



A Technical Deep Dive into Elastic Security 7.9

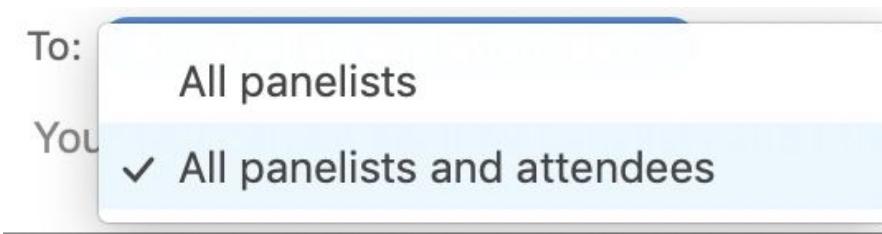
Mike Paquette | Director of Product, Elastic SIEM

Braden Preston | Director of Product, Elastic Endpoint Security

October 7, 2020

Housekeeping & Logistics

- Attendees are automatically muted when joining Zoom webinar
- Q+A will be at the end of the webinar
- Ask questions for us in the Zoom chat during the webinar
 - Adjust Zoom chat settings to: “All panelists and attendees”



- More questions? Try <https://discuss.elastic.co/c/security>
- Recording will be available after the webinar and emailed to all registrants



Mike Paquette

Director of Product, Elastic SIEM



Braden Preston

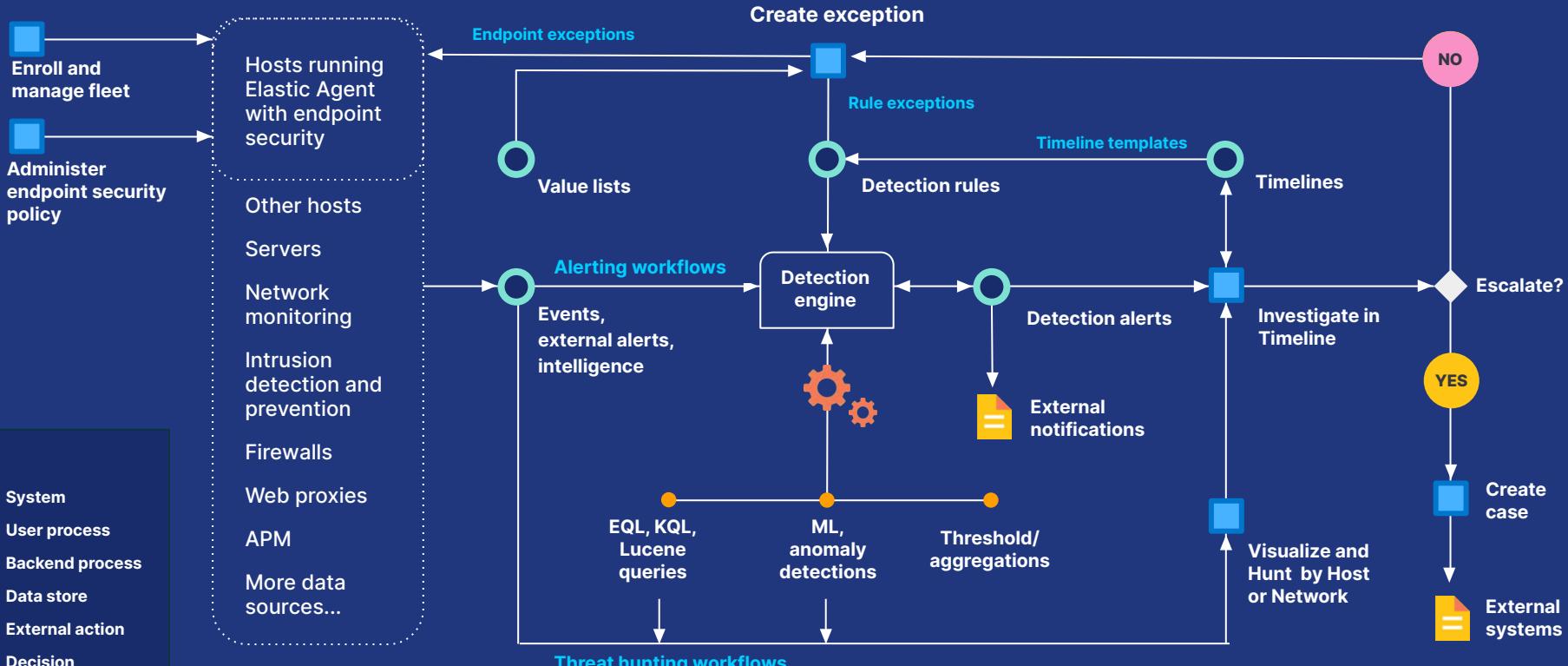
Director of Product,
Elastic Endpoint Security

Webinar Abstract

- Protecting data and networks against cyber attacks is challenging. Many security teams have been using Elastic Security for SIEM use cases to collect and analyze endpoint data, add enterprise context, and hunt for and detect threat activity.
- With the 7.9 release, Elastic Security now provides free, integrated endpoint security through the introduction of signatureless malware prevention and kernel-level data collection on the new Elastic Agent.
- **Highlights:**
 - a. New free and open anti-malware capability for Windows and macOS
 - b. Interactive process tree visualization
 - c. Enhanced capabilities and workflows for automated threat detection
 - d. Expanded set of prebuilt detection rules



Elastic Security 7.9 - Operational Workflows





What's new in Elastic Security 7.9

Highlights of Elastic Security 7.9



Elastic agent for data collection and endpoint protection



Deep visibility and malware prevention across your environment



Prebuilt protections and expanded detection methods



Streamlined analyst workflows

Elastic Agent

Making it **EASY** to set up



Simpler setup

A single, unified Elastic Agent



Faster time to insight

1-click integrations for popular services



Easier management

Centrally manage all your agents at scale

Simple instrumentation

Elastic Agent

One agent to rule them all!

BEFORE

ON EVERY HOST:

- **Filebeat** for logs
- **Metricbeat** for metrics
- **APM agents** for app traces
- **Heartbeat** for uptime
- **Endpoint** for security
- **Winlogbeat** - windows data



NOW

ON EVERY HOST:

- **Elastic Agent** for logs, metrics, and security. *Uptime, windows data and traces coming soon.*



One thing to **install, configure and scale.**

Web UI to edit agent policies

Collecting data is now as easy as 

BEFORE

```
1 ##### Filebeat Configuration Example #####
2
3 # This file is an example configuration file highlighting only the most common
4 # options. The filebeat.reference.yml file from the same directory contains all the
5 # supported options with more comments. You can use it as a reference.
6 #
7 # You can find the full configuration reference here:
8 # https://www.elastic.co/guide/en/beats/filebeat/index.html
9
10 # For more available modules and options, please see the filebeat.reference.yml sample
11 # configuration file.
12
13 # ===== Filebeat inputs =====
14
15 filebeat.inputs:
16
17 # Each - is an input. Most options can be set at the input level, so
18 # you can use different inputs for various configurations.
19 # Below are the input specific configurations.
20
21 - type: log
22
23 # Change to true to enable this input configuration.
24 enabled: false
25
26 # Paths that should be crawled and fetched. Glob based paths.
27 paths:
28   - /var/log/*.log
29   #- c:\programdata\elasticsearch\logs\*
30
31 # Exclude lines. A list of regular expressions to match. It drops the lines that are
32 # matching any regular expression from the list.
33 #exclude_lines: ['^DBG']
34
35 # Include lines. A list of regular expressions to match. It exports the lines that are
36 # matching any regular expression from the list.
37 #include_lines: ['ERR', 'WARN']
38
39 # Exclude files. A list of regular expressions to match. Filebeat drops the files that
40 # are matching any regular expression from the list. By default, no files are dropped.
41 #exclude_files: ['.gz$']
42
```



NOW

- Collect logs from Nginx instances
- Collect metrics from Nginx instances

Now using API keys

Minimal permissions, better control

BEFORE

- Beats have username/password
- Password saved in YAML config
- Default user has superuser permissions
- One or few passwords for all Beats



NOW

- API keys for Fleet and Elasticsearch
- Fleet saves keys automatically
- Minimal permissions on each Agent
- One key per Agent makes it easy to revoke

Fast time to insight and action

Integrate popular services in 1-click

- 1 click adds out of the box parsing and dashboards, deploys to agents
- ~40 integrations today with many more coming soon

Search for integrations

EXPERIMENTAL  Apache Apache Integration	EXPERIMENTAL  AWS AWS Integration	EXPERIMENTAL  Barracuda Web Application Firewall Barracuda Web Application Firewall Integration
EXPERIMENTAL  Blue Coat Director Blue Coat Director Integration	EXPERIMENTAL  Cisco Cisco Integration	EXPERIMENTAL  Citrix XenApp Citrix XenApp Integration
EXPERIMENTAL  CylanceProtect CylanceProtect Integration	BETA  Elastic Endpoint Security Protect your hosts with threat prevention, detection, and deep security data visibility.	EXPERIMENTAL  Big-IP Access Policy Manager Big-IP Access Policy Manager Integration
EXPERIMENTAL  HAProxy HAProxy Integration	EXPERIMENTAL  IIS IIS Integration	EXPERIMENTAL  Imperva SecureSphere Imperva SecureSphere Integration

Protect hosts from security threats

- While you observe, why not protect?
- Automated response to security threats on hosts, like malware
- Deploy to Elastic Agent with 1 click

[Back to endpoint hosts](#)

Endpoints	Online	Offline	Error
1	1	0	0

[Cancel](#) [Save](#)

test

Protections

Type	Operating System	
Malware	Windows, Mac	<input checked="" type="checkbox"/> Malware Protections Enabled

Protection Level

Detect Prevent

[View related detection rules.](#) Prebuilt rules are tagged "Elastic" on the Detection Rules page.

Settings

Type	Operating System	
Event Collection	Windows	7 / 7 event collections enabled

Events

DLL and Driver Load
 DNS
 File
 Network
 Process
 Registry
 Security

Event Collections

Type	Operating System	
Event Collection	Mac	3 / 3 event collections enabled

Parse fields in custom logs

- Out of the box pipelines included in integrations
- New UI for building pipelines makes it easier
- Powerful processors like grok, split and more

Create pipeline

[Create pipeline docs](#)

Name

A unique identifier for this pipeline.

Add version number

Name

logs-system.syslog-0.5.3-copy

Description

A description of what this pipeline does.

Description (optional)

Pipeline for parsing Syslog messages.

Processors [Import](#)

The processors used to pre-process documents before indexing. [Learn more.](#)

• **Grok** No description

...

• **Remove** No description

...

• **Rename** No description

...

• **Date** No description

...

Failure handlers

• **Append** No description

...

• **Date** No description

...

Failure handlers

• **Append** No description

...

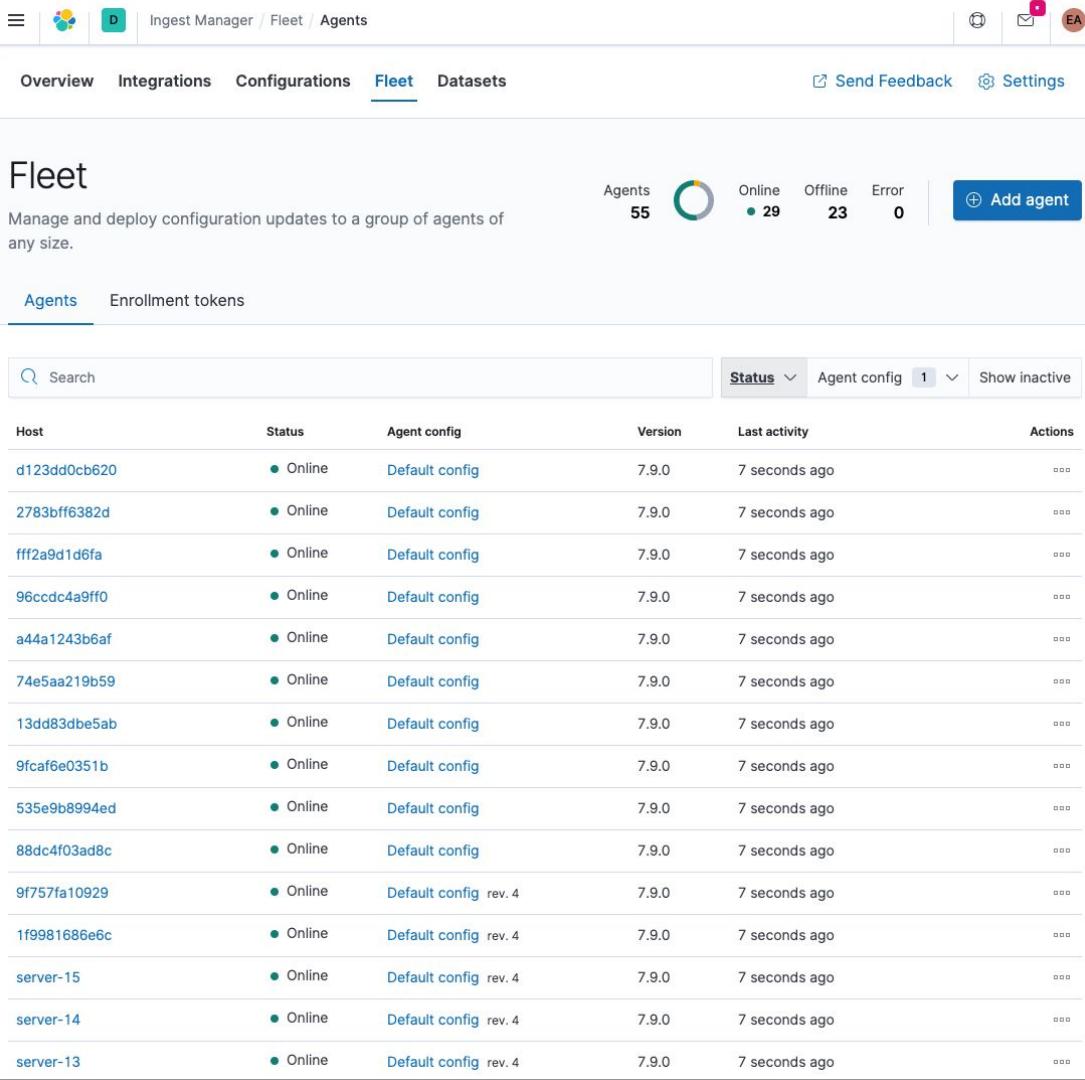
• **Remove** No description

...

Easy management

Centrally manage agents with Fleet

- Quick visibility to the status of your fleet
- Update agent policies and binaries remotely
- Manage agents at scale
- API for full automation



The screenshot shows the Ingest Manager interface with the 'Fleet' tab selected. At the top, there are navigation links: Overview, Integrations, Configurations, Fleet (which is underlined in blue), and Datasets. To the right of these are 'Send Feedback' and 'Settings' buttons, along with a user profile icon.

The main title is 'Fleet', with a subtitle: 'Manage and deploy configuration updates to a group of agents of any size.' Below this, a summary box shows 'Agents 55' with a circular progress bar, 'Online 29' (indicated by a green dot), 'Offline 23' (indicated by a grey dot), and 'Error 0'. A blue button labeled '+ Add agent' is on the right.

Below the summary, there are two tabs: 'Agents' (which is selected and underlined in blue) and 'Enrollment tokens'. A search bar is followed by a table with the following columns: Host, Status, Agent config, Version, Last activity, and Actions.

Host	Status	Agent config	Version	Last activity	Actions
d123dd0cb620	● Online	Default config	7.9.0	7 seconds ago	...
2783bff6382d	● Online	Default config	7.9.0	7 seconds ago	...
fff2a9d1d6fa	● Online	Default config	7.9.0	7 seconds ago	...
96ccdc4a9ff0	● Online	Default config	7.9.0	7 seconds ago	...
a44a1243b6af	● Online	Default config	7.9.0	7 seconds ago	...
74e5aa219b59	● Online	Default config	7.9.0	7 seconds ago	...
13dd83dbe5ab	● Online	Default config	7.9.0	7 seconds ago	...
9fcacf6e0351b	● Online	Default config	7.9.0	7 seconds ago	...
535e9b8994ed	● Online	Default config	7.9.0	7 seconds ago	...
88dc4f03ad8c	● Online	Default config	7.9.0	7 seconds ago	...
9f757fa10929	● Online	Default config rev. 4	7.9.0	7 seconds ago	...
1f9981686e6c	● Online	Default config rev. 4	7.9.0	7 seconds ago	...
server-15	● Online	Default config rev. 4	7.9.0	7 seconds ago	...
server-14	● Online	Default config rev. 4	7.9.0	7 seconds ago	...
server-13	● Online	Default config rev. 4	7.9.0	7 seconds ago	...

Mass updates in 1 click

- Just 1 click updates the policy across all agents
- No more headaches with Powershell, Chef, Ansible, etc.

Add integration

<input checked="" type="checkbox"/>	Apache	
<input type="checkbox"/>	aws	AWS
<input type="checkbox"/>	Barracuda	Web Application Firewall
<input type="checkbox"/>	Blue Coat	Director
<input type="checkbox"/>	Check Point	

Save and deploy changes X

ⓘ This action will update 56 agents

Fleet has detected that the selected agent policy, **Default policy**, is already in use by some of your agents. As a result of this action, Fleet will deploy updates to all agents that use this policy.

This action can not be undone. Are you sure you wish to continue?

Cancel Save and deploy changes

Advanced options >

Collect logs from Apache instances ▼

Collect metrics from Apache instances ▼

Drill down to see agent details

- View the state and logs from each Elastic Agent right in Kibana
- Offers deep visibility to debug problems quickly

Ingest Manager / Fleet / Agents / jason-VB-Development

Overview Integrations Policies **Fleet** Data streams

[Send feedback](#) [Settings](#)

[View all agents](#)

jason-VB-Development

Status Online Policy Default policy Actions

Activity log Agent details

Search for activity logs

Refresh

Timestamp	Type	Subtype	Message
Aug 28, 2020, 8:02:33 PM	State	Running	Application: endpoint-security--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State ...
Aug 28, 2020, 8:02:23 PM	Action result	Acknowledged	Action `fc8af417-50c4-413c-91c6-09023d2523c6` of type 'CONFIG_CHANGE' acknowledged.
Aug 28, 2020, 8:02:23 PM	State	Running	Application: endpoint-security--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State ...
Aug 28, 2020, 7:55:53 PM	State	Running	Application: endpoint-security--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State ...
Aug 28, 2020, 7:52:53 PM	State	Running	Application: endpoint-security--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State ...
Aug 28, 2020, 7:52:33 PM	State	Running	Application: endpoint-security--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State ...
Aug 28, 2020, 7:52:33 PM	State	Running	Application: endpoint-security--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State ...
Aug 28, 2020, 7:52:14 PM	State	Running	Application: metricbeat--7.9.0-SNAPSHOT--36643631373035623733363936343635[9fde6e22-ef03-...]
Aug 28, 2020, 7:52:14 PM	State	Running	Application: metricbeat--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State chang...
Aug 28, 2020, 7:52:14 PM	State	Running	Application: filebeat--7.9.0-SNAPSHOT--36643631373035623733363936343635[9fde6e22-ef03-41...
Aug 28, 2020, 7:52:14 PM	State	Running	Application: filebeat--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State changed t...
Aug 28, 2020, 7:52:11 PM	Action result	Acknowledged	Action `a25f50f0-cac6-4a0a-b269-78e0d53840b2` of type 'CONFIG_CHANGE' acknowledged.
Aug 28, 2020, 7:52:11 PM	State	Starting	Application: metricbeat--7.9.0-SNAPSHOT--36643631373035623733363936343635[9fde6e22-ef03-...]
Aug 28, 2020, 7:52:10 PM	State	Starting	Application: filebeat--7.9.0-SNAPSHOT--36643631373035623733363936343635[9fde6e22-ef03-41...
Aug 28, 2020, 7:52:10 PM	State	Starting	Application: metricbeat--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State chang...
Aug 28, 2020, 7:52:09 PM	State	Starting	Application: filebeat--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State changed t...
Aug 28, 2020, 7:52:08 PM	State	Starting	Application: endpoint-security--7.9.0-SNAPSHOT[9fde6e22-ef03-41ce-8c1b-2814d822d82a]: State ...

Easy data management

- Better visibility to data usage
- More control over lifecycle management and permissions

Ingest Manager / Data streams

Overview Integrations Policies Fleet Data streams

Send feedback Settings

Data streams

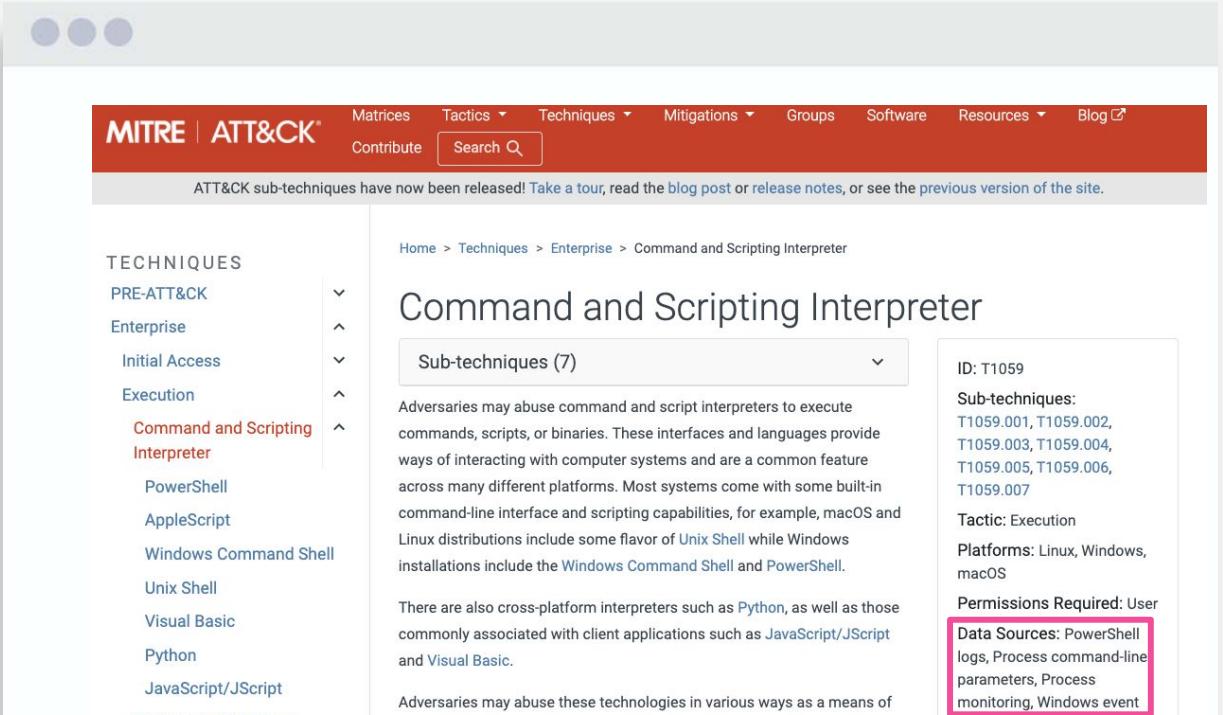
Manage the data created by your agents.

Filter data streams		Dataset	Type	Namespace	Integration	Last activity	Size	Actions
<input type="text"/>	<button>Reload</button>	elastic.agent.filebeat	logs	default		Aug 28, 2020 @ 20:19:05.485	2.8MB	...
		system.process	metrics	default	system	Aug 28, 2020 @ 20:19:03.938	1.5MB	...
		nginx.stubstatus	metrics	default	nginx	Aug 28, 2020 @ 20:19:03.801	61.4KB	...
		system.process_summary	metrics	default	system	Aug 28, 2020 @ 20:19:03.761	196.8KB	...
		system.socket_summary	metrics	default	system	Aug 28, 2020 @ 20:19:03.742	102.2KB	...
		elastic.agent.metricbeat	metrics	default		Aug 28, 2020 @ 20:19:03.704	237.8KB	...
		system.diskio	metrics	default	system	Aug 28, 2020 @ 20:19:03.704	1,023.2KB	...
		elastic.agent.filebeat	metrics	default		Aug 28, 2020 @ 20:19:03.703	233.5KB	...
		elastic.agent.endpoint-security	metrics	default		Aug 28, 2020 @ 20:19:03.684	166.8KB	...
		system.uptime	metrics	default	system	Aug 28, 2020 @ 20:19:03.663	69.9KB	...
		system.cpu	metrics	default	system	Aug 28, 2020 @ 20:19:03.662	143.4KB	...
		system.load	metrics	default	system	Aug 28, 2020 @ 20:19:03.662	67.2KB	...
		system.memory	metrics	default	system	Aug 28, 2020 @ 20:19:03.662	122.4KB	...
		system.network	metrics	default	system	Aug 28, 2020 @ 20:19:03.634	210.1KB	...
		elastic.agent.metricbeat	logs	default		Aug 28, 2020 @ 20:18:54.859	7.2MB	...
		nginx.access	logs	default	nginx	Aug 28, 2020 @ 20:18:53.000	61.1KB	...
		endpoint.events.network	logs	default	endpoint	Aug 28, 2020 @ 20:18:23.803	434.6KB	...

Deep data visibility

Data Visibility

- MITRE ATT&CK™ provides the data sources required to detect **250+ adversary techniques**
- There are **50+ unique data sources**
- Examples include, “Process Monitoring”, “DNS Records”, “Authentication Logs”, and more!



MITRE | ATT&CK™

Matrices Tactics Techniques Mitigations Groups Software Resources Blog

Contribute Search

ATT&CK sub-techniques have now been released! Take a tour, read the blog post or release notes, or see the previous version of the site.

Home > Techniques > Enterprise > Command and Scripting Interpreter

Command and Scripting Interpreter

Sub-techniques (7)

TECHNIQUES

- PRE-ATT&CK
- Enterprise
- Initial Access
- Execution
- Command and Scripting Interpreter
- PowerShell
- AppleScript
- Windows Command Shell
- Unix Shell
- Visual Basic
- Python
- JavaScript/JScript

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript/JScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of

ID: T1059
Sub-techniques: T1059.001, T1059.002, T1059.003, T1059.004, T1059.005, T1059.006, T1059.007
Tactic: Execution
Platforms: Linux, Windows, macOS
Permissions Required: User
Data Sources: PowerShell logs, Process command-line parameters, Process monitoring, Windows event

Data integrations

- Microsoft Defender ATP
- Windows PowerShell
- G Suite: login events, admin activity, Drive, and more
- Sophos XG Firewalls, via a community contribution



Windows Defender



Plus over 40 more integrations

Support for 15+ common network and application security technologies



NETSCOUT



imperva

BlackBerry
CYLANCE.

JUNIPER
NETWORKS

zscaler™

SONICWALL

f5

tenable™

Infoblox

CITRIX®

Free malware prevention

Elastic Endpoint Security

Free and Open Endpoint Security

Available to all Basic+ customers

Centrally Managed through Agent/Fleet

Install one agent and get access to over 20 integrations including Elastic Endpoint Security

Integrations

Browse integrations for popular apps and services.

All integrations Installed integrations



Browse by category

All 9

Security 1


Cisco Integration


Elastic Endpoint Security
Protect your hosts with threat prevention, detection, and deep security data visibility.


Kafka Integration

[Browse all integrations](#)


Elastic Endpoint Security BETA Version 0.11.0 [Add Elastic Endpoint Security](#)

Elastic Endpoint Security Integration [Collapse](#)

This integration sets up templates and index patterns required for Elastic Endpoint Security.

Compatibility
For compatibility information view our [documentation](#).

Logs
The log type of documents are stored in the `logs-endpoint.*` indices. The following sections define the mapped fields sent by the endpoint.

alerts

EXPORTED FIELDS

Field	Description	Type
<code>@timestamp</code>	Datetime when the event originated. This is the date/time extracted from the event, typically representing when the event was generated by the source. If the event source has no original timestamp, this value is typically populated by the first time the event was received by the pipeline. Required field for all events.	date
<code>Endpoint.policy</code>	The policy fields are used to hold information about applied policy.	object
<code>Endpoint.policy.applied</code>	information about the policy that is applied	object
<code>Endpoint.policy.applied.id</code>	the id of the applied policy	keyword
<code>Endpoint.policy.applied.name</code>	the name of this applied policy	keyword
<code>Endpoint.policy.applied.status</code>	the status of the applied policy	keyword
<code>Endpoint.policy.applied.version</code>	the version of this applied policy	keyword

Protect your Hosts in 2 Clicks

Really Easy to Get Started

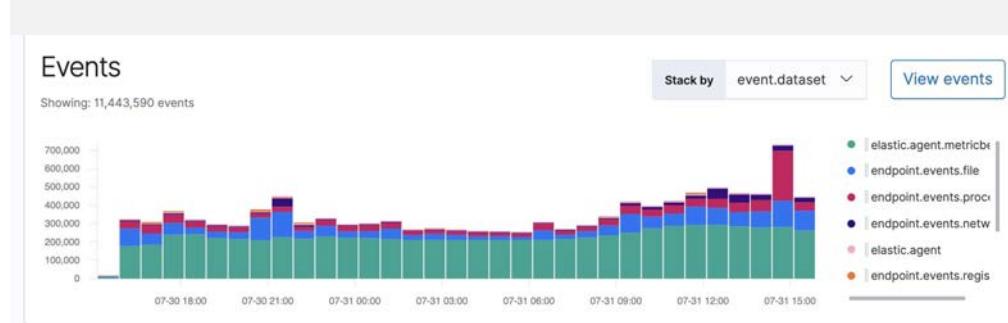
Once agent is installed and running, endpoint protection is just 2 clicks away.

Prevention and Visibility Default

Out of the box malware prevention and kernel level data collection

The image shows two screenshots of the Elastic Stack interface. The top screenshot is titled 'Add Elastic Endpoint Security integration' and shows the 'Select an agent configuration' step, where 'Default config' is selected. The bottom screenshot shows the 'Add agent' interface, specifically the 'Fleet' tab, with a list of hosts including 'response-win-1', 'security-win-2', 'security-win-1', 'ingest-win-2', 'mgti-win-1', 'data-viz-win-1', 'ingest-win-1', 'ingest-linux-1', 'security-linux-2', 'security-linux-1', and 'ingest-linux-2'. The 'Agents' tab is selected. The right side of the bottom screenshot is a 'Add agent' wizard with three steps: 1. Download the Elastic Agent (with a link to elastic.co/downloads), 2. Choose an agent configuration (with a list of configurations including 'System' and 'Elastic Endpoint Security'), and 3. Enroll and start the Elastic Agent (with a 'Windows' section containing command lines for enrollment and starting the agent).

Deep Data Visibility



Windows

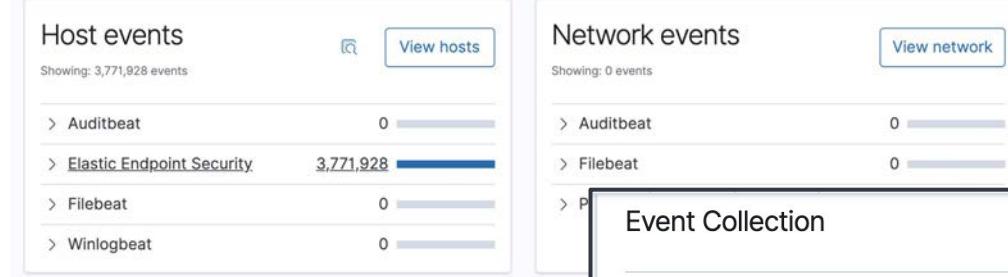
Events: Process, Network, File, DNS, DLL and Driver Loads, Registry, Security

macOS

Events: Process, Network, File

Linux:

Events: Process, Network, File



Event Collection

Events

- DLL and Driver Load
- DNS
- File
- Network
- Process
- Registry
- Security

Stop Attacks

Malware Prevention

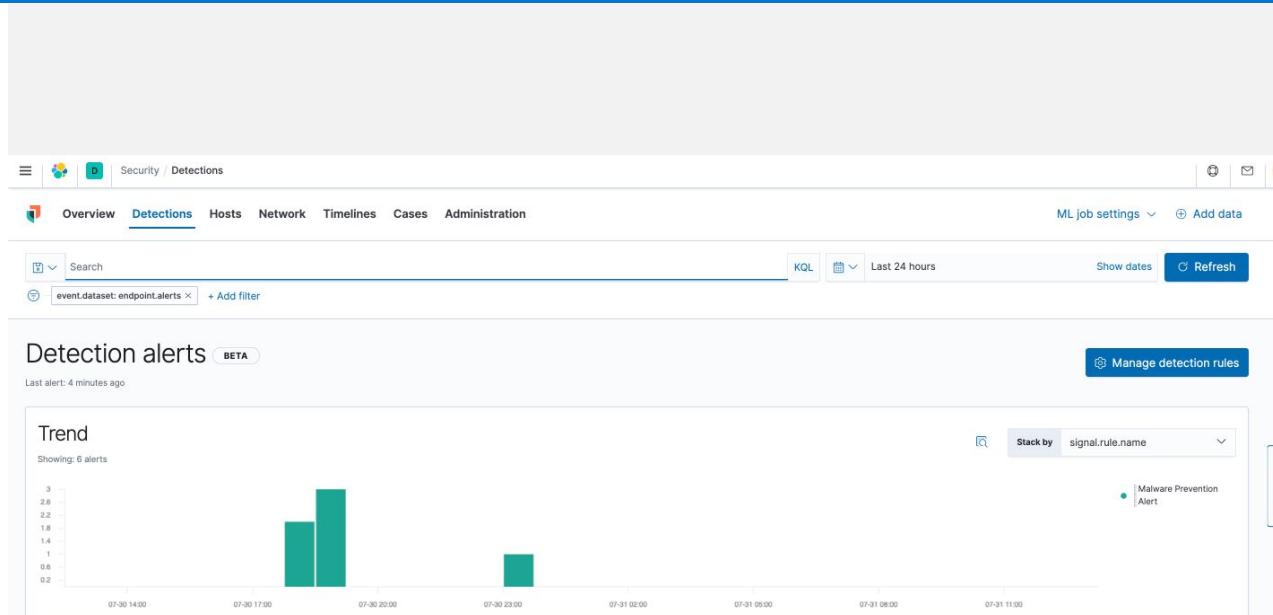
Machine Learning Malware Prevention proven to be over 99% effective at stopping malware*

Auto Quarantine

Malicious files are automatically removed from user access to eliminate repeat infection attempts

Zero System Impact

Scored “Fast” on performance tests when protecting hosts*



The screenshot shows the Elastic Stack interface for 'Detections'. The top navigation bar includes 'Overview', 'Detections' (which is selected), 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. Below the navigation is a search bar with 'event.dataset: endpoint.alerts' and a 'KQL' button. The main area is titled 'Detection alerts (BETA)' and shows a bar chart titled 'Trend' with 6 alerts. The x-axis shows dates from 07-30 14:00 to 07-31 11:00, and the y-axis shows values from 0.2 to 3.0. A legend indicates 'Malware Prevention Alert' with a green dot. Below the chart is a table of 6 alerts, with columns for '@timestamp', 'Rule', 'host.name', 'Versi...', 'Method', 'Severity', 'Risk Score', 'event.module', 'event.action', 'event.category', and 'user.name'. Each alert row includes a checkbox, a timestamp, a rule name, a host name, a version, a method (query), a medium severity, a risk score of 73, an endpoint module, an unknown action, and a malware category. The table also includes 'Open', 'In progress', and 'Closed' status filters and an 'Additional filters' dropdown.

Showing 6 alerts Selected 0 alerts Take action Select all 6 alerts Open In progress Closed Additional filters											
	@timestamp	Rule	host.name	Versi...	Method	Severity	Risk Score	event.module	event.action	event.category	user.name
<input type="checkbox"/>	Jul 30, 2020 @ 23:04:43.633	Malware Prevention Alert	bpreston-mba	1	query	medium	73	endpoint	unknown	malware	
<input type="checkbox"/>	Jul 30, 2020 @ 18:43:41.360	Malware Prevention Alert	crowenss-Mac.local	1	query	medium	73	endpoint	unknown	malware	
<input type="checkbox"/>	Jul 30, 2020 @ 18:33:42.490	Malware Prevention Alert	mindy-mbp	1	query	medium	73	endpoint	unknown	malware	

Analyze Events

Identify the Origin and Extent of an attack

Streamline alert triage, hunt, investigation, and response

Equip analysts to spot potential adversary behaviors and attack progression

The image displays two main interface sections of the Elastic Stack. The top section is a table titled 'Showing 6 alerts' with columns for '@timestamp', 'Rule', 'host.name', 'Versi...', 'Method', 'Severity', 'Risk Score', 'event.module', and 'event'. A callout box labeled 'Analyze event' points to the first row, which shows a 'Malware Prevention Alert' from 'bpreston-mba' at 'Jul 30, 2020 @ 23:04:43.633'. The bottom section is titled 'Events' and shows a 'BETA' label. It includes a sidebar titled 'All Process Events' listing processes like 'systemd', 'gdm3', and 'gnome-session...' with their timestamps. The main area displays a process flow diagram with nodes for 'RUNNING PROCESS bash' and 'TERMINATED PROCESS bash'. Arrows between nodes are labeled with times such as '2 milliseconds', '424 milliseconds', '11 seconds', and '17 milliseconds'. A legend on the right identifies the node types: a blue hexagon for 'RUNNING PROCESS' and a green hexagon for 'TERMINATED PROCESS'.

Eliminate False Positives

Exception workflow for all alerts

Apply exceptions all the way down to the endpoint

Add Endpoint Exception

Malware Prevention Alert

AND

file.Ext.code_signature.subject	is	Search field value...
file.Ext.code_signature.trusted	is	false
file.path.text	is	/Users/bpreston/Documents/Leia-master/modules/generate_mac_
file.hash.sha1	is	f10b043652da8c444e04aede3a9ce4a10ef9028e
...

Close this alert

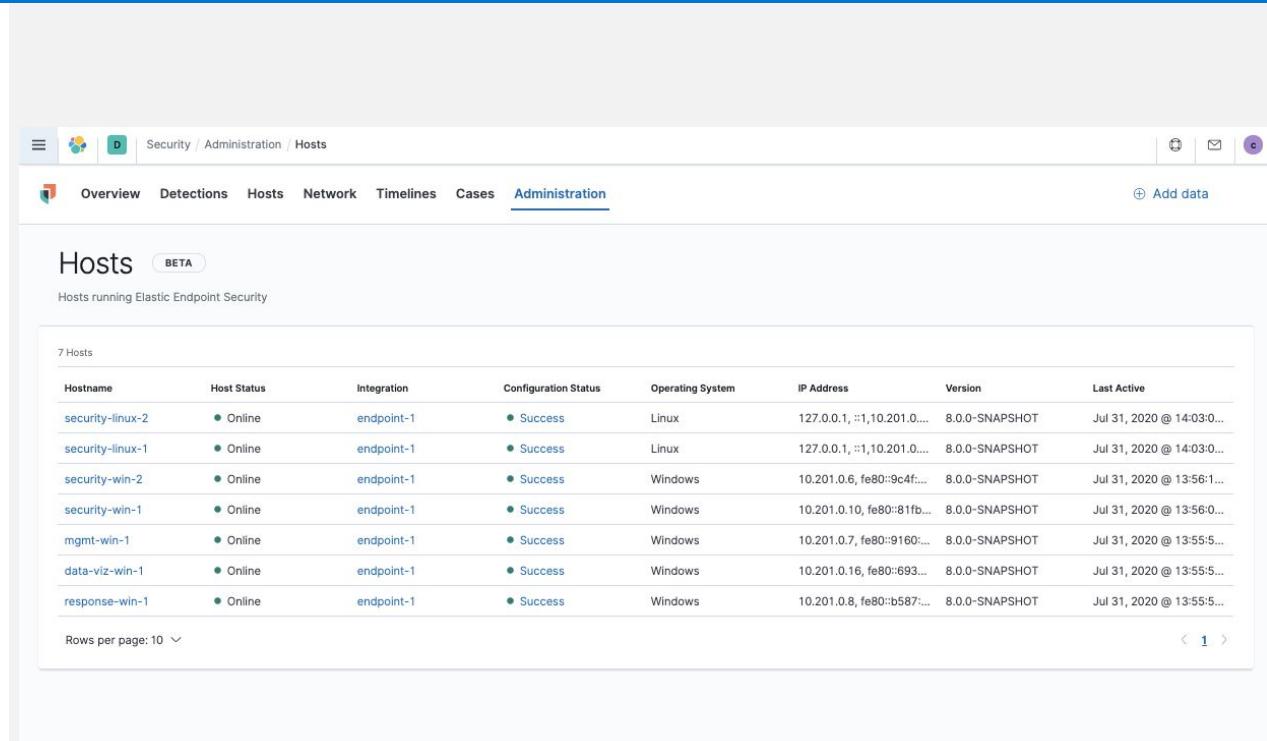
Close all alerts that match this exception, including alerts generated by other rules

Any file in quarantine on any endpoint that matches the attribute(s) selected will automatically be restored to its original location. This exception will apply to any rule that is linked to the Global Endpoint Exception List.

[Cancel](#) [Add Exception](#)

Close alert	Malware Prevention Alert	bpreston-mba	1	query	medium
Mark in progress	Malware Prevention Alert	crowenss-Mac.local	1	query	medium
Add Endpoint exception	Malware Prevention Alert	mindy-mbp	1	query	medium
Add exception	Malware Prevention Alert	crowens-mbp	1	query	medium
Malware Prevention Alert	mindy-mbp	1	query	medium	

View Hosts Running Endpoint Security



The screenshot shows the Elastic Stack interface with the following details:

- Header:** Security / Administration / Hosts
- Navigation:** Overview, Detections, Hosts, Network, Timelines, Cases, Administration, Add data
- Section:** Hosts (BETA)
- Text:** Hosts running Elastic Endpoint Security
- Table:** 7 Hosts

Hostname	Host Status	Integration	Configuration Status	Operating System	IP Address	Version	Last Active
security-linux-2	Online	endpoint-1	Success	Linux	127.0.0.1, ::1, 10.201.0....	8.0.0-SNAPSHOT	Jul 31, 2020 @ 14:03:0...
security-linux-1	Online	endpoint-1	Success	Linux	127.0.0.1, ::1, 10.201.0....	8.0.0-SNAPSHOT	Jul 31, 2020 @ 14:03:0...
security-win-2	Online	endpoint-1	Success	Windows	10.201.0.6, fe80::9c4f:...	8.0.0-SNAPSHOT	Jul 31, 2020 @ 13:56:1...
security-win-1	Online	endpoint-1	Success	Windows	10.201.0.10, fe80::81fb...	8.0.0-SNAPSHOT	Jul 31, 2020 @ 13:56:0...
mgmt-win-1	Online	endpoint-1	Success	Windows	10.201.0.7, fe80::9160...	8.0.0-SNAPSHOT	Jul 31, 2020 @ 13:55:5...
data-viz-win-1	Online	endpoint-1	Success	Windows	10.201.0.16, fe80::693...	8.0.0-SNAPSHOT	Jul 31, 2020 @ 13:55:5...
response-win-1	Online	endpoint-1	Success	Windows	10.201.0.8, fe80::b587...	8.0.0-SNAPSHOT	Jul 31, 2020 @ 13:55:5...

- Page Controls:** Rows per page: 10, Page 1 of 1

Full Configurability and Control

Change the configuration to meet your needs

Easy toggles to adjust the security settings that match your risk profile.

The screenshot shows the 'Edit integration' page for 'Endpoint Security' in the 'Configurations' section of the Ingest Manager. The page title is 'Edit Elastic Endpoint Security integration'. The 'Integration settings' section includes fields for 'Integration name' (set to 'endpoint-1') and 'Description'. A note says 'Choose a name and description to help identify how this integration will be used.' Below this is a link to 'Advanced options'. The main content area has a note: 'Click [here](#) to edit advanced configuration options.' To the right, the 'Administration' tab is selected in the navigation bar, showing 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. The 'Administration' tab has a sub-section for 'endpoint-1' with 'Hosts' (7), 'Online' (7), 'Offline' (0), and 'Error' (0) status. A 'Save' button is visible. The 'Protections' section shows 'Type' as 'Malware' and 'Operating System' as 'Windows, Mac', with a 'Malware Protections Enabled' toggle switch. The 'Protection Level' is set to 'Prevent'. A note says 'View related detection rules. Prebuilt rules are tagged "Elastic" on the Detection Rules page.' The 'Settings' section shows 'Type' as 'Event Collection' and 'Operating System' as 'Windows', with '7 / 7 event collections enabled'. The 'Events' section lists checked items: 'DLL and Driver Load', 'DNS', 'File', 'Network', 'Process', 'Registry', and 'Security'. The 'Mac' section shows 'Event Collection' as 'Type' and 'Operating System' as 'Mac', with '3 / 3 event collections enabled' and a checked 'File' and 'Process' item.

Error Reporting

Overview Detections Hosts Network Timelines Cases Administration

Hosts BETA

Hosts running Elastic Endpoint Security

Hostname	Host Status	Integration	Configuration Status	Operating System	IP Address
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.5...
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.5...
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.6...
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.7...
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.5...
bpreston-mba	Offline	lava	Failure	macOS	127.0.0.1, ::1, fe80::1...
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.5...
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.6...
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.6...
mainqa-aticolo-10-0...	Online	x5d prevent malware	Success	Linux	127.0.0.1, ::1, 10.0.5...

Rows per page: 10 ▾

bpreston-mba

Endpoint Details

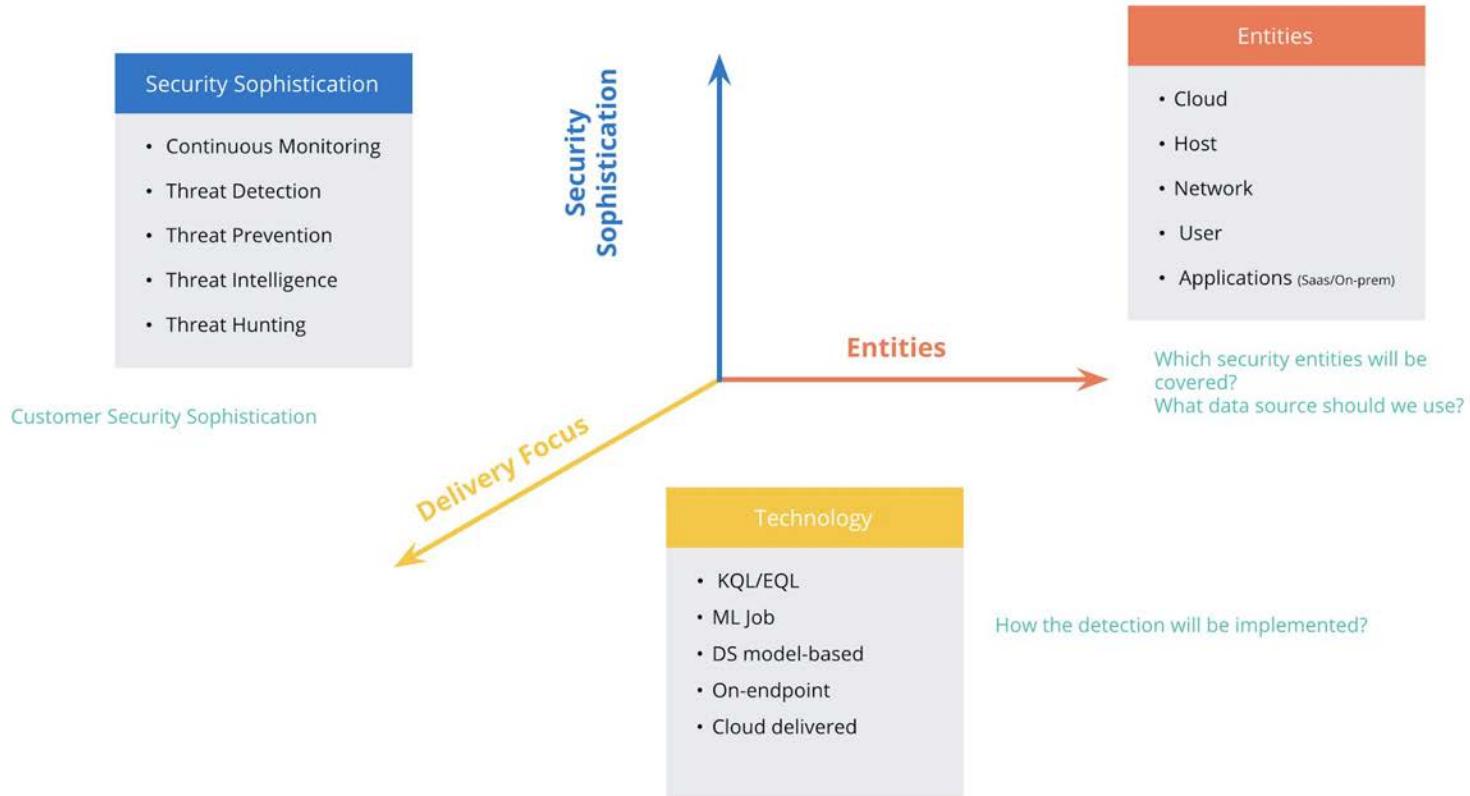
Configuration Response

- Streaming 1
 - Agent Connectivity ● Failed
 - Load Config ● Success
 - Read ElasticSearch Config ● Success
 - Configure Elastic Search Connection ● Success
 - Workflow ● Success
- Malware 1
 - Agent Connectivity ● Failed
 - Load Config ● Success
 - Workflow ● Success
 - Download Global Artifacts ● Success
 - Download User Artifacts ● Success
 - Configure Malware ● Success
 - Read Malware Config ● Success
 - Load Malware Model ● Success

Prebuilt protections and expanded detection methods

The Cube

Turn-key protections across the organization



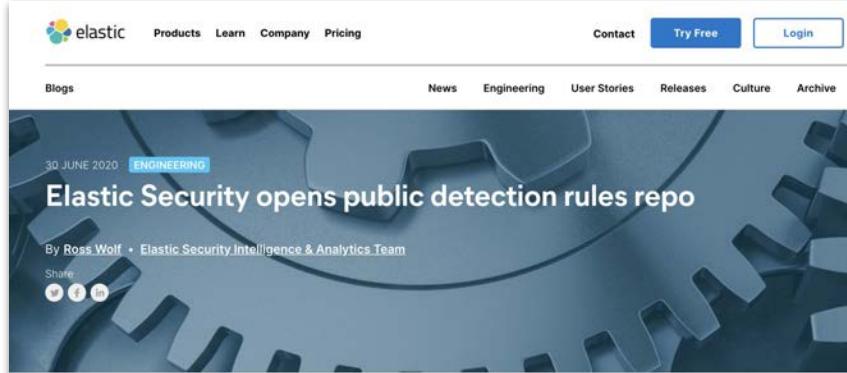
Stop threats at scale...

You know, in a free and open way

Elastic Security Detections Repository

Open	<i>Elastic Security + Community = building the best detections to protect the world's data</i>
Free	<i>Detections are free and under Elastic License</i>
Growing	<i>All new detections will be available there all the time</i>
Coverage	<i>Across MITRE ATT&CK and Cybersecurity frameworks for SecOps</i>

- [elastic/detection-rules](https://github.com/elastic/detection-rules)
- [Release Blog](#)



The screenshot shows a blog post on the elastic.com website. The header includes the elastic logo, navigation links for Products, Learn, Company, Pricing, Contact, Try Free, and Login. The main content is a blog post titled "Elastic Security opens public detection rules repo" by Ross Wolf, published on 30 JUNE 2020. The post discusses the release of a GitHub repository for detection rules and its importance for the security community. It includes sections for Elasticsearch: Getting Started, Recommended Content, and a "How to build React search experiences quickly" sidebar.

At Elastic, we believe in the [power of open source](#) and understand the importance of community. By putting the community first, we ensure that we create the best possible product for our users. With Elastic Security, [two of our core objectives](#) are to stop threats at scale and arm every analyst. Today, we're opening up a new GitHub repository, [elastic/detection-rules](#), to work alongside the security community, stopping threats at a greater scale.

The release of the [detection engine](#) in Elastic Security brought automated threat detection to the Elastic Stack. Since the initial launch of the detection engine, the Elastic Security Intelligence & Analytics team has added 50+ additional rules, increasing the visibility of attacker techniques on Linux, macOS, and Windows operating systems. As we continue to expand coverage, you'll see increased breadth in detections, covering new domains such as cloud services and user behavior.

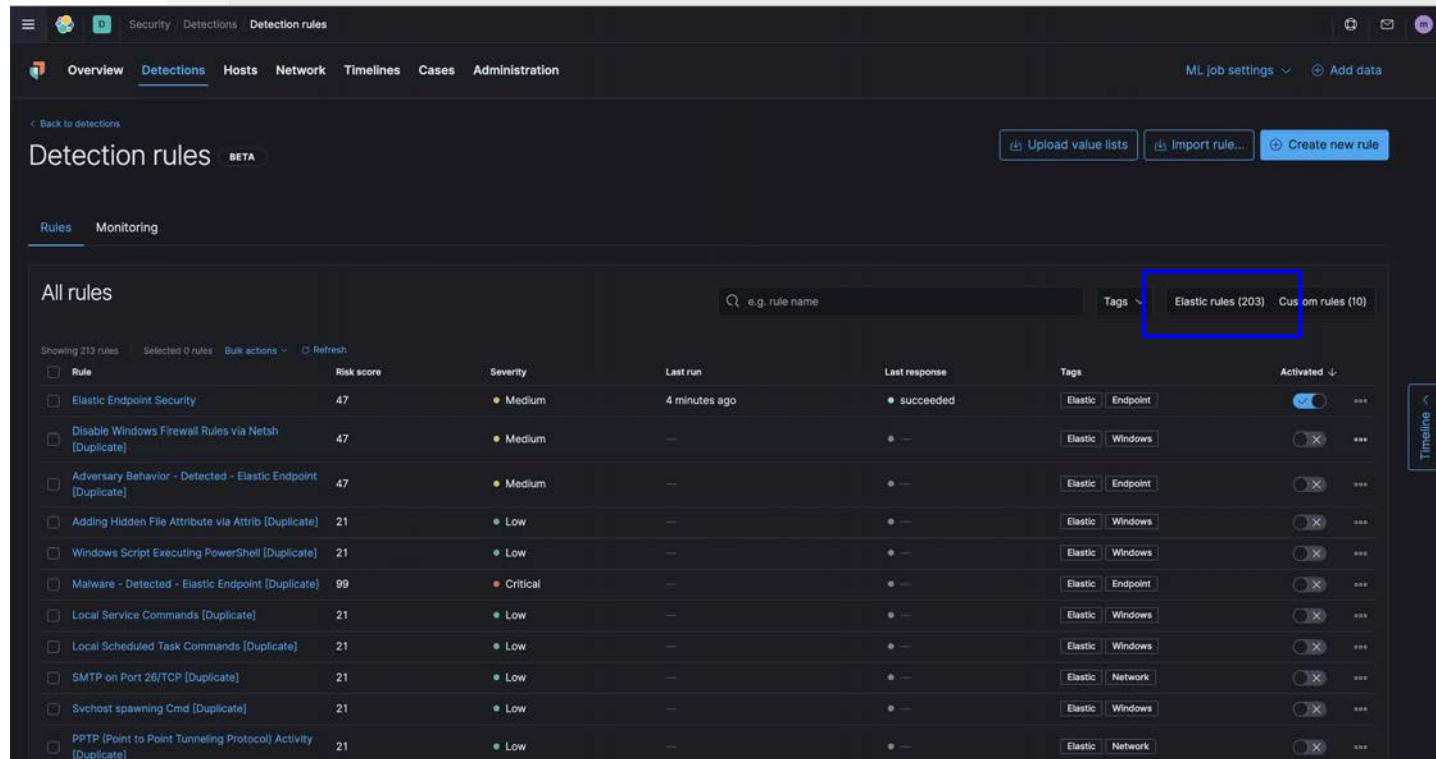
Over the past few releases, we used an internal repository to manage rules for the detection engine. We've iteratively improved our testing procedures by adding automated tests for new contributions that validate Kibana Query Language (KQL) syntax, schema usage, and other metadata. Our rule development has matured, so we can move fast without breaking things.

By opening up our [elastic/detection-rules](#) GitHub repository, Elastic Security will develop rules in the open alongside the community, and we're welcoming your community-driven detections. This is an opportunity for all of us to share our collective knowledge, learn from each other, and make an impact by working together.



Out-of-the-Box (Prebuilt) Detection Rules in 7.9

- 203 rules included in 7.9 distribution
- All tagged with “Elastic” +
- 28 ML Jobs
- **37 AWS**
- **17 Okta**
- 23 Network
- 4 APM
- 67 Windows
- 39 Linux
- 16 Elastic endpoint alert
- All contain severity, risk_score, and tags



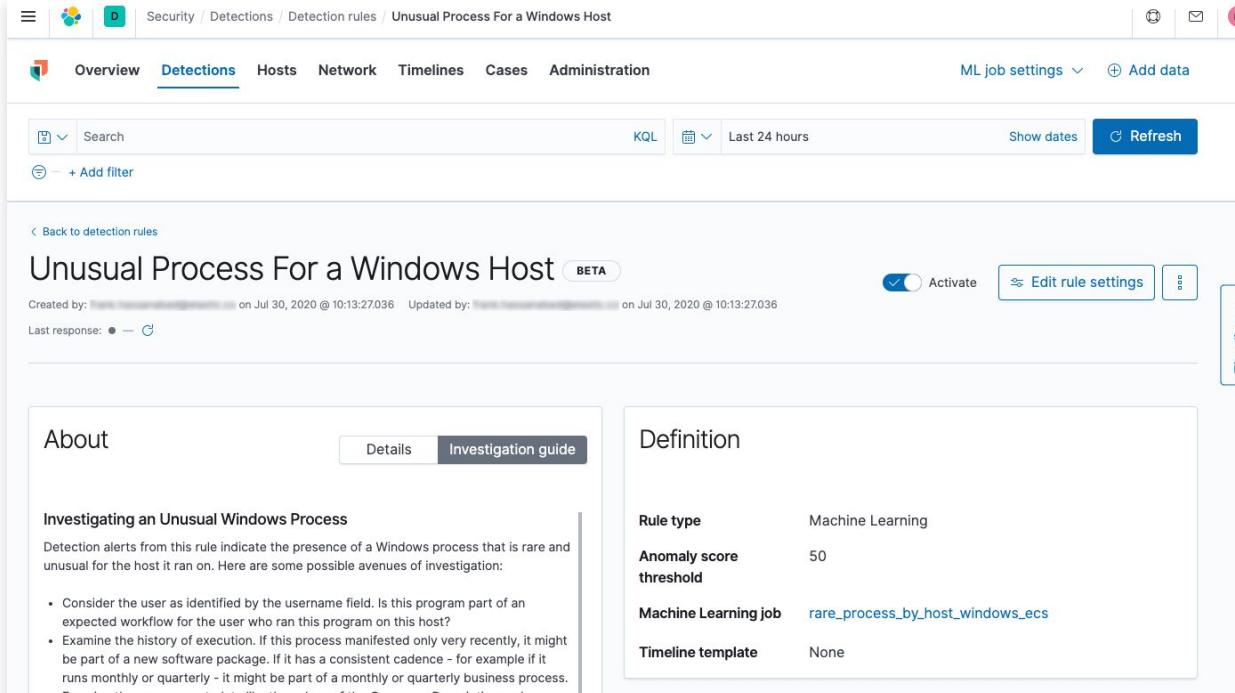
The screenshot shows the 'Detection rules' page in the Elastic Stack interface. The top navigation bar includes 'Overview', 'Detections' (which is selected), 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. On the right, there are buttons for 'ML job settings', 'Add data', 'Upload value lists', 'Import rule...', and 'Create new rule'. A blue box highlights the 'Tags' section, which shows 'Elastic rules (203)' and 'Custom rules (10)'. The main table lists 213 rules, with columns for 'Rule' (checkbox), 'Risk score', 'Severity' (color-coded), 'Last run', 'Last response' (status), 'Tags', and 'Activated' (checkbox). The 'Activated' column for the first rule is checked. A blue box also highlights the first few rows of the table. The interface has a dark theme with light-colored text and icons.

Streamlined analyst workflows

Investigation guides for prebuilt detection rules

Suggests questions, actions, and next steps to analysts investigating an alert

Creating a new investigation guide is as simple as updating a markdown field



The screenshot shows the Splunk Security Cloud interface. At the top, there are navigation icons for Home, Security, Detections, and Detection rules, followed by the title 'Unusual Process For a Windows Host'. The main navigation bar includes Overview, Detections (which is underlined), Hosts, Network, Timelines, Cases, and Administration. On the right, there are buttons for 'ML job settings', 'Add data', 'Search' (with a KQL dropdown), 'Last 24 hours', 'Show dates', 'Refresh', and 'Edit rule settings'.

The main content area displays the 'Unusual Process For a Windows Host' rule. It shows the rule was created on Jul 30, 2020, at 10:13:27.036 and updated on the same date at 10:13:27.036. There is an 'Activate' toggle switch, which is turned on. Below the rule title, there are tabs for 'About' and 'Details' (which is currently selected). The 'About' tab contains a section titled 'Investigating an Unusual Windows Process' with a list of investigation steps:

- Consider the user as identified by the username field. Is this program part of an expected workflow for the user who ran this program on this host?
- Examine the history of execution. If this process manifested only very recently, it might be part of a new software package. If it has a consistent cadence - for example if it runs monthly or quarterly - it might be part of a monthly or quarterly business process.
- Examine the process metadata like the values of the Company, Description and

The 'Details' tab shows the rule's definition with the following parameters:

Rule type	Machine Learning
Anomaly score threshold	50
Machine Learning job	rare_process_by_host_windows_ecs
Timeline template	None

Unified alert exceptions workflow

Enables faster reduction in false positives, which are analysts' top frustration

Add Exception
Port scanning

Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
host.user.name	is	service.account

OR

Field	Operator	Value
host.user.name	is	admin

AND

Field	Operator	Value
destination.geo.city_name	is	Montreal

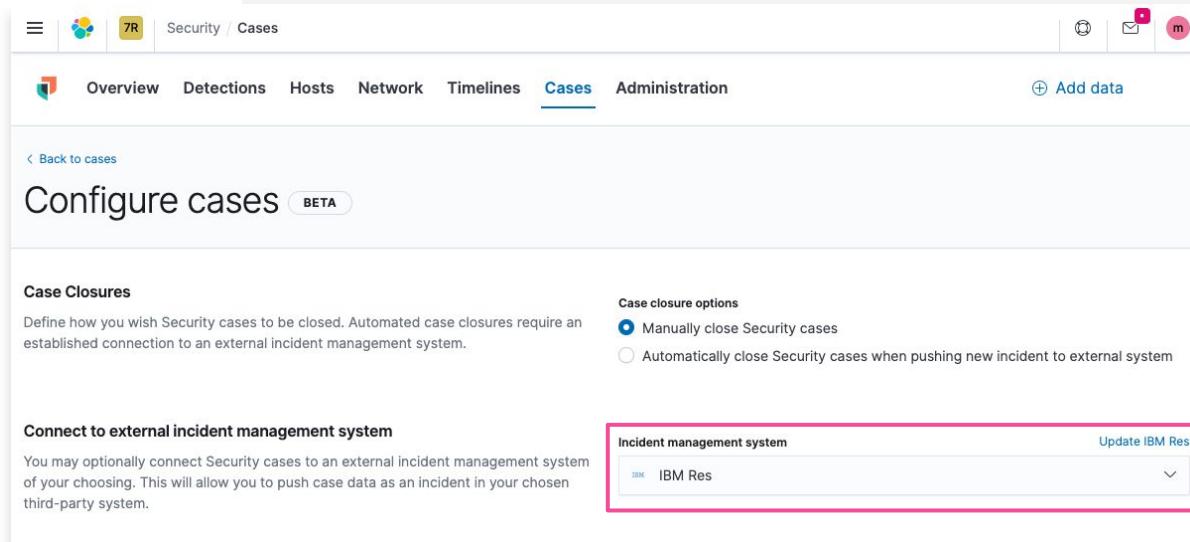
Approved by Riley Hunter on August 17, 2020.

Close this alert

Close all alerts that match this exception, including alerts generated by other rules

IBM Security Resilient integration

Enables a quick connection to the widely-deployed security incident response platform



Security | Cases

Overview Detections Hosts Network Timelines Cases Administration [Add data](#)

Back to cases

Configure cases BETA

Case Closures
Define how you wish Security cases to be closed. Automated case closures require an established connection to an external incident management system.

Case closure options

- Manually close Security cases
- Automatically close Security cases when pushing new incident to external system

Connect to external incident management system
You may optionally connect Security cases to an external incident management system of your choosing. This will allow you to push case data as an incident in your chosen third-party system.

Incident management system [Update IBM Res](#)

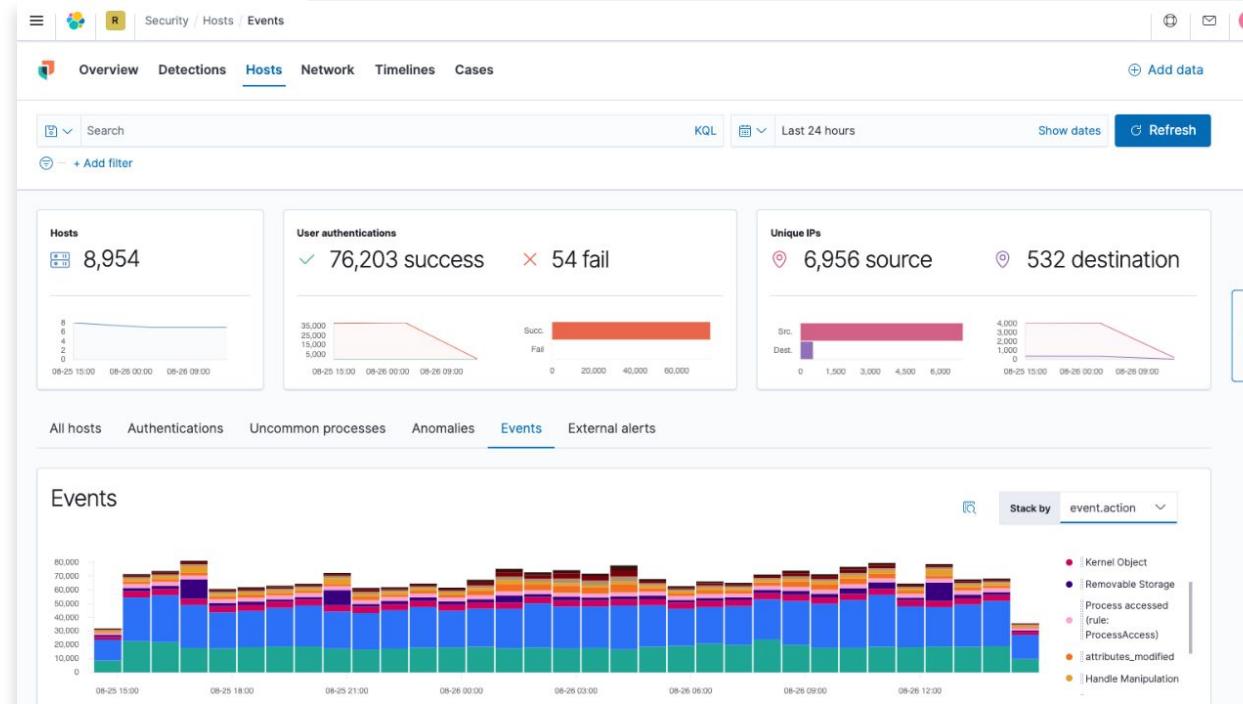
- IBM Res

Further analyst workflow enhancements

Full-screen mode and infinite scroll put analysts in control

Customizable timeline templates enable curated views for specific alerts

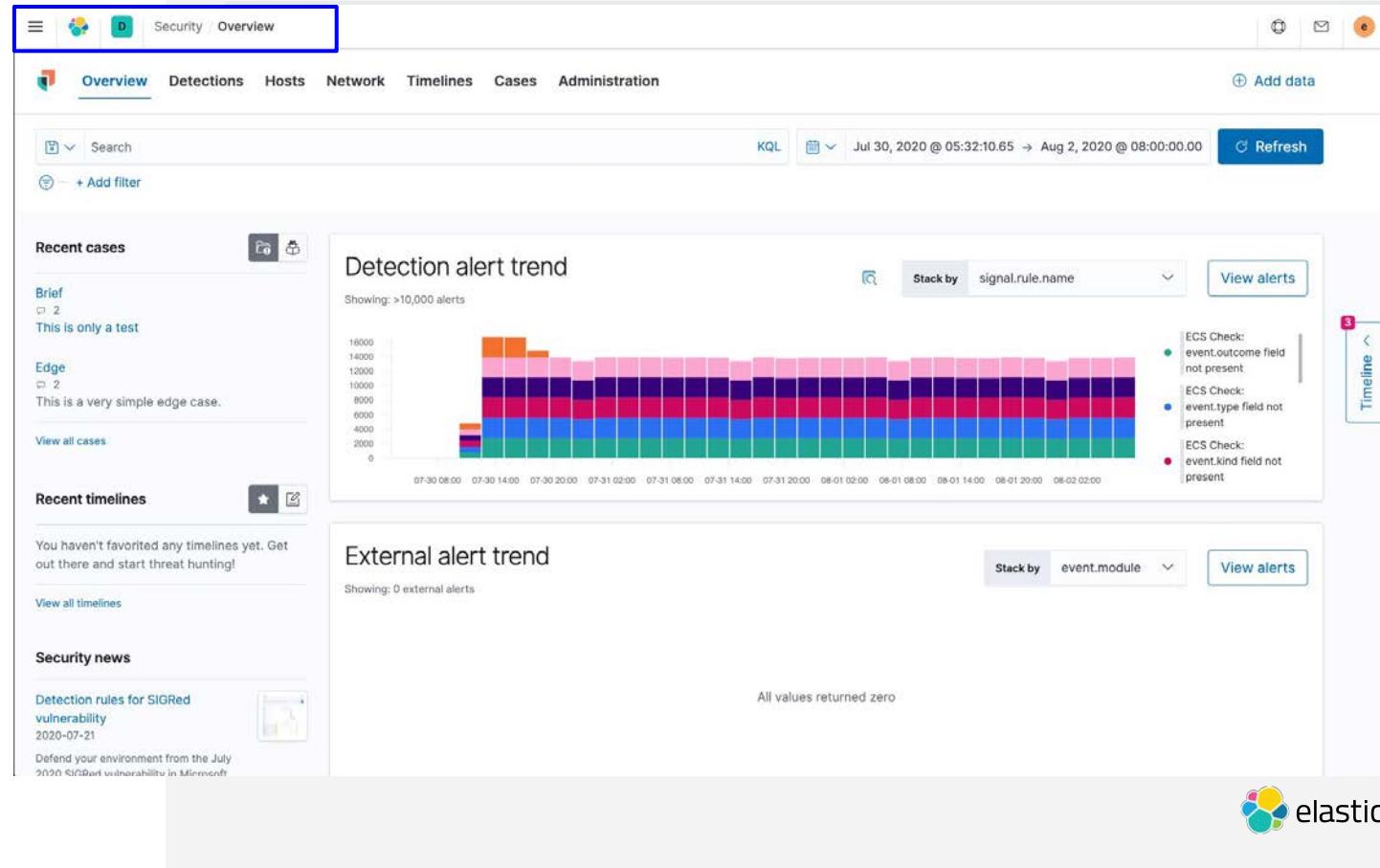
Other enhancements fulfill requests from our global community



Analyst Workflow Enhancements

- Signals now called **Detection Alerts**
- Exceptions workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

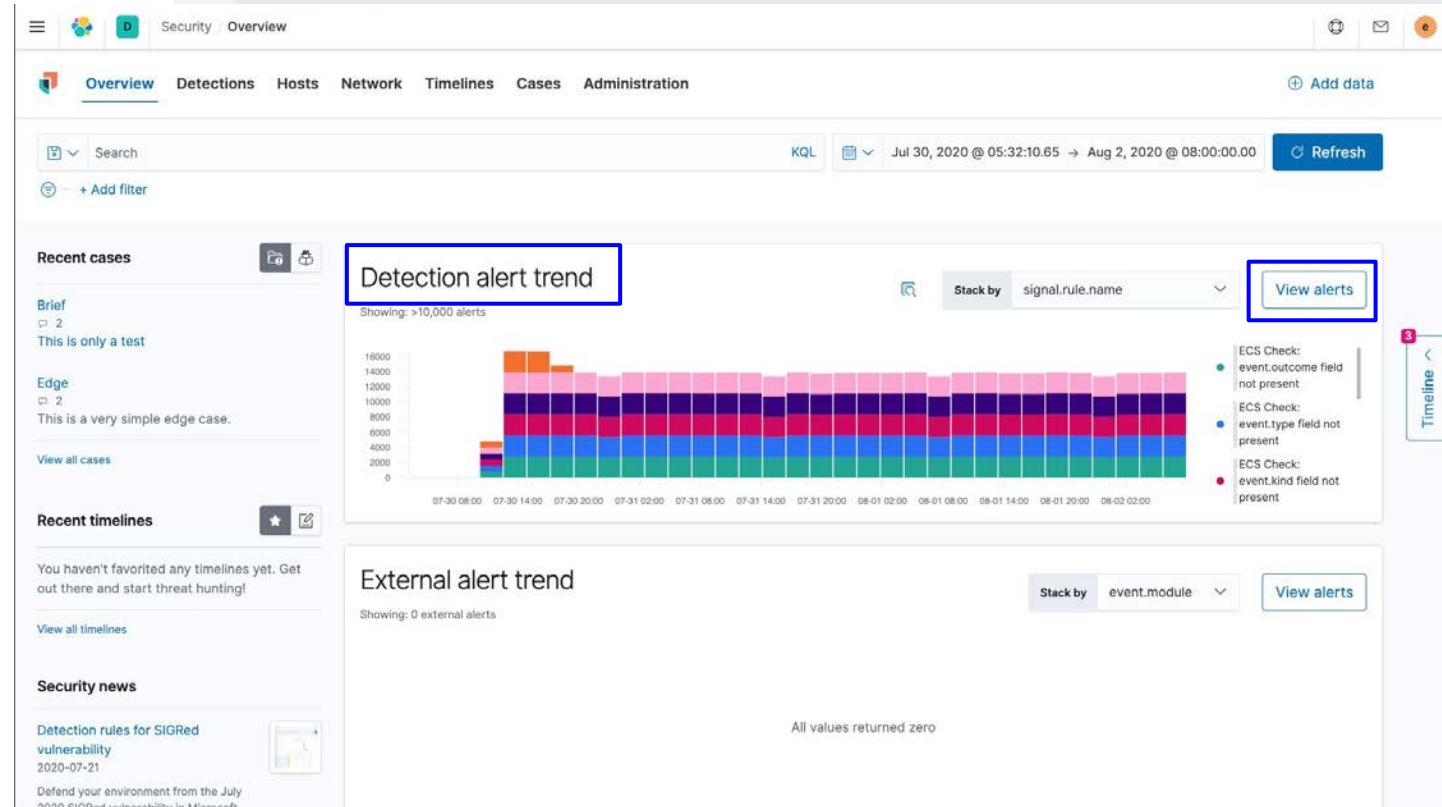
App name changed from "SIEM" to "Security." In-app breadcrumbs now show "Security"



Analyst Workflow Enhancements

- Signals now called **Detection Alerts**
- Exceptions workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

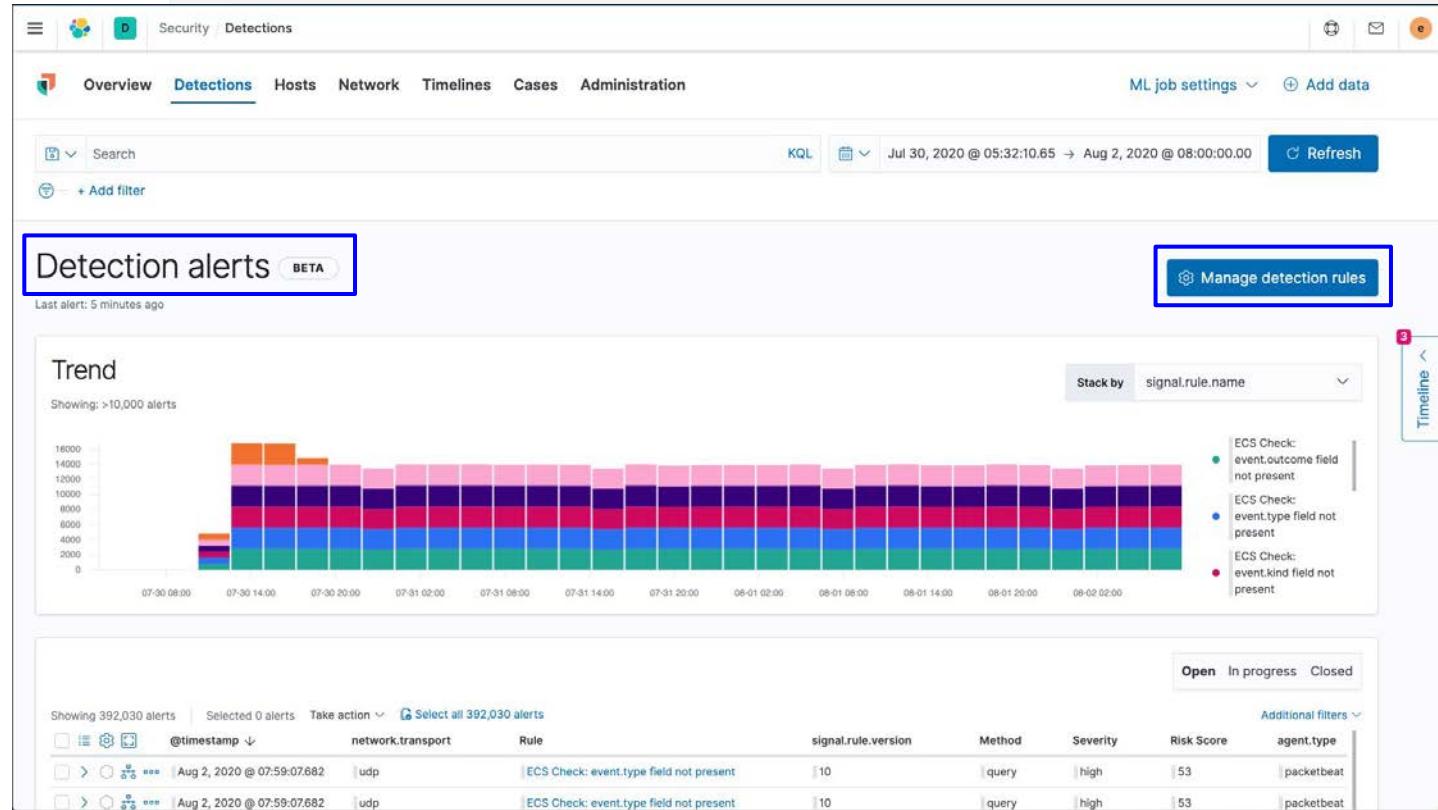
In-app titles, descriptions, and documentation now refer to "Detection alerts" instead of signals.



Analyst Workflow Enhancements

- Signals now called Alerts
- Exceptions workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

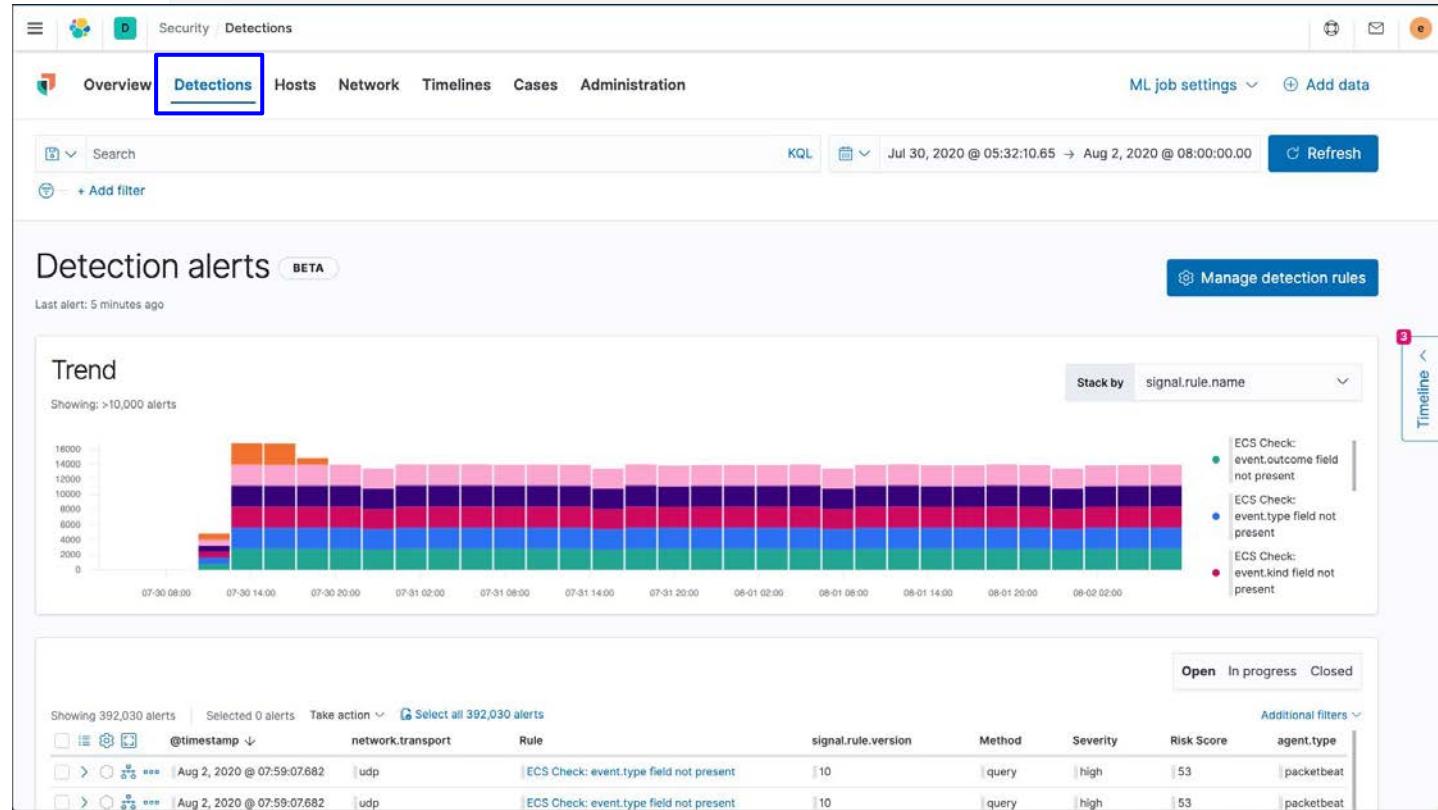
Signals table is now "Detection alerts" table. Note that "External alerts" view is gone. Rules now called "detection rules."



Analyst Workflow Enhancements

- Signals now called Alerts
- Exceptions workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

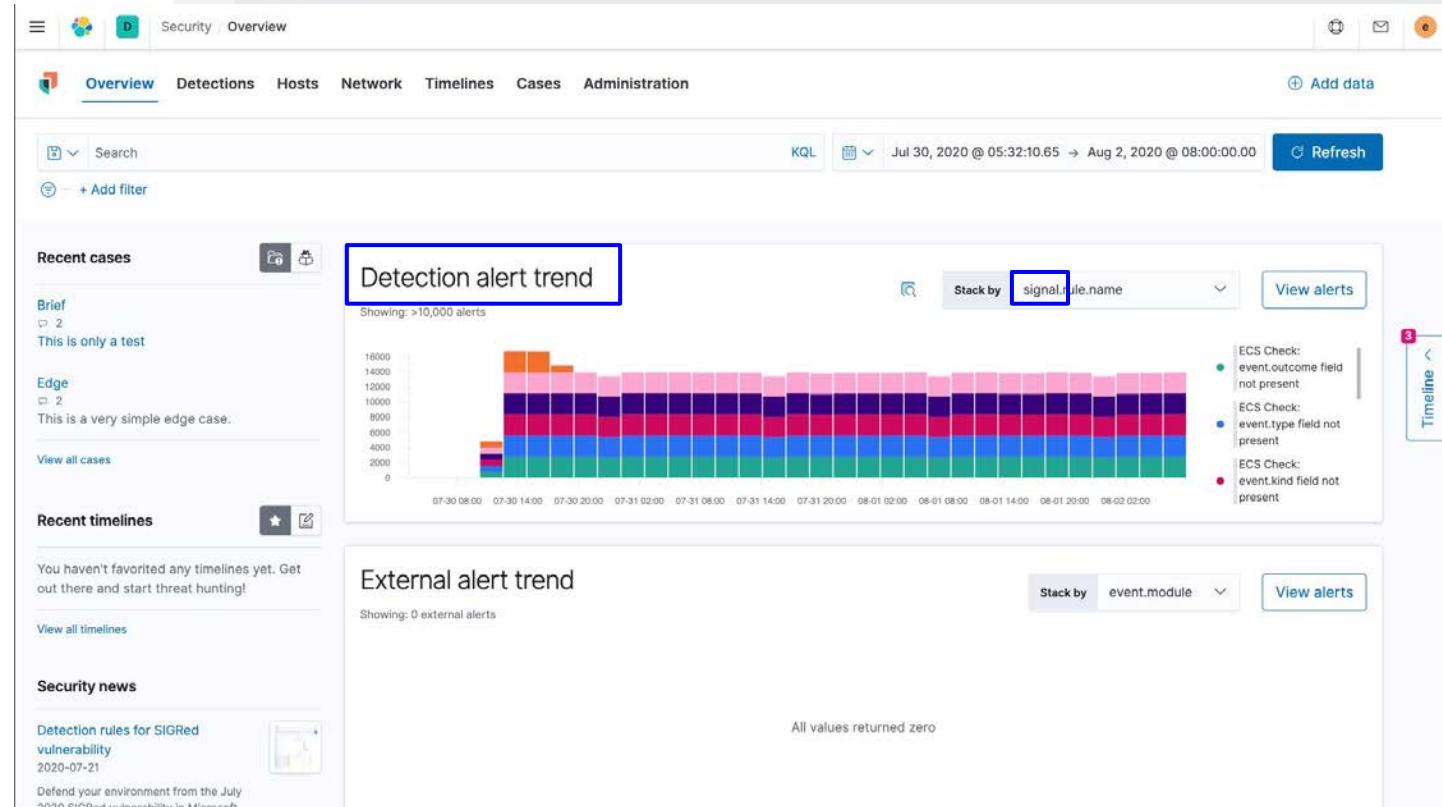
Primary Navigation still "Detections" - ties together detection rules and detection alerts for consistency.



Analyst Workflow Enhancements

- Signals now called Alerts
- Exceptions workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

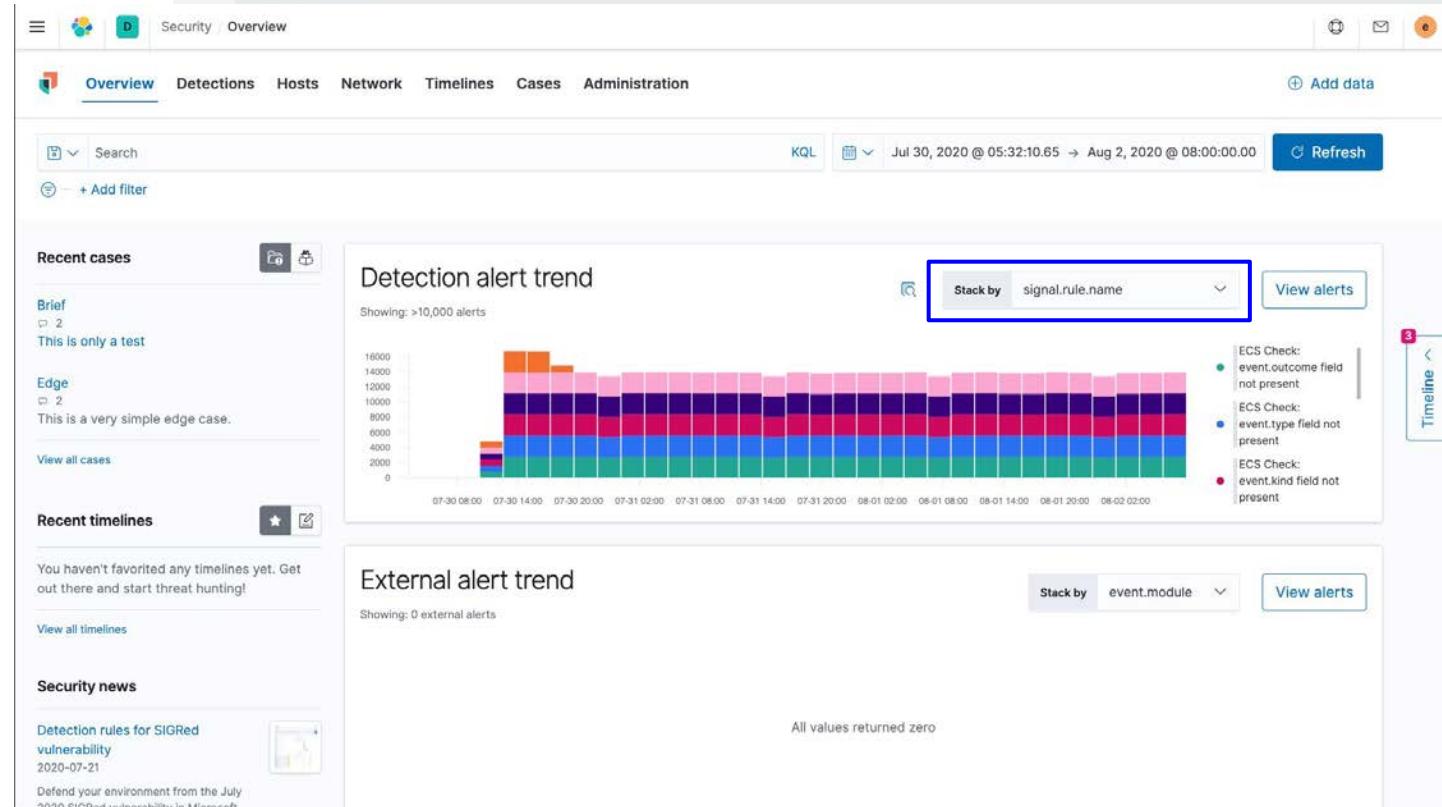
Underlying field names and indices still are called signals. E.g., .siem-signals- index pattern, signal.* field names.*



Analyst Workflow Enhancements

- Signals now called Alerts
- Exceptions workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Default histogram stacking is now by rule name. Note continued use of signal.rule.name here.



Analyst Workflow Enhancements

- Signals now called **Alerts**
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Rule details view now shows “Detection alerts” generated by this rule.

The screenshot shows the Elastic Stack interface with the 'Detections' tab selected. The main view displays a detection rule titled 'ECS Check: event.type field contains disallowed value'. The rule is set to 'Activate' and has 'Edit rule settings' and 'Timeline' buttons. The 'About' section provides details about the rule, including its purpose (to ensure the 'event.type' field is populated with allowed values), severity (High), risk score (21), reference URLs (link to ECS allowed values), and tags (ECS, Categorization). The 'Definition' section shows the index patterns (apm-* transaction*, auditbeat*, endpoint*, filebeat*, packetbeat*, winlogbeat*) and the custom query: `event.type:*` and not `event.type:access and not event.type:admin and not event.type:allowed and not event.type:change and not event.type:creation and not event.type:connection and not event.type:deletion and not event.type:denied and not event.type:end and not event.type:error and not event.type:info and not event.type:group and not event.type:installation and not event.type:protocol, and not event.type:start and not event.type:user`. The 'Rule type' is 'Query' and the 'Timeline template' is 'ECS Checker 1'. The 'Schedule' section shows the rule runs every 5m with an additional look-back time of 1m. At the bottom, there are tabs for 'Detection alerts', 'Exceptions', and 'Failure History', with 'Detection alerts' highlighted by a blue box.

Analyst Workflow Enhancements

- Signals now called Alerts
- **Exception workflows for detection engine and endpoint**
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

New in-app capability for adding exceptions to detection rules. Can be initiated right from Detection alerts table.

The screenshot shows the Elasticsearch 'Detections' interface. At the top, there are tabs for Overview, Detections (which is selected), Hosts, Network, Timelines, Cases, and Administration. Below the tabs, there are search and filter fields, and a timeline selector set from Jul 30, 2020 @ 05:32:10.65 to Aug 2, 2020 @ 08:00:00.00. A 'Refresh' button is also present.

The main area is titled 'Detection alerts' (BETA). It shows a 'Trend' chart with a legend for 'Stack by signal.rule.name'. The chart displays alert counts over time, with a significant spike on July 31st. A tooltip for the chart says 'Showing: >10,000 alerts'. The legend items are: ECS Check: event.outcome field not present (orange), ECS Check: event.type field not present (blue), and ECS Check: event.kind field not present (red).

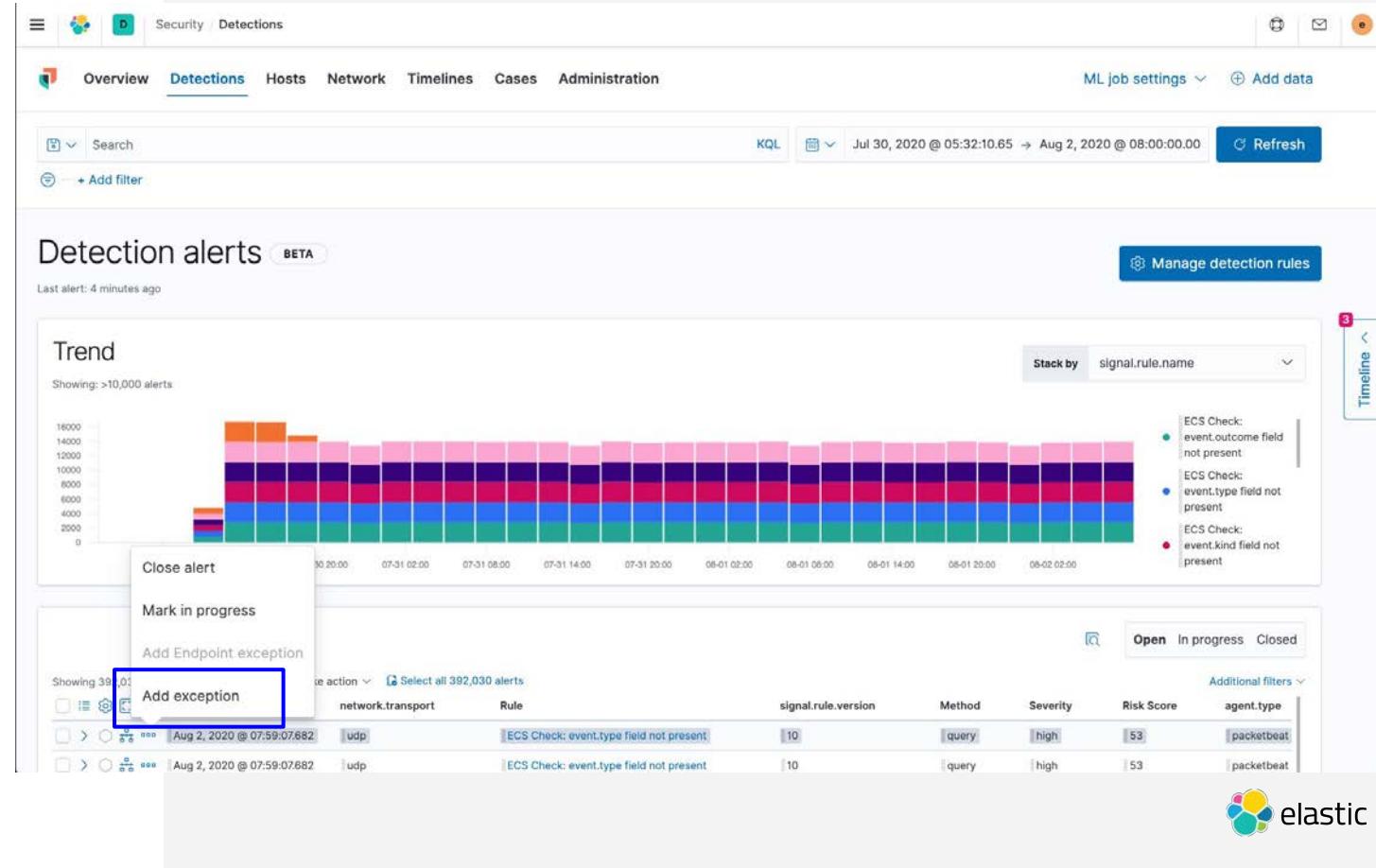
Below the chart, there are buttons for 'Close alert', 'Mark in progress', and 'Add Endpoint exception'. A blue box highlights the 'Add exception' button. The table below shows 392,030 alerts, with columns for action, network.transport, Rule, signal.rule.version, Method, Severity, Risk Score, and agent.type. The first two rows in the table are:

action	network.transport	Rule	signal.rule.version	Method	Severity	Risk Score	agent.type
Select all 392,030 alerts	network.transport	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

Analyst Workflow Enhancements

- Signals now called Alerts
- **Exception workflows for detection engine and endpoint**
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Note: Exceptions are applied to the "detection rule" that created this detection alert." Exceptions do not modify the rule logic.



The screenshot shows the Elasticsearch Detections interface. At the top, there are tabs for Overview, Detections (which is selected), Hosts, Network, Timelines, Cases, and Administration. Below the tabs, there are search and filter fields, and a time range from Jul 30, 2020 @ 05:32:10.65 to Aug 2, 2020 @ 08:00:00.00. A 'Refresh' button is also present.

The main area is titled 'Detection alerts' (BETA). It shows a 'Trend' chart with a legend for 'ECS Check' rules. The legend indicates:

- ECS Check: event.outcome field not present (green)
- ECS Check: event.type field not present (blue)
- ECS Check: event.kind field not present (red)

The chart shows a significant spike in alerts on July 31, 2020, around 20:00 UTC, with the green bar reaching approximately 15,000. Below the chart, there are buttons for 'Close alert', 'Mark in progress', and 'Add Endpoint exception'. A modal window is open, showing a table of alerts with the following data:

Action	Aug 2, 2020 @ 07:59:07.682	Aug 2, 2020 @ 07:59:07.682	Rule	Method	Severity	Risk Score	agent.type	
Open	1	1	network.transport	signal.rule.version	query	high	53	packetbeat
In progress	0	0	network.transport	signal.rule.version	query	high	53	packetbeat
Closed	0	0	network.transport	signal.rule.version	query	high	53	packetbeat

Additional filters and a timeline sidebar are visible on the right.

Analyst Workflow Enhancements

- Signals now called Alerts
- **Exception workflows for detection engine and endpoint**
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Detection rule logic identifies “potential” detection alerts. Will become detection alerts EXCEPT when any exception condition matches.

Add Exception

ECS Check: event.type field not present

Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
host.name	is	Mikes-MacBook-Pro.local

AND OR Add nested condition

E I don't want to be generating a lot of detection alerts when I'm working on ECS development.

Close this alert

Close all alerts that match this exception, including alerts generated by other rules

Cancel Add Exception

Showing 382,030 alerts Selected Datasets Take action Select all 382,030 alerts

@timestamp	network.transport	Rule	signal.rule.version	Method	Severity	Risk Score	agent.type
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.683	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

Open In progress Closed Additional filters

elastic

Analyst Workflow Enhancements

- Signals now called Alerts
- **Exception workflows for detection engine and endpoint**
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Exception items are arranged in "OR of ANDs" configuration, similar to timeline query builder.

Add Exception

ECS Check: event.type field not present

Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
host.name	is	Mikes-MacBook-Pro.local

+ AND + OR Add nested condition

I don't want to be generating a lot of detection alerts when I'm working on ECS development.

Close this alert

Close all alerts that match this exception, including alerts generated by other rules

Cancel Add Exception

Showing 382,030 alerts Selected Datasets Take action Select all 382,030 alerts

@timestamp	network.transport	Rule	signal.rule.version	Method	Severity	Risk Score	agent.type
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.683	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

Timeline

elasticsearch

Analyst Workflow Enhancements

- Signals now called Alerts
- **Exception workflows for detection engine and endpoint**
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Rich commenting capability for analysts to document WHY the exception was created. Allows SOC manager reviews and helps recall why.

Add Exception

ECS Check: event.type field not present

Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
host.name	is	Mikes-MacBook-Pro.local

E I don't want to be generating a lot of detection alerts when I'm working on ECS development.

Close this alert

Close all alerts that match this exception, including alerts generated by other rules

Cancel

Showing 382,030 alerts Selected Datasets Take action

Time	Event Type	Rule	Signal Rule Version	Method	Severity	Risk Score	Agent Type
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.683	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

Timeline

Timeline

Open In progress Closed

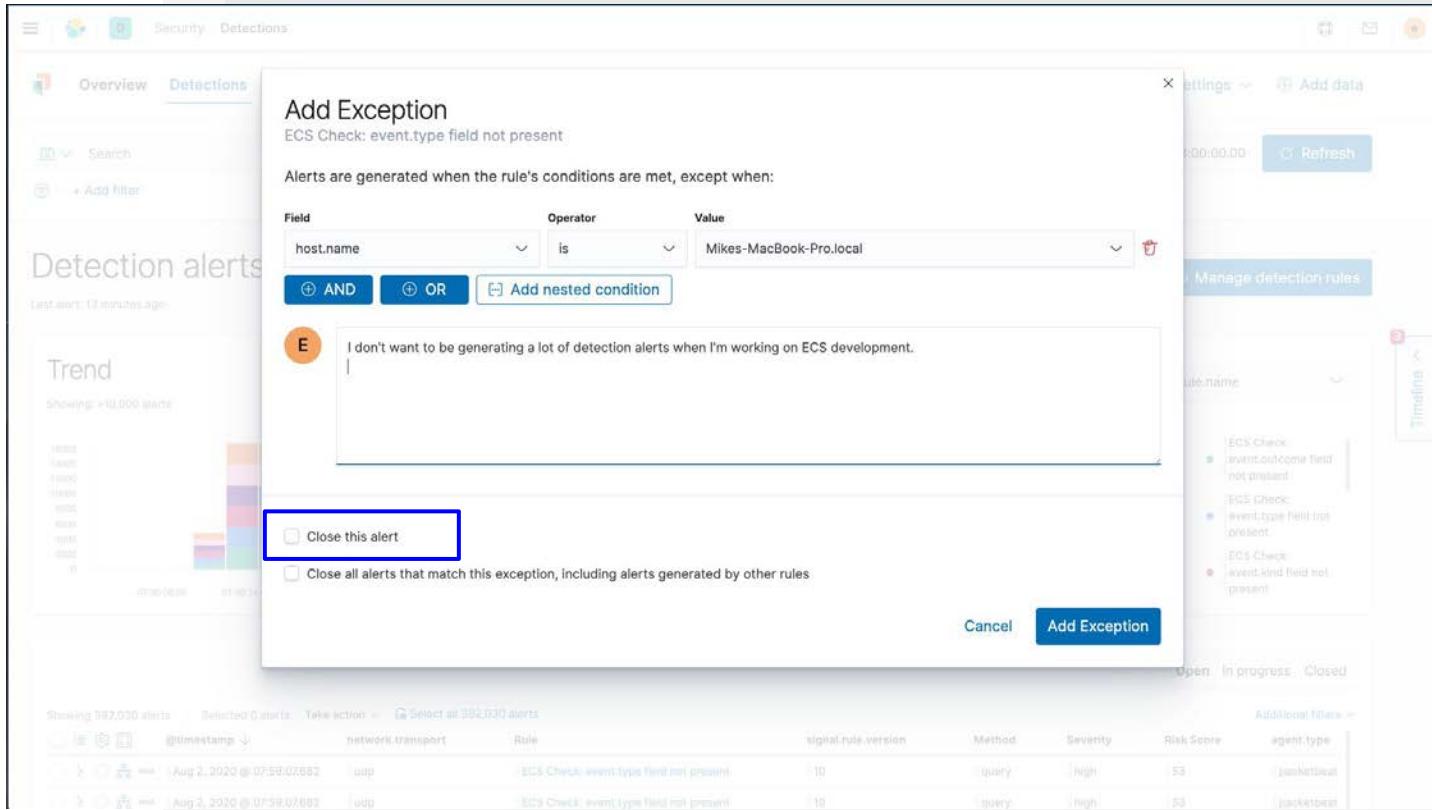
Additional filters

elastic

Analyst Workflow Enhancements

- Signals now called Alerts
- **Exception workflows for detection engine and endpoint**
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Detection alert can be closed automatically when exception is created.



Add Exception

ECS Check: event.type field not present

Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
host.name	is	Mikes-MacBook-Pro.local

E I don't want to be generating a lot of detection alerts when I'm working on ECS development.

Close this alert

Close all alerts that match this exception, including alerts generated by other rules

Cancel

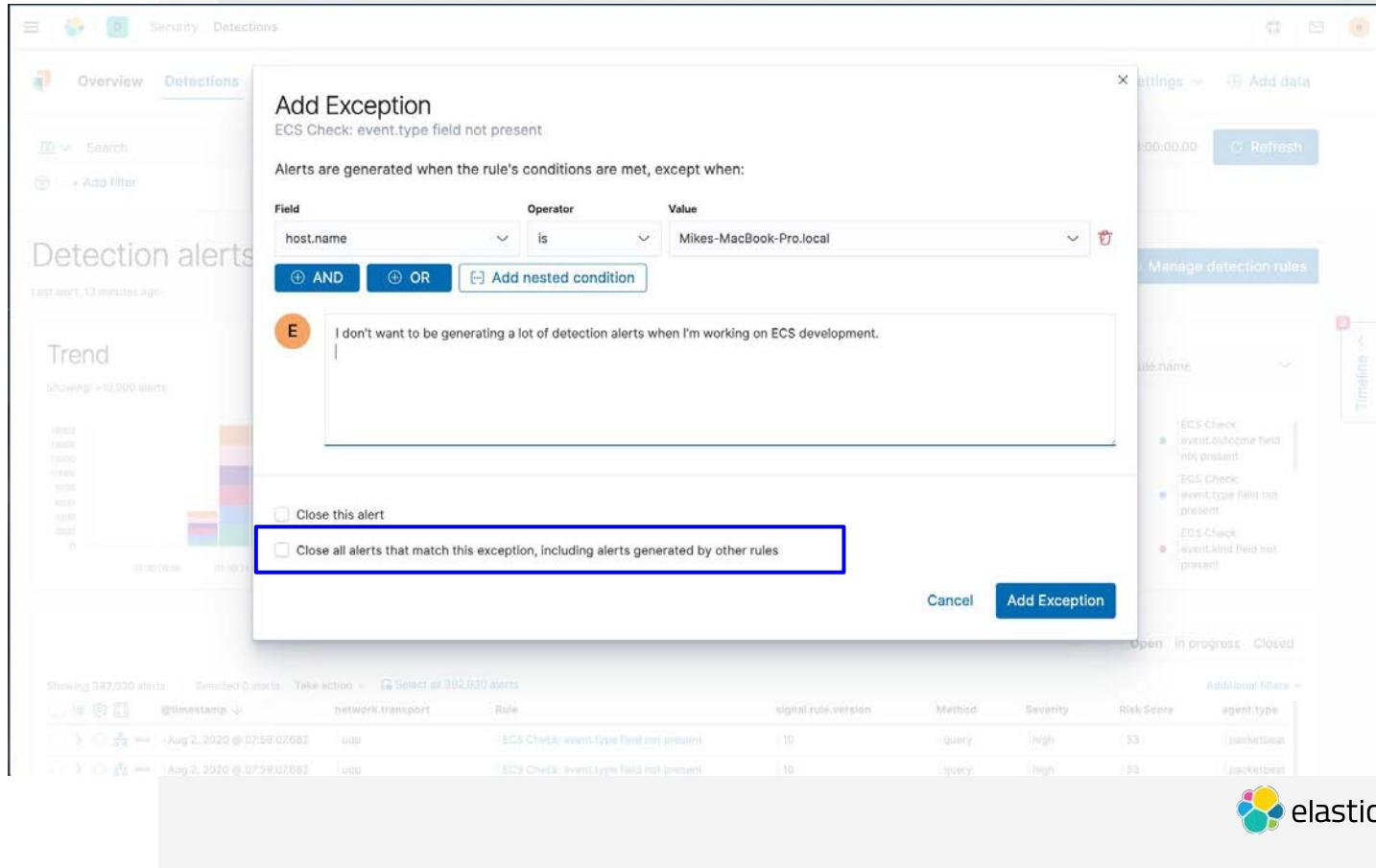
Showing 382,030 alerts Selected Datasets Take action

Time	Event Type	Rule	Signal Rule Version	Method	Severity	Risk Score	Agent Type
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.683	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

Analyst Workflow Enhancements

- Signals now called Alerts
- **Exception workflows for detection engine and endpoint**
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Optionally, multiple detection alerts can be closed when exception is created. Note: this function extends to alerts from all rules.



Add Exception

ECS Check: event.type field not present

Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
host.name	is	Mikes-MacBook-Pro.local

E I don't want to be generating a lot of detection alerts when I'm working on ECS development.

Close this alert

Close all alerts that match this exception, including alerts generated by other rules

Cancel

Showing 382,030 alerts Selected Datasets Take action

Time	Event Type	Rule	Signal Rule Version	Method	Severity	Risk Score	Agent Type
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.683	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

Open In progress Closed Additional filters

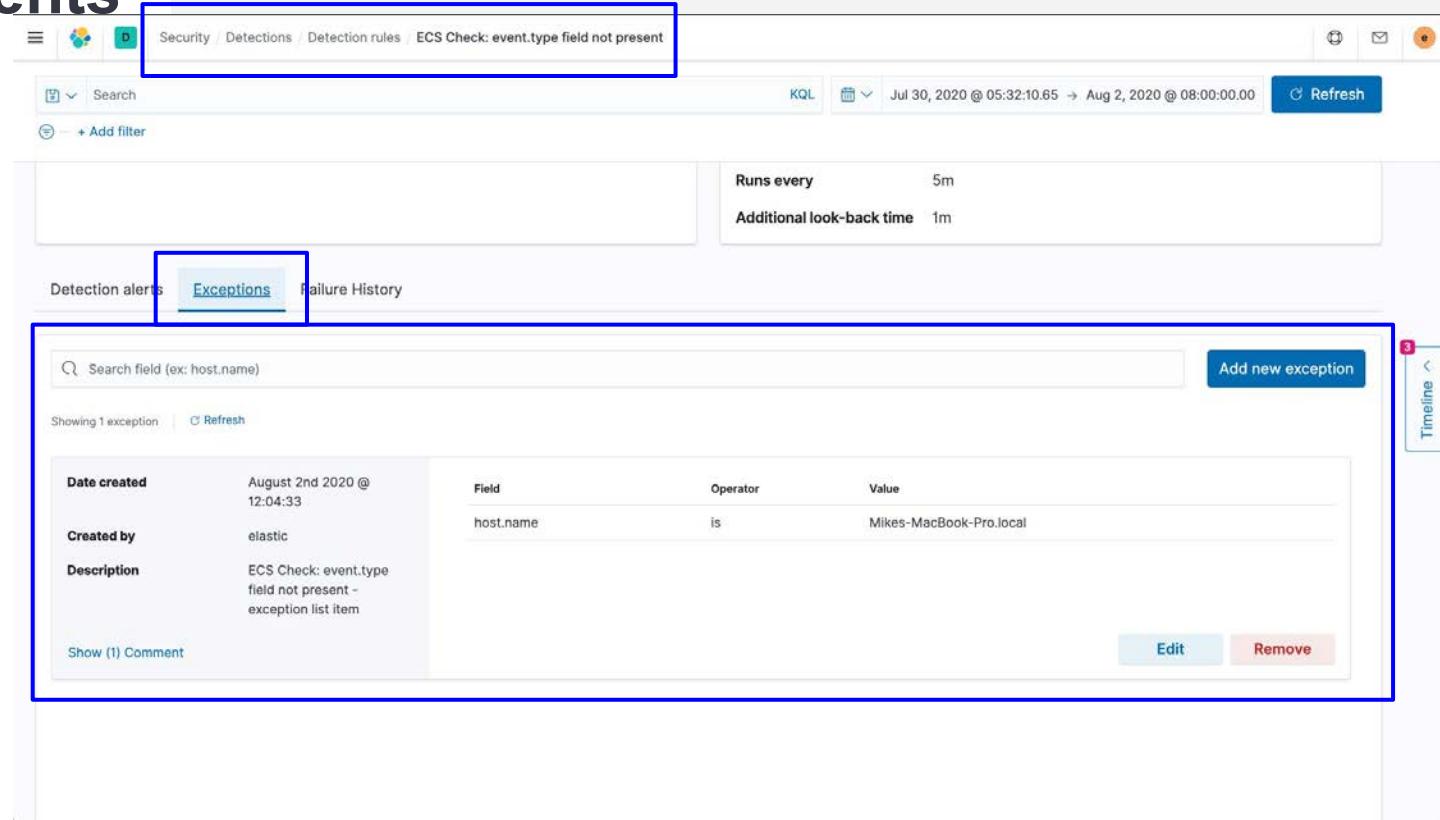
Timeline

elasticsearch

Analyst Workflow Enhancements

- Signals now called Alerts
- **Exception workflows for detection engine and endpoint**
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Exceptions tab in Detection Rule details view shows all exceptions applied to this rule. Can edit exception or add a new one from here.



The screenshot shows the Elasticsearch Detection Rules interface. A blue box highlights the top navigation bar where the title 'ECS Check: event.type field not present' is displayed. Another blue box highlights the 'Exceptions' tab in the navigation bar of the main content area. The main content area shows a table with one exception entry:

Date created	August 2nd 2020 @ 12:04:33	Field	Operator	Value
Created by	elastic	host.name	is	Mikes-MacBook-Pro.local
Description	ECS Check: event.type field not present - exception list item			

At the bottom right of the table, there are 'Edit' and 'Remove' buttons. The right side of the interface shows a vertical timeline and a sidebar with a 'Timeline' tab.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- **Value lists to support exceptions**
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Exceptions allow multiple KQL operators. We've added one new one, called "is in list."

Add Exception
ECS Check: event.type field not present

Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
host.name	is	Mikes-MacBook-Pro.local

E I don't want to be generating a lot of alerts when I'm working on ECS development.

Close this alert
 Close all alerts that match this exception, including alerts generated by other rules

Cancel Add Exception

Timeline

Open In progress Closed

Timestamp	Transport	Rule	signal.rule.version	Method	Severity	Risk Score	agent.type
Aug 2, 2020 @ 07:59:07.882	udp	ECS Check: event.type field not present	10	query	high	52	packetbeat
Aug 2, 2020 @ 07:59:07.882	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- **Value lists to support exceptions**
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

When "is in list" is chosen operator, available lists are shown. These lists are called "Value lists"

The screenshot shows the Elastic Stack interface with the 'Detections' tab selected. A modal dialog titled 'Add Exception' is open, with the condition 'ECS Check: event.type field not present' defined. The 'Value' field is set to 'is in list' and contains two entries: 'Value_List_Keyword_Zonefiles_Compromised_Domains.csv' and 'Value_List_Keyword_ECS_Field_Names.csv'. A tooltip 'E' explains: 'I don't want to be generating a lot of detection alerts when I'm working on ECS development.' Below the modal, a table lists 392,030 alerts, with the first two rows shown:

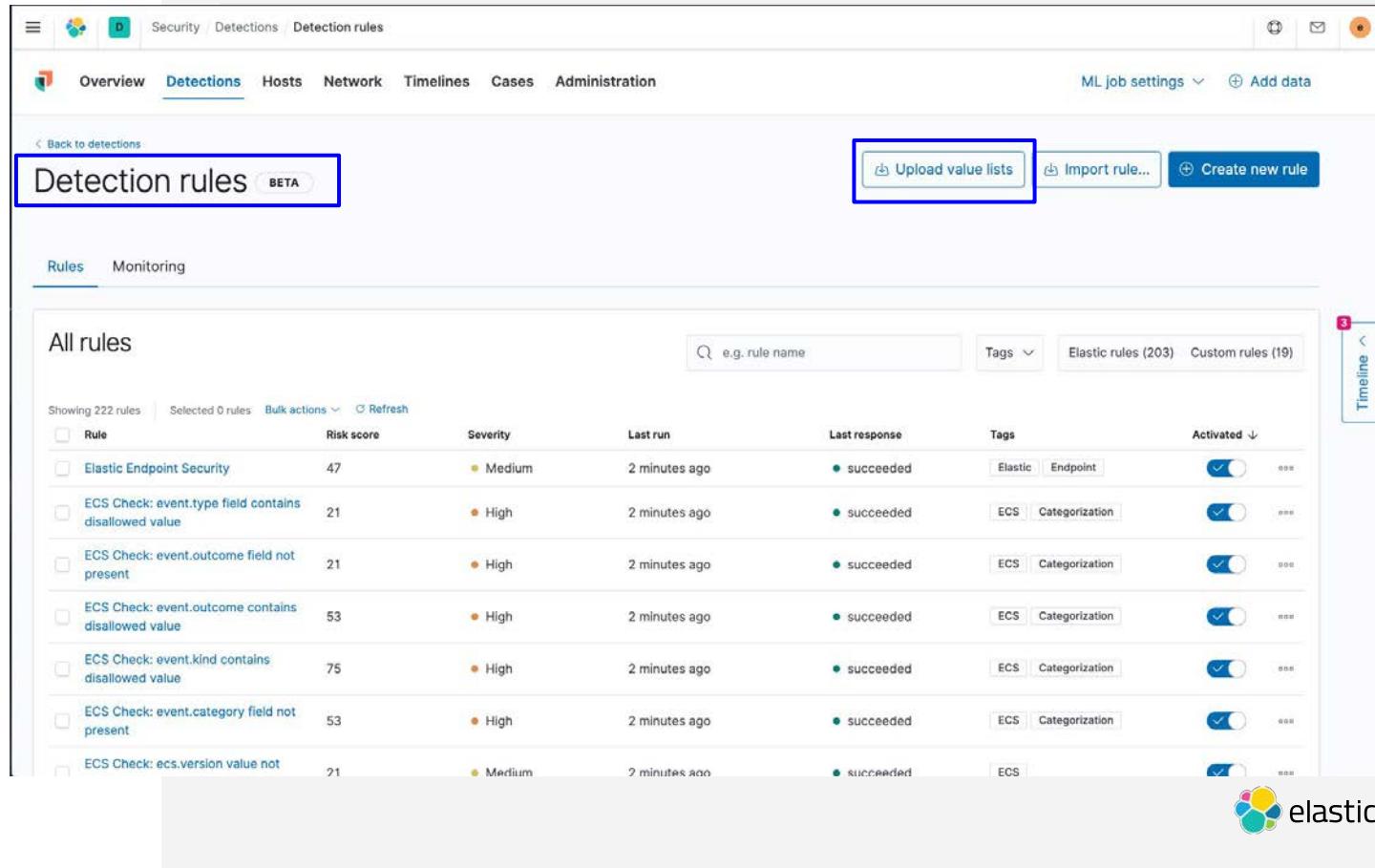
Selected	@timestamp	network.transport	Rule	signal.rule.version	Method	Severity	Risk Score	agent.type
	Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	52	packetbeat
	Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

The bottom right corner features the Elastic logo.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- **Value lists to support exceptions**
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Value lists can be added from the Detection rules page. You can upload a CSV file. Note: Value lists are stored in Elasticsearch indices.



The screenshot shows the 'Detection rules' page in the Elasticsearch interface. The top navigation bar includes 'Security', 'Detections', and 'Detection rules'. Below the navigation is a sub-navigation bar with 'Overview', 'Detections' (which is selected and highlighted in blue), 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. On the right side of the top bar are 'ML job settings', 'Add data', and three small icons. A blue box highlights the 'Upload value lists' button in the top right corner of the main content area. The main content area is titled 'Detection rules (BETA)' and contains tabs for 'Rules' (selected) and 'Monitoring'. Below this is a search bar with 'e.g. rule name' and a 'Refresh' button. A table lists 'All rules', showing 222 rules. The columns include 'Rule' (checkbox), 'Risk score', 'Severity' (color-coded), 'Last run', 'Last response' (green dot for succeeded), 'Tags' (Elastic, Endpoint), and 'Activated' (checkbox). The first few rows of the table are: 'Elastic Endpoint Security' (47, Medium, 2 minutes ago, succeeded, Elastic, Endpoint, activated), 'ECS Check: event.type field contains disallowed value' (21, High, 2 minutes ago, succeeded, ECS, Categorization, activated), 'ECS Check: event.outcome field not present' (21, High, 2 minutes ago, succeeded, ECS, Categorization, activated), 'ECS Check: event.outcome contains disallowed value' (53, High, 2 minutes ago, succeeded, ECS, Categorization, activated), 'ECS Check: event.kind contains disallowed value' (75, High, 2 minutes ago, succeeded, ECS, Categorization, activated), 'ECS Check: event.category field not present' (53, High, 2 minutes ago, succeeded, ECS, Categorization, activated), and 'ECS Check: ecs.version value not' (21, Medium, 2 minutes ago, succeeded, ECS, activated). A vertical sidebar on the right is titled 'Timeline' and shows a small '3' icon. The bottom right corner features the Elastic logo.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- **Value lists to support exceptions**
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Value lists are single value lists - i.e., one-column in a CSV file.

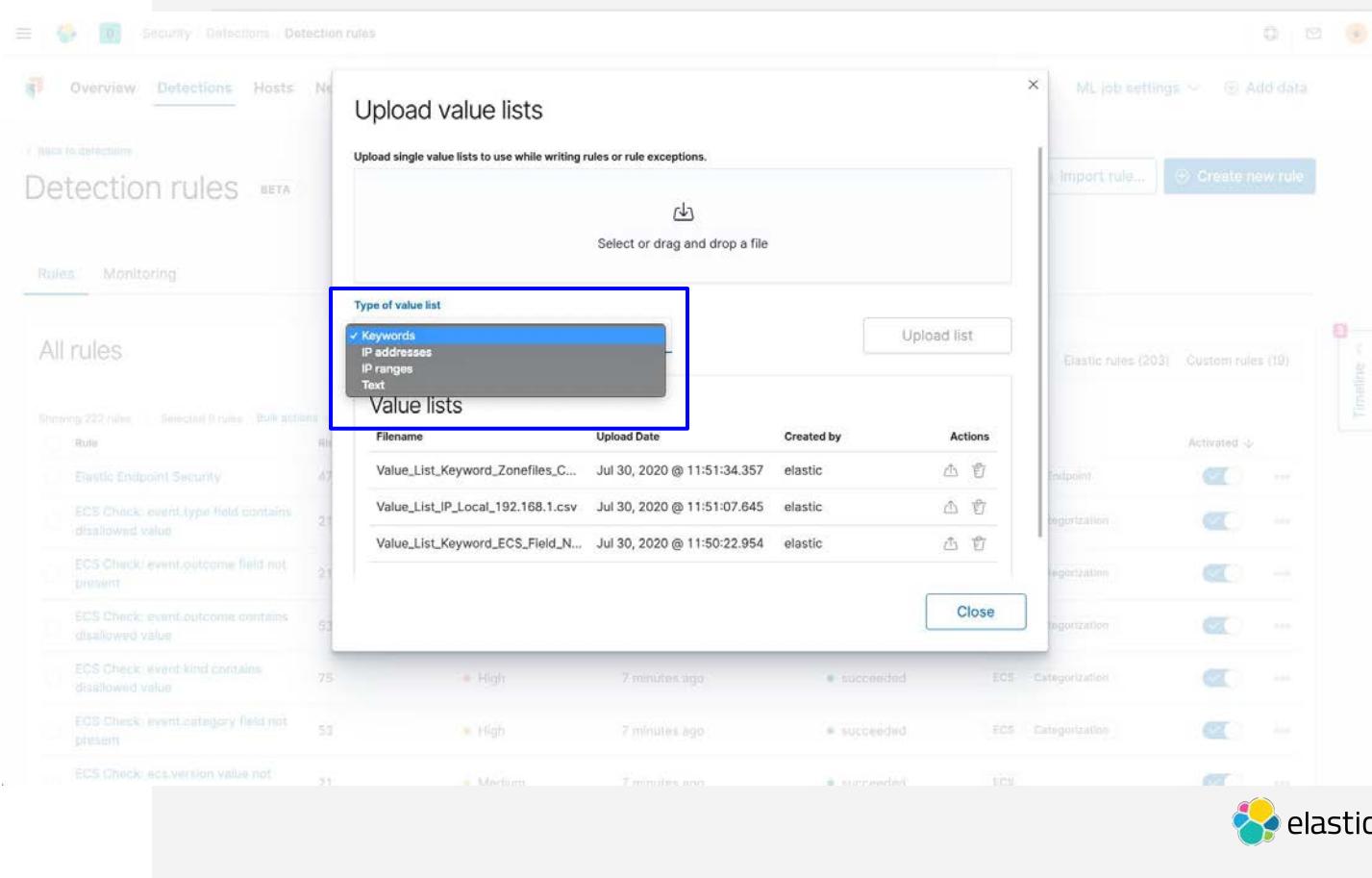
The screenshot shows the Elastic Detection rules interface. At the top, there are tabs for Overview, Detections, Hosts, and Rules (selected). Below this, a sub-menu for 'Detection rules' is open, showing 'Rules' and 'Monitoring'. The main area displays a table of 'All rules' with columns for Rule, Type, ID, and Actions. A modal window titled 'Upload value lists' is open, containing a text input field with the placeholder 'Upload single value lists to use while writing rules or rule exceptions.' and a 'Select or drag and drop a file' button. Below the modal, a table titled 'Value lists' shows three entries: 'Value_List_Keyword_Zoneflies_C...', 'Value_List_IP_Local_192.168.1.csv', and 'Value_List_Keyword_ECS_Field_N...'. The table has columns for 'Filename', 'Upload Date', 'Created by', and 'Actions'. The 'Actions' column for each entry includes a 'Download' and a 'Delete' icon. A 'Close' button is at the bottom right of the modal. The background shows the main interface with sections for 'Elastic rules (203)', 'Custom rules (18)', and 'Timeline'.

Filename	Upload Date	Created by	Actions
Value_List_Keyword_Zoneflies_C...	Jul 30, 2020 @ 11:51:34.357	elastic	
Value_List_IP_Local_192.168.1.csv	Jul 30, 2020 @ 11:51:07.645	elastic	
Value_List_Keyword_ECS_Field_N...	Jul 30, 2020 @ 11:50:22.954	elastic	

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- **Value lists to support exceptions**
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Four types of value lists are supported in 7.9, based on Elasticsearch datatypes: keywords, text, IP addresses, and IP ranges.



Upload value lists

Upload single value lists to use while writing rules or rule exceptions.

Select or drag and drop a file

Type of value list

- Keywords
- IP addresses
- IP ranges
- Text

Value lists

Filename	Upload Date	Created by	Actions
Value_List_Keyword_Zonefiles_C...	Jul 30, 2020 @ 11:51:34.357	elastic	Edit Delete
Value_List_IP_Local_192.168.1.csv	Jul 30, 2020 @ 11:51:07.645	elastic	Edit Delete
Value_List_Keyword_ECS_Field_N...	Jul 30, 2020 @ 11:50:22.954	elastic	Edit Delete

Close

ML job settings Add data

Import rule... Create new rule

Timeline

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- **Value lists to support exceptions**
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Upload file size is limited to 9 MB in 7.9. E.g., Zonefiles domain list 115,000 entries is only 2.4 MB.

Upload value lists

Upload single value lists to use while writing rules or rule exceptions.

9 MB MAX

Select or drag and drop a file

Type of value list

Keywords
IP addresses
IP ranges
Text

NOTE: ONLY KEYWORDS AND IP ADDRESSES SUPPORTED IN 7.9

Upload list

Filename	Upload Date	Created by	Actions
Value_List_Keyword_Zonefiles.C...	Jul 30, 2020 @ 11:51:34.357	elastic	Edit Delete
Value_List_IP_Local_192.168.1.csv	Jul 30, 2020 @ 11:51:07.645	elastic	Edit Delete
Value_List_Keyword_ECS_Field_N...	Jul 30, 2020 @ 11:50:22.954	elastic	Edit Delete

Close

Timeline

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- **New threshold rule type** and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

New Threshold rule uses Elasticsearch terms aggregation and generates detection alert when bucket size exceeds specified threshold.

The screenshot shows the 'Create new rule' interface in the Elasticsearch 'Detections' section. The 'Detections' tab is selected. The process is at step 1, 'Define rule'. Three options are shown: 'Custom query' (selected), 'Machine Learning', and 'Threshold'. The 'Threshold' option is highlighted with a blue box. Below the rule type are 'Index patterns' for various log types. The right side of the interface has a 'Timeline' sidebar with a '3' notification.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- **New threshold rule type** and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

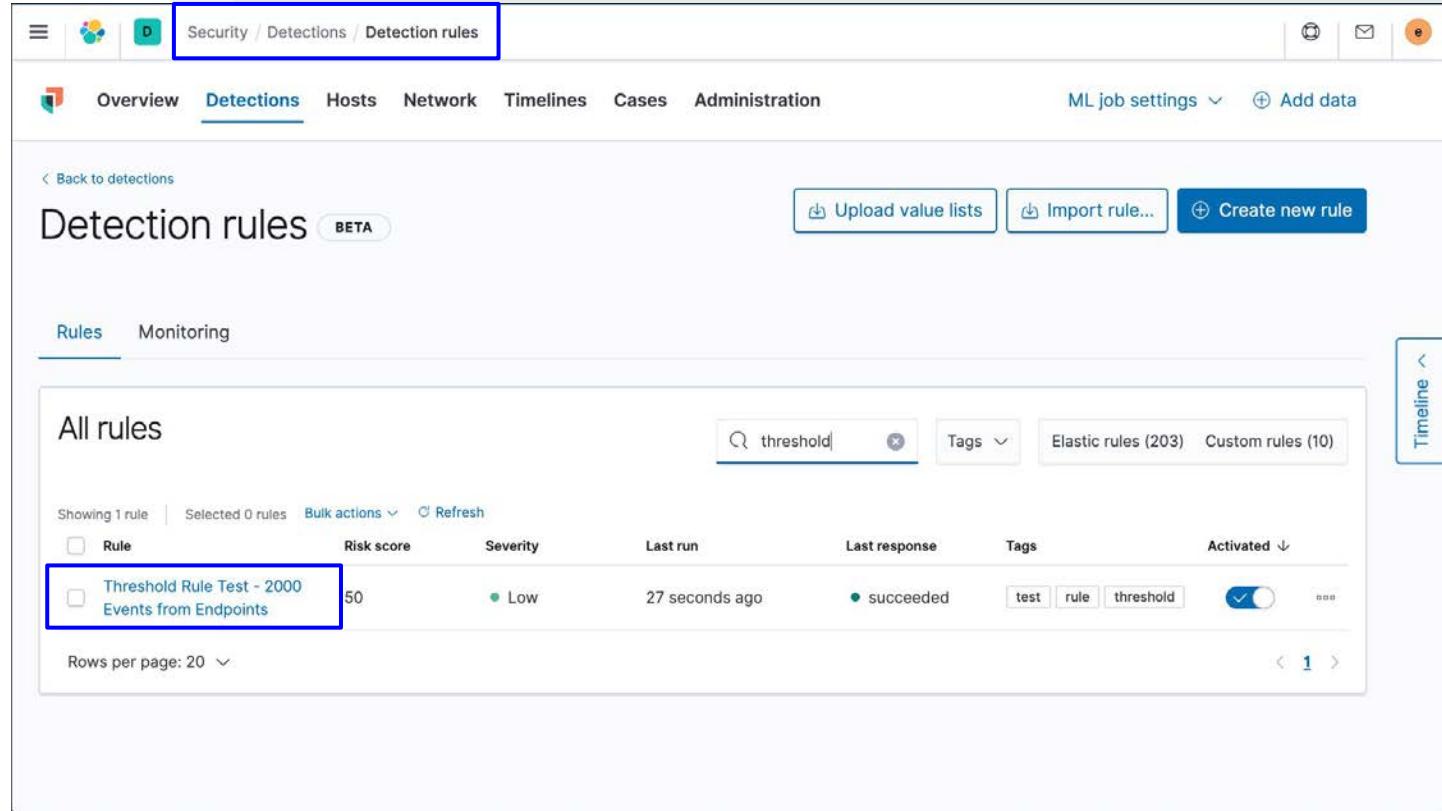
Similar to Custom query rule type, but can specify a field on which to perform terms aggregation, and threshold for number of matches.

Similar to Custom query rule type, but can specify a field on which to perform terms aggregation, and threshold for number of matches.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- **New threshold rule type** and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Example: threshold rule to detect any host from which we've received 2000 or more endpoint events (not alerts) in the past 24 hours.



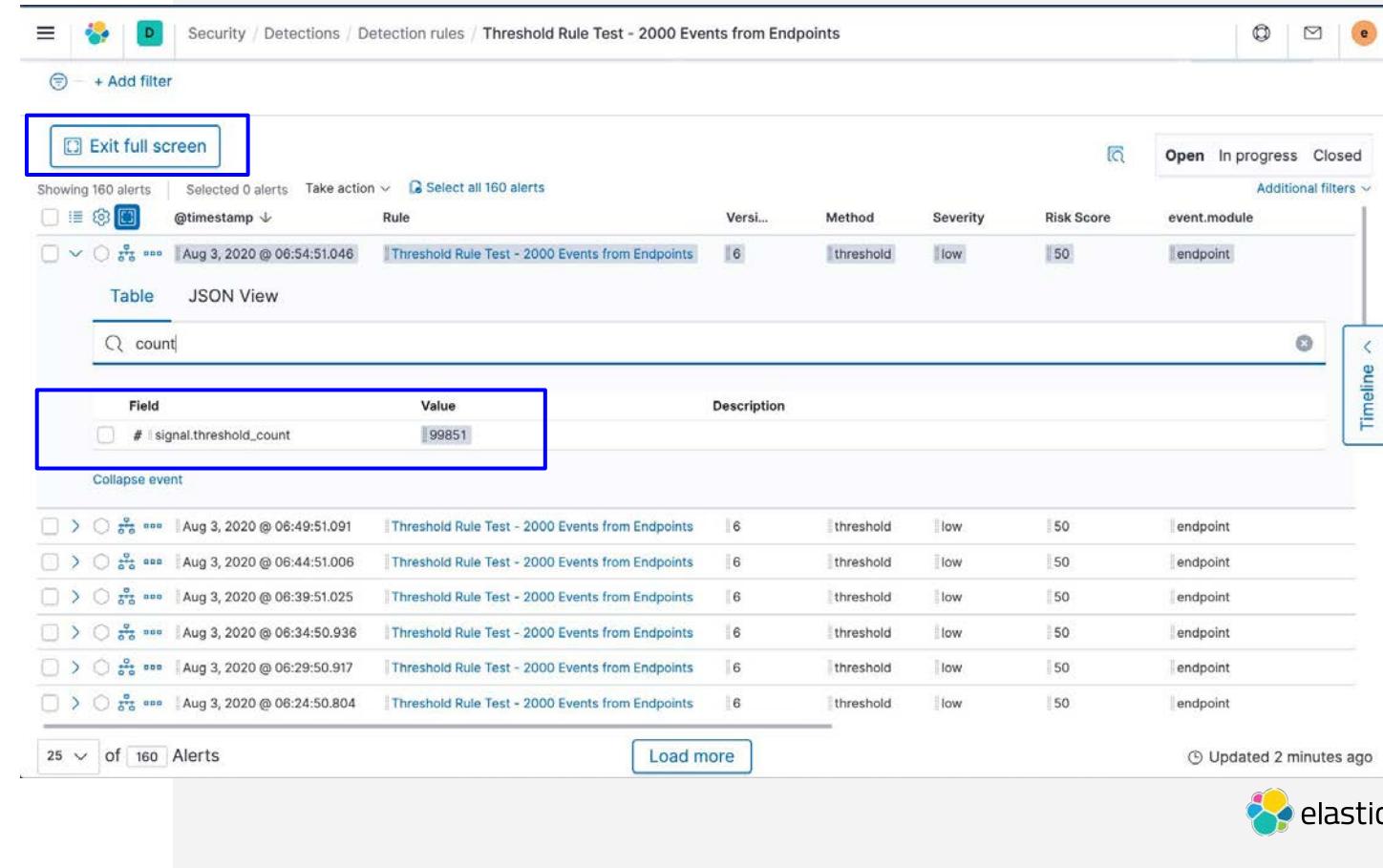
The screenshot shows the 'Detection rules' page in the Elastic Security interface. The top navigation bar includes 'Security / Detections / Detection rules'. Below the navigation is a header with tabs: 'Overview', 'Detections' (which is selected and highlighted in blue), 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. To the right of the tabs are 'ML job settings' and an 'Add data' button. Below the header, there are buttons for 'Upload value lists', 'Import rule...', and 'Create new rule'. The main content area is titled 'Detection rules' with a 'BETA' badge. It has two tabs: 'Rules' (selected) and 'Monitoring'. The 'All rules' section shows a single rule: 'Threshold Rule Test - 2000 Events from Endpoints'. This rule is highlighted with a blue box. The table for this rule includes columns for 'Rule' (checkbox), 'Risk score' (50), 'Severity' (Low), 'Last run' (27 seconds ago), 'Last response' (succeeded), 'Tags' (test, rule, threshold), and 'Activated' (switch is turned on). The bottom of the table shows 'Rows per page: 20' and navigation arrows. A vertical 'Timeline' sidebar is visible on the right.

Rule	Risk score	Severity	Last run	Last response	Tags	Activated
<input type="checkbox"/> Threshold Rule Test - 2000 Events from Endpoints	50	Low	27 seconds ago	succeeded	test rule threshold	<input checked="" type="checkbox"/>

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- **New threshold rule type** and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Detection alert contains new field signal.threshold_count, which contains actual number of events from this host. Note full screen!!



Security / Detections / Detection rules / Threshold Rule Test - 2000 Events from Endpoints

+ Add filter

Showing 160 alerts | Selected 0 alerts | Take action | Select all 160 alerts

Rule	Ver...	Method	Severity	Risk Score	event.module
Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low	50	endpoint

Table JSON View

count

Field	Value	Description
# signal.threshold_count	99851	

Collapse event

Aug 3, 2020 @ 06:49:51.091	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low	50	endpoint
Aug 3, 2020 @ 06:44:51.006	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low	50	endpoint
Aug 3, 2020 @ 06:39:51.025	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low	50	endpoint
Aug 3, 2020 @ 06:34:50.936	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low	50	endpoint
Aug 3, 2020 @ 06:29:50.917	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low	50	endpoint
Aug 3, 2020 @ 06:24:50.804	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low	50	endpoint

25 of 160 Alerts

Load more

Updated 2 minutes ago

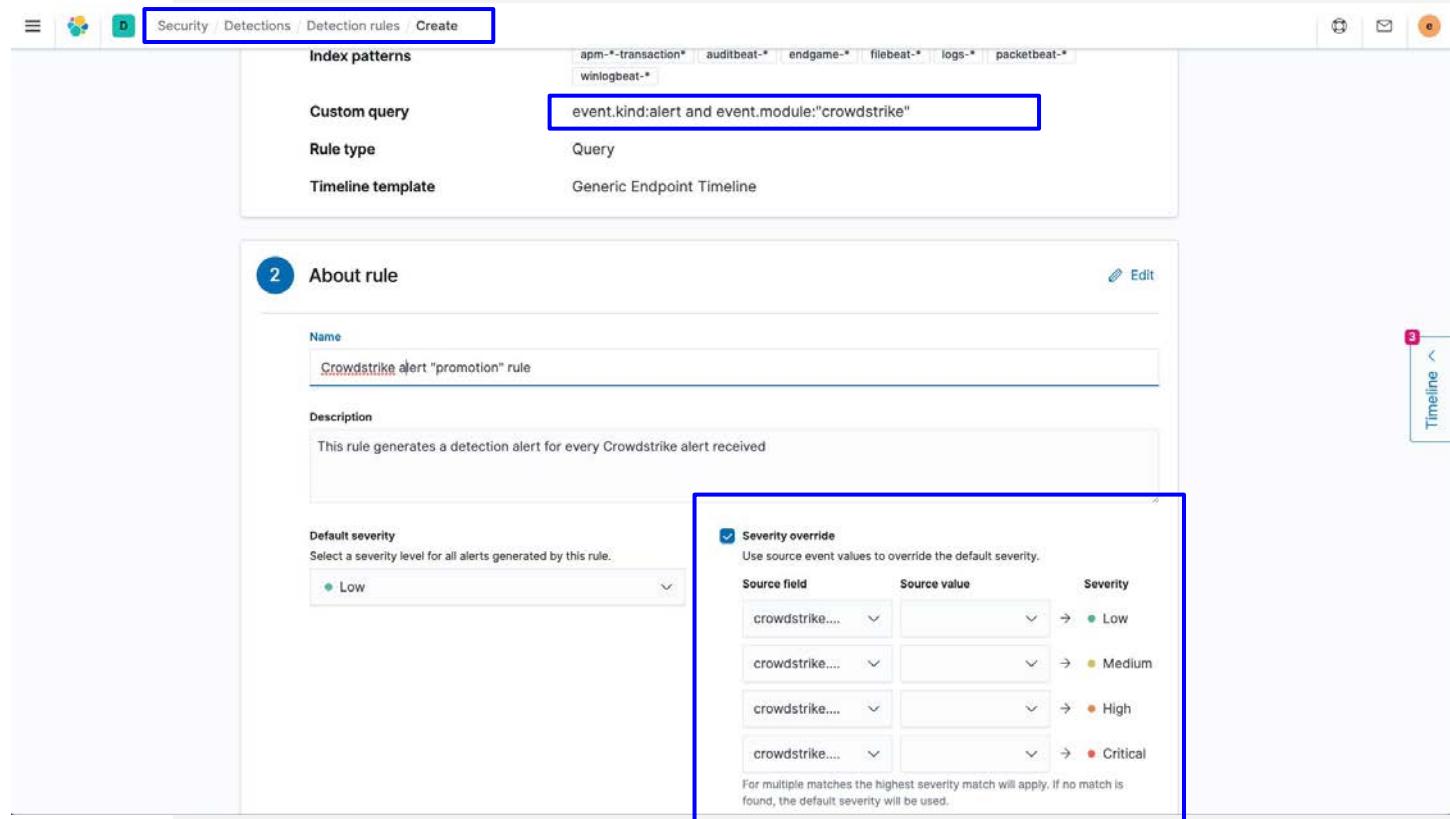
Timeline

elasticsearch

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation**
- **enhancements in detection engine**
- Timeline new templates, performance improvements, and full-screen displays

Severity override setting uses a value derived from the source event to populate the severity of the detection alert.



The screenshot shows the Elasticsearch Security interface for creating a detection rule. The top navigation bar includes 'Security', 'Detections', 'Detection rules', and 'Create'. The 'Create' button is highlighted with a blue box. The main configuration area includes:

- Index patterns:** 'apm-*-transaction*', 'auditbeat-*', 'endgame-*', 'filebeat-*', 'logs-*', 'packetbeat-*', 'winlogbeat-*'. A specific pattern 'event.kind:alert and event.module:"crowdstrike"' is highlighted with a blue box.
- Custom query:** 'event.kind:alert and event.module:"crowdstrike"'
- Rule type:** 'Query'
- Timeline template:** 'Generic Endpoint Timeline'

Below this, the 'About rule' section (step 2) is shown:

- Name:** 'Crowdstrike alert "promotion" rule'
- Description:** 'This rule generates a detection alert for every CrowdStrike alert received'
- Default severity:** 'Low' (selected)
- Severity override:** A table for mapping source event fields to detection alert severities. The table is highlighted with a blue box and contains the following data:

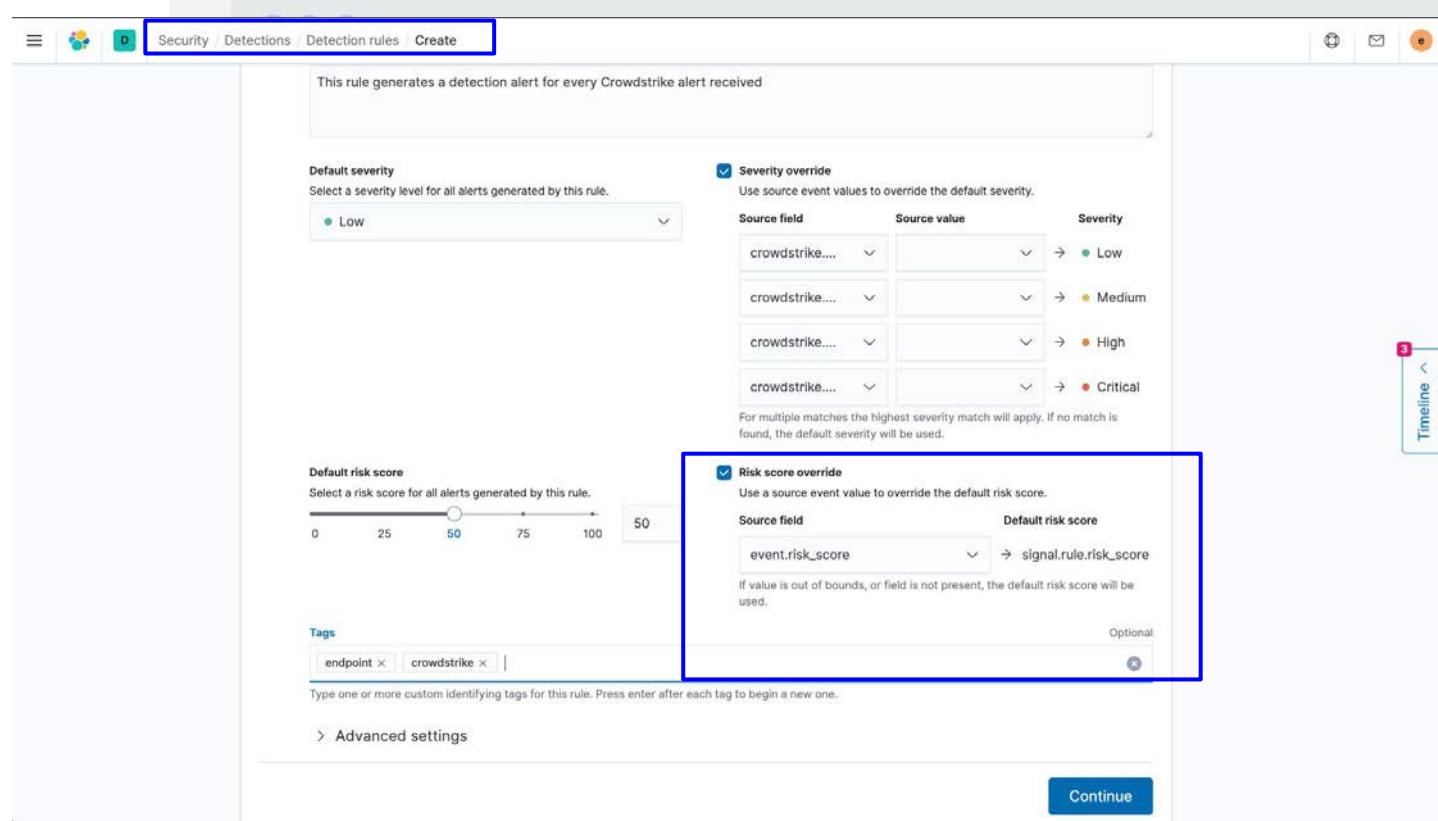
Source field	Source value	Severity
crowdstrike....		Low
crowdstrike....		Medium
crowdstrike....		High
crowdstrike....		Critical

For multiple matches the highest severity match will apply. If no match is found, the default severity will be used.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation enhancements in detection engine**
- Timeline new templates, performance improvements, and full-screen displays

Risk_score override setting uses a value directly from the source event to populate the risk_score of the detection alert.

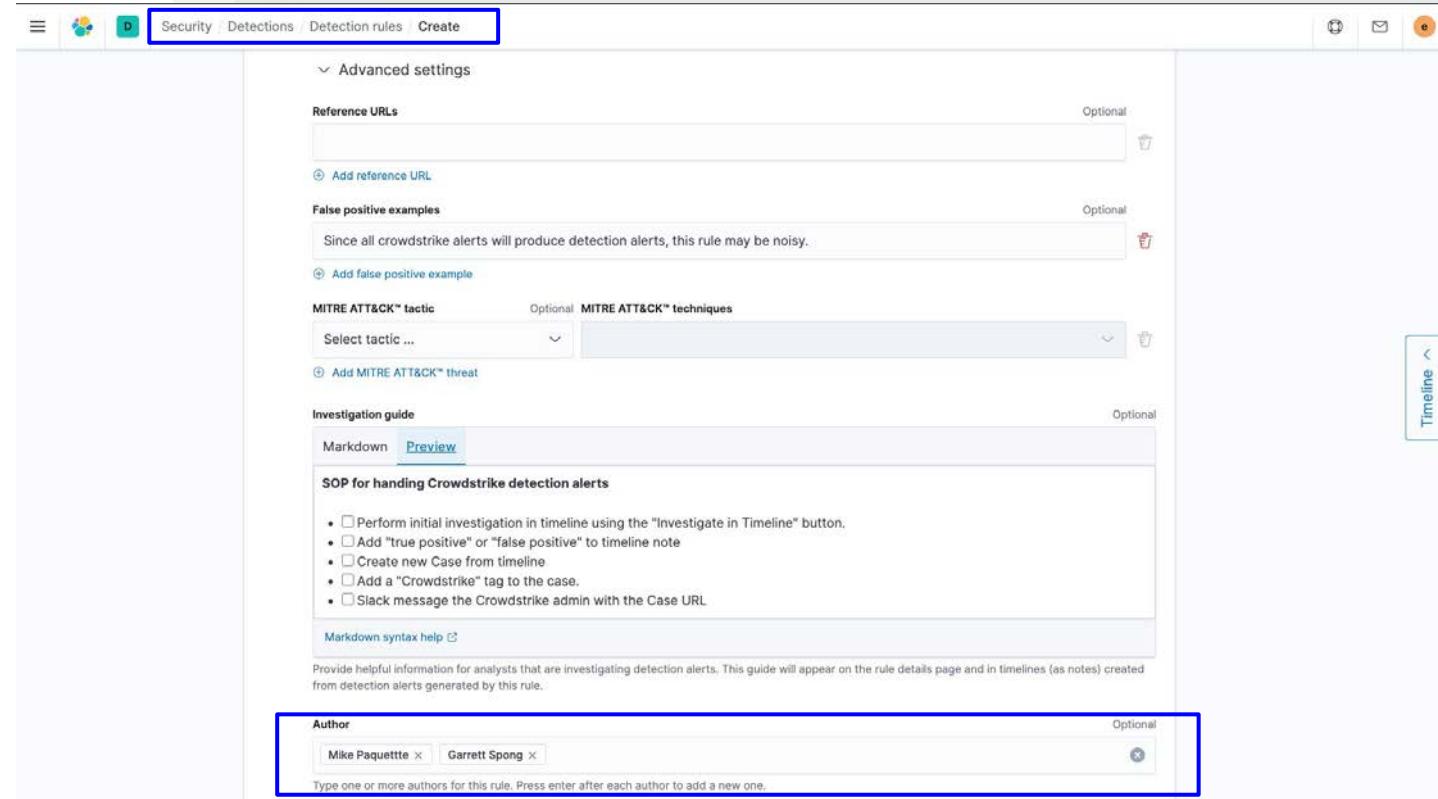


The screenshot shows the 'Create' tab in the Elastic Security interface. The 'Security' tab is highlighted with a blue border. The main content area displays a rule configuration for generating detection alerts from CrowdStrike alerts. It includes sections for 'Default severity' (set to 'Low') and 'Severity override' (using source event values to override the default severity for CrowdStrike alerts, with options for 'Low', 'Medium', 'High', and 'Critical'). Below these is a 'Default risk score' slider set to 50, and a 'Risk score override' section (also using source event values to override the default risk score, with a source field of 'event.risk_score' mapped to 'signal.rule.risk_score'). The 'Tags' section contains 'endpoint' and 'crowdstrike'. A 'Continue' button is at the bottom right. A blue box highlights the 'Risk score override' section.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation enhancements in detection engine**
- Timeline new templates, performance improvements, and full-screen displays

Optional "author" field allows listing all authors. Proper attribution is expected in community rule sharing.

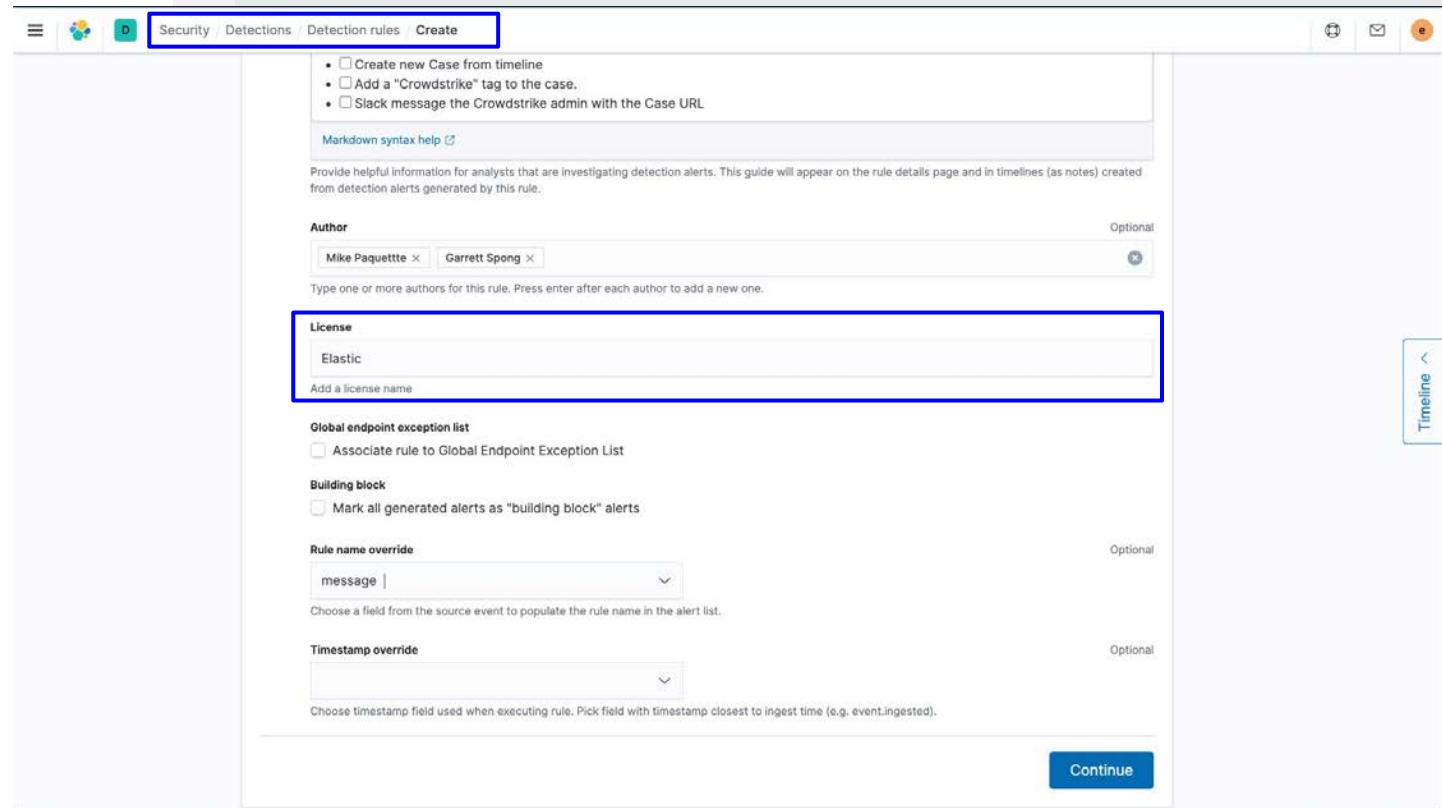


The screenshot shows the 'Create' tab selected in the navigation bar. The interface includes sections for 'Advanced settings', 'Reference URLs' (optional), 'False positive examples' (optional), 'MITRE ATT&CK™ tactic' (optional), 'MITRE ATT&CK™ techniques' (optional), 'Investigation guide' (optional), and an 'Author' field (optional). The 'Investigation guide' section contains an 'SOP for handling Crowdstrike detection alerts' with a list of tasks and a 'Markdown syntax help' link. A note at the bottom of the guide section states: 'Provide helpful information for analysts that are investigating detection alerts. This guide will appear on the rule details page and in timelines (as notes) created from detection alerts generated by this rule.'

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation enhancements in detection engine**
- Timeline new templates, performance improvements, and full-screen displays

New "License" field in Advanced Settings allows specification of license under which this rule is published. E.g., Elastic, MIT, DRL.



The screenshot shows the 'Create' page for a detection rule in the CrowdStrike interface. The 'License' field is highlighted with a blue box. The page includes sections for 'Create new Case from timeline', 'Author' (with Mike Paquette and Garrett Spong listed), 'Optional' (Global endpoint exception list and Building block checkboxes), 'Rule name override' (set to 'message'), 'Optional' (Timestamp override dropdown), and a 'Continue' button.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation**
enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Check this box to cause exceptions to this rule to be pushed down to hosts running Elastic Endpoint Security.

Security
Detections
Detection rules
Create

- Create new Case from timeline
- Add a "CrowdStrike" tag to the case.
- Slack message the CrowdStrike admin with the Case URL

[Markdown syntax help](#)

Provide helpful information for analysts that are investigating detection alerts. This guide will appear on the rule details page and in timelines (as notes) created from detection alerts generated by this rule.

Author
Optional

Type one or more authors for this rule. Press enter after each author to add a new one.

License
Optional

Add a license name

Global endpoint exception list

Associate rule to Global Endpoint Exception List

Building block
Optional

Mark all generated alerts as "building block" alerts

Rule name override
Optional

Choose a field from the source event to populate the rule name in the alert list.

Timestamp override
Optional

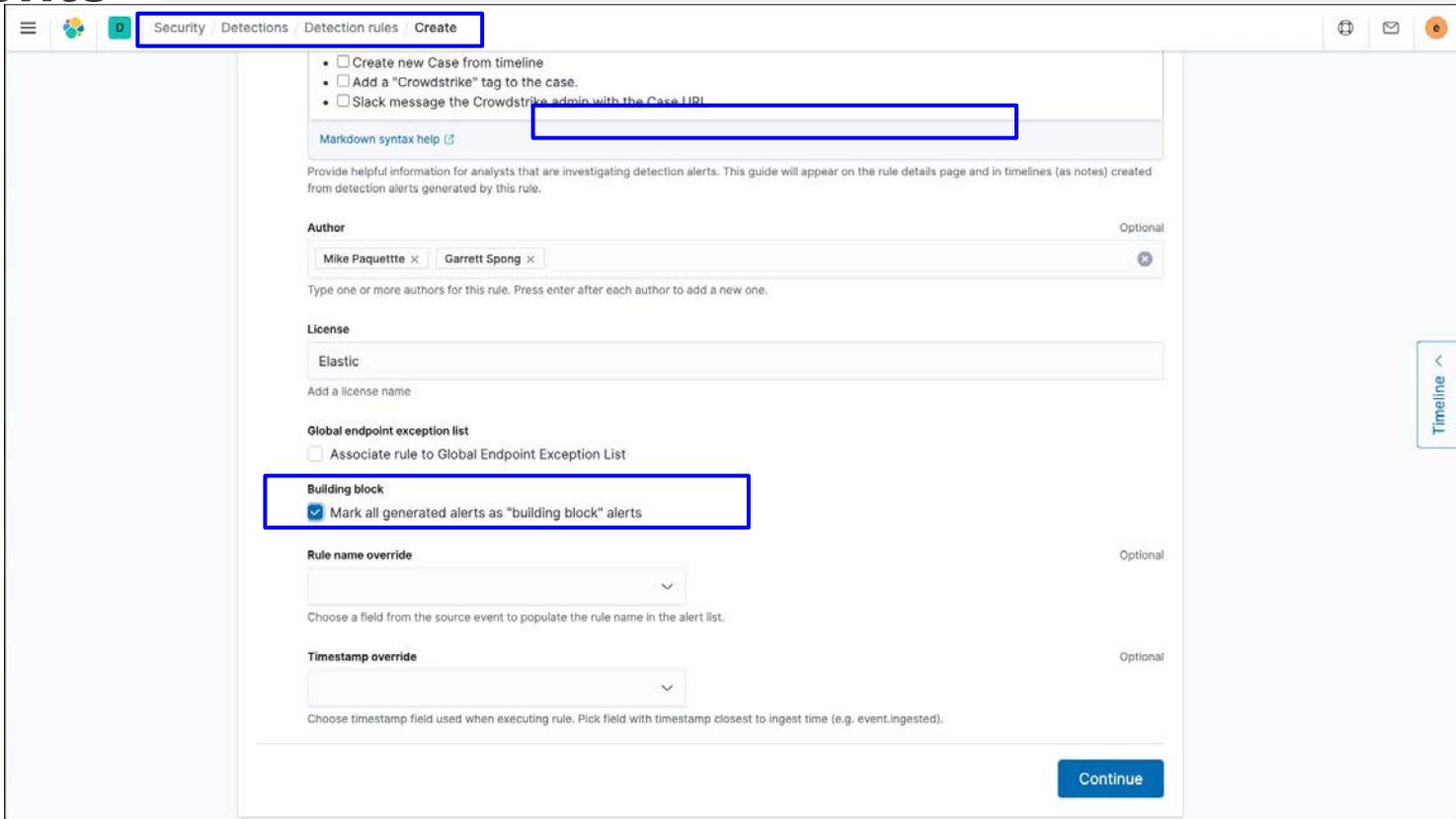
Choose timestamp field used when executing rule. Pick field with timestamp closest to ingest time (e.g. event.ingested).

Continue

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation enhancements in detection engine**
- Timeline new templates, performance improvements, and full-screen displays

Detection alerts created by "Building block" alerts will not appear in the detection alerts tables by default.



The screenshot shows the 'Create' page for a 'Detection rule' in the CrowdStrike interface. The top navigation bar includes 'Security', 'Detections', 'Detection rules', and 'Create'. The main content area is titled 'Create' and contains several configuration sections:

- Actions:** A list of checkboxes including 'Create new Case from timeline', 'Add a "Crowdstrike" tag to the case', and 'Slack message the Crowdstrike admin with the Case URL'. The third checkbox is currently selected.
- Markdown syntax help:** A link to help for using Markdown in notes.
- Author:** A section for entering authors, with 'Mike Paquette' and 'Garrett Spong' listed. A note says 'Type one or more authors for this rule. Press enter after each author to add a new one.'
- License:** A section for entering a license name, with 'Elastic' listed.
- Global endpoint exception list:** A checkbox for 'Associate rule to Global Endpoint Exception List'.
- Building block:** A section with a checkbox 'Mark all generated alerts as "building block" alerts'. This checkbox is selected and highlighted with a blue box.
- Rule name override:** A dropdown menu for selecting a field to override the rule name.
- Timestamp override:** A dropdown menu for selecting a timestamp field.

At the bottom right is a 'Continue' button. A vertical 'Timeline' sidebar is visible on the right edge of the interface.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation enhancements in detection engine**
- Timeline new templates, performance improvements, and full-screen displays

If necessary, can show building block detection alerts in detection alert table by enabling under "Additional filters"

The screenshot shows the Elasticsearch Security/Detections interface. At the top, there are navigation icons and a search bar. Below the search bar are buttons for 'KQL' and 'Last 24 hours', and a 'Show dates' button. A 'Refresh' button is also present. The main area is divided into two sections: 'Trend' and an 'Alerts' table.

Trend Section: This section displays a stacked bar chart titled 'Trend' showing the count of alerts over time. The chart is for 'signal.rule.name' and spans from 08-02 08:00 to 08-03 05:00. The legend indicates three ECS checks: 'event.outcome field not present' (green), 'event.category field not present' (blue), and 'event.kind field not present' (pink). The total count of alerts is shown as >10,000.

Alerts Table Section: This section shows a table of 112,799 alerts. The columns include: a checkbox, a timestamp, the event type ('network.transport'), the rule name ('rule'), and the signal rule version ('signal.rule.version'). The table also includes a 'Take action' dropdown and a 'Select all 112,799 alerts' button. A blue box highlights the 'Additional filters' section, which contains a checkbox for 'Include building block alerts'.

Bottom Right: The Elastic logo is located in the bottom right corner.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation enhancements in detection engine**
- Timeline new templates, performance improvements, and full-screen displays

Rule name override allows one detection rule to produce detection alerts with rule names specific to the source event. ECS message field typical.

The screenshot shows the 'Create' page for a detection rule. The top navigation bar includes 'Security', 'Detections', 'Detection rules', and 'Create'. The 'Create' tab is selected. The page contains the following sections:

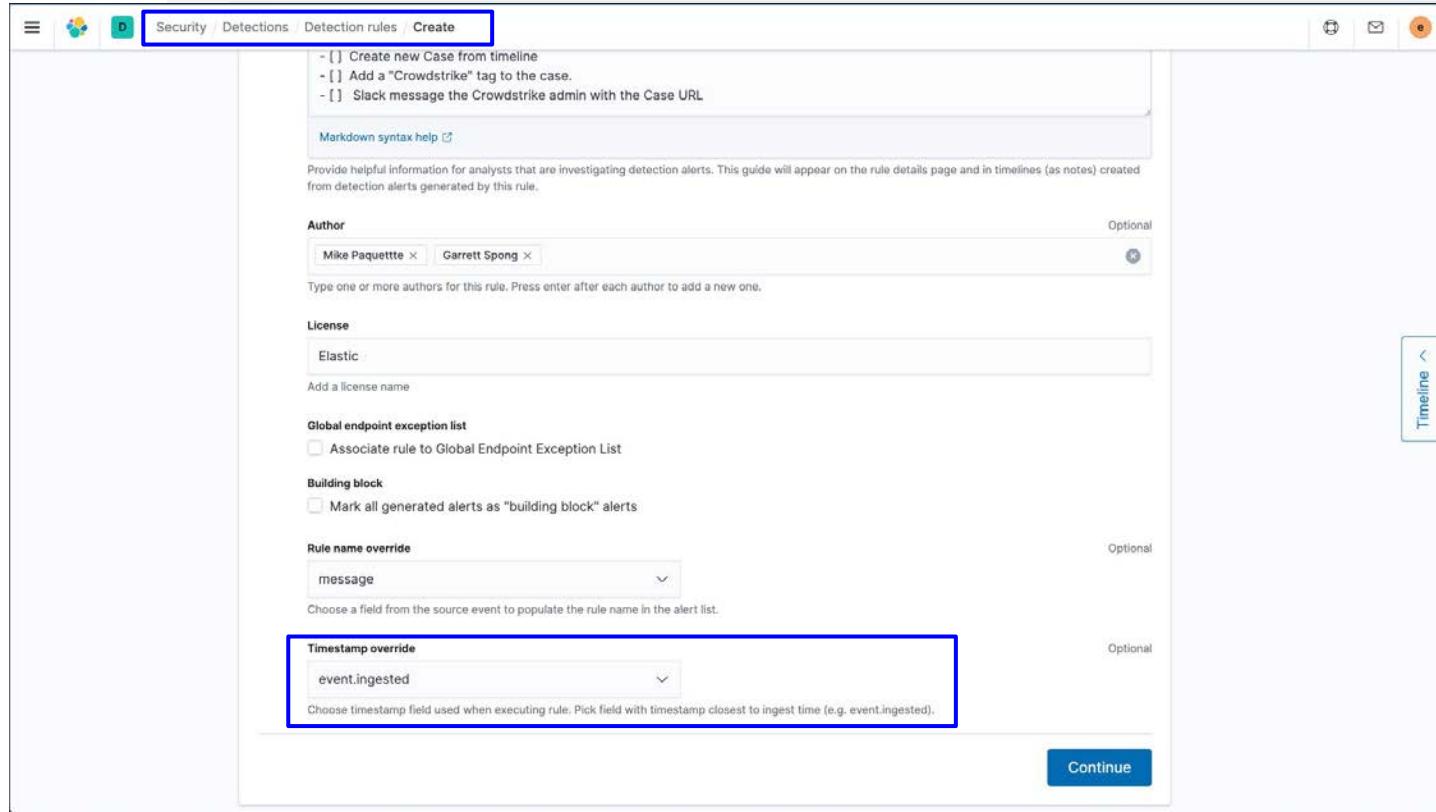
- Notes:** A list of checkboxes:
 - Create new Case from timeline
 - Add a "Crowdstrike" tag to the case.
 - Slack message the Crowdstrike admin with the Case URL
- Markdown syntax help:** A link to help for Markdown syntax.
- Author:** A field showing 'Mike Paquette' and 'Garrett Spong' with an 'Optional' label and a 'Timeline' sidebar.
- License:** A field showing 'Elastic' with an 'Optional' label and a 'Timeline' sidebar.
- Global endpoint exception list:** A checkbox for 'Associate rule to Global Endpoint Exception List'.
- Building block:** A checkbox for 'Mark all generated alerts as "building block" alerts'.
- Rule name override:** A field containing 'message' with a dropdown and an 'Optional' label. A note below says: 'Choose a field from the source event to populate the rule name in the alert list.'
- Timestamp override:** A field with a dropdown and an 'Optional' label. A note below says: 'Choose timestamp field used when executing rule. Pick field with timestamp closest to ingest time (e.g. event.ingested).'

A 'Continue' button is at the bottom right.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation enhancements in detection engine**
- Timeline new templates, performance improvements, and full-screen displays

Timestamp override causes rule execution to use specified timestamp. Useful for delayed events. ECS event.ingested typical.



The screenshot shows the CrowdStrike detection rule creation interface. The 'Create' tab is selected in the top navigation bar. The main area contains a list of actions: 'Create new Case from timeline', 'Add a "Crowdstrike" tag to the case.', and 'Slack message the Crowdstrike admin with the Case URL'. Below this is a 'Markdown syntax help' link. A note provides guidance for analysts investigating detection alerts. The 'Author' field is populated with 'Mike Paquette' and 'Garrett Spong'. The 'License' field is set to 'Elastic'. Under 'Global endpoint exception list', there is an unchecked checkbox for 'Associate rule to Global Endpoint Exception List'. Under 'Building block', there is an unchecked checkbox for 'Mark all generated alerts as "building block" alerts'. The 'Rule name override' field is set to 'message'. A note below it says 'Choose a field from the source event to populate the rule name in the alert list.' The 'Timestamp override' field is set to 'event.ingested'. A note below it says 'Choose timestamp field used when executing rule. Pick field with timestamp closest to ingest time (e.g. event.ingested)'. The 'Continue' button is located at the bottom right. A 'Timeline' sidebar is visible on the right edge of the interface.

Analyst Workflow Enhancements

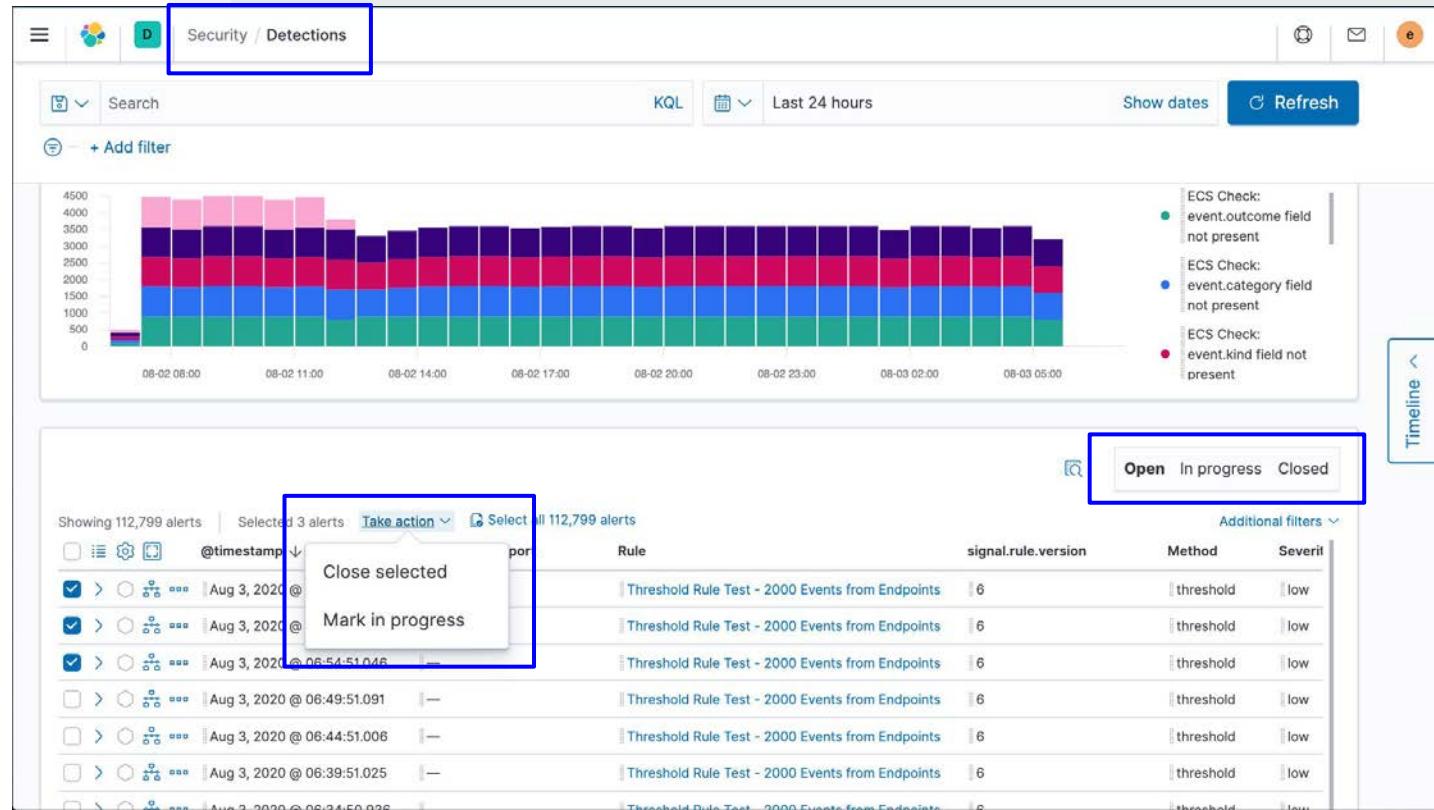
- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and **other rule creation**
enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Larger, multi-line query bar available during rule creation, allowing complete view of long or complex queries. Rule authors rejoice!

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

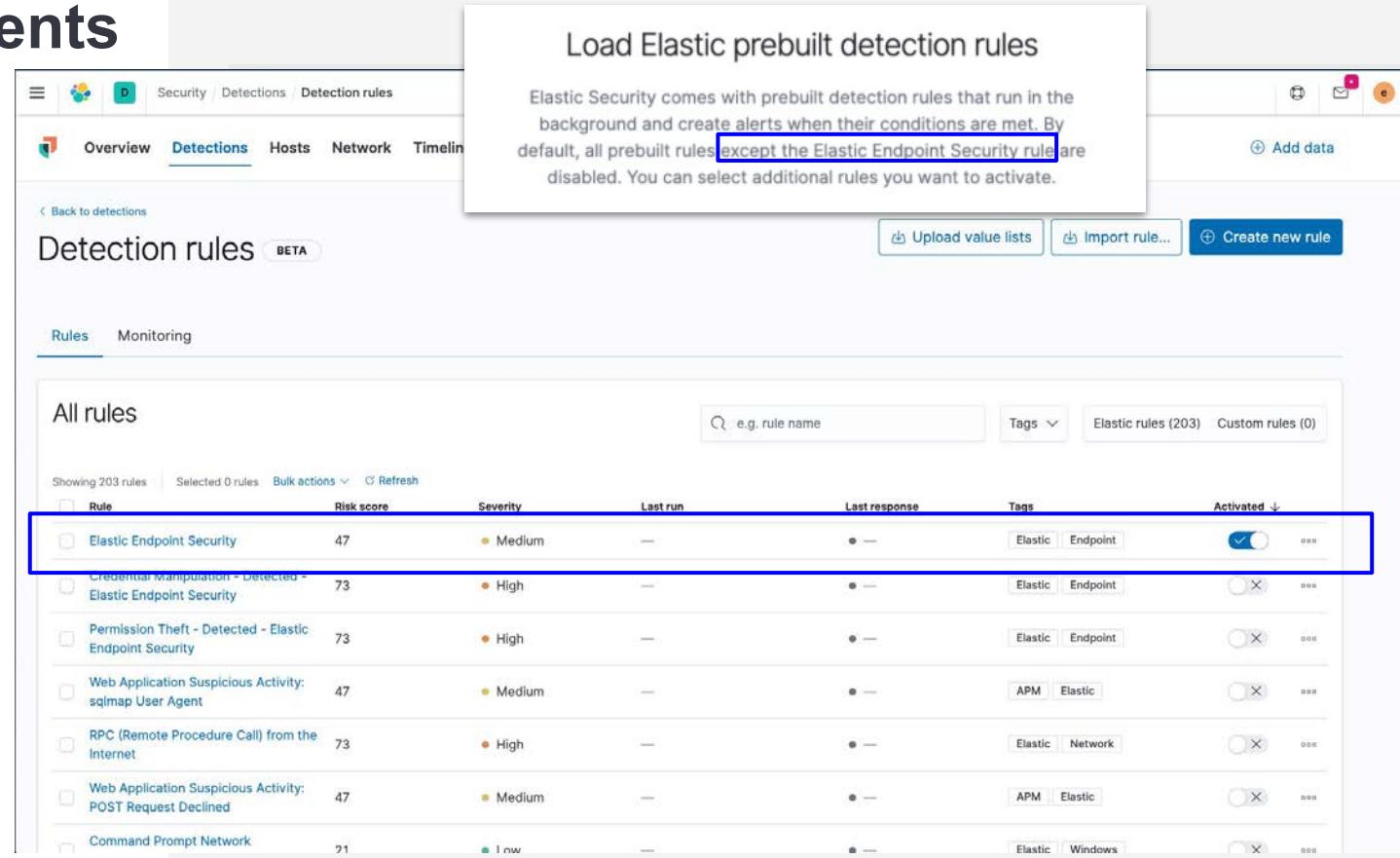
Detection alerts support new "in progress" state. Can mark in bulk and filter on "in progress" detection alerts.



Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

Note: New Elastic Endpoint Security rule is activated by default.



Load Elastic prebuilt detection rules

Elastic Security comes with prebuilt detection rules that run in the background and create alerts when their conditions are met. By default, all prebuilt rules **except the Elastic Endpoint Security rule** are disabled. You can select additional rules you want to activate.

Rule	Risk score	Severity	Last run	Last response	Tags	Activated
Elastic Endpoint Security	47	Medium	—	—	Elastic Endpoint	<input checked="" type="checkbox"/>
Credential Manipulation - Detected - Elastic Endpoint Security	73	High	—	—	Elastic Endpoint	<input type="checkbox"/>
Permission Theft - Detected - Elastic Endpoint Security	73	High	—	—	Elastic Endpoint	<input type="checkbox"/>
Web Application Suspicious Activity: sqlmap User Agent	47	Medium	—	—	APM Elastic	<input type="checkbox"/>
RPC (Remote Procedure Call) from the Internet	73	High	—	—	Elastic Network	<input type="checkbox"/>
Web Application Suspicious Activity: POST Request Declined	47	Medium	—	—	APM Elastic	<input type="checkbox"/>
Command Prompt Network	21	Low	—	—	Elastic Windows	<input type="checkbox"/>

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

7.9 ships with three prebuilt timeline templates: generic network, generic process, and generic endpoint

Timelines **Templates**

e.g. template name, or description

Only favorites 0 Elastic templates 3 Custom templates 0

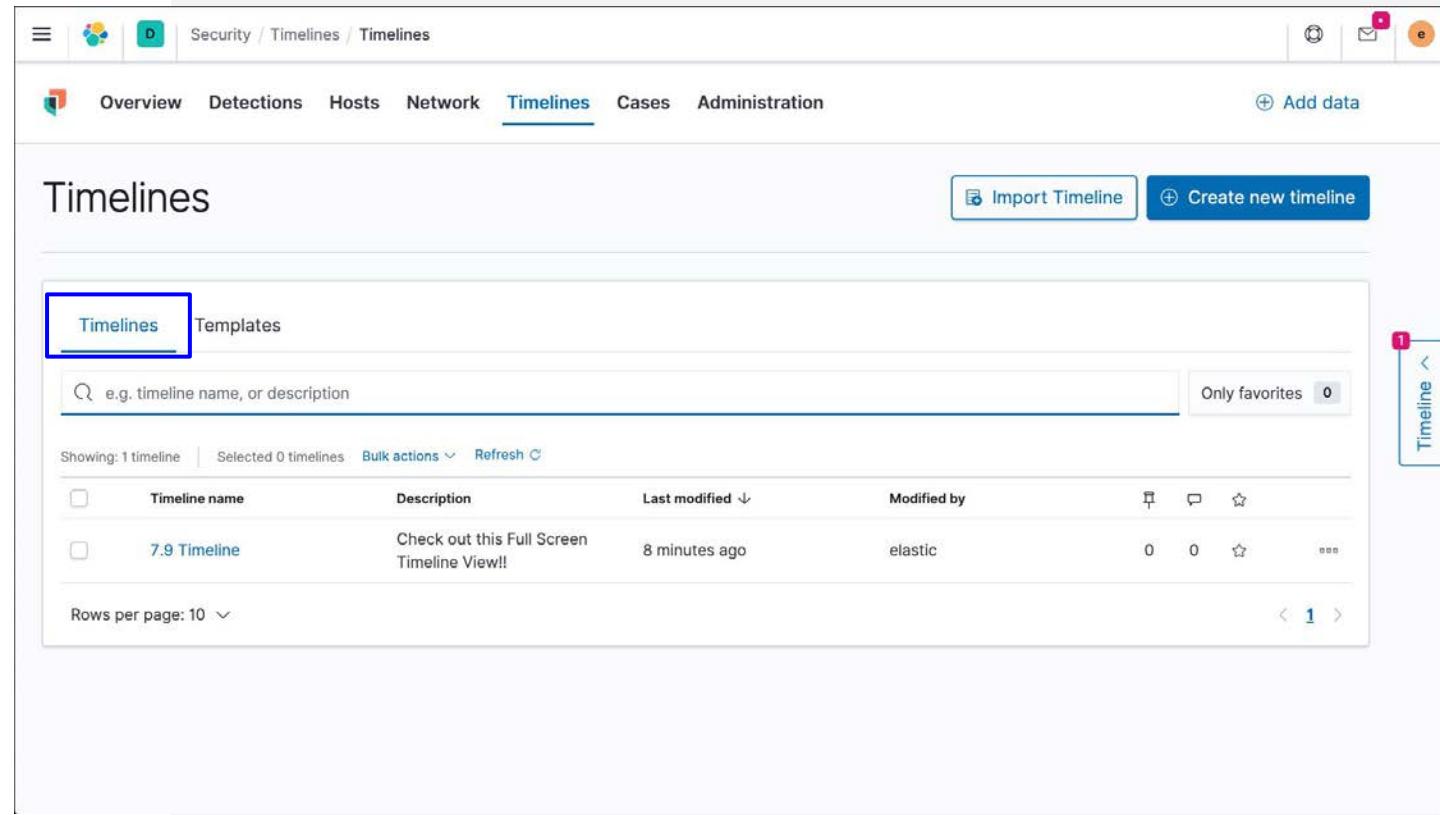
Template name	Description	Last modified	Modified by	Actions
Generic Network Timeline	—	24 minutes ago	Elastic	...
Generic Process Timeline	—	24 minutes ago	Elastic	...
Generic Endpoint Timeline	—	24 minutes ago	Elastic	...

Rows per page: 10

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

Separate tabs help analyst keep track of templates vs. investigative timelines.



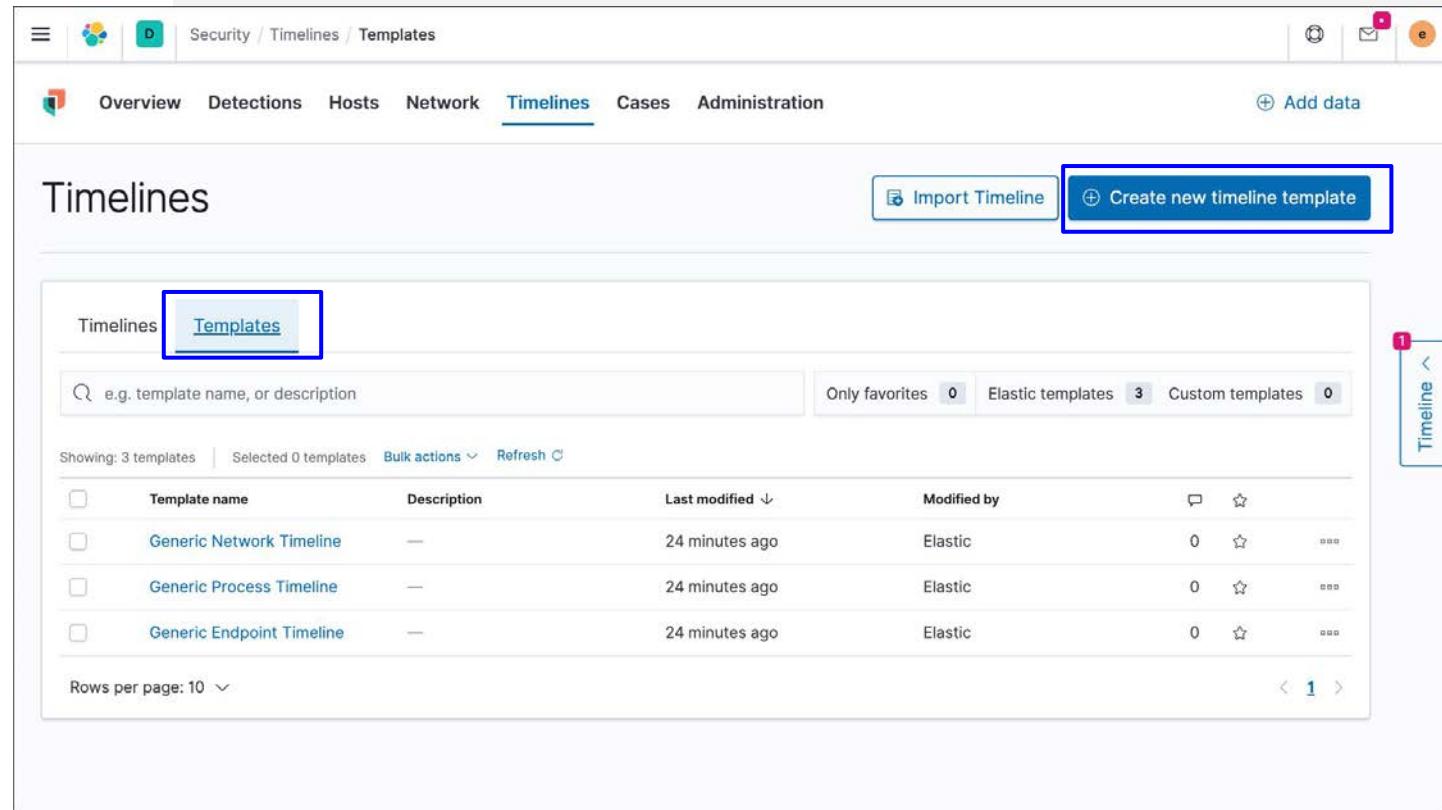
The screenshot shows the Elastic Security interface with the 'Timelines' tab selected. The top navigation bar includes 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines' (which is underlined in blue), 'Cases', and 'Administration'. Below the navigation is a search bar with the placeholder 'e.g. timeline name, or description'. A table lists one timeline: '7.9 Timeline' (Description: 'Check out this Full Screen Timeline View!!', Last modified: '8 minutes ago', Modified by: 'elastic', with 0 rows and 0 columns). Buttons for 'Import Timeline' and 'Create new timeline' are visible. A sidebar on the right shows a 'Timeline' section with a '1' badge.

Timeline name	Description	Last modified	Modified by	Rows	Columns
7.9 Timeline	Check out this Full Screen Timeline View!!	8 minutes ago	elastic	0	0

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

In 7.9, can create your own timeline template!



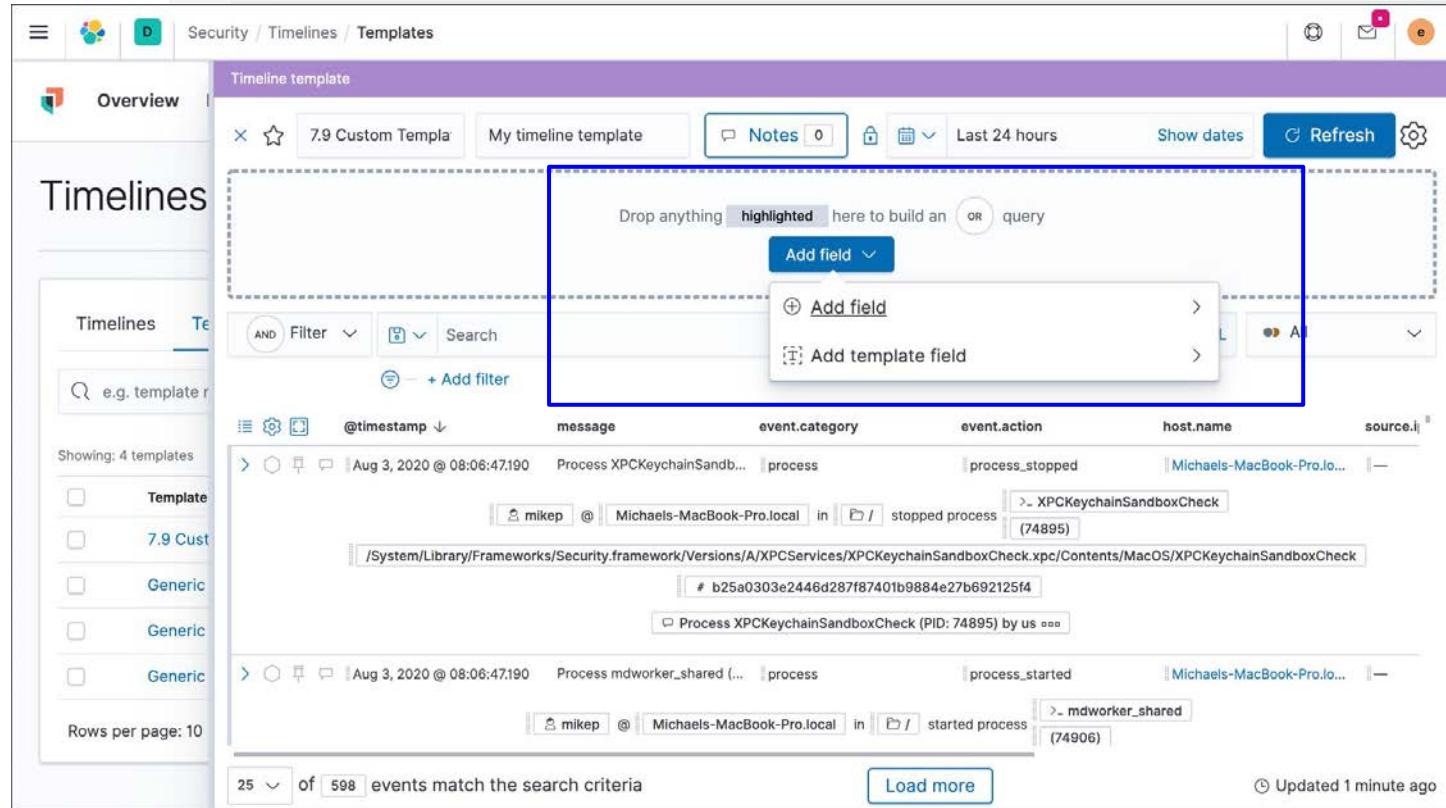
The screenshot shows the Elasticsearch UI for 'Timelines'. The top navigation bar includes 'Security / Timelines / Templates', a user icon, and a search bar. Below the navigation is a secondary navigation bar with tabs: Overview, Detections, Hosts, Network, Timelines (which is underlined), Cases, and Administration. To the right of this bar is a 'Add data' button. The main content area is titled 'Timelines' and contains a 'Create new timeline template' button, which is highlighted with a blue box. Below this, there are tabs for 'Timelines' and 'Templates', with 'Templates' being the active tab, also highlighted with a blue box. A search bar with placeholder text 'e.g. template name, or description' is present. To the right of the search bar are filters for 'Only favorites' (0), 'Elastic templates' (3), and 'Custom templates' (0). The main table lists three templates: 'Generic Network Timeline', 'Generic Process Timeline', and 'Generic Endpoint Timeline', each with a checkbox, a description, 'Last modified' timestamp (24 minutes ago), 'Modified by' (Elastic), and a star icon. At the bottom of the table are buttons for 'Rows per page' (10) and navigation arrows. A vertical sidebar on the right is labeled 'Timeline'.

Template name	Description	Last modified	Modified by	Actions
Generic Network Timeline	—	24 minutes ago	Elastic	Star, More
Generic Process Timeline	—	24 minutes ago	Elastic	Star, More
Generic Endpoint Timeline	—	24 minutes ago	Elastic	Star, More

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

Can start from events in time, or can now start from scratch, with the new "Add Field" capability. Use fixed value or new "template field"



The screenshot shows the Elasticsearch Security / Timelines / Templates interface. The main area is titled 'Timeline template' and shows a '7.9 Custom Template' with 'My timeline template' selected. A 'Notes' section indicates 0 notes, and a 'Last 24 hours' filter is applied. A 'Refresh' button and a gear icon are in the top right. The left sidebar has 'Timelines' selected. The main content area displays a table of log events with columns: @timestamp, message, event.category, event.action, host.name, and source.ip. The 'message' column shows log entries related to XPCKeychainSandboxCheck and mdworker_shared processes. A 'Filter' and 'Search' bar are at the top of the table. A 'Rows per page' dropdown is set to 25. At the bottom, it says '25 of 598 events match the search criteria' and 'Load more'. A blue box highlights the 'Add field' dropdown menu, which contains 'Add field' and 'Add template field' options. The bottom right corner shows 'Updated 1 minute ago'.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

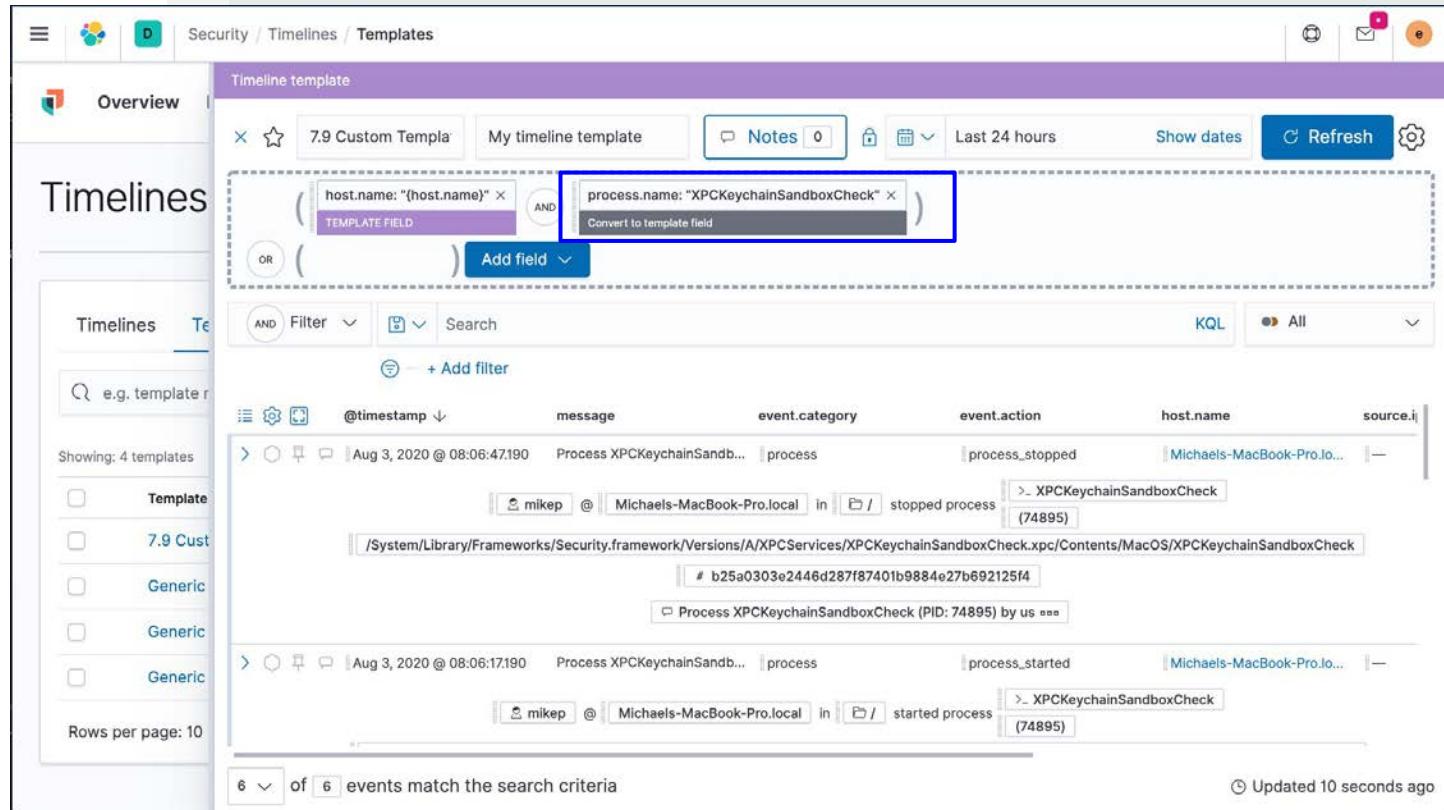
Filter containing template field will be modified with value from detection alert when analyst chooses to "Investigate in Timeline"

The screenshot shows the 'Timeline template' interface in the Elastic Security platform. The top navigation bar includes 'Security / Timelines / Templates' and various icons. The main area is titled 'Timeline template' with a sub-section '7.9 Custom Template' and 'My timeline template'. It features a search bar with 'Notes 0', a date range 'Last 24 hours', and a 'Refresh' button. The interface is divided into sections: 'Timelines' (selected), 'Template' (list of templates like '7.9 Cust', 'Generic'), 'Filter' (with 'AND' and 'OR' options), 'Search' (with a 'KQL' button), and a results table. The results table has columns: '@timestamp', 'message', 'event.category', 'event.action', 'host.name', and 'source.ip'. It shows two events from August 3, 2020, at 08:06:47.190. The first event is 'Process XPCKeychainSandboxCheck' (process_stopped) on 'Michaels-MacBook-Pro.local' (PID 74895). The second event is 'Process mdworker_shared' (process_started) on 'Michaels-MacBook-Pro.local' (PID 74906). The bottom of the interface shows '25 of 598 events match the search criteria', a 'Load more' button, and a timestamp 'Updated 10 seconds ago'.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

Filter containing standard field will not be modified with value from detection alert but will keep its specified value.

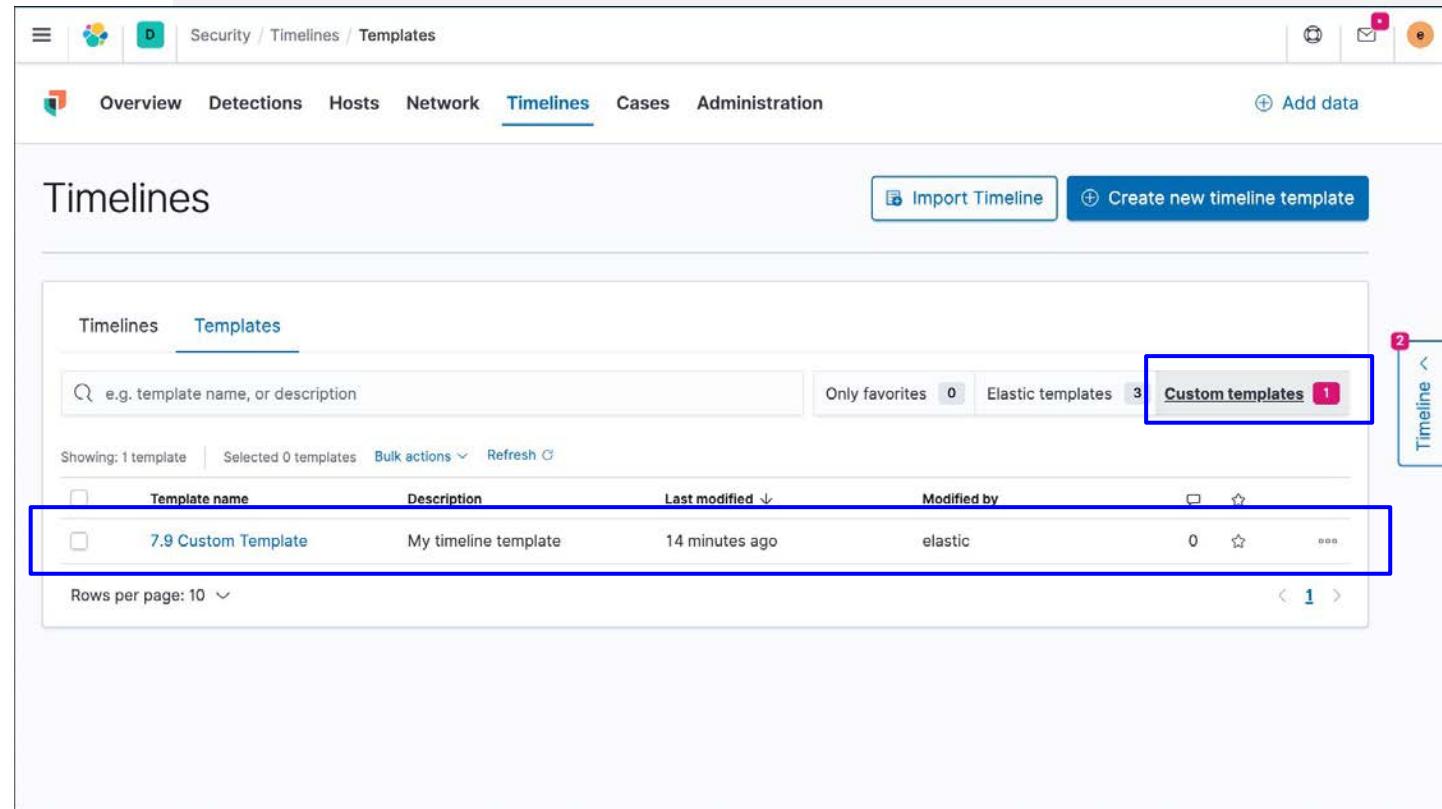


The screenshot shows the 'Timelines' section of the Elastic Security interface. A 'Timeline template' is being edited, specifically '7.9 Custom Template'. The query editor shows a complex search pattern: 'host.name: "{host.name}" AND process.name: "XPCKeychainSandboxCheck"'. A blue box highlights the 'process.name' field, which is identified as a 'TEMPLATE FIELD'. Below the query, the results table displays two log entries from August 3, 2020, at 08:06:47.190. The first entry is a 'process_stopped' event for 'XPCKeychainSandboxCheck' (PID: 74895), and the second is a 'process_started' event for the same process (PID: 74895). The interface includes a sidebar for 'Timelines' and a bottom status bar indicating 'Updated 10 seconds ago'.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

Can filter for custom timeline templates, Elastic prebuilt templates, or both.



The screenshot shows the Elastic Security interface with the 'Timelines' tab selected. A blue box highlights the 'Custom templates' section, which contains a single entry: '7.9 Custom Template' (My timeline template, last modified 14 minutes ago by elastic). The interface includes a search bar, filters for 'Only favorites' and 'Elastic templates', and a 'Create new timeline template' button.

Template name	Description	Last modified	Modified by	Actions
7.9 Custom Template	My timeline template	14 minutes ago	elastic	0 ⭐ ...

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

All timeline templates, including custom templates, are available during rule creation step 1.

Security / Detections / Detection rules / Create

Rule type

Custom query

Machine Learning

Threshold

e.g. Timeline template name or Only favorites

None

7.9 Custom Template

Import query from saved timeline

KQL

Select which timeline to use when investigating generated alerts.

Continue

Timeline

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

Timeline now supports a full-screen view by clicking on this icon.

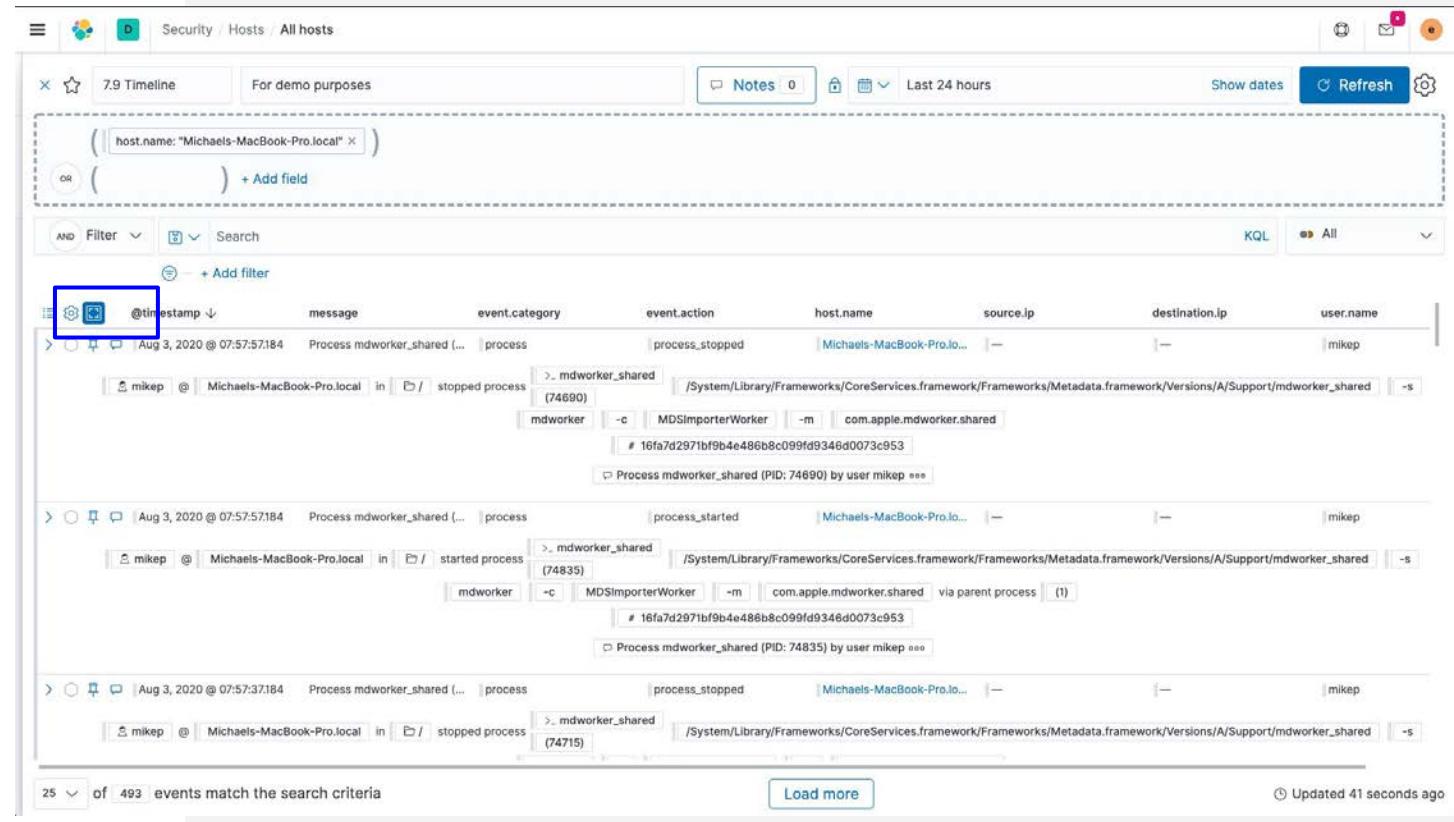
The screenshot displays the Elastic Security interface with the following sections:

- Hosts:** Shows 1 host (Michael's MacBook Pro.local) with 0 user authentications. The timeline shows a single event: "Process mdworker_shared (process) stopped" on Aug 3, 2020, at 07:57:57.184, initiated by user mikep on the host.
- Timeline:** Shows the same event in a detailed timeline view with expanded logs. The event is shown as a process chain: mdworker_shared (74690) -> MDSimporterWorker -> com.apple.mdworker.shared (# 16fa7d2971bf9b4e486b8c099fd9346d0073c953). The event is labeled as a stopped process.
- Logs:** Shows the raw log entries for the event, including the process start and stop logs.

Analyst Workflow Enhancements

- Signals now called Alerts
- Exception workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- **Timeline new templates, performance improvements, and full-screen displays**

Full-screen timeline allows analysts to use all vertical space, see more events, improve velocity!



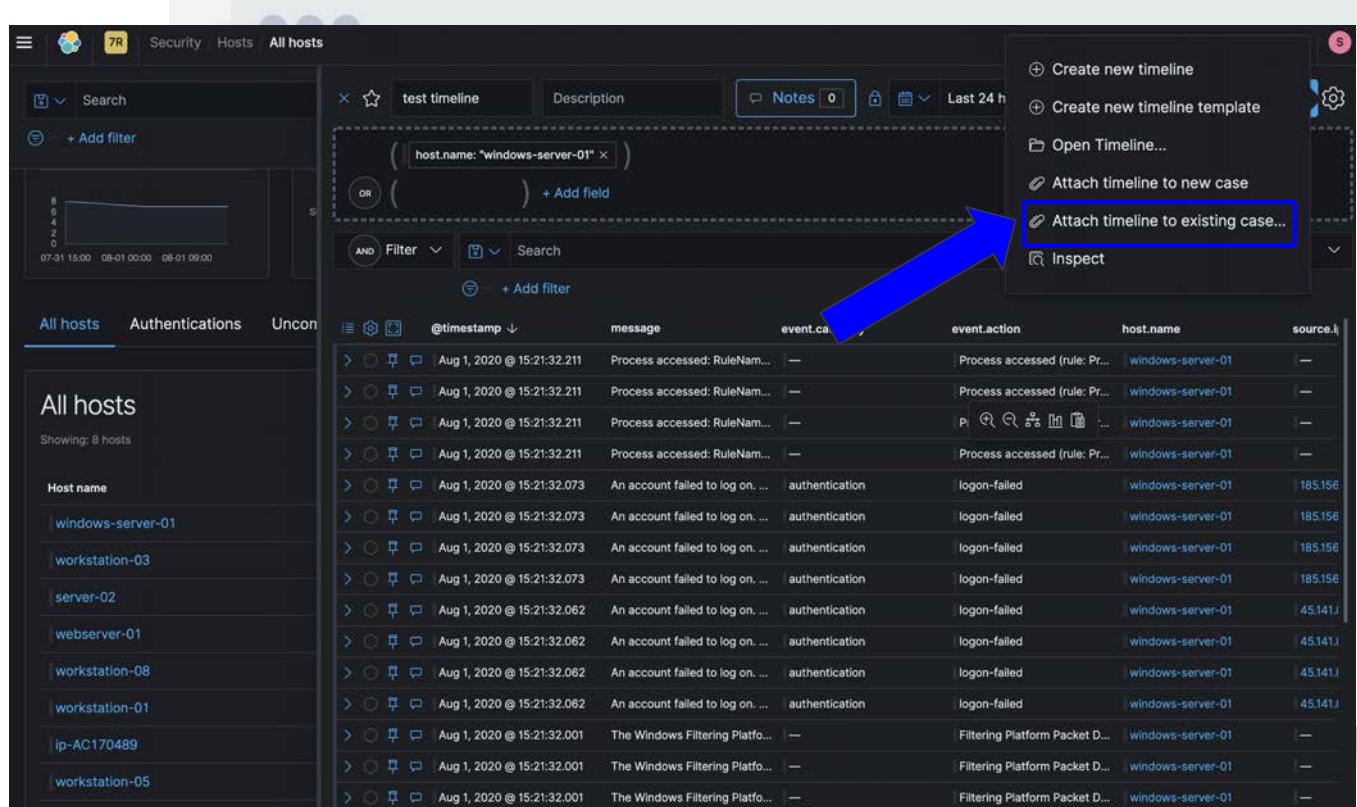
The screenshot shows the Elasticsearch full-screen timeline interface. At the top, there is a search bar with the query "host.name: 'Michaels-MacBook-Pro.local'". Below the search bar, there are several search filters and a search button. The main area displays a table of search results with columns: @timestamp, message, event.category, event.action, host.name, source.ip, destination.ip, and user.name. The first result is a process named "mdworker_shared" that was stopped. The second result is a process named "mdworker_shared" that was started. The third result is another process named "mdworker_shared" that was stopped. The table has a header row and several data rows. At the bottom of the table, it says "25 of 493 events match the search criteria". There is a "Load more" button and a timestamp "Updated 41 seconds ago".

Case Management Workflows

Case Management Workflows

- Send cases to IBM Resilient

- Create cases from within cases view
- Or create cases from the Timeline view
- New in 7.9, attach timeline to existing case**



The screenshot shows the Elasticsearch Case Management interface. On the left, there's a sidebar with 'All hosts' selected. The main area has a timeline titled 'test timeline' with a search bar and a 'Last 24 h' button. Below the timeline is a table of events. A context menu is open on the right, with the 'Attach timeline to existing case...' option highlighted by a blue arrow. The table of events includes columns for @timestamp, message, event.ca, event.action, host.name, and source.ip.

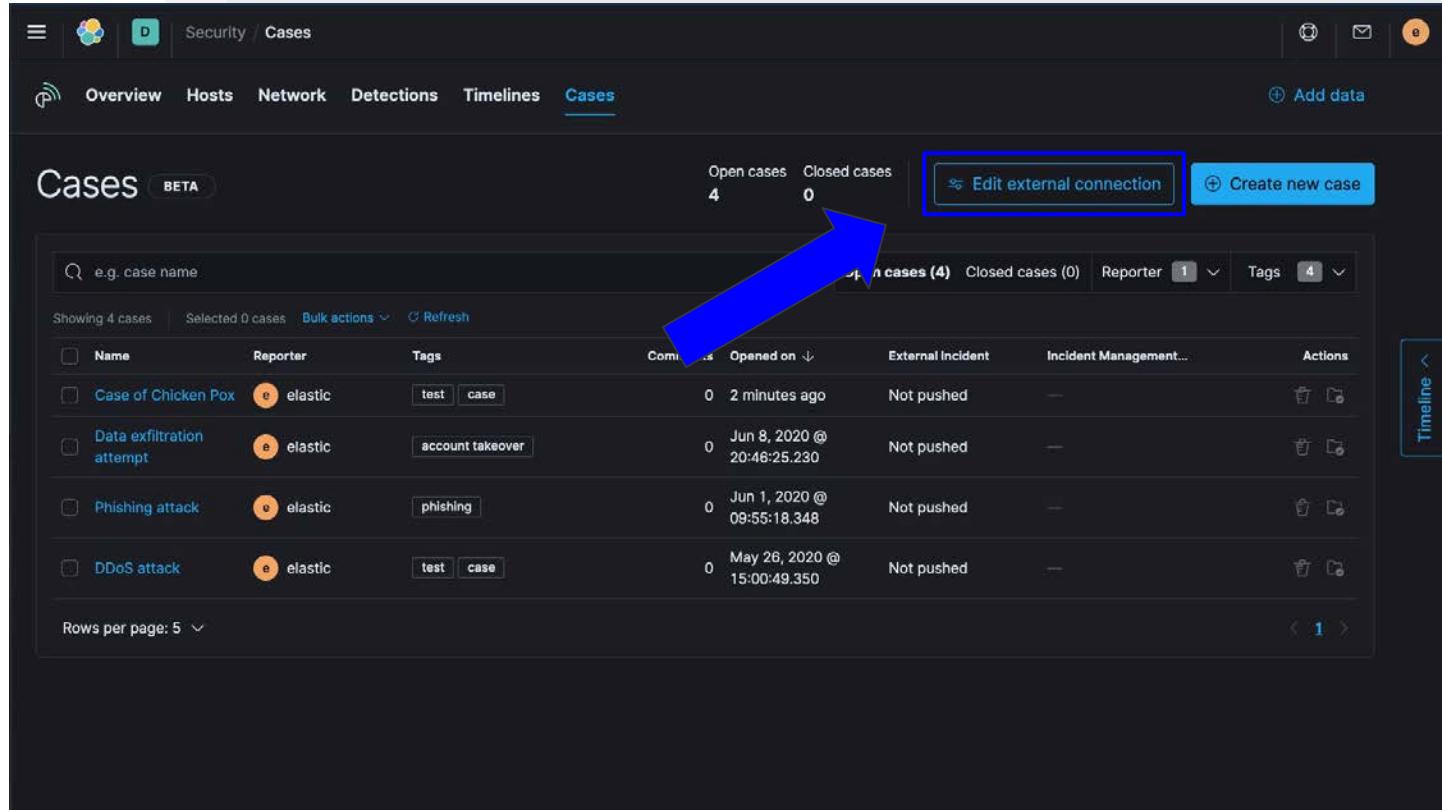
@timestamp	message	event.ca	event.action	host.name	source.ip
Aug 1, 2020 @ 15:21:32.211	Process accessed: RuleNam...	—	Process accessed (rule: Pr...	windows-server-01	—
Aug 1, 2020 @ 15:21:32.211	Process accessed: RuleNam...	—	Process accessed (rule: Pr...	windows-server-01	—
Aug 1, 2020 @ 15:21:32.211	Process accessed: RuleNam...	—	Process accessed (rule: Pr...	windows-server-01	—
Aug 1, 2020 @ 15:21:32.211	Process accessed: RuleNam...	—	Process accessed (rule: Pr...	windows-server-01	—
Aug 1, 2020 @ 15:21:32.073	An account failed to log on. ...	authentication	logon-failed	windows-server-01	185.156
Aug 1, 2020 @ 15:21:32.073	An account failed to log on. ...	authentication	logon-failed	windows-server-01	185.156
Aug 1, 2020 @ 15:21:32.073	An account failed to log on. ...	authentication	logon-failed	windows-server-01	185.156
Aug 1, 2020 @ 15:21:32.062	An account failed to log on. ...	authentication	logon-failed	windows-server-01	45.141.J
Aug 1, 2020 @ 15:21:32.062	An account failed to log on. ...	authentication	logon-failed	windows-server-01	45.141.J
Aug 1, 2020 @ 15:21:32.062	An account failed to log on. ...	authentication	logon-failed	windows-server-01	45.141.J
Aug 1, 2020 @ 15:21:32.001	The Windows Filtering Platfo...	—	Filtering Platform Packet D...	windows-server-01	—
Aug 1, 2020 @ 15:21:32.001	The Windows Filtering Platfo...	—	Filtering Platform Packet D...	windows-server-01	—
Aug 1, 2020 @ 15:21:32.001	The Windows Filtering Platfo...	—	Filtering Platform Packet D...	windows-server-01	—

Case Management Workflows

Case Management Workflows

- Send cases to IBM Resilient

- Can also send cases to external systems
- No external systems configured by default
- Create an external connector using in-app experience for connecting to an external incident management system



The screenshot shows the IBM Resilient Case Management interface. At the top, there are navigation tabs: Overview, Hosts, Network, Detections, Timelines, and Cases. The Cases tab is selected. Below the tabs, there are two buttons: 'Edit external connection' (highlighted with a blue box and arrow) and 'Create new case'. A summary shows 4 Open cases and 0 Closed cases. The main area displays a table of cases with columns: Name, Reporter, Tags, Comments, Opened on, External Incident, Incident Management..., and Actions. The table lists four cases: 'Case of Chicken Pox', 'Data exfiltration attempt', 'Phishing attack', and 'DDoS attack'. Each case is reported by 'elastic' and has specific tags like 'test' and 'case' or 'account takeover'. The 'Opened on' column shows the date and time of each case's creation. The 'Actions' column contains icons for delete and edit. A sidebar on the right is titled 'Timeline'.

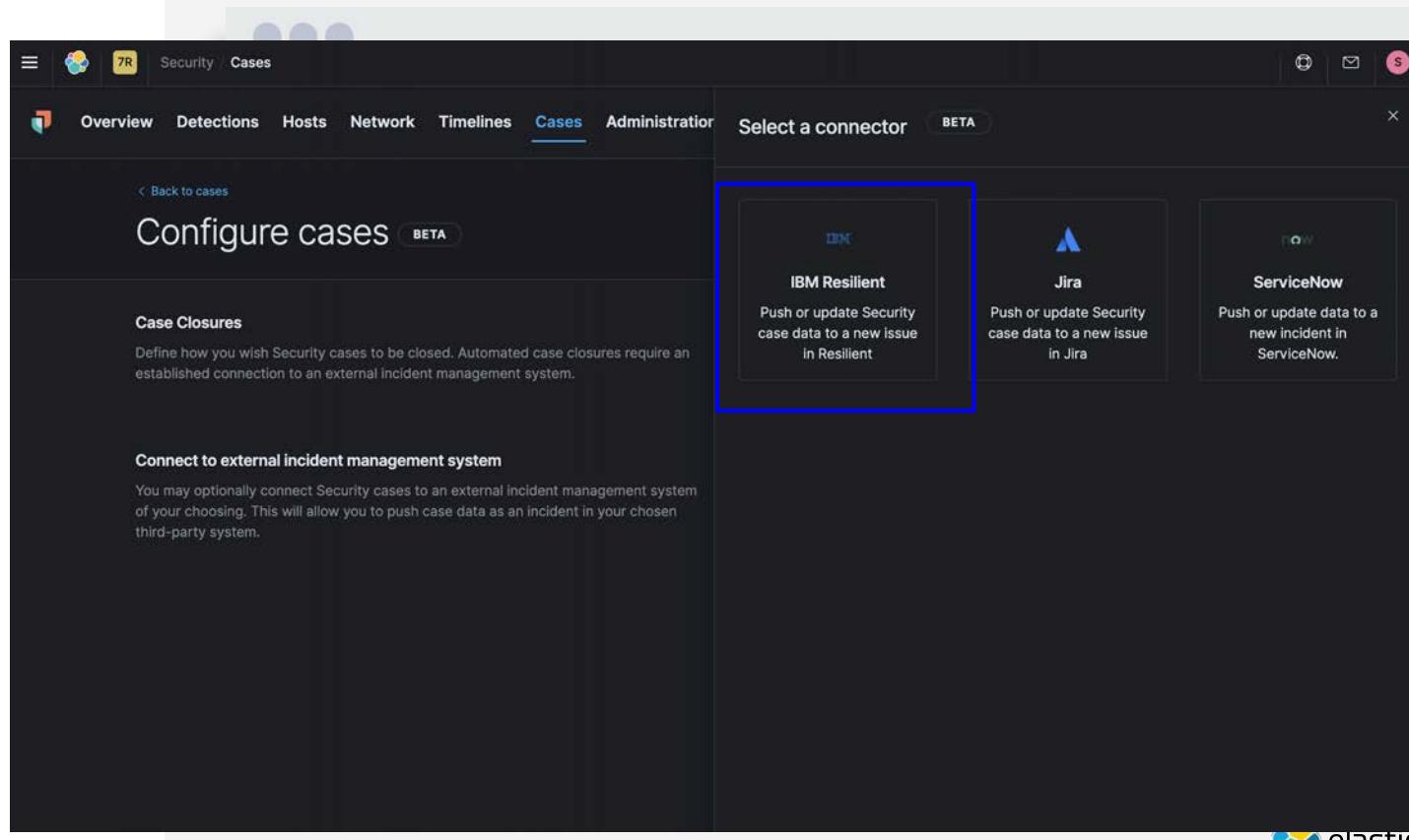
Name	Reporter	Tags	Comments	Opened on	External Incident	Incident Management...	Actions
Case of Chicken Pox	elastic	test case	0	2 minutes ago	Not pushed	—	 
Data exfiltration attempt	elastic	account takeover	0	Jun 8, 2020 @ 20:46:25.230	Not pushed	—	 
Phishing attack	elastic	phishing	0	Jun 1, 2020 @ 09:55:18.348	Not pushed	—	 
DDoS attack	elastic	test case	0	May 26, 2020 @ 15:00:49.350	Not pushed	—	 

Case Management Workflows

Case Management Workflows

- Send cases to IBM Resilient

- In 7.9 we have added support for IBM Resilient. Previous releases had ServiceNow ITSM, and Jira



The screenshot shows the Elastic Security interface with the 'Cases' tab selected. A modal window titled 'Select a connector' is open, showing three options: 'IBM Resilient', 'Jira', and 'ServiceNow'. The 'IBM Resilient' option is highlighted with a blue box. The 'IBM Resilient' card contains the text: 'Push or update Security case data to a new issue in Resilient'. Below the modal, there are sections for 'Case Closures' and 'Connect to external incident management system'.

Case Closures

Define how you wish Security cases to be closed. Automated case closures require an established connection to an external incident management system.

Connect to external incident management system

You may optionally connect Security cases to an external incident management system of your choosing. This will allow you to push case data as an incident in your chosen third-party system.

IBM Resilient

Push or update Security case data to a new issue in Resilient

Jira

Push or update Security case data to a new issue in Jira

ServiceNow

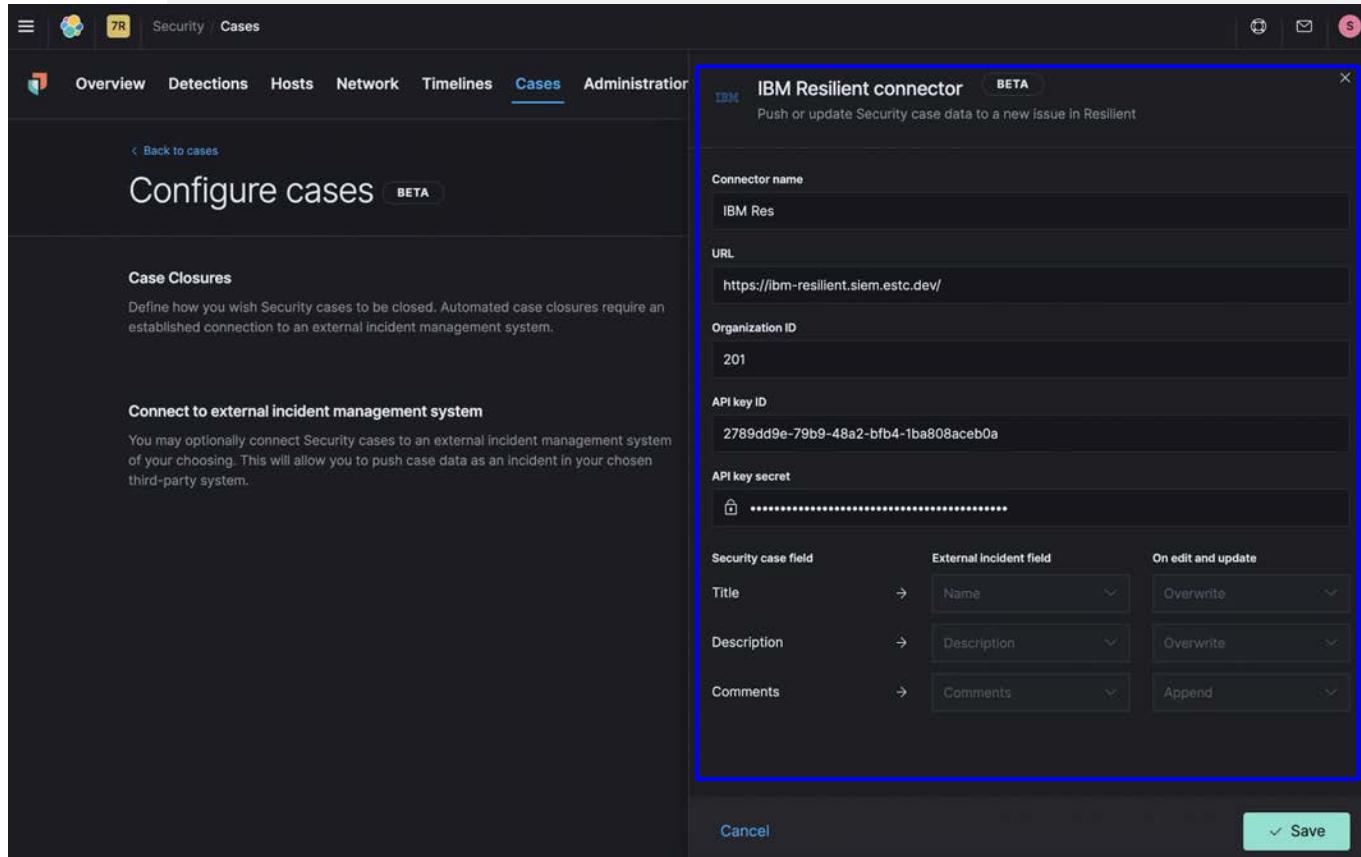
Push or update data to a new incident in ServiceNow.

Case Management Workflows

- Provide details about your IBM Resilient Instance
- No ability to configure custom field mappings at this point

Case Management Workflows

- Send cases to IBM Resilient



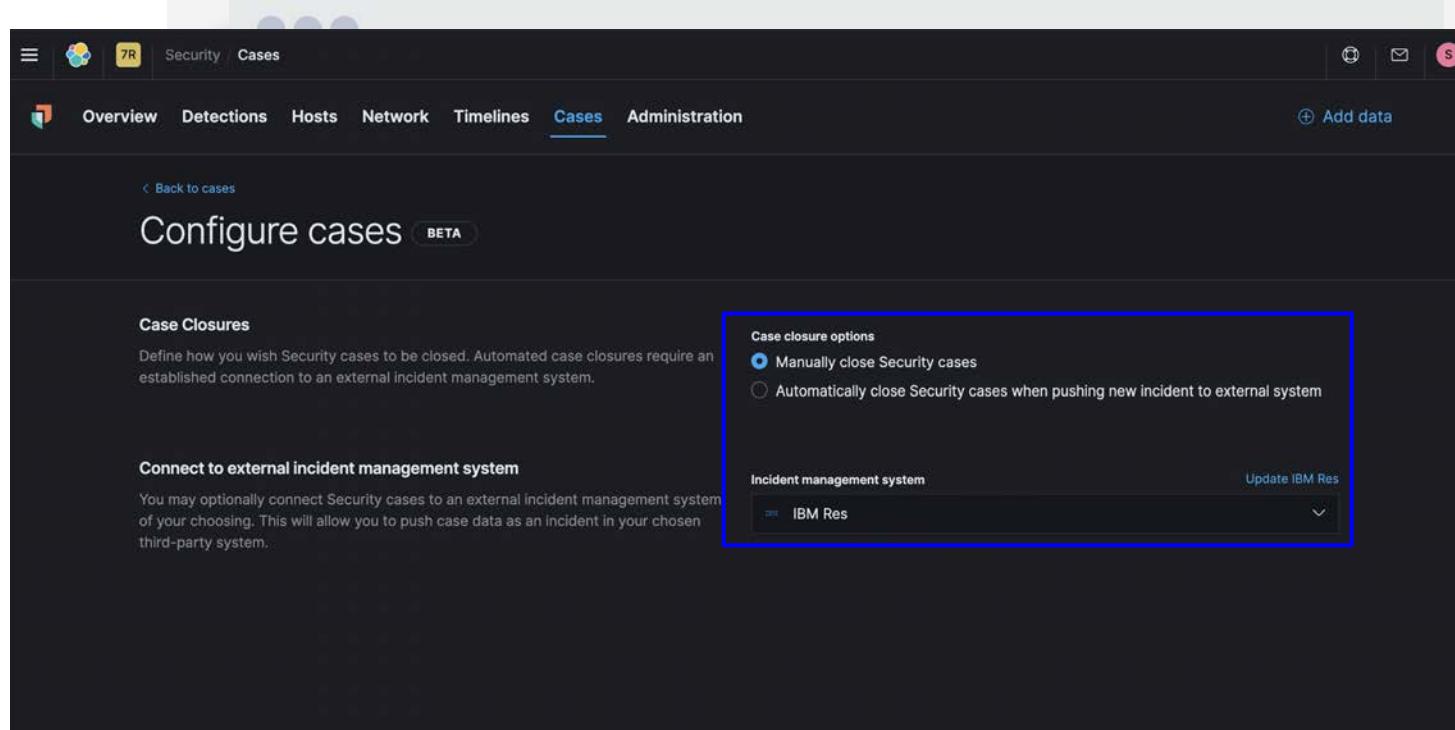
The screenshot shows the IBM Security Case Management interface. The top navigation bar includes 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines', 'Cases' (which is selected), and 'Administration'. A sub-menu for 'Cases' shows 'Configure cases' and 'Case Closures'. The main content area is titled 'Configure cases' (BETA) and contains sections for 'Case Closures' and 'Connect to external incident management system'. The 'Connect to external incident management system' section is expanded, showing configuration for the 'IBM Resilient connector' (BETA). The configuration form includes fields for 'Connector name' (set to 'IBM Res'), 'URL' (set to 'https://ibm-resilient.siem.estc.dev/'), 'Organization ID' (set to '201'), 'API key ID' (set to '2789dd9e-79b9-48a2-bfb4-1ba808aceb0a'), and 'API key secret' (a masked value). Below this is a table for mapping 'Security case field' to 'External incident field' with options for 'On edit and update' (e.g., 'Title' to 'Name' with 'Overwrite' selected). At the bottom are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted.

Case Management Workflows

Case Management Workflows

- Send cases to IBM Resilient

- Provide details about your IBM Resilient Instance
- No ability to configure custom field mappings at this point
- **Choose if you want to have cases closed automatically**



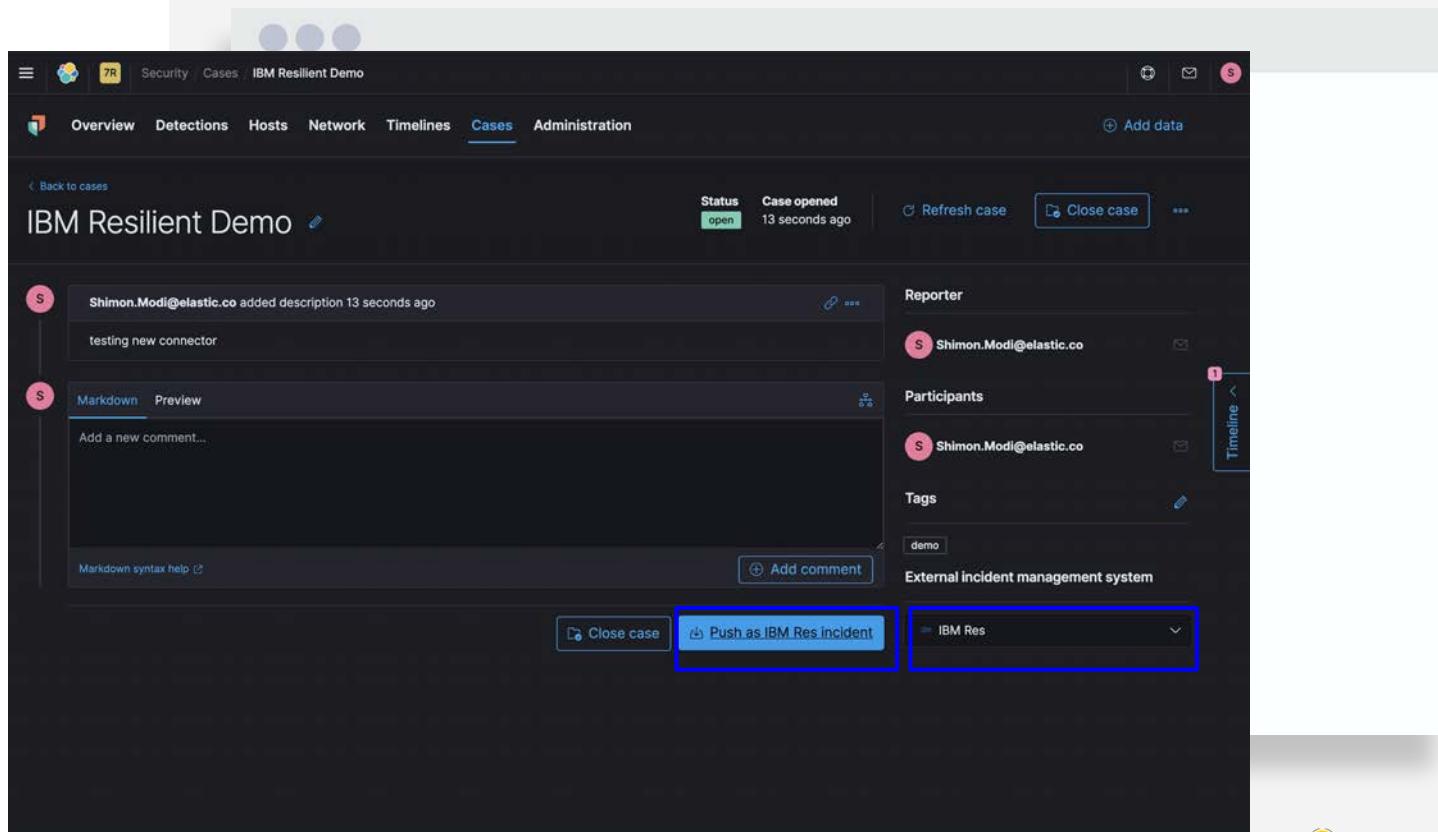
The screenshot shows the 'Cases' tab in the IBM Security interface. The main heading is 'Configure cases' (BETA). On the left, there's a section for 'Case Closures' with a sub-section 'Connect to external incident management system'. On the right, a box is highlighted with a blue border, containing 'Case closure options' with two radio buttons: 'Manually close Security cases' (selected) and 'Automatically close Security cases when pushing new incident to external system'. Below this is a dropdown for 'Incident management system' with 'IBM Res' selected. The top navigation bar includes 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines', 'Cases' (selected), and 'Administration', along with an 'Add data' button.

Case Management Workflows

Case Management Workflows

- Send cases to IBM Resilient

- Push the case to the external IBM Resilient instance, along with comments and deep link to Timeline (if available)



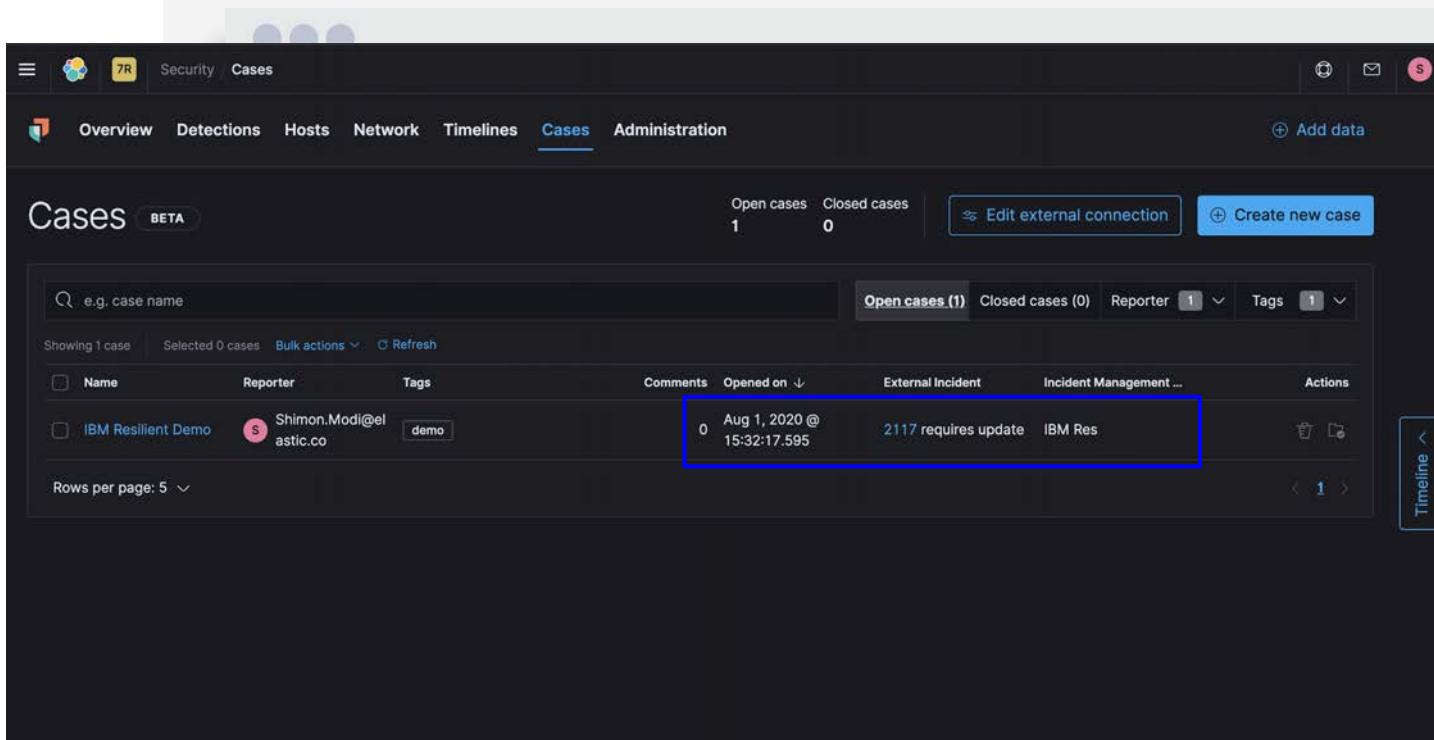
The screenshot shows the IBM Resilient Case Management interface. A new case titled "IBM Resilient Demo" is open. The case status is "open" and was "Case opened 13 seconds ago". The "Cases" tab is selected in the navigation bar. The main content area shows a comment from "Shimon.Modi@elastic.co" adding a description and testing the new connector. Below the comment is a text input field for "Add a new comment..." with "Markdown" and "Preview" options. At the bottom of the comment section are "Add comment" and "Close case" buttons. To the right of the comment section are sections for "Reporter" (Shimon.Modi@elastic.co), "Participants" (Shimon.Modi@elastic.co), and "Tags" (demo). A "Timeline" section is partially visible. At the bottom right are buttons for "Close case", "Push as IBM Res Incident" (which is highlighted with a blue box), and "IBM Res". The top navigation bar includes "Overview", "Detections", "Hosts", "Network", "Timelines", "Administration", and an "Add data" button. The top right corner shows user icons for profile, notifications, and settings.

Case Management Workflows

Case Management Workflows

- Send cases to IBM Resilient

- Push the case to the external IBM Resilient instance
- Case Status updated to show push**



The screenshot shows the IBM Security Case Management interface. The top navigation bar includes 'Security' and 'Cases' tabs. Below the navigation is a sub-navigation bar with 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines', 'Cases' (which is underlined), and 'Administration' tabs. On the right side of the top bar are 'Add data', 'Edit external connection', and 'Create new case' buttons. The main area is titled 'Cases (BETA)'. It displays 'Open cases: 1' and 'Closed cases: 0'. A search bar at the top of the list table contains the placeholder 'e.g. case name'. Below the search bar are filters for 'Open cases (1)', 'Closed cases (0)', 'Reporter (1)', and 'Tags (1)'. The table has columns for 'Name', 'Reporter', 'Tags', 'Comments', 'Opened on', 'External Incident', 'Incident Management ...', and 'Actions'. A single row is visible, representing a case named 'IBM Resilient Demo' reported by 'Shimon.Modi@elastict.co' with tag 'demo'. The 'Opened on' field shows 'Aug 1, 2020 @ 15:32:17.595' and the 'External Incident' field shows '2117 requires update IBM Res'. The bottom right corner of the table row is highlighted with a blue border. A 'Timeline' button is located on the far right edge of the interface.

Name	Reporter	Tags	Comments	Opened on	External Incident	Incident Management ...	Actions
IBM Resilient Demo	Shimon.Modi@elastict.co	demo	0	Aug 1, 2020 @ 15:32:17.595	2117 requires update	IBM Res	 

Case Management Workflows

Case Management Workflows

- Send cases to IBM Resilient

- Case is created in IBM Resilient project specified by Organization ID provided during configuration

All Open Incidents  Save As  (Shared) 

Incident Disposition: Confirmed, Uncon Name: All Status: Active More... 

23 results Show 100 

<input type="checkbox"/>	ID	Name	Description	Date Discovered	Date Determined	Next Due Date	Date Created	Owner	Phase	Severity	Status
<input type="checkbox"/>	2117	IBM Resilient Demo (created at 2020-08-01T22:32:17.595Z by Shimon.Modi@elastic.co)	testing new connector (created at 2020-08-01T22:32:17.595Z by Shimon.Modi@elastic.co)	08/01/2020	08/01/2020	—	08/01/2020	 Default Group	Respond	—	Active
<input type="checkbox"/>	2116	testing connector configuration (created at 2020-07-31T13:12:44.352Z by elastic)	yes (created at 2020-07-31T13:12:44.352Z by elastic)	07/31/2020	07/31/2020	—	07/31/2020	 Default Group	Respond	—	Active
<input type="checkbox"/>	2115	Testing IBM (updated at 2020-07-31T13:10:12.554Z by elastic)	Testing IBM (updated at 2020-07-31T13:10:12.554Z by elastic)	07/31/2020	07/31/2020	—	07/31/2020	 Default Group	Respond	—	Active
<input type="checkbox"/>	2114	Brief (updated at 2020-07-30T18:23:08.787Z by elastic)	[This is only a test] (https://fb05569d2392489db66d07913ff0a9f.europe-west1.gcp.cloud.es.io:9243/app/security/timelines?timeline=(id:50de0580-d291-11ea-8f85-df3137ab5e5b;isOpen:!!) (updated at 2020-07-30T18:23:08.787Z by elastic))	07/30/2020	07/30/2020	—	07/30/2020	 Default Group	Respond	—	Active
<input type="checkbox"/>	2113	Edge (updated at 2020-07-30T14:39:33.100Z by elastic)	This is a very simple edge case. (updated at 2020-07-30T14:39:33.100Z by elastic)	07/30/2020	07/30/2020	—	07/30/2020	 Default Group	Respond	—	Active
<input type="checkbox"/>	2112	multiple participants - tester edit (updated at 2020-07-20T12:10:55.635Z by tester)	Test case: Multiple participants - tester edit (updated at 2020-07-20T12:10:55.635Z by tester)	07/20/2020	07/20/2020	—	07/20/2020	 Default Group	Respond	—	Active
<input type="checkbox"/>	2111	Switching connectors update (created at 2020-07-20T12:02:30.352Z by elastic)	Switching connectors desc update (created at 2020-07-20T12:02:30.352Z by elastic)	07/20/2020	07/20/2020	—	07/20/2020	 Default Group	Respond	—	Active
<input type="checkbox"/>	2110	IBM resilient (updated at 2020-07-20T08:33:12.798Z by elastic)	test (updated at 2020-07-20T08:33:12.798Z by elastic)	07/20/2020	07/20/2020	—	07/20/2020	 Default Group	Respond	—	Active

Case Management Workflows

Case Management Workflows

- Send cases to IBM Resilient

- Case is created in IBM Resilient project specified by Organization ID provided during configuration
- Move case through normal IBM Resilient workflows used by your organization**

IBM Resilient Demo (created at 2020-08-01T22:32:17.595Z by S...)

Actions ▾

Description

testing new connector (created at 2020-08-01T22:32:17.595Z by Shimon.Modi@elastic.co)

Tasks

Details

Breach

Notes

Members

News Feed

Attachments

Stats

Timeline

Artifacts

Email

Edit

Basic Details

Name 

IBM Resilient Demo (created at 2020-08-01T22:32:17.595Z by Shimon.Modi@elastic.co)

Description 

testing new connector (created at 2020-08-01T22:32:17.595Z by Shimon.Modi@elastic.co)

Incident Type 

—

NIST Attack Vectors 

—

Incident Disposition 

Unconfirmed

Phase 

Respond

Resolution 

—

Resolution Summary 

—

Owner

 Default Group

Created By

 Shimon Key

Date and Location

Date Created 

08/01/2020 15:34

Date Occurred 

—

Date Discovered 

08/01/2020 15:34:10

Address 

—

City

—

Country/Region

—

Postal Code

—

Implications

Summary

ID 2117

Phase Respond

Severity —

Date Created 08/01/2020

Date Occurred —

Date Discovered 08/01/2020

Date Determined 08/01/2020

Was personal information or personal data involved?
Unknown

Incident Type —

People

Created By  Shimon Key

Owner  Default Group

Members *There are no members.*

Related Incidents

No related incidents.

Attachments

There are no attachments.

Newsfeed

Shimon Key updated the task list on the incident 08/01/2020 15:34:11

Shimon Key created the incident 08/01/2020 15:34:11

Elastic Security 7.9 Feature Summary

New Free and Open Endpoint Security (Beta)

- Anti-malware capabilities
- Installed through Elastic agent via Ingest Manager, managed by Fleet
- New in-app Administration page for endpoint security configuration/policy and endpoint system status

Analyst Workflow Enhancements

- Signals now called Alerts
- Exceptions workflows for detection engine and endpoint
- Value lists to support exceptions
- New threshold rule type and other rule creation enhancements in detection engine
- Timeline new templates, performance improvements, and full-screen displays

Out-of-the-Box Protections

- Free and Open detections in the new Elastic Security Repository
- 58 new prebuilt rules focus on Cloud Infrastructure and SaaS - reminder, also available in detection-rules repo
 - New Elastic Endpoint Security rule enabled by default
- Five new ML jobs (Anomaly Detection) for AWS CloudTrail - along with corresponding rules
- Manage rules at scale: New navigation by use case, vendor. New Investigation guide content. 3 prebuilt timeline templates

Case Workflow and Integrations

- Send and update cases to IBM Resilient (Requires Platinum subscription)

Data Source Integration Updates

- Filebeat modules for *GSuite*, *Microsoft Defender ATP* and *SophosXG* firewalls (Beta)
- 20 experimental modules and packages for a broad range of security data sources, including *Barracuda*, *Cylance*, *F5*, *Imperva*, *Juniper*, *Tenable*, *Sonicwall* and *ZScaler* (Experimental)
- All Beats modules updated to ECS 1.5
- Improved handling of forwarded events (e.g. syslog servers and Windows forwarded events)

Join the Elastic Security community



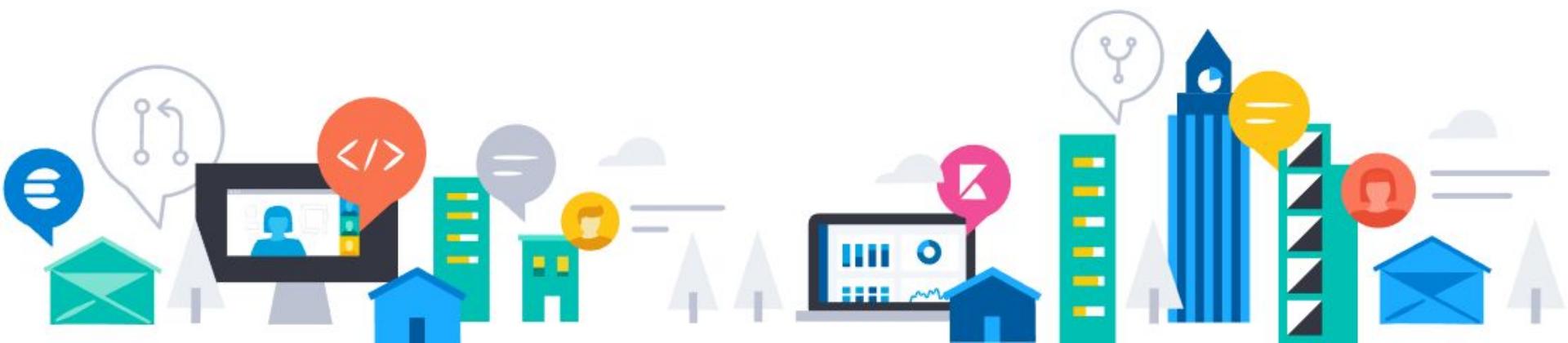
Take a quick spin:
demo.elastic.co



Try free on Cloud:
ela.st/security-trial



Connect on Slack:
ela.st/slack



VIRTUAL USER CONFERENCE

ElasticON Global

13 - 15 October 2020

Learn how to bring the power of search to your enterprise search, observability, and security use cases with Elastic solutions and the Elastic Stack. Bring your whole team and get inspired in conversations with Trevor Noah and Megan Rapinoe. ElasticON Global is free and open to everyone.



Tuesday, October 13

Global public sector event

- Public sector user stories
- Breakouts on geo, cloud, and cyber
- Federal and education peer panels
- FedRAMP and Elastic Cloud update

Wednesday, October 14

Americas

- Opening keynote with Shay Banon
- Training workshops
- Customer stories
- Elastic solution deep dives
- Networking opportunities
- Group discussion sessions

Thursday, October 15

Asia Pacific, Europe, Middle East, Africa

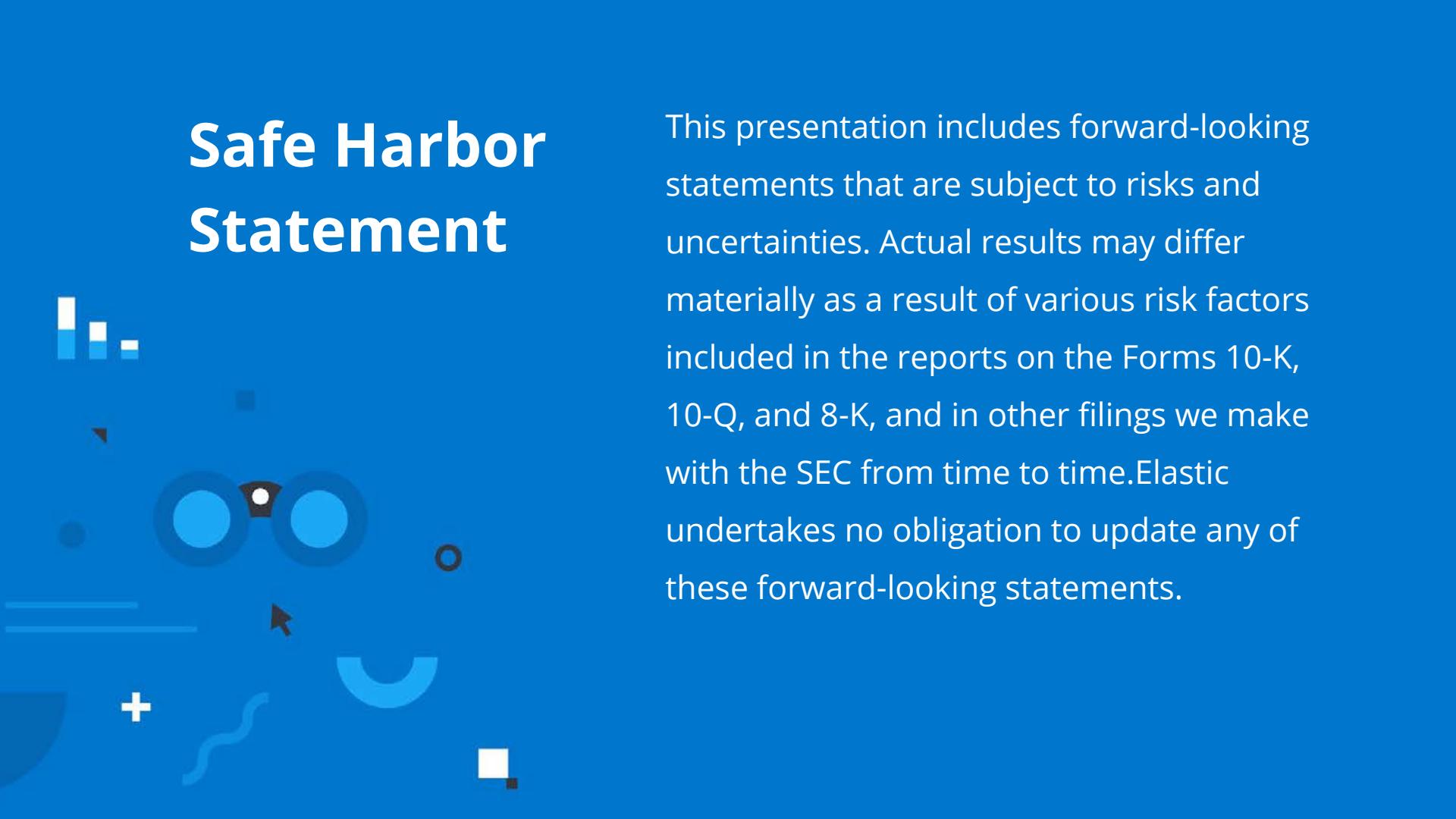
- Opening keynote with Shay Banon
- Training workshops
- Customer stories
- Elastic solution deep dives
- Networking opportunities
- Group discussion sessions



Thank You

Questions?

Safe Harbor Statement

The background of the slide features a blue gradient with various white and light blue geometric shapes and icons scattered across it. These include small squares, a plus sign, a minus sign, a magnifying glass, a gear, and a small figure of a person. There are also some abstract circular patterns and a small white arrow.

This presentation includes forward-looking statements that are subject to risks and uncertainties. Actual results may differ materially as a result of various risk factors included in the reports on the Forms 10-K, 10-Q, and 8-K, and in other filings we make with the SEC from time to time. Elastic undertakes no obligation to update any of these forward-looking statements.