# Next-Gen Security Operation Center Services for Critical National Infrastructures

Alexios Lekidis * , Yagmur Yigit , Leandros A. Maglaras , Konstantinos Karantzalos , George Spanoudakis

Posted Date: 5 May 2026

doi: 10.20944/preprints202605.0201.v1

Keywords: SOC; cybersecurity; NIS2

*Article*

# Next-Gen Security Operation Center Services for Critical National Infrastructures

**Alexios Lekidis [1,*], Yagmur Yigit [2], Leandros A. Maglaras [2], Konstantinos Karantzalos [3] and George Spanoudakis [4]**

[1] Department of Energy Systems, University of Thessaly, Larisa, Greece
[2] School of Computing, Engineering and The Build Environment, Edinburgh Napier University, UK
[3] Remote Sensing Lab., National Technical University of Athens, Athens, Greece
[4] Sphynx Technology Solutions AG Zug, Switzerland
* Correspondence: alekidis@uth.gr

**Abstract**

Critical National Infrastructures (CNIs) have evolved over the last years through the digitization of their services, which simultaneously led to an increase of their threat surface. Meanwhile the exponential rise of Artificial Intelligence (AI) technologies has given the means to adversaries to perform targeted attacks against high impact systems as the ones found in CNIs. Current regulation directives as the NIS2 or the Cyber Resilience Act (CRA) focus on the presence of Security Operation Centers (SOC), which include different security technologies for the detection and response to cyber-attacks. Nevertheless, such baseline SOCs do not provide the ability to perform a coordinated and orchestrated detection and response cycle for existing cyber threats, but also do not provide proactive measures for zero-day threats. To this end, this paper presents a new approach for automating the orchestration of the incident lifecycle through Next Generation SOC services able to detect/mitigate sophisticated attacks against CNIs, but also implement proactive detection measures against zero-day threats.

**Keywords:** SOC; cybersecurity; NIS2

## 1. Introduction

Cyber threats towards critical infrastructures, which are defined based on the NIS2 directive [1], have had a recent exponential increase due to the abundance of interfaces that are present in different applications [2]. Moreover, the technological advances that are recently introduced through the Machine Learning (ML) and Artificial Intelligence (AI) models are automating the attacks, but also allowing the adversaries to launch sophisticated and complex targeted attacks against operational systems of critical infrastructures [3].

Moreover, the expansion and heavy deployment of AI systems has led to the development of a new attack surface that focuses on exploiting vulnerabilities in ML and AI models and compromising their function (e.g., reducing their accuracy). Such attacks are focusing on production-based ML and AI models and in literature they are termed Adversarial Machine Learning (AML) in [4,5]. AML attacks are usually based on data poisoning (i.e., attacks targeting the training data of an AI system) via the deployment of an ensemble learning model that will combine well-known ML and DL models (e.g., Convolutional Neural Networks (CNN), Multi-layer Perceptron. (MLP), RF) and distance metrics (e.g., Euclidean distance, Manhattan distance, Minkowski distance) to accurately detect poisoning samples in training datasets.

With cyber incidents increasing in number and sophistication, countries around the world are trying to improve their smart defenses [5,6]. Creating diplomatic toolboxes and shaping incident response procedures is not always enough [7]. While regulations like NIS2 and the Cyber Resilience Act (CRA) mandate the use of Security Operation Centers (SOCs) among other solutions [8], baseline

 doi:10.20944/preprints202605.0201.v1



SOCs are currently insufficient for coordinated or proactive response. The gap between having a box-ticking compliance SOC and a truly resilient operational center capable of handling zero-day threats is still to be met. Concepts like securability that combine security compliance and reliability analysis were also recently proposed [9] EU strategic approach against cyber attacks is shifting from isolated responsibility of an organization or company to a collective and cross-border resilience model [10]. This model includes policies and procedures for exchanging real-time information about an attack or sensitive information about new threats. There is a clear need for Next-Gen services that go beyond the Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) solutions[11].

Based on these findings, this article makes the following contributions:

1. Presents a new approach for automating the orchestration of the incident lifecycle.
2. Introduces Next-Generation SOC services specifically designed for Critical National Infrastructures (CNIs).
3. Proposes a conceptual architecture that integrates proactive detection for zero-day threats.

The remainder of this paper is organized as follows: Section 2 provides preliminaries on current threat landscape and baseline SOC services. Section 3 analyzes the technological and regulatory requirements for next-gen environments. Section 4 presents the proposed conceptual architecture, and Section 5 concludes the work.

## 2. Preliminaries

In this section, we present the current threat landscape, especially those targeting CNIs and the baseline services that are offered in existing SOCs.

### *2.1. Critical Infrastructure Threat Landscape*

Critical infrastructures are becoming more exposed to cyber risk as their services grow more digital, more connected, and more dependent on cloud, edge, IT, and OT integration [12]. Energy, transport, healthcare, water, public administration, and digital public services now depend on interconnected platforms, remote monitoring, and cyber-physical assets for daily operation. This improves efficiency and automation, but it also creates new attack paths and weakens the separation between environments that were once more isolated [13,14]. These are also sectors where a successful cyberattack can cause consequences beyond the loss of information. Services may fail, safety may be affected, reputation may be damaged, and financial loss may occur. Electricity distribution, water supply, transport coordination, hospital services, financial services, and digital government services all face cyber threats and, therefore, cyber risk. This broader view, based on resilience, safety, and service continuity [15,16], is also reflected in more recent EU legislation covering energy, finance, health, and water infrastructures [17–19].

One of the most damaging threats is ransomware, which can lock operational systems, encrypt critical data, or disable essential organisational functions. In practice, this may disrupt emergency response, utility services, healthcare delivery, and financial transactions [13,20]. Phishing and social engineering also remain effective because they are often used to obtain internal credentials or initial access through staff in administrative or operational roles. Once access is gained, attackers may move toward administrative systems or operational technology. DDoS attacks against publicly accessible services and communication platforms are another major concern, especially because disruption can create immediate operational impact. ENISA identifies public administration, transport, banking, and digital infrastructure among the sectors most affected by DDoS activity, which shows how exposed critical digital services remain to availability attacks [13].

Critical infrastructures also depend on third-party software, managed services, cloud infrastructure, hardware vendors, and maintenance providers that remain outside the direct control of the operator. Because of this, a malicious update, a compromised library, a weak supplier, or a tainted software component may give attackers indirect access to a high-value environment before the operator

 doi:10.20944/preprints202605.0201.v1



notices the issue. This is why supplier assurance, dependency management, and third-party risk have become important concerns in recent EU regulations [14,21]. The same logic is also visible in DORA for the financial sector [17,22]. This issue becomes more serious with the growing use of IIoT and OT in critical services that depend on SCADA, PLCs, RTUs, gateways, field sensors, and remote monitoring devices. These industrial systems often operate under strict real-time and high-availability requirements. At the same time, they may still rely on weak authentication, insecure industrial protocols, poor IT/OT separation, slow patching practices, weak or missing encryption, insecure remote access paths, and limited monitoring of the physical processes they control. Such weaknesses can enable process manipulation, service disruption, or even physical impact [18,19,23]. Similar concerns have also been reported in healthcare and other highly digitalised sectors [20,24].

Generative artificial intelligence can support cyber defence, but it can also help adversaries scale phishing campaigns, generate convincing malicious content, and improve deception operations. At the same time, the transition to post-quantum cryptography and the migration of legacy cryptographic systems in long-lifecycle infrastructures create additional long-term challenges. As energy, water, healthcare, and financial services become more digitalised and interconnected, the resilience of critical infrastructures depends increasingly on the security and assurance of their digital assets [17,18]. Recent EU policy developments also suggest that cyber resilience is now treated more as a collective and cross-border issue than as a purely internal organisational responsibility [25,26].

Table 1 summarises the main cyber threat classes affecting critical infrastructures, together with their common attack vectors, likely target environments, and operational impact. Taken together, these threats show that isolated security products are not enough. Critical infrastructures need continuous monitoring, dependable detection, incident correlation, and timely response across heterogeneous environments. They also need coordinated security operations with visibility across endpoints, networks, platforms, and operational assets. This is why baseline SOC services are no longer optional support functions. They have become a basic operational requirement for protecting modern critical infrastructures.

**Table 1.** Main cyber threat categories in critical infrastructures and their operational impact.

| Threat category | Typical attack vector | Potential target environment | Operational impact |
|---|---|---|---|
| Ransomware | Malicious payloads, exploited vulnerabilities, compromised remote access | Enterprise IT systems, operational servers, service platforms | Service interruption, delayed recovery, financial loss, and safety risk |
| Phishing and social engineering | Deceptive emails, fake portals, employee manipulation, credential harvesting | Staff accounts, administrative systems, communication platforms | Unauthorized access, credential theft, lateral movement, and data exposure |
| DDoS attacks | Traffic flooding from botnets or distributed sources | Public portals, communication gateways, digital public services | Service unavailability, disrupted public access, and degraded emergency communication |
| Data breaches | Database compromise, stolen credentials, insider misuse | Citizen records, financial databases, administrative repositories | Privacy loss, fraud, reputational damage, and follow-up attacks |
| Supply-chain compromise | Malicious updates, tainted libraries, compromised vendors, hardware tampering | Software supply chain, managed services, hardware procurement chain | Indirect compromise, stealthy infiltration, and operational disruption |
| IIoT/OT exploitation | Insecure industrial protocols, weak segmentation, remote access abuse | SCADA, PLCs, RTUs, gateways, and field devices | Process manipulation, cyber-physical disruption, and persistent operational risk |
| Infrastructure sabotage | Malicious commands, control tampering, destructive actions | Utility controls, transport systems, and public safety platforms | Physical disruption, degraded continuity, and public safety consequences |
| Zero-day exploits | Previously unknown software vulnerabilities | Control applications, service platforms, software stacks | Undetected intrusion, rapid escalation, and high-impact compromise |
| Credential theft | Password theft, token abuse, account compromise | Remote access systems, privileged accounts, internal platforms | Unauthorized changes, account abuse, and service compromise |
| Insider threats | Malicious or accidental misuse of legitimate access | Trusted personnel, contractors, privileged environments | Security bypass, data leakage, and intentional or accidental disruption |

 doi:10.20944/preprints202605.0201.v1



### 2.2. Current State for Baseline SOC Services

The baseline services that are offered in existing SOCs have as an initial foundation the Endpoint Detection and Response (EDR) and the Network Detection and Response (NDR) systems. EDR systems focus on detecting and responding to threats at the endpoint level. They provide continuous monitoring and analysis of endpoint activities to detect, investigate, and remediate potential security incidents. On the other hand, NDR tools monitor and analyze network traffic to detect malicious activities, unusual patterns, and potential threats. They provide visibility into network communications and help in identifying and responding to network-based threats.

Both EDR and NDR systems collect security events and logs that are provided to SIEM systems in order to aggregate and correlate security event data from various sources across the organization's infrastructure. SIEM systems allow to perform triaging, scoping and investigation within a SOC environment and since this is the main source that the SOC analysts look at, eventually leads to the identification of false positives from the real incidents.

Finally, incident response is handled through SOAR platforms that integrate security operations and incident response workflows, enabling automation, orchestration, and response to security incidents. They enhance the efficiency and effectiveness of incident response by providing actionable insights and automating repetitive tasks.

## 3. Requirement Analysis for Next-Gen SOC Environments

### 3.1. Sectorial, National & EU-Level Resilience Requirements

In Europe, critical infrastructure resilience is no longer defined by a single regulation or by one sector alone. It depends on a wider governance structure that brings together EU cybersecurity legislation, sector-specific obligations, national implementation mechanisms, incident reporting duties, information-sharing channels, and assurance frameworks. In this setting, resilience cannot be treated as a narrow technical task. For critical infrastructures, it has become a continuous requirement covering prevention, detection, response, recovery, and coordination across both national and cross-border environments [14,27].

NIS2 is the main EU cybersecurity baseline for essential and important entities. Compared with the earlier NIS framework, it applies to a broader range of sectors, places stronger obligations on management bodies, and gives more emphasis to incident reporting, risk management, business continuity, and supply chain security [14,28]. Under this framework, organisations are expected to implement technical, operational, and organisational measures that match their risk exposure. These include incident handling, vulnerability management, access control, cryptographic protection, multi-factor authentication, and secure practices for the acquisition, development, and maintenance of network and information systems [15,16]. The CER Directive extends this view further by focusing on the availability and continuity of essential services under disruption, rather than on cyber defence alone [27]. This baseline is strengthened further by sector-specific instruments. In the financial sector, DORA introduces a harmonised framework for ICT risk management, ICT-related incident reporting, resilience testing, third-party risk management, and cyber threat information sharing [17,22]. In electricity, the Network Code on Cybersecurity sets stricter requirements for risk assessment, incident management, business continuity, supply chain security, and coordinated information sharing among actors involved in cross-border electricity exchange [18]. In healthcare, the European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers places greater emphasis on prevention, early warning, rapid response, training, and sector-specific support [20,24]. The same resilience logic can also be seen in newer initiatives for submarine cable and water infrastructure, including the EU Action Plan on Cable Security [29] and the European Water Resilience Strategy [30]. These legal requirements are implemented within each Member State through national authorities, CSIRTs, supervisory authorities, and sectoral bodies. As a result, the governance, response, and notification processes of critical infrastructure operators need to align not only with EU legislation, but also with national enforcement and implementation structures [14,27]. In practice, resilience is therefore managed across layered

 doi:10.20944/preprints202605.0201.v1



environments that combine EU-level obligations, sector-specific controls, and national operational requirements.

In line with these frameworks, NIS2 provides a multi-level structure for coordinated response, including early warning, incident notification, and incident reporting [14,15]. Similarly, DORA requires harmonised reporting of significant ICT-related incidents across the financial sector in the EU [17,21]. When an ICT incident involves personal data, the GDPR may also require notification to the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of the incident [31]. The Cyber Solidarity Act reflects the same collective logic at the EU level through joint alerting and standby mechanisms for major cyber incidents [25,26]. Although these instruments differ in legal form and sectoral scope, they are all built around prevention, detection, response, and recovery, as shown in Figure 1. These remain the common resilience dimensions across sectors and regulatory environments. Resilience should therefore be understood not as a box-ticking compliance exercise, but as a continuous operational cycle involving monitoring, coordination, reporting, and service restoration.

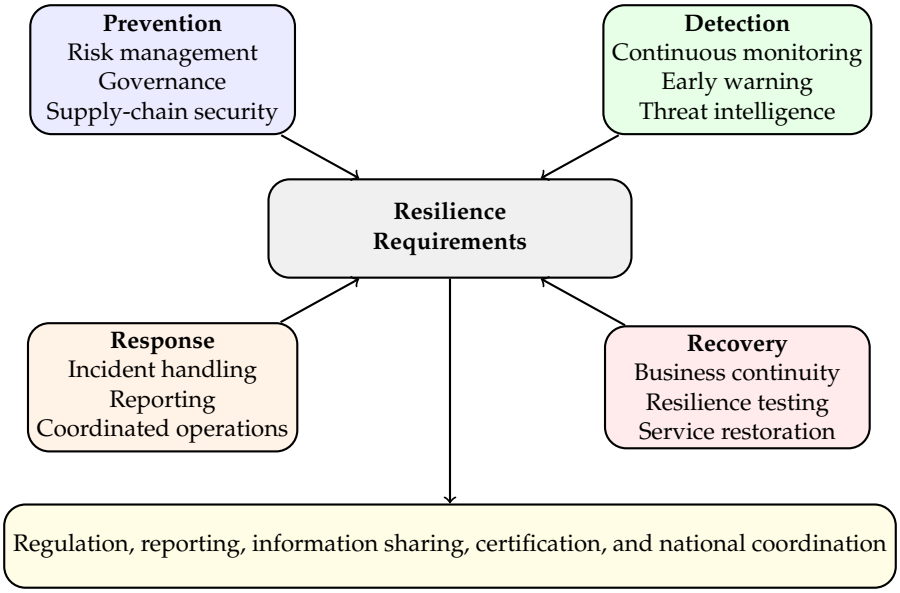


**Figure 1.** Core resilience pillars shaping critical infrastructure resilience.

Certification of critical digital elements is another important part of this resilience picture. The EUCC scheme provides a certification path under the European Union cybersecurity certification framework for ICT products, services, and processes established by the EU Cybersecurity Act [32,33]. This direction has been reinforced further by the Cyber Resilience Act, which introduces horizontal cybersecurity requirements for products with digital elements while supporting more secure-by-design supply chains [34]. In this way, certification can strengthen resilience by establishing a common assurance baseline and reducing fragmentation in the cybersecurity assessment of critical digital technologies.

At the operational level, resilience also depends on how these expectations are applied in daily practice. Continuous risk assessment, asset criticality analysis, incident response planning, resilience testing, cross-border information sharing, and structured third-party risk management all remain important. Table 2 summarises these areas and links them to the needs of resilience-oriented SOC environments. It also shows that modern SOCs are expected to support not only alert handling and threat response, but also evidence generation, supplier visibility, compliance-focused reporting, and coordination across different infrastructure layers.

 doi:10.20944/preprints202605.0201.v1



**Table 2.** Best-practice areas supporting resilience-oriented SOC environments.

| Requirement area | Best-practice focus | Operational implication for SOCs |
|---|---|---|
| Risk management | Continuous risk assessment, asset criticality analysis, governance accountability | Support risk-aware monitoring, alert prioritization, and escalation workflows |
| Incident reporting | Early warning, structured notification, final reporting, evidence retention | Generate timely alerts, preserve reporting evidence, and support compliance-driven reporting |
| Continuous monitoring | Real-time visibility across endpoints, networks, cloud, and OT/IIoT assets | Integrate telemetry sources and reduce attacker dwell time through early detection |
| Threat detection & correlation | Event aggregation, anomaly detection, alert triage, cross-domain correlation | Distinguish true incidents from noise and improve visibility of multi-stage attacks |
| Supply-chain security | Third-party risk visibility, dependency monitoring, secure procurement, vendor assurance | Extend monitoring beyond internal assets and track supplier-related attack exposure |
| Resilience testing | Scenario-based exercises, penetration testing, disaster recovery drills, readiness validation | Validate detection and response performance under disruptive conditions |
| Information sharing | Cross-border intelligence exchange, CSIRT cooperation, coordinated situational awareness | Operationalize threat intelligence and support coordinated incident response |
| Business continuity & recovery | Service restoration planning, crisis coordination, post-incident analysis, lessons learned | Support recovery workflows and feed incident lessons back into resilience planning |

Overall, these sectoral, national, and EU-level requirements show that resilience cannot rely on isolated security controls or fragmented operational practices. It requires continuous monitoring, governance accountability, third-party risk visibility, structured incident reporting, privacy-aware information sharing, and coordinated operational response. For this reason, next-generation SOC environments should be designed not only for threat detection and response, but also for compliance support, evidence generation, cross-domain coordination, and resilience-oriented decision making across different regulatory and sectoral contexts. These observations directly motivate the technological and operational requirements discussed in the next subsection.

### *3.2. Technological & Operational Requirements*

The important part of a next-generation SOC for critical infrastructures is not only the number of tools, but especially whether those tools work together in a consistent security operations approach. In a critical infrastructure SOC, it is not sufficient to only raise alerts. It is also important for the SOC to maintain a system-wide view of what is going on, especially in a dynamic threat environment. This wider role also fits with the resilience perspective of NIS2 and the CER Directive, especially with regard to governmental and defence-sensitive environments [14,27]. Continuously monitoring the environment is critical for the effectiveness of triage, investigation and response functions later in the incident response process. Therefore, SOC telemetry should cover not only endpoints and enterprise networks, but also cloud services, operational technology, internet of things (IoT), and field systems. EDR, NDR, and SIEM should therefore be considered integrative components of one monitoring layer. The monitoring layer in critical infrastructures should also contain protocol-aware monitoring of SCADA systems, PLCs, RTUs, and related field devices, given the strict availability and safety requirements their components need to meet [18,19]. This monitoring structure is a core part of the SOC as shown in Figure 2.

 doi:10.20944/preprints202605.0201.v1



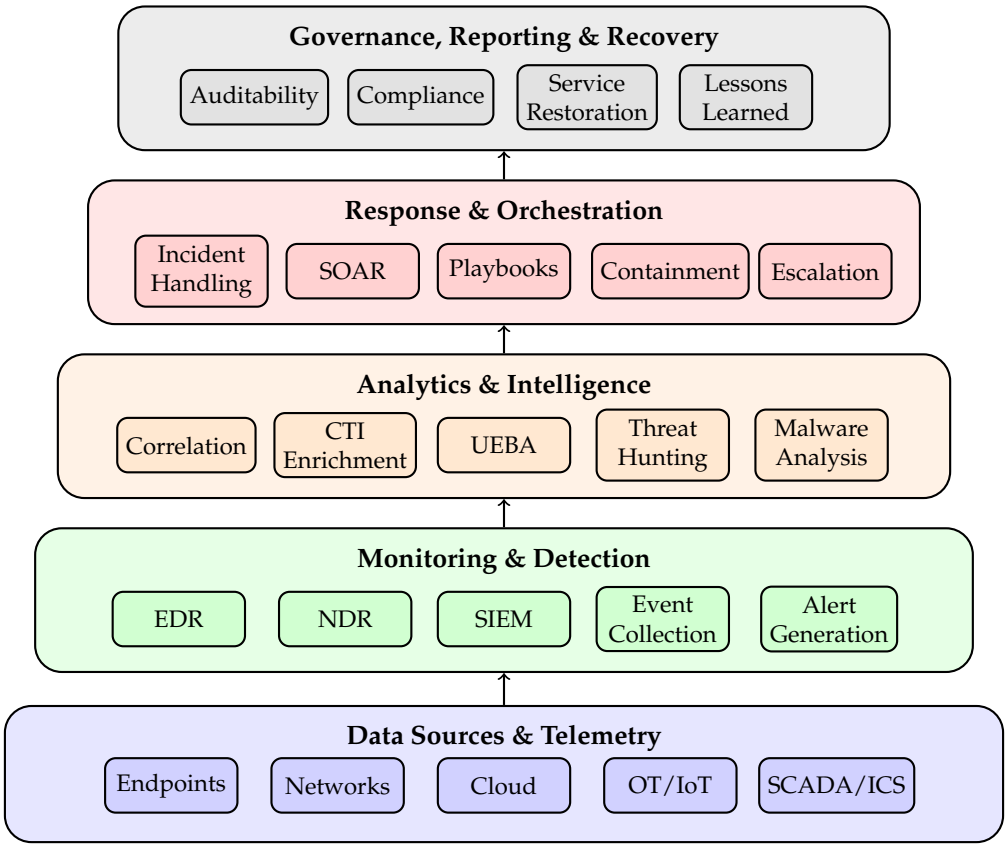


**Figure 2.** Core functional layers of a Security Operations Center.

However, visibility alone is not enough. The SOC must also understand what the observed activity means and why it matters. For this reason, cyber threat intelligence (CTI) is an essential part of SOC operations. CTI should not be treated as a separate function or only as an external feed. In addition, it should use both internal and external CTI, such as indicators of compromise, malware artefacts, attacker behaviour, and context and provide the ability for daily alert analysis, investigation, prioritisation, and threat hunting. It is also useful to map observed activity to attacker TTPs, which are most commonly associated with the MITRE ATT&CK framework [35], to help analysts understand attacker behavior and find gaps in detection coverage. Similar conclusions apply to analytics. A SOC based on static rules alone may not respond adequately to stealthy attacks, insider threats or multi-stage attacks, and should therefore focus on improved behavioural analysis and anomaly detection for post hoc and real-time analyses. This would allow user and entity behaviour analytics (UEBA) to identify signs of anomalous account usage and unusual access patterns sooner, as well as provide greater visibility into the actions of malware payloads and attackers through malware analysis and sandboxing. Applications of machine learning models for tasks such as scoring, anomaly detection, and classification may also pose a risk of their own. Data poisoning, evasion attacks and model drift are attacks on analytics themselves. Resources such as MITRE ATLAS and the OWASP Machine Learning Security Top 10 can help to design more secure analytics pipelines [36,37].

Another area where baseline SOCs may be insufficient is in the area of response, where critical infrastructures may require very fast but controlled responses. Thus, orchestration and automation of triaging, containing, notifying, and escalating requires interoperability among the SIEM, EDR, IAM, firewall, and ticketing systems. Full automation may not be feasible or appropriate when handling classified information, mission-critical systems, or where legal implications may exist [17,38]. Thus, while automation is used to speed and ensure consistency, humans must remain in the loop for oversight. Thus, the success of the SOC will ultimately depend on how well it is operated. Just having a good technical platform is not enough. Whether or not the SOC runs daily depends on its governance, staffing, procedures, and performance control. As shown in Figure 3, operational readiness depends on

 doi:10.20944/preprints202605.0201.v1



several interrelated factors. These include coordination with national authorities and CSIRT structures, dedicated resources and expertise, a consistent approach to incident handling and notification, and clear performance targets for detection, response, and service availability. Without these foundations, even advanced SOC technologies may operate in a fragmented and ineffective manner.

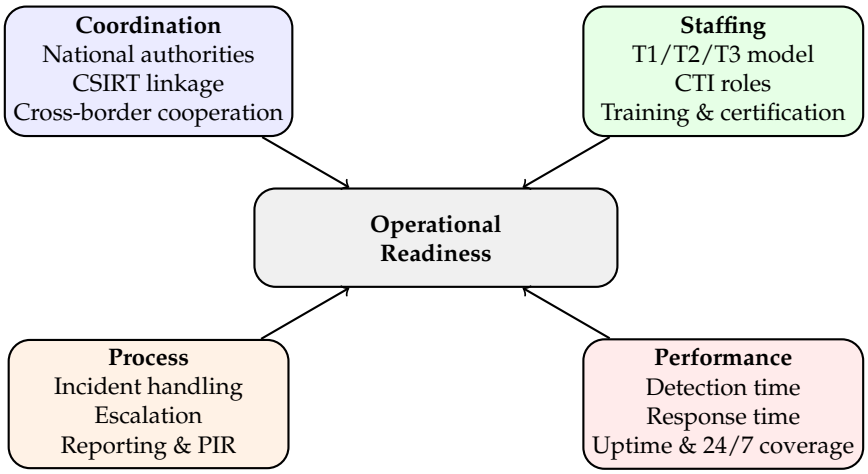


**Figure 3.** Operational readiness dimensions for advanced SOC environments.

These issues become even more important in national and defence-grade environments, where the baseline is expected to be higher than in a typical enterprise SOC. Security zoning, data separation, cross-domain protection, zero trust access control, role-based access control, multi-factor authentication, and microsegmentation should all be treated as baseline design requirements. It is also important to preserve analyst actions in tamper-evident logs, including which alerts were raised, which tools were used, and which actions were taken. This supports both auditability and evidentiary value. The need becomes stronger when the SOC supports both classified and unclassified systems, or when later incident reconstruction may be required [27,39]. A next-generation SOC should also support multi-stakeholder coordination, since incidents in critical infrastructures are rarely limited to one team or one institution. In multi-party, cross-sector, and cross-border incidents, the SOC should enable secure communication with national competent authorities, national CSIRTs, and sectoral supervisory authorities. It should also support coordinated incident handling and escalation to national authorities when needed. In cross-border cases, this also depends on alignment in threat intelligence exchange, reporting, and coordinated response practices [25,26]. In this sense, interoperability should be treated as part of resilience rather than as a purely technical capability.

Human factors of SOCs include role separation, incident escalation, periodic training, and sustainable 24/7 coverage. SOCs often have tiered analyst teams, with tier 1 analysts reviewing and validating alerts. Tier 2 analysts investigate, scope, and assist with containing incidents. Tier 3 analysts focus on threat hunting, forensics, advanced analytics, and complex response. CTI analysts and SOC managers provide the intelligence and governance functions needed for operational maturity. Training should not be occasional. Cyber range exercises, ATT&CK-aligned scenarios, standards-based simulations, and post-incident learning loops should be used to maintain readiness under different threat conditions [35,38]. Service-level performance, such as detection time, response time, platform availability, and analyst actions, should also be defined as operational requirements. Critical incidents should be detected within short and realistic time windows. Response workflows should start within thresholds defined by severity. Core SOC platforms should provide high availability and reliable failover capabilities. These are not only performance metrics. They are also resilience requirements. The weaker the visibility, detection, or escalation process, the longer adversaries can remain undetected and the greater the resulting impact. Therefore, architecture, staffing, processes, and governance should be treated as interconnected parts of one operational system.

 doi:10.20944/preprints202605.0201.v1



Table 3 gives the main requirement areas discussed in this subsection and shows the shift from baseline SOC functions to next-generation resilience-oriented SOC environments. Overall, a future-ready SOC for critical infrastructures should move beyond fragmented monitoring and reactive alert handling. It should provide continuous visibility, intelligence-informed analysis, orchestrated response, strict operational control, trained personnel, and measurable service performance within a single resilience model. These requirements directly shape the conceptual next-generation SOC architecture presented in the next section.

**Table 3.** Technological and operational requirements for next-generation SOC environments.

| Requirement | Baseline SOC capability | Next-generation SOC capability | Operational value |
|---|---|---|---|
| Telemetry & monitoring | Endpoint and network monitoring with centralized log collection | Continuous telemetry fusion across IT, OT, cloud, and field assets with protocol-aware visibility | Stronger situational awareness and reduced blind spots |
| Threat intelligence | Feed ingestion and basic IoC matching | Multilayer CTI fusion, ATT&CK mapping, automated enrichment, and contextual prioritization | Faster and more accurate triage |
| Analytics & threat hunting | Rule-based detection and limited anomaly analysis | UEBA, proactive threat hunting, malware analysis, and AI-assisted analytics with AML safeguards | Earlier detection of stealthy and adaptive attacks |
| Response & orchestration | Manual triage, analyst-driven escalation, and isolated response actions | SOAR-driven playbooks, API-based integrations, automated containment, and HITL control | Faster and more consistent incident handling |
| Defense-specific controls | Standard access control and routine logging | Security zoning, cross-domain protection, zero trust access, RBAC/MFA, and tamper-evident audit trails | Higher assurance for sensitive and classified environments |
| Asset visibility | Static inventories and manual asset discovery | Dynamic asset tracking across IT, OT, and hybrid cloud with shadow asset discovery | Better exposure awareness and prioritization |
| Alert management | High alert volume and manual prioritization | Intelligent scoring, false-positive reduction, benign alert suppression, and contextual enrichment | Lower analyst fatigue and better alert quality |
| Staffing & readiness | Basic analyst coverage and conventional shift operation | Tiered analyst roles, CTI specialization, cyber range training, certification, and resilient 24/7 staffing | Higher operational maturity and continuity |
| Processes & procedures | Generic incident handling and limited procedural standardization | Standardized workflows, defined escalation thresholds, post-incident review, and auditable documentation | Better traceability, repeatability, and compliance |
| Service performance | Best-effort detection and response | Defined targets for detection time, response time, uptime, and KPI tracking | Measurable and resilience-oriented SOC performance |

## 4. Next-Gen SOC Conceptual Architecture

The conceptual architecture of the proposed next generation SOC is illustrated in Figure 4. It is formed by the intelligent SOC layer that integrates with the Core SOC layer, in order to 1) receive information about local and remote monitoring, and 2) provide the raw internal data upon which the rest of the components operate. These will holistically cover network and compute assets, through endpoint and network monitoring and protection technologies (e.g., host-level EDR, anti-malware, host and network log aggregation tools, network intrusion detection and NDR). The components of the Next Generation SOC architecture forming an intelligent SOC layer are:

 doi:10.20944/preprints202605.0201.v1



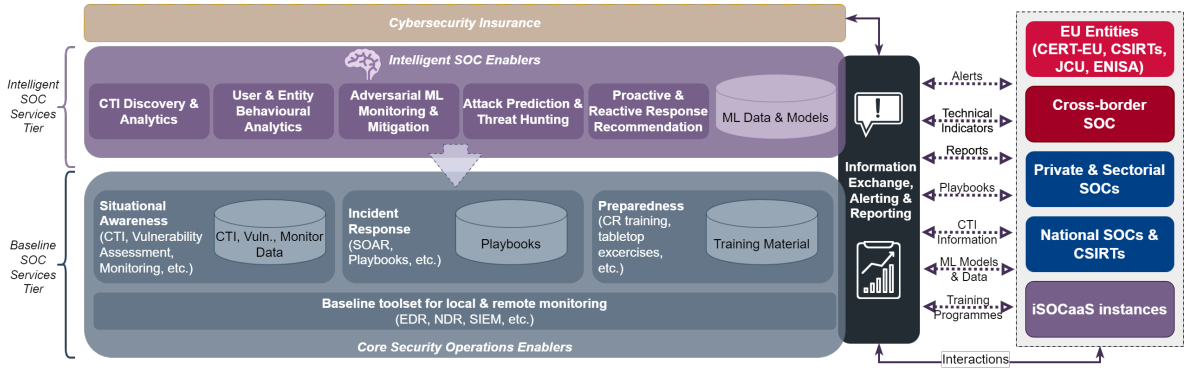


**Figure 4.** Next Generation Security Operation Center architecture

1. **Cyber Threat Intelligence (CTI) Discovery and Analytics**: This component leverages the capabilities of emerging AI models, to extend the breadth, depth and freshness of CTI information, including Large Language Models (LLMs) will be leveraged to provide CTI Discovery and Analytics capacities. The adoption of well-known LLMs, such as LlaMA 2 [40] and Bloom, will overcome the struggle of traditional Natural Language Processing (NLP) methods, such as TF-IDF [41], allowing the handling the intricacy of text data from diverse data sources and their complex interrelationships paving the way for more efficient CTI contextualization and sentiment analysis for the identification, extraction, and classification of security-related indicators and attack predictions. Moreover, the novel method of Retrieval Augmented Generation (RAG) will be investigated and deployed along with the generation-based models (i.e., LLMs) to enhance their context understanding (i.e., overcome the limitation of comprehend new context apart from the context they have been trained on) and improve the retrieving of relevant information from large knowledge bases. In particular, the LLMs text classification abilities will be leveraged to classify the CTI information, which will be collected from heterogeneous, unstructured (e.g., human readable) threat intelligence sources (such as dark web, social media, blogs, articles), structuring them based on the STIX domain object categories (e.g., attack pattern, campaign, course of action, etc.). This text classification is a complex task that cannot be effectively performed using traditional NLP methods; thus, with the employment of LLMs empowered with RAG methods, this module will contribute to the overall improvement the SOTA in CTI discovery and analytics.
2. **User and Entity Behavioral Analytics (UEBA)**: This component uses pseudonymized user data for training the system's AutoML module, and user behavior analytics will be handled as ML tasks. Subsequently, the generated models will be applied to forecast fresh data or assess the model's efficiency. Periodic comparisons of model performance and data validity will also be carried out. There will be an integrated statistics module including informative, summary, and inferential statistical approaches in addition to the machine learning portion. Additionally, the MLFlow framework will provide version control and metadata information storage for every analysis. A similar approach will be utilized for entity behavior analytics, or device behavior analytics. However, depending on the nuances of the device (data type and volume, interaction patterns, etc.), various AI techniques (ML, Federated Learning, Statistical Analysis, etc.) will be investigated through the in order to determine the best method for characterizing the behavior of the particular device (or device type, if clustering is relevant). The objective is to create a suitable and distributable behavioral profile that may serve as a starting point for UEBA device monitoring across different deployment scenarios
3. **Adversarial Machine Learning Monitoring and Mitigation**: This component allows to: (i) detect threats and vulnerabilities in AI systems, exploiting the information provided in publicly available sources, such as MITRE ATLAS and OWASP Machine Learning Security Top Ten and (ii) detect AML attacks (Figure 5). The ensemble learning model will be pre-trained combining the outputs of the CTI Discovery and Analytics with heterogeneous data sources (i.e., MITRE ATLAS, dark web, social media, etc.) augmented with adversarial examples powered from well-known

 doi:10.20944/preprints202605.0201.v1



AML attacks (e.g., JSMA, FGSM, and DeepFool [42]) based on widely recognized tools, such as Adversarial Robustness Toolbox and CleverHans [43]. Moreover, the pre-trained models will be fine-tuned using de-anonymized data from the organizations in which the component is implemented to identify fluctuations in the deployed training data. The outputs of this component will be exploited by the Attack Prediction and Threat Hunting to further investigate whether the detected threats, vulnerabilities, and Adversarial ML attacks are related to an APT that during its operation it compromises AI systems as well as by the core SOC enablers (i.e., Situational Awareness) to offer vulnerability detection capabilities and security assurance assessments specifically for AI systems.

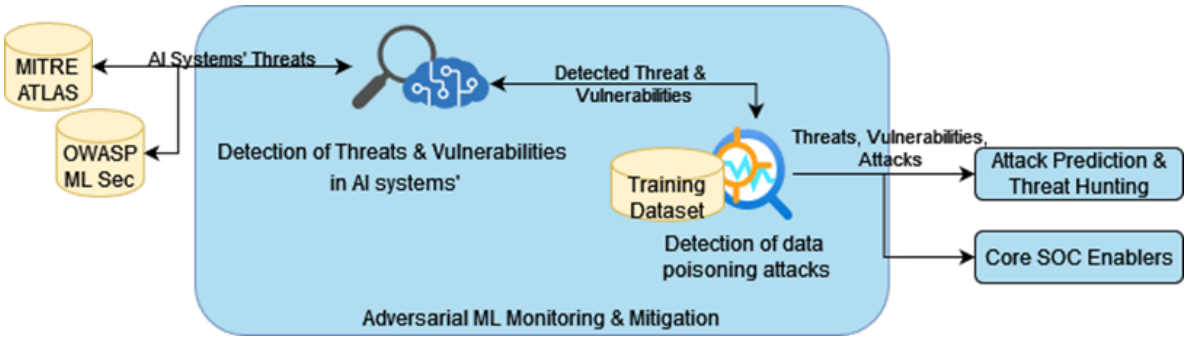


**Figure 5.** Adversarial ML Monitoring and Mitigation component

4. **Attack Prediction and Threat Hunting**: This component combines the outputs of the Baseline toolkit along with the thorough threat landscape information that will be obtained from the Situational Awareness components (core and AI-based) to identify most probable and most impactful potential attacks, to inform control implementation and prioritization as well as to drive proactive threat hunting in a cost-effective way (Figure 6). This is achieved through an ML-assisted threat hunting approach that will unfold in two steps. The first step will act as a pre-filtering mechanism leveraging the power of semi-supervised learning to construct a data-driven anomaly detection model that will perform an initial filtering of the organization's network traffic and log files (acquired from the baseline tools and situational awareness core SOC services) to suspicious in case that it has been identified an event related an APT activity or benign in case that it has not. The anomaly detection model will be originally trained using data from publicly available sources which contain network activity or log files of sophisticated and prominent attacks and APTs (e.g., malware-traffic-analysis.net[1], APT-Malware[2]). Later, the second step will be triggered in case that the anomaly detection system flags an event as suspicious, this event will be further examined using the KESTREL language [44] to provide a more thorough analysis. The major benefit of the Attack Prediction and Threat Hunting component is that it minimizes the manual intervention of security analysts in the threat hunting process, which is widely known that it is a severe and time-consuming procedure, enhancing also the efficacy compared to traditional human-driven threat hunting. The output of this component (i.e., predicted APT attacks) is employed by the *Proactive and Reactive Response Recommendation* component to facilitate both proactive (by indicating the exact location of the incident) and reactive response recommendation processes (by identifying threats before an incident occurs). The Attack Prediction and Threat Hunting will overall improve the capabilities of the Situational Awareness and Incident Response core SOC enablers by limiting the manual intervention in the threat identification and analysis processes exploiting the method of semi-supervised learning.

[1] https://malware-traffic-analysis.net/
[2] https://github.com/cyber-research/APTMalware

 doi:10.20944/preprints202605.0201.v1



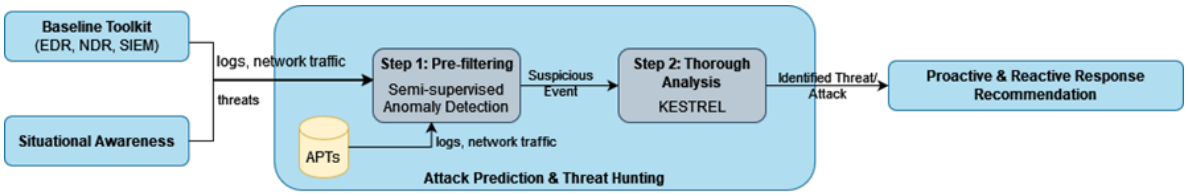


**Figure 6.** Attack Prediction and Threat Hunting module

5. **Proactive and Reactive Response Recommendation**: This component constitutes a Decision Support System (DSS) that considers outputs of other components (e.g., monitoring, vulnerability and penetration testing, risk assessments, CTI, attack predictions) and the list of known mitigation actions (from relevant knowledge bases, such as MITRE ATT&CK Enterprise[3] and ICS[4], ATLAS[5] and D3FEND[6]), to recommend - or even directly trigger, if needed - the most appropriate of the available courses of actions, as encoded in the relevant Playbooks. The playbook categories that are used include : a) Prevention Playbooks (e.g., specifying actions to prevent a threat from materializing), b) Assessment Playbooks (e.g., to automate vulnerability assessments), c) Detection Playbooks (e.g., automating monitoring for specific Indicators of Compromise (IoCs) that are received through the *CTI Discovery and Analytics* component), d) Mitigation Playbooks (e.g., encoding actions that mitigate the effects of a security incident, such as isolating an offending host), e) Remediation Playbooks (e.g., encoding steps to return affected systems to a good operating state), f) Investigation Playbooks (e.g., encoding post-incident analysis orchestration steps, to investigate how and why the incident took place), and g) Business Continuity playbooks (e.g., encoding the workflow to be followed for the activation of a business continuity plan).

Aside from these components the Next Generation SOC architecture also includes a additional component for *Information Exchange, Alerting and Reporting* which, essentially, facilitates the transition to shared situational awareness, coordinated incident response and joint preparedness amongst EU's cyber-defenders. To that end, this component includes the mechanisms and processes for information exchange with third parties (e.g., other SOCs, CSIRTs, National, Cross-border and EU-level actors), covering exchanges during day-to-day SOC operations (e.g., CTI information), periodic exchanges (e.g., periodic reports to National Authorities), as well as time-sensitive information (e.g., alerts, reports) exchanged in the case of cyber incidents. It will also support incident reporting in the various formats required by the different frameworks (e.g., NIS/NIS2, CyCLONe, GDPR), to be sent to the relevant Authorities and bodies. Overall, the trustworthy, privacy-aware and sanitized exchange of the following information is supported:

- time-sensitive (e.g., early warning) alerts
- technical indicators (e.g., IoCs)
- structured reports (e.g., CyCLONe or in national formats)
- sanitized CACAO playbooks of all types
- CTI information of all levels (including CTI discovered and enriched through the service's intelligent enablers)
- re-usable, pre-trained ML models and anonymized data (for ML training) from the intelligent SOC architecture components
- training material for preparedness against different types of cyber-attacks

A key consideration in this subsystem is the provision of an implementation that satisfies the most recent European mandates for coordinated response and the eventual interlinking of relevant

[3] https://attack.mitre.org/matrices/enterprise/
[4] https://attack.mitre.org/matrices/ics/
[5] https://atlas.mitre.org/
[6] https://d3fend.mitre.org/

 doi:10.20944/preprints202605.0201.v1



EU-level parties at the strategic and political level, as well as cybersecurity incident response actors (CSIRTs network, ENISA, NIS CG, CyCLONe) and other third parties (e.g., private entities).

## 5. Conclusions and Future Work

Over the last years, Critical National Infrastructures (CNIs) have experienced rapid digitization. While this has advanced the offered services to the citizens, it has also expanded the potential attack surface of CNIs. This problem is further enhanced by the rise of Artificial Intelligence (AI), which enables adversaries to launch sophisticated, targeted strikes against critical systems. While current regulatory frameworks like NIS2 and the Cyber Resilience Act (CRA) focus on the need for the deployment of more sophisticated Security Operation Centers (SOCs), traditional SOC models often fall short. They often lack the capability to coordinate detection and response actions and remain reactive, leaving systems vulnerable against zero-day attacks. To address these problems, the current paper introduces novel Next-Generation SOC services. The proposed framework automates the orchestration of the incident lifecycle, making it able to mitigate complex attacks while implementing proactive measures to defend against zero-day attacks.

**Funding:** The authors would like to acknowledge the financial support provided for the following project: 'Intelligent, Managed Security Operation Centre Services for Sectorial, National & Cross-border Cyber Resilience' (iSOCaaS) project, which has received funding from the European Union's Digital Europe Programme (DEP) programme under grant agreement No 101190388. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above mentioned projects.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Mikac, R. Protection of the EU's critical infrastructures: Results and challenges. *Applied cybersecurity & internet governance* **2023**, *2*, 1–25.
2. Osei-Kyei, R.; Tam, V.; Ma, M.; Mashiri, F. Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction* **2021**, *60*, 102316.
3. Lehto, M. Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection*; Springer, 2022; pp. 3–42.
4. Moradpoor, N.; Abah, E.; Robles-Durazno, A.; Maglaras, L. Adversarial Attacks on Supervised Energy-Based Anomaly Detection in Clean Water Systems. *Electronics* **2025**, *14*, 639.
5. Lekidis, A.; Karalashvili, M.; Maglaras, L.; Karantzalos, K.; Spanoudakis, G. Intelligent Security Operation Centre Services for Critical National Infrastructures. In Proceedings of the 2025 IEEE Conference on Communications and Network Security (CNS). IEEE, 2025, pp. 1–2.
6. Nautiyal, N.S.; Mardonov, A. Emerging threats in aviation: A study of recent cyber and hybrid attacks on global airports. *Journal of Transportation Security* **2026**, *19*, 18.
7. Lehto, M. National Cyber Space. In *Cyber Security: Policy and Technology*; Springer, 2026; pp. 3–37.
8. Möller, D.P. Application Domain Network and Information Security (NIS2). In *Cybersecurity for Network and Information Security: Principles, Techniques and Applications*; Springer, 2026; pp. 217–252.
9. Maglaras, L.; Janicke, H.; Ferrag, M.A. Combining security and reliability of critical infrastructures: The concept of securability, 2022.
10. Sotiropoulos, L. The European Cybersecurity Framework: Challenges, Legal Aspects and Regulations. In *Digital Lawscapes: Artificial Intelligence, Cybersecurity and the New European Order*; ADJURIS–International Academic Publisher, 2025; pp. 57–71.
11. Narra, S.L. The Future of Endpoint Security: Autonomous Agents and Self-Healing Systems. *Journal Of Multidisciplinary* **2025**, *5*, 109–117.
12. Stephens, G. Cybercrime in the year 2025. *Futurist* **2008**, *42*, 32.

 doi:10.20944/preprints202605.0201.v1




13. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024, 2024. Accessed: 2026-03-24.
14. European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng, 2022. Accessed: 2026-03-24.
15. Vandezande, N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review* **2024**, *52*, 105890.
16. Singh, C. The European Approach to Cybersecurity in 2023: A Review of the Changes Brought in by the Network and Information Security 2 (NIS2) Directive 2022/2555. *International Company and Commercial Law Review* **2023**, *5*, 251–261.
17. European Union. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng, 2022. Accessed: 2026-03-24.
18. European Union. Commission Delegated Regulation (EU) 2024/1366 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows. https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng, 2024. Accessed: 2026-03-24.
19. Smeets, M.; van Loon, G.; Shires, J.; Rolland, A. Under Pressure: Securing Europe's Resource-Constrained Critical Infrastructure. https://virtual-routes.org/under-pressure-securing-europes-resource-constrained-critical-infrastructure/, 2025. Accessed: 2026-03-24.
20. European Commission. European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers. https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en, 2025. Accessed: 2026-03-24.
21. Neumannová, A.; Bernroider, E.W.; Elshuber, C. The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review. In Proceedings of the European, Mediterranean, and Middle Eastern Conference on Information Systems. Springer, 2022, pp. 570–585.
22. European Insurance and Occupational Pensions Authority (EIOPA). Digital Operational Resilience Act (DORA). https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en, 2025. Accessed: 2026-03-24.
23. Yigit, Y.; Canberk, B. Graph-Based Digital Twin Blueprint for Securing 6G Local Area Networks. *IEEE Wireless Communications* **2025**, *32*, 51–58. https://doi.org/10.1109/MWC.2025.3602932.
24. Kalliola, M.; Huovila, M.; Lindroth, M. Towards Safer Healthcare: Insights on the European Action Plan on Cybersecurity for Hospitals and Healthcare Providers. Working Paper 39, Sitra, Helsinki, 2025.
25. European Commission. EU Cyber Solidarity Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity, 2025. Accessed: 2026-03-24.
26. Villani, S. The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System. *European Journal of Risk Regulation* **2025**, pp. 1–13.
27. European Union. Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng, 2022. Accessed: 2026-04-01.
28. Dragomir, A.V. What's New In The NIS 2 Directive Proposal Compared To The Old NIS Directive. *SEA – Practical Application of Science* **2021**, *9*, 155–162.
29. European Commission and High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication to strengthen the security and resilience of submarine cables. https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables, 2025. Accessed: 2026-04-01.
30. European Commission. European Water Resilience Strategy. https://environment.ec.europa.eu/publications/european-water-resilience-strategy_en, 2025. Accessed: 2026-04-01.
31. European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679, 2016. Accessed: 2026-04-01.
32. European Union. Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act). https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng, 2019. Accessed: 2026-04-01.
33. European Union Agency for Cybersecurity (ENISA). EUCC in Application. https://certification.enisa.europa.eu/news/eucc-application-2025-02-27_en, 2025. Accessed: 2026-03-24.
34. European Union. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng, 2024. Accessed: 2026-04-01.

 doi:10.20944/preprints202605.0201.v1




35. MITRE. MITRE ATT&CK Framework. https://attack.mitre.org/, 2025. Accessed: 2026-04-01.
36. MITRE. MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems. https://atlas.mitre.org/, 2025. Accessed: 2026-04-01.
37. OWASP Foundation. OWASP Top 10 for Large Language Model Applications and Machine Learning Security Guidance. https://owasp.org/www-project-top-10-for-large-language-model-applications/, 2025. Accessed: 2026-04-01.
38. National Institute of Standards and Technology. Computer Security Incident Handling Guide (SP 800-61 Rev. 2). https://csrc.nist.gov/pubs/sp/800/61/r2/final, 2012. Accessed: 2026-04-01.
39. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. https://www.nist.gov/cyberframework, 2024. Accessed: 2026-04-01.
40. Touvron, H.; Martin, L.; Stone, K.; Albert, P.; Almahairi, A.; Babaei, Y.; Bashlykov, N.; Batra, S.; Bhargava, P.; Bhosale, S.; et al. Llama 2: Open foundation and fine-tuned chat models. *arXiv preprint arXiv:2307.09288* **2023**.
41. Guleria, P.; Frnda, J.; Srinivasu, P.N. NLP based text classification using TF-IDF enabled fine-tuned long short-term memory: An empirical analysis. *Array* **2025**, p. 100467.
42. Mihaylova, D.A. Baseline Adversarial Machine Learning Attacks-a Comparative Study. In Proceedings of the 2025 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST). IEEE, 2025, pp. 1–4.
43. Agarwal, A.; Nene, M.J. Advancing trustworthy ai: A comparative evaluation of ai robustness toolboxes. *SN Computer Science* **2025**, *6*, 234.
44. Ebden, P.; Sproat, R. The Kestrel TTS text normalization system. *Natural Language Engineering* **2015**, *21*, 333–353.