**Indian Health Service**

# Incident Response Modernization: How Incident Response Procedures Prevent Industry Average $10M Breaches

TYLER BRUMMER

OIT/DIS CSIRT LEAD (ACTING)

AUGUST 23RD, 2023

# About Me

15 years with IHS

Currently serving as acting lead of the Division of Information Security Cybersecurity Incident Response Team

Primary incident coordinator for high profile/severity/risk incidents

# What is an “Incident”?

Any unauthorized access, use, disclosure, or destruction of digital information or data.

Examples:

- Data breaches
- Cyber attacks
- Malware infections
- Phishing scams
- Insider threats
- Any other malicious activity that compromises the security and confidentiality of digital information.

# Cost of an Incident

IBM Security - “Cost of a Data Breach Report 2023”

- Average cost of a ransomware attack is $4.5 million
- Healthcare data breach costs are up 53% since 2020
- Average cost of a data breach for Healthcare and Public Health sector is $10.9 million
- 1.5M average cost savings by organization with high levels of IR planning and testing.

# Cost of an Incident

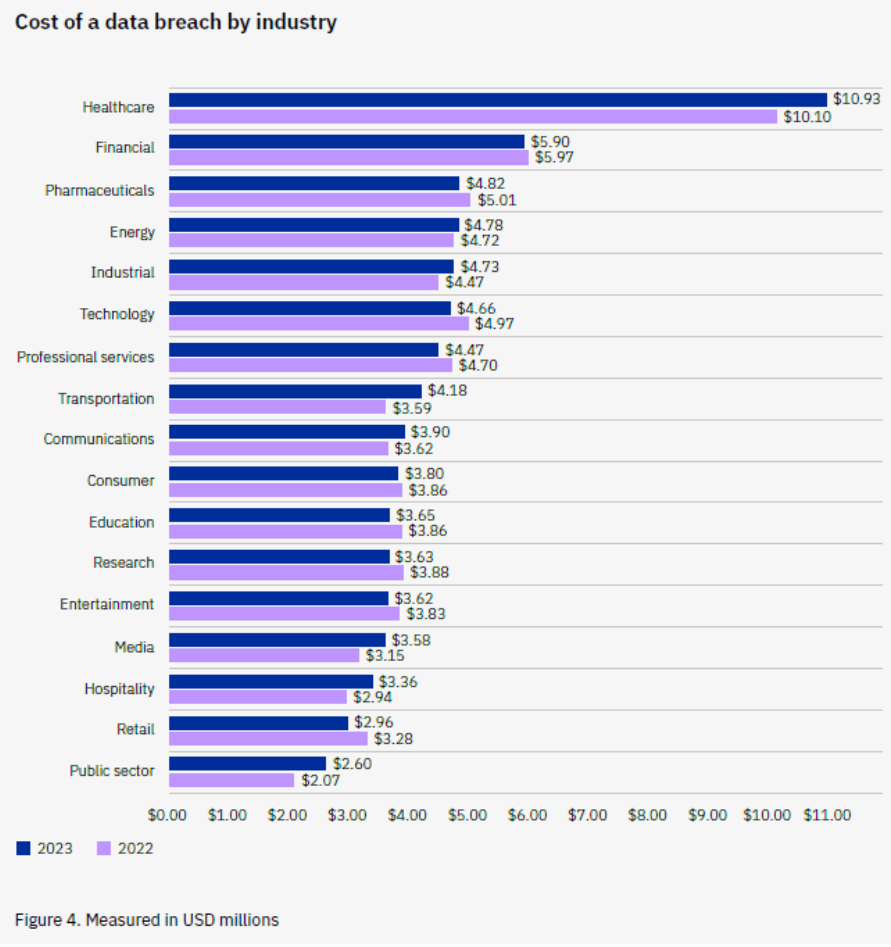



Figure 4. Measured in USD millions

# Cost of an Incident

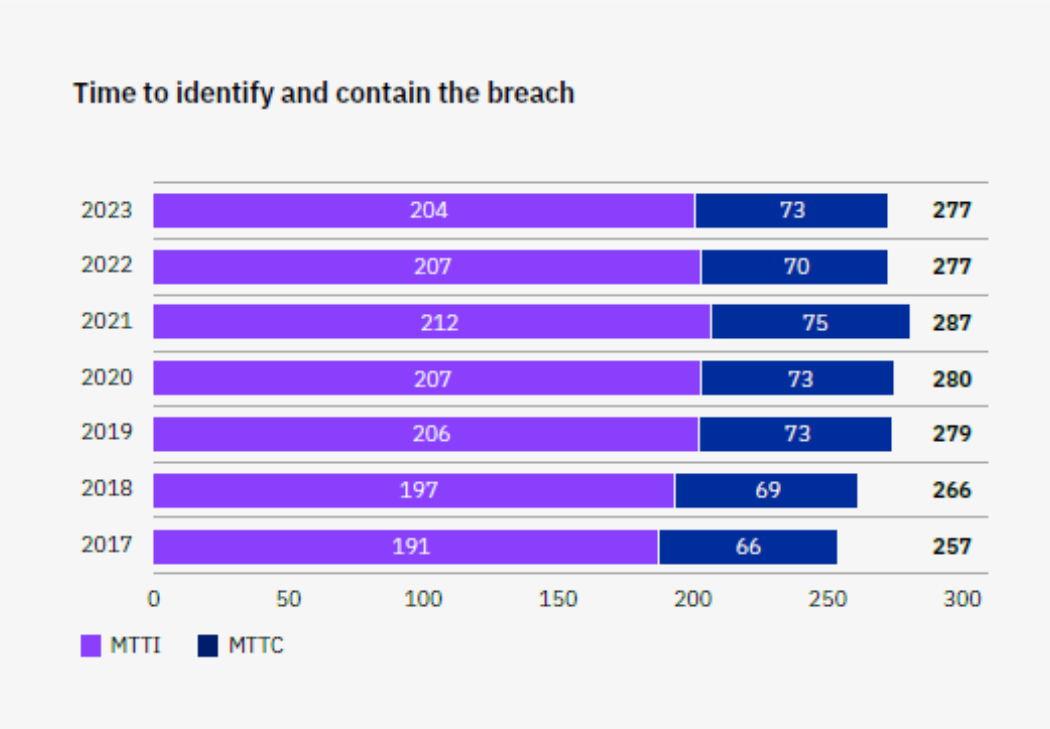
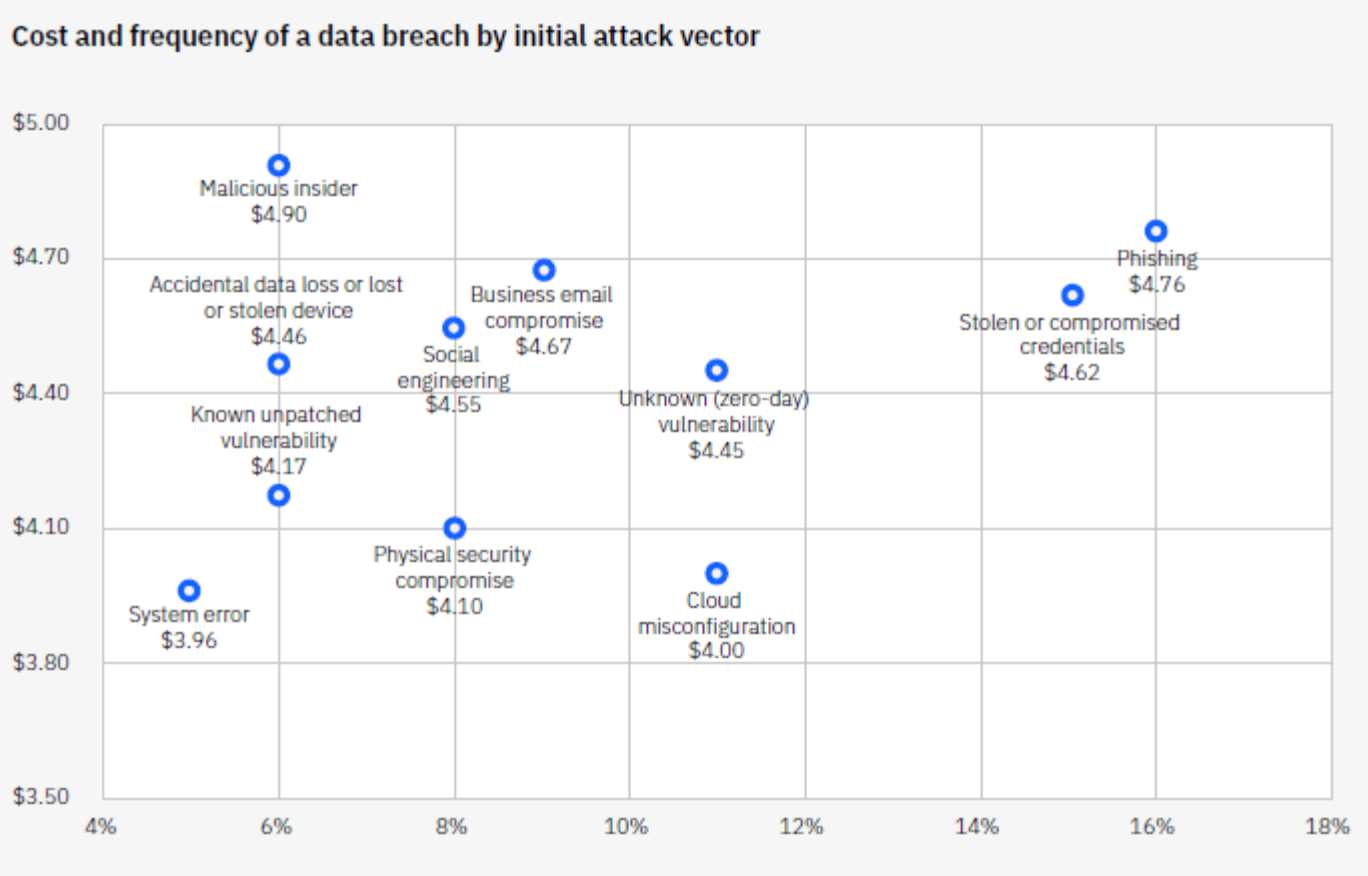



Figure 5. Measured in days

# Cost of an Incident



# Cost of an Incident

Non-monetary costs:

Reputation

- Local community, state, national… global? – United Kingdom National Health Service

Second order patient harm

- Sensitive patient data online

Distrust

# Cost of an Incident

OPM Breaches of 2015

- 21.5 million individuals SSNs from background checks affecting past, present, and prospective employees
- 4.2 million current and former employees full name, birth date, home address, and social security numbers

USPS Breach of 2018

- USPS Informed Visibility System API privilege mismanagement
- 60 million user accounts containing e-mail address, username, user ID, account number, stress address, phone number, authorized users, mailing campaign data, and more.

# Importance of Cybersecurity to the IHS Mission

Protecting the confidentiality, integrity, and availability of patient data is a foundational building block to successful patient care in modernity.

Failure can lead to negative patient outcomes related to:

- Loss of health records
- Loss of integrity via tampering with data resulting in patient harm
- Loss of access to critical services during times of emergency or critical care

# So What Can We Do?

"An Ounce of Prevention is Worth a Pound of Cure"

# Harden Devices

Limit access to ports to minimally expected traffic using host firewalls. Sometimes application firewalls can be an additional helpful layer.

Examples:

RPMS to EHR

CT to DICOM Gateways

# Segment Devices

Group “like” devices and control access to them bi-directionally. Use VLANs with Access Control Lists or Network Firewalls to limit accessibility.

Examples:

Vital Sign Monitors

CT Scanners

Nurse Workstations

# Least Privilege Access Control

Networking Layer

The minimum required connectivity between devices.

User Access Layer

The minimum required access on a per user basis required to function in their role and responsibility.

# Maintain Configuration and Data Backups

Take full system backups on a regular basis to limit total impact during a cybersecurity event.

Store backups on a segregated secured network, consider a copy of backups for storage offsite for critical systems.

Provides agility reducing total downtime during catastrophic events, regardless of if operation or cybersecurity related.

# Patch Devices

Maintain up-to-date patch levels.

Security flaws exist everywhere, once public knowledge, expect exploitation.

Common Types of Critical Vulnerabilities:

- Remote Code Execution
- Privilege Escalation
- Denial of Service

# Patch Devices

Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities (KEV)

3 weeks to patch

IHS places devices that are found extremely errant of this directive into a protective quarantine until mitigated or a Plan Of Action and Milestone

# Develop an Incident Response Plan

Know who to contact

- Report cybersecurity incidents to Incident@ihs.gov
- Notify your Site and Area Information System Security Officers
- Anyone primary points of contacts that manage operations that are affected by the incident

Document backup retrieval and recovery procedures

- How long does a restore from backup take?
- Is the backup on site (data transfer speed limitations) or held off site (physically shipped to location)?

Document interconnectivity of systems to report lateral risk and operational impact

- RPMS <-> EHR
- CT Scanners <-> DICOM Gateways

# Write Continuing Security Support Into Your Contracts

The assumption of inherent security or “good out of the box” is wrong.

Always ask about security support for medical devices.

Medical devices age into vulnerabilities, write SLA support for fixing these vulnerabilities into contracts.

Medical Devices more critical to IHS mission -> Goal: Highest Security and Support

THE FDA’S ROLE IN MEDICAL DEVICE CYBERSECURITY

https://www.fda.gov/media/123052/download

# Security Orchestration Automation Response (SOAR)

Goals

False positive reductions

Time savings

Metrics

Ticketing

Human error reduction homogenization

Workflows/Playbooks

Real world examples

# Security Orchestration Automation Response (SOAR)

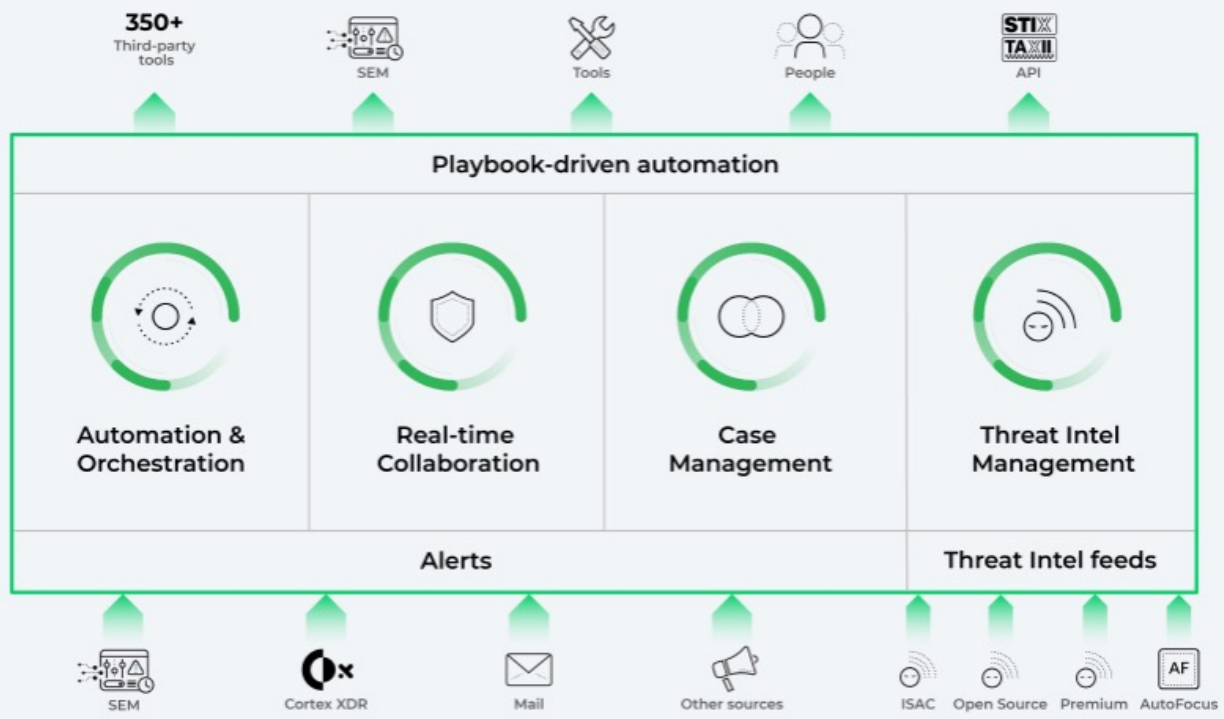
**What is it?**

*Ideally*

- Single pane of glass
- Primary system of record for incident response activities
- Supports automated processes and work flows reducing false positives, labor spent, and homogenizing incident response procedures

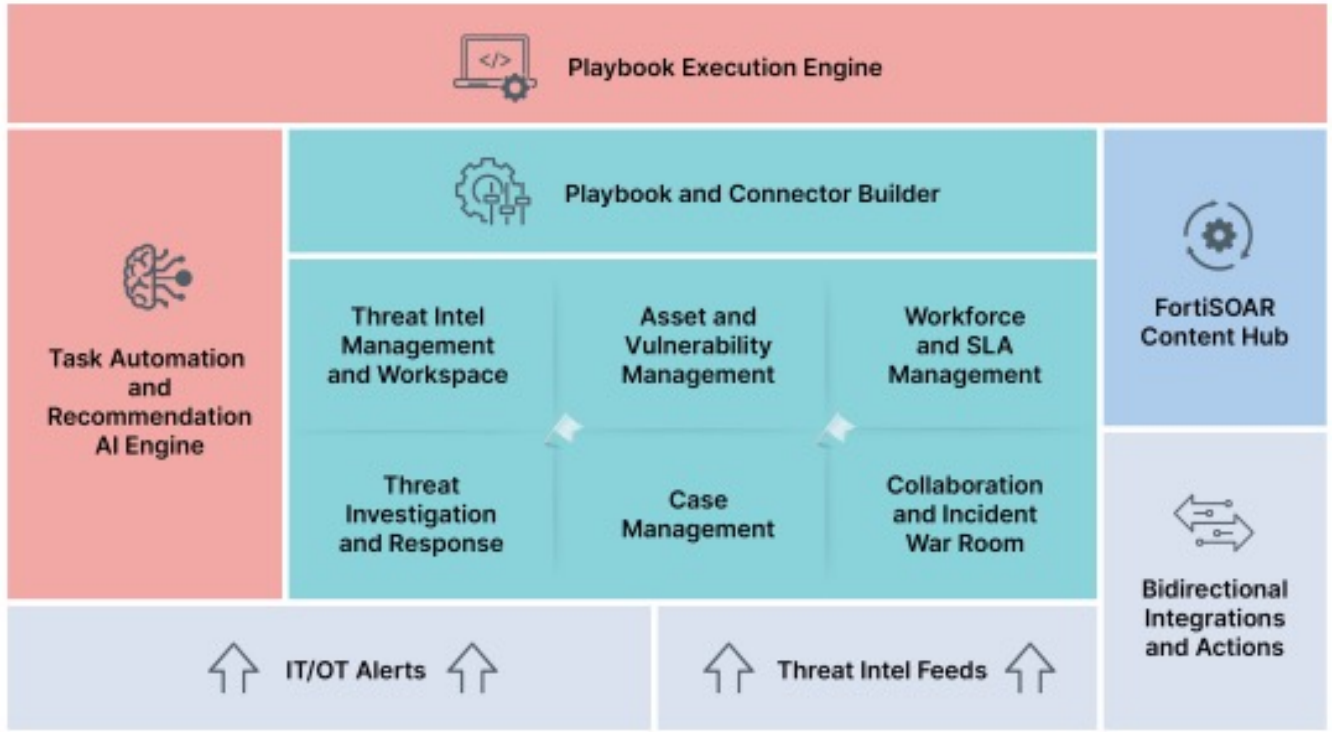
# Security Orchestration Automation Response (SOAR)

**Vendor Examples**

# Security Orchestration Automation Response (SOAR)

**Vendor Examples**



# Security Orchestration Automation Response (SOAR)

**Goals**

False-positive reduction, human-error reduction, process homogenization

- Workflows/Playbooks

Time savings/Cost savings

- Automation of expected activities for all events of a “type”
  - No reinventing the wheel

Metrics/Ticketing

- Primary system of record

# Security Orchestration Automation Response (SOAR)

**GOAL - False-positive reduction – Playbooks/Workflows**

All relevant details researched, enriched, and contextualized in the ticket before the analyst even opens the ticket.

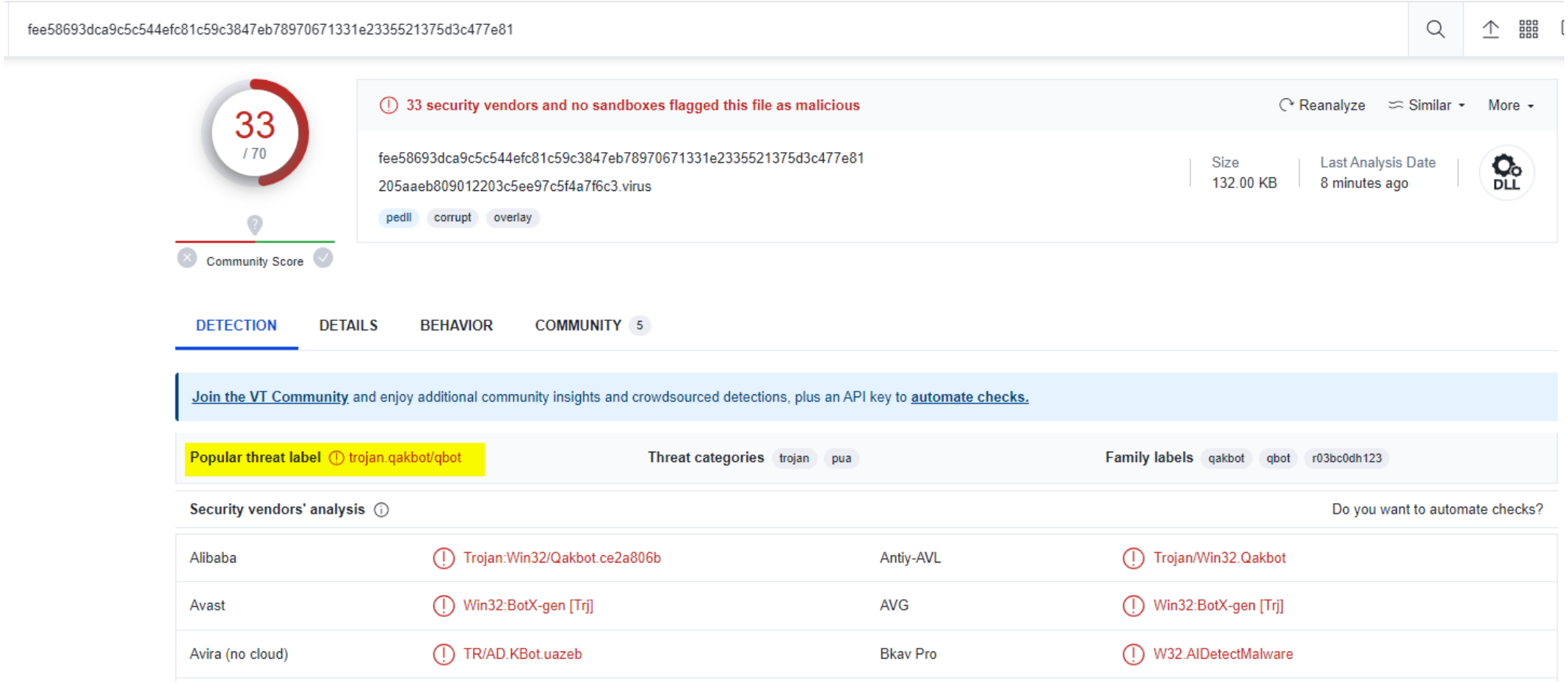
# Security Orchestration Automation Response (SOAR)

**GOAL - Human-error reduction – Playbooks/Workflows**

Check a hash if it’s malicious:

Feed3c477e8158693dca9c5c544efc81c59c3847eb78970671331e2335521375

# Security Orchestration Automation Response (SOAR)



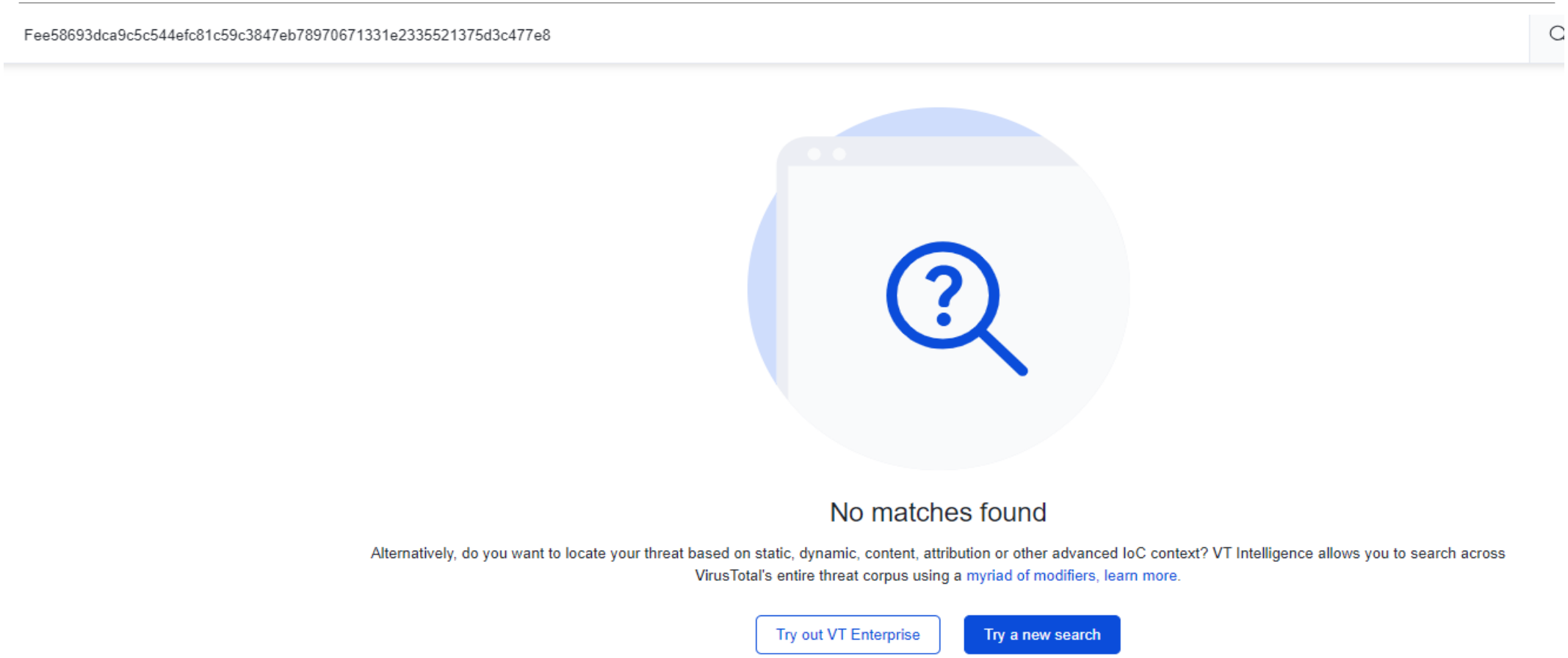
# Security Orchestration Automation Response (SOAR)

**GOAL - Human-error reduction – Playbooks/Workflows**

The analyst copy pastes an incomplete hash:

Fee58693dca9c5c544efc81c59c3847eb78970671331e2335521375d3c477e8

# Security Orchestration Automation Response (SOAR)



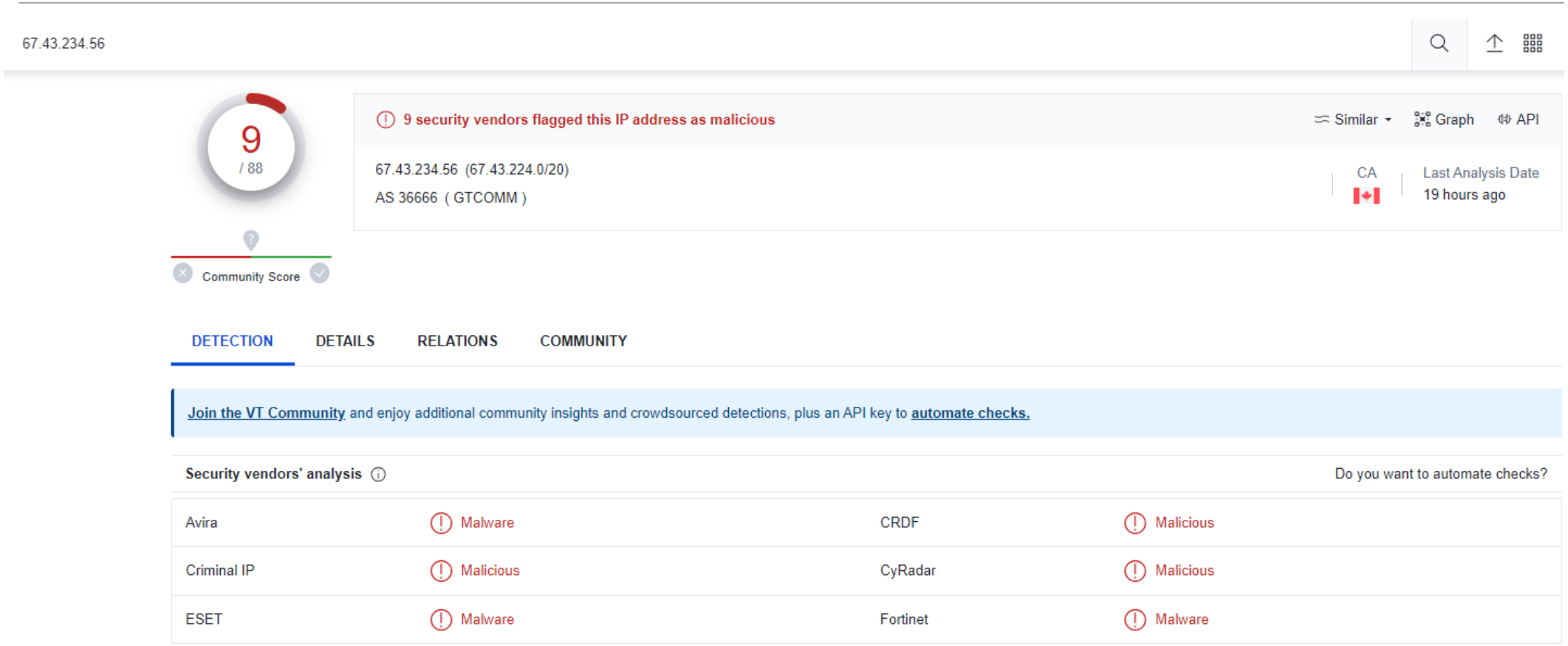
# Security Orchestration Automation Response (SOAR)

**GOAL - Human-error reduction – Playbooks/Workflows**

The analyst checks the reputation of an IP:

67.43.234[.]56

# Security Orchestration Automation Response (SOAR)



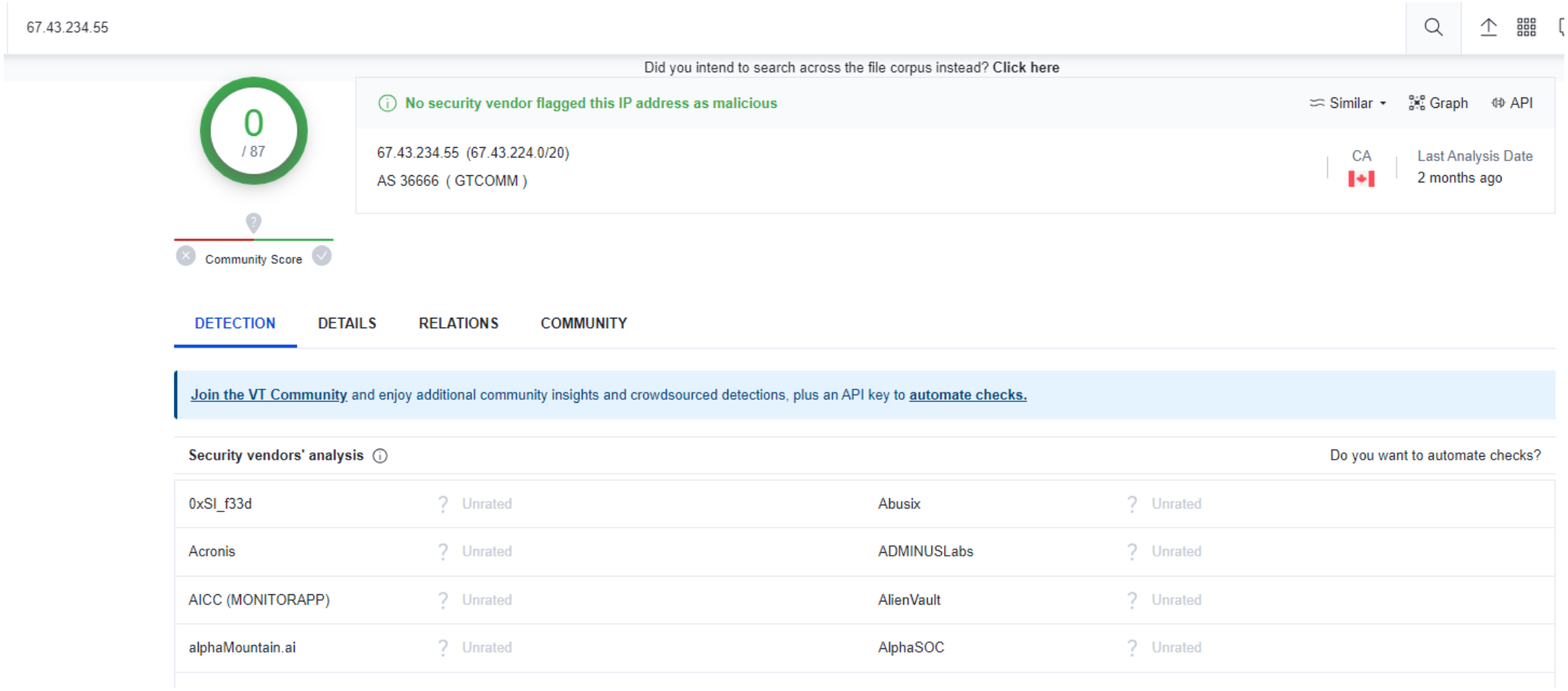
# Security Orchestration Automation Response (SOAR)

**GOAL - Human-error reduction – Playbooks/Workflows**

The analyst typos the IP:

67.43.234[.]55

# Security Orchestration Automation Response (SOAR)



# Security Orchestration Automation Response (SOAR)

**GOAL – Time savings/Cost Savings – Automation**

Mastercard presented at Splunk .Conf23 this year touting the success of their SOAR program.

YOY they reported:

- ~80% reduction in false positives
- 6,000+ hours of raw time savings

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert**

Real Event, Resulted in Ransomware at Non-Federal entity, Pre-detonation Lateral Activity Attempts Observed

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Triggering Detection**

Splunk SIEM runs an alert that detects when an IP address is observed doing an unusual large amount of connections across the network.

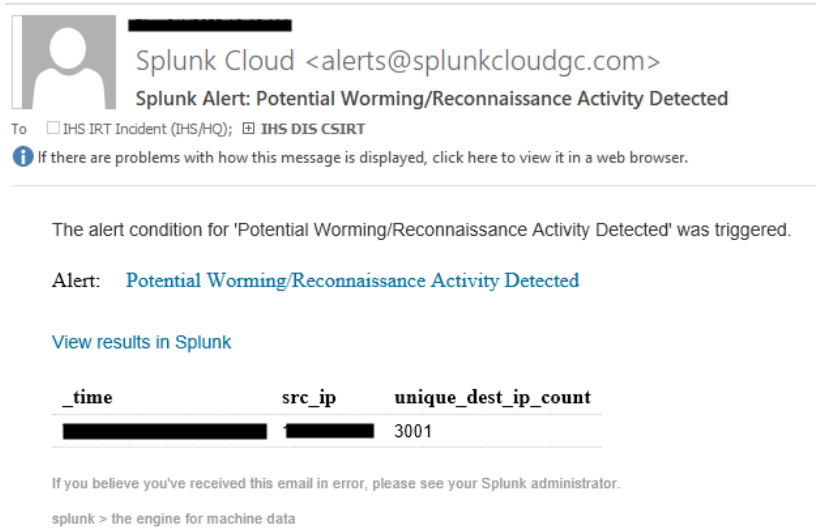

Every hour, measure connections by src_ip where over 1000 unique destinations were observed. When true, send an alert to generate workflow.

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Ticket Creation**

E-mail arrives into SOAR appliance with subject “Potential Worming/Reconnaissance Activity Detected”.

Based upon that e-mail string, a ticket is opened, a workflow is assigned, and automated actions kick off.


[redacted]
Splunk Cloud <alerts@splunkcloudgc.com>
Splunk Alert: Potential Worming/Reconnaissance Activity Detected
To IHS IRT Incident (IHS/HQ); IHS DIS CSIRT
If there are problems with how this message is displayed, click here to view it in a web browser.

The alert condition for 'Potential Worming/Reconnaissance Activity Detected' was triggered.

Alert: Potential Worming/Reconnaissance Activity Detected

View results in Splunk

| _time | src_ip | unique_dest_ip_count |
|---|---|---|
| [redacted] | [redacted] | 3001 |

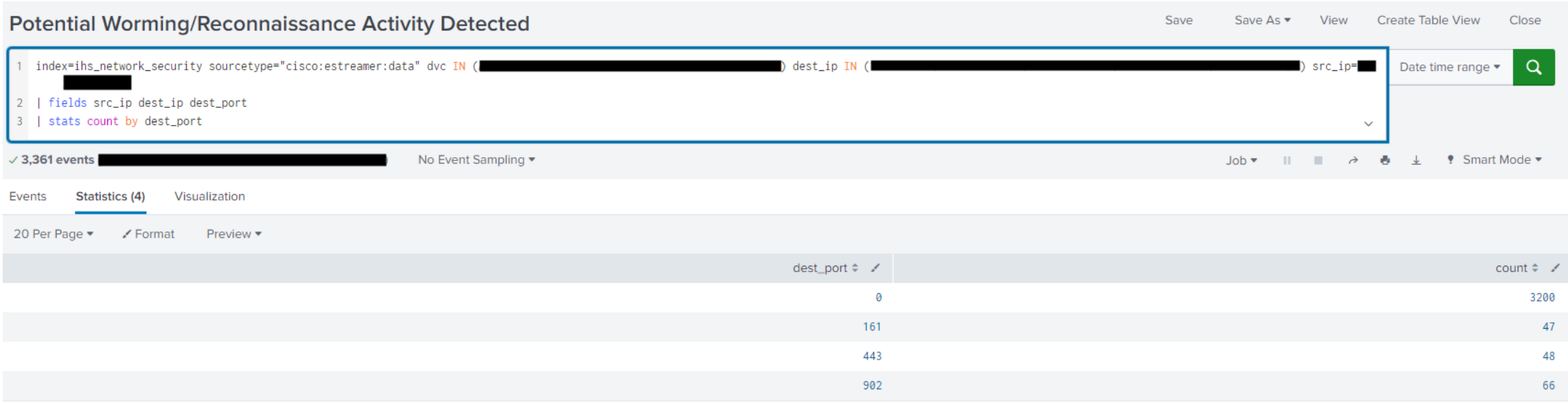
If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Automated Action #1**

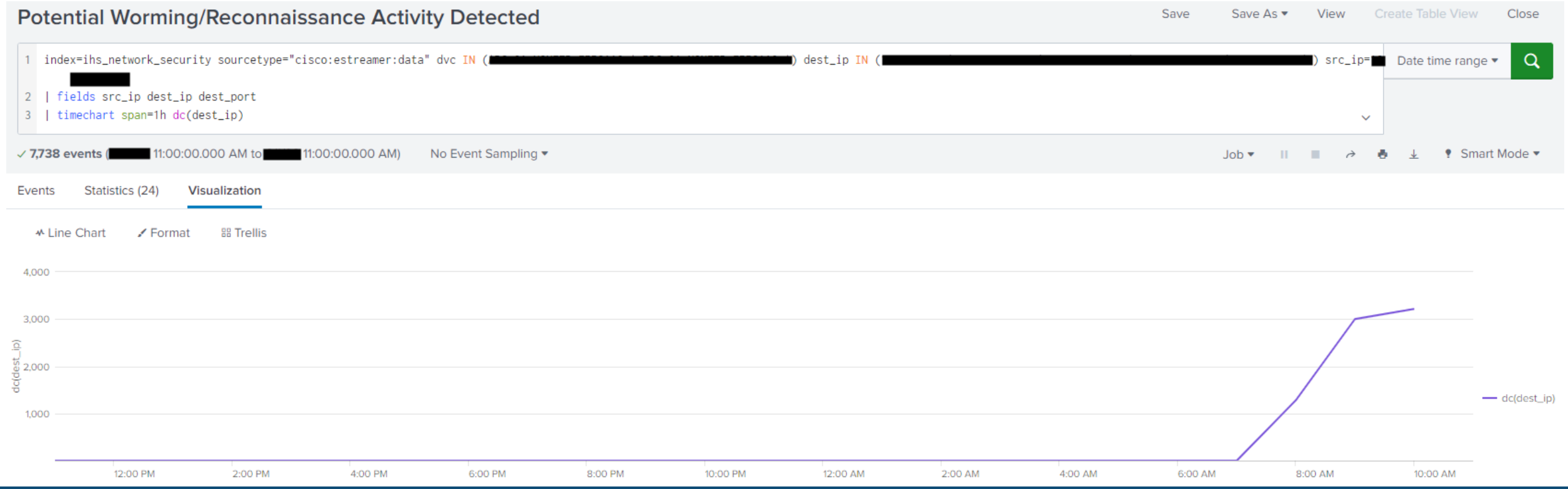
Run a query for each src_ip, determining dest_port traffic patterns:



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Automated Action #2**

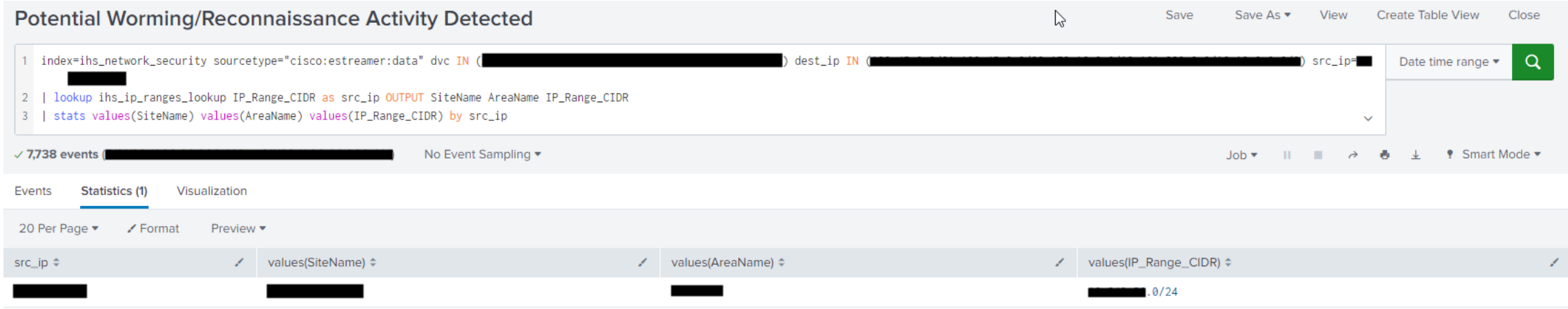
Run a last 24 hour timechart to determine if this is unique traffic or not:



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Automated Action #3**

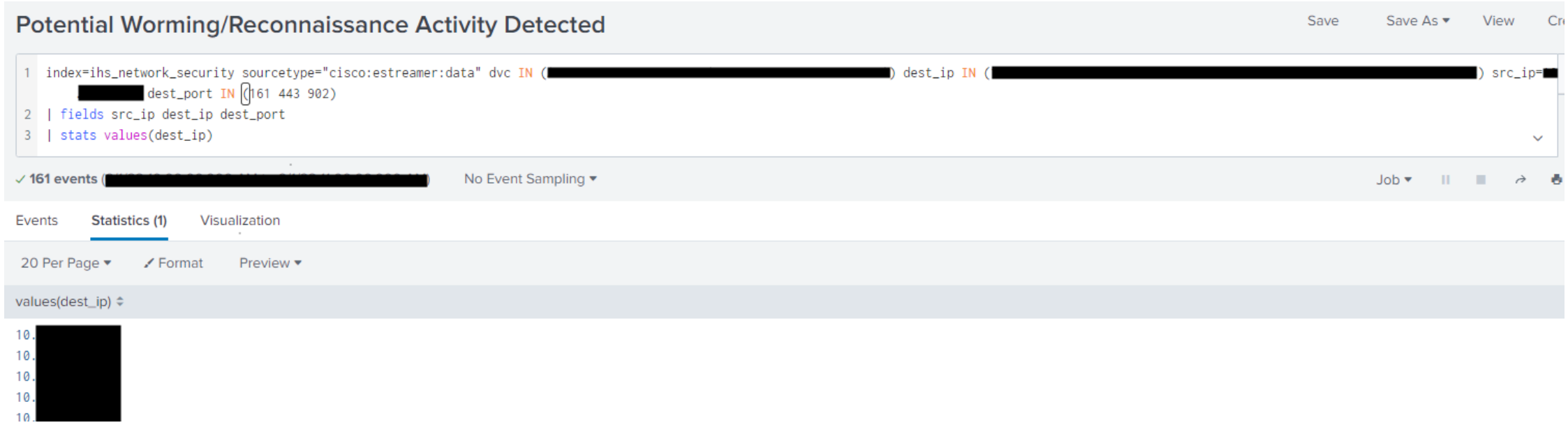
Where is this Source IP located?



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Automated Action #4**

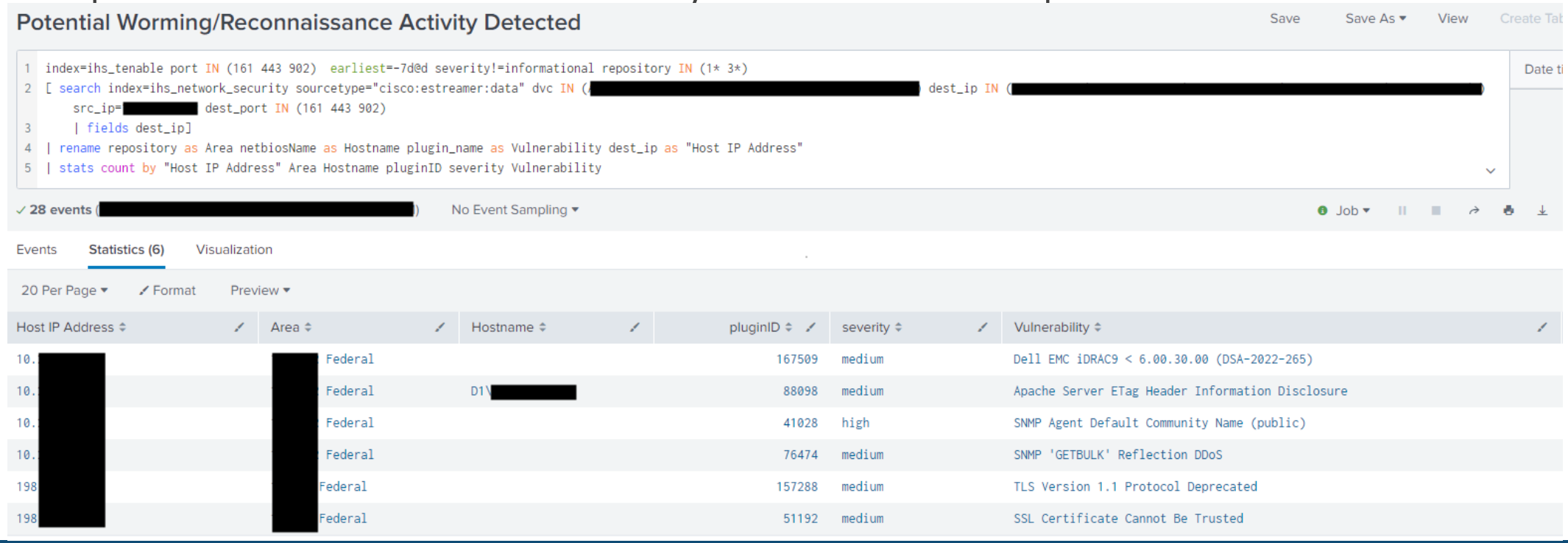
Collect all “touched” potentially impacted hosts on the identified ports (161, 443, 902) – 161 hosts:



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Automated Action #5**

Search potentially impacted host list (161 hosts) for vulnerabilities on the identified 161, 443, 902 ports to measure risk of lateral activity and determine focal points.



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Manual/Automated Action Using Template #6**

Send e-mail to NOSC and CC Area ISSO of order to disconnect the site to prevent further risk to greater IHS mission.

Good afternoon,

The IHS CSIRT is requesting an immediate block on all traffic from [redacted] as we are seeing suspicious and potentially malicious signs of scanning behavior from this IP address. [redacted] there may be an infected device on the other side of this tribal network that is scanning for SNMP and VMWare related ports across the entire [redacted] area.

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Manual/Automated Action Using Template #7**

Send e-mail to Area ISSO requesting assistance contacting local entity.

Good afternoon [redacted]

The IHS CSIRT has been receiving a series of worming/reconnaissance alerts on [redacted] that are originating from a host in the [redacted] network. The majority of this traffic is ICMP traffic that was sent out to over 2000 unique IP Addresses across the [redacted] Area. Here are the details from the alert:

| _time | src_ip | dest_port | unique_dest_ip_count |
|---|---|---|---|
| [redacted] | | | |

Please contact the site's IT team to identify what this host is, whether this traffic is known by the system owner, and whether this activity warrants further investigation as evidence of a potentially malicious process. Thank you!

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Worming/Reconnaissance Alert – Additional Hypotheticals**

Quarantine Host?

Run web access logs over last 24 hours? 7 days? To determine potential malicious activity?

Dump process executions, installed software, startup services over last hour, last 4 hours, last 24 hours?

Immediately collect WinEventLog? Send response script to Crowdstrike to automatically dump and collect all WinEventLog

Install Forensic tools and immediately begin grabbing forensic image?

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Denial of Service Alert – Triggering Detection**

### RDC DDoS Connection Rate Monitoring

```
1  index=ihs_palo_alto sourcetype=pan:traffic host=[redacted] OR host=[redacted] dest_zone!=outside
2  | bucket _time span=1m
3  | stats count by _time
4  | stats avg(count) as avg
5  | where avg>100000
```

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Denial of Service Alert – Ticket Creation**

E-mail arrives into SOAR appliance with subject “RDC DDoS Connection Rate Monitoring”.

Based upon that e-mail string, a ticket is opened, a workflow is assigned, and automated actions kick off.

**Subject:** Splunk Alert: RDC DDoS Connection Rate Monitoring
**Importance:** High

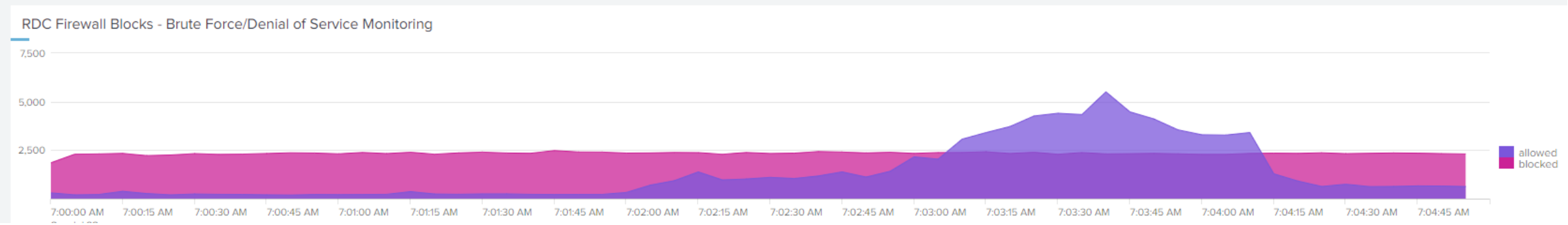
The alert condition for 'RDC DDoS Connection Rate Monitoring' was triggered. Connection rate monitoring has determined a potential DDoS event has occurred or is occurring. Please use the below Rockville DDoS Monitoring dashboard to investigate. If there is a positive DDoS event, immediately engage the NOSC for cooperative investigation and event mitigation. LINK

Trigger: Saved Search [RDC DDoS Connection Rate Monitoring]: number of events (1)

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Denial of Service Alert – Automated Action #1**

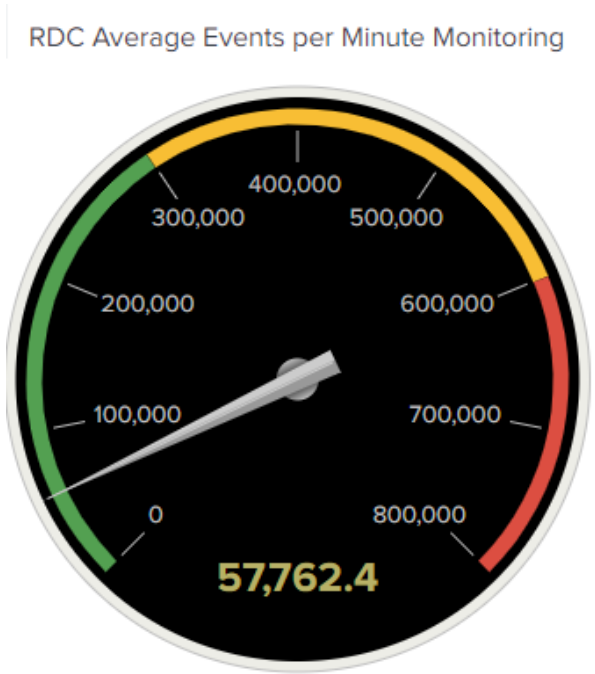
Timechart of events by action.



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Denial of Service Alert – Automated Action #2**

Average events per minute visual dial:



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Denial of Service Alert – Automated Action #3**

Top Source IPs:

DDoS Source IP Monitoring

| src_ip | Country | count | percent |
|---|---|---|---|
| 100.27.42.165 | United States | 120127 | 54.614353 |
| 100.27.42.242 | United States | 7488 | 3.404333 |
| 107.170.237.74 | United States | 1412 | 0.641949 |
| 192.241.208.106 | United States | 1312 | 0.596486 |
| 192.241.230.5 | United States | 1212 | 0.551022 |
| 170.76.165.148 | United States | 790 | 0.359164 |
| 194.169.217.81 | Germany | 661 | 0.300516 |
| 89.248.168.235 | Netherlands | 523 | 0.237776 |
| 77.90.185.80 | Germany | 479 | 0.217772 |
| 77.90.185.100 | Germany | 432 | 0.196404 |

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Denial of Service Alert – Automated Action #4**

Top Destination IPs:

DDoS Destination IP Monitoring

| dest_ip | count | percent |
|---|---|---|
| 161.223 [redacted] | 128054 | 58.216684 |
| 198.45. [redacted] | 60047 | 27.298930 |
| 198.45. [redacted] | 7499 | 3.409241 |
| 198.45. [redacted] | 1618 | 0.735585 |
| 161.223 [redacted] | 761 | 0.345970 |
| 161.223 [redacted] | 255 | 0.115930 |
| 198.45. [redacted] | 219 | 0.099563 |
| 161.223 [redacted] | 210 | 0.095471 |
| 161.223 [redacted] | 208 | 0.094562 |
| 198.45. [redacted] | 205 | 0.093198 |

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Denial of Service Alert – Automated Action #5**

Top Source Ports:

DDoS Source Port Monitoring

| transport | src_port | count | percent |
|---|---|---|---|
| tcp | 59223 | 59953 | 27.256195 |
| tcp | 59225 | 59941 | 27.250740 |
| icmp | 0 | 1397 | 0.635113 |
| tcp | 49371 | 663 | 0.301417 |
| tcp | 41830 | 524 | 0.238224 |
| tcp | 53341 | 479 | 0.217766 |
| tcp | 53418 | 433 | 0.196853 |
| tcp | 53377 | 334 | 0.151845 |
| tcp | 52865 | 282 | 0.128205 |
| tcp | 52791 | 259 | 0.117748 |

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Denial of Service Alert – Automated Action #6**

Top Destination Ports:

DDoS Destination Port Monitoring

| transport | dest_port | count | percent |
|---|---|---|---|
| udp | 53 | 58549 | 26.617900 |
| tcp | 443 | 13284 | 6.039252 |
| tcp | 49443 | 3685 | 1.675297 |
| tcp | 5672 | 1629 | 0.740586 |
| tcp | 8040 | 1609 | 0.731493 |
| tcp | 4200 | 1549 | 0.704216 |
| tcp | 53 | 1414 | 0.642841 |
| icmp | 0 | 1397 | 0.635113 |
| tcp | 80 | 1348 | 0.612836 |
| tcp | 7680 | 732 | 0.332786 |

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Triggering Detection**

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Ticket Creation**

| Remote_Host_IP | CIDS_Signature_String | Traffic_Direction | count |
|---|---|---|---|
| 10.[redacted] | OS Attack: SMB Validate Provider Callback CVE-2009-3103 | Inbound | 141 |

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Automated Action #1 – Grab RAW logs**

SEP Network Host Exploitation Monitoring - Malicious Traffic Indicating Potential ...

```
1  index=sep sourcetype=symantec:ep:security:file Remote_Host_IP=10.[redacted] CIDS_Signature_String="OS Attack: SMB Validate Provider Callback CVE-2009-3103"
```

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Automated Action #1 – Graw RAW logs**

| i | Event |
|---|---|
| > | 2023-08-12 21:51:48,Critical,[redacted],Event Description: [SID: 30011] OS Attack: SMB Validate Provider Callback CVE-2009-3103 attack blocked. Traffic has been blocked for this application: SYSTEM,Event Type: Intrusion Prevention System Intrusion Detected,Local Host IP: 10.[redacted],Local Host MAC: 000000000000,Remote Host Name: ,Remote Host IP: 10.[redacted],Remote Host MAC: 000000000000,Inbound,TCP,Blocked,Begin: 2023-08-12 21:51:36,End Time: 2023-08-12 21:51:36,Occurrences: 2,Application: SYSTEM,Location: Default,User Name: none,Domain Name: ,Local Port: 445,Remote Port: 58146,CIDS Signature ID: 30011,CIDS Signature string: OS Attack: SMB Validate Provider Callback CVE-2009-3103,CIDS Signature SubID: 65536,Intrusion URL: ,Intrusion Payload URL: ,SHA-256: ,MD-5: ,Intensive Protection Level: N/A,URL Risk: N/A,URL Category: N/A |

Impacted Host

Impacted Host IP

Attacker IP

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Automated Action #2 – Correlate with Statistical Analysis**

SEP Network Host Exploitation Monitoring - Malicious Traffic Indicating Potential D...

Save | Save As | View | Create Table View | Close

```
1 index=sep sourcetype=symantec:ep:security:file Remote_Host_IP=10.[redacted] CIDS_Signature_String="OS Attack: SMB Validate Provider Callback CVE-2009-3103"
2 | stats count by src_ip dest_ip dest_port Host_Name action
3 | rename src_ip as "Attacking IP" dest_ip as "Victim IP" dest_port as "Attacked Port" Host_Name as "Victim Machine" action as Action
```

Date time range

✓ **247 events** (8/10/23 3:00:00.000 AM to 8/13/23 4:00:00.000 AM) No Event Sampling

Job | Smart Mode

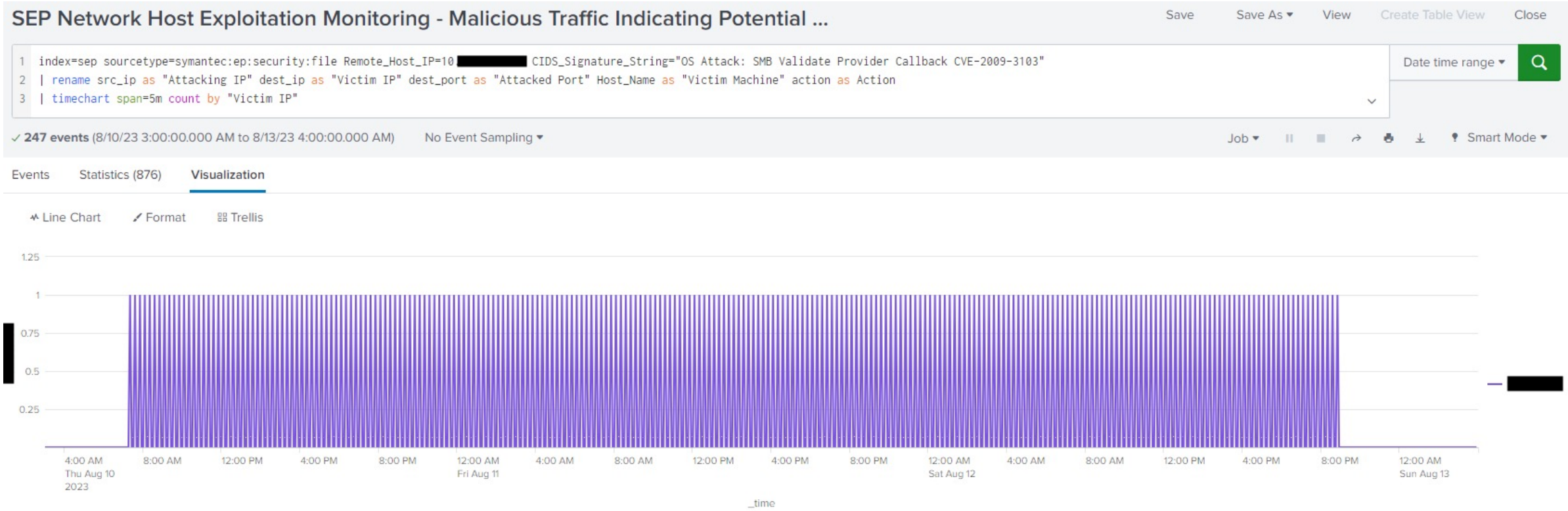
Events | **Statistics (1)** | Visualization

20 Per Page | Format | Preview

| Attacking IP | Victim IP | Attacked Port | Victim Machine | Action | count |
|---|---|---|---|---|---|
| 10.[redacted] | 10.[redacted] | 445 | [redacted] | blocked | 247 |

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Automated Action #3 – Timechart for Patterns**



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Automated Action #4 – Is the Victim Host Vulnerable to the Attack:**

SEP Network Host Exploitation Monitoring - Malicious Traffic Indicating Potential D...

```
1 index=ihs_tenable dest_ip=[redacted] severity!=informational
2 | stats values(plugin_name) by dest_ip severity
```

✓ **25 events** (8/10/23 3:00:00.000 AM to 8/13/23 4:00:00.000 AM) No Event Sampling

Events (25) **Statistics (3)** Visualization

20 Per Page ▾ Format Preview ▾

| dest_ip | severity | values(plugin_name) |
|---|---|---|
| 10.[redacted] | critical | KB5025230: Windows 2022 / Azure Stack HCI 22H2 Security Update (April 2023)<br>KB5026370: Windows 2022 / Azure Stack HCI 22H2 Security Update (May 2023)<br>KB5027225: Windows 2022 / Azure Stack HCI 22H2 Security Update (June 2023)<br>KB5028171: Windows 2022 / Azure Stack HCI 22H2 Security Update (July 2023)<br>KB5029250: Windows 2022 / Azure Stack HCI 22H2 Security Update (August 2023)<br>Microsoft Silverlight Unsupported Version Detection (Windows) |
| 10.[redacted] | high | Microsoft Edge (Chromium) < 114.0.1823.106 / 115.0.1901.200 Multiple Vulnerabilities<br>Microsoft Edge (Chromium) < 114.0.1823.67 Multiple Vulnerabilities<br>Microsoft Edge (Chromium) < 114.0.1823.82 Multiple Vulnerabilities<br>Microsoft Edge (Chromium) < 114.0.1901.183 / 115.0.1901.183 Multiple Vulnerabilities<br>Microsoft Windows Update Reboot Required<br>Security Updates for Microsoft .NET Framework (August 2023)<br>Security Updates for Microsoft .NET Framework (June 2023) |
| 10.[redacted] | medium | Curl Use-After-Free < 7.87 (CVE-2022-43552) |

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Automated Action #4 – Is the Victim Host Vulnerable to the Attack:**

# Security Orchestration Automation Response (SOAR)

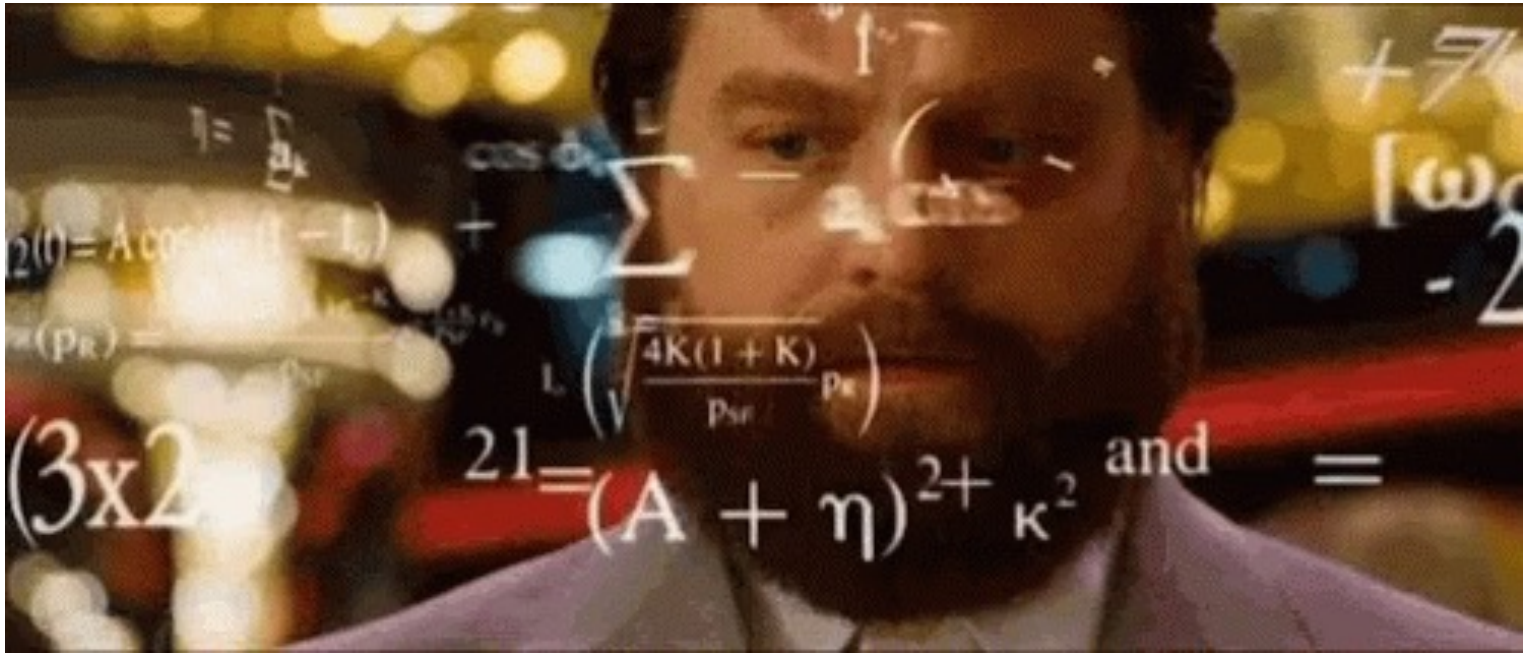
**Real World Examples: Network Host Exploitation Monitoring – Manual Action #1 - Review**

Analyst reviews statistical analysis, timechart, host risk to determine severity.

- What do we know?
  - Host to host traffic
  - Low-ish and consistent volume (once per 15 minutes)
  - Old/obscure vulnerability
  - Modern operating system

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Results**



# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Results**

**False Positive!**

# Security Orchestration Automation Response (SOAR)

**Real World Examples: Network Host Exploitation Monitoring – Hypotheticals**

**Severity Low – Send FYSA close ticket.**

**Severity Medium – Request action by ISSO, Local IT, System owner to investigate – ticket remains open until investigation satisfied.**

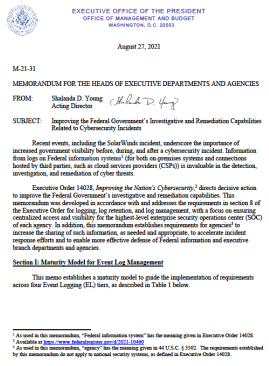
**Severity High – Immediately quarantine host, escalate to tier 2+, Scrape WinEventLogs, Etc.**

# OMB M-21-31 – Improving the Federal Government's Investigative and Remediation Capabilities

Executive Order 14028 Improving the Nation's Cybersecurity

Appendix C - Over 30 pages of technical details on what data to log and how long it should be retained for cybersecurity incident response investigations.

TL;DR – Log everything and retain it for a long time.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 27, 2021

M-21-31

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

Recent events, including the SolarWinds incident, underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on Federal information systems[1] (for both on-premises systems and connections hosted by third parties, such as cloud services providers (CSPs)) is invaluable in the detection, investigation, and remediation of cyber threats.

Executive Order 14028, *Improving the Nation's Cybersecurity*,[2] directs decisive action to improve the Federal Government's investigative and remediation capabilities. This memorandum was developed in accordance with and addresses the requirements in section 8 of the Executive Order for logging, log retention, and log management, with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center (SOC) of each agency. In addition, this memorandum establishes requirements for agencies[3] to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of Federal information and executive branch departments and agencies.

Section I: Maturity Model for Event Log Management

This memo establishes a maturity model to guide the implementation of requirements across four Event Logging (EL) tiers, as described in Table 1 below.

[1] As used in this memorandum, "Federal information system" has the meaning given in Executive Order 14028.
[2] Available at https://www.federalregister.gov/d/2021-10460
[3] As used in this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502. The requirements established by this memorandum do not apply to national security systems, as defined in Executive Order 14028.

# Q&A and Contacts – Thank You!

Tyler.Brummer@ihs.gov

Division of Information Security

- Policy Questions:
  - Cybersecurity@ihs.gov
- Vulnerability or Incident Response Questions
  - ihsdiscsirt@ihs.gov
- Architecture Questions:
  - ihsdisarchitectureandengineering@ihs.gov
- Reporting a Cybersecurity Incident:
  - Incident@ihs.gov
- Reporting a Privacy Incident:
  - ihsprivacyincidents@ihs.gov


INDIAN HEALTH SERVICE
PHS · 1955 ·