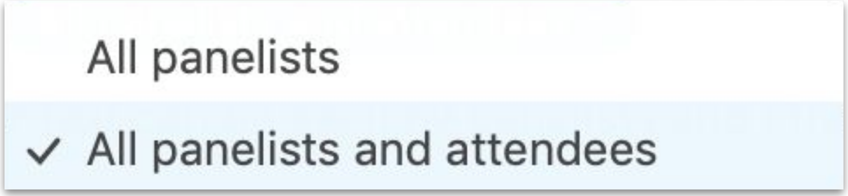
elastic

Gain control over the data your SOC needs with Elastic Security

Mike Paquette & Mark Settle
May 6, 2021

Housekeeping & Logistics

- Attendees are automatically muted upon joining 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”



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

elastic

Gain control over the data your SOC needs with Elastic Security

Mike Paquette & Mark Settle
May 6, 2021

Mark Settle

Sr. Manager, Product Marketing

Mike Paquette

Director of Product, Elastic Security for SIEM

elastic

Agenda

1. Intro and overview
2. Avoid the impossible task of choosing which data sources to ingest
3. Improve efficacy of detection while minimizing alert fatigue
4. Improve efficiency of investigation and incident response
5. Gain control of security data with data tiers
6. Q&A

gabriel boorse @gnboorse

Really loving #Elasticsearch right now. @elastic That's it. That's the tweet.

Liago Faria @0xtf

Really awe
These cha
informatic

Vevek Pandian @VevekPandian

Have been going deep into #elasticsearch #elkstack @elastic . Such an awesome and fantastic tool for building search engine for distributed systems.

Artem Russakovskii @ArtemR

@elastic is amazing - now raw search queries take 3-10ms.

Grant Visser @ICantSeeSharp

Yo. @elastic Application Performance Metrics are literally magic.

Elastic is a ***search*** company.

Liago Faria @0xtf

Really awe
These cha
informatic

elastic

Elastic is a ***search*** company.

Security is a ***data*** problem.

Three solutions powered by one stack

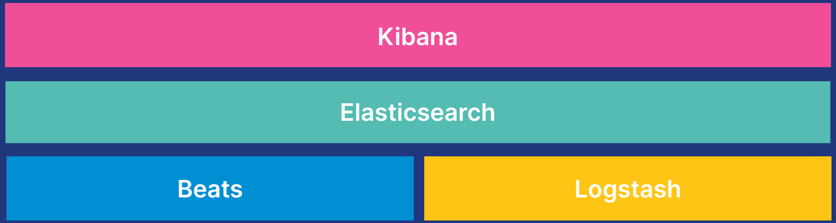
3 solutions

Enterprise Search

Observability

Security

Powered by
the Elastic Stack



Kibana

Elasticsearch

Beats

Logstash

Deployed
anywhere

Elastic Cloud

Elastic Cloud
Enterprise

Elastic Cloud
on Kubernetes

SaaS

Orchestration

elastic

Elastic Security

Collect

Data Sources

P/I/SaaS

User

Network Activity

Endpoint

Server

Wire & Flow Data

Code Repository

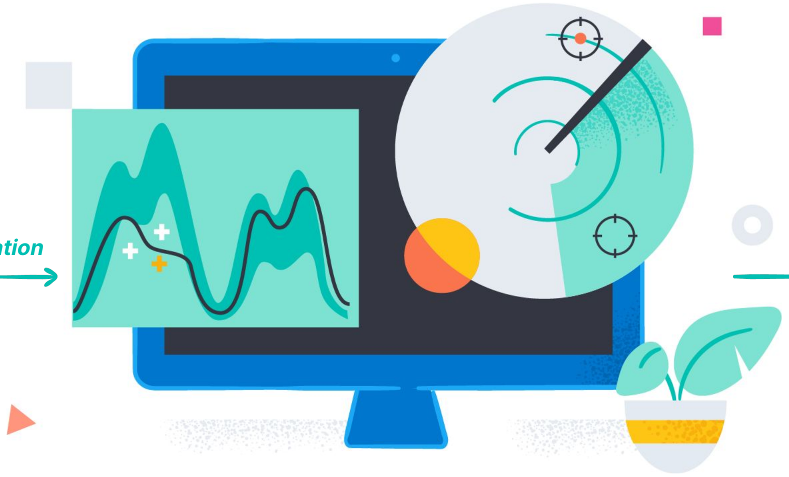
Connected Devices & Physical Security

Collection and Prevention

Elastic Agent

Normalization →

Detect, Analyze, Investigate



Built on Fast, Scalable Search

→

Respond

Response

Elastic Agent

SOAR

SIRP

ITSM

Custom

Reporting

Lens + Canvas

The Foundation of Modern Security, Observability, and more

Designed for tomorrow’s environments: bring your search to the data

elastic

Elastic Agent

One agent, one click, any use case

Centrally manage your Agents in Fleet

Scale and manage Agents from a simple UI

Hundreds of OOTB data integrations

One-click collection and preparation:
elastic.co/integrations

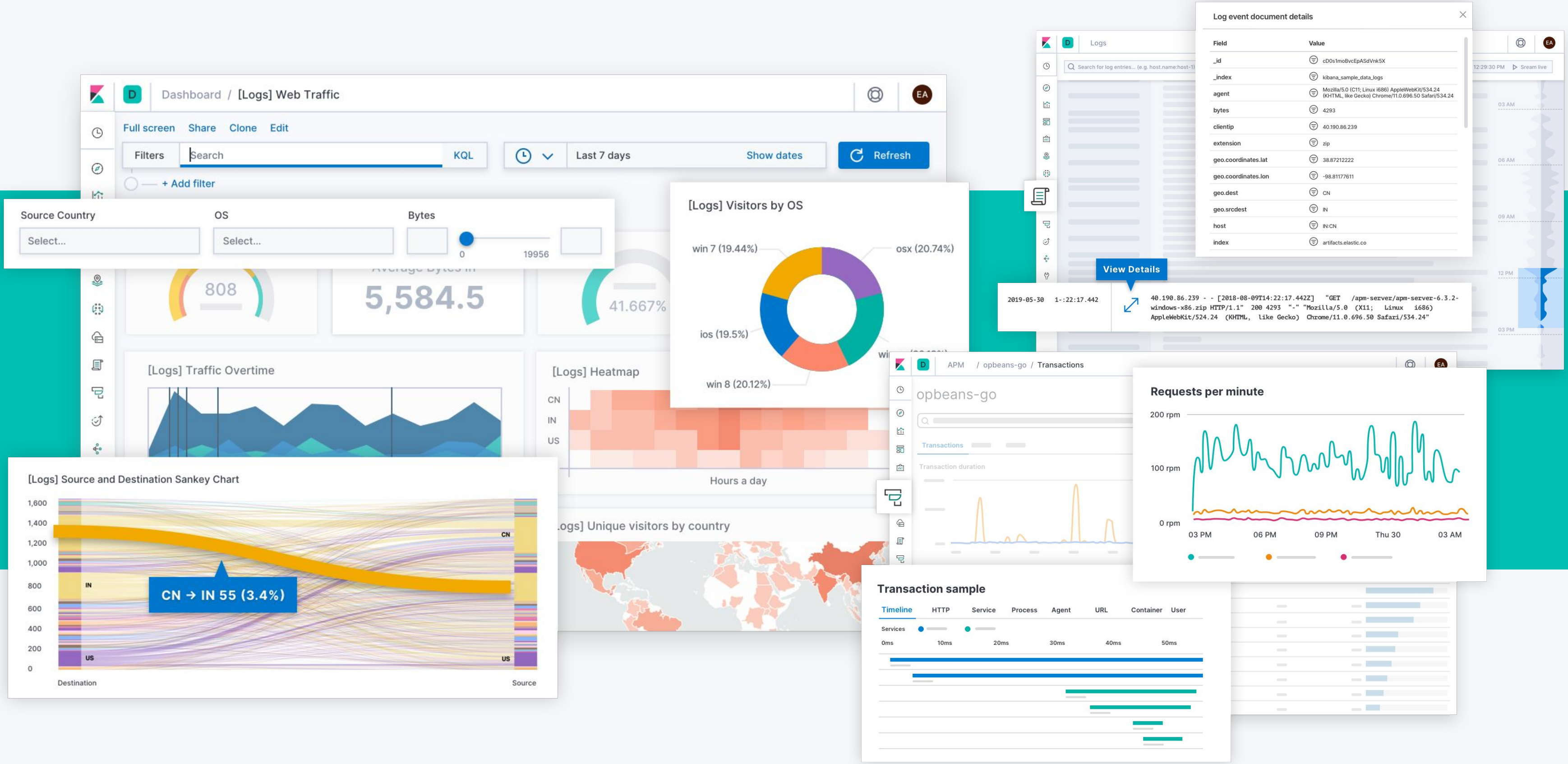
Prevention built in

Signatureless malware prevention provided free;
behavioral ransomware stops tomorrow’s attacks

>50% of MITRE techniques require endpoint visibility

Section 1

Avoid the impossible task of choosing which data sources to ingest

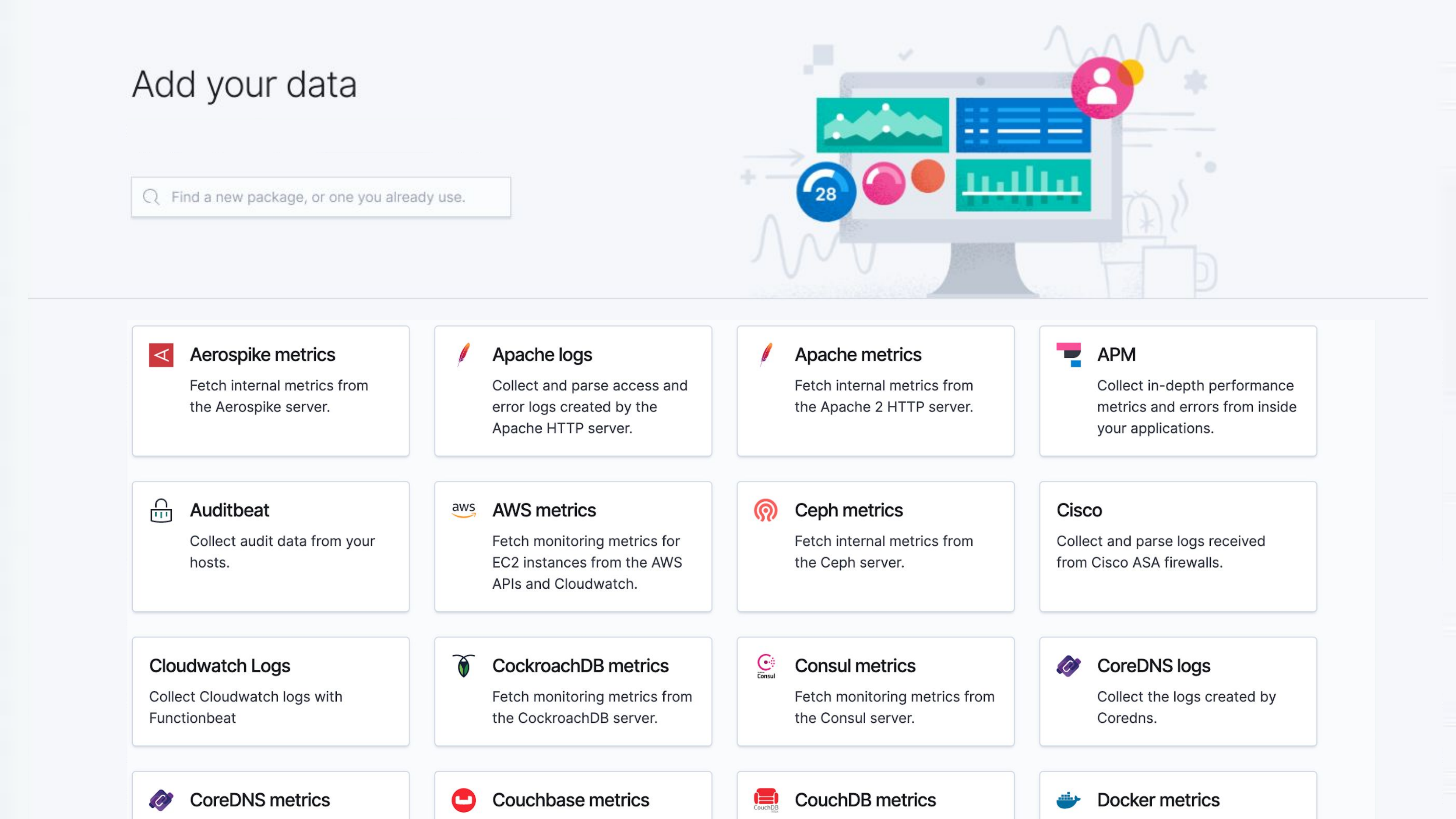


Log event document details

Field	Value
_id	cD0s1moBvcEpASdVnk5X
_index	kibana_sample_data_logs
agent	Mozilla/5.0 (C11; Linux i686) AppleWebKit/534.24 (KHTML, like Gecko) Chrome/11.0.696.50 Safari/534.24
bytes	4293
clientip	40.190.86.239
extension	zip
geo.coordinates.lat	38.87212222
geo.coordinates.lon	-98.81177611
geo.dest	CN
geo.srcdest	IN
host	IN:CN
index	artifacts.elastic.co

```
2019-05-30   1-:22:17.442
40.190.86.239 - - [2018-08-09T14:22:17.442Z]  “GET  /apm-server/apm-server-6.3.2-windows-x86.zip HTTP/1.1”  200 4293  “-“ “Mozilla/5.0  (X11;  Linux  i686) AppleWebKit/524.24  (KHTML,  like Gecko)  Chrome/11.0.696.50 Safari/534.24”
```

elastic



Add your data

Find a new package, or one you already use.

Aerospike metrics
Fetch internal metrics from the Aerospike server.

Apache logs
Collect and parse access and error logs created by the Apache HTTP server.

Apache metrics
Fetch internal metrics from the Apache 2 HTTP server.

APM
Collect in-depth performance metrics and errors from inside your applications.

Auditbeat
Collect audit data from your hosts.

AWS metrics
Fetch monitoring metrics for EC2 instances from the AWS APIs and Cloudwatch.

Ceph metrics
Fetch internal metrics from the Ceph server.

Cisco
Collect and parse logs received from Cisco ASA firewalls.

Cloudwatch Logs
Collect Cloudwatch logs with Functionbeat

CockroachDB metrics
Fetch monitoring metrics from the CockroachDB server.

Consul metrics
Fetch monitoring metrics from the Consul server.

CoreDNS logs
Collect the logs created by Coredns.

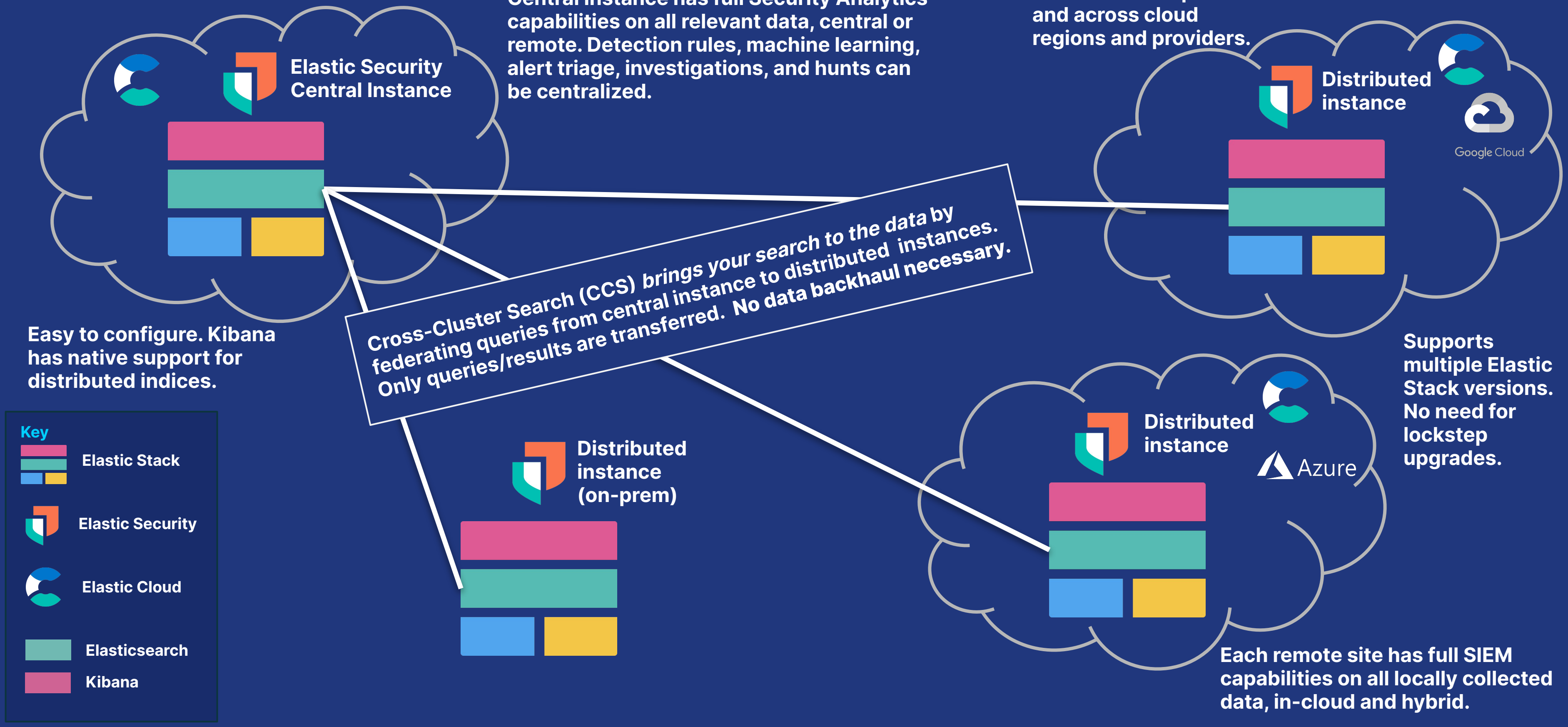
CoreDNS metrics

Couchbase metrics

CouchDB metrics

Docker metrics

Bring your Search to the Data with Cross-Cluster Search



Elastic Security Central Instance

Central Instance has full Security Analytics capabilities on all relevant data, central or remote. Detection rules, machine learning, alert triage, investigations, and hunts can be centralized.

Works with on-prem and across cloud regions and providers.

Distributed instance

Cross-Cluster Search (CCS) *brings your search to the data by* federating queries from central instance to distributed instances. Only queries/results are transferred. No data backhaul necessary.

Easy to configure. Kibana has native support for distributed indices.

Distributed instance (on-prem)

Distributed instance

Supports multiple Elastic Stack versions. No need for lockstep upgrades.

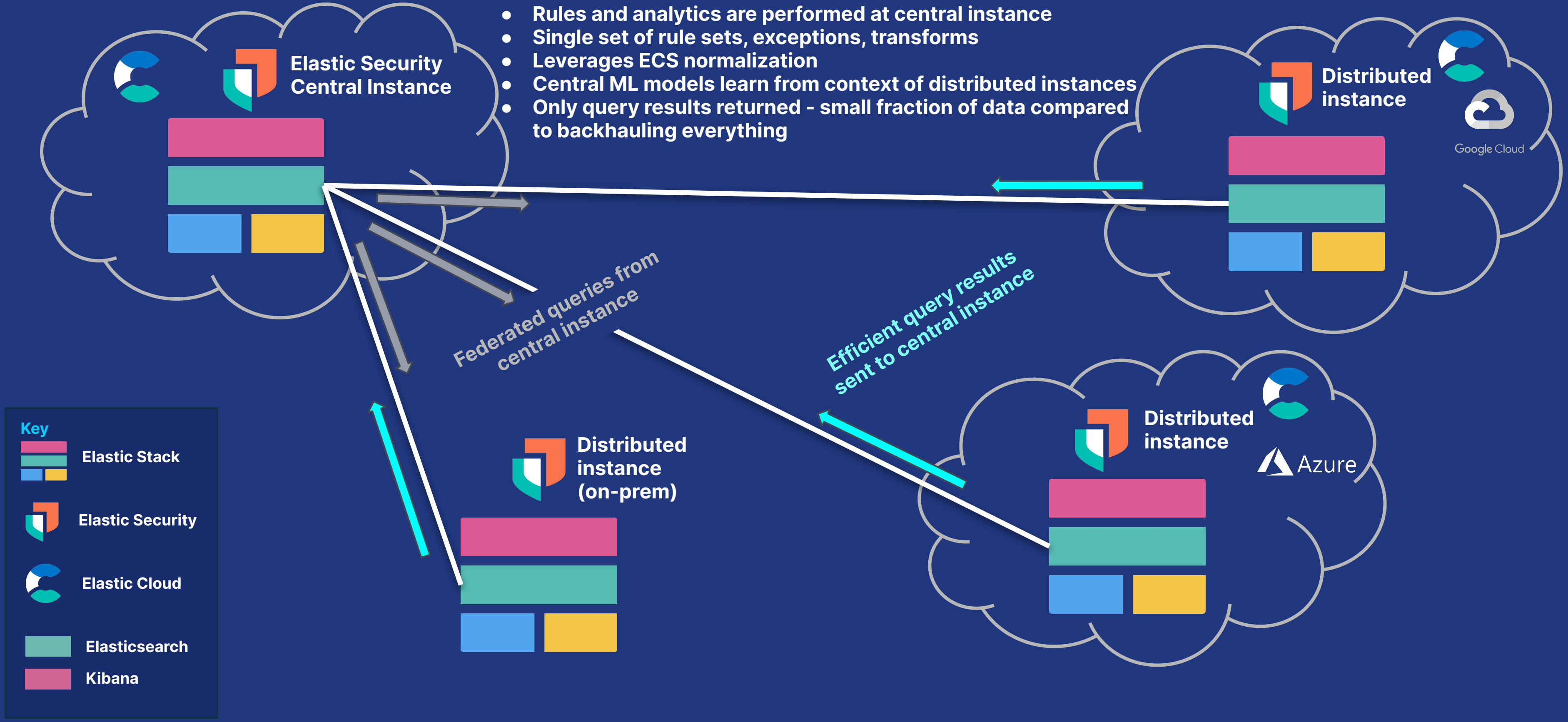
Each remote site has full SIEM capabilities on all locally collected data, in-cloud and hybrid.

Key

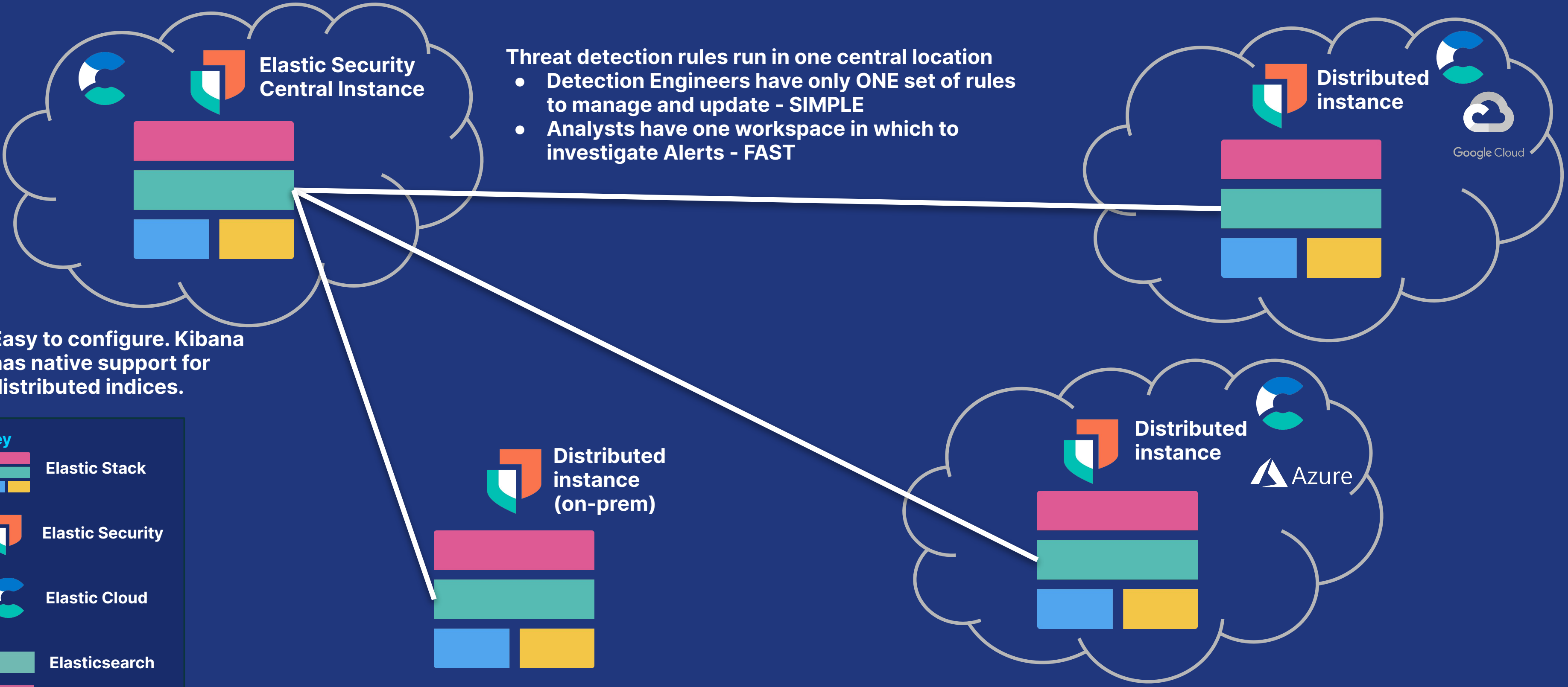
- Elastic Stack
- Elastic Security
- Elastic Cloud
- Elasticsearch
- Kibana

Cross-Cluster Search - Holistic View w/o Data Backhaul

- Rules and analytics are performed at central instance
- Single set of rule sets, exceptions, transforms
- Leverages ECS normalization
- Central ML models learn from context of distributed instances
- Only query results returned - small fraction of data compared to backhauling everything


Elastic Security Central Instance
Distributed instance
Google Cloud
Federated queries from central instance
Efficient query results sent to central instance
Distributed instance (on-prem)
Distributed instance
Azure
Key
Elastic Stack
Elastic Security
Elastic Cloud
Elasticsearch
Kibana

Cross-Cluster Search - Simple Detection Management



Elastic Security Central Instance

Distributed instance

Google Cloud

Distributed instance

Azure

Distributed instance (on-prem)

Threat detection rules run in one central location

- Detection Engineers have only ONE set of rules to manage and update - SIMPLE
- Analysts have one workspace in which to investigate Alerts - FAST

Easy to configure. Kibana has native support for distributed indices.

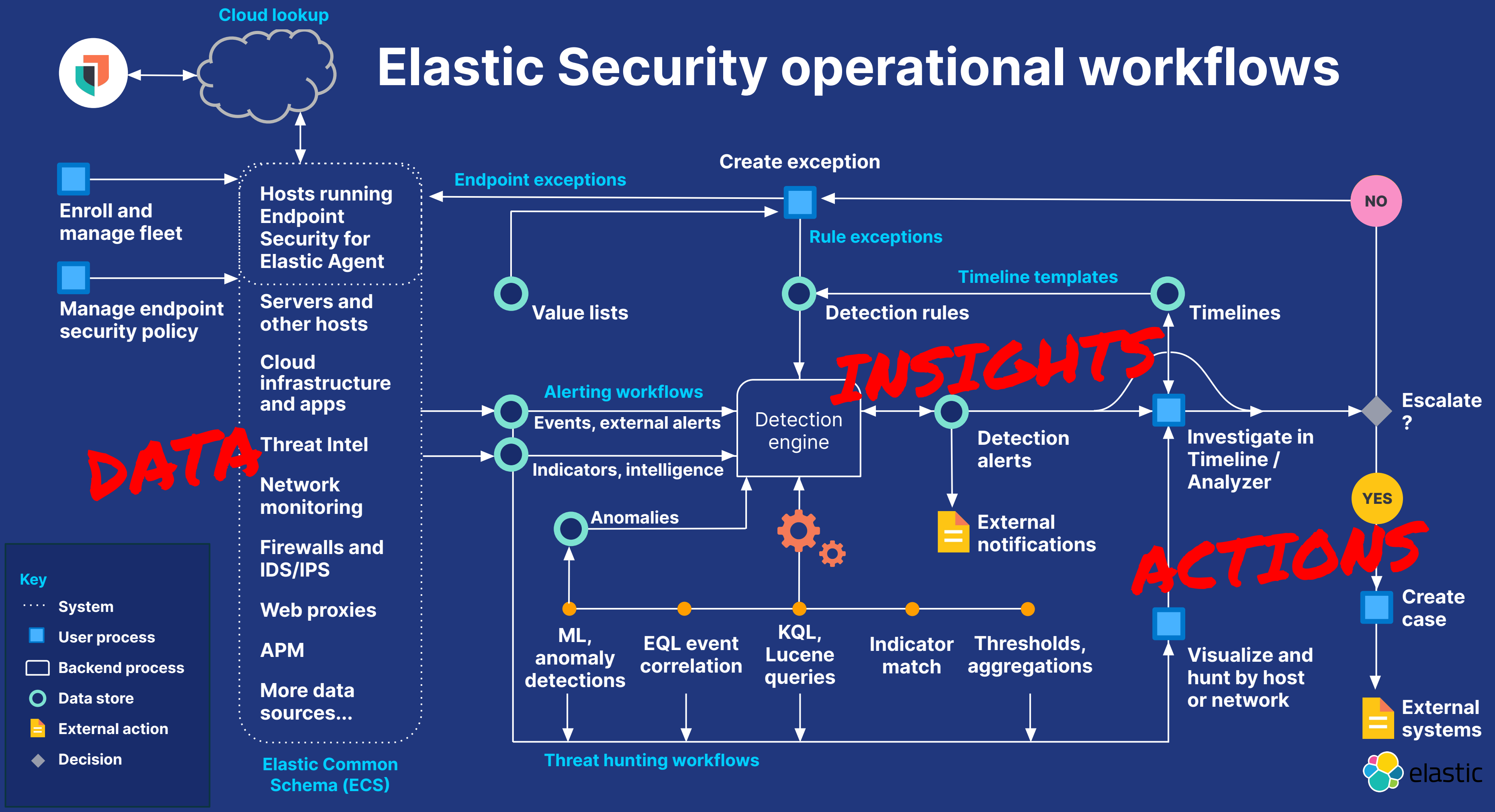
Key

- Elastic Stack
- Elastic Security
- Elastic Cloud
- 🟩 Elasticsearch
- 🟥 Kibana

Section 2

Improve efficacy of detection while minimizing alert fatigue

Elastic Security operational workflows



Cloud lookup

Enroll and manage fleet

Manage endpoint security policy

Hosts running Endpoint Security for Elastic Agent

Servers and other hosts

Cloud infrastructure and apps

Threat Intel

Network monitoring

Firewalls and IDS/IPS

Web proxies

APM

More data sources...

Elastic Common Schema (ECS)

DATA

Create exception

Endpoint exceptions

Rule exceptions

Value lists

Detection rules

Timeline templates

Timelines

INSIGHTS

Alerting workflows

Events, external alerts

Indicators, intelligence

Detection engine

Detection alerts

External notifications

Anomalies

ML, anomaly detections

EQL event correlation

KQL, Lucene queries

Indicator match

Thresholds, aggregations

Threat hunting workflows

Investigate in Timeline / Analyzer

Visualize and hunt by host or network

NO

Escalate ?

YES

ACTIONS

Create case

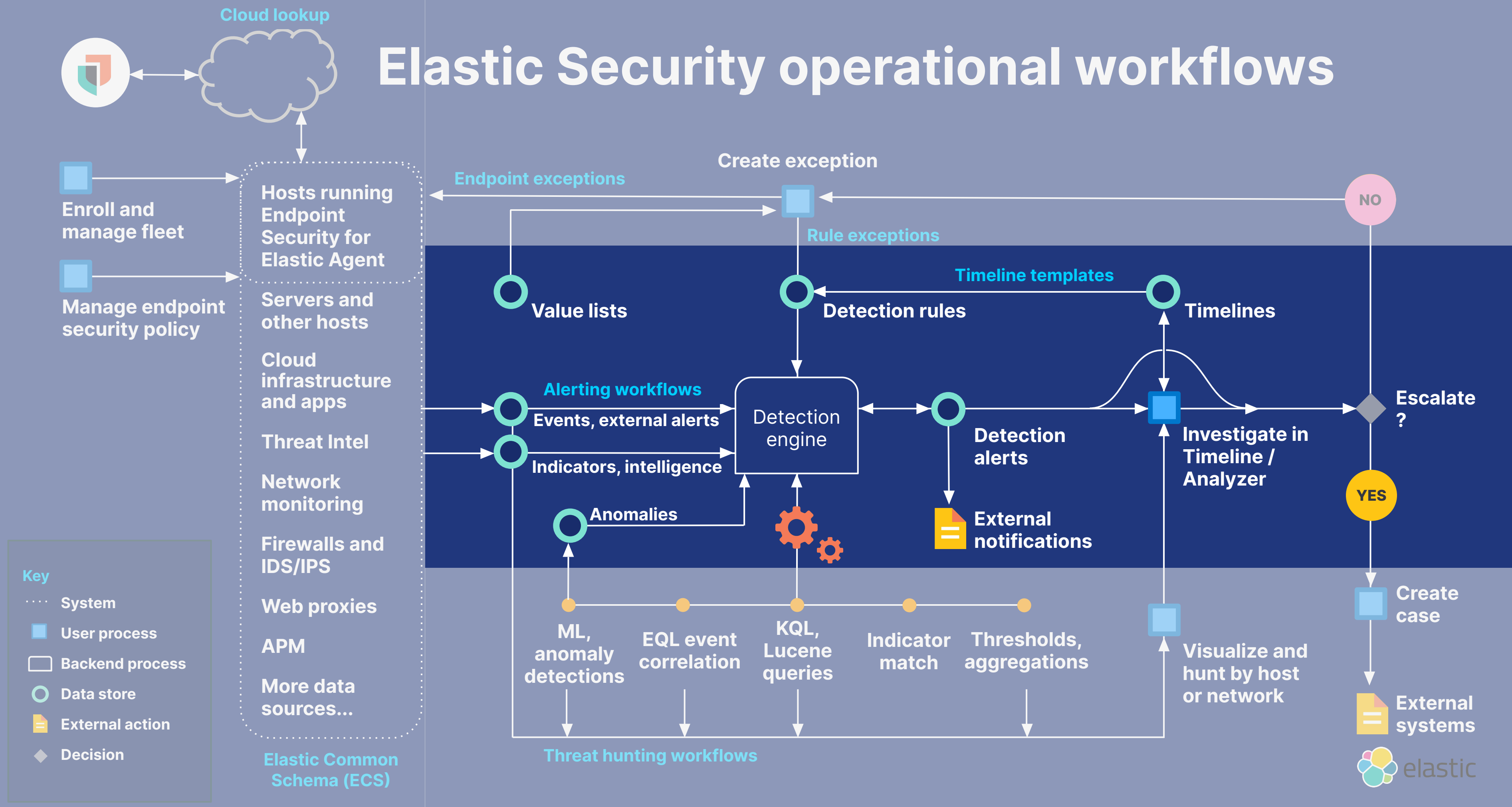
External systems

Key

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

elastic

Elastic Security operational workflows



Elastic 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

- 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

elastic

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
```

Write logic independent from the data source

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)

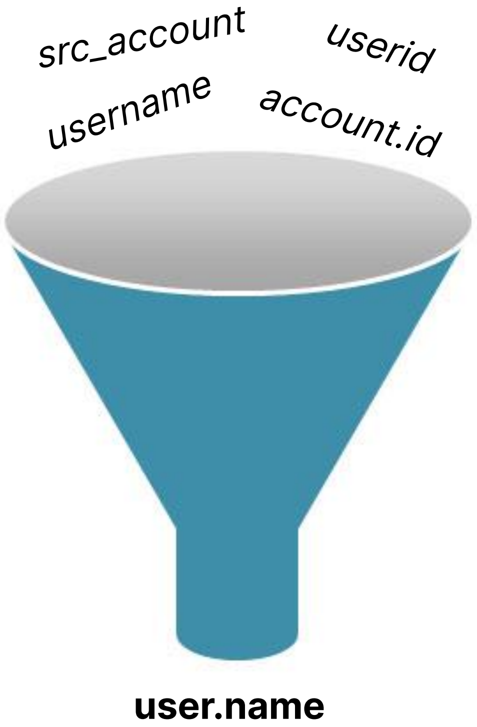
https://github.com/elastic/ecs

- 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

Elastic Common Schema

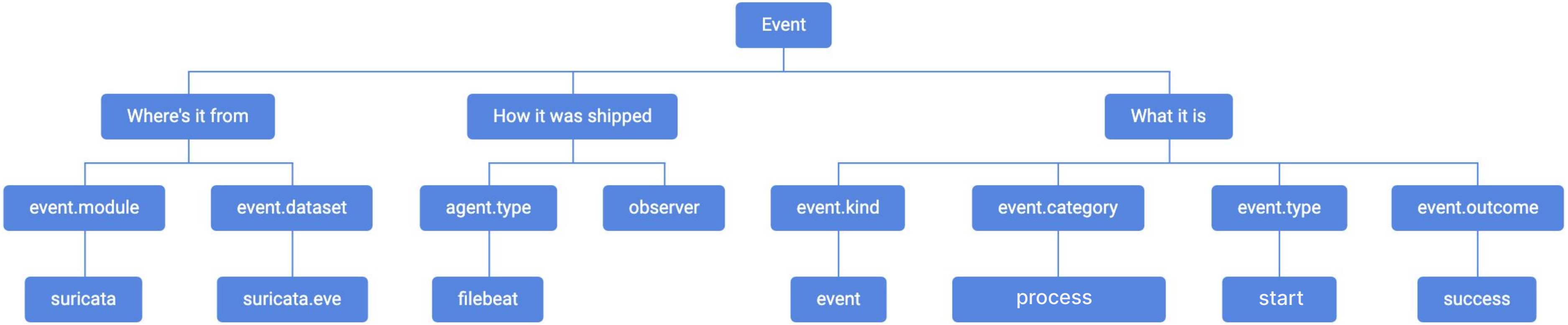
Normalization is hard — but worth it

- Reduce blind spots during analysis
- Makes it easier to remember **commonly used field names**



Elastic Common Schema

ECS - Common set of categories for inclusion in visualizations and analysis



Event

Where's it from

How it was shipped

What it is

event.module

event.dataset

agent.type

observer

event.kind

event.category

event.type

event.outcome

suricata

suricata.eve

filebeat

event

process

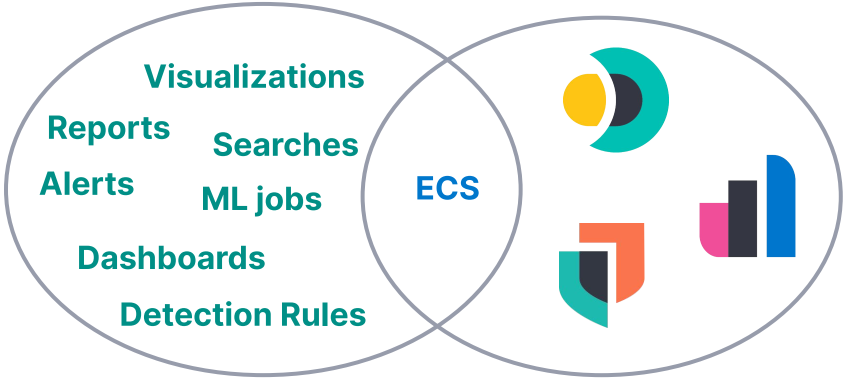
start

success

Elastic Common Schema

- Re-use analysis content across multiple data sources ♻️

- Leverage content in any environment, without modification
  - Elastic
  - Partners
  - Community



Visualizations

Reports

Searches

Alerts

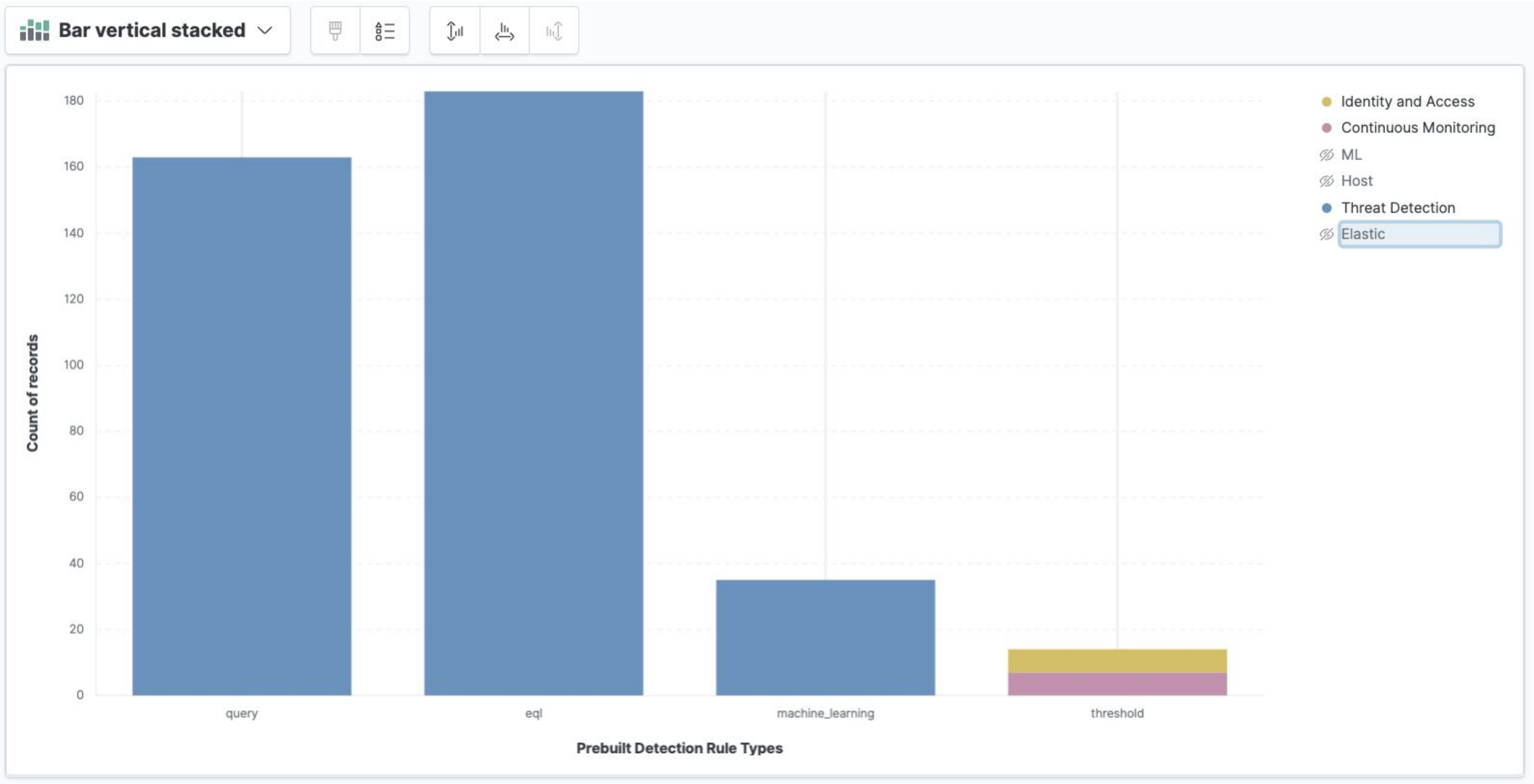
ML jobs

Dashboards

Detection Rules

ECS

Elastic Prebuilt Detection Rules



Section 3

Improve efficiency of investigation and incident response

Investigation & collaboration

Analyst-driven correlation with EQL queries

Drive ad hoc investigations by exploring the relationships between your data points

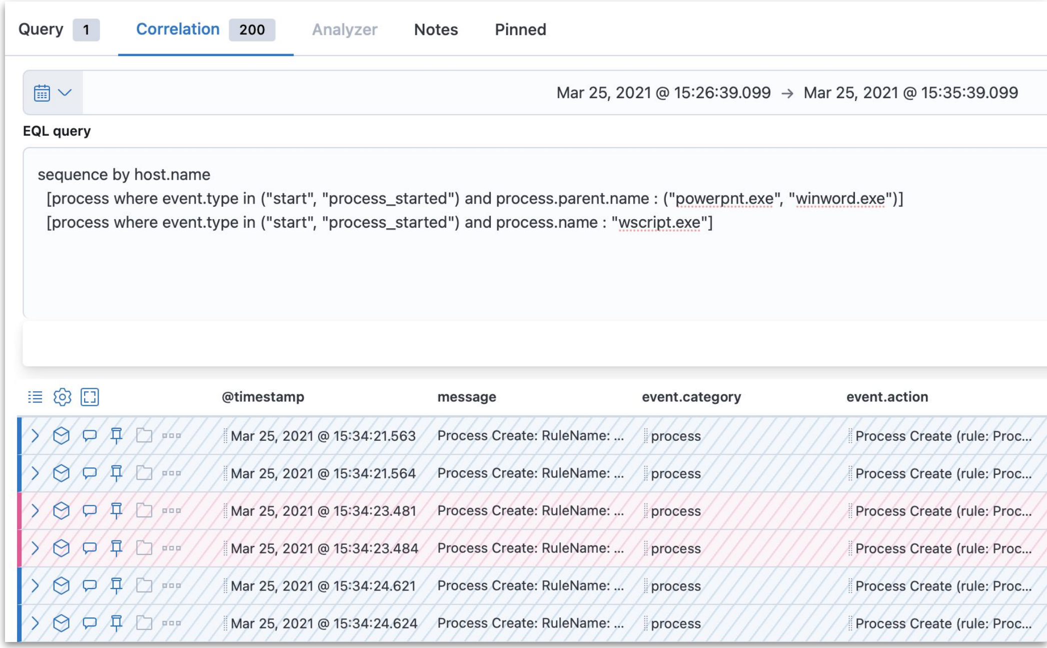
What and Why it matters

Perform comprehensive analysis with cross-index correlation

Analyze with the power of sequencing, mathematical functions and other methods

Align with organizational workflows (use from Timeline; copy-and-paste into custom detection rules)

Syntax validation simplifies adoption



Mar 25, 2021 @ 15:26:39.099 → Mar 25, 2021 @ 15:35:39.099

EQL query

```
sequence by host.name
  [process where event.type in ("start", "process_started") and process.parent.name : ("powerpnt.exe", "winword.exe")]
  [process where event.type in ("start", "process_started") and process.name : "wscript.exe"]
```

@timestamp	message	event.category	event.action
Mar 25, 2021 @ 15:34:21.563	Process Create: RuleName: ...	process	Process Create (rule: Proc...
Mar 25, 2021 @ 15:34:21.564	Process Create: RuleName: ...	process	Process Create (rule: Proc...
Mar 25, 2021 @ 15:34:23.481	Process Create: RuleName: ...	process	Process Create (rule: Proc...
Mar 25, 2021 @ 15:34:23.484	Process Create: RuleName: ...	process	Process Create (rule: Proc...
Mar 25, 2021 @ 15:34:24.621	Process Create: RuleName: ...	process	Process Create (rule: Proc...
Mar 25, 2021 @ 15:34:24.624	Process Create: RuleName: ...	process	Process Create (rule: Proc...

Standard/Basic | GA

elastic

New and deeper ServiceNow integrations

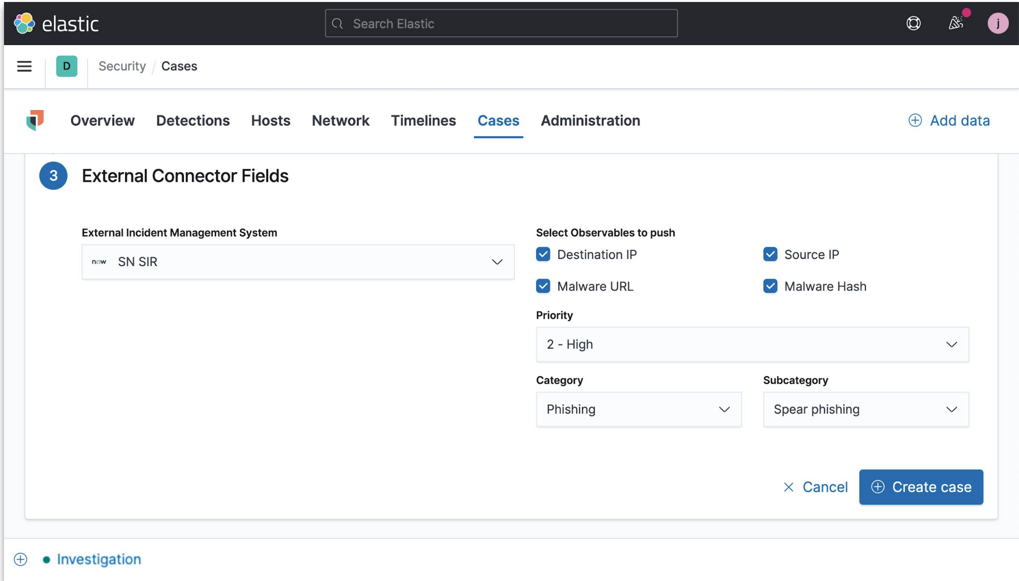
Align analysts with organizational processes, defined by existing IR/SOAR platform

What and Why it matters

Easily forward key detection observables from Elastic Security to ServiceNow SecOps

Fits into existing workflows via Elastic Security case management

Simple to configure



3 External Connector Fields

External Incident Management System: SN SIR

Select Observables to push

☑ Destination IP ☑ Source IP

☑ Malware URL ☑ Malware Hash

Priority: 2 - High

Category: Phishing

Subcategory: Spear phishing

Platinum | GA

Network and host details side panel

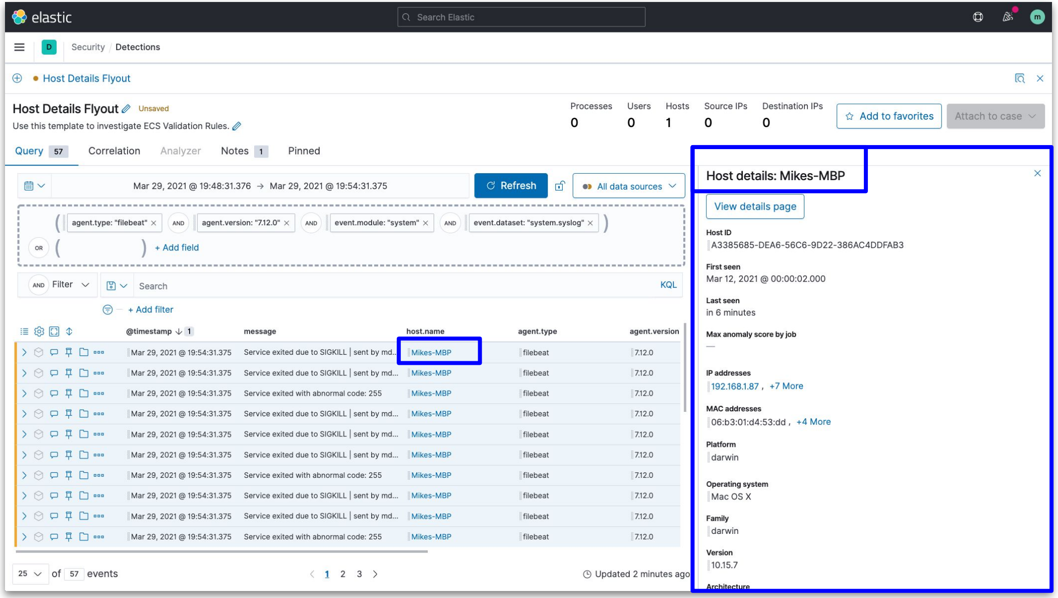
Maintain Analyst Velocity to Reduce MTTR

Host details available in Timeline

With one click, access key context while keeping focus on investigation

Easy pivot to full details for host or IP

Same familiar flyout used for Alert details



Host Details Flyout Unsaved

Use this template to investigate ECS Validation Rules.

Processes	Users	Hosts	Source IPs	Destination IPs
0	0	1	0	0

Mar 29, 2021 @ 19:48:31.376 → Mar 29, 2021 @ 19:54:31.375

(agent.type: "filebeat" AND agent.version: "7.12.0" AND event.module: "system" AND event.dataset: "system.syslog")
OR ( ) + Add field

@timestamp ↓ 1	message	host.name	agent.type	agent.version
Mar 29, 2021 @ 19:54:31.375	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited with abnormal code: 255	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited with abnormal code: 255	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat	7.12.0
Mar 29, 2021 @ 19:54:31.375	Service exited with abnormal code: 255	Mikes-MBP	filebeat	7.12.0

25 of 57 events

Updated 2 minutes ago

Host details: Mikes-MBP

Host ID
A3385685-DEA6-56C6-9D22-386AC4DDFAB3

First seen
Mar 12, 2021 @ 00:00:02.000

Last seen
in 6 minutes

Max anomaly score by job
—

IP addresses
192.168.1.87 , +7 More

MAC addresses
06:b3:01:d4:53:dd , +4 More

Platform
darwin

Operating system
Mac OS X

Family
darwin

Version
10.15.7

Architecture

Standard/Basic | GA

Network and host details side panel

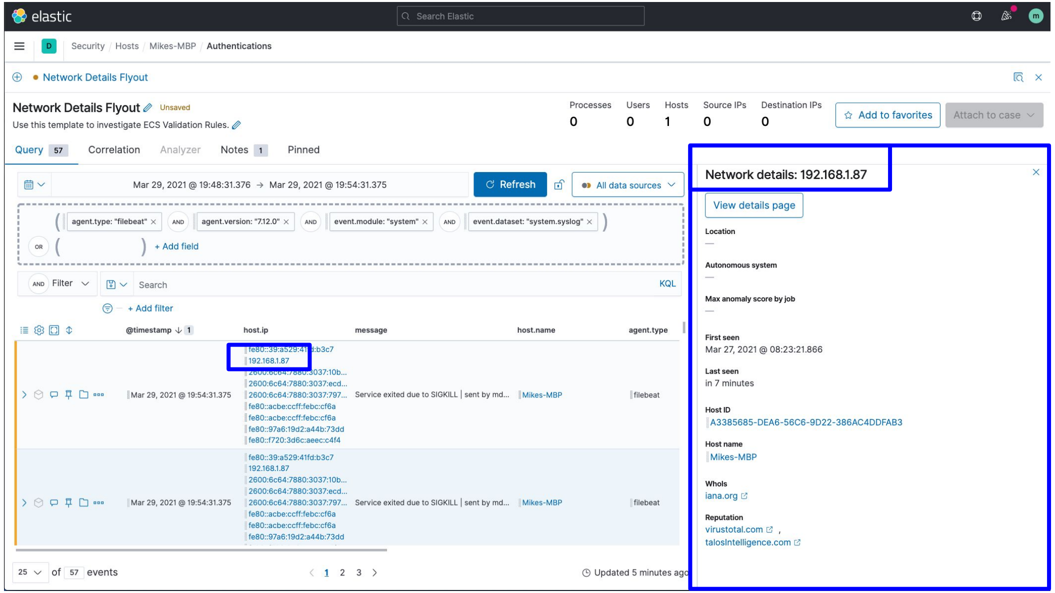
Maintain Analyst Velocity to Reduce MTTR

Network details available in Timeline

Analysts get 1-click context about host or IP address while keeping focus on investigation

Easy pivot to full details for host or IP

Same familiar flyout used for Alert details



Network Details Flyout Unsaved

Use this template to investigate ECS Validation Rules.

Processes	Users	Hosts	Source IPs	Destination IPs
0	0	1	0	0

Mar 29, 2021 @ 19:48:31.376 → Mar 29, 2021 @ 19:54:31.375

(agent.type: "filebeat" AND agent.version: "7.12.0" AND event.module: "system" AND event.dataset: "system.syslog")
OR ( ) + Add field

@timestamp ↓ 1	host.ip	message	host.name	agent.type
Mar 29, 2021 @ 19:54:31.375	fe80::39:a529:41fd:b3c7 192.168.1.87 2600:6c64:7880:3037:10b... 2600:6c64:7880:3037:ecd... 2600:6c64:7880:3037:797... fe80::acbe:ccff:febc:cf6a fe80::acbe:ccff:febc:cf6a fe80::97a6:19d2:a44b:73dd fe80::f720:3d6c:aeec:c4f4	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat
Mar 29, 2021 @ 19:54:31.375	fe80::39:a529:41fd:b3c7 192.168.1.87 2600:6c64:7880:3037:10b... 2600:6c64:7880:3037:ecd... 2600:6c64:7880:3037:797... fe80::acbe:ccff:febc:cf6a fe80::acbe:ccff:febc:cf6a fe80::97a6:19d2:a44b:73dd	Service exited due to SIGKILL | sent by md...	Mikes-MBP	filebeat

25 of 57 events

Updated 5 minutes ago

Network details: 192.168.1.87

Location
—

Autonomous system
—

Max anomaly score by job
—

First seen
Mar 27, 2021 @ 08:23:21.866

Last seen
in 7 minutes

Host ID
A3385685-DEA6-56C6-9D22-386AC4DDFAB3

Host name
Mikes-MBP

WhoIs
iana.org

Reputation
virustotal.com ,
talosIntelligence.com

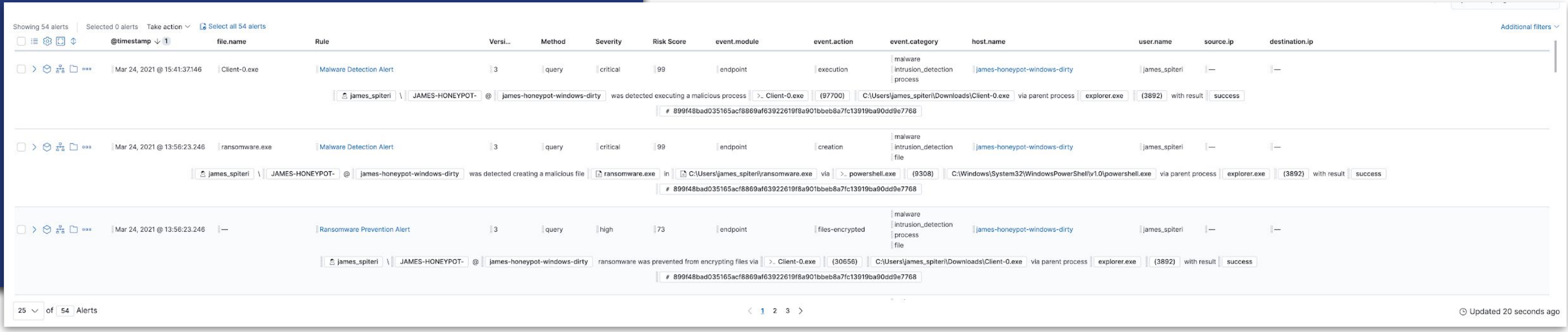
Standard/Basic | GA

Analyst-friendly rendering for Endpoint events

Close Up

Arm every analyst - maintain analyst velocity

All get the built-in, analyst friendly, easy-to-read, story-like presentation in timeline investigation experience



Showing 54 alerts | Selected 0 alerts | Take action | Select all 54 alerts | Additional filters

@timestamp ↓ 1	file.name	Rule	Versi...	Method	Severity	Risk Score	event.module	event.action	event.category	host.name	user.name	source.ip	destination.ip
Mar 24, 2021 @ 15:41:37.146	Client-0.exe	Malware Detection Alert	3	query	critical	99	endpoint	execution	malware intrusion_detection process	james-honeypot-windows-dirty	james_spiteri	—	—
Mar 24, 2021 @ 13:56:23.246	ransomware.exe	Malware Detection Alert	3	query	critical	99	endpoint	creation	malware intrusion_detection file	james-honeypot-windows-dirty	james_spiteri	—	—
Mar 24, 2021 @ 13:56:23.246	—	Ransomware Prevention Alert	3	query	high	73	endpoint	files-encrypted	malware intrusion_detection process file	james-honeypot-windows-dirty	james_spiteri	—	—

james_spiteri \ JAMES-HONEYPOT- @ james-honeypot-windows-dirty was detected executing a malicious process >_ Client-0.exe (97700) C:\Users\james_spiteri\Downloads\Client-0.exe via parent process explorer.exe (3892) with result success
899f48bad035165acf8869af63922619f8a901bbeb8a7fc13919ba90dd9e7768

james_spiteri \ JAMES-HONEYPOT- @ james-honeypot-windows-dirty was detected creating a malicious file ransomware.exe in C:\Users\james_spiteri\ransomware.exe via >_ powershell.exe (9308) C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe via parent process explorer.exe (3892) with result success
899f48bad035165acf8869af63922619f8a901bbeb8a7fc13919ba90dd9e7768

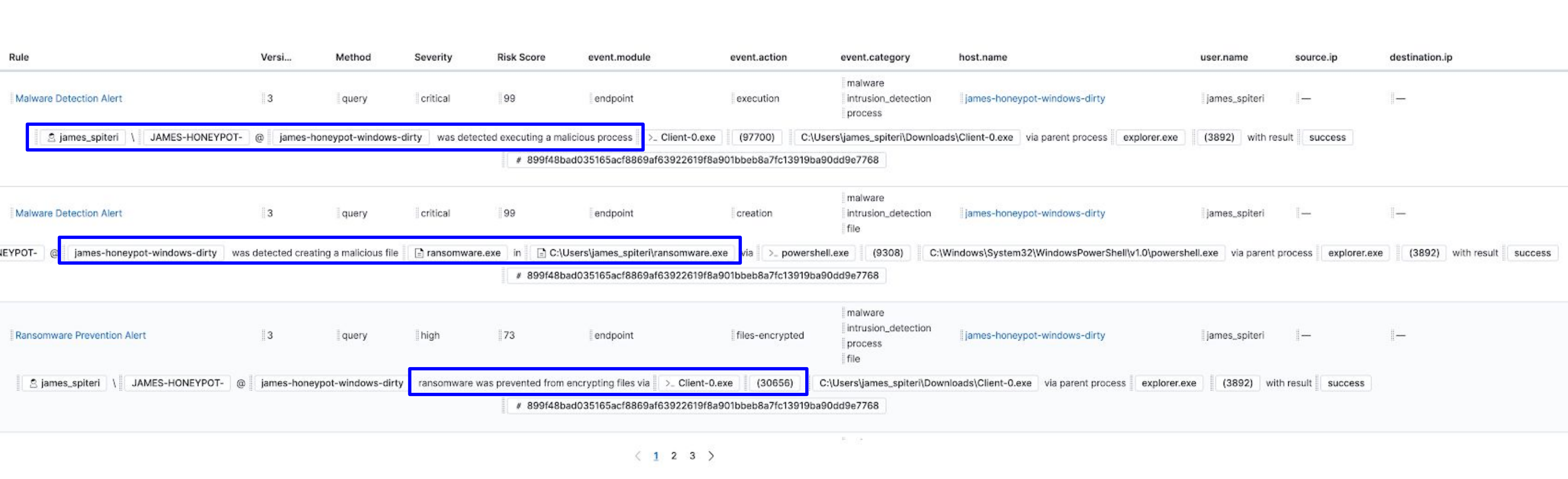
james_spiteri \ JAMES-HONEYPOT- @ james-honeypot-windows-dirty ransomware was prevented from encrypting files via >_ Client-0.exe (30656) C:\Users\james_spiteri\Downloads\Client-0.exe via parent process explorer.exe (3892) with result success
899f48bad035165acf8869af63922619f8a901bbeb8a7fc13919ba90dd9e7768

25 of 54 Alerts | 1 2 3 | Updated 20 seconds ago

Standard/Basic | GA

Analyst-friendly rendering for Endpoint events

Close-up



Rule	Versi...	Method	Severity	Risk Score	event.module	event.action	event.category	host.name	user.name	source.ip	destination.ip
Malware Detection Alert	3	query	critical	99	endpoint	execution	malware intrusion_detection process	james-honeypot-windows-dirty	james_spiteri	—	—
Malware Detection Alert	3	query	critical	99	endpoint	creation	malware intrusion_detection file	james-honeypot-windows-dirty	james_spiteri	—	—
Ransomware Prevention Alert	3	query	high	73	endpoint	files-encrypted	malware intrusion_detection process file	james-honeypot-windows-dirty	james_spiteri	—	—

james_spiteri \ JAMES-HONEYPOT- @ james-honeypot-windows-dirty was detected executing a malicious process >_ Client-0.exe (97700) C:\Users\james_spiteri\Downloads\Client-0.exe via parent process explorer.exe (3892) with result success

# 899f48bad035165acf8869af63922619f8a901bbeb8a7fc13919ba90dd9e7768

EYPOT- @ james-honeypot-windows-dirty was detected creating a malicious file ransomware.exe in C:\Users\james_spiteri\ransomware.exe via >_ powershell.exe (9308) C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe via parent process explorer.exe (3892) with result success

# 899f48bad035165acf8869af63922619f8a901bbeb8a7fc13919ba90dd9e7768

james_spiteri \ JAMES-HONEYPOT- @ james-honeypot-windows-dirty ransomware was prevented from encrypting files via >_ Client-0.exe (30656) C:\Users\james_spiteri\Downloads\Client-0.exe via parent process explorer.exe (3892) with result success

# 899f48bad035165acf8869af63922619f8a901bbeb8a7fc13919ba90dd9e7768

‹ 1 2 3 ›

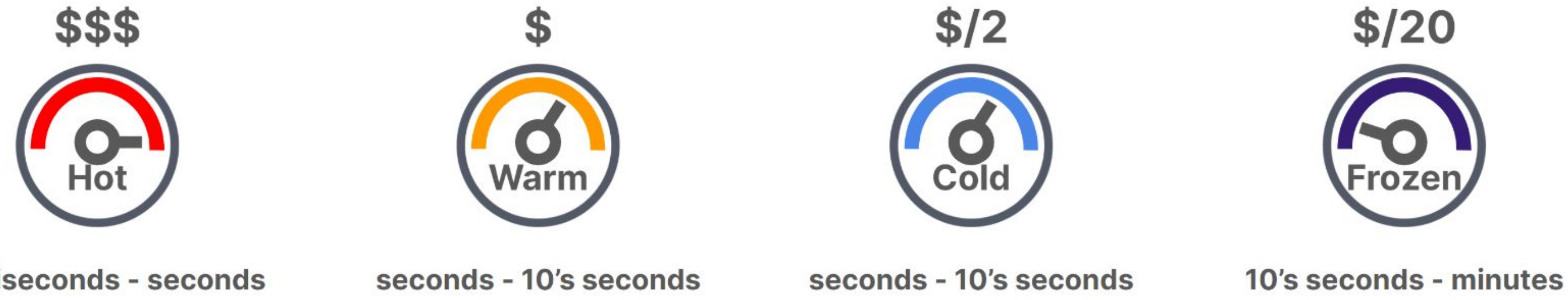
Standard/Basic | GA

Section 4

Gain control of your security data with data tiers

Performance and cost

Control your data with Elastic data tiers



$$$	$	$/2	$/20
Hot	Warm	Cold	Frozen
milliseconds - seconds	seconds - 10’s seconds	seconds - 10’s seconds	10’s seconds - minutes

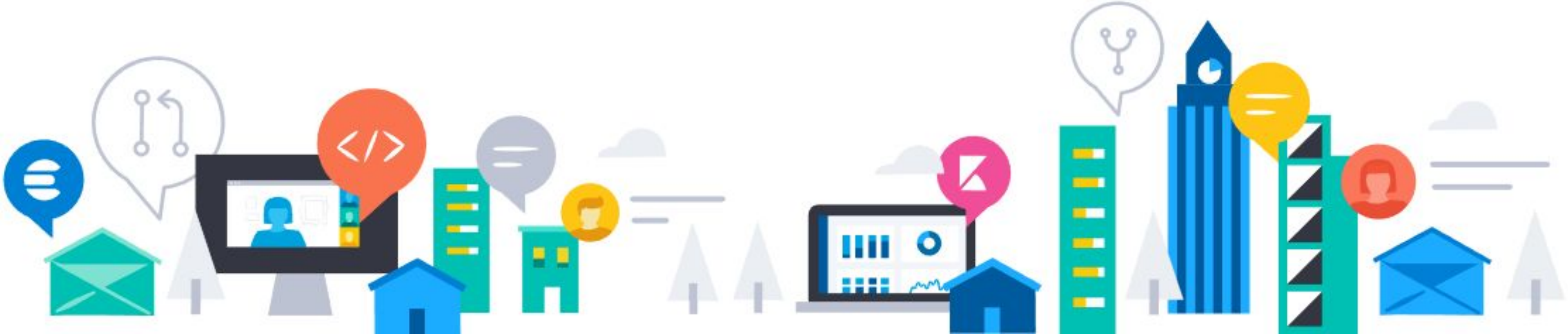
Note: Frozen tier is in Technical Preview

Join the Elastic Security community

Take a quick spin:
demo.elastic.co

Try free on Cloud:
ela.st/siem

Connect on Slack:
ela.st/slack



Questions