



NetEye

 **User Group**
2023

21.09.2023

Romantik Hotel Rottner
Stein bei Nürnberg

Agenda



- Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten
- Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic
- Erfahrungen und Herausforderungen bei der Implementierung



whoami



- Reinhold TROCKER
 - >25 years of experience in IT
 - ~ 20 years of experience in IT security

 - Master of computer science (Dipl-Ing) in Vienna (AT)
 - (ISC)2 CISSP

 - ~ 20 years at data center for local banks in South Tyrol (IT)
 - ~ 1 year at Wuerth-Phoenix as technical consultant for Neteye SIEM
- ▶ reinhold.trocker@wuerth-phoenix.net



Agenda



- **Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten**
- Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic
- Erfahrungen und Herausforderungen bei der Implementierung



Agenda



- **Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten**
- ▶ Herausforderungen der IT-Sicherheit
 - ▶ Daten + Personen
 - ▶ Aufgaben
 - ▶ Speed
 - ▶ DATA
- ▶ SIEM
- ▶ Architektur
- ▶ Security Workflow im Schnelldurchlauf



Data + people



THE DATA DILEMMA

5+

Data Domains

Practitioners analyze endpoint, cloud, network, application, user, and more!

1B+

Events Per Day

Most organizations average 1 billion events per day

<5

SOC Analysts

Security Operation Centers vary in size, but most have less than 5 analysts

What does security need today?



Slow down the
attackers



Speed up the
defenders



Make it actionable at scale

Tasks



Elastic Security

SIEM, Endpoint, Cloud

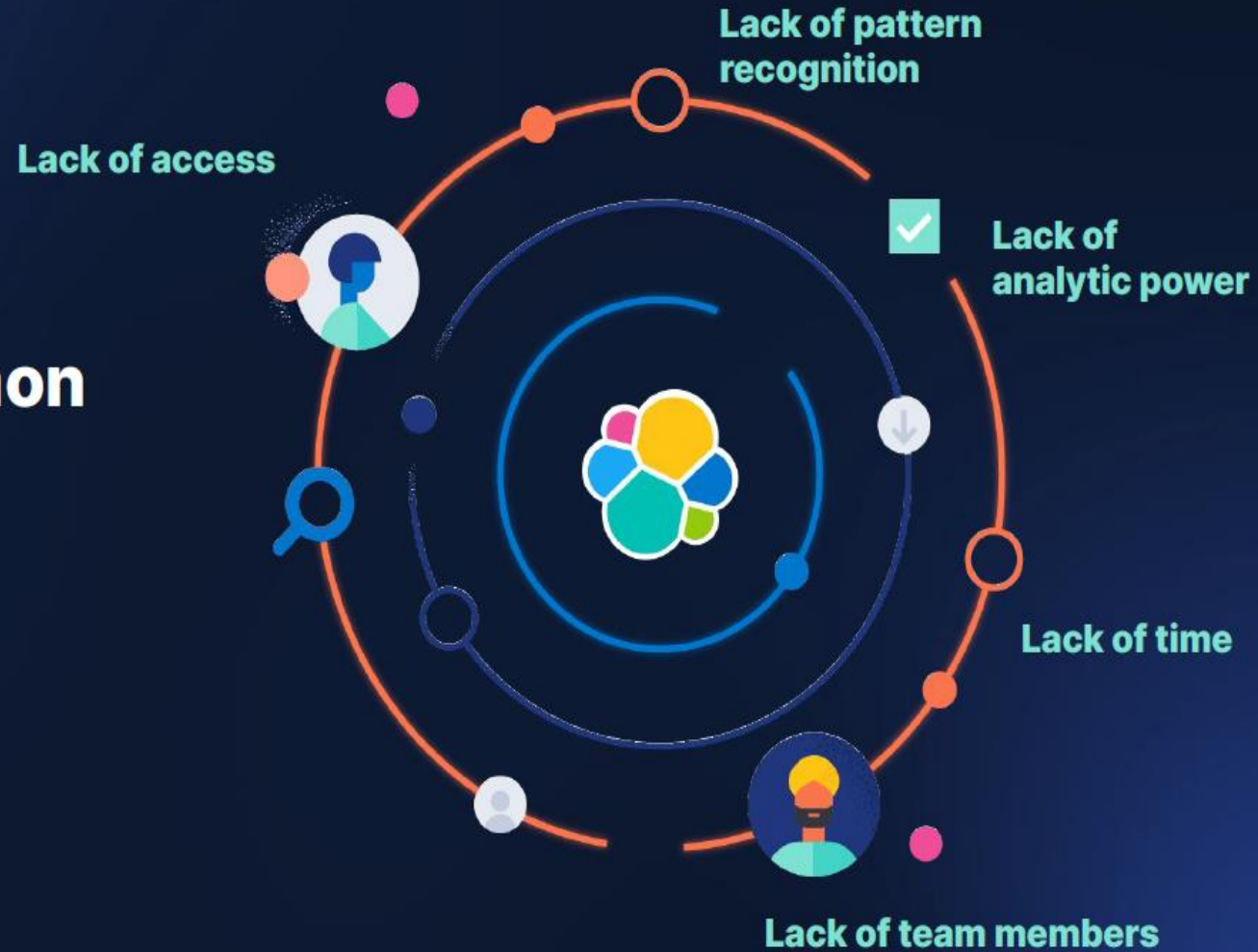
Monitoring
and Compliance

Threat Prevention
and Detection

Hunting and
Incident Response



Data is the common denominator



SIEM
— is the foundation —
of Elastic Security

architecture

The Elastic Search Platform



workflow



▶ **QUICKLY SHOW WORKFLOW**



1. Protect the Endpoints/Assets/Workloads

Hosts running Elastic Agent
Endpoint / Workload Preventions
Osquery management
Posture / risk monitoring

Servers and other hosts

Threat Intel

Network monitoring

Firewalls and IDS/IPS

Web proxies

APM

More data sources...

Elastic Common Schema (ECS)

Detection rules, ML Jobs

Alerting workflows

Events, external alerts, findings
Indicators, intelligence

Detection engine

Detection Alerts

Triage

Timelines

Investigate in Timeline / Analyzer / Correlation / Session Viewer

Escalate?

Create case

Cases

External systems

Respond

Threat hunting workflows

Visualize, understand, and hunt by host, network, user, session, indicator, or cloud asset

Key

- System
- User process
- Backend process
- Data store (Index)
- External action
- Decision

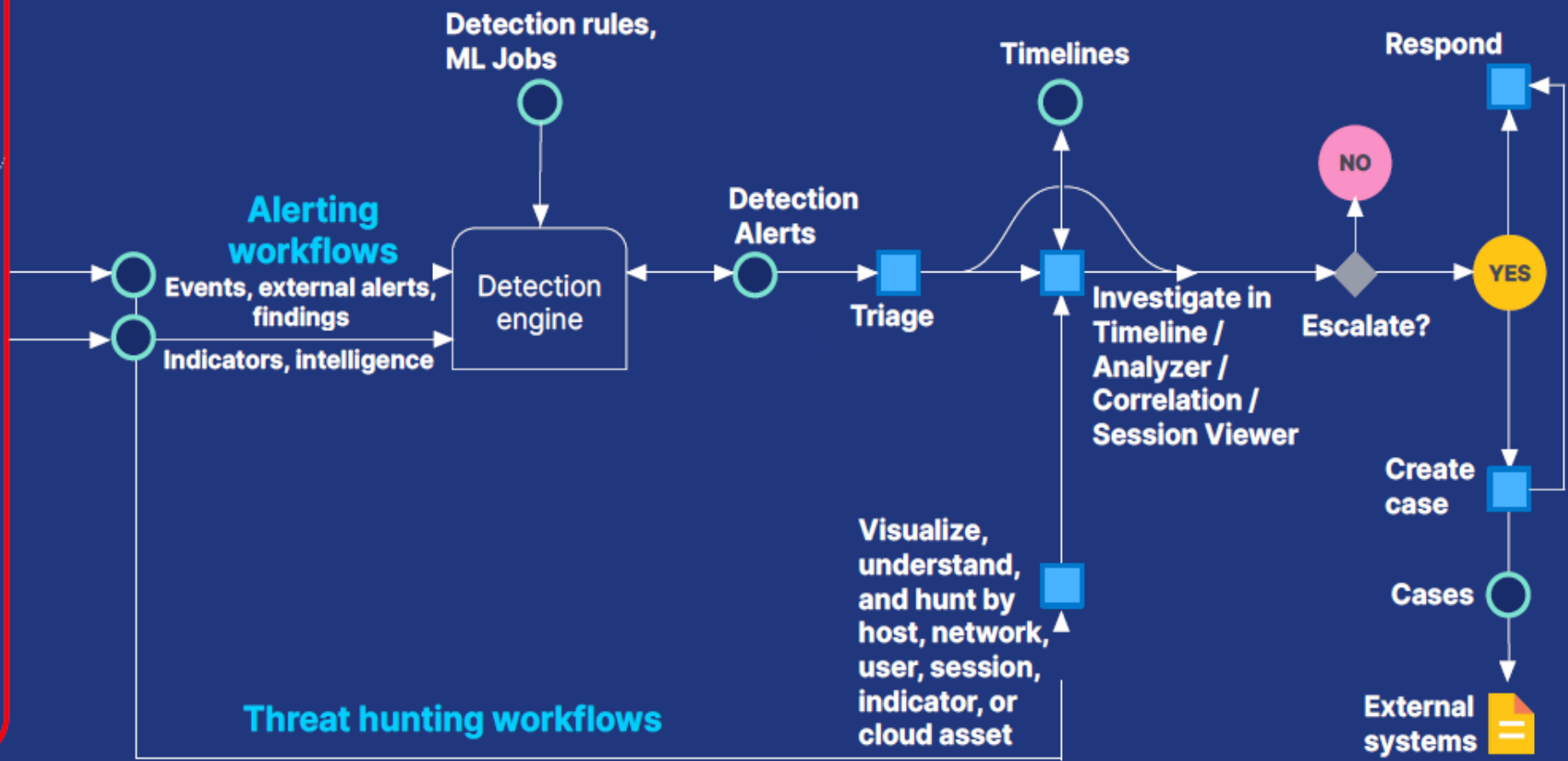
2. Ingest & Normalize All Security Data

- Hosts running Elastic Agent
 - Endpoint / Workload Preventions
 - Osquery management
 - Posture / risk monitoring
- Servers and other hosts
- Threat Intel
- Network monitoring
- Firewalls and IDS/IPS
- Web proxies
- APM
- More data sources...

Elastic Common Schema (ECS)

Key

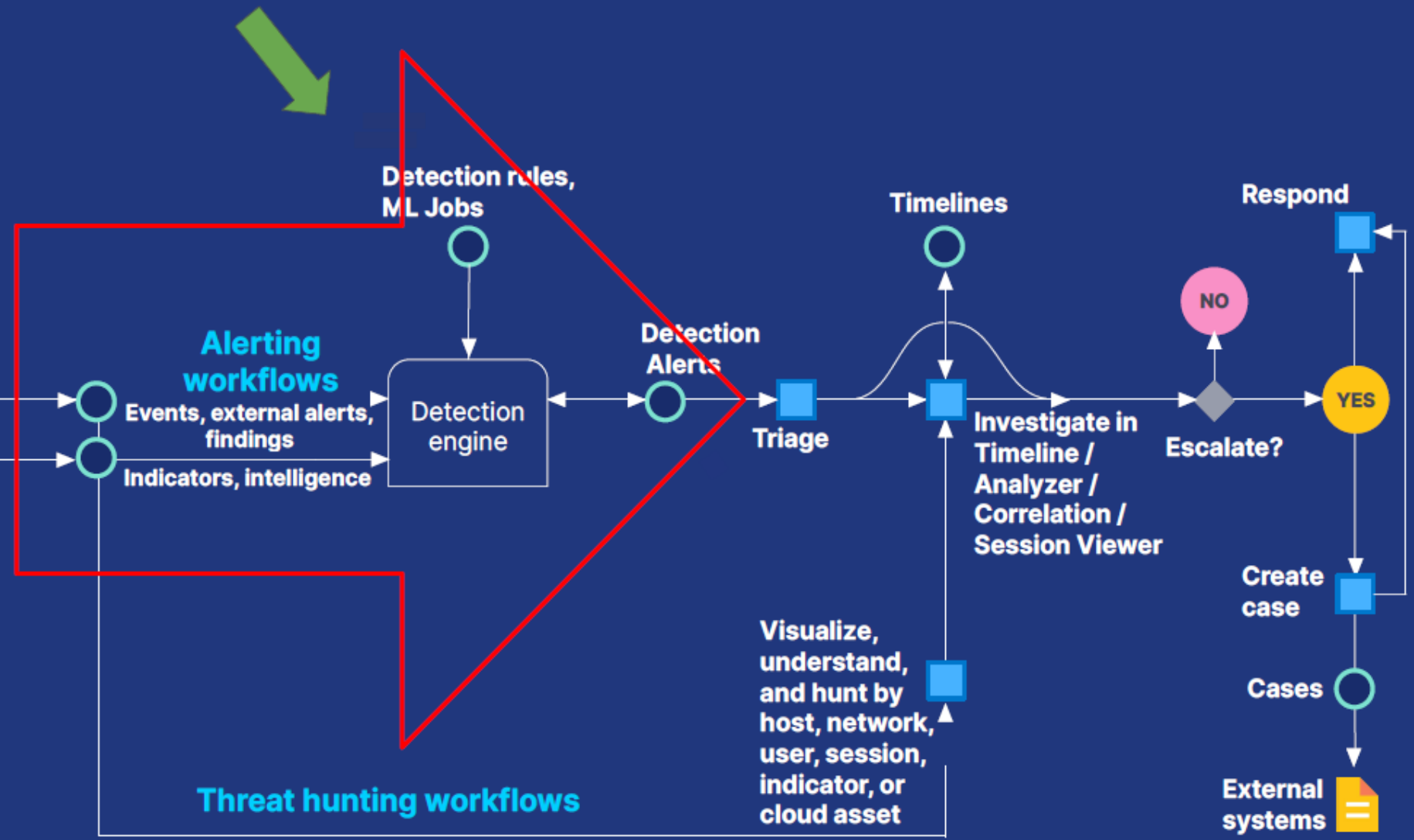
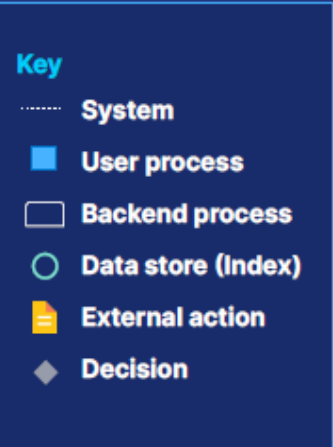
- System
- User process
- Backend process
- Data store (Index)
- External action
- Decision



3. Automated Detection and Alerting

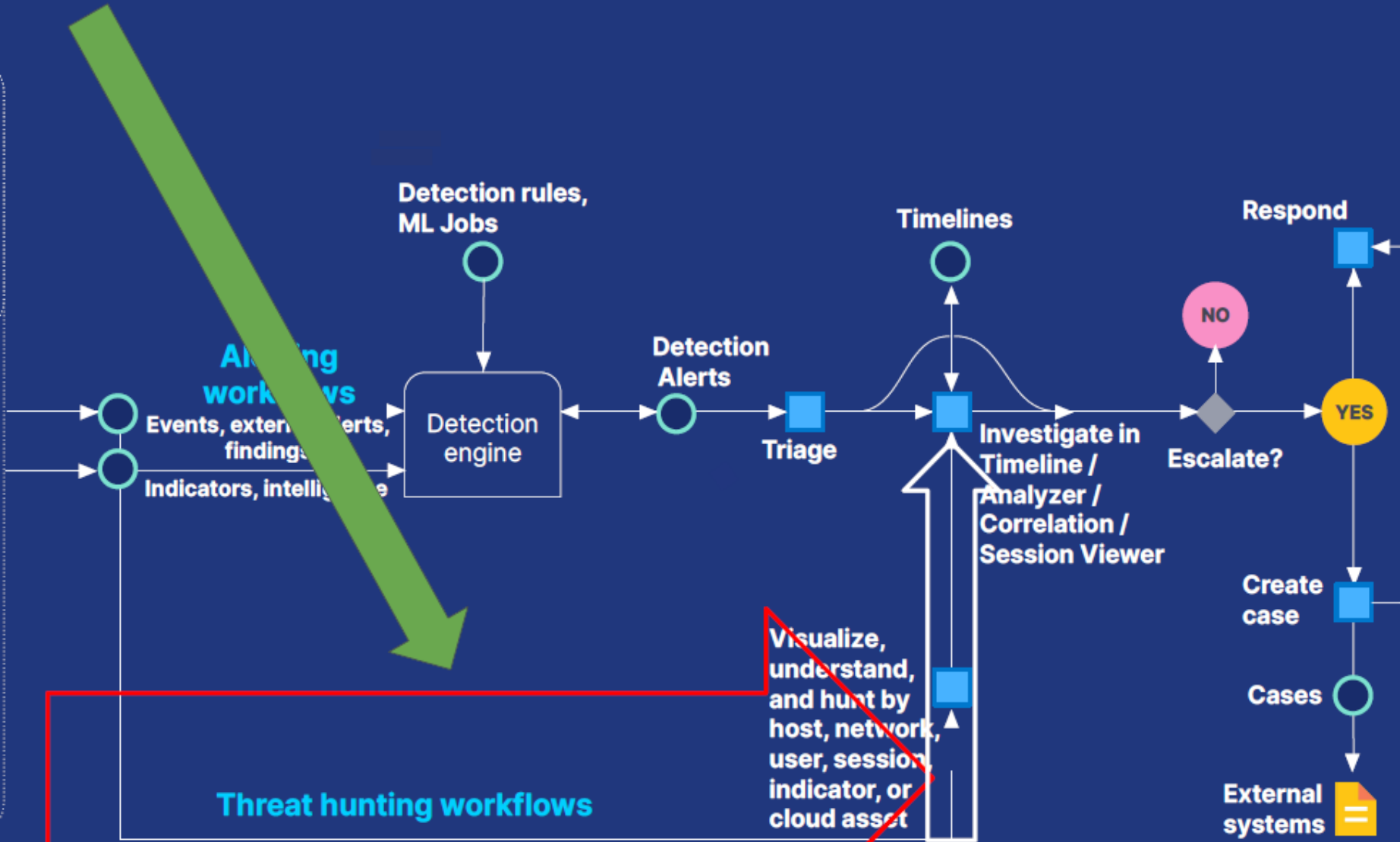
- Hosts running Elastic Agent
 - Endpoint / Workload Preventions
 - Osquery management
 - Posture / risk monitoring
- Servers and other hosts
- Threat Intel
- Network monitoring
- Firewalls and IDS/IPS
- Web proxies
- APM
- More data sources...

Elastic Common Schema (ECS)



4. Threat Hunting

- Hosts running Elastic Agent
 - Endpoint / Workload Preventions
 - Osquery management
 - Posture / risk monitoring
- Servers and other hosts
- Threat Intel
- Network monitoring
- Firewalls and IDS/IPS
- Web proxies
- APM
- More data sources...
- Elastic Common Schema (ECS)



Visualize, understand, and hunt by host, network, user, session, indicator, or cloud asset

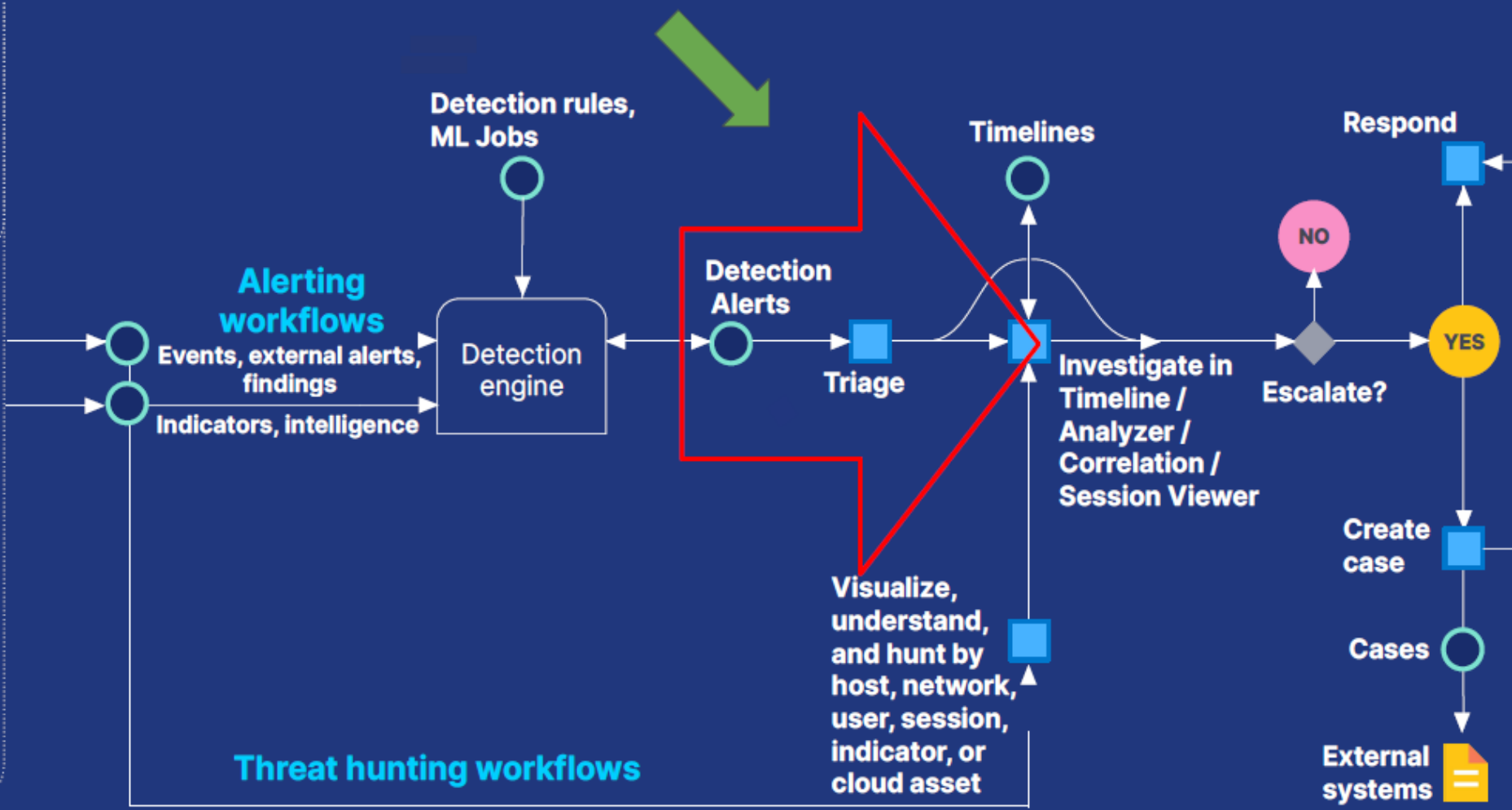
5. Alert Triage

- Hosts running Elastic Agent
 - Endpoint / Workload Preventions
 - Osquery management
 - Posture / risk monitoring
- Servers and other hosts
- Threat Intel
- Network monitoring
- Firewalls and IDS/IPS
- Web proxies
- APM
- More data sources...

Elastic Common Schema (ECS)

Key

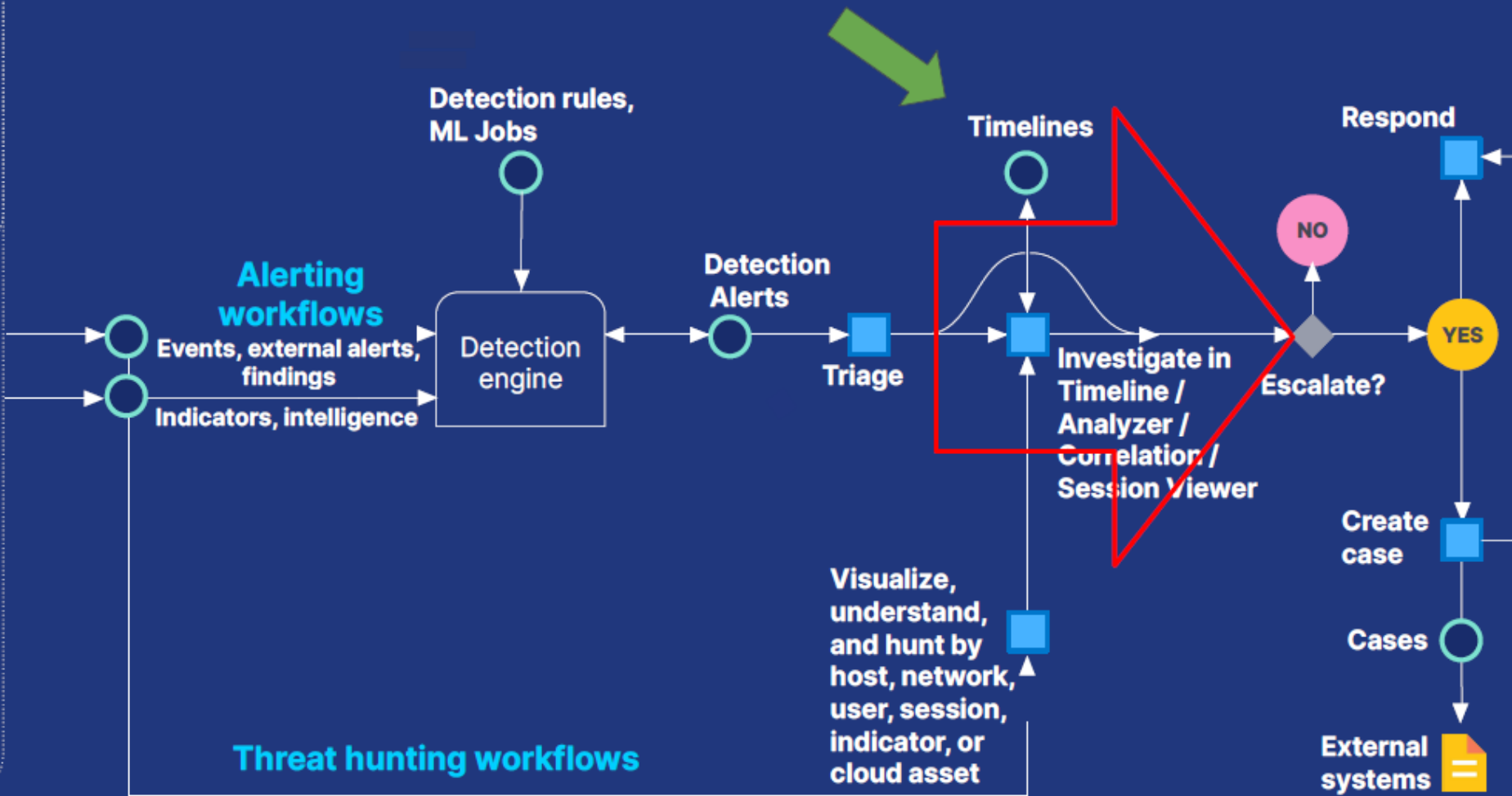
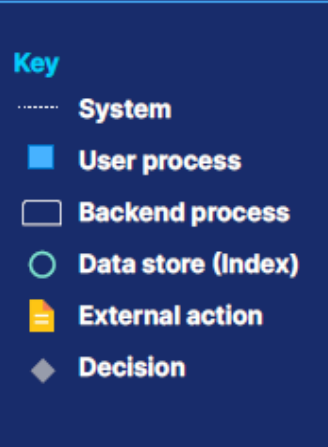
- System
- User process
- Backend process
- Data store (Index)
- External action
- Decision



6. Investigate

- Hosts running Elastic Agent
 - Endpoint / Workload Preventions
 - Osquery management
 - Posture / risk monitoring
- Servers and other hosts
- Threat Intel
- Network monitoring
- Firewalls and IDS/IPS
- Web proxies
- APM
- More data sources...

Elastic Common Schema (ECS)



Threat hunting workflows

7. Escalate

Hosts running Elastic Agent
Endpoint / Workload Preventions
Osquery management
Posture / risk monitoring

Servers and other hosts

Threat Intel

Network monitoring

Firewalls and IDS/IPS

Web proxies

APM

More data sources...

Elastic Common Schema (ECS)

Detection rules, ML Jobs

Alerting workflows

Events, external alerts, findings
Indicators, intelligence

Detection engine

Detection Alerts

Triage

Timelines

Investigate in Timeline / Analyzer / Correlation / Session Viewer

Visualize, understand, and hunt by host, network, user, session, indicator, or cloud asset

Threat hunting workflows

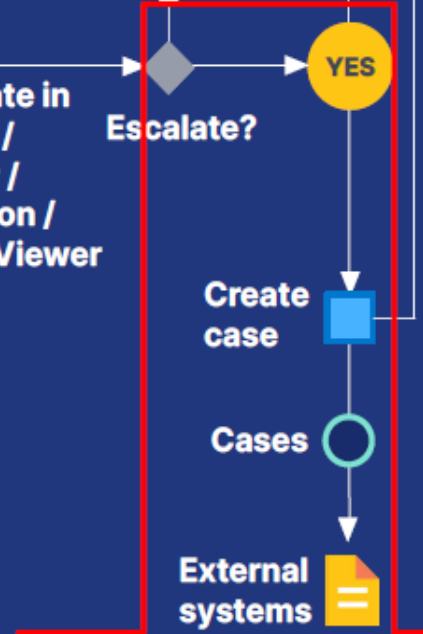
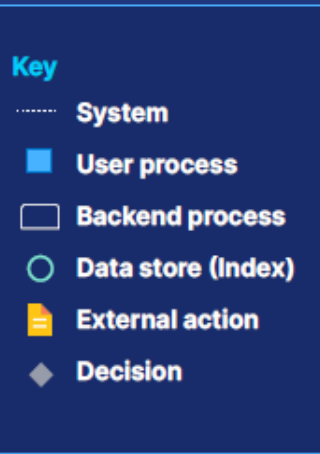
Respond

Escalate?

Create case

Cases

External systems



Agenda



- Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten
- **Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic**
- Erfahrungen und Herausforderungen bei der Implementierung



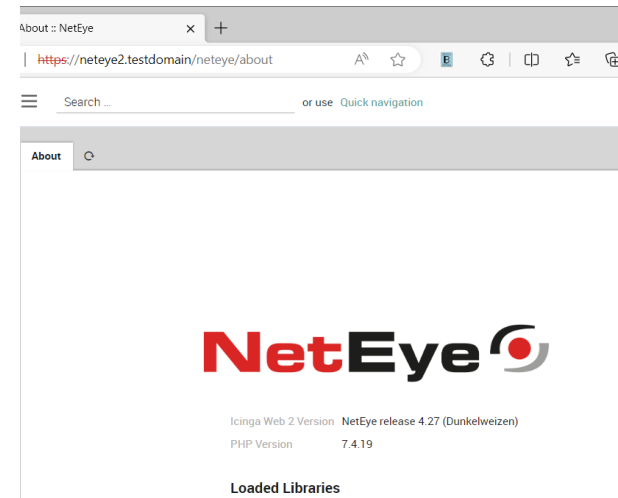
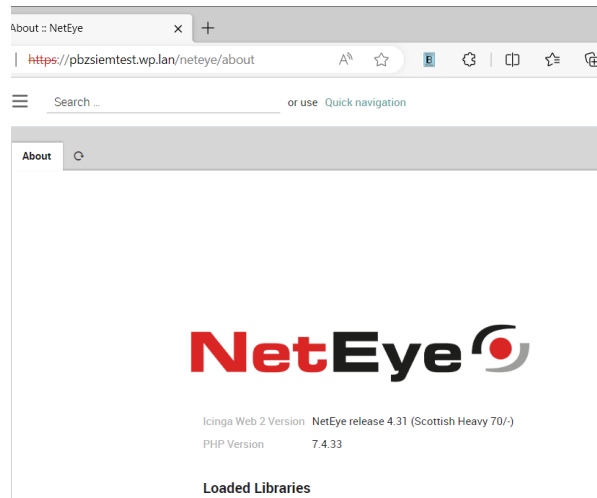
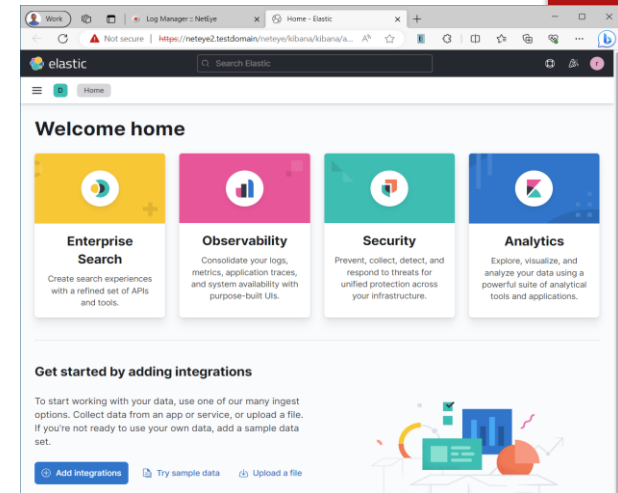
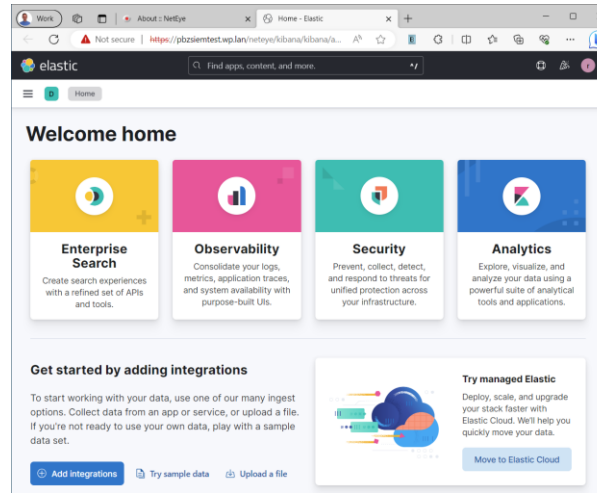
Agenda



- Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten
- **Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic**
 - ▶ Neteye alt vs. neu
 - ▶ Liste einiger Änderungen
 - ▶ Benutzerfreundlichkeit
 - ▶ Performance



Changes?



▶ NetEye 4.27 vs NetEye 4.31

Some changes



- ▶ Kibana index patterns -> Kibana data views
- ▶ API keys authorization editable
- ▶ *beats -> elastic agent with integrations
- ▶ more elastic integrations (~ 270 -> 340)
 - ▶ APM, http json, hadoop, GCP storage
- ▶ beta integrations available (~30)
- ▶ enhanced integrations
 - ▶ TCP listener + TLS
 - ▶ XDR...

All categories	269
AWS	29
Azure	24
Cloud	33
Communications	3
Config management	1
Containers	17
Credential Management	1
Custom	25
Custom Logs	1
Database	27
DNS	2
EDR/XDR	9
Elastic Stack	17
Email	3
File storage	5
Firewall	6
Google Cloud	3

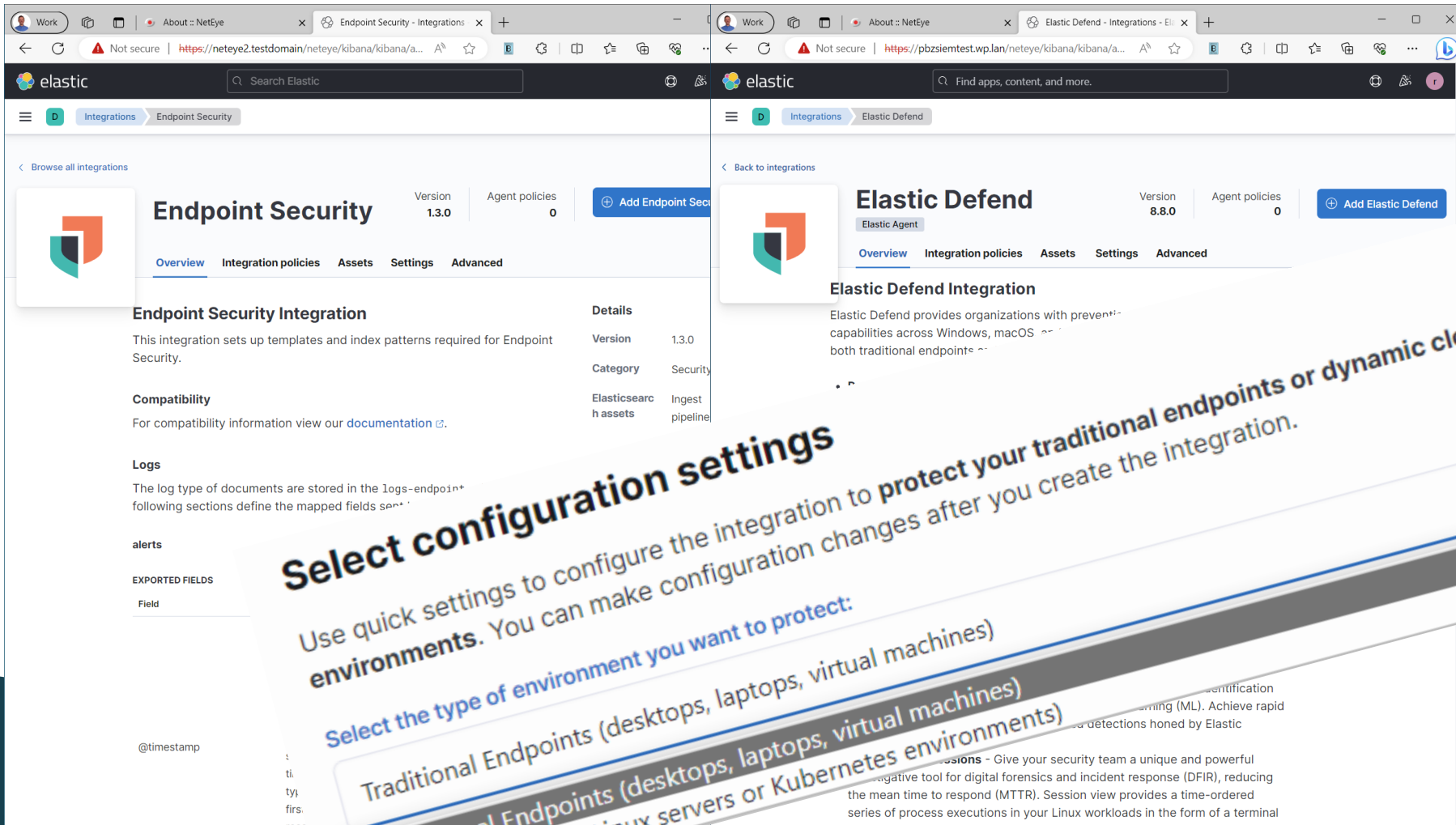
All categories	340
APM	1
AWS	36
Azure	25
Cloud	5
Containers	15
Custom	34
Database	36
Elastic Stack	30
Elasticsearch SDK	9
Enterprise Search	36
Google Cloud	19
Network	53
Observability	112
Operating Systems	6
Productivity	1
Security	165

X Display beta integrations

The image shows two browser windows side-by-side, both displaying the Elastic integration management interface. The left window is titled 'Endpoint Security' and shows details for version 1.3.0. The right window is titled 'Elastic Defend' and shows details for version 8.8.0. Both windows include a navigation menu, a search bar, and a list of integration details such as version, agent policies, and a list of exported fields.

XDR

V 1.3.0 -> V 8.8.0



Select configuration settings

Use quick settings to configure the integration to protect your traditional endpoints or dynamic cloud environments. You can make configuration changes after you create the integration.

Select the type of environment you want to protect:

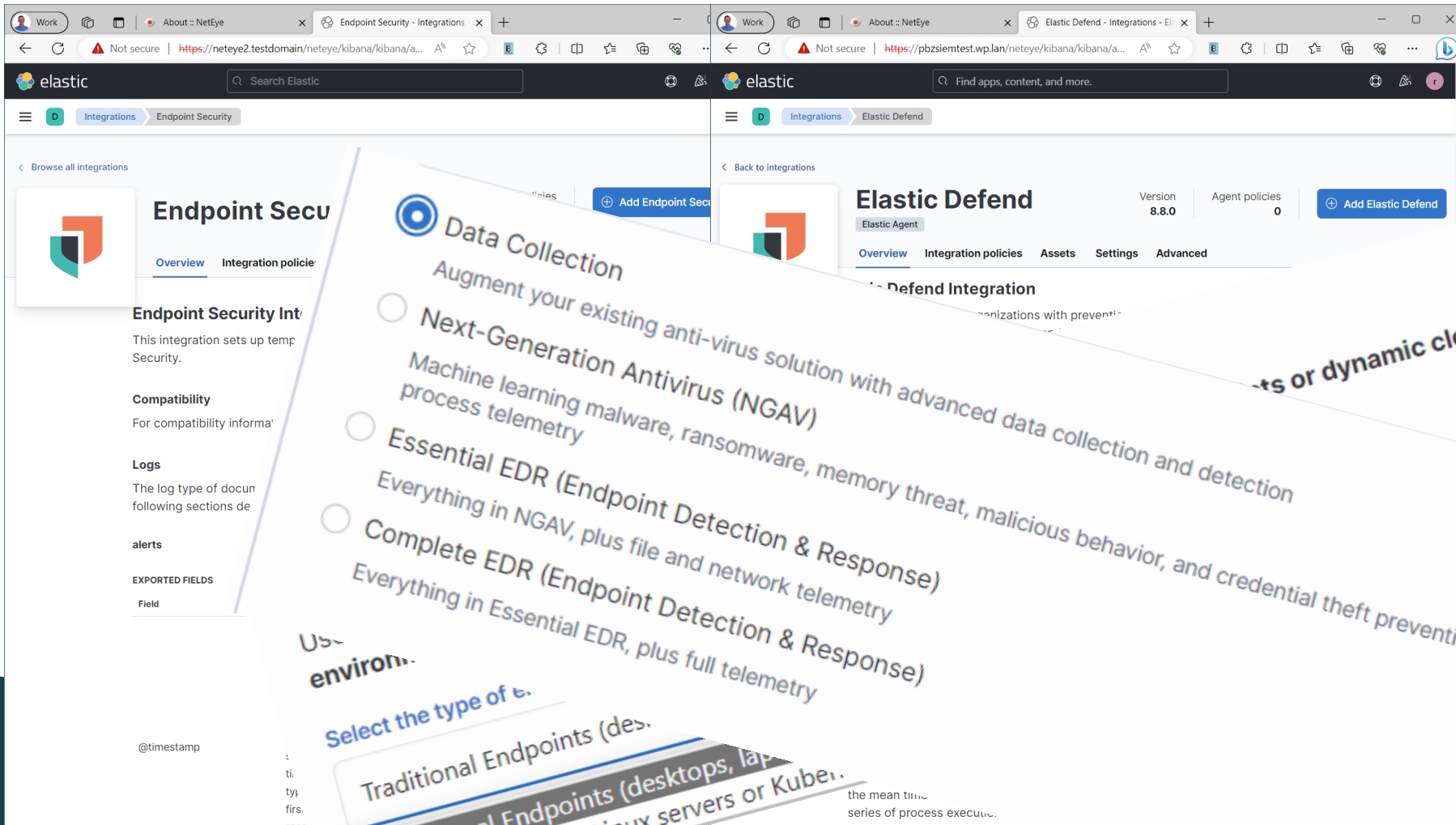
Traditional Endpoints (desktops, laptops, virtual machines)

Traditional Endpoints (desktops, laptops, virtual machines)

Cloud Workloads (Linux servers or Kubernetes environments)

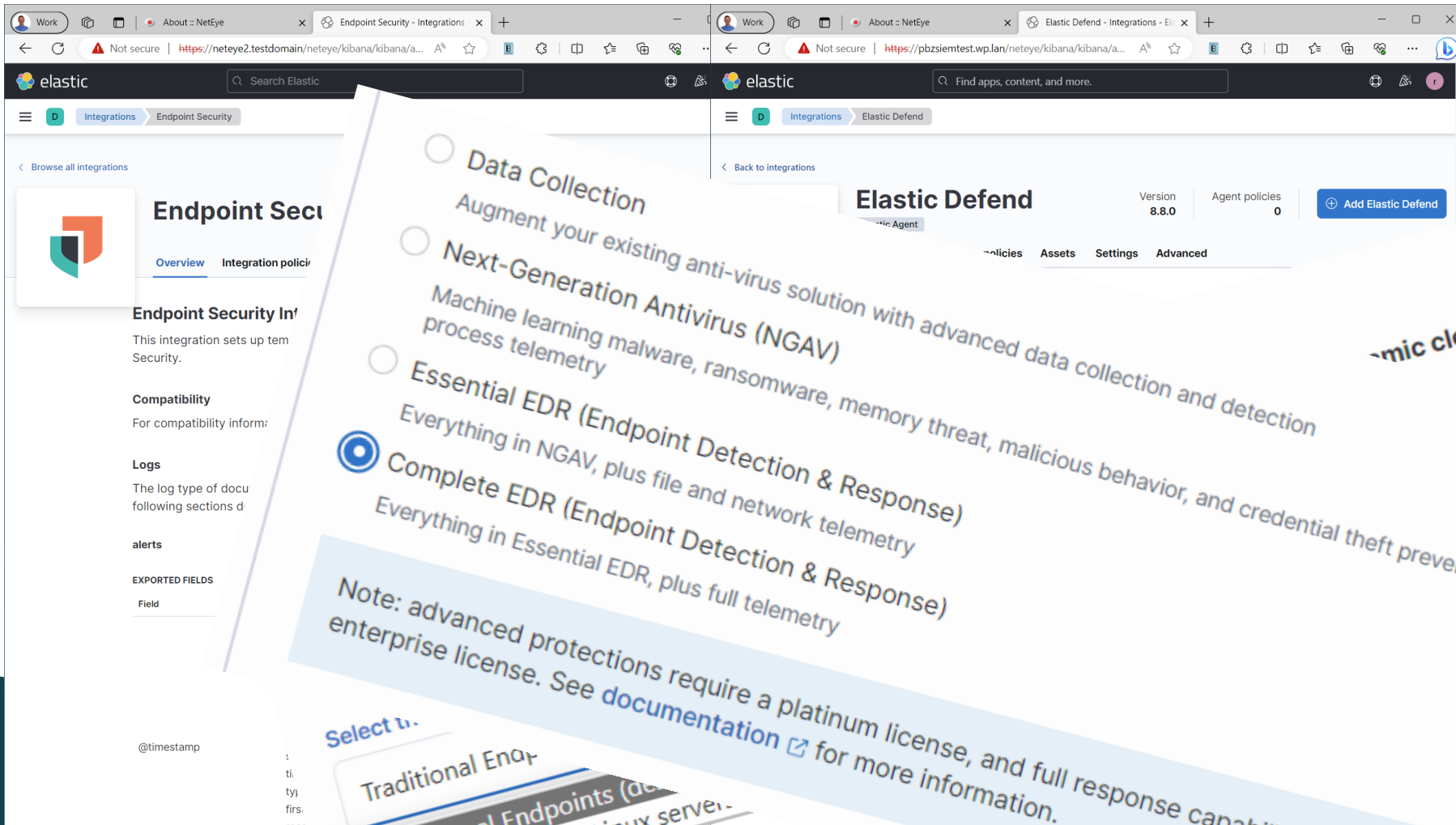
XDR

V 1.3.0 -> V 8.8.0



XDR

V 1.3.0 -> V 8.8.0



- Data Collection
Augment your existing anti-virus solution with advanced data collection and detection
 - Next-Generation Antivirus (NGAV)
Machine learning malware, ransomware, memory threat, malicious behavior, and credential theft preventions, plus process telemetry
 - Essential EDR (Endpoint Detection & Response)
Everything in NGAV, plus file and network telemetry
 - Complete EDR (Endpoint Detection & Response)
Everything in Essential EDR, plus full telemetry
- Note: advanced protections require a platinum license, and full response capabilities require an enterprise license. See [documentation](#) for more information.

Select to...

- Traditional Endp...
- Traditional Endpoints (de...
- Cloud Workloads (Linux server...

XDR

V 1.3.0 -> V 8.8.0

Ease of use

Work | About :: NetEye | Add integration - Elastic Defend

Not secure | <https://pbzsiemtest.wp.lan/neteye/kibana/kib...>

elastic Find apps, content, and more.

Integrations Elastic Defend Add integration Send feedback

< Cancel

Add Elastic Defend integration

Agent policy windowsclients

Configure an integration for the selected agent policy.

This package has 2 transform assets which will be created and started with the same roles as the user installing the package.

1 Configure integration

Integration settings

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

Integration name xdrwinclients

Description Optional

> Advanced options

Select configuration settings

Use quick settings to configure the integration to **protect your traditional endpoints or dynamic cloud environments**. You can make configuration changes after you create the integration.

Select the type of environment you want to protect:

Traditional Endpoints (desktops, laptops, virtual machines)

Data Collection
Augment your existing anti-virus solution with advanced data collection and detection

Next-Generation Antivirus (NGAV)
Machine learning malware, ransomware, memory threat, malicious behavior, and credential theft preventions, plus process telemetry

Essential EDR (Endpoint Detection & Response)
Everything in NGAV, plus file and network telemetry

Complete EDR (Endpoint Detection & Response)
Everything in Essential EDR, plus full telemetry

2 Where to add this integration?

New hosts Existing hosts

Agent policy

Agent policies are used to manage a group of integrations across a set of agents.

Agent policy windowsclients

1 agent is enrolled with the selected agent policy.

Cancel Save and continue



Ease of use

The image displays two overlapping screenshots of the Elastic Defend web interface. The background screenshot shows the 'Add integration' page, which includes a search bar, a list of integrations, and a table with columns for Name, Integration, Namespace, CPU, Memory, Last activity, and Version. The foreground screenshot shows the 'Integrations' page for the 'windowsclients' agent policy, featuring a search bar, a list of integrations, and a table with columns for Name, Integration, Namespace, CPU, Memory, Last activity, and Version. A yellow highlight is placed on the '29 seconds ago' value in the 'Last activity' column of the foreground screenshot.

Background Screenshot: Add integration - Elastic Defend

Revision 19 | Integrations 3 | Agents 1 agent | Last updated on Sep 14, 2023 | Actions

Name	Integration	Namespace	CPU	Memory	Last activity	Version	Actions
system-3	System v1.38.2	default					...
winlog-1	Custom Windows Event Logs v1.17.0	default					...
xdrwinclients	Elastic Defend v8.8.0	default	1.70 %	109 MB	29 seconds ago	8.8.2	...

Showing 1 agent | Clear filters

Agent policy: windowsclients rev. 19

Agent policy: windowsclients

1 agent is enrolled with the selected agent policy.

Cancel Save and continue



Agenda



- Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten
- Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic
- **Erfahrungen und Herausforderungen bei der Implementierung**



Agenda



- Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten
- Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic
- **Erfahrungen und Herausforderungen bei der Implementierung**
 - ▶ Tipps für die Implementierung
 - ▶ Positive Erfahrungen
 - ▶ Tipps



Improvements



- ▶ Fleet Management got better, can deal with proxies and more than 1 URL
- ▶ Performance is better – ingestion and kibana UI
- ▶ More features (of integrations)
- ▶ More features in kibana
- ▶ Focus on data streams
- ▶ *beats -> elastic agent



Tipps



- ▶ For upgrades (neteye 4.30 / Elastic 7.17 -> neteye 4.31 / Elastic 8.8)
 - ▶ Follow all upgrade documentation at <https://neteye.guide>
 - ▶ For integrators / programmers: get knowhow about data streams before upgrading
 - ▶ prepare your environment (update all *beats) before upgrading
- ▶ Integrations / Fleet / XDR / FIM: wait for Elastic8 when possible
- ▶ Use XDR in 'Data collection only' when using other XDR solution in parallel



Agenda - outro



- Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten
- Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic
- Erfahrungen und Herausforderungen bei der Implementierung



Complete solution



Prevent. Detect. Respond.

Endpoint security with Agent

- Ransomware & malware prevention
- Memory threat prevention
- Malicious behavior protection

Prebuilt data integrations

Cloud: platforms, applications, APM

Network: logs, flows, traffic analysis

Hosts: OS & security logs, state, FIM

Users: activity, context

IoT & OT: sensors, physical security

Threat context: feeds & TIPs, CVEs

Prebuilt analytics

ML jobs, detection rules, investigation guides, dashboards, searches

Elastic Common Schema

Kibana

Monitor dashboards, detect at scale with ML & correlation, streamline investigation with powerful workflows, & integrations

Elasticsearch

Ingest data of any kind, store it for years, search & analyze it in seconds

Agent

Protect & collect at every host

Beats

Ship data without adding overhead

Logstash

Process data with server-side pipelines

Prebuilt workflow integrations

- Security orchestration, automation, & response (SOAR)
- Security incident response tools
- Ticketing & case management
- Email, Slack, & custom tools

Host inspection & response with Agent

- On-demand osquery inspection
- Remote host isolation

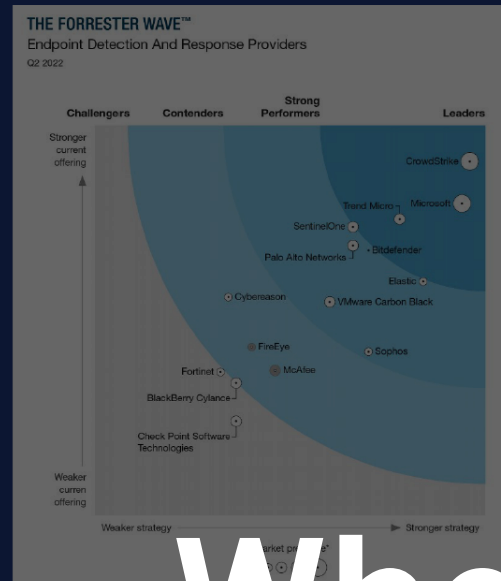
For continuous monitoring, automated threat protection, investigation & response, & threat hunting

The Foundation of Modern Security, Observability, and more



Elastic named a Strong Performer in The Forrester Wave for EDR Providers, Q2 2022

- Elastic envisions security as a data problem and prioritizes features that enable customers to use that data as they see fit.
- It has nurtured an online community so that security teams can crowdsource expertise, which customer references find valuable.



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change.

Validated by experts

MITRE Engenuity
Elastic stops ransomware and Linux threats in latest MITRE Engenuity Eval

Forrester XDR Wave
Elastic named in The Forrester Wave Report for XDR

Gartner Peer Insights
Users choose Elastic for Gartner Peer Insights Customer Choice Award

SIEM MQ
Gartner places Elastic in the 2021 Magic Quadrant for SIEM

Customer stories
Teams around the world use and love Elastic Security



OPSWAT.

VTENTERPRISE

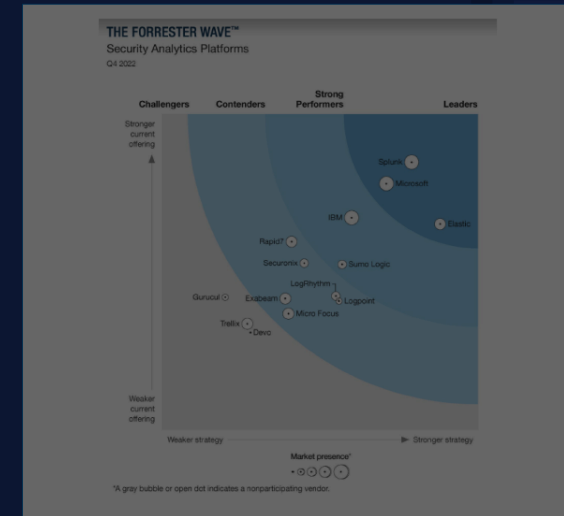
amtso

What others found out

Elastic Security

Elastic named a Leader in The Forrester Wave™ Security Analytics Platforms Q4 2022

- "Elastic provides incredible flexibility and visualizations in an open offering."
- "Reference customers value the flexibility on pricing and subsequent cost savings that Elastic provides."
- "Elastic Security best suits clients comfortable with security engineering looking for an extremely customizable product."



FORRESTER

WAVE LEADER 2022

Security Analytics Platforms

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change.



Thx + questions

