…more than
software,
your IT partner

NIS2-Richtlinie und Umsetzung

Richtlinien zur Erhöhung der Cybersicherheit

WÜRTHPHOENIX

About

Patrick Zambelli

- NetEye project consulting basierend auf Produkt-Portfolio von Würth Phoenix
- Focus auf Monitoring and SIEM Usecases
- Curious about what's outside in this infinite world of usecases to discover
- Like the mountains … even with snow on it

NetEye
IT Monitoring
ecosystem
NetEye cloud

sec4U
Offense / Defense
SOC

satayo
SEARCH ALL THINGS ABOUT YOUR ORG
Cyber Threat Intelligence

Managed Services
Dynamics 365 + BI + CRM
Pimcore, eShop, …

GLPI ATLASSIAN
Project Management
Service Management
Asset Management
ITSM & ESM

NIS - Verbesserung der Cyberabwehr

Regelwerk zur Umsetzung wesentlicher Sicherheitsrichtlinen

NIS2

Network and Information Systems Directive 2

Umfassendes EU-Regelwerk zur Definition von **Abwehrstrategien für Cyber-Bedrohungen**

Merkmale:

1. Ausweitung der Sektoren nach Wichtigkeit
2. Effektive Benachrichtigung von Security Incidents
3. Fokus auf Lieferketten
4. Stärkung nationaler Stellen für Cyber-Angelegenheiten
5. Verantwortung & Sanktionen
6. Compliance vs. Security

NIS2 – Wer ist betroffen ?

WER

- private und öffentliche Organisationen in der EU
- Lieferketten von Organisationen (auch Nicht-EU)

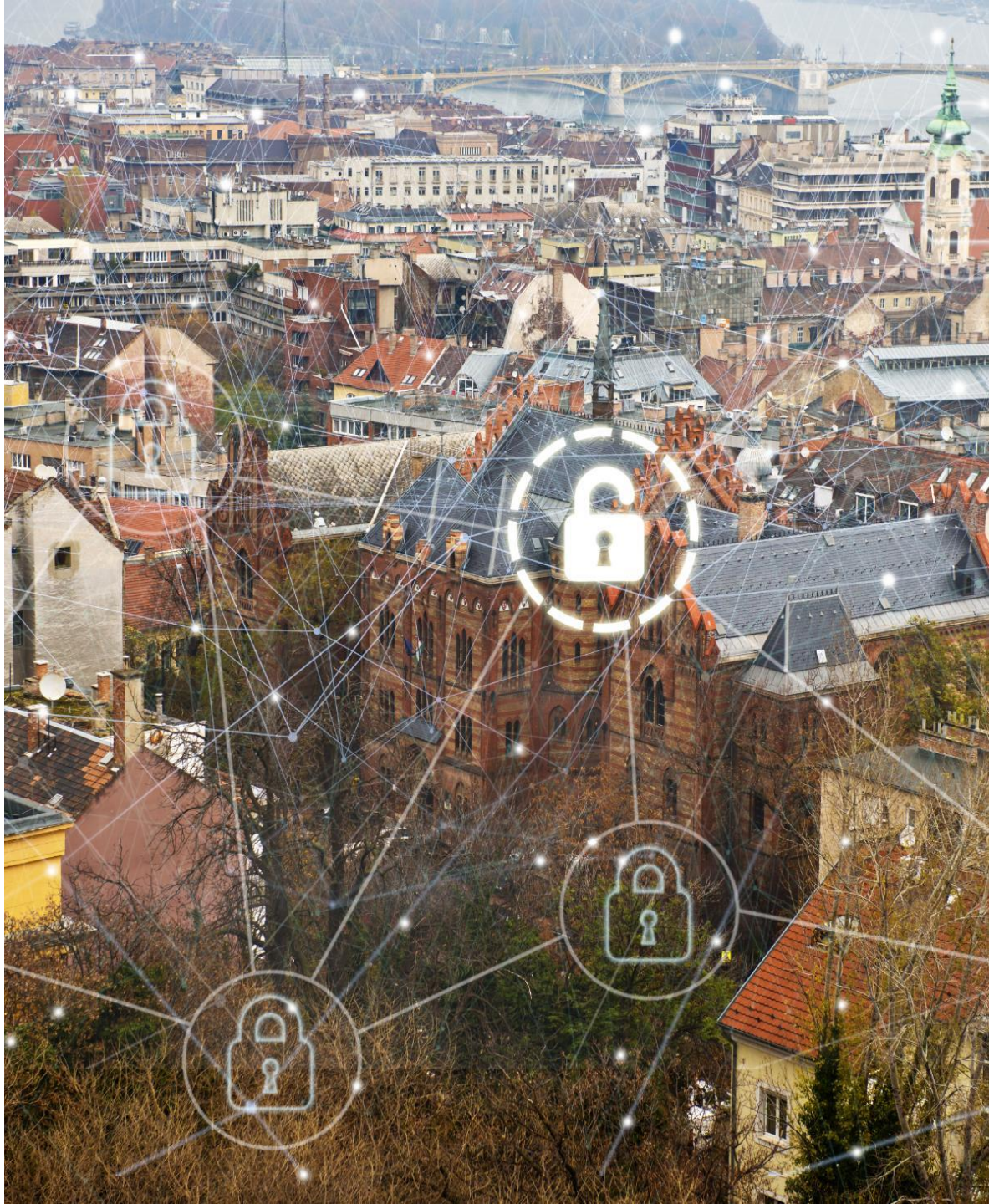
Termine

- Verabschiedung EU-Parlament Dezember 2022
  RICHTLINIE 2022/2555 (NIS2)
- Übernahme NIS2-Richtlinie in nationale Gesetzgebung durch Mitgliedsstaaten innerhalb Oktober 2024
- Juli 2024 wird der Gesetzentwurf zur Umsetzung im deutschen Recht vorgelegt.

Klassifizierung

- Besonders wichtige u. kritische Einrichtungen „KRITIS“ mit hoher Bedeutung für Gesellschaft und Wirtschaft
  Große Unternehmen im Bereich Energie, Transport, Finanzen, Gesundheit, Infrastrukturen, IT
- Wichtige Bereiche
  Große und Mittlere Unternehmen aus relevanten Teilsektoren bzw. Lieferketten

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html



NIS2 – Anforderungen zur Umsetzung

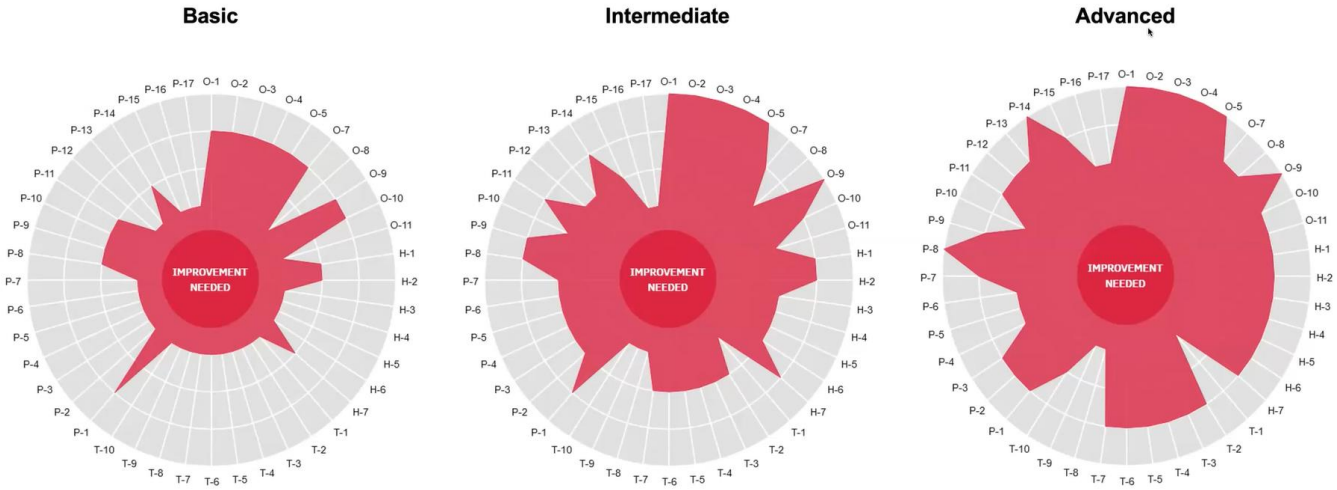
- **Cyber-Risikomanagement**
  Verankerung im Top-level Management
  Persönliche Haftung
  Bedeutende Strafen
- **Technische und organisatorische Maßnahmen**
  Überwachung und Erkennung mittels geeigneter Tools
- **Vorfallmanagement u. Meldepflichten**
  Prozesse zur Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen
  a) Cyberangriffe, b) Datenlecks: c) Systemausfälle: d) Manipulation von IT-Systemen
- **Geschäftskontinuität**
  Aufrechterhaltung Betrieb im Falle eines Cybervorfalls
  Regelmäßige Überprüfungen zur Einhaltung der Sicherheitsstandards
- **Schulung und Sensibilisierung**
  Sensibilisierung für Cyber-Sicherheitsrisiken

Security Frameworks

Compliance vs. Security ?

ENISA

- Europäische Agentur für Cyber-Sicherheit
- Beratung > Zusammenarbeit > Sensibilisierung für EU Instituzionen
- Cybersecurity Reifemodelle
- Angleich der EU-Bestimmungen an bestehende Frameworks wie SIM3



EUROPEAN UNION AGENCY FOR CYBERSECURITY

[ENISA: SIM3 self-assessment tool](https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity/sim3-v2i)

SIM3

Security Incident Management Maturity Model

- Erhebung der Reife von CSIRT and SOC team
- Praxisorientierte Erhebung

Vier Hauptkategorien:

- **O**rganisation: Strukturelle und organisatorische Aspekte
- **H**uman: Fähigkeiten, Schulung und Rollen der Mitarbeiter
- **T**ools: Technische Werkzeuge und Ressourcen.
- **P**rozesse: Verfahren und Arbeitsabläufe

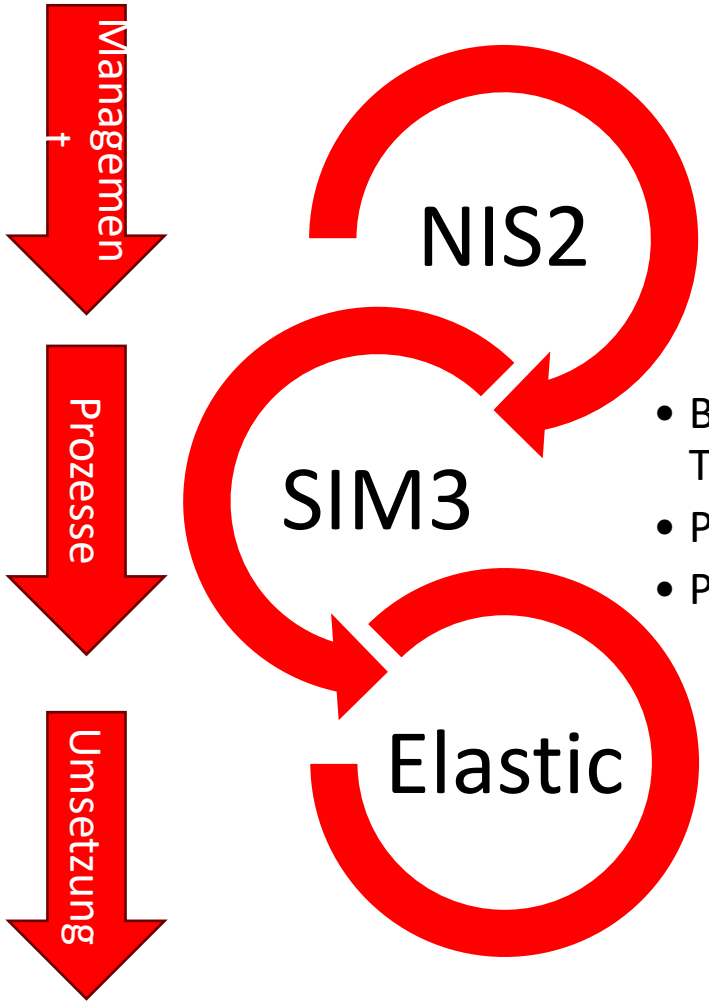
Definiert durch „Open CSIRT“ Foundation

Table 1- Overview of SIM3v2i parameters [12]

Parameter number	Parameter description	Parameter number	Parameter Description
O-1	Mandate	T-6	Resilient Messaging
O-2	Constituency	T-7	Resilient Internet Access
O-3	Authority	T-8	Incident Prevention Toolset
O-4	Responsibility	T-9	Incident Detection Toolset
O-5	Service Description	T-10	Incident Resolution Toolset
O-6	Public Media Policy	P-1	Escalation to Governance Level
O-7	Service Level Description	P-2	Escalation to Press Function
O-8	Incident Classification	P-3	Escalation to Legal Function
O-9	Participation in CSIRT Systems	P-4	Incident Prevention Process
O-10	Organisational Framework	P-5	Incident Detection Process
O-11	Security Policy	P-6	Incident Resolution Process
H-1	Code of Conduct/Practice/Ethics	P-7	Specific Incident Processes
H-2	Staff Resilience	P-8	Audit & Feedback Process
H-3	Skillset Description	P-9	Emergency Reachability Process
H-4	Staff Development	P-10	Best Practice Internet Presence
H-5	Technical Training	P-11	Secure Information Handling Process
H-6	Soft Skills Training	P-12	Information Sources Process
H-7	External Networking	P-13	Outreach Process
T-1	IT Assets & Configuration	P-14	Governance Reporting Process
T-2	Information Sources List	P-15	Constituency Reporting Process
T-3	Consolidated Messaging System(s)	P-16	Meeting Process
T-4	Incident Tracking System	P-17	Peer Collaboration Process
T-5	Resilient Voice Calls		

Umsetzung SIEM mit Elastic Security

NIS2 und SIM3 in Elastic Security



- Monitoring der Cyber-Threats, Schwachstellen und Sicherheitsvorfälle
- Meldung und Maßnahmen
- Risikomanagement und Analyse Cybersecurity Vorfälle

- Bewertung der Reife von Sicherheitsvorfall-Management-Teams
- Praxisorientierter Leitfaden
- Prozesse > Tools > Personen

- Anbindung der Log-Quellen
- Integration: Normalisierung und Aggregierung
- Analyse: Erkennung von Bedrohungen
- Response und Case-Management

SIEM: Relevante Log Quellen

- **Netzwerk**
  Access Layer wie Firewall, Switches, VPN-Gateway, Access Points, DNS
- **Servers**
  Authentication via Active Directory, Identity Provider
- **Client Endgeräte**
  EDR/Antivirus-Programme, Systemlogs/Sysmon
- **Cloud-Dienste**
  Azure mit Office365, Exchange Online, Teams
- **IT-Applikationen**
  Custom Application Stack,
  Cloud-Applikationen Openshift/Kubernetes
  IT/OT Landschaften

Anwendung Log-Quellen zur Erkennung eines Ransomware-Angriffs

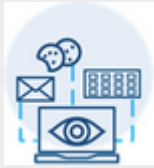
- **Netzwerk**
  Access Layer wie Firewall, Switches, VPN-Gateway, Access Points, DNS
- **Servers**
  Authentication via Active Directory, Identity Provider
- **Client Endgeräte**
  EDR/Antivirus-Programme, Systemlogs/Sysmon
- **Cloud-Dienste**
  Azure mit Office365, Exchange Online, Teams
- **IT-Applikationen**
  Custom Application Stack, Cloud-Applikationen Openshift/Kubernetes IT/OT Landschaften

Einbruch
RDP-Zugänge, Authentifizierungsereignisse nach Parameter IP, Standort, Computername.

Rechteerweiterung
Unübliche Nutzung Kommandozeile (Powershell)

Ausbreitung
Auslesen Anmeldedaten (Verwendung von Tools Mimikatz, Procdum, Zugriff Registry)
Auskundschaften Netzwerk (Scan Prozesse am Endpoint, LDAP Anfragen)

Verschlüsselung
Command & Control Kommunikation (HTTPS/Proxy Traffic)



Datenabfluss
Exfiltration von Daten (Zugriff Dateipfade)

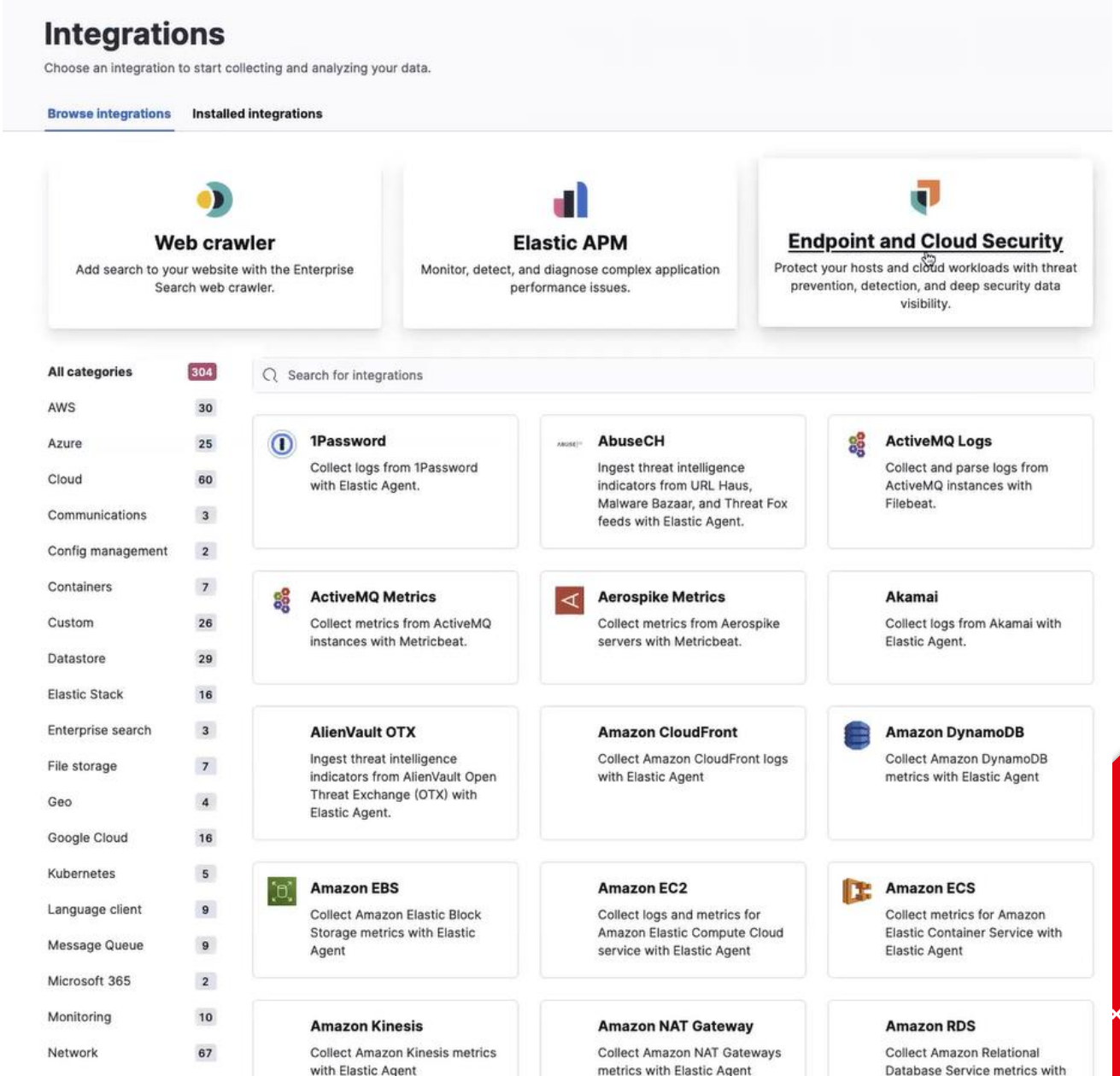
Datensammlung und aktive Abwehr

Prevent & Ingest

Detect & Investigate

Escalate & Responde

- Verteilung Elastic Agent
- Standardisierte Vorlagen für Datensammlung
- Verteilung der Konfigurationen
- Antivirus / EDR auf Clients



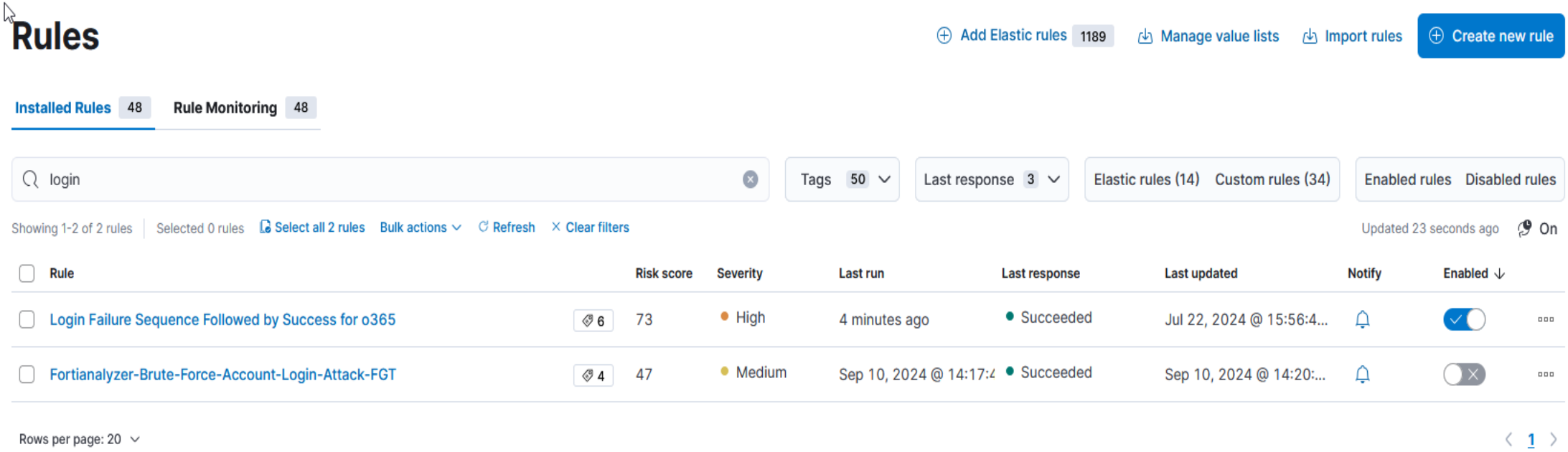
Erkennung und Analyse

Prevent & Ingest

Detect & Investigate

Escalate & Responde

- Rules: Abgestimmt an Vorlage für Datensammlung
- Optimierung der False-Positives durch Pflege von Ausnahmen (80-20 Regel/Pareto Rule)
- Detektion Logik mit ML Unterstützung (zB. Erkennung Anomalie)
- Erweiterbar durch Custom Rules



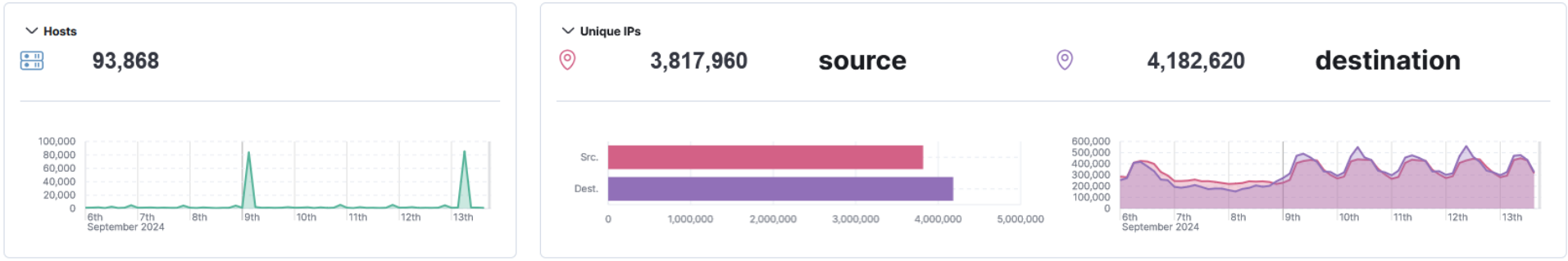
Erkennung und Analyse

Prevent & Ingest

Detect & Investigate

Escalate & Responde

- Erkennungs-Logik mit ML-Unterstützung (zB. Erkennung Anomalie)
  - Host: Untypische Prozesse,
  - User: Unübliche Logins / Anzahl Login Versuche



Events | All hosts | Uncommon processes | Anomalies | Host risk

Uncommon processes

Showing: 768 processes

Process name	Hosts	Instances	Host names	Last command	Last user
CredentialEnrollmentManager.exe	1	1	[redacted]	C:\Windows\system32\CredentialEnrollmentManager.exe	[redacted]
CredentialUIBroker.exe	1	1	[redacted]	C:\Windows\System32\CredentialUIBroker.exe +2 More	[redacted]
DeskUpdateNotifier.exe	1	1	[redacted]	C:\Program Files (x86)\Fujitsu\DeskUpdate\DeskUpdateNotifier.exe	[redacted]
DisplaySwitch.exe	1	1	[redacted]	DisplaySwitch.exe	[redacted]

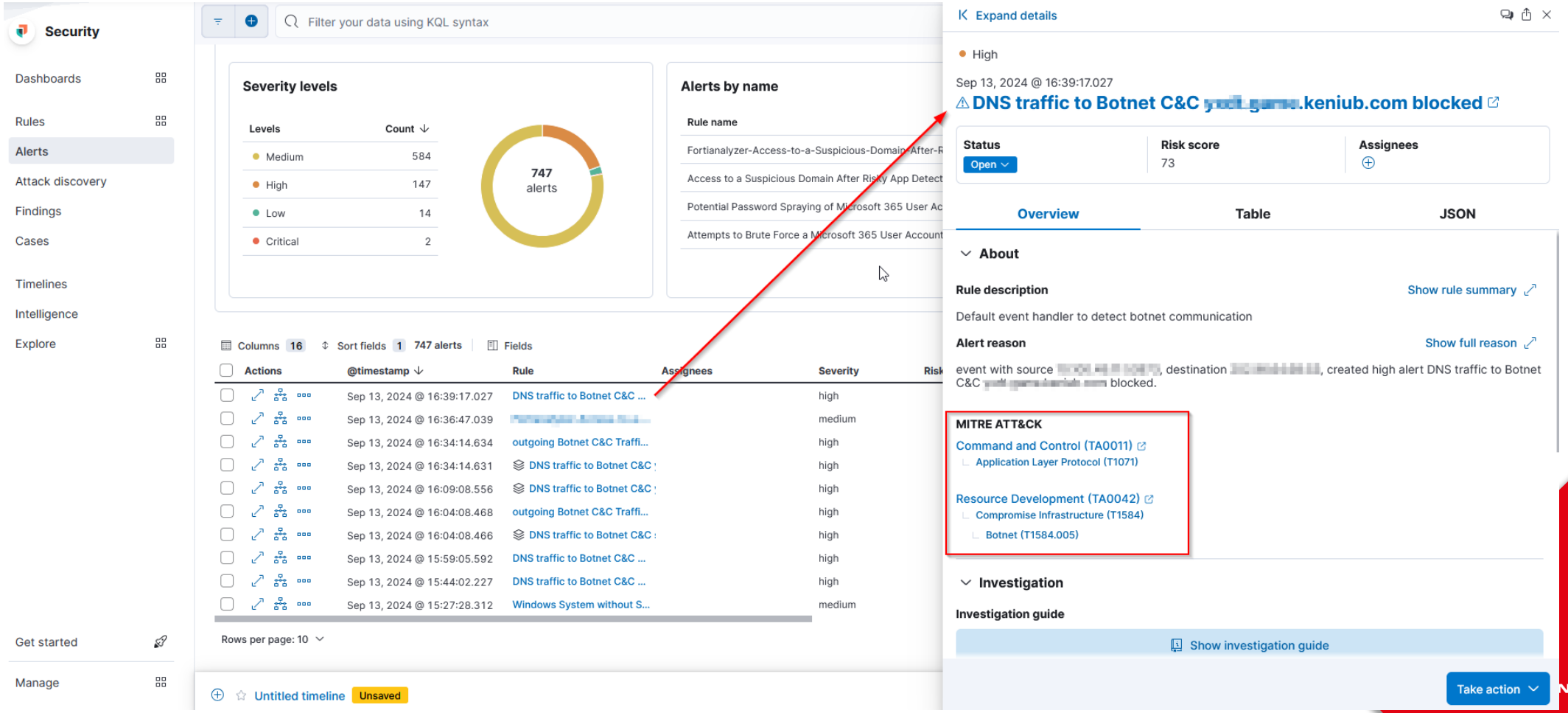
Erkennung und Analyse

Prevent & Ingest

Detect & Investigate

Escalate & Responde

- Alert nach Erkennung durch Rule
- Mapping nach Mitre Attack&Tactiques / Severity Scoring



Erkennung und Analyse/Reaktion

Prevent & Ingest

Detect & Investigate

Escalate & Responde

- Interaktive Analyse am Endpoint
- Auswertung Prozesse
- Isolation des Hosts

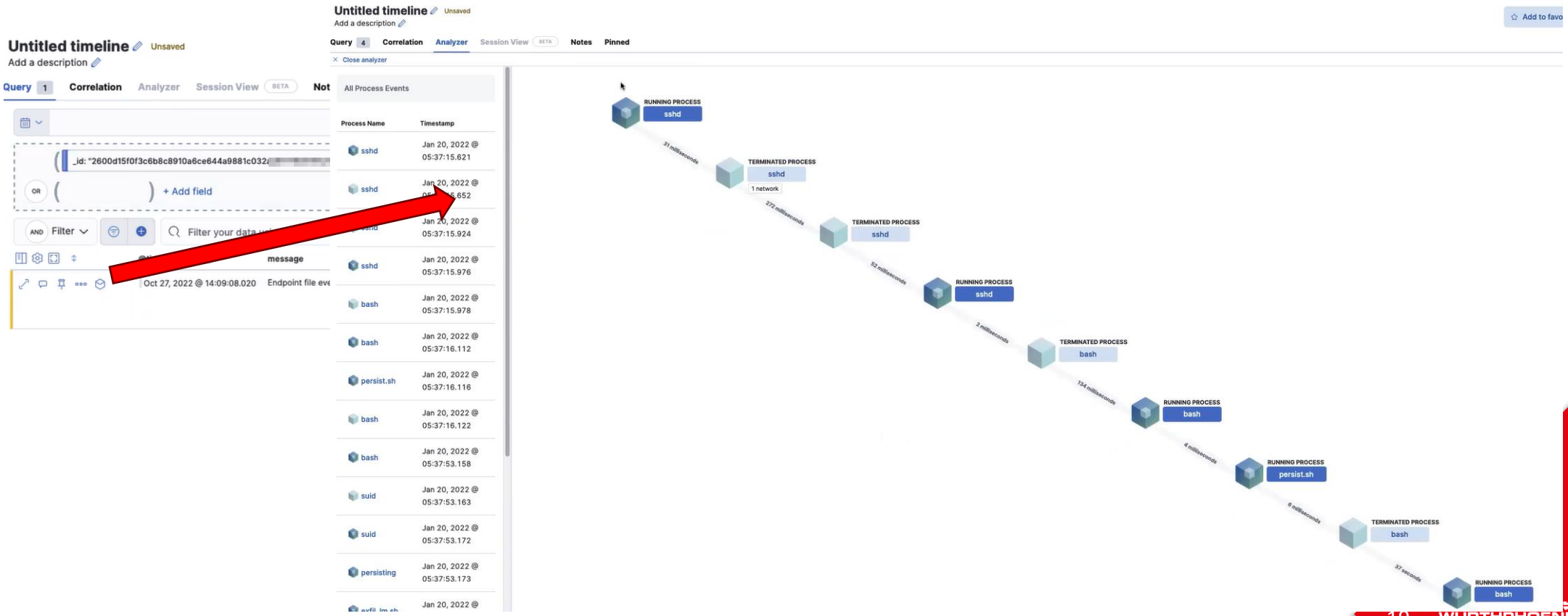
Erkennung und Analyse/Reaktion

Prevent & Ingest

Detect & Investigate

Escalate & Responde

- Interaktive Analyse am Endpoint
- Auswertung Prozesse
- Isolation des Hosts



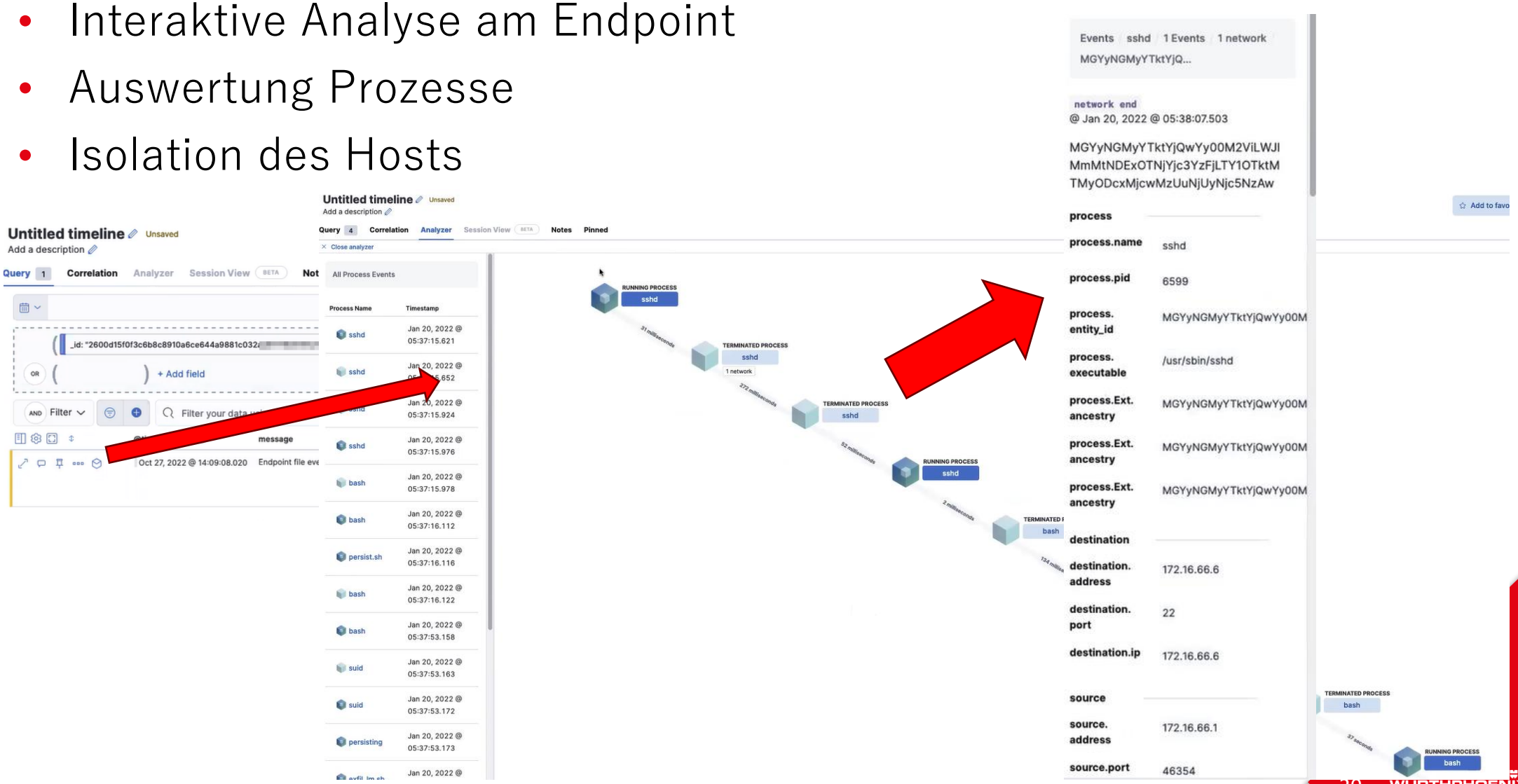
Erkennung und Analyse/Reaktion

Prevent & Ingest

Detect & Investigate

Escalate & Responde

- Interaktive Analyse am Endpoint
- Auswertung Prozesse
- Isolation des Hosts



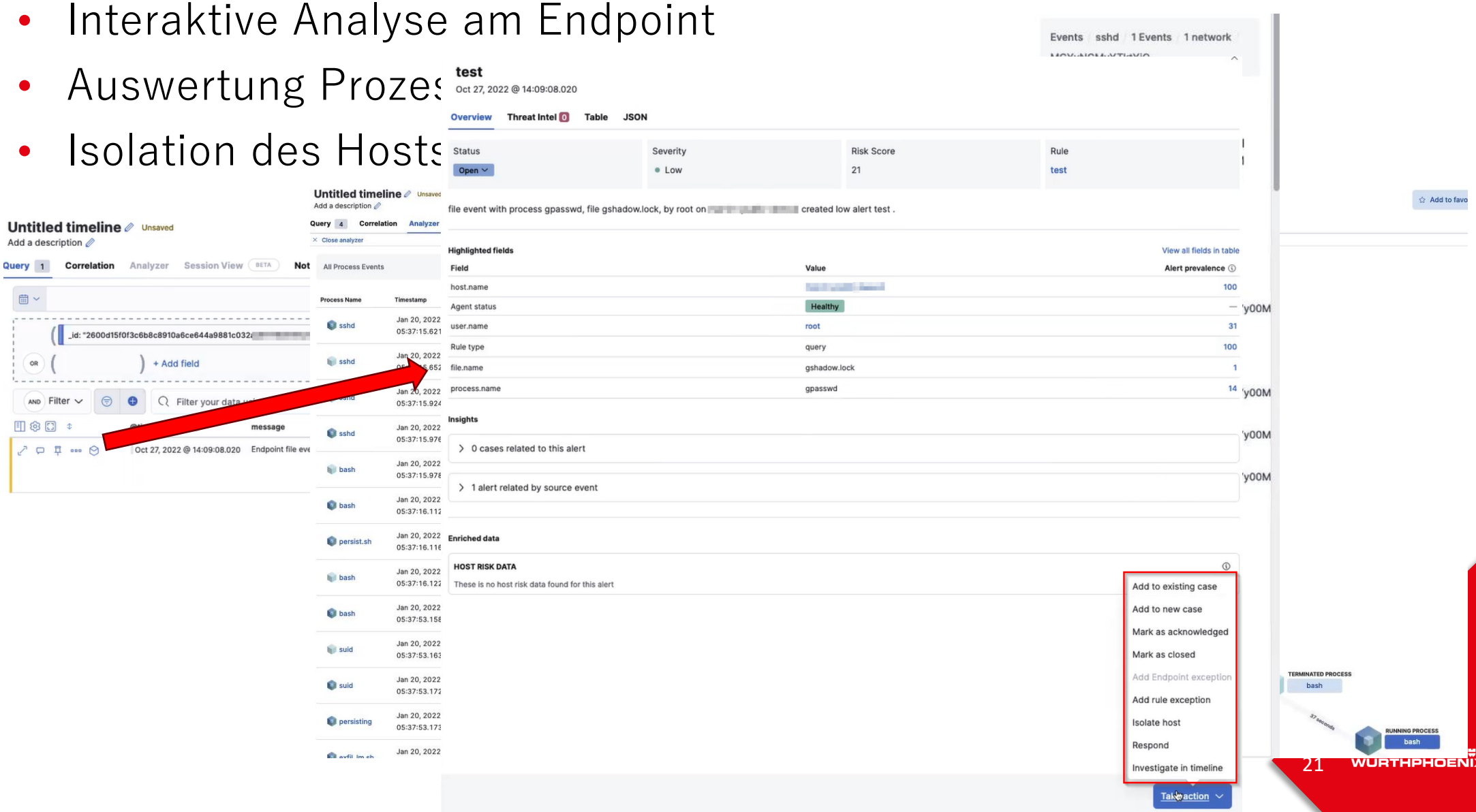
Erkennung und Analyse/Reaktion

Prevent & Ingest

Detect & Investigate

Escalate & Responde

- Interaktive Analyse am Endpoint
- Auswertung Prozes
- Isolation des Hosts



Meldeprozess und Reaktion

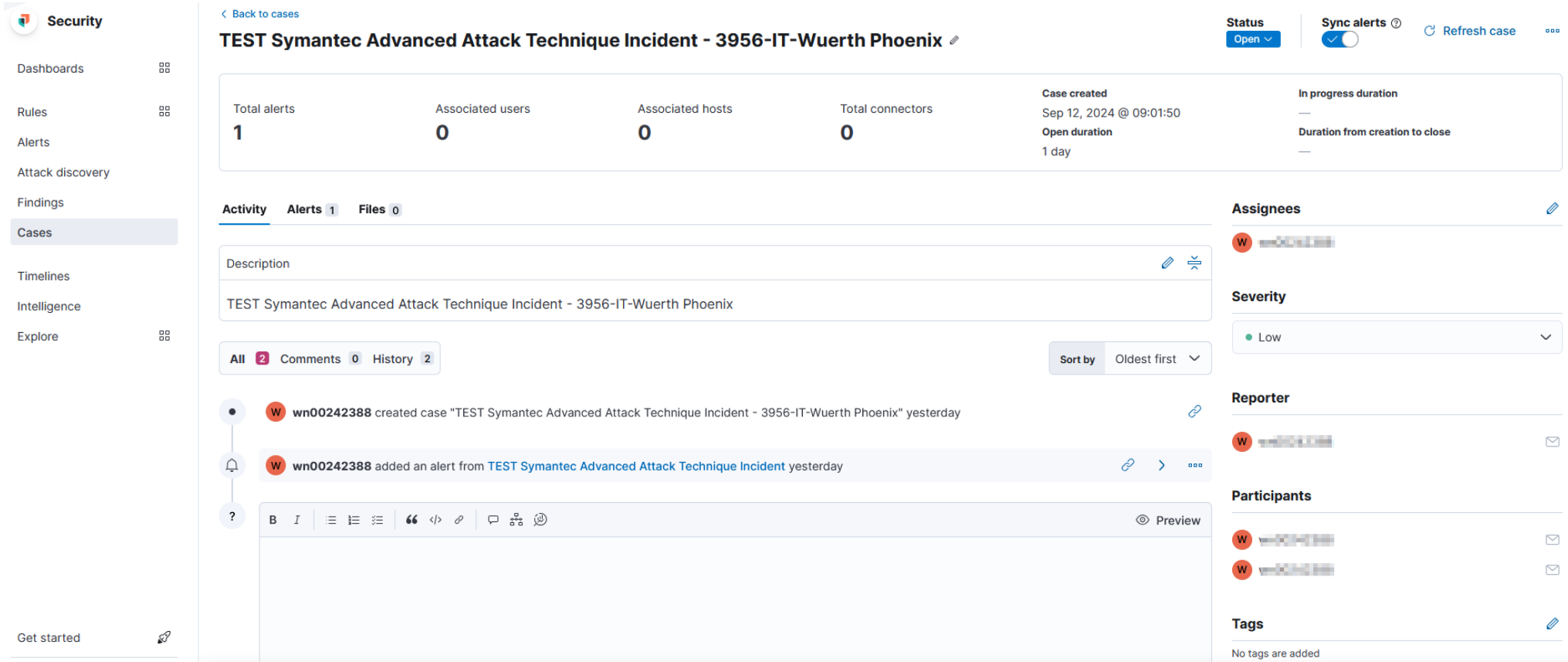
Prevent & Ingest

Detect & Investigate

Escalate & Responde

Meldeprozess via „Case“

- Incident Details für Analyst
- Eskalation via Connector



NIS2:
Was gilt es zu tun ?

Handlungsempfehlung NIS2

- Thema NIS2 einsteigen
- Relevanz der Regelung für das Unternehmen bewerten
- Bewusstsein entwickeln, in Massnahmen zur Cybersicherheit zu Investieren und in die Praxis umsetzen.
- Internes Know-How nutzen, externe Unterstützung einbeziehen
- Bestehende Mangementsysteme nutzen zB. ISO 27001 (zB. Bestehendens Risikomanagement)
- Systeme zur Erkennung und Reaktion von Cyber-Bedrohungen vorsehen

NIS2

…more than software, your IT partner

20/09/2024

Gesamtheitliche Überwachung

NetEye

WÜRTHPHOENIX