elastic

Intro to the Public Repository for Detection Rules

Elastic Security

July 15th, 2020

Paul Ewing
Sr. Product Manager,
Elastic Security

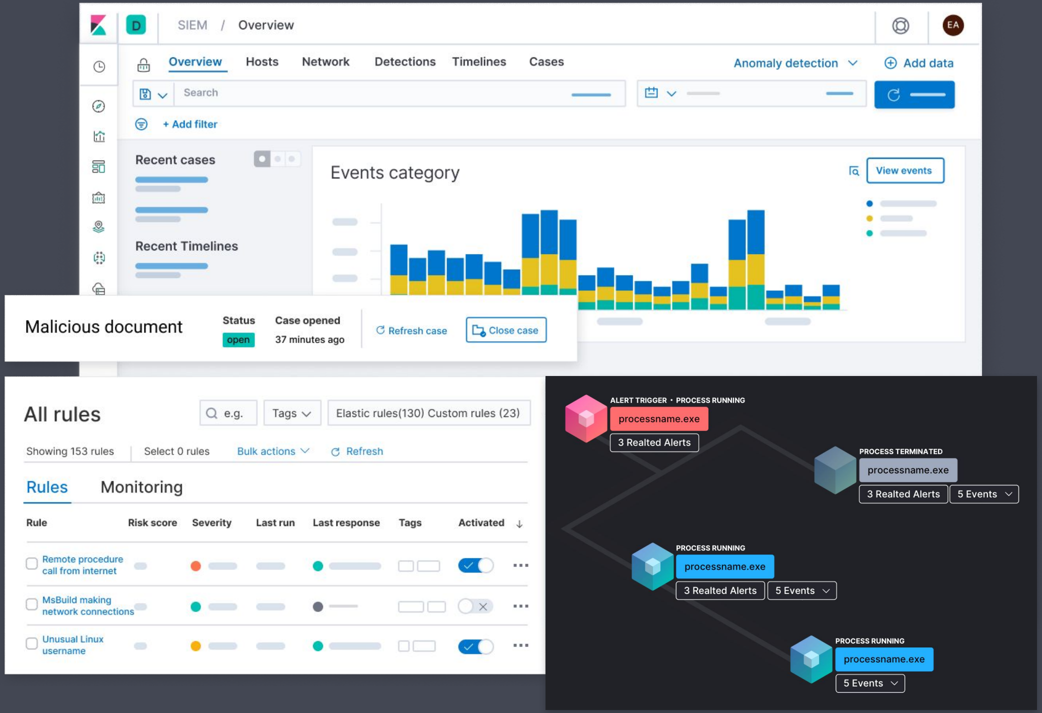
Ross Wolf
Sr. Security Research Engineer,
Elastic Security

elastic

Elastic Security

Unified protection for everyone

Elastic Security arms analysts to prevent, detect, and respond to threats — and it’s free and open, available to analysts everywhere



Rule	Risk score	Severity	Last run	Last response	Tags	Activated
□ Remote procedure call from internet		●		●		✓
□ MsBuild making network connections		●		●		✕
□ Unusual Linux username		●		●		✓

elastic

Prevent

Detect

Respond

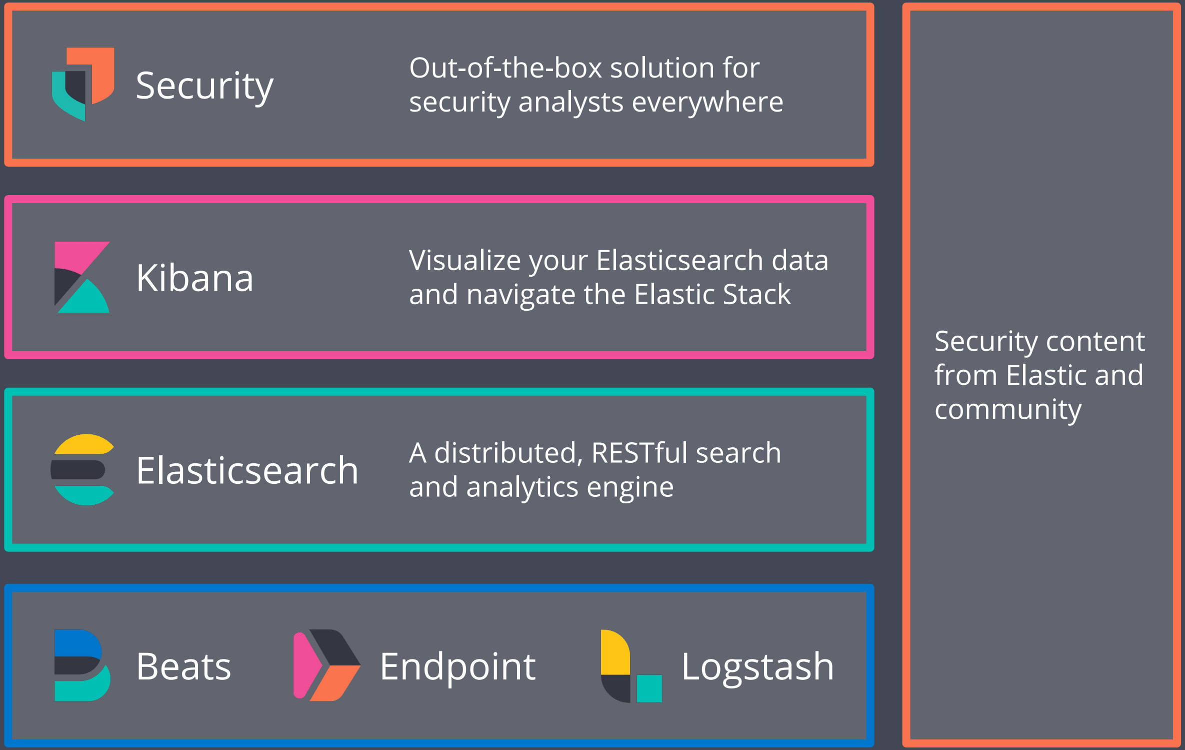
Elastic Security

Unlimited insights across all your data for all time

elastic

Elastic Security

Prevention, Detection, and Response for unified Protection



Security

Out-of-the-box solution for security analysts everywhere

Kibana

Visualize your Elasticsearch data and navigate the Elastic Stack

Elasticsearch

A distributed, RESTful search and analytics engine

Beats

Endpoint

Logstash

Security content from Elastic and community

Agenda

1 Elastic Security Timeline

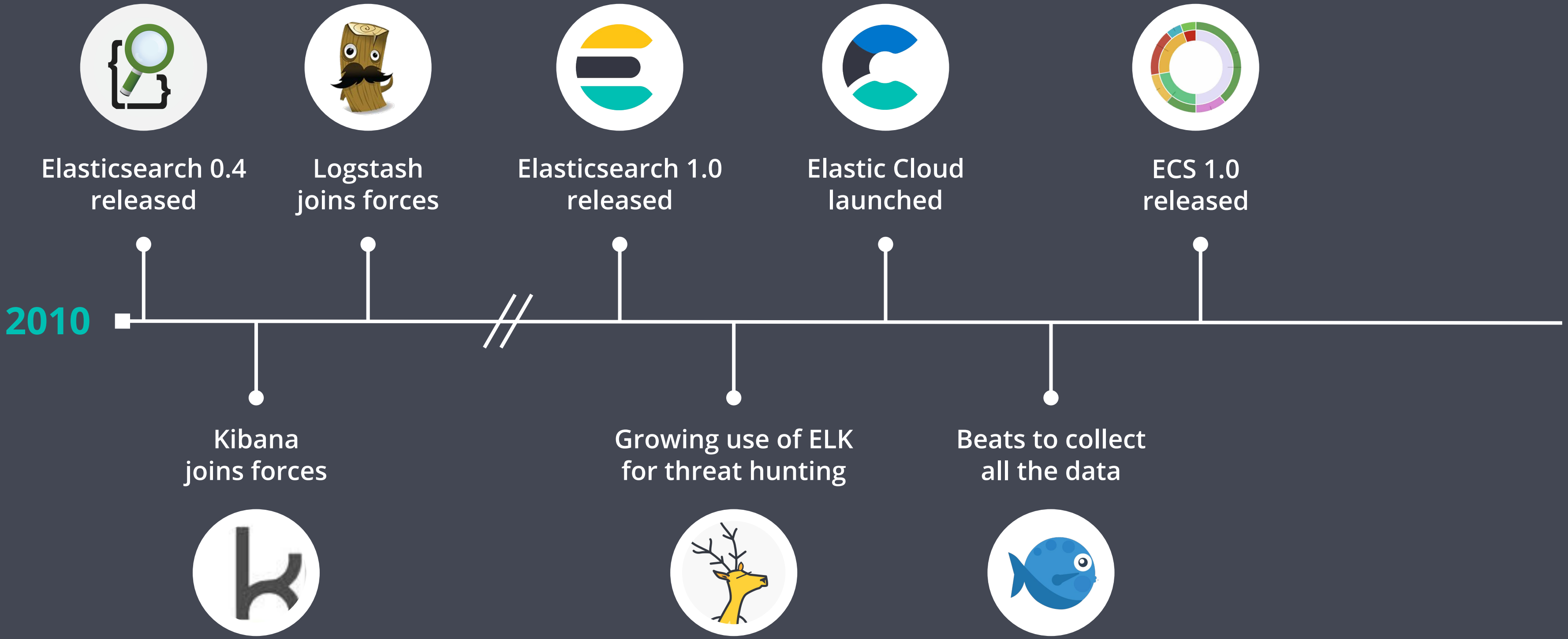
2 Introduction to the Rules Repo

3 Detection Engineering

4 Contributing

5 Demo

Elastic Security



2010

Elasticsearch 0.4 released

Kibana joins forces

Logstash joins forces

Elasticsearch 1.0 released

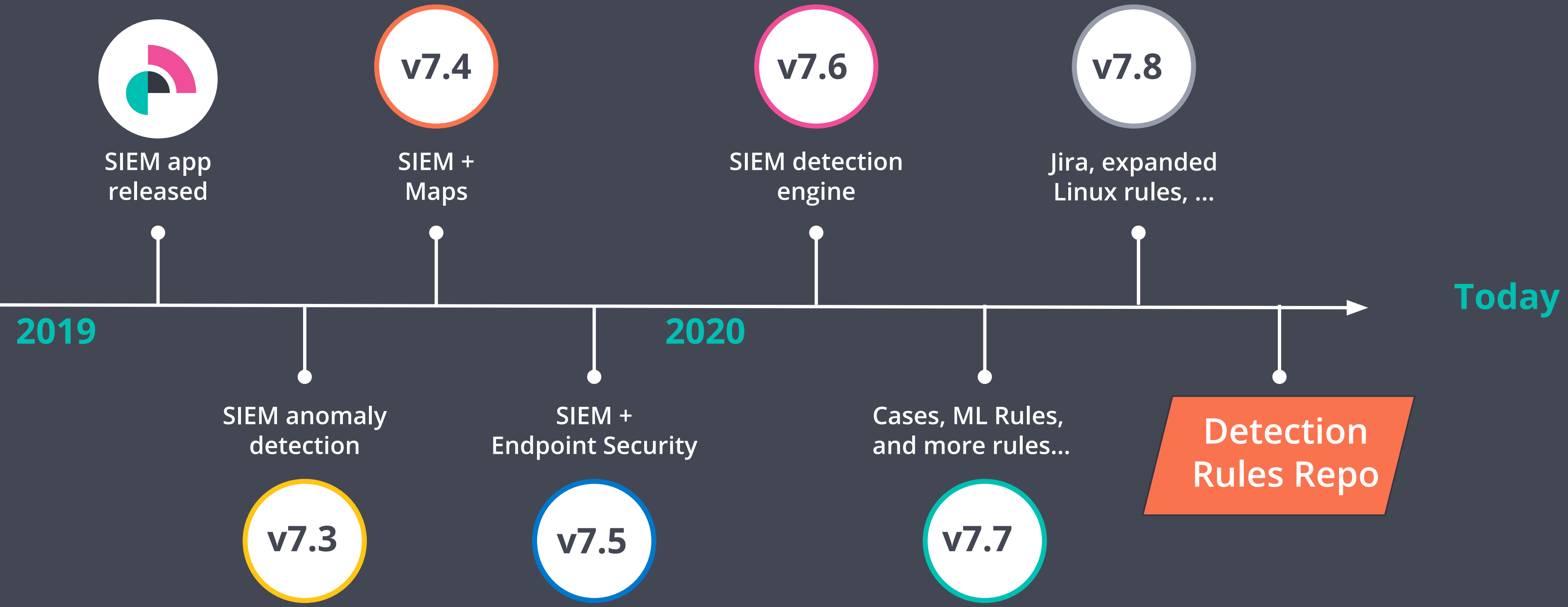
Growing use of ELK for threat hunting

Elastic Cloud launched

Beats to collect all the data

ECS 1.0 released

Elastic Security



2019

SIEM app released

v7.3

SIEM anomaly detection

v7.4

SIEM + Maps

v7.5

SIEM + Endpoint Security

2020

v7.6

SIEM detection engine

v7.7

Cases, ML Rules, and more rules…

v7.8

Jira, expanded Linux rules, …

Detection Rules Repo

Today

Elastic Security

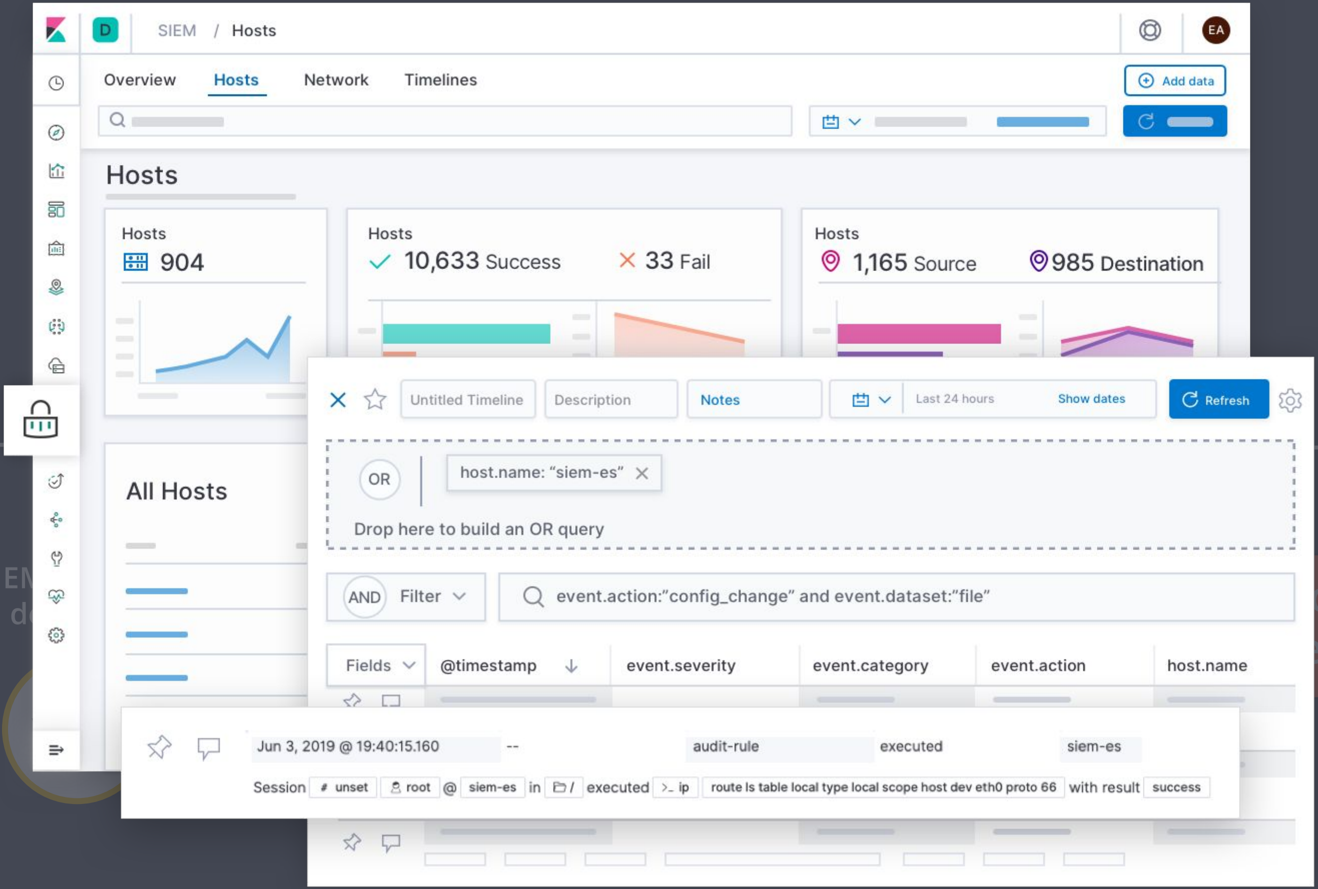
SIEM app released

2019

SIEN
d

on
epo

Today



SIEM / Hosts

Overview | Hosts | Network | Timelines

Add data

Hosts

Hosts 904

Hosts ✓ 10,633 Success ✕ 33 Fail

Hosts 1,165 Source 985 Destination

All Hosts

Untitled Timeline | Description | Notes | Last 24 hours | Show dates | Refresh

OR host.name: "siem-es"

Drop here to build an OR query

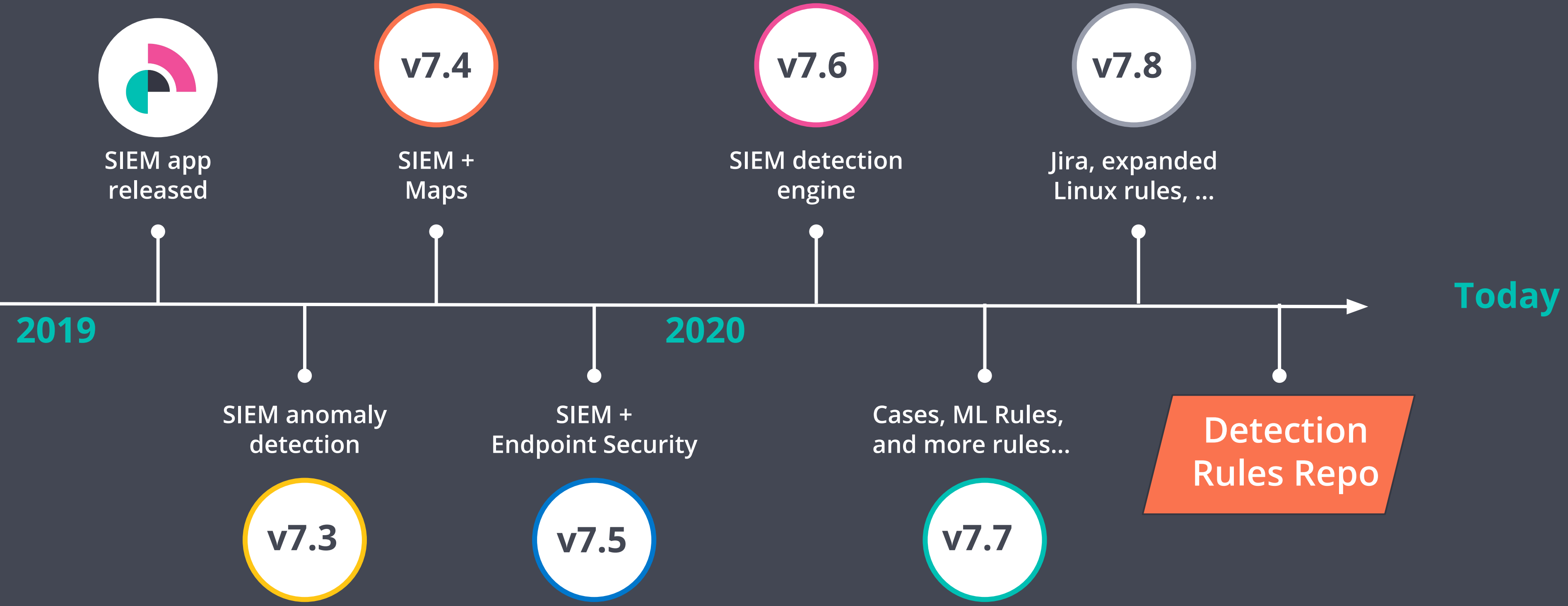
AND Filter event.action:"config_change" and event.dataset:"file"

Fields	@timestamp	event.severity	event.category	event.action	host.name
	Jun 3, 2019 @ 19:40:15.160	--	audit-rule	executed	siem-es

Session # unset root @ siem-es in / executed >_ ip route ls table local type local scope host dev eth0 proto 66 with result success

elastic

Elastic Security



2019

SIEM app released

v7.3

SIEM anomaly detection

v7.4

SIEM + Maps

v7.5

SIEM + Endpoint Security

2020

v7.6

SIEM detection engine

v7.7

Cases, ML Rules, and more rules...

v7.8

Jira, expanded Linux rules, ...

Detection Rules Repo

Today

Elastic Security

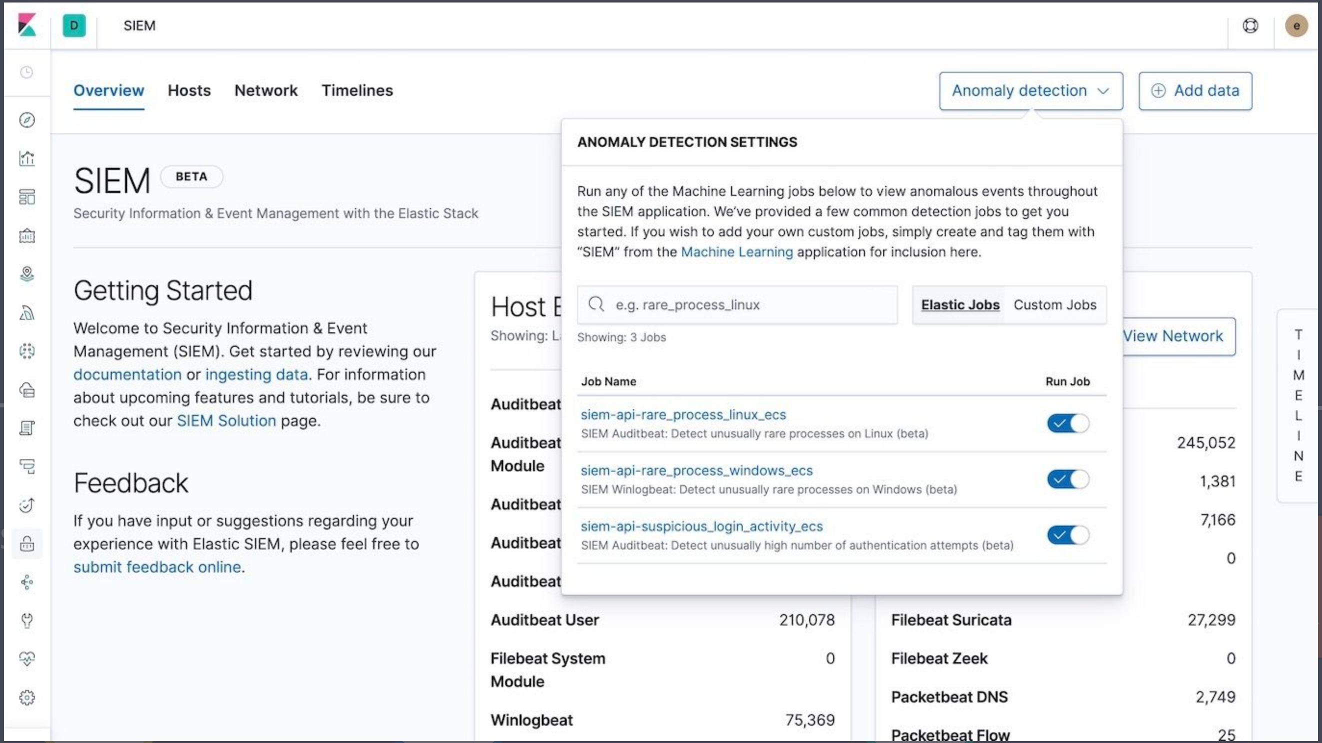
SIEM app released

2019

Today

ion

epo



SIEM BETA

Security Information & Event Management with the Elastic Stack

Getting Started

Welcome to Security Information & Event Management (SIEM). Get started by reviewing our documentation or ingesting data. For information about upcoming features and tutorials, be sure to check out our SIEM Solution page.

Feedback

If you have input or suggestions regarding your experience with Elastic SIEM, please feel free to submit feedback online.

Host E

Showing: L

Auditbeat	
Auditbeat Module	
Auditbeat	
Auditbeat	
Auditbeat	
Auditbeat User	210,078
Filebeat System Module	0
Winlogbeat	75,369

	245,052
	1,381
	7,166
	0
Filebeat Suricata	27,299
Filebeat Zeek	0
Packetbeat DNS	2,749
Packetbeat Flow	25

ANOMALY DETECTION SETTINGS

Run any of the Machine Learning jobs below to view anomalous events throughout the SIEM application. We've provided a few common detection jobs to get you started. If you wish to add your own custom jobs, simply create and tag them with "SIEM" from the Machine Learning application for inclusion here.

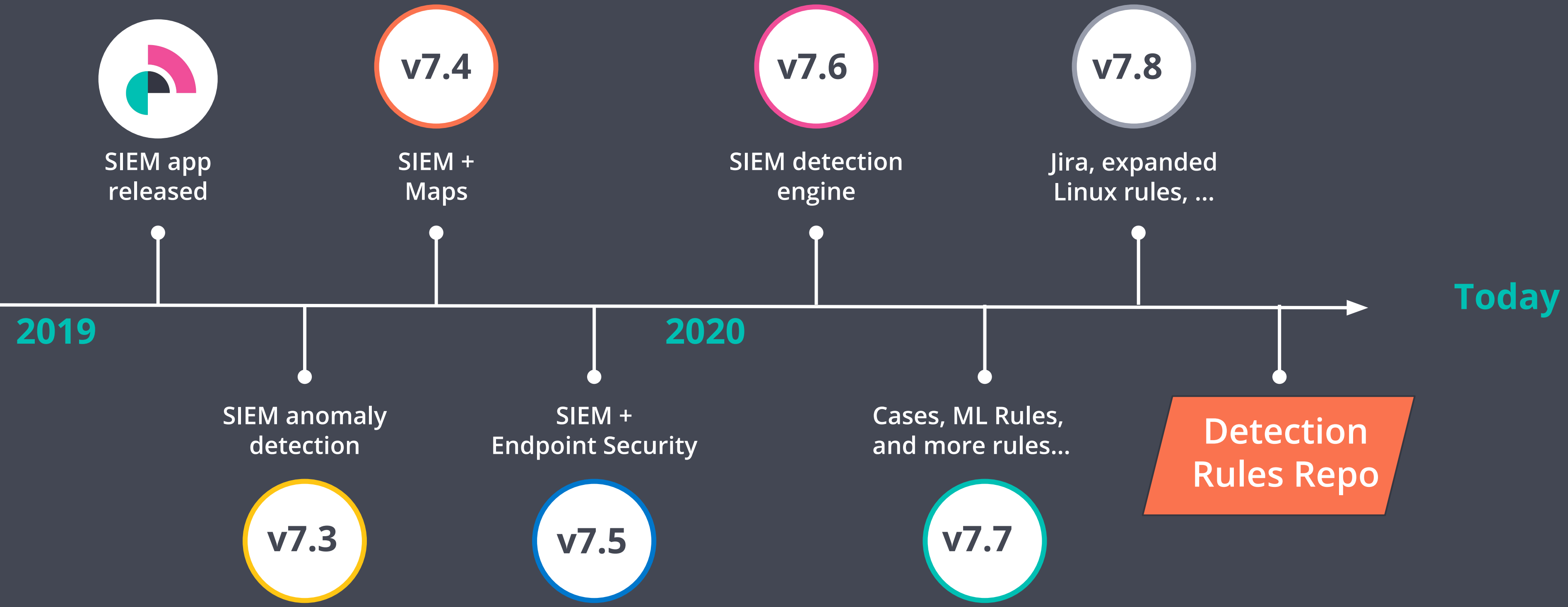
e.g. rare_process_linux

Elastic Jobs | Custom Jobs

Showing: 3 Jobs

Job Name	Run Job
siem-api-rare_process_linux_ecs SIEM Auditbeat: Detect unusually rare processes on Linux (beta)	✓
siem-api-rare_process_windows_ecs SIEM Winlogbeat: Detect unusually rare processes on Windows (beta)	✓
siem-api-suspicious_login_activity_ecs SIEM Auditbeat: Detect unusually high number of authentication attempts (beta)	✓

Elastic Security



2019

SIEM app released

v7.3

SIEM anomaly detection

v7.4

SIEM + Maps

v7.5

SIEM + Endpoint Security

2020

v7.6

SIEM detection engine

v7.7

Cases, ML Rules, and more rules...

v7.8

Jira, expanded Linux rules, ...

Detection Rules Repo

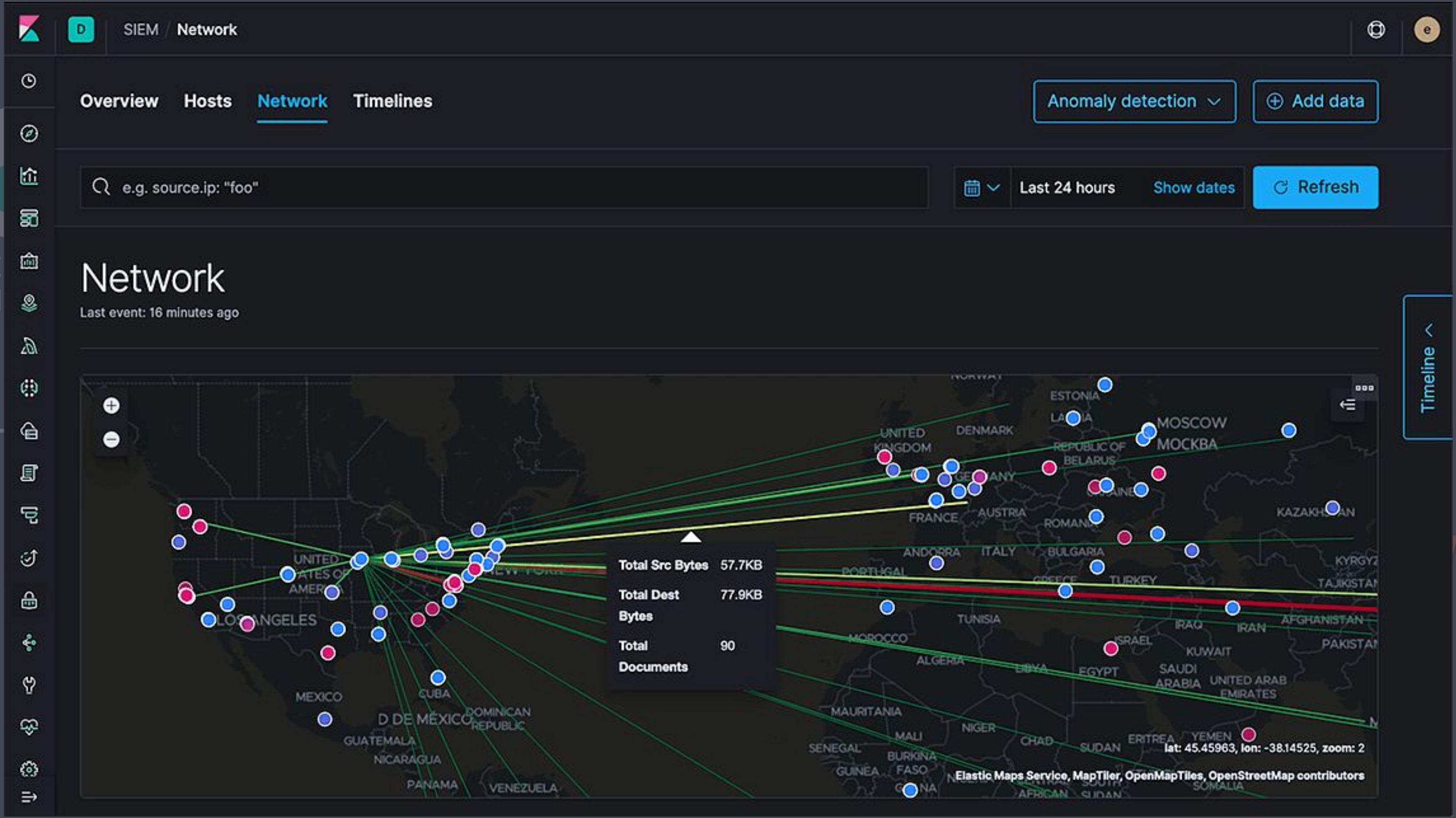
Today

Elastic Security

SIE
rel

2019

Today



SIEM / Network

Overview Hosts Network Timelines

Anomaly detection ⌄ ⊕ Add data

e.g. source.ip: "foo"

Last 24 hours Show dates Refresh

Network

Last event: 16 minutes ago

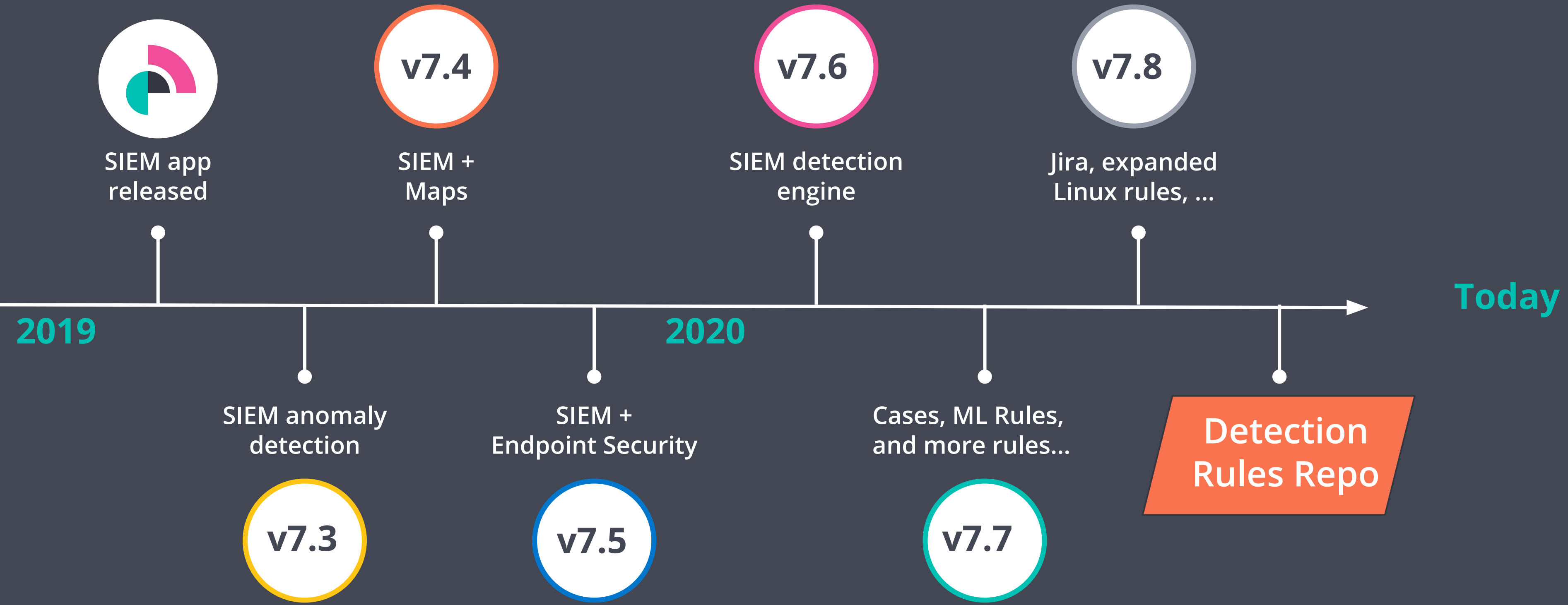
Total Src Bytes	57.7KB
Total Dest Bytes	77.9KB
Total Documents	90

lat: 45.45963, lon: -38.14525, zoom: 2

Elastic Maps Service, MapTiler, OpenMapTiles, OpenStreetMap contributors

elastic

Elastic Security



2019

SIEM app released

v7.3

SIEM anomaly detection

v7.4

SIEM + Maps

v7.5

SIEM + Endpoint Security

2020

v7.6

SIEM detection engine

v7.7

Cases, ML Rules, and more rules...

v7.8

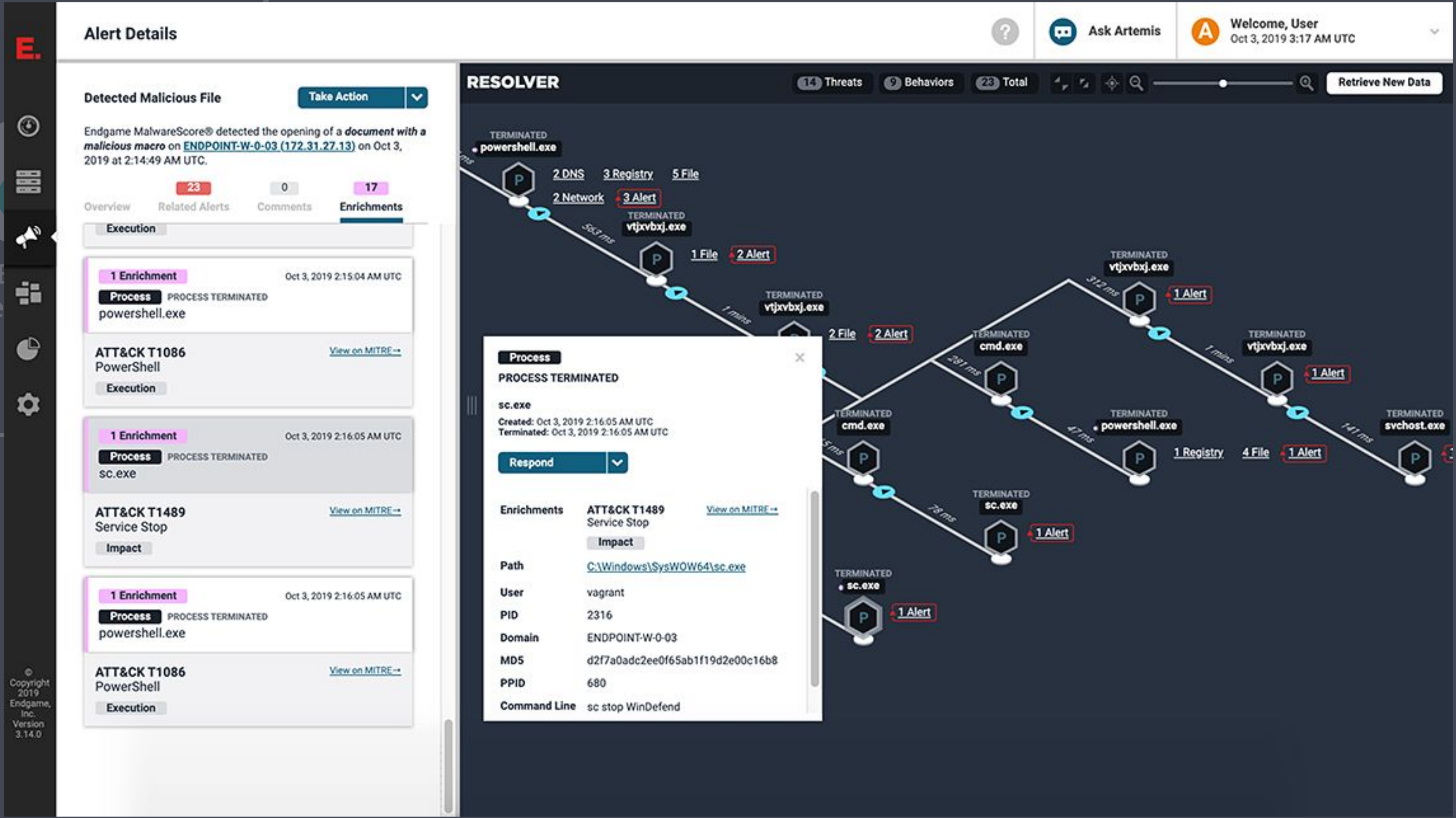
Jira, expanded Linux rules, ...

Detection Rules Repo

Today

Elastic Security

2019



Alert Details

Ask Artemis

Welcome, User
Oct 3, 2019 3:17 AM UTC

Detected Malicious File — Take Action

Endgame MalwareScore® detected the opening of a *document with a malicious macro* on ENDPOINT-W-0-03 (172.31.27.13) on Oct 3, 2019 at 2:14:49 AM UTC.

Overview | 23 Related Alerts | 0 Comments | 17 Enrichments

Execution

1 Enrichment — Oct 3, 2019 2:15:04 AM UTC
Process — PROCESS TERMINATED
powershell.exe

ATT&CK T1086
PowerShell
Execution
View on MITRE→

1 Enrichment — Oct 3, 2019 2:16:05 AM UTC
Process — PROCESS TERMINATED
sc.exe

ATT&CK T1489
Service Stop
Impact
View on MITRE→

1 Enrichment — Oct 3, 2019 2:16:05 AM UTC
Process — PROCESS TERMINATED
powershell.exe

ATT&CK T1086
PowerShell
Execution
View on MITRE→

© Copyright 2019 Endgame, Inc. Version 3.14.0

RESOLVER

Process
PROCESS TERMINATED

sc.exe
Created: Oct 3, 2019 2:16:05 AM UTC
Terminated: Oct 3, 2019 2:16:05 AM UTC

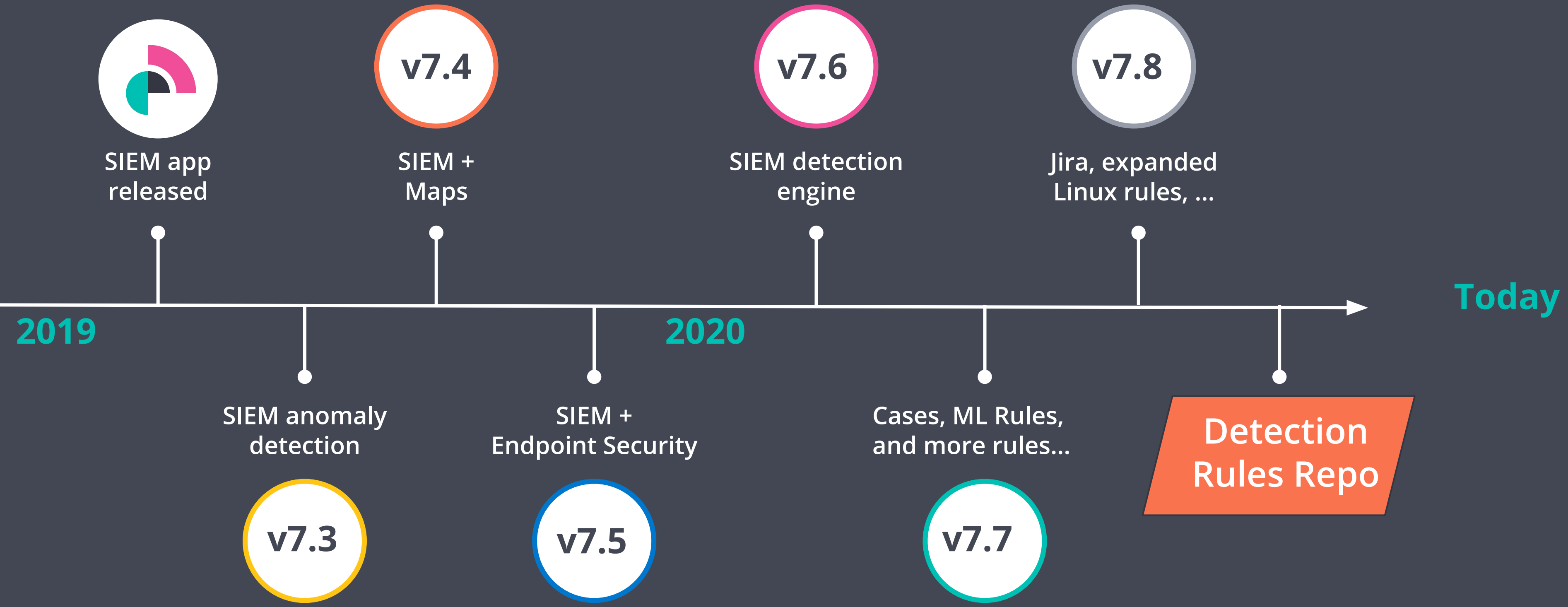
Respond

Enrichments	ATT&CK T1489 Service Stop Impact View on MITRE→
Path	C:\Windows\SysWOW64\sc.exe
User	vagrant
PID	2316
Domain	ENDPOINT-W-0-03
MD5	d2f7a0adc2ee0f65ab1f19d2e00c16b8
PPID	680
Command Line	sc stop WinDefend

Today

elastic

Elastic Security



2019

SIEM app released

v7.3

SIEM anomaly detection

v7.4

SIEM + Maps

v7.5

SIEM + Endpoint Security

2020

v7.6

SIEM detection engine

v7.7

Cases, ML Rules, and more rules...

v7.8

Jira, expanded Linux rules, ...

Detection Rules Repo

Today

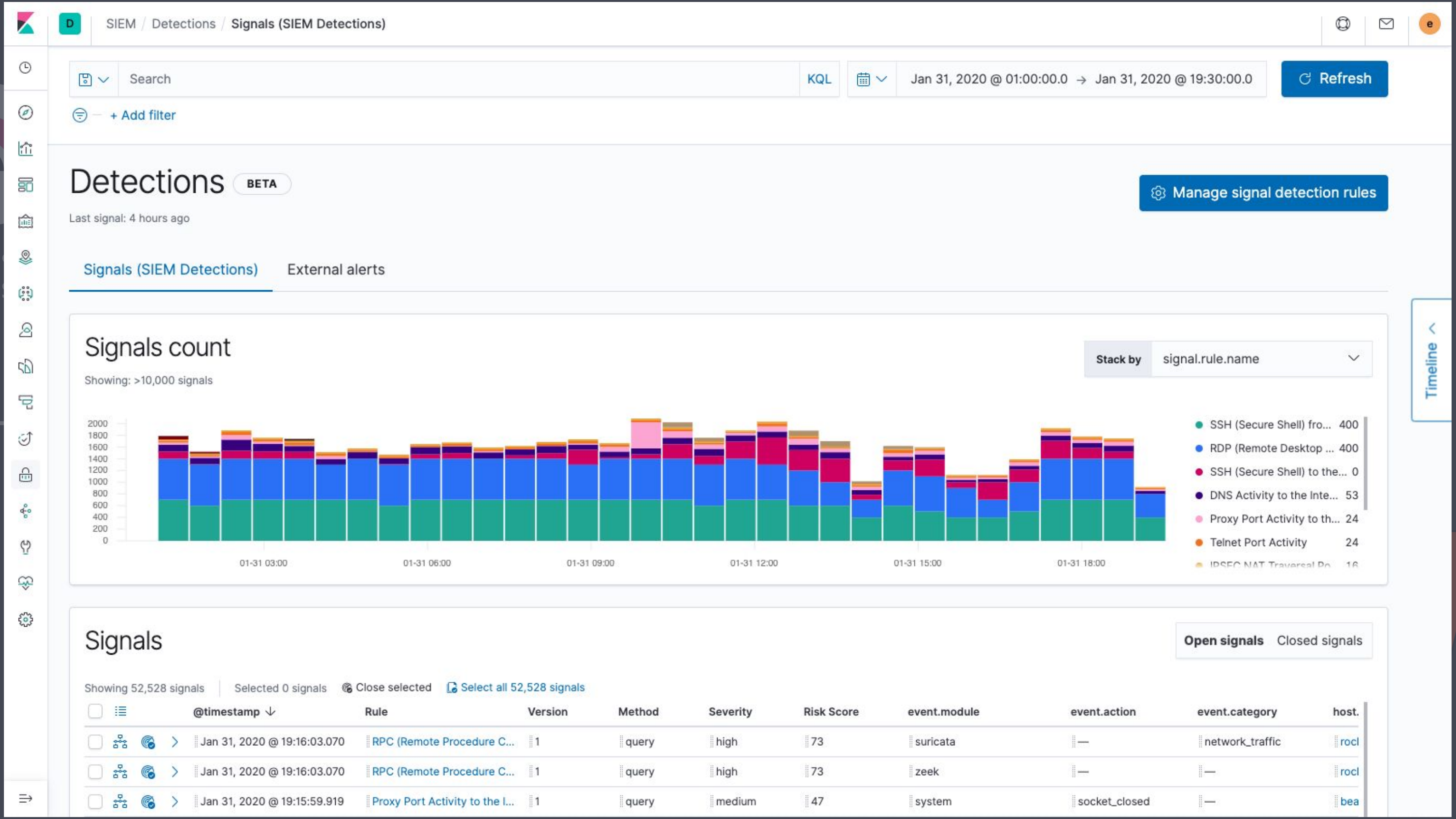
Elastic Security

SIEM

releas

2019

Today



Jan 31, 2020 @ 01:00:00.0 → Jan 31, 2020 @ 19:30:00.0

Detections BETA

Last signal: 4 hours ago

Manage signal detection rules

Signals (SIEM Detections) | External alerts

Signals count

Showing: >10,000 signals

Stack by: signal.rule.name

●	SSH (Secure Shell) fro...	400
●	RDP (Remote Desktop ...	400
●	SSH (Secure Shell) to the...	0
●	DNS Activity to the Inte...	53
●	Proxy Port Activity to th...	24
●	Telnet Port Activity	24
●	IPSEC NAT Traversal Po...	16

Signals

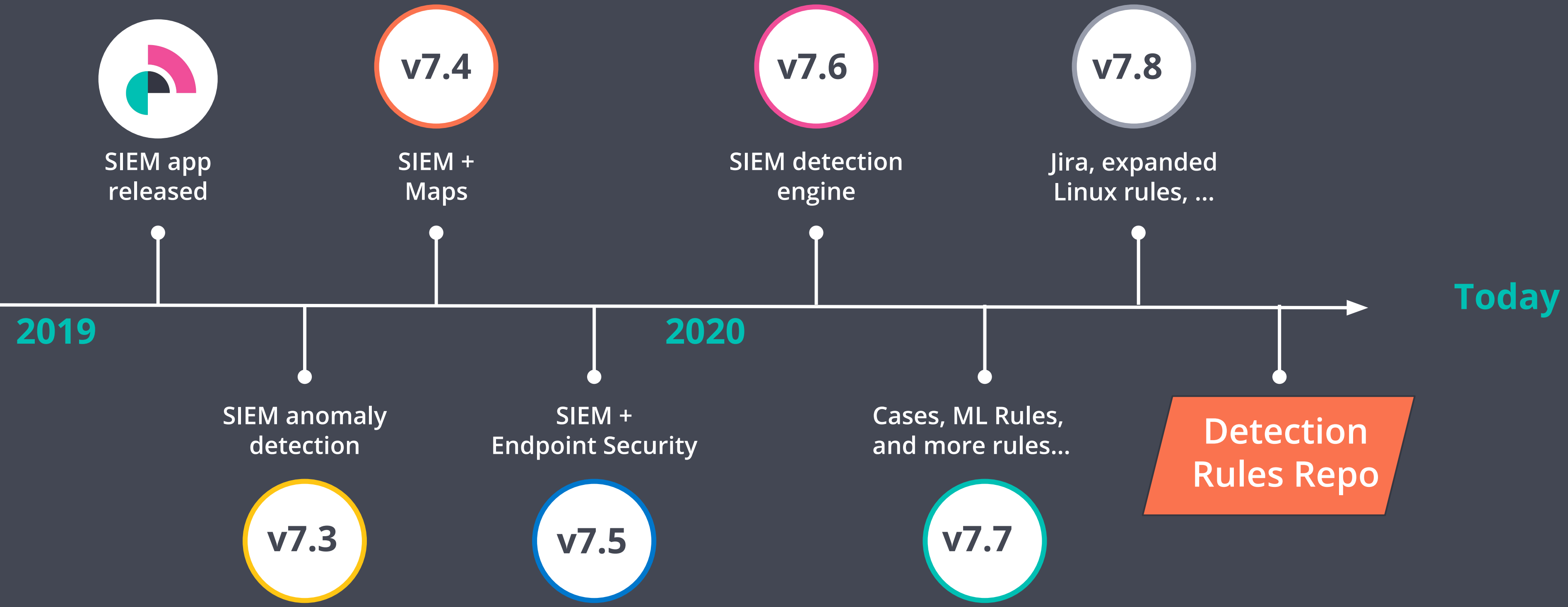
Open signals | Closed signals

Showing 52,528 signals | Selected 0 signals | Close selected | Select all 52,528 signals

@timestamp ↓	Rule	Version	Method	Severity	Risk Score	event.module	event.action	event.category	host.
Jan 31, 2020 @ 19:16:03.070	RPC (Remote Procedure C...	1	query	high	73	suricata	—	network_traffic	rocl
Jan 31, 2020 @ 19:16:03.070	RPC (Remote Procedure C...	1	query	high	73	zeek	—	—	rocl
Jan 31, 2020 @ 19:15:59.919	Proxy Port Activity to the I...	1	query	medium	47	system	socket_closed	—	bea

elastic

Elastic Security



2019

SIEM app released

v7.3

SIEM anomaly detection

v7.4

SIEM + Maps

v7.5

SIEM + Endpoint Security

2020

v7.6

SIEM detection engine

v7.7

Cases, ML Rules, and more rules…

v7.8

Jira, expanded Linux rules, …

Detection Rules Repo

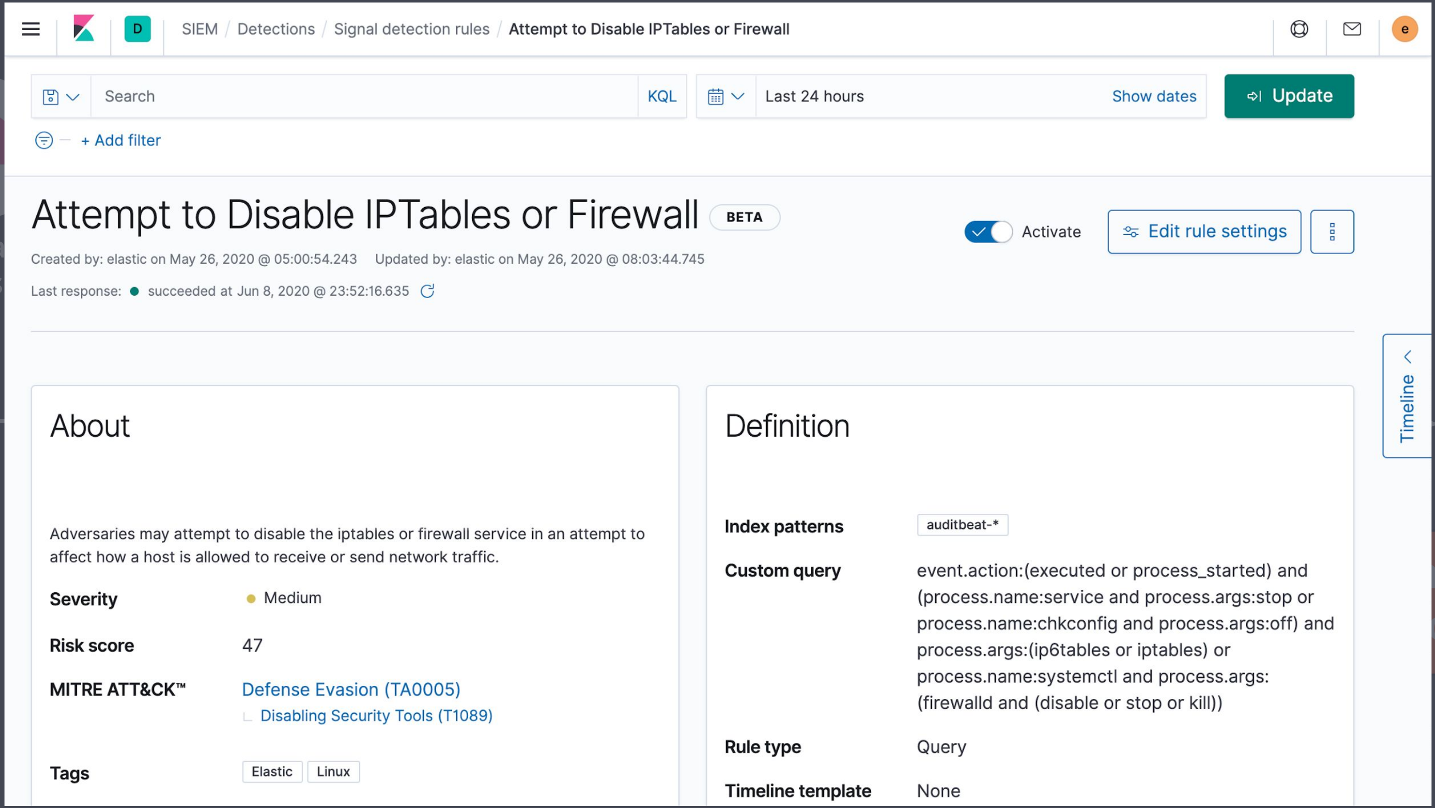
Today

Elastic Security

SIEM a
releas

2019

Today



SIEM / Detections / Signal detection rules / Attempt to Disable IPTables or Firewall

Search KQL

Last 24 hours Show dates Update

+ Add filter

Attempt to Disable IPTables or Firewall BETA

Activate Edit rule settings

Created by: elastic on May 26, 2020 @ 05:00:54.243 Updated by: elastic on May 26, 2020 @ 08:03:44.745

Last response: ● succeeded at Jun 8, 2020 @ 23:52:16.635

About

Adversaries may attempt to disable the iptables or firewall service in an attempt to affect how a host is allowed to receive or send network traffic.

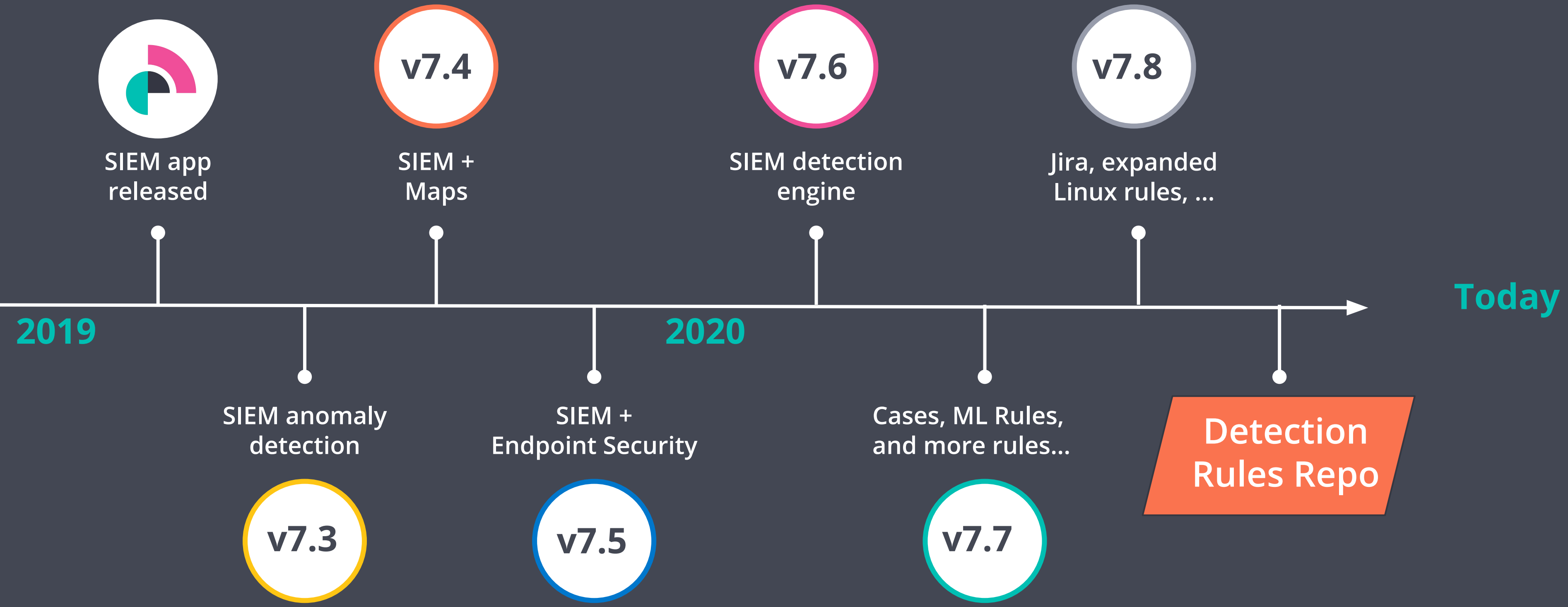
Severity	● Medium
Risk score	47
MITRE ATT&CK™	Defense Evasion (TA0005) Disabling Security Tools (T1089)
Tags	Elastic Linux

Definition

Index patterns	auditbeat-*
Custom query	event.action:(executed or process_started) and (process.name:service and process.args:stop or process.name:chkconfig and process.args:off) and process.args:(ip6tables or iptables) or process.name:systemctl and process.args:(firewalld and (disable or stop or kill))
Rule type	Query
Timeline template	None

elastic

Elastic Security



2019

SIEM app released

v7.3

SIEM anomaly detection

v7.4

SIEM + Maps

v7.5

SIEM + Endpoint Security

2020

v7.6

SIEM detection engine

v7.7

Cases, ML Rules, and more rules…

v7.8

Jira, expanded Linux rules, …

Detection Rules Repo

Today

Agenda

1 Elastic Security Timeline

2 Introduction to the Rules Repo

3 Detection Engineering

4 Contributing

5 Demo

elastic

Agenda

1 Elastic Security Timeline

2 Introduction to the Rules Repo

3 Detection Engineering

4 Contributing

5 Demo

elastic

Repo at a Glance

github.com/elastic/detection-rules

Community & Collaboration

- A dev-first mentality for malicious behavior detection

The Rules

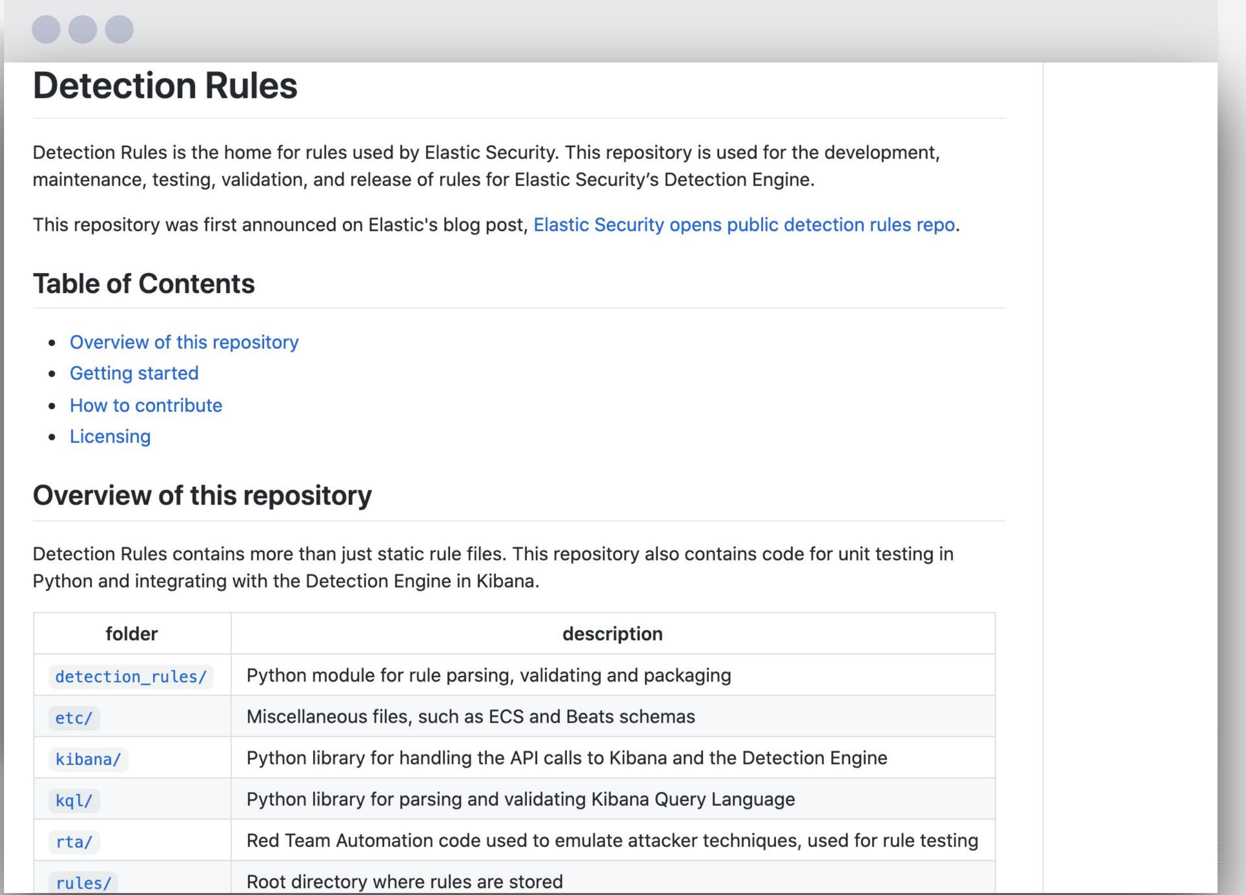
- A place to engage on rules for all users of Elastic Security

Contribution Guides

- Creating issues, submitting PRs, our philosophy, and more!

Developer Tools

- Interactive CLI to create rules
- Syntax validation, ECS schemas, metadata checker, etc.



Detection Rules

Detection Rules is the home for rules used by Elastic Security. This repository is used for the development, maintenance, testing, validation, and release of rules for Elastic Security’s Detection Engine.

This repository was first announced on Elastic's blog post, Elastic Security opens public detection rules repo.

Table of Contents

- Overview of this repository
- Getting started
- How to contribute
- Licensing

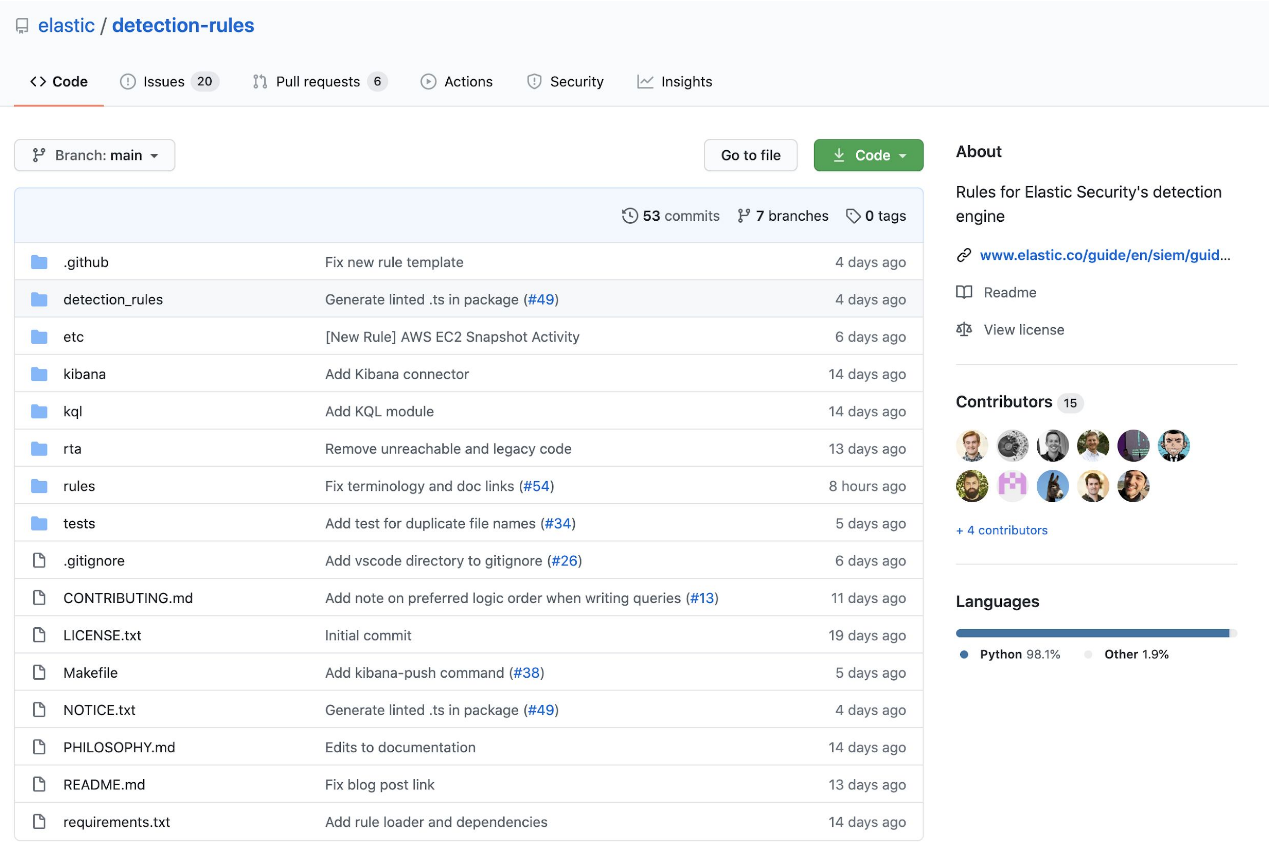
Overview of this repository

Detection Rules contains more than just static rule files. This repository also contains code for unit testing in Python and integrating with the Detection Engine in Kibana.

folder	description
`detection_rules/`	Python module for rule parsing, validating and packaging
`etc/`	Miscellaneous files, such as ECS and Beats schemas
`kibana/`	Python library for handling the API calls to Kibana and the Detection Engine
`kql/`	Python library for parsing and validating Kibana Query Language
`rta/`	Red Team Automation code used to emulate attacker techniques, used for rule testing
`rules/`	Root directory where rules are stored

Repo Walkthrough

detection-rules



elastic / detection-rules

53 commits 7 branches 0 tags

.github	Fix new rule template	4 days ago
detection_rules	Generate linted .ts in package (#49)	4 days ago
etc	[New Rule] AWS EC2 Snapshot Activity	6 days ago
kibana	Add Kibana connector	14 days ago
kql	Add KQL module	14 days ago
rta	Remove unreachable and legacy code	13 days ago
rules	Fix terminology and doc links (#54)	8 hours ago
tests	Add test for duplicate file names (#34)	5 days ago
.gitignore	Add vscode directory to gitignore (#26)	6 days ago
CONTRIBUTING.md	Add note on preferred logic order when writing queries (#13)	11 days ago
LICENSE.txt	Initial commit	19 days ago
Makefile	Add kibana-push command (#38)	5 days ago
NOTICE.txt	Generate linted .ts in package (#49)	4 days ago
PHILOSOPHY.md	Edits to documentation	14 days ago
README.md	Fix blog post link	13 days ago
requirements.txt	Add rule loader and dependencies	14 days ago

About

Rules for Elastic Security's detection engine

www.elastic.co/guide/en/siem/guid...

Readme

View license

Contributors 15

+ 4 contributors

Languages

Python 98.1% Other 1.9%

detection-rules

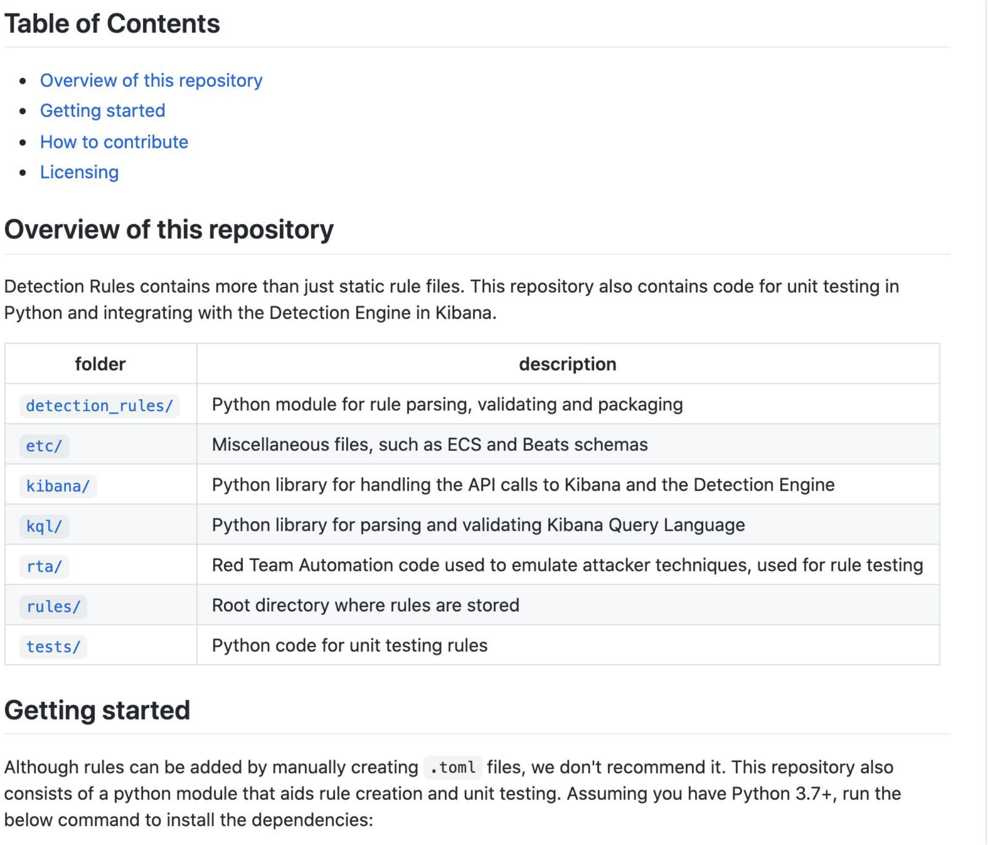


Table of Contents

Overview of this repository

Detection Rules contains more than just static rule files. This repository also contains code for unit testing in Python and integrating with the Detection Engine in Kibana.

folder	description
`detection_rules/`	Python module for rule parsing, validating and packaging
`etc/`	Miscellaneous files, such as ECS and Beats schemas
`kibana/`	Python library for handling the API calls to Kibana and the Detection Engine
`kql/`	Python library for parsing and validating Kibana Query Language
`rta/`	Red Team Automation code used to emulate attacker techniques, used for rule testing
`rules/`	Root directory where rules are stored
`tests/`	Python code for unit testing rules

Getting started

Although rules can be added by manually creating `.toml` files, we don't recommend it. This repository also consists of a python module that aids rule creation and unit testing. Assuming you have Python 3.7+, run the below command to install the dependencies:

detection-rules

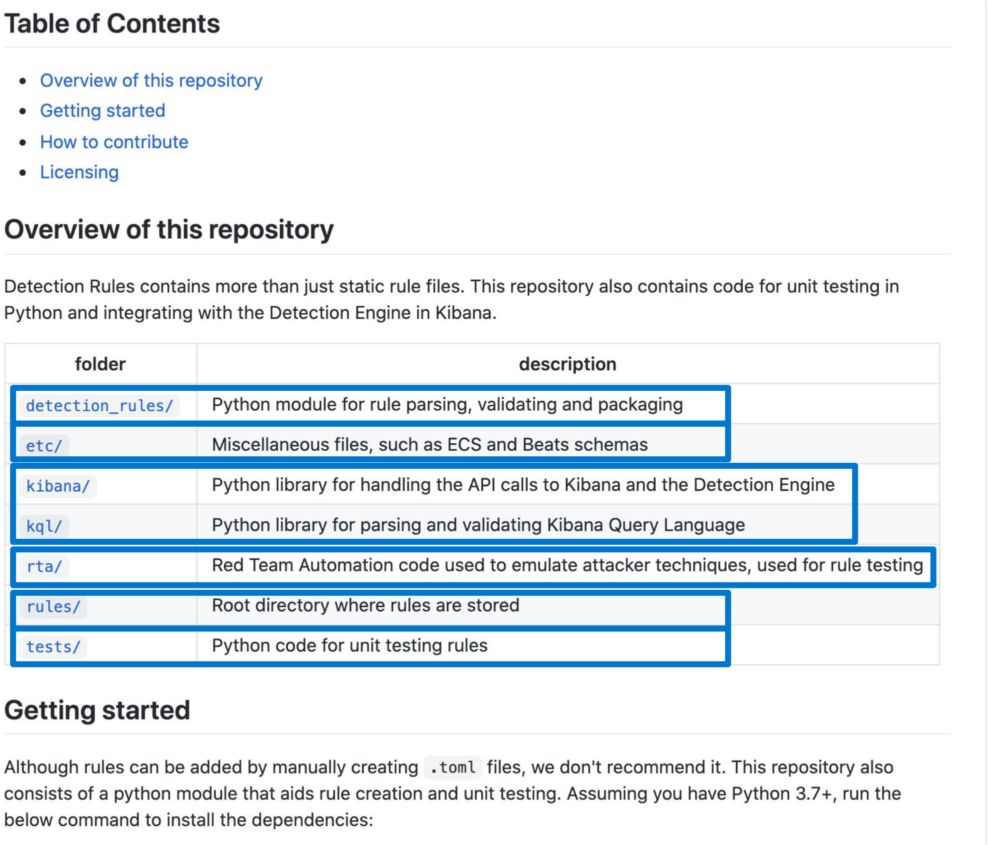


Table of Contents

Overview of this repository

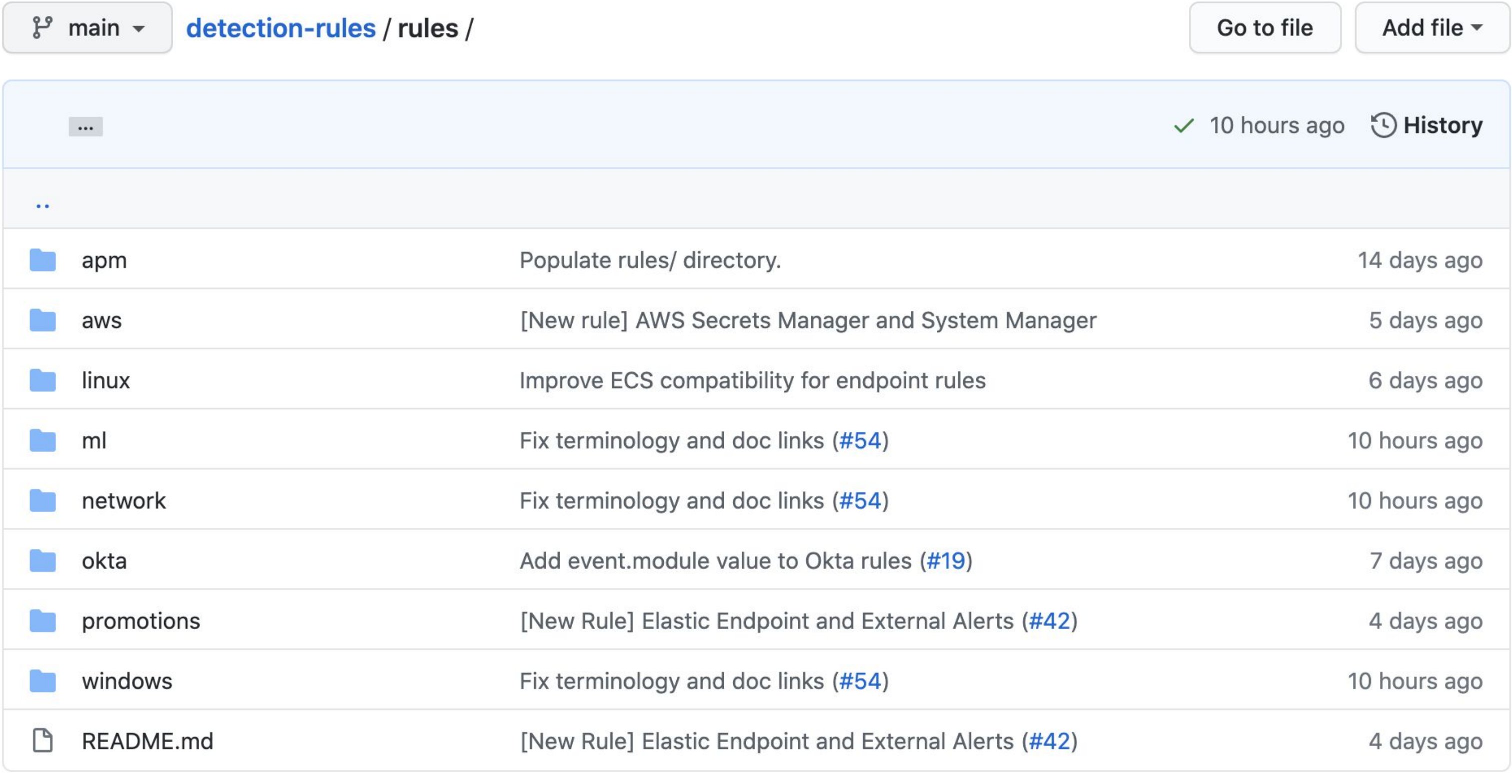
Detection Rules contains more than just static rule files. This repository also contains code for unit testing in Python and integrating with the Detection Engine in Kibana.

folder	description
`detection_rules/`	Python module for rule parsing, validating and packaging
`etc/`	Miscellaneous files, such as ECS and Beats schemas
`kibana/`	Python library for handling the API calls to Kibana and the Detection Engine
`kql/`	Python library for parsing and validating Kibana Query Language
`rta/`	Red Team Automation code used to emulate attacker techniques, used for rule testing
`rules/`	Root directory where rules are stored
`tests/`	Python code for unit testing rules

Getting started

Although rules can be added by manually creating `.toml` files, we don't recommend it. This repository also consists of a python module that aids rule creation and unit testing. Assuming you have Python 3.7+, run the below command to install the dependencies:

detection-rules/rules/

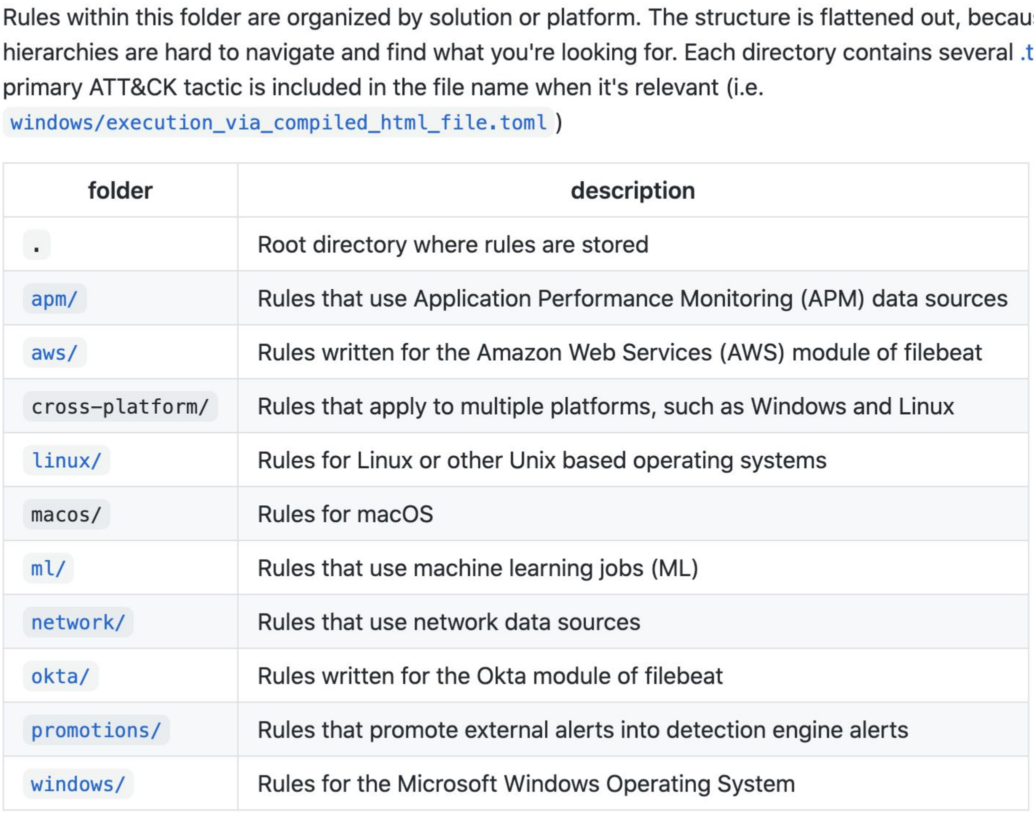


detection-rules / rules /

✓ 10 hours ago

..		
apm	Populate rules/ directory.	14 days ago
aws	[New rule] AWS Secrets Manager and System Manager	5 days ago
linux	Improve ECS compatibility for endpoint rules	6 days ago
ml	Fix terminology and doc links (#54)	10 hours ago
network	Fix terminology and doc links (#54)	10 hours ago
okta	Add event.module value to Okta rules (#19)	7 days ago
promotions	[New Rule] Elastic Endpoint and External Alerts (#42)	4 days ago
windows	Fix terminology and doc links (#54)	10 hours ago
README.md	[New Rule] Elastic Endpoint and External Alerts (#42)	4 days ago

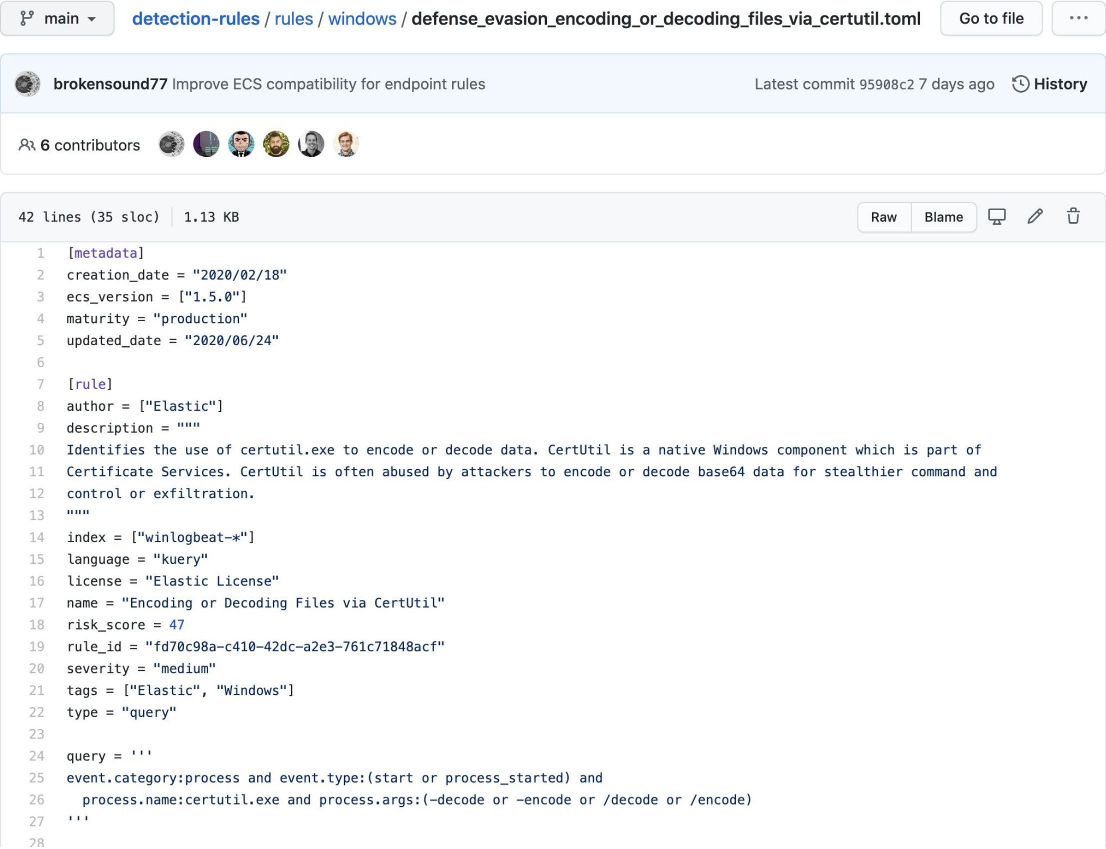
detection-rules/rules/



Rules within this folder are organized by solution or platform. The structure is flattened out, because nested file hierarchies are hard to navigate and find what you're looking for. Each directory contains several .toml files, and the primary ATT&CK tactic is included in the file name when it's relevant (i.e. `windows/execution_via_compiled_html_file.toml`)

folder	description
`.`	Root directory where rules are stored
`apm/`	Rules that use Application Performance Monitoring (APM) data sources
`aws/`	Rules written for the Amazon Web Services (AWS) module of filebeat
`cross-platform/`	Rules that apply to multiple platforms, such as Windows and Linux
`linux/`	Rules for Linux or other Unix based operating systems
`macos/`	Rules for macOS
`ml/`	Rules that use machine learning jobs (ML)
`network/`	Rules that use network data sources
`okta/`	Rules written for the Okta module of filebeat
`promotions/`	Rules that promote external alerts into detection engine alerts
`windows/`	Rules for the Microsoft Windows Operating System

detection-rules/rules/



detection-rules / rules / windows / defense_evasion_encoding_or_decoding_files_via_certutil.toml

brokensound77 Improve ECS compatibility for endpoint rules

Latest commit 95908c2 7 days ago History

6 contributors

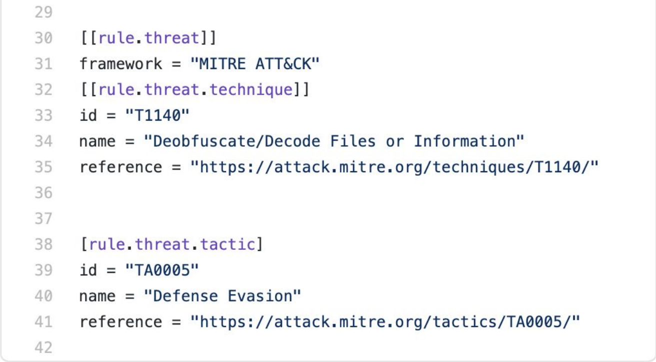
42 lines (35 sloc) | 1.13 KB

```
[metadata]
creation_date = "2020/02/18"
ecs_version = ["1.5.0"]
maturity = "production"
updated_date = "2020/06/24"

[rule]
author = ["Elastic"]
description = """
Identifies the use of certutil.exe to encode or decode data. CertUtil is a native Windows component which is part of
Certificate Services. CertUtil is often abused by attackers to encode or decode base64 data for stealthier command and
control or exfiltration.
"""
index = ["winlogbeat-*"]
language = "kuery"
license = "Elastic License"
name = "Encoding or Decoding Files via CertUtil"
risk_score = 47
rule_id = "fd70c98a-c410-42dc-a2e3-761c71848acf"
severity = "medium"
tags = ["Elastic", "Windows"]
type = "query"

query = '''
event.category:process and event.type:(start or process_started) and
  process.name:certutil.exe and process.args:(-decode or -encode or /decode or /encode)
'''

```



```

[[rule.threat]]
framework = "MITRE ATT&CK"
[[rule.threat.technique]]
id = "T1140"
name = "Deobfuscate/Decode Files or Information"
reference = "https://attack.mitre.org/techniques/T1140/"


[rule.threat.tactic]
id = "TA0005"
name = "Defense Evasion"
reference = "https://attack.mitre.org/tactics/TA0005/"

```

What we want to accomplish

github.com/elastic/detection-rules

- Improve security with the power of **open source**
- Share **best practices** for high fidelity rules
- **Develop quickly** and learn with you
- Provide the best **experience** for Elastic Security users

Agenda

1 Elastic Security Timeline

2 Introduction to the Rules Repo

3 Detection Engineering

4 Contributing

5 Demo

Agenda

1 Elastic Security Timeline

2 Introduction to the Rules Repo

3 Detection Engineering

4 Contributing

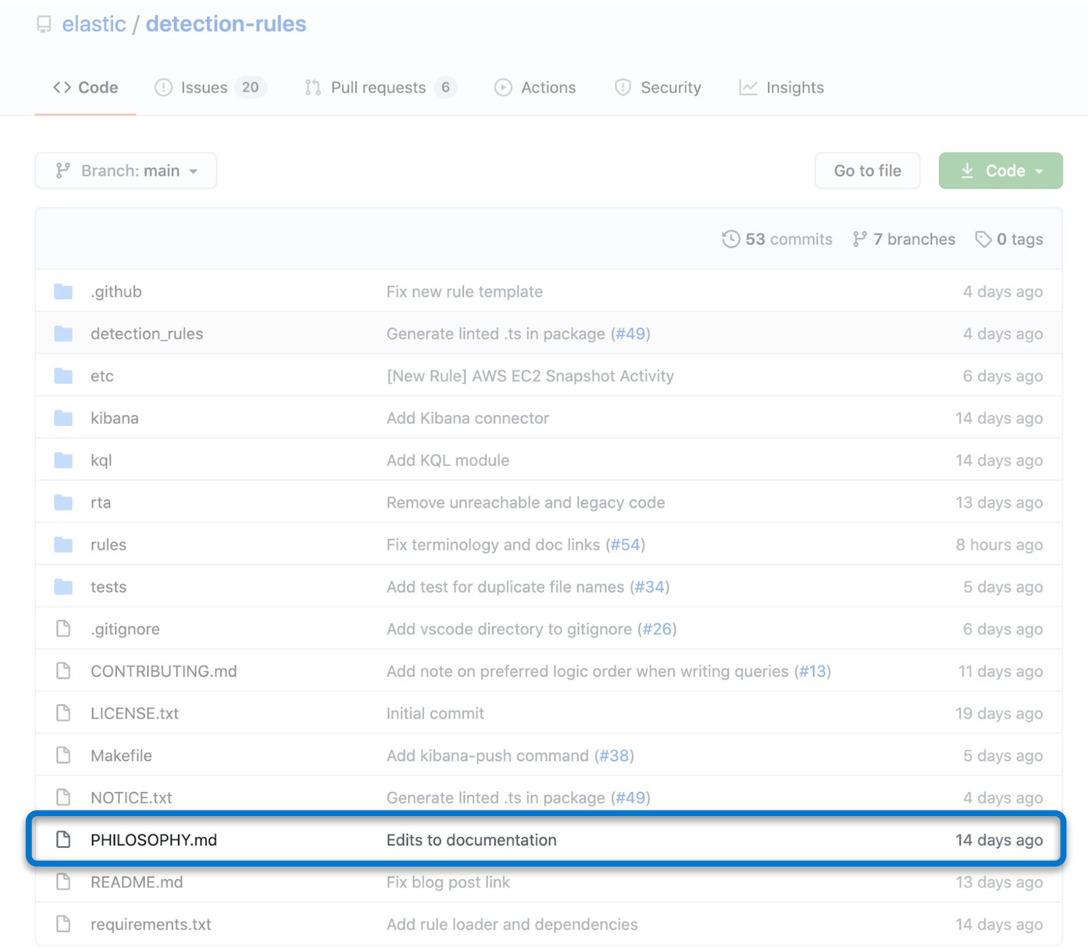
5 Demo

Detection engineering with Elastic Security

elastic

PHILOSOPHY.md

The latest information is always in the repo



53 commits · 7 branches · 0 tags

.github	Fix new rule template	4 days ago
detection_rules	Generate linted .ts in package (#49)	4 days ago
etc	[New Rule] AWS EC2 Snapshot Activity	6 days ago
kibana	Add Kibana connector	14 days ago
kql	Add KQL module	14 days ago
rta	Remove unreachable and legacy code	13 days ago
rules	Fix terminology and doc links (#54)	8 hours ago
tests	Add test for duplicate file names (#34)	5 days ago
.gitignore	Add vscode directory to gitignore (#26)	6 days ago
CONTRIBUTING.md	Add note on preferred logic order when writing queries (#13)	11 days ago
LICENSE.txt	Initial commit	19 days ago
Makefile	Add kibana-push command (#38)	5 days ago
NOTICE.txt	Generate linted .ts in package (#49)	4 days ago
PHILOSOPHY.md	Edits to documentation	14 days ago
README.md	Fix blog post link	13 days ago
requirements.txt	Add rule loader and dependencies	14 days ago

Our approach to detection engineering

PHILOSOPHY.md

- Shaped by our collective **real-world experience**
- Focus on **behaviors** more than custom tools
- Write logic **independent from the data source**
- Detect **true positives** while avoiding **false positives**
- Improve Elasticsearch **performance** when possible

Our approach to detection engineering

PHILOSOPHY.md

- Shaped by our collective **real-world experience**
- Focus on **behaviors** more than custom tools
- Write logic **independent from the data source**
- Detect **true positives** while avoiding **false positives**
- Improve Elasticsearch **performance** when possible

Detect behaviors more than custom tools

PHILOSOPHY.md

- Emphasize **technique**, not **indicators**
  - Forces you to write generic detections
  - Avoids the risk of overfitting
  - Similar philosophy to MITRE ATT&CK®
- **Make exceptions** where it makes sense
  - When a high-fidelity behavioral detection is nontrivial

https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Detect behaviors more than custom tools

PHILOSOPHY.md

❌ Indicator

```
process.name:mimikatz.exe or
process.command_line:*sekurlsa*
```

✅ Behavior

```
event.module:sysmon and
event.code:10 and
winlog.event_data.TargetImage:
  lsass.exe
```

Our approach to detection engineering

PHILOSOPHY.md

- Shaped by our collective **real-world experience**
- Focus on **behaviors** more than custom tools
- Write logic **independent from the data source**
- Detect **true positives** while avoiding **false positives**
- Improve Elasticsearch **performance** when possible

Write logic independent of data sources

PHILOSOPHY.md

- **Accommodate** various data sources
- Use Elastic Common Schema (**ECS**)
  - Use fields and categorization in ECS
- Make rules **plug-and-play**
  - Requires data source to map correctly to ECS
  - Less logic to maintain

Using Elastic Common Schema (ECS)

https://github.com/elastic/ecs

- Defines a **common** set of field names and types
- Enumerates **categorization fields** and **values** to bin similar events together
- Designed to be **extensible** and grow with our needs
- ECS is **adopted** throughout the Elastic Stack

Write logic independent of data sources

PHILOSOPHY.md

❌ Specific to each source

```
src:10.42.42.42 or
client_ip:10.42.42.42 or
apache2.access.remote_ip:
    10.42.42.42 or
context.user.ip:10.42.42.42
```

✔ With standard ECS field

```
source.ip:10.42.42.42
```

Our approach to detection engineering

PHILOSOPHY.md

- Shaped by our collective **real-world experience**
- Focus on **behaviors** more than custom tools
- Write logic **independent from the data source**
- Detect **true positives** while avoiding **false positives**
- Improve Elasticsearch **performance** when possible

Detect true positives while avoiding false positives

PHILOSOPHY.md

- Generic detections **increase FPs** disproportionately
    - Many techniques abuse built-in behavior and generate high volumes of benign activity
- Look for logic to **tip the scales towards TP**
- Attempt to **evade your detections**
    - Iterate until logic is rigorous

Detect true positives while avoiding false positives

PHILOSOPHY.md

- **Create or Modify System Process: Windows Service**
  - ATT&CK technique T1543 subtechnique 003
- **System Services: Service Execution**
  - ATT&CK technique T1569, subtechnique 002

Detect true positives while avoiding false positives

PHILOSOPHY.md

❌ Too vague

```
process.name:sc.exe
```

❌ Too many false positives

```
process.name:sc.exe and
process.args:(create or config)
```

Detect true positives while avoiding false positives

PHILOSOPHY.md

❌ Too easy to evade

```
process.command_line:
    "sc *create * binPath*"
```

❌ Too easy to evade

```
process.name:sc.exe and
process.command_line:
    "* create * binPath*"
```

Detect true positives while avoiding false positives

PHILOSOPHY.md

❌ Too overfitted

```
process.name:sc.exe and
process.args:(create or config)
and process.parent.name:cmd.exe
```

✔ Good FP and TP balance

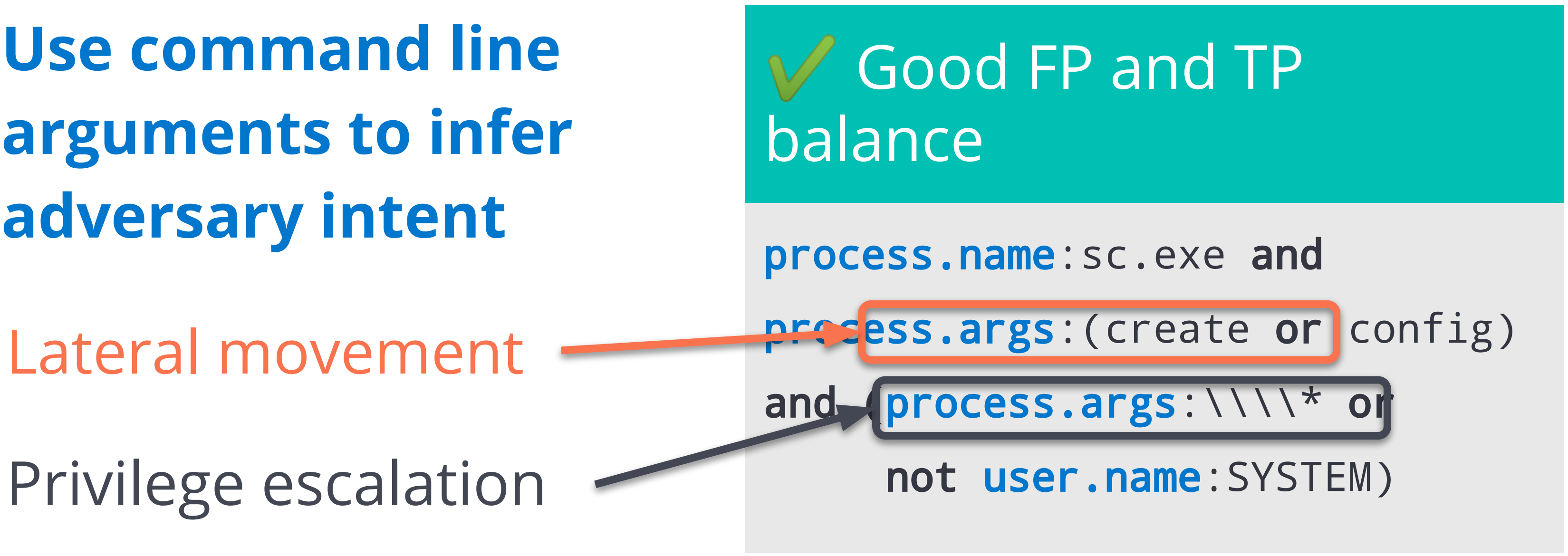
```
process.name:sc.exe and
process.args:(create or config)
and (process.args:\\\\* or
     not user.name:SYSTEM)
```

https://github.com/elastic/detection-rules/issues/47

Detect true positives while avoiding false positives

PHILOSOPHY.md

Use command line arguments to infer adversary intent



Lateral movement

Privilege escalation

✓ Good FP and TP balance

```
process.name:sc.exe and
process.args:(create or config)
and (process.args:\\\\* or
     not user.name:SYSTEM)
```

Our approach to detection engineering

PHILOSOPHY.md

- Shaped by our collective **real-world experience**
- Focus on **behaviors** more than custom tools
- Write logic **independent from the data source**
- Detect **true positives** while avoiding **false positives**
- Improve Elasticsearch **performance** when possible

Improve Elasticsearch performance when possible

PHILOSOPHY.md

- Use the proper **index patterns** when using Beats
- Target **ECS array fields** instead of parsing on the fly
- Prefer **exact matches** or **trailing wildcards**
- Don’t be afraid to ask!

Improve Elasticsearch performance when possible

PHILOSOPHY.md

❌ Unnecessary wildcards

```
process.name:sc.exe and
process.command_line:(
  *create* or *config*
)
```

✔ Use parsed fields

```
process.name:sc.exe and
process.args:(create or config)
```

Agenda

1 Elastic Security Timeline

2 Introduction to the Rules Repo

3 Detection Engineering

4 Contributing

5 Demo

Agenda

1 Elastic Security Timeline

2 Introduction to the Rules Repo

3 Detection Engineering

4 **Contributing**

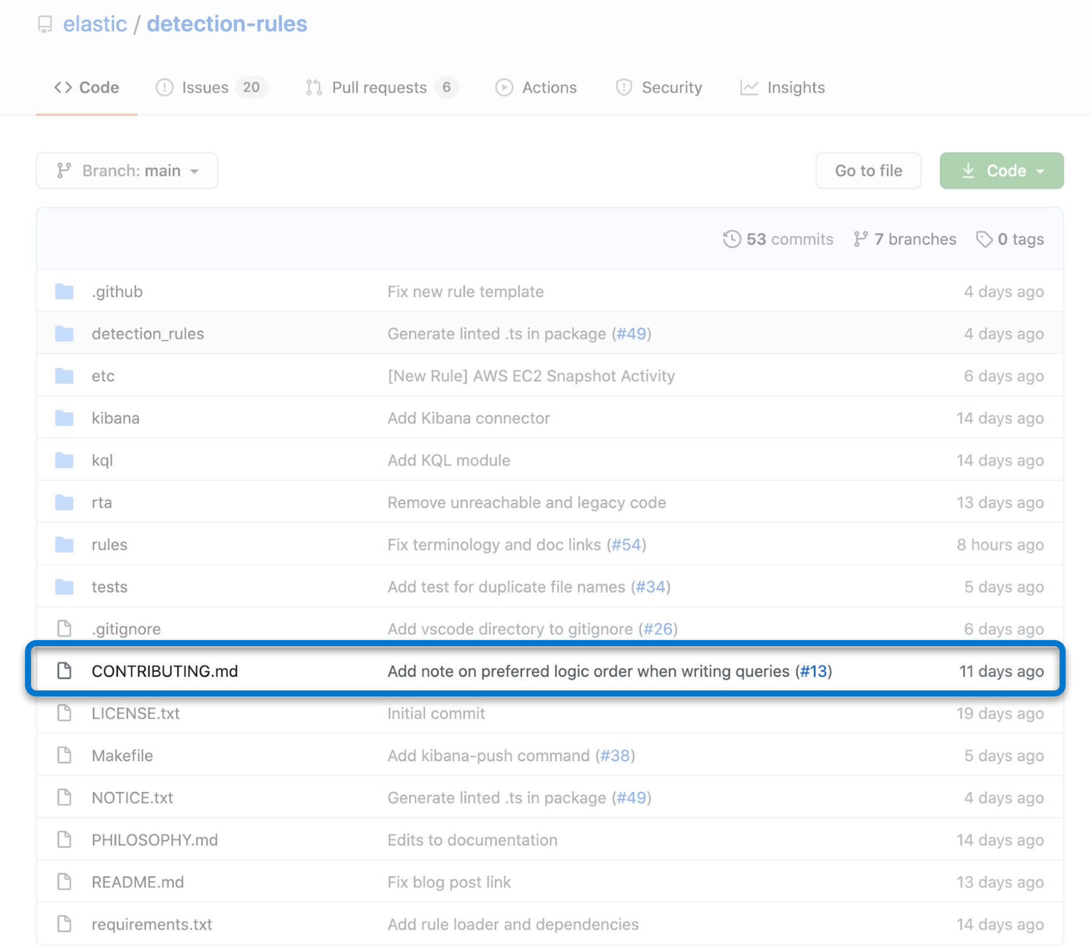
5 Demo

How to contribute to detection rules

elastic

CONTRIBUTING.md

The latest information is always in the repo



.github	Fix new rule template	4 days ago
detection_rules	Generate linted .ts in package (#49)	4 days ago
etc	[New Rule] AWS EC2 Snapshot Activity	6 days ago
kibana	Add Kibana connector	14 days ago
kql	Add KQL module	14 days ago
rta	Remove unreachable and legacy code	13 days ago
rules	Fix terminology and doc links (#54)	8 hours ago
tests	Add test for duplicate file names (#34)	5 days ago
.gitignore	Add vscode directory to gitignore (#26)	6 days ago
CONTRIBUTING.md	Add note on preferred logic order when writing queries (#13)	11 days ago
LICENSE.txt	Initial commit	19 days ago
Makefile	Add kibana-push command (#38)	5 days ago
NOTICE.txt	Generate linted .ts in package (#49)	4 days ago
PHILOSOPHY.md	Edits to documentation	14 days ago
README.md	Fix blog post link	13 days ago
requirements.txt	Add rule loader and dependencies	14 days ago

Contributing to the repository

CONTRIBUTING.md

- Create a GitHub issue **first**
- **Fork** and **clone** the repository
- Use the **CLI** to create a rule
- Run **local tests** to validate syntax and logic
- Finally, submit a **pull request**

Contributing to the repository

CONTRIBUTING.md

- Create a GitHub issue **first**
- **Fork** and **clone** the repository
- Use the **CLI** to create a rule
- Run **local tests** to validate syntax and logic
- Finally, submit a **pull request**

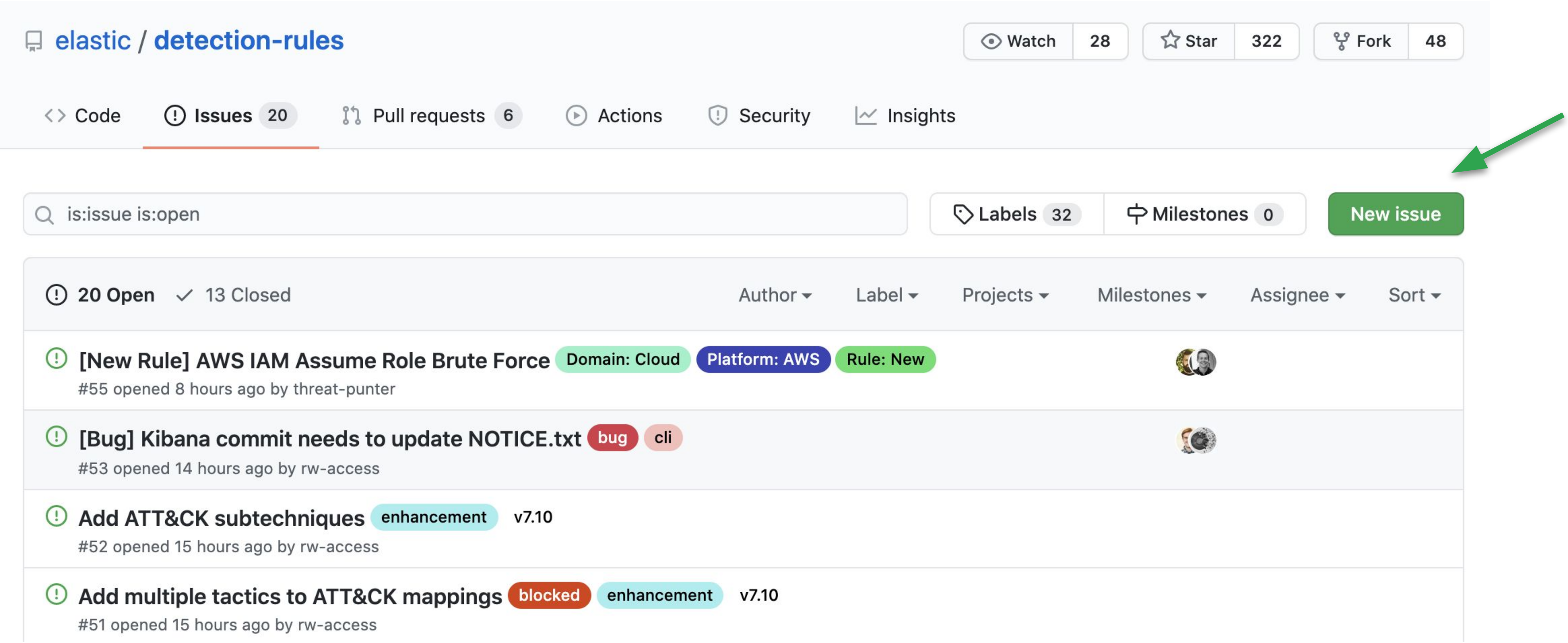
Create a GitHub issue first

CONTRIBUTING.md

- Forces us to **discuss early** in the process
  - Learn from each other and share ideas
- Choose from our **existing templates**
- **Include licenses** and links for external rules
- **Improves productivity** for pull requests
  - Less back-and-forth and more merging!

Create a GitHub issue first

CONTRIBUTING.md



elastic / detection-rules

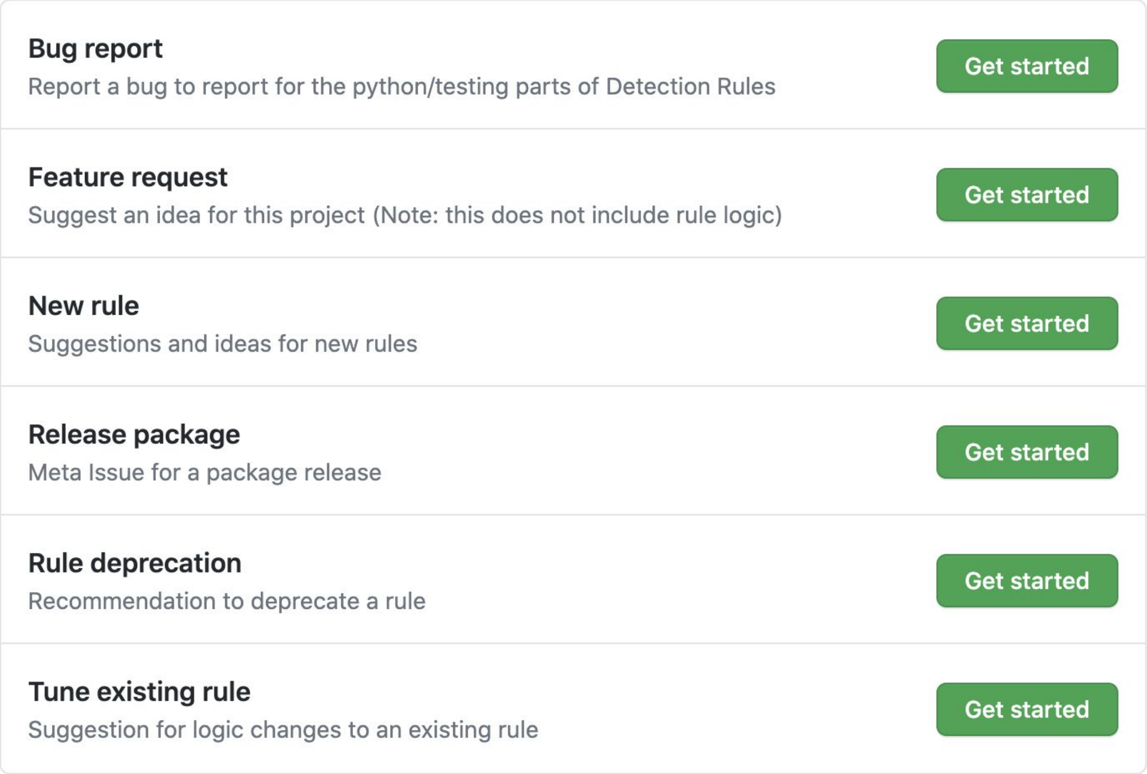
is:issue is:open

20 Open ✓ 13 Closed

- [New Rule] AWS IAM Assume Role Brute Force — Domain: Cloud, Platform: AWS, Rule: New
  #55 opened 8 hours ago by threat-punter
- [Bug] Kibana commit needs to update NOTICE.txt — bug, cli
  #53 opened 14 hours ago by rw-access
- Add ATT&CK subtechniques — enhancement — v7.10
  #52 opened 15 hours ago by rw-access
- Add multiple tactics to ATT&CK mappings — blocked, enhancement — v7.10
  #51 opened 15 hours ago by rw-access

Create a GitHub issue first

CONTRIBUTING.md



Bug report
Report a bug to report for the python/testing parts of Detection Rules

Feature request
Suggest an idea for this project (Note: this does not include rule logic)

New rule
Suggestions and ideas for new rules

Release package
Meta Issue for a package release

Rule deprecation
Recommendation to deprecate a rule

Tune existing rule
Suggestion for logic changes to an existing rule

Don’t see your issue here? Open a blank issue.

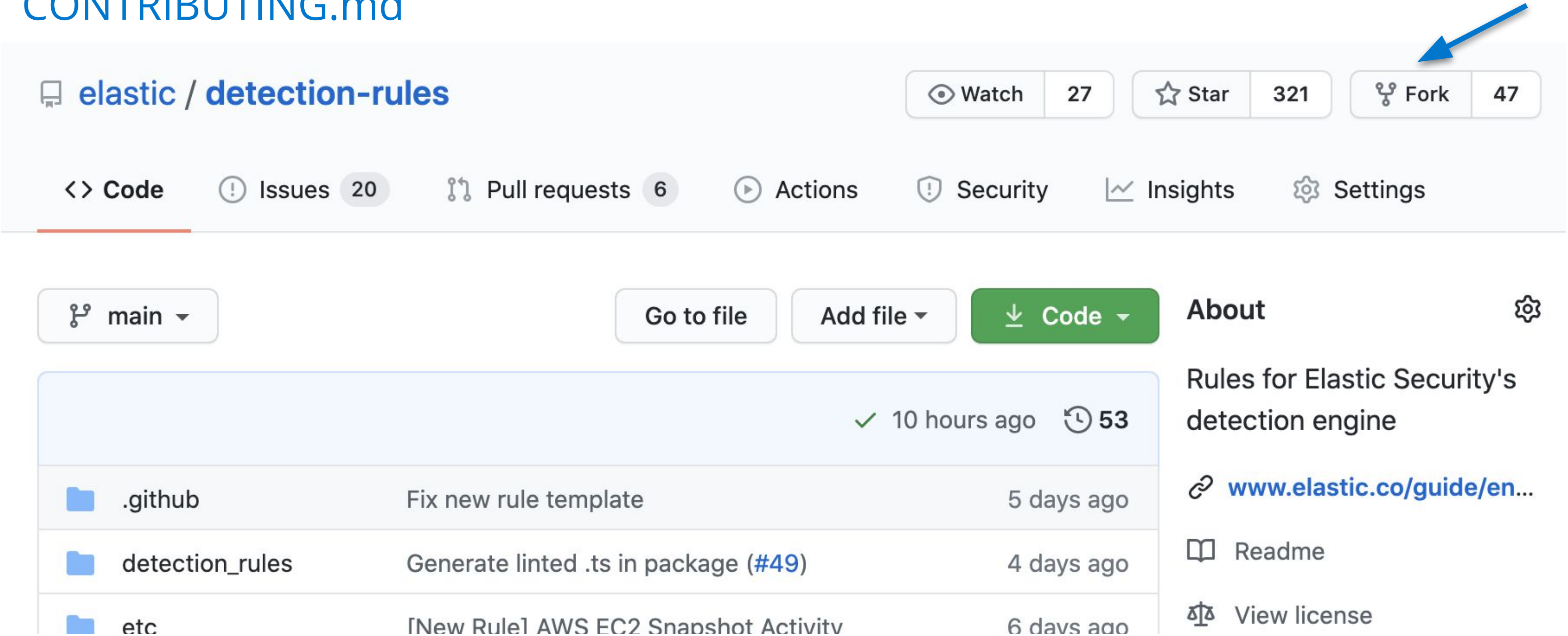
Contributing to the repository

CONTRIBUTING.md

- Create a GitHub issue **first**
- **Fork** and **clone** the repository
- Use the **CLI** to create a rule
- Run **local tests** to validate syntax and logic
- Finally, submit a **pull request**

Fork and clone the repository

CONTRIBUTING.md



Rules for Elastic Security's detection engine

.github	Fix new rule template	5 days ago
detection_rules	Generate linted .ts in package (#49)	4 days ago
etc	[New Rule] AWS EC2 Snapshot Activity	6 days ago

https://docs.github.com/en/github/getting-started-with-github/fork-a-repo

Fork and clone the repository

CONTRIBUTING.md

```
git clone https://github.com/<username>/detection-rules.git
```

```
cd detection-rules
```

```
git remote add upstream https://github.com/elastic/detection-rules.git
```

https://docs.github.com/en/github/getting-started-with-github/fork-a-repo

Contributing to the repository

CONTRIBUTING.md

- Create a GitHub issue **first**
- **Fork** and **clone** the repository
- Use the **CLI** to create a rule
- Run **local tests** to validate syntax and logic
- Finally, submit a **pull request**

Use the CLI to create a rule

CONTRIBUTING.md

➔

```
python -m detection_rules create-rule rules/<path-to-rule>.toml [--required-only]
```

```
Rule type (machine_learning, query, saved_id): query

actions (multi, comma separated):

description (required): Look for child processes of MsBuild

...

Rule <name> saved to rules/<path-to-rule>.toml
```

https://docs.github.com/en/github/getting-started-with-github/fork-a-repo

Contributing to the repository

CONTRIBUTING.md

- Create a GitHub issue **first**
- **Fork** and **clone** the repository
- Use the **CLI** to create a rule
- Run **local tests** to validate syntax and logic
- Finally, submit a **pull request**

Run local tests to validate syntax and logic

CONTRIBUTING.md

➔ **python** `-m detection_rules test`

```
================================ test session starts =================================
collected 73 items

tests/test_all_rules.py::TestValidRules::test_all_rule_files PASSED              [  1%]
tests/test_all_rules.py::TestValidRules::test_all_rule_queries_optimized PASSED  [  2%]
tests/test_all_rules.py::TestValidRules::test_all_rules_as_rule_schema PASSED    [  4%]
tests/test_all_rules.py::TestValidRules::test_all_rules_tuned PASSED             [  5%]
...
tests/kuery/test_parser.py::ParserTests::test_number_exists PASSED               [ 98%]
tests/kuery/test_parser.py::ParserTests::test_number_wildcard_fail PASSED        [100%]

================================= 73 passed in 8.47s =================================
```

Contributing to the repository

CONTRIBUTING.md

- Create a GitHub issue **first**
- **Fork** and **clone** the repository
- Use the **CLI** to create a rule
- Run **local tests** to validate syntax and logic
- Finally, submit a **pull request**

Submit a pull request

CONTRIBUTING.md

- **Commit** your local changes in a new branch
- **Push** your branch to your fork
- **Open** a pull request
- Wait for review and expect to **make changes**
- When it’s ready, we’ll update labels and **merge**

Agenda

1. Elastic Security Timeline
2. Introduction to the Rules Repo
3. Detection Engineering
4. Contributing
5. Demo

Agenda

1 Elastic Security Timeline

2 Introduction to the Rules Repo

3 Detection Engineering

4 Contributing

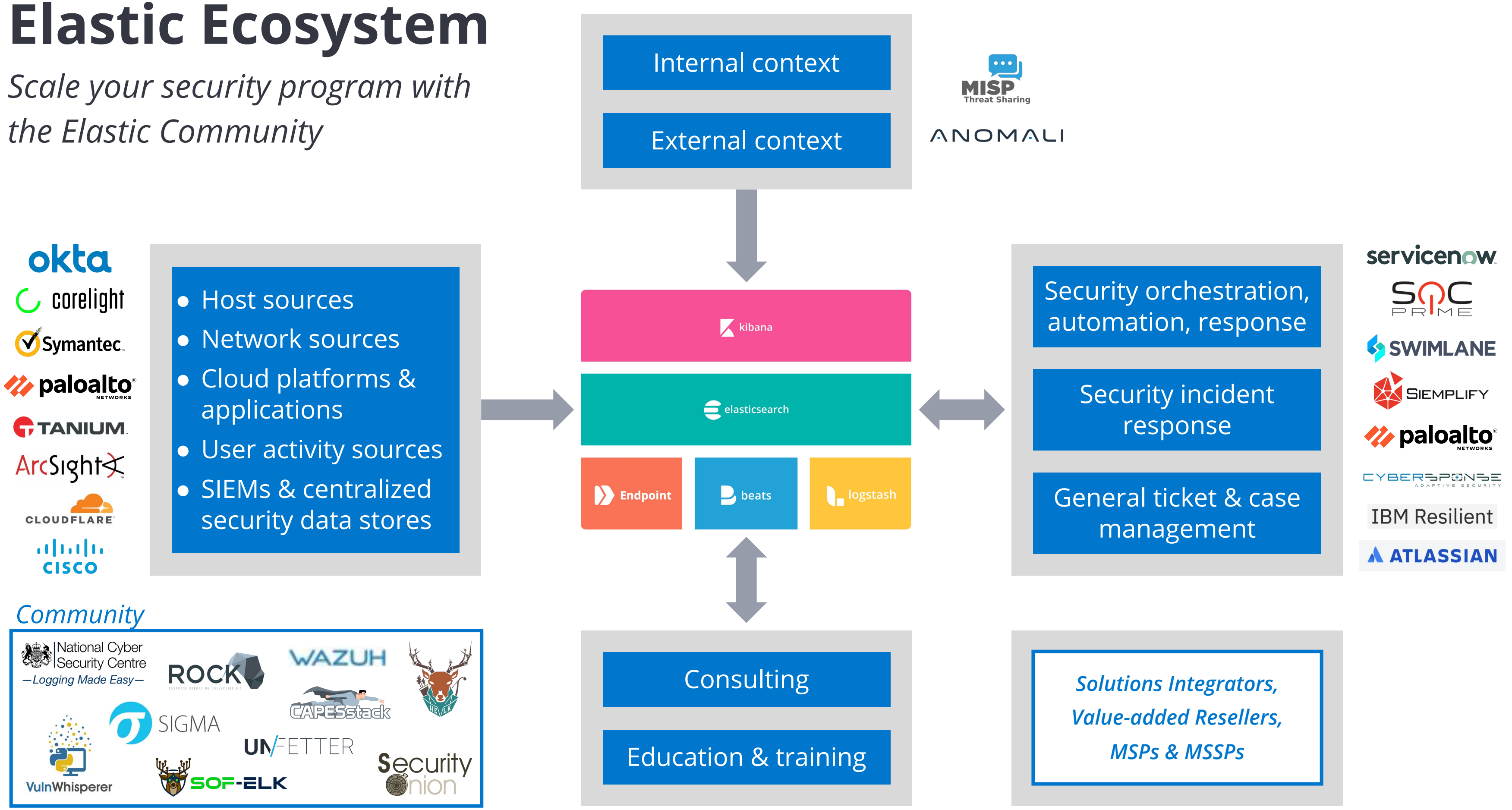
5 Demo

DEMO

elastic

Elastic Ecosystem

Scale your security program with the Elastic Community



Internal context

External context

- Host sources
- Network sources
- Cloud platforms & applications
- User activity sources
- SIEMs & centralized security data stores

Security orchestration, automation, response

Security incident response

General ticket & case management

Consulting

Education & training

Community

Solutions Integrators, Value-added Resellers, MSPs & MSSPs

These are just some of our partners, community members, and integrations. The presence of a vendor logo doesn't imply a business relationship with Elastic.

elastic

Connect to the Elastic Security Community

1

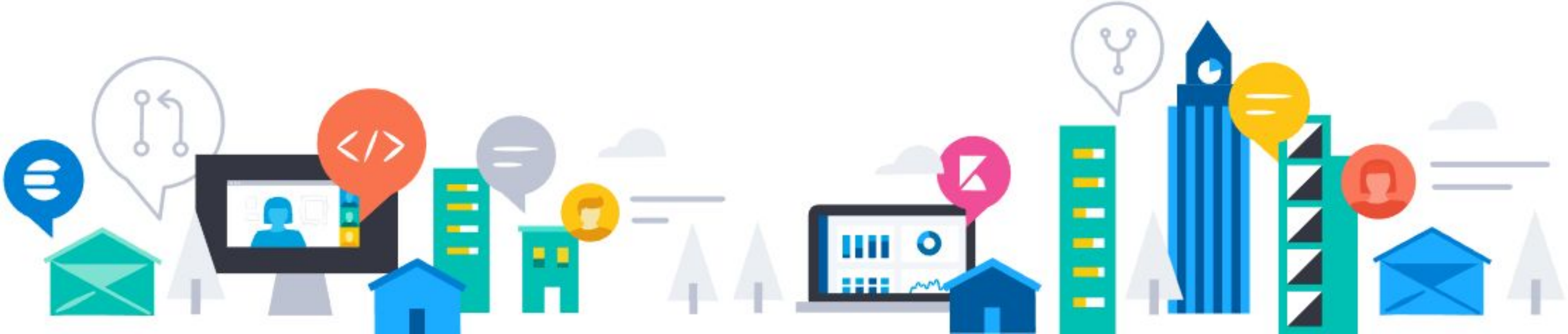
Take a quick spin:
demo.elastic.co

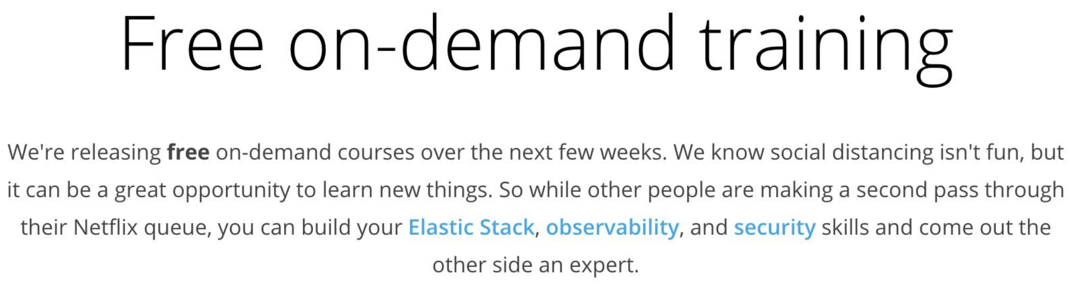
2

Try free on Cloud:
elastic.co/cloud

3

Join us on Slack:
ela.st/slack





Free on-demand training

We're releasing **free** on-demand courses over the next few weeks. We know social distancing isn't fun, but it can be a great opportunity to learn new things. So while other people are making a second pass through their Netflix queue, you can build your Elastic Stack, observability, and security skills and come out the other side an expert.

https://training.elastic.co/learn-from-home

elastic

Thank You!

...check out the repo, github.com/elastic/detection-rules

...join us on Slack, #detection-rules @ ela.st/slack

Elastic is a Search Company.

www.elastic.co