



...more than  
software,  
your IT partner

# NIS2-Richtlinie und Umsetzung

*Richtlinien zur Erhöhung der Cybersicherheit*

# 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

**satay**  
SEARCH ALL THINGS ABOUT YOUR ORG

Cyber Threat Intelligence

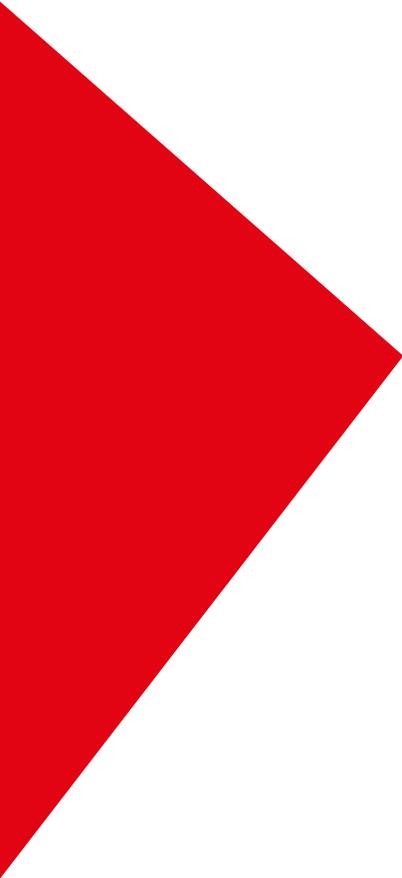
**Managed Services**

Dynamics 365 + BI + CRM  
Pimcore, eShop, ...



**GLPI** **ATLASSIAN**

Project Management  
Service Management  
Asset Management  
ITSM & ESM



NIS - Verbesserung der Cyberabwehr

Regelwerk zur Umsetzung wesentlicher  
Sicherheitsrichtlinien

# 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

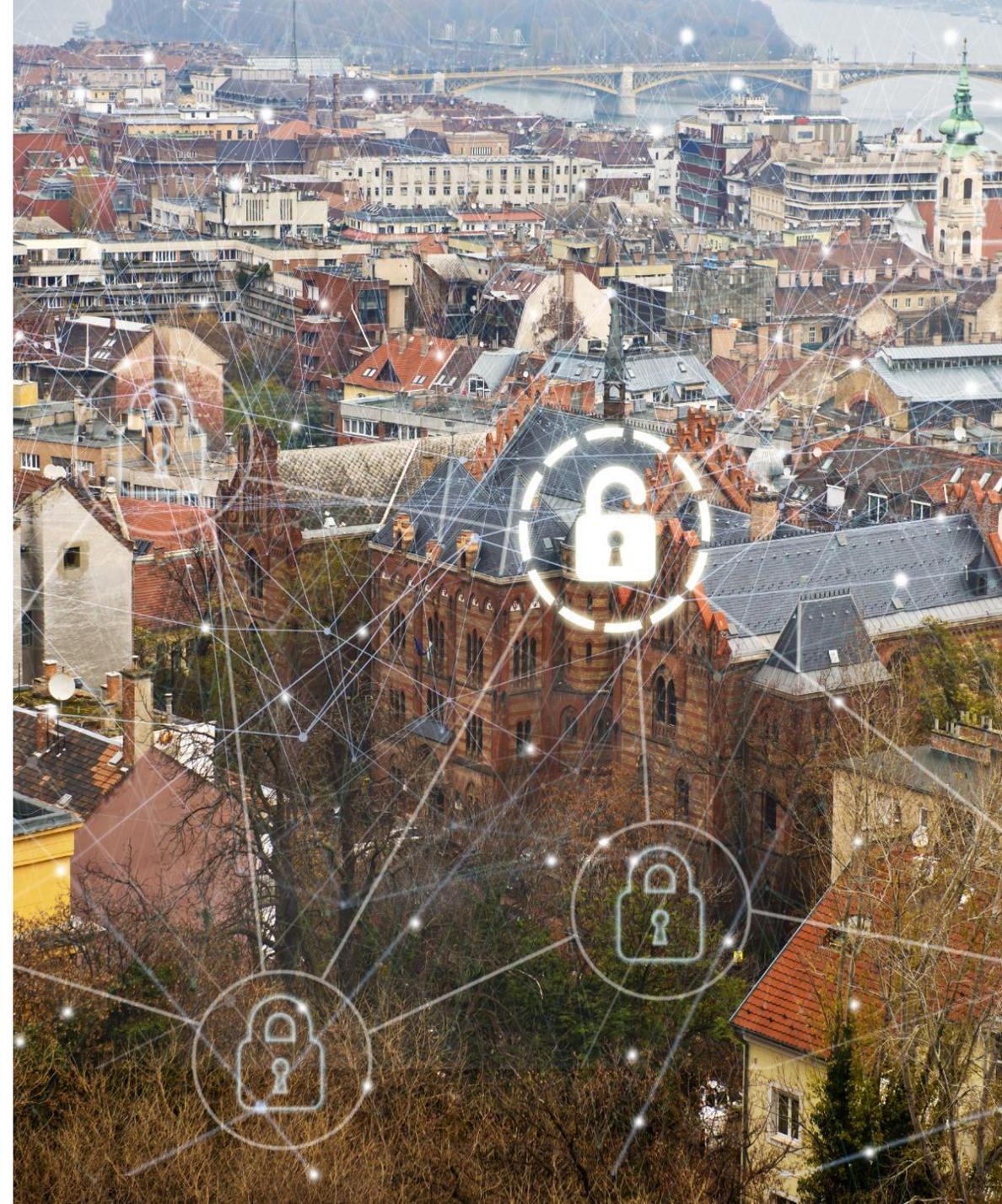
- private und öffentliche Organisationen in der EU
- Lieferketten von Organisationen (auch Nicht-EU)

## 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 Teilssektoren bzw. Lieferketten



# 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

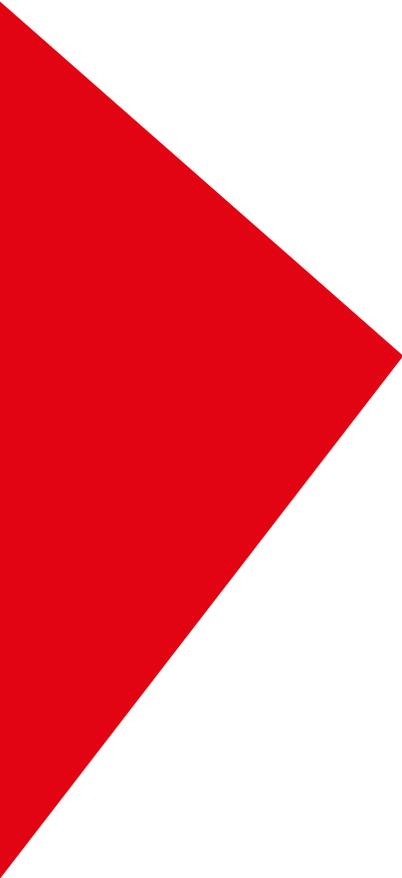
- ▶ **Geschäftskontinuität**

  - Aufrechterhaltung Betrieb im Falle eines Cybervorfalls

  - Regelmäßige Überprüfungen zur Einhaltung der Sicherheitsstandards

- ▶ **Schulung und Sensibilisierung**

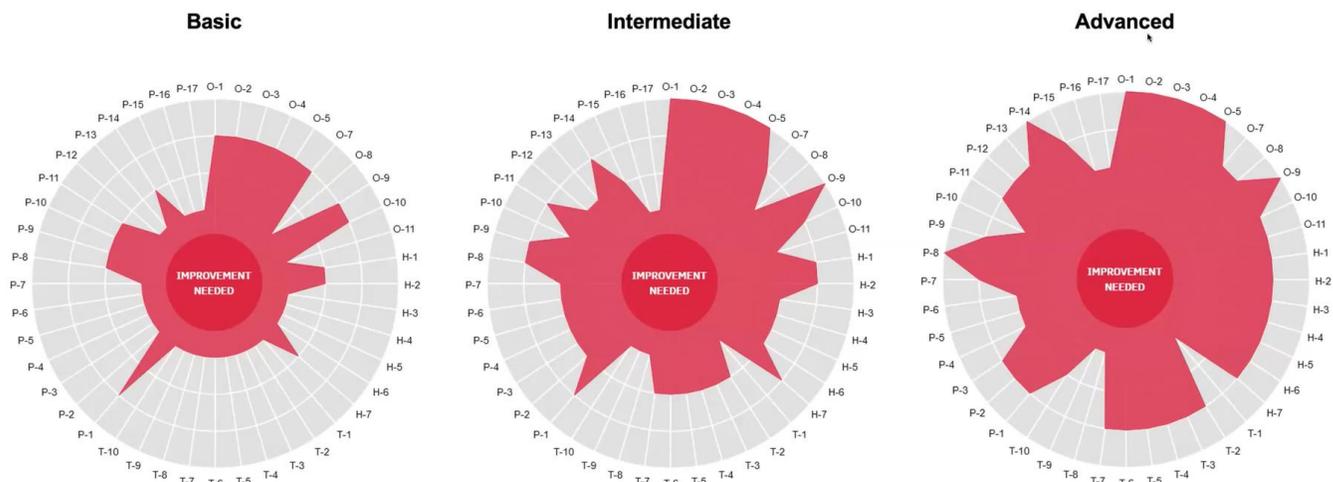
  - Sensibilisierung für Cyber-Sicherheitsrisiken



# Security Frameworks Compliance vs. Security ?

# ENISA

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



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

<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

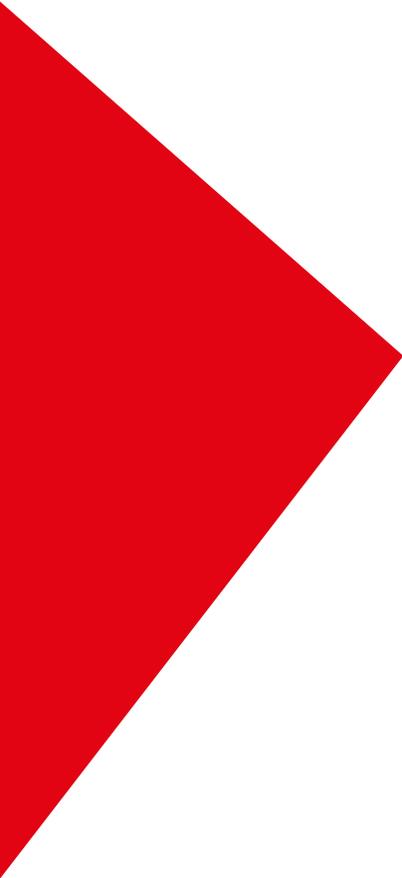
### Vier Hauptkategorien:

- **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 <sup>12</sup>

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



# 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 & Respond

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

## Integrations

Choose an integration to start collecting and analyzing your data.

[Browse integrations](#) **Installed integrations**

**Web crawler**  
Add search to your website with the Enterprise Search web crawler.

**Elastic APM**  
Monitor, detect, and diagnose complex application performance issues.

**Endpoint and Cloud Security**  
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

**All categories** 304

AWS	30	 <b>1Password</b> Collect logs from 1Password with Elastic Agent.	 <b>AbuseCH</b> Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.	 <b>ActiveMQ Logs</b> Collect and parse logs from ActiveMQ instances with Filebeat.
Azure	25	 <b>ActiveMQ Metrics</b> Collect metrics from ActiveMQ instances with Metricbeat.	 <b>Aerospike Metrics</b> Collect metrics from Aerospike servers with Metricbeat.	<b>Akamai</b> Collect logs from Akamai with Elastic Agent.
Cloud	60	<b>AlienVault OTX</b> Ingest threat intelligence indicators from AlienVault Open Threat Exchange (OTX) with Elastic Agent.	<b>Amazon CloudFront</b> Collect Amazon CloudFront logs with Elastic Agent	 <b>Amazon DynamoDB</b> Collect Amazon DynamoDB metrics with Elastic Agent
Communications	3	 <b>Amazon EBS</b> Collect Amazon Elastic Block Storage metrics with Elastic Agent	<b>Amazon EC2</b> Collect logs and metrics for Amazon Elastic Compute Cloud service with Elastic Agent	 <b>Amazon ECS</b> Collect metrics for Amazon Elastic Container Service with Elastic Agent
Config management	2	<b>Amazon Kinesis</b> Collect Amazon Kinesis metrics with Elastic Agent	<b>Amazon NAT Gateway</b> Collect Amazon NAT Gateways metrics with Elastic Agent	<b>Amazon RDS</b> Collect Amazon Relational Database Service metrics with
Containers	7			
Custom	26			
Datastore	29			
Elastic Stack	16			
Enterprise search	3			
File storage	7			
Geo	4			
Google Cloud	16			
Kubernetes	5			
Language client	9			
Message Queue	9			
Microsoft 365	2			
Monitoring	10			
Network	67			

# Erkennung und Analyse

Prevent & Ingest

Detect & Investigate

Escalate & Respond

- 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

## Rules

[Add Elastic rules](#) 1189 [Manage value lists](#) [Import rules](#) [Create new rule](#)

[Installed Rules](#) 48 [Rule Monitoring](#) 48

login  Tags 50 Last response 3 Elastic rules (14) Custom rules (34) Enabled rules Disabled rules

Showing 1-2 of 2 rules | Selected 0 rules [Select all 2 rules](#) [Bulk actions](#) [Refresh](#) [Clear filters](#) Updated 23 seconds ago [On](#)

<input type="checkbox"/>	Rule		Risk score	Severity	Last run	Last response	Last updated	Notify	Enabled
<input type="checkbox"/>	Login Failure Sequence Followed by Success for o365	6	73	High	4 minutes ago	Succeeded	Jul 22, 2024 @ 15:56:4...	<a href="#">Notify</a>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Fortianalyzer-Brute-Force-Account-Login-Attack-FGT	4	47	Medium	Sep 10, 2024 @ 14:17:4	Succeeded	Sep 10, 2024 @ 14:20:...	<a href="#">Notify</a>	<input type="checkbox"/>

Rows per page: 20

< 1 >

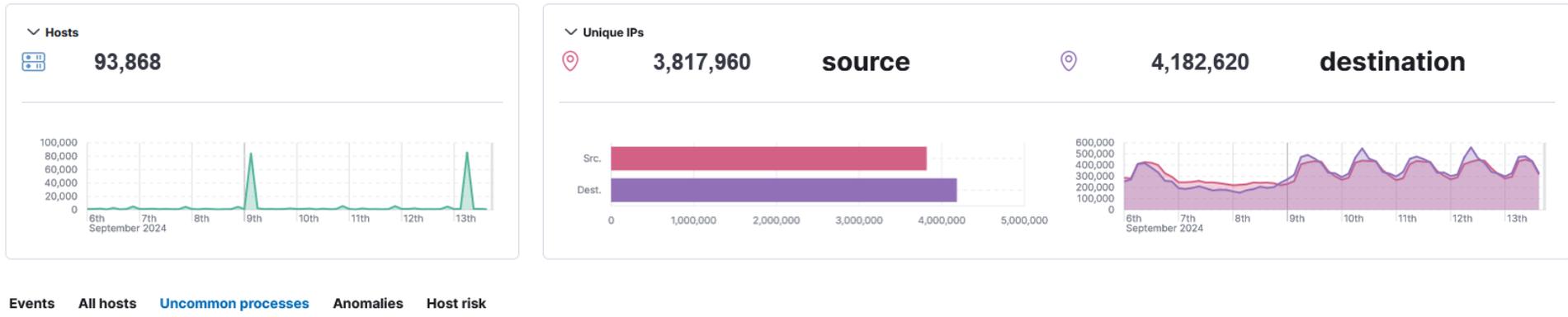
# Erkennung und Analyse

Prevent & Ingest

Detect & Investigate

Escalate & Respond

- 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	192.168.1.100	C:  Windows\system32\CredentialEnrollmentManager.exe	SYSTEM
CredentialUIBroker.exe	1	1	192.168.1.100	C:\Windows\System32\CredentialUIBroker.exe +2 More	SYSTEM
DeskUpdateNotifier.exe	1	1	192.168.1.100	C:\Program Files (x86)\Fujitsu\DeskUpdate\DeskUpdateNotifier.exe	SYSTEM
DisplaySwitch.exe	1	1	192.168.1.100	DisplaySwitch.exe	SYSTEM

# Erkennung und Analyse

Prevent & Ingest

Detect & Investigate

Escalate & Respond

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

**Severity levels**

Levels	Count ↓
Medium	584
High	147
Low	14
Critical	2

747 alerts

**Alerts by name**

Rule name
Fortianalyzer-Access-to-a-Suspicious-Domain-After-R...
Access to a Suspicious Domain After Risky App Detect...
Potential Password Spraying of Microsoft 365 User Ac...
Attempts to Brute Force a Microsoft 365 User Account...

**Alerts Table**

Actions	@timestamp ↓	Rule	Assignees	Severity	Risk
<input type="checkbox"/>	Sep 13, 2024 @ 16:39:17.027	DNS traffic to Botnet C&C ...		high	
<input type="checkbox"/>	Sep 13, 2024 @ 16:36:47.039	...		medium	
<input type="checkbox"/>	Sep 13, 2024 @ 16:34:14.634	outgoing Botnet C&C Traff...		high	
<input type="checkbox"/>	Sep 13, 2024 @ 16:34:14.631	DNS traffic to Botnet C&C ;		high	
<input type="checkbox"/>	Sep 13, 2024 @ 16:09:08.556	DNS traffic to Botnet C&C ;		high	
<input type="checkbox"/>	Sep 13, 2024 @ 16:04:08.468	outgoing Botnet C&C Traff...		high	
<input type="checkbox"/>	Sep 13, 2024 @ 16:04:08.466	DNS traffic to Botnet C&C ;		high	
<input type="checkbox"/>	Sep 13, 2024 @ 15:59:05.592	DNS traffic to Botnet C&C ...		high	
<input type="checkbox"/>	Sep 13, 2024 @ 15:44:02.227	DNS traffic to Botnet C&C ...		high	
<input type="checkbox"/>	Sep 13, 2024 @ 15:27:28.312	Windows System without S...		medium	

**Alert Details: DNS traffic to Botnet C&C ; [redacted].keniub.com blocked**

Status: Open | Risk score: 73 | Assignees: +

**MITRE ATT&CK**

- Command and Control (TA0011) [↗](#)
  - Application Layer Protocol (T1071)
- Resource Development (TA0042) [↗](#)
  - Compromise Infrastructure (T1584)
  - Botnet (T1584.005)

Take action

# Erkennung und Analyse/Reaktion

Prevent &  
Ingest

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

Detect &  
Investigate

Untitled timeline Unsaved  
Add a description

Processes 1 Users 1 Hosts 1 Source IPs 0 Destination IPs 0

Query 1 Correlation Analyzer Session View BETA Notes Pinned

Oct 27, 2022 @ 14:03:08.021 → Oct 27, 2022 @ 14:09:08.020 Refresh

(  AND  )

OR ( ) + Add field

AND Filter

@timestamp	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Oct 27, 2022 @ 14:09:08.020	Endpoint file event	file	deletion	marvin-public-demo2	—	—	root
				root @	deleted a file	gshadow.lock in /etc/gshadow.lock	via >. gpasswd (6438)

Escalate &  
Respond

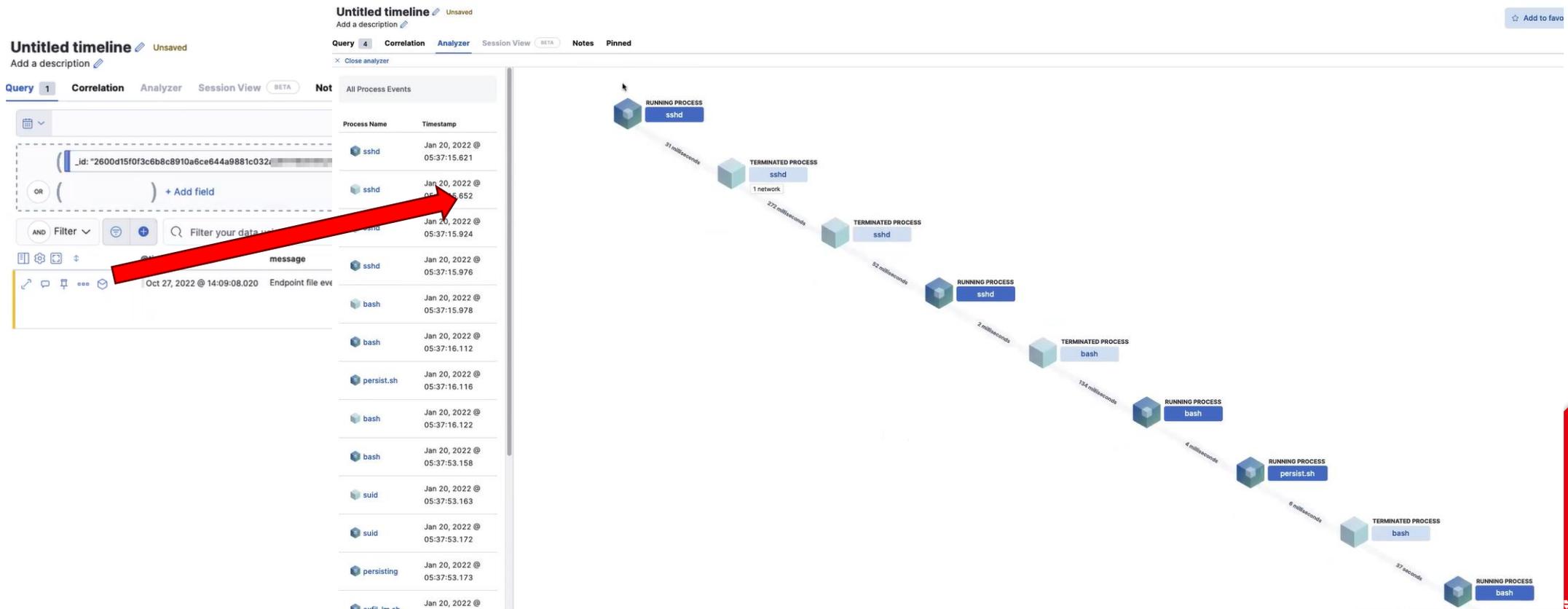
# Erkennung und Analyse/Reaktion

Prevent & Ingest

Detect & Investigate

Escalate & Respond

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



# Erkennung und Analyse/Reaktion

Prevent & Ingest

Detect & Investigate

Escalate & Respond

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

The screenshot displays a security analysis interface with three main sections:

- Query and Filter Section:** Shows a query editor with a filter for process ID: `"_id: "2600d15f0f3c6b8c8910a6ce644a9881c032..."`. Below it is a table of process events.
- Timeline Section:** A central timeline visualization showing the lifecycle of processes. It starts with a **RUNNING PROCESS sshd**, followed by a **TERMINATED PROCESS sshd** (1 network), another **TERMINATED PROCESS sshd**, a **RUNNING PROCESS sshd**, and finally a **TERMINATED PROCESS bash**. A large red arrow points from the timeline to the details panel.
- Details Panel:** Provides metadata for the selected process (sshd):
  - process.name: sshd
  - process.pid: 6599
  - process.entity\_id: MGYyNGMyYTkYjQwYy00M2VlLWJI
  - process.executable: /usr/sbin/sshd
  - process.Ext.ancestry: MGYyNGMyYTkYjQwYy00M
  - process.Ext.ancestry: MGYyNGMyYTkYjQwYy00M
  - process.Ext.ancestry: MGYyNGMyYTkYjQwYy00M
  - destination.address: 172.16.66.6
  - destination.port: 22
  - destination.ip: 172.16.66.6
  - source.address: 172.16.66.1
  - source.port: 46354

# Erkennung und Analyse/Reaktion

Prevent & Ingest

Detect & Investigate

Escalate & Respond

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

The screenshot displays a security dashboard interface. At the top, there's a navigation bar with 'Events', 'sshd', '1 Events', and '1 network'. Below this, a header for the alert 'test' is shown, dated 'Oct 27, 2022 @ 14:09:08.020'. The main content area is divided into several sections:

- Overview:** Shows the alert status as 'Open', severity as 'Low', risk score as '21', and rule as 'test'.
- Highlighted fields:** A table listing fields and their values:

Field	Value	Alert prevalence
host.name	[redacted]	100
Agent status	Healthy	- yOOM
user.name	root	31
Rule type	query	100
file.name	gshadow.lock	1
process.name	gpasswd	14 yOOM
- Insights:** Shows '0 cases related to this alert' and '1 alert related by source event'.
- Enriched data:** A section for 'HOST RISK DATA' which is currently empty.
- Timeline:** A list of process events with columns for Process Name and Timestamp. A red arrow points from the 'message' field in the timeline to the 'file.name' field in the highlighted fields table.

At the bottom right, a 'Take Action' menu is open, listing several options: 'Add to existing case', 'Add to new case', 'Mark as acknowledged', 'Mark as closed', 'Add Endpoint exception', 'Add rule exception', 'Isolate host', 'Respond', and 'Investigate in timeline'. The 'Isolate host' option is highlighted. In the bottom right corner, there's a 'TERMINATED PROCESS' (bash) and a 'RUNNING PROCESS' (bash) indicator, with a '37 seconds' duration shown between them. The page number '21' and the logo 'WURTHPHOENIX' are visible in the bottom right corner.

# Meldeprozess und Reaktion

Prevent & Ingest

Detect & Investigate

Escalate & Respond

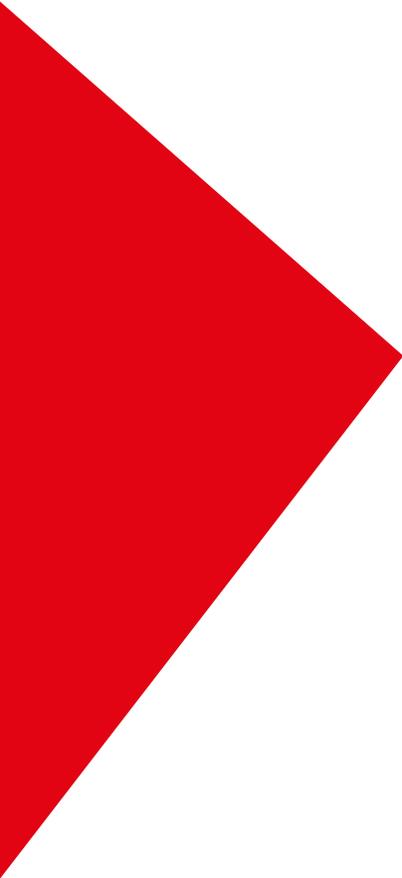
## Meldeprozess via „Case“

- Incident Details für Analyst
- Eskalation via Connector

The screenshot displays a security case management interface. On the left is a navigation sidebar with options: Dashboards, Rules, Alerts, Attack discovery, Findings, Cases (selected), Timelines, Intelligence, and Explore. The main content area shows a case titled "TEST Symantec Advanced Attack Technique Incident - 3956-IT-Wuerth Phoenix". A summary bar at the top right includes "Status: Open", "Sync alerts" (checked), and "Refresh case". Below this is a metrics table:

Total alerts	Associated users	Associated hosts	Total connectors	Case created	In progress duration
1	0	0	0	Sep 12, 2024 @ 09:01:50	—
				Open duration	Duration from creation to close
				1 day	—

The "Activity" tab is active, showing a list of events: "wn00242388 created case 'TEST Symantec Advanced Attack Technique Incident - 3956-IT-Wuerth Phoenix' yesterday" and "wn00242388 added an alert from TEST Symantec Advanced Attack Technique Incident yesterday". The right sidebar contains sections for "Assignees", "Severity" (set to Low), "Reporter", "Participants", and "Tags" (No tags are added).



# 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. Bestehens Risikomanagement)
- Systeme zur Erkennung und Reaktion von Cyber-Bedrohungen vorsehen





...more than  
software,  
your IT partner

20/09/2024

Gesamtheitliche Überwachung

