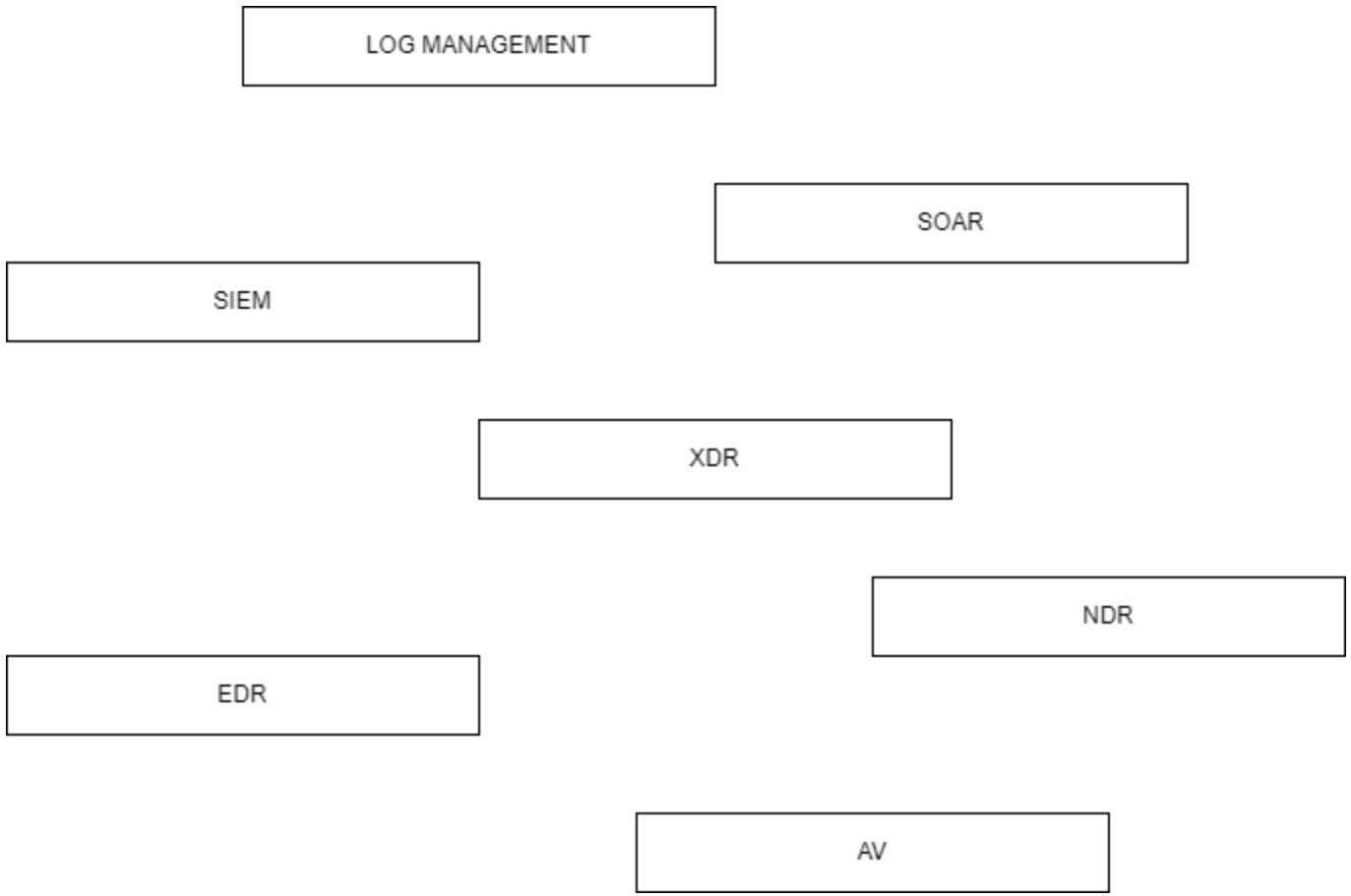
Elasticsearch jako řešení pro bezpečnostní dohled

Jindřich Němec


LOG MANAGEMENT
SOAR
SIEM
XDR
NDR
EDR
AV

Shay Banon

Founder & CTO at Elastic

San Francisco Bay Area · Contact info

Elastic

Connect | Message | More

Activity

846 followers

Shay hasn't posted lately

Shay's recent posts and comments will be displayed here.

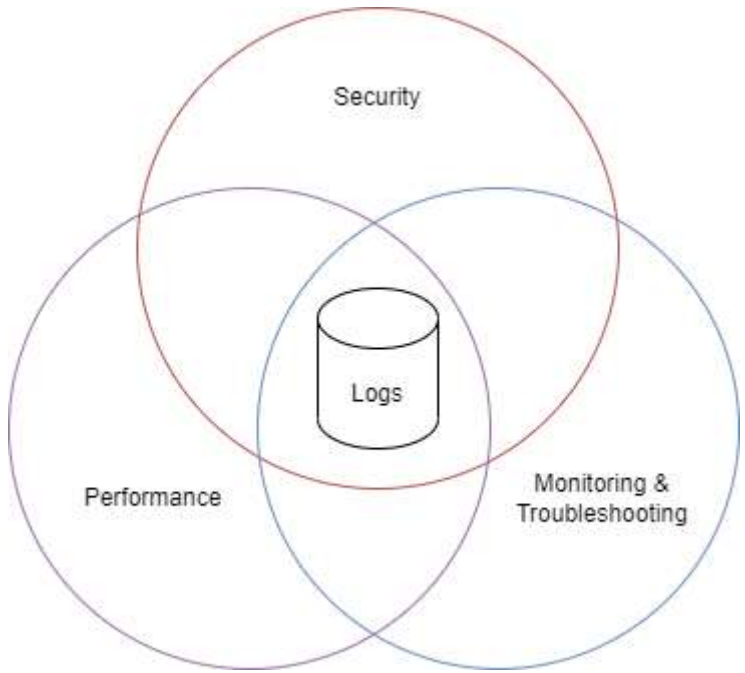
Show all activity →

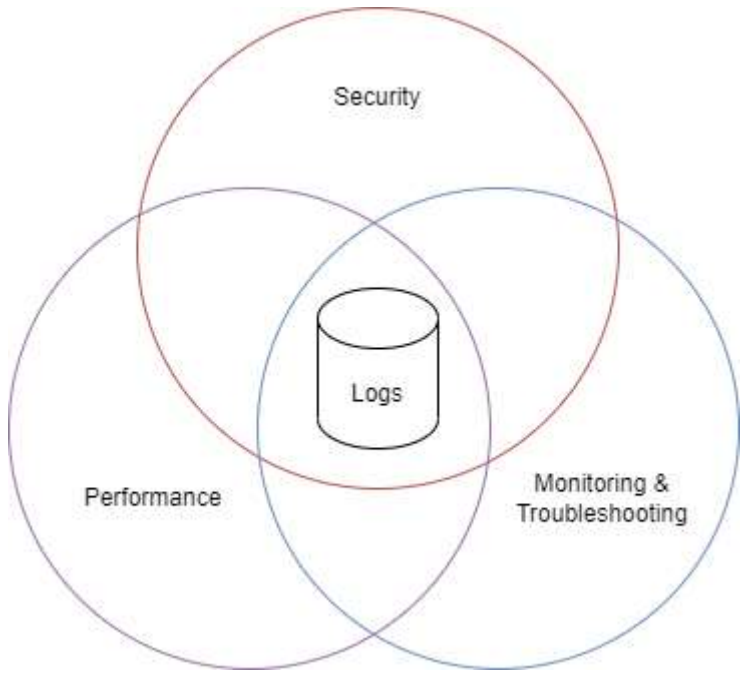
Experience

Chief Technology Officer

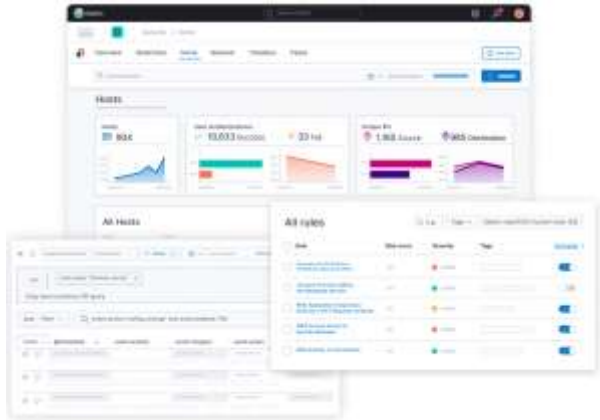
Elastic

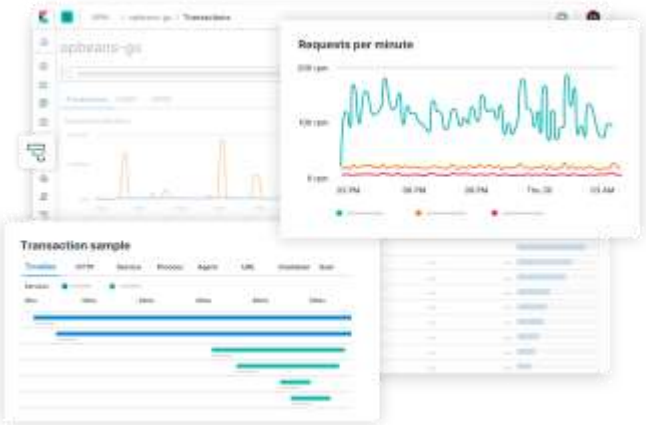
May 2012 - Present · 11 yrs

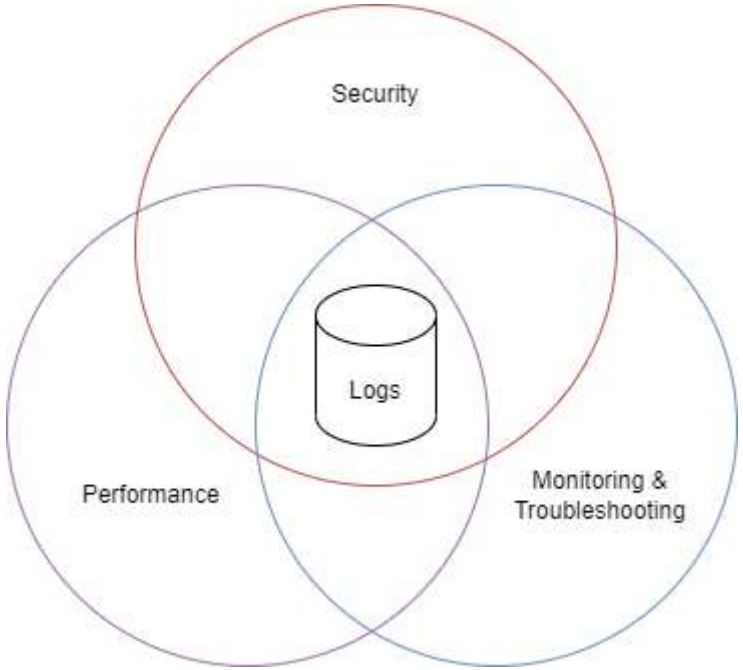

Security
Logs
Performance
Monitoring &
Troubleshooting

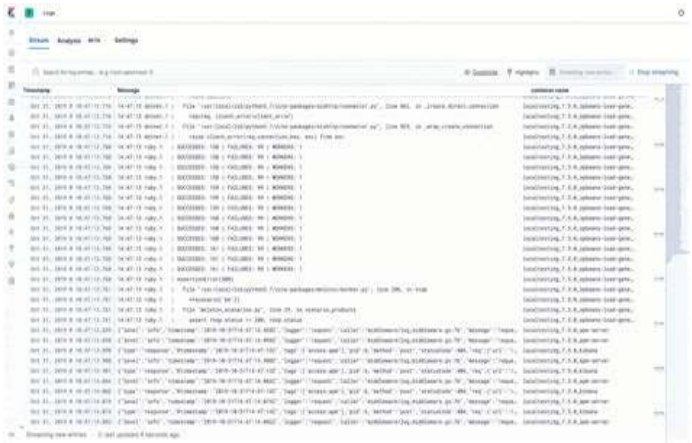

Security
Logs
Performance
Monitoring &
Troubleshooting

Elastic Stack



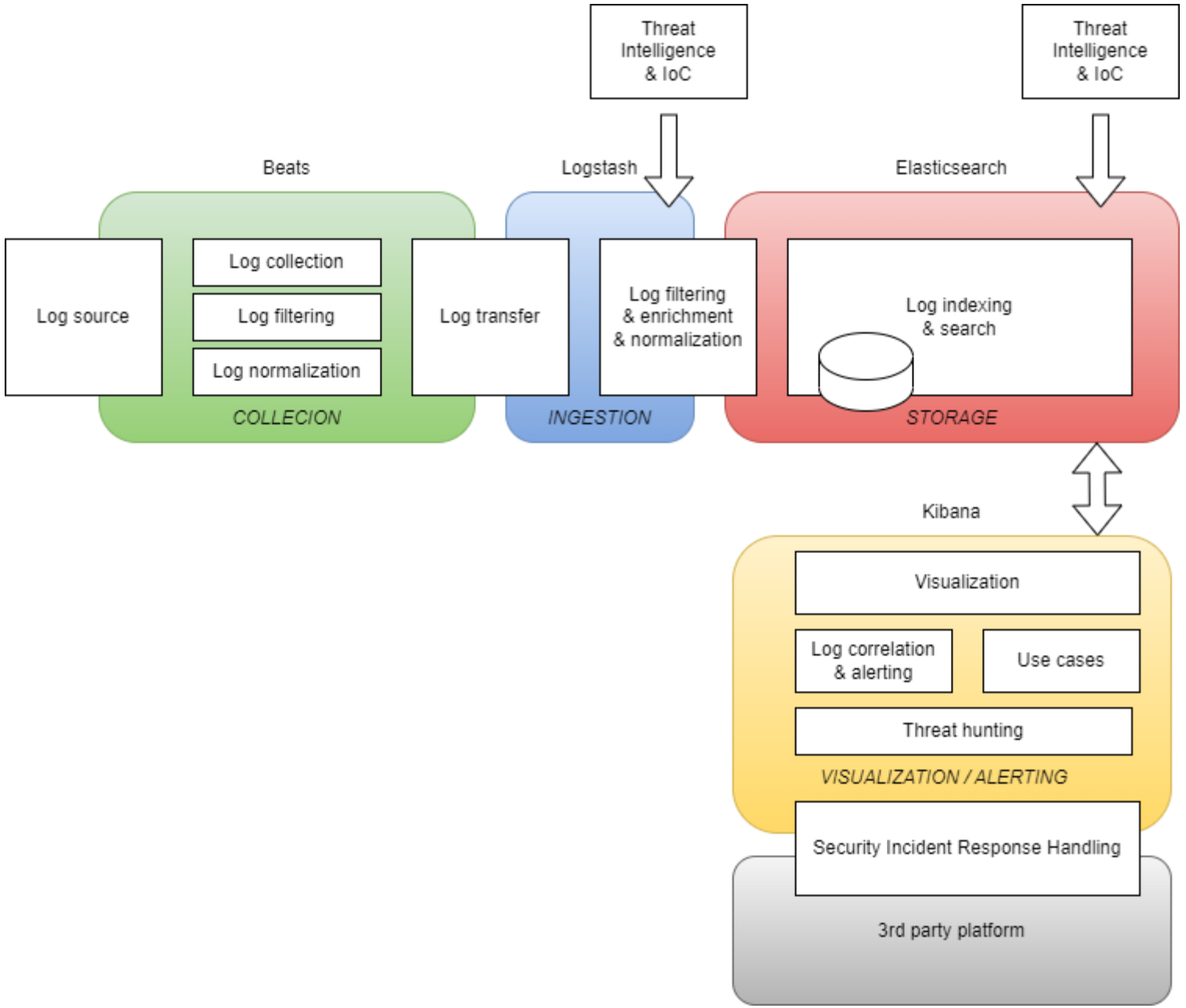


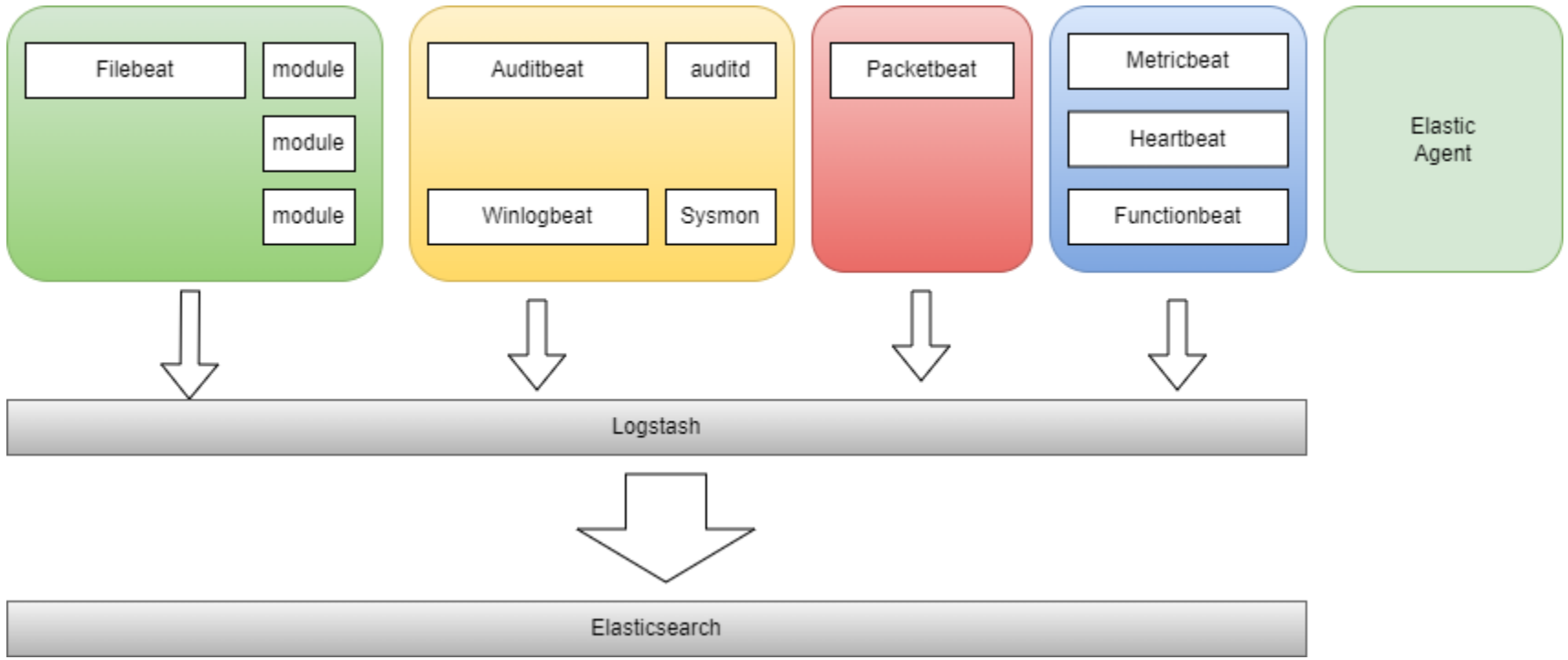


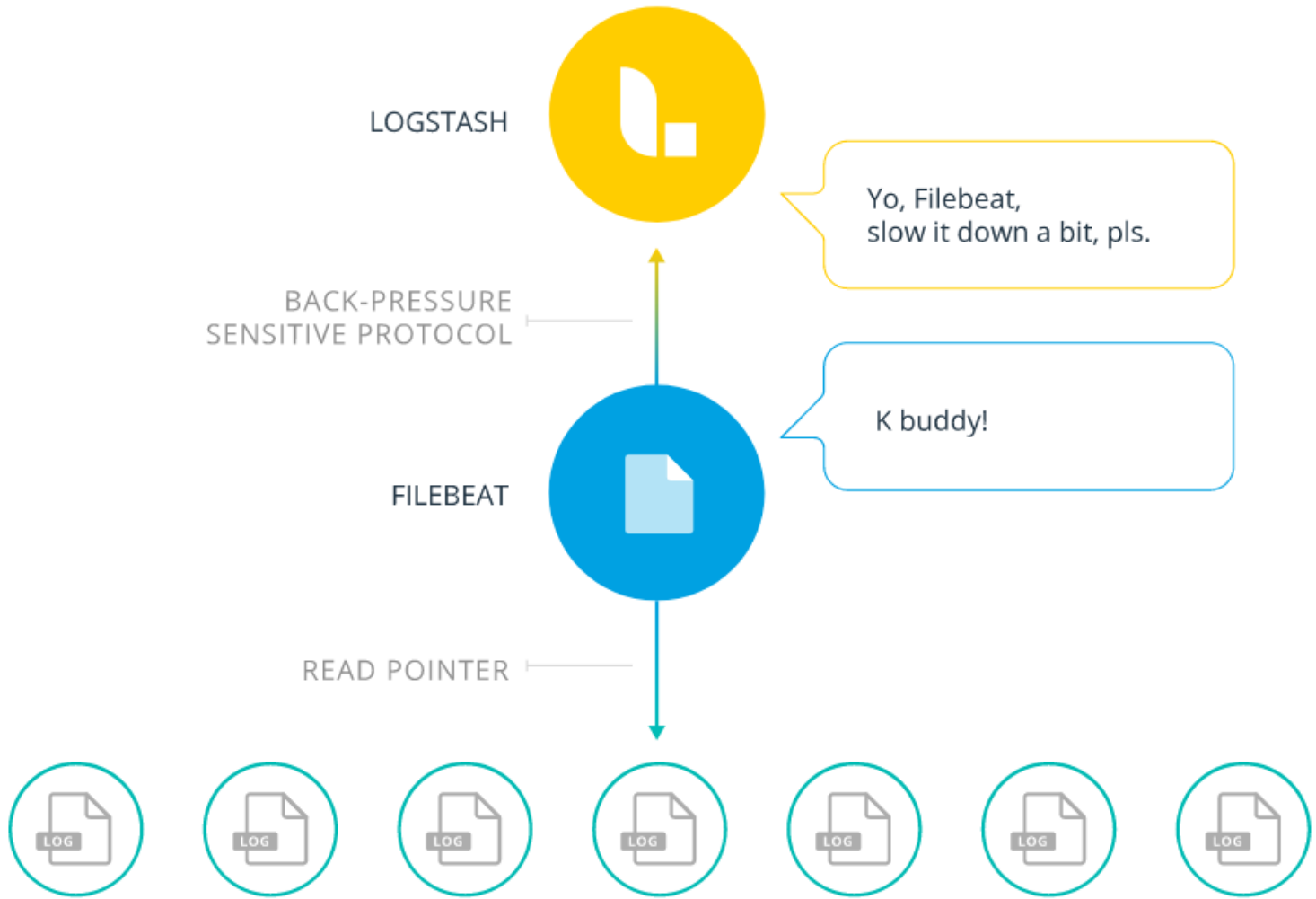


Magic Quadrant for Security Information and Event Management

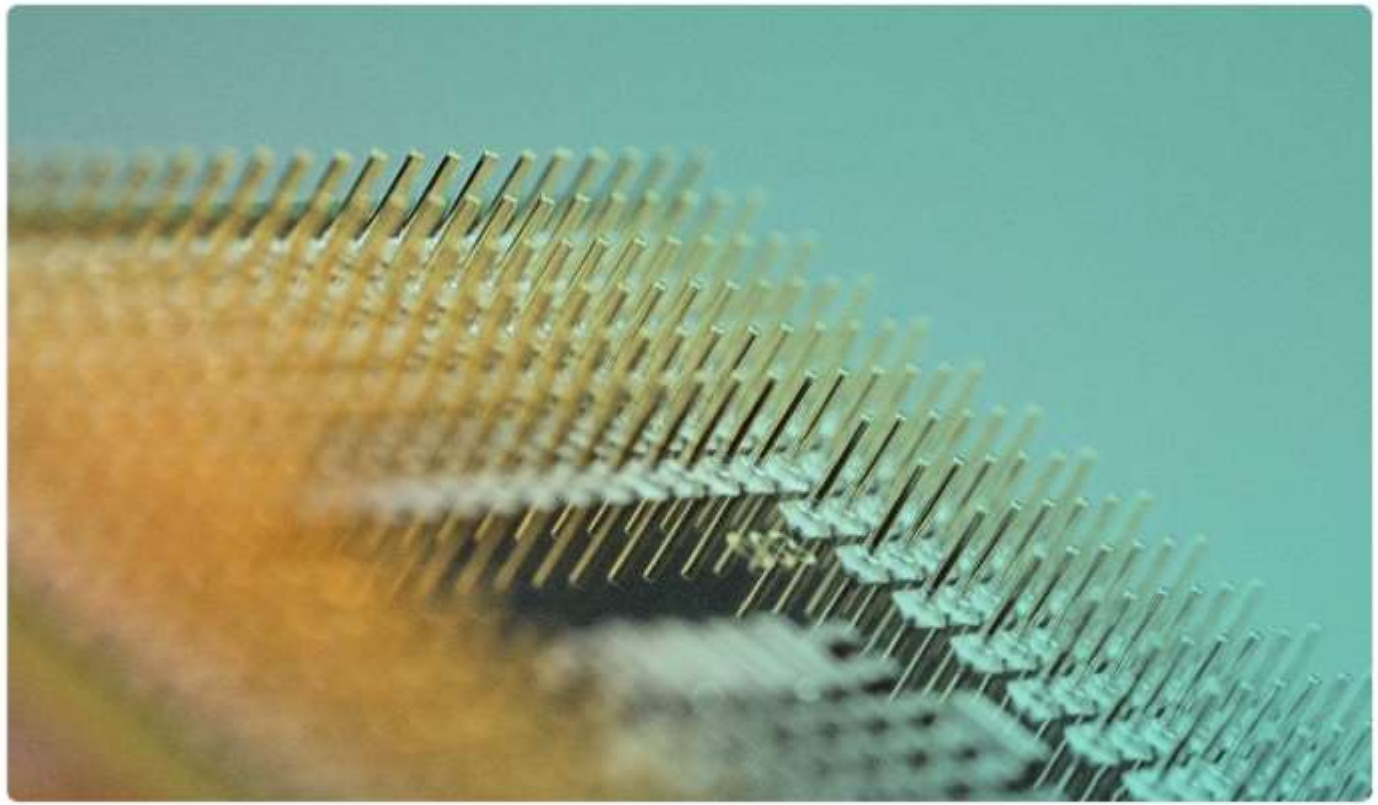
Elastic Stack




Filebeat
module
module
module
Auditbeat
auditd
Winlogbeat
Sysmon
Packetbeat
Metricbeat
Heartbeat
Functionbeat
Elastic
Agent
Logstash
Elasticsearch


LOGSTASH
Yo, Filebeat,
slow it down a bit, pls.
BACK-PRESSURE
SENSITIVE PROTOCOL
K buddy!
FILEBEAT
READ POINTER
LOG
LOG
LOG
LOG
LOG
LOG
LOG
THE ORIGINAL LOG LINES ACT LIKE A QUEUE

Ingesting threat data with the Threat Intel Filebeat module

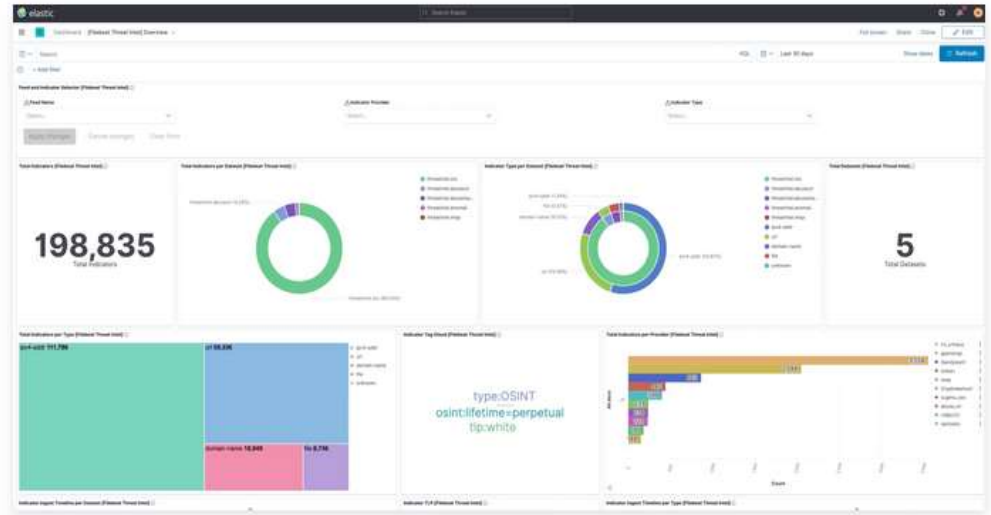


The ability for security teams to integrate threat data into their operations substantially helps their organization identify potentially malicious endpoint and network events using indicators identified by other threat research teams. In this blog, we'll cover how to ingest threat data with the Threat Intel Filebeat module. In future blog posts, we'll cover enriching threat data with the Threat ECS fieldset and

Using these capabilities, the Threat Intel Filebeat module:

- Consumes threat data from six open source feeds
- Loads threat data into Elasticsearch
- Normalizes threat data into the Threat ECS fieldset
- Enables threat analysis through dashboards and visualizations

Analysts and threat hunters can use this data for raw threat hunting, enrichment, intelligence analysis and production, and detection logic.



The six feeds included with the 7.13 Filebeat Threat Intel module are as follows (additional feeds may be added in the future):

- Abuse.ch Malware
- Abuse.ch URL
- AlienVault Open Threat Exchange (OTX)
- Anomali Limo
- Malware Bazaar
- Malware Information Sharing Platform (MISP)

F5 module
Fortinet module
Google Cloud module
Google Workspace module
HAproxy module
IBM MQ module
Icinga module
IIS module
Imperva module
Infoblox module
Iptables module
Juniper module
Kafka module
Kibana module
Logstash module
Microsoft module
MISP module
MongoDB module
MSSQL module
MySQL module
MySQL Enterprise module
NATS module
NetFlow module
Netscout module
Nginx module
Office 365 module
Okta module
Oracle module
Osquery module
Palo Alto Networks module

F5 module

WARNING This functionality is in technical preview and may be changed or removed in a future release. Elastic will apply best effort to fix any issues, but features in technical preview are not subject to the support SLA of official GA features.

Prefer to use Elastic Agent for this use case?

Refer to the Elastic Integrations documentation.

▸ Learn more

This is a module for F5 network device's logs. It includes the following filesets for receiving logs over syslog or read from a file:

- `bigipapm` fileset: supports F5 Big-IP Access Policy Manager.
- `bigipafm` fileset: supports F5 Big-IP Advanced Firewall Manager.

TIP Read the quick start to learn how to configure and run modules.

Configure the module

You can further refine the behavior of the `f5` module by specifying variable settings in the `modules.d/f5.yml` file, or overriding settings at the command line.

You must enable at least one fileset in the module. **Filesets are disabled by default.**

Variable settings

Each fileset has separate variable settings for configuring the behavior of the module. If you don't specify variable settings, the `f5` module uses the defaults.

For advanced use cases, you can also override input settings. See Override input settings.

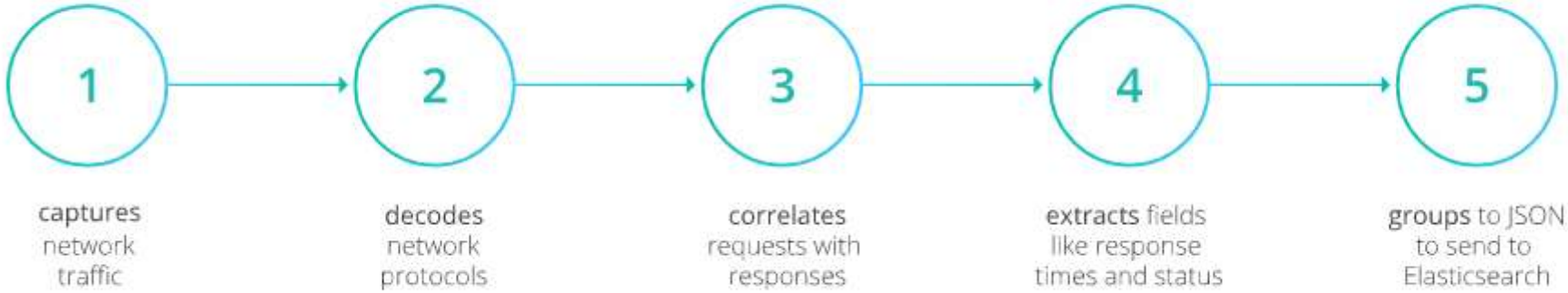
TIP When you specify a setting at the command line, remember to prefix the setting with the module name, for example, `f5.bigipapm.var.paths` instead of `bigipapm.var.paths`.

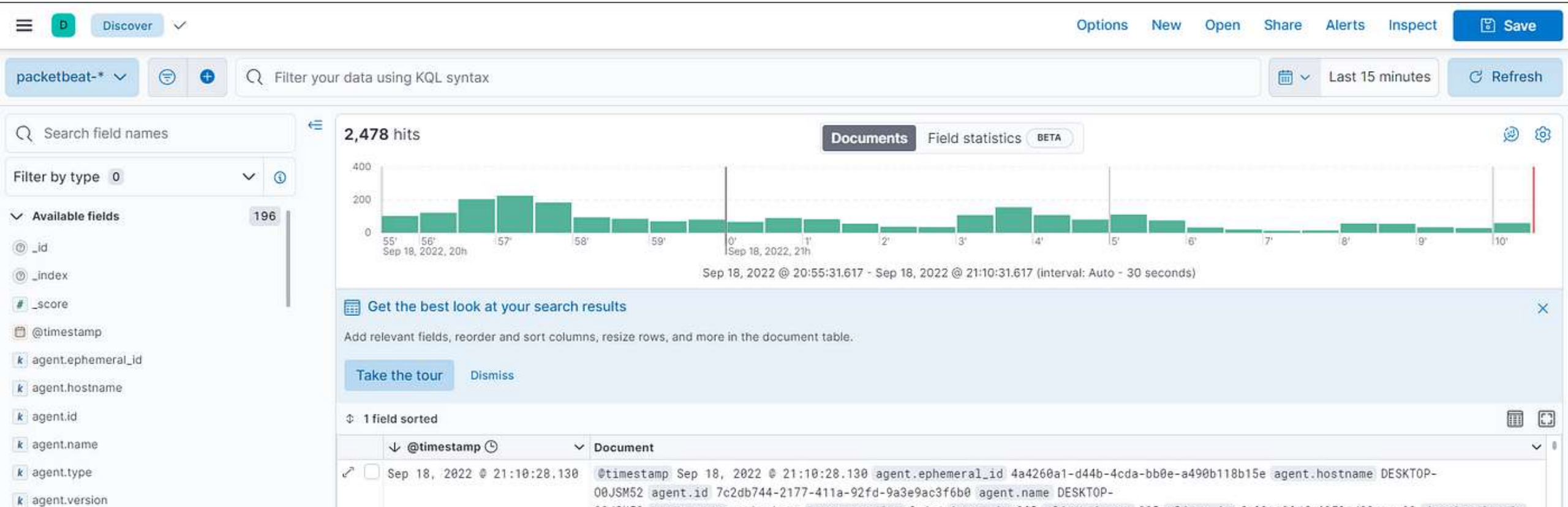
On this page

Configure the module
Variable settings
bigipapm fileset settings
bigipafm fileset settings
Fields

Beats

Packetbeat





Beats

Auditbeat

elastic

Search Elastic

Discover > auditbeat: file integrity

New Save Open Share Inspect

Search KQL Last 7 days Show dates Refresh

event.module: file_integrity × file.path: /etc/shadow × + Add filter

auditbeat-*

Search field names

Filter by type 0

Selected fields 3

- host.name
- file.path
- event.action

Available fields 48

Popular

- agent.name
- event.category
- host.hostname
- _id
- _index
- _score
- _type
- @timestamp
- @version
- agent.ephemeral_id
- agent.hostname
- agent.id
- agent.type
- agent.version
- ecs.version
- error.message
- event.dataset

19 hits Reset search Apr 17, 2023 @ 00:00:00.000 - Apr 24, 2023 @ 16:43:52.271 Auto Hide chart

Time	host.name	file.path	event.action
Apr 23, 2023 @ 03:02:29.223	[redacted]	/etc/shadow	attributes_modified
Apr 22, 2023 @ 23:03:39.363		/etc/shadow	attributes_modified
Apr 22, 2023 @ 21:04:33.912		/etc/shadow	attributes_modified
Apr 22, 2023 @ 21:03:24.840		/etc/shadow	attributes_modified
Apr 22, 2023 @ 16:03:14.652		/etc/shadow	attributes_modified
Apr 22, 2023 @ 16:02:43.869		/etc/shadow	attributes_modified
Apr 22, 2023 @ 16:02:25.445		/etc/shadow	attributes_modified
Apr 22, 2023 @ 16:02:23.903		/etc/shadow	attributes_modified
Apr 22, 2023 @ 16:02:23.414		/etc/shadow	attributes_modified
Apr 22, 2023 @ 10:16:53.731		/etc/shadow	attributes_modified
Apr 22, 2023 @ 01:32:11.987		/etc/shadow	attributes_modified
Apr 17, 2023 @ 11:16:37.154		/etc/shadow	updated, attributes_modified
Apr 17, 2023 @ 05:33:08.909		/etc/shadow	attributes_modified
Apr 17, 2023 @ 05:33:06.905		/etc/shadow	attributes_modified

Filter for value

Beats

Auditbeat

Discover > auditbeat: executed

New Save Open Share Inspect

Search KQL Last 7 days Show dates Refresh

event.action: executed × + Add filter

auditbeat-*

Search field names

Filter by type 0

Selected fields 6

- host.name
- auditd.summary.actor.primary
- process.args
- process.working_directory
- user.group.name
- user.name

Available fields 89

Popular

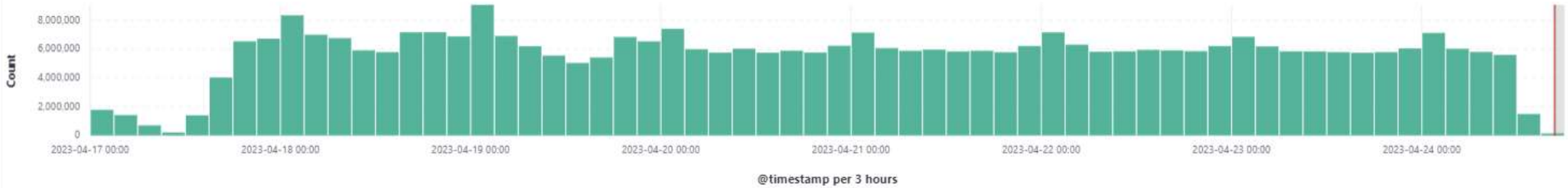
- agent.name
- event.action
- event.category
- event.module
- file.path
- host.hostname

- _id
- _index
- _score
- _type
- @timestamp
- @version
- agent.ephemeral_id
- agent.hostname
- agent.id

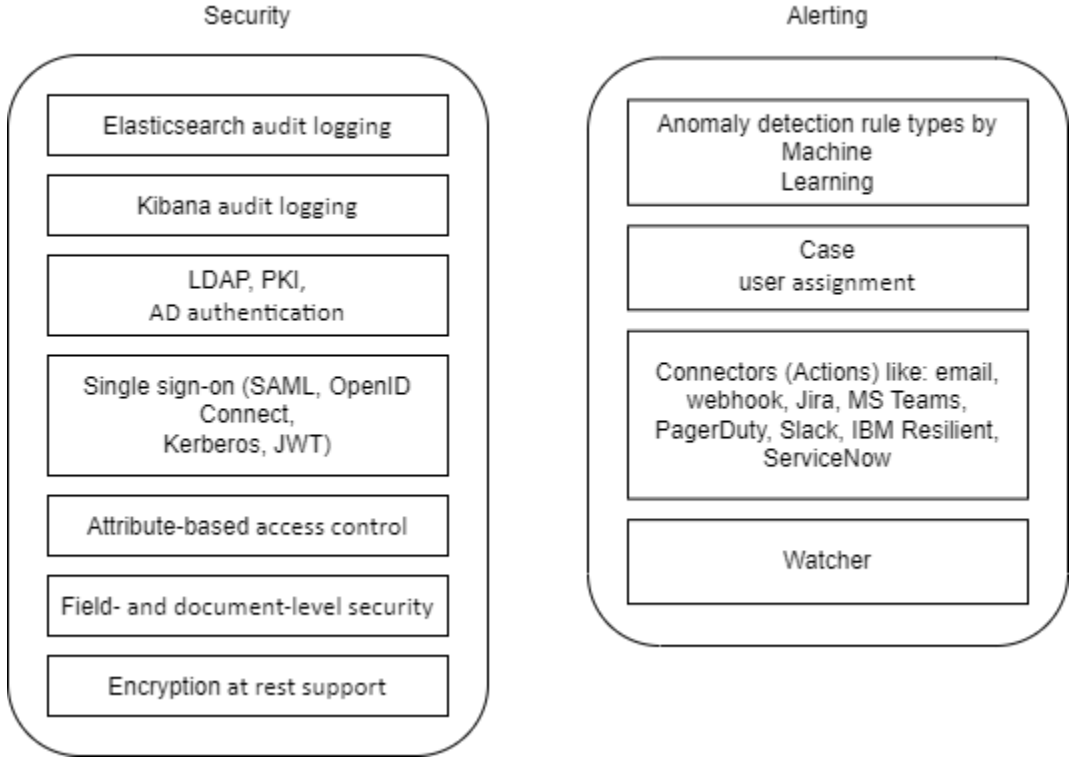
350,666,776 hits Reset search

Apr 17, 2023 @ 00:00:00.000 - Apr 24, 2023 @ 16:46:07.105 Auto

Hide chart

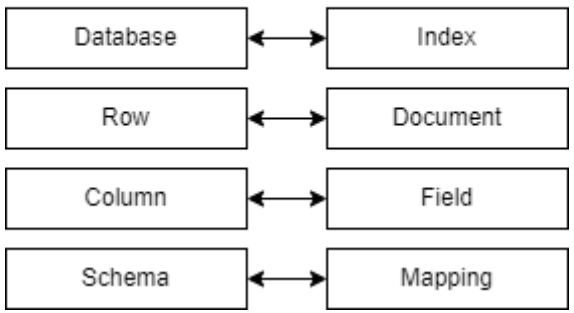


Time	host.name	auditd.summary.actor.primary	process.args	process.working_directory	user.group.name	user.name
Apr 24, 2023 @ 15:41:04.267	[redacted]	kubao99	/oracle/middleware/web12213/wlserver/../ohs/bin/launch, -p, 36766	/appl3w/oracle/wlsdomain/ohs/nodemanager	dba	oracle
Apr 24, 2023 @ 15:41:01.562		nagios	uname, -m	/home/nagios	nagios	nagios
Apr 24, 2023 @ 15:41:01.520		nagios	ls, /etc/bash_completion.d	/home/nagios	nagios	nagios
Apr 24, 2023 @ 15:41:01.509		nagios	/usr/bin/logname	/home/nagios	nagios	nagios
Apr 24, 2023 @ 15:41:01.508		nagios	/usr/bin/logname	/home/nagios	nagios	nagios
Apr 24, 2023 @ 15:41:01.507		nagios	/usr/bin/test, -z, tlidmas1	/home/nagios	nagios	nagios
Apr 24, 2023 @ 15:41:01.505		nagios	hostname	/home/nagios	nagios	nagios
Apr 24, 2023 @ 15:41:01.504		nagios	/usr/bin/test, 10000, =, 0	/home/nagios	nagios	nagios
Apr 24, 2023 @ 15:41:01.501		nagios	/bin/sh, /usr/bin/egrep, (^dba$\|^dba\|dba\|dba$)	/home/nagios	nagios	nagios
Apr 24, 2023 @ 15:41:01.499		nagios	grep, -E, (^postgres$\|^postgres\|postgres\|postgres$)	/home/nagios	nagios	nagios



	Free and open - Basic [1, 2]	Platinum	Enterprise	Gold (Discontinued)[9]
ELASTIC STACK OPERATIONS & MANAGEMENT				
Storage types				
Inverted index (for search)	✓	✓	✓	✓
Evaluating calculated fields at index time	✓	✓	✓	✓
Runtime fields	✓	✓	✓	✓

Relační DB vs. Elasticsearch

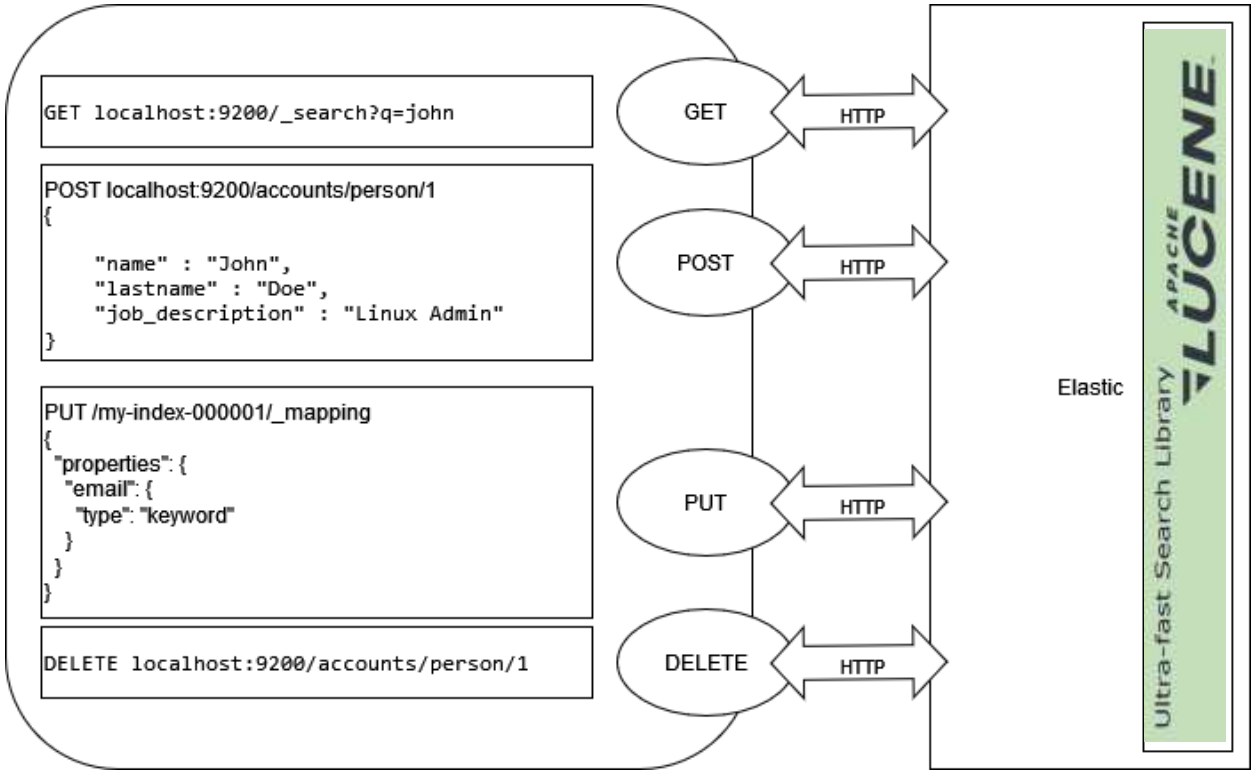


XML

```
<empinfo>
   <employees>
      <employee>
         <name>James Kirk</name>
         <age>40></age>
      </employee>
      <employee>
         <name>Jean-Luc Picard</name>
         <age>45</age>
      </employee>
      <employee>
         <name>Wesley Crusher</name>
         <age>27</age>
      </employee>
   </employees>
</empinfo>
```

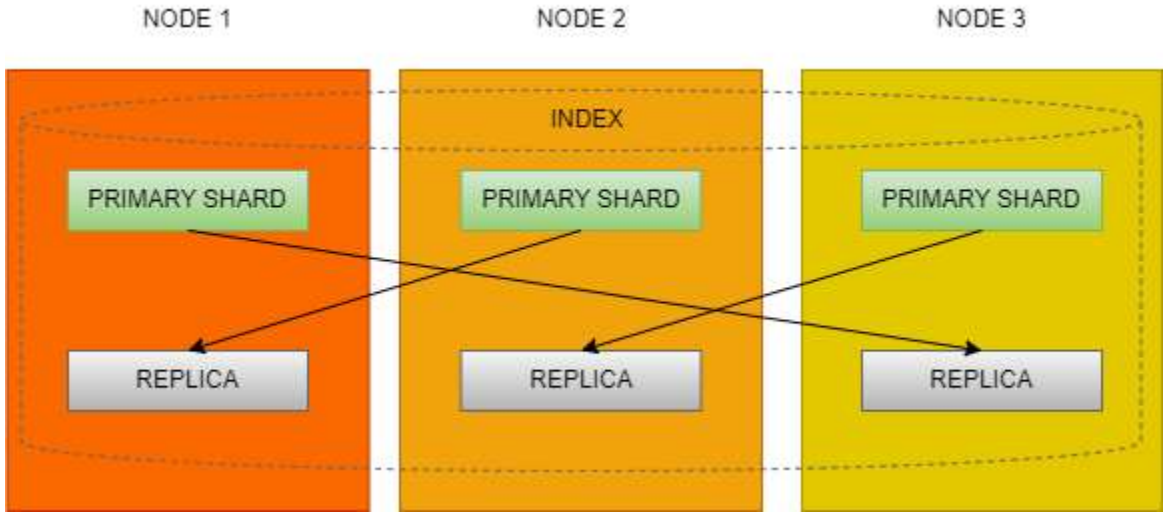
JSON

```
{  "empinfo" :
    {
        "employees" :  [
        {
            "name" : "James Kirk",
            "age" : 40,
        },
        {
            "name" : "Jean-Luc Picard",
            "age" : 45,
        },
        {
            "name" : "Wesley Crusher",
            "age" : 27,
        }
                        ]
    }
}
```




```
GET /
```

```
{
  "name" : "d1
  "cluster_name" :
  "cluster_uuid" :
  "version" : {
    "number" : "7.17.2",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "de7261de50d90919ae53b0eff9413fd7e5307301",
    "build_date" : "2022-03-28T15:12:21.446567561Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```




```
GET /_cat/shards/my_index
```

```
index_name shard_id   state    docs  store         ip              node_name
my_index   0          STARTED  21234 100.2mb       192.168.1.100   node1
my_index   1          STARTED  25678 200.1mb       192.168.1.101   node2
my_index   2          STARTED  29101 100.8mb       192.168.1.102   node3
```

Management

Ingest
Ingest Node Pipelines

Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters

Alerts and Insights
Rules and Connectors
Reporting

Security
Users
Roles
API keys

Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings

Index Management

Index Management docs

Indices | Data Streams | Index Templates | Component Templates

Update your Elasticsearch indices individually or in bulk. Learn more.

Include rollup indices | Include hidden indices

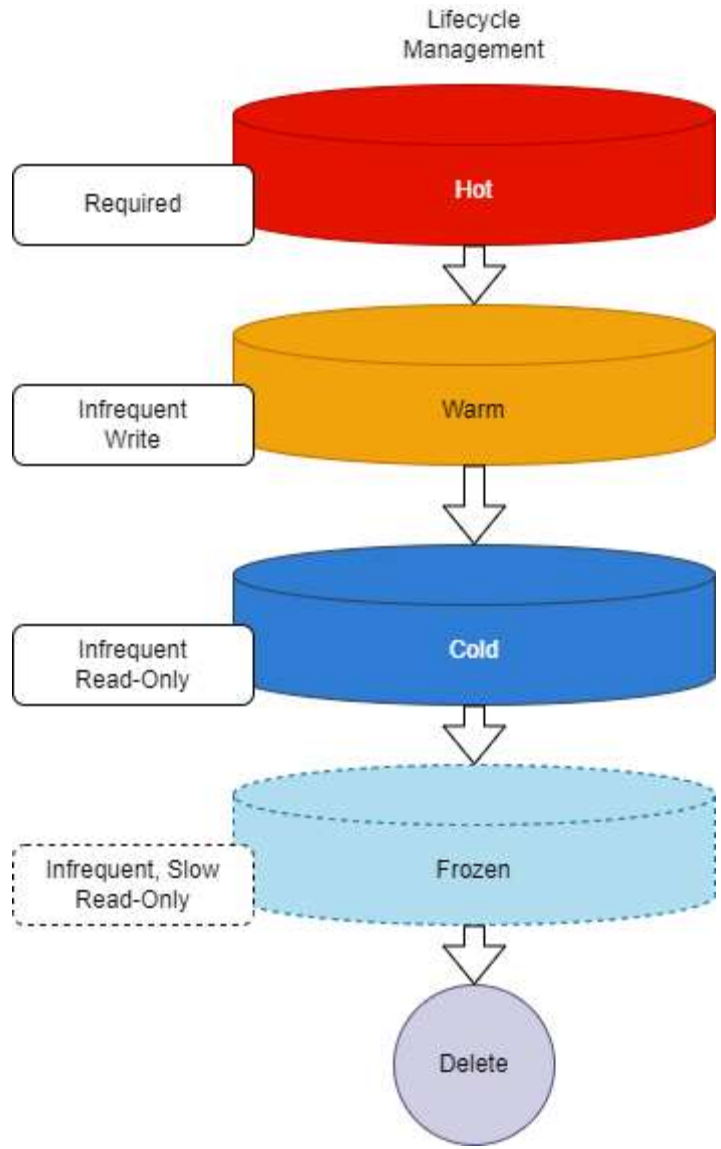
2 indices have lifecycle errors

Show errors

proxy

Lifecycle status | Lifecycle phase | Reload indices

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
syslog-proxy-202206	green	open	8	0	271260801	129.5gb	
syslog-proxy-202207	green	open	8	0	227570045	108.2gb	
syslog-proxy-202208	green	open	8	0	755894055	366.7gb	
syslog-proxy-202209	green	open	8	0	864632133	431.2gb	
syslog-proxy-202210	green	open	8	0	934454504	459.7gb	
syslog-proxy-202211	green	open	8	0	797886742	400.8gb	
syslog-proxy-202212	green	open	8	0	792882181	369.3gb	
syslog-proxy-202301	green	open	8	0	934128988	480.7gb	
syslog-proxy-202302	green	open	8	0	564933327	307.7gb	
syslog-proxy-202303	yellow	open	8	1	894992723	880.1gb	


Lifecycle
Management
Hot
Required
Warm
Infrequent
Write
Cold
Infrequent
Read-Only
Frozen
Infrequent, Slow
Read-Only
Delete

Management

Ingest

Ingest Node Pipelines

Data

Index Management

Index Lifecycle Policies

Snapshot and Restore

Rollup Jobs

Transforms

Remote Clusters

Alerts and Insights

Rules and Connectors

Reporting

Security

Users

Roles

API keys

Kibana

Index Patterns

Saved Objects

Tags

Search Sessions

Spaces

Advanced Settings

Stack

License Management

Edit policy syslog-proxy-lifecycle

Documentation

You are editing an existing policy. Any changes you make will affect the indices that are attached to this policy. Alternatively, you can save these changes in a new policy.

Save as new policy

Policy summary

This policy moves data through the following phases. Learn about timing

Hot phase | Warm phase | Cold phase

Hot phase Required

Store your most recent, most frequently-searched data in the hot tier. The hot tier provides the best indexing and search performance by using the most powerful, expensive hardware.

Advanced settings

Warm phase

Move data into phase when: 32 days old

Move data to the warm tier when you are still likely to search it, but infrequently need to update it. The warm tier is optimized for search performance over indexing performance.

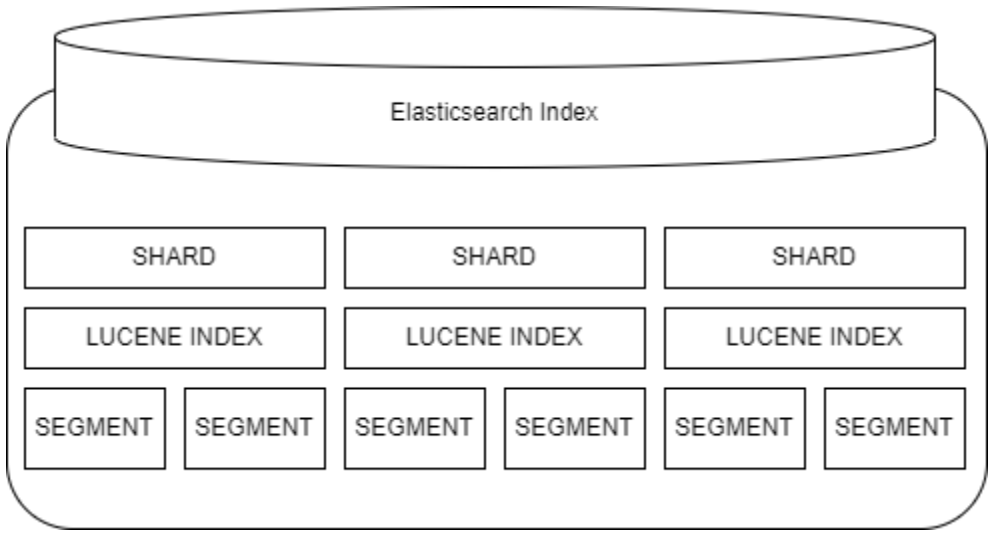
Advanced settings

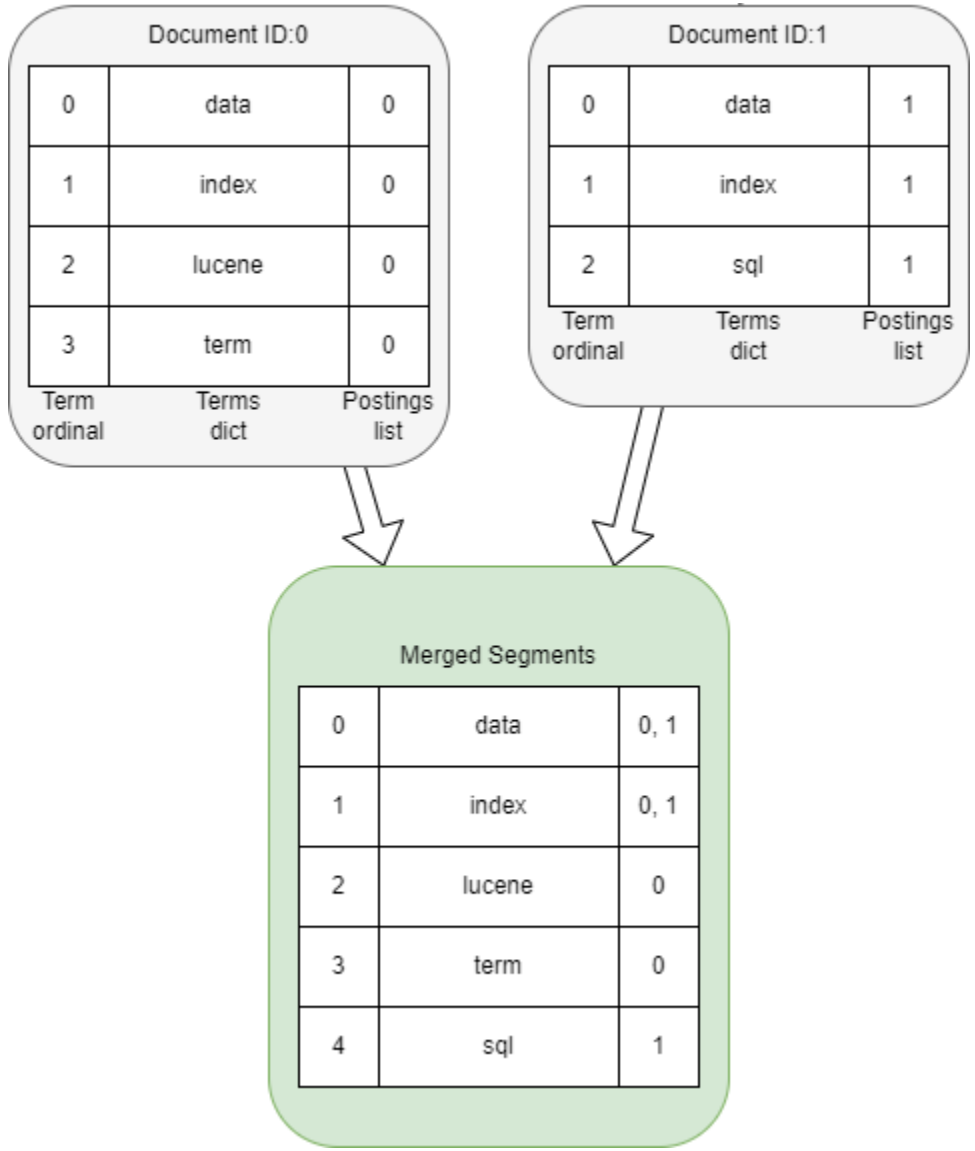
Replicas

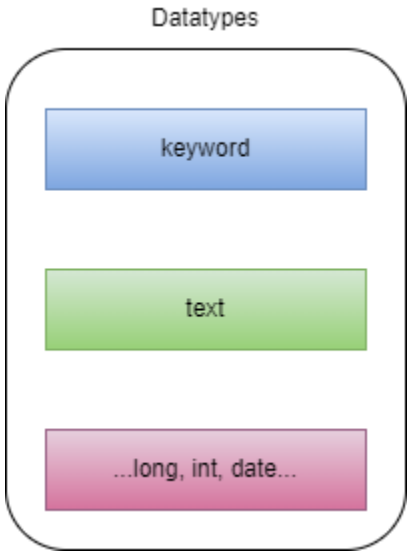
Set the number of replicas. Remains the same as the previous phase by default.

Number of replicas: 1

Set replicas


Elasticsearch Index
SHARD
SHARD
SHARD
LUCENE INDEX
LUCENE INDEX
LUCENE INDEX
SEGMENT
SEGMENT
SEGMENT
SEGMENT
SEGMENT
SEGMENT


Document ID:0
0 data 0
1 index 0
2 lucene 0
3 term 0
Term ordinal
Terms dict
Postings list
Document ID:1
0 data 1
1 index 1
2 sql 1
Term ordinal
Terms dict
Postings list
Merged Segments
0 data 0, 1
1 index 0, 1
2 lucene 0
3 term 0
4 sql 1




```
curl -XPUT 'http://localhost:9200/twitter/_doc/_mapping' -H 'Content-Type: application/json'  -d '
{
    "_doc" : {
        "properties" : {
            "user" : {"type" : "keyword", "null_value" : "na"},
            "message" : {"type" : "text"},
            "postDate" : {"type" : "date"},
            "priority" : {"type" : "integer"},
            "rank" : {"type" : "float"}
        }
    }
}
'
```

Management

Ingest
Ingest Node Pipelines

Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters

Alerts and Insights
Rules and Connectors
Reporting

Security
Users
Roles
API keys

Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings

Stack
License Management
8.0 Upgrade Assistant

Indices | Data Streams | Index Templates | Component Templates

Use composable index templates to automatically apply settings, mappings, and aliases to in

Search...

Name	Index patterns
ilm-history Managed	ilm-history-5*
logs Managed	logs-*-*
metrics Managed	metrics-*-*
ntl-pattern	crp-ntl-*, ntl-*, test-ntl-*
synthetics Managed	synthetics-*-*

Rows per page: 20

Legacy index templates

⚠ Legacy index templates are deprecated in favor of composable index templates

Learn more.

proxy

Name	Index patterns
syslog-proxy-template	syslog-proxy-*

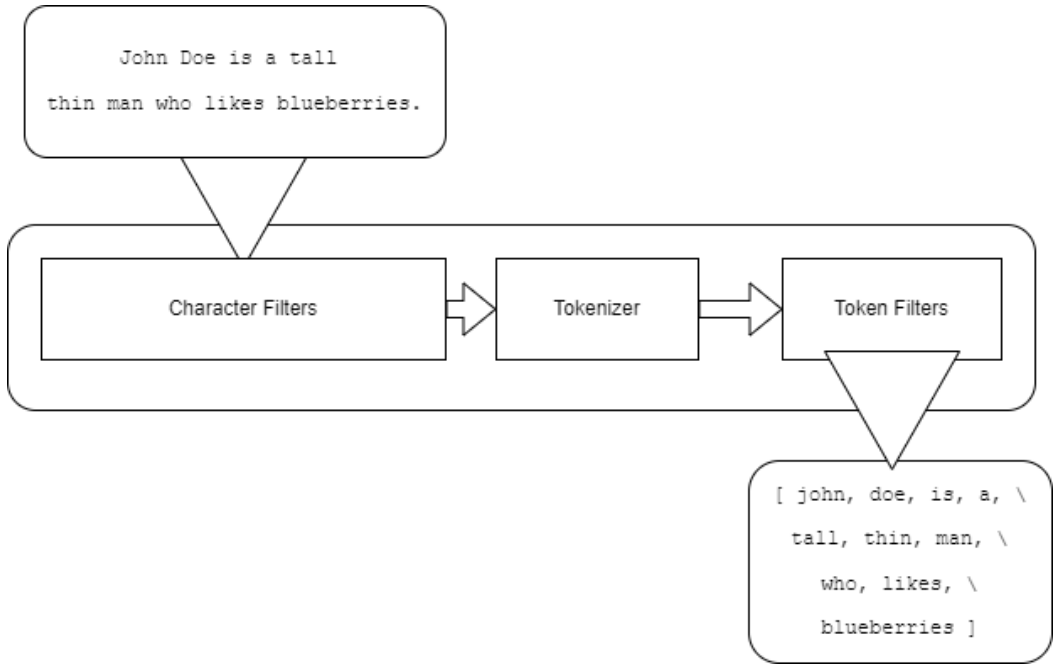
Rows per page: 20

syslog-proxy-template


```
      }
    },
    "custom4": {
      "type": "text"
    },
    "custom1": {
      "type": "keyword"
    },
    "custom2": {
      "type": "keyword"
    },
    "custom5": {
      "type": "text"
    },
    "custom6": {
      "type": "text"
    },
    "timestamp": {
      "type": "long"
    },
    "cache": {
      "type": "keyword"
    },
    "method": {
      "type": "keyword"
    },
    "custom0": {
      "type": "keyword"
    },
    "message": {
      "type": "text"
    },
    "tags": {
      "eager_global_ordinals": false,
      "norms": false,
      "index": true,
      "store": false,
      "type": "keyword",
      "split_queries_on_whitespace": false,
      "index_options": "docs",
      "doc_values": true
    },
    "dst_fqdn": {
      "type": "text",
      "fields": {
        "keyword": {
```


Close

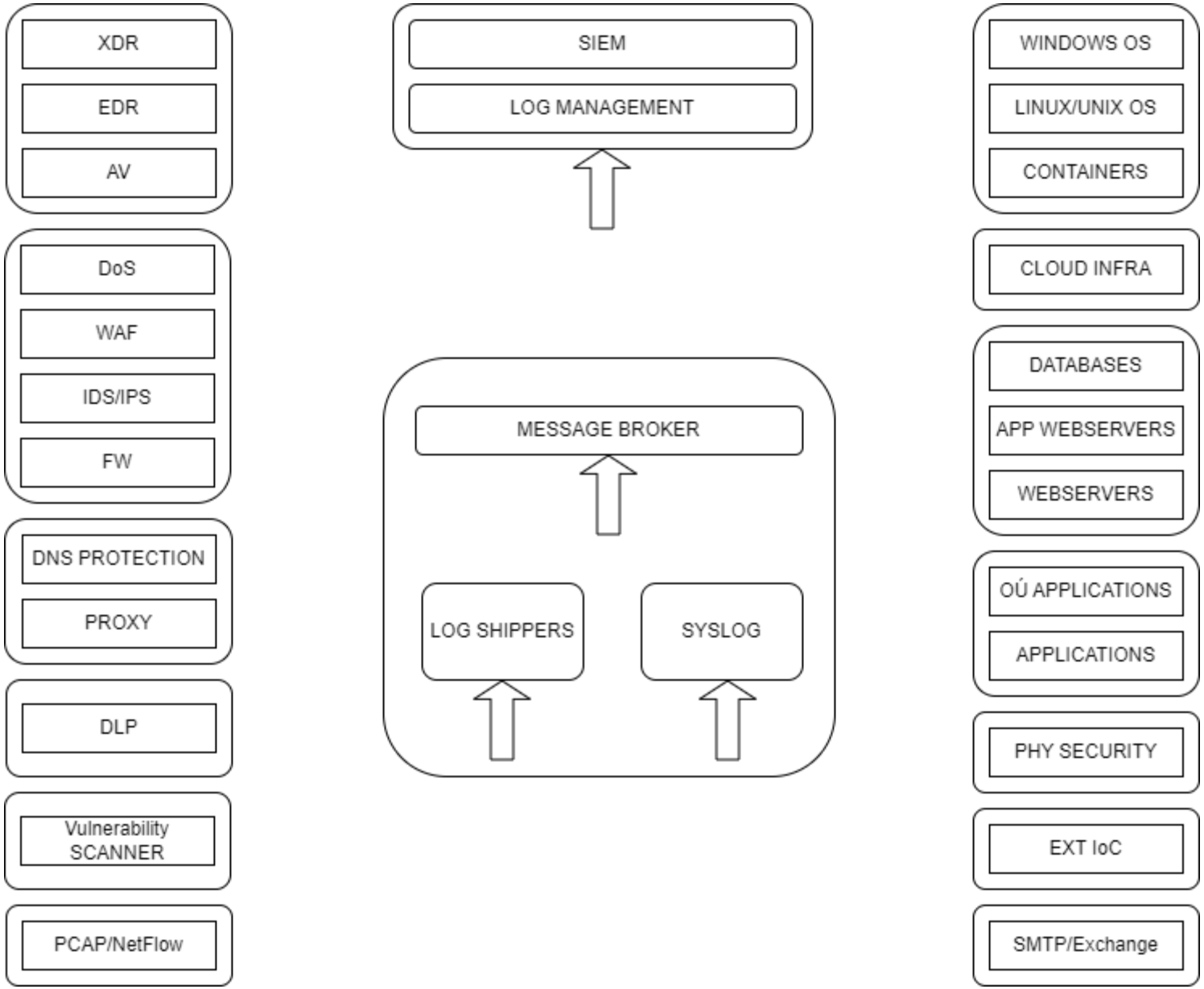
Manage




```
GET /talk-demo-index/_analyze
{
  "text": "John Doe is a tall thin man who likes blueberries."
}
```

```
{
  "tokens" : [
    {
      "token" : "john",
      "start_offset" : 0,
      "end_offset" : 4,
      "type" : "<ALPHANUM>",
      "position" : 0
    },
    {
      "token" : "doe",
      "start_offset" : 5,
      "end_offset" : 8,
      "type" : "<ALPHANUM>",
      "position" : 1
    },
```

Elastic Security



CEF

Common Event Format (ArcSight CEF)

ECS

Elastic Common Scheme

OSSEM

Open Source Security Events Metadata

ASIM

Advanced Security Information Model

```
CEF:0|MyCompany|WebServer|1.0|100|Web Access|6|\
src=192.168.0.1 spt=443 dst=10.0.0.1 dpt=8080 \
requestMethod=GET requestUrl=/index.html
```

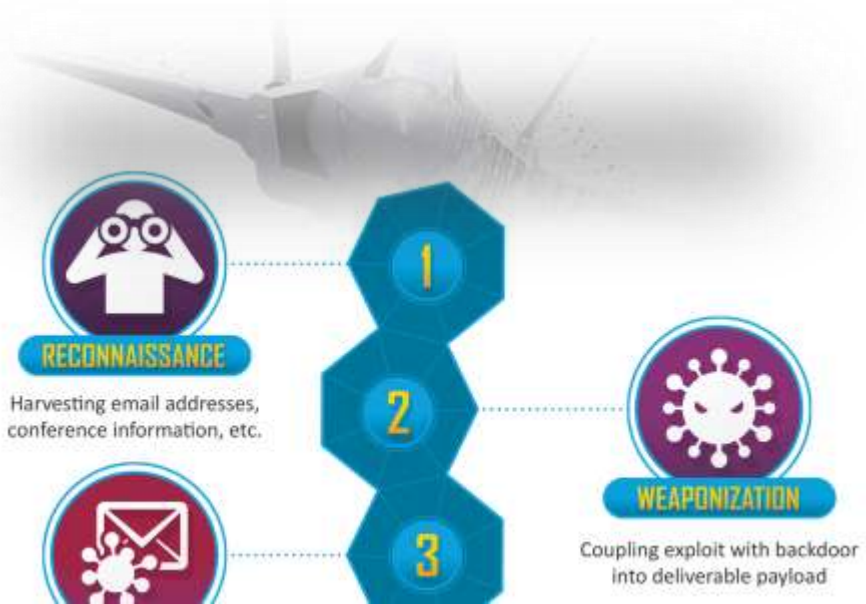
```
{
  "@timestamp": "2023-04-25T15:23:00.000Z",
  "event": {
    "category": "web",
    "action": "access"
  },
  "source": {
    "ip": "192.168.0.1",
    "port": 443
  },
  "destination": {
    "ip": "10.0.0.1",
    "port": 8080
```

```
{
    "event": {
        "id": "d08fa6f2-bb8f-42fd-b7fd-f5610c04dc25",
        "category": ["access"],
        "type": ["web"],
        "severity": "info",
        "timestamp": "2023-04-25T15:23:00.000Z"
    },
    "source": {
        "ip": "192.168.0.1",
        "port": 443
    },
```

Elastic Security

Lockheed Marting Kill Chain

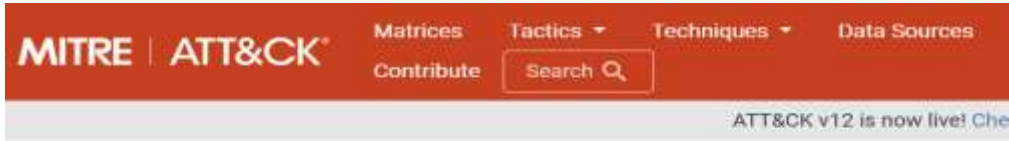
- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Act on the Objective



MITRE ATT&CK Matrix

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Technique	Sub-Technique
Phishing	Spearphising Attachment
	Spearphising Link
	Spearphising Service
Valid Accounts	Default Account
	Domain Accounts
	Local Accounts
	Cloud Accounts



MITRE ATT&CK® is a 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.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK®

KQL

KQL was created by Elastic as a way to search through Elasticsearch data in Kibana. While searching with Lucene is available, KQL has a lower barrier for entry and can even suggest fields, operators, or values based on what is available in dataset.

```
event.category: network AND
source.port: [5000 to 7000]
```

Lucene

Lucene Query Lanquage can perform REGEX queries (i.e. subdomain with exactly three characters, and another subdomain with exactly eight digits).

```
[a-z]{3}.stage.[0-9]{8}
```

EQL

At high level, EQL allows you to express relationships (as sequences, times, and categories) between events.

```
sequence by
process.entity_id with
maxspan = 1m
```

Elastic Security

[metadata]

```
creation_date = "2022/09/14"
integration = ["system"]
maturity = "production"
min_stack_comments = "New fields added: required_fields, related_integrations, setup"
min_stack_version = "8.3.0"
updated_date = "2023/02/22"
```

[rule]

```
from = "now-9m"
index = ["auditbeat-*", "logs-system.auth-*"]
language = "eql"
name = "Potential Linux SSH Brute Force Detected"
risk_score = 47
rule_id = "1c27fa22-7727-4dd3-81c0-de6da5555feb"
severity = "medium"
tags = ["Elastic", "Host", "Linux", "Threat Detection", "Credential Access"]
type = "eql"
query = '''
sequence by host.id, source.ip, user.name with maxspan=10s
  [authentication where host.os.type == "linux" and event.action  in ("ssh_login", "user_login") and
    event.outcome == "failure" and source.ip != null and source.ip != "0.0.0.0" and source.ip != "::" ] with runs=10
'''
```

[[rule.threat]]

```
framework = "MITRE ATT&CK"
```

[[rule.threat.technique]]

```
id = "T1110"
name = "Brute Force"
reference = "https://attack.mitre.org/techniques/T1110/"
```

[[rule.threat.technique.subtechnique]]

```
id = "T1110.001"
name = "Password Guessing"
reference = "https://attack.mitre.org/techniques/T1110/001/"
```

[[rule.threat.technique.subtechnique]]

```
id = "T1110.003"
name = "Password Spraying"
reference = "https://attack.mitre.org/techniques/T1110/003/"
```

[rule.threat.tactic]

```
id = "TA0006"
name = "Credential Access"
reference = "https://attack.mitre.org/tactics/TA0006/"
```

Elastic Security

elastic

Search Elastic

Security / Overview

Add data

Security

Overview

Detect
- Alerts
- Rules
- Exceptions

Explore
- Hosts
- Network

Investigate
- Timelines
- Cases

Manage
- Endpoints
- Trusted applications
- Event filters

Search | KQL | Today | Show dates | Refresh

signal.rule.name: Execution of Persistent Suspicious Program [Duplicate] × | + Add filter

Data sources

Recent cases

[redacted]

0

můžete se prosím podívat [redacted] windows\system32{A6D608F0-0BDE-491A-97AE-5C4B05D86E01}.bat", o co se jedná?

Dle detekce na tento soubor byl nastaven skrytý attribut pomocí příkazu : "attrib +R +H +S +A *.cui"".

View all cases

Recent timelines

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

View all timelines

Security news

Elastic Security Labs outlines an attack chain that leads to XWORM and AGENTTESLA

2023-04-07

Threat actors are deploying XWorm and Agent Tesla RATs using custom .NET loaders.

Detection alert trend

Showing: 4 alerts

Stack by: signal.rule.name | View alerts

External alert trend

Showing: 0 external alerts

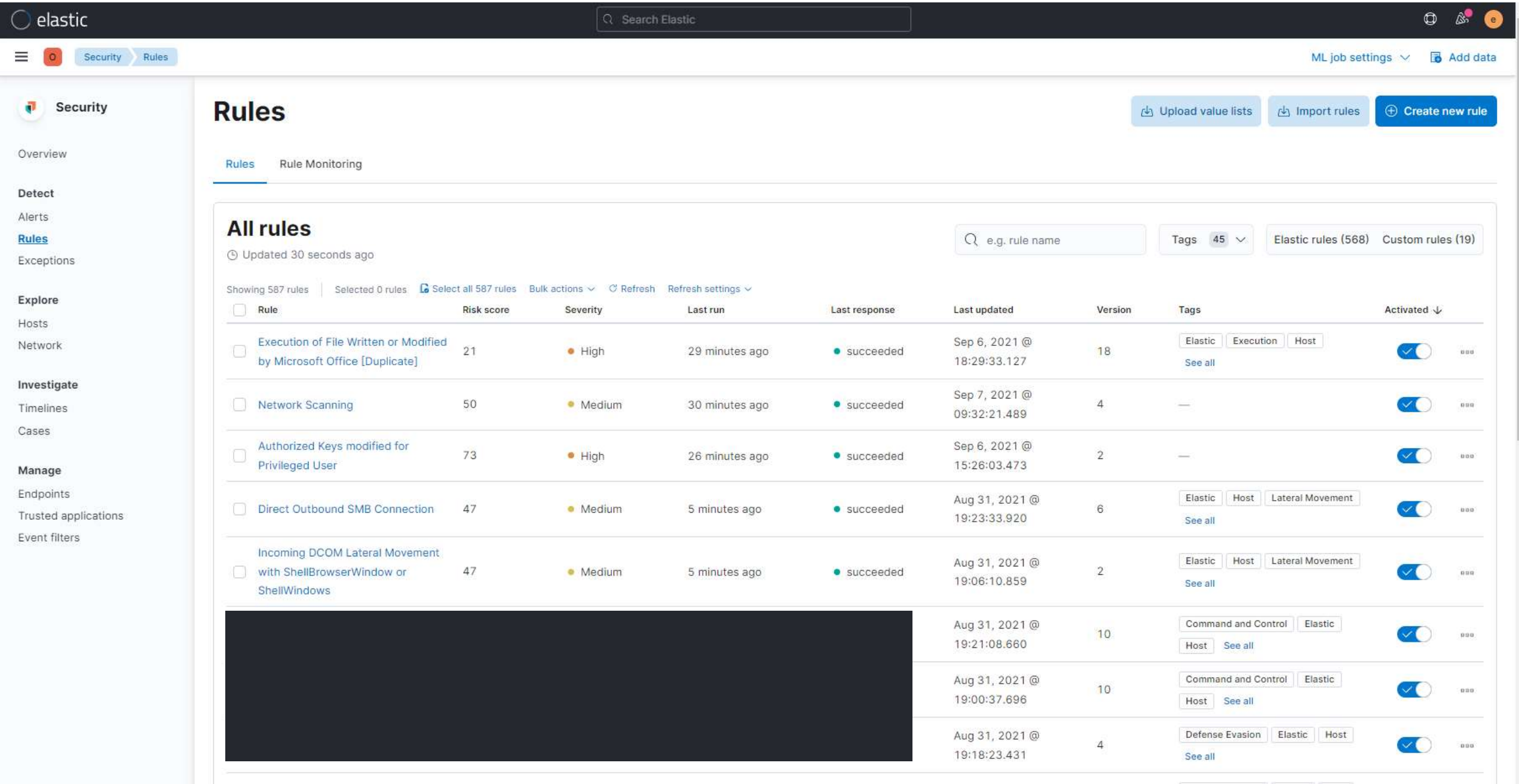
Stack by: event.module | View alerts

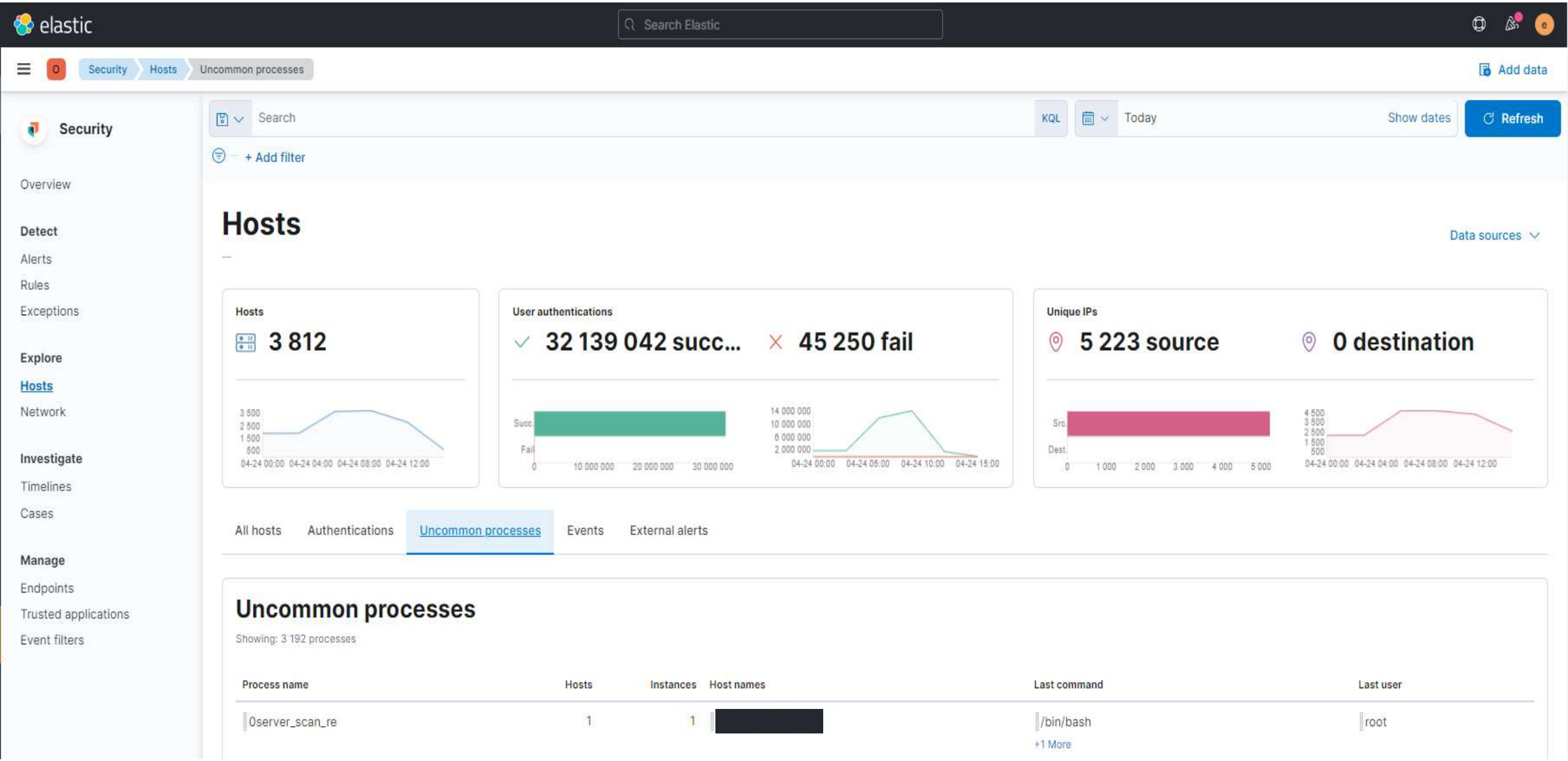
All values returned zero

Events

Showing: 0 events

Stack by: event.dataset | View events


elastic
Search Elastic
Security
Rules
ML job settings
Add data
Security
Overview
Detect
Alerts
Rules
Exceptions
Explore
Hosts
Network
Investigate
Timelines
Cases
Manage
Endpoints
Trusted applications
Event filters
Rules
Upload value lists
Import rules
Create new rule
Rules
Rule Monitoring
All rules
Updated 30 seconds ago
e.g. rule name
Tags 45
Elastic rules (568)
Custom rules (19)
Showing 587 rules
Selected 0 rules
Select all 587 rules
Bulk actions
Refresh
Refresh settings
Rule
Risk score
Severity
Last run
Last response
Last updated
Version
Tags
Activated
Execution of File Written or Modified by Microsoft Office [Duplicate]
21
High
29 minutes ago
succeeded
Sep 6, 2021 @ 18:29:33.127
18
Elastic
Execution
Host
See all
Network Scanning
50
Medium
30 minutes ago
succeeded
Sep 7, 2021 @ 09:32:21.489
4
Authorized Keys modified for Privileged User
73
High
26 minutes ago
succeeded
Sep 6, 2021 @ 15:26:03.473
2
Direct Outbound SMB Connection
47
Medium
5 minutes ago
succeeded
Aug 31, 2021 @ 19:23:33.920
6
Elastic
Host
Lateral Movement
See all
Incoming DCOM Lateral Movement with ShellBrowserWindow or ShellWindows
47
Medium
5 minutes ago
succeeded
Aug 31, 2021 @ 19:06:10.859
2
Elastic
Host
Lateral Movement
See all
Aug 31, 2021 @ 19:21:08.660
10
Command and Control
Elastic
Host
See all
Aug 31, 2021 @ 19:00:37.696
10
Command and Control
Elastic
Host
See all
Aug 31, 2021 @ 19:18:23.431
4
Defense Evasion
Elastic
Host
See all


elastic
Search Elastic
Security
Hosts
Uncommon processes
Add data
Security
Overview
Detect
Alerts
Rules
Exceptions
Explore
Hosts
Network
Investigate
Timelines
Cases
Manage
Endpoints
Trusted applications
Event filters
Search
KQL
Today
Show dates
Refresh
+ Add filter
Hosts
Data sources
Hosts
3 812
User authentications
32 139 042 succ...
45 250 fail
Unique IPs
5 223 source
0 destination
All hosts
Authentications
Uncommon processes
Events
External alerts
Uncommon processes
Showing: 3 192 processes
Process name
Hosts
Instances
Host names
Last command
Last user
0server_scan_re
1
1
/bin/bash
+1 More
root

Deployments
My deployment
- Edit
- Monitoring
  - Health
  - Logs and metrics
  - Performance
- Elasticsearch
  - Snapshots
  - API console
- Kibana
- Integrations Server
- Enterprise Search
- Activity
- Security

Features

Support

My deployment

Open Kibana | Actions

HEALTHY · AZURE - Ireland (northeurope) · Deployment ID 84d347

Autoscaling is available

You can now enable autoscaling on your deployment. When the deployment approaches the disk allocation threshold, storage capacity will scale up automatically. Additionally, for machine learning nodes RAM can scale both up and down. Learn more

Enable autoscaling

Deployment name

My deployment Edit

Applications

Elasticsearch	Copy endpoint	Copy cluster ID	
Kibana	Copy endpoint	Copy component ID	Open
APM	Copy endpoint	Copy component ID	Open
Fleet	Copy endpoint	Copy component ID	Open
Enterprise Search	Copy endpoint	Copy component ID	

Tags

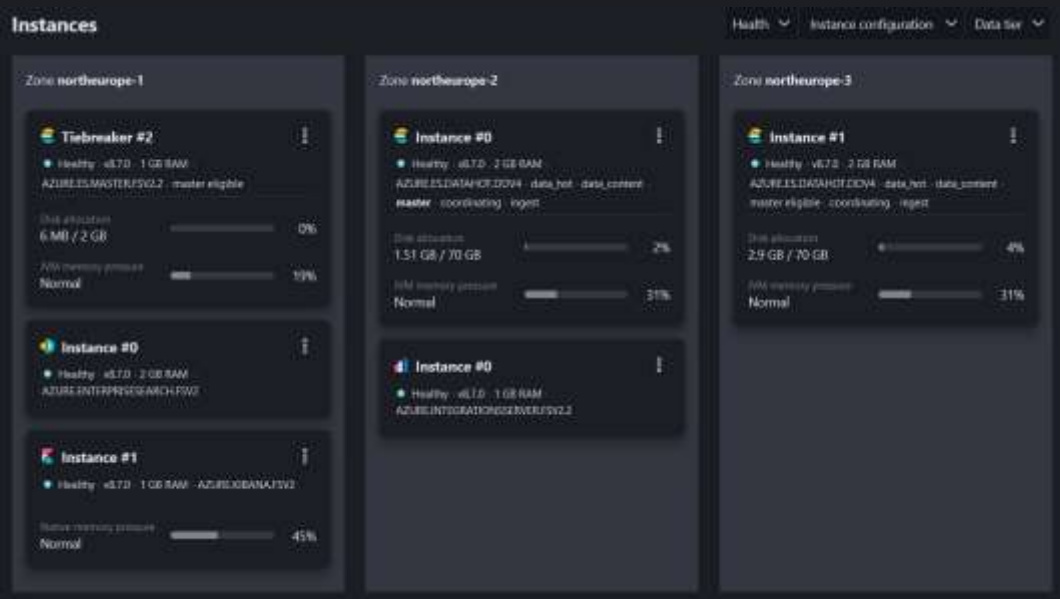
Custom endpoint alias

my-deployment-84d347

Hardware profile

General purpose Edit

Instances



Děkuji za pozornost

Další zdroje

- https://github.com/TheHive-Project/TheHive
- https://www.misp-project.org/

Koncept

Dokumentace instalace

Dokumentace datových zdrojů

SLA