ECSO 10 YEARS
EUROPEAN CYBER SECURITY ORGANISATION

cyberhive®
discover solutions from EUROPE™

EVALUATION OF EUROPEAN CYBERSECURITY SOLUTIONS

cyberhive® MATRIX 2026

ECSO WORKING GROUP
Cybersecurity Market Development

thecyberhive.eu
ecs-org.eu

DISCLAIMER

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources, including external websites referenced in this publication.

COPYRIGHT NOTICE

© European Cyber Security Organisation (ECSO), 2026
Reproduction is authorised provided the source is acknowledged.

ABOUT THE CYBERHIVE MATRIX

The Cyberhive Matrix™ is a simple overview supporting end-users and investors when exploring European cybersecurity solutions. The Matrix is based on Cyberhive and open-source data, focusing on User Experience and European Readiness of the solutions during the assessment.

The European Cyber Security Organisation (ECSO), owner and initiator of Cyberhive, is an independent entity analyzing and evaluating solutions. The methodology is transparent and was constructed with the input of industry experts part of the Cyberhive Task Force. This supported approach puts trustworthiness, replicability, and usability central in the design process.

The Cyberhive Matrix™ is a report published annually. It consists of a matrix visual and a report. The visual showcases the solutions and includes two axes with criteria and aims to provide clarity at a glance. The report dives deeper into the solutions with descriptions, vendor profiles and European compliance.

ABOUT THE CYBERHIVE EUROPE

The **Cyberhive EUROPE®** is the digital marketplace for European cybersecurity solutions offering unified matchmaking tools to discover solutions beyond your local borders. ECSO membership is not required to enter Cyberhive, because we believe that an inclusive platform is integral to empowering an independent and transparent European cybersecurity industry.

ABOUT ECSO

The **European Cyber Security Organisation (ECSO)** is the pan-European, private-public federation (non-profit) focused on empowering European cybersecurity communities.

Established in 2016 as the European Commission's contractual partner for the Public-Private Partnership in Cybersecurity (2016-2020), we have built on the successes of that partnership to strengthen European cybersecurity by providing a platform for cooperation, community advocacy, public-private collaboration, and more.

CONTENTS

INTRO

1.

METHODOLOGY & CRITERIA

The criteria are a combination of all the input gathered from the **3 user groups** (providers, end-users, and investors). Each criterion is measured in a different unit, which can be assessed through **quantitative data** (numeric), or **qualitative data** (descriptive). The measured data is gathered via The Cyberhive EUROPE or open-source data.

The quantitative data is measurable and replicable. The qualitative data can be collected from text, from open-source data or Cyberhive. The quantitative analyses end up in the axes of the visual. Qualitative data can be used for descriptive text in the final document, quality marks, or seals or medals when a solution complies with a standard.

The criteria are measurable and replicable and serve as input for the analyses that are included in The Cyberhive Matrix with '**User experience**' and '**European readiness**' as axes. The criteria, units (how the criteria are measured) and their weights are indicated in the following pages. **The score used ranges from 0 to 5 for all existing criteria**.

Product vs Service

The Cyberhive Matrix 2026 is characterised by the distinction between a **cybersecurity product** and a **cybersecurity service**. A crucial difference that allows ECSO to perform score evaluation taking into account the specification of each solution. Some criteria that might be applicable to products, may not be suitable for services. That's why products and services are displayed in specific Matrix, where the axis 'User Experience' reflects each criterion designed for that purpose.

A cybersecurity **product** is a technology-based solution, typically software, hardware, or a hybrid system, designed to perform specific, repeatable security functions with minimal human intervention. Its value lies primarily in the capabilities built into the technology itself, which the customer operates and manages.

A cybersecurity **service** is an expert-driven activity delivered by professionals who apply processes, methodologies, and tools to improve an organisation's security posture. Its value comes primarily from human expertise, decision-making, and ongoing management, rather than from a standalone technical feature.

USER EXPERIENCE

For **products**, user experience criteria are directly linked to the solution itself, covering aspects such as ease of deployment, scalability and overall integration into different environments. It also reflects adaptability to evolving needs and user confidence in performance.

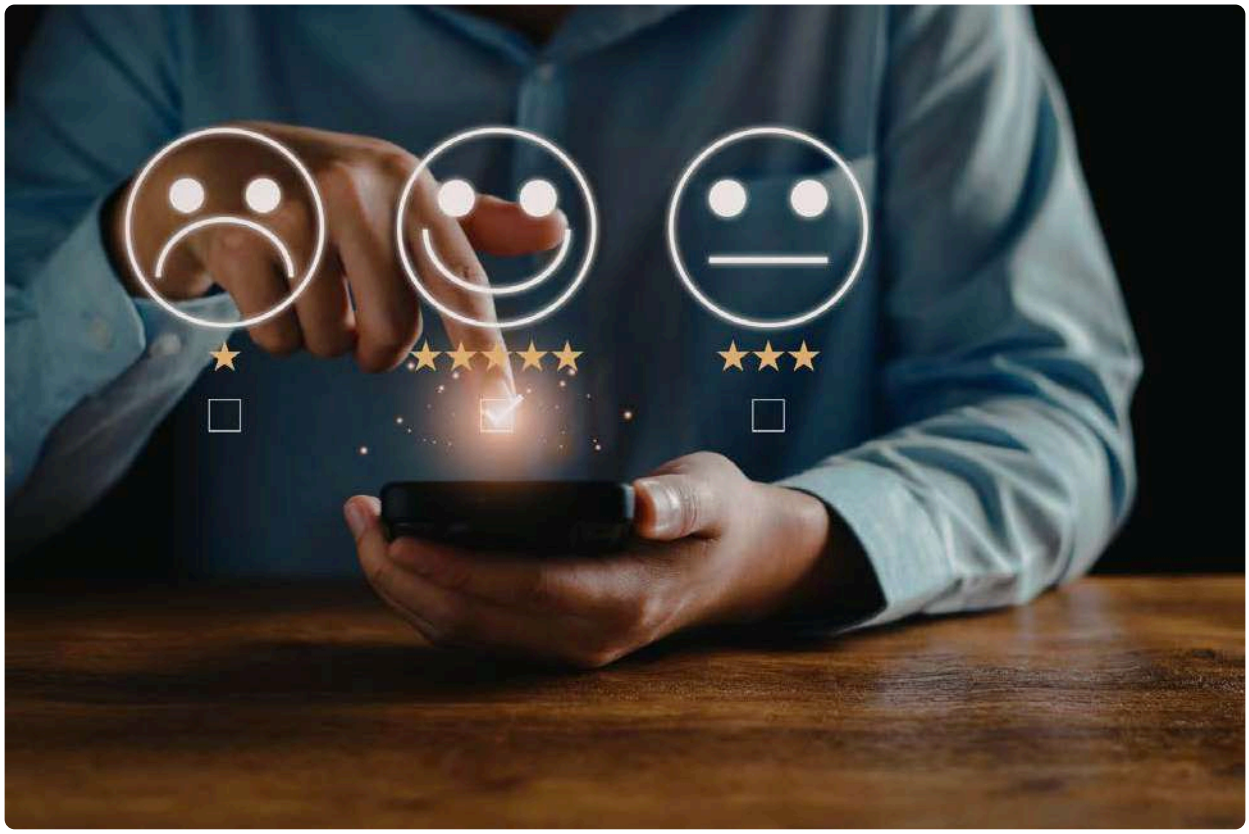
For **services**, user experience is directly linked to the category the solution belongs to, with tailored criteria designed to better reflect the nature of each service.

User Experience (Product)

CRITERIA	UNIT OF MEASUREMENT	WEIGHT
Overall user experience	Average overall rating (1-10 Open-Source)	30%
	Amount of recommendations (Weighted NPS - Open-Source)	30%
Ease of scalability	Average ease-of-scalability score (average 1-5 Open-Source and Cyberhive Score)	15%
Deployment support	Average ease-of-deployment score (average 1-5 Open-Source and Cyberhive Score)	15%
	Included deployment docs (Yes/no)	5%
	Included supporting docs (Yes/no)	5%

User Experience (Service)

CRITERIA	UNIT OF MEASUREMENT	WEIGHT
Overall user experience	Average overall rating (1-10 Open-Source)	30%
	Amount of recommendations (Weighted NPS - Open-Source)	30%
Category Custom	Average 1-5 (Open-Source and Cyberhive Score)	15%
Category Custom	Average 1-5 (Open-Source and Cyberhive Score)	15%
Support	Included SLA docs (Yes/no)	5%
	Included supporting docs (Yes/no)	5%



EUROPEAN READINESS

When referring to E**uropean Readiness**, the specific criterion is applied at the organisational level rather than to individual solutions. Therefore, the distinction between cybersecurity products and services is not applicable in this context. For this reason, a uniform calculation methodology has been adopted across all solutions. The parameters considered reflect the organisation's level of maturity and the extent to which the provider aligns with the European framework.

European readiness (product and service)

CRITERIA	UNIT OF MEASUREMENT	WEIGHT
Gender balance	% female, % male	15%
Governance transparency	Availability of company transparency: • Availability of website and LinkedIn (Yes/no) • Transparency of Board of Directors (Yes/no) • Transparency of ownership of the company (Yes/no)	35%
Language availability	Language coverage of solutions/support (% of languages covered in the EU)	10%
Promotion of EU (fit) solution	Phases of involvement through European association(s) or promotional means: • No representation via associations or promotion • Association or Cybersecurity Made in Europe Label • Association + Cybersecurity Made in Europe Label + The Cyberhive EUROPE	10%
Operational sovereignty	Data located in the EU (Yes/no/not applicable)	20%
	HQ established in an EU Member State (Yes/no)	10%

THE NEW ECSO CYBERSECURITY TAXONOMY

Another key difference in this year's edition is the introduction of the new **ECSO Cybersecurity Taxonomy**, which we are using to categorise each solution presented within the Cyberhive Matrix. Why did we decide to create a new taxonomy for cybersecurity solutions?

In recent years, we have witnessed an incredible boost in the cybersecurity sector, which has been increasing its market share by around 10% every year. At the same time, cybersecurity solutions have become far more effective, protecting devices against potential threats and offering a broader range of services associated with each solution.

At ECSO, through our digital marketplace, the Cyberhive, we observed that the original taxonomy, structured around the six NIST Cybersecurity Framework (CSF) functions (Detect, Protect, Identify, Recover, Respond, and Govern), is no longer sufficient to accurately describe what each solution actually does. Many solutions fall under multiple categories, which can create difficulties for potential buyers who are trying to explore the market and find the options that best suit their needs.

That is why, thanks to a panel of cybersecurity experts who worked alongside ECSO for several months, we created our new cybersecurity solutions taxonomy. Much like Copernicus's shift from a geocentric to a heliocentric model, our taxonomy reorients the analytical perspective from theoretical cybersecurity frameworks to the realities of the market.

Assumptions

Given the complexity of the task, we decided to work under certain **assumptions** that more clearly define the **scope** of our investigation. These assumptions set clear limitations on our analysis and help the reader understand the context within which each category lies. For this purpose, we defined the 13 principles highlighted below.

PRINCIPLE	DESCRIPTION
Security-Lens	Categories are limited to core security functionalities. They are designed to encompass any solution deployed to deliver cybersecurity protection, enforce security controls, or support compliance with widely recognised cybersecurity frameworks and regulatory requirements. Solutions that primarily address general IT operations, infrastructure management, or application functionality, without a primary and explicit security objective, are considered out of scope.
Functional categories	Categories are defined according to fundamental and persistent security functions, rather than vendor-specific terminology or marketing-driven labels. They are structured to remain stable and applicable over time, even as solution bundles evolve and new implementation models emerge.

PRINCIPLE	DESCRIPTION
Usability	The total number of categories is intentionally constrained to maximise usability and maintain a clear navigation structure. Highly granular categories derived from sub-functions or isolated features are excluded, as their inclusion would introduce unnecessary complexity and hinder effective comparison across solutions.
Category Distinctiveness	A category should exist as a standalone entity only when the security function it represents is clearly distinct in purpose from those of other categories. If combining it with another category would dilute its functional specificity or mislead users regarding its primary security value, it must remain separate.
Solutions Specificity	A revision of the taxonomy may be warranted when a significant number of solution providers consistently deliver cybersecurity capabilities that align with a distinct functional category not currently represented. In such cases, introducing a new category ensures that the taxonomy remains comprehensive, reflective of market reality, and capable of accurately classifying emerging solution domains.
Deployment Agnostic	Categories are independent of the deployment model (e.g., on-premise, cloud, or hybrid). Classification is determined solely by the security function delivered, focusing on what the solution accomplishes rather than how or where it is deployed.
Asset Agnostic	Categories are independent of the type of asset being protected (e.g., mobile, endpoint, network). Classification is driven by the security function performed, not by the specific asset on which that function is applied.
Layer Agnostic	Categories are independent of the type of asset being protected (e.g., mobile, endpoint, network). Classification is driven by the security function performed, not by the specific asset on which that function is applied.
Product vs. Service	Categories are independent of the provider's business model. When an organisation provides both a product and a distinct service, these offerings must be differentiated through dedicated metadata tags. This ensures clear classification, e.g., an MDR platform and its SOC-as-a-Service delivery model should be represented separately.
Services Definition	Cybersecurity services deliver security outcomes through the application of specialized expertise, structured processes, and supporting technologies. They encompass advisory, operational, and reactive activities designed to enhance an organisation's security posture, manage risk, and respond effectively to threats.

PRINCIPLE	DESCRIPTION
Versions Variations	Solutions available in multiple editions are listed separately only when their core security functions differ in a material way (e.g., substantial functional distinctions between Pro and Enterprise versions). No dedicated metadata tagging is applied for minor edition variations.
Core Function	A solution is assigned to the category that reflects its primary security purpose. Multi-function solutions are classified according to the dominant capability that defines their core contribution to the security domain.
Market Presence	A solution is included only if it is actively used in the market. Legacy releases and end-of-life (EOL) versions are excluded from classification. No dedicated metadata tagging is applied for deprecated editions.

Taxonomy List

As mentioned, for the 2026 edition of the Matrix Report, ECSO has decided to apply the new Cybersecurity Taxonomy. The list below presents the 12 categories identified.

CATEGORY	DEFINITION
Governance, Risk & Compliance (GRC)	A strategic framework implemented by organisations to align business objectives with operational processes and procedures, manage risks effectively, and ensure compliance with applicable laws, regulations and industry standards. At its core, GRC defines and enforces security policies, measures risk posture, and automate compliance with regulations.
Identity & Access Management (IAM)	The cybersecurity discipline that deals with provisioning and protecting digital identities and user access permissions in an IT system. IAM tools help ensure that the right people can access the right resources for the right reasons at the right time.
Data Security & Prevention (DSP)	The practice of protecting digital information from unauthorized access, corruption or theft through its lifecycle. A system's ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction within a centralized management framework.

CATEGORY	DEFINITION
Monitoring & Performance (MON)	An integral component of cybersecurity efforts that involves the observation and analysis of an IT ecosystem with the intent of safeguarding the environment and ensuring standards are met for specified needs. It consists in continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected.
Detection & Response (DnR)	The tools and processes organisations used to detect, investigate and mitigate cybersecurity threats. It combines advanced detection methods, automated response capabilities and integrated security solutions to help organisations reduce risk and adapt to an evolving threat landscape.
Vulnerability Management (VULN)	A continuous, proactive, and often automated process that keeps your computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. As such, it is an important part of an overall security program. By identifying, assessing, and addressing potential security weaknesses, organisations can help prevent attacks and minimize damage if one does occur. The goal of vulnerability management is to reduce the organisation's overall risk exposure by mitigating as many vulnerabilities as possible.
Offensive Security (OFFSEC)	A cybersecurity discipline focused on actively identifying, probing, and exploiting vulnerabilities in systems, networks, applications, and processes by simulating real-world attack techniques. Its purpose is to proactively uncover weaknesses before malicious actors can exploit them, enabling organisations to strengthen their defensive posture. Offensive Security uses the same tactics, techniques, and procedures (TTPs) as real attackers, but within a controlled, ethical, and authorised environment.
Orchestration (ORC)	Cybersecurity solutions that integrate, coordinate, and automate interactions between multiple security tools, systems, and processes to streamline operations and enable consistent, efficient, and scalable incident response. Orchestration platforms unify disparate technologies and operational workflows, ensuring that data, alerts, and actions can flow seamlessly across the security stack.
Cyber Threat Intelligence (CTI)	The process of collecting, analysing, and applying data on cyber threats, adversaries, and attack methodologies to enhance an organisation's security posture. It involves taking raw threat data from various sources and transforming it into actionable insights that enable organisations to anticipate, detect, and respond to cyber risks. Threat intelligence can be categorized into strategic intelligence, operational intelligence, and tactical intelligence, all of which offer strategic advantage against cybercriminals, nation-state actors, and insider threats. Properly informed and equipped, organisations can move beyond reactive defense and adopt a proactive security approach to mitigate risks before they materialize.

CATEGORY	DEFINITION
Recovery (REC)	The cybersecurity capabilities, processes, and technologies that enable an organisation to restore systems, data, and services to normal operation after a cyber incident. The Recovery function focuses on maintaining resilience, minimising downtime, and ensuring that critical business operations can continue or resume rapidly following disruptions caused by cyberattacks or system failures.
Digital Forensics Investigations (DFI)	The specialised cybersecurity discipline focused on the identification, collection, preservation, analysis, and documentation of digital evidence in a manner that maintains its integrity and admissibility. DFI aims to reconstruct events, determine the root cause of incidents, attribute malicious activity, and support legal, regulatory, or internal investigative processes.
Training (TRN)	Solutions and platforms that provide structured, hands-on learning environments designed to develop, enhance, and assess the skills of cybersecurity professionals and learners. These solutions use realistic simulations, interactive exercises, and guided scenarios to strengthen technical, operational, and decision-making capabilities relevant to defending against cyber threats.

Taxonomy requirements: examples and exclusions

Governance Risk & Compliance (GRC)

INDICATIVE REQUIREMENTS	• Maintain a versioned library of policies and controls. • Map controls major regulations (e.g., GDPR) and standard (e.g. ISO 27001, NIST). • Collect and store audit evidence. • Calculate and visualize risk scores and heatmaps. • Coordinate remediation workflows and attestations. • Obtain assurance and evidence of supply chain risk.
EXAMPLES	Policy-management, GRC solutions, audit treatment automation, compliance dashboards, risk analysis and management, supply chain risk management, awareness.
EXCLUSIONS	• Maintain a versioned library of policies and controls. • Map controls major regulations (e.g., GDPR) and standard (e.g. ISO 27001, NIST).

Identity and Access Management (IAM)

INDICATIVE REQUIREMENTS	• Manage full lifecycle of users, devices, and services. • Apply role-based and attribute-based access controls. • Support and potentially enforce authentication and authorisation policies. • Log authentication and authorization events for audit.
EXAMPLES	SSO, MFA, PAM, PKI, identity governance and administration, access proxy, CIAM, ISPM, activity audit trails, password managers.
EXCLUSIONS	• Data encryption solutions (DSP).

Data Security & Prevention (DSP)

INDICATIVE REQUIREMENTS	• Encrypt data at rest (symmetric, asymmetric, quantum-safe or post-quantum cryptography). • Encrypt data in transit (symmetric, asymmetric, quantum). • Encryption Key Management. • Enforce data-centric access controls & classification. • Inspect and block threats inline at network, web or app layers. • Tokenize or mask sensitive information. • Secure data deletion / erasure.
EXAMPLES	DLP, encryption gateways, tokenization platforms, PETS, MPCs, HSM, NGFW, WAF, host-based firewalls, VPN (Endpoint, Site2Site, VPN-SSL), Wiping solutions, database encryption, SAN/NAS/HD encryption.
EXCLUSIONS	• Access brokering (IAM). • Vulnerability scanners, patch-deployment systems (VULN).

Monitoring & Performance (MON)

INDICATIVE REQUIREMENTS	• Collect metrics and logs via agent-based or agentless methods. • Present real-time dashboards and multi-channel alerts for further analysis. • Allow external integration (e.g., with EDR/XDR).
EXAMPLES	Metric/log collectors, SIEM, network-flow analyzers, OT (security-related infrastructure monitoring).
EXCLUSIONS	• Manual threat-hunting workflows (Analytics & Detection).

Detection and Response (DnR)

INDICATIVE REQUIREMENTS

- Detect indicators of compromise and anomalous behaviors.
- Execute automated containment actions (quarantine, isolate).
- Use predefined playbooks or runbooks for incident workflows.
- Sandboxed execution environment.

EXAMPLES

EDR, IDS/IPS, automated quarantine, XDR, MDR (service), email security, malware analysis.

EXCLUSIONS

- Endpoint hardening solutions without active detection or containment (Prevention).

Vulnerability Management (VULN)

INDICATIVE REQUIREMENTS

- Scan assets continuously across on-premises, cloud, and container environments.
- Support static (SAST) and dynamic (DAST) analysis, and configuration scans (CSPM).
- Prioritize vulnerabilities by business impact and exploit risk.
- Track remediation progress and integration with ticketing systems.
- Keep update lists of all components, libraries and modules in a software product (SBOM).

EXAMPLES

SAST/DAST, container/cloud posture management, vulnerability scanners, CNAPP, application security testing.

EXCLUSIONS

- Patch-deployment systems (Prevention).
- Phishing simulations (TRN).

Offensive Security (OFFSEC)

INDICATIVE REQUIREMENTS	• Emulate adversary techniques. • Allow custom test plans and exploit configurations. • Generate prioritized findings and remediation recommendations.
EXAMPLES	Pentest frameworks, breach-and-attack-simulation (BAS), Red Team platforms.
EXCLUSIONS	• Passive monitoring solutions (Monitoring).

Orchestration (ORC)

INDICATIVE REQUIREMENTS	• Allow design of playbooks. • Drive playbook execution across solutions. • Facilitate coordination between team members. • Provide connectors for other security solutions.
EXAMPLES	SOAR platforms, case management, ticketing, automated workflows.
EXCLUSIONS	• Single-solution playbooks embedded in SIEM (Monitoring).

Cyber Threat Intelligence (CTI)

INDICATIVE REQUIREMENTS	• Ingest and normalize external feeds (OSINT, dark web, vulnerabilities). • Enrich and map TTP. • Alerting on IOC matches or feed changes. • Honeypots and deceptive security.
EXAMPLES	Threat-intel platforms, curated feeds, threat hunting rules platforms.
EXCLUSIONS	• Internal log analysis (Monitoring).

Recovery (REC)

INDICATIVE REQUIREMENTS

- Backup data and restore capabilities.
- Automate failover and failback mechanisms to minimize downtime.
- Integrate with incident response, security monitoring, and orchestration solutions for coordinated recovery.
- Regularly test recovery plans and validate RTO/RPO objectives.

EXAMPLES

Backup solution, redundancy systems, ransomware recovery, cloud recovery and resilience solutions, Business Continuity Planning (BCP) and DR orchestration solutions.

EXCLUSIONS

- Alert dashboards (Monitoring).

Digital Forensics Investigations (DFI)

INDICATIVE REQUIREMENTS

- Acquire forensic images of disks and memory dumps.
- Reconstruct event timelines from file and registry artifacts.
- Recover deleted files and extract detailed metadata.
- Reverse engineering of malware.
- Produce chain-of-custody evidence reports.

EXAMPLES

Memory-dump analysis, forensic imaging.

EXCLUSIONS

- Backups (Recovery).

Training (TRN)

INDICATIVE REQUIREMENTS

- Offer realistic, isolated environments for simulating cyberattacks and defense scenarios.
- Enable scenario customization and progression for different skill levels.
- Facilitate team-based exercises and collaboration.

EXAMPLES

Cyber ranges gamified trainings.

EXCLUSIONS

- Phishing simulations (Offensive).

JOIN THE CYBERHIVE EUROPE

The Cyberhive EUROPE® is accessible to **European organisations** that were established in Europe and have their headquarters in Europe. For privately or publicly held businesses, the majority of shareholders must be European entities. “Europe” is defined as the European Union (EU27), the European Free Trade Association (EFTA), the European Economic Area (EEA), and the United Kingdom (UK).

In addition, the following criteria apply:

1. Headquarter in Europe. If the company is part of a group, the group’s headquarters must be registered in Europe.

2. No major ownership or control from outside Europe.

3. Compliance with European laws and regulations applicable to the company, including data protection and privacy requirements defined by the EU’s General Data Protection Regulation (GDPR).

Featuring your cybersecurity solution in the Cyberhive Matrix is free and open for everyone. As an official participant of the Cyberhive Matrix, your solutions will be showcased to professionals from all across Europe and beyond, boosting your presence in the cybersecurity industry. Discover more **here** or scan the QRcode below:

INTEGRITY & INDEPENDENCE DISCLAIMER

The companies are rated according to the listed criteria by the European Cyber Security Organisation (ECSO), the initiator and owner of The Cyberhive EUROPE. ECSO is a non-profit based in Brussels. ECSO is a membership association and contributes to Europe’s Digital Sovereignty & Strategic Autonomy and to strengthening its cyber resilience. ECSO members are entities headquartered in the EU, EEA, EFTA or associated Horizon 2020 countries. These are defined as ‘ECSO countries’, and hold the right to participate in working groups and apply for board positions allowing voting at the General Assembly and eligibility to the Board of Directors. Associated members are not located in the earlier defined ECSO country. The ECSO statutes can be found here.

ECSO members outside the EU, EEA or EFTA are not included in The Cyberhive Matrix™, because these entities cannot enter Cyberhive (find the entry criteria here). The membership fee is fixed, and ECSO has no interest in favouring their members over other European players. The interest of ECSO is to **promote and increase the visibility of all European organisations** with solutions included in The Cyberhive Matrix™.

CYBERHIVE MATRIX 2026

DETECTION AND RESPONSE (PRODUCTS)

2.

CYBERHIVE MATRIX 2026

Detection and Response (Products) Matrix

*The scoring table is provided on the following page

CYBERHIVE MATRIX 2026

Detection and Response (Products) Matrix

Detection and Response (Products) scoring table

Cybersecurity solution	User experience	European readiness	Final score
ESET Protect XDR	4,76	4,70	**4,73**
Bitdefender GravityZone PHASR	4,84	4,60	**4,72**
Withsecure Elements XDR	4,73	4,55	**4,64**
Labyrinth Cyber Deception platform	4,64	4,35	**4,50**
Perimetrical by Transparent Edge	4,58	4,35	**4,47**
Aramis by aizoOn Technology	4,70	4,20	**4,45**
Nucleon EDR by Nucleon Security	4,28	4,10	**4,19**
Anantis TrapEye Deception Platform	4,25	4,00	**4,13**
Gryphon by Istrosec	3,80	4,35	**4,08**
Sekoia Defend	4,63	3,35	**3,99**
Endpoint Security HarfangLab	4,75	2,95	**3,85**
Nightshift by Digital Trust AS	3,60	3,05	**3,33**

ESET PROTECT XDR Platform

By ESET

ESET PROTECT is a cloud-first XDR cybersecurity platform that combines AI-native next-gen prevention, detection and proactive threat hunting. ESET provides modern Endpoint Protection Platform (EPP) capabilities via the ESET PROTECT Platform, covering Windows, Mac, Linux and both Android and iOS operating systems, providing Mobile Device Management functionality. To address evolving threats, ESET complements the platform with a wide range of services, including managed detection and response. It comes with multi-tenant management, ensuring real-time visibility for both on-premises and off-premises endpoints as well as full reporting for ESET enterprise-grade solutions from a single pane of glass. ESET PROTECT management platform can be securely deployed on-premise or in-cloud. Purchasing is easy. ESET offers and promotes comprehensive offering packages – rather than single standalone products – to better cover the customer's evolving EPP and XDR needs.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*1105 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,73

User Experience

Average rating	9,4*
Ease of scalability	4,6
Ease of Deployment	4,6
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Customers' Choice in the 2026 GPI Voice of the Customer for Endpoint Protection Platforms (EPP)

The only Challenger in the 2026 Gartner MQ for Endpoint Protection Platforms

Major Player in the IDC MarketScape: Worldwide XDR Software 2025

ESET PROTECT XDR Platform

By ESET

Solution	
Deployment support	Cloud, Hybrid, On-premises.
Supported platforms	Windows, macOS, Linux, Android, iOS.
Pricing Model	Subscription (monthly/yearly), Perpetual license.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	29% female / 71% male
Supported languages	English, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, Swedish, Ukrainian (98,99% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ESET adheres to globally recognized standards and certifications, including ISO 9001, ISO 27001, ISO 15408 (Common Criteria), FIPS 140-2 Level 1, SOC 2 Type 1 & 2, NIST Cybersecurity Framework, PCI DSS 3.2.1 and 4.0.0, and supports regulatory requirements such as HIPAA, GDPR, and NIS2. For more information, click here.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Bitdefender GravityZone PHASR

By Bitdefender

Bitdefender GravityZone PHASR is a groundbreaking Dynamic Attack Surface Reduction solution that proactively shuts down ransomware attack paths and augments any EDR solution by automatically hardening endpoints and restricting up to 95% of risky tools and actions.

Unlike conventional security, GravityZone PHASR uses self-learning AI models to continuously learn each user's behavior and correlate it with threat vectors to identify and automatically apply deep hardening, without requiring static rules and exceptions or impacting productivity.

Bitdefender GravityZone PHASR integrates seamlessly into the GravityZone security, risk and compliance management platform, minimizing deployment time and complexity for IT teams, and boosting operational and cost efficiency.

The innovative product is part of Bitdefender's Risk and Compliance vision of enabling organisations to proactively manage risks, effortlessly achieve compliance and focus on their business. This is achieved through a comprehensive set of risk, vulnerability, and exposure management capabilities that enable 360º visibility, pragmatic prioritization, automated compliance reporting and risk mitigation.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*718 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO CISO Community STRATEGIC PARTNER

ECSO OFFICIAL MEMBER

Final score	4,72

User Experience

Average rating	9.4*
Ease of scalability	4,7
Ease of Deployment	4,8
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

A Visionary in the 2025 Gartner® Magic Quadrant™ for EPPs²

A Customers' Choice – Gartner® Peer Insights™ Voice of the customer for Endpoint Protection Platforms 2026

A Vendor to Watch – IDC Market Analysis Perspective: European Endpoint Security, 2026

Bitdefender GravityZone PHASR

By Bitdefender

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	Windows for workstations, Windows for servers, Linux, macOS.
Pricing Model	Subscription (yearly).
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	PHASR is available as an add-on license to Bitdefender GravityZone Business Security Enterprise, MDR offerings and the GravityZone Cloud MSP Security Solutions , and as a standalone product, compatible with 3rd party EDR/XDR tools.

European readiness	
Gender balance	30% female / 70% male
Supported languages	English, French, German, Italian, Spanish, Romanian, Polish, Czech (39,63% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO/IEC 27001, ISO/IEC 27017:2021 , ISO/IEC 27002 for cloud services, ISO/IEC 27018:2020, SOC2 Type 2 Compliant, HIPAA Compliant, ISO 9001: Quality management systems.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

WithSecure Elements XDR

By WithSecure

WithSecure Elements Extended Detection and Response (XDR) WithSecure Elements XDR is a cloud-native software designed to provide prevention, extended detection and response capabilities for organisations seeking to enhance their cybersecurity posture. The software integrates threat detection in broad context, incident response, and automated response across endpoints, identities, email and other collaboration, cloud, and network environments. It consolidates security data from multiple sources to automatically identify advanced threats in real-time, offering analysis tools for rapid investigation and response to incidents. Organisations use the software to reduce the likelihood of beign attacked and streamline processes for proactive prevention, monitoring, investigations, and containment. The software addresses business challenges related to increasing complexity of threats across modern IT environments and the necessity for centralized visibility and control over security operations.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*144 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,64**

User Experience

Average rating	9.0*
Ease of scalability	4,5
Ease of Deployment	4,7
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

AV-TEST Best Protection 2024 (7th award).

A Champion and the #1 Midmarket Endpoint Protection Solution in the 2025 Emotional Footprint Awards by SoftwareReviews.

WithSecure Elements XDR

By WithSecure

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	Desktop Mac, Desktop Windows, Desktop Chromebook, Server Windows, Server Linux, Mobile Android, Mobile iOS, Microsoft Entra ID, Microsoft Azure.
Pricing Model	Pay as you go. Subscription (monthly/yearly).
Total Cost of Ownership (TCO) justification	One of the lowest TCO in AV-Comparatives' EPR test (2021).
Pricing Transparency	Cloud-based services with all-inclusive subscriptions.
European readiness	
Gender balance	25% female / 75% male
Supported languages	English, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Norwegian, Polish, Portuguese, Romanian, Spanish, Swedish (76,67% EU coverage).
EU Compliance driven	Strongly EU compliance-driven, incl. GDPR, NIS2.
Company standards & certifications	ISO/IEC 27001 Information Security Management Systems; ISAE 3402 Type II; NCSC UK Cyber Incident Response (CIR) Level 2; NCSC Germany Cyber Incident Response (CIR); CREST Cyber Security Incident Response (CSIR); CREST TIBER EU (Europe).
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Labyrinth Cyber Deception platform

By Labyrinth

Labyrinth creates the illusion of a real infrastructure vulnerability for an attacker. The solution is based on Points, a smart host simulation. Each part of the simulation environment reproduces the services and content of an actual network segment. The system consists of four components that interact with each other. The main components of the Platform are:
Admin VM is the main component. All collected information is sent to it for analysis. The console notifies the security team and sends the necessary data to third-party systems.
Worker - a host/virtual machine for deploying a set of Labyrinth network decoys (Points) on it. It can work in several VLANs simultaneously. Several Worker hosts can be connected to the same management console simultaneously.
Points are intelligent hosts that mimic software services, content, routers, devices, etc. Points detect all malicious activities within the corporate network, providing complete coverage of all possible attack vectors.
Seeder agents deployed on servers and workstations imitate the most attractive file artifacts for an attacker. By creating various decoy files, the agent directs attackers to network decoys (Points) through their contents.
The Platform automatically deploys points (decoys) in the IT/OT network based on information about services and devices in the network environment. In addition, decoys can be deployed manually, providing users with a powerful tool to develop their unique deception platform based on their specific needs and best practices. The Labyrinth provokes an attacker to act and detects suspicious activity. As the attacker passes through the fake target infrastructure, the Platform captures all the details of the enemy. The security team receives information about the sources of threats, the tools used, the vulnerabilities exploited, and the attacker's behavior. At the same time, the entire real infrastructure continues to operate without any negative impact.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✗ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✓ Videos
- ✓ Webinars

*5 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,50**

User Experience

Average rating	9.8*
Ease of scalability	4.8
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

ECSO's CISO Choice Award 2025 Winner.

Labyrinth Cyber Deception platform

By Labyrinth

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	All web browser supporting OSs, On-premise Windows, On-premise Linux.
Pricing Model	The license metric is a point (trap/decoy). One point corresponds to one trap/decoy. The standard minimum subscription is 10 traps/decoys per year, with a minimum annual price of 3990 EUR.
Total Cost of Ownership (TCO) justification	No additional cost needed.
Pricing Transparency	Single license metric – number of points (trap/decoys). Subscription model. No hidden costs, predictable pricing.

European readiness	
Gender balance	18% female / 82% male
Supported languages	English, Polish, Ukrainian (21,11% EU coverage).
EU Compliance driven	It is compliant with GDPR.
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

Perimetrical

By Transparent Edge

Perimetrical is a comprehensive protection for web applications and API that is simple, comprehensive, and quick to deploy. It features a next-generation firewall operating at the edge (WAAP) and includes cyberthreat detection and edge logic.

Perimetrical mitigates bots, protects against DDoS, is compliant and correlated with the OWASP Core Rule Set (CRS), manages anomalies, and provides API protection.

Our solution features advanced list management and Under Attack Mode (UAM). The anomaly management system allows you to configure automatic reactions from Anti-DDoS, WAF, and Anti-Bot based on different behaviors and custom thresholds.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*5 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,47**

User Experience

Average rating	9.4*
Ease of scalability	5
Ease of Deployment	4,8
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Perimetrical

By Transparent Edge

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	EUR 999/month.
Total Cost of Ownership (TCO) justification	Logic implemented and run at the edge nodes reduces the number of requests to origin, resulting in lower egress traffic from cloud provider; mid-tier (aka origin shield) reduces the number of requests to origin, resulting in lower egress traffic from cloud provider; image optimization at the edge reduces both requests to origin and storage space, again reducing overall cost; unlimited invalidations included in monthly fee; unique global rate, avoiding surcharges for delivery in remote regions; WAF service paid only for inspected requests (typically 10%–20% of total requests).
Pricing Transparency	N/A

European readiness

Gender balance	40% female / 60% male
Supported languages	English, Spanish (17,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO/IEC 27011 (Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations) National Security Framework (Esquema Nacional de Seguridad - ENS).
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Aramis

By aizoOn Technology

Aramis is a software designed to support advanced analytics and optimization for supply chain and production management. The software provides tools for data collection, modeling, forecasting, and scenario analysis to assist businesses in addressing operational challenges and improving efficiency. It enables organisations to monitor key performance indicators, evaluate resource utilization, and streamline decision-making processes in areas such as logistics, inventory, and manufacturing. By integrating data from various sources, the software facilitates simulation and prediction of process outcomes, contributing to cost control and risk management objectives for companies seeking to improve supply chain performance and production planning.

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,46**

User Experience

Average rating	10*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✗ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✗ Videos
- ✗ Webinars

*3 Reviews

Aramis

By aizoOn Technology

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Size and complexity of the company and type of service.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	31% female / 69% male
Supported languages	English (13,70% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	N/A
Privacy Policy compliant with EU GDPR	Yes

Nucleon EDR

By Nucleon Security

Nucleon Security provides an endpoint detection and response (EDR) solution designed to help organisations detect, investigate, and respond to cyber threats in real-time. Nucleon EDR combines behavioral analysis, threat intelligence, and machine learning to identify suspicious activities and block malicious behavior across endpoints. The platform offers deep visibility into endpoint activity, automated response capabilities, and customizable detection rules, helping organisations strengthen their cyber resilience. Nucleon EDR can be deployed on premises or in the cloud, with a strong focus on operational efficiency and data sovereignty. Beyond EDR, Nucleon Security delivers a broader cybersecurity stack that includes XDR, MDR, Malprob, ScorX, and ATOM AI, enabling organisations to extend protection from endpoint security to threat detection, investigation, prioritization, and SOC automation.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*7 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,19

User Experience

Average rating	9.2*
Ease of scalability	4
Ease of Deployment	4
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Nucleon EDR

By Nucleon Security

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux, Desktop Mac, Desktop Windows, Desktop Linux, Desktop Chromebook Mobile Android, Mobile iOS.
Pricing Model	45€/Endpoint/Year.
Total Cost of Ownership (TCO) justification	Nucleon Security offers a highly competitive TCO by combining an all-in-one SaaS model with strong operational efficiency. With no hidden costs, the subscription includes hosting, maintenance, updates, and premium support, eliminating the need for additional infrastructure or third-party tools.
Pricing Transparency	N/A

European readiness	
Gender balance	11% female / 89% male
Supported languages	English (13,70% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Anantis TrapEye Deception Platform

By Anantis

Anantis TrapEye is an advanced cybersecurity deception platform that detects intruders the moment they interact with your network. Deploy realistic honeypots and decoy assets across cloud and on-premise environments to gain instant visibility into attacker activity, reduce Mean Time to Detect (MTTD), and stop advanced threats before they cause damage. Highlights:

- Real-time deception-based intrusion detection using honeypots and decoy assets with near-zero false positives.
- Deployed in less than 30 minutes to protect Cloud, hybrid, and on-premise environments with a single deception platform.
- Reduce detection time dramatically by exposing lateral movement and attacker activity at first interaction.

High-fidelity, deception-based alerts eliminate noise and false positives, providing security teams with actionable intelligence. TrapEye integrates seamlessly with existing SOC workflows and SIEM platforms, and supports deployment across AWS, hybrid, and on-premise environments. Each detected interaction is automatically mapped to the MITRE ATT&CK® framework, giving analysts clear visibility into attacker tactics and techniques.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*1 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE ×

ECSO OFFICIAL MEMBER ×

Final score	4,13

User Experience

Average rating	9*
Ease of scalability	4
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Anantis TrapEye Deception Platform

By Anantis

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux.
Pricing Model	Pricing is custom and depends on the size and complexity of the client's infrastructure.
Total Cost of Ownership (TCO) justification	Faster detection of threats: Reducing the Mean Time to Detect helps limit the impact of incidents and avoid costly escalations. Less triage fatigue: A low number of false positives means analysts spend less time investigating noise and more time on real threats. Fast deployment across Cloud & On-Prem: The solution can be deployed quickly without heavy infrastructure or complex setup, which keeps implementation costs low.
Pricing Transparency	N/A

European readiness

Gender balance	0% female / 100% male
Supported languages	English, French, German (21,11% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

GRYPHON Ransomware Protection Toolkit

By IstroSec

IstroSec is a trusted European cybersecurity vendor, combining proprietary R&D and global technology alliances to deliver advanced intelligence services, strengthening organisational resilience against complex threats with innovation, measurable protection, and strategic trust.

GRYPHON Ransomware Protection Toolkit is a European agent-based solution to detect and protect organisation against the most pervasive and costly forms of cyberattacks, mainly ransomware and APT, as a next security layer to common EDR/XDR solutions.

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,08**

User Experience

Average rating	8*
Ease of scalability	4
Ease of Deployment	3
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Support services offered

- ✓ Email/Help desk
- ✓ FAQs/Forum
- ✓ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✗ Live online
- ✗ Videos
- ✗ Webinars

*1 Reviews

GRYPHON Ransomware Protection Toolkit

By IstroSec

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux.
Pricing Model	44.05 EUR / user / yearly subscription.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	21% female / 79% male
Supported languages	English, Slovak, Czech (21,11% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Sekoia Defend

By Sekoia

Sekoia Defend (Next-Gen SIEM) is an AI SOC platform for eXtended Detection and Response (XDR) in SaaS mode and powered by AI and exclusive cyber threat intelligence. Anticipation of attacks, automation, numerous integrations and verified detection rules simplify the protection of hybrid environments.

Cyberhive Page	
Distinctions	
Basic Cyberhive Member	
CYBERSECURITY MADE IN EUROPE	
ECSO OFFICIAL MEMBER	
Final score	3,99
User Experience	
Average rating	9.6*
Ease of scalability	4,9
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes
Awards	

No awards received yet.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*12 Reviews

Sekoia Defend

By Sekoia

Solution	
Deployment support	Cloud, SaaS, web-based, on-premise / private cloud.
Supported platforms	All web browsers.
Pricing Model	Subscription (monthly/yearly)
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	30% female / 70% male
Supported languages	English (13,70% EU coverage).
EU Compliance driven	Data hosted & processed in the EU GDPR compliant. Supports NIS2 implementation (link); empowers CRA compliance (link); terms of use (link).
Company standards & certifications	PCI-DSS Certification, ISO 27001 certification, SOC 2 Type 1 report (NEW).
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Endpoint Security HarfangLab

By HarfangLab

HarfangLab endpoint security solutions are made in Europe. Designed to detect and respond to cyberattacks on workstations and servers, the solution is composed of lightweight agents that can be quickly and easily deployed in both Cloud and On-Premise environments. Supporting Windows, macOS, and Linux operating systems, these agents integrate multiple detection engines that generate security alerts based on suspicious behaviors or identified threats. They enable automatic blocking actions on the most critical security events. Finally, they also empower preventive actions such as USB device control and firewall.

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	3,85

User Experience

Average rating	9.8*
Ease of scalability	4,7
Ease of Deployment	4,8
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Support services offered

- ✓ Email/Help desk
- ✓ FAQs/Forum
- ✓ Knowledge base
- ✗ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✗ Live online
- ✓ Videos
- ✓ Webinars

*33 Reviews

Endpoint Security HarfangLab

By HarfangLab

Solution

Deployment support	Cloud, SaaS, On-premise.
Supported platforms	On-premise Linux, Desktop Mac Desktop Windows, Desktop Linux, On-premise Windows.
Pricing Model	Subscription (monthly/yearly) Depending on deployment type - On-prem vs Cloud.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness

Gender balance	20% female / 80% male
Supported languages	English, French, German (21,11% EU coverage).
EU Compliance driven	Yes
Company standards & certifications	Certification de Sécurité de Premier Niveau (CSPN), BSI, Qualification By ANSSI.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

NightShift

By Digital Trust AS

NightShift is an AI-native software platform that helps CTOs, CIOs, and technical founders understand and manage cybersecurity risk across the technology environment their organisation depends on.

Built for organisations where security matters but team capacity is limited, NightShift flags emerging risks, ranks them by business impact and technical severity, and provides evidence-backed reports for leadership, customers, partners, investors, and compliance reviews.

NightShift can act as a next-generation SIEM eliminating need for full-scale SOC or analytical team.

Cyberhive Page

Distinctions

- Basic Cyberhive Member
- CYBERSECURITY MADE IN EUROPE ×
- ECSO OFFICIAL MEMBER ×

Final score	3,33

User Experience

Average rating	8*
Ease of scalability	4
Ease of Deployment	5
Incl. deployment docs	N/A
Incl. supporting docs	N/A

Awards

No awards received yet.

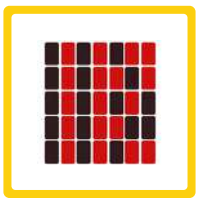
Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✗ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✗ Videos
- ✗ Webinars

*1 Reviews



NightShift

By Digital Trust AS

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	From 1300 EUR / month
Total Cost of Ownership (TCO) justification	Due to the flat pricing structure, we don't charge per asset (compared to many other SIEM solutions), which gives a predictable and fair pricing to our customers.
Pricing Transparency	N/A

European readiness

Gender balance	50% female / 50% male
Supported languages	English, Norwegian, Spanish (21,11% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

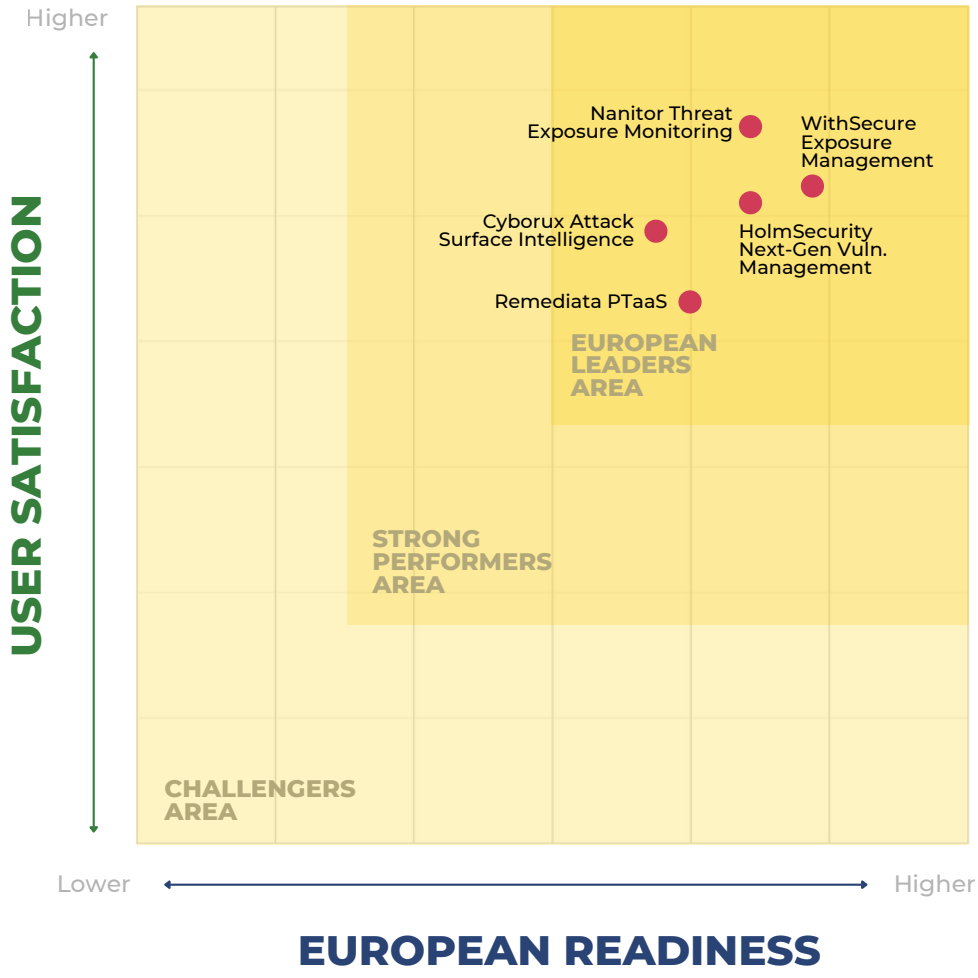
CYBERHIVE MATRIX 2026

VULNERABILITY MANAGEMENT

3.

CYBERHIVE MATRIX 2026

Vulnerability Management Matrix



Vulnerability Management scoring table

Cybersecurity solution	User experience	European readiness	Final score
WithSecure Element Exposure Management	4,55	4,45	**4,50**
Nanitor Continuous Threat Exposure Monitoring	4,70	4,25	**4,48**
Holm Security Next-Gen Vulnerability Management Platform	4,52	4,25	**4,39**
Cyborux Attack Surface Intelligence	4,48	3,90	**4,19**
Remediata PTaaS Platform	4,25	4,00	**4,13**

WithSecure Element Exposure Management

By WithSecure

WithSecure Elements Exposure Management is a cloud-native software designed to identify, classify, and prioritize security vulnerabilities across modern IT environments.

The software enables continuous vulnerability scanning and assessment of external attack surface and networked assets including servers, endpoints, identities, and cloud resources. The software uses patent-pending AI-based attack path simulation technologies for heuristic exposure hunting and adversarial exposure validation. It provides automated detection through a centralized dashboard, reporting tools, and actionable insights to assist organisations in addressing exposures before they can be exploited. The software supports workflow integration by allowing users to track remediation progress and monitor compliance with security policies. By facilitating continuous assessments and clear reporting, this software helps organisations strengthen their cyber resilience and manage risks associated with exploitable security weaknesses.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*72 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,50**

User Experience

Average rating	9.2*
Ease of scalability	4.8
Ease of Deployment	4
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

The Best Vulnerability Management Solution award at teissAwards2025.

A Champion in the Vulnerability Management category of SoftwareReviews 2026 Data Quadrant.

WithSecure Element Exposure Management

By WithSecure

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	Desktop Windows, Desktop Mac, Server Windows, Microsoft Entra ID, Microsoft Azure, Amazon Web Services.
Pricing Model	Pay as you go. Subscription (monthly/yearly).
Total Cost of Ownership (TCO) justification	Proactive cyber risk reduction. AI-based attack path simulation catches an attack path before an attacker does. Significantly reduces the need for penetration testing and red teaming exercises.
Pricing Transparency	Cloud-based services with all-inclusive subscriptions.
European readiness	
Gender balance	25% female / 75% male
Supported languages	English, Finnish, French, German, Italian, Norwegian, Polish, Portuguese, Spanish, Swedish (43,33% EU coverage).
EU Compliance driven	Strongly EU compliance-driven, incl. GDPR, NIS2.
Company standards & certifications	ISO/IEC 27001 Information Security Management Systems; ISAE 3402 Type II; NCSC UK Cyber Incident Response (CIR) Level 2; NCSC Germany Cyber Incident Response (CIR); CREST Cyber Security Incident Response (CSIR); CREST TIBER EU (Europe).
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Nanitor Continuous Threat Exposure Monitoring

By Nanitor

Nanitor delivers a modern Continuous Threat Exposure Management (CTEM) platform that gives organisations real-time clarity and control over their entire attack surface.

Unlike traditional vulnerability scanners that provide periodic snapshots, Nanitor continuously discovers assets, validates exposures, and prioritizes what truly matters based on actual business impact, not risk guesswork.
At the core of the platform is Nanitor Diamond, a unique prioritization model that moves beyond simple CVSS scores. It combines exploitability, exposure context, configuration posture, and compensating controls to highlight the issues that genuinely put your organisation at risk. The result: fewer false alarms, faster remediation, and sharper focus for IT and security teams.

Nanitor integrates seamlessly into existing environments, consolidating vulnerabilities, misconfigurations, compliance gaps, and identity risks into a single, actionable workflow. Automated validation, stakeholder-ready reporting, and built-in collaboration tools make it simple to turn insights into measurable security improvements.

Designed and built in Europe, Nanitor supports both cloud and on-prem deployments and includes multi-tenant capabilities purpose-built for MSPs and MSSPs.

With Nanitor, security teams move from reactive firefighting to proactive, continuous resilience — reducing risk, strengthening compliance, and eliminating blind spots across their digital estate.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✓ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✗ Live online
- ✓ Videos
- ✗ Webinars

*4 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,48**

User Experience

Average rating	10*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Nanitor Continuous Threat Exposure Monitoring

By Nanitor

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux.
Pricing Model	Subscription (monthly/yearly). Custom pricing.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	19% female / 81% male
Supported languages	English (13,70% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO/IEC 27001 Information Security Management Systems.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Holm Security Next-Gen Vulnerability Management Platform

By Holm Security

Holm Security is a European leader in vulnerability and exposure management, helping organisations build a systematic, risk-based, and proactive cyber defense. As the threat landscape grows in complexity and regulatory pressure intensifies across Europe, Holm Security gives security teams the visibility and control they need to reduce risk by managing exposure effectively. Built and operated on European infrastructure, Holm Security's platform combines deep vulnerability management with built-in attack surface management, delivering both security excellence and the data sovereignty that organisations increasingly demand. Learn more here.

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE ×

ECSO OFFICIAL MEMBER ×

Final score	**4,39**

User Experience

Average rating	9*
Ease of scalability	4,3
Ease of Deployment	4,5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Gartner Peer Insights, Voice of the Customer (Vulnerability Assessment).

PCI ASV (Approved Scanning Vendor) — PCI DSS v4.0.

ISO/IEC 27001:2022 certified.

NIS/NIS2 certified.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*86 Reviews

Holm Security Next-Gen Vulnerability Management Platform

By Holm Security

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	Systems & servers (Windows, Linux), Network devices, Cloud-native platforms (Microsoft Azure, AWS, Google Cloud, Oracle Cloud), Microsoft 365, Operational Technology (OT), IoT devices, Kubernetes, Web applications, APIs.
Pricing Model	Subscription-based SaaS pricing with flexible tiers scaling from approximately €1 – €50 per asset/month depending on module and asset type. Optional annual Success and Certification Programs also available.
Total Cost of Ownership (TCO) justification	Total Cost of Ownership typically ranges from €10,000 to €250,000 per year, scaling with size and support tier.
Pricing Transparency	Public pricing guidance and FAQ available here.

European readiness	
Gender balance	25% female / 75% male
Supported languages	Danish, Dutch, English, French, German, Hungarian, Italian, Norwegian, Polish, Spanish, Swedish, Ukrainian (54,44% EU coverage).
EU Compliance driven	NIS2 Directive, DORA, Cyber Resilience Act (CRA), ISO/IEC 27001, PCI DSS v4.0, and GDPR.
Company standards & certifications	ISO/IEC 27001:2022 certified, NIS2 compliant, PCI DSS v4.0 Approved Scanning Vendor (ASV).
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Cyborux Attack Surface Intelligence

By Cyborux

Most organisations don't know what's exposed about them on the internet. Cyborux continuously scans and monitors your external attack surface so you can find and fix risks before attackers exploit them. Key capabilities:

- Asset discovery: automatically identifies exposed subdomains, forgotten infrastructure, and misconfigurations.
- Credential monitoring: detects leaked email credentials and data breaches linked to your organisation
- Phishing risk assessment: identifies employees and digital identities most vulnerable to social engineering
- Document metadata analysis: surfaces sensitive information leaked through publicly accessible files
- Deep web scanning: assesses exposure and threats beyond the surface web
- Continuous automated monitoring: alerts you when new risks appear, no manual checks needed
- White-label ready: IT service providers and consultancies can deliver Cyborux intelligence under their own brand.

Support services offered

- ✓ Email/Help desk
- ✓ FAQs/Forum
- ✗ Knowledge base
- ✗ Phone support

Training services offered

- ✓ Documentation
- ✗ In person
- ✗ Live online
- ✗ Videos
- ✗ Webinars

*10 Reviews

Cyberhive Page	
Distinctions	
Basic Cyberhive Member	
CYBERSECURITY MADE IN EUROPE	✗
ECSO OFFICIAL MEMBER	✗
Final score	4,19
User Experience	
Average rating	8,5*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	N/A
Incl. supporting docs	Yes
Awards	

INCIBE x Wayra Finalist.

Cyborux Attack Surface Intelligence

By Cyborux

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Pricing starts at €449.90/month for continuous monitoring of up to 5 domains. One-time assessments available from €139.90. Enterprise and white-label plans available on request. Pricing is per domain analysed, not per user and not credit-based.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness

Gender balance	0% female / 100% male
Supported languages	English, Spanish (17,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

Remediata PTaaS Platform

By Remediata

Remediata is a boutique offensive security consultancy delivering high-impact penetration testing and red teaming for ambitious tech and enterprise teams. We pair elite, expert-led security assessments with our proprietary PTaaS and vulnerability management platform to turn real-world attack insights into continuous, measurable risk reduction.
Remediata offensive security platform combining expert-led penetration testing with continuous vulnerability management, helping teams track findings, validate fixes, and maintain real-world security readiness in one unified workspace.

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE ×

ECSO OFFICIAL MEMBER ×

Final score	4,19

User Experience

Average rating	9*
Ease of scalability	5
Ease of Deployment	4
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✓ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✗ In person
- ✓ Live online
- ✓ Videos
- ✗ Webinars

*3 Reviews

Remediata PTaaS Platform

By Remediata

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Pricing is not based on a per-user/month model. Remediata is priced based on scope, environment size, and service requirements. Custom pricing.
Total Cost of Ownership (TCO) justification	Total cost of ownership depends on deployment scope and testing requirements. The Remediata platform reduces operational security costs by consolidating vulnerability tracking, remediation workflows, and penetration testing outputs into a single platform, reducing manual effort, duplicated tooling, and remediation delays.
Pricing Transparency	N/A

European readiness	
Gender balance	10% female / 90% male
Supported languages	English, Czech, Slovak, Ukrainian (24,81% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	IISO/IEC 27001 certified Information Security Management System, CREST accredited.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

CYBERHIVE MATRIX 2026

OFFENSIVE SECURITY

4.

CYBERHIVE MATRIX 2026

Offensive Security Matrix

Offensive Security scoring table

Cybersecurity solution	User experience	European readiness	Final score
SelfHack AI	4,40	4,85	**4,62**
Bug Bounty Platform by Unguess Security	4,73	4,45	**4,59**
Security Reporter by DongIT	4,43	4,70	**4,57**
Cybersecurity Services by Cybernetica AS	3,90	4,20	**4,05**
Offensive Security and Exposure Management Platform by YesWeHack	4,78	2,95	**3,87**
Auditguard	4,20	3,00	**3,60**

SelfHack AI

By Self Hack

SelfHack AI is an autonomous AI-driven offensive security platform built as an AI army of coordinated attack agents. It continuously attacks organisations' systems the same way real adversaries do across web applications, APIs, cloud environments, Kubernetes clusters, and external networks etc.

Unlike traditional vulnerability scanners and point-in-time pentests, SelfHack AI does not rely on static signatures, checklists, or one-off assessments. It replaces scanners and manual pentesting with real attack execution, exploit validation, and continuous verification of security posture. SelfHack AI does not simply report findings. It proves risk, verifies exploitability, and confirms remediation.

SelfHack AI enables organisations to move from reactive security and false-positive noise to continuous, proof-based offensive security where security is not assumed, scanned, or promised, but continuously tested and demonstrated.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✗ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✓ Videos
- ✗ Webinars

*3 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,62

User Experience

Average rating	9*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

SelfHack AI

By Self Hack

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Subscription (monthly/yearly). Perpetual license. Custom pricing.
Total Cost of Ownership (TCO) justification	SelfHack AI significantly reduces Total Cost of Ownership (TCO) by eliminating the need for continuous manual penetration testing and expensive security consultancy. Our autonomous AI agent conducts high-quality, human-like security assessments without requiring in-house pentesting teams or outsourced services.Unlike traditional models that require repeated manual effort and training, our solution: Runs 24/7 with zero fatigue, Offers predictable and fixed pricing, Generates compliance-ready reports, Requires no large infrastructure or license dependencies.
Pricing Transparency	N/A

European readiness

Gender balance	50% female / 50% male
Supported languages	English, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, Swedish (98,99% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

Bug Bounty Program

By Unguess Security

UNGUESS Security is a continuous, always-on offensive security platform designed to help organisations scale vulnerability discovery and validation using a managed model, a community of 200+ vetted, European certified ethical hackers and AI agents working in close collaboration with internal security and engineering teams.
At its core, UNGUESS Security combines two elements:

A trusted community of European security researchers.

UNGUESS Security is backed by a growing community (with a strong Italian and French footprint) of certified professionals who are technically assessed, identity-verified (KYC), and contractually bound by terms, privacy policies, and a code of conduct. Researchers are ranked and invited to private programs based on proven performance, enabling companies to tap into diverse skill sets (web, mobile, API, cloud, IoT/OT, etc.) without the typical bottlenecks of hiring and retention: https://security.unguess.io/

AI Agents Frameworks.

UNGUESS AI Pentest combines the speed and scale of agentic AI with the judgment and expertise of certified human hackers. Built on the UNGUESS Security platform and backed by a community of 200+ European ethical hackers, it goes far beyond generic scanners—emulating real-world attacker behavior, surfacing exploitable risk, and validating every finding with a human expert. The result: broad coverage at machine
speed, with the depth and accuracy only human intelligence can deliver.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✗ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✗ In person
- ✓ Live online
- ✓ Videos
- ✓ Webinars

*27 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,59

User Experience

Average rating	9,6*
Ease of scalability	4,8
Ease of Deployment	4,8
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Bug Bounty Program

By Unguess Security

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Pay as you go, subscription (monthly/yearly), custom pricing.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	40% female / 60% male
Supported languages	English, French, German, Italian, (24,81% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	Company certifications: ISO 20000, ISO 27001, ISO 9001, ISO 14001, ISO 14064, ISO 45001, ISO 37001, PAS 24000; UNI/PdR 125 Hacker certifications: CRTO, CPENT, LPT MASTER, CAED, OSCP, OSCP+, CPTS, GPEN, CCNA, CCNP, eCPTX, eCPPTv2, eCPPT, CRTP, OSCE³, OSED, OSEP, OSWE, eWPT, eWPTXv2, eJPT, APISec, eWPTX, OSCE, eCXD, PCI ASV, OPSA, JFP, MFE, CRTE, CEH, eMAPT, CESCAS.
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

Security Reporter

By DongIT

Security Reporter is a self-hosted platform for professional security assessment teams. It centralizes the full engagement lifecycle — scoping, credentials, findings, peer review, client collaboration, and remediation tracking — in a single workspace, on infrastructure you control.
Designed for teams that handle high-stakes security assessments, Reporter reduces manual reporting effort, improves report quality, and keeps assessment data under your own control. Researchers document findings as they work, in structured format, eliminating manual report assembly and reducing the administrative overhead that typically consumes senior researcher time at the end of an engagement. Reports are consistent, methodology-driven, and client-ready without reconciliation across multiple tools or file versions. Security Reporter supports structured reporting for TIBER-EU, NIS2, DORA, and CRA-aligned assessments, making it suitable for firms operating in regulated sectors or serving clients with compliance reporting requirements. Available as on-premise deployment for Windows and Linux. Assessment data remains on your own infrastructure at all times.

- Self-hosted deployment — full control over sensitive assessment data, no third-party cloud dependency.
- End-to-end engagement workflow — scoping, credentials, findings, and report generation in one centralized workspace.
- Structured peer review and QA flows — consistent report quality across every engagement and every team member.
- Reusable methodology and template library — supports TIBER-EU, NIS2, DORA, and CRA-aligned assessment frameworks.
- Client collaboration and remediation tracking — structured follow-up after delivery, so the engagement doesn't end when the PDF is sent.
- API and webhook integrations — connects with Burp Suite, Nessus, and existing security tooling.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✓ Knowledge base
- ✓ Phone support

Training services offered

N/A

*5 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,57**

User Experience

Average rating	9,2*
Ease of scalability	4,5
Ease of Deployment	4,5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Security Reporter

By DongIT

Solution	
Deployment support	On-premise.
Supported platforms	Multiple platforms, flexible self-hosted platform.
Pricing Model	Subscription (yearly).
Total Cost of Ownership (TCO) justification	Depends on the company's setup.
Pricing Transparency	Tier model pricing.

European readiness	
Gender balance	27% female / 73% male
Supported languages	English, Dutch, French, German, Spanish + Custom (100% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO 27001, CCV KeurmerkPentesten.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Cybersecurity Services

By Cybernetica AS

Cybersecurity Department is created to protect and defend organisations from threats in cyberspace.

Cybernetica provides cybersecurity solutions that create better cyber situational awareness for the protected systems. We help systematically identify and assess the elements (like system mission and processes, assets, threats, vulnerabilities, risks) required for obtaining adequate situational awareness, as well as help to convert the data of elements into organised, relevant and insightful information that enables comprehension of situation. We train, test and assess the experts, implemented systems and protective measures to create the ability to predict or anticipate the future states or events of the situation.
Cybernetica provides assessment, testing and advisory services for organisations who care about their real-world cybersecurity.

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,05

User Experience

Average rating	9,0*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	No
Incl. supporting docs	No

Awards

No awards received yet.

Support services offered

N/A

Training services offered

- ✓ Documentation
- ✗ In person
- ✗ Live online
- ✗ Videos
- ✗ Webinars

*1 Reviews

Cybersecurity Services

By Cybernetica AS

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux, Desktop Mac, Desktop Windows, Desktop Linux, Desktop Chromebook, Mobile Android, Mobile iOS.
Pricing Model	Custom Pricing.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	31% female / 69% male
Supported languages	English, Estonian (17,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Offensive Security and Exposure Management platform

By YesWeHack

YesWeHack is a leading Offensive Security and Exposure Management platform. It provides a comprehensive suite of integrated, API-based solutions designed to secure organisations' growing attack surfaces.

The YesWeHack platform comprises:

Bug Bounty: Crowdsourced vulnerability discovery leveraging a global community of 135,000+ skilled ethical hackers through a cost-efficient, platform-driven model.
Autonomous Pentest: Comprehensive asset discovery combined with ongoing exposure validation to secure your attack surface against the most exploited vulnerabilities.
Continuous Pentesting: Human-led security assessments that ensure 0 false positives and help support compliance at scale.

Vulnerability Management: Unified workflows to aggregate and manage findings from external sources.
This multi-layered approach to offensive security empowers organisations to deploy agile, continuous and exhaustive testing strategies across their entire digital footprint.

All YesWeHack solutions are built with a human-in-the-loop philosophy, ensuring that critical decisions remain firmly in human hands.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✓ Knowledge base
- ✗ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✗ Live online
- ✗ Videos
- ✗ Webinars

*45 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	3,87

User Experience

Average rating	9,8*
Ease of scalability	4,9
Ease of Deployment	4,8
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Offensive Security and Exposure Management platform

By YesWeHack

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Annual subscription, priced based on scope.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A
European readiness	
Gender balance	40% female / 60% male
Supported languages	English (13,70% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	CREST Simulated Targeted Attack and Response; ISO/IEC 27001, ISO/IEC 27017:2021.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

AuditGuard

By AuditGuard

AuditGuard is an AI-powered penetration testing platform that deliver standardised, deterministic, and scalable security assessments and pentests.

Main features:

- Attack Surface Management: Spot and visualise the most relevant threats in just few click
- Vulnerabilities Monitoring: Get live updates on vulnerabilities, risk levels, and changes in your attack surface.
- Risk Insight: Assess threats by severity, exposure, and business impact - instantly.
- Reports & Certificates: Get instantaneous Audit Reports, Pentesting, Certificates and Executive Summaries.
- AI-Augmented Remediations
- Get step-by-step tailored procedure to mitigate risks: Audit Management
- One single platform to manage Audits and Pentesting activities.
- Compliance: Check your system compliance against standards and regulations (NIST, CIS, ISO...)

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✗ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✓ Videos
- ✗ Webinars

*3 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE ✗

ECSO OFFICIAL MEMBER ✗

Final score	3,60

User Experience

Average rating	9,3*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	N/A
Incl. supporting docs	Yes

Awards

2025 La Bourse French Tech by Bpifrance.

AuditGuard

By AuditGuard

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Pay as you go, Subscription (monthly/yearly), custom pricing.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	22% female / 78% male
Supported languages	English, French (17,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

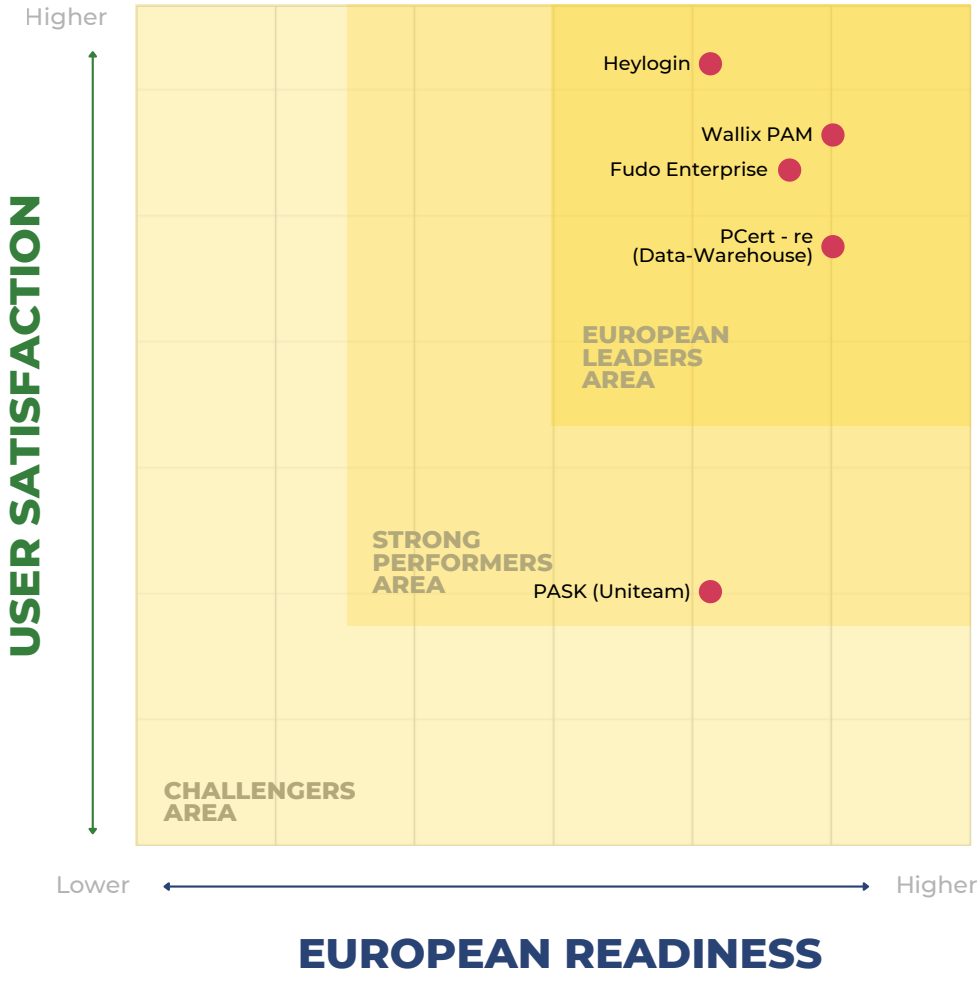
CYBERHIVE MATRIX 2026

IDENTITY AND ACCESS MANAGEMENT

5.

CYBERHIVE MATRIX 2026

Identity and Access Management Matrix



Identity and Access Management scoring table

Cybersecurity solution	User experience	European readiness	Final score
Wallix PAM	4,67	4,50	**4,59**
Fudo Enterprise	4,60	4,35	**4,48**
PCert - re by Data-Warehouse GmbH	4,45	4,50	**4,48**
heylogin	4,84	4,05	**4,45**
PASK by Uniteam SP. z o. o.	3,60	4,05	**3,83**

WALLIX PAM

By WALLIX Group

WALLIX is a European cybersecurity software vendor that offers companies robust identity and access security solutions, guaranteeing smooth and secure digital interactions. WALLIX's innovative technologies in privileged access management, employee access, and governance access protect critical assets, streamline compliance, and improve operational efficiency. Committed to providing simple and secure identity and access solutions, WALLIX's mission is to enable secure operations in digital (IT) and industrial (OT) environments.

WALLIX PAM is a Privileged Access Management solution that delivers robust security and oversight over privileged access to critical IT infrastructure. As an agentless solution, WALLIX PAM can be seamlessly deployed across on-premises, private, and public cloud infrastructures.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*208 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE ×

ECSO OFFICIAL MEMBER ×

Final score	4,59

User Experience

Average rating	9*
Ease of scalability	4,3
Ease of Deployment	4,5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

WALLIX PAM

By WALLIX Group

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Linux.
Pricing Model	Subscription (monthly/yearly), perpetual license.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	30% female / 70% male
Supported languages	English, French, German, Italian, Spanish (28,52% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO/IEC 27001 Information Security Management Systems. BSI BSZ certification (Germany) for WALLIX PAM, with mutual recognition by ANSSI (France) via the BSI–ANSSI agreement. Qualiopi certification for WALLIX Academy training programmes.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Fudo Enterprise

By Fudo Security

Fudo Security is a Polish technology company headquartered in Warsaw, specializing in Privileged Access Management (PAM) solutions, as well as the monitoring and securing of privileged access in IT and OT/ICS environments. Operating in over 35 markets, the company offers rapid deployments and advanced AI-driven behavioral analytics. Since January 2026, the company has been led by Paweł Dawidek as CEO of Fudo Security.

It is estimated that up to 74 percent of data breaches begin with unauthorized access to privileged accounts. Fudo Security not only enables more comprehensive oversight of these accounts but also frees up time for the client's internal experts. It allows them to focus on other critical digital security tasks within the organisation. Fudo Security offers intelligent PAM solutions backed by the company's deep expertise and broad experience. The prestige of these systems is reflected in a portfolio that includes key strategic entities, such as the military, hospitals, and public administration units. The company stands out from the competition not only through its advanced technology but also by delivering tangible cost savings and rapid implementation.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*46 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,48

User Experience

Average rating	9,4*
Ease of scalability	4,4
Ease of Deployment	4,5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Cyber150 (Fast Growth Vendor).

Best Artificial Intelligence (AI) Threat Detection.

Most Innovative Cybersecurity Company.

Privileged Access Management.

Fudo Enterprise

By Fudo Security

Solution	
Deployment support	On-premise, Cloud, SaaS, Hybrid.
Supported platforms	Hardware appliance, VMware, Hyper-V, KVM, Azure, AWS, GCP.
Pricing Model	Custom-based upon technology and services.
Total Cost of Ownership (TCO) justification	No additional costs needed.
Pricing Transparency	The price depends on number of devices and modules adopted.

European readiness	
Gender balance	22% female / 78% male
Supported languages	English, Polish, Ukrainian, German (24,81% EU coverage).
EU Compliance driven	NIS2, ISO 27001, DORA, GDPR.
Company standards & certifications	In progress: ISO 27001, SOC2.
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

PCert - re: align trust - PQC, CBOM, SBOM, inventory

By Data-Warehouse GmbH

PCert enables the complete automated cryptography discovery, inventory (ACDI) and risk assessment of cryptographic components.

It can be used as a universal toolbox for various application scenarios and allows this with its outstanding discovery capabilities:
The simplest is the management of certificates (monitoring, managing, exchanging), but other tasks such as managing the Software Bill of Materials (SBOM), managing the CBOM (Cryptographic Bill of Materials), analyzing vulnerabilities, optimizing internal communication for digital hygiene, checking cybersecurity aspects such as identifying potentially dangerous certificates or already abused software libraries, checking the security of keystores or simply checking the entire infrastructure for unwanted dependencies. The cryptographic MRT allows to verify, prioritize, manage any transition like Post Quantum Migrations or exchanging PKI technology.

The software is used in the NCCOE Post Quantum Migration Lab and MITRE/CISA as a universal tool for discovery/inventory/risk assessment.

Support services offered

- ✓ Email/Help desk
- ✓ FAQs/Forum
- ✓ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✗ Videos
- ✓ Webinars

*2 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE ✗

ECSO OFFICIAL MEMBER ✗

Final score	4,48

User Experience

Average rating	9,3
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

PCert - re: align trust - PQC, CBOM, SBOM, inventory

By Data-Warehouse GmbH

Solution	
Deployment support	On premise, Cloud, SaaS, web-based.
Supported platforms	Any operating system supporting java runtime environment (no installation required).
Pricing Model	Licensing by number of managed devices (endpoints/IP addresses). Alternative per scan (only discovery and inventory), starting from 20€ for single scan.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	28% female / 72% male
Supported languages	English, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, Swedish (100,00% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO 9001, ISO 27001, AeroExcellence (Aviation supplier certification).
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

heylogin

By heylogin GmbH

heylogin is the first passwordless password manager. Instead of remembering and typing a long master password, you simply confirm your login, using your smartphone, FIDO2 security key, Windows Hello, Touch ID, or even a smartwatch. This makes heylogin 2-factor secure by default and saves up to 3 hours per employee per month.

As a German company, we place a strong emphasis on data privacy. We are not only truly GDPR-compliant and ISO 27001-certified, but we also host our service exclusively on German servers and rely solely on European data processors.

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,45**

User Experience

Average rating	9,2*
Ease of scalability	5,0
Ease of Deployment	4,7
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✓ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✗ Videos
- ✓ Webinars

* 116 Reviews

heylogin

By heylogin GmbH

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	Desktop Mac, Desktop Windows, Desktop Linux Desktop Chromebook, Mobile Android Mobile iOS.
Pricing Model	• Free: €0/user/month. • Business: €3.99/user/month (yearly) or €4.99/user/month (monthly). • Enterprise: on request (yearly billing only).
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	20% female / 80% male
Supported languages	English, German (17,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO/IEC 27001 Information Security Management Systems.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

PASK

By Uniteam SP. z o. o.

PASK is a modern, intuitive system for digital identity management and comprehensive control of access to organisation's IT resources (IdM). PASK gives you a clear picture of who and when has access and what the access is for. It ensures security of data stored in IT systems and other company resources. Our goal was to simplify the identity and permission management process and to create a product that's available to companies of all sizes. Uniteam is the exclusive authorized distributor of PASK.

Benefits:

- Automatic onboarding and offboarding: PASK monitors the authorization expiration dates and ensures they are granted or revoked at appropriate time, either automatically by the system or manually by admins.
- Role-Based Access Control: RBAC creates identity profiles based on their attributes and automates granting and revoking permissions, ensuring access compliance throughout the identity lifecycle.
- Incident protection and security: protection against unauthorized access significantly mitigates the risk of data leakage incidents
- Instant audit: quick preview of current and historical permissions allows you to easily browse the database and, if necessary, revoke access or close accounts.
- Flexibility: PASK allows you to effectively tailor access levels to needs of specific users and teams, enabling a more personalized approach to identity management. It guarantees an access security investment adequate to the scale of the company's operations.
- Compliance with legal requirements: ensuring appropriate security for IT resources and their data fulfils the requirements of applicable legal standards, such as GDPR, ISO 27001, Recommendation D of the Polish Financial Supervision Authority, NIS2 or DORA.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*4 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	3,83

User Experience

Average rating	8,5*
Ease of scalability	4
Ease of Deployment	3,5
Incl. deployment docs	No
Incl. supporting docs	No

Awards

No awards received yet.

PASK

By Uniteam SP. z o. o.

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux, Desktop Mac Desktop Windows, Desktop Linux, Desktop Chromebook, Mobile Android, Mobile iOS.
Pricing Model	Per active identity, in three variants: monthly and annual subscriptions and perpetual licenses. The cost per one active identity is 2,5 € monthly.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	19% female / 81% male
Supported languages	English, Polish (17,14% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

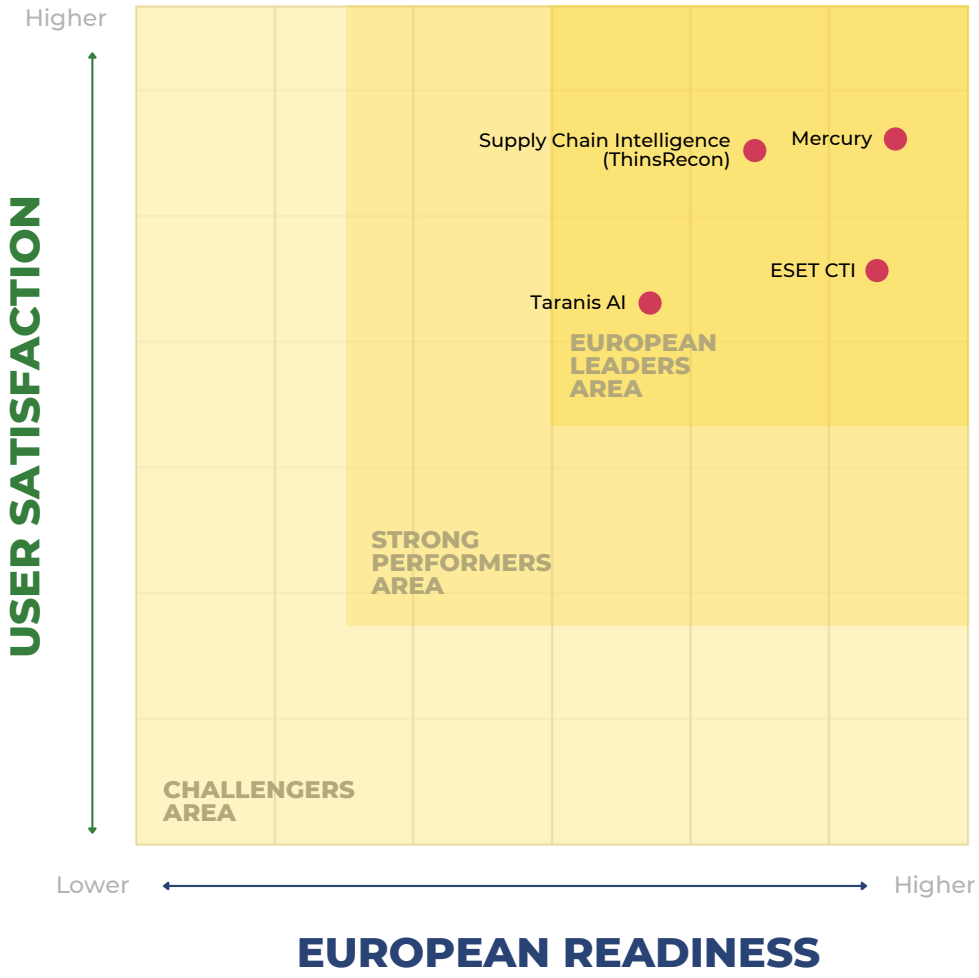
CYBERHIVE MATRIX 2026

CYBER THREAT INTELLIGENCE

6.

CYBERHIVE MATRIX 2026

Cyber Threat Intelligence Matrix



Cyber Threat Intelligence scoring table

Cybersecurity solution	User experience	European readiness	Final score
Mercury by Quointelligence	4,66	4,75	**4,71**
ESET Threat Intelligence Service	4,36	4,70	**4,53**
Supply Chain Intelligence by ThingsRecon	4,64	4,25	**4,45**
Taranis Ai by Austrian Institute of Technology	4,25	3,90	**4,08**

Mercury

By QuoIntelligence

Frankfurt-based threat intelligence vendor founded in February 2020 by Marco Riccardi as a spinoff of QuoScient. Incorporated under German law with additional entities in Spain and Italy; all intelligence data stored under EU jurisdiction, product developed in EU and all support located in EU. Serves European mid-market clients in finance, government, manufacturing, retail and transportation.

Positioning: Markets "Unified Risk Intelligence" — finished, pre-analysed intelligence covering cyber, physical and geopolitical risks, delivered within an hour of onboarding and designed for organisations without an in-house analyst team. Differentiates on EU sovereignty vs. US/Israeli incumbents (Recorded Future, Flashpoint, etc.), ease of use through conversational agent and no specially trained personnel required to interpret data.

Platform: Mercury integrates Threat Intelligence (TTPs, IoCs, vulnerability alerts), Digital Risk Protection, External Attack Surface Management and Supply Chain Monitoring. KARLA, a conversational AI analyst, delivers tailored briefings and scenarios in plain language. Analyst-first model: European analysts curate every output by sector and language.

Funding & traction: €7.3M Series A closed Apr 2026 (led by Elevator Ventures and BMH; eCAPITAL follow-on; Mercurius PE new); €5M Seed in 2023. Reports zero client churn in 2025 and ~6x LTV growth since 2023. Aligned to NIS2/DORA; ISO 27001 certified and listed as an ENISA provider.

Support services offered

N/A

Training services offered

N/A

*11 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,71**

User Experience

Average rating	10*
Ease of scalability	4,7
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Gartner Peer Insights reviewed.

Mercury

By QuoIntelligence

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	Mercury platform, multi-tenant SaaS.
Pricing Model	QuoIntelligence offers a flexible, tiered pricing model to meet the needs of organisations at different stages of maturity. Each tier determines the features and services included, with customizable plan sizes (S, M, L) to fit organisational needs.
Total Cost of Ownership (TCO) justification	Subscription model replaces in-house team (vendor cites 6-figure analyst-team cost avoidance).
Pricing Transparency	Tiered (S/M/L) with extra functionality available as bundles.

European readiness	
Gender balance	37% female / 63% male
Supported languages	English, French, German, Greek, Italian, Polish, Spanish (35,93% EU coverage).
EU Compliance driven	German-incorporated; data stored in EU; developed in EU and Analysts located in EU aligned to NIS2 & DORA; ENISA-listed; ISO 27001.
Company standards & certifications	Bescheinigungsstelle, Forschungszulage, Cybersecurity Made in Europe (eurobits eV).
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

ESET Threat Intelligence Service

By ESET

ESET's Threat Intelligence service provides global knowledge, gathered by ESET experts, on targeted attacks, advanced persistent threats (APTs, eCrime), zero-days and botnet activities. Informed by ESET intelligence feeds and in-house research, organizations gain clearer visibility into threat activity relevant to their environment and can improve their proactive security posture, as well as enhance threat hunting and remediation capabilities. These feeds cover a wide range of threat types, including ransomware, phishing, mobile threats, and potentially unwanted applications, and are structured for straightforward enrichment of SIEM, SOAR, XDR, and CTI platforms. ESET's feeds are highly curated and provided several times a day; they are deduplicated, disambiguated, containing only fresh and prevalent IoCs - and delivered with confidence scoring. ESET's APT Reports package includes in-depth technical reports describing recent campaigns, toolsets and related subjects, providing a very high level of context, and monthly summary overviews ideal for C-level audience. Complementing this, eCrime Reports offer structured insights into financially motivated threats, including ransomware and infostealer operations, their tooling, infrastructure, and affiliate ecosystem. In addition, every customer ordering the APT Reports PREMIUM package will have access to an ESET analyst. This provides an opportunity to discuss topics in greater detail and help costumers gain deeper contextual understanding of threats and threat actors.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*4 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,53

User Experience

Average rating	8,6*
Ease of scalability	4,3
Ease of Deployment	4,8
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

ESET Threat Intelligence Service

By ESET

Solution	
Deployment support	Cloud, Hybrid, On-premises.
Supported platforms	Desktop Mac, Desktop Windows, Desktop Linux, Mobile Android, Mobile iOS.
Pricing Model	Subscription (monthly/yearly), Perpetual license, Custom pricing.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	29% female / 71% male
Supported languages	English, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, Swedish (98,99% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ESET adheres to globally recognized standards and certifications, including ISO 9001, ISO 27001, ISO 15408 (Common Criteria), FIPS 140-2 Level 1, SOC 2 Type 1 & 2, NIST Cybersecurity Framework, PCI DSS 3.2.1 and 4.0.0, and supports regulatory requirements such as HIPAA, GDPR, and NIS2. For more information, click here.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Supply Chain Intelligence

By ThingsRecon

ThingsRecon's Supply Chain Intelligence Platform provides continuous visibility into the digital connections between your organisation and its third-party ecosystem, by reconstructing your external footprint from the outside in. It continuously discovers and maps supplier infrastructure, shared services, and hidden dependencies, including domains, APIs, certificates, web applications, and inherited third-party assets, revealing exposure that traditional vendor risk and point-in-time assessments miss.

Each discovery is enriched with technical, business, and risk signals, including 100+ security hygiene indicators, financial and geopolitical context, and compliance-relevant data. Through a proprietary, patent-pending measure of Digital Proximity, ThingsRecon adds a new dimension to cyber risk: not just how severe a vulnerability is, but how close it is to your core systems, and how far it can propagate. This helps security teams prioritize risk based on real impact and ripple effects, and detect exposure shifts early; thus enabling faster response, stronger resilience, and defensible oversight across the extended supply chain.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*4 Reviews

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,45

User Experience

Average rating	9,6*
Ease of scalability	4,7
Ease of Deployment	4,7
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Supply Chain Intelligence

By ThingsRecon

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Subscription (monthly/yearly)
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness

Gender balance	22% female / 78% male
Supported languages	English, Portuguese (17,41% EU coverage).
EU Compliance driven	Designed to support NIS2 and DORA third-party risk obligations. Data hosted in the EU. HQ in the EU.
Company standards & certifications	SOC 2 Type II, Cybersecurity Made in Europe label.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Taranis AI - OSINT Analysis

By Austrian Institute of Technology (AIT)

Taranis AI is an advanced Open-Source Intelligence (OSINT) tool, leveraging Artificial Intelligence to revolutionize information gathering and situational analysis. Taranis AI navigates through diverse data sources like websites to collect unstructured news articles, utilizing Natural Language Processing and Artificial Intelligence to enhance content quality. Analysts then refine these AI-augmented articles into structured reports that serve as the foundation for deliverables such as PDF files, which are ultimately published. Taranis AI is available under the EUPL free of charge here.

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,08

User Experience

Average rating	9*
Ease of scalability	4
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Support services offered

- ✗ Email/Help desk
- ✓ FAQs/Forum
- ✗ Knowledge base
- ✗ Phone support

Training services offered

- ✓ Documentation
- ✗ In person
- ✗ Live online
- ✓ Videos
- ✗ Webinars

*1 Reviews

Taranis AI - OSINT Analysis

By Austrian Institute of Technology (AIT)

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Linux.
Pricing Model	EUPL (free to use); optional commercial support available.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	12% female / 88% male
Supported languages	English (13,70% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

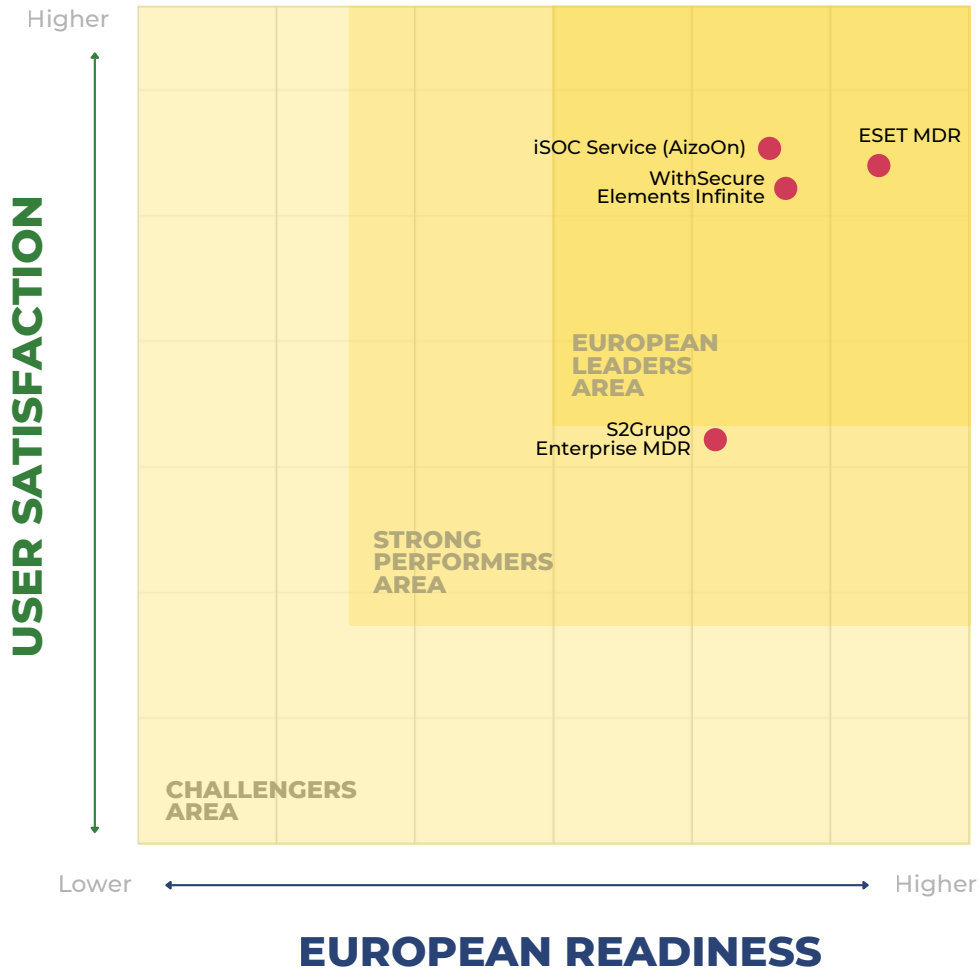
CYBERHIVE MATRIX 2026

DETECTION AND RESPONSE (SERVICES)

7.

CYBERHIVE MATRIX 2026

Detection and Response (Services) Matrix



Detection and Response (Services) scoring table

Cybersecurity solution	User experience	European readiness	Final score
ESET Protect MDR	4,58	4,70	**4,64**
iSOC Service by AizoOn Technology	4,61	4,30	**4,46**
WithSecure Elements Infinite	4,55	4,35	**4,45**
Enterprise Managed Detection & Response by S2Grupo	3,95	4,05	**4,00**

ESET PROTECT MDR

By ESET

ESET Managed Detection and Response Services provide 24/7 monitoring, proactive threat hunting, and rapid incident response powered by ESET's global threat intelligence and cybersecurity experts. Delivered natively on the ESET PROTECT platform, the service provides unified visibility across endpoints, servers, and additional security layers through a single management console. Designed to close the cybersecurity skills gap, MDR ensures fast detection and containment of advanced threats, including ransomware and APTs, supported by proprietary detection technologies, multilayered telemetry, and AI-driven protection, combined with expert human analysis. This approach helps customers achieve greater cyber resilience.

Two service tiers are available: ESET MDR, a comprehensive and affordable service for SMBs that offers a 6-minute incident response time to help combat zero-day attacks and meet evolving cybersecurity insurance and compliance expectations; and ESET MDR Ultimate, a premium service for enterprises and organisations with the highest demands, where ESET experts deploy, optimize, and manage daily operations, including executing response actions on behalf of the customer, so they can focus on their core business. More about ESET MDR Service available here.

Support services offered

N/A

Training services offered

N/A

*61 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,64

User Experience

Average rating	9,2*
Ease of scalability	4,5
Ease of Deployment	4,5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Strong Performer in The Forrester Wave™: Managed Detection And Response Services In Europe, Q3 2025 report

Market Leader in KuppingerCole's 2026 Leadership Compass for MDR report

Aspiring Vendor in the 2026 GPI Voice of the Customer for MDR

ESET PROTECT MDR

By ESET

Solution	
Deployment support	Cloud, Hybrid, On-premises, air-gapped
Supported platforms	Windows, macOS, Linux, Android, iOS
Pricing Model	Subscription (monthly/yearly), Perpetual license.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	29% female / 71% male
Supported languages	English, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, Swedish, Ukrainian (98,99% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	SET adheres to globally recognized standards and certifications, including ISO 9001, ISO 27001, ISO 15408 (Common Criteria), FIPS 140-2 Level 1, SOC 2 Type 1 & 2, NIST Cybersecurity Framework, PCI DSS 3.2.1 and 4.0.0, and supports regulatory requirements such as HIPAA, GDPR, and NIS2. For more information, please click here.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

iSOC Service

By aizoOn Technology

In today's rapidly evolving cyber landscape, threats are becoming more sophisticated, targeted, and relentless. A traditional Security Operations Center (SOC) is no longer enough to protect your business. You need a next generation, intelligence-driven SOC that anticipates threats before they strike. The aizoOn iSOC Service (intelligence-driven SOC) brings world-class cybersecurity directly to your organisation, combining cutting-edge technology, expert security analysts, and an intelligence-driven approach to protect your business around the clock. With seamless integration into your existing infrastructure, our iSOC Service adapts to your unique environment, providing 24/7 monitoring, rapid incident response, and proactive threat hunting tailored to meet the demands of today's complex threat landscape. iSOC Service adapts to evolving cybersecurity threats and organisational growth ensuring scalability to handle increasing data volumes, integrate new security tools, and support expanding infrastructure without performance degradation. Our service leverages cloud-based solutions, automation, and modular architectures, enabling rapid setup and seamless integration with existing IT environments minimizing deployment complexity and operational overhead.

aizoOn offers a Threat Intelligence-Powered SOC, designed to provide:

- Real-Time Threat Detection & Response
- Threat Hunting
- Advanced Threat Intelligence
- Incident Response & Digital Security Orchestration Automation (SOAR)

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✗ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✗ Videos
- ✗ Webinars

*11 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,46

User Experience

Average rating	9,4*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

iSOC Service

By aizoOn Technology

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Size and complexity of the company and type of service.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	31% female / 69% male
Supported languages	English, Italian, Spanish (21,11% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	N/A
Privacy Policy compliant with EU GDPR	Yes

WithSecure Elements Infinite

By WithSecure

WithSecure Elements Infinite is a cybersecurity service designed to provide 24/7 proactive and reactive protection against various digital threats. The service offers features that include endpoint protection, exposure management, identity security, cloud security, and detection and response capabilities. The service proactively monitors, hunts threats, detects, and responds to security incidents across hybrid and cloud environments. With centralized management tools, the service facilitates the implementation of proactive security measures, security policies and outsources continuous improvement of your security posture, and security monitoring, investigation and incident response tasks. Its capabilities help businesses reduce cyber risks and address challenges related to cyberattacks, data breaches, and compliance requirements.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*61 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,45**

User Experience

Average rating	9*
Ease of scalability	4,5
Ease of Deployment	4,5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

The highest possible scores in the criteria of Innovation, Data sovereignty and European Service Delivery.

Service localization in The Forrester Wave™ MDR Services in Europe, Q3 2025.

WithSecure Elements Infinite

By WithSecure

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	Desktop Mac, Desktop Windows, Server Windows, Server Linux, Microsoft Entra ID, Microsoft Azure, Amazon Web Services.
Pricing Model	Subscription (monthly/yearly).
Total Cost of Ownership (TCO) justification	Reduced costs from staffing a 24/7 Security Operations Center (SOC). Proactive exposure management significantly reduces the need for penetration testing and red teaming exercises.
Pricing Transparency	Cloud service with all-inclusive subscriptions.

European readiness	
Gender balance	25% female / 75% male
Supported languages	English, Finnish, French, German, (24,81% EU coverage).
EU Compliance driven	Yes . WithSecure is strongly EU compliance-driven, incl. GDPR, NIS2.
Company standards & certifications	ISO/IEC 27001 Information Security Management Systems – ISAE 3402 Type II, NCSC UK Cyber Incident Response (CIR) Level 2, NCSC Germany Cyber Incident Response (CIR), CREST Cyber Security Incident Response (CSIR), CREST TIBER EU (Europe).
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Enterprise Managed Detection & Response

By S2Grupo

S2 Grupo Enterprise Managed Detection & Response (MDR) service offers a comprehensive, 24/7 managed security solution that combines advanced technology with the expertise of our analysts to protect your organisation from emerging threats. We integrate both proactive detection and immediate incident response, ensuring that your business is always protected and operational, without the need to manage an internal SOC as we have our own SOC and it is at the heart of S2Group operations.

- 24/7/365 expert monitoring: Our highly skilled specialists monitor global and local threats in real-time, ensuring your organisation is always protected.
- Immediate action and efficient response: We act in real-time to mitigate incidents, minimizing risk and damage, quickly restoring critical services. We perform forensic analysis and in-depth expertise to prevent future problems.
- Optimized methodology and regulatory compliance: We develop and optimize our own methodology that guarantees continuous improvement, ensuring compliance with security standards and regulations applicable to your sector.
- Solutions tailored to your business: We offer flexibility to customize our solutions according to the specific needs and characteristics of your organisation and sector, ensuring adequate protection in your context.
- Cost and resource optimization: We provide a managed security service that eliminates the need to maintain an internal SOC, optimizing costs without compromising the effectiveness of threat detection and neutralization.

With our Enterprise MDR solution, you can focus on what really matters: your business, while we ensure the continuous protection of your infrastructure and data.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✓ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✓ Videos
- ✓ Webinars

*1 Reviews

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,00

User Experience

Average rating	8*
Ease of scalability	4
Ease of Deployment	4
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Enterprise Managed Detection & Response

By S2Grupo

Solution	
Deployment support	N/A
Supported platforms	N/A
Pricing Model	N/A
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	22% female / 78% male
Supported languages	English, Spanish (14,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

HONORARY MENTIONS

8.

GitProtect

By Xopero Software

Category: **Recovery**

GitProtect by Xopero Software is a world-class, security-first Backup & Disaster Recovery platform designed specifically for modern DevOps environments. The solution delivers fully automated, centrally managed protection for critical data across the entire DevOps stack — including Jira, Bitbucket, GitHub, GitLab, Azure DevOps, and more.

Built for Jira Administrators, DevOps, and Security Teams, GitProtect ensures continuous data availability and uninterrupted workflows in any event of failure. Whether recovering a single issue, repository, or configuration, or restoring an entire environment after a major incident, GitProtect combines granular recovery with enterprise-grade Disaster Recovery technologies, protecting organisations from every data loss scenario, from human error and malicious activity to system failures and large-scale outages.

Unbreakable encryption and security are at the core of GitProtect: data residency of choice (US/UK/AU/Custom), SSO, IdPs, role-based access, and AES encryption with your own key, among other advanced protections. Trusted by security-conscious teams, GitProtect is SOC 2 Type II and ISO 27001 compliant, understanding firsthand that security standards require a reliable backup.

With unlimited retention for compliance, GitProtect goes beyond standard 365-day retention, helping organisations meet Shared Responsibility, legal, and regulatory requirements effortlessly. Advanced reporting, audit-ready governance, and best-in-class security controls give teams full visibility and confidence in their data protection strategy.

Support services offered

- ✓ Email/Help desk
- ✓ FAQs/Forum
- ✓ Knowledge base
- ✗ Phone support

Training services offered

- ✓ Documentation
- ✗ In person
- ✓ Live online
- ✓ Videos
- ✓ Webinars

*36 Reviews

CYBERSECURITY PRODUCT

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,40

User Experience

Average rating	9,4*
Ease of scalability	4,6
Ease of Deployment	4,6
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

GitProtect

By Xopero Software

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux.
Pricing Model	Subscription (monthly/yearly).
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	20% female / 80% male
Supported languages	English, German, Polish (21,11% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO/IEC 27001 Information Security Management Systems, NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework), PCI Data Security Standard (PCI SSC), Soc2 Type II, EN 50600, EN 1047-2 standard, SOC 3, FISMA compliance, DOD standard, DCID, HIPAA, ISO 50001, LEED Gold Certified, SSAE 16.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

HyperBUNKER

By HyperBUNKER LTD

Category: **Recovery**

HyperBUNKER is a physical, fully offline recovery vault designed for the moment when cyber incidents break all assumptions.

When identity is compromised, networks are untrusted, cloud consoles are inaccessible, and backups cannot be safely used, recovery still has to start somewhere. HyperBUNKER provides that fixed, trusted recovery anchor. It is not backup, not storage, and not part of existing security stack.

HyperBUNKER operates completely outside production systems, identity, networks, and orchestration layers. The vault preserves a predefined set of operational data required to restart and legally operate after a severe cyber incident — even under total compromise scenarios.

Built on real-world recovery experience from tens of thousands of ransomware and incident response cases, HyperBUNKER exists specifically for the last mile of cyber resilience: restarting operations when everything else has failed.

Delivered as a managed recovery service with strict offline guarantees, integrity checks, and auditable restore procedures, HyperBUNKER serves organisations where downtime, loss of control, or failed recovery is not an option.

When recovery assumptions fail, HyperBUNKER is what remains.

Support services offered

- ✓ Email/Help desk
- ✓ FAQs/Forum
- ✗ Knowledge base
- ✗ Phone support

Training services offered

- ✓ Documentation
- ✗ In person
- ✓ Live online
- ✗ Videos
- ✓ Webinars

*3 Reviews

CYBERSECURITY PRODUCT

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	4,21

User Experience

Average rating	9,3*
Ease of scalability	4,7
Ease of Deployment	4,7
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

HyperBUNKER

By Hyperbunker LTD

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	The solution runs on dedicated, isolated hardware.
Pricing Model	Subscription-based (Recovery-as-a-Service), defined by SLA, capacity, and validation frequency.
Total Cost of Ownership (TCO) justification	HyperBUNKER replaces the need for complex recovery orchestration in worst-case scenarios. It reduces downtime risk, eliminates dependency on compromised systems (identity, backup, infrastructure), and provides a guaranteed recovery baseline. TCO is driven by avoided operational loss rather than cost per user.
Pricing Transparency	N/A

European readiness

Gender balance	13% female / 87% male
Supported languages	English, German (17,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	ISO 27001 and ISO 9001.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Logmanager

By Logmanager

Category: **Monitoring & Performance**

Logmanager is a log management platform enhanced with SIEM capabilities that radically simplifies responses to cyberthreats, legal compliance, and troubleshooting. By transforming diverse logs, events, metrics, and traces into actionable insights, it helps security and operations teams respond swiftly to any incident. Experience effortless self-management and customization, uncompromised functionality, and the flexibility to take control of your entire technology stack.

CYBERSECURITY PRODUCT

Cyberhive Page

Distinctions

- Basic Cyberhive Member
- CYBERSECURITY MADE IN EUROPE ✗
- ECSO OFFICIAL MEMBER ✗

Final score	3,65

User Experience

Average rating	9,4*
Ease of scalability	4,7
Ease of Deployment	4,7
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Winner of the ECSO Cyber Investor Days 2025 in Prague.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✓ Knowledge base
- ✓ Phone support

Training services offered

- ✓ Documentation
- ✓ In person
- ✓ Live online
- ✗ Videos
- ✓ Webinars

*36 Reviews

Logmanager

By Logmanager

Solution

Deployment support	On-premise, cloud, web-based.
Supported platforms	140+ integration available.
Pricing Model	Public pricing. Pricing based on the volume of data stored per month.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	Subscription (monthly/yearly), perpetual license, custom pricing.

European readiness

Gender balance	17% female / 83% male
Supported languages	English, Czech (17,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	GDPR, ISO 27001, NIS2.
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

PrepJam

By Secure Practice

Category: **Training**

Secure Practice is the European leader in cybersecurity awareness and preparedness.

Kickstart your team's cybersecurity training with PrepJam interactive exercises that build your team's real-world response skills, together.

- Save time with PrepJam's catalogue of pre-built scenarios. Adapt as needed, or build from scratch. No design skills required.
- Gain first-hand experience with live exercises that bridge gaps in roles and responsibilities. Build alignment and respond as a team.
- Turn your team into cybersecurity action heroes, ready to tackle any challenge with speed, strategy and real-world skills.

PrepJam makes it easy to facilitate exercises whether your team is small and focused, medium-sized like entire departments, or even at all-hands sessions with up to 500 simultaneous participants.

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*3 Reviews

CYBERSECURITY PRODUCT

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	**4,66**

User Experience

Average rating	9,7*
Ease of scalability	4,3
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

PrepJam

By Secure Practice

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Transparency	N/A
Total Cost of Ownership (TCO) justification	N/A
Pricing Model	Subscription (monthly/yearly).

European readiness	
Gender balance	48% female / 52% male
Supported languages	Danish, Dutch, English, German, Latvian, Lithuanian, Norwegian, Polish, Spanish, Swedish (47,04% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Zepo Intelligence

By Zepo

Category: **Training**

Zepo Intelligence is an AI-powered Human Risk Management platform that protects organisations from AI-driven social engineering across the modern workspace. Its Gateway Security layer detects and blocks social engineering threats in real-time across email, messaging, and collaboration channels, while its adaptive training engine turns those real attacks into hyper-personalized micro-learning interventions triggered by actual user behavior. Combined with multi-vector simulations (phishing, smishing, vishing, deepfakes) and a real-time Human Risk Index, Zepo connects detection, simulation, training, and analytics in a single loop that measurably reduces human cyber risk over time.

Support services offered

N/A

Training services offered

N/A

*6 Reviews

CYBERSECURITY PRODUCT

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	3,79

User Experience

Average rating	10*
Ease of scalability	4,8
Ease of Deployment	4,7
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Zepo Intelligence

By Zepo

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	Pricing varies with the size of the customer. Average: €35.
Total Cost of Ownership (TCO) justification	N/A
Pricing Transparency	N/A

European readiness	
Gender balance	24% female / 76% male
Supported languages	English, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, Swedish (98,99% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Blue Networks

Category: **Governance Risk & Compliance**

Blue Networks is a dynamic and innovative organisation, fueled by a passion for security and dedicated to making data protection simple and accessible for small and medium businesses and public sector institutions.

Blue Networks offer the following services:

- Cyber Resilience Act (CRA) Security & Compliance for Connected Products (Sovereign-by-Design)
- Vendor Risk Management & Customer Due Diligence Support for Fintechs (Sovereign-by-Design)
- Cyber Risk Assessment & Prioritisation (Sovereign-by-Design)
- NIS2 & DORA Readiness for Digital SMEs and Fintechs (Sovereign-by-Design)
- vCISO & Cyber Governance for Digital SMEs (Sovereign-by-Design)

Support services offered

- Email/Help desk
- FAQs/Forum
- Knowledge base
- Phone support

Training services offered

- Documentation
- In person
- Live online
- Videos
- Webinars

*3 Reviews

CYBERSECURITY SERVICE

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

Final score	3,93

User Experience

Average rating	10*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Blue Networks

Solution	
Deployment support	N/A
Supported platforms	N/A
Pricing Model	Subscription (monthly/yearly).
Total Cost of Ownership (TCO) justification	The Total Cost of Ownership varies depending on the scope, infrastructure, and compliance requirements. We propose solutions with the lowest TCO on the market, because our entire offering is based on enterprise-grade Open-Source Software. Our approach is optimize costs by reducing risks, minimizing incident impact, and streamlining compliance processes.
Pricing Transparency	N/A

European readiness	
Gender balance	50% female / 50% male
Supported languages	English, Italian (17,41% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	Yes
Privacy Policy compliant with EU GDPR	Yes

Amleth

By Digital Trust AS

Category: Governance Risk & Compliance

Amleth brings cybersecurity help right to your Slack and Teams channels, based on your business priorities and technology context. We answer your security questions and provide actionable advice, whether it's a routine concern, a product or vendor review, or a live incident.

Amleth gives you direct access to a team of security professionals with broad, hands-on expertise — available on demand through your existing communication platforms. We provide practical guidance, technical insight, and AI-augmented responses to help you tackle cybersecurity challenges and stay compliant without adding headcount.

Key Benefits:

- Quality and Trust: Direct access to vendor-neutral cybersecurity experts with proven experience.
- Cost-Effective: Get only the expertise you need, exactly when you need it - at a fraction of the cost of hiring.
- Simple: No new tools or portals. We integrate directly into the communication platforms you already use.
- Scalable: As your business grows, our support scales with you - from quick advice to full security programs.

Support services offered

- ✓ Email/Help desk
- ✗ FAQs/Forum
- ✓ Knowledge base
- ✗ Phone support

Training services offered

- ✗ Documentation
- ✓ In person
- ✓ Live online
- ✗ Videos
- ✗ Webinars

*1 Reviews

CYBERSECURITY PRODUCT

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE ✗

ECSO OFFICIAL MEMBER ✗

Final score	3,55

User Experience

Average rating	10*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	N/A
Incl. supporting docs	N/A

Awards

No awards received yet.

Amleth

By Digital Trust AS

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	N/A
Pricing Model	From 1400 EUR / month.
Total Cost of Ownership (TCO) justification	Hiring a dedicated security professional costs €80.000 - €130.000 per year once salary, taxes, benefits, tools, and recruitment are factored in. For €1.400 per month, our service provides unlimited security support for startups and SMBs at a fraction of that cost, with immediate availability and no long-term employment commitment.
Pricing Transparency	N/A

European readiness	
Gender balance	50% female / 50% male
Supported languages	English, Norwegian, Spanish (21,11% EU coverage).
EU Compliance driven	N/A
Company standards & certifications	N/A
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

Cymph

By Cymph

Category: **Orchestration**

Cymph is a cybersecurity software company building an Incident Response Readiness platform that helps organisations understand what cyber threats they are prepared to respond to, where gaps exist, and how to close them. The platform unifies procedures and playbooks across tools into a single operational view, mapped to industry frameworks such as MITRE ATT&CK and ISO 27001. By turning fragmented documentation into structured, actionable workflows, Cymph enables continuous visibility and improvement of response capabilities. It is designed for security teams, MSSPs, and regulated organisations that need to move from compliance to operational readiness.

CYBERSECURITY PRODUCT

Cyberhive Page

Distinctions

- Basic Cyberhive Member
- CYBERSECURITY MADE IN EUROPE ✗
- ECSO OFFICIAL MEMBER ✗

Final score	3,57

User Experience

Average rating	9*
Ease of scalability	5
Ease of Deployment	5
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

Support services offered

- ✓ Email/Help desk
- ✓ FAQs/Forum
- ✗ Knowledge base
- ✗ Phone support

Training services offered

- ✓ Documentation
- ✗ In person
- ✓ Live online
- ✗ Videos
- ✗ Webinars

*1 Reviews

Cymph

By Cymph

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Linux.
Pricing Model	Pricing is currently provided through tailored plans based on mondus operanti e.g. MSSP, Enterprise, organisation size, deployment model, and required capabilities. The platform supports flexible licensing models (from a freemium license up to enterprise), ensuring alignment with both SMEs and large organisations.
Total Cost of Ownership (TCO) justification	The Total Cost of Ownership (TCO) for Cymph includes: Platform licensing , Optional infrastructure costs (for on-prem), Optional integration or onboarding support (if required). Cymph does not impose hidden costs. In particular, AI-related functionality follows a Bring Your Own LLM (BYO-LLM) approach, allowing organisations to use their preferred provider and control associated usage costs directly.
Pricing Transparency	N/A

European readiness

Gender balance	25% female / 75% male
Supported languages	All EU languages via automated AI translator.
EU Compliance driven	N/A
Company standards & certifications	As a company bone but one founding member has ISO 27001:2022 Lead Auditor certifications.
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

ACKNOWLEDGEMENTS

9.

ACKNOWLEDGMENTS

We would like to thank all the European cybersecurity providers whose solutions are featured in the Cyberhive Matrix 2026.

Through their solutions and expertise, they actively support the development of a more secure, resilient, and competitive digital ecosystem across Europe.

- AizoOn
- Anantis
- AuditGuard
- Austrian Institute of Technology
- Bitdefender
- Blue Networks
- Cybernetica
- Cyborux
- Cymph
- Data-Warehouse GmbH
- Digital Trust AS
- DongIT
- ESET
- Fudo Security
- HarfangLab
- Heylogin
- Holm Security
- HyperBUNKER
- IstroSec
- Labyrinth
- Logmanager
- Nanitor
- Nucleon Security
- QuoIntelligence
- Remediata
- S2 Grupo
- Sekoia
- Secure Practice
- SelfHack
- ThingsRecon
- Transparent Edge
- Unguess
- Uniteam
- Wallix
- WithSecure
- Xopero
- YesWeHack
- Zepo

ECSO 10 YEARS
EUROPEAN CYBER SECURITY ORGANISATION

cyberhive®
discover solutions from EUROPE™

EMPOWERING EUROPEAN CYBERSECURITY COMMUNITIES

CONTACTS

ECSO Working Group on Market Development
marketdev_team@ecs-org.eu

Daniele Dionisi
Product Owner of The Cyberhive EUROPE
daniele.dionisi@ecs-org.eu

Matteo Nicolussi
Junior Manager for Communications & Marketing
matteo.nicolussi@ecs-org.eu

ECS 10 YEARS
EUROPEAN CYBER SECURITY ORGANISATION

cyberhive®
discover solutions from EUROPE™

Avenue des Arts 46, 1000, Brussels (Belgium)
marketdev_team@ecs-org.eu
www.ecs-org.eu