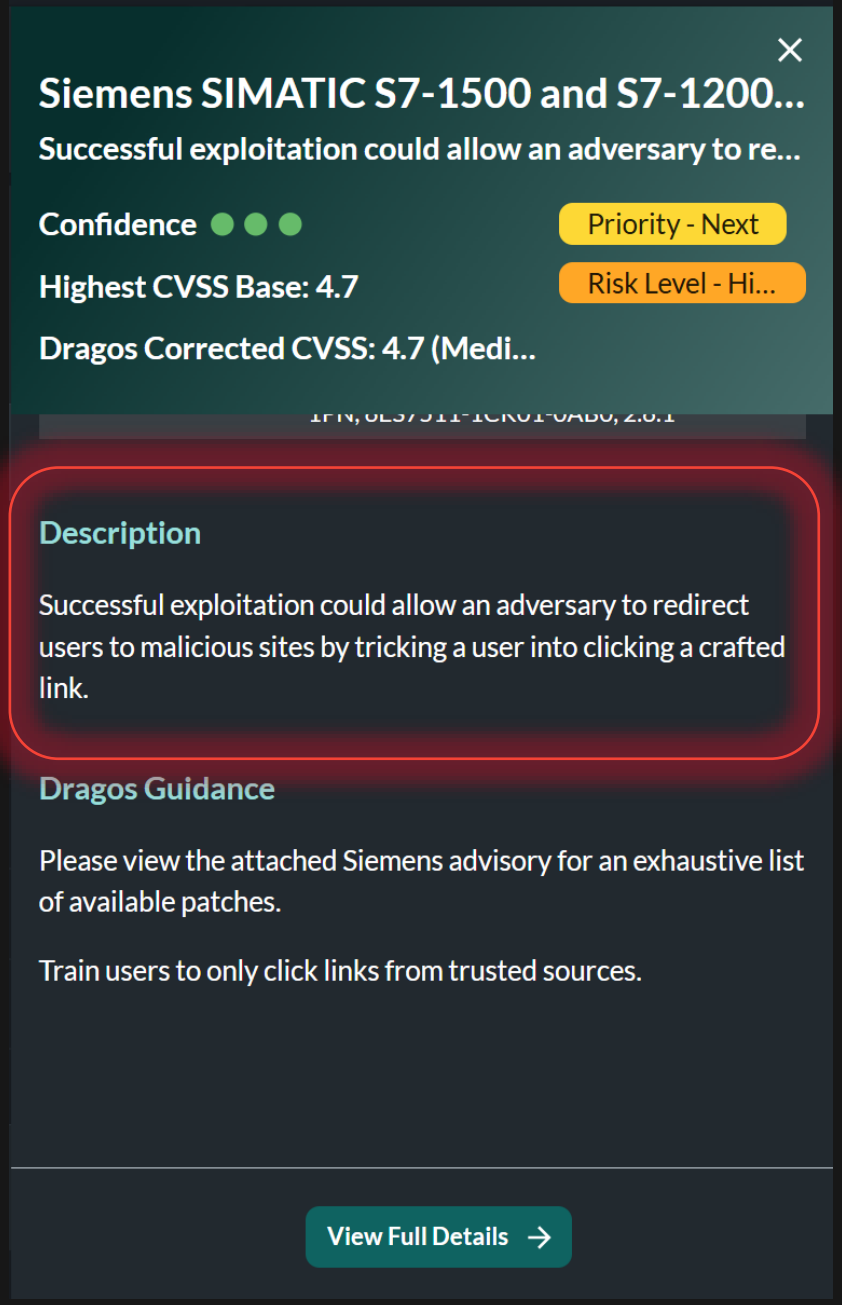


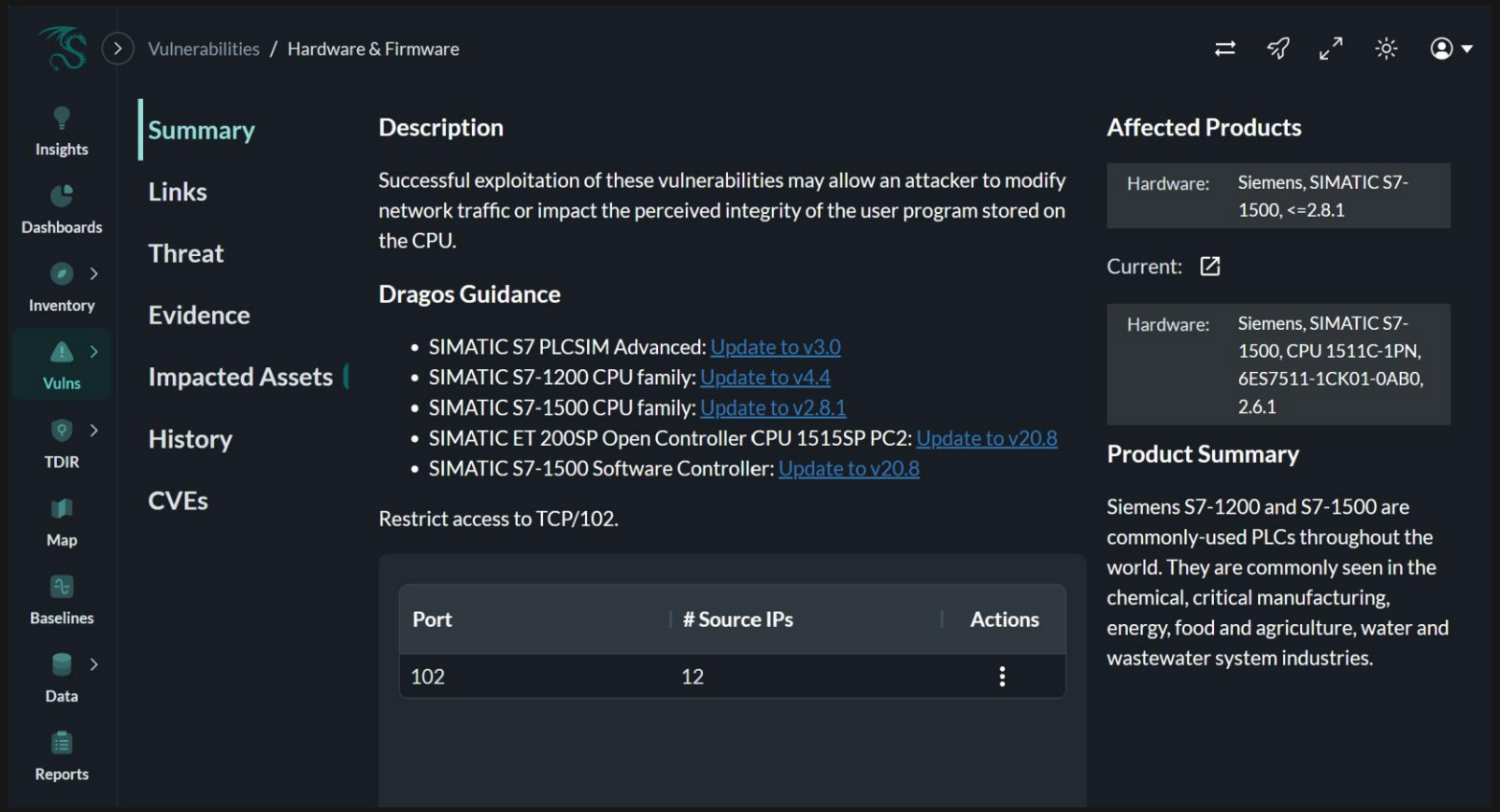
Triage – Context & intel inline

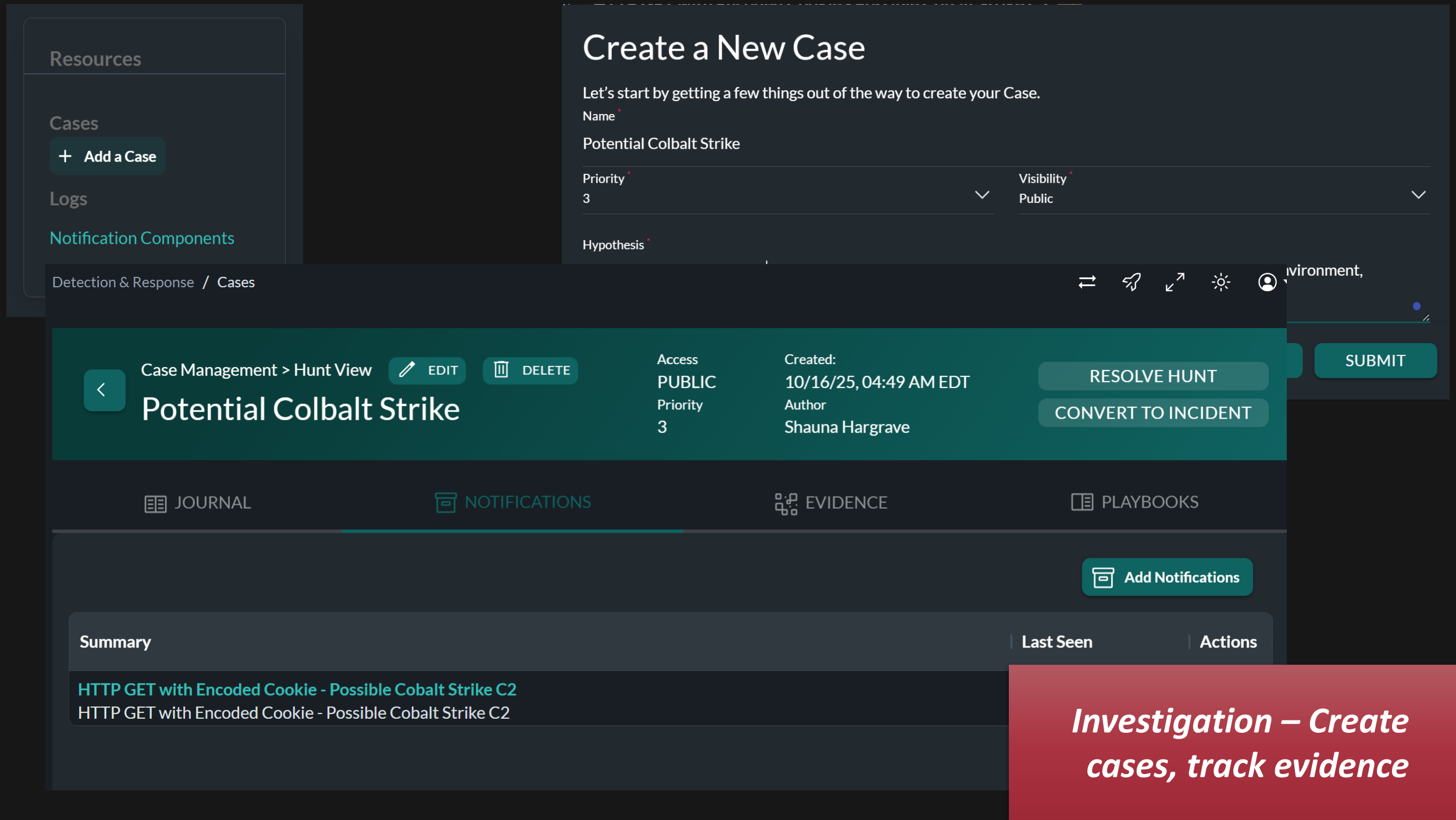

Find apps, content, and more.
Discover
Try ES|QL
Inspect
Alerts
Save
Data view
pipeline_*
Filter your data using Lucene syntax
Last 90 days
message: HTTP GET with Encoded Cookie - Possible Cobalt Strike C2
Auto interval
No breakdown
honeywell_srp_message_type_description
honeywell_srp_message_version
lontalk_application_message_format
lontalk_transport_message_type
lontalk_transport_message_type_description
message
message_type
ntlmssp.message_type.description
ntlmssp.message_type.value
ovation_highway_message_type_description
Jul 18, 2025 @ 00:00:00.000 - Oct 16, 2025 @ 08:24:43.164 (interval: Auto - day)
Documents (6,330)
Patterns
Field statistics
Columns 4
Sort fields 1
timestamp
src.ip
dst.ip
message
Oct 16, 2025 @ 07:02:57.131 10.10.10.20 10.10.0.1 HTTP GET with Encoded Cookie - Possible Cobalt Strike C2
Oct 16, 2025 @ 07:02:57.128 10.10.10.20 10.10.0.1 HTTP GET with Encoded Cookie - Possible Cobalt Strike C2
Oct 16, 2025 @ 07:02:57.038 10.10.10.20 10.10.0.1 HTTP GET with Encoded Cookie - Possible Cobalt Strike C2
Rows per page: 100
1 2 3 4 5

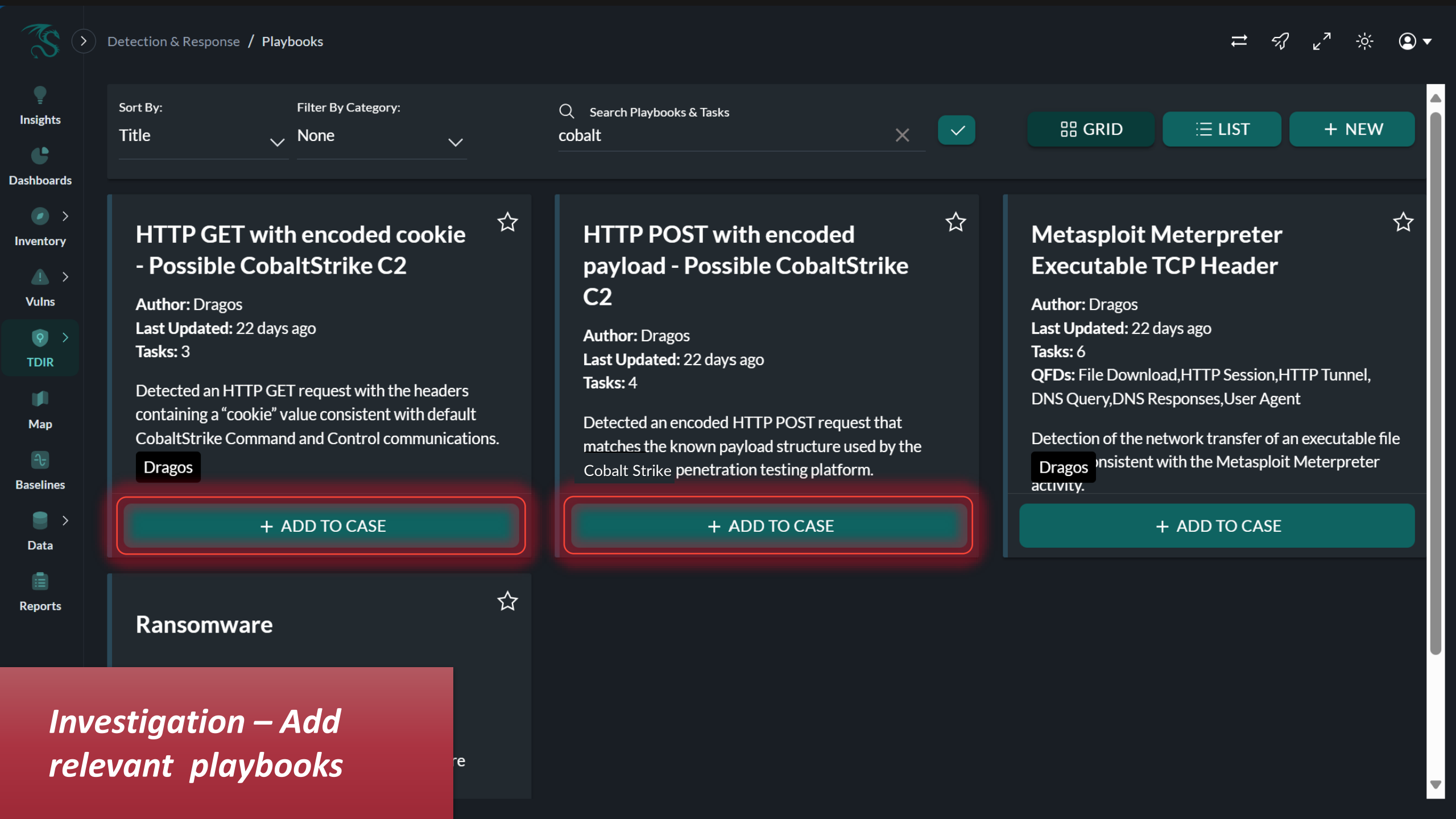


Triage – Vulnerabilities (NOW/NEXT/NEVER)


Siemens SIMATIC S7-1500 and S7-1200...
Successful exploitation could allow an adversary to re...
Confidence
Priority - Next
Highest CVSS Base: 4.7
Risk Level - Hi...
Dragos Corrected CVSS: 4.7 (Medi...
Description
Successful exploitation could allow an adversary to redirect users to malicious sites by tricking a user into clicking a crafted link.
Dragos Guidance
Please view the attached Siemens advisory for an exhaustive list of available patches.
Train users to only click links from trusted sources.
View Full Details


Vulnerabilities / Hardware & Firmware
Insights
Dashboards
Inventory
Vulns
TDIR
Map
Baselines
Data
Reports
Summary
Links
Threat
Evidence
Impacted Assets
History
CVEs
Description
Successful exploitation of these vulnerabilities may allow an attacker to modify network traffic or impact the perceived integrity of the user program stored on the CPU.
Dragos Guidance
SIMATIC S7 PLCSIM Advanced: Update to v3.0
SIMATIC S7-1200 CPU family: Update to v4.4
SIMATIC S7-1500 CPU family: Update to v2.8.1
SIMATIC ET 200SP Open Controller CPU 1515SP PC2: Update to v20.8
SIMATIC S7-1500 Software Controller: Update to v20.8
Restrict access to TCP/102.
Port
Source IPs
Actions
102
12
Affected Products
Hardware: Siemens, SIMATIC S7-1500, <=2.8.1
Current:
Hardware: Siemens, SIMATIC S7-1500, CPU 1511C-1PN, 6ES7511-1CK01-0AB0, 2.6.1
Product Summary
Siemens S7-1200 and S7-1500 are commonly-used PLCs throughout the world. They are commonly seen in the chemical, critical manufacturing, energy, food and agriculture, water and wastewater system industries.


Resources
Cases
+ Add a Case
Logs
Notification Components
Create a New Case
Let's start by getting a few things out of the way to create your Case.
Name *
Potential Colbalt Strike
Priority *
3
Visibility *
Public
Hypothesis *
vironment,
SUBMIT
Detection & Response / Cases
Case Management > Hunt View
EDIT
DELETE
Potential Colbalt Strike
Access
PUBLIC
Priority
3
Created:
10/16/25, 04:49 AM EDT
Author
Shauna Hargrave
RESOLVE HUNT
CONVERT TO INCIDENT
JOURNAL
NOTIFICATIONS
EVIDENCE
PLAYBOOKS
Add Notifications
Summary
Last Seen
Actions
HTTP GET with Encoded Cookie - Possible Cobalt Strike C2
HTTP GET with Encoded Cookie - Possible Cobalt Strike C2
Investigation – Create cases, track evidence


Detection & Response / Playbooks
Insights
Dashboards
Inventory
Vulns
TDIR
Map
Baselines
Data
Reports
Sort By:
Title
Filter By Category:
None
Search Playbooks & Tasks
cobalt
GRID
LIST
+ NEW
HTTP GET with encoded cookie - Possible CobaltStrike C2
Author: Dragos
Last Updated: 22 days ago
Tasks: 3
Detected an HTTP GET request with the headers containing a "cookie" value consistent with default CobaltStrike Command and Control communications.
Dragos
+ ADD TO CASE
HTTP POST with encoded payload - Possible CobaltStrike C2
Author: Dragos
Last Updated: 22 days ago
Tasks: 4
Detected an encoded HTTP POST request that matches the known payload structure used by the Cobalt Strike penetration testing platform.
+ ADD TO CASE
Metasploit Meterpreter Executable TCP Header
Author: Dragos
Last Updated: 22 days ago
Tasks: 6
QFDs: File Download,HTTP Session,HTTP Tunnel, DNS Query,DNS Responses,User Agent
Detection of the network transfer of an executable file
Dragos
activity.
+ ADD TO CASE
Ransomware
Investigation – Add relevant playbooks

2

Verify the detected cookie value

The first step in responding to this detection is to confirm that detected cookie value, and other properties of the corresponding HTTP communication, match those of the default Cobalt Strike C2 communication.
To review the communication metadata and confirm the cookie and header details:

1. In the Notification details window, locate the "`Notification Components`" section and click on "`View in Kibana`". A new tab will open, with Kibana results filtered down to the corresponding traffic record. -- Tip: If no record is displayed in the Kibana window that opens, try extending the search time range by clicking on the date picker in top-right of the Kibana window and setting it to a higher number of days
2. With the record displayed, the date histogram displayed above the record should have a green bar, corresponding to the time of the detection occurrence. Narrow down the search time range to the detection window by clicking on this bar. The time range should limit to +/- 30 minutes of the detection.
3. Now that the time range is narrowed down, change the filter to find the exact cookie value that triggered the detection, instead of showing the detection itself. To do so, delete the "`uuid:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx`" in the search field and replace it with the following regular expression: "`headers:/.*COOKIE\|[A-Za-z0-9\/\+]*=.*/`" -- Tip: If you receive a "Lucene syntax warning" popup, make sure to change the search query language from "KQL" to "Lucene" by clicking on "KQL" displayed to the right of the search field and toggling the "`Kibana Query Language`" switch to "`Off`"; rerun the above query.
4. You should see one or more HTTP communication records displayed below. Inspect them for presence of a long, pseudo-random string being contained in the "`headers`" field, following the "`COOKIE|`" identifier. A typical Cobalt Strike Beacon cookie value will look like this: "`RFlfgsvJpeTZmpyzavnskBeIeBSDRF2B0b3v5+[...]WaRaOI=`"
5. Find the record matching the detection, by comparing the "`Occurred At`" timestamp, "`Source IP`", "`Destination IP`" and "`Destination Port`" captured in the previous step to the corresponding "`timestamp`", "`src_ip`", "`dst_ip`" and "`dst_port`" fields. -- Tip: You can click on the "greater than" (">") symbol to the left of the record, to expand it and make reviewing field values easier.
6. Review and document other properties of the HTTP communication if present -- Value following the "`HOST|`" identifier in the "`headers`" field (typically an IP address or domain name) -- Value of the "`host`" field (typically an IP address, matching the "`dst_ip`" value) -- Value following the "`USER-AGENT|`" identifier in the "`headers`" field (typically an alphanumeric string, starting with "Mozilla") -- Value of the "`uri`" field (typically a

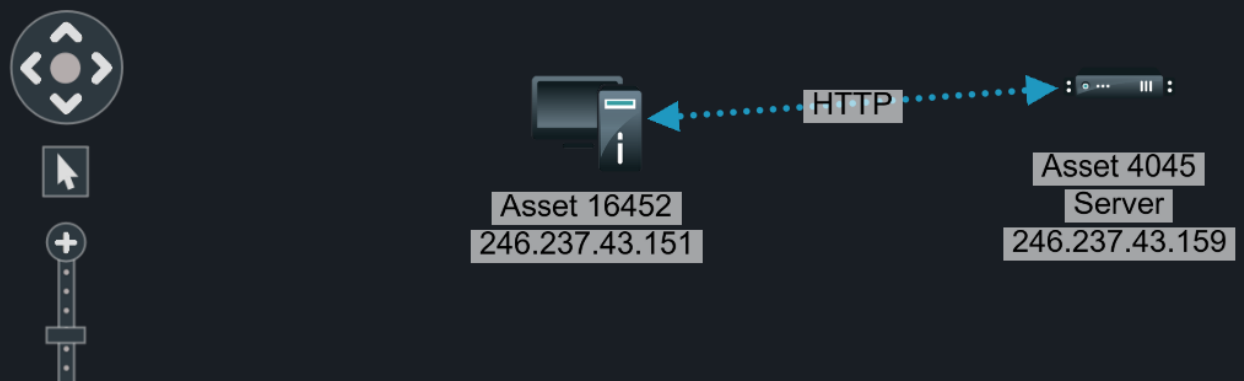
ID: 356734 **File Transfer Matched File Signature Rule** 4

Actions

Type	ID	Name		Dir
Server	4045	Asset 4045	246.237.43.159	dst
Asset	16452	Asset 16452	246.237.43.151	src

Rows per page: 10 1 1 - 2 of 2 Items

Communications



Cases

+ Add a Case

Files

Crack password Koyo D...

Logs

Notification Record

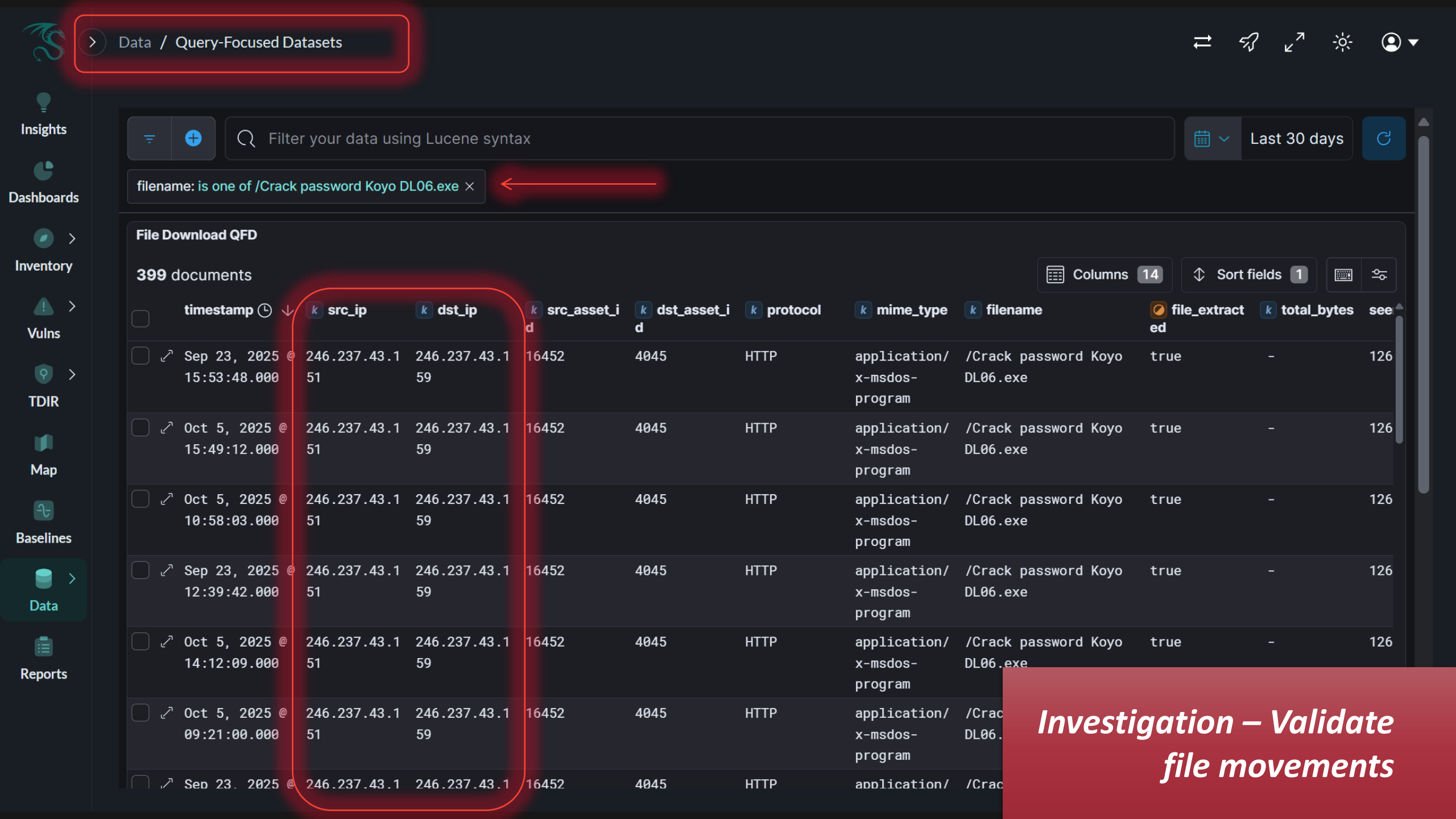
Notification Components

QFDs

YARA

File Download

Investigation – Consult logs and pull artifacts


Data / Query-Focused Datasets
Insights
Dashboards
Inventory
Vulns
TDIR
Map
Baselines
Data
Reports
Filter your data using Lucene syntax
Last 30 days
filename: is one of /Crack password Koyo DL06.exe
File Download QFD
399 documents
Columns 14
Sort fields 1
timestamp
src_ip
dst_ip
src_asset_id
dst_asset_id
protocol
mime_type
filename
file_extracted
total_bytes
Sep 23, 2025 @ 15:53:48.000 246.237.43.151 246.237.43.159 16452 4045 HTTP application/x-msdos-program /Crack password Koyo DL06.exe true - 126
Oct 5, 2025 @ 15:49:12.000 246.237.43.151 246.237.43.159 16452 4045 HTTP application/x-msdos-program /Crack password Koyo DL06.exe true - 126
Oct 5, 2025 @ 10:58:03.000 246.237.43.151 246.237.43.159 16452 4045 HTTP application/x-msdos-program /Crack password Koyo DL06.exe true - 126
Sep 23, 2025 @ 12:39:42.000 246.237.43.151 246.237.43.159 16452 4045 HTTP application/x-msdos-program /Crack password Koyo DL06.exe true - 126
Oct 5, 2025 @ 14:12:09.000 246.237.43.151 246.237.43.159 16452 4045 HTTP application/x-msdos-program /Crack password Koyo DL06.exe true - 126
Oct 5, 2025 @ 09:21:00.000 246.237.43.151 246.237.43.159 16452 4045 HTTP application/x-msdos-program
Investigation – Validate file movements

Insights
Dashboards
Inventory
Vulns
TDIR
Map
Baselines
Data

Filter your data using Lucene syntax

Last 30 days

DNS Queries QFD

70,308 documents

Columns 6 | Sort fields 1

timestamp	client_id	query_name	server	first_seen	last_seen
Oct 16, 2025 @ 08:59:49.792	-	vcsa.vmware.com	208.91.112.53	Sep 12, 2025 @ 16:58:28.283	Oct 16, 2025 @ 08:59:49.792
Oct 16, 2025 @ 09:13:03.284	-	netnod.se	208.91.112.52	Sep 13, 2025 @ 00:20:21.207	Oct 16, 2025 @ 09:13:03.284
Oct 16, 2025 @ 09:07:14.310	-	mtalk.google.com	208.91.112.52	Sep 12, 2025 @ 16:41:53.770	Oct 16, 2025 @ 09:07:14.310
Oct 16, 2025 @ 09:07:14.316	-	mtalk.google.com	192.168.210.2	Sep 12, 2025 @ 16:21:11.615	Oct 16, 2025 @ 09:07:14.316
Oct 16, 2025 @	-	msn.com	208.91.112.52	Sep 12, 2025 @ 16:27:35.357	Oct 16, 2025 @ 09:09:35.587

Case Management > Hunt View

EDIT DELETE

Potential Colbalt Strike

Access
PUBLIC
Priority
3

Created:
10/16/25, 04:49 AM EDT
Author
Shauna Hargrave

RESOLVE HUNT
CONVERT TO INCIDENT

JOURNAL NOTIFICATIONS EVIDENCE PLAYBOOKS

Filter Playbook
HTTP GET with encoded cookie - Possible CobaltStri...

Filter By Status
All

HTTP GET with encoded cookie - Possible Cobal...

1 Capture alert and asset details.

2 Verify the detected cookie value.

3 Initiating incident response .

HTTP GET with encoded cookie - Possible CobaltStrike C2

Detected an HTTP GET request with the headers containing a “cookie” value consistent with default CobaltStrike Command and Control communications.

Cobalt Strike is a popular penetration testing platform that allows an attacker to deploy an agent named “Beacon” on the victim machine. Beacon includes a wealth of functionality to the attacker. In addition to enabling command execution, key logging, file transfers, privilege escalation, and so on, Beacon enables outbound Command-and-Control (C2) over several common communication protocols, including HTTP. In its default configuration, the HTTP cookie value used by the Beacon follows a common pattern, which can be used to detect its communications.

When responding to this detection it is important to determine whether the detected cookie and other HTTP communication properties are consistent with the use of Cobalt Strike C2, prior to escalating to incident response.

Resolution – Convert to incident; contain

DRAGOS PLATFORM

- Asset Visibility
- Network Monitoring
- Segmentation Validation
- Vulnerability Management
- Detection and Response

Secure OT South of the Firewall

Provide Critical Expertise & Operational Capabilities

Adapt Deployment to Your Environment

Expanded Coverage, Easier to Scale

Accelerate Time to Action & Resolution

Automated Insights & Facilitate Independence

OTWatch Complete Managed Platform Service

Fully supported OT cybersecurity workflow, executed in the Dragos Platform.

Preparation & Establish Baseline
Supported by OT Watch Complete

Continuous Monitoring
Supported by OT Watch Complete

Triage & Prioritization
Supported by OT Watch Complete

Investigation & Analysis
Supported by OT Watch Complete

Incident Response
Rapid Response Retainer

Recovery & Report
Rapid Response Retainer

Continuous Improvement
Supported by OT Watch Complete

Join us at the 9th annual Dragos Industrial Security Conference

Register at: dragos.com/disc

QUESTIONS AND ANSWERS