elastic

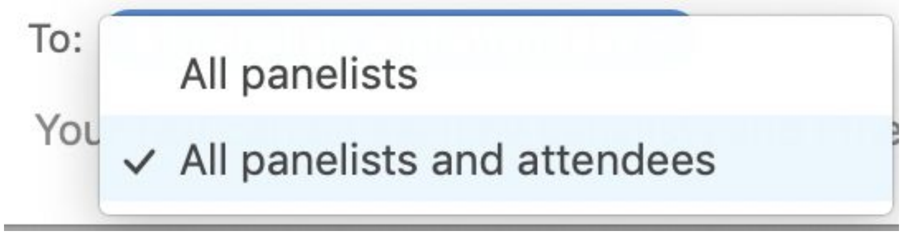
A Technical Deep Dive into Elastic Security 7.9

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”



To:

All panelists

✓ 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

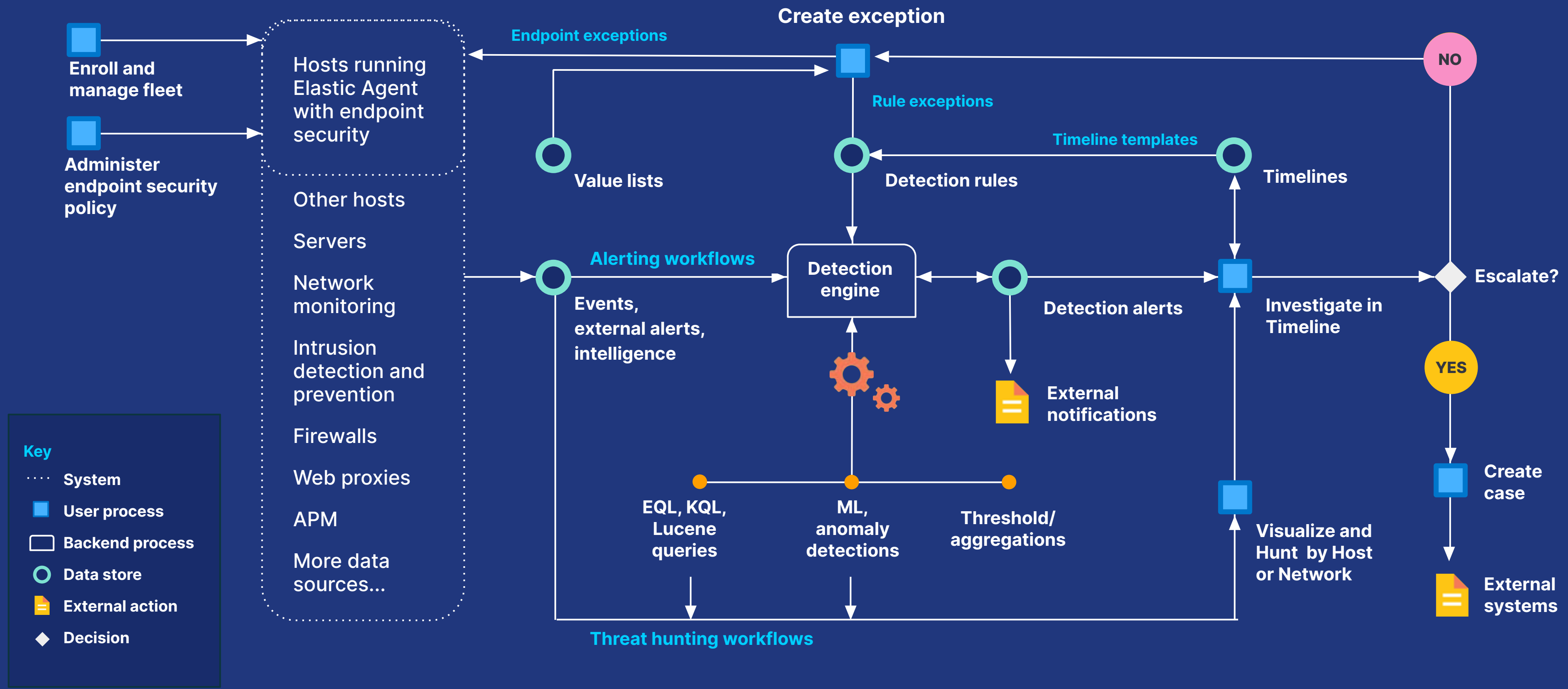
Braden Preston

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



Key

- ⋯ System
- ■ User process
- ▭ Backend process
- ○ Data store
- External action
- ◆ Decision

elastic

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

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.*

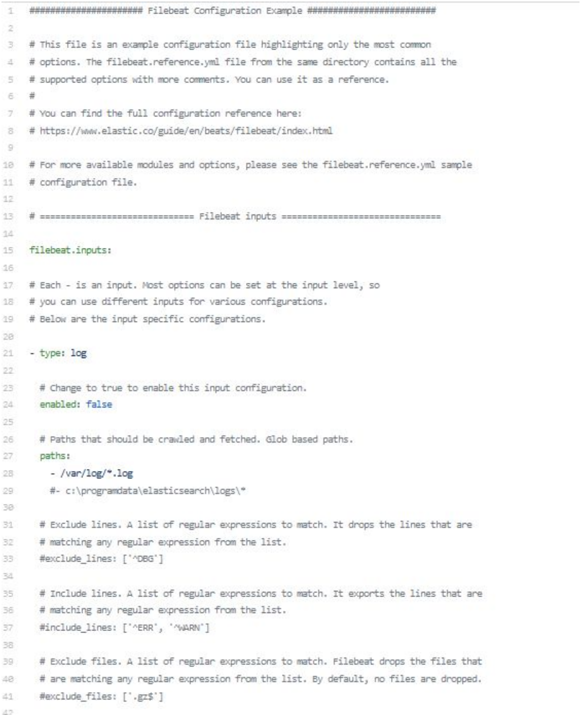
One thing to **install, configure and scale.**

Web UI to edit agent policies

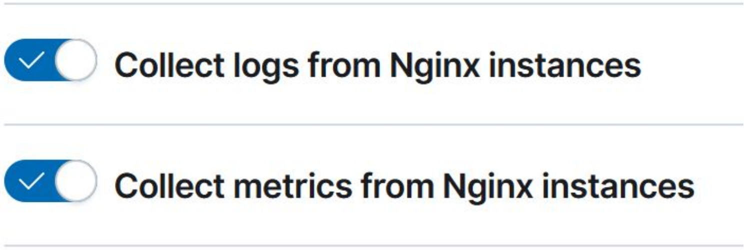
Collecting data is now as easy as ☑️

BEFORE

NOW



```
###################### Filebeat Configuration Example #########################

# This file is an example configuration file highlighting only the most common
# options. The filebeat.reference.yml file from the same directory contains all the
# supported options with more comments. You can use it as a reference.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/filebeat/index.html

# For more available modules and options, please see the filebeat.reference.yml sample
# configuration file.

# ============================== Filebeat inputs ===============================

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

- type: log

  # Change to true to enable this input configuration.
  enabled: false

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/*.log
    #- c:\programdata\elasticsearch\logs\*

  # Exclude lines. A list of regular expressions to match. It drops the lines that are
  # matching any regular expression from the list.
  #exclude_lines: ['^DBG']

  # Include lines. A list of regular expressions to match. It exports the lines that are
  # matching any regular expression from the list.
  #include_lines: ['^ERR', '^WARN']

  # Exclude files. A list of regular expressions to match. Filebeat drops the files that
  # are matching any regular expression from the list. By default, no files are dropped.
  #exclude_files: ['.gz$']
```



✓ 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

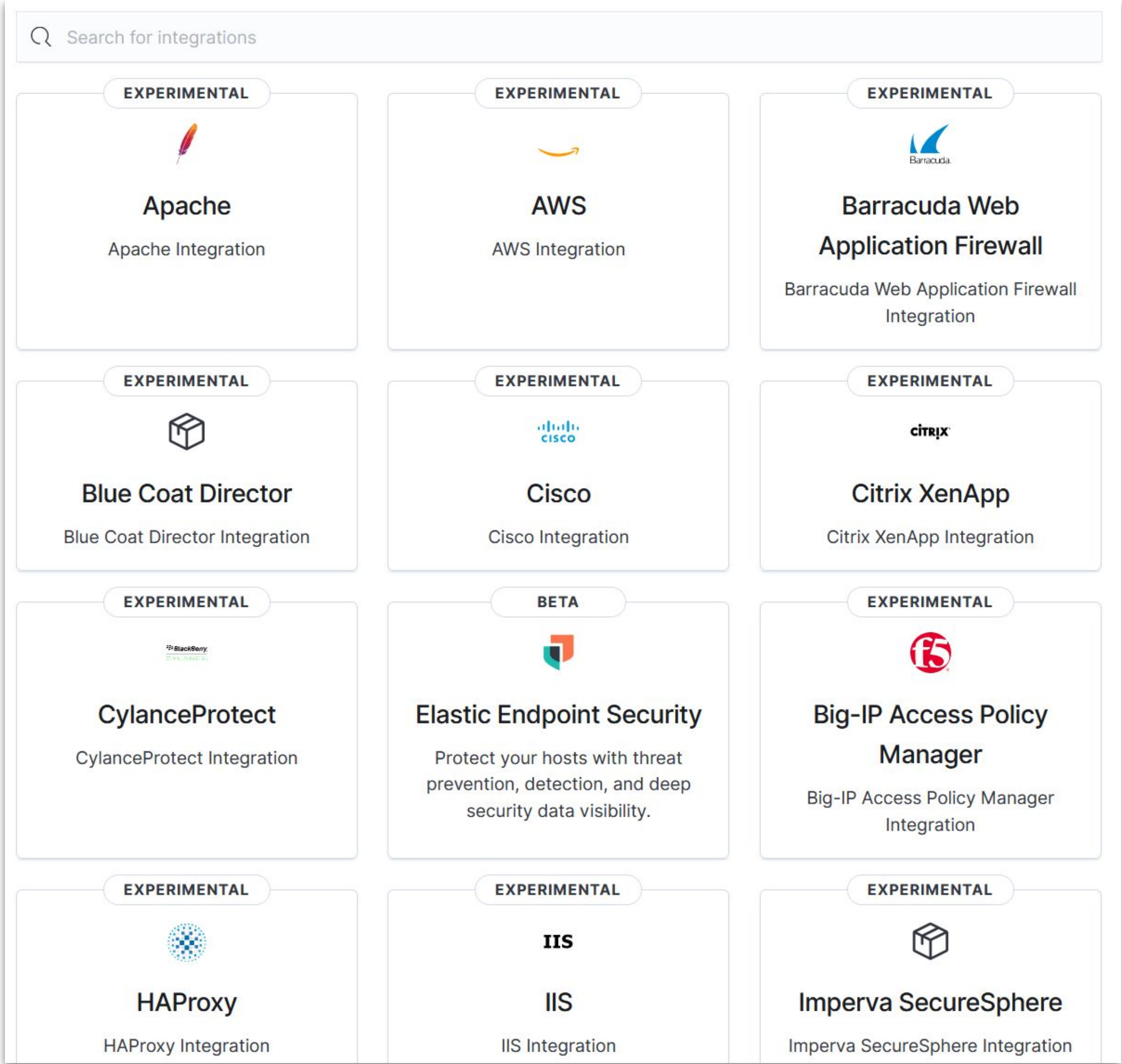
- API keys for Fleet and Elasticsearch
- Fleet saves keys automatically
- Minimal permissions on each Agent
- One key per Agent makes it easy to revoke

Fast time to insight and action

elastic

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

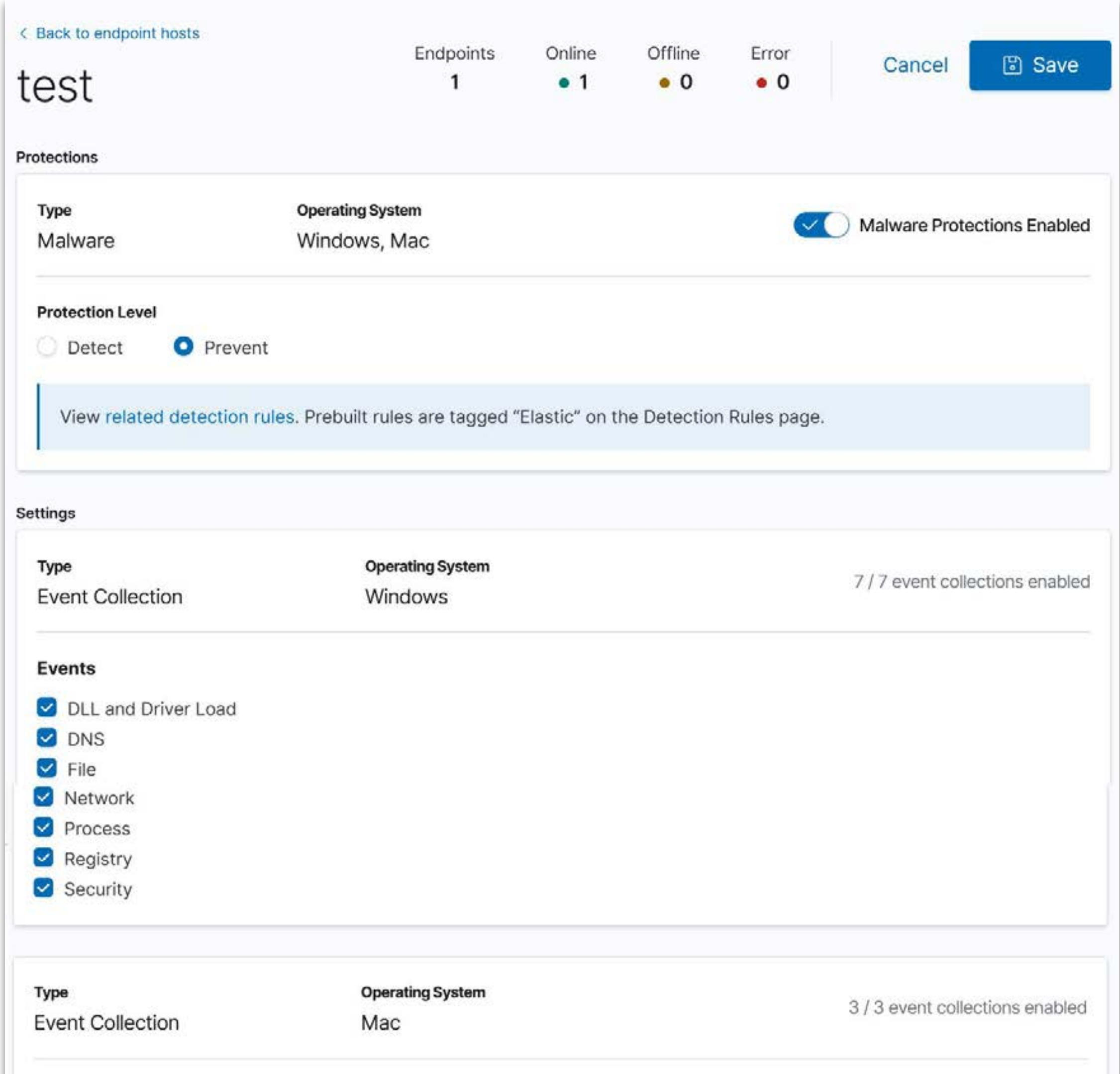
EXPERIMENTAL
HAProxy
HAProxy Integration

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

test

Endpoints	Online	Offline	Error
1	● 1	● 0	● 0

Cancel Save

Protections

Type: Malware
Operating System: Windows, Mac
Malware Protections Enabled

Protection Level
○ Detect ● Prevent

View related detection rules. Prebuilt rules are tagged "Elastic" on the Detection Rules page.

Settings

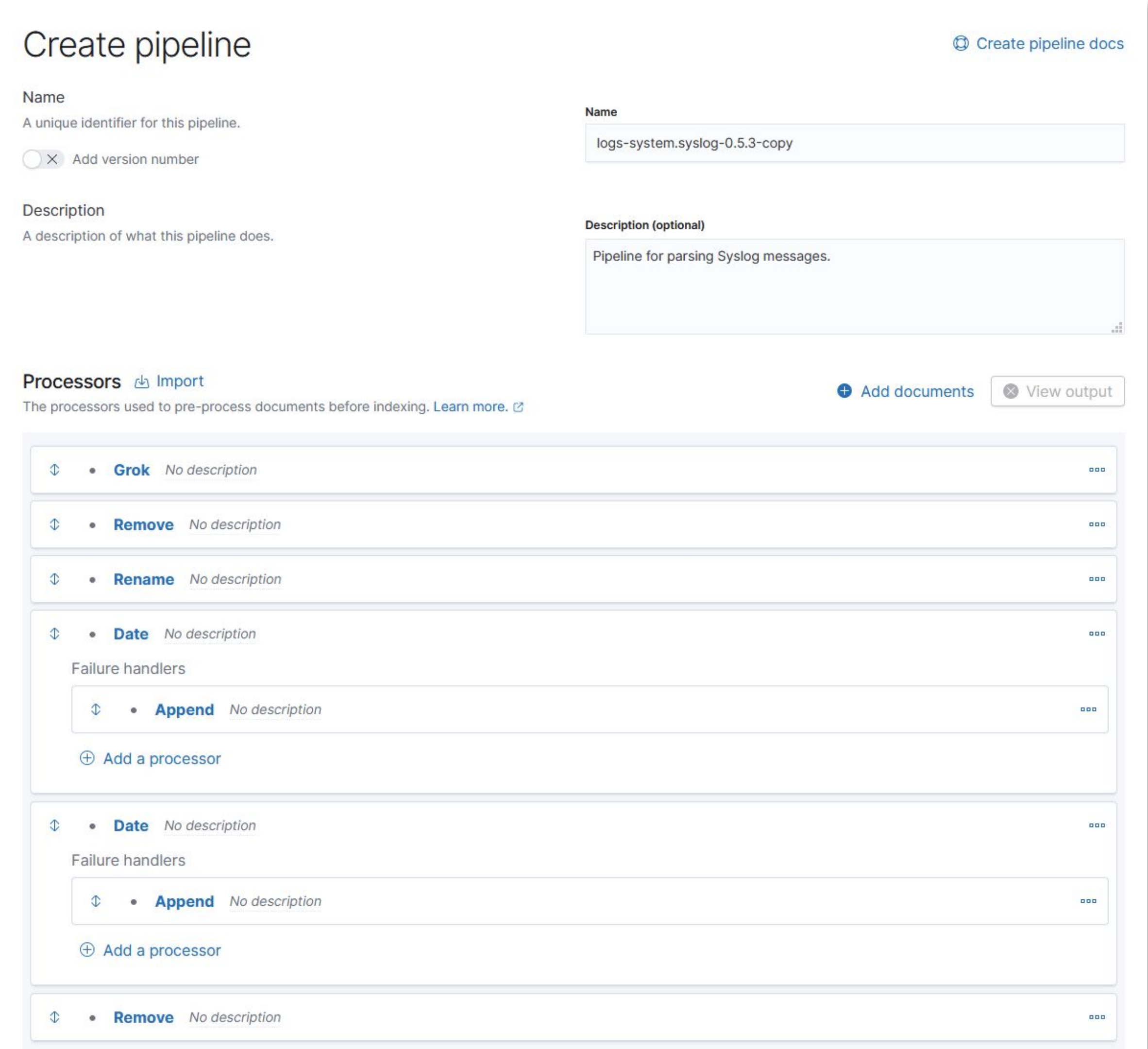
Type: Event Collection
Operating System: Windows
7 / 7 event collections enabled

Events
☑ DLL and Driver Load
☑ DNS
☑ File
☑ Network
☑ Process
☑ Registry
☑ Security

Type: Event Collection
Operating System: 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.

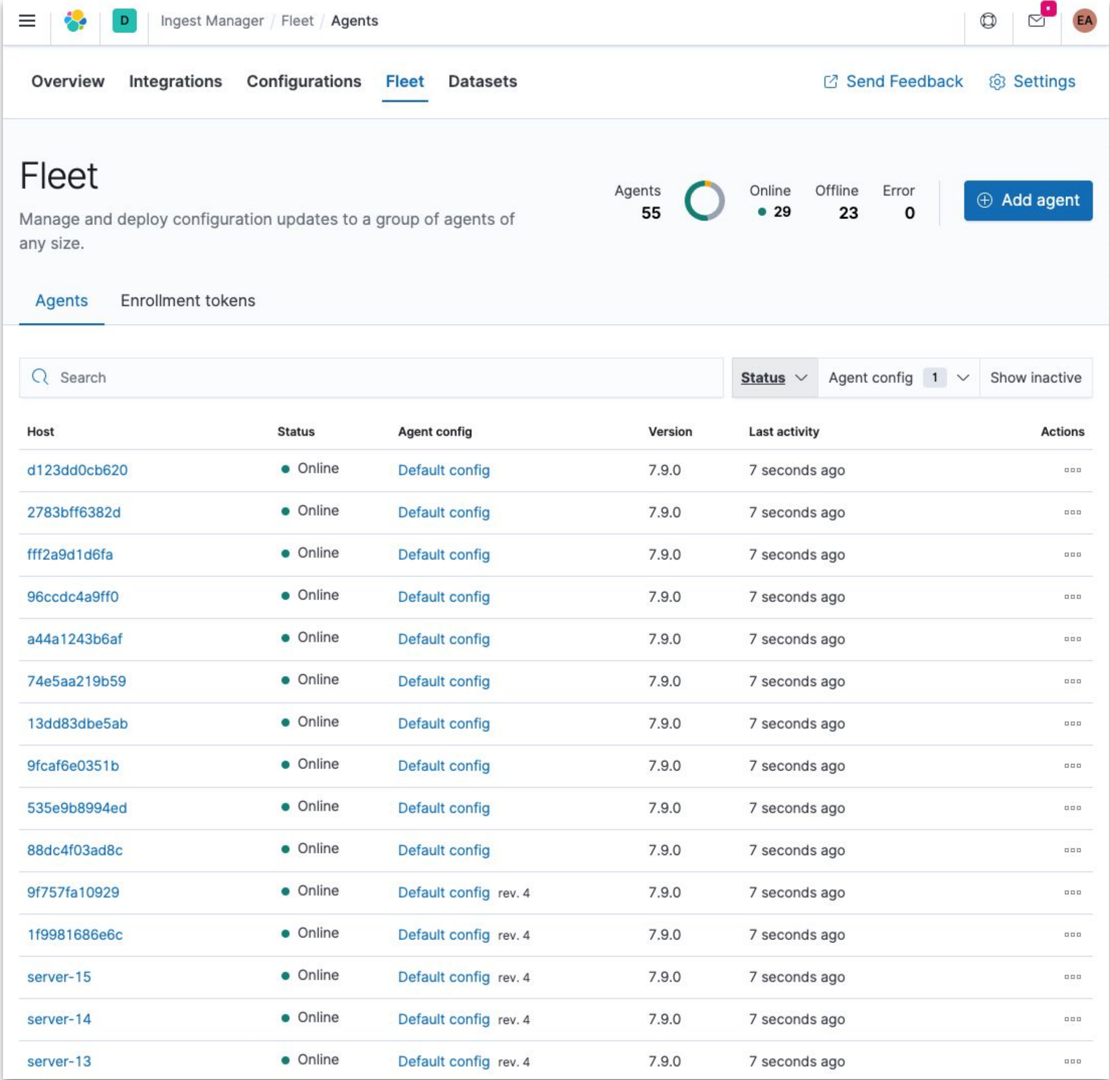
- **Grok** *No description*
- **Remove** *No description*
- **Rename** *No description*
- **Date** *No description*
  Failure handlers
  - **Append** *No description*
  Add a processor
- **Date** *No description*
  Failure handlers
  - **Append** *No description*
  Add a processor
- **Remove** *No description*

Easy management

elastic

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



Fleet

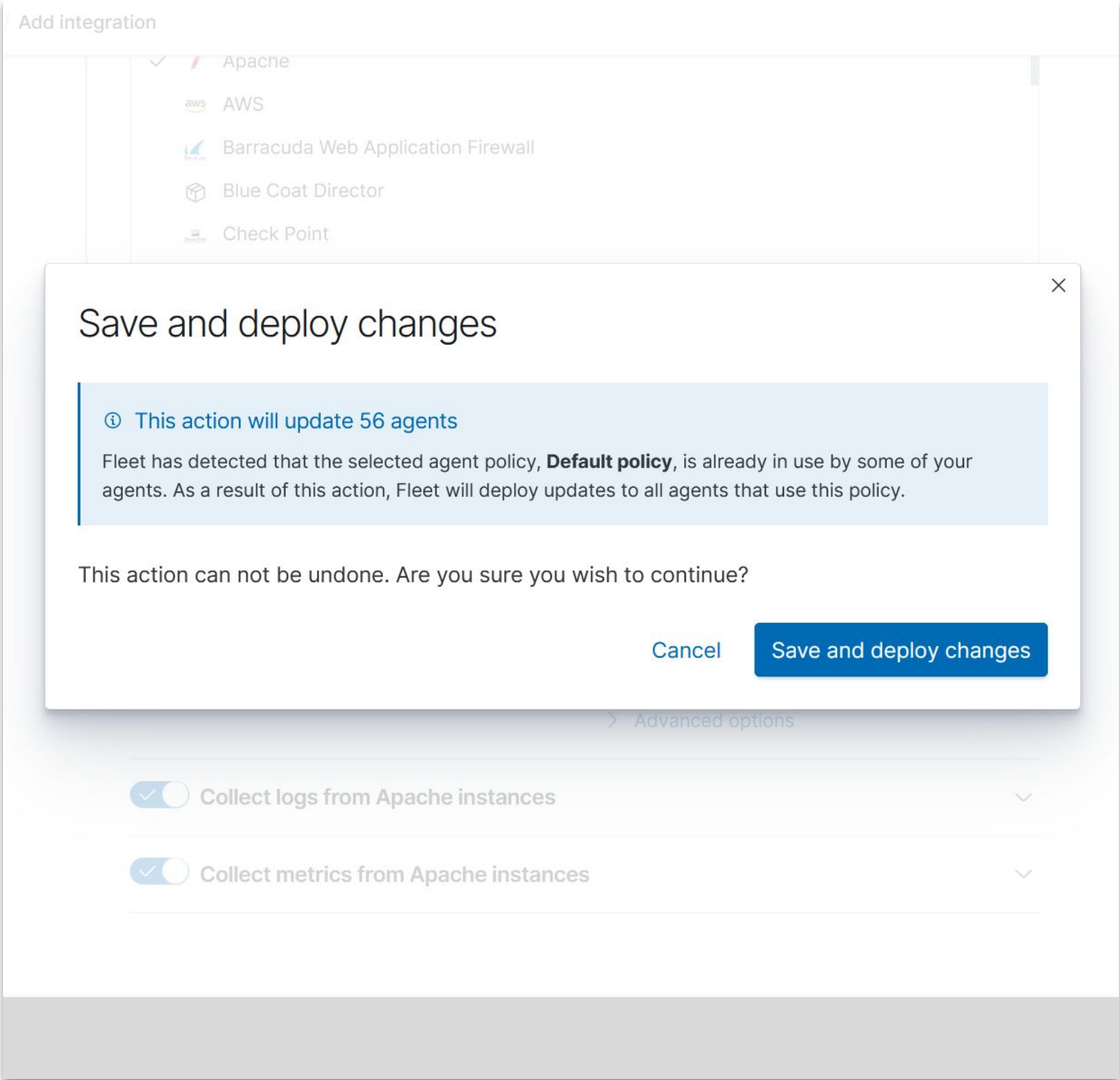
Manage and deploy configuration updates to a group of agents of any size.

Agents 55 · Online ● 29 · Offline 23 · Error 0

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	···
9fcaf6e0351b	● 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
Apache
AWS
Barracuda Web Application Firewall
Blue Coat Director
Check Point

Save and deploy changes

ⓘ This action will update 56 agents

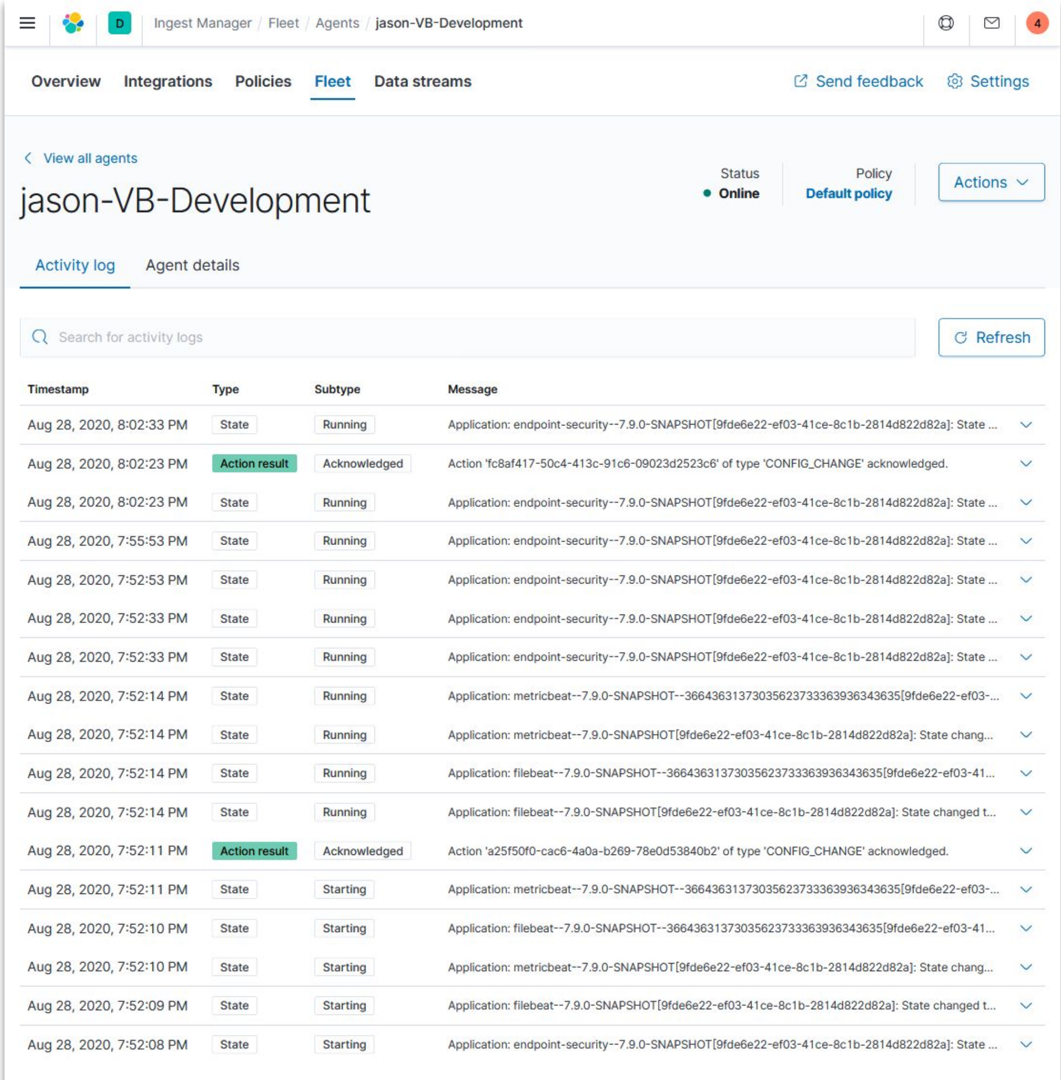
Fleet has detected that the selected agent policy, **Default policy**, is already in use by some of your agents. As a result of this action, Fleet will deploy updates to all agents that use this policy.

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

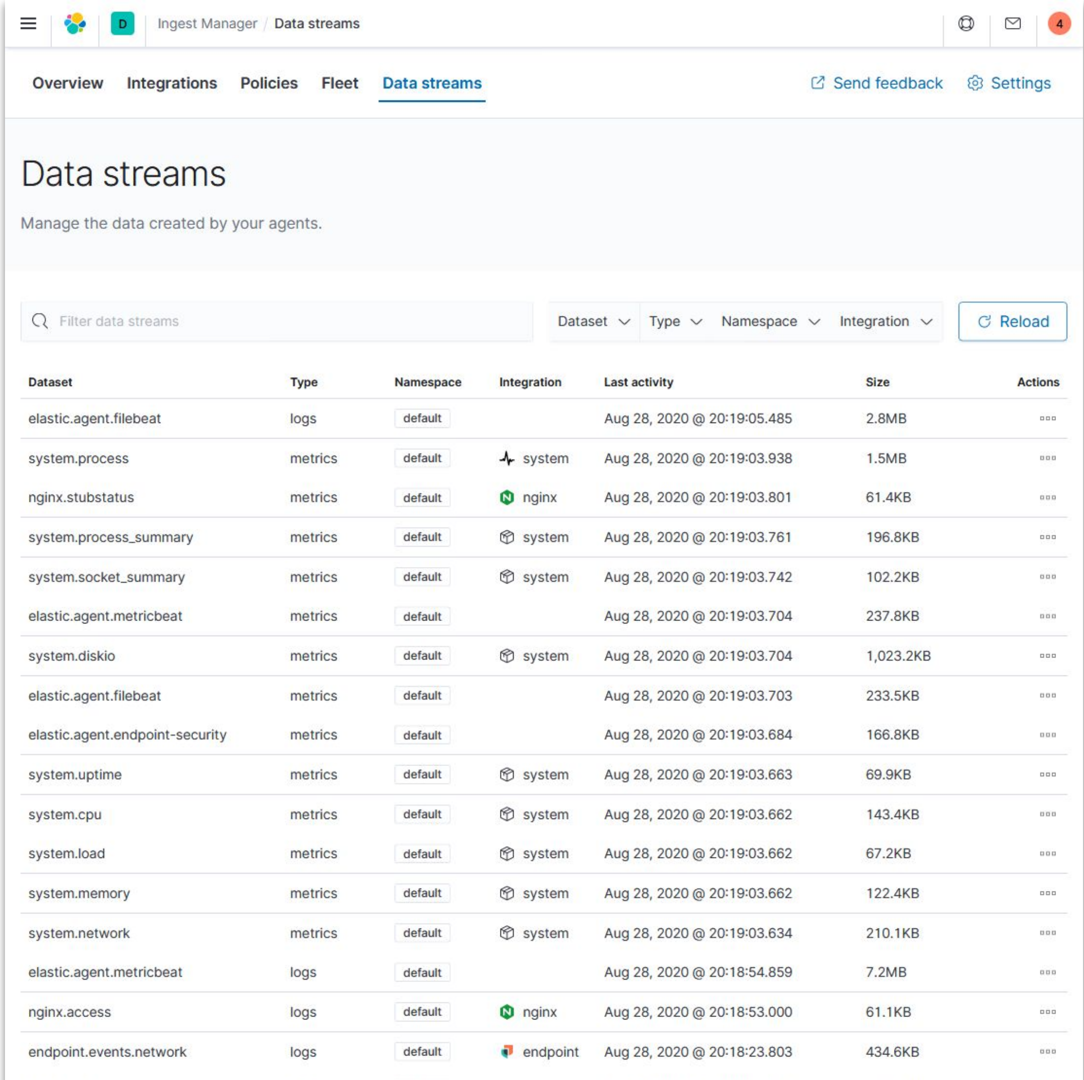


jason-VB-Development

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



Data streams

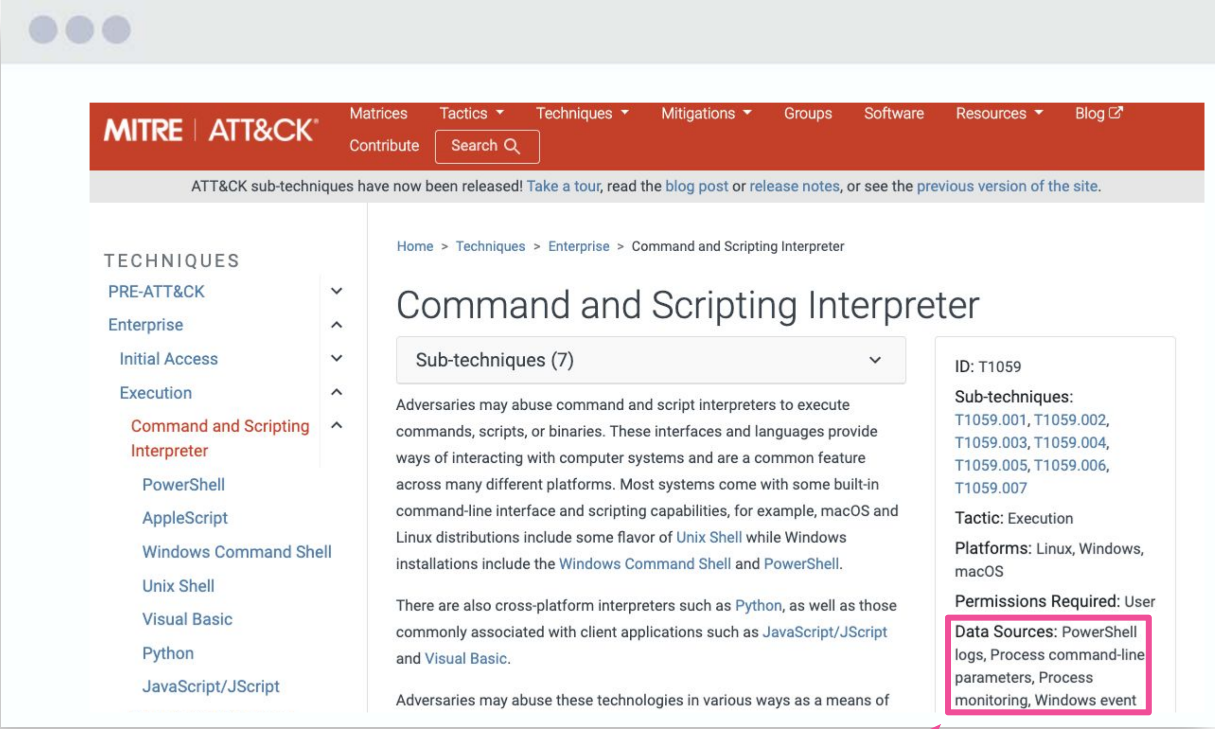
Manage the data created by your agents.

Dataset	Type	Namespace	Integration	Last activity	Size	Actions
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!



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.

Command and Scripting Interpreter

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

Plus over 40 more integrations

Support for 15+ common network and application security technologies

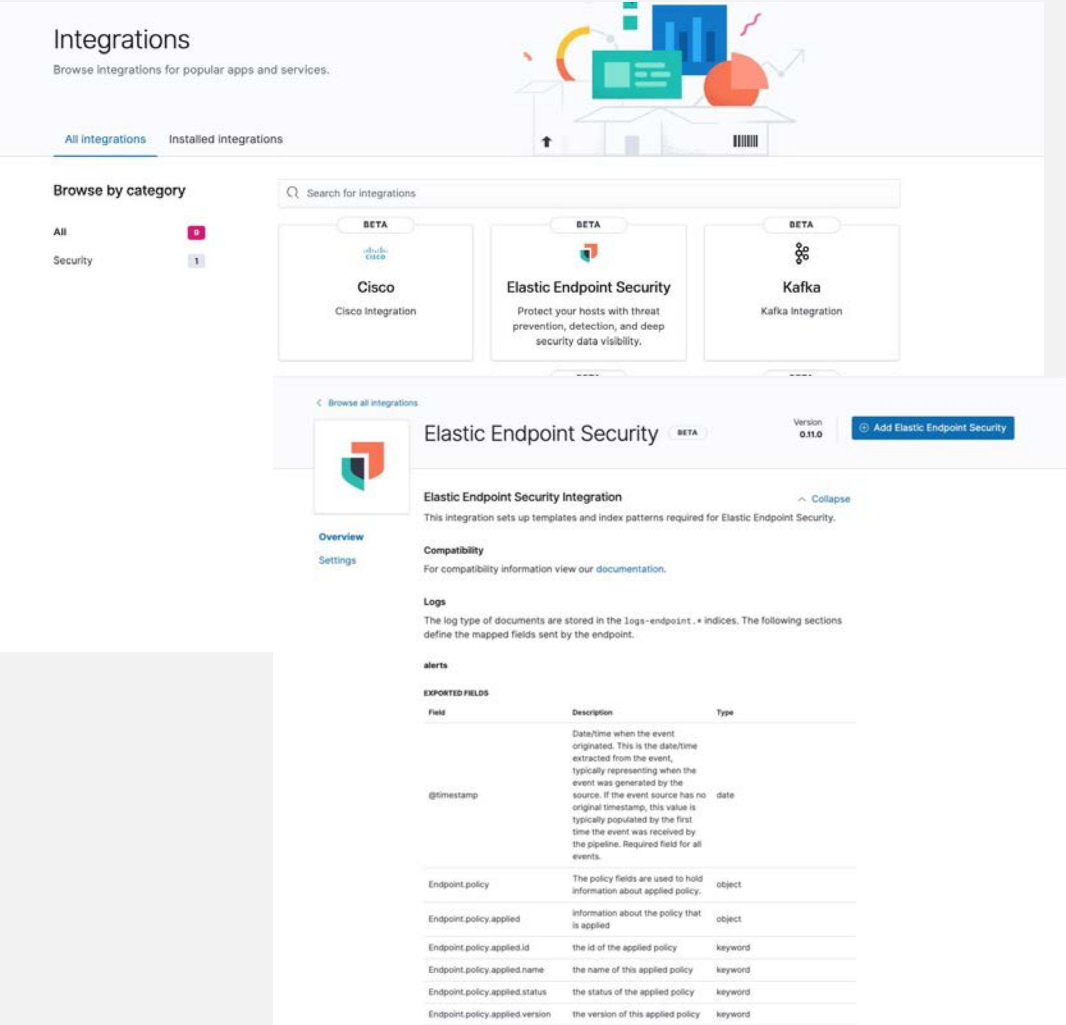
Barracuda
NETSCOUT
radware
imperva
BlackBerry CYLANCE
JUNIPER NETWORKS
zscaler
SONICWALL
f5
tenable
Infoblox
CiTRIX

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.

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

Elastic Endpoint Security

Elastic Endpoint Security Integration

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
@timestamp	Date/time 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
Endpoint.policy	The policy fields are used to hold information about applied policy.	object
Endpoint.policy.applied	information about the policy that is applied	object
Endpoint.policy.applied.id	the id of the applied policy	keyword
Endpoint.policy.applied.name	the name of this applied policy	keyword
Endpoint.policy.applied.status	the status of the applied policy	keyword
Endpoint.policy.applied.version	the version of this applied policy	keyword

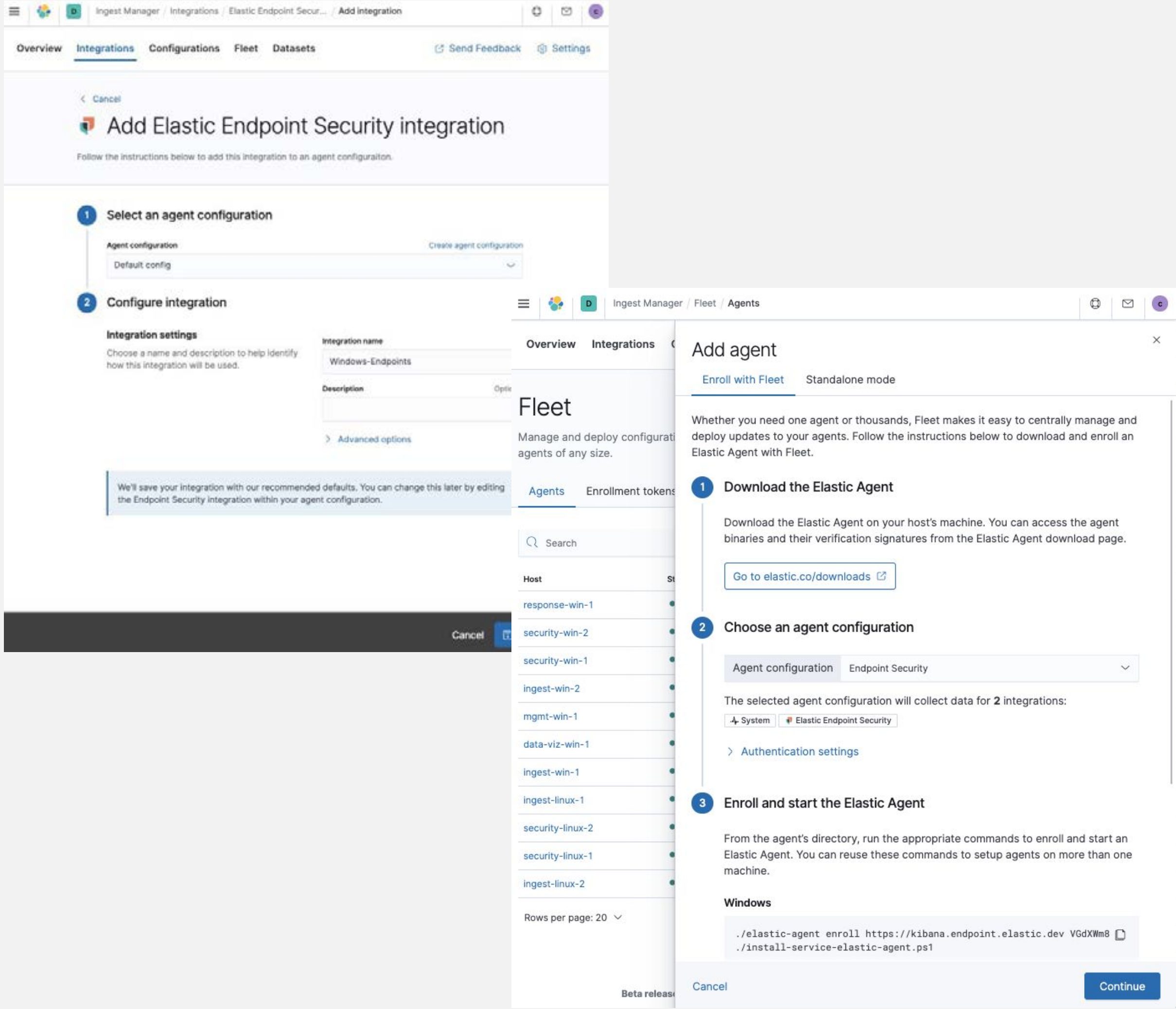
Protect your Hosts in 2 Clicks

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



Ingest Manager / Integrations / Elastic Endpoint Secur... / Add integration
Overview
Integrations
Configurations
Fleet
Datasets
Send Feedback
Settings
Cancel

Add Elastic Endpoint Security integration

Follow the instructions below to add this integration to an agent configuraiton.

1 Select an agent configuration

Agent configuration: Default config

Create agent configuration

2 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: Windows-Endpoints

Description Optio

We'll save your integration with our recommended defaults. You can change this later by editing the Endpoint Security integration within your agent configuration.

Fleet

Manage and deploy configurati agents of any size.

Host	St
response-win-1	
security-win-2	
security-win-1	
ingest-win-2	
mgmt-win-1	
data-viz-win-1	
ingest-win-1	
ingest-linux-1	
security-linux-2	
security-linux-1	
ingest-linux-2	

Rows per page: 20

Beta releas

Add agent

Whether you need one agent or thousands, Fleet makes it easy to centrally manage and deploy updates to your agents. Follow the instructions below to download and enroll an Elastic Agent with Fleet.

1 Download the Elastic Agent

Download the Elastic Agent on your host's machine. You can access the agent binaries and their verification signatures from the Elastic Agent download page.

2 Choose an agent configuration

Agent configuration: Endpoint Security

The selected agent configuration will collect data for **2** integrations:

System | Elastic Endpoint Security

3 Enroll and start the Elastic Agent

From the agent's directory, run the appropriate commands to enroll and start an Elastic Agent. You can reuse these commands to setup agents on more than one machine.

Windows

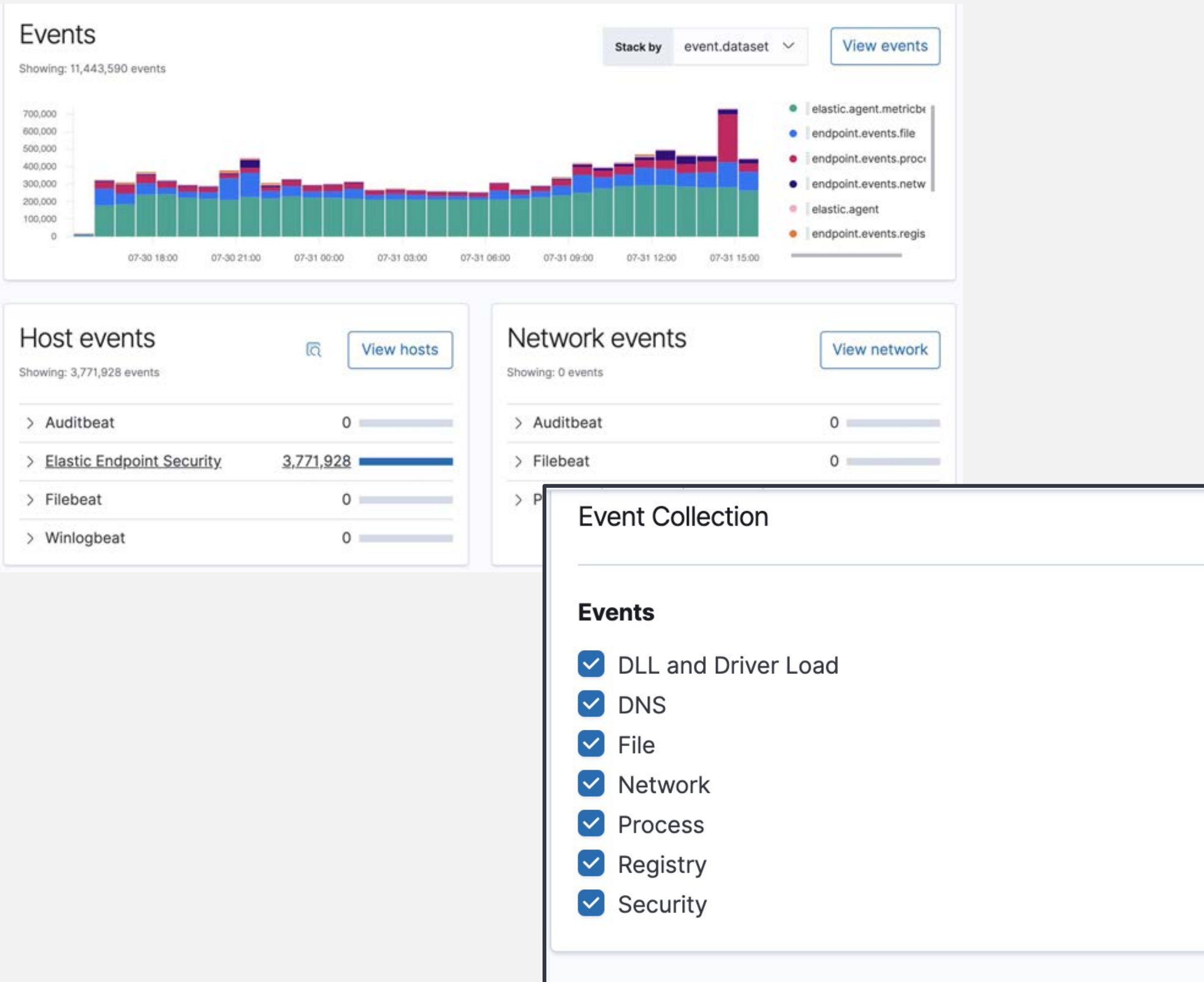
```
./elastic-agent enroll https://kibana.endpoint.elastic.dev VGdXWm8
./install-service-elastic-agent.ps1
```

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



Events

Showing: 11,443,590 events

Stack by: event.dataset

Host events

Showing: 3,771,928 events

Auditbeat	0
Elastic Endpoint Security	3,771,928
Filebeat	0
Winlogbeat	0

Network events

Showing: 0 events

Auditbeat	0
Filebeat	0
P	

Event Collection

Events

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

Stop Attacks

Malware Prevention

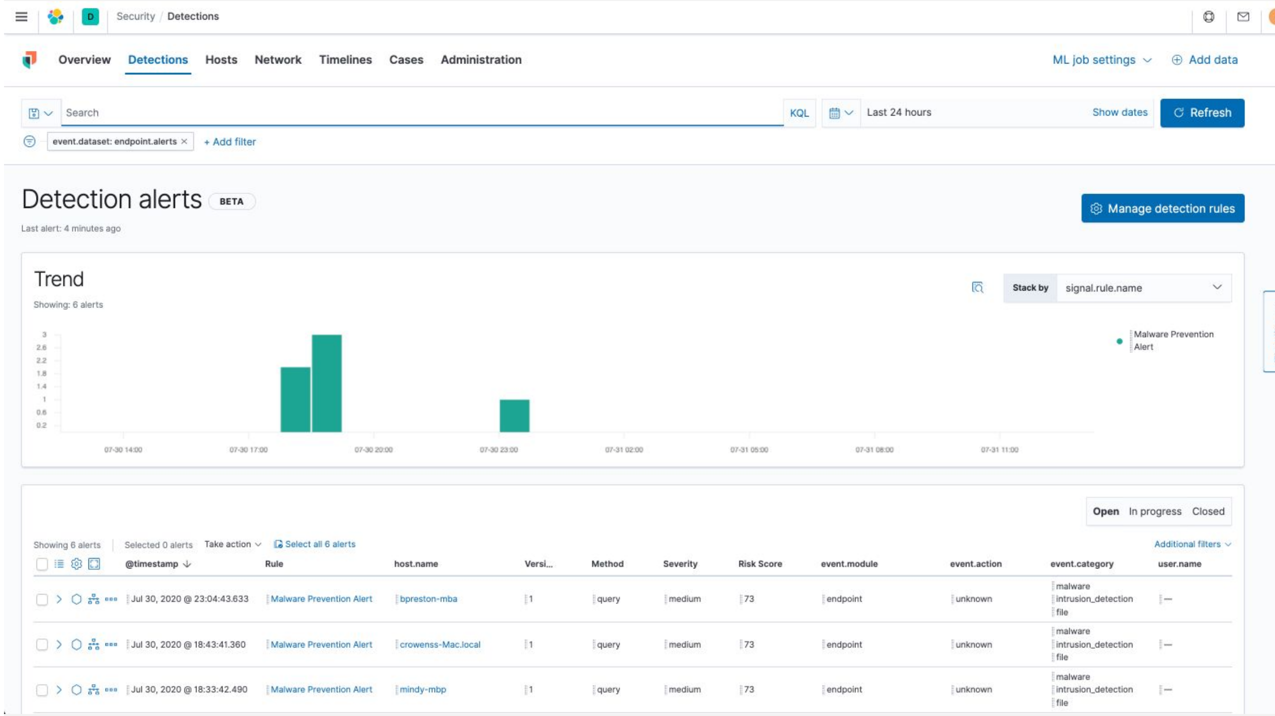
Machine Learning Malware Prevention proven to be over 99% effective at stopping malware*

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*



Detection alerts BETA

Last alert: 4 minutes ago

@timestamp	Rule	host.name	Versi...	Method	Severity	Risk Score	event.module	event.action	event.category	user.name
Jul 30, 2020 @ 23:04:43.633	Malware Prevention Alert	bpreston-mba	1	query	medium	73	endpoint	unknown	malware intrusion_detection file	—
Jul 30, 2020 @ 18:43:41.360	Malware Prevention Alert	crowenss-Mac.local	1	query	medium	73	endpoint	unknown	malware intrusion_detection file	—
Jul 30, 2020 @ 18:33:42.490	Malware Prevention Alert	mindy-mbp	1	query	medium	73	endpoint	unknown	malware intrusion_detection file	—

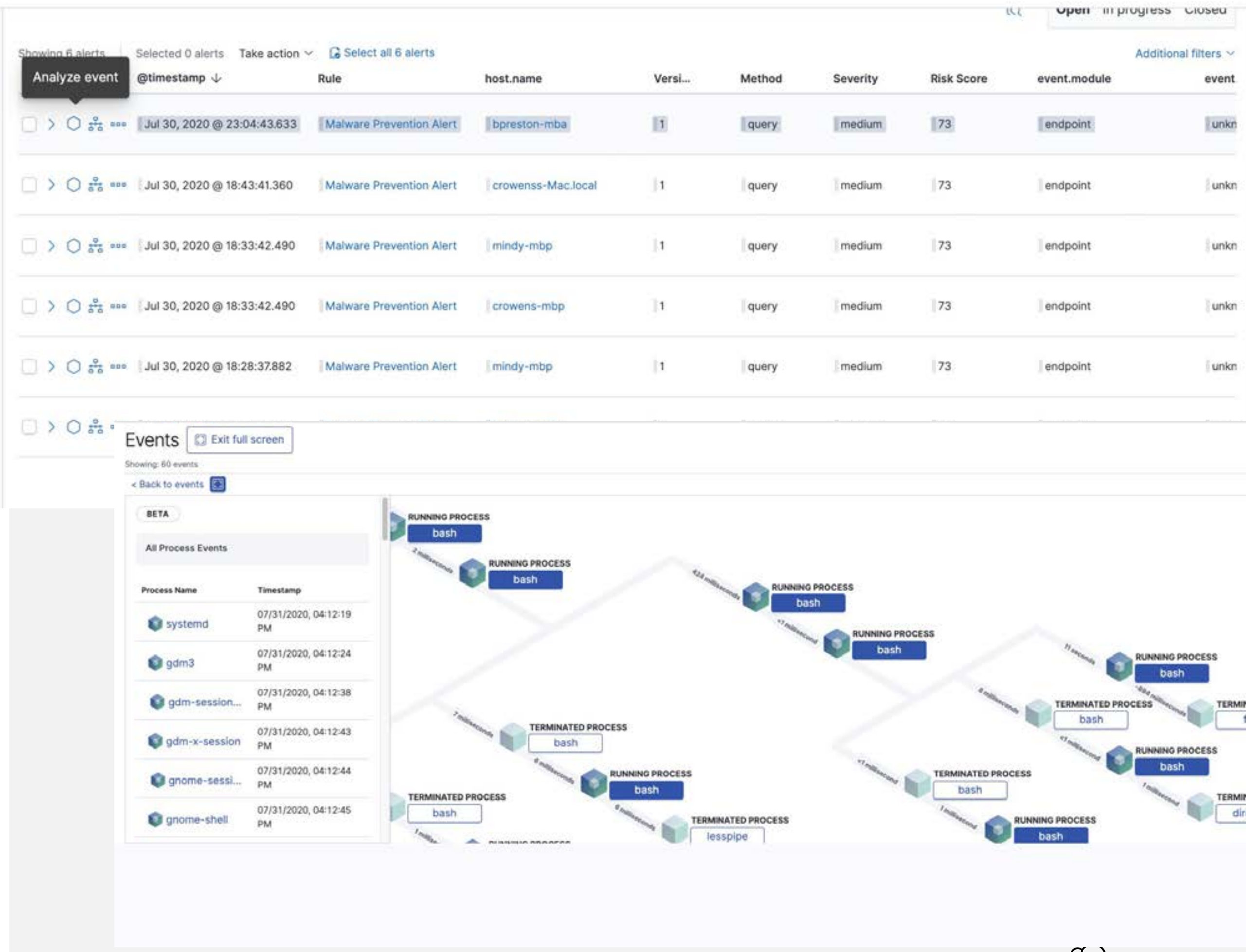
elastic

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



Open In progress Closed

Showing 6 alerts | Selected 0 alerts | Take action | Select all 6 alerts | Additional filters

Analyze event

@timestamp	Rule	host.name	Versi...	Method	Severity	Risk Score	event.module	event
Jul 30, 2020 @ 23:04:43.633	Malware Prevention Alert	bpreston-mba	1	query	medium	73	endpoint	unkn
Jul 30, 2020 @ 18:43:41.360	Malware Prevention Alert	crowenss-Mac.local	1	query	medium	73	endpoint	unkn
Jul 30, 2020 @ 18:33:42.490	Malware Prevention Alert	mindy-mbp	1	query	medium	73	endpoint	unkn
Jul 30, 2020 @ 18:33:42.490	Malware Prevention Alert	crowens-mbp	1	query	medium	73	endpoint	unkn
Jul 30, 2020 @ 18:28:37.882	Malware Prevention Alert	mindy-mbp	1	query	medium	73	endpoint	unkn

Events | Exit full screen

Showing: 60 events

< Back to events

BETA

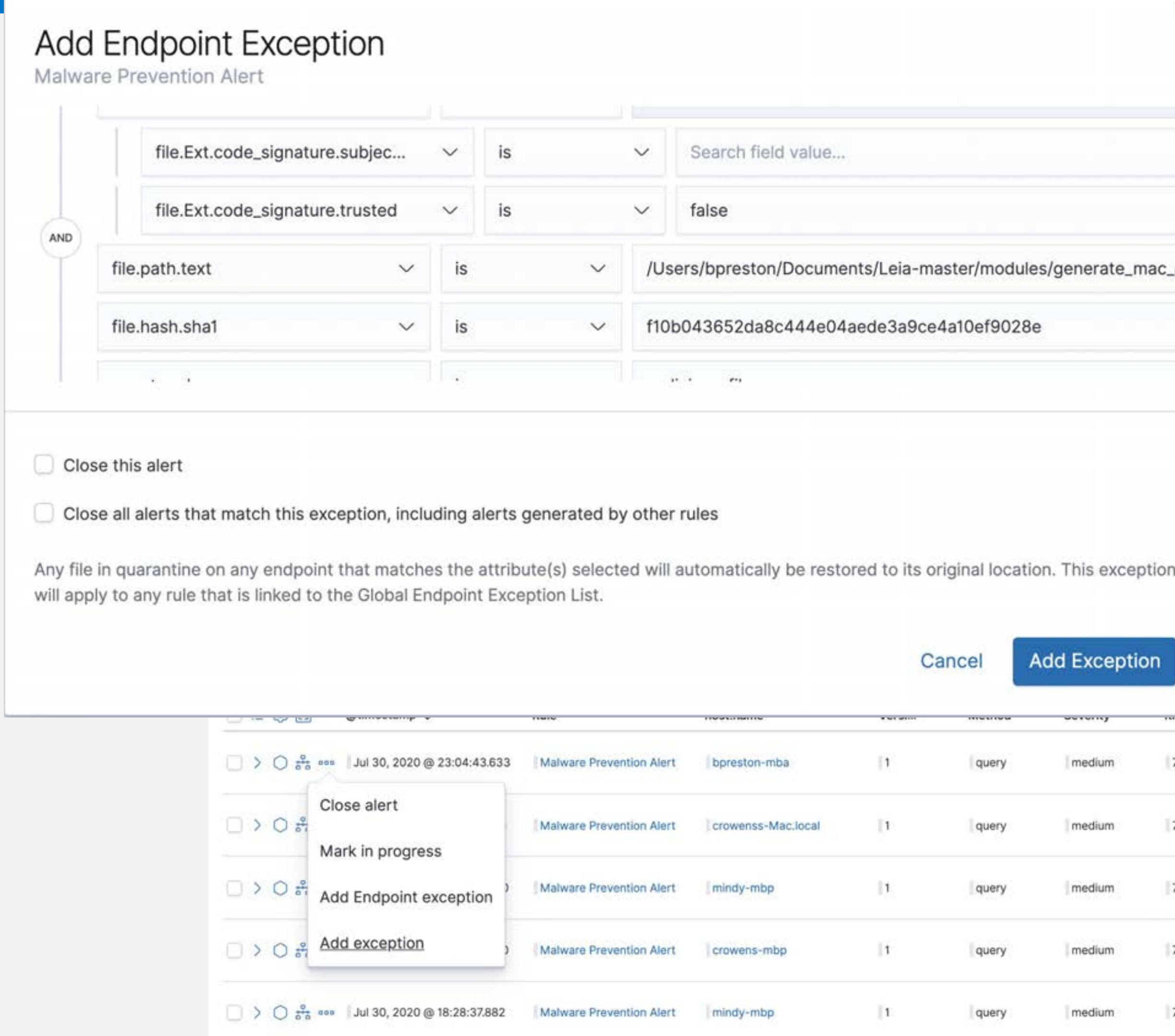
All Process Events

Process Name	Timestamp
systemd	07/31/2020, 04:12:19 PM
gdm3	07/31/2020, 04:12:24 PM
gdm-session...	07/31/2020, 04:12:38 PM
gdm-x-session	07/31/2020, 04:12:43 PM
gnome-sessi...	07/31/2020, 04:12:44 PM
gnome-shell	07/31/2020, 04:12:45 PM

Eliminate False Positives

Exception workflow for all alerts

Apply exceptions all the way down to the endpoint



Add Endpoint Exception

Malware Prevention Alert

file.Ext.code_signature.subjec... 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

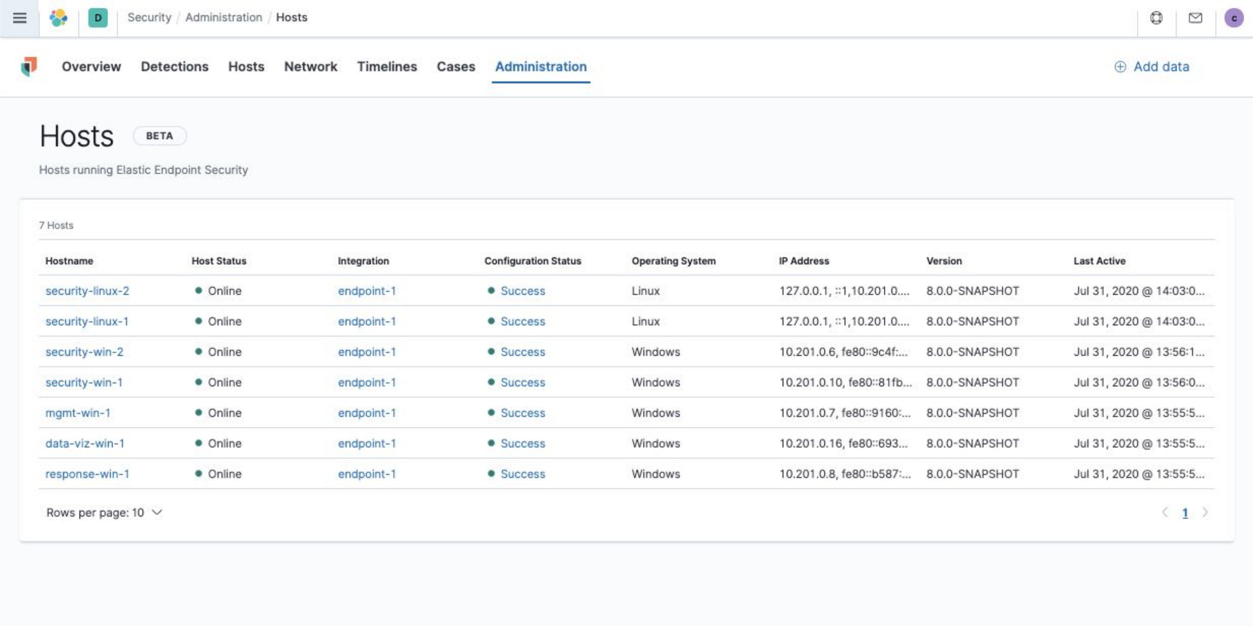
☐ Close this alert

☐ 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.

Jul 30, 2020 @ 23:04:43.633	Malware Prevention Alert	bpreston-mba	1	query	medium
	Malware Prevention Alert	crowenss-Mac.local	1	query	medium
	Malware Prevention Alert	mindy-mbp	1	query	medium
	Malware Prevention Alert	crowens-mbp	1	query	medium
Jul 30, 2020 @ 18:28:37.882	Malware Prevention Alert	mindy-mbp	1	query	medium

View Hosts Running Endpoint Security



Hosts BETA

Hosts running Elastic Endpoint Security

7 Hosts

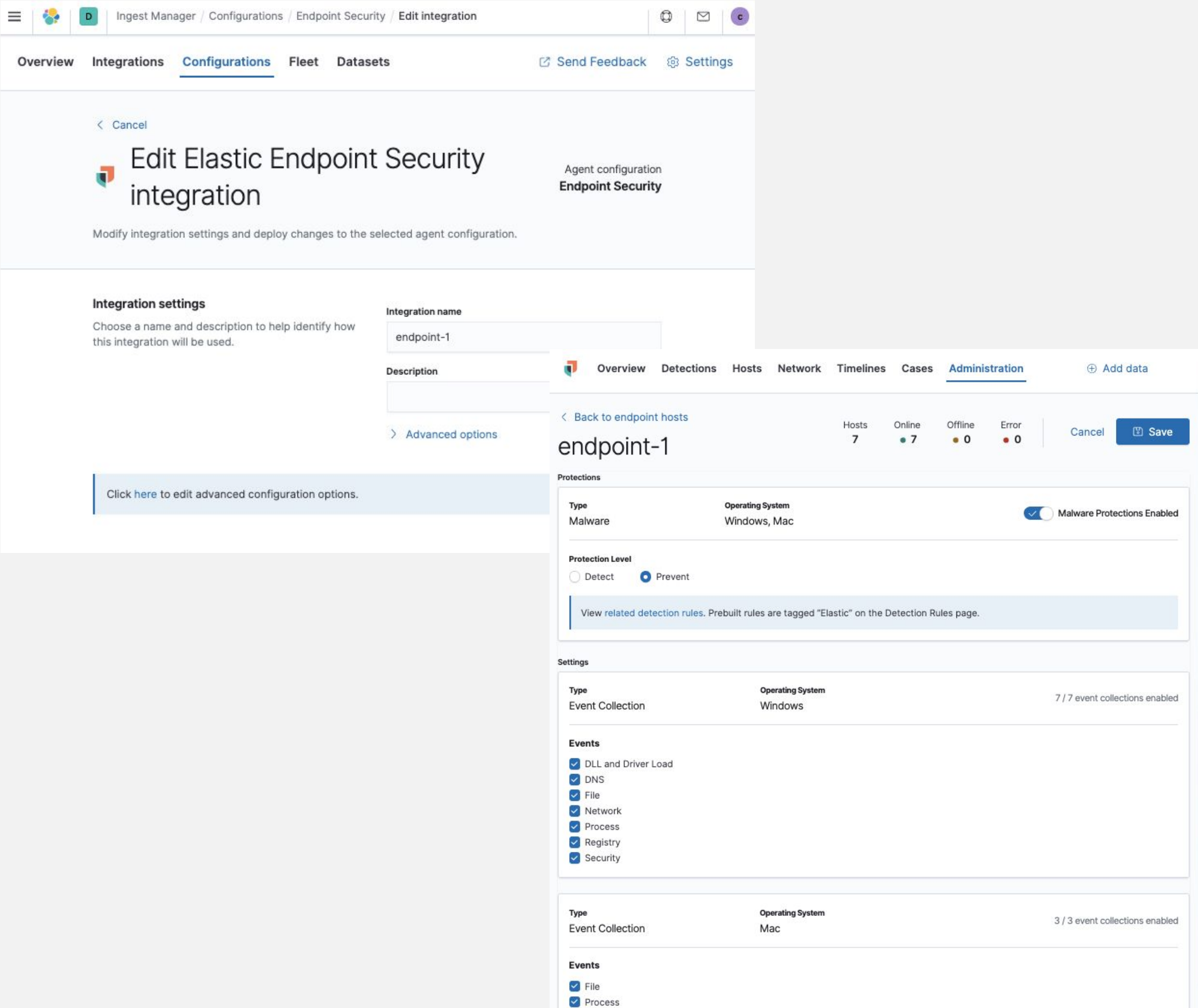
Hostname	Host Status	Integration	Configuration Status	Operating System	IP Address	Version	Last Active
security-linux-2	● Online	endpoint-1	● Success	Linux	127.0.0.1, ::1,10.201.0....	8.0.0-SNAPSHOT	Jul 31, 2020 @ 14:03:0...
security-linux-1	● Online	endpoint-1	● Success	Linux	127.0.0.1, ::1,10.201.0....	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...

Rows per page: 10

Full Configurability and Control

Change the configuration to meet your needs

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



Edit Elastic Endpoint Security integration

Agent configuration
Endpoint Security

Modify integration settings and deploy changes to the selected agent configuration.

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: endpoint-1

Description:

Click here to edit advanced configuration options.

endpoint-1

Hosts	Online	Offline	Error
7	● 7	● 0	● 0

Protections

Type: Malware
Operating System: Windows, Mac
Malware Protections Enabled

Protection Level
○ Detect ● Prevent

View related detection rules. Prebuilt rules are tagged "Elastic" on the Detection Rules page.

Settings

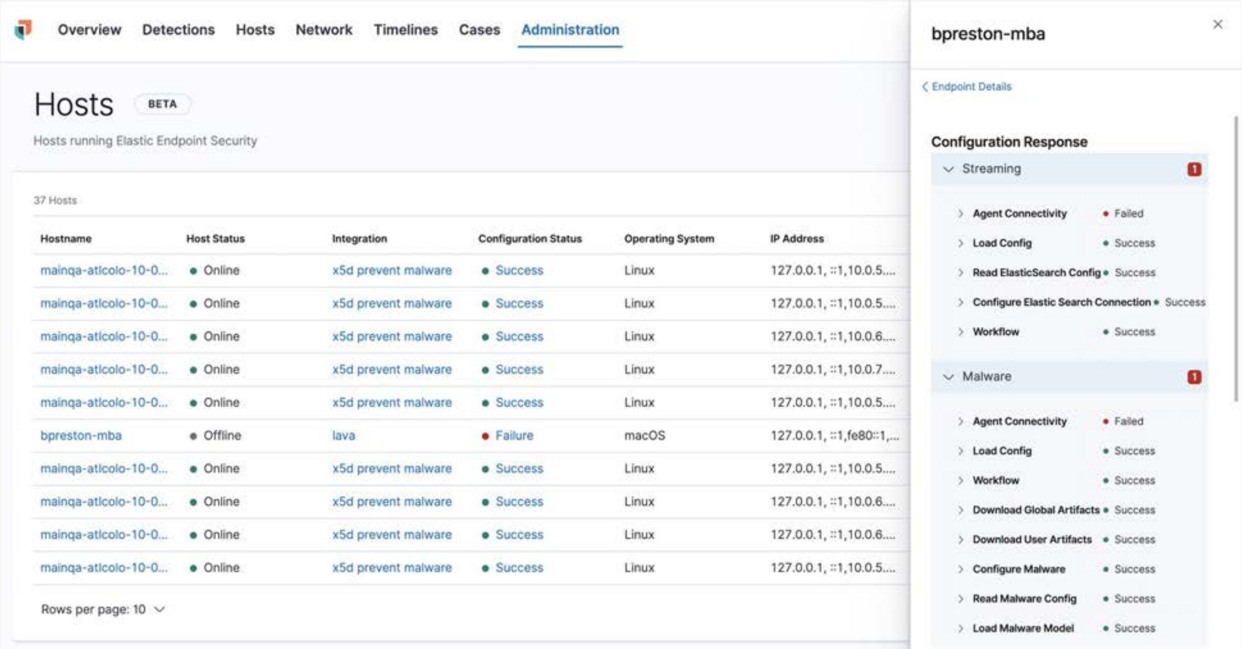
Type: Event Collection
Operating System: Windows
7 / 7 event collections enabled

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

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

Events
- ☑ File
- ☑ Process

Error Reporting



Hosts BETA

Hosts running Elastic Endpoint Security

37 Hosts

Hostname	Host Status	Integration	Configuration Status	Operating System	IP Address
mainqa-atlcolo-10-0...	● Online	x5d prevent malware	● Success	Linux	127.0.0.1, ::1,10.0.5....
mainqa-atlcolo-10-0...	● Online	x5d prevent malware	● Success	Linux	127.0.0.1, ::1,10.0.5....
mainqa-atlcolo-10-0...	● Online	x5d prevent malware	● Success	Linux	127.0.0.1, ::1,10.0.6....
mainqa-atlcolo-10-0...	● Online	x5d prevent malware	● Success	Linux	127.0.0.1, ::1,10.0.7....
mainqa-atlcolo-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-atlcolo-10-0...	● Online	x5d prevent malware	● Success	Linux	127.0.0.1, ::1,10.0.5....
mainqa-atlcolo-10-0...	● Online	x5d prevent malware	● Success	Linux	127.0.0.1, ::1,10.0.6....
mainqa-atlcolo-10-0...	● Online	x5d prevent malware	● Success	Linux	127.0.0.1, ::1,10.0.6....
mainqa-atlcolo-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

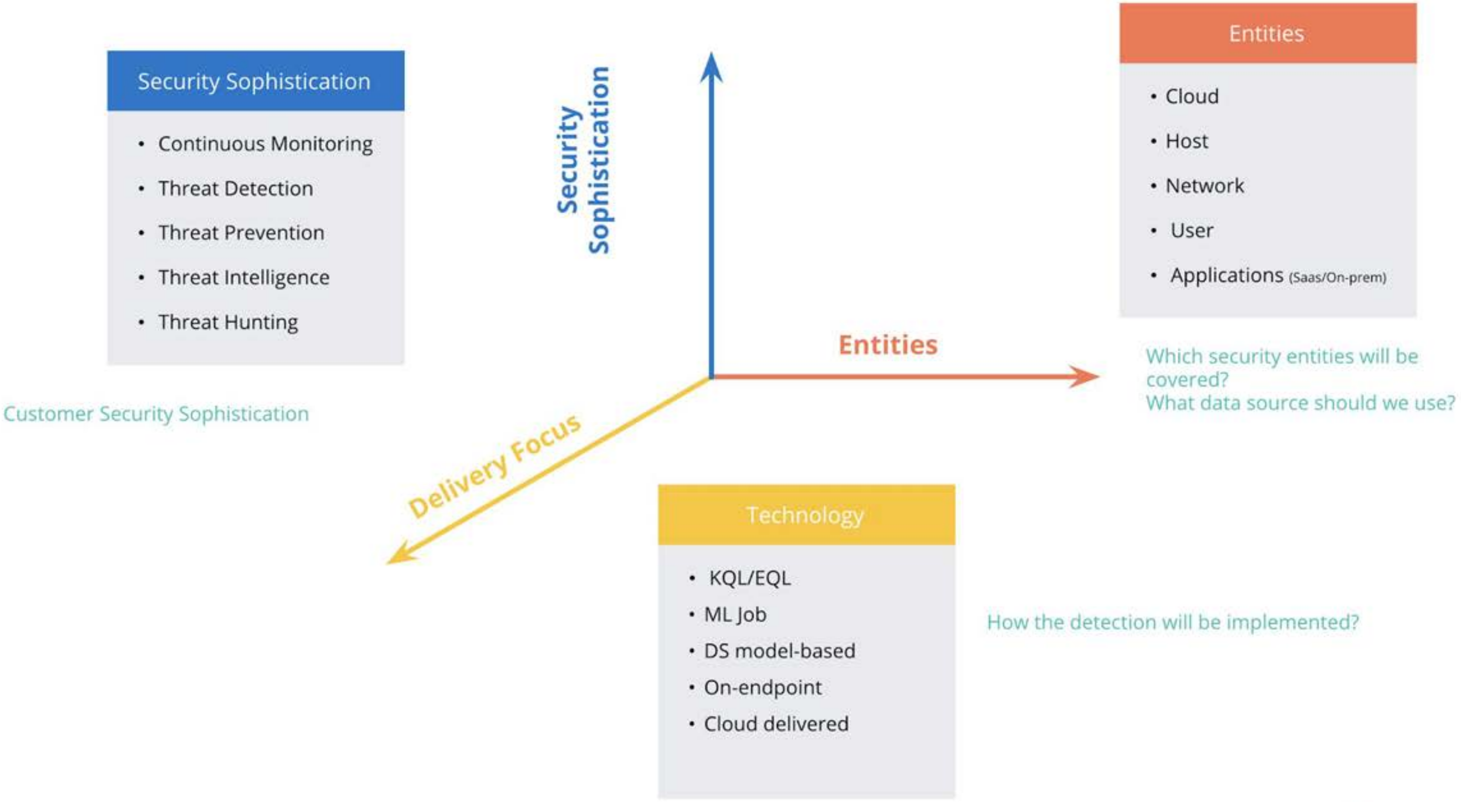
Agent Connectivity	● Failed
Load Config	● Success
Workflow	● Success
Download Global Artifacts	● Success
Download User Artifacts	● Success
Configure Malware	● Success
Read Malware Config	● Success
Load Malware Model	● Success

Prebuilt protections and expanded detection methods

elastic

The Cube

Turn-key protections across the organization



Security Sophistication

- Continuous Monitoring
- Threat Detection
- Threat Prevention
- Threat Intelligence
- Threat Hunting

Customer Security Sophistication

Entities

- Cloud
- Host
- Network
- User
- Applications (Saas/On-prem)

Which security entities will be covered?
What data source should we use?

Technology

- KQL/EQL
- ML Job
- DS model-based
- On-endpoint
- Cloud delivered

How the detection will be implemented?

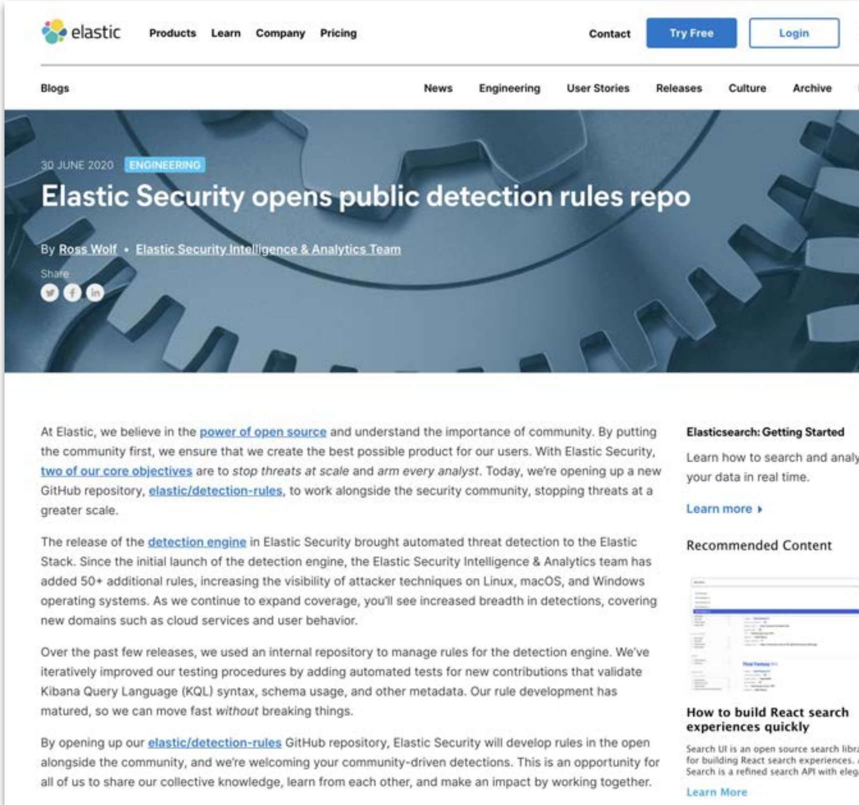
Stop threats at scale...

You know, in a free and open way

Elastic Security Detections Repository

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

- [elastic/detection-rules]
- [Release Blog]



30 JUNE 2020 ENGINEERING

Elastic Security opens public detection rules repo

By Ross Wolf • Elastic Security Intelligence & Analytics Team

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.

Elasticsearch: Getting Started

Learn how to search and analy
your data in real time.

Learn more ›

Recommended Content

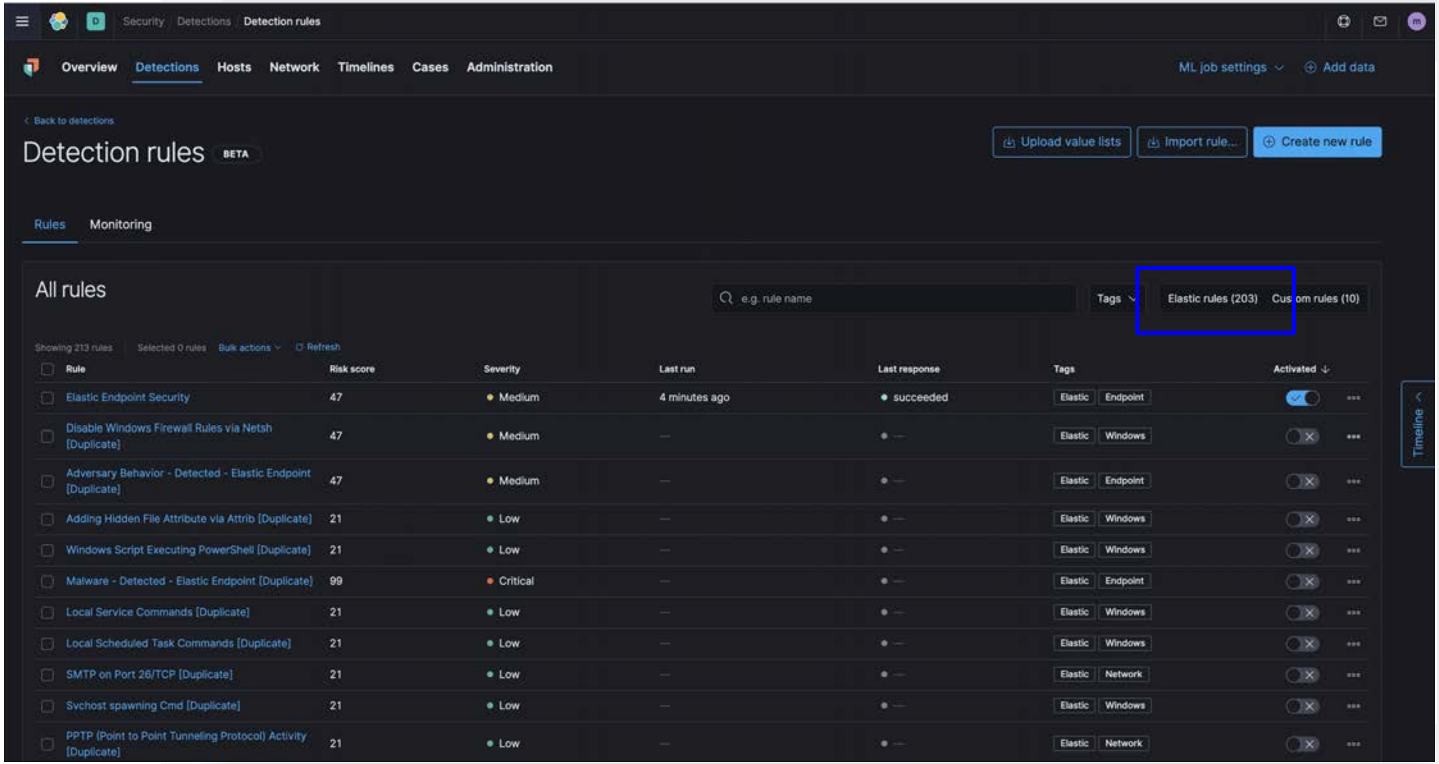
How to build React search experiences quickly

Search UI is an open source search libra
for building React search experiences.
Search is a refined search API with eleg

Learn More

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



Detection rules BETA

All rules

Elastic rules (203) Custom rules (10)

Showing 213 rules | Selected 0 rules Bulk actions Refresh

Rule	Risk score	Severity	Last run	Last response	Tags	Activated ↓
Elastic Endpoint Security	47	● Medium	4 minutes ago	● succeeded	Elastic Endpoint	✓
Disable Windows Firewall Rules via Netsh [Duplicate]	47	● Medium	—	● —	Elastic Windows	✗
Adversary Behavior - Detected - Elastic Endpoint [Duplicate]	47	● Medium	—	● —	Elastic Endpoint	✗
Adding Hidden File Attribute via Attrib [Duplicate]	21	● Low	—	● —	Elastic Windows	✗
Windows Script Executing PowerShell [Duplicate]	21	● Low	—	● —	Elastic Windows	✗
Malware - Detected - Elastic Endpoint [Duplicate]	99	● Critical	—	● —	Elastic Endpoint	✗
Local Service Commands [Duplicate]	21	● Low	—	● —	Elastic Windows	✗
Local Scheduled Task Commands [Duplicate]	21	● Low	—	● —	Elastic Windows	✗
SMTP on Port 26/TCP [Duplicate]	21	● Low	—	● —	Elastic Network	✗
Svchost spawning Cmd [Duplicate]	21	● Low	—	● —	Elastic Windows	✗
PPTP (Point to Point Tunneling Protocol) Activity [Duplicate]	21	● Low	—	● —	Elastic Network	✗

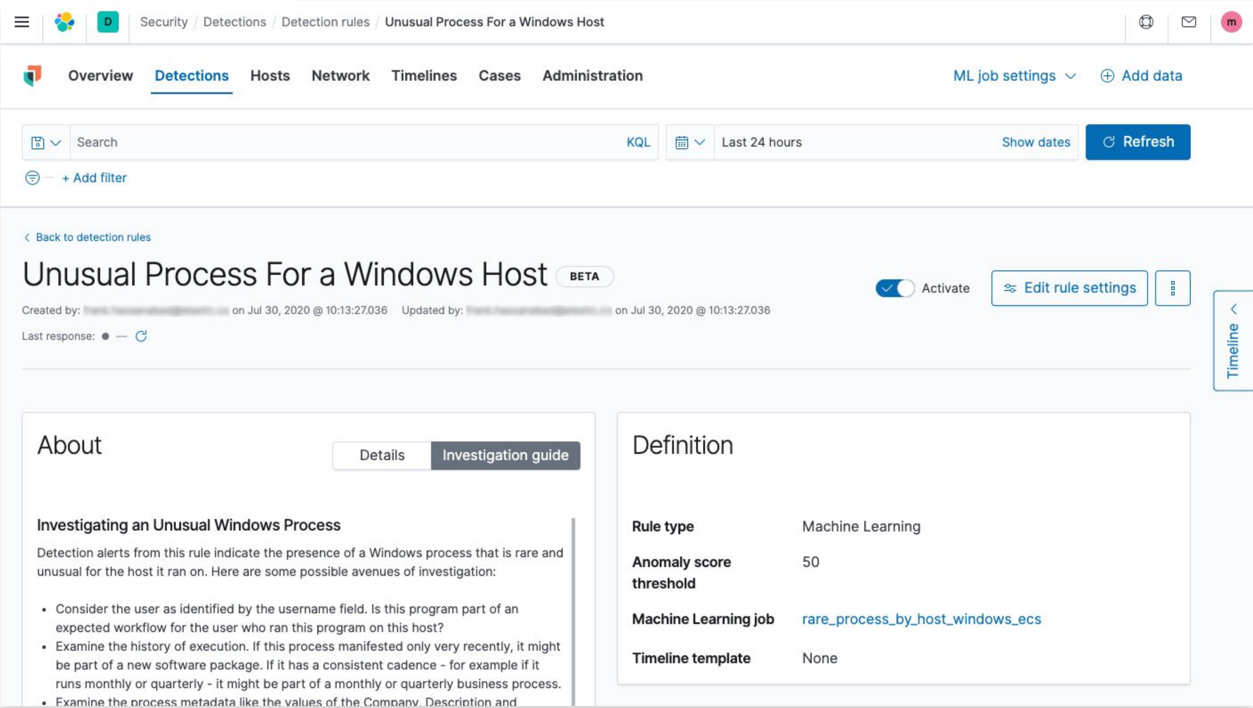
Streamlined analyst workflows

License | Beta

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



Unusual Process For a Windows Host BETA

Created by: [redacted] on Jul 30, 2020 @ 10:13:27.036 Updated by: [redacted] on Jul 30, 2020 @ 10:13:27.036

Last response: ● —

About

Investigating an Unusual Windows Process

Detection alerts from this rule indicate the presence of a Windows process that is rare and unusual for the host it ran on. Here are some possible avenues of investigation:

- 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

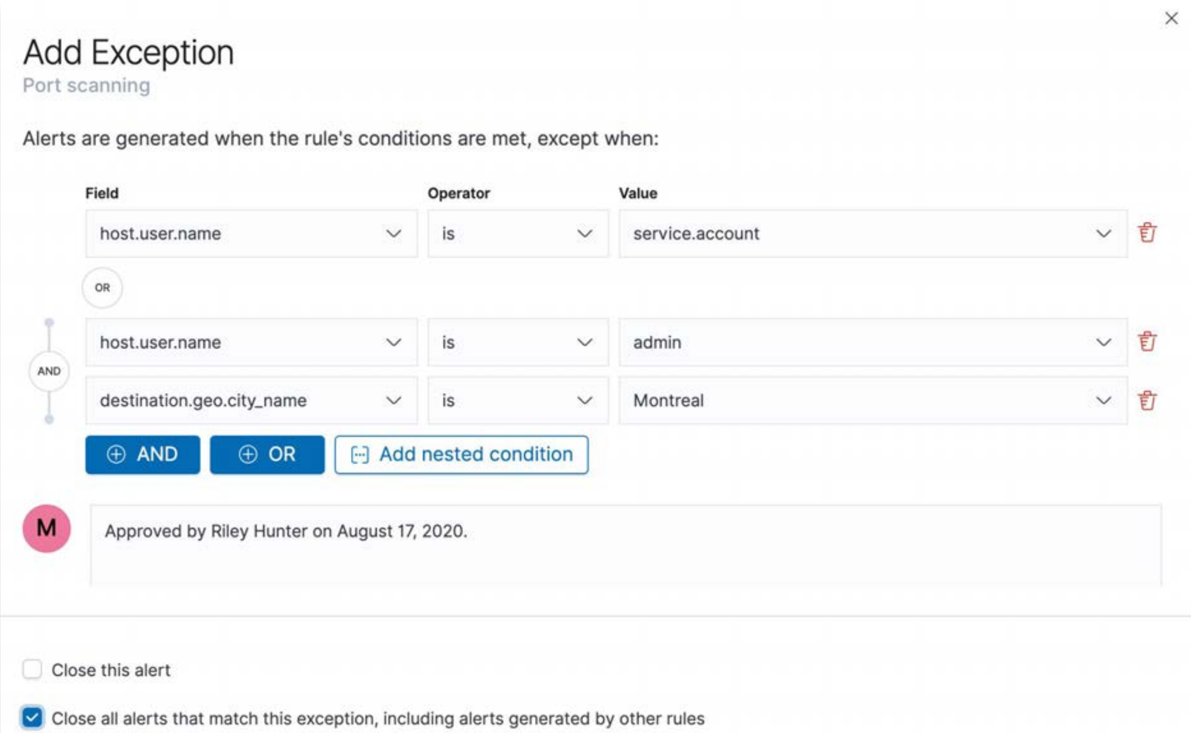
Definition

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

License | Beta

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		
host.user.name	is	admin
AND		
destination.geo.city_name	is	Montreal

Approved by Riley Hunter on August 17, 2020.

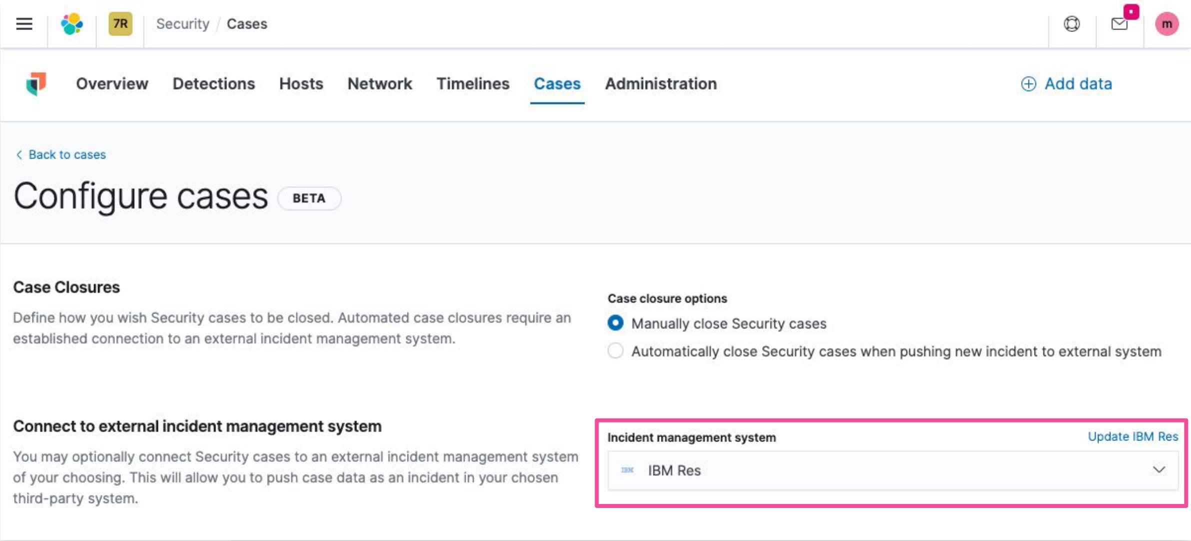
□ Close this alert

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

License | Beta

IBM Security Resilient integration

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



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: IBM Res

Update IBM Res

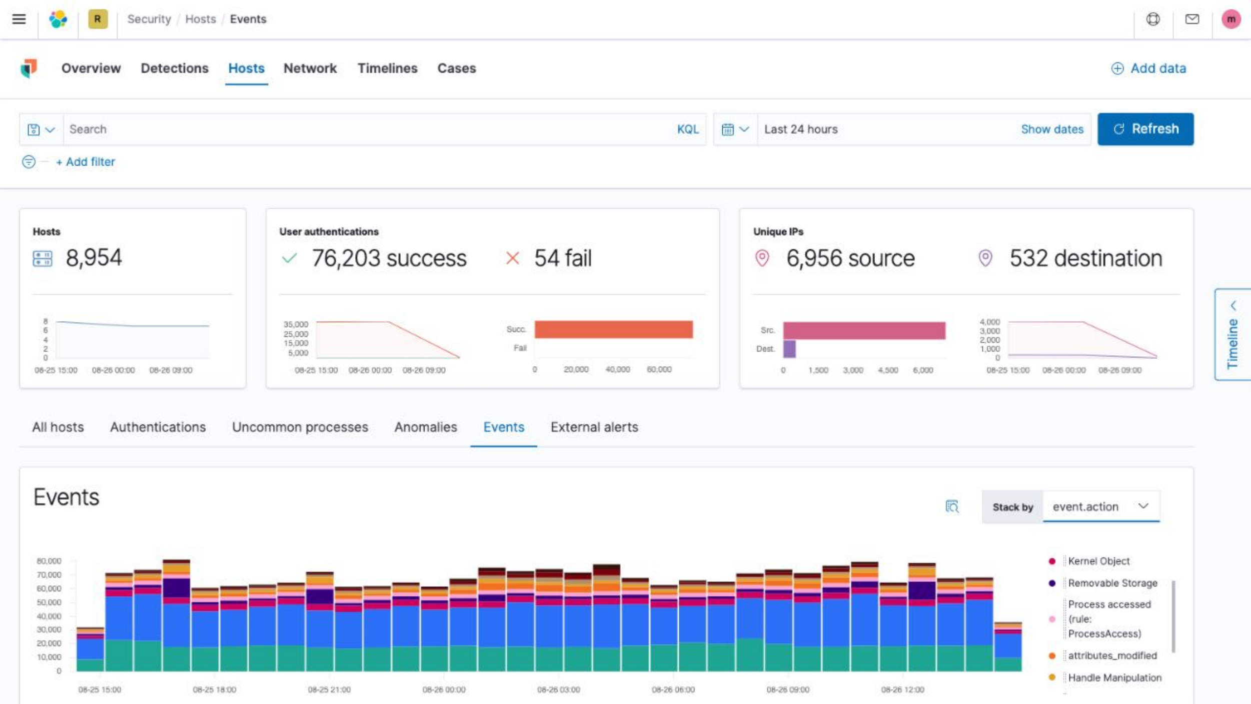
License | Beta / GA

Further analyst workflow enhancements

Full-screen mode and infinite scroll put analysts in control

Customizable timeline templates enable curated views for specific alerts

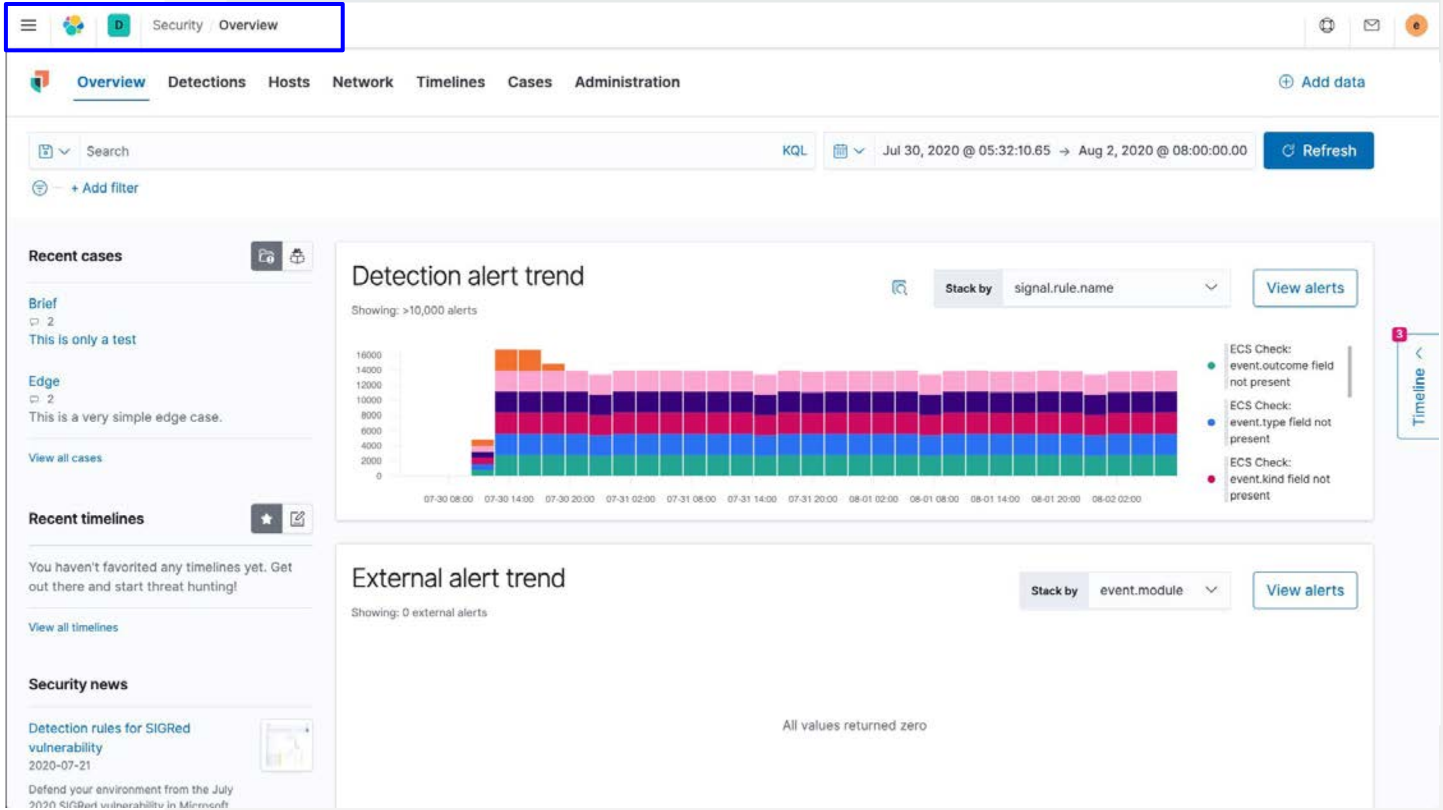
Other enhancements fulfill requests from our global community



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”



Showing: >10,000 alerts

- ● ECS Check: event.outcome field not present
- ● ECS Check: event.type field not present
- ● ECS Check: event.kind field not present

Brief
2
This is only a test

Edge
2
This is a very simple edge case.

View all cases

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Showing: 0 external alerts

All values returned zero

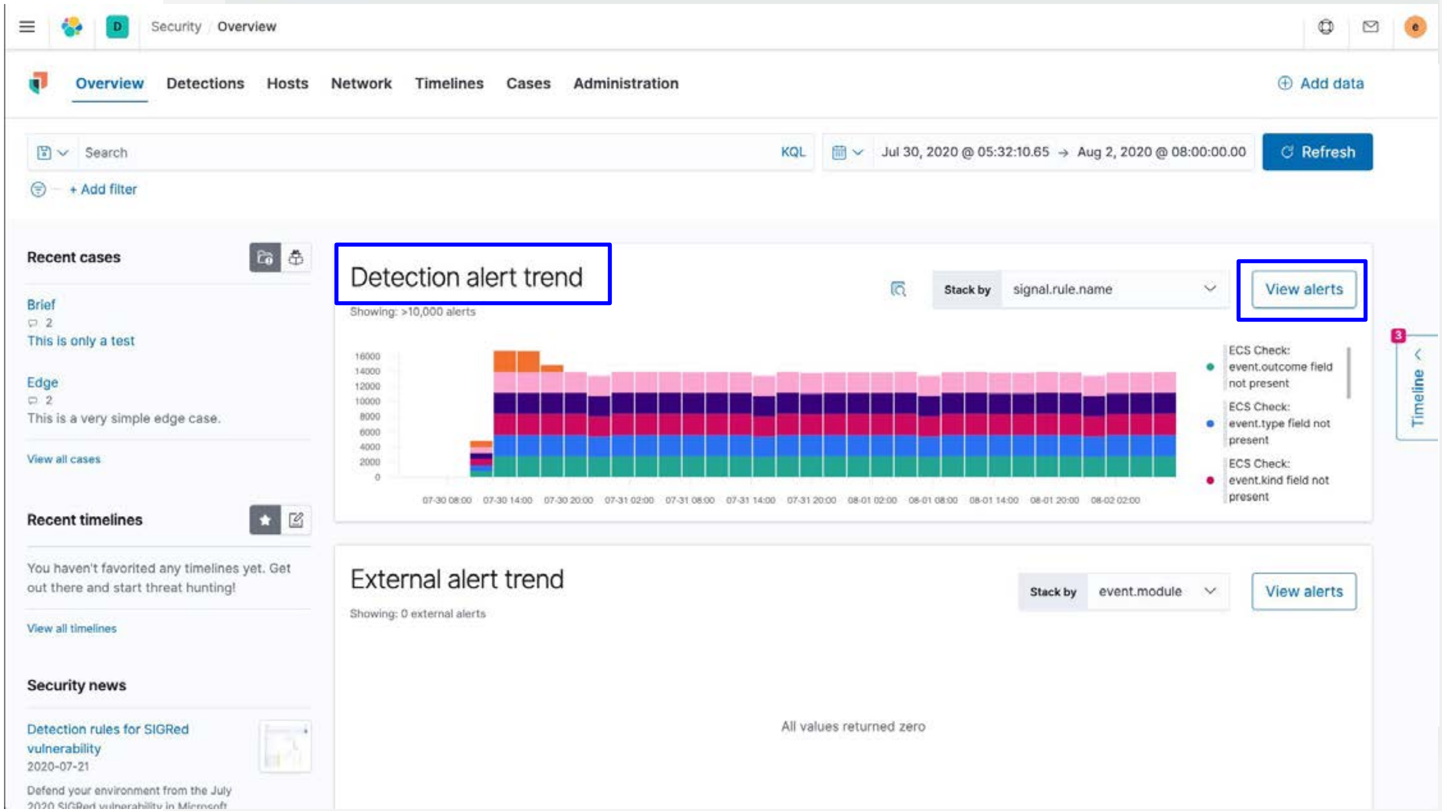
Detection rules for SIGRed vulnerability
2020-07-21

Defend your environment from the July 2020 SIGRed vulnerability in Microsoft

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.



Recent cases

Brief
2
This is only a test

Edge
2
This is a very simple edge case.

View all cases

Recent timelines

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Security news

Detection rules for SIGRed vulnerability
2020-07-21
Defend your environment from the July 2020 SIGRed vulnerability in Microsoft

Detection alert trend
Showing: >10,000 alerts
Stack by signal.rule.name
View alerts

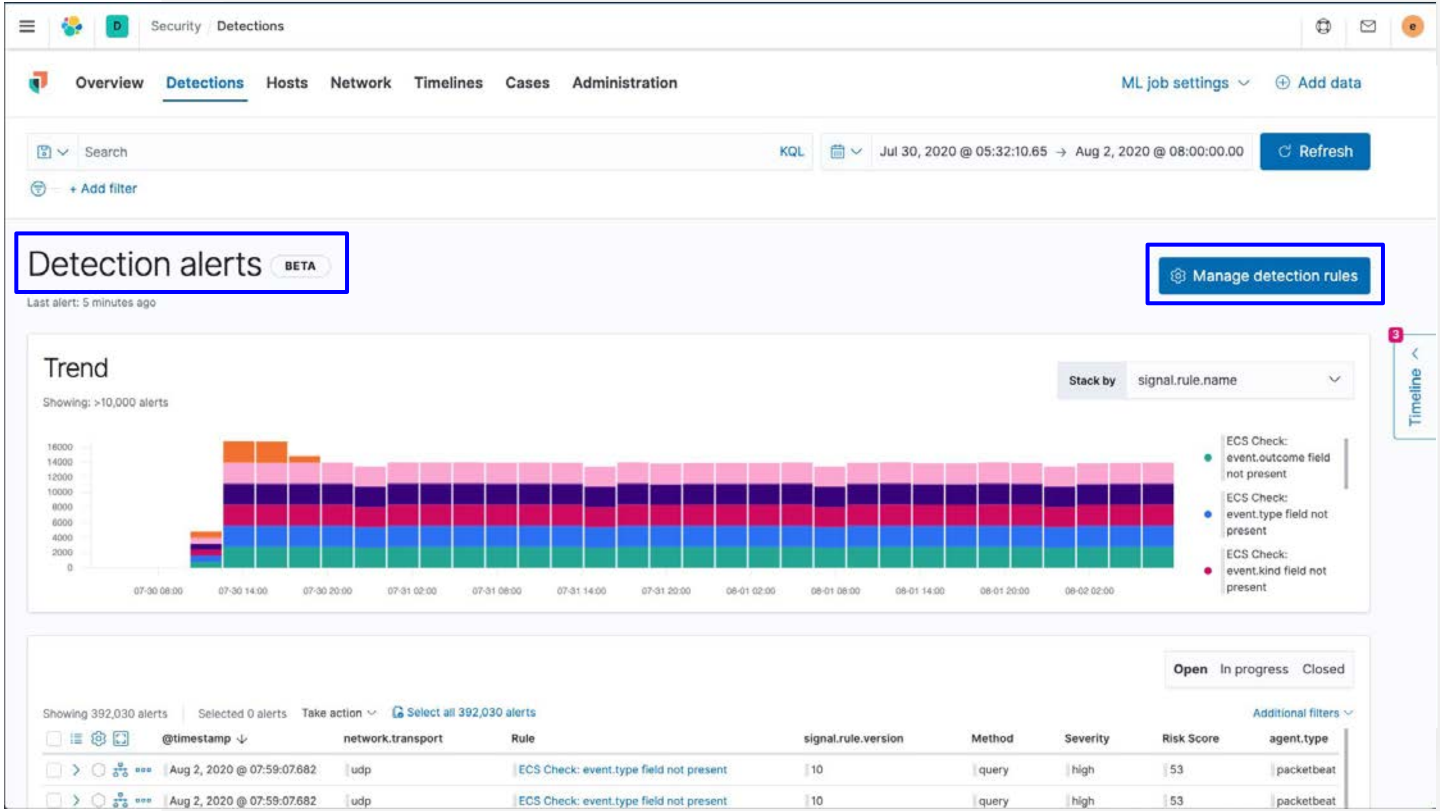
External alert trend
Showing: 0 external alerts
Stack by event.module
View alerts

All values returned zero

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.”



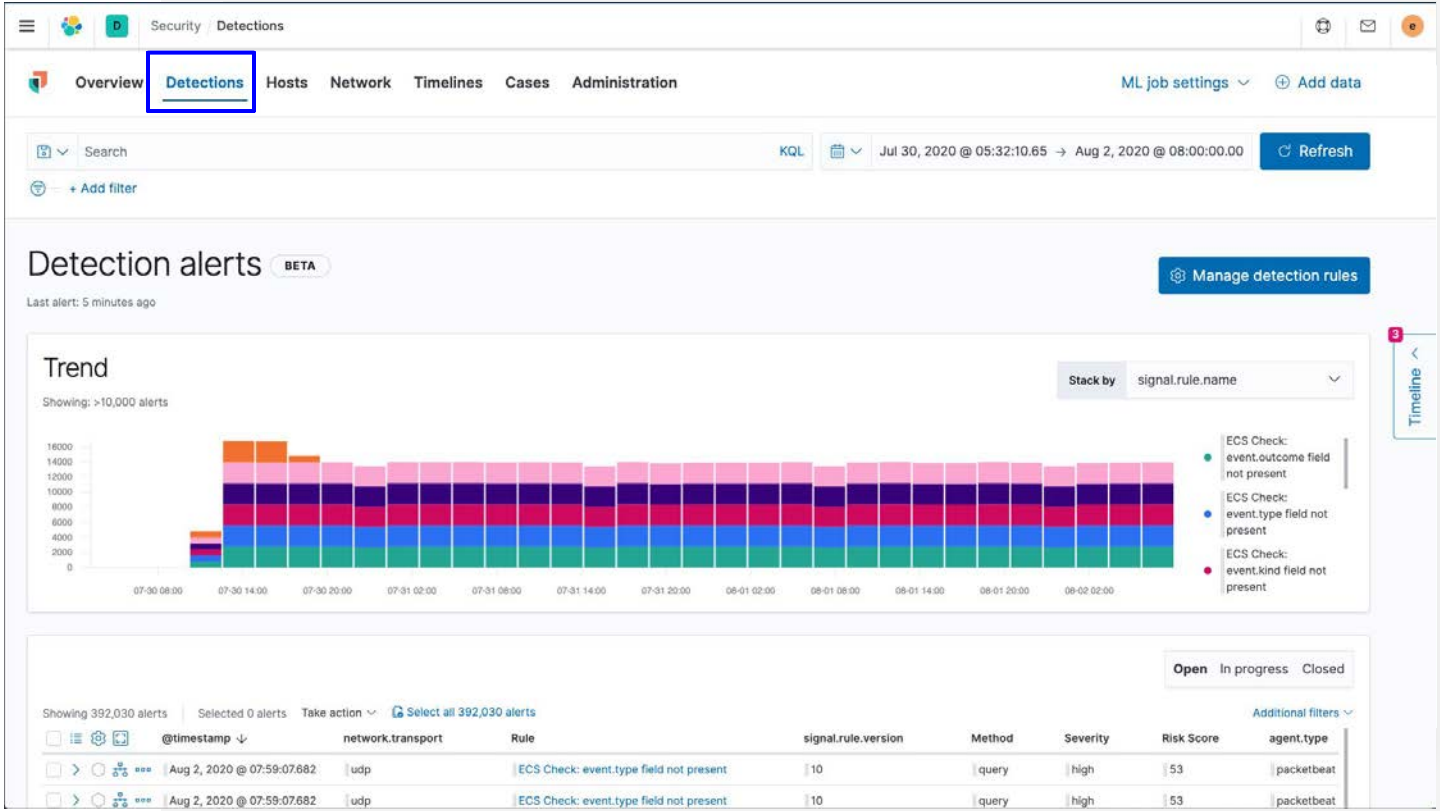
Showing 392,030 alerts   Selected 0 alerts

@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 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

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.

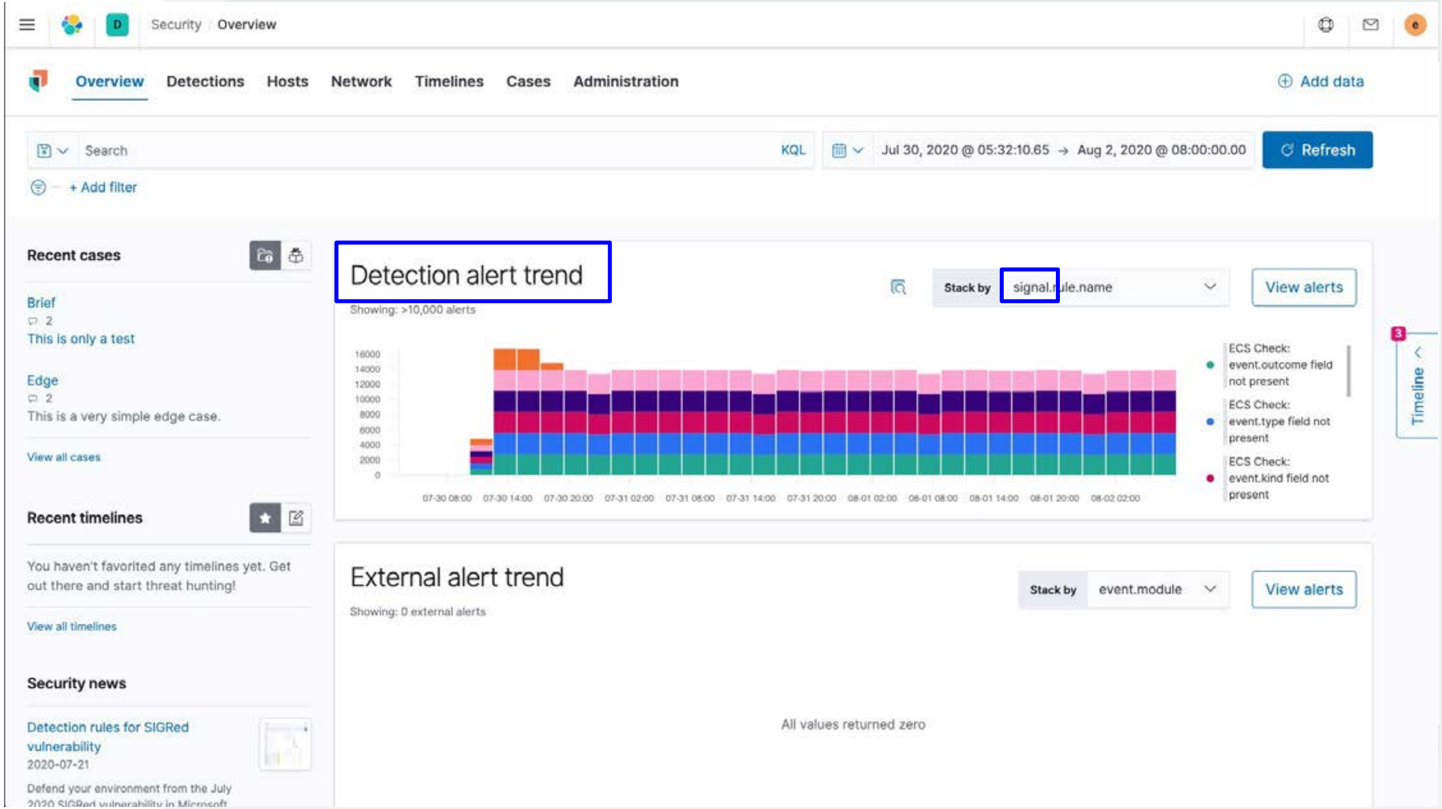


@timestamp	network.transport	Rule	signal.rule.version	Method	Severity	Risk Score	agent.type
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

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.*



Jul 30, 2020 @ 05:32:10.65 → Aug 2, 2020 @ 08:00:00.00

Brief
2
This is only a test

Edge
2
This is a very simple edge case.

View all cases

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Detection rules for SIGRed vulnerability
2020-07-21
Defend your environment from the July 2020 SIGRed vulnerability in Microsoft

Stack by: signal.rule.name

Showing: >10,000 alerts

● ECS Check: event.outcome field not present
● ECS Check: event.type field not present
● ECS Check: event.kind field not present

Stack by: event.module

Showing: 0 external alerts

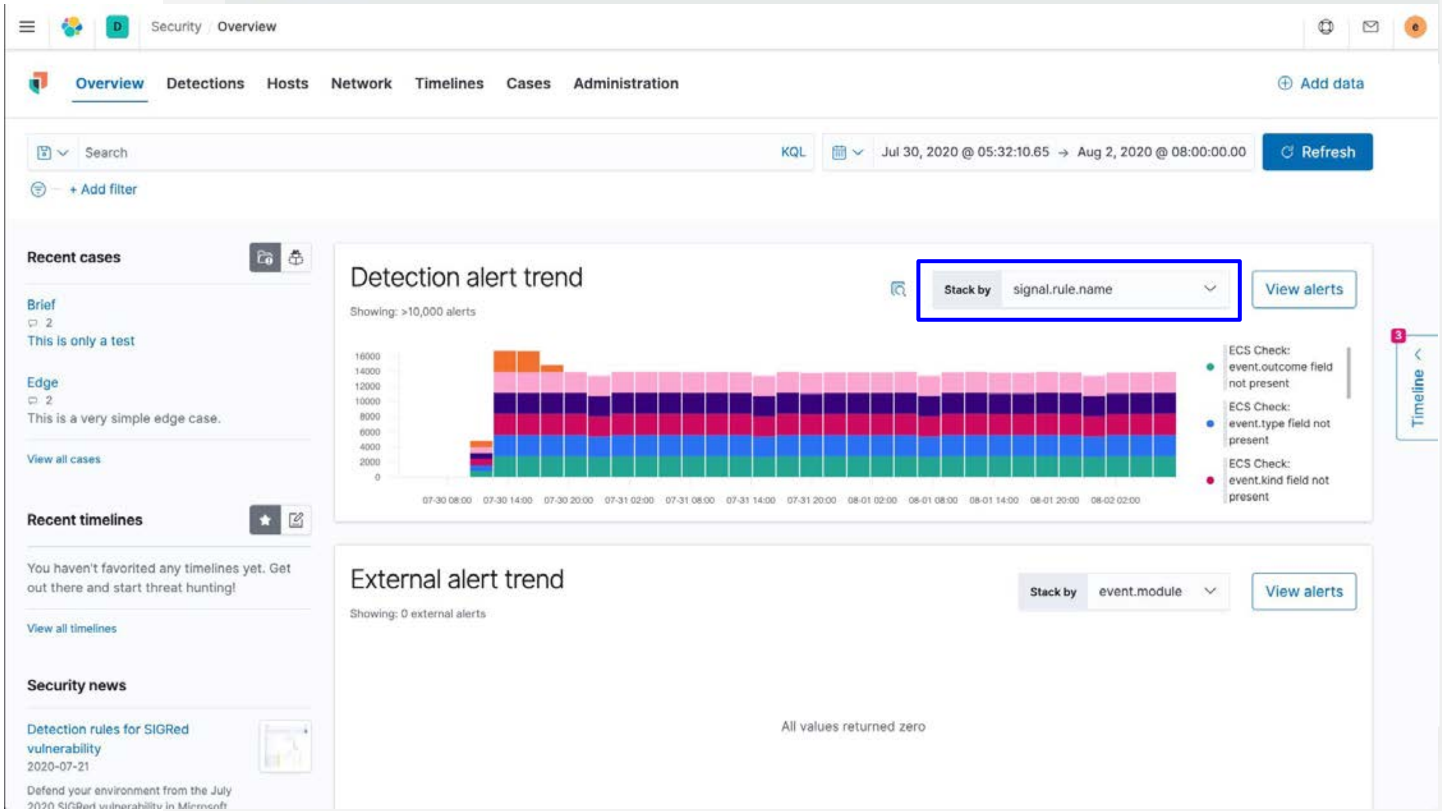
All values returned zero

elastic

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.



Jul 30, 2020 @ 05:32:10.65 → Aug 2, 2020 @ 08:00:00.00

Recent cases

Brief
2
This is only a test

Edge
2
This is a very simple edge case.

View all cases

Recent timelines

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Security news

Detection rules for SIGRed vulnerability
2020-07-21
Defend your environment from the July 2020 SIGRed vulnerability in Microsoft

Detection alert trend

Showing: >10,000 alerts

Stack by: signal.rule.name

● ECS Check: event.outcome field not present
● ECS Check: event.type field not present
● ECS Check: event.kind field not present

External alert trend

Showing: 0 external alerts

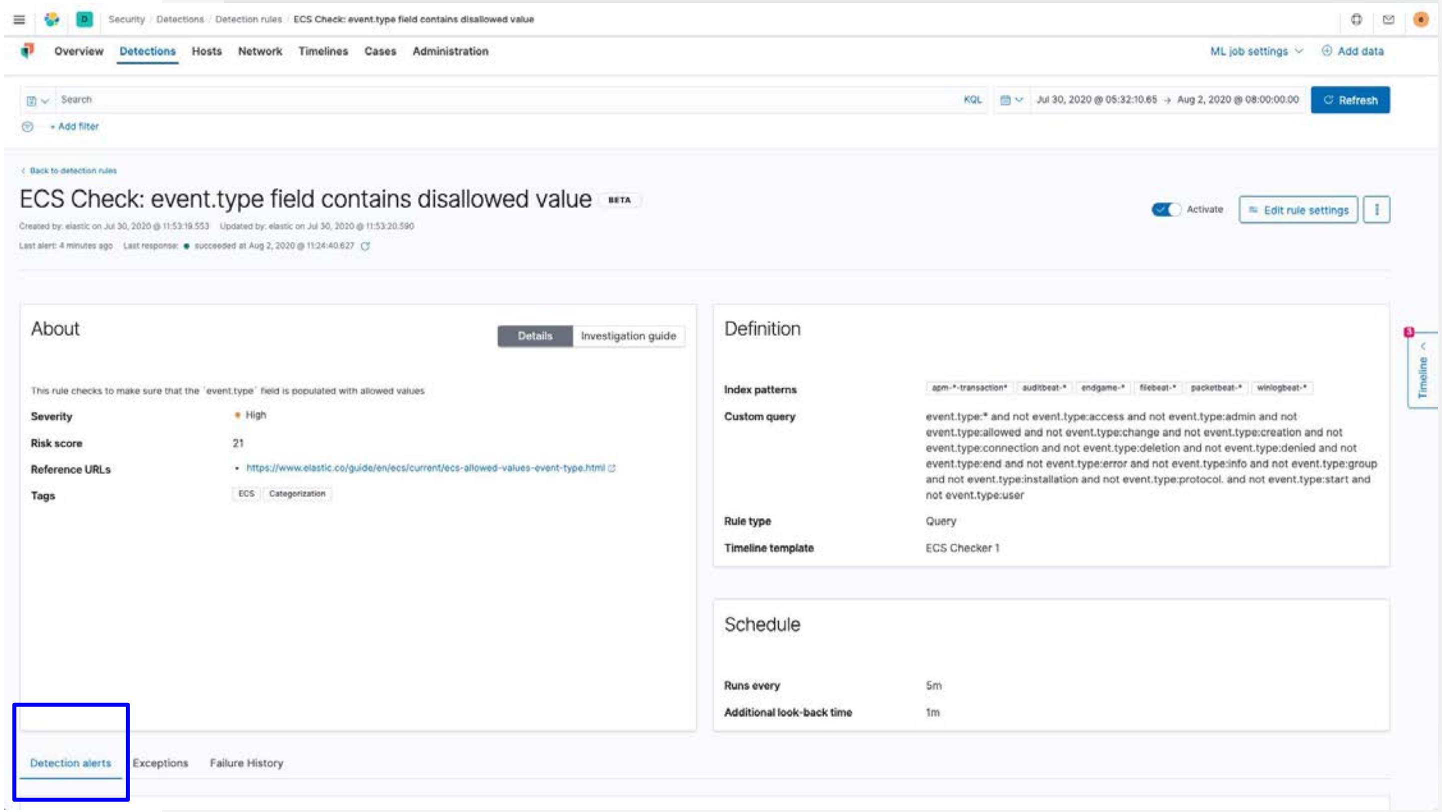
Stack by: event.module

All values returned zero

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.



ECS Check: event.type field contains disallowed value BETA

Created by: elastic on Jul 30, 2020 @ 11:53:19.553 Updated by: elastic on Jul 30, 2020 @ 11:53:20.590

Last alert: 4 minutes ago Last response: ● succeeded at Aug 2, 2020 @ 11:24:40.627

About

This rule checks to make sure that the `event.type` field is populated with allowed values

Severity	● High
Risk score	21
Reference URLs	• https://www.elastic.co/guide/en/ecs/current/ecs-allowed-values-event-type.html
Tags	ECS Categorization

Definition

Index patterns	apm-*-transaction* auditbeat-* endgame-* filebeat-* packetbeat-* winlogbeat-*
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
Rule type	Query
Timeline template	ECS Checker 1

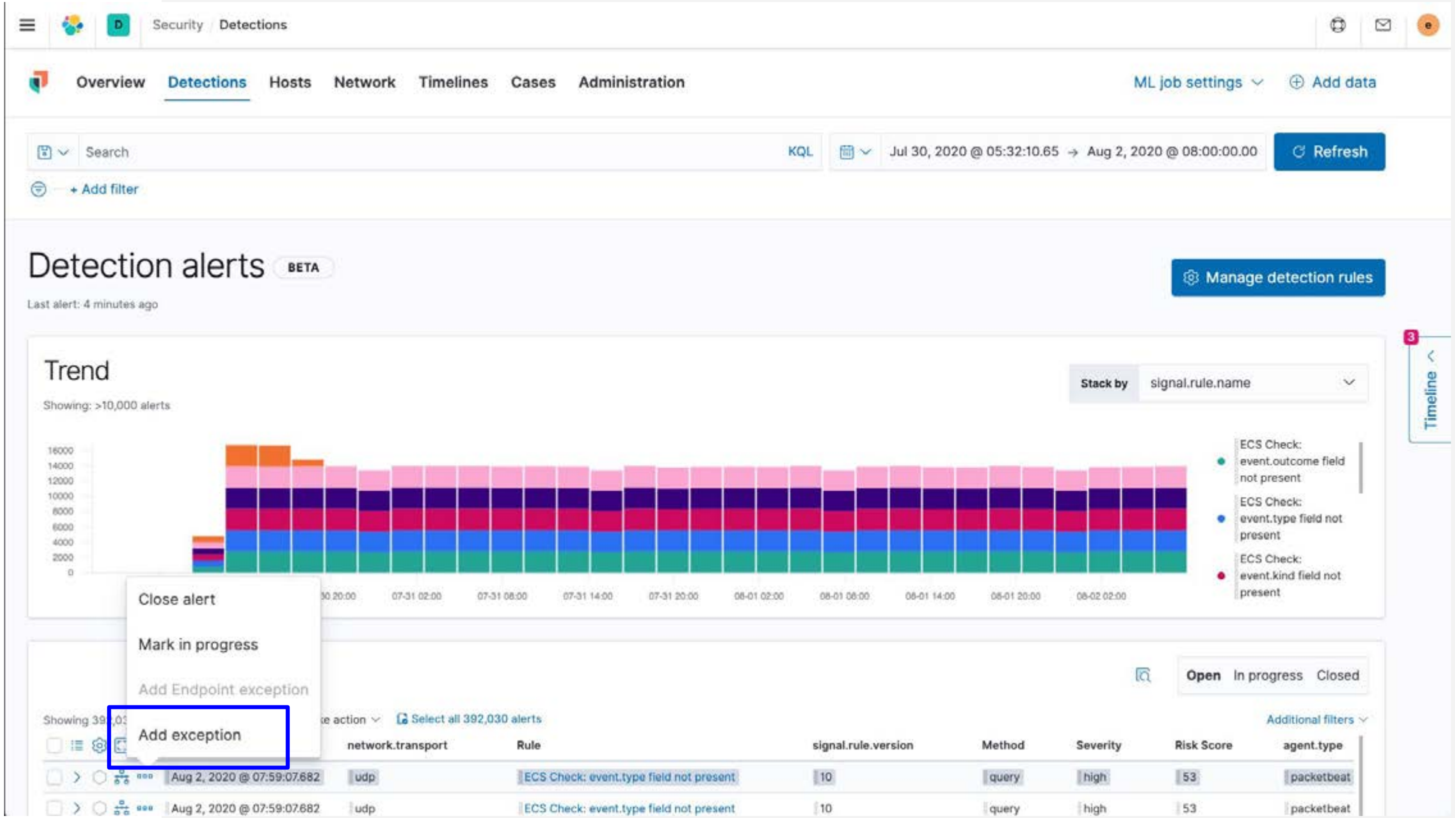
Schedule

Runs every	5m
Additional look-back time	1m

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.



Detection alerts BETA

Last alert: 4 minutes ago

Trend

Showing: >10,000 alerts

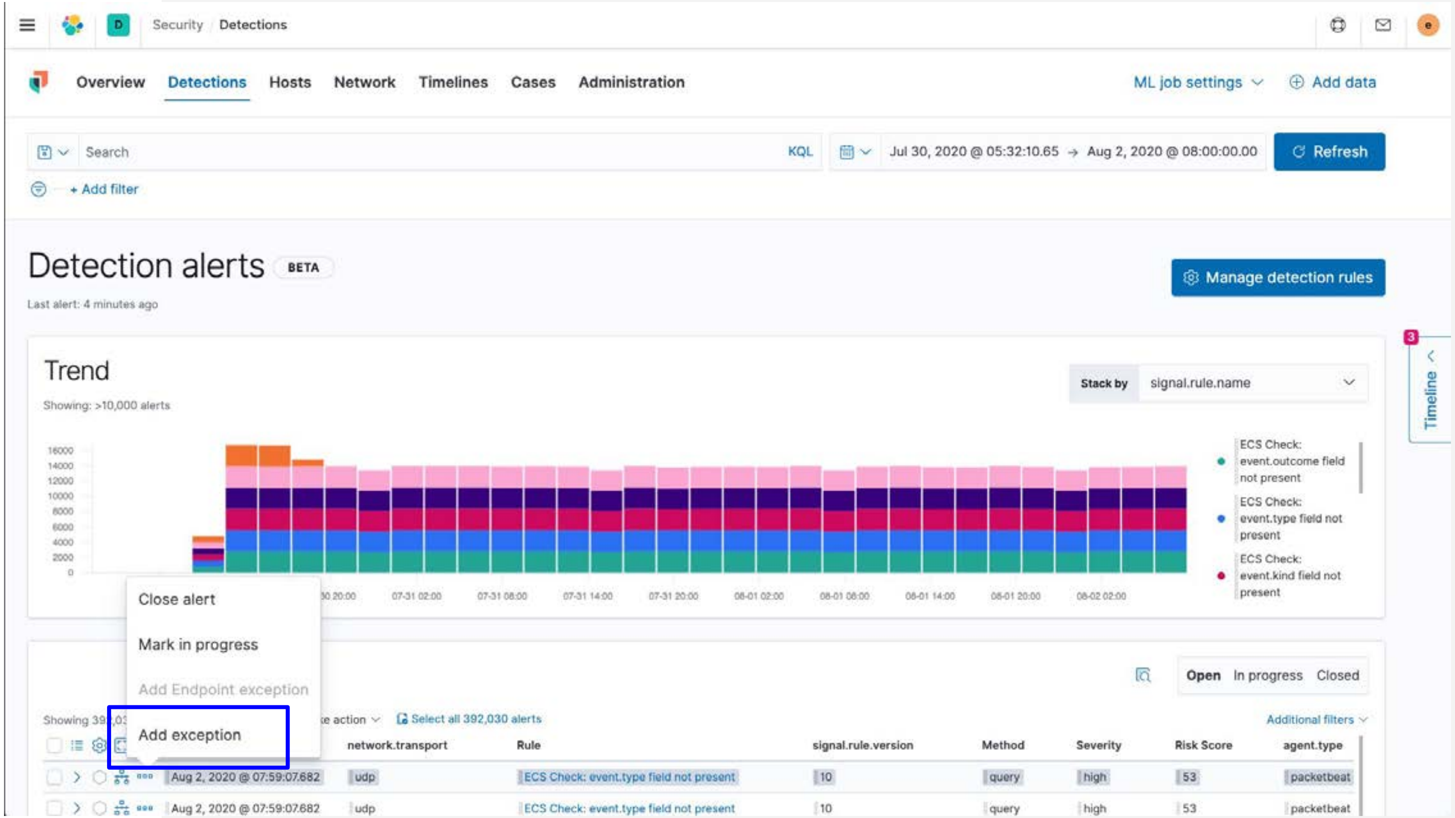
	network.transport	Rule	signal.rule.version	Method	Severity	Risk Score	agent.type
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

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

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

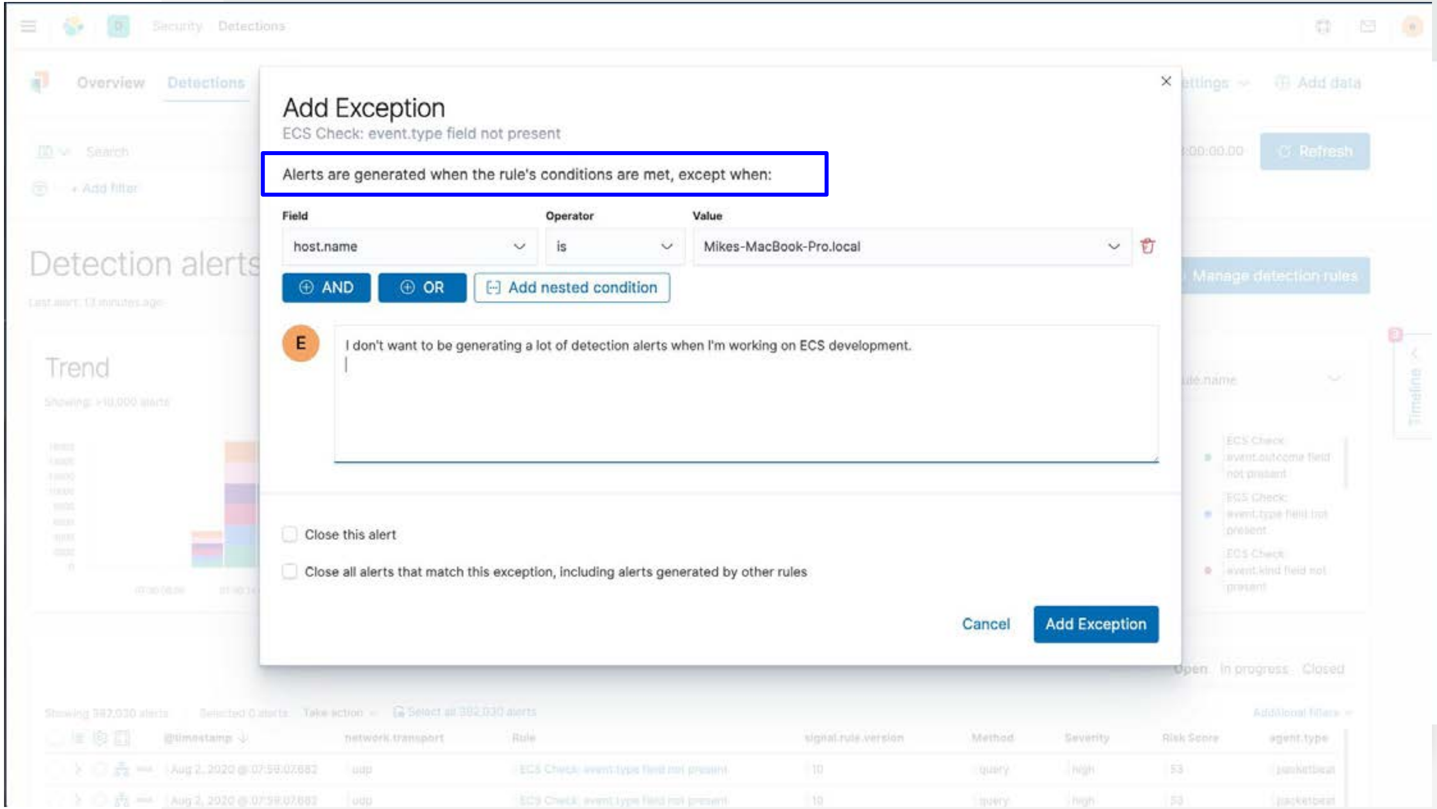


	network.transport	Rule	signal.rule.version	Method	Severity	Risk Score	agent.type
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat
Aug 2, 2020 @ 07:59:07.682	udp	ECS Check: event.type field not present	10	query	high	53	packetbeat

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

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

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

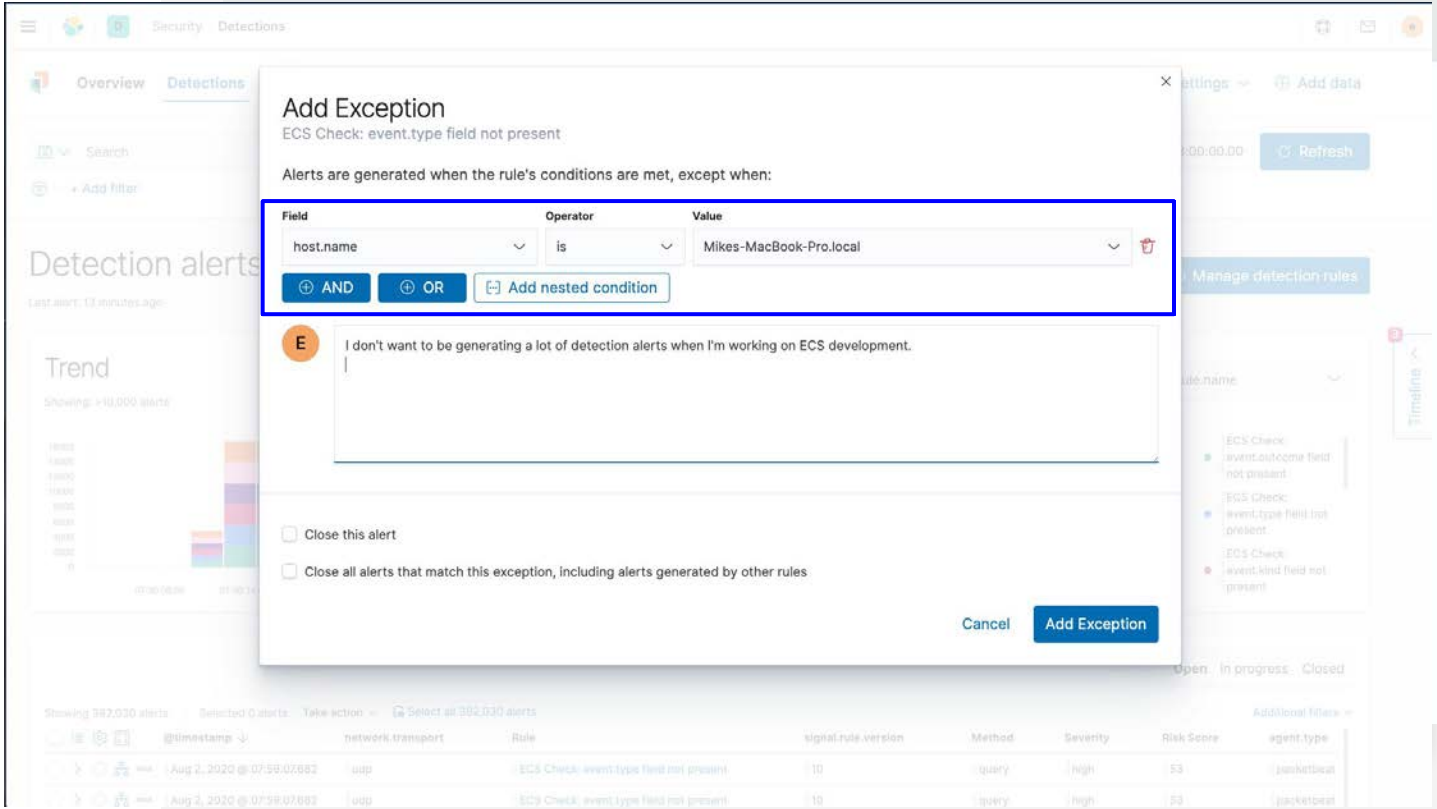
□ Close this alert

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

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

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

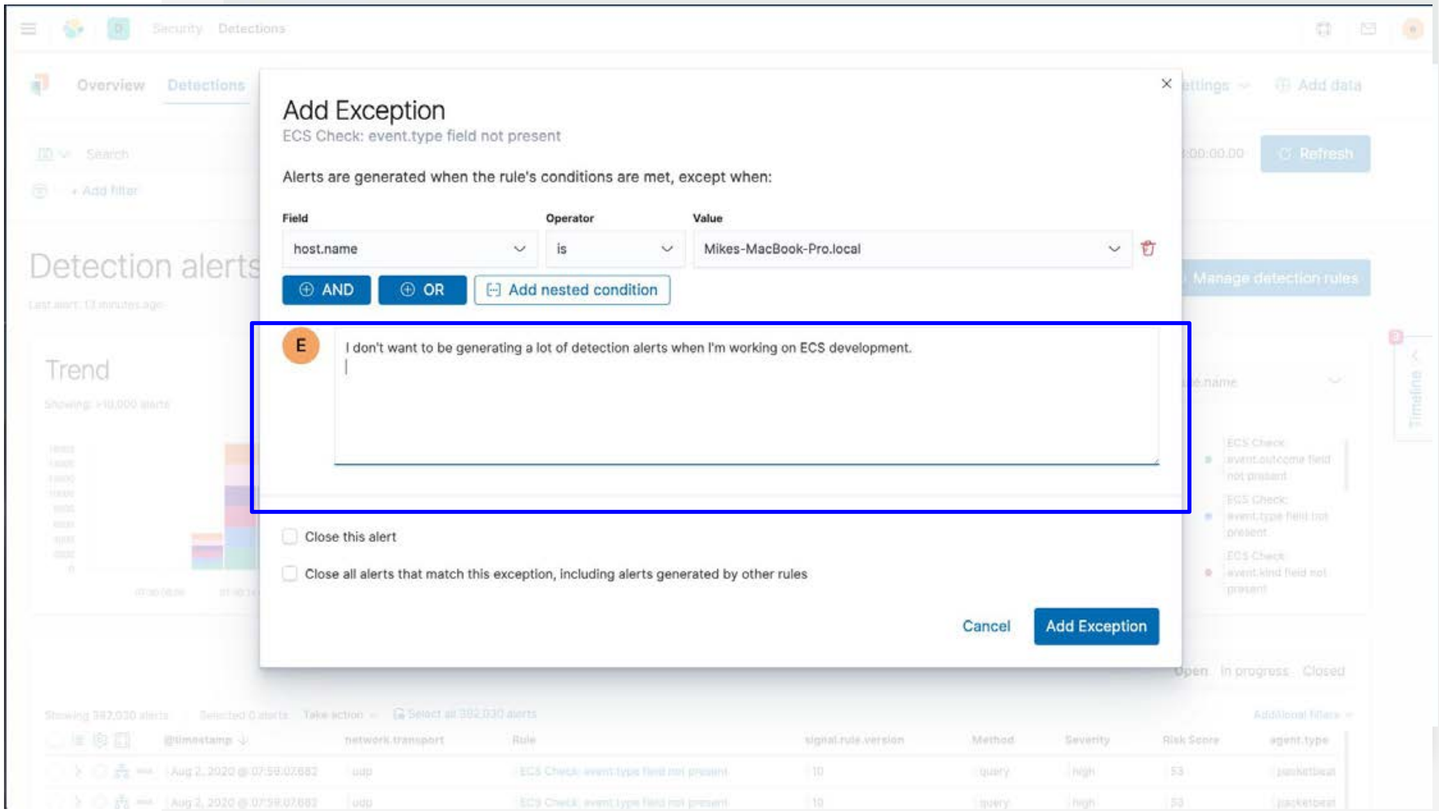
□ Close this alert

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

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

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

□ Close this alert

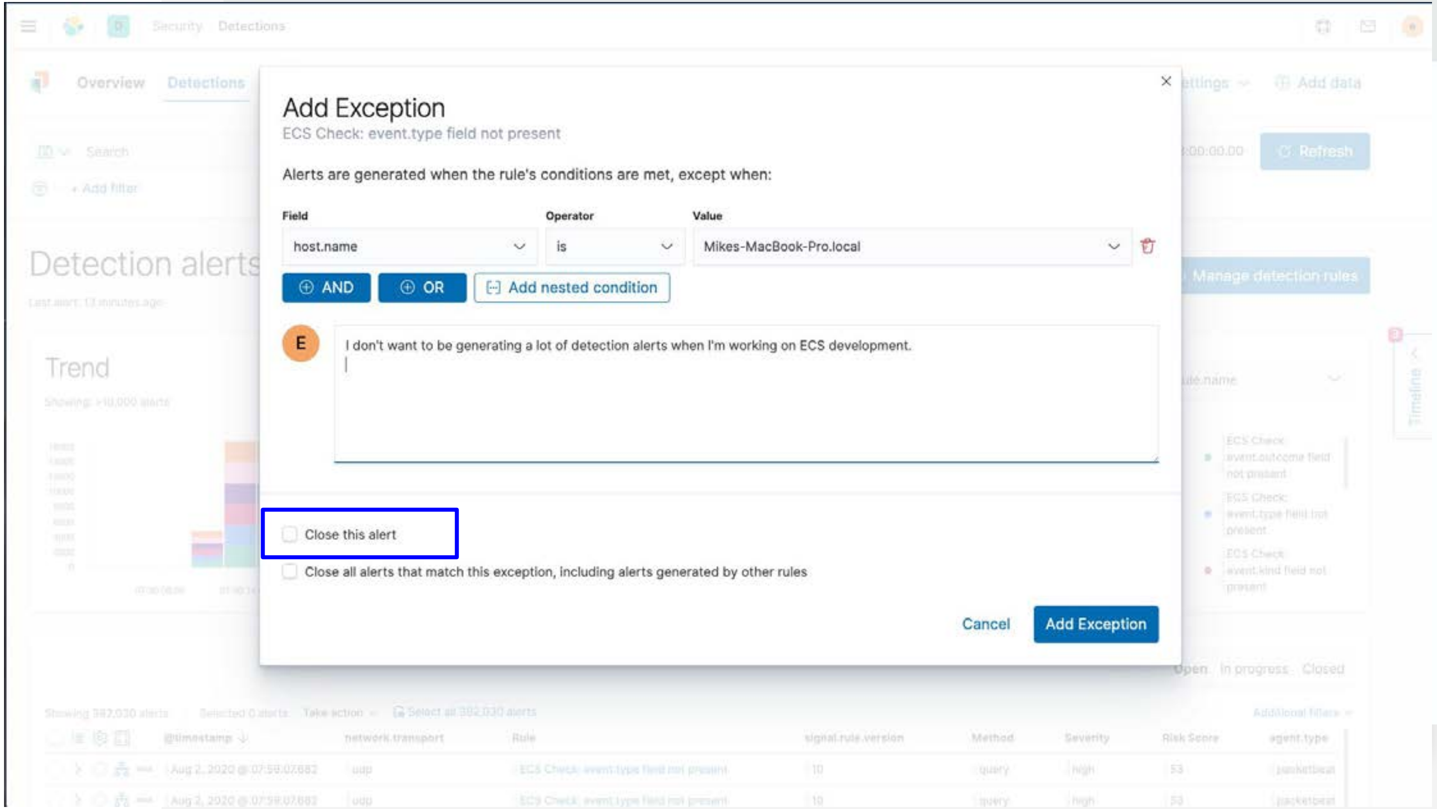
□ Close all alerts that match this exception, including alerts generated by other rules

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

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

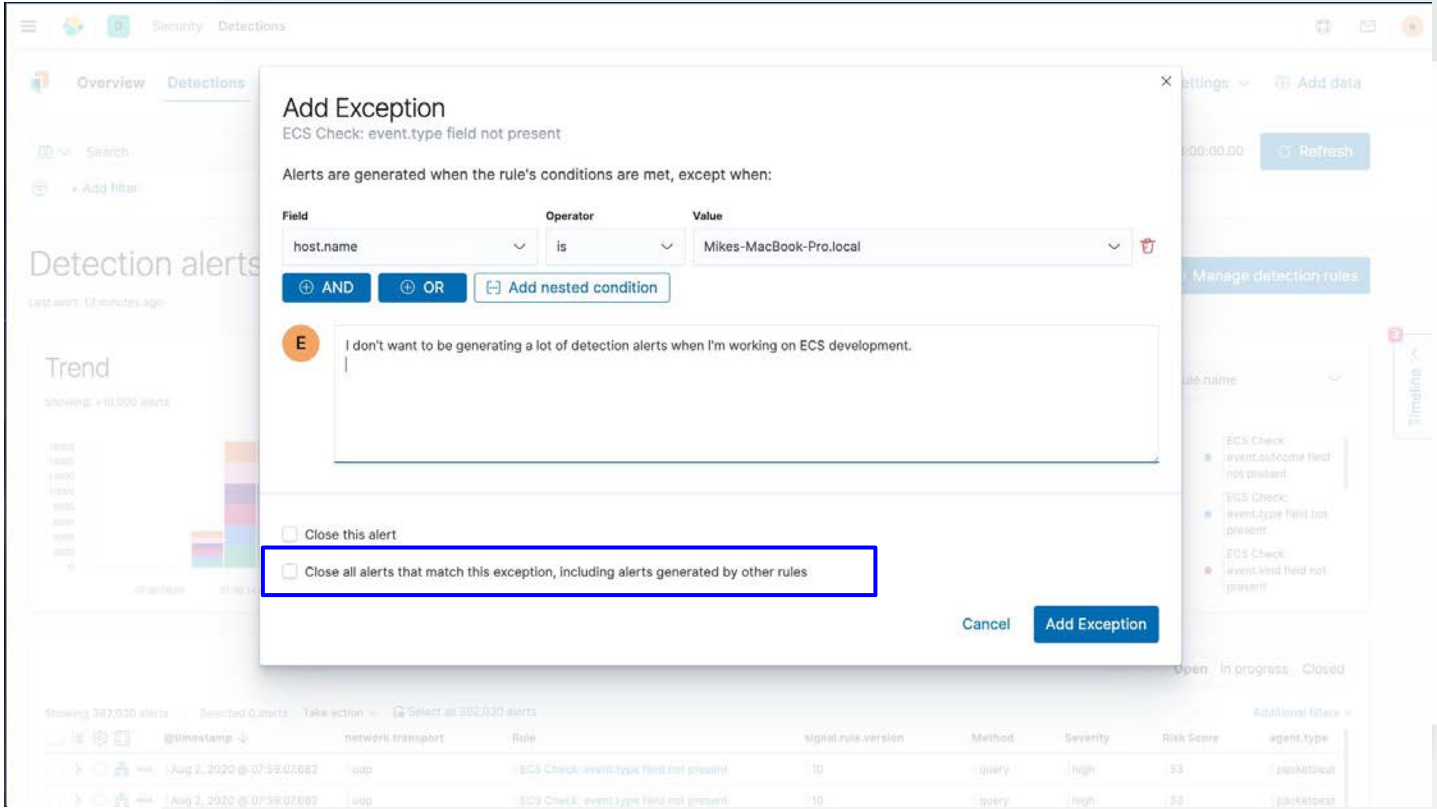
□ Close this alert

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

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

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

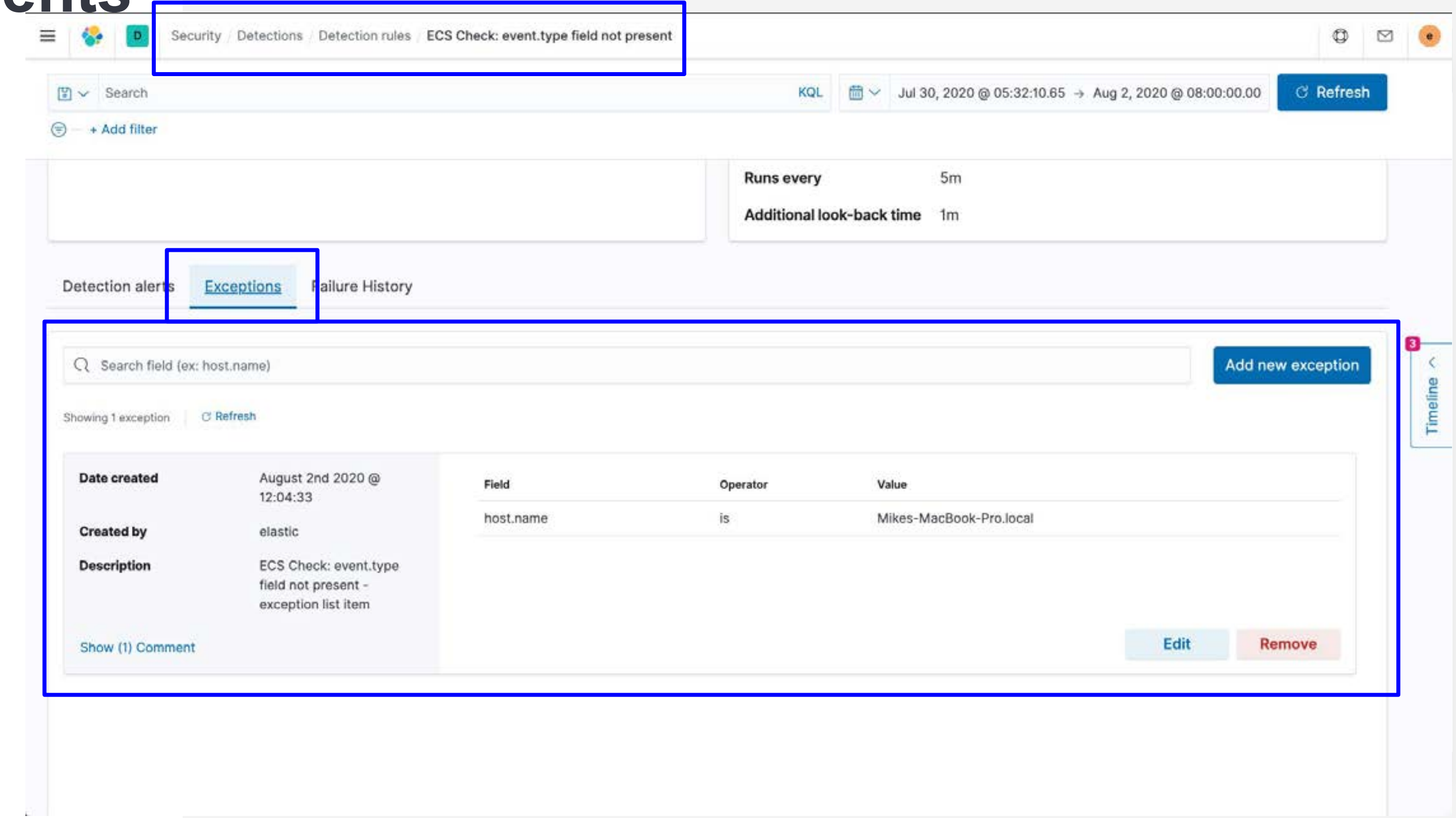
□ Close this alert

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

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.



Security / Detections / Detection rules / ECS Check: event.type field not present
Search
KQL
Jul 30, 2020 @ 05:32:10.65 → Aug 2, 2020 @ 08:00:00.00
Refresh
+ Add filter
Detection alerts
Exceptions
Failure History
Search field (ex: host.name)
Add new exception
Showing 1 exception
Refresh
Show (1) Comment
Edit
Remove
Timeline

Runs every	5m
Additional look-back time	1m

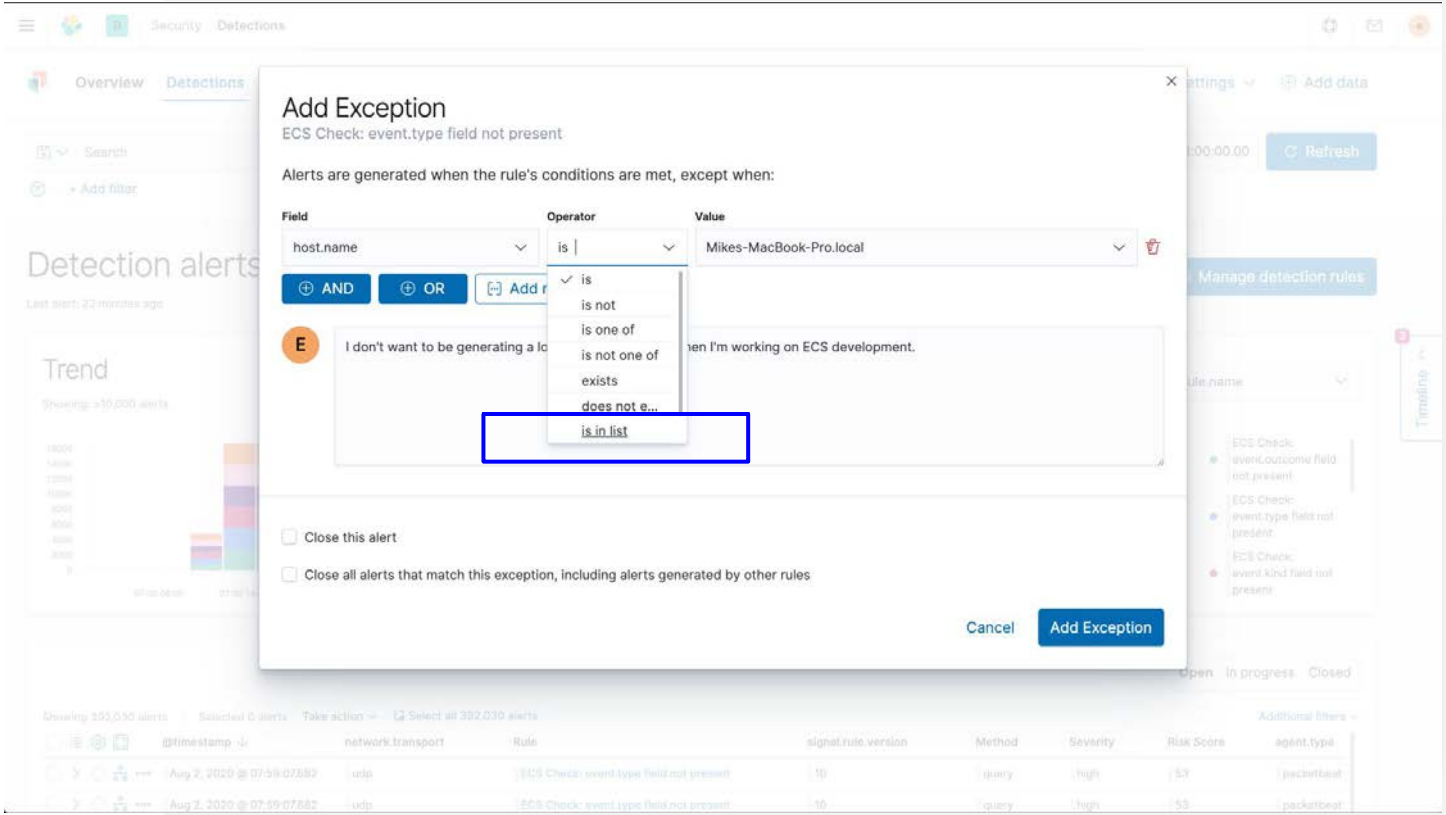
Date created	August 2nd 2020 @ 12:04:33
Created by	elastic
Description	ECS Check: event.type field not present - exception list item

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

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

I don't want to be generating a lo ... hen I'm working on ECS development.

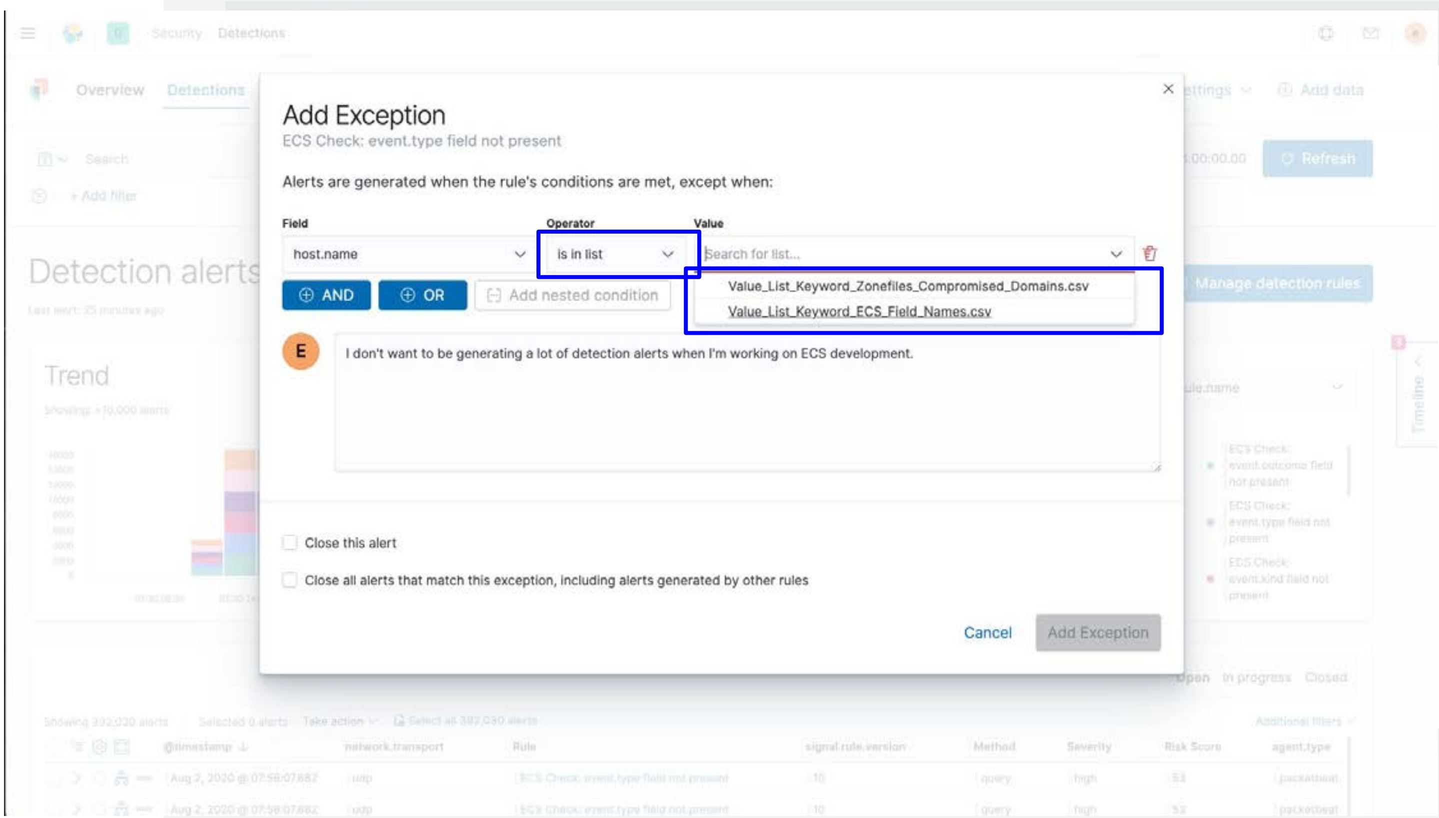
□ Close this alert

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

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"



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 in list	Search for list...

- Value_List_Keyword_Zonefiles_Compromised_Domains.csv
- Value_List_Keyword_ECS_Field_Names.csv

⊕ 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

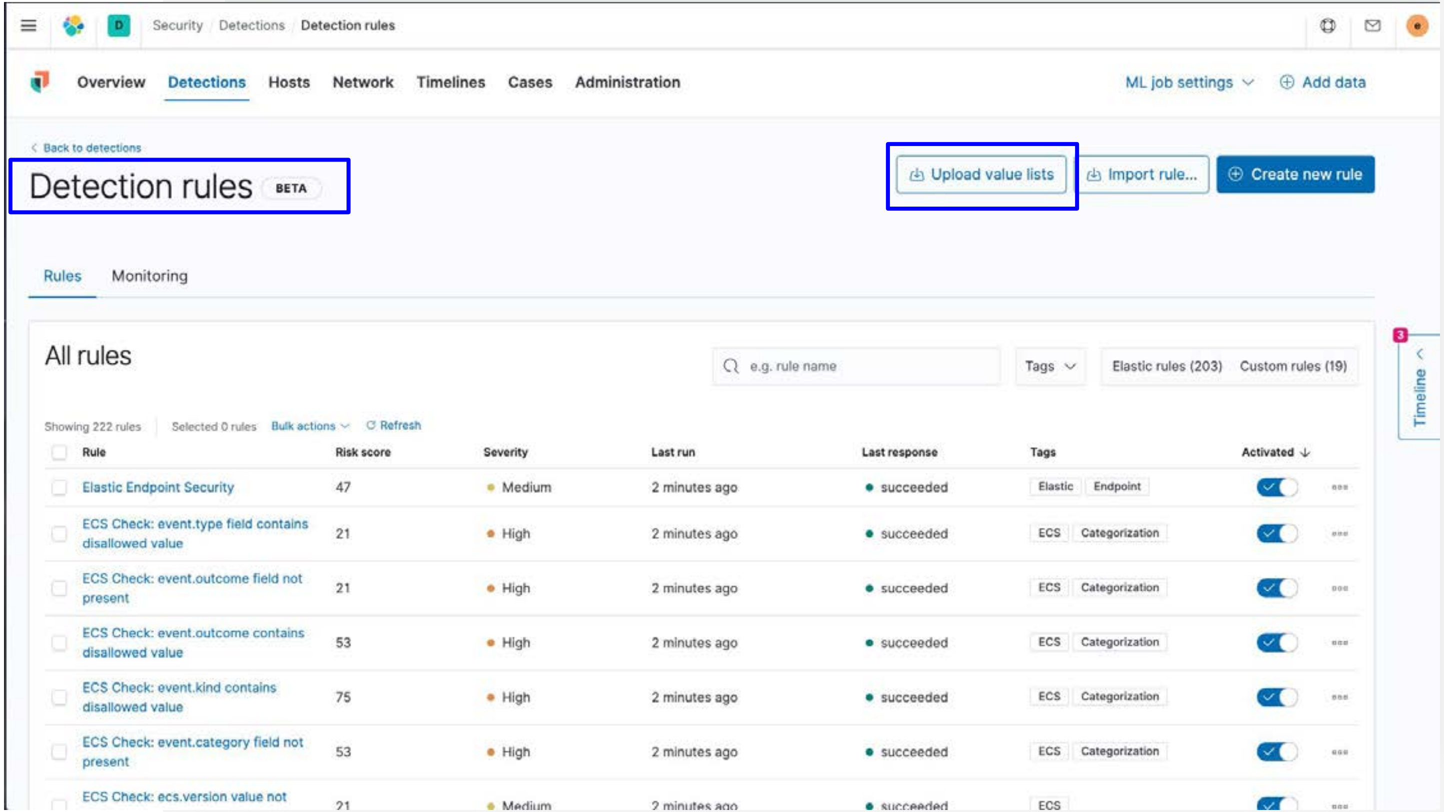
Cancel Add Exception

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

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



Detection rules BETA

All rules

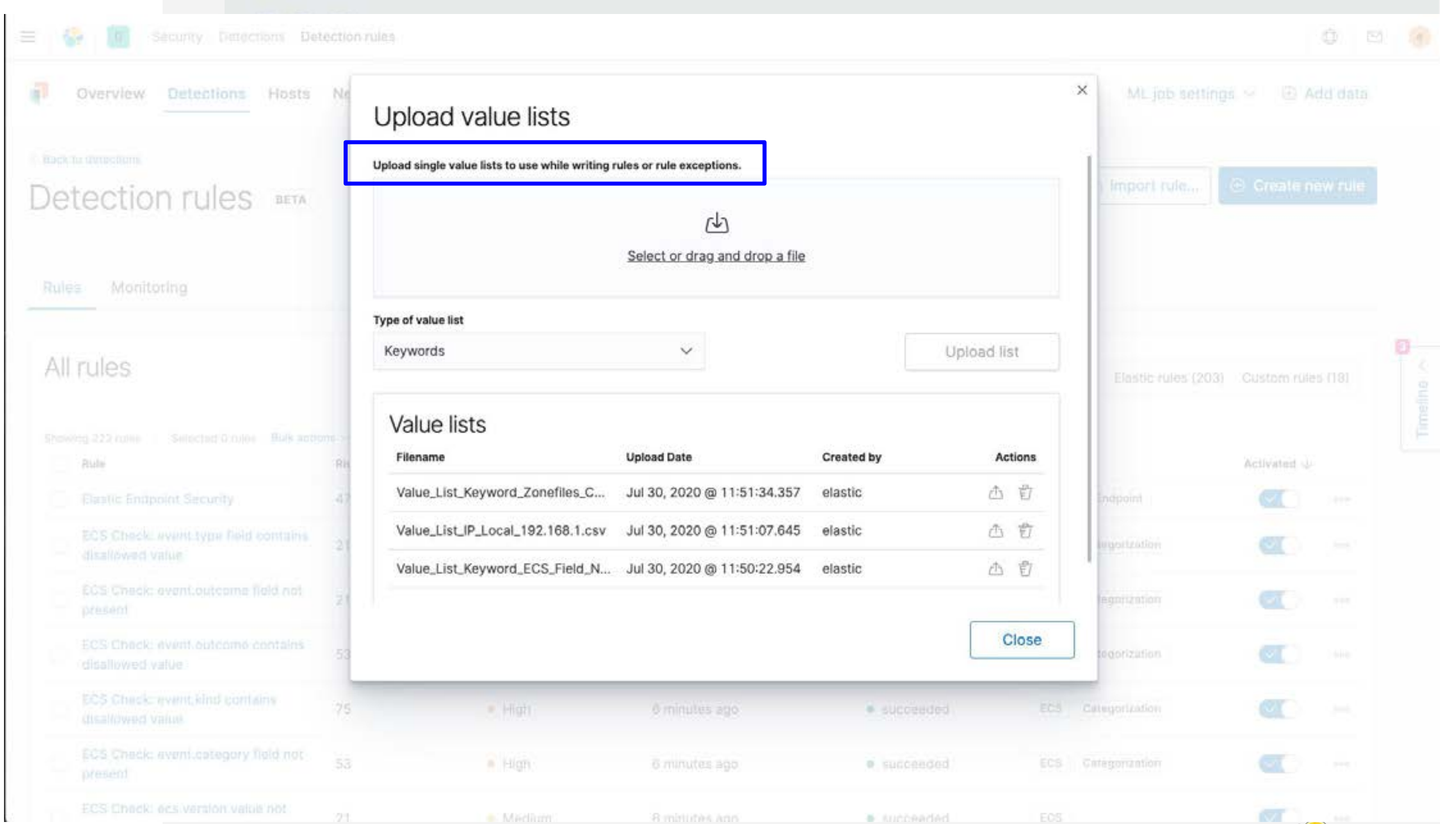
Showing 222 rules | Selected 0 rules

Rule	Risk score	Severity	Last run	Last response	Tags	Activated ↓
Elastic Endpoint Security	47	● Medium	2 minutes ago	● succeeded	Elastic Endpoint	✓
ECS Check: event.type field contains disallowed value	21	● High	2 minutes ago	● succeeded	ECS Categorization	✓
ECS Check: event.outcome field not present	21	● High	2 minutes ago	● succeeded	ECS Categorization	✓
ECS Check: event.outcome contains disallowed value	53	● High	2 minutes ago	● succeeded	ECS Categorization	✓
ECS Check: event.kind contains disallowed value	75	● High	2 minutes ago	● succeeded	ECS Categorization	✓
ECS Check: event.category field not present	53	● High	2 minutes ago	● succeeded	ECS Categorization	✓
ECS Check: ecs.version value not	21	● Medium	2 minutes ago	● succeeded	ECS	✓

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.



Upload value lists

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

Type of value list

Keywords

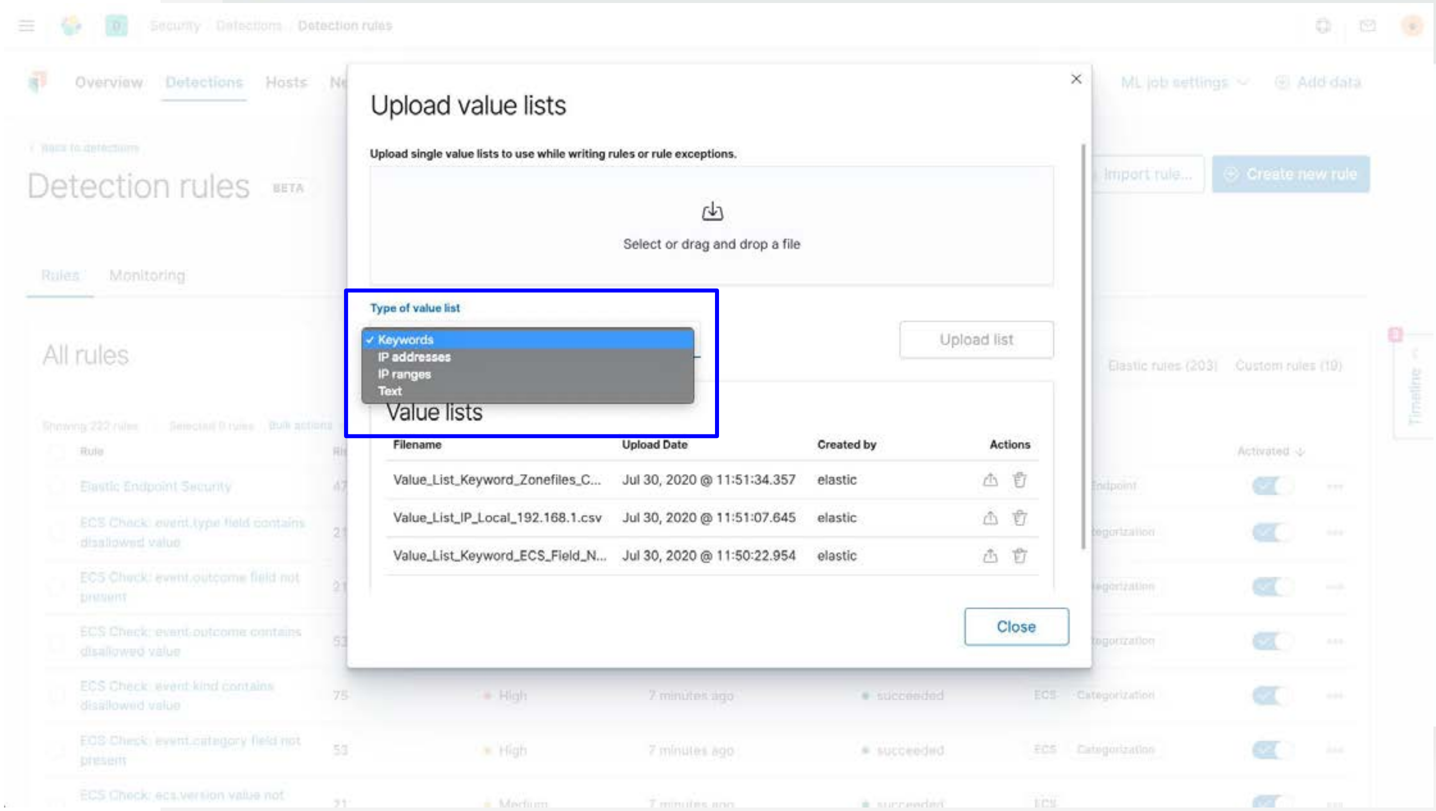
Value lists

Filename	Upload Date	Created by	Actions
Value_List_Keyword_Zonefiles_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

Value lists

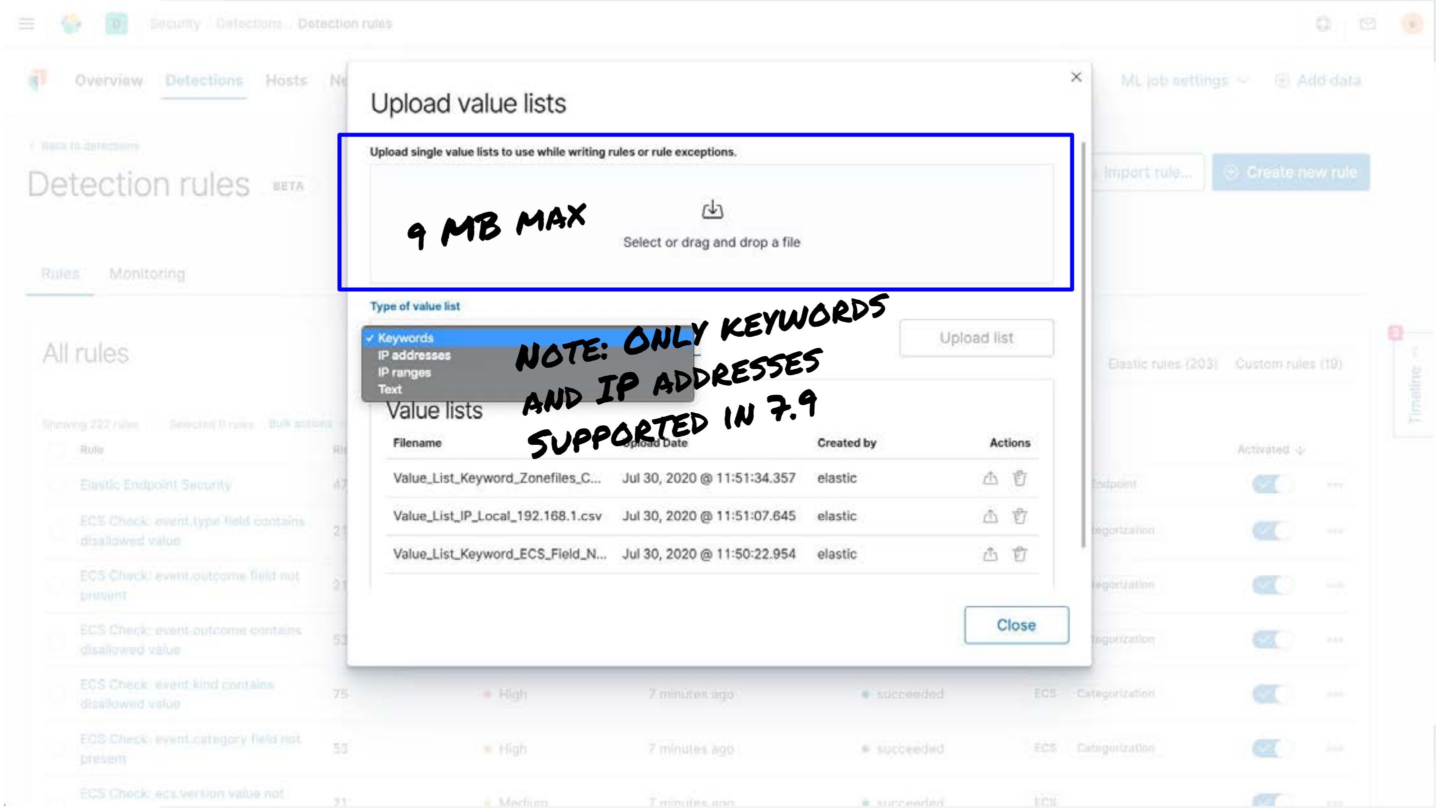
Filename	Upload Date	Created by	Actions
Value_List_Keyword_Zonefiles_C...	Jul 30, 2020 @ 11:51:34.357	elastic	
Value_List_IP_Local_192.168.1.csv	Jul 30, 2020 @ 11:51:07.645	elastic	
Value_List_Keyword_ECS_Field_N...	Jul 30, 2020 @ 11:50:22.954	elastic	

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

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

Value lists

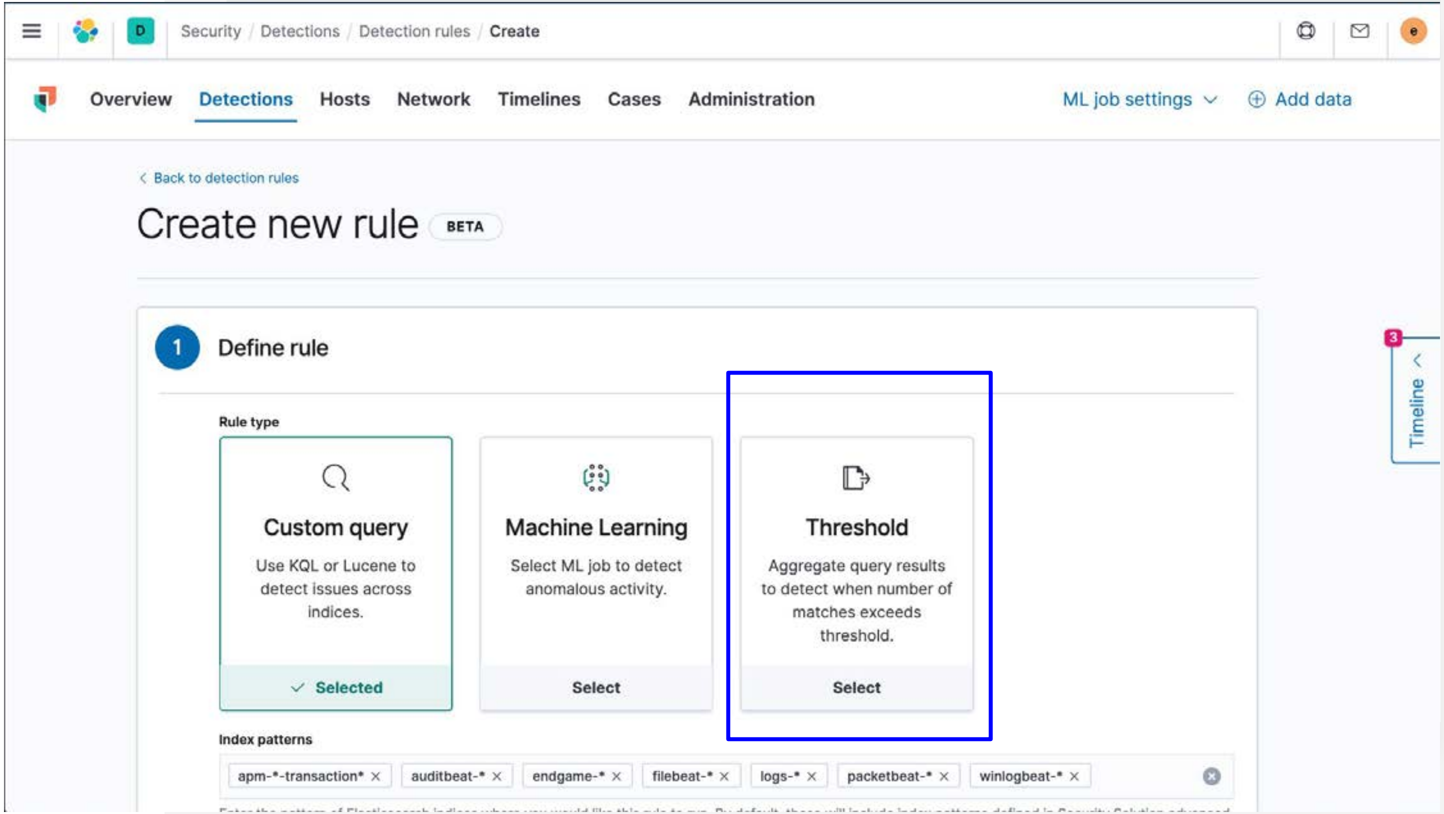
Filename	Upload Date	Created by	Actions
Value_List_Keyword_Zonefiles_C...	Jul 30, 2020 @ 11:51:34.357	elastic	
Value_List_IP_Local_192.168.1.csv	Jul 30, 2020 @ 11:51:07.645	elastic	
Value_List_Keyword_ECS_Field_N...	Jul 30, 2020 @ 11:50:22.954	elastic	

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

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



Create new rule BETA

1 Define rule

Rule type

Custom query
Use KQL or Lucene to detect issues across indices.
✓ Selected

Machine Learning
Select ML job to detect anomalous activity.
Select

Threshold
Aggregate query results to detect when number of matches exceeds threshold.
Select

Index patterns

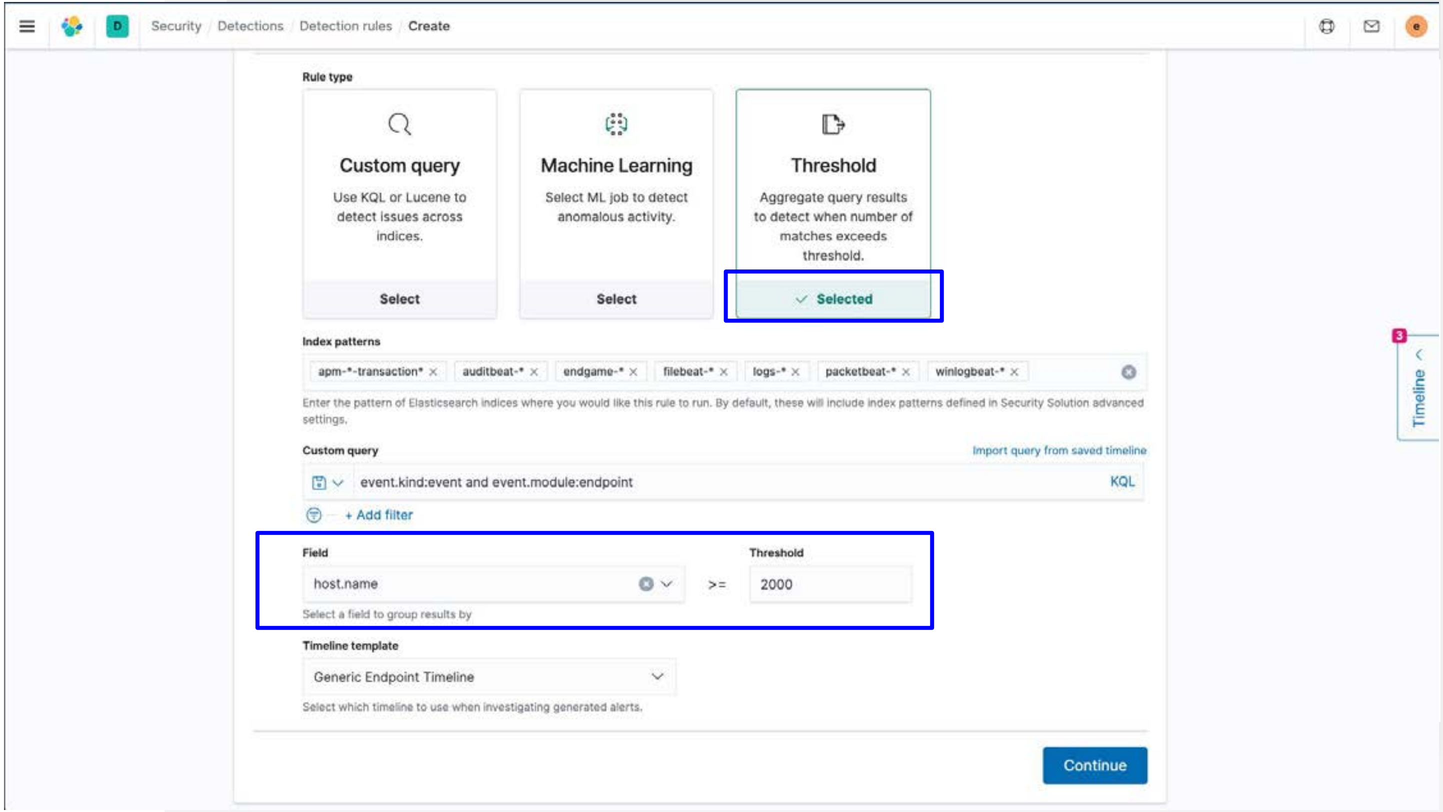
apm-*-transaction* × auditbeat-* × endgame-* × filebeat-* × logs-* × packetbeat-* × winlogbeat-* ×

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

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



Rule type

Custom query
Use KQL or Lucene to detect issues across indices.
Select

Machine Learning
Select ML job to detect anomalous activity.
Select

Threshold
Aggregate query results to detect when number of matches exceeds threshold.
✓ Selected

Index patterns

apm-*-transaction* × auditbeat-* × endgame-* × filebeat-* × logs-* × packetbeat-* × winlogbeat-* ×

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

Custom query — Import query from saved timeline

event.kind:event and event.module:endpoint — KQL

+ Add filter

Field: host.name >= Threshold: 2000

Select a field to group results by

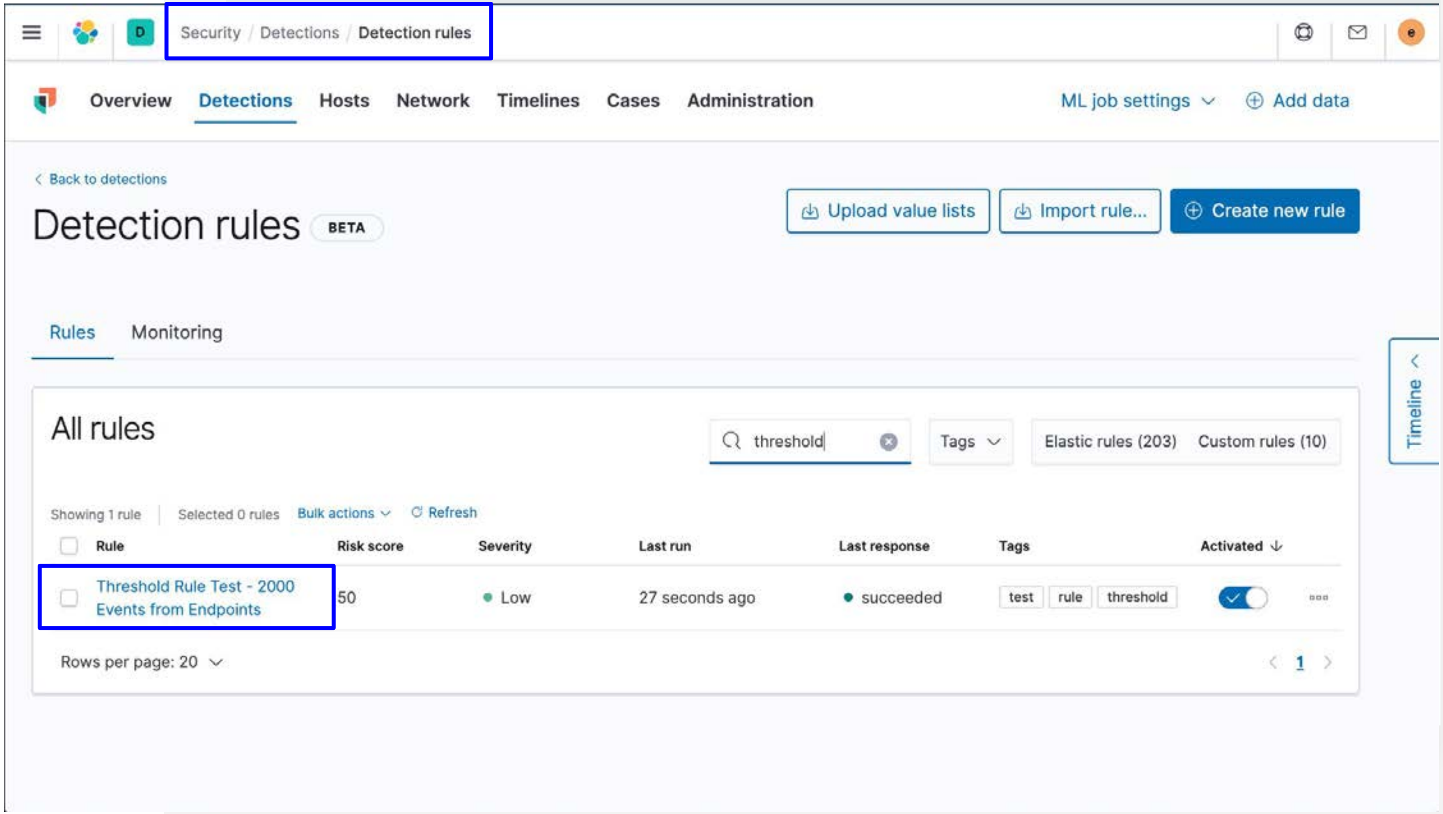
Timeline template: Generic Endpoint Timeline

Select which timeline to use when investigating generated 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

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



Security / Detections / Detection rules

Detection rules BETA

Rules | Monitoring

All rules

threshold | Tags | Elastic rules (203) | Custom rules (10)

Showing 1 rule | Selected 0 rules | Bulk actions | Refresh

□	Rule	Risk score	Severity	Last run	Last response	Tags	Activated
□	Threshold Rule Test - 2000 Events from Endpoints	50	● Low	27 seconds ago	● succeeded	test rule threshold	✓

Rows per page: 20

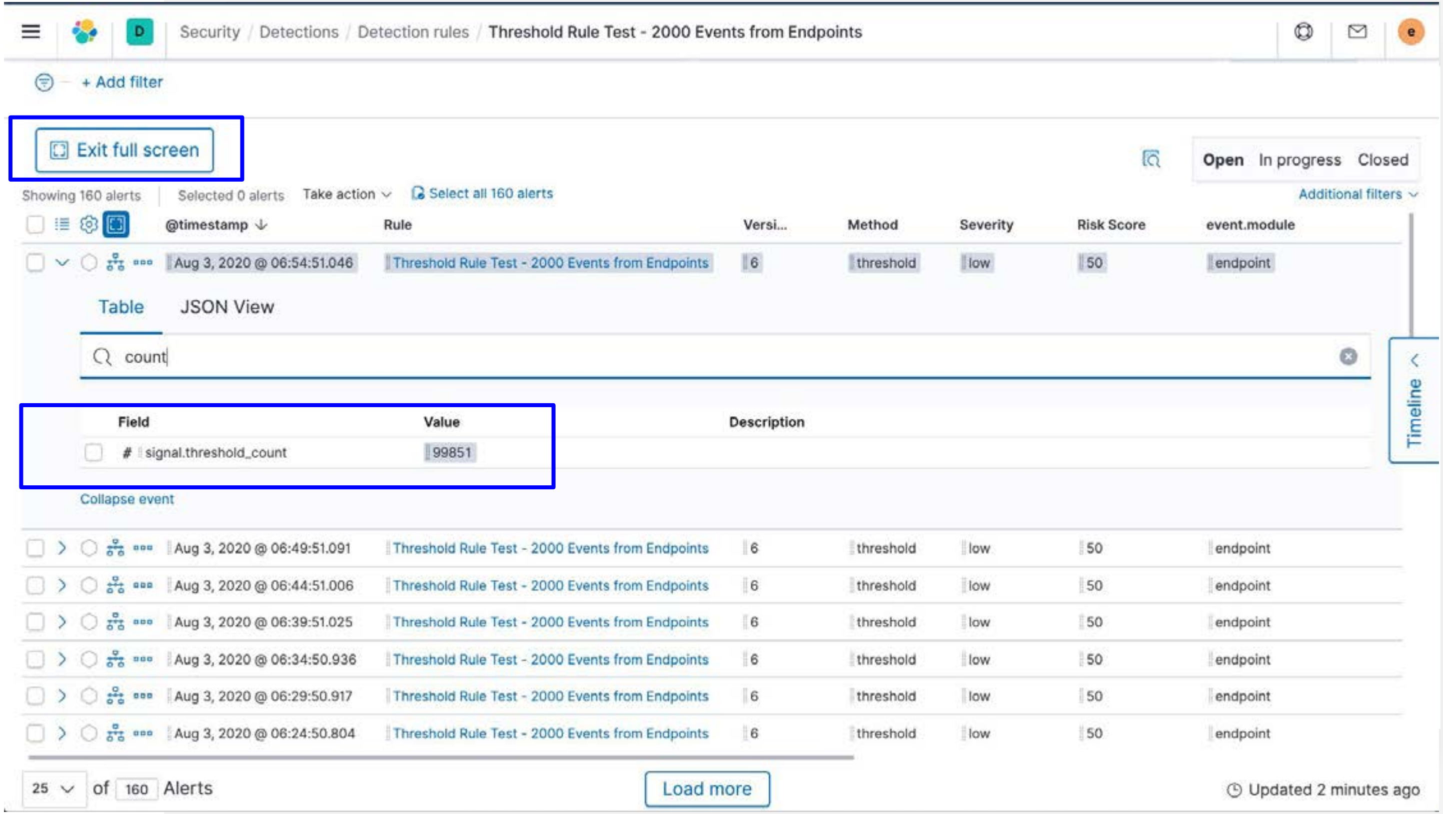
1

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 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

Exit full screen

Open In progress Closed

Additional filters

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

@timestamp	Rule	Versi...	Method	Severity	Risk Score	event.module
Aug 3, 2020 @ 06:54:51.046	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

@timestamp	Rule	Versi...	Method	Severity	Risk Score	event.module
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

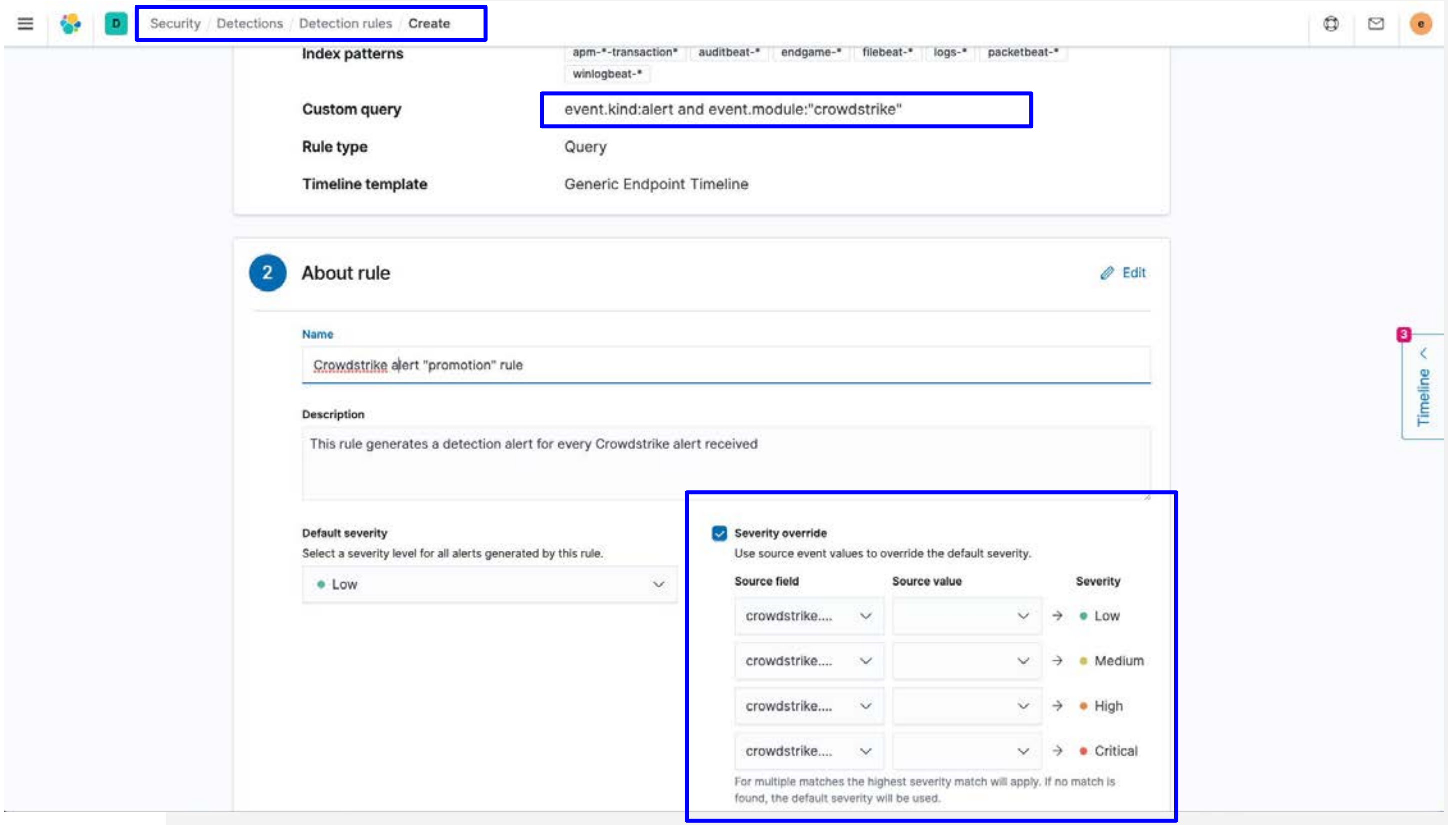
25 of 160 Alerts Load more Updated 2 minutes ago

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

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



Index patterns apm-*-transaction* auditbeat-* endgame-* filebeat-* logs-* packetbeat-* winlogbeat-*

Custom query event.kind:alert and event.module:"crowdstrike"

Rule type Query

Timeline template Generic Endpoint Timeline

2 About rule

Name: Crowdstrike alert "promotion" rule

Description: This rule generates a detection alert for every Crowdstrike alert received

Default severity
Select a severity level for all alerts generated by this rule.
● Low

☑ **Severity override**
Use source event values to override the default severity.

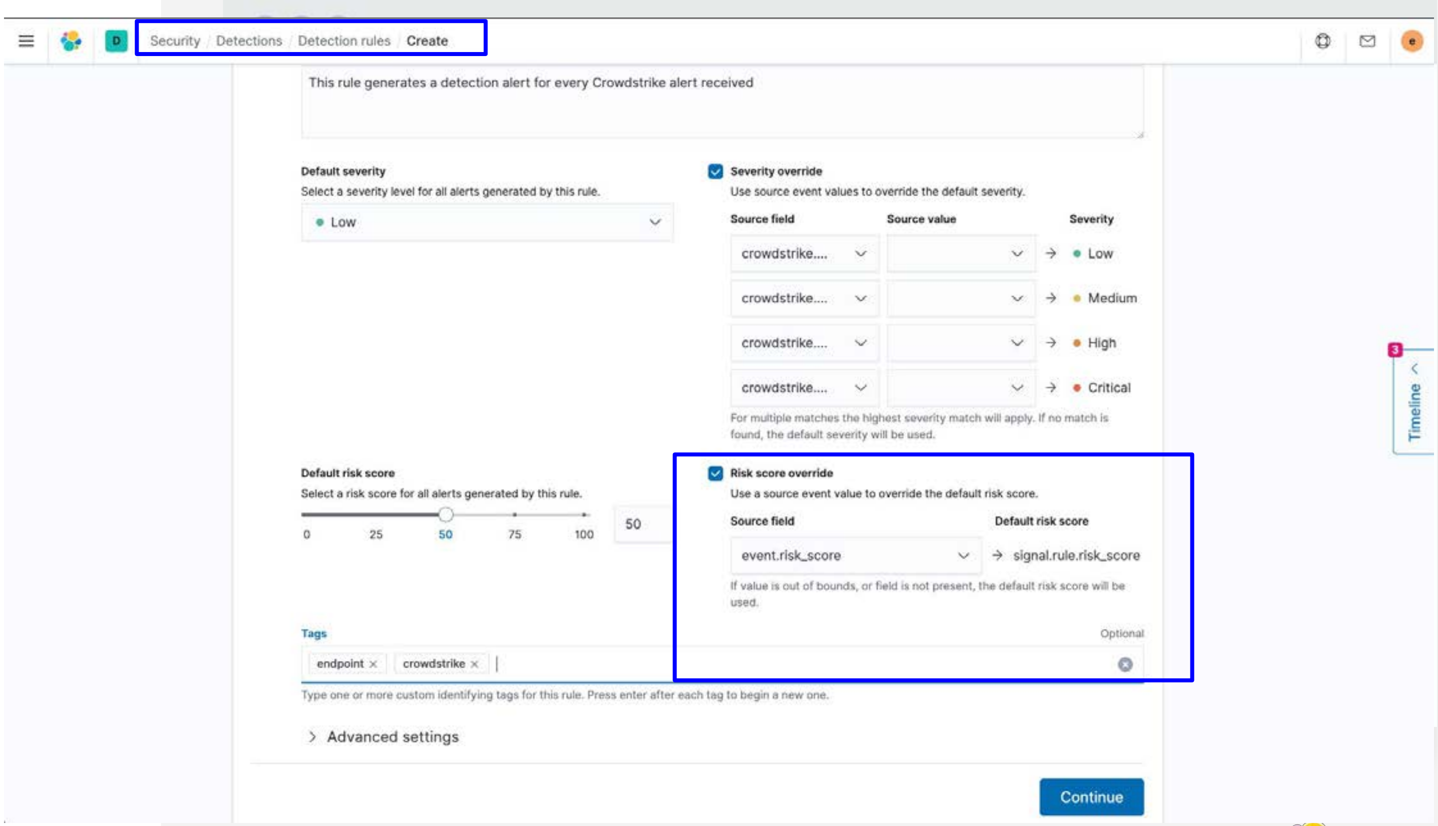
Source field	Source value		Severity
crowdstrike....		→	● Low
crowdstrike....		→	● Medium
crowdstrike....		→	● High
crowdstrike....		→	● Critical

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.



Security / Detections / Detection rules / Create

This rule generates a detection alert for every Crowdstrike alert received

Default severity

Select a severity level for all alerts generated by this rule.

● Low

☑ **Severity override**

Use source event values to override the default severity.

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.

Default risk score

Select a risk score for all alerts generated by this rule.

0 25 50 75 100 — 50

☑ **Risk score override**

Use a source event value to override the default risk score.

Source field		Default risk score
event.risk_score	→	signal.rule.risk_score

If value is out of bounds, or field is not present, the default risk score will be used.

Tags Optional

endpoint × crowdstrike ×

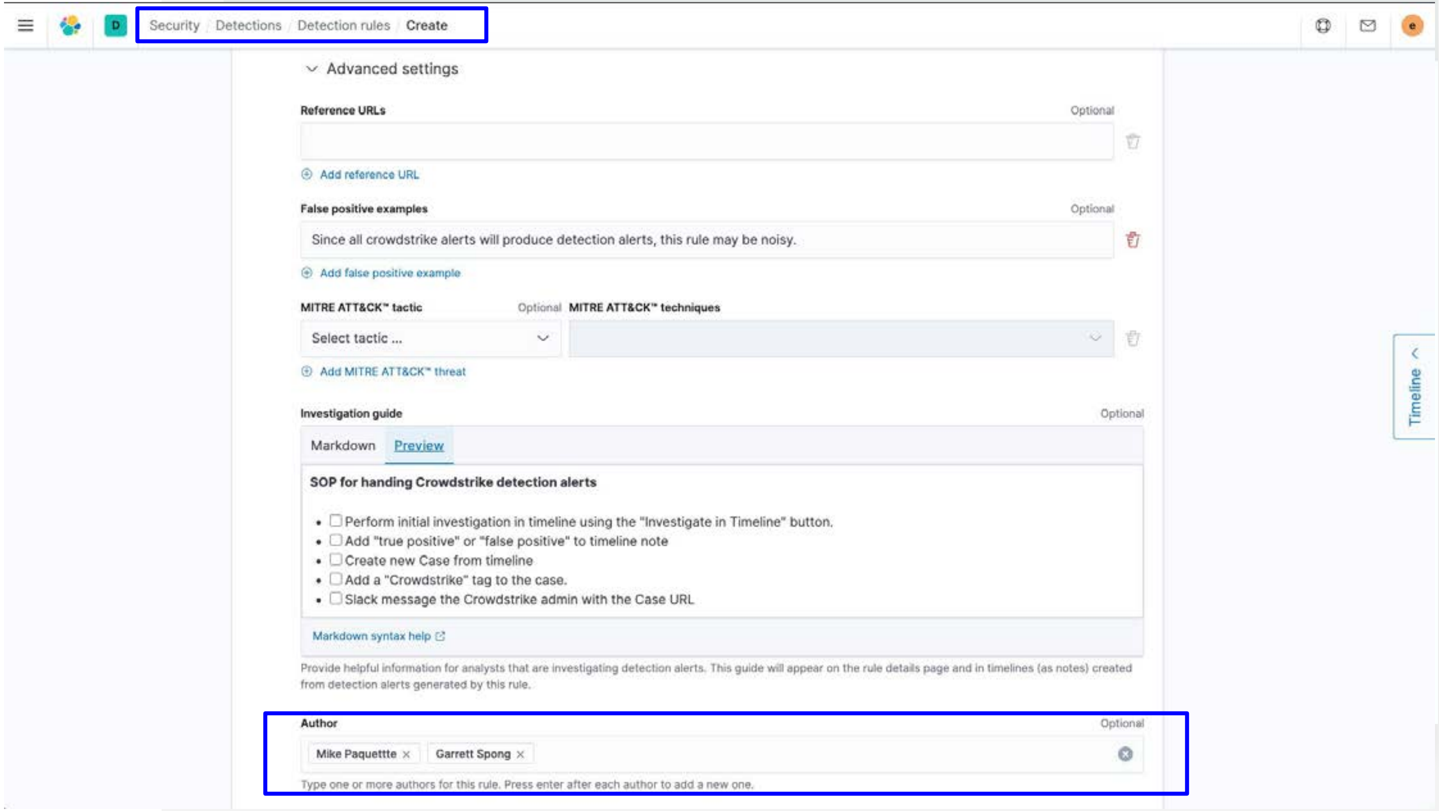
Type one or more custom identifying tags for this rule. Press enter after each tag to begin a new one.

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

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



Reference URLs — Optional

False positive examples — Optional

Since all crowdstrike alerts will produce detection alerts, this rule may be noisy.

MITRE ATT&CK™ tactic — Optional: Select tactic ...

MITRE ATT&CK™ techniques

Investigation guide — Optional

SOP for handing Crowdstrike detection alerts

- □ Perform initial investigation in timeline using the "Investigate in Timeline" button.
- □ Add "true positive" or "false positive" to timeline note
- □ Create new Case from timeline
- □ Add a "Crowdstrike" tag to the case.
- □ Slack message the Crowdstrike admin with the Case URL

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.

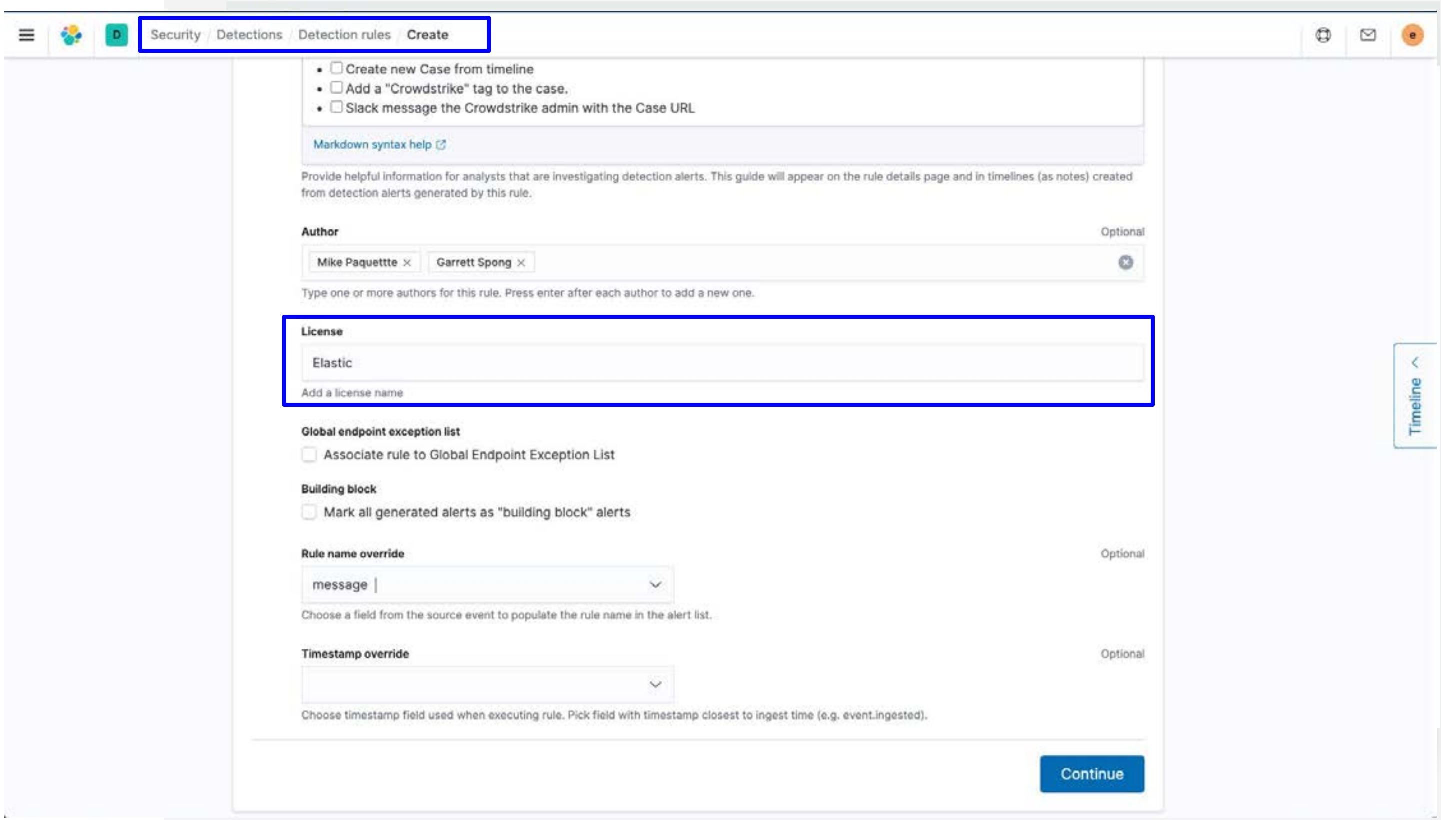
Author — Optional: Mike Paquettte × Garrett Spong ×

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

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 rule is published. E.g., Elastic, MIT, DRL.



- □ 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

Mike Paquettte × Garrett Spong ×

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

License

Elastic

Add a license name

Global endpoint exception list

□ Associate rule to Global Endpoint Exception List

Building block

□ Mark all generated alerts as "building block" alerts

Rule name override Optional

message |

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

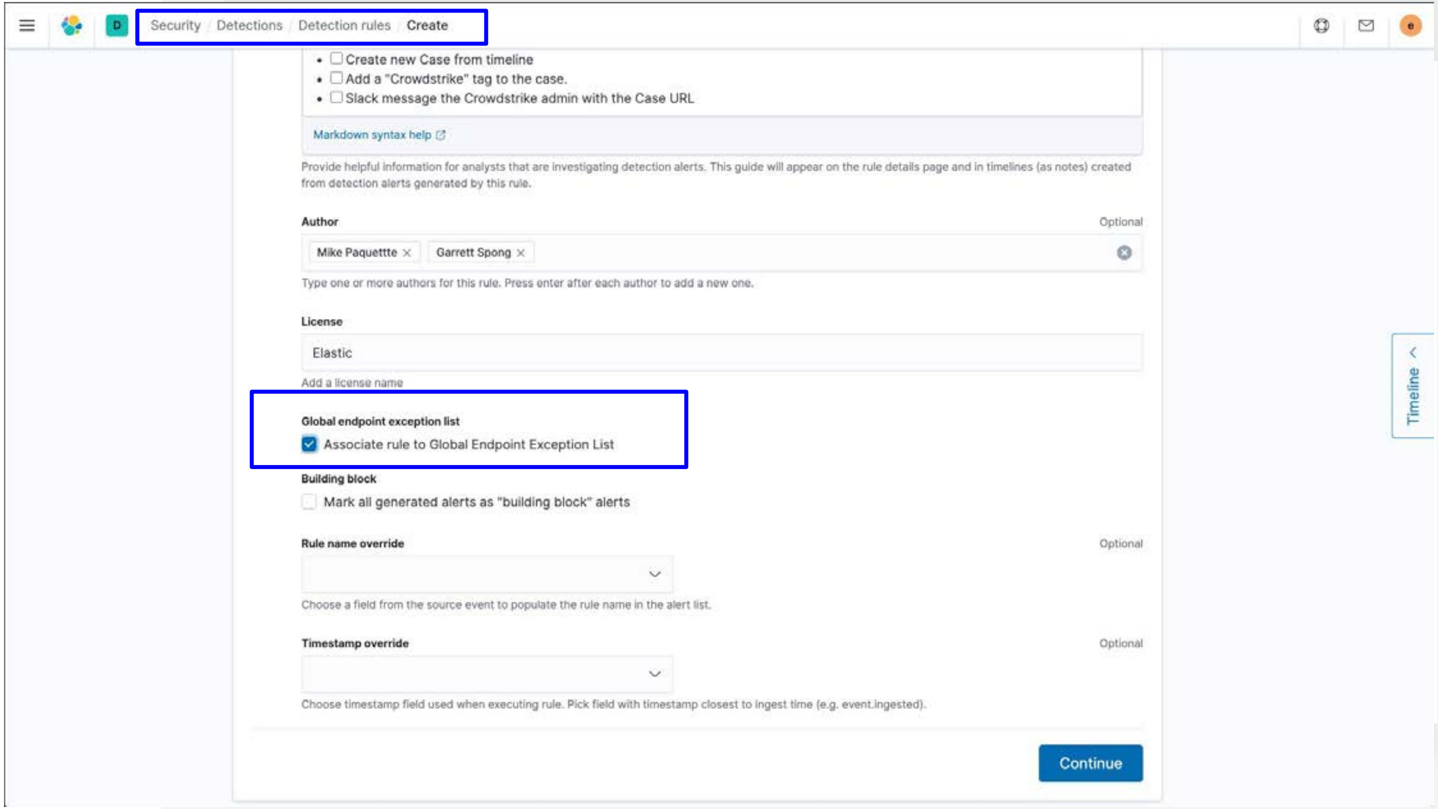
Timestamp override Optional

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

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.



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

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

Mike Paquettte × Garrett Spong ×

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

License

Elastic

Add a license name

Global endpoint exception list

☑ Associate rule to Global Endpoint Exception List

Building block

☐ 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.

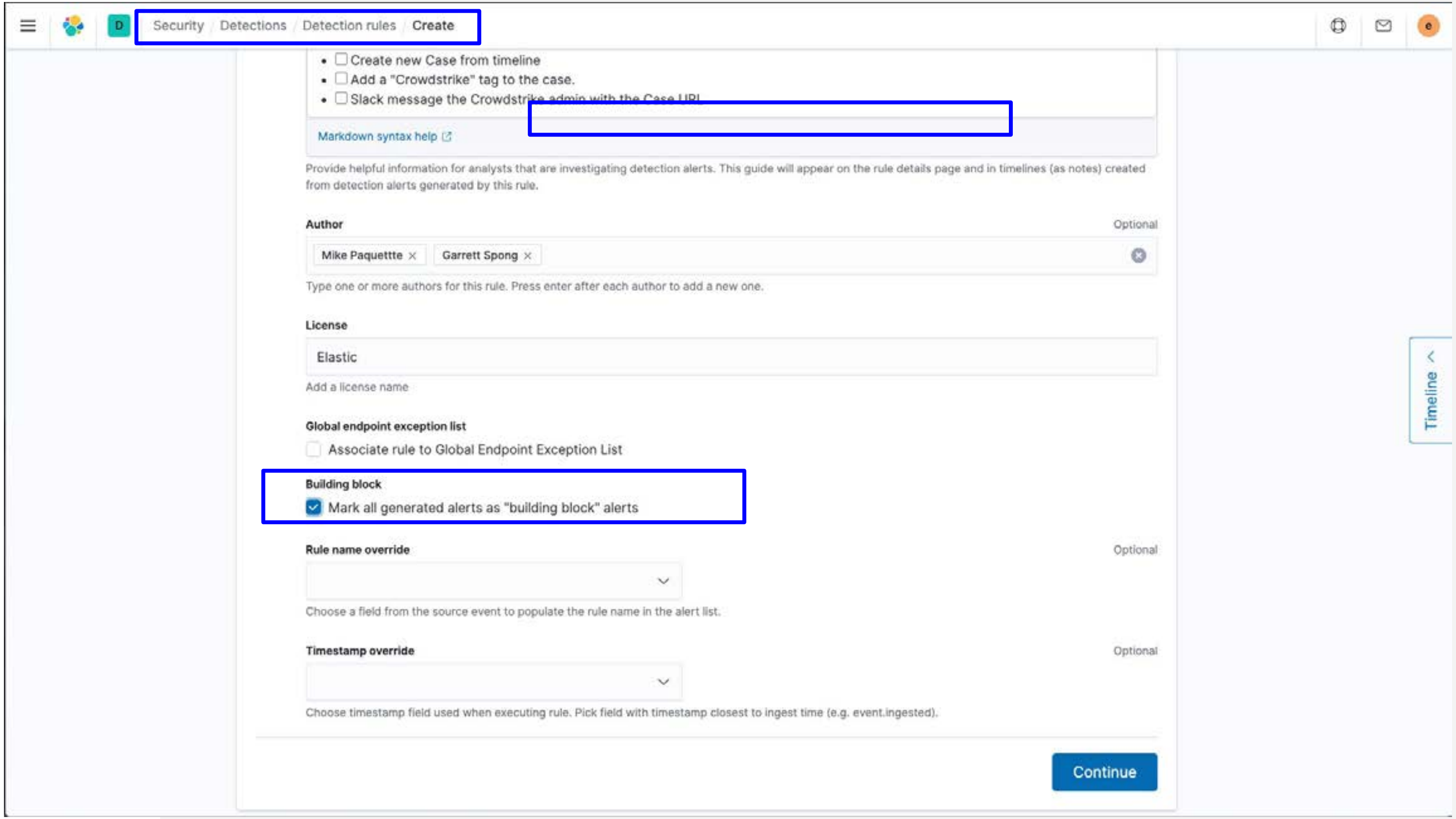
Timestamp override Optional

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

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.



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

Mike Paquettte × Garrett Spong ×

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

License

Elastic

Add a license name

Global endpoint exception list

□ Associate rule to Global Endpoint Exception List

Building block

☑ 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.

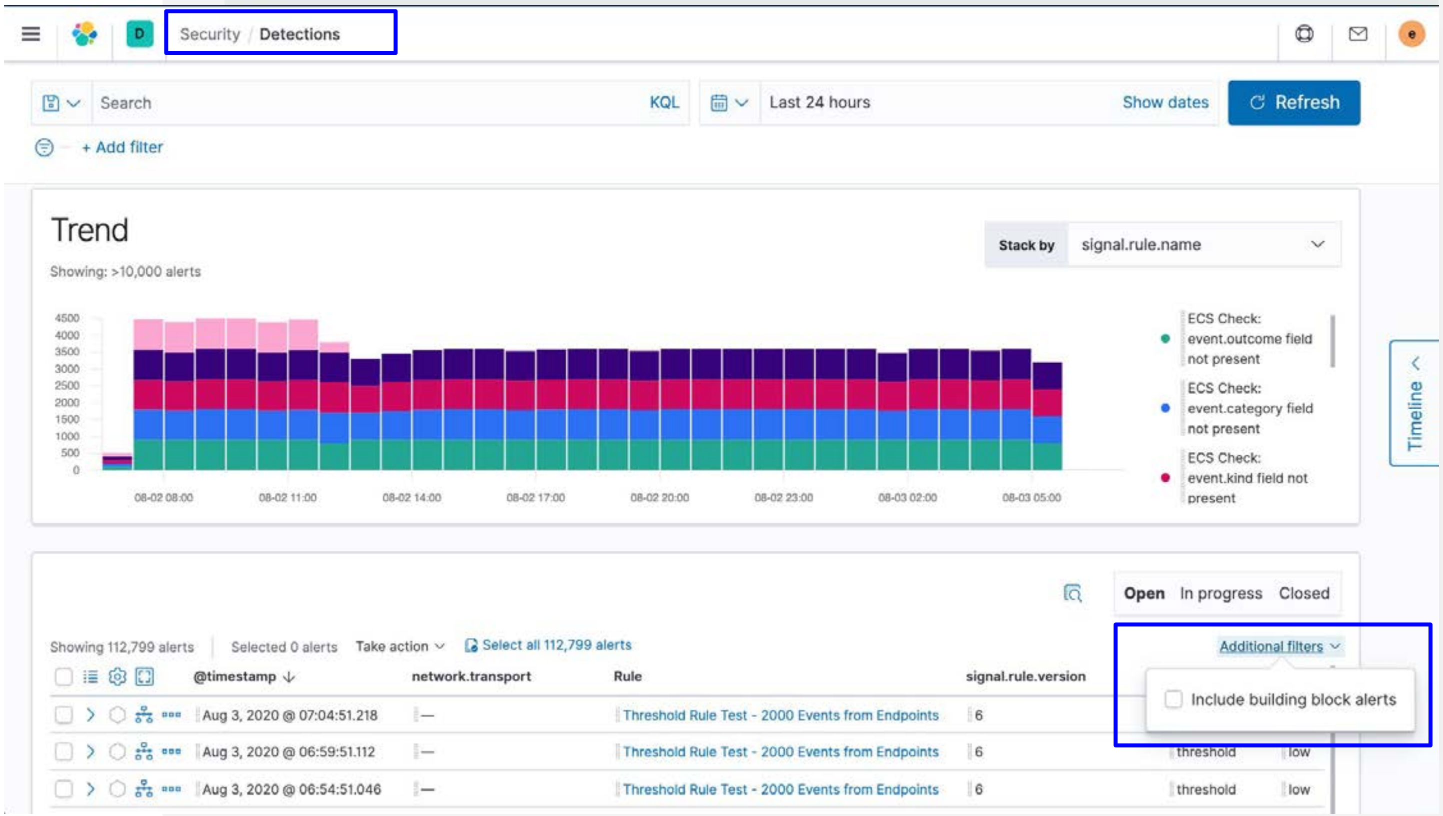
Timestamp override Optional

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

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"



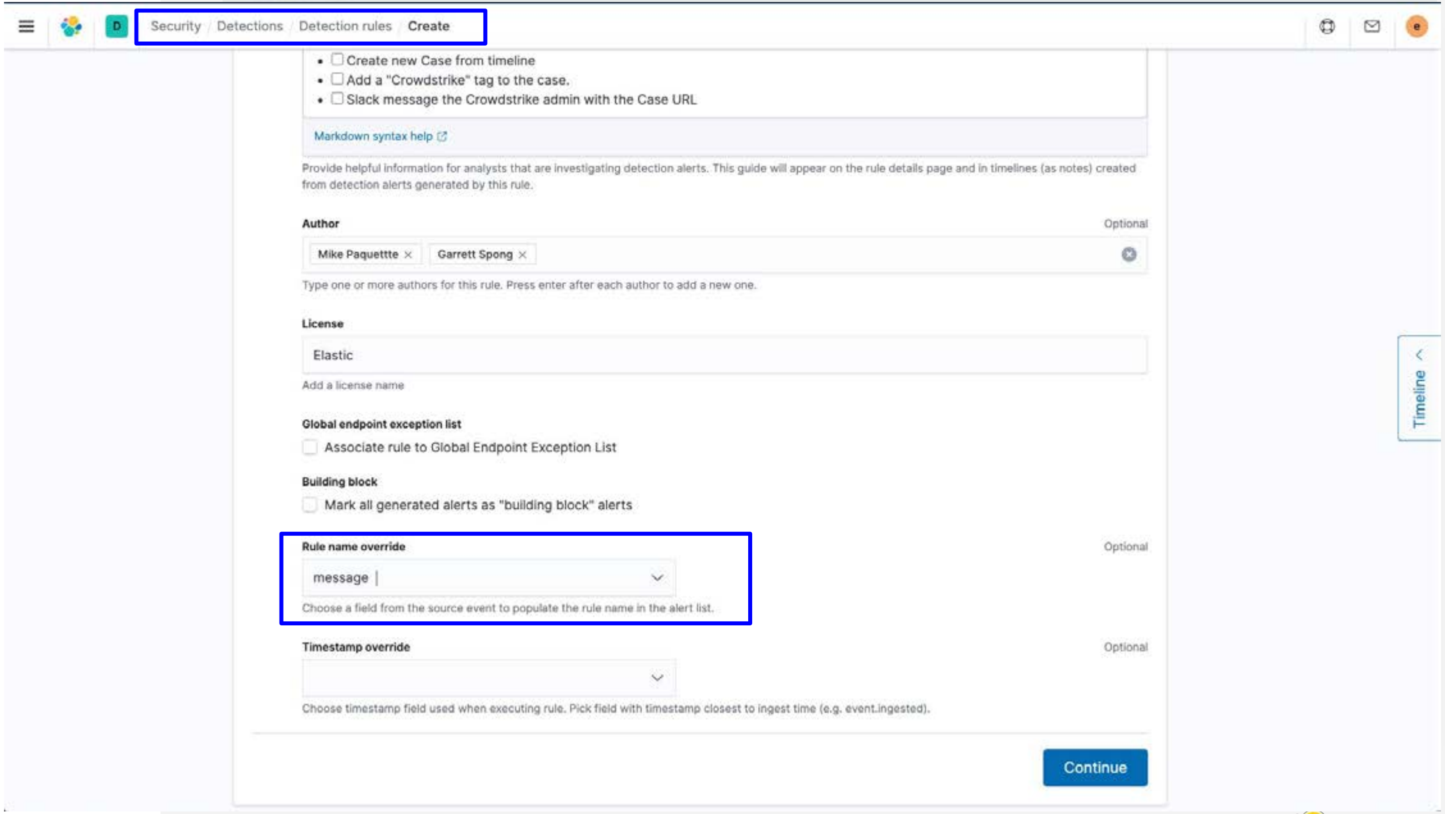
Showing 112,799 alerts | Selected 0 alerts | Take action | Select all 112,799 alerts

@timestamp	network.transport	Rule	signal.rule.version		
Aug 3, 2020 @ 07:04:51.218	—	Threshold Rule Test - 2000 Events from Endpoints	6		
Aug 3, 2020 @ 06:59:51.112	—	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low
Aug 3, 2020 @ 06:54:51.046	—	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low

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.



- □ 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

Mike Paquettte × Garrett Spong ×

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

License

Elastic

Add a license name

Global endpoint exception list

□ Associate rule to Global Endpoint Exception List

Building block

□ Mark all generated alerts as "building block" alerts

Rule name override Optional

message |

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).

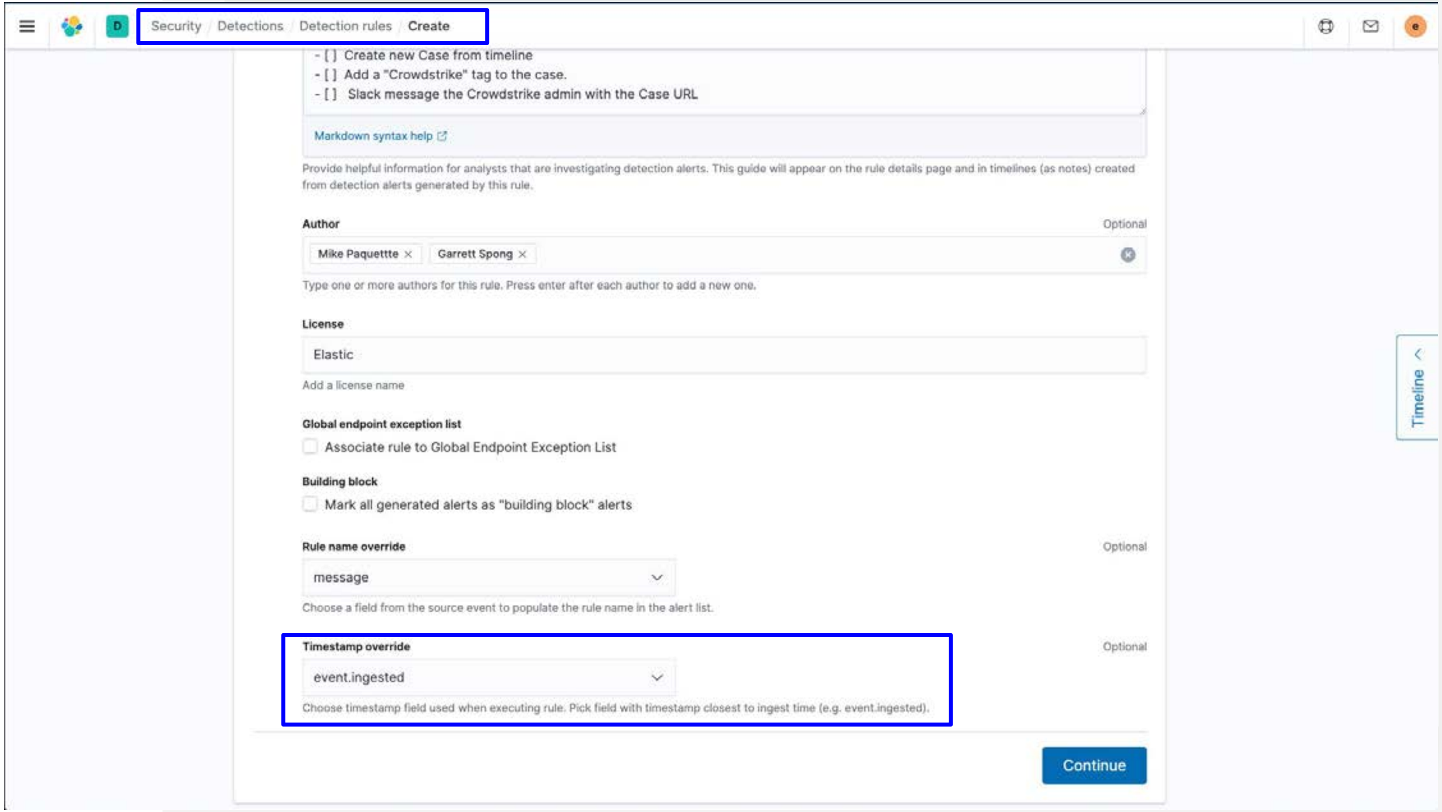
Continue

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

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



- [ ] 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

Mike Paquettte × Garrett Spong ×

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

License

Elastic

Add a license name

Global endpoint exception list

□ Associate rule to Global Endpoint Exception List

Building block

□ Mark all generated alerts as "building block" alerts

Rule name override — Optional

message

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

Timestamp override — Optional

event.ingested

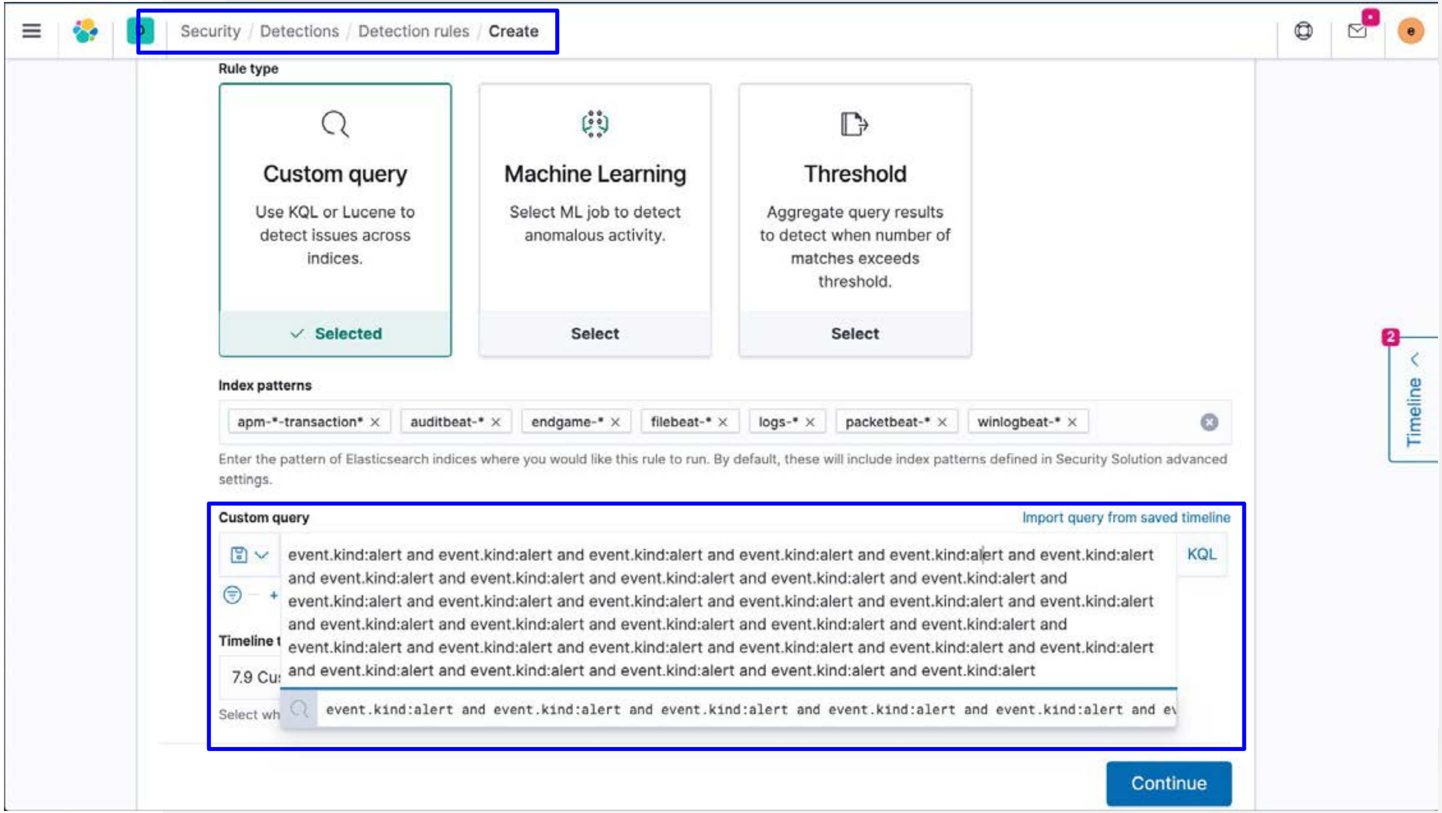
Choose timestamp field used when executing rule. Pick field with timestamp closest to ingest time (e.g. event.ingested).

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

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


Security / Detections / Detection rules / Create
Rule type
Custom query
Use KQL or Lucene to detect issues across indices.
✓ Selected
Machine Learning
Select ML job to detect anomalous activity.
Select
Threshold
Aggregate query results to detect when number of matches exceeds threshold.
Select
Index patterns
apm-*-transaction* ×
auditbeat-* ×
endgame-* ×
filebeat-* ×
logs-* ×
packetbeat-* ×
winlogbeat-* ×
Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.
Custom query
Import query from saved timeline
KQL
Timeline t
7.9 Cu
Select wh
Timeline
2
Continue

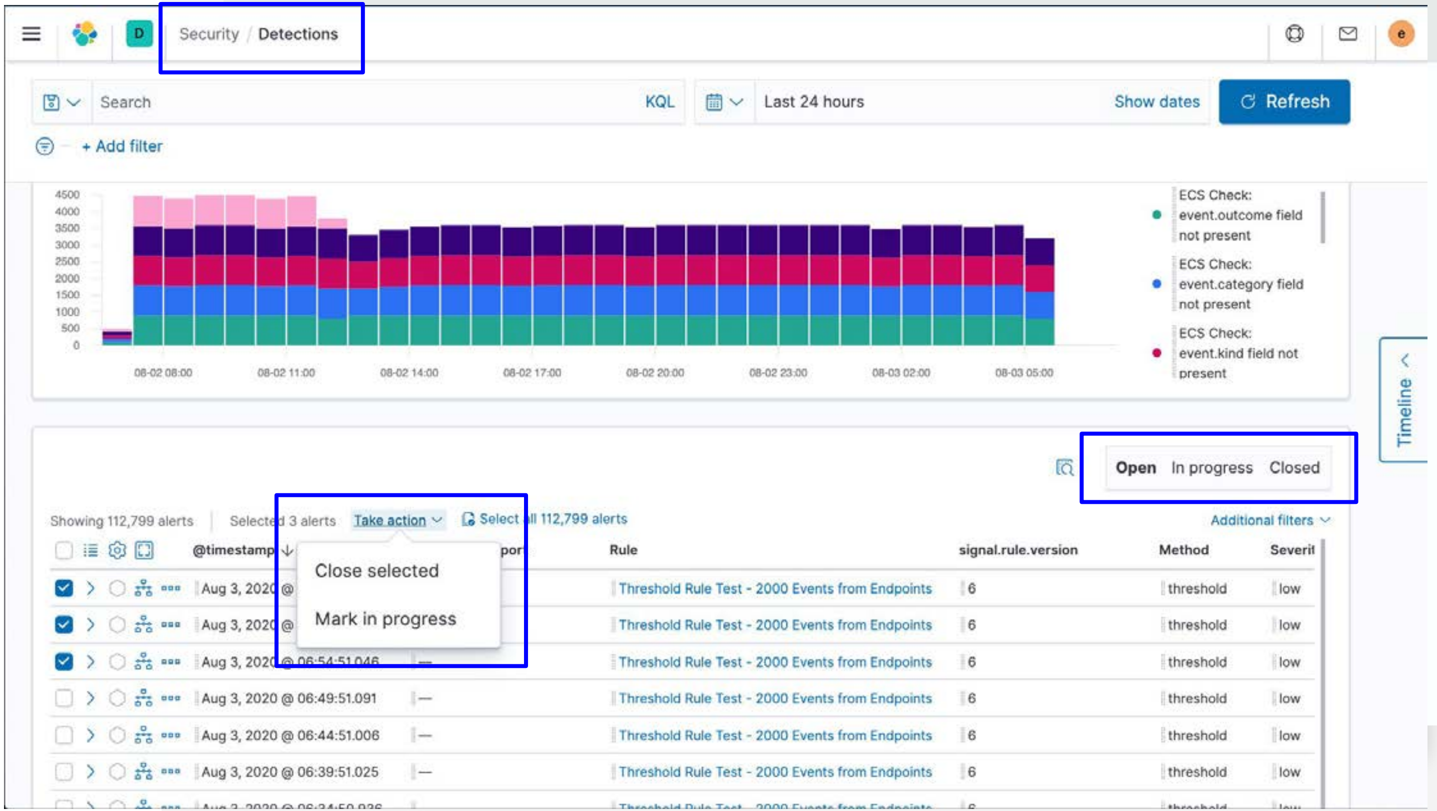
```
event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert
and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and
event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert
and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and
event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert
and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert
```

```
event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and event.kind:alert and ev
```

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 filteron “in progress detection alerts.



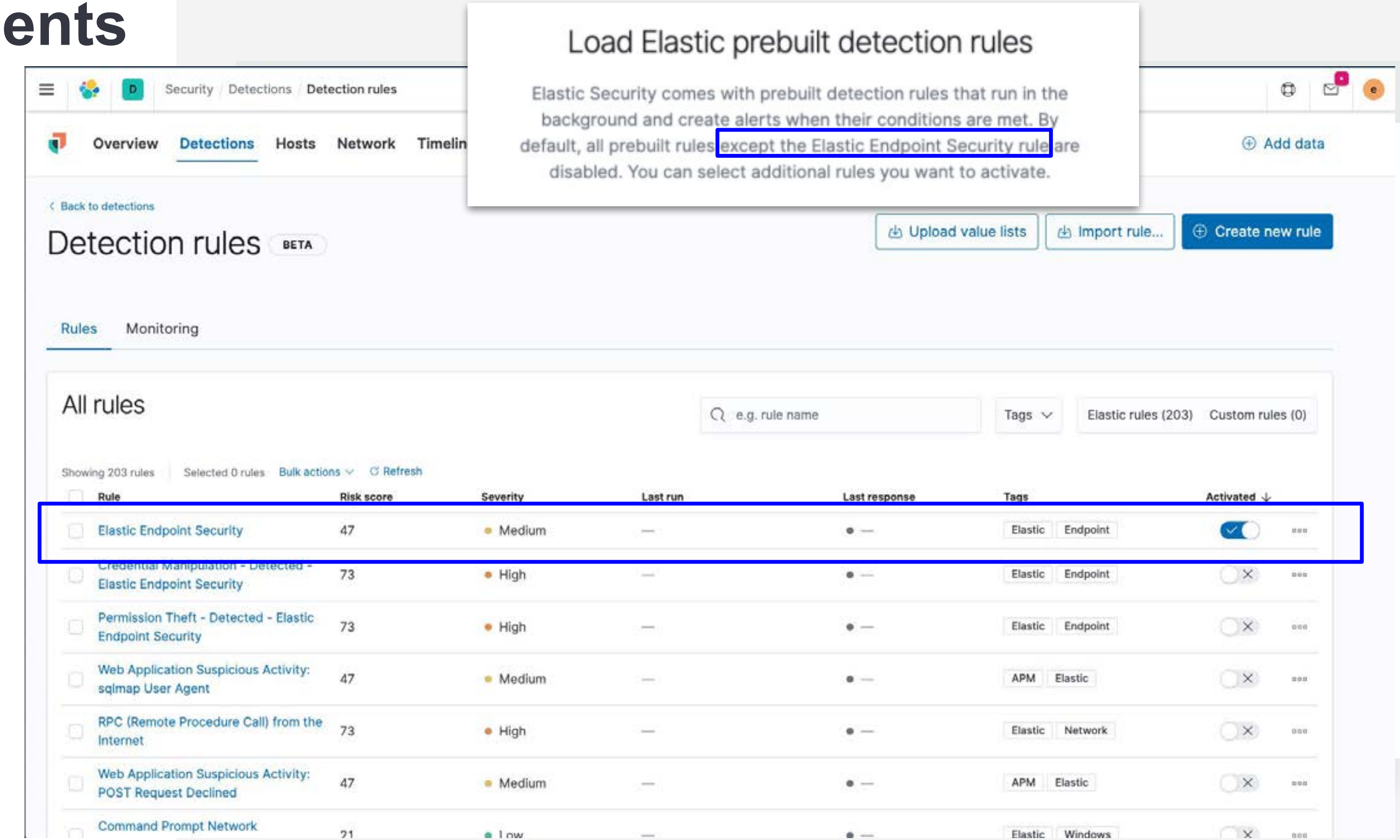
Showing 112,799 alerts | Selected 3 alerts | Select all 112,799 alerts

	@timestamp	por	Rule	signal.rule.version	Method	Severit
☑	Aug 3, 2020 @		Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low
☑	Aug 3, 2020 @		Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low
☑	Aug 3, 2020 @ 06:54:51.046	—	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low
□	Aug 3, 2020 @ 06:49:51.091	—	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low
□	Aug 3, 2020 @ 06:44:51.006	—	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low
□	Aug 3, 2020 @ 06:39:51.025	—	Threshold Rule Test - 2000 Events from Endpoints	6	threshold	low

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.

Detection rules BETA

Rules | Monitoring

All rules

e.g. rule name | Tags | Elastic rules (203) | Custom rules (0)

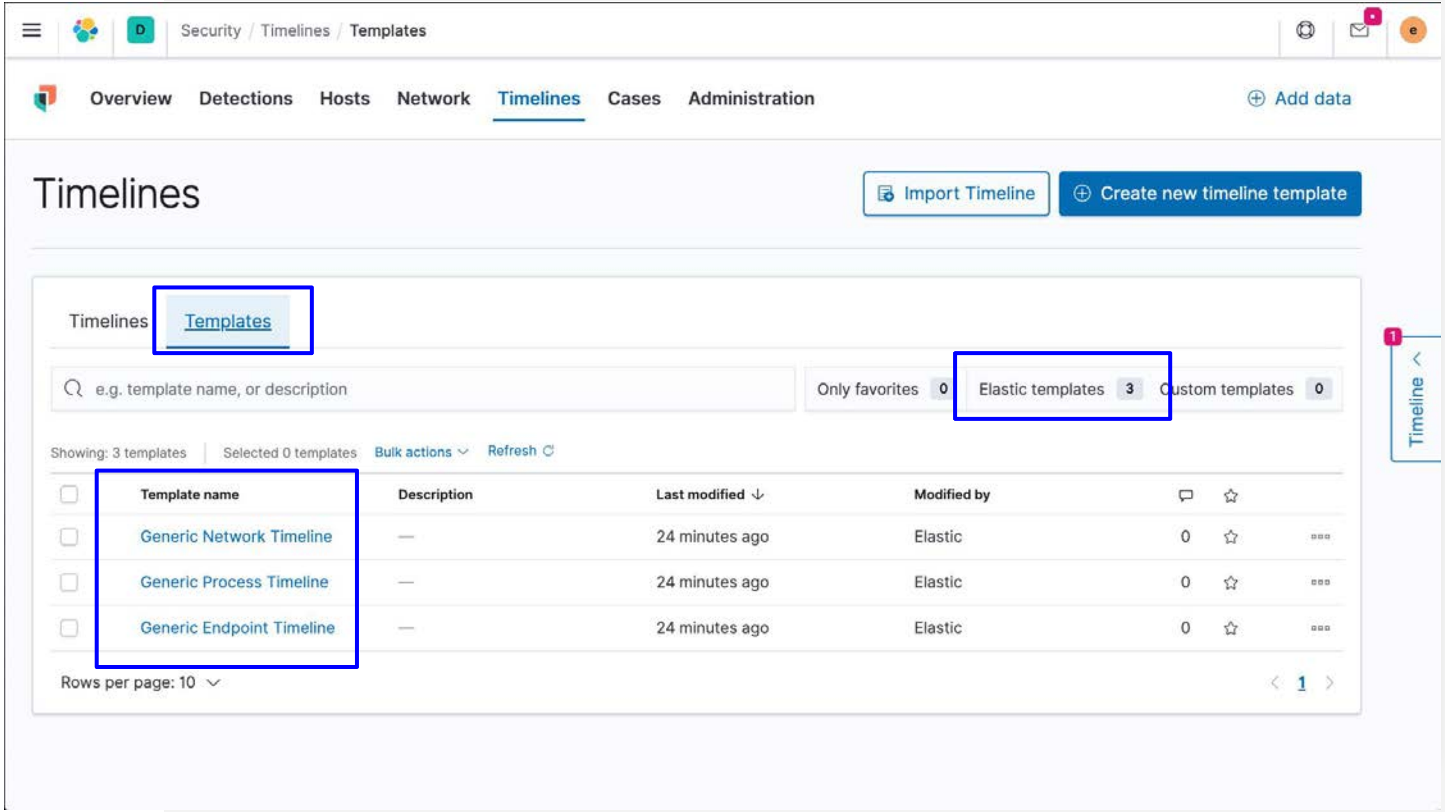
Showing 203 rules | Selected 0 rules | Bulk actions | Refresh

Rule	Risk score	Severity	Last run	Last response	Tags	Activated ↓
Elastic Endpoint Security	47	● Medium	—	● —	Elastic Endpoint	✓
Credential Manipulation - Detected - Elastic Endpoint Security	73	● High	—	● —	Elastic Endpoint	✕
Permission Theft - Detected - Elastic Endpoint Security	73	● High	—	● —	Elastic Endpoint	✕
Web Application Suspicious Activity: sqlmap User Agent	47	● Medium	—	● —	APM Elastic	✕
RPC (Remote Procedure Call) from the Internet	73	● High	—	● —	Elastic Network	✕
Web Application Suspicious Activity: POST Request Declined	47	● Medium	—	● —	APM Elastic	✕
Command Prompt Network	21	● Low	—	● —	Elastic Windows	✕

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



Security / Timelines / Templates

Overview · Detections · Hosts · Network · Timelines · Cases · Administration · Add data

Timelines

Import Timeline · Create new timeline template

Timelines · Templates

e.g. template name, or description

Only favorites 0 · Elastic templates 3 · Custom templates 0

Showing: 3 templates · Selected 0 templates · Bulk actions · Refresh

□	Template name	Description	Last modified ↓	Modified by	🗨	☆	
□	Generic Network Timeline	—	24 minutes ago	Elastic	0	☆	···
□	Generic Process Timeline	—	24 minutes ago	Elastic	0	☆	···
□	Generic Endpoint Timeline	—	24 minutes ago	Elastic	0	☆	···

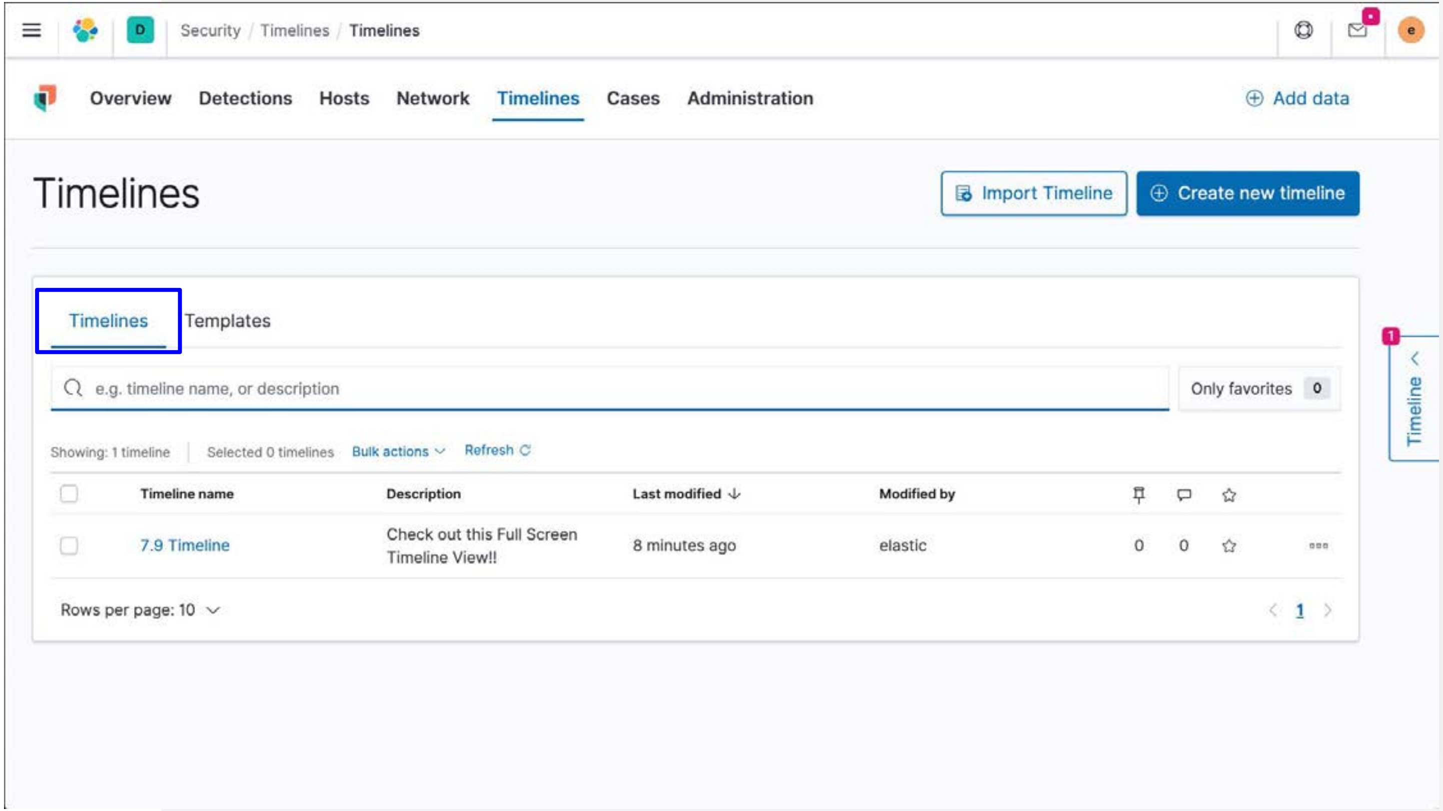
Rows per page: 10

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**

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



Showing: 1 timeline | Selected 0 timelines

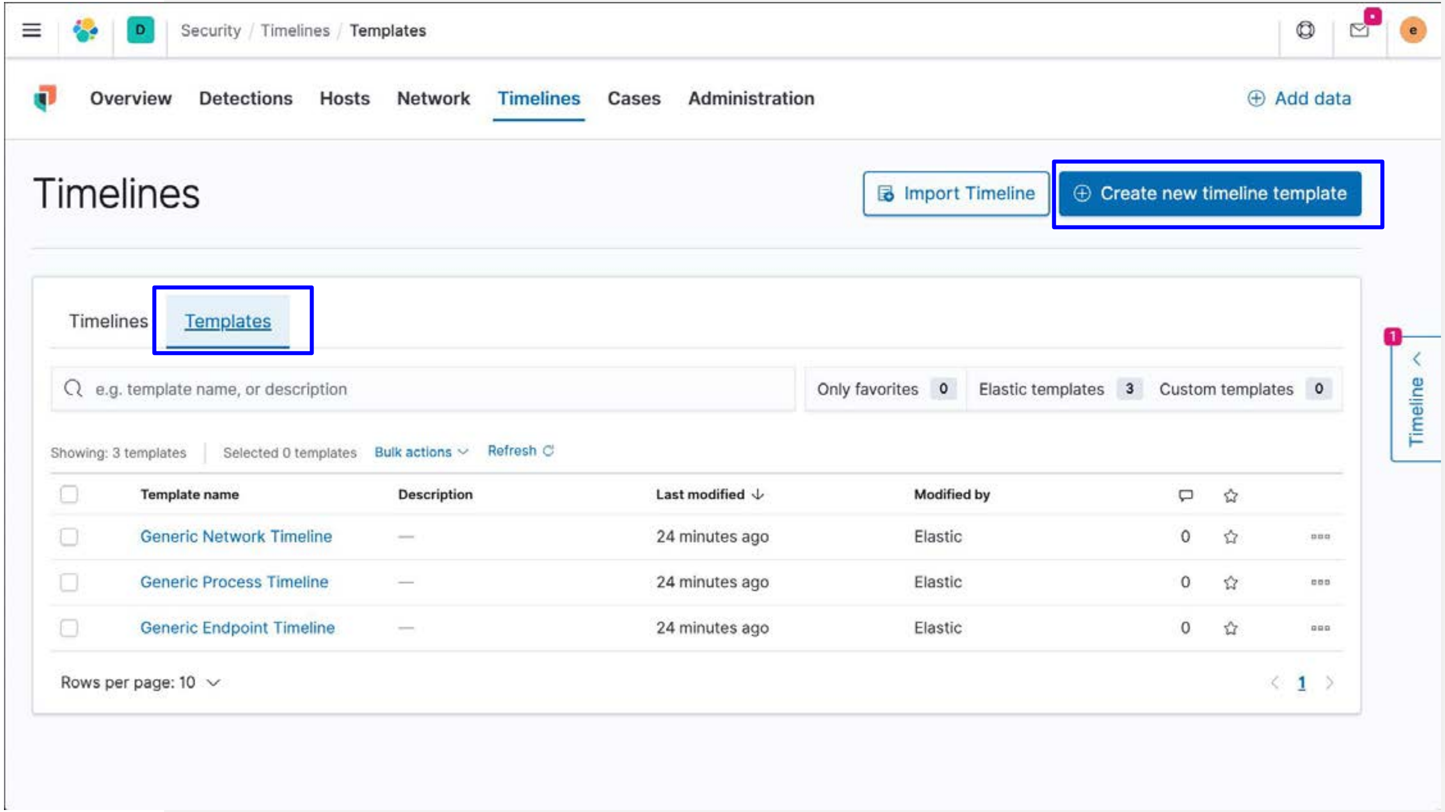
□	Timeline name	Description	Last modified ↓	Modified by			
□	7.9 Timeline	Check out this Full Screen Timeline View!!	8 minutes ago	elastic	0	0	☆

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**

In 7.9, can create your own timeline template!



Showing: 3 templates | Selected 0 templates Bulk actions Refresh

□	Template name	Description	Last modified ↓	Modified by	💬	☆	
□	Generic Network Timeline	—	24 minutes ago	Elastic	0	☆	...
□	Generic Process Timeline	—	24 minutes ago	Elastic	0	☆	...
□	Generic Endpoint Timeline	—	24 minutes ago	Elastic	0	☆	...

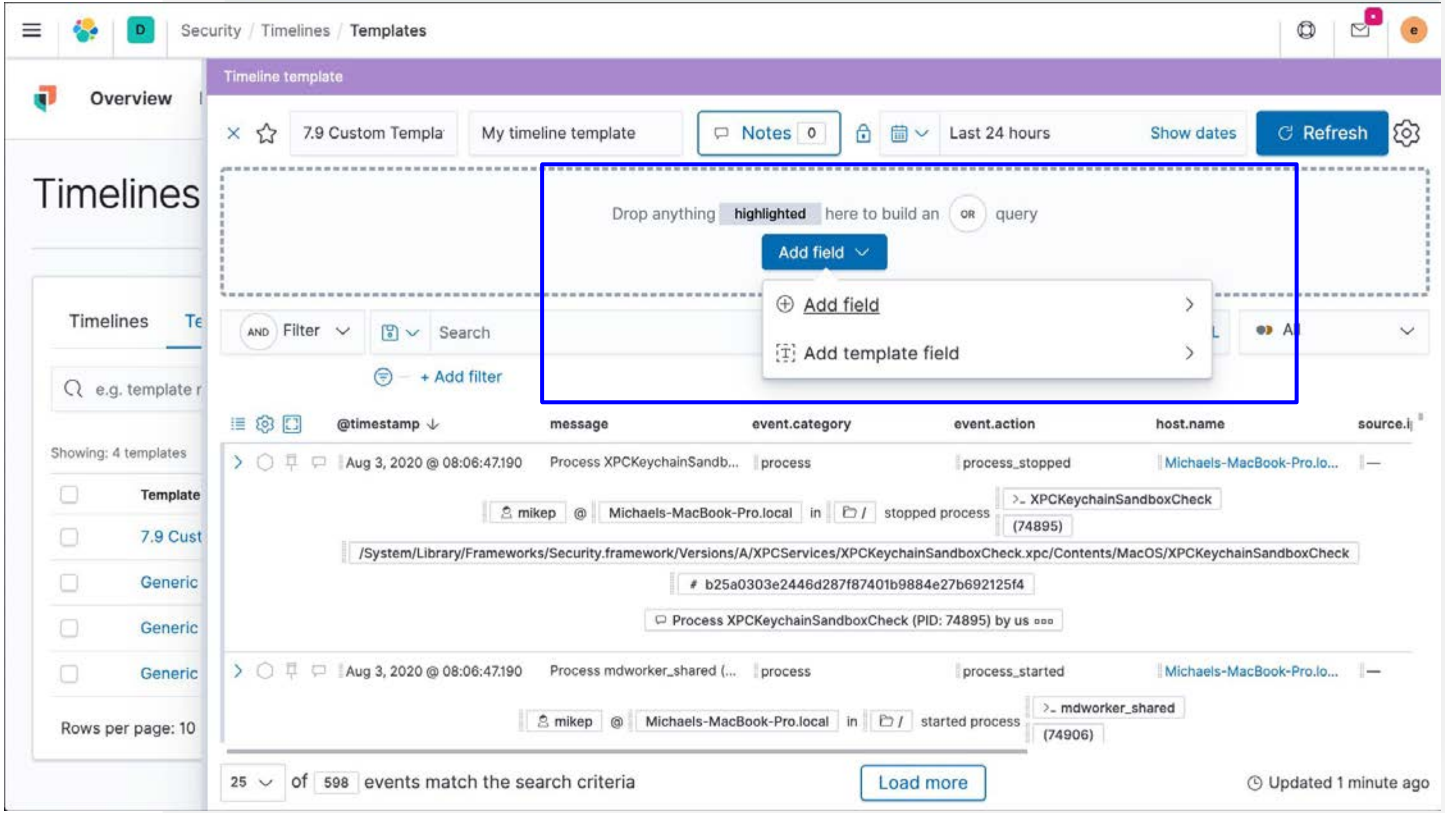
Rows per page: 10 ‹ 1 ›

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**

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"



@timestamp	message	event.category	event.action	host.name	source.i
Aug 3, 2020 @ 08:06:47.190	Process XPCKeychainSandb...	process	process_stopped	Michaels-MacBook-Pro.lo...	—
Aug 3, 2020 @ 08:06:47.190	Process mdworker_shared (...	process	process_started	Michaels-MacBook-Pro.lo...	—

mikep @ Michaels-MacBook-Pro.local in / stopped process >_ XPCKeychainSandboxCheck (74895)

/System/Library/Frameworks/Security.framework/Versions/A/XPCServices/XPCKeychainSandboxCheck.xpc/Contents/MacOS/XPCKeychainSandboxCheck

b25a0303e2446d287f87401b9884e27b692125f4

Process XPCKeychainSandboxCheck (PID: 74895) by us

mikep @ Michaels-MacBook-Pro.local in / started process >_ mdworker_shared (74906)

25 of 598 events match the search criteria

Load more

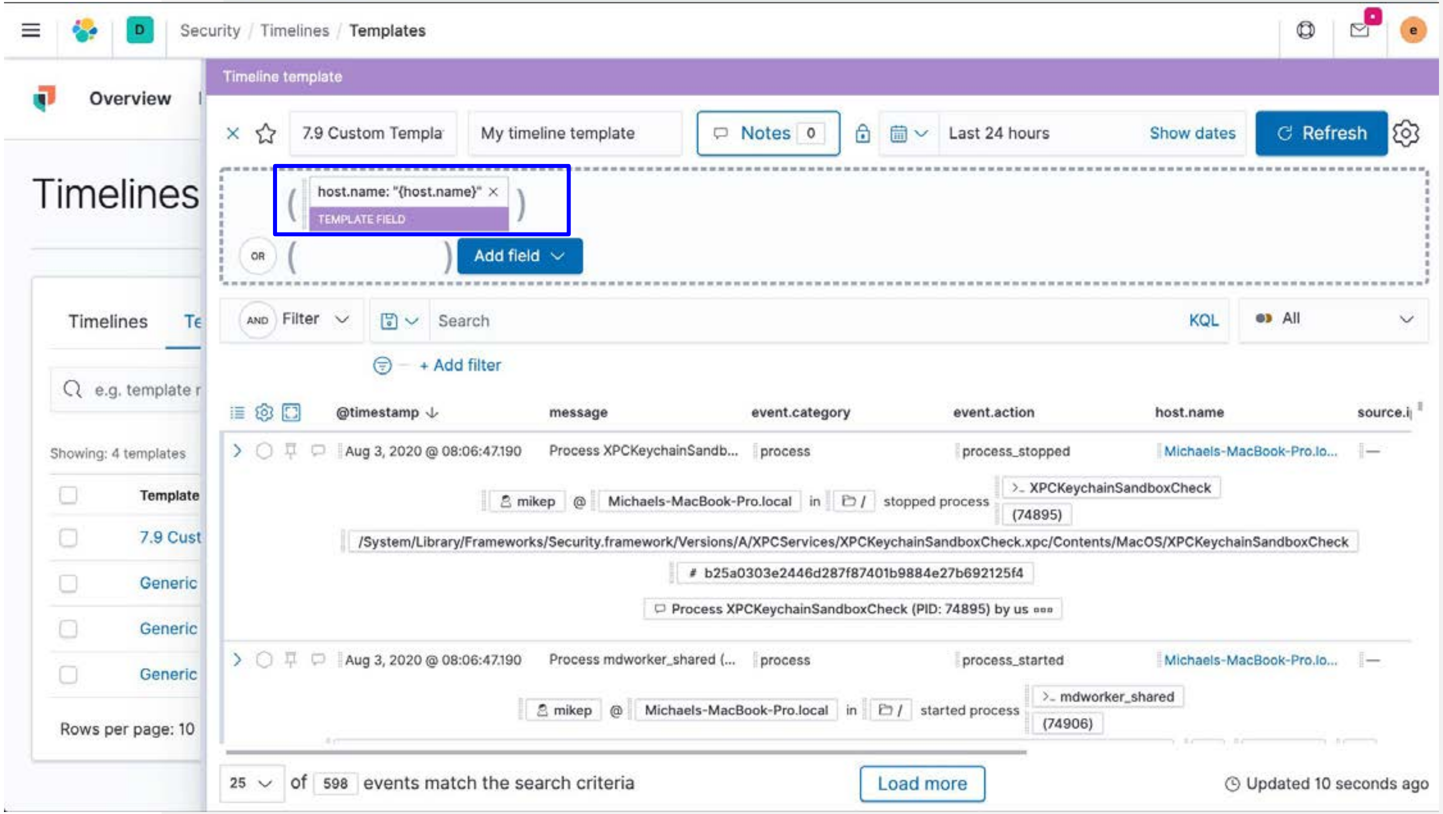
Updated 1 minute ago

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**

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



Security / Timelines / Templates

Overview

Timelines

Timelines Te

e.g. template r

Showing: 4 templates

□	Template
□	7.9 Cust
□	Generic
□	Generic
□	Generic

Rows per page: 10

Timeline template

7.9 Custom Templa | My timeline template | Notes 0 | Last 24 hours | Show dates | Refresh

(host.name: "{host.name}" × TEMPLATE FIELD)

OR ( ) Add field

AND Filter | Search | KQL | All

+ Add filter

@timestamp	message	event.category	event.action	host.name	source.i
Aug 3, 2020 @ 08:06:47.190	Process XPCKeychainSandb...	process	process_stopped	Michaels-MacBook-Pro.lo...	—
Aug 3, 2020 @ 08:06:47.190	Process mdworker_shared (...	process	process_started	Michaels-MacBook-Pro.lo...	—

```
mikep @ Michaels-MacBook-Pro.local in / stopped process >_ XPCKeychainSandboxCheck (74895)
/System/Library/Frameworks/Security.framework/Versions/A/XPCServices/XPCKeychainSandboxCheck.xpc/Contents/MacOS/XPCKeychainSandboxCheck
# b25a0303e2446d287f87401b9884e27b692125f4
Process XPCKeychainSandboxCheck (PID: 74895) by us ...
```

```
mikep @ Michaels-MacBook-Pro.local in / started process >_ mdworker_shared (74906)
```

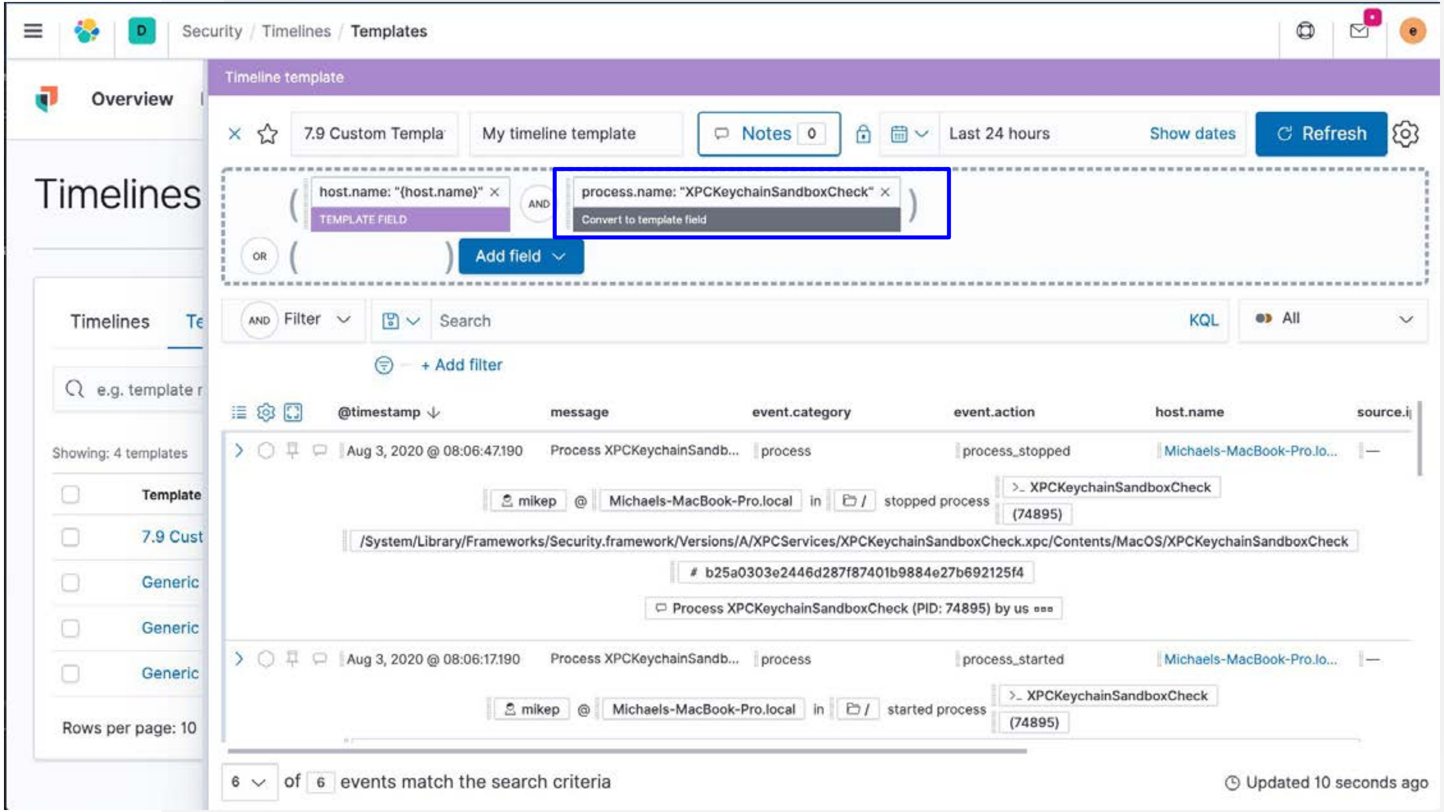
25 of 598 events match the search criteria | Load more | Updated 10 seconds ago

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**

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



@timestamp	message	event.category	event.action	host.name	source.i
Aug 3, 2020 @ 08:06:47.190	Process XPCKeychainSandb...	process	process_stopped	Michaels-MacBook-Pro.lo...	—
Aug 3, 2020 @ 08:06:17.190	Process XPCKeychainSandb...	process	process_started	Michaels-MacBook-Pro.lo...	—

mikep @ Michaels-MacBook-Pro.local in / stopped process >_ XPCKeychainSandboxCheck (74895)

/System/Library/Frameworks/Security.framework/Versions/A/XPCServices/XPCKeychainSandboxCheck.xpc/Contents/MacOS/XPCKeychainSandboxCheck

b25a0303e2446d287f87401b9884e27b692125f4

Process XPCKeychainSandboxCheck (PID: 74895) by us ...

mikep @ Michaels-MacBook-Pro.local in / started process >_ XPCKeychainSandboxCheck (74895)

6 of 6 events match the search criteria

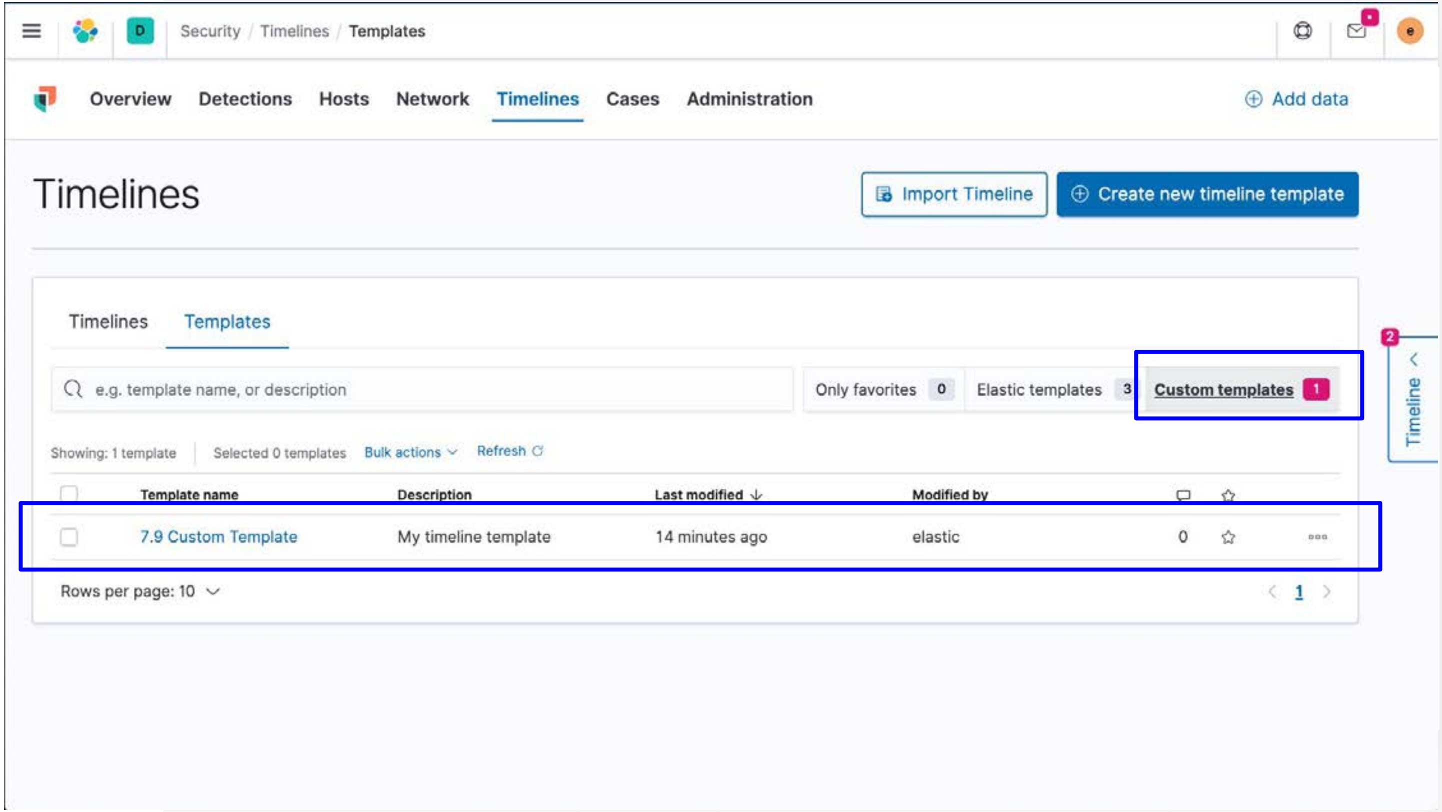
Updated 10 seconds ago

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**

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



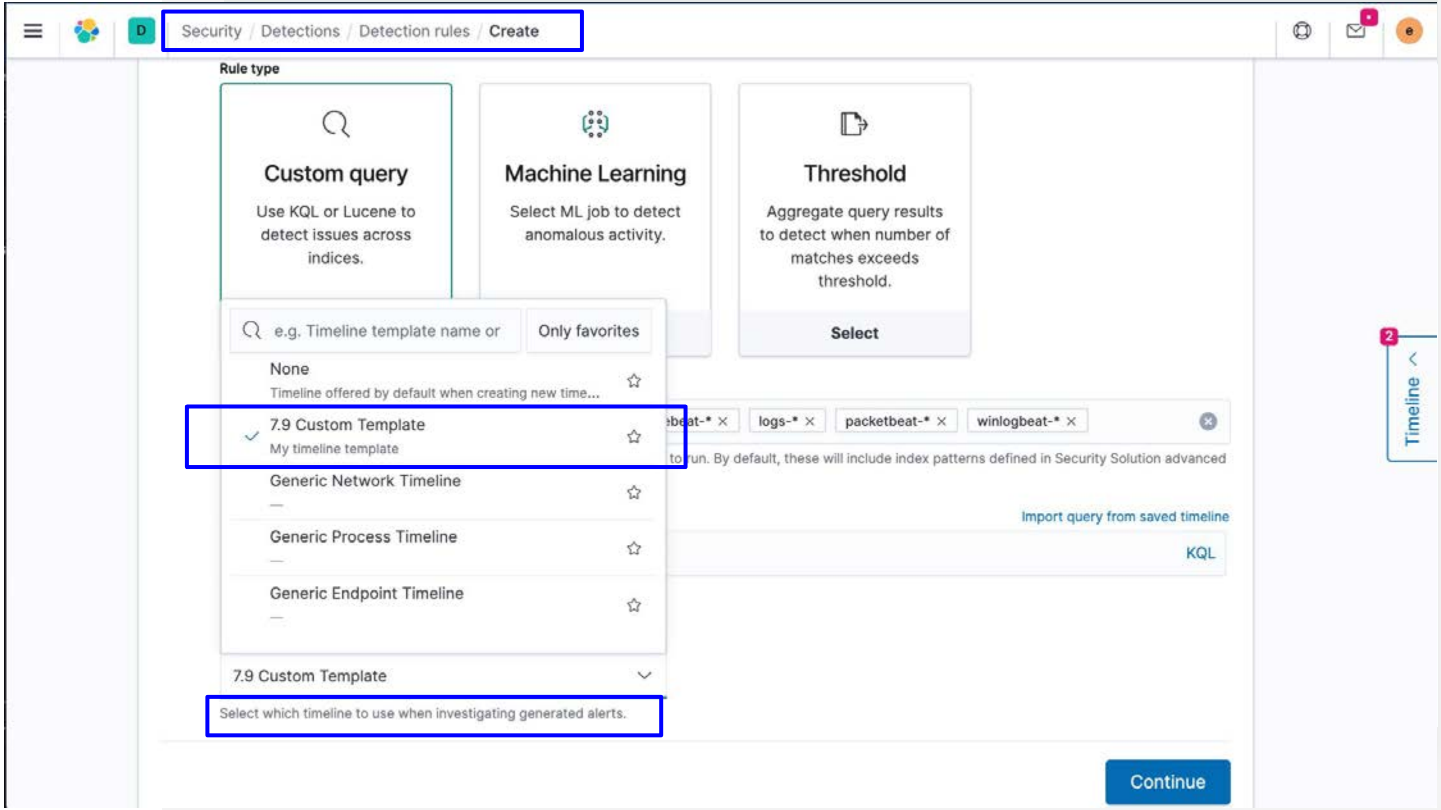
	Template name	Description	Last modified ↓	Modified by		
□	7.9 Custom Template	My timeline template	14 minutes ago	elastic	0	☆

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**

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



D
Security / Detections / Detection rules / Create
Timeline
2

Rule type

Custom query
Use KQL or Lucene to detect issues across indices.

Machine Learning
Select ML job to detect anomalous activity.

Threshold
Aggregate query results to detect when number of matches exceeds threshold.

Select
e.g. Timeline template name or
Only favorites

None
Timeline offered by default when creating new time...

✓ 7.9 Custom Template
My timeline template

Generic Network Timeline
—

Generic Process Timeline
—

Generic Endpoint Timeline
—

…to run. By default, these will include index patterns defined in Security Solution advanced

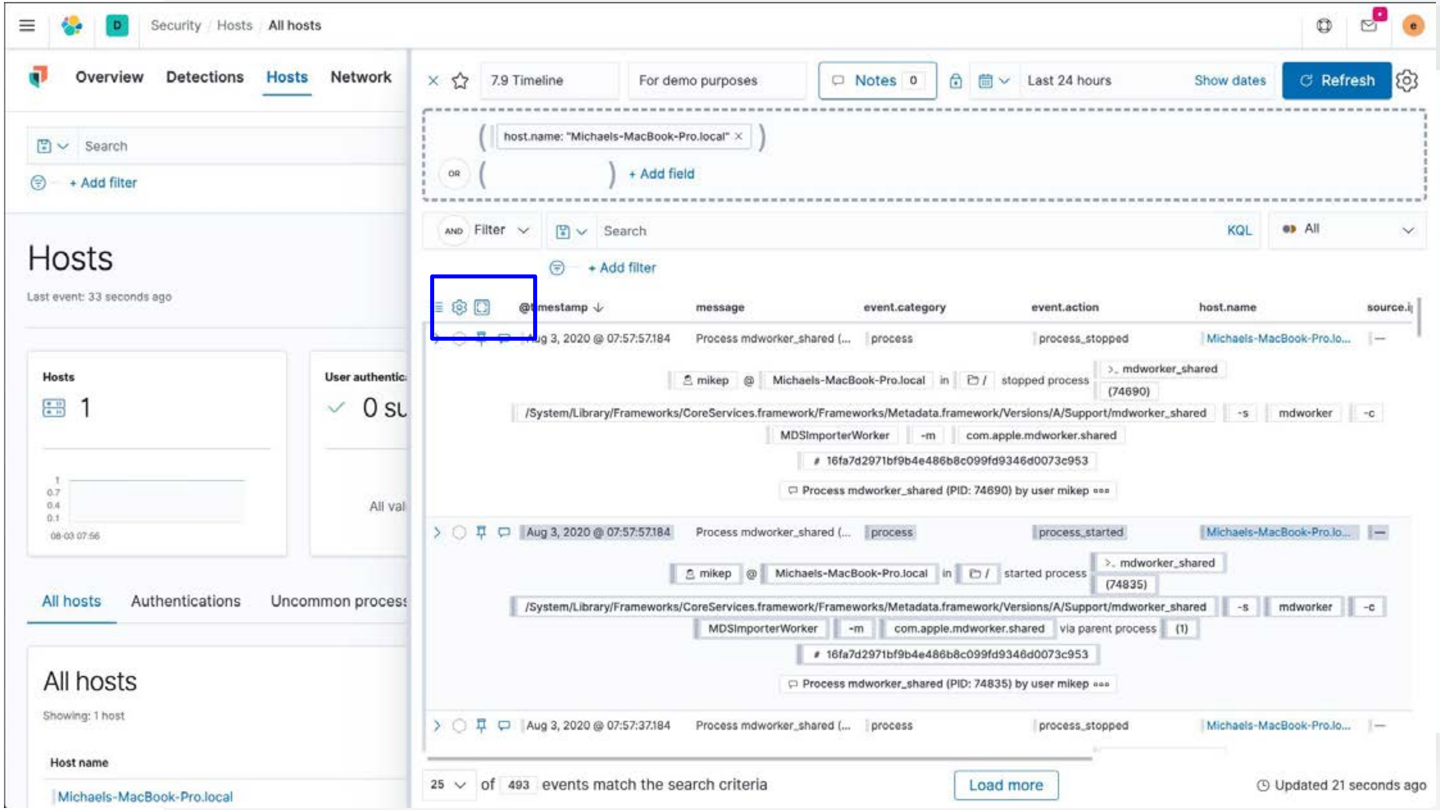
7.9 Custom Template

Select which timeline to use when investigating generated 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**

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



host.name: "Michaels-MacBook-Pro.local"

@timestamp	message	event.category	event.action	host.name	source.i
Aug 3, 2020 @ 07:57:57.184	Process mdworker_shared (...	process	process_stopped	Michaels-MacBook-Pro.lo...	—

mikep @ Michaels-MacBook-Pro.local in / stopped process >_ mdworker_shared (74690)
/System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared -s mdworker -c MDSImporterWorker -m com.apple.mdworker.shared
16fa7d2971bf9b4e486b8c099fd9346d0073c953
Process mdworker_shared (PID: 74690) by user mikep

@timestamp	message	event.category	event.action	host.name	source.i
Aug 3, 2020 @ 07:57:57.184	Process mdworker_shared (...	process	process_started	Michaels-MacBook-Pro.lo...	—

mikep @ Michaels-MacBook-Pro.local in / started process >_ mdworker_shared (74835)
/System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared -s mdworker -c MDSImporterWorker -m com.apple.mdworker.shared via parent process (1)
16fa7d2971bf9b4e486b8c099fd9346d0073c953
Process mdworker_shared (PID: 74835) by user mikep

@timestamp	message	event.category	event.action	host.name	source.i
Aug 3, 2020 @ 07:57:37.184	Process mdworker_shared (...	process	process_stopped	Michaels-MacBook-Pro.lo...	—

25 of 493 events match the search criteria

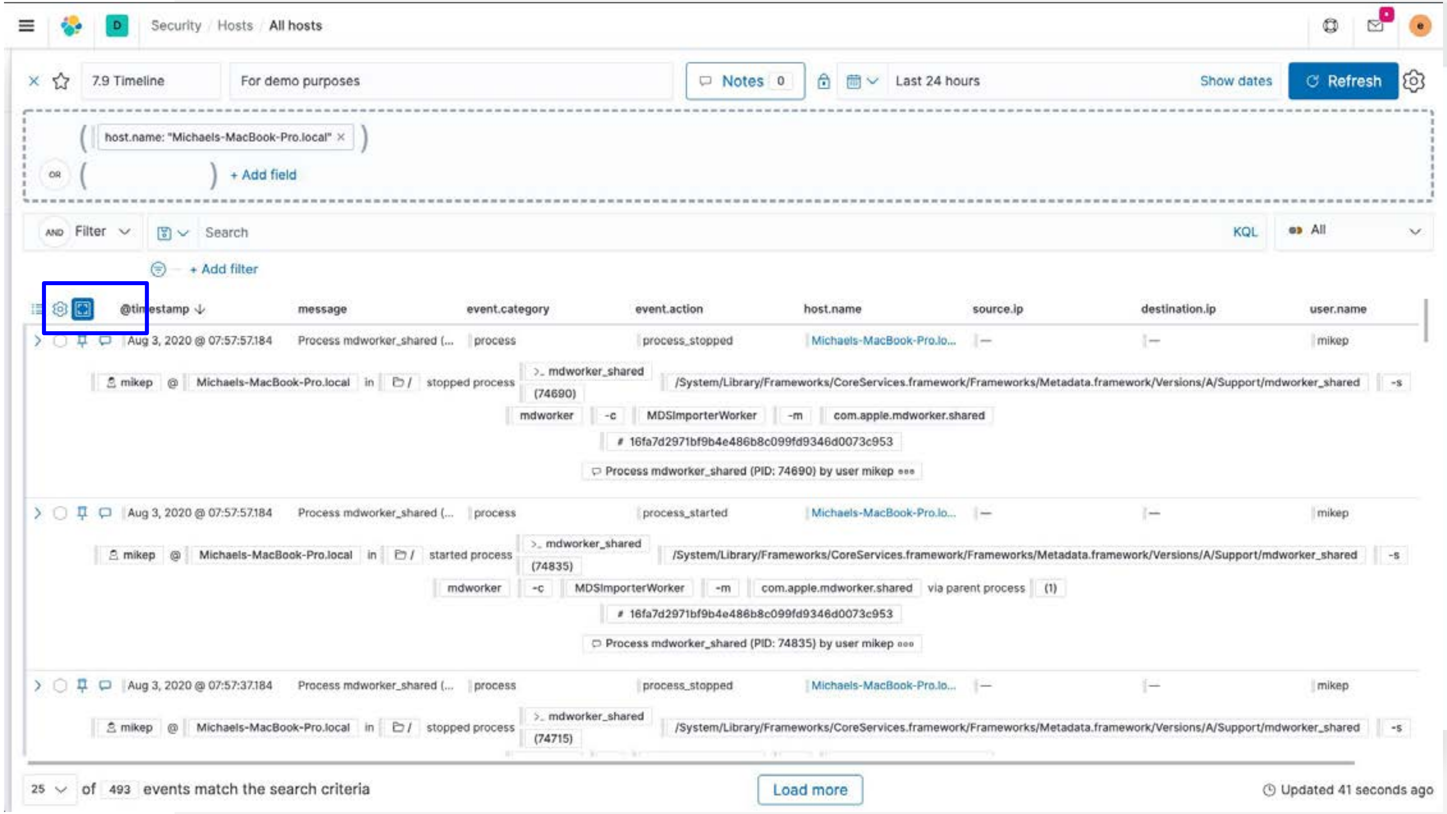
Load more

Updated 21 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**

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



7.9 Timeline

For demo purposes

(host.name: "Michaels-MacBook-Pro.local" ×)

@timestamp ↓	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Aug 3, 2020 @ 07:57:57.184	Process mdworker_shared (...	process	process_stopped	Michaels-MacBook-Pro.lo...	—	—	mikep

mikep @ Michaels-MacBook-Pro.local in / stopped process >_ mdworker_shared (74690) /System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared -s mdworker -c MDSImporterWorker -m com.apple.mdworker.shared

16fa7d2971bf9b4e486b8c099fd9346d0073c953

Process mdworker_shared (PID: 74690) by user mikep ···

@timestamp ↓	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Aug 3, 2020 @ 07:57:57.184	Process mdworker_shared (...	process	process_started	Michaels-MacBook-Pro.lo...	—	—	mikep

mikep @ Michaels-MacBook-Pro.local in / started process >_ mdworker_shared (74835) /System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared -s mdworker -c MDSImporterWorker -m com.apple.mdworker.shared via parent process (1)

16fa7d2971bf9b4e486b8c099fd9346d0073c953

Process mdworker_shared (PID: 74835) by user mikep ···

@timestamp ↓	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Aug 3, 2020 @ 07:57:37.184	Process mdworker_shared (...	process	process_stopped	Michaels-MacBook-Pro.lo...	—	—	mikep

mikep @ Michaels-MacBook-Pro.local in / stopped process >_ mdworker_shared (74715) /System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared -s

25 of 493 events match the search criteria

Updated 41 seconds ago

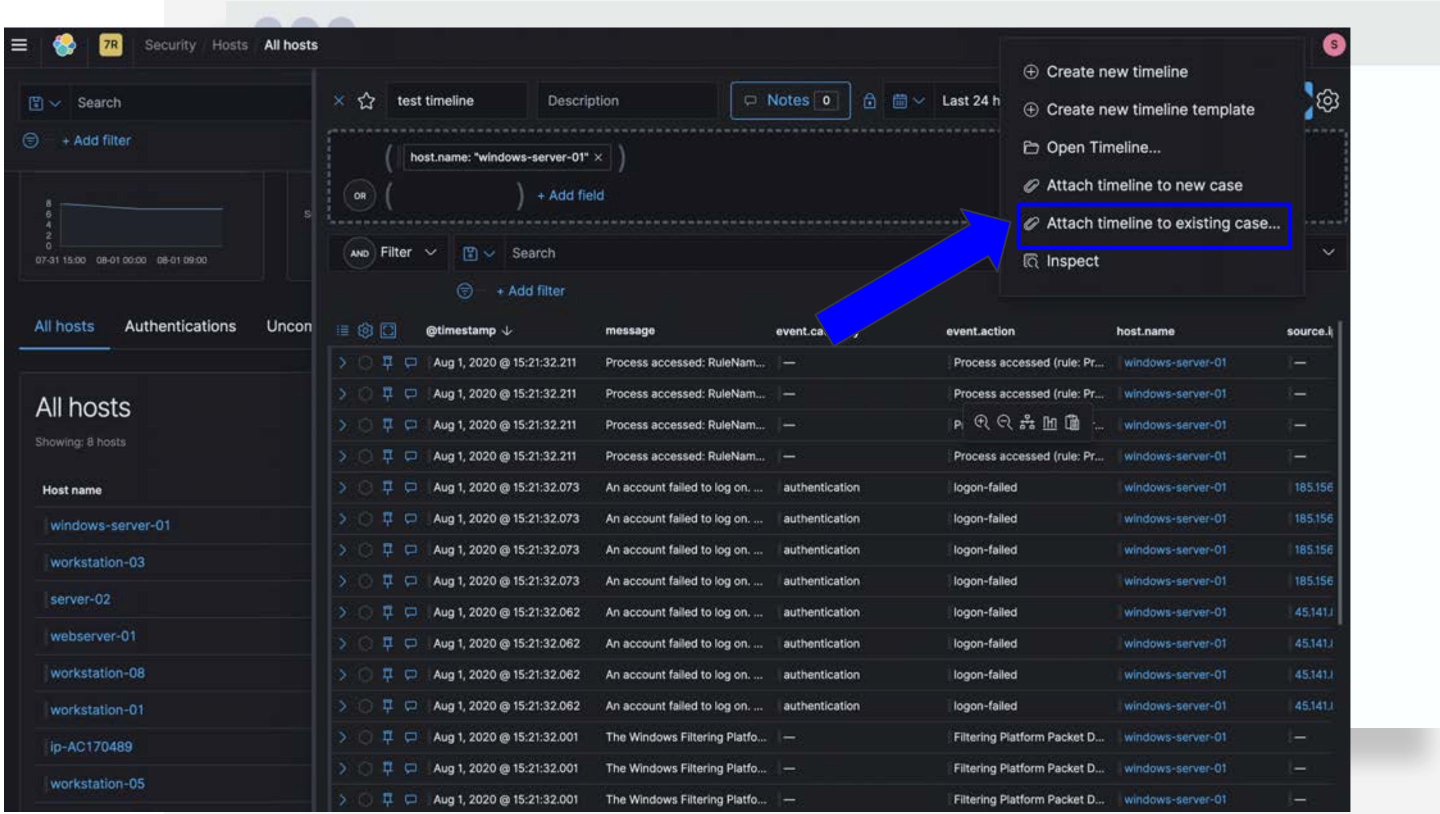
elastic

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**



@timestamp	message	event.ca	event.action	host.name	source.i
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...	—	P[illegible]...	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 @ 15:21:32.073	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.(
Aug 1, 2020 @ 15:21:32.062	An account failed to log on. ...	authentication	logon-failed	windows-server-01	45.141.(
Aug 1, 2020 @ 15:21:32.062	An account failed to log on. ...	authentication	logon-failed	windows-server-01	45.141.(
Aug 1, 2020 @ 15:21:32.062	An account failed to log on. ...	authentication	logon-failed	windows-server-01	45.141.(
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	—

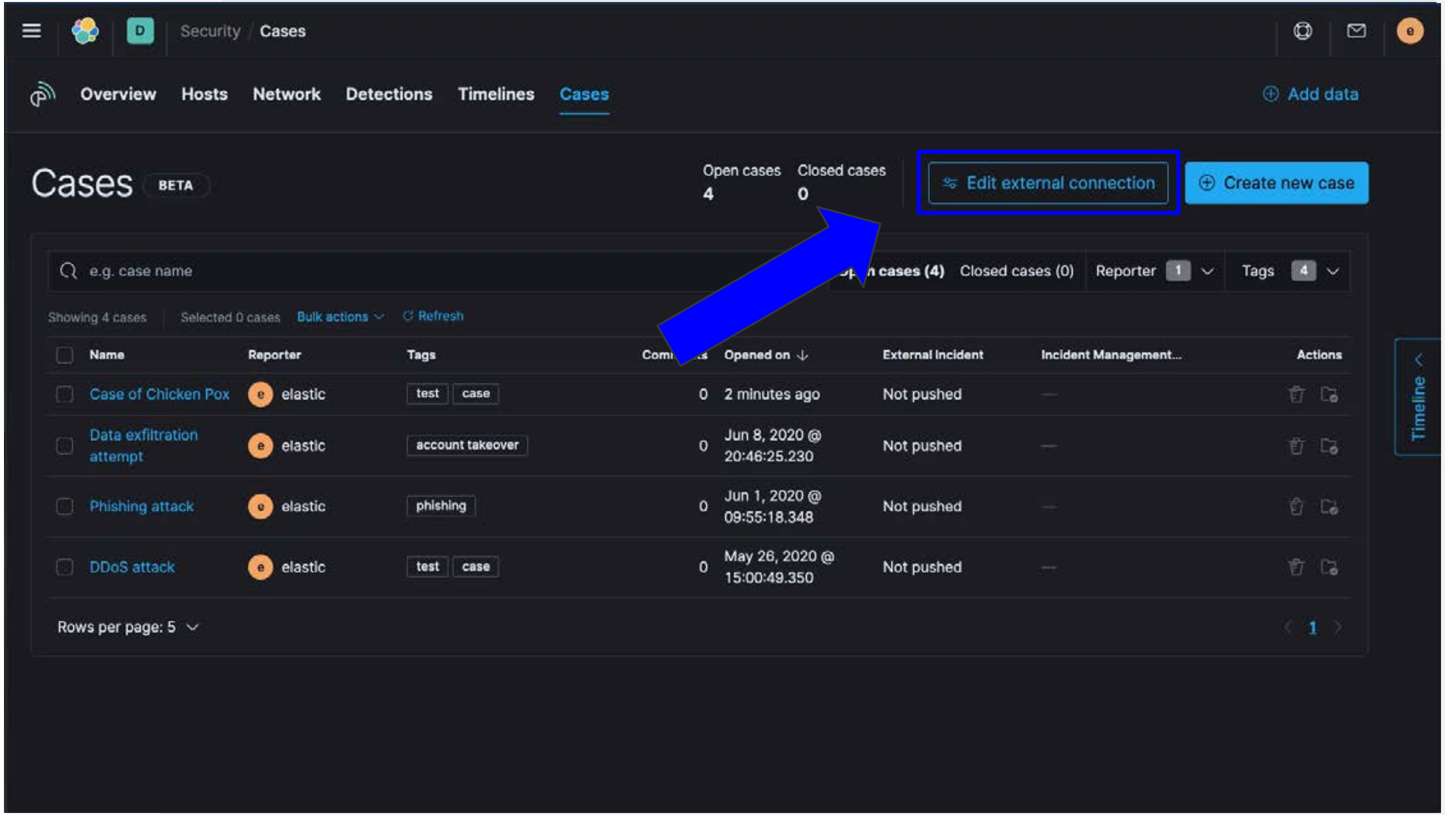
elastic

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**



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

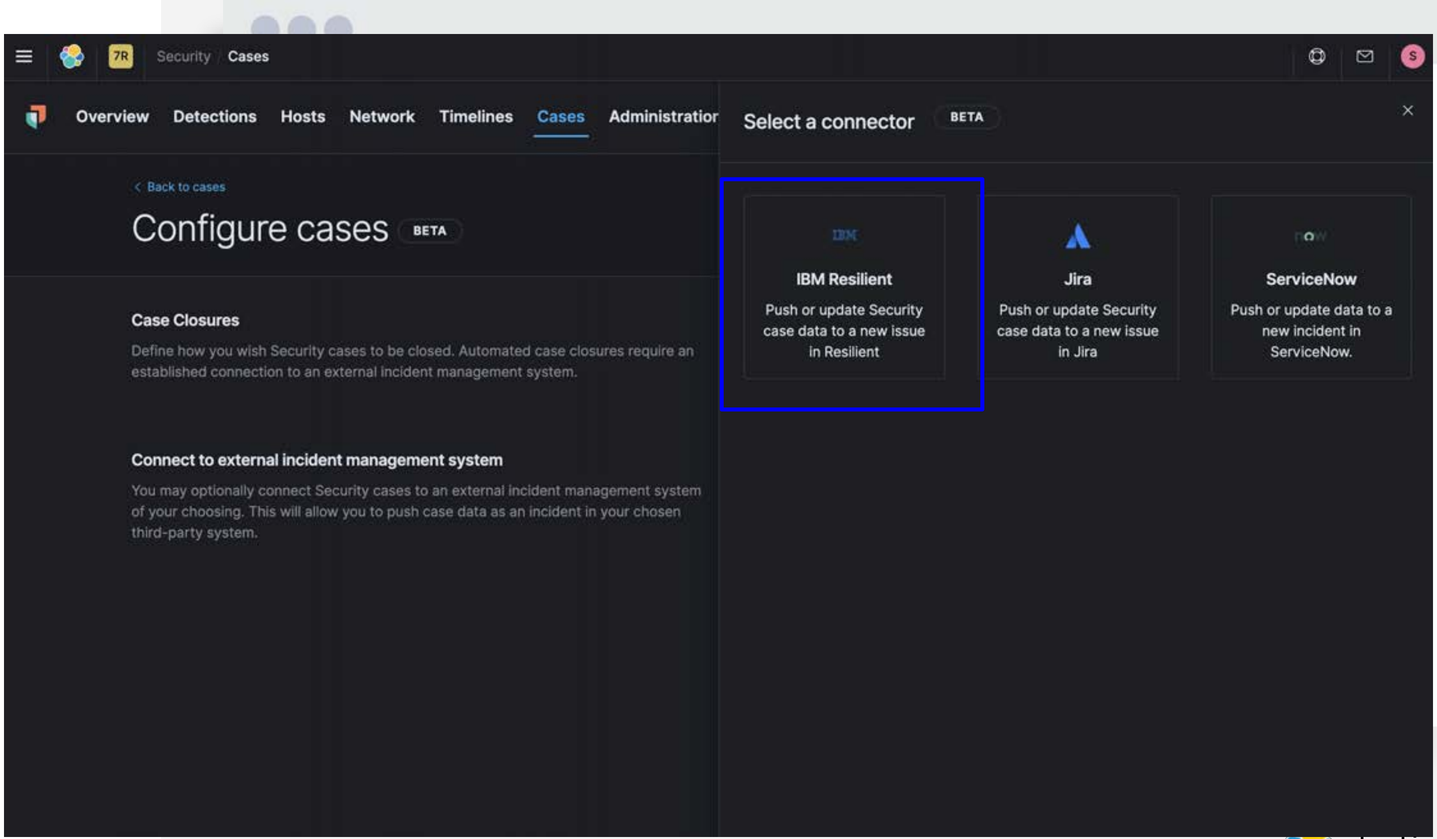
Rows per page: 5

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



‹ 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.

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.

Select a connector BETA

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

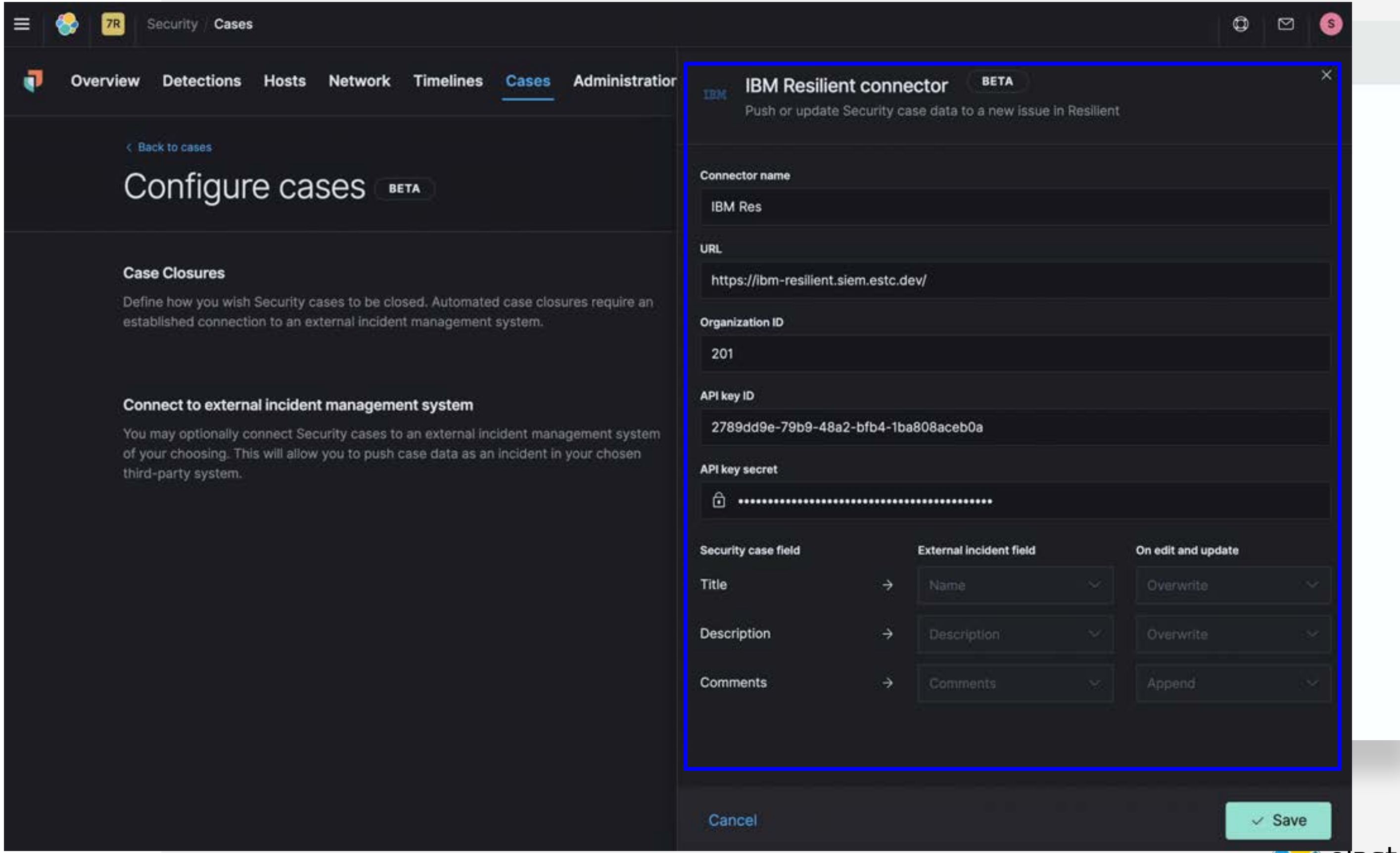
ServiceNow
Push or update data to a new incident in ServiceNow.

Case Management Workflows

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**



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.

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 connector BETA

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

Connector name: IBM Res

URL: https://ibm-resilient.siem.estc.dev/

Organization ID: 201

API key ID: 2789dd9e-79b9-48a2-bfb4-1ba808aceb0a

API key secret: ••

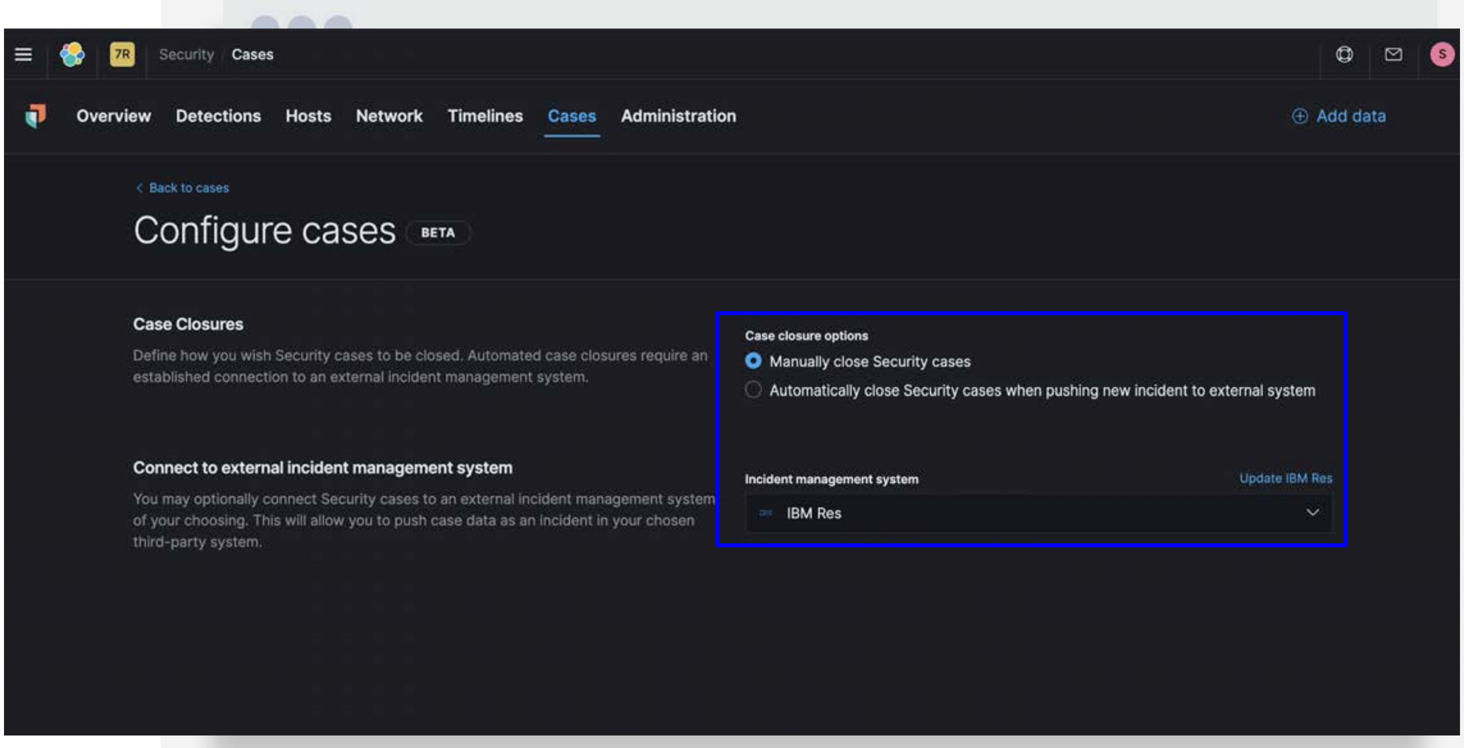
Security case field		External incident field	On edit and update
Title	→	Name	Overwrite
Description	→	Description	Overwrite
Comments	→	Comments	Append

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**



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.

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.

Case closure options

● Manually close Security cases

○ Automatically close Security cases when pushing new incident to external system

Incident management system

Update IBM Res

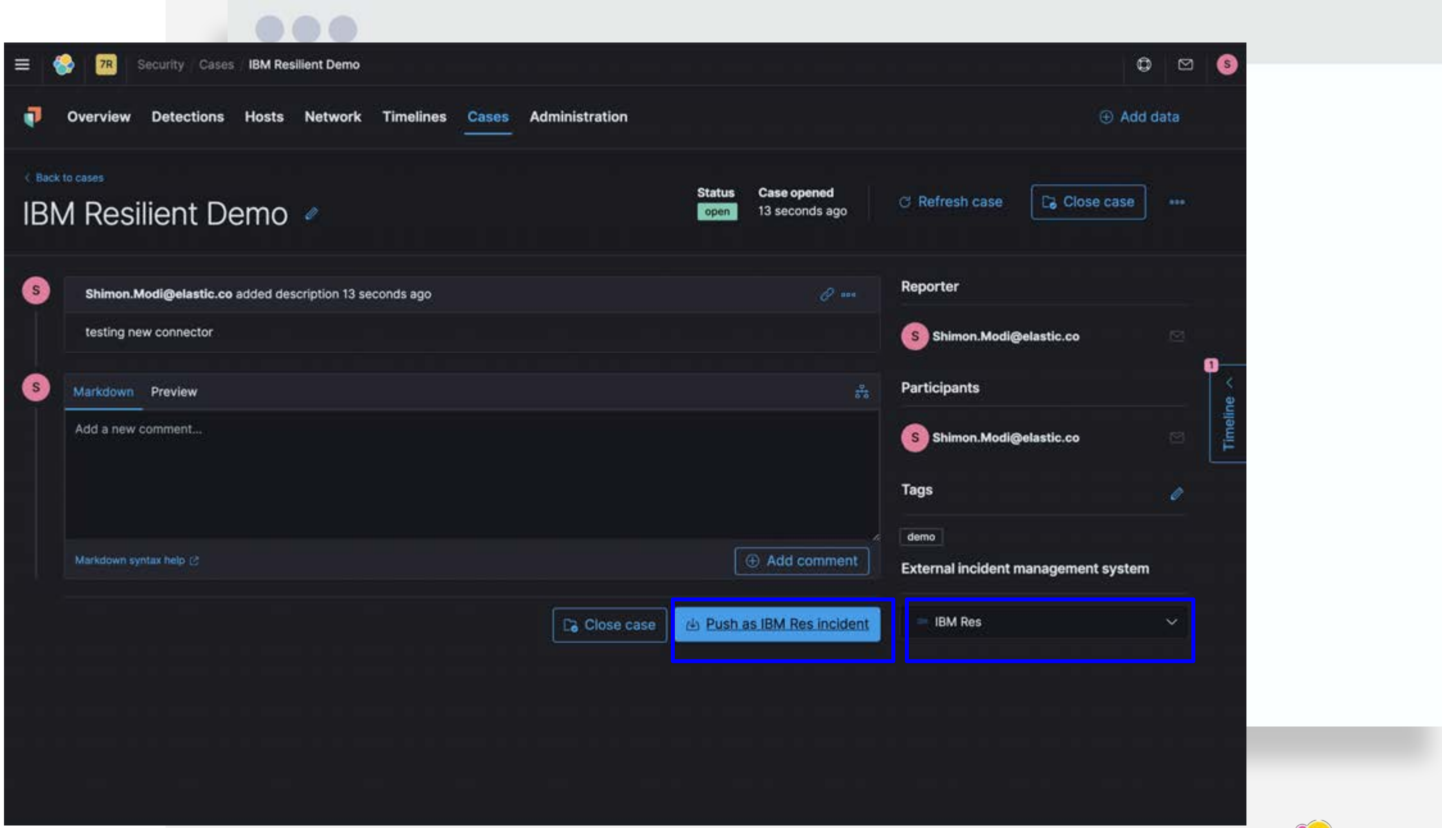
IBM Res

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)**



IBM Resilient Demo

Status: open

Case opened: 13 seconds ago

Shimon.Modi@elastic.co added description 13 seconds ago

testing new connector

Reporter: Shimon.Modi@elastic.co

Participants: Shimon.Modi@elastic.co

Tags: demo

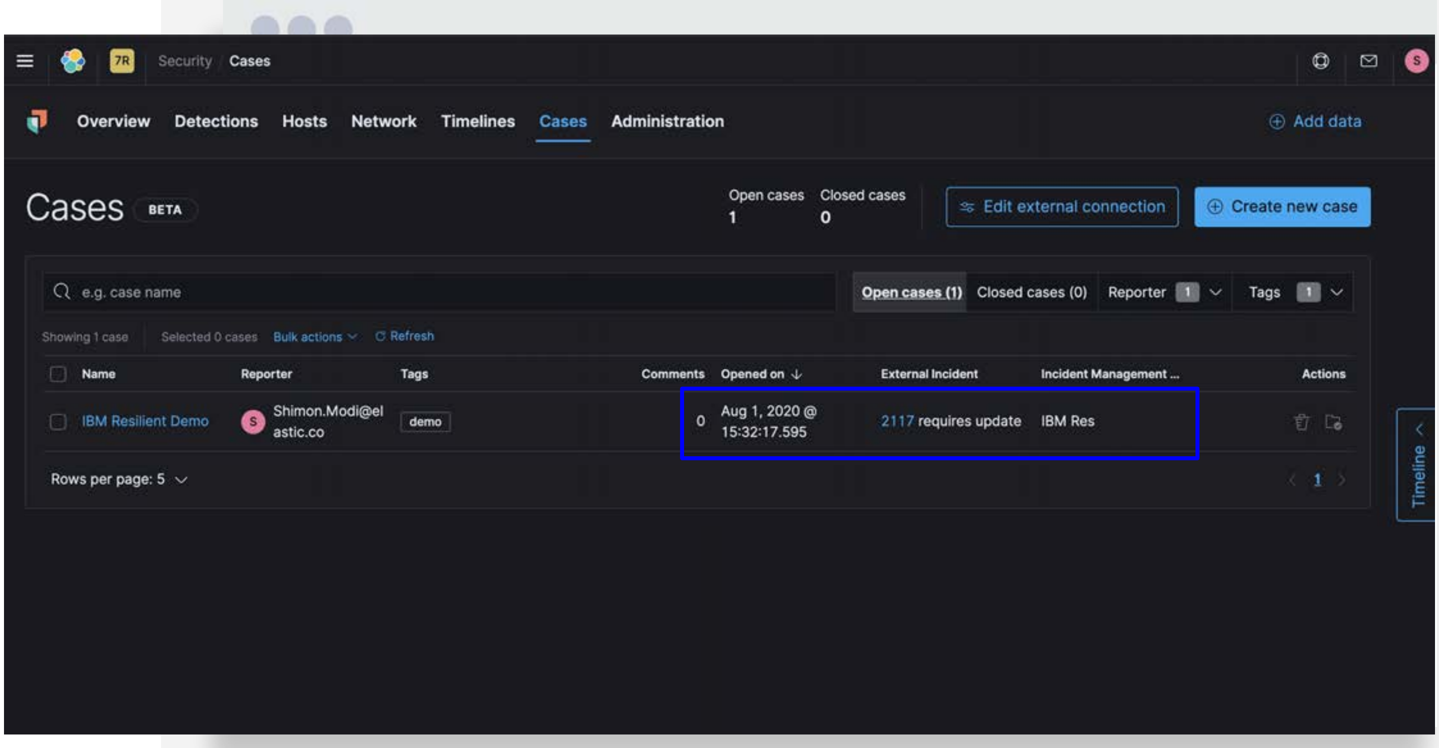
External incident management system: IBM Res

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**



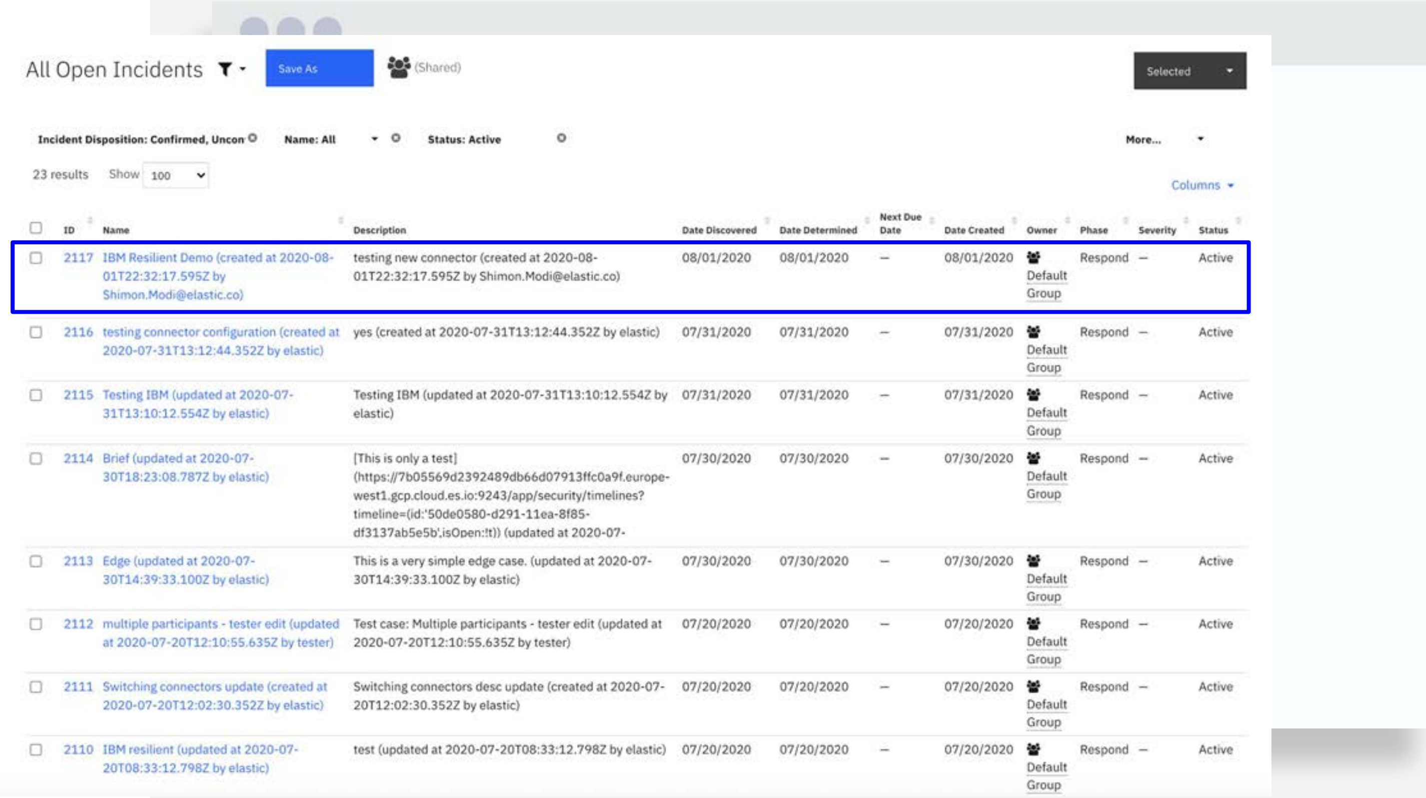
Open cases	Closed cases
1	0

Name	Reporter	Tags	Comments	Opened on	External Incident	Incident Management ...	Actions
IBM Resilient Demo	Shimon.Modi@elastic.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

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

23 results   Show 100

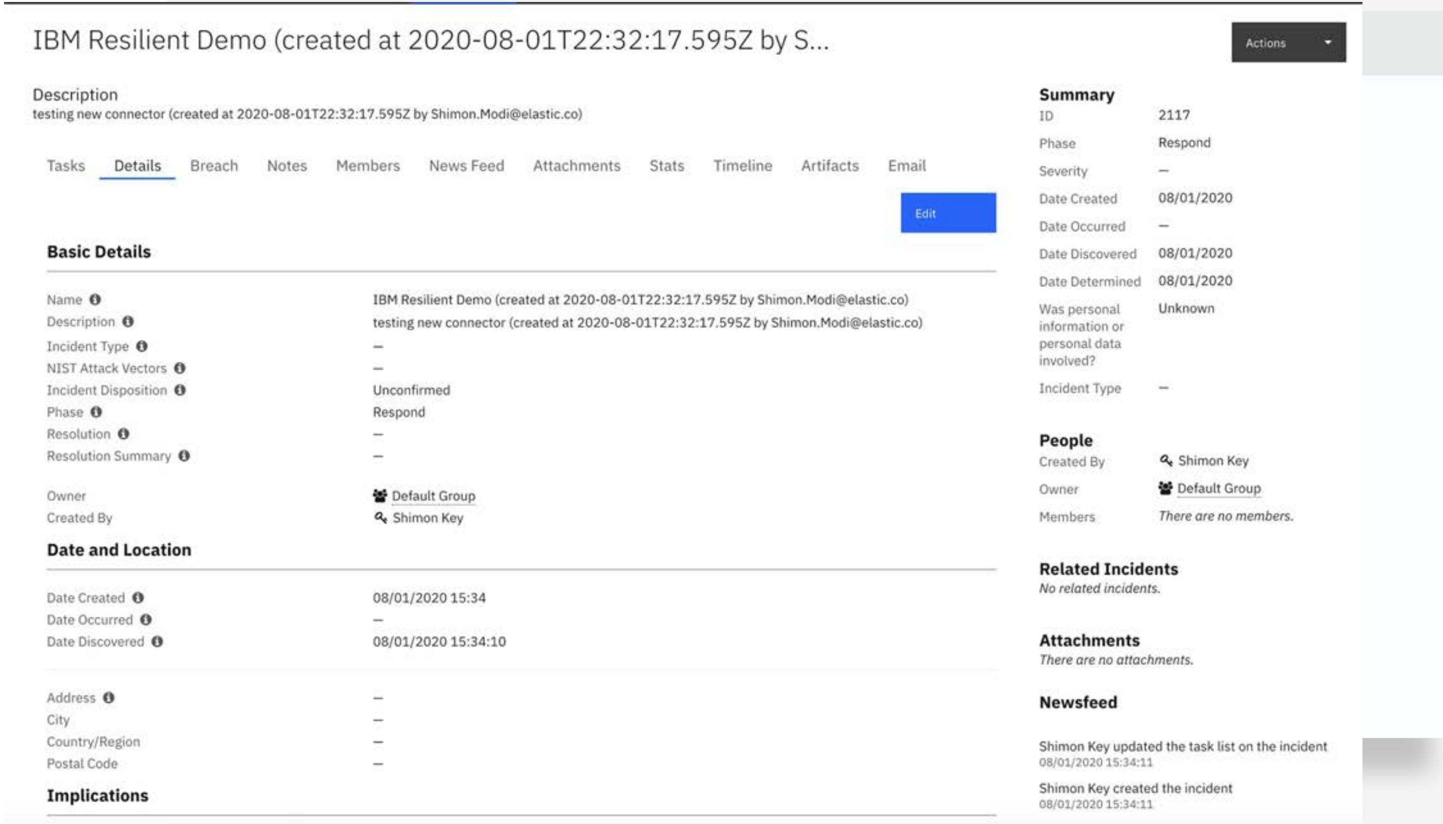
□	ID	Name	Description	Date Discovered	Date Determined	Next Due Date	Date Created	Owner	Phase	Severity	Status
□	2117	IBM Resilient Demo (created at 2020-08-01T22:32:17.595Z by Shimon.Modi@elastic.co)	testing new connector (created at 2020-08-01T22:32:17.595Z by Shimon.Modi@elastic.co)	08/01/2020	08/01/2020	—	08/01/2020	Default Group	Respond	—	Active
□	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
□	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
□	2114	Brief (updated at 2020-07-30T18:23:08.787Z by elastic)	[This is only a test] (https://7b05569d2392489db66d07913ffc0a9f.europe-west1.gcp.cloud.es.io:9243/app/security/timelines?timeline=(id:'50de0580-d291-11ea-8f85-df3137ab5e5b',isOpen:!t)) (updated at 2020-07-	07/30/2020	07/30/2020	—	07/30/2020	Default Group	Respond	—	Active
□	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
□	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
□	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
□	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...

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

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

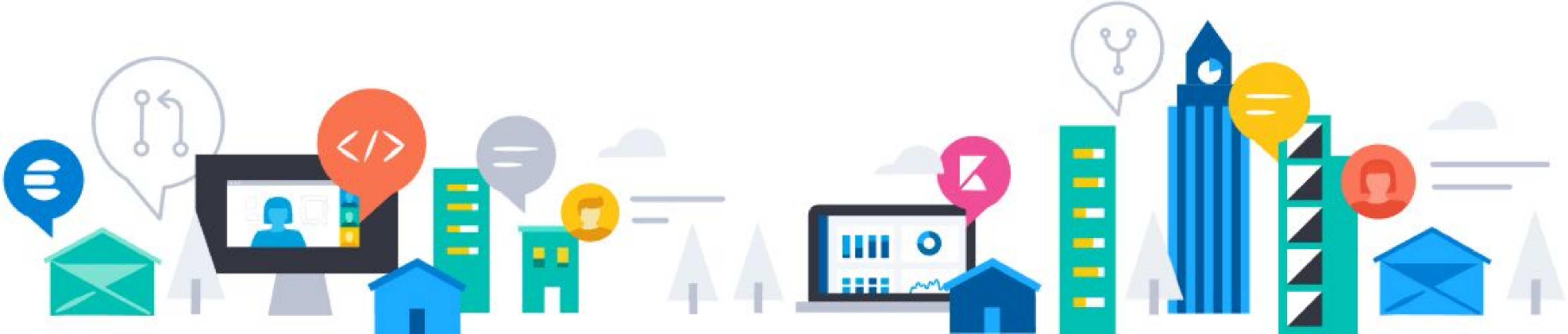
- Filebeat modules for *GSuite, Microsoft Defender ATP* and *SophosXG* firewalls (Beta)
- 20 experimental modules and packages for a broad range of security data sources, including *Barracuda, Cylance, F5, Imperva, Juniper, Tenable, Sonicwall* and *ZScaler* **(**Experimental)
- All Beats modules updated 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

elastic

Thank You

Questions?

Safe Harbor Statement

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.