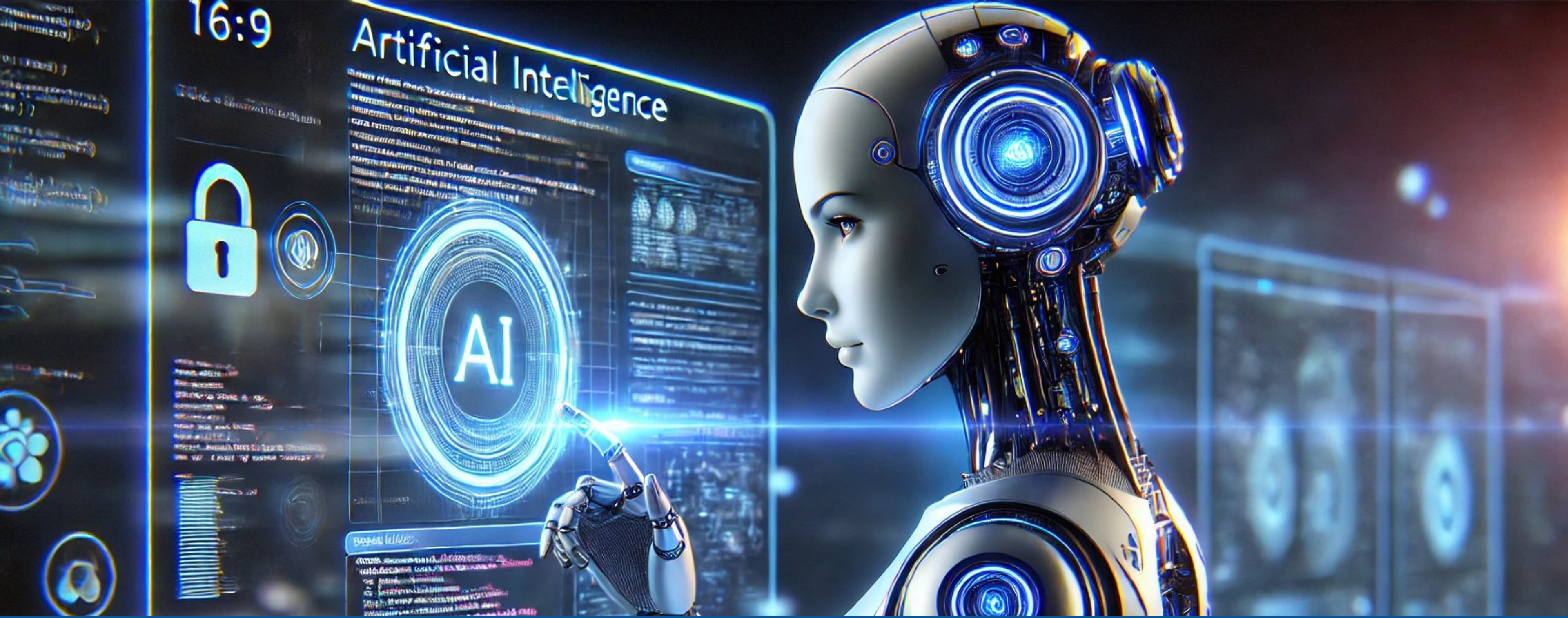


Resistine AI in CyberSecurity 2025

TLP:GREEN

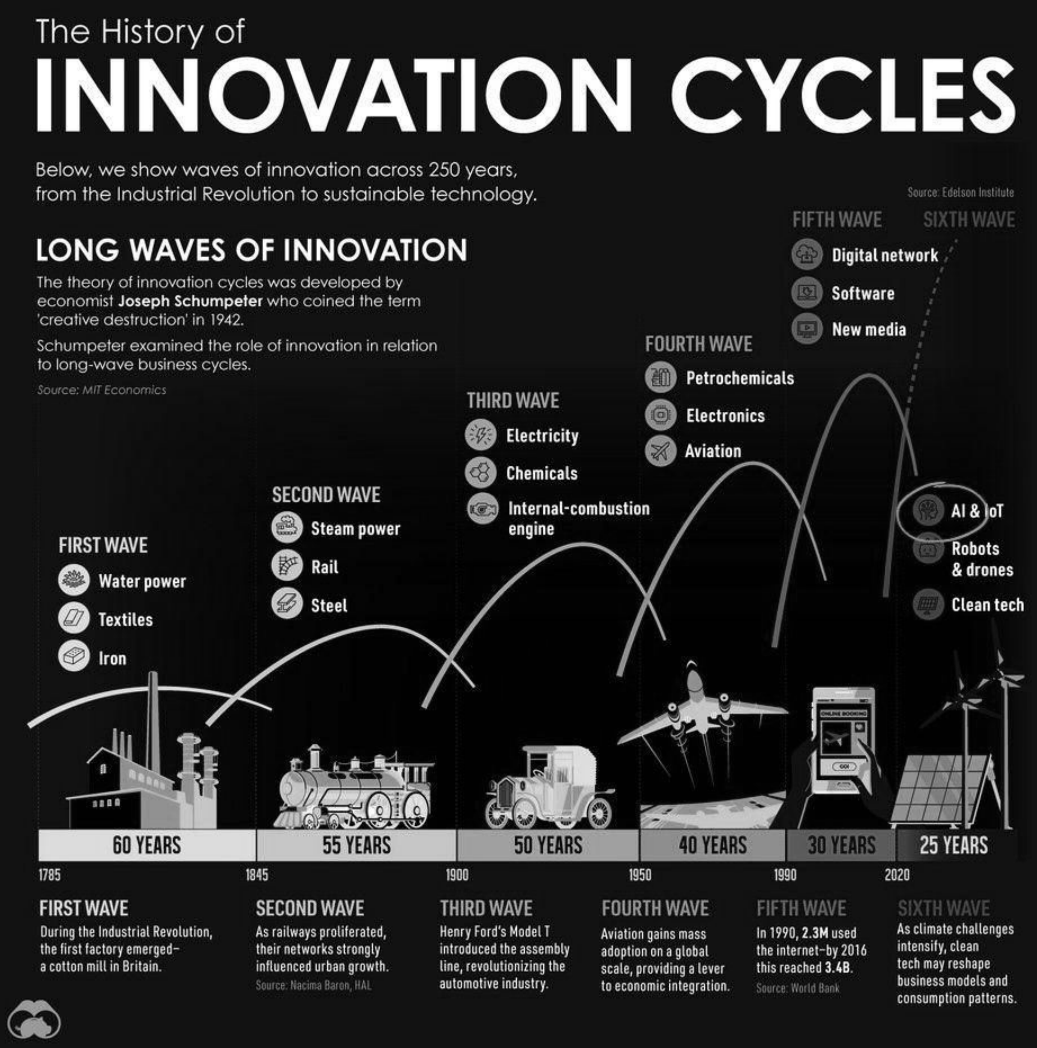
Petr Chmelar petr@resistine.com

Artificial intelligence?

Artificial intelligence is the last really big thing I will see in my lifetime.

Since the Industrial Revolution, we've replaced muscles…

Now, we should learn how to replace our brains 😅



The History of

INNOVATION CYCLES

Below, we show waves of innovation across 250 years, from the Industrial Revolution to sustainable technology.

Source: Edelson Institute

LONG WAVES OF INNOVATION

The theory of innovation cycles was developed by economist **Joseph Schumpeter** who coined the term 'creative destruction' in 1942.

Schumpeter examined the role of innovation in relation to long-wave business cycles.

Source: MIT Economics

FIRST WAVE
- Water power
- Textiles
- Iron

SECOND WAVE
- Steam power
- Rail
- Steel

THIRD WAVE
- Electricity
- Chemicals
- Internal-combustion engine

FOURTH WAVE
- Petrochemicals
- Electronics
- Aviation

FIFTH WAVE
- Digital network
- Software
- New media

SIXTH WAVE
- AI & IoT
- Robots & drones
- Clean tech

FIRST WAVE
During the Industrial Revolution, the first factory emerged–a cotton mill in Britain.

SECOND WAVE
As railways proliferated, their networks strongly influenced urban growth.
Source: Nacima Baron, HAL

THIRD WAVE
Henry Ford's Model T introduced the assembly line, revolutionizing the automotive industry.

FOURTH WAVE
Aviation gains mass adoption on a global scale, providing a lever to economic integration.

FIFTH WAVE
In 1990, 2.3M used the internet–by 2016 this reached 3.4B.
Source: World Bank

SIXTH WAVE
As climate challenges intensify, clean tech may reshape business models and consumption patterns.

Petr?

The first LMs

BRNO UNIVERSITY OF TECHNOLOGY

AI Challenges

aws

NIST CYBERSECURITY FRAMEWORK

NVIDIA

Monitoring NATO Cyber exercises

CCDCOE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

Waiting for the exit

GREYCORTEX

TLP:GREEN

Resistine

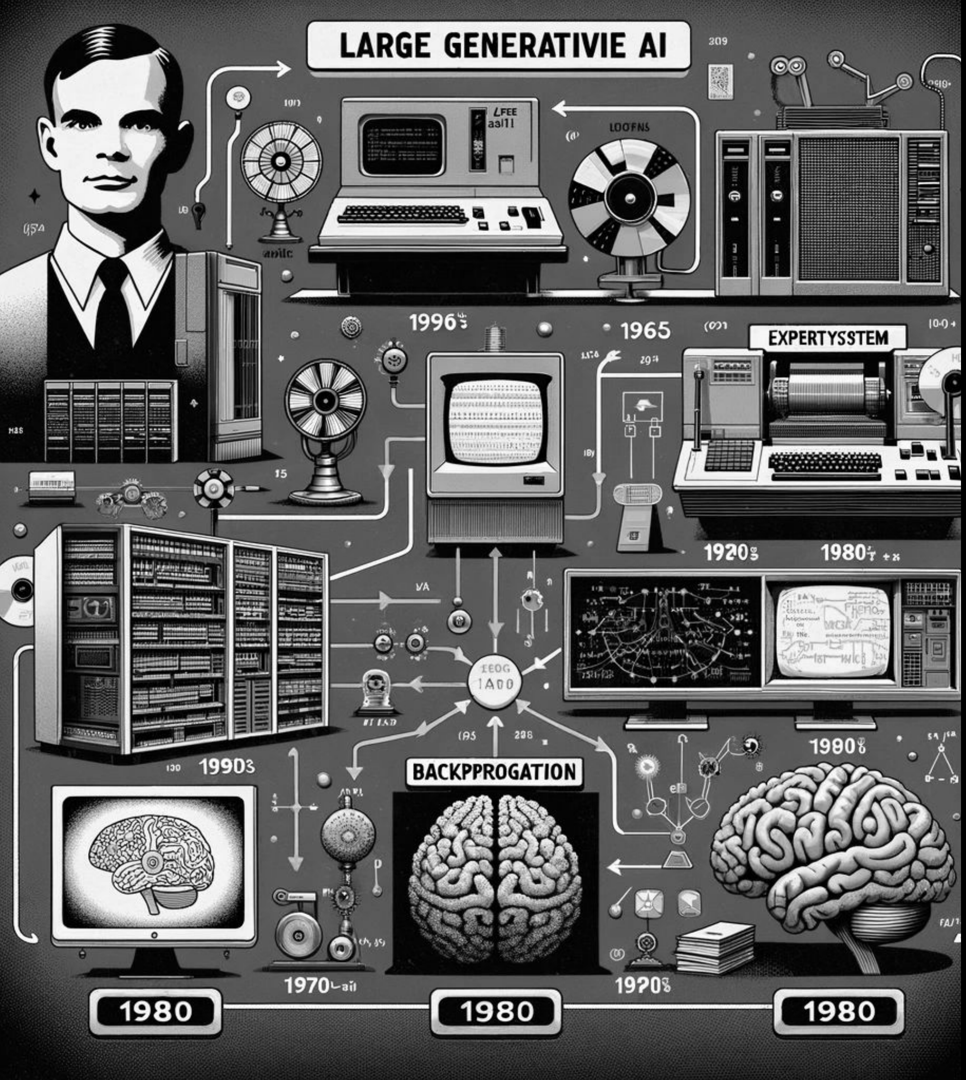
Erly inrgarve Researcher and founder
NANTOC
CORVAIRES
NARAS
SUNVEK
AI MELLAFEIWUMOOR PRRAGURBIEKE
IRLRRBONG PAST
CONLDWAHR THRATER

Resistine

What is AI?

- AI is a simulation of human intelligence in machines that are programmed to think like humans and mimic their actions

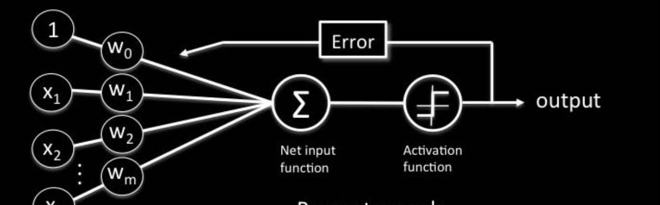
- AI is a machine that exhibits traits associated with a human mind such as responding to questions, reasoning or problem-solving



Resistine

How did it started...

- **1940s–1960s: The concepts**
  Alan Turing created the Test
  to measure Machine Intelligence
- **1943–1957: The Perceptron**
  the first Neuron was created in UK
- **1950s+: Expert systems**
  specific domain knowledge
  and a set of rules
- **1962–1980s: The backpropagation**
  algorithm to adjust weight and train the network



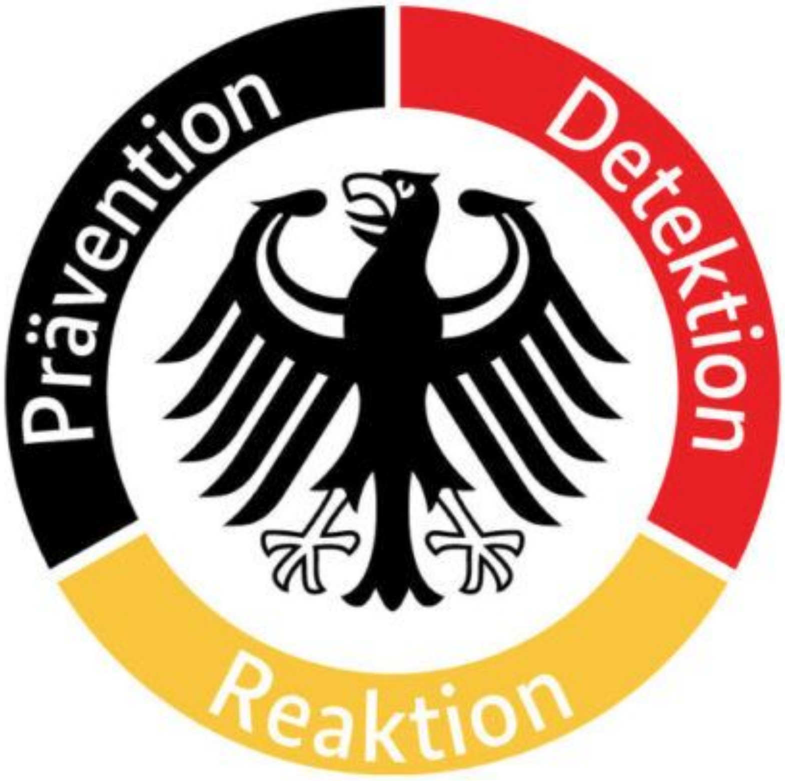
Perceptron rule.

What is CyberSecurity?

- **Govern**: that’s the centerpoint of it
- **Prevent**: **Identify** Assets and Risks, Educate and **Protect** the Good
- Detect Vulnerabilities, Threats and the Ugly and then
- React: **Respond** and **Recover** the Bad

That’s what the EC calls (Cyber) Hygiene

Security is everyone’s business



Source: EU, NIST and BSI

What is CyberSecurity?

Today?

- **Govern**: that's the centerpoint of it
- **Prevent**: **Identify** Assets and Risks, Educate and **Protect** the Good
- Detect Vulnerabilities, Threats and the Ugly and then
- React: **Respond** and **Recover** the Bad

That's what the EC calls (Cyber) Hygiene

Security is everyone's business

TLP:GREEN

Source: EU, NIST and BSI

What is CyberSecurity?

Today?

NIST NIS 2 DDoS DORA

Detection and Response Risk IDS EDR

SoC VPN DLP Firewall Authentication

Prevent Headache Too much data*

Lack of skilled

Insurance 3.4M people* tired

Windows Antivirus BSI Router

Security Information XDR

BackUp Zero Trust Protect Update

Ransomware Endpoint NDR XDR

Threat Intelligence Password Management

ISO 27000 Low Training* SIEM burnout

eats Analysts

TLP:GREEN

…meaning of life?

*Source: ISC2 - 2023 Cyberthreat Defense Report

How AI in CyberSecurity started?

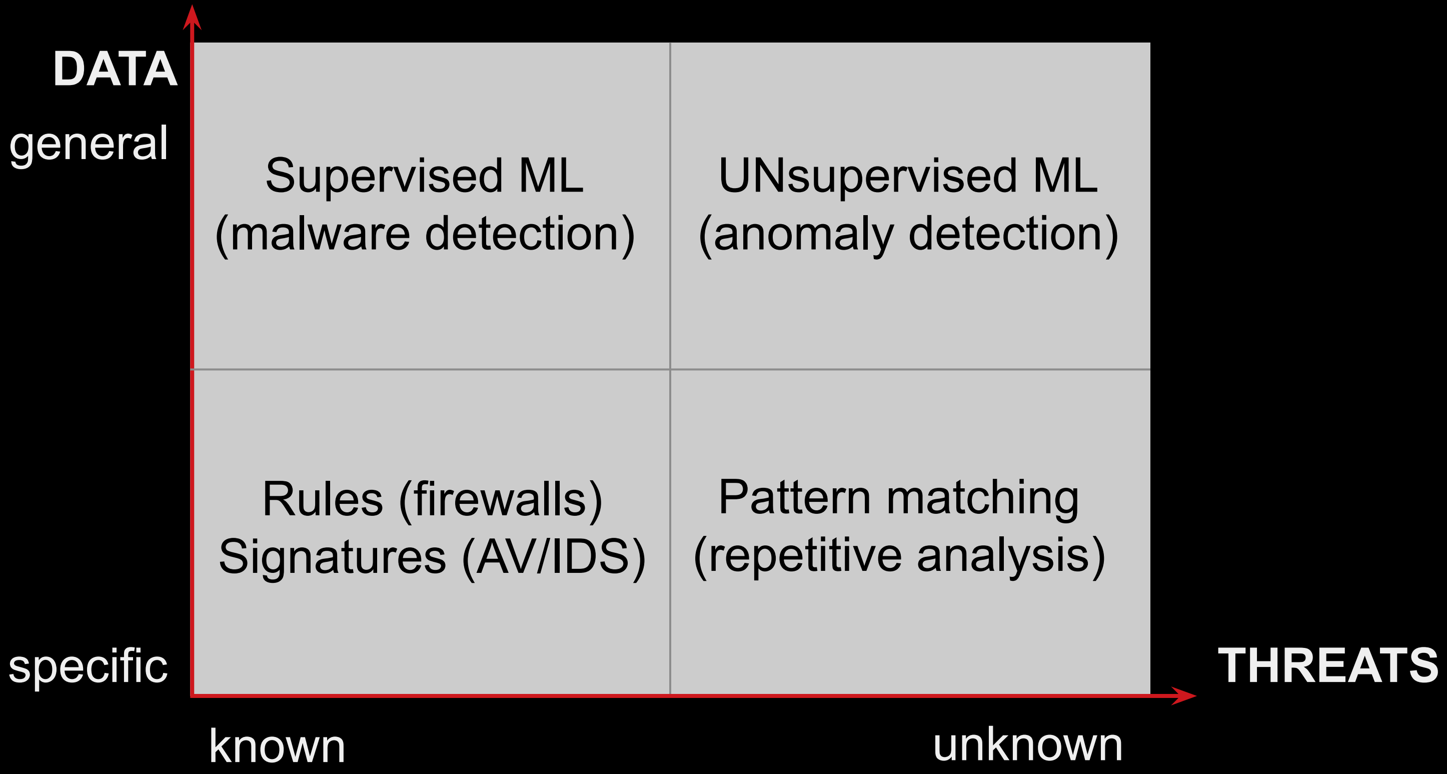
- We want a system that can separate good from bad, normal from abnormal
- Since the late 1980s: Researchers have tried to integrate of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity solutions, but progress has been slow[1]
- Since 1987: Focusing on intrusion detection systems (IDS) to identify unauthorized access or **anomalies** within networks
- In 1999: DARPA (the government agency that created the Internet), created benchmark sets an called for research on ML methods in security... KDD Cup 1999
- But it was based on Decision Trees... and full of false positives

[1] A brief history of machine learning in cybersecurity | Security Info Watch, **2019**

First Practical Uses

- 1990s: Heuristic Analysis
  utilizing rule-based approaches to detect previously unknown viruses by companies like AVG, Avast or ESET
- 2000s: Spam, phishing, and URL filtering
  using **supervised learning**.
  These systems compared incoming data to labeled threats—like blacklisted URLs—to identify and block malicious content based on learned patterns.
- Late 2000s: Malware Detections
  first practical **supervised** threat detections

Machine Learning (ML) Use Cases

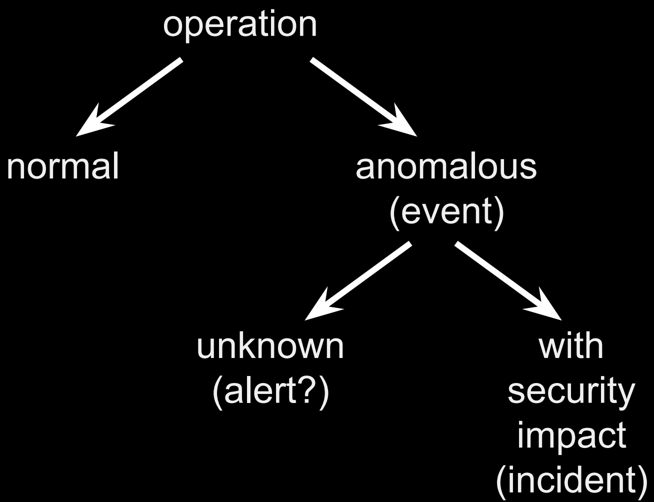


DATA

	known	unknown
general	Supervised ML (malware detection)	UNsupervised ML (anomaly detection)
specific	Rules (firewalls) Signatures (AV/IDS)	Pattern matching (repetitive analysis)

THREATS

Relation of **Anomalous Events** and **Security Incidents**



operation

normal

anomalous (event)

unknown (alert?)

with security impact (incident)

F1: Volumetric, normal, content-based and security-related anomaly.

What About Real AI?

- 2020s: Large Language Models
  Models trained to analyze PowerShell scripts, binary files, and even log data using NLP techniques...

  Or even create some malware

- 2023: Microsoft Security Copilot
  - Summarize incidents
  - Suggest remediation
  - Interpret logs
  - May generate detection rules

  Can't do what analysts do yet

TLP:GREEN

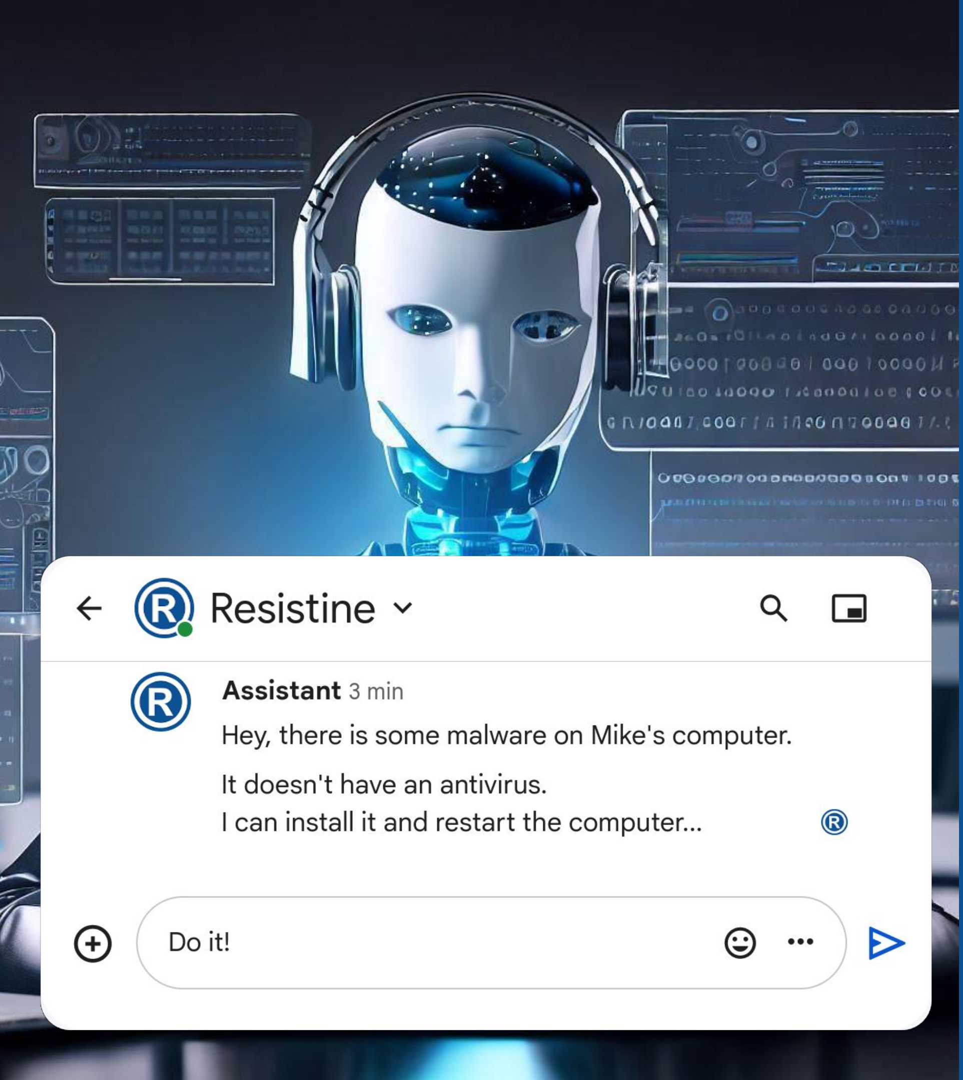
Resistine

Real Change!

AI CyberSecurity Assistant

www.resistine.com

TLP:GREEN



Hey, there is some malware on Mike's computer.

It doesn't have an antivirus.
I can install it and restart the computer...

Do it!

Resistine

AI CyberSecurity Assistant

1. identifies assets and risks,
2. detects vulnerabilities and threats,
3. suggests responses and
4. communicates with everyone for training and compliance

to improve your cybersecurity.

With chat interface – easy to use!

Finally!

TLP:GREEN

AI Language Model

- Assistant
  AI Chat provides help on cyber-topics
- generates data queries and summarizes their results

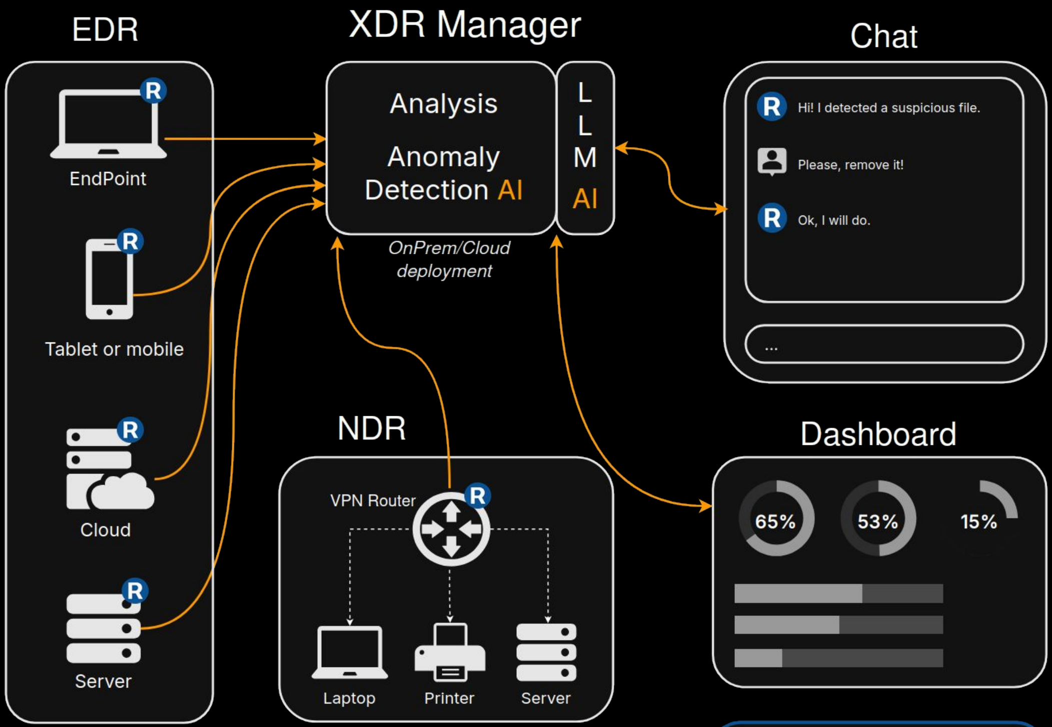
- AutoPilot*
  automatically builds knowledge similarly to L1 Security Operation Center expert
- alerts admins and managers
- communicates with everyone
  for training and compliance
  using Resistine Apps or even eg. Slack

TLP:GREEN

* Limited pilot customers only

Resistine

How Does it Work?



Hi! I detected a suspicious file.

Please, remove it!

Ok, I will do.

...

+ Custom Solutions for Enterprises

AI CyberSecurity AutoPilot

EndPoint Detection and Response
EDR

Network Detection and Response
NDR

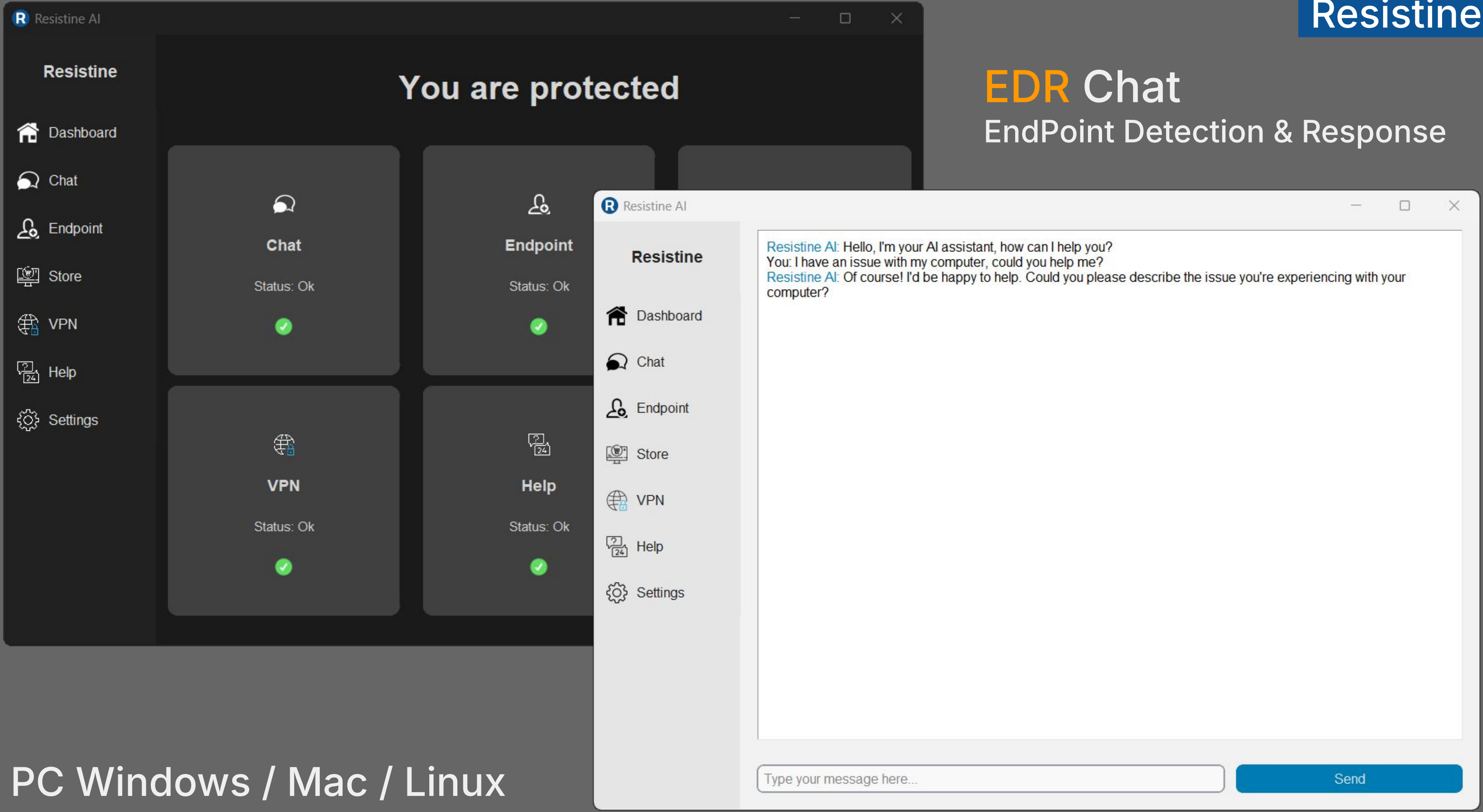
Extended Detection and Response
XDR

Choose Your Interface:
Dashboard or Interactive?

Resistine

EDR Chat

EndPoint Detection & Response

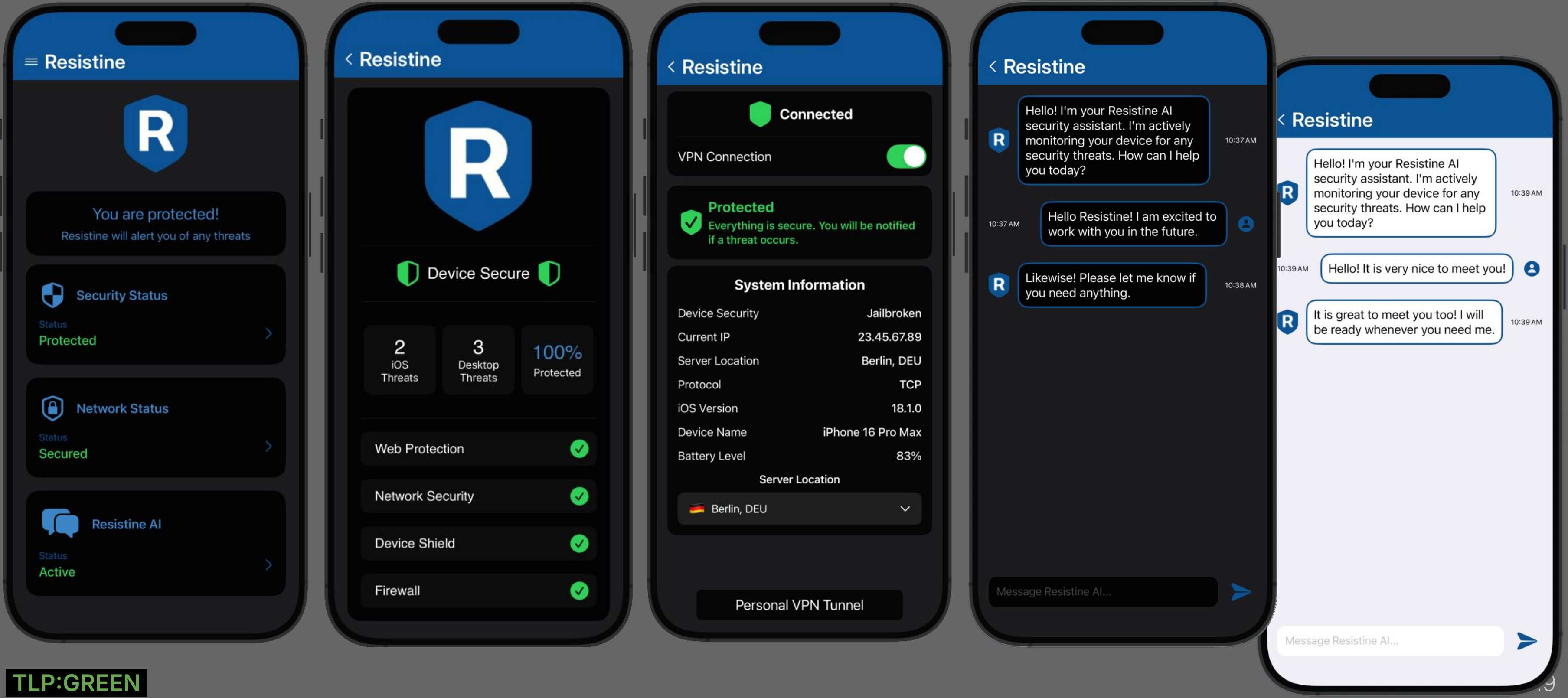


Resistine AI: Hello, I'm your AI assistant, how can I help you?
You: I have an issue with my computer, could you help me?
Resistine AI: Of course! I'd be happy to help. Could you please describe the issue you're experiencing with your computer?

PC Windows / Mac / Linux

Resistine

Resistine for iOS in Development



≡ Resistine

You are protected!
Resistine will alert you of any threats

Security Status
Status
Protected

Network Status
Status
Secured

Resistine AI
Status
Active

‹ Resistine

Device Secure

2 iOS Threats	3 Desktop Threats	100% Protected

- Web Protection ✓
- Network Security ✓
- Device Shield ✓
- Firewall ✓

‹ Resistine

Connected

VPN Connection ●

Protected
Everything is secure. You will be notified if a threat occurs.

System Information

Device Security	Jailbroken
Current IP	23.45.67.89
Server Location	Berlin, DEU
Protocol	TCP
iOS Version	18.1.0
Device Name	iPhone 16 Pro Max
Battery Level	83%

Server Location
Berlin, DEU

Personal VPN Tunnel

‹ Resistine

Hello! I'm your Resistine AI security assistant. I'm actively monitoring your device for any security threats. How can I help you today? 10:37 AM

10:37 AM Hello Resistine! I am excited to work with you in the future.

Likewise! Please let me know if you need anything. 10:38 AM

‹ Resistine

Hello! I'm your Resistine AI security assistant. I'm actively monitoring your device for any security threats. How can I help you today? 10:39 AM

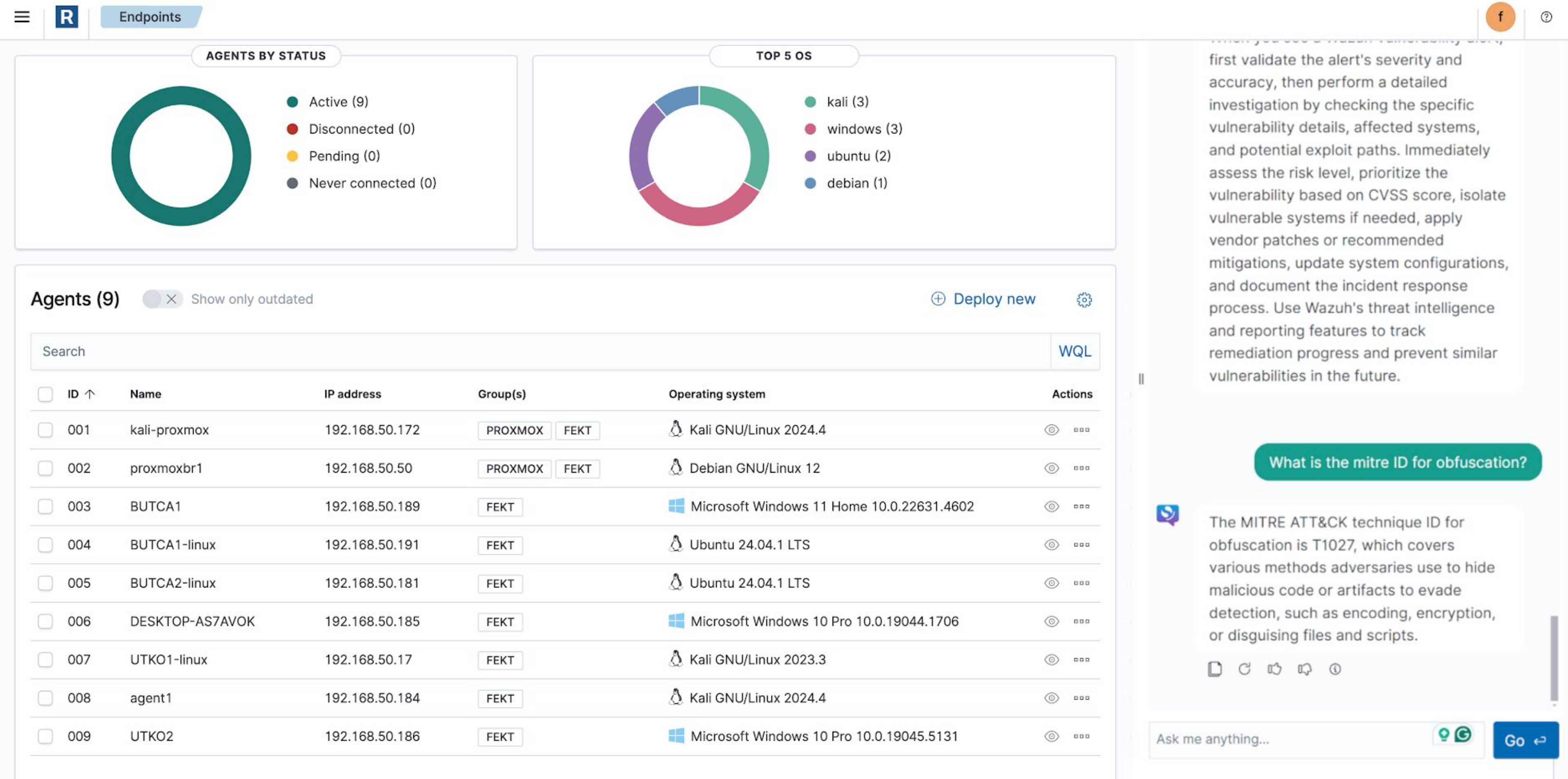
10:39 AM Hello! It is very nice to meet you!

It is great to meet you too! I will be ready whenever you need me. 10:39 AM

TLP:GREEN

XDR Manager

Resistine



AGENTS BY STATUS

- ● Active (9)
- ● Disconnected (0)
- ● Pending (0)
- ● Never connected (0)

TOP 5 OS

- ● kali (3)
- ● windows (3)
- ● ubuntu (2)
- ● debian (1)

Agents (9) Show only outdated

ID	Name	IP address	Group(s)	Operating system	Actions
001	kali-proxmox	192.168.50.172	PROXMOX FEKT	Kali GNU/Linux 2024.4	
002	proxmoxbr1	192.168.50.50	PROXMOX FEKT	Debian GNU/Linux 12	
003	BUTCA1	192.168.50.189	FEKT	Microsoft Windows 11 Home 10.0.22631.4602	
004	BUTCA1-linux	192.168.50.191	FEKT	Ubuntu 24.04.1 LTS	
005	BUTCA2-linux	192.168.50.181	FEKT	Ubuntu 24.04.1 LTS	
006	DESKTOP-AS7AVOK	192.168.50.185	FEKT	Microsoft Windows 10 Pro 10.0.19044.1706	
007	UTKO1-linux	192.168.50.17	FEKT	Kali GNU/Linux 2023.3	
008	agent1	192.168.50.184	FEKT	Kali GNU/Linux 2024.4	
009	UTKO2	192.168.50.186	FEKT	Microsoft Windows 10 Pro 10.0.19045.5131	

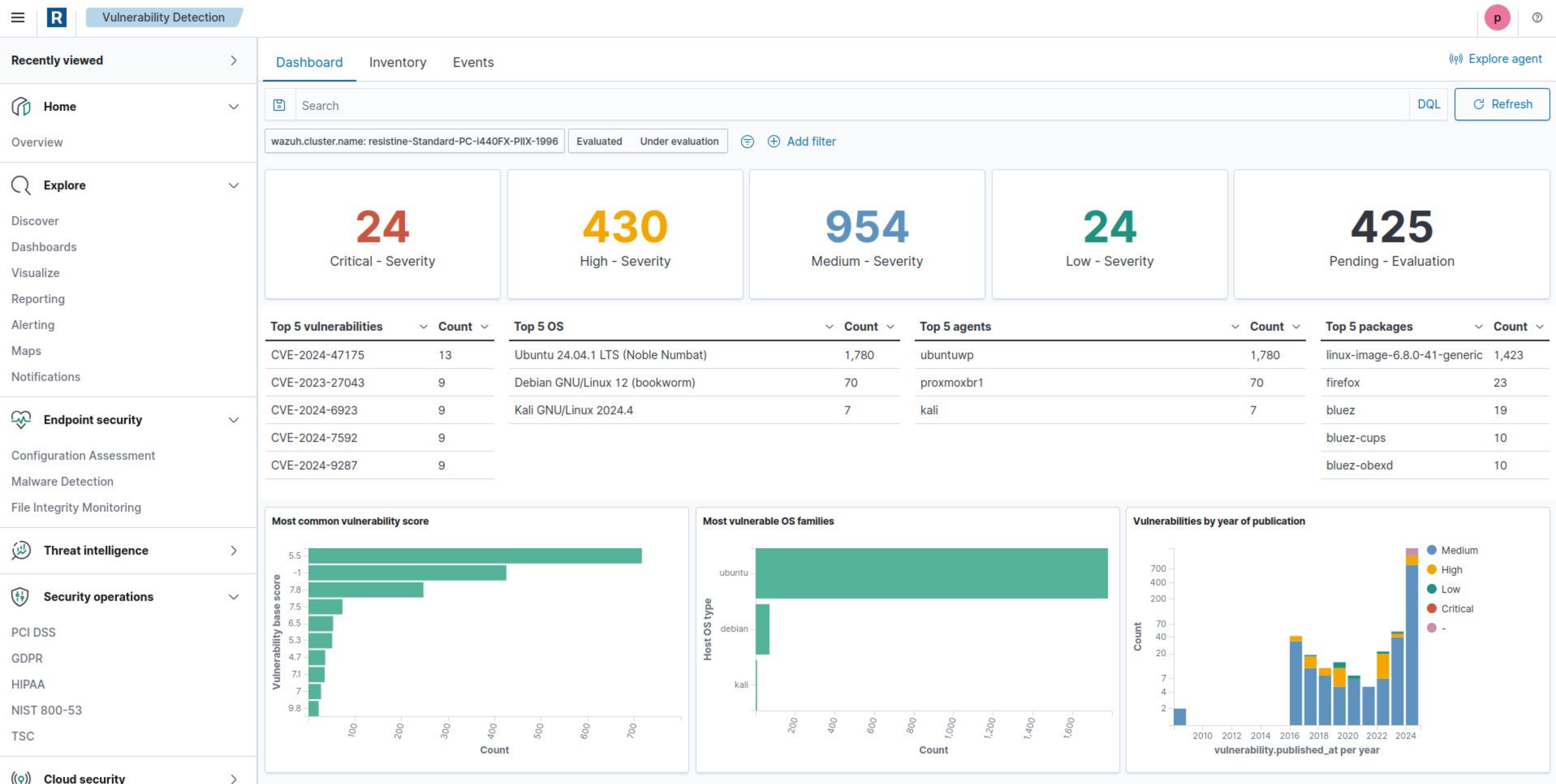
first validate the alert's severity and accuracy, then perform a detailed investigation by checking the specific vulnerability details, affected systems, and potential exploit paths. Immediately assess the risk level, prioritize the vulnerability based on CVSS score, isolate vulnerable systems if needed, apply vendor patches or recommended mitigations, update system configurations, and document the incident response process. Use Wazuh's threat intelligence and reporting features to track remediation progress and prevent similar vulnerabilities in the future.

What is the mitre ID for obfuscation?

The MITRE ATT&CK technique ID for obfuscation is T1027, which covers various methods adversaries use to hide malicious code or artifacts to evade detection, such as encoding, encryption, or disguising files and scripts.

XDR & Vulnerability Manager

Resistine



wazuh.cluster.name: resistine-Standard-PC-i440FX-PIIX-1996

Evaluated Under evaluation

24 Critical - Severity

430 High - Severity

954 Medium - Severity

24 Low - Severity

425 Pending - Evaluation

Top 5 vulnerabilities	Count
CVE-2024-47175	13
CVE-2023-27043	9
CVE-2024-6923	9
CVE-2024-7592	9
CVE-2024-9287	9

Top 5 OS	Count
Ubuntu 24.04.1 LTS (Noble Numbat)	1,780
Debian GNU/Linux 12 (bookworm)	70
Kali GNU/Linux 2024.4	7

Top 5 agents	Count
ubuntuwp	1,780
proxmoxbr1	70
kali	7

Top 5 packages	Count
linux-image-6.8.0-41-generic	1,423
firefox	23
bluez	19
bluez-cups	10
bluez-obexd	10

Most common vulnerability score

Most vulnerable OS families

Vulnerabilities by year of publication

Resistine.com

to make customers and the world safer and more free

Petr Chmelar petr@resistine.com

Berlin – Brno – ?