NetEye User Group 2023

21.09.2023
Romantik Hotel Rottner
Stein bei Nürnberg

Agenda

NetEye User Group 2023

- 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

NetEye User Group 2023

- 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

NetEye User Group 2023

- **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

NetEye User Group 2023

- **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

NetEye User Group 2023

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

elastic

NetEye User Group 2023

What does security need today?

Slow down the attackers

Speed up the defenders

Make it actionable at scale

elastic

Tasks

NetEye User Group 2023

Elastic Security

SIEM, Endpoint, Cloud

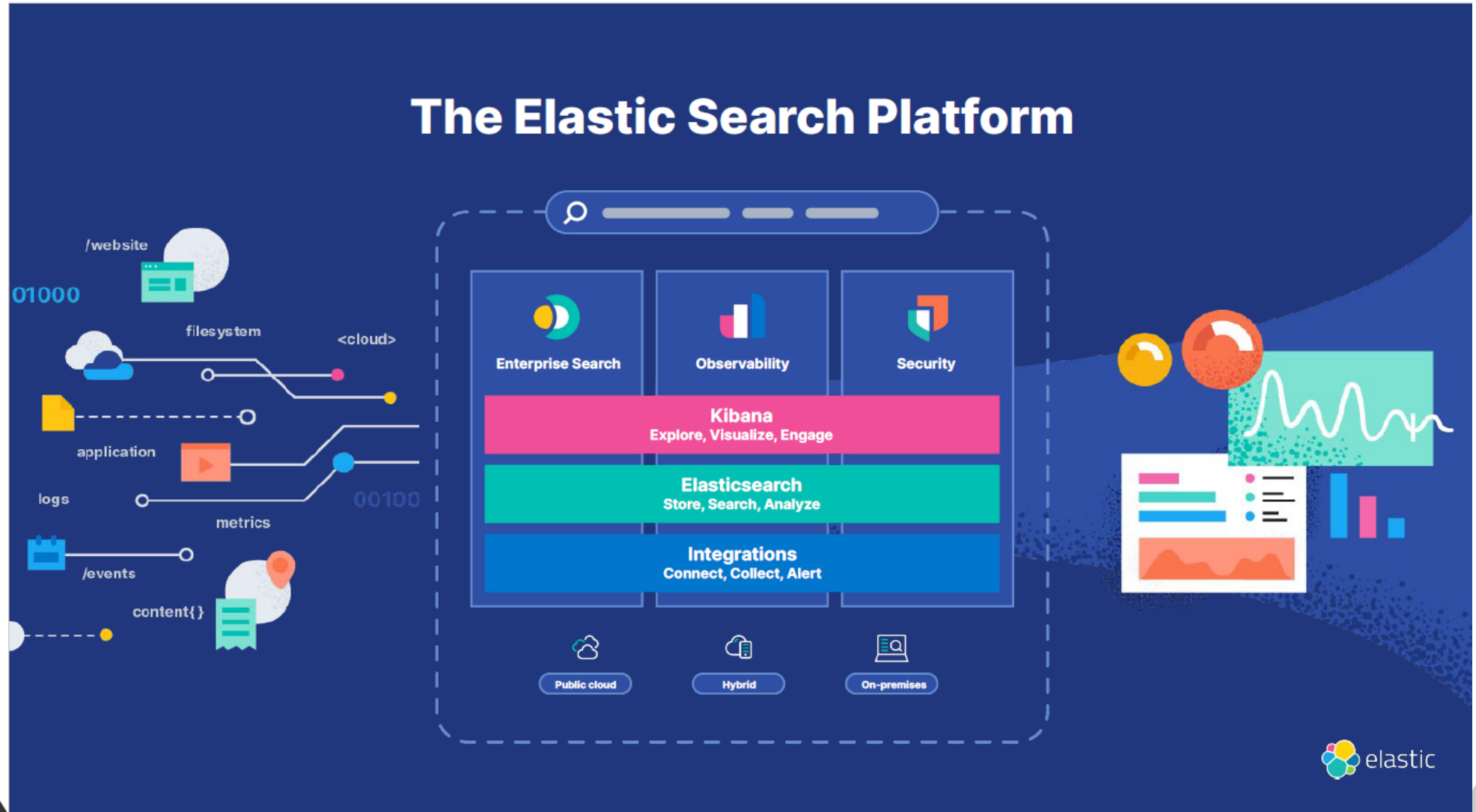
Monitoring and Compliance	Threat Prevention and Detection	Hunting and Incident Response

NetEye User Group 2023

NetEye User Group 2023

architecture

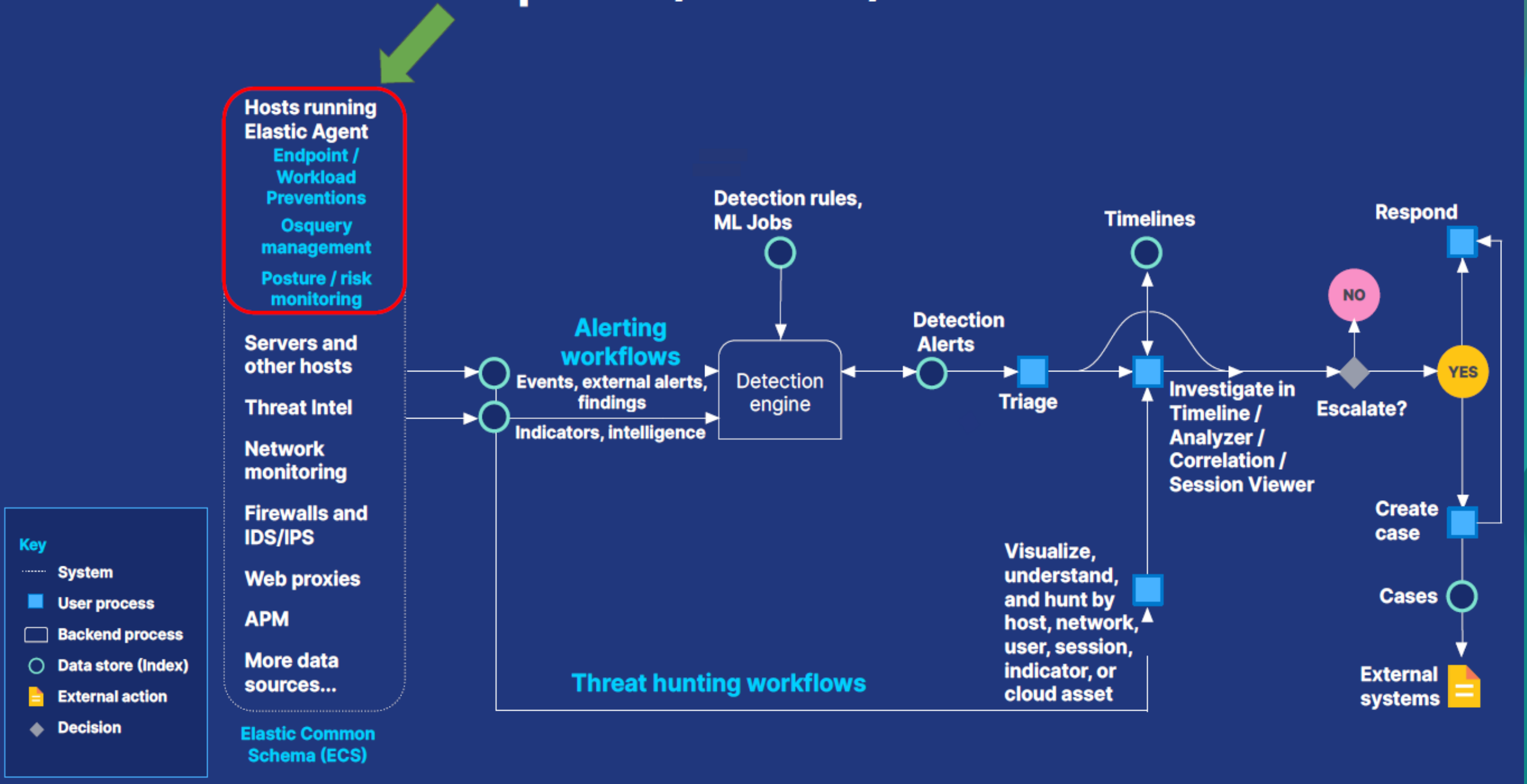
NetEye User Group 2023



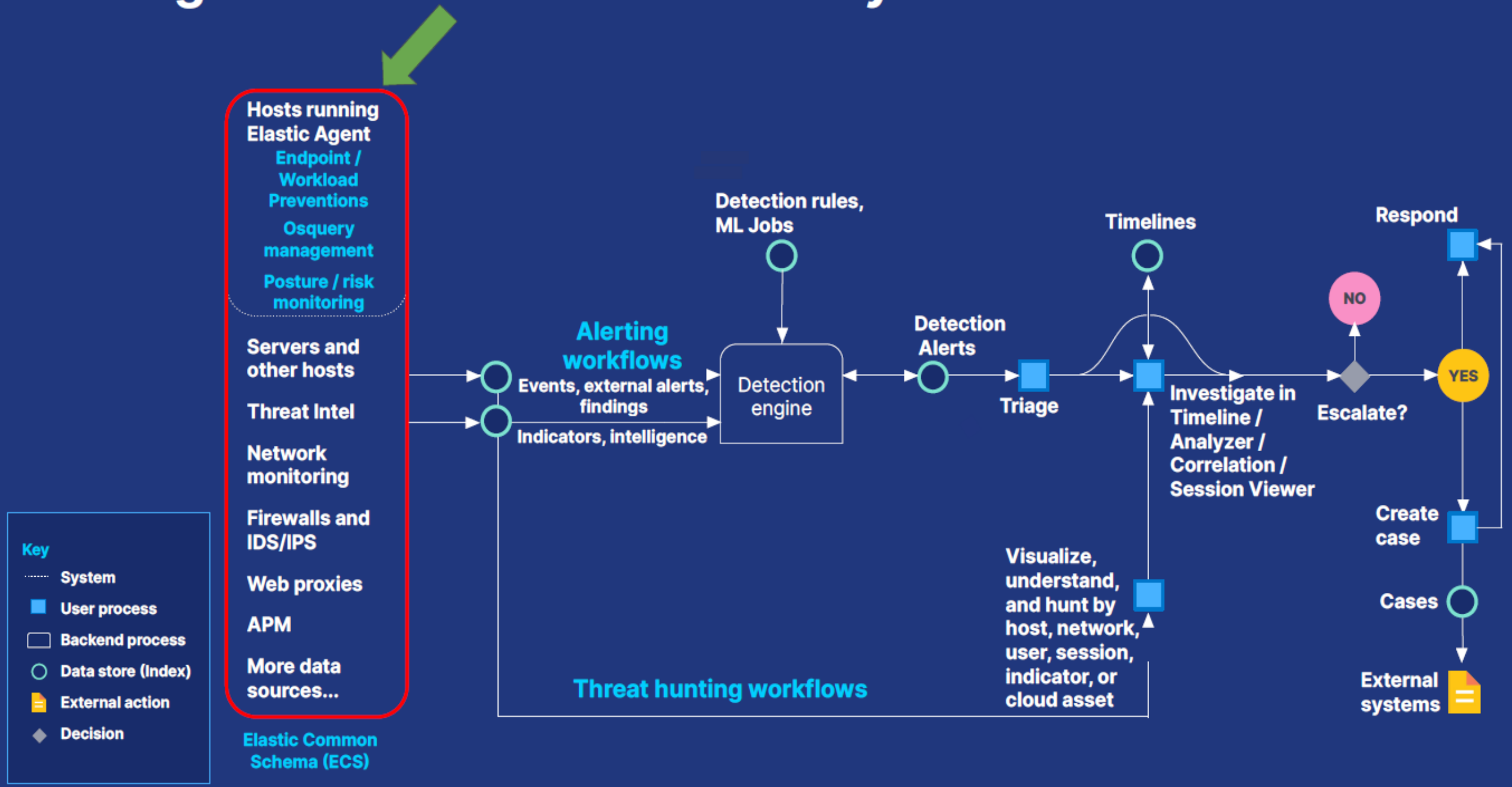
NetEye User Group 2023

QUICKLY SHOW WORKFLOW

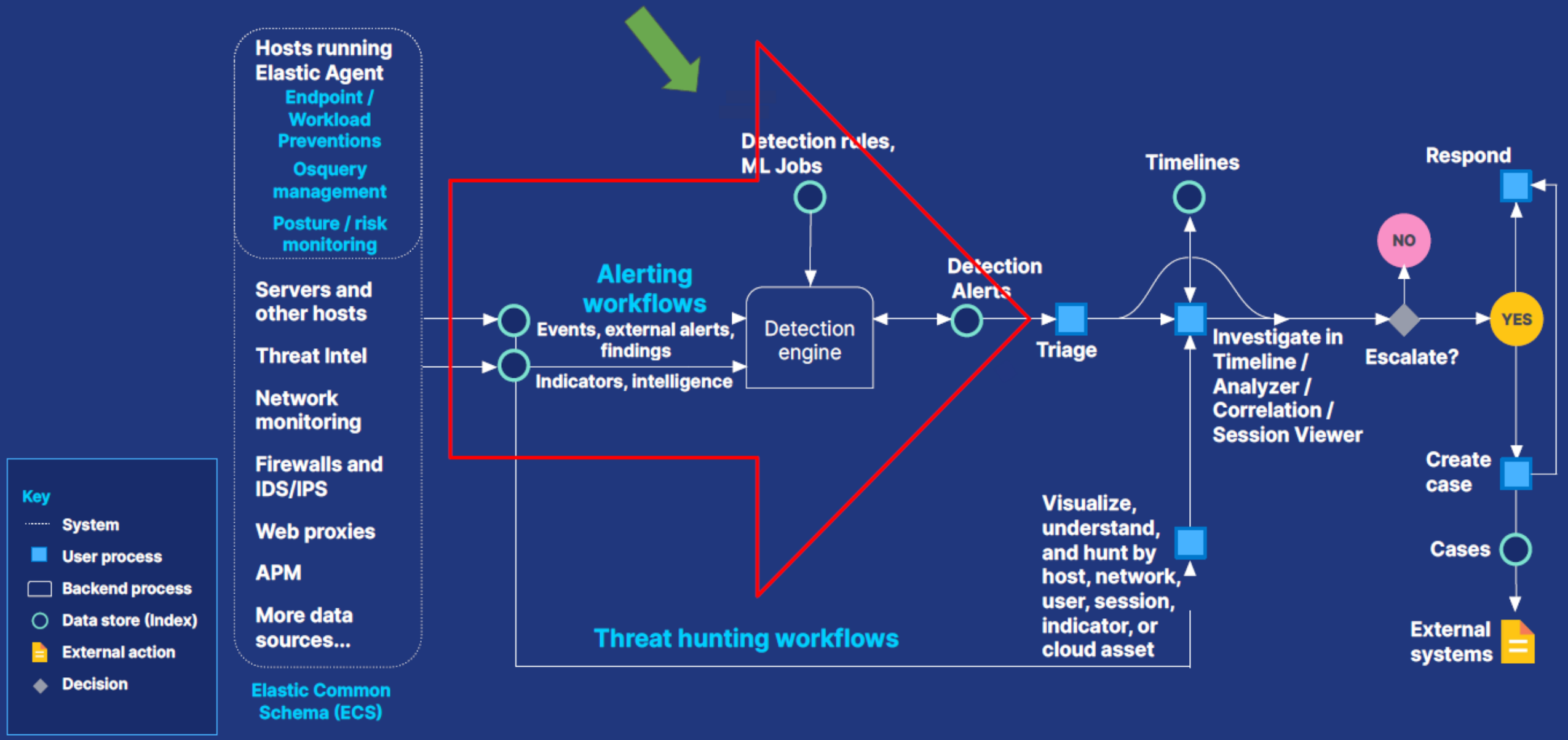
1. Protect the Endpoints/Assets/Workloads



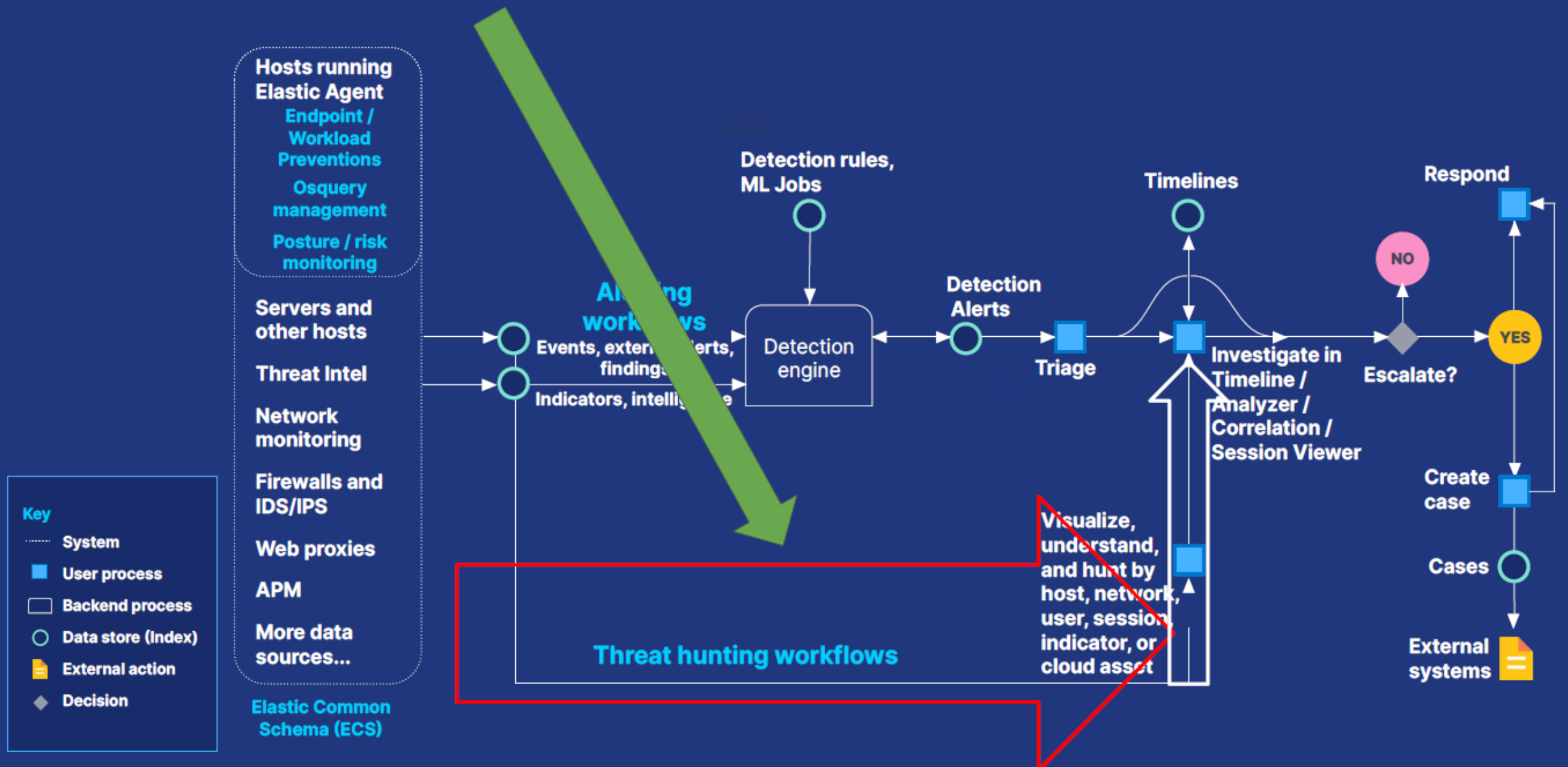
2. Ingest & Normalize All Security Data



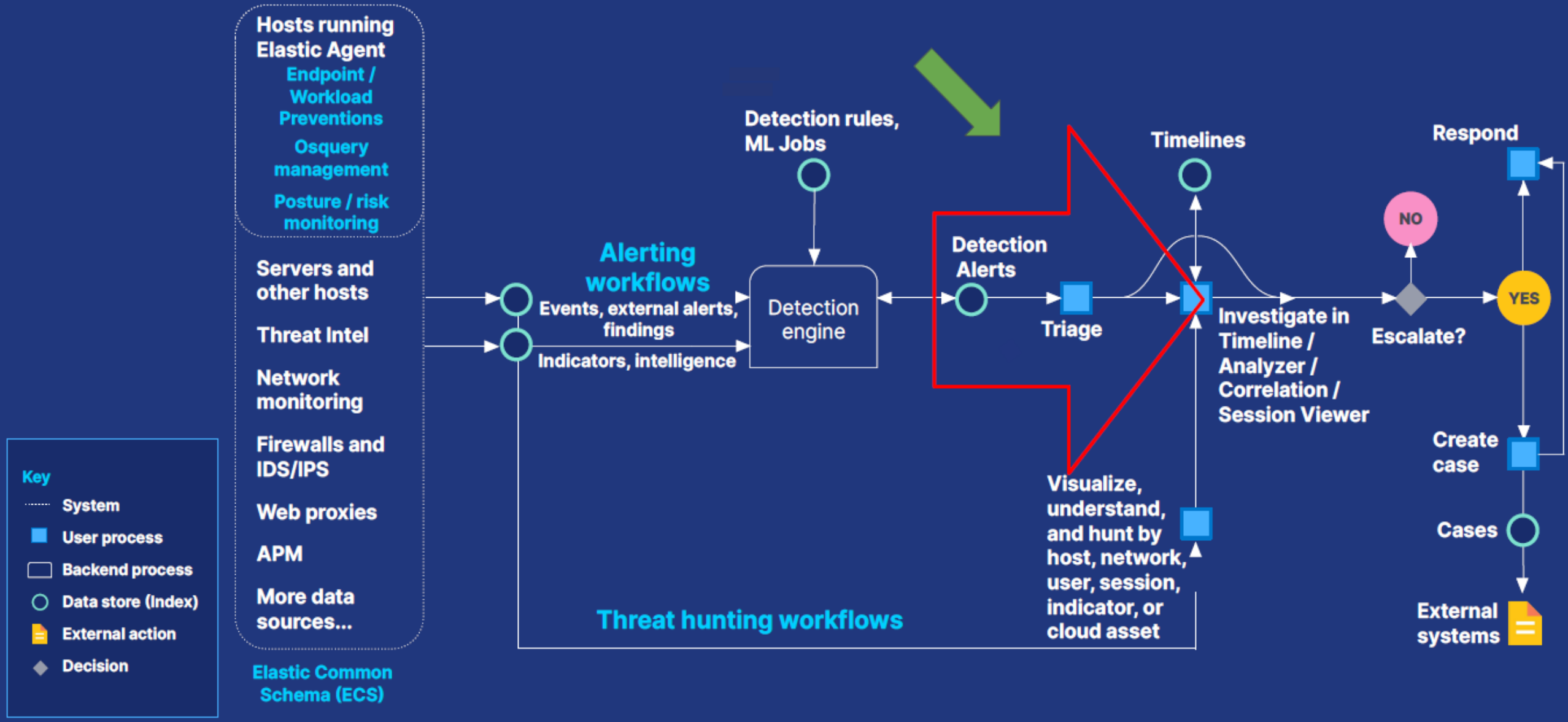
3. Automated Detection and Alerting



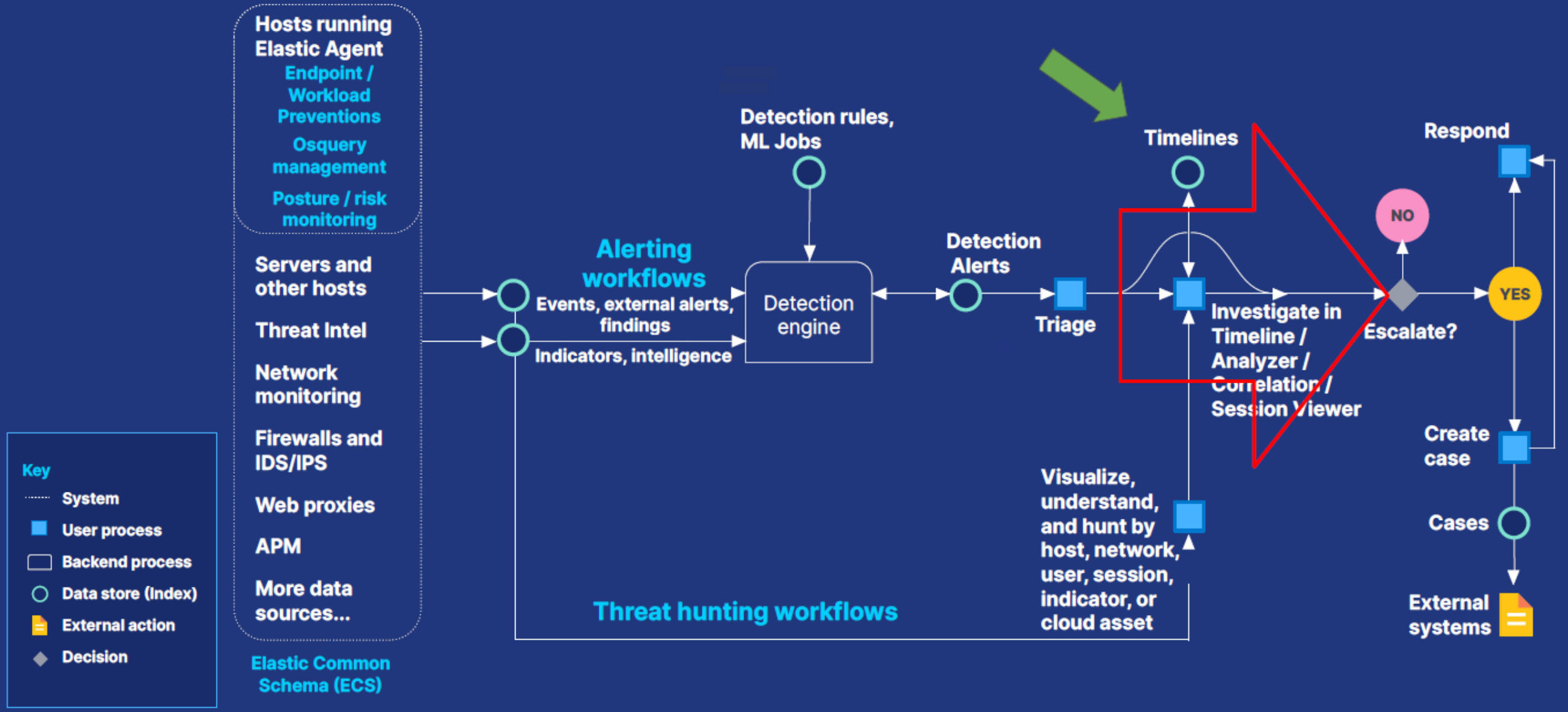
4. Threat Hunting



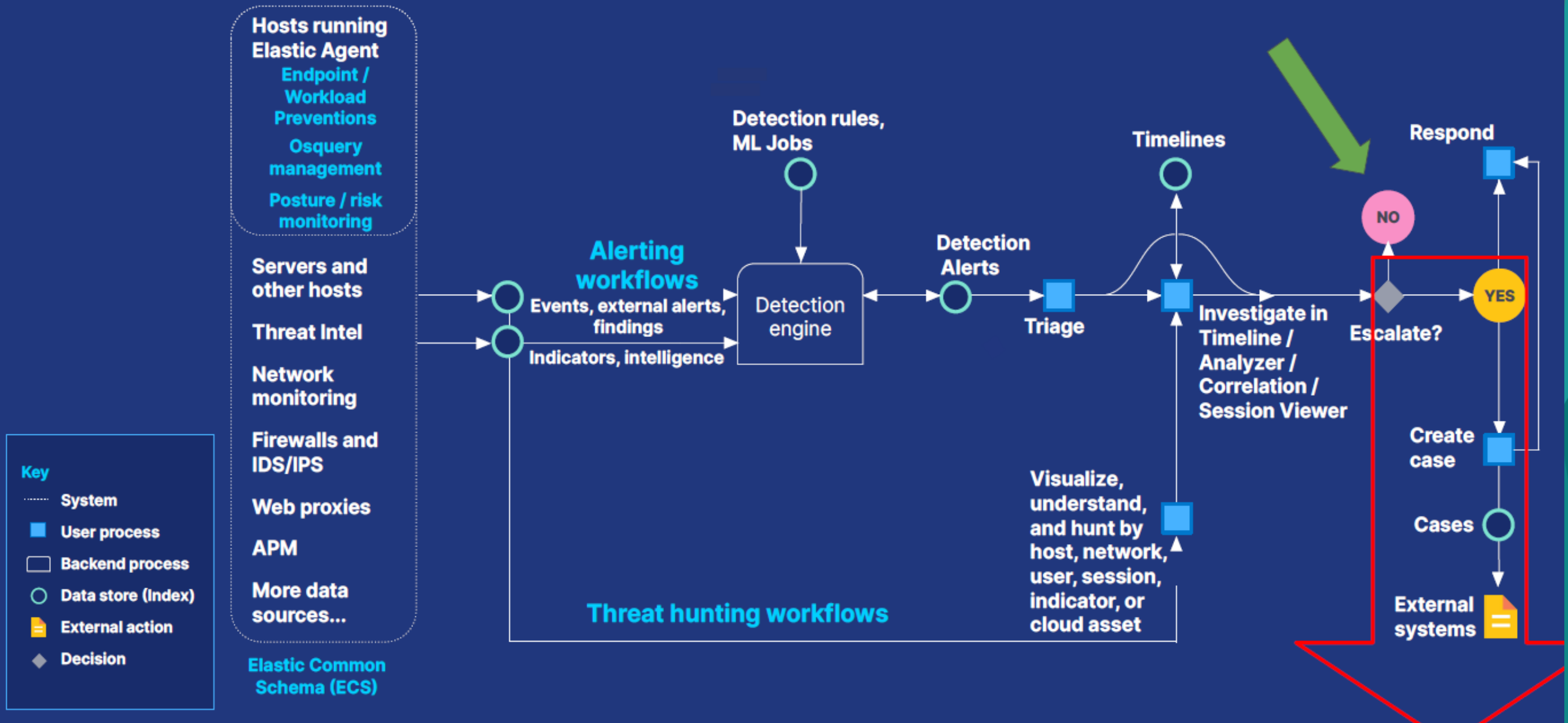
5. Alert Triage



6. Investigate



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)
Alerting workflows
Events, external alerts, findings
Indicators, intelligence
Detection rules, ML Jobs
Detection engine
Detection Alerts
Triage
Timelines
Investigate in Timeline / Analyzer / Correlation / Session Viewer
Escalate?
NO
YES
Respond
Create case
Cases
External systems
Visualize, understand, and hunt by host, network, user, session, indicator, or cloud asset
Threat hunting workflows
Key
System
User process
Backend process
Data store (Index)
External action
Decision

Agenda

NetEye User Group 2023

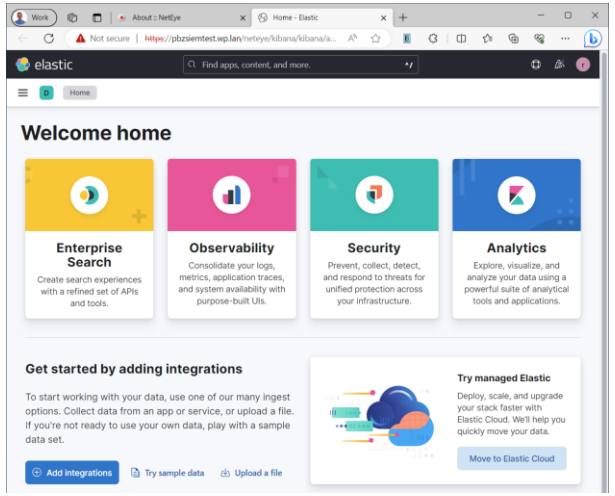
- Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten
- **Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic**
- Erfahrungen und Herausforderungen bei der Implementierung

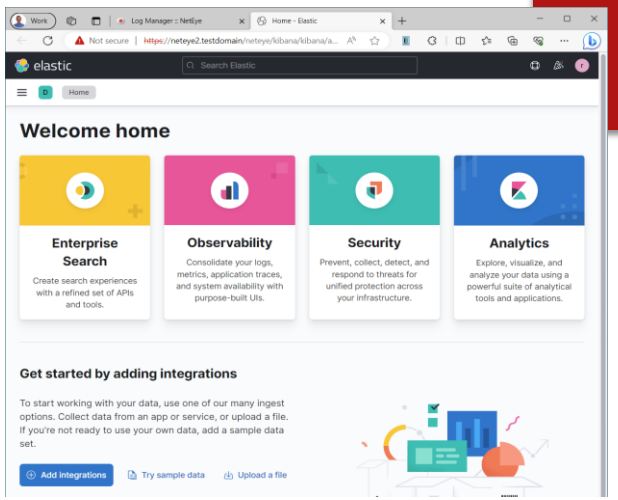
Agenda

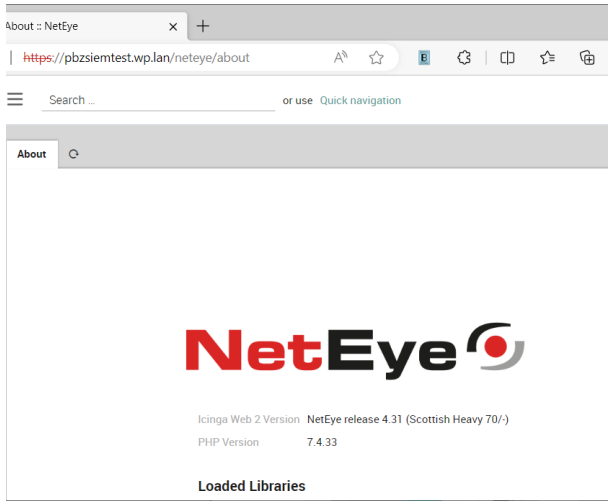
NetEye User Group 2023

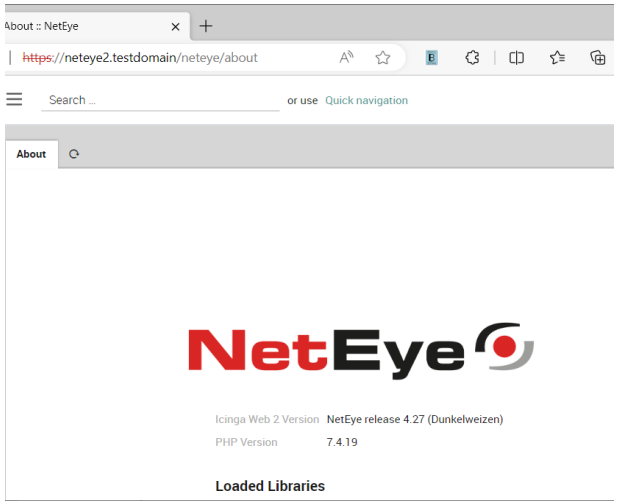
- Eine Einführung in Elastic und seine Bedeutung für die Suche und Analyse von Daten
- **Vorstellung von neuen Funktionen und Verbesserungen in NetEye SIEM powered by Elastic**
  - Neteye alt vs. neu
  - Liste einiger Änderungen
  - Benutzerfreundlichkeit
  - Performance

Changes?







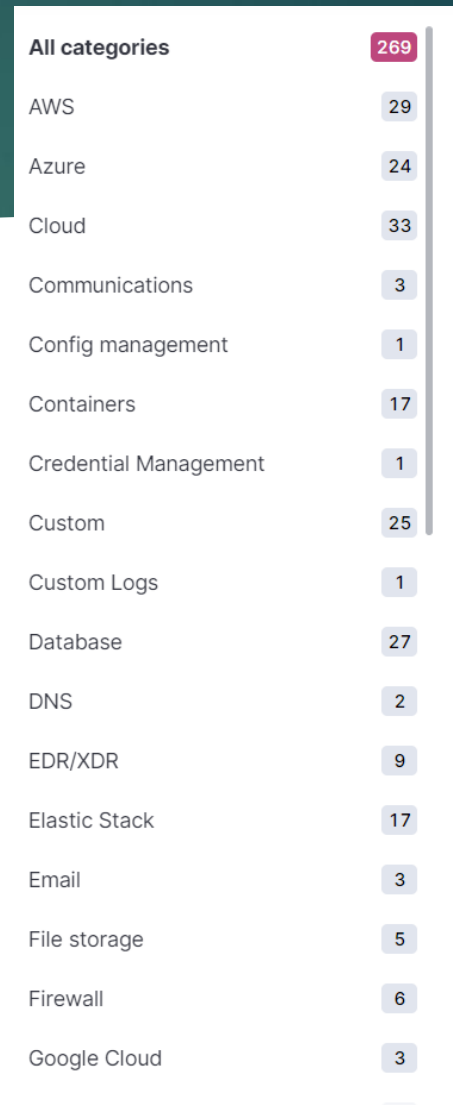


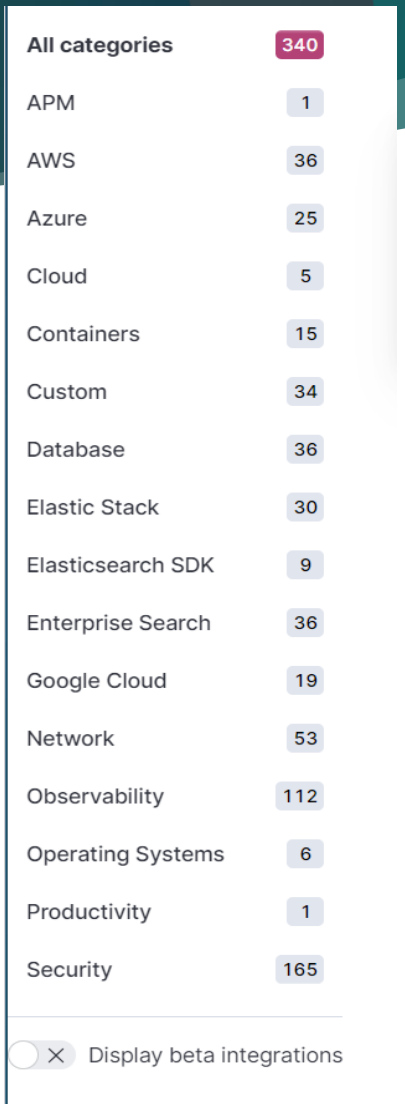
- NetEye 4.27 vs NetEye 4.31

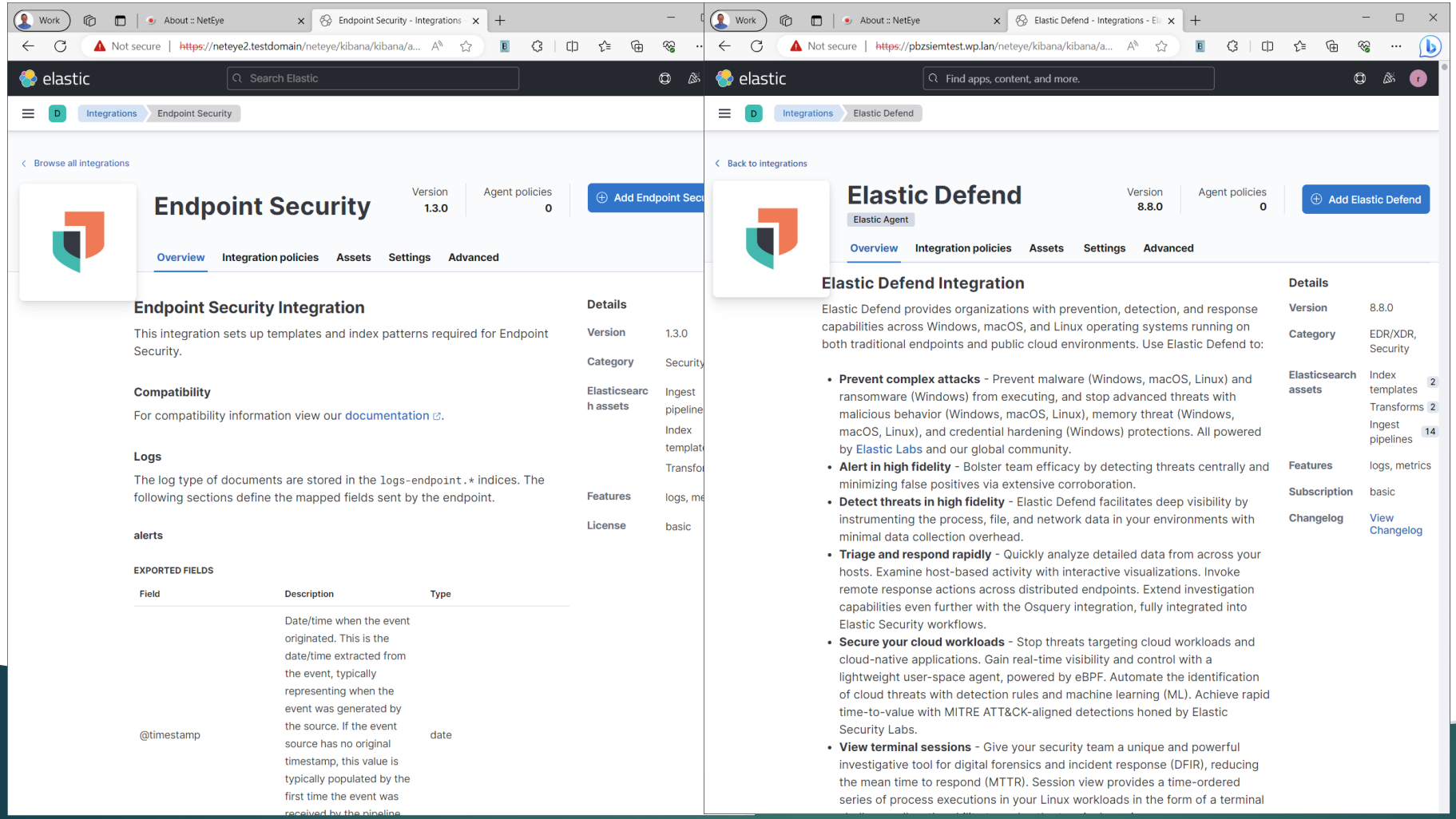
Some changes

NetEye User Group 2023

- 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…

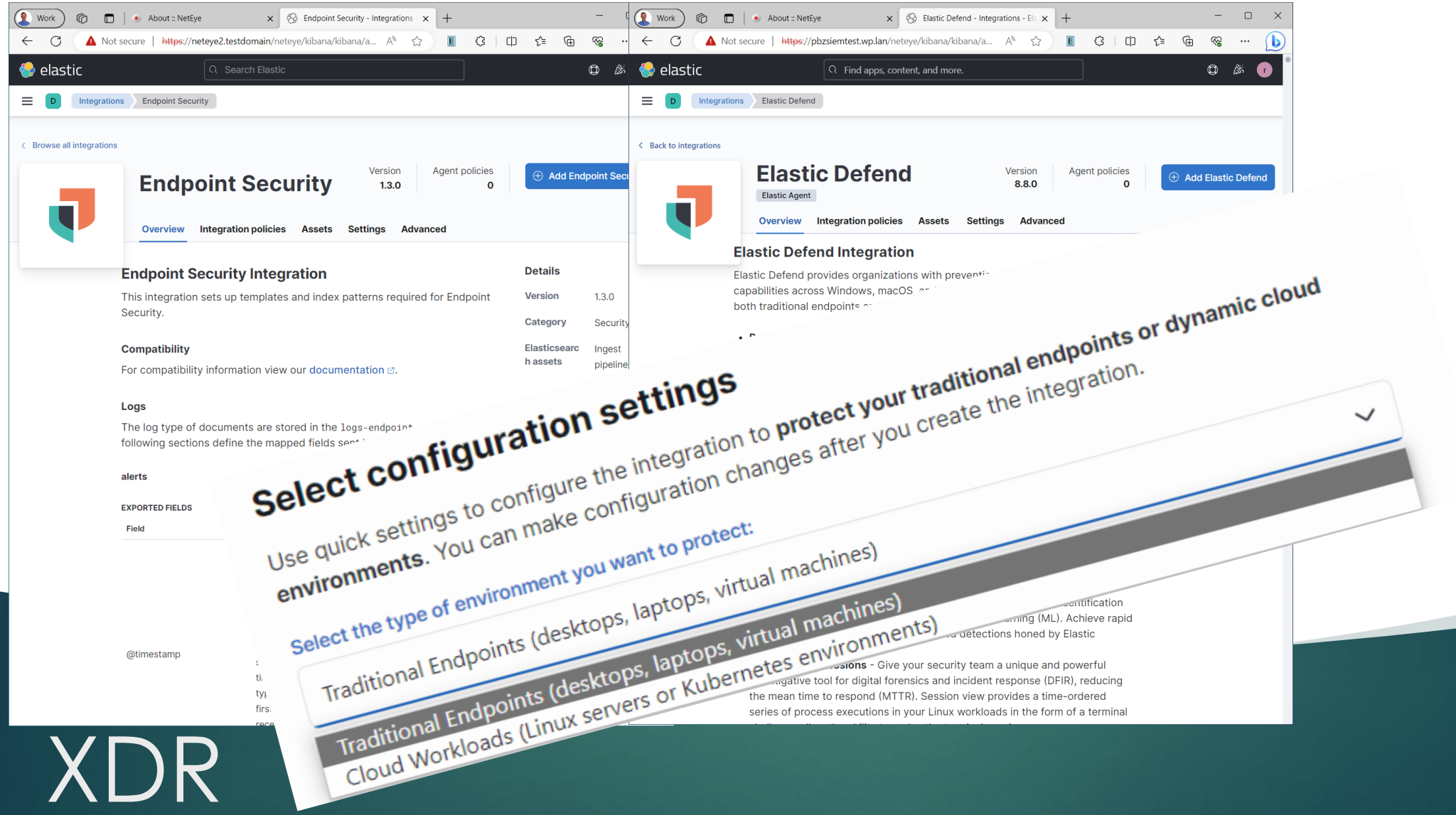






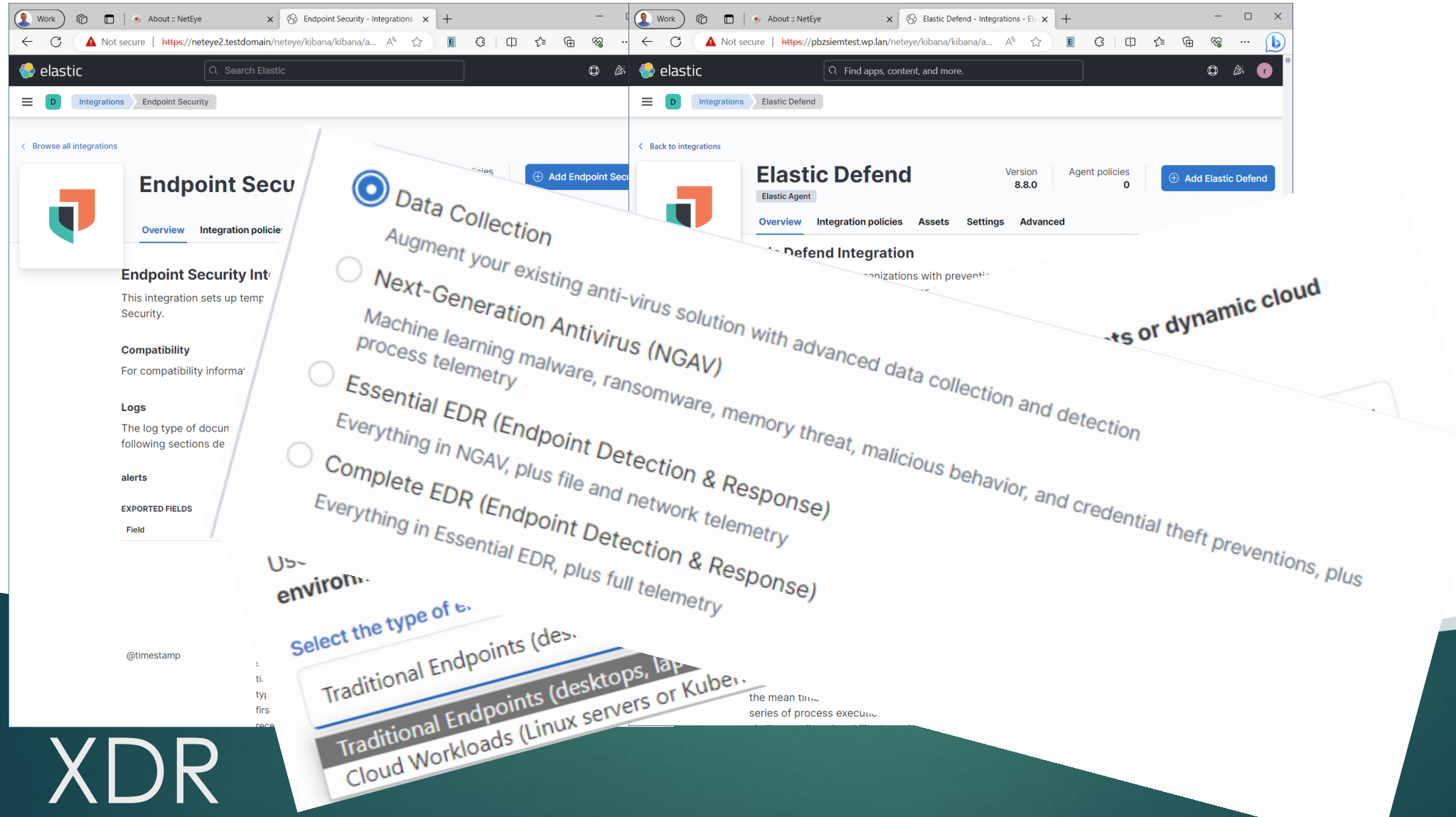
XDR

V 1.3.0 -> V 8.8.0



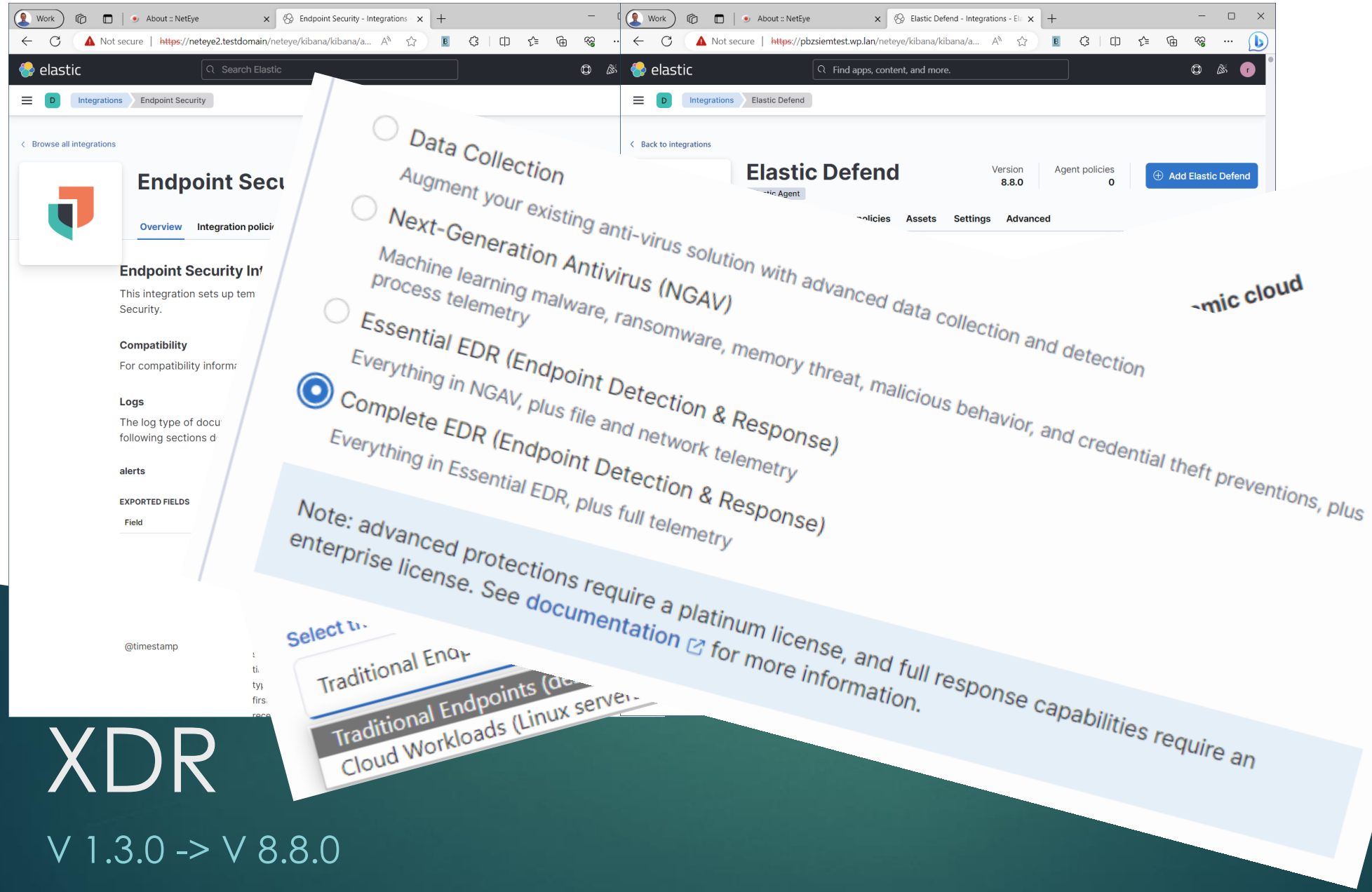
XDR

V 1.3.0 -> V 8.8.0



XDR

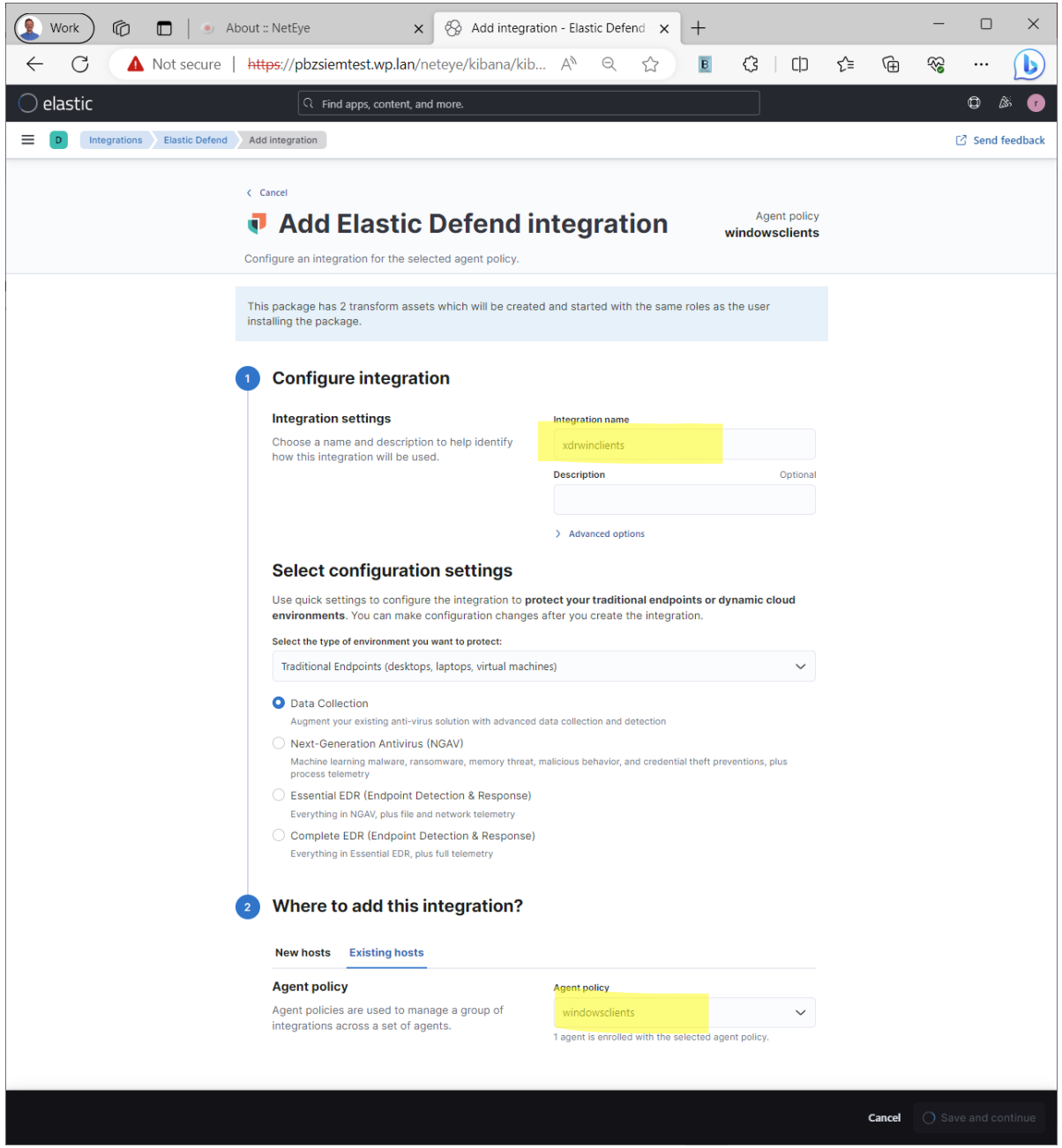
V 1.3.0 -> V 8.8.0



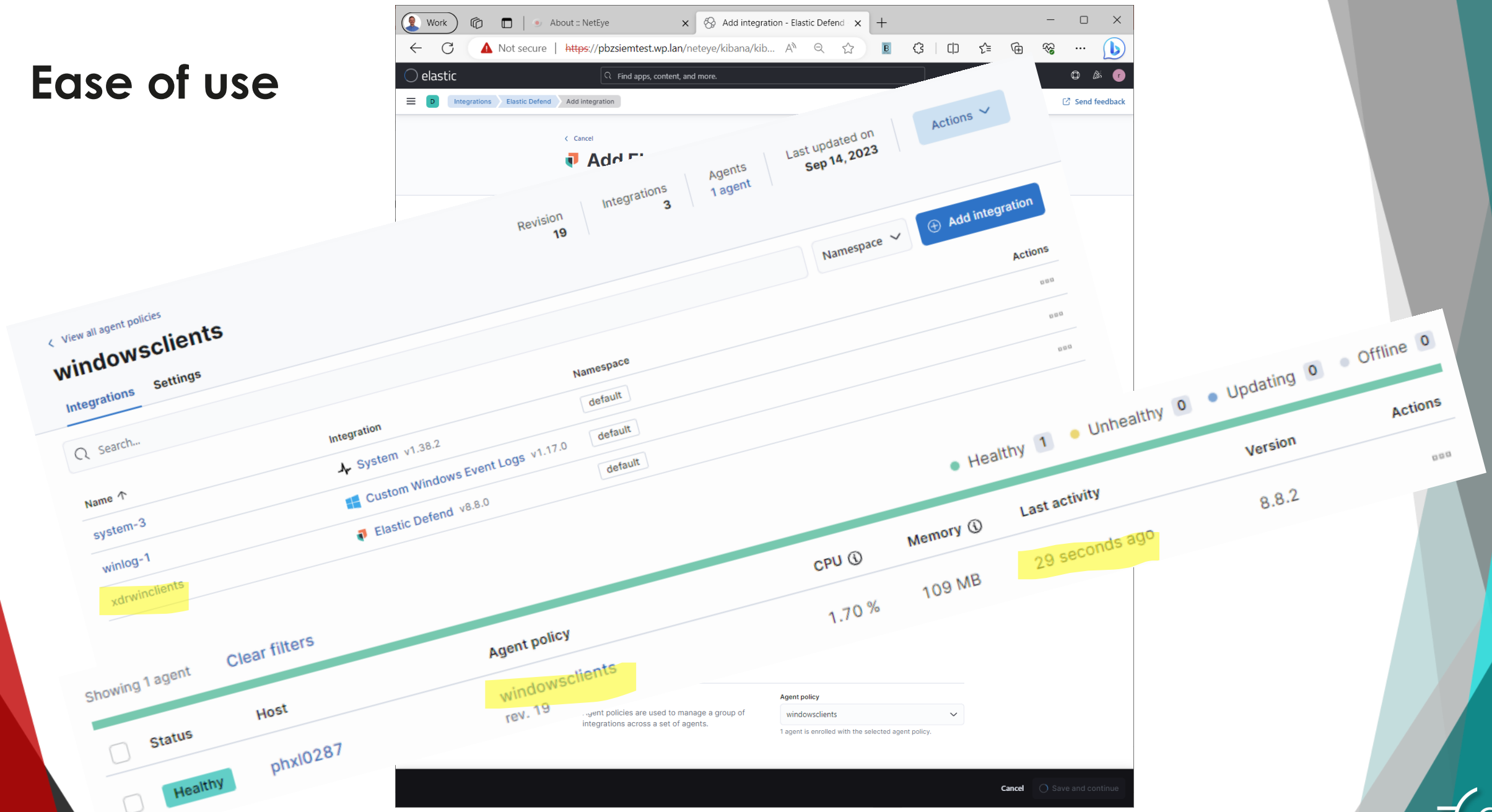
XDR

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


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
Revision 19
Integrations 3
Agents 1 agent
Last updated on Sep 14, 2023
Actions
Add integration
Namespace
Actions
View all agent policies
windowsclients
Integrations
Settings
Search...
Integration
Namespace
System v1.38.2
default
Custom Windows Event Logs v1.17.0
default
Elastic Defend v8.8.0
default
Name
system-3
winlog-1
xdrwinclients
Healthy 1
Unhealthy 0
Updating 0
Offline 0
Showing 1 agent
Clear filters
Agent policy
CPU
Memory
Last activity
Version
Actions
Status
Host
windowsclients
rev. 19
1.70 %
109 MB
29 seconds ago
8.8.2
Healthy
phxl0287
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

Agenda

NetEye User Group 2023

- 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

NetEye User Group 2023

- 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

NetEye User Group 2023

- 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

NetEye User Group 2023

- 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

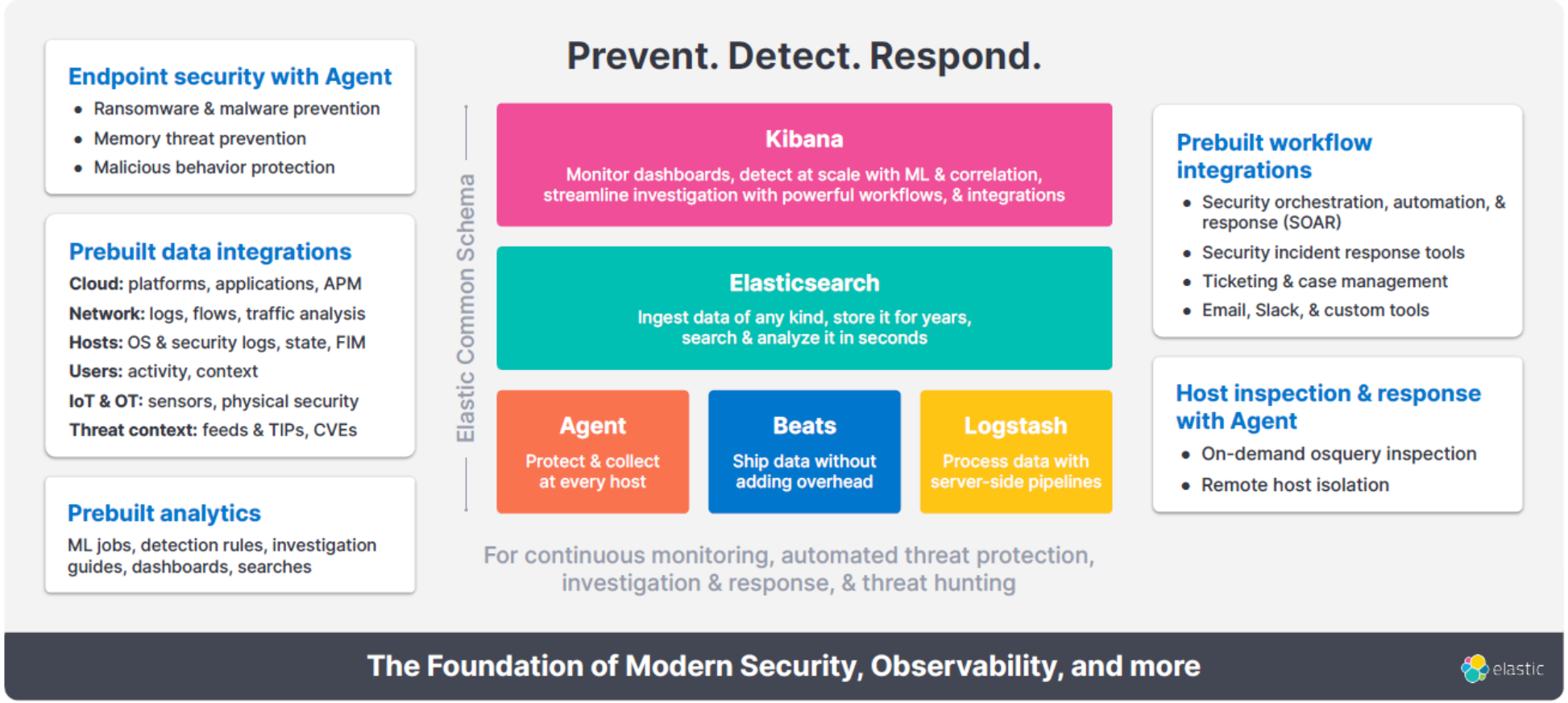
NetEye User Group 2023

- 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

NetEye User Group 2023

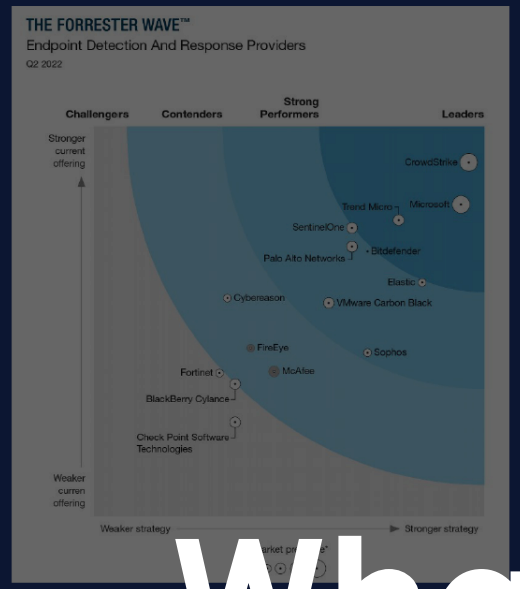
Elastic Security



What others found out

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.



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

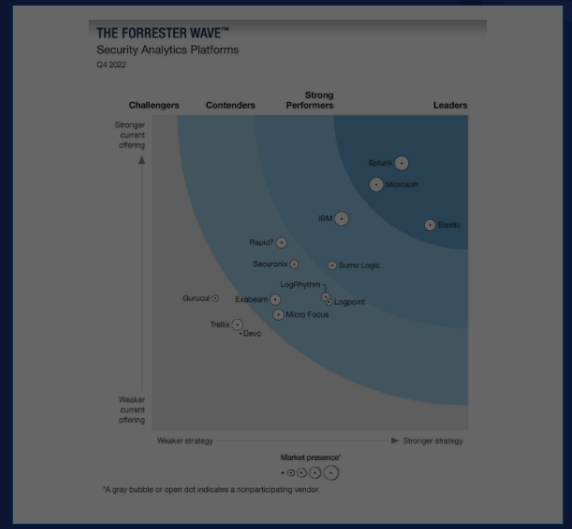
Customer stories
Teams around the world use and love Elastic Security

AV Comparatives · OPSWAT · VTENTERPRISE · amtso

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

elastic

Thx + questions

NetEye User Group 2023