SIEMBIOT Deeptech learning platform

By Expertware

SIEMBIOT®

Co-funded by the European Union

ECCC

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Expertware

Full stack Development
Business Process Optimization

Be spoke web apps, ERP deployments & upgrades, Process automation, Self-service portals, Cash collection orchestration, Resource planning and tracking, Auto bidding, Custom Web, Mobile, Desktop Architecture, Enterprise applications integrations (ITSM - CRM – HR- FI - CO).

Cyber Security

End-to-End Protection, Vulnerability & Threat Management, Active Defense, Cyberthreat intelligence, Forensics, Advanced Hunting, Cross Reporting, Network Access Control, Incident Response, SIEM & SOC as a services, Blue / Red / Purple teams, Honeypots, Penetration testing.

Managed Services (hybrid cloud, network, storage, systems and apps)

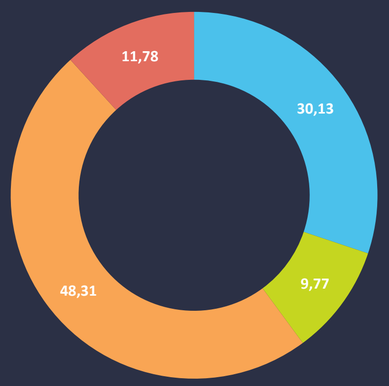
Cloud Solution Provider, Cloud Migrations, interconnects Multi-Cloud Integrations, Data Management, Connectivity & Design for Private, Public and Hybrid Clouds. Workspace & Unified Communications, High Availability & Business Continuity, Application management

Business Intelligence, Analytics & ML

Microsoft Data Platform and Bigdata Gold Partner, Virtual Data Warehouse design, deploy and operations. Rich dashboard and reporting capabilities unifying data, transforming and correlating across heterogeneous sources. Highlight real time KPIs and knowledge graphs.

7.5+ mil EUR estimated revenue in 2024 (Ro + Be)

Revenue split



www.expertware.net

Cyber Security Squeeze

[Blackberry Research]

11.5 attacks per minute

Mar–May 2023

[Statista]

Cyber crime costs predicted to grow by 23% YOY

In the next 5 years

[Cybercrime Magazine]

Businesses will lose $10.5 trillions

by 2025

[Purplesec]

70% of small businesses are unprepared

Now

SMEs

4 mil jobs opened

28% increase YOY

Tougher regulations (NIS2, NIST)

Political unrest

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Cyber Security

Europe Cyber Sec challenges

Struggling to have a competitive and stable cyber security operational team ?

EU market

260 working days but only 218 effective days per full time employee.

12 + 1 + 1 yearly salaries

1,2 resources needed without considering unplanned absences.

High risk loosing good resources.

70k-120k/year/budget for 2 resources.

Mandatory indexation every year.

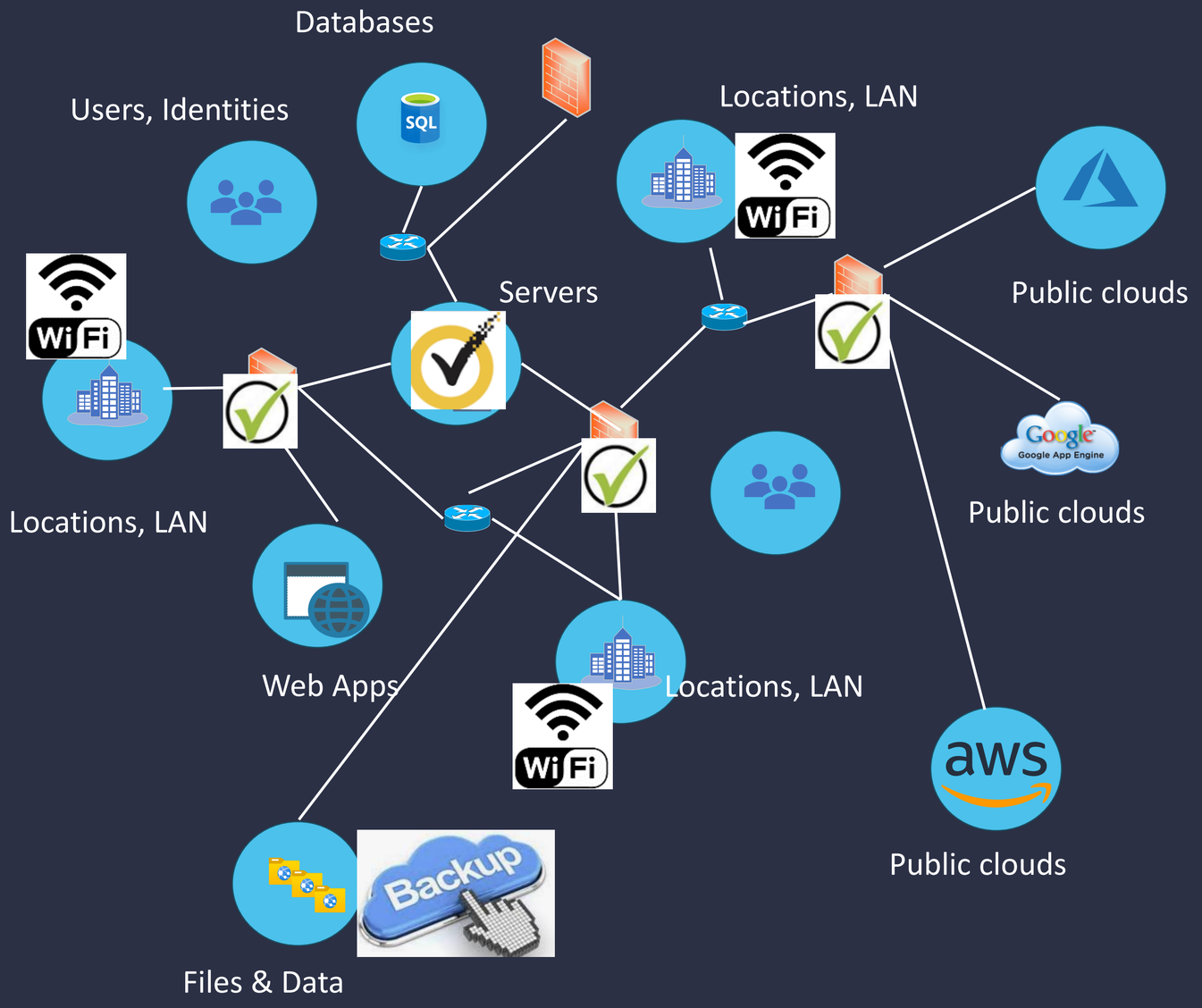
Hard to find

Expensive to keep

Unpredictable

Inefficient

Are organizations protecting themselves ?




Mobiles


Laptops

"Yes, we have firewalls"

"Yes, we have Antivirus"

"Yes, we have Backups"

"Yes, we have 2 IT support guys"

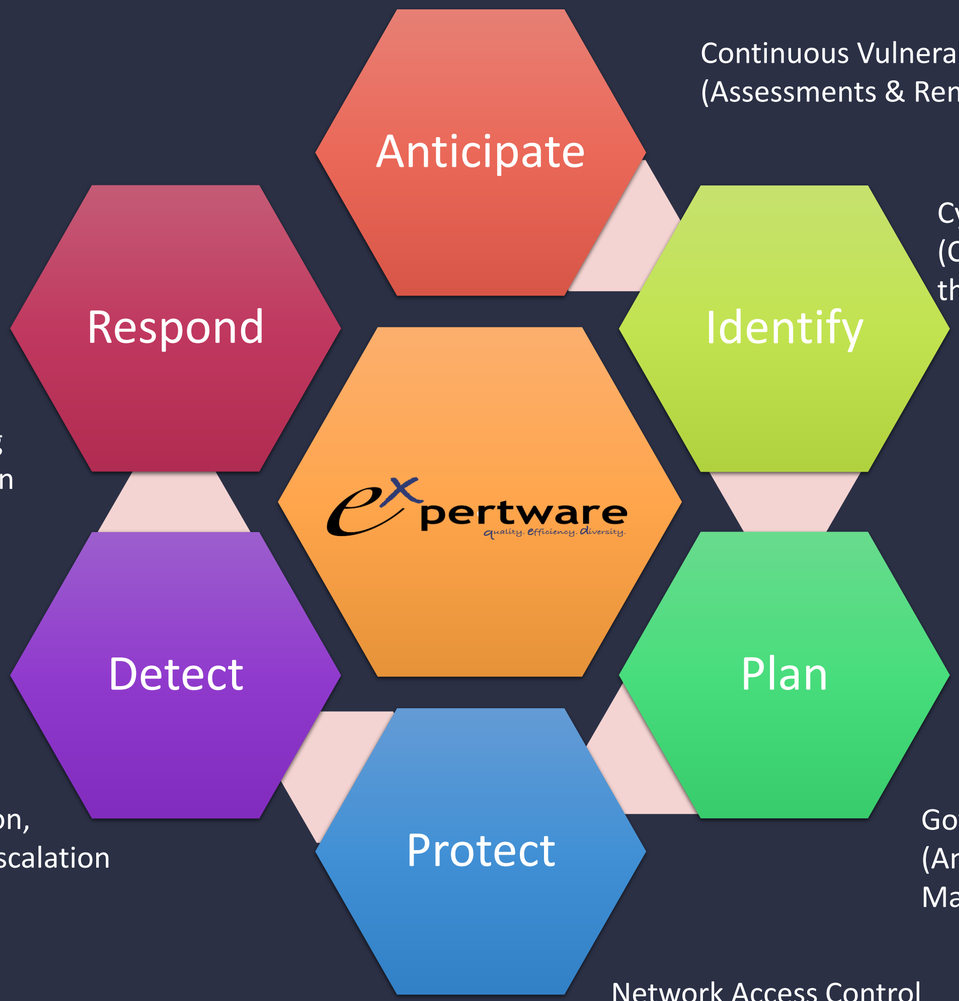
Is it enough?

Cyber Security

Services offered as MSSP, white labeling

Security Operations Centre (SOC)

Complete Security Lifecycle



Continuous Vulnerability (Assessments & Remediation)

Cyber Threat Intelligence (Continuous Evaluate of new threats against customer)

IT Security Consulting Services (security, privileged access ,risk , business continuity assessments, pen testing)

Review Security Architecture, Define monitoring, log collection, log aggregation,

Governance Risk Compliance (Analyse, Deploy, Customize & Managed GRC solutions)

Network Access Control (deploy & manage)

Identity Access Management (IAM) (deploy, customize, operate)

Managed SIEM
Detection rules
Security alerts classification,
Incident investigation & escalation
Security Analytics

Advanced threat hunting
Remediation & mitigation runbooks

Ransomware recovery
Forensics investigations

SIEMBIOT®

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

What are you missing ?

Is it not enough to have tools, you need also competences, processes, automations, training an research.

Expertware' s added value: Anonymized training and research data lake, NAC + SIEM + SOC, Vulnerability management, Threat intelligence, Forensics, Incident response platform

"Security architecture "

"Access Control for WI-FI and LAN"

"Network & communication protection"

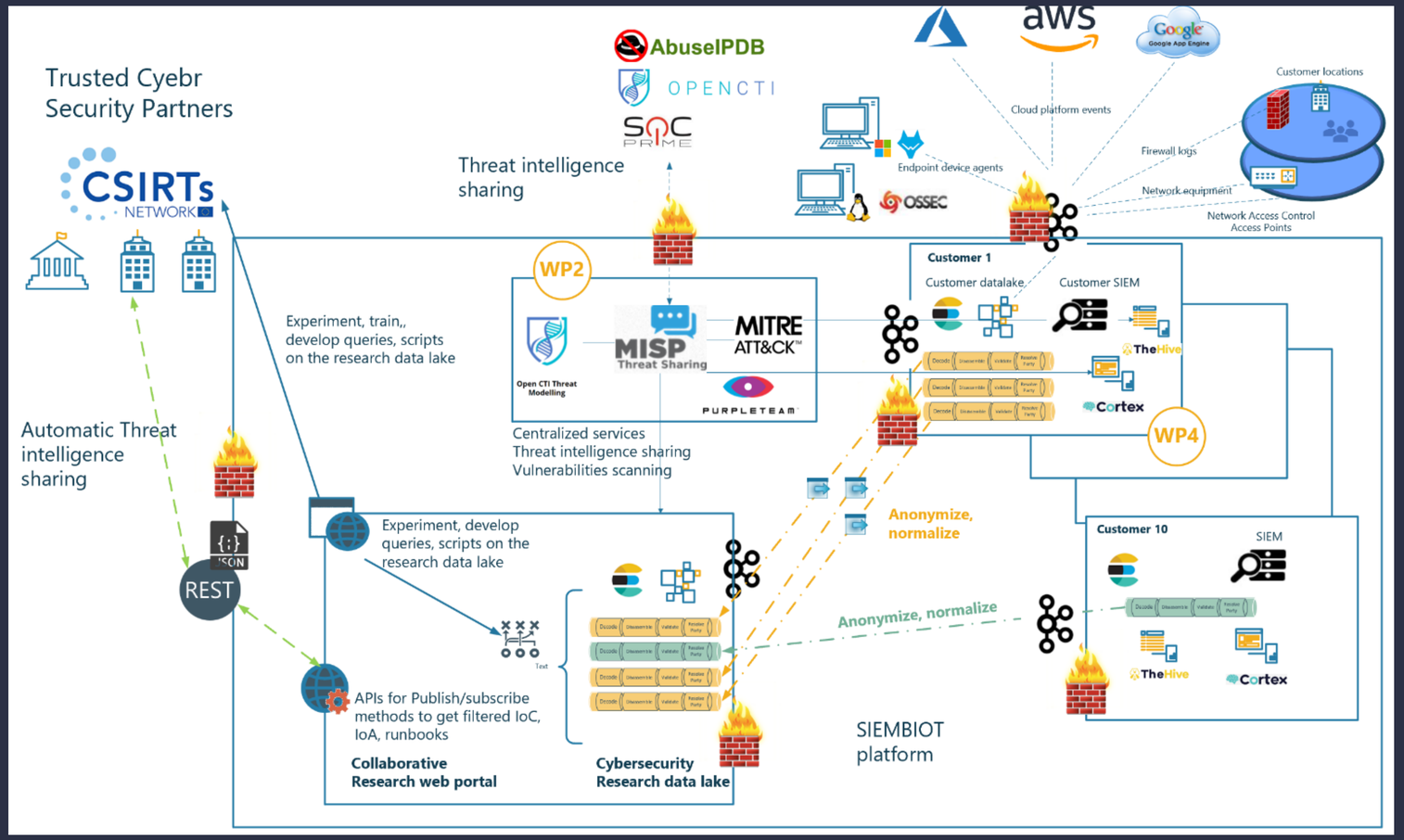
"24x7 Security events collection (SIEM)"

"24x7 SOC Monitoring

"24x7 Vulnerability monitoring"

24x7 "Threat intelligence Correlations"

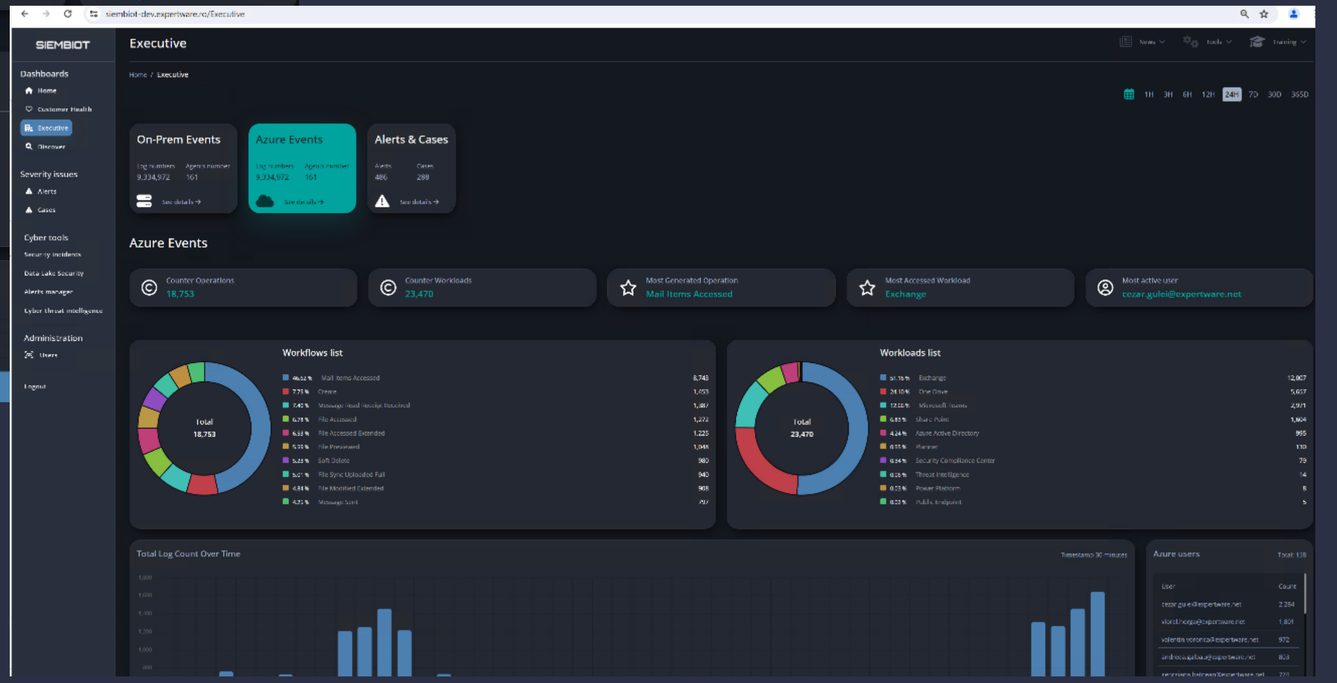
24x7 "Incident responses & Forensics"



Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

What are you missing ?

Live security posture dashboards



- *Realtime executive dashboards*
- *Aggregation of events, alerts, incidents*
- *Vulnerabilities, threat intelligence, asset inventory*

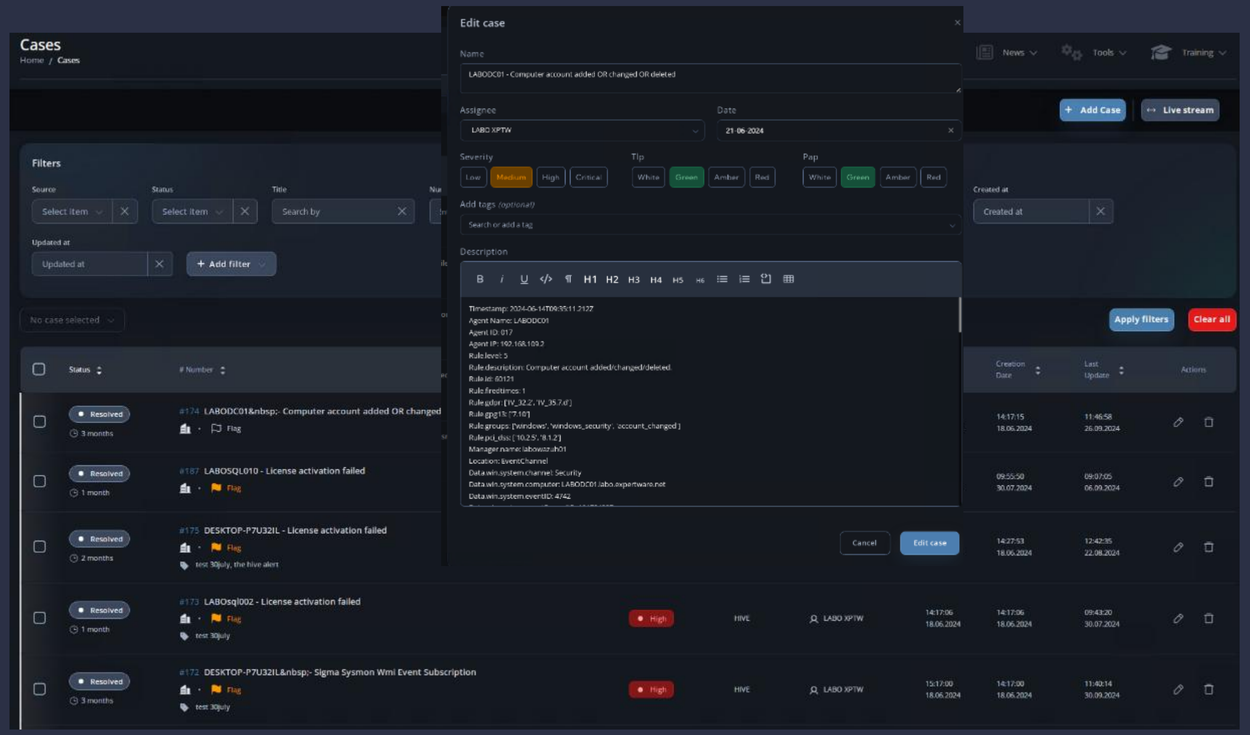
- *Multi sources : private cloud, public cloud, network, devices.*
- *SIEM and automatic detection playbooks.*
- *Metrics and history for all logs, events, vulnerabilities.*

SIEMBIOT®

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

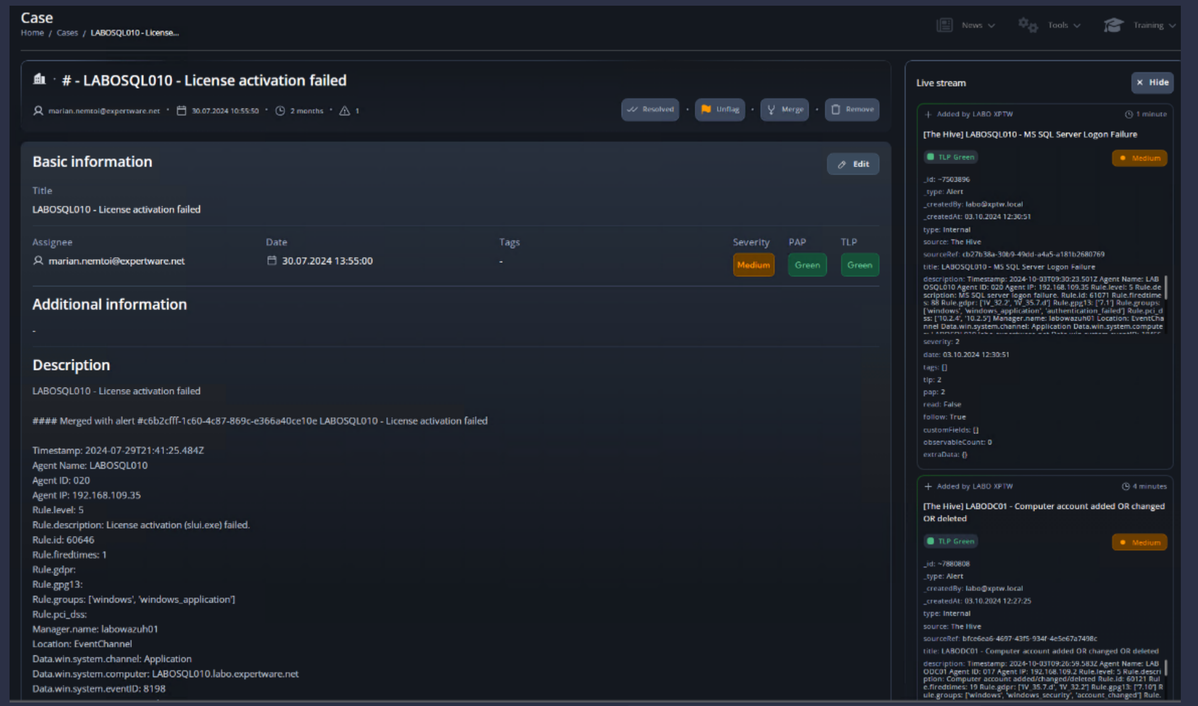
What are you missing ?

Security alerts collection, qualification & aggregation



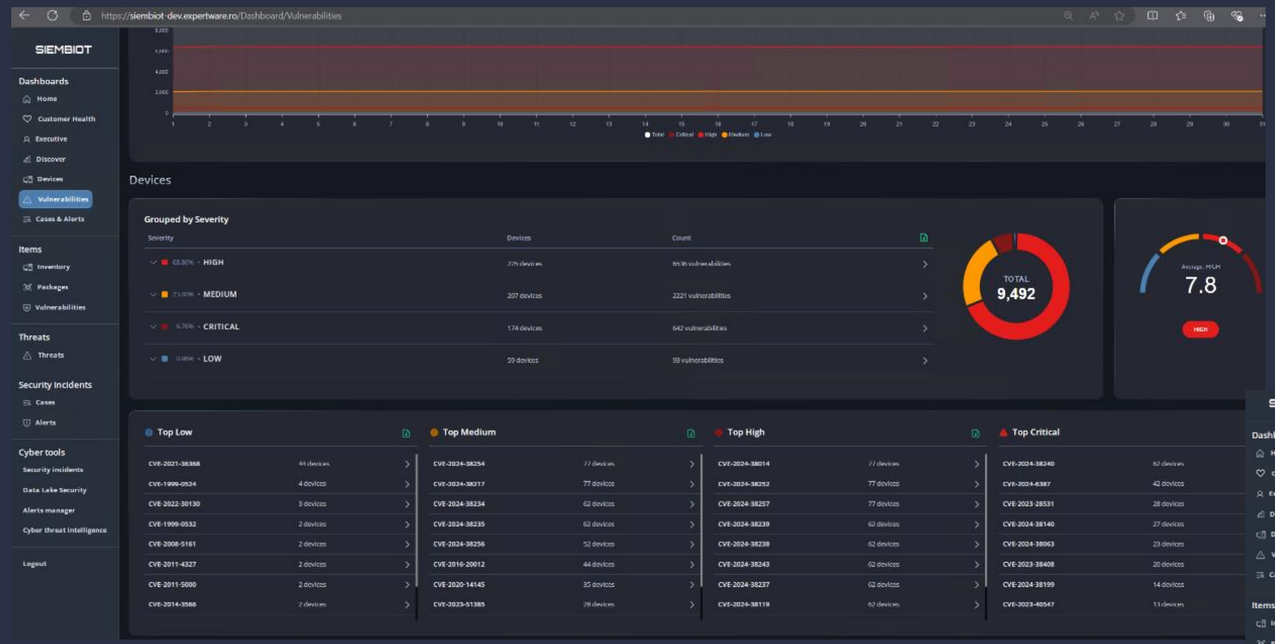
- *Multi source alert collection, aggregation and qualification*
- *Prioritization and contextualization of alerts.*
- *Integrated security incident management engine.*

- *Live event and CTI streams to ease qualification.*
- *Advanced filtering and investigation capabilities.*
- *Full audit, facilitates updates SOC / Ops /Business.*

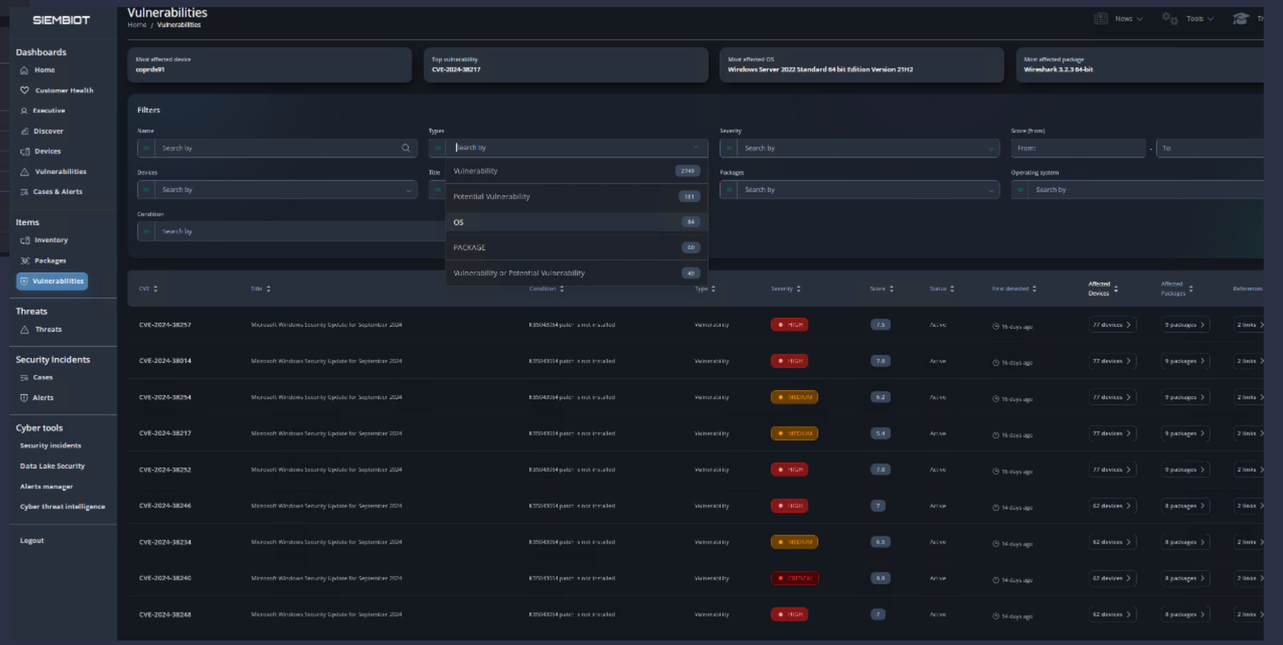


What are you missing ?

Multi-angle Vulnerability Detection & Correlations (NIS2, Mitre, CISA))



- *Advanced reporting (VMs not fixed in SLA, VMs per device, Devices with VM, etc.)*
- *Flexible filtering and exports.*
- *Enrichment and remediation instructions.*



- *Correlation of vulnerability and compliance data from multiple sources: Qualys/Nessus/OpenVAS + EDRs*
- *Integration with CTI and VM remediation sources.*
- *Automatic prioritization and mini GRC capabilities*

SIEMBIOT®

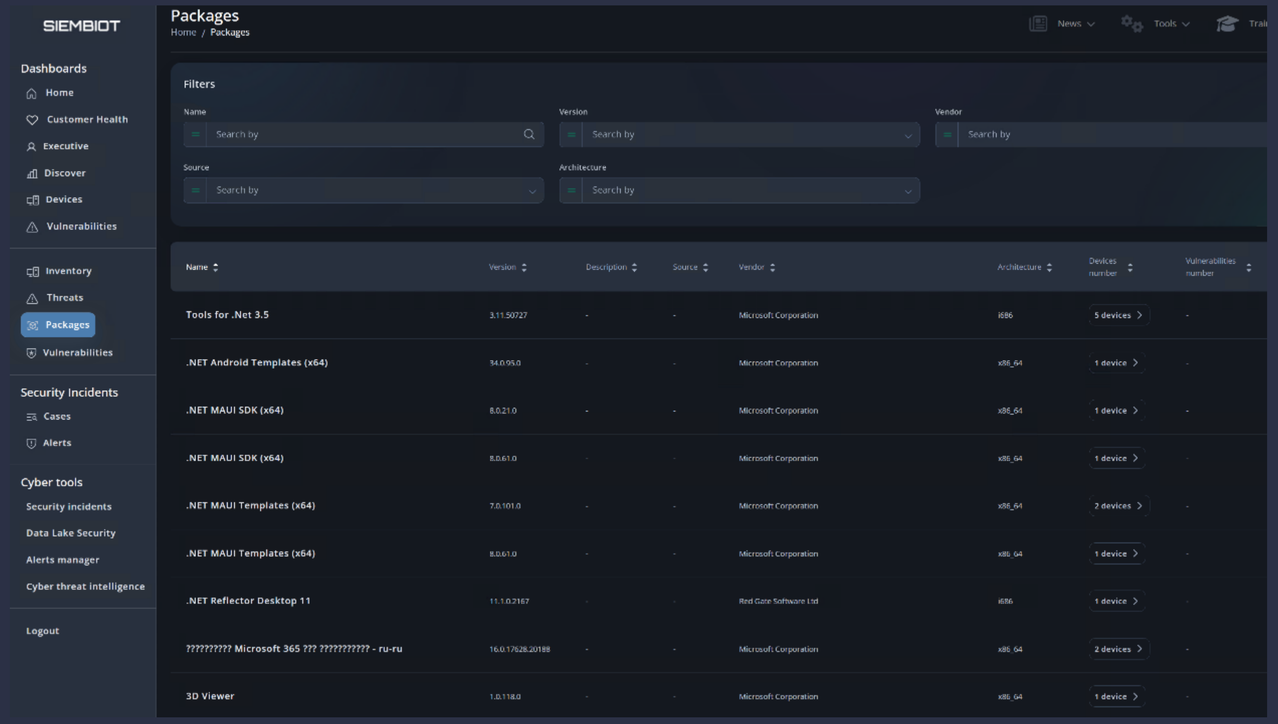
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

What are you missing ?

Asset Management with enrichments

- *Multi-source automatic device scanning, detection: AD/Azure/EDR/VM.*
- *Software package collection.*
- *Configuration comparison today vs. historical (2-180 days).*

- *Automatic reporting of detected vulnerabilities*
- *Security compliance reporting*
- *Detection of anomalies (e.g. computer device without EDR agent)*

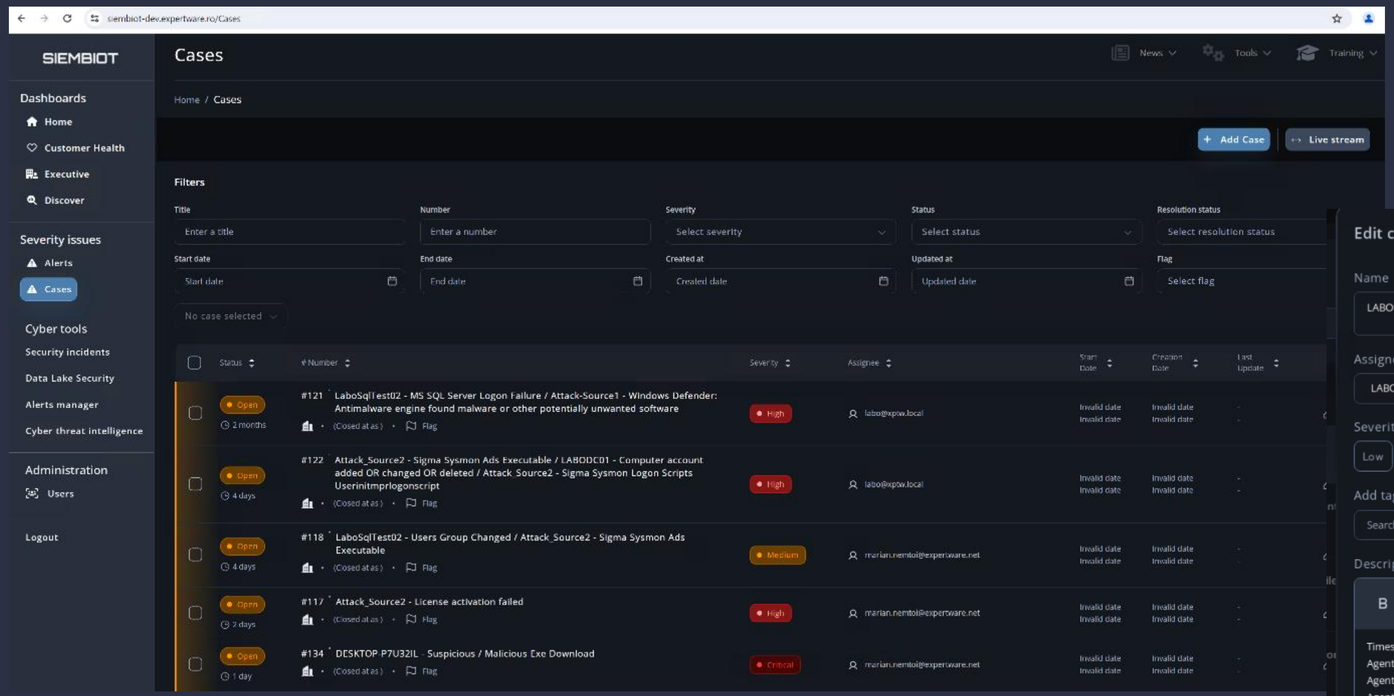


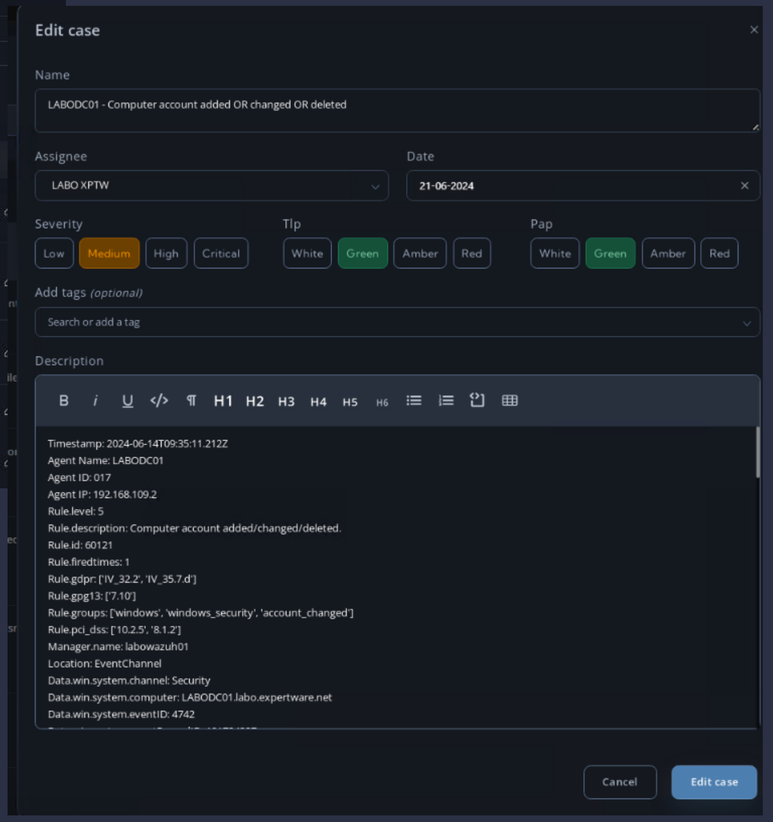
SIEMBIOT®

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

What are you missing ?

Security incidents management





- *Full investigation audit*
- *RBAC capabilities: SOC analysts, IT Ops, customer*
- *Advanced tagging and enrichment capabilities*

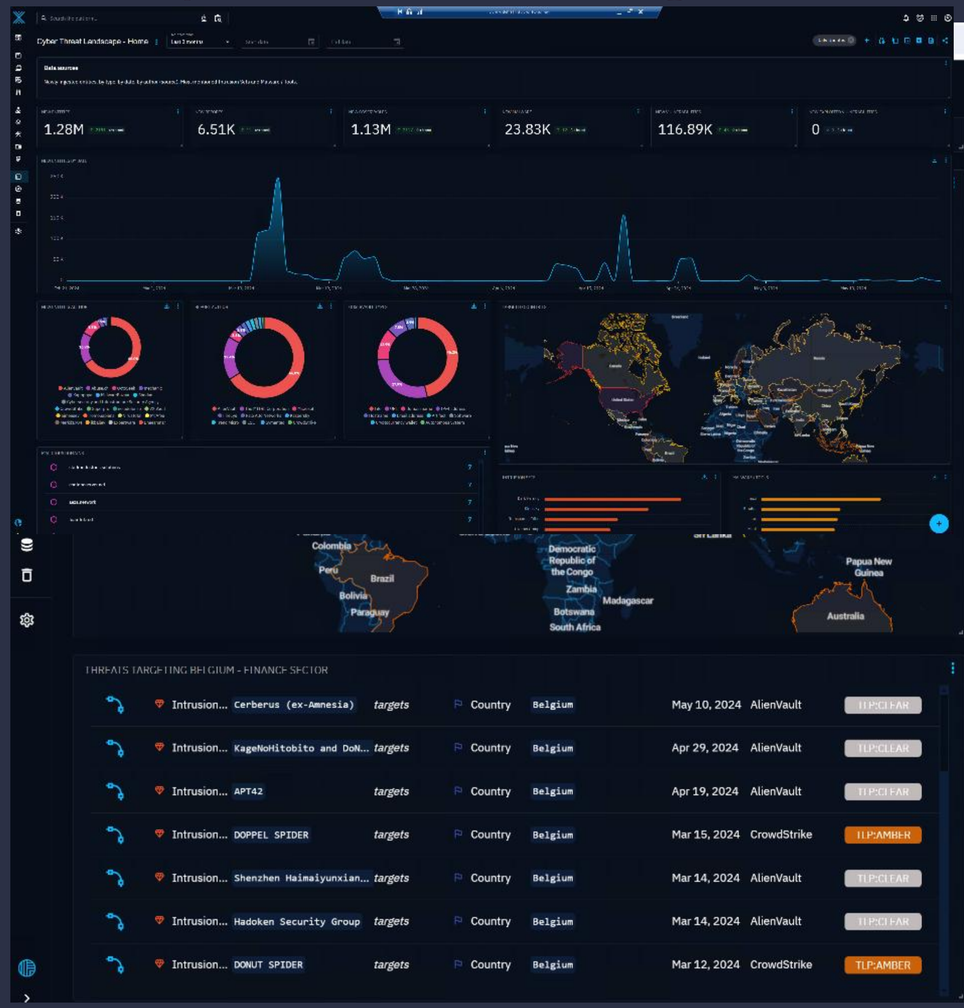
- *Qualification of alerts to security incidents*
- *Investigation workflow*
- *Integrated live stream*

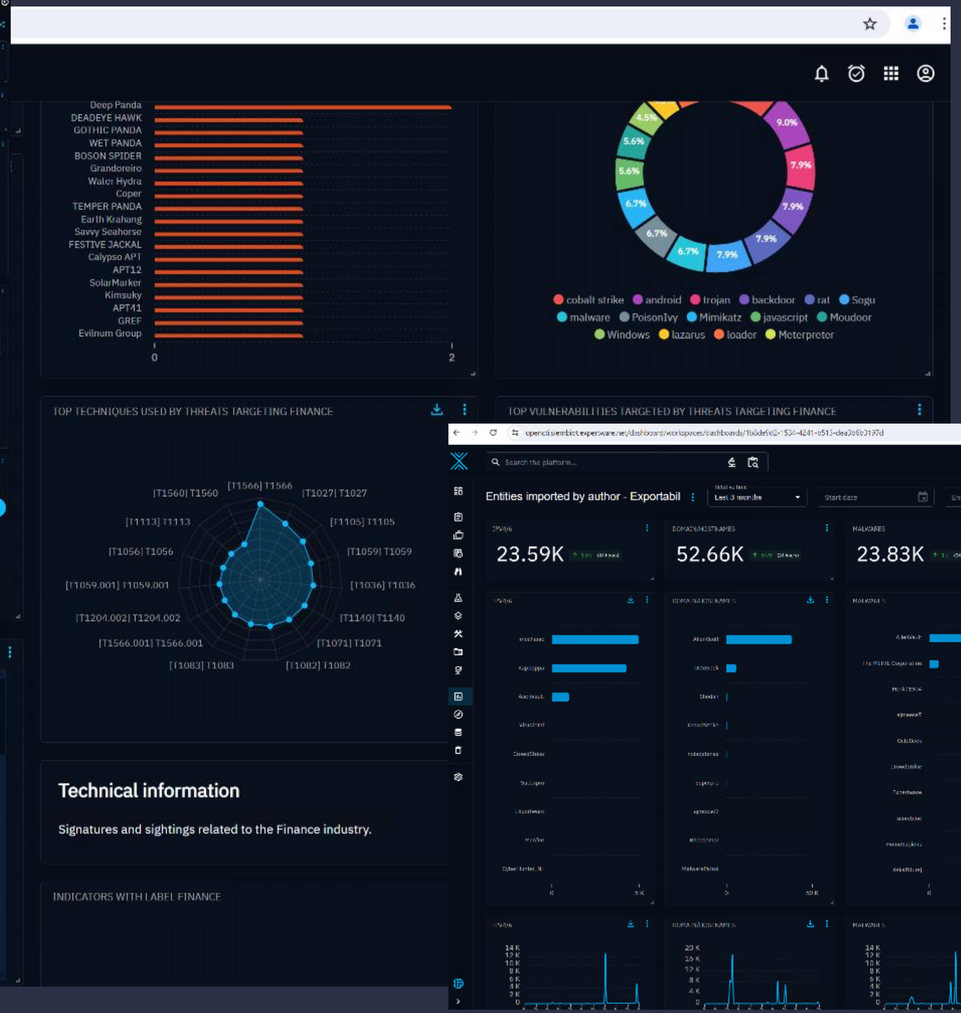
SIEMBIOT®

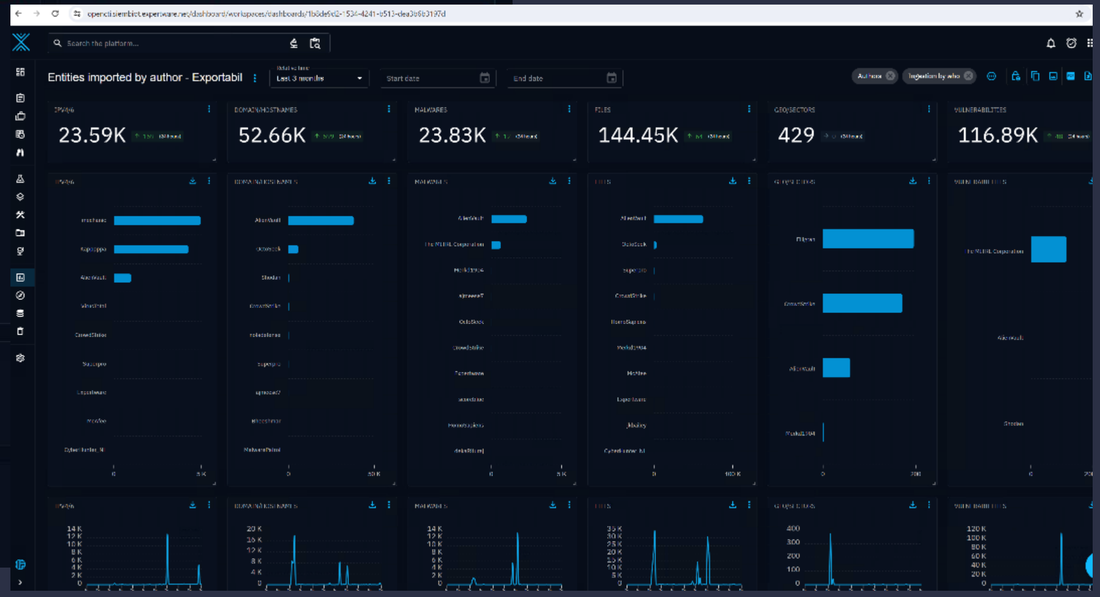
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

What are you missing ?

Live Cyber Threat Intelligence feeds & enrichments







- *12 billions CTIs*
- *15000 new CTIs ingested daily*
- *Industry tailored*

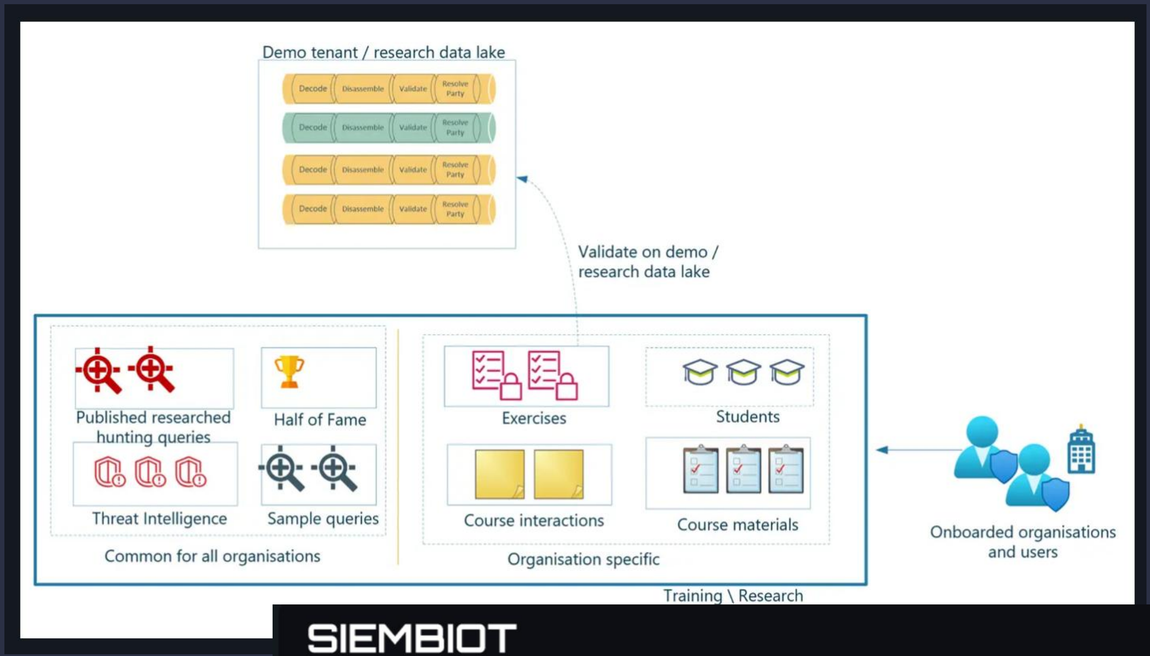
SIEMBIOT®

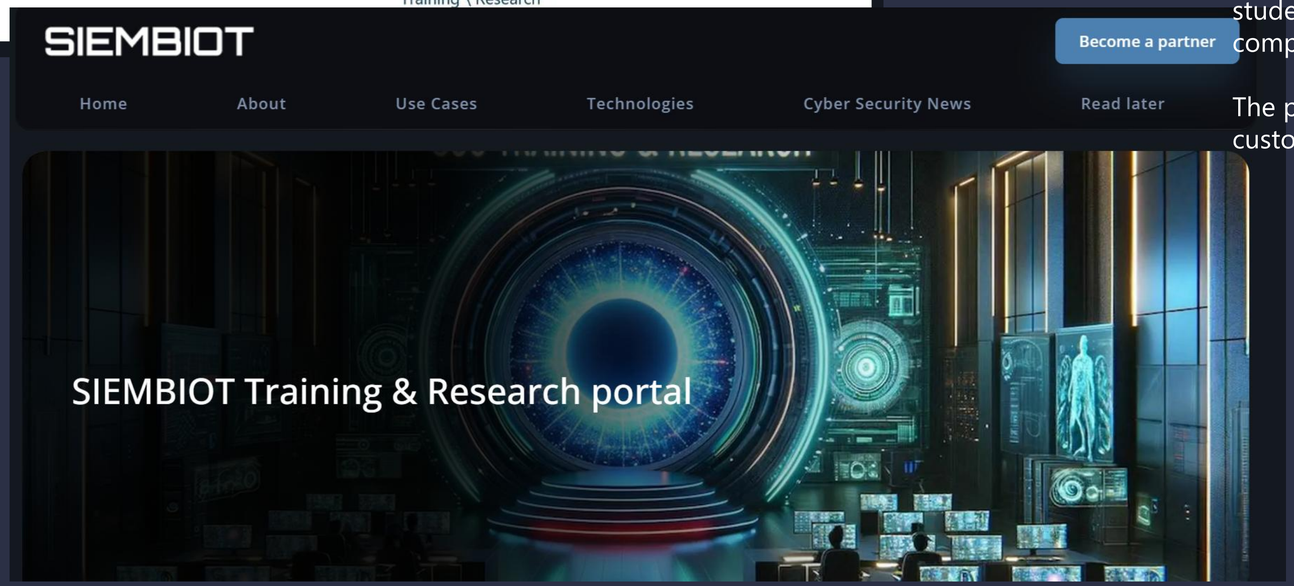
Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Training & Research





As of 2025 SIEMBIOT provides a complex training & research cyber range combining anonymized security events from multiple live customers' environments (10+ customers, 5000+ devices).

Training & research role-based web portal which complements the SOCaaS customer tenants allowing onboarded customer organizations and cyber security partners to train their teams for security incident management and threat hunting.

Organisations onboarded on the SIEMBIOT research platform will receive a dedicated portal space where they can demo attack scenarios, work collaboratively taking notes, storing knowledge articles, having access to cyber security news, developing, and saving new hunting queries. If they wish they can submit advanced hunting queries which after validation from the portal admins can be made available for the other organisations onboarded.

The portal will allow uploading course documents, defining exercising, collecting students results, evaluating them and overall improving their skills and competences.

The platform offers real life training based on attack simulation against live customers.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

What’s next ?

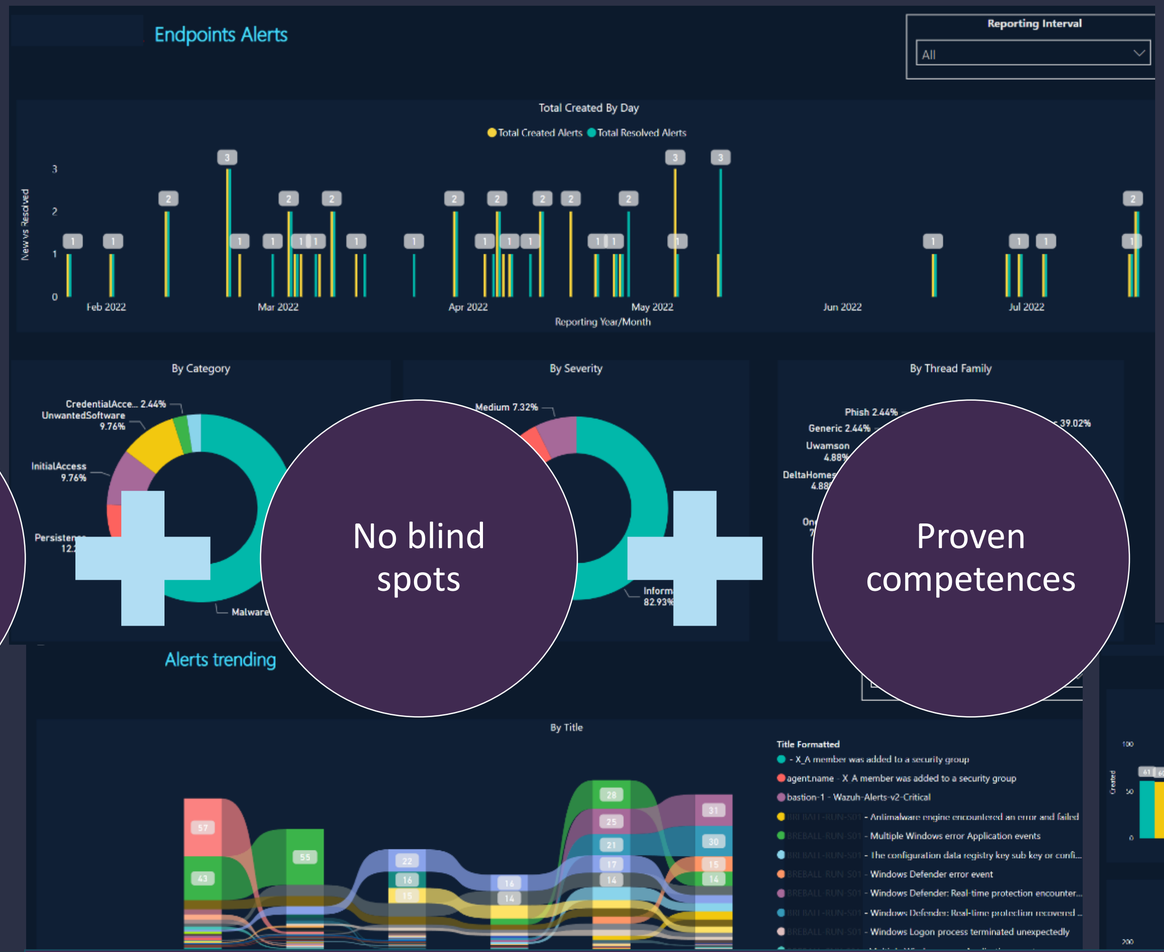
Open modular solution

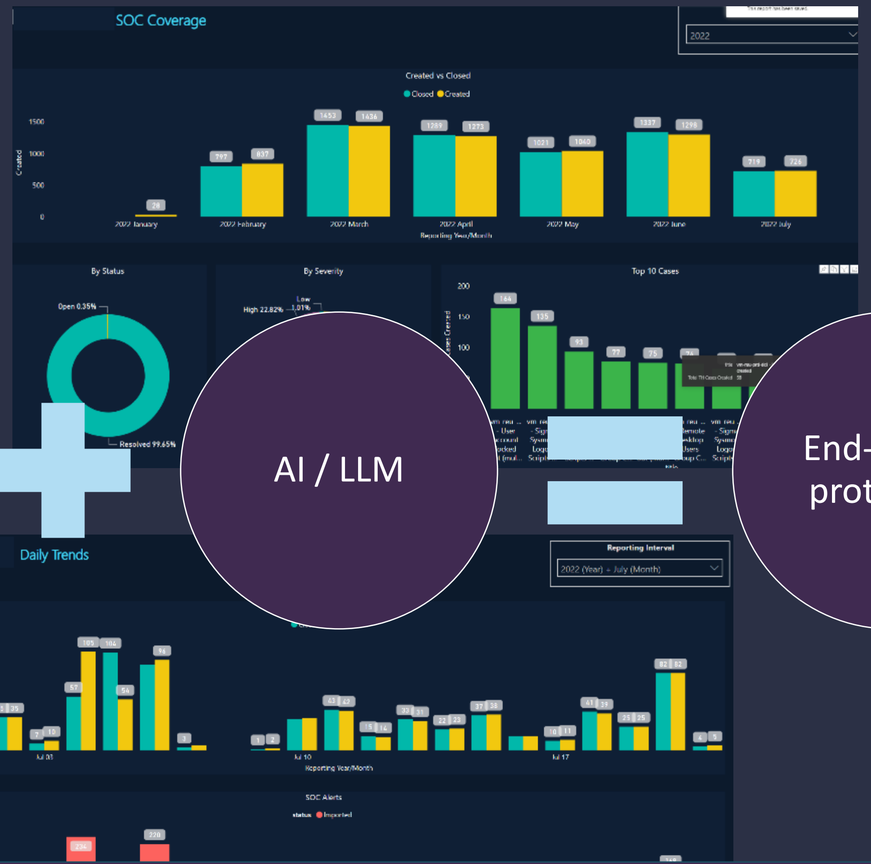
No blind spots

Proven competences

AI / LLM

End-to-end protection





The Power of the many: Collaborative threat intelligence platform easy to deploy and use.

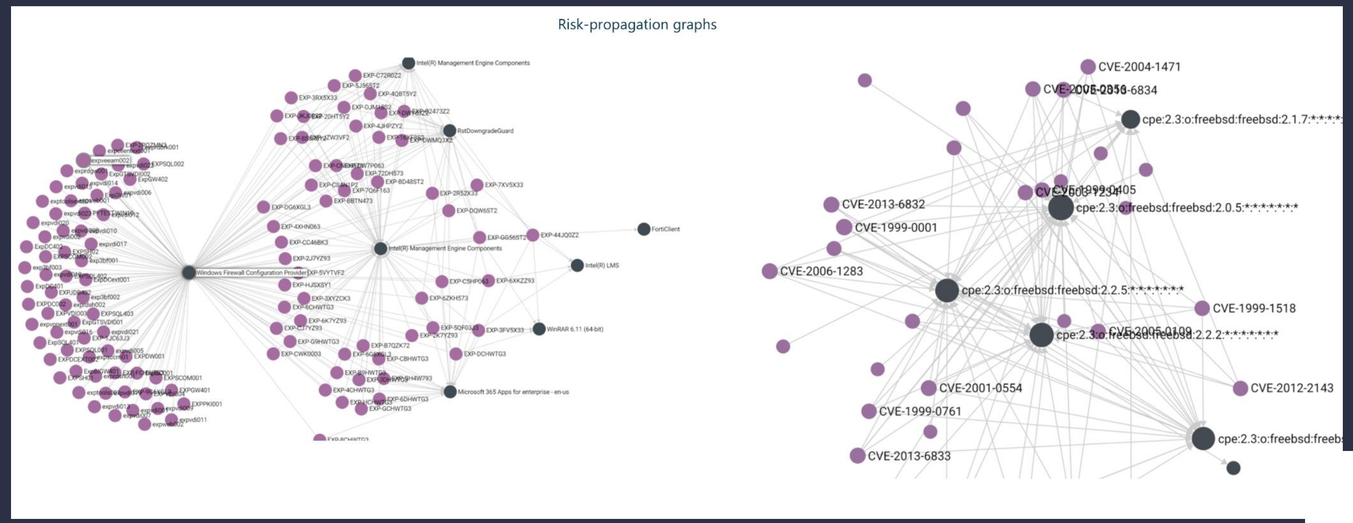
SIEMBIOT®

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

What’s next ?



User & Entity Behavior Analysis (UEBA) is being used by the major cyber security vendors. It aims to complement the security events with behavioral statistical metrics and to facilitate the detection of anomalies for early detection and decision support. Endpoint detection tools like Microsoft Defender have a mature data schema and collects data to train its own ML models.

Existing UEBA models include user, device and activity insights (application used, actions performed, countries connected from,). aSIEMmetry combines data from different sources / vendors, it normalizes and enriches it aiming to detect more complex patterns.

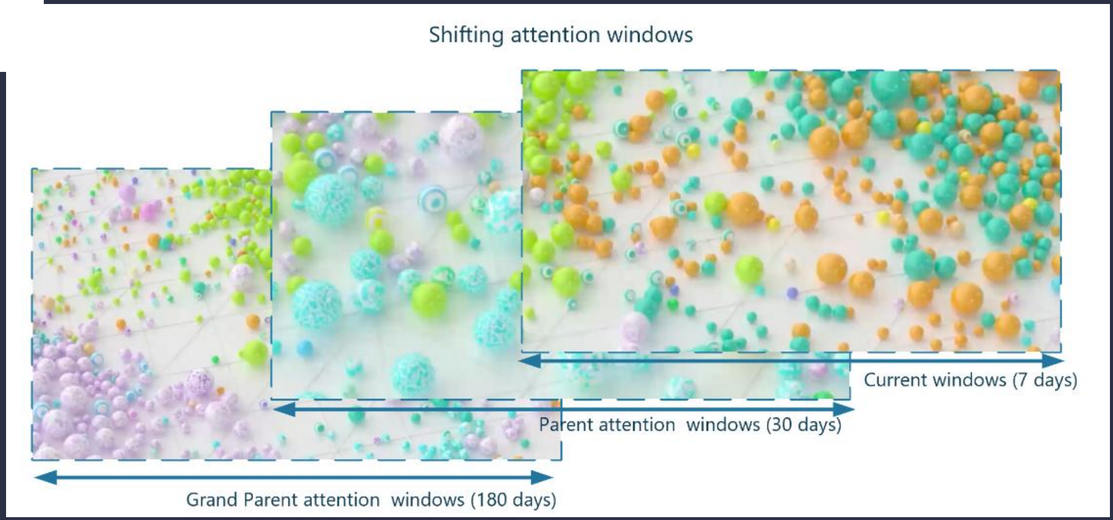
We baseline the “security entropy” model which allows identifying behavioral anomalies based on binary (suspicious, not suspicious) and multi-class classifications (known traffic, suspicious traffic partners, suspicious traffic volume deviation, suspicious traffic schedules). ion (performance and accuracy)

To overcome limitations, we developed cross-domain solutions to automate the analysis of large data. Since 2022

Expertware uses graphs connectivity algorithms (GNN) to enhance the vulnerability management process for managed assets, identifying cyber security risk propagation.

aSIEMmetry builds on the previous work expanding the model with user & entity behavioral analysis.

We built already SIEM vendor agnostic queries to collect, store and compare KPIs over longer periods of time to understand the metrics where we can potentially harness machine learning capabilities.



SIEMBIOT® – Platform functionalities

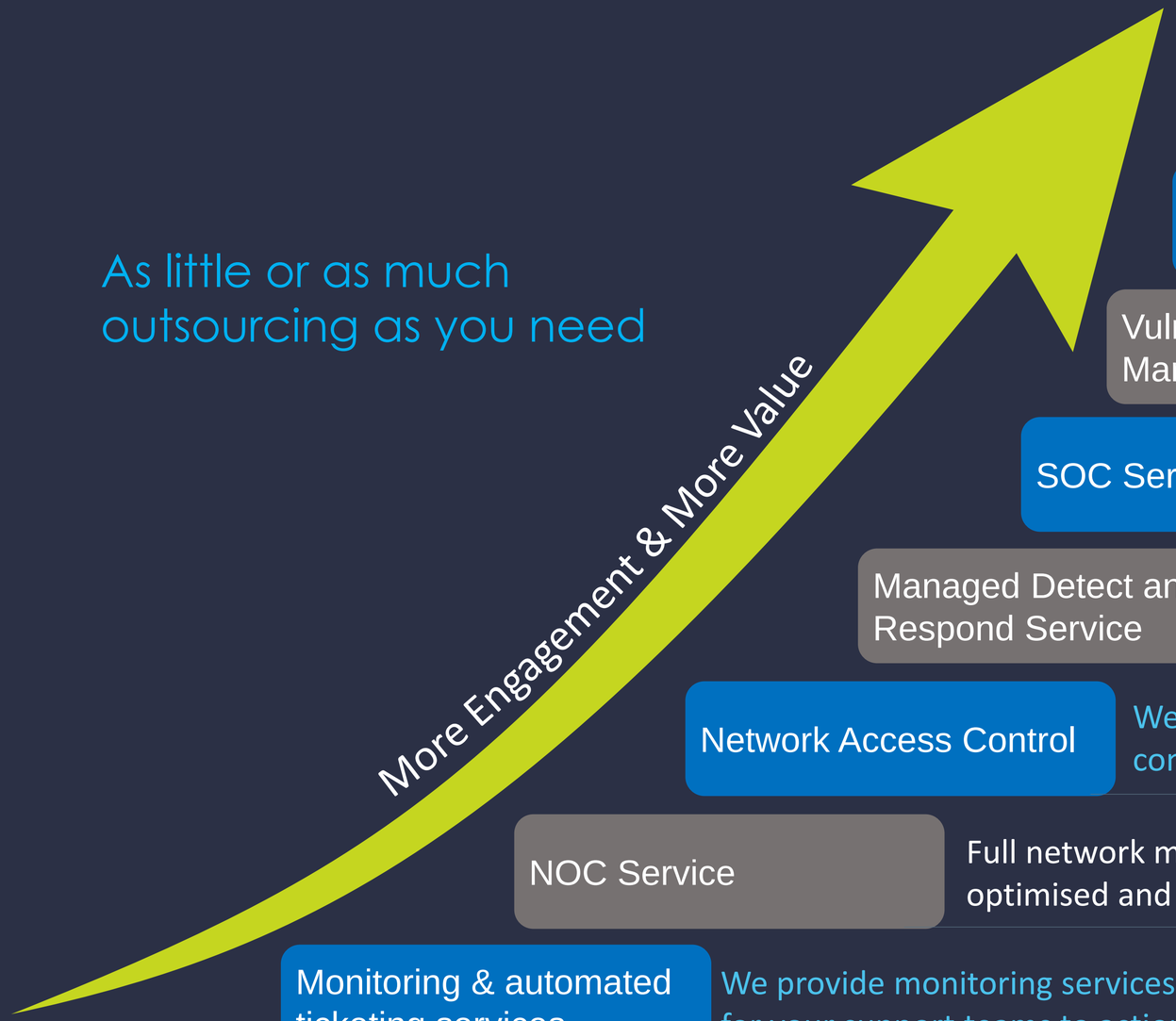
SIEMBIOT® Demo Tenant (dedicated)	Dedicated security data lake, open source EDR , open SIEM, 30+ connectors, 5000+ active alerts based on Sigma detections and many more.
SIEMBIOT® Cyber Threat Intelligence (shared)	20+ multiple CTI sources ingested continuously, tailored views basedo customer industry & location
SIEMBIOT® Vulnerability Scanning (shared)	Continuous multi-angle vulnerability detection, correlation and reporting
SIEMBIOT® Advanced Threat Hunting (automatic playbooks)	300+ detection and mitigation playbooks, compliance validation (CIS/NIS2/HIPAA)
SIEMBIOT® Asset Management	Multi-angle asset & software discovery, enrichment, detection of anomalies and historical comparison.
SIEMBIOT® Reporting	Live dashboards (executive, engineering, discovery, hunting, vulennrabilities, threats, cyber news)
SIEMBIOT® Training & Research Portal	Training and research portal, based on an anonymized data lake combining security events from multiple real customers & geographies. Capability to share and reuse CTF scenarios and advanced hunting playbooks.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Cyber Security

Other services where you can leverage us

As little or as much outsourcing as you need



CISOaaS
A complete outsourced Cybersecurity service

Managed SIEM
We provide a fully managed SIEM service with logging and data analytics

Vulnerability & Threat Management
We use Threat data and analytics to asses and resolve vulnerabilities and real world threats

SOC Service
We actively manage the Security stance of your IT environment

Managed Detect and Respond Service
We detect security issues in the environment and take action to resolve them

Network Access Control
We provide a managed network access control solution to ensure only validated & compliant devices connect to your network

NOC Service
Full network management, Monitoring, and Support service to ensure that your network is optimised and operational at all times.

Monitoring & automated ticketing services
We provide monitoring services that are constantly watching your network and devices reporting any anomalies for your support teams to action.

Why is Expertware the Answer ?

70k-120k/year/budget for 2 resources.

Mandatory indexation every year.

Traditional employment

VS

100k for a team of 3 named cyber security analysts ~ 260 days coverage




30% savings

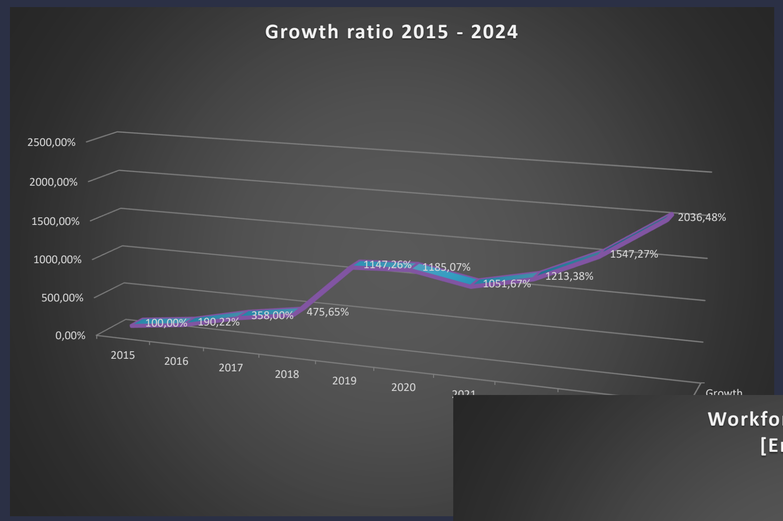
Expertware Team Augmentation Proposal

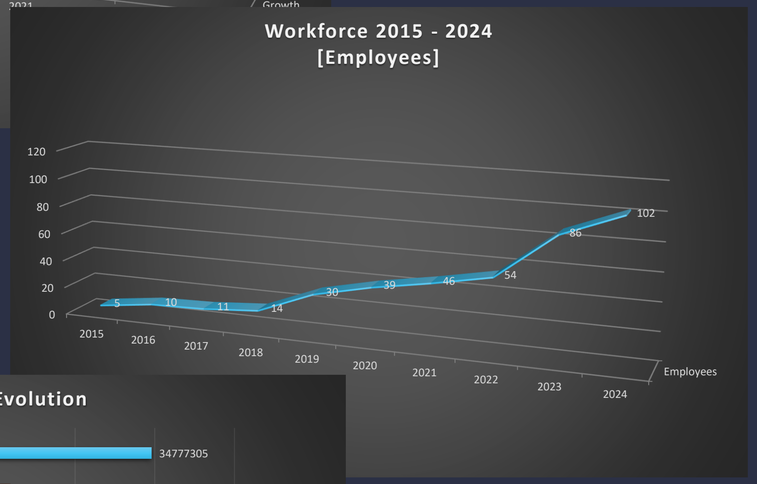
- Top senior consultants, 20+ years experience, vendor agnostic always seeking customers interests.
- Trusted by top European companies with multi billion yearly turnover
- Optimal costs , no surprises for the yearly budgets
- Exceptional employee retention (98% in the last 5 years). Stable assignments
- Exceptional customer retention (100% in the last 5 years).
- Proven competences and skills: 150+ certifications.
- Strong, focused partnership with top cyber security companies.

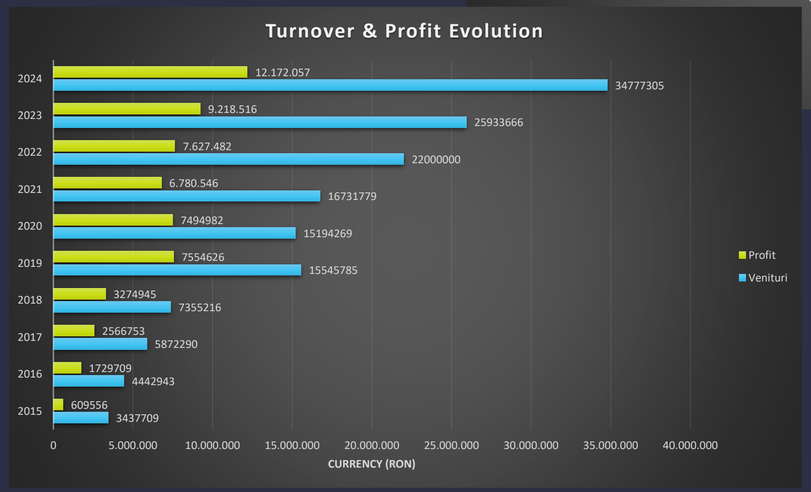
SIEMBIOT®

Co-funded by the European Union | ECCC European Cybersecurity Competence Centre | Directoratul Național de Securitate Cibernetică

Why Expertware?







History of proven results.

- 1st IT consultancy company in NE Romania for the last years.
- 25x financial growth in the last 18 years
- 20% Year on Year Growth in number of employees.
- 100+ Employees across 3 countries, 300+ IT certifications.
- Extensive Research Network, partnerships with top Universities.
- 4+ mil EU grants for 3 innovation projects (2023-2026)
- 100% customer retention over the last 5 years.
- Building characters, people, teams, solutions and applications.

www.expertware.net

Who trusts us today ?

24h/7 managed security services with granular service levels

Offices in **Romania, Tunisia, Belgium, UK**

Top European Customers with **multi-billion $ yearly revenues**.
100% large customer retention in the last **6 years**.

Large European MSPs (Econocom, Getronics, Telenet) trust us **as sole partner** for **Cybersecurity , BI, Hybrid-Cloud & Bespoke Development services.**

Year on year expansion with **1-2 blue-chip customers**.
Flexible support in : **English**, French, German, Romanian

Capability to bring rapid **business value (-25% TCO, + 25% productivity)** with the right mix of IT services (BI, analytics, workspace, cybersecurity)

Beneficiary of **3 European Innovation Grants** in the field of Cybersecurity.
~4 mil USD for the next 3 years.

These companies trust us, so can you!

BNP PARIBAS FORTIS	9.642 billions EUR
Audi	6.180 billions EUR
econocom	2.718 billions EUR
telenet	2.700 billions EUR
ENGIE	93,9 bill EUR
ERGO	20 bill EUR
Revantage / Blackstone	$326 billion of investor capital managed

SIEMBIOT®

Co-funded by the European Union · ECCC European Cybersecurity Competence Centre · Directoratul Național de Securitate Cibernetică

Partnership opportunity

Our collaborative Cyber intelligence platform welcomes you shortly as a beneficiary and partner !

- 6 to 12 months trial for full End-to-End protection: SIEM + EDR + CTI + VM + optional SOC services (incident response is optional and priced separately) .
- You cannot have a SOC without the prerequisites.
- Expertware & DNSC (“Directoratul National de Securitate Cibernetica”) partners in EU cyber project SIEMBIOT.
- Expertware has been involved in recent Ro hospitals ransomware investigations which could have been prevented by our Cyber Sec platform.
- SIEMBIOT research will continuously evolve offering enhanced protection for your users, networks, devices & applications
- Trial spots are limited. **Join us** before the capacity runs out.

Thank you!

CONTACT DETAILS

We’d love to hear from you!

info@expertware.net

https://Expertware.net

http:// siembiot.eu

Tiberiu Baraboi

- tiberiu.baraboi@expertware.net
- https://linkedin.com/in/tiberiubaraboi/