ECSO
EUROPEAN CYBER SECURITY ORGANISATION

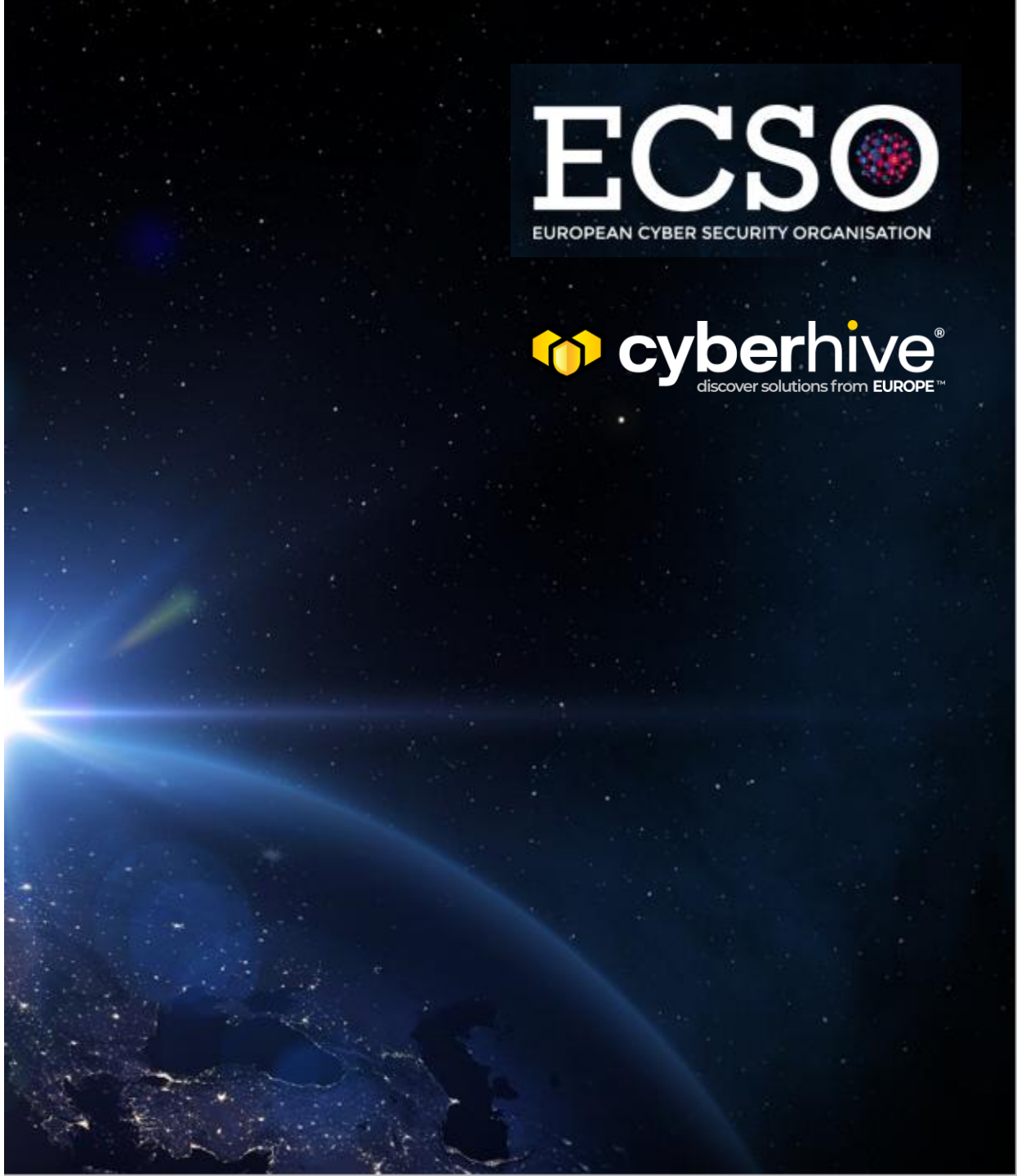
cyberhive®
discover solutions from EUROPE™

A new Taxonomy for Cybersecurity solutions

Daniele Dionisi

Product Owner of The Cyberhive

Table of contents



The European Cybersecurity Organisation

About ECSO

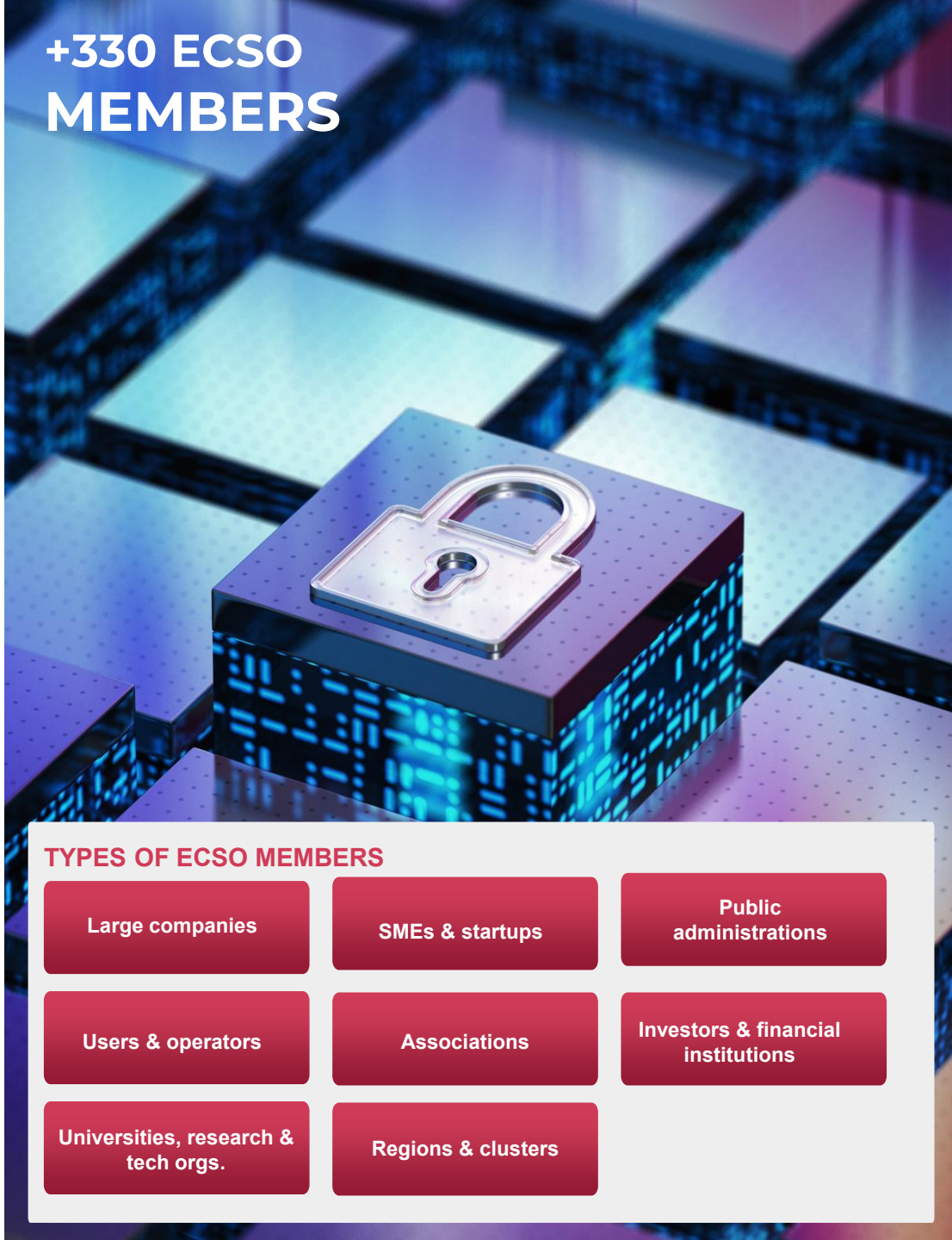
The European Cyber Security Organisation (ECSO) is the **pan-european**, private-public federation (**non-profit**) developing Europe's cybersecurity resilience and strategic autonomy.

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 grow our membership and continue to **empower cybersecurity communities** by providing a platform for cooperation, community advocacy, public-private collaboration, and more.

ECSO AREAS OF ACTIVITY

Ecso's work is structured on different areas correspondent to specific Working Groups (WG); in particular:

1. Trusted Supply Chains
2. Market Development
3. Threat Management
4. Skills & Human Factors
5. Research & Innovation
6. Policy Analysis & Outreach



About The Cyberhive

➢ History

The Cyberhive EUROPE® evolved from the ECSO market radar, an initiative to analyze Europe's cybersecurity market maturity by identifying its companies and their solution offerings.

➢ Mission

A competitive European cybersecurity market with internationally recognized solutions and strong synergies among cybersecurity stakeholders.

➢ Criteria

Cyberhive EUROPE is accessible for European organisations that:

1. Have their headquartered in Europe. If the company is a part of a group, then the group headquarters must be registered in Europe.
2. Have no major ownership/control from outside of Europe.
3. Respect the European laws and regulation applicable to the company. Like data and privacy requirements, defined by the EU's General Data Protection Regulation (GDPR)

Why we needed a new Taxonomy?

The background

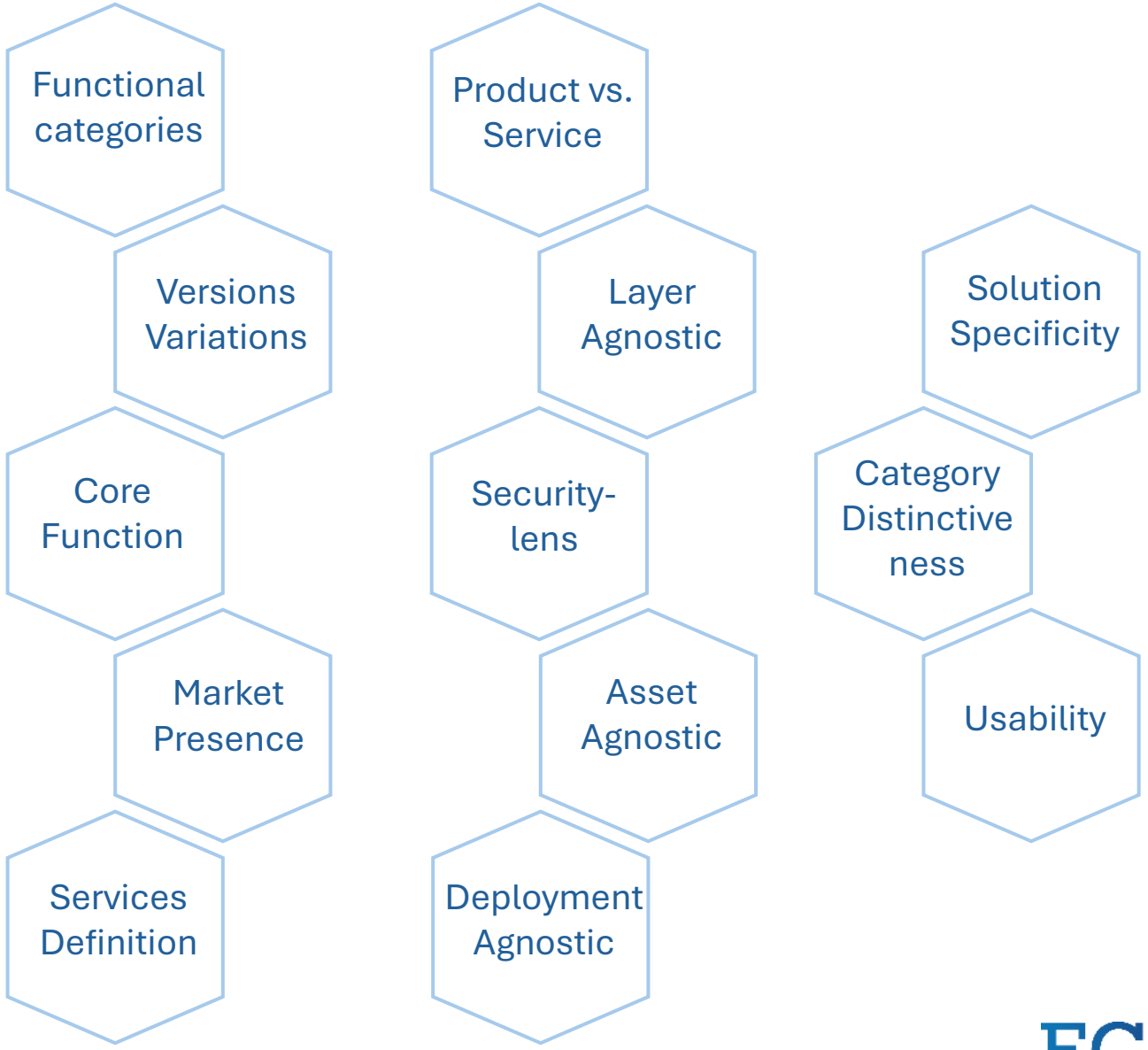
In recent years, we have witnessed an incredible boost in the cybersecurity sector, which has been increasing its market share by around 10% every year. At the same time, cybersecurity solutions have become far more effective, protecting devices against potential threats and offering a **broader range of services** associated with each solution.
At **ECSO**, through our digital marketplace **The Cyberhive**, we observed that the original NIST taxonomy, structured around six pillars (Detect, Protect, Identify, Recover, Respond, Govern), is **no longer sufficient** to describe what each solution actually does. Many solutions now 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.

The output

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



Assumptions – Detailed table

Principle	Description
Security-Lens	Categories cover core exclusively security purposes. They are intended to cover any solution deployed to provide cybersecurity protection and/or satisfy compliance with commonly accepted cybersecurity controls Categories catering to general IT, infrastructure, or application solutions, without a primary security function, are considered out of scope.
Functional Categories	Categories are based on enduring security functions, not vendor branding or marketing terms. Categories are expected to stay valid despite evolving solutions bundles.
Usability	The number of categories is limited to maximise user-friendliness. Categories based on sub-functions and/or features are not considered, as they would overwhelm comparison and navigation.
Category Distinctiveness	A category should exist as a standalone only if the function it represents is sufficiently distinct in purpose from other categories, and if merging it would obscure its unique role or mislead users about its primary value.
Solution Specificity	In cases where a substantial number of providers offer cybersecurity solutions within a specific category not presently represented, the taxonomy may be revised.
Deployment Agnostic	Categories are not dependent on the deployment model (e.g., on-premise, cloud, hybrid). The focus is on what the solution achieves, rather than on how or where it operates.
Asset Agnostic	Categories are not dependent on the type of asset protected (e.g., mobile, endpoint, network).
Layer Agnostic	Categories apply regardless of layer (e.g., infrastructure vs. application).
Product vs. Service	Categories are not dependent on the business model. If a vendor offers both a product and a distinct service, dedicated metadata tags are to be used to distinguish them (e.g., SOC-as-a-Service through MDR platform may be split).
Services Definition	Cybersecurity services deliver outcomes through expertise, processes, and technology, including advisory, operational, and reactive services aimed at improving security posture.
Versions Variations	Solutions sold in multiple editions are only listed separately if they differ materially in core function. (e.g., Pro vs. Enterprise). No dedicated tagging is foreseen.
Core Function	A solution is assigned to the category reflecting its primary purpose. Multi-function solutions are assigned according to their main capability.
Market Presence	A solution is included if actively used in the market. Old versions and end of life (EOL) solutions shall be ignored. No dedicated tagging is foreseen.

The new Taxonomy list

1. *Governance, Risk & Compliance (GRC)*
2. *Identity and Access Management (IAM)*
3. *Data Security & Prevention (DSP)*
4. *Monitoring and Performance (MON)*
5. *Detection and Response (DnR)*
6. *Vulnerability Management (VULN)*
7. *Offensive Security (OFFSEC)*
8. *Orchestration (ORC)*
9. *Cyber Threat Intelligence (CTI)*
10. *Recovery (REC)*
11. *Digital Forensics Investigations (DFI)*
12. *Training (TRN)*

Governance, Risk & Compliance (GRC)

Definition

Is a strategic framework implemented by organizations 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, trough GRC define and enforce security policies, measure risk posture, and automate compliance with regulations.

Indicative Requirements

- Maintain a versioned library of policies and controls
- Map controls to 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 risks

Excluded examples

- Data loss prevention (DSP)
- Automated evidence collection for audit (VULN)

Solution category examples

- Policy-management
- GRC solutions
- Audit treatment automation
- Compliance dashboards
- risk analysis and management
- Supply chain risk management
- Awareness

Identity and Access Management (IAM)

Definition

Is 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.

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

Excluded examples

- Data encryption solutions (DSP)

Solution category examples

- SSO
- MFA
- PAM
- PKI
- Identity governance and administration
- Access proxy
- CIAM
- ISPM
- Activity audit trails
- Password managers

Data Security & Prevention (DSP)

Definition

Is the practice of protecting digital information from unauthorized access, corruption or theft throughout its lifecycle. A systems 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.

Indicative Requirements

- Encrypt data at rest (symmetric, asymmetric, quantum-safe or post-quantum cryptography)
- Encrypt data in transit (symmetric, asymmetric, quantic)
- 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

Excluded examples

- Access brokering (IAM)
- Vulnerability scanners
- Patch-deployment systems (VULN)

Solution category examples

- DLP
- Encryption gateways
- Tokenization platforms
- PETS
- MPCs
- HSM
- NGFW
- WAF
- host-based firewalls
- VPN (End-Point, Site2Site, VPN-SSL)
- Wiping solutions
- database encryption
- SAN/NAS/HD encryption

Monitoring and Performance (MON)

Definition

Is 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 consist in continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected.

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)

Excluded examples

- Manual threat-hunting workflows (Analytics & Detection)

Solution category examples

- Metric/log collectors
- SIEM
- Network-flow analyzers
- OT (security-related infrastructure monitoring)

Detection and Response (DnR)

Definition

Refers to the tools and processes organizations use to detect, investigate and mitigate cybersecurity threats. It combines advanced detection methods, automated response capabilities and integrated security solutions to help organizations reduce risk and adapt to an evolving threat landscape.

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

Excluded examples

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

Solution category examples

- EDR
- IDS/IPS
- Automated quarantine
- XDR
- MDR (service)
- Email security
- Malware analysis

Vulnerability Management (VULN)

Definition

Is 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, organizations can help prevent attacks and minimize damage if one does occur. The goal of vulnerability management is to reduce the organization's overall risk exposure by mitigating as many vulnerabilities as possible.

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 integrate with ticketing systems
- Keep update lists of all components, libraries and modules in a software product (SBOM)

Excluded examples

- Patch-deployment systems (Prevention)
- Phishing simulations

Solution category examples

- SAST/DAST
- Container/cloud posture management
- Vulnerability scanners
- CNAPP
- Application security testing

Offensive Security (OFFSEC)

Definition

Refers to solutions that strengthen an organization's security posture by testing and exploiting defences to validate controls and surface exploitable weaknesses before genuine adversaries do.

Indicative Requirements

- Emulate adversary techniques
- Allow custom test plans and exploit configurations
- Generate prioritized findings and remediation recommendations

Excluded examples

- Passive monitoring solutions (Monitoring)

Solution category examples

- Pentest frameworks
- Breach-and-attack-simulation (BAS)
- Red Team platforms

Orchestration (ORC)

Definition

Is a software solution that enables security teams to integrate and coordinate separate security tools, automate repetitive tasks and streamline incident and threat response workflows.

Indicative Requirements

- Allow design of playbooks
- Drive playbook execution across solutions
- Facilitate coordination between team members
- Provide connectors for other security solutions

Excluded examples

- Single-solution playbooks embedded in SIEM (Monitoring)

Solution category examples

- SOAR platforms
- Case management
- Ticketing
- Automated workflows

Cyber Threat Intelligence (CTI)

Definition

Helps security teams take a more proactive approach to detecting, mitigating and preventing cyberattacks. It focuses on the structured collection, analysis, and dissemination of data regarding potential or existing cyber threats and provides organizations with the insights necessary to anticipate, prevent, and respond to cyberattacks by understanding the behavior of threat actors, their tactics, and the vulnerabilities they exploit.

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

Excluded examples

- Internal log analysis (Monitoring)

Solution category examples

- Threat-intel platforms
- Curated feeds
- Threat hunting rules platforms

Recovery (REC)

Definition

Restoring systems, data, and operations to a secure and functional state, ensuring business continuity and minimizing downtime.

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

Excluded examples

- Alert dashboards (Monitoring)

Solution category examples

- Backup solution
- Redundancy systems
- Ransomware recovery
- Cloud recovery and resilience solutions
- Business Continuity Planning (BCP)
- DR orchestration solutions

Digital Forensics Investigations (DFI)

Definition

Preserving and analyzing digital evidence post-incident to reconstruct timelines, root causes and scope. Digital Forensics is a subset of forensic science. It is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Digital forensic techniques can be used for many purposes, such as investigating crimes and internal policy violations, reconstructing security incidents and troubleshooting operational problems.

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

Excluded examples

- Backups (Recovery)

Solution category examples

- Memory-dump analysis
- Forensic imaging

Training (TRN)

Definition

Providing simulated environments and interactive exercises to develop and assess cybersecurity skills for individuals and teams.

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

Excluded examples

- Phishing simulations (Offensive)

Solution category examples

- Cyber ranges gamified trainings

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Daniele Dionisi daniele.dionisi@ecs-org.eu