ECSO
EUROPEAN CYBER SECURITY ORGANISATION

cyberhive®
discover solutions from EUROPE™

cyberhive® MATRIX

PREVIEW EDITION
Q1 2025

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

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 maturity and European readiness of the solutions during the assessment. ECSO, owner and initiator of Cyberhive, is an independent entity analyzing and evaluating solutions.

The methodology is completely transparent and was constructed with the input of industry experts in the Cyberhive Task Force. This industry supported approach puts trustworthiness, replicability, and usability central in the design process.

The Cyberhive Matrix™ is a half-year published report. The report 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 compliances.

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 a non-profit membership-based organisation established in 2016 as the contractual counterpart to the European Commission for implementing Europe’s unique Public-Private Partnership in Cybersecurity (2016-2020). The partnership aimed to foster cooperation between public and private actors, ensuring access to innovative and trustworthy European cybersecurity solutions.

Today, ECSO builds on the partnership’s successes and, with its cross-sectoral membership base, contributes to developing cybersecurity communities and strengthening the European cybersecurity ecosystem. ECSO’s diverse membership, encompassing a broad range of stakeholders from both the public and private sectors, enables comprehensive coverage of cybersecurity topics

CONTENTS

CYBERHIVE MATRIX Q1 2025 **PREVIEW EDITION**

INTRO

1.

METHODOLOGY & CRITERIA

The criteria are a combination of all the input gathered from the **3 user groups** (vendors, 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 user reviews. The quantitative analyses will 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. These will not be used to 'rank' the solutions in the axes.

The criteria are measurable and replicable. The criteria 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 table below. **The score used ranges from 0 to 5 for all existing criteria.**

User experience

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

The **User Satisfaction** criterion is directly linked to the solution itself, showcasing the **overall user experience**, **ease of deployment, and scalability**. It reflects how well the solution integrates into different environments, its adaptability to evolving needs, and the level of user confidence in its performance.

European readiness which is indicated in the horizontal axis indicates how well the solution is adapted to Europe in terms of values (like transparency, and gender balance) and fit to the European market (language availability and operational sovereignty).

European readiness

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 Task Force decided to incorporate the **European Readiness** dimension into our evaluation, recognizing the urgent need to enhance **competitiveness, resilience, and investment** across Europe. By doing so, we aim to foster a more robust cybersecurity ecosystem that not only meets global standards but also strengthens Europe's strategic autonomy. This initiative supports innovation, drives market confidence, and ensures that European organisations remain at the forefront of cybersecurity excellence in an increasingly complex digital landscape.

THE CYBERHIVE TASK FORCE

On the 22nd of March 2024, we established the "Cyberhive Solution Listing Task Force"—a temporary group of industry experts dedicated to designing a trustworthy and replicable mechanism for evaluating European cybersecurity solutions.

Through four workshops, the task force actively contributed to the creation of the Cyberhive platform and the Matrix, reinforcing our commitment to developing a transparent, industry-backed solution evaluation.

A special thanks to the current members of the Task Force and to Tom Bastiaans, Original Product Owner of The Cyberhive EUROPE!

End-Users:

- Marc Vael
- Matthias Muhlert
- Petri Kuivala
- Andrzej Bartosiewicz
- Simone Fortin

Vendors:

- Ignacio Sbampato
- Regis Cazenave
- Patricia Shields
- Zuzana Legathova

Investors:

- Bart Houlleberechts
- Carlos Hoerl
- Alejandro Wright

Are you interested in **joining** the **Cyberhive Task Force**? Reach out to Guillermo Ferrer Hernáez, Manager of The Cyberhive EUROPE. A Task Force meeting is scheduled for the end of February 2025, so now is the perfect time to get involved!

THE CYBERHIVE EUROPE CONTACT

Guillermo Ferrer Hernáez
Manager of The Cyberhive Europe
guillermo.ferrer@ecs-org.eu

CONTACT

HOW TO FEATURE YOUR SOLUTIONS FOR FREE

Featuring your cybersecurity solutions in the Cyberhive Matrix is free and open for everyone. To include them, just follow these steps:

1. Register in The Cyberhive EUROPE (thecyberhive.eu, it's free!)

2. Fill in the submission survey: Members of The Cyberhive EUROPE will receive it in Q3 2025, ahead of the next edition of the Cyberhive Matrix.

3. Say hi, the world is watching! 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.

This Cyberhive Matrix edition focuses on providers with a SOC as Service, NDR, MDR, XDR related solutions, but next one will include more categories.

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™.

WOMEN4CYBER AWARDS

The Cyberhive Europe recognizes the challenges regarding the inclusion of women in management roles. To address this, we are proud to highlight companies that have been granted the Women4Cyber Awards. These awards celebrate organizations that exemplify progress in gender diversity.

The underrepresentation of women in leadership positions remains a complex and pressing issue, with barriers ranging from societal expectations to structural inequities. Companies honored with the Women4Cyber Awards stand out as pioneers in overcoming these challenges, demonstrating a clear commitment to empowering women and cultivating diverse decision-making at the highest levels.

By specifically mentioning these award-winning organizations, The Cyberhive Europe seeks to inspire others in the industry to adopt similar practices and set ambitious goals for gender inclusivity by including it in the Cyberhive Matrix.

The **Women4Cyber Recognition Award** is assigned once a year to a selected cybersecurity company that distinguished itself for its efforts in enhancing gender diversity in the cybersecurity field, while fostering an unbiased hiring process, pay equity, and other DEI measures.

The **Women4Cyber Entrepreneurship Award** is aimed at cybersecurity companies (co)-founded by women and/or with at least 30% of women on the board. The winners of the W4C Awards are assessed by the Women4Cyber Administrative Body.

At the Cyberhive, we provide one professional membership on the Cyberhive to the winners of the Awards.

WOMEN™
4CYBER
EUROPEAN CYBER SECURITY ORGANISATION

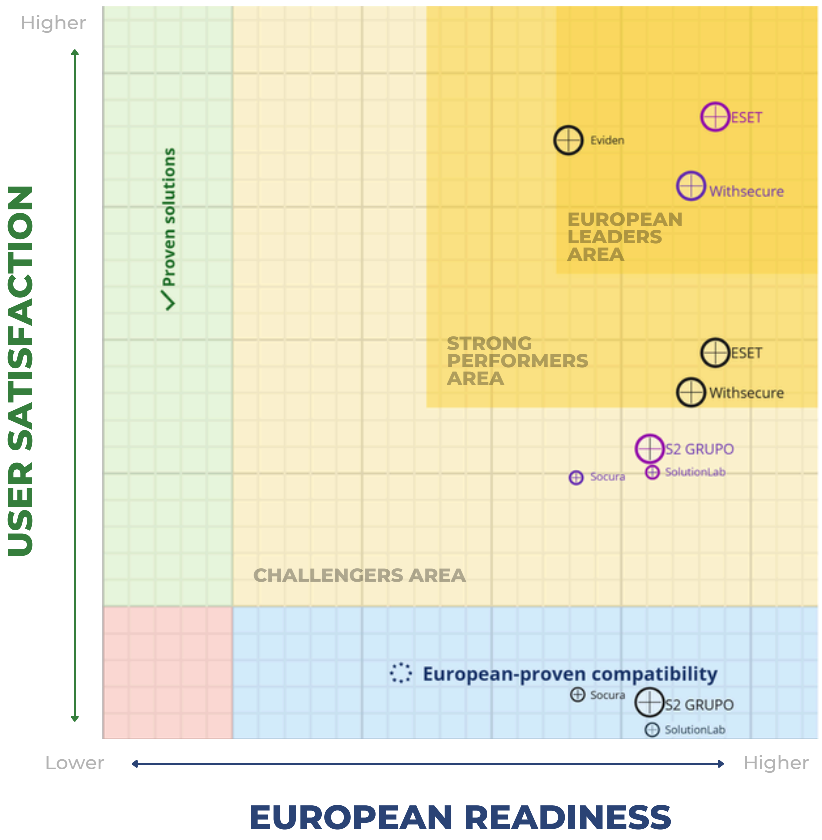
MDR SOLUTIONS

CYBERHIVE MATRIX Q1 2025 **PREVIEW EDITION**

2.

CYBERHIVE MATRIX Q1 2025

MDR Solutions Matrix



Legend

Company sizes

- Micro company (10-)
- Small company (50-)
- Medium company (250-)
- Enterprise (250+)

Colours

- ● Current results
- ● Results if the **Cyberhive Reviews Score*** was 5/5 , as some solutions do not have reviews yet on The Cyberhive Europe.

*in ease of scalability and deployment.

EVALUATED VENDORS

eset	EVIDEN
S2GRUPO Anticipating a cyber secure world	SOCURA
SolutionLab	WITH secure

ESET Protect MDR

By ESET

Solution All-in-one protection with 24/7 MDR service Superior AI-native protection with continuous threat hunting and monitoring. Access world-leading ESET expertise and threat intelligence via managed detection & response, delivered as a 24/7 service.The service combines the skills of ESET's world-class IT security research teams and incident responders, and the cutting-edge technology of ESET's IT security products. Its responsive, tailored support reduces the risk of any interruption in operational continuity. o Guaranteed response times o XDR deployment and optimization o Suspicious behavior investigation o Digital forensics o Proactive threat hunting and threat monitoring.

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY™ MADE IN EUROPE

ECSO OFFICIAL MEMBER

User Experience

Average rating	4.6
Ease of scalability	0(5)[1]
Ease of Deployment	0(5[1]
Peer Recommendation	51,2%
Incl. deployment docs	Yes[2]
Incl. supporting docs	Yes

Awards

Market Leader on MDR Services 2025

Gartner Market Guide Managed Detection Response 2024

*We anticipate that it will also be available in the Amazon environment.

[1] ESET PROTECT MDR solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

[2] Remote management platform is available as cloud-based or on-premises deployment. No need to buy or maintain additional hardware, reducing the total cost of ownership.

Support

☒ Not specified

Training

☒ Not specified

ESET Protect MDR

By ESET

Solution	
Deployment support	Cloud, Hybrid, On-premises.
Supported platforms	Windows, MacOS, Linux, Android, iOS.
Pricing Transparency	The vendor did not specify this information.
Total Cost of Ownership (TCO) justification	The vendor did not specify this information.
Pricing Model	Subscription (monthly/yearly), flexible subscription, perpetual license, custom pricing.

European readiness	
Gender balance	27% female / 63% male
Supported languages	Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, Swedish, Ukrainian (100 % EU coverage) Moreover, ESET Solutions are in total available in 39 languages, some non-EU including Japanese, Turkish, Chinese and Russian.
Company standards & certifications	ISO 9001, ISO 27001, FIPS 140-2 Level 1, LINCE Certification, NIST Cybersecurity Framework
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

EVIDEN

AI-Driven Managed Detection and Response

By Eviden

Eviden's MDR service is a next-gen cybersecurity solution that leverages AI and cybersecurity mesh to protect your digital estate from evolving threats. It integrates and enhances your existing security tools, provides 24/7/365 monitoring and response from its 17 modern security operations centres (MSOC), and delivers actionable insights to improve your security posture and compliance. Request a proof-of-concept trial today and see how Eviden MDR can transform your security.

Support

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

Training

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

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE™

ECSO OFFICIAL MEMBER

User Experience

Average rating	4.6*
Ease of scalability	5
Ease of Deployment	5
Peer Recommendation	100%
Incl. deployment docs	Yes
Incl. supporting docs	No

Awards

PAC RADAR awards for SAP Services 2024- one of the best IT service providers for SAP.

Leader in the 2023 MDR services PEAK matrix report by Everest, Worldwide.

Major Player in the 2024 IDC Marketscape for MDR, Worldwide.

Representative Vendor in the 2024 Gartner MDR Market Guide, Worldwide.

Security Innovation of the Year award from Belgian Computable Awards, 2023 for Eviden AIsaac MDR platform, Europe.

*18 Reviews

AI-Driven Managed Detection and Response

By Eviden

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	All web browsers supporting OSs, on premise Windows.
Pricing Transparency	The vendor did not specify this information.
Total Cost of Ownership (TCO) justification	The vendor did not specify this information.
Pricing Model	Subscription (monthly/yearly), custom pricing.

European readiness

Gender balance	40% female / 60% male
Supported languages	Bulgarian, Croatian, Dutch, English, Estonian, French, German, Spanish (39,6% EU coverage).
Company standards & certifications	ISO/IEC 27001 Information Security Management Systems – Requirements Other: SOC 2 Type 2
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

Enterprise Managed Detection & Response

By S2 Grupo

Our 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 organization 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 our operations.

Key aspects: 24/7/365 expert monitoring: Our highly skilled specialists monitor global and local threats in real time, ensuring your organization 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 organization 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.

[1] S2 Grupo MDR solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

Support

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

Training

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

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY™ MADE IN EUROPE ✗

ECSO OFFICIAL MEMBER

User Experience

Average rating	0*
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	0
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards received yet.

*We anticipate that it will also be available in the Amazon environment.

Enterprise Managed Detection & Response

By S2 Grupo

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Linux, Desktop Mac, Desktop Windows, Desktop Linux, Desktop Chromebook.
Pricing Transparency	Price varies according to customer.
Total Cost of Ownership (TCO) justification	The vendor did not specify this criterion.
Pricing Model	Subscription (monthly/yearly), custom pricing.

European readiness

Gender balance	22% female / 78% male
Supported languages	English and Spanish (17,41% EU Coverage).
Company standards & certifications	ISO 9001, ISO/EIC 27001, ISO/EIC 20000-1, ISO 22301, ISO 22301, UNE 166002, ISO 14001, Certified IQ NT Management System
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

SOCURA

Managed Detection and Response

By Socura

Socura reduces cyber risk by proactively detecting and responding to threats, 24/7. Our Managed Detection and Response (MDR) service operates as an extension of your team - supplying highly skilled SOC experts and the additional capabilities you need to scale your security operations and accelerate response to attacks.

Cyberhive Page

Distinctions

Basic Cyberhive Member

✗ CYBERSECURITY™ MADE IN EUROPE

ECSO OFFICIAL MEMBER

User Experience

Average rating	N/A
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	N/A
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

MSP Alert Top MSSP 2024

Computing Security Awards 2024 – Project of the Year (CymruSOC)

Support

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

Training

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

[1] Socura MDR solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

Managed Detection and Response

By Socura

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux, Desktop Mac, Desktop Windows, Desktop Linux, Desktop Chromebook, Movbile Android, Mobile iOS.
Pricing Transparency	Custom based upon technologies and service.
Total Cost of Ownership (TCO) justification	The vendor has not displayed this information.
Pricing Model	Custom pricing.

European readiness	
Gender balance	18% female /82% male
Supported languages	English (13,70% EU Coverage).
Company and solution standards & certifications	ISO9001, ISO27001, CREST SOC Accredited, Cyber Essentials Plus
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

SolutionLab MDR

By SolutionLab

SolutionLab provides services as a professional consultancy, running from **SOC service 24/7** from 2 state-of-the-art centres in Italy and Lithuania. With our security team, the client can get Managed Technologies Services for Network and End-Point Monitoring. By means of the Network Traffic Analyser, we define infected workstations inside the client network, even with encrypted traffic. AI technologies / Machine Learning, which constantly adapt to a client-specific network, will detect any small deviations from normal.

Support

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

Training

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

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY™ MADE IN EUROPE

ECSO OFFICIAL MEMBER

User Experience

Average rating	N/A
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	N/A
Incl. deployment docs	No
Incl. supporting docs	No

Awards

No awards received yet.

SolutionLab MDR

By SolutionLab

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	All web browser supporting OSs
Pricing Transparency	*“We use an agnostic approach to fit any complex environment, scouting for the best suiting solutions for our customers however specific their requirements are. On top of this approach, we constantly master our excellence in certain vertical technological skills.”*
Total Cost of Ownership (TCO) justification	Range can be between 200K to 250K EUR, but depending on user requirements.
Pricing Model	Custom pricing.

European readiness

Gender balance	15% female / 85% male
Supported languages	English, Greek, Lithuanian, Portuguese, Swedish, Estonian, Italian, Lithuanian (28,52% EU coverage).
Company standards & certifications	Quality Management System (ISO 9001), Service Management System (ISO 20000), Business Continuity Management System (ISO 22301), Information Security Management Systems (ISO 27001), Information Security Incident Management (ISO 27035).
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

WithSecure Countercept

By WithSecure

WithSecure Countercept is a Managed Detection and Response (**MDR**) service built by attackers for defenders, delivered in partnership with clients' IT Security teams, by threat hunters who form a 'battle-fit' Detection and Response Team (DRT). WithSecure's 24/7 Detection and Response Team (DRT) deals with cyber threats to your organization in minutes.

WithSecure Countercept MDR acts as an extension of your cyber security team, sharing out threat hunting expertise, helping your team learn and grow, and continuously improving your security. WithSecure also offers a **Europe-only Countercept MDR** option that is delivered wholly within Europe and eliminating data access to anyone outside.

Support

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

Training

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

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY™ MADE IN EUROPE

ECSO OFFICIAL MEMBER

User Experience

Average rating	4,5
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	51,78%
Incl. deployment docs	Yes
Incl. supporting docs	No

Awards

95% Recommendation on Gartner Peer Insights

Best Protection award in 6 years by AV-TEST

AI Excellent Award for Project Blackfin

*57 Reviews

[1] Withsecure MDR solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

WithSecure Countercept

By WithSecure

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	All web browsers supporting OSs, Desktop Mac, Desktop Windows, Desktop Linux, Server Linux, Server Windows, Identities: Microsoft Entra ID, Cloud platforms: Microsoft Azure, Amazon Web Services.
Pricing Transparency	The price depends on number of devices and modules adopted.
Total Cost of Ownership (TCO) justification	An independent 3rd party review by AV-Comparatives states that WithSecure delivers a low TCO combined with exceptional technical capabilities and reasonable costs.
Pricing Model	Subscription (monthly/yearly), custom pricing.

European readiness

Gender balance	25% female / 75% male
Supported languages	Chinese, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Norwegian, Polish, Portuguese, Romanian, Spanish, Swedish (76,7% EU coverage)
Solution standards & certifications	ISO/IEC 27001 Information Security Management Systems – Requirements, ISAE 3402 Type II, CREST Simulated Targeted Attack and Response (STAR), CREST Intelligence Led Penetration Testing (STAR), CREST Cyber Security Incident Response (CSIR), CREST Penetration Testing (PEN TEST), NCSC UK Cyber Incident Response (CIR) Level 2, NCSC Germany Cyber Incident Response (CIR), CREST TIBER EU (Europe), ISA/IEC 62433 (Security for Industrial Automation and Control Systems)

Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.	Privacy Policy compliant with EU GDPR	Yes

MDR Scoring Tables

Criteria	User Experience						Final
	Overall user satisfcation		Average ease of scalability	Average ease of deployment	Deployment support		
	Average overall rating	Average NPS			Included deployment docs.	Included support. docs.	
ESET	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Eviden	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
S2 Grupo	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Socura	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
SolutionLab	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
WithSecure	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Criteria	European readiness						Final
	Gender balance	Govern. transparency	Language availability	Promotion of EU (-fit) solution	Operational Sovereignty		
					Data in EU?	HQ in EU?	
ESET	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Eviden	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
S2 Grupo	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Socura	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
SolutionLab	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
WithSecure	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

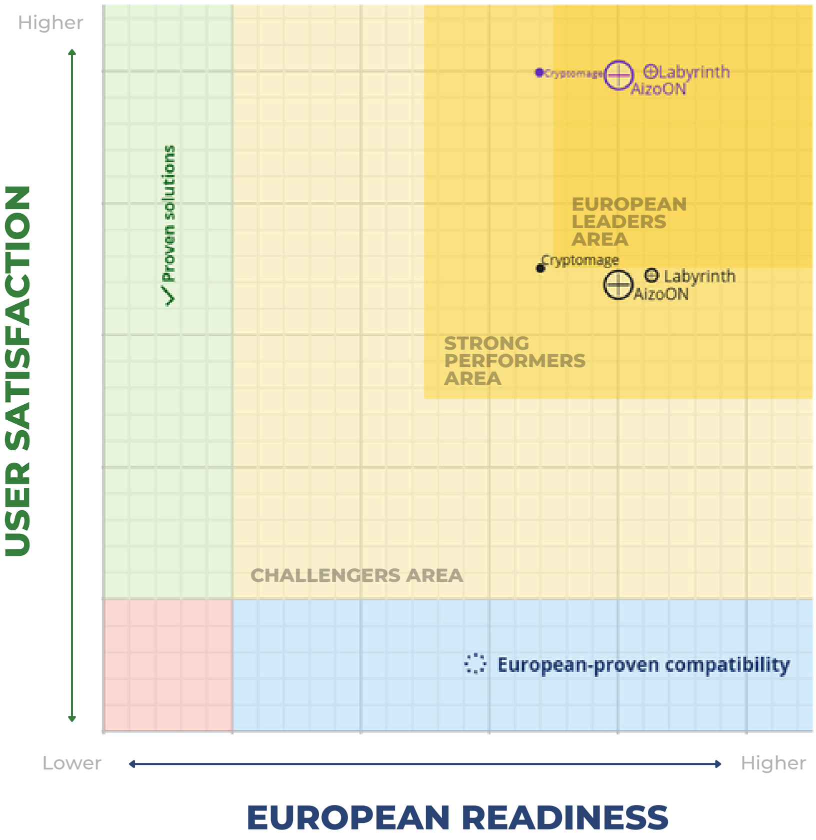
CYBERHIVE MATRIX Q1 2025 **PREVIEW EDITION**

NDR SOLUTIONS

3.

CYBERHIVE MATRIX Q1 2025

NDR Solutions Matrix



Legend

Company sizes

- Micro company (10-)
- Small company (50-)
- Medium company (250-)
- Enterprise (250+)

Colours

- ● Current results
- ● Results if the **Cyberhive Reviews Score*** was 5/5 , as some solutions do not have reviews yet on The Cyberhive Europe.

*in ease of scalability and deployment.

EVALUATED VENDORS

aizoon®

cryptomage®

LABYRINTH
Better protection. Less complexity. More confidence.

ARAMIS

By aizoOn

The ARAMIS Solution by aizoOn is an innovative platform that integrates machine learning, threat intelligence, and advanced cyber analytics to redefine the standards of cybersecurity. Designed to combat the increasing complexity of cyber threats, ARAMIS leverages cutting-edge technology to augment human expertise with artificial intelligence.

[1] Ease of scalability: guaranteed by increasing the number of ADS and ALS. ADS (Aramis Distributed Sensor) acquires network traffic for monitoring and directs it toward ALS (Aramis Learning Server), the information processing server.

[2] Ease of deployment: provided within the documentation.

Support

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

Training

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

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE ✗

ECSO OFFICIAL MEMBER

User Experience

Average rating	5
Ease of scalability	N/A[1]
Ease of Deployment	N/A[2]
Peer Recommendation	100%
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Gartner Cool Vendor 2016

*10 Reviews

ARAMIS

By aizoOn

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	Open-premise Linux
Pricing Transparency	Custom depending on customer needs and size.
Total Cost of Ownership (TCO) justification	The vendor did not specify this information.
Pricing Model	Subscription (monthly/yearly), custom pricing.

European readiness

Gender balance	31% female / 69% male
Supported languages	English, Italian, Spanish.
Company standards & certifications	List of certification: ISO/IEC 27001 , ISO 9001, ISO 22301, CSA Certified SOC Analyst, OffSec OSCP, GIAC Certified Forensic Analyst, GIAC Certified Reverse, Engineering Malware. List of patents: method for detecting systematic communications in a communications network, corresponding device, and computer program product (IT102021000011267); method for detecting anomalies in SSL and/or TLS communications, corresponding device, and computer program product (IT102021000015782); method for detecting anomalies in network communications, corresponding device, and computer program product (IT102021000033203); method for detecting phishing attacks, and corresponding system and computer program product (IT102023000019872)
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

Cryptomage Cyber Eye

By Cryptomage

Cryptomage Cyber Eye™ Network Detection and Response-class network probe is much more than a simple traffic flow analytics tool. It provides real-time, network-based anomaly detection and prediction powered by the low-level network protocol, machine learning (ML), and artificial intelligence (AI) algorithms. As a result, organizations can identify, monitor and triage traffic flows, connections, and potential malicious events.

[1] Cryptomage NDR solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

Support

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

Training

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

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

User Experience

Average rating	5
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	100%
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

ECSO STARtup Award 2023

*10 Reviews

Cryptomage Cyber Eye

By Cryptomage

Solution

Deployment support	Cloud, SaaS, web-based, On-premise Linux.
Supported platforms	All web browsers supporting OSs, Linux.
Pricing Transparency	The list price for the solution ranges between 1,606 EUR and 9,790 EUR per month, depending on the selected licensing options, such as bandwidth and number of hosts.
Total Cost of Ownership (TCO) justification	The monthly cost ranges from 1,606 EUR to 9,790 EUR, depending on selected licensing parameters such as: License period: 12, 24, or 36 months Bandwidth: from 1 Gbps to 5 Gbps Number of hosts: from 1,000 to 50,000 There is an option for a one-time payment.
Pricing Model	Subscription (monthly/yearly), Perpetual license, Custom pricing

European readiness

Gender balance	7% female / 93% male
Supported languages	English, Polish (17,4% EU coverage).
Solution/Company standards & certifications	The vendor did not specifiy this information.
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

Cyber Deception Platform

By Labyrinth

Labyrinth Deception Platform is a cyber threat detection platform that intentionally protects the network from targeted attacks, unknown threats, botnets, 0-day and malicious insiders by detecting and blocking cyberattacks within the corporate network.

The solution does not require additional software installation and has an intuitive interface. The platform provides a simple and effective tool for detecting intruders as soon as possible and complete visibility into the development of attacks with event correlation to make correct and quick decisions. For MSSPs, it is critical to have tools that will allow them to provide services to customers with low hardware costs and minimal time to deploy the necessary components/modules.

Network Monitoring:

1. Monitor your network for early threat detection, potentially slowing down attacks.
2. Similar functionality to NDR (Network Detection and Response) and IDS (Intrusion Detection System) solutions.

Intrusion Detection System:

1. Monitor network traffic and detect intrusions.
2. Comparable to NDR and traditional IDS solutions.

Security Operations Center (SOC):

1. Provide alerts for SOC, SIEM (Security Information and Event Management).
2. XDR (Extended Detection and Response) systems These alerts can be correlated with other systems to confirm and enrich incident data.

[1] Labyrinth Deception Platform solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE™

ECSO OFFICIAL MEMBER

User Experience

Average rating	4,8*
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	80%
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

ECSO CISO Choice Award 2025 Finalist

*5 Reviews

Cyber Deception Platform

By Labyrinth

Solution

Deployment support	Cloud, SaaS, web-based
Supported platforms	All web browsers supporting OSs, On-premise Windows, On-premise Linux.
Pricing Transparency	Subscription (monthly/yearly), 3,500 per pack of 10 decoys.
Total Cost of Ownership (TCO) justification	No additional cost needed.
Pricing Model	Subscription (monthly/yearly). Custom pricing.

European readiness

Gender balance	18% female / 82% male
Supported languages	English, Polish, Ukranian (21,11% EU coverage).
Solution/Company standards & certifications	The vendor did not specifiy this information.
Proof of a third party audit report (max. 2 years old) available?	No
Privacy Policy compliant with EU GDPR	Yes

NDR Scoring Tables

Criteria	User Experience						Final
	Overall user satisfcation		Average ease of scalability	Average ease of deploy-ment	Deployment support		
	Average overall rating	Average NPS			Included deployment docs.	Included support. docs.	
aizoOn	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Cryptomage	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Labyrinth	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Register for free to read the complete edition cyberhive®

Criteria	European readiness						Final
	Gender balance	Govern. transpa-rency	Language availability	Promotion of EU (-fit) solution	Operational Sovereignty		
					Data in EU?	HQ in EU?	
aizoOn	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Cryptomage	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Labyrinth	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Register for free to read the complete edition cyberhive®

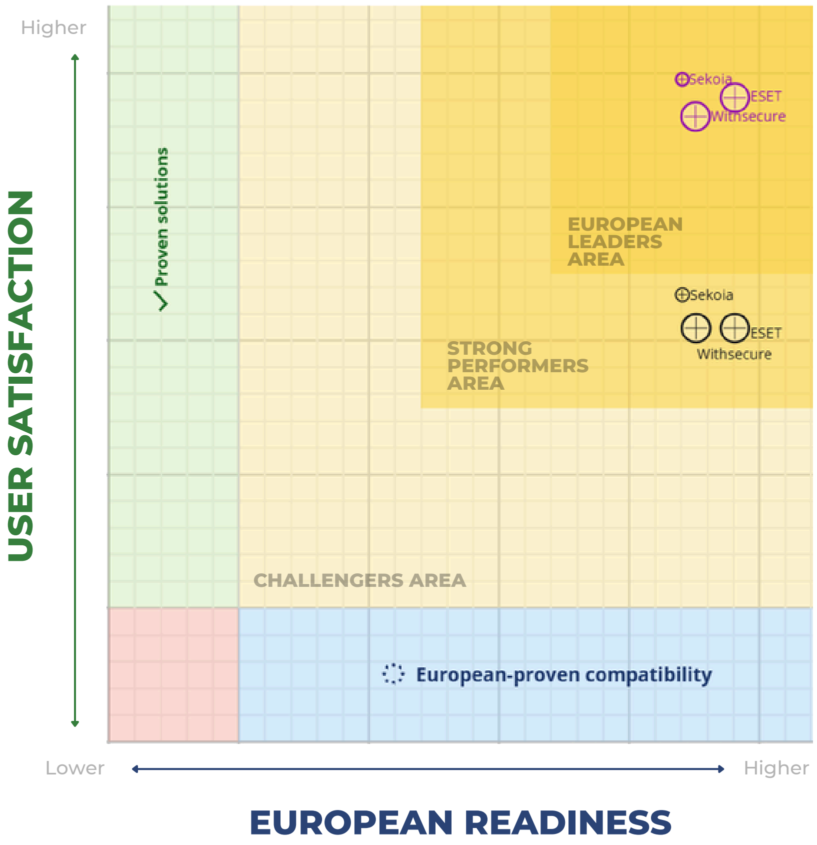
XDR SOLUTIONS

CYBERHIVE MATRIX Q1 2025 **PREVIEW EDITION**

4.

CYBERHIVE MATRIX Q1 2025

XDR Solutions Matrix



Legend

Company sizes

- Micro company (10-)
- Small company (50-)
- Medium company (250-)
- Enterprise (250+)

Colours

- ● Current results
- ● Results if the **Cyberhive Reviews Score*** was 5/5 , as some solutions do not have reviews yet on The Cyberhive Europe.

*in ease of scalability and deployment.

EVALUATED VENDORS

eset

sekoia

W/TH secure

ESET Protect XDR Platform

By ESET

Extended detection and response (XDR) from ESET empowers you to quickly and effectively identify anomalous behavior and breaches, and provides advanced threat hunting, risk assessment, incident response, investigation and remediation capabilities.

The platform integrates balanced breach prevention, detection, and response capabilities, complemented by ESET's managed and professional services, as well as threat intelligence. It is simple, modular, adaptable, and continuously innovated—always with the benefit of ESET's customers in mind.

[1] ESET XDR solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

Support

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

Training

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

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE™

ECSO OFFICIAL MEMBER

User Experience

Average rating	4,5*
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	64.8%
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

ESET named Certified EPR 2024 Strategic Leader

ESET earned 97 badges in the G2 Fall 2024 reports.

ESET recognized as a Midsize Enterprise Customers' Choice for Endpoint Protection Platforms 2024

*955 Reviews

ESET Protect XDR Platform

By ESET

Solution

Deployment support	Cloud, Hybrid, On-premises.
Supported platforms	Windows, MacOS, Linux.
Pricing Transparency	The vendor did not specify this information.
Total Cost of Ownership (TCO) justification	The vendor did not specify this information.
Pricing Model	Subscription (monthly/yearly), perpetual license, custom pricing.

European readiness

Gender balance	27% female / 63% male		
Supported languages	Dutch, Polish, French, Hungarian, Romanian, Slovenian, Spanish, Czech, German, Italian, Portuguese, Hungarian, Italian, Slovakian, Latvian, Swedish, Maltese, Luxembourgish, English (87,78% EU coverage) Moreover,ESET Solutions arein total available in 39 languages, some non-EU.		
Company standards & certifications	ISO 9001, ISO 27001, FIPS 140-2 Level 1, LINCE Certification, NIST Cybersecurity Framework.		
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.	Privacy Policy compliant with EU GDPR	Yes

Sekoia Defend

By Sekoia.io

Sekoia Defend **(Next-Gen SIEM)** is an Extended Detection and Response (XDR) SOC platform available in SaaS mode and powered by 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

User Experience

Average rating	5*
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	100%
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

European Finalist for Cyber Scale-up by ECSO/ECCC

Label France Cybersecurity 2024

Sekoia.io listed in the Sifted Leaderboard

*5 Reviews

Support

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

Training

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

[1] SEKOIA Defend XDR solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

Sekoia Defend

By Sekoia.io

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	All web browsers supporting OSs.
Pricing Transparency	The vendor did not specify this information.
Total Cost of Ownership (TCO) justification	The vendor did not specify this information.
Pricing Model	Different subscriptions based on the number of assets to supervise.

European readiness

Gender balance	30% female / 70% male
EU Compliance Driven	English, French (13,7% EU coverage).
Company standards & certifications	ISO27001 ce, PCI-DSS certification.
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

WithSecure Elements XDR

By WithSecure

WithSecure's modular **Elements Cloud cyber security platform seamlessly integrates XDR**, Exposure Management and Co-Security Services into a single unified solution. Through our flexible Elements modules made of cutting-edge software and high-quality services, customers can find the optimal solution for their needs. Together, the modules offer end-to-end business and cloud coverage.

In today's unpredictable, ever-changing business environment, our all-in-one security platform helps you build and maintain a resilient business. Elements Cloud includes all security capabilities in one platform. Elements XDR, running on Elements Cloud, includes modules for Endpoint Protection, EDR, Identity Security, and Collaboration Protection. Element Endpoint Protection is always included as it represents the most fundamental module.

[1] Withsecure XDR solution has the potential to earn a perfect 5 in both ease of deployment and ease of scalability, provided end-users share their reviews on the Cyberhive Solution page.

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE™

ECSO OFFICIAL MEMBER

User Experience

Average rating	4,6*
Ease of scalability	0(5)[1]
Ease of Deployment	0(5)[1]
Peer Recommendation	72.93%
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Support

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

Training

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

Awards

94% recommend WithSecure Elements Endpoint Protection on Gartner Peer Insights, in January 2025

Best Protection award in 6 years by AV-TEST

AI Excellent Award for Project Blackfin

*57 Reviews

WithSecure Elements XDR

By WithSecure

Solution

Deployment support	Cloud, SaaS, web-based.
Supported platforms	All web browsers supporting OSs, Desktop Mac, Desktop Windows, Desktop Linux, Server Linux, Server Windows, dentities: Microsoft Entra ID, Cloud platforms: Microsoft Azure, Amazon Web Services
Pricing Transparency	The price depends on the adopted modules.
Total Cost of Ownership (TCO) justification	The AV-Comparatives EPR CyberRisk Quadrant as an independent evaluation factors in the effectiveness of each product at preventing breaches in addition to its purchase and accuracy costs and the calculated savings as a result. WithSecure is a Strategic Leaders described as “endpoint prevention and response products that have a very high return on investment and provide a very low total cost of ownership (TCO) - all due to exceptional technical capabilities combined with reasonable costs.
Pricing Model	Pay as you go. Subscription (monthly/yearly).

European readiness

Gender balance	25% female / 75% male
Supported languages	Chinese, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish. (80.3%)
Solution standards & certifications	ISO/IEC 27001 Information Security Management Systems – Requirements, ISAE 3402 Type II, CREST Simulated Targeted Attack and Response (STAR), CREST Intelligence Led Penetration Testing (STAR), CREST Cyber Security Incident Response (CSIR), CREST Penetration Testing (PEN TEST), NCSC UK Cyber Incident Response (CIR) Level 2, NCSC Germany Cyber Incident Response (CIR), CREST TIBER EU (Europe), ISA/IEC 62433 (Security for Industrial Automation and Control Systems).
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

XDR Scoring Tables

Criteria	User Experience						Final
	Overall user satisfcation		Average ease of scalability	Average ease of deployment	Deployment support		
	Average overall rating	Average NPS			Included deployment docs.	Included support. docs.	
ESET	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Sekoia	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
WithSecure	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Criteria	European readiness						Final
	Gender balance	Govern. transparency	Language availability	Promotion of EU (-fit) solution	Operational Sovereignty		
					Data in EU?	HQ in EU?	
ESET	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Sekoia	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
WithSecure	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

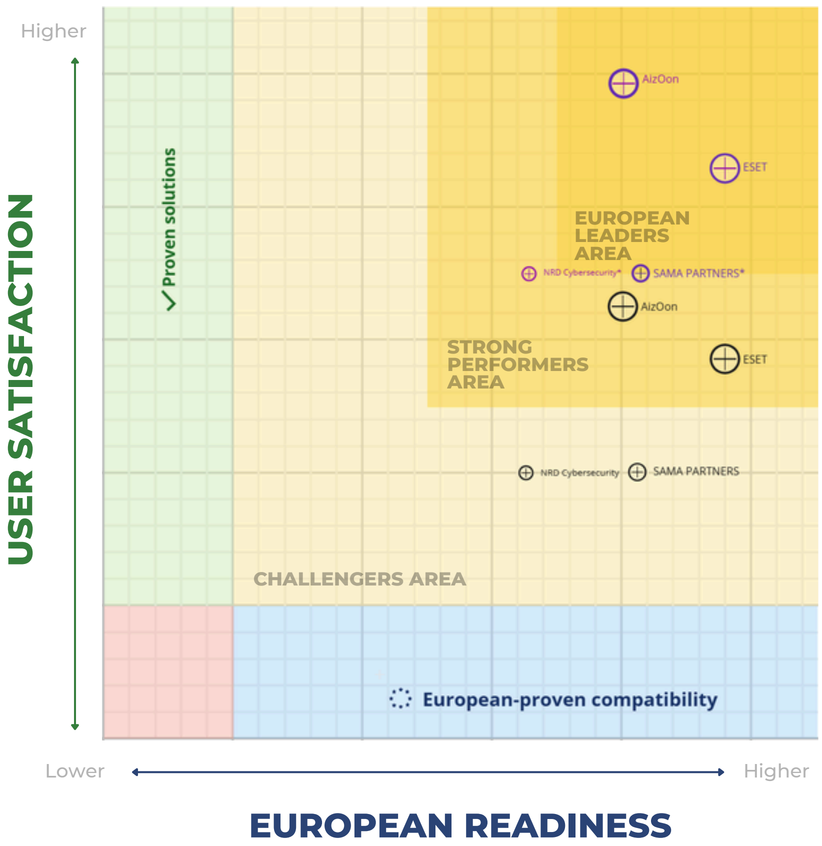
CYBERHIVE MATRIX Q1 2025 **PREVIEW EDITION**

SOC RELATED SOLUTIONS

5.

CYBERHIVE MATRIX Q1 2025

SOC Related Solutions Matrix



Legend

Company sizes

- Micro company (10-)
- Small company (50-)
- Medium company (250-)
- Enterprise (250+)

Colours

- ● Current results
- ● Results if the **Cyberhive Reviews Score*** was 5/5 , as some solutions do not have reviews yet on The Cyberhive Europe.

*in ease of scalability and deployment.

EVALUATED VENDORS

aizoon

SAMA PARTNERS

eset

NRD Cyber Security

iSOC Service (Managed SOC Service)

By aizoOn

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 organization, 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 organizational 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.

*Being a SOC-related solution, positive customer feedback and recommendations are available but cannot be listed publicly due to contractual and security reasons. References are available upon request and can only be shared via direct, one-to-one email communication.

Support

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

Training

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

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE™

ECSO OFFICIAL MEMBER

User Experience

Average rating	4,7
Ease of scalability	N/A
Ease of Deployment	N/A
Peer Recommendation	81.82%*
Incl. deployment docs,	N/A

Incl. supporting docs.

N/A

Awards

No awards received yet.

iSOC Service (Managed SOC Service)

By aizoOn

Solution

Deployment support	Cloud, SaaS, web-based
Supported platforms	N/A
Pricing Transparency	Subscription (monthly/yearly), custom pricing.
Total Cost of Ownership (TCO) justification	The vendor has not displayed this information
Pricing Model	Subscription (monthly/yearly), custom pricing.

European readiness

Gender balance	31% female / 69% male
Supported languages	English, Italian, Spanish.
Company standards & certifications	ISO/IEC 27001 , ISO 9001 Other: CEH Certifiied Ethical Hacker, CSA Certified SOC Analyst, CND Certified Network Defender, CTIA Certified Threat Intelligence, GIAC Certified Detection Analyst, GIAC Certified, Enterprise Defender, GIAC Certified Forensic Analyst, GIAC Certified Incident Handler, GIAC Certified Reverse, Engineering Malware, CompTIA Cybersecurity Analyst, CompTIA Security+
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

SOCurity

By SAMA PARTNERS

SOCurity® is the SOC-as-a-Service solution from SAMA PARTNERS and helps organisations to minimize risks, manage security operations effectively, and achieve regulatory compliance. SOCurity® identifies cyber threats in real time using log data analysis from myriad data sources within your organization. Up-to-the-second analysis of log data to maintain a strong security posture. Set-it-and forget-it solutions and constant monitoring in order to protect your business assets. Cutting-edge technology, process and expertise to deliver dynamic 24/7 security and a cost-effective monitoring.

Other functionalities include:

1. Filtering Out the Vast Majority of False Alarms
2. Guaranteeing Threat Lifecycle Visibility
3. Providing Customized Options
4. Remediating Threats
5. Supplying Threat Intelligence Reports

*Being a SOC-related solution, positive customer feedback and recommendations are available but cannot be listed publicly due to contractual and security reasons. References are available upon request and can only be shared via direct, one-to-one email communication.

*Ease of scalability: Based on client's requirements, scalability is given any time: asset coverage (based on client's size from small to enterprise); time coverage (from 8/5 model to 24/7 model); scalability of services on a modular base; scalability of resources (SAMA has its own academy to train SOC analysts).

*Ease of deployment: Seamless Integration of client's landscape: onboarding process; log integration process; flexible timeline (client priorities); additional activities conduced to enable client readiness for integration.

Support

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

Training

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

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE ✕

ECSO OFFICIAL MEMBER

User Experience

Average rating	N/A*
Ease of scalability	N/A*
Ease of Deployment	N/A*
Peer Recommendation	N/A
Incl. deployment docs,	Yes

Incl. supporting docs.

Possibility to book a demo,

Awards

'UnternehmerStar' prize by BVMW in 2018 as the best medium-sized company of the year in Germany (Category: Digitalisation / Industry 4.0)

SOCurity

By SAMA PARTNERS

Solution

Deployment support	On-premise Windows, on-premise Linux.
Supported platforms	N/A
Pricing Transparency	Based on number of assets under management/monitoring. Alignment with growth of the client.
Total Cost of Ownership (TCO) justification	Transparent costs including license consumption and flexible for the client’s choice (all-inclusive or client-owned licenses)
Pricing Model	Subscription (monthly/yearly/adhoc service for example forensics/ threat hunting)

European readiness

Gender balance	25% female / 75% male
Supported languages	English, French, German, Hungarian, Romanian (28,52% EU coverage), and Arabian.
Company standards & certifications	SO27001, Information Security Management Systems – Requirements, ISA/IEC 62433 (Security for Industrial Automation and Control Systems), SOC CMM, Security certifications (People): IBM, PECB, EC-Council, IATA.
Proof of a third party audit report (max. 2 years old) available?	TÜV SÜD ISO/IEC 27001:2022 Audit successfully conducted (December 2024) .
Privacy Policy compliant with EU GDPR	Yes

ESET SOC as a Service related

By ESET

ESET's Threat Intelligence service provides global knowledge, gathered by ESET experts, on targeted attacks, advanced persistent threats (APTs), zero-days and botnet activities. Informed by ESET intelligence feeds, organizations can improve their proactive security posture and enhance their threat hunting and remediation capabilities. 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. 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 resolve any outstanding issues.

*Being a SOC-related solution, positive customer feedback and recommendations are available but cannot be listed publicly due to contractual and security reasons. References are available upon request and can only be shared via direct, one-to-one email communication.

Support

☒ Not specified

Training

☒ Not specified

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE™

ECSO OFFICIAL MEMBER

User Experience

Average rating	4
Ease of scalability	N/A*
Ease of Deployment	N/A*
Peer Recommendation	100%
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Market Analysis Perspective: Worldwide Threat Intelligence, 2024

Forrester Best Practice Report 2025- How To Measure The Effectiveness And Value Of Threat Intelligence

IDC Market Glance: Threat Intelligence, 2Q24

*965 Reviews

ESET SOC as a Service related

By ESET

Solution	
Deployment support	Cloud, Hybrid, On-premises.
Supported platforms	Windows, MacOS, Linux, Android, iOS.
Pricing Transparency	Contact the company for further information.
Total Cost of Ownership (TCO) justification	The vendor did not specify this information.
Pricing Model	Subscription (monthly/yearly), perpetual license, custom pricing.

European readiness	
Gender balance	27% / 63%
Supported languages	Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Norwegian, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, Swedish, Ukrainian (100 % EU coverage) Moreover, ESET Solutions are in total available in 39 languages, some non-EU including Japanese, Turkish, Chinese and Russian.
Company standards & certifications	Data are supplied in standardised formats such as JSON and STIX feeds via TAXII – so that integration into any tool is possible.
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

NRD Cyber Security

CyberSet

By NRD Cyber Security

CyberSet is a CSIRT or SOC services automation toolkit. It works as a set of technologies and operational procedures, which provides CSIRTs and SOCs with typical service delivery capabilities, such as security monitoring and incident management. The toolkit enables cybersecurity teams to gain service delivery capabilities much faster and in a more structured manner than by developing them organically. When setting-up a CSIRT or SOC, organisations are faced with alternatives for acquiring service delivery capabilities. One common alternative is the "do-it-yourself" approach, where the organization develops and organizes all aspects internally, handling both the technology and operational procedures. However, this method requires the team to have substantial experience and expertise in relevant technologies, processes, and clearly defined roles and responsibilities. With CyberSet, these critical elements are pre-integrated, providing a ready-made solution that ensures a more cohesive and efficient service deployment.

*Being a SOC-related solution, positive customer feedback and recommendations are available but cannot be listed publicly due to contractual and security reasons. References are available upon request and can only be shared via direct, one-to-one email communication.

Support

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

Training

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

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY™ MADE IN EUROPE ✗

ECSO OFFICIAL MEMBER

User Experience

Average rating	N/A*
Ease of scalability	N/A*
Ease of Deployment	N/A*
Peer Recommendation	100%
Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

No awards given yet

*965 Reviews

CyberSet

By NRD Cyber Security

Solution

Deployment support	Deployment manuals, implementation via docker images.
Supported platforms	Ubuntu Linux LTS
Pricing Transparency	Contact the company for further information.
Total Cost of Ownership (TCO) justification	The vendor did not specify this information.
Pricing Model	Perpetual license. Custom pricing

European readiness

Gender balance	50% / 50%
Supported languages	English
Company standards & certifications	ISO/IEC 27001 Information; Security Management Systems Requirements; TL 9000 Quality Management System Other: TF-CSIRT TI Accredited
Proof of a third party audit report (max. 2 years old) available?	The vendor did not specify this information
Privacy Policy compliant with EU GDPR	Yes

SOC Rel. Solutions Scoring Tables

Criteria	User Experience						Final
	Overall user satisfcation		Average ease of scalability	Average ease of deployment	Deployment support		
	Average overall rating	Average NPS			Included deployment docs.	Included support. docs.	
aizoOn	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Sama Partners	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
ESET	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
NRD CyberSet	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Criteria	European readiness						Final
	Gender balance	Govern. transparency	Language availability	Promotion of EU (-fit) solution	Operational Sovereignty		
					Data in EU?	HQ in EU?	
aizoOn	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Sama Partners	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
ESET	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
NRD CyberSet	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

HONORARY MENTIONS

6.

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 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 was mainly funded by the Connecting Europe Facility (CEF) program in course of the project AWAKE (2020-AT-IA-0254). It has further received funding from the European Defence Fund through the projects EUCINF (101121418) and NEWSROOM (101121403), as well as by the Austrian security research programme KIRAS of the Federal Ministry of Finance (BMF) in course of the projects ASOC (FO999905301) and Testcat (FO999911248).

Cyberhive Page

Distinctions

Basic Cyberhive Member

CYBERSECURITY MADE IN EUROPE ✕

ECSO OFFICIAL MEMBER

User Experience

Incl. deployment docs	Yes
Incl. supporting docs	Yes

Awards

Taranis AI is a well adopted Github community project which received considerable adoption demonstrated through Github stars and number of contributors

Taranis AI - OSINT Analysis

by Austrian Institute of Technology (AIT)

Solution	
Deployment support	Cloud, SaaS, web-based, On-premise Linux.
Supported platforms	All web browser supporting OSs and Linux.
Pricing Transparency	Free
Total Cost of Ownership (TCO) justification	Open source.
Pricing Model	Free, open source.
European readiness	
Supported languages	English (10% of EU Coverage)
Contributions	We welcome contributions and provide a DevSetup.
Privacy Policy compliant with EU GDPR	Yes

CanaryBit

Confidential Cloud

by Canary Bit

Confidential Cloud is CanaryBit's solution for Businesses and Public Authorities that are willing to collaborate by exchanging sensitive data and algorithms, and in need of a hardware-encrypted execution environment protected from unauthorized access. Run workloads On-prem or on Public Clouds and get an auditable verification of the encrypted, running environment.Confidential Cloud helps address legal risks for the customer entity's information asset: confidentiality, integrity, and availability.

Common risks include the risk of the Cloud Service Provider being obligated to provide access to third country Government Agencies such as law enforcement or intelligence agencies. Well known examples impacting European-based companies using e.g. MS Azure, AWS, GCP and others, are the United States Federal Law named CLOUD Act and the Foreign Intelligence Surveillance Act - FISA Section 702.Data and algorithms processed in Confidential Cloud cannot be technically accessed by anyone else but their respective owners.

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY™ MADE IN EUROPE ×

ECSO OFFICIAL MEMBER

User Experience

Incl. deployment docs	Yes
Incl. supporting docs	Demo

Awards

The Royal Swedish Academy of Engineering Sciences (IVA) TOP 100-list in 2023 listing research projects focusing on climate change, energy supply, welfare technology, cyber security, and crisis preparedness.

Confidential Cloud

by Canary Bit

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux.
Pricing Transparency	Subscription (monthly/yearly).
Pricing Model	Subscription (monthly/yearly), custom pricing.
European readiness	
Gender balance	20% female / 80% male
Supported languages	English, German, Italian, Swedish (24,81 %EU Coverage)
Company standards & certifications	ISO27001 Information Security Management Systems – Requirements ISA/IEC 62433 (Security for Industrial Automation and Control Systems)
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

CanaryBit

Confidential AI

by Canary Bit

Confidential AI is an operations management and compliance platform for Secure AI.

It orchestrates secure environments On-premise and in Public Clouds, collecting security properties from infrastructure platforms to enforce code/model identity and data integrity.

It performs continuous testing and validation of AI models and data for secure data collaboration.

Cyberhive Page

Distinctions

Professional Cyberhive Member

CYBERSECURITY MADE IN EUROPE

ECSO OFFICIAL MEMBER

User Experience

Incl. deployment docs	Yes
Incl. supporting docs	Demo

Awards

Leonardo Business Innovation Factory award selected as the best startup among more than 170 applications from all over the world in the first edition (2022).

CanaryBit

Confidential AI

by Canary Bit

Solution	
Deployment support	Cloud, SaaS, web-based.
Supported platforms	On-premise Windows, On-premise Linux.
Pricing Transparency	Subscription (monthly/yearly).
Pricing Model	Subscription (monthly/yearly), custom pricing.

European readiness	
Gender balance	20% female / 80% male
Supported languages	English, German, Italian, Swedish (24,81 %EU Coverage)
Company standards & certifications	SO27001 Information Security Management Systems – Requirements ISA/IEC 62433 (Security for Industrial Automation and Control Systems)
Proof of a third party audit report (max. 2 years old) available?	Yes, upon request.
Privacy Policy compliant with EU GDPR	Yes

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

cyberhive®
discover solutions from EUROPE™

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