



A Data-Center Protection System Based on a Security Operations Center (SOC): A Comparative Architectural Framework and Performance-Indicator Analysis

Dr. Ghedar Alrefai

Associate professor at the Dept. Information and Communication Engineering, Faculty of Engineering, EBLA Private University and Lecturer at Cordoba Private University, Syria

ARTICLE INFO

KEYWORDS

security operations center; data-center protection; SIEM; SOAR; zero trust; SOC maturity; NIST CSF 2.0.

HOW TO CITE

Alrefai, D. G. (2026). A Data-Center Protection System Based on a Security Operations Center (SOC): A Comparative Architectural Framework and Performance-Indicator Analysis. International Journal of Information & Digital Security, 4(2), 22-39.

<https://doi.org/10.54878/tq4szd72>

ABSTRACT

Data centers have become a critical node of the digital economy, hosting identity systems, cloud services, business applications, and facility-operation technologies. As the attack surface expands and workloads migrate to hybrid and multi-cloud environments, perimeter-only controls are no longer sufficient. This study examines the Security Operations Center (SOC) as an operational protection system for data centers rather than a mere collection of monitoring tools. The research follows a comparative analytical method that synthesizes peer-reviewed literature published from 2020 onward, official industry and agency reports (IBM, Verizon, ENISA, and Uptime Institute), and authoritative frameworks (NIST CSF 2.0, NIST SP 800-61r3, ISO/IEC 27001:2022, ISO/IEC 27035:2023, and the NIS 2 Directive). The evidence shows that the global average cost of a data breach was USD 4.44 million in IBM's 2025 report and rose to USD 4.99 million in the 2026 report, while mean time to identify and contain fell to 241 days; ransomware appeared in 44% of breaches analyzed by Verizon in 2025; and distributed denial-of-service remains the most frequently observed threat in the European landscape. The paper proposes a six-layer DC-SOC model that integrates cyber telemetry with cyber-physical facility signals (BMS/OT) and risk-based governance. Effectiveness, the study concludes, is not achieved by procuring a single platform, but by balancing people, process, and technology and by measuring maturity through MTTD, MTTR, and analysis quality rather than raw alert volume.



Double-blind peer review by independent reviewers.

Received: 02 Jul 2026, Accepted: 11 Nov 2026, Published: 06 Dec 2026

*Corresponding author: ghedar.refai@ebla.edu.sy

Copyright: © 2026 by the author. Licensee Emirates Scholar Center for Research & Studies, UAE.

Open access under the Creative Commons Attribution (CC BY) license

<https://creativecommons.org/licenses/by/4.0>

1. Introduction

Data centers constitute the silent infrastructure on which governmental, financial, healthcare, and commercial services depend. Any disruption of their availability, or of the confidentiality of the assets they host, is no longer a local technical incident; it rapidly becomes a financial loss, a regulatory exposure, and a public-trust failure. Recent reports document that the global average cost of a data breach reached USD 4.44 million in 2025, while the identify-and-contain lifecycle declined to 241 days, the lowest level in nine years [4]. IBM's 2026 report, however, recorded a return to USD 4.99 million, with AI-enabled attacks concentrating on critical-infrastructure sectors [5].

At the same time, Verizon's 2025 Data Breach Investigations Report analyzed 22,052 security incidents, including 12,195 confirmed breaches across 139 countries. Vulnerability exploitation accounted for 20% of breaches, third-party relationships contributed to approximately 30%, and ransomware appeared in 44% of cases [6]. At the European level, the ENISA Threat Landscape 2024 observed more than eleven thousand incidents, with distributed denial-of-service (DDoS) and ransomware dominating the landscape [7]. The 2025 edition confirmed the continued predominance of DDoS, at approximately 76.7% of recorded cases in the European sample [8].

Against this background, the Security Operations Center has emerged as the organizational and technical unit that unifies monitoring, detection, response, and continuous improvement in a single cycle. Peer-reviewed literature has long warned against reducing the SOC to a technology platform. Vielberth, Böhm, Fichtinger, and Pernul showed that academic research has tended to emphasize people and technology while neglecting the non-technical processes that bind them [1]. Subsequent studies have demonstrated that alert fatigue, high rates of non-actionable alarms, and inconsistent analyst-performance metrics remain structural barriers to SOC effectiveness [13][14][15].

The problem becomes more complex when the protected object is a data center rather than a conventional enterprise network. A data center combines information-technology assets, facility operational technology (power, cooling, building-management systems, and physical access control), multi-cloud connectivity, and edge devices. The Uptime Institute 2025 security survey reported that most operators experienced a cyber incident during the observation window, that fewer than half maintain a dedicated cybersecurity team, and that the most impactful incidents began to exceed USD 50 million [19].

1.1 Research problem

The research problem is dual. The first gap is epistemic: many studies still treat the SOC as a generic construct without sufficient specialization for the cyber-physical character of data centers. The second gap is operational: organizations procure monitoring platforms without securing an operating model, performance indicators, or telemetry integration from facility systems and cloud services. The result is prolonged dwell time, alert inflation, and weak demonstrability of compliance with contemporary frameworks such as NIST CSF 2.0 and the NIS 2 Directive [2][18].

1.2 Objectives and research questions

The study pursues four interrelated objectives:

- First, to analyze the contemporary threat landscape of data centers using verifiable official sources.
- Second, to compare SOC operating models, technical platforms, and normative frameworks in a systematic manner.
- Third, to propose an architectural framework, termed DC-SOC, suited to traditional and hybrid data centers.
- Fourth, to connect protection effectiveness to measurable performance indicators and an explicit maturity path.

The guiding questions are: which properties distinguish data-center protection from generic enterprise-network protection? Which operating model is most appropriate given scale and compliance constraints? How can cyber-physical telemetry be integrated without overwhelming analysts? And which indicators should be used to evaluate a SOC scientifically rather than commercially?

1.3 Significance and scope

The significance of the study lies in combining three levels that are rarely treated together: the statistical level of threat and cost, the normative level of international frameworks, and the architectural level of a protection system specialized for data centers. Its principal limitation is methodological. The paper does not claim a new field experiment inside a production data center; it offers a comparative synthesis of published evidence and a testable model for subsequent empirical work. References were restricted to authentic sources published in 2020 or later in order to preserve currency.

1.4 Organization of the paper

Section 2 reviews the literature. Section 3 presents the method. Section 4 analyzes the threat landscape and statistics. Section 5 explains the architectural construction of the SOC. Section 6 develops the comparisons. Section 7 proposes the DC-SOC model. Section 8 discusses performance indicators and analytical results. Section 9 offers the discussion, followed by recommendations and the conclusion.

2. Literature review and theoretical framework

2.1 The SOC concept and its triadic construction

A Security Operations Center may be defined as an organizational and technical unit that combines people, processes, and technologies to monitor a digital environment, detect incidents, respond to them, and continuously improve controls [1]. The systematic review by Vielberth, Böhm, Fichtinger, and Pernul concluded that the absence of a generally accepted holistic view has impeded innovation, and that the most notable gap lies in the processes that connect the analyst to the platform rather than in a shortage of tools [1]. Later work has confirmed that building a SOC is as much a problem of people, time, and procedural discipline as it is a procurement problem [17].

The conventional construction comprises three analytical tiers: a first-level analyst for rapid triage, a second-level analyst for deep investigation, and a third-level analyst or threat hunter for advanced patterns. This division is insufficient unless analyst functions and performance indicators are defined systematically. Agyepong and colleagues proposed a framework for measuring analyst performance based on analysis quality, report quality, time-based measures, and absolute task counts, and later developed the SOC-AAM method using a Delphi panel and the analytic hierarchy process [13].

2.2 Alert fatigue and alarm quality

Alarm quality is the operational bottleneck. Alahmadi, Axon, and Martinovic showed that practitioners describe very high rates of non-actionable alarms, and that much of what is labeled a false positive is in fact a “benign trigger”: a true signature match that reflects legitimate behavior in the environment [14]. Tariq, Baruwat Chhetri, Nepal, and Paris (2025) surveyed academic and industry work on alert fatigue, identified four major causes, and argued for mitigation through automation, augmentation, and human-AI collaboration [15]. The same team later proposed a human-AI teaming model

that reduces fatigue without displacing human judgment [24].

2.3 Governing frameworks

In February 2024, the U.S. National Institute of Standards and Technology released Cybersecurity Framework 2.0 and added a Govern function to the previous five, producing a six-function core: Govern, Identify, Protect, Detect, Respond, and Recover [2]. Revision 3 of Special Publication 800-61, finalized in April 2025, recast incident response as a CSF 2.0 Community Profile rather than as an isolated four-phase cycle [3]. This shift provides a scientific rationale for embedding the SOC in enterprise risk management instead of leaving it as a detached monitoring room.

Internationally, ISO/IEC 27001:2022 specifies requirements for an information security management system, and Annex A, together with ISO/IEC 27002:2022, provides a control set for continual improvement [10][23]. The ISO/IEC 27035:2023 series details incident-management principles, preparation, and lessons learned [11][12]. In the European Union, the NIS 2 Directive (Directive (EU) 2022/2555) raised obligations for essential and important entities, including digital infrastructure and data centers within critical value chains [18]. Zero Trust Architecture, as defined in NIST SP 800-207, moves the center of gravity from the network perimeter to continuous verification of identity, device, and context before every session [9].

2.4 The SOC in data-center and multi-cloud settings

da Silva, Costa, and Almeida emphasized that a SOC is not a one-size-fits-all solution and that infrastructure and operating-model choices should precede tool procurement, particularly under NIS-related obligations [17]. Bassey, Chinda, and Idowu presented a scalable architecture based on open-source tools (Wazuh, TheHive, and Suricata) and demonstrated detection of common scenarios such as brute force, malware, and denial of service [16]. Chamkar, Maleh, and Gherabi mapped use cases to coverage gaps against MITRE ATT&CK, arguing that SOC value should be measured by adversarial-behavior coverage rather than by the number of purchased rules [22][21].

NIST SP 800-53 Revision 5 supplies a detailed control catalog that can be projected onto SOC services, from continuous monitoring to incident response and audit logging [20]. The picture is completed by the Uptime Institute survey, which found that IT software and network-configuration issues remain leading causes of incidents, with patch management, default

configurations, and weak access-control separation recurring as direct causes [19]. The literature gap addressed by this paper is therefore clear: a protection model is needed that binds the SOC to cyber-physical data-center assets, not merely to the information-technology network.

3. Research method

The study adopts a multi-source comparative analytical design. No primary data were collected inside a named production data center. Results are instead built from a scientific synthesis of verifiable published evidence. This design was chosen because the research question is architectural and operational in nature, and because a comprehensive field experiment in a production facility would confront confidentiality and safety constraints. The contribution is therefore a comparative framework and a proposed model, not a randomized trial or a new laboratory measurement.

3.1 Data sources and inclusion criteria

Three classes of sources were included: (a) peer-reviewed journal and conference papers published between 2020 and 2026 in IEEE, ACM, USENIX, Elsevier, MDPI, and Dagstuhl venues; (b) normative publications issued by NIST, ISO/IEC, and the European Union; and (c) official reports with disclosed methods, namely IBM's Cost of a Data Breach Reports for 2025 and 2026, Verizon DBIR 2025, the ENISA Threat Landscape reports for 2024 and 2025, and the Uptime Institute Data Center Security Survey 2025. Undated sources, marketing reports that do not disclose sample size or collection method, and references earlier than 2020 were excluded, except where required to understand a standard that itself was published after that date.

3.2 Analytic procedure

Analysis proceeded in four stages. First, statistical facts were extracted as stated in the original sources, without re-estimation or interpolation. Second, operating models (in-house, hybrid, managed service) and platforms (SIEM, XDR, SOAR, NDR) were classified along six dimensions: visibility, time to capability, cost, privacy, 24/7 coverage, and business-context depth. Third, SOC functions were mapped onto the NIST CSF 2.0 functions and the NIST SP 800-61r3 cycle. Fourth, the proposed

DC-SOC model was composed as a normative-operational framework measurable through MTTD, MTTR, analysis quality, ATT&CK coverage, and maturity level. Scientific citation practice was observed by avoiding long verbatim extracts and by using numbered in-text references in the form [n].

3.3 Validity and scholarly integrity

Construct validity was strengthened by using independent sources for the same phenomenon whenever possible (for example, breach cost from IBM, breach structure from Verizon, and threat distribution from ENISA). Scholarly integrity was protected by distinguishing published facts from the author's analytical inferences. No experimental results were fabricated, and no percentage was altered. Replicability is achieved by retracing the references listed in APA 7 format.

4. Contemporary threat landscape and statistics

4.1 Breach economics and their implications for data centers

The IBM reports provide a quantitative window on the cost of late detection. In the 2025 report, the global average declined to USD 4.44 million from USD 4.88 million in 2024. The publisher attributed part of the decline to improved identification and containment assisted by artificial intelligence and automation, while the United States remained at USD 10.22 million and healthcare at USD 7.42 million despite a relative decrease [4]. The global average then rose to USD 4.99 million in the 2026 report. AI-enabled breaches cost approximately USD 6 million on average, whereas extensive use of AI and automation in security operations saved about USD 1.93 million per breach [5].

These figures have two direct implications for data centers. First, faster detection is not an operational luxury but an economic variable: mean time to identify and contain fell to 241 days, and extensive automation reduced the breach lifecycle by about 80 days [4]. Second, the larger saving is realized when automation is embedded in operations rather than purchased as an isolated tool. Figures 1, 2, and 12 display this quantitative relationship.

Figure 1. Global average cost of a data breach (IBM)

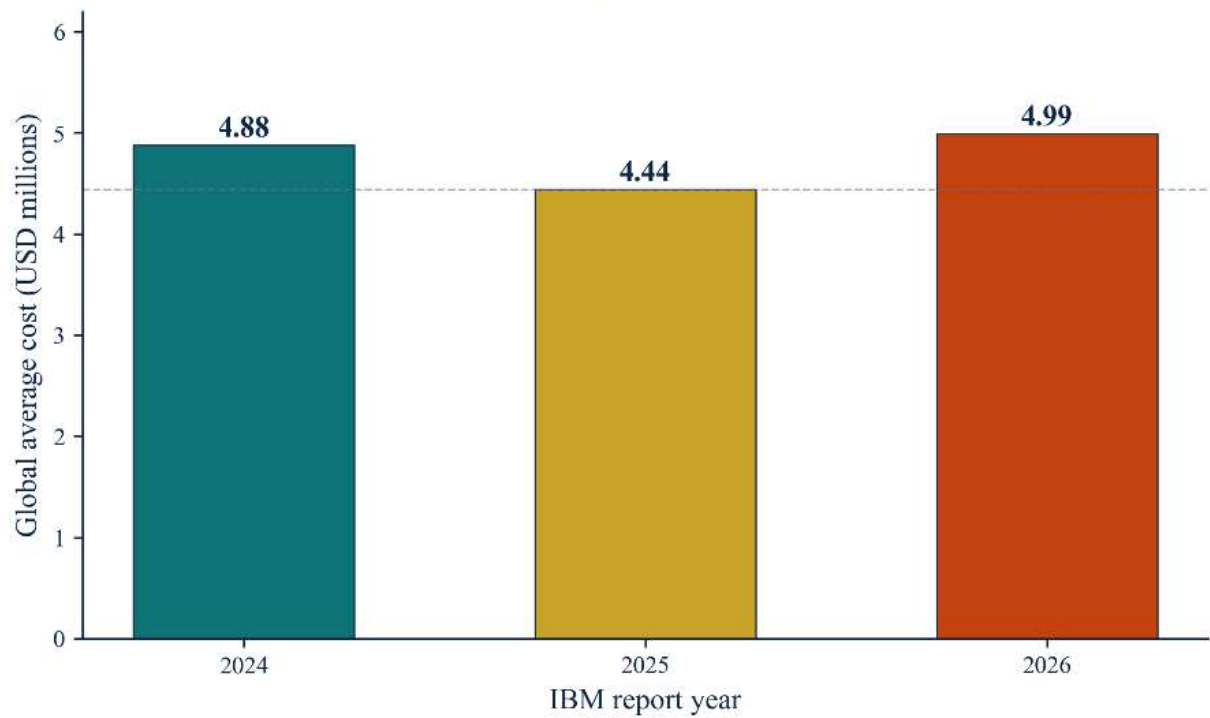


Figure 1. Global average cost of a data breach according to IBM reports, 2024–2026 [4][5]

Figure 2. Breach lifecycle and the effect of AI/automation (IBM 2025)

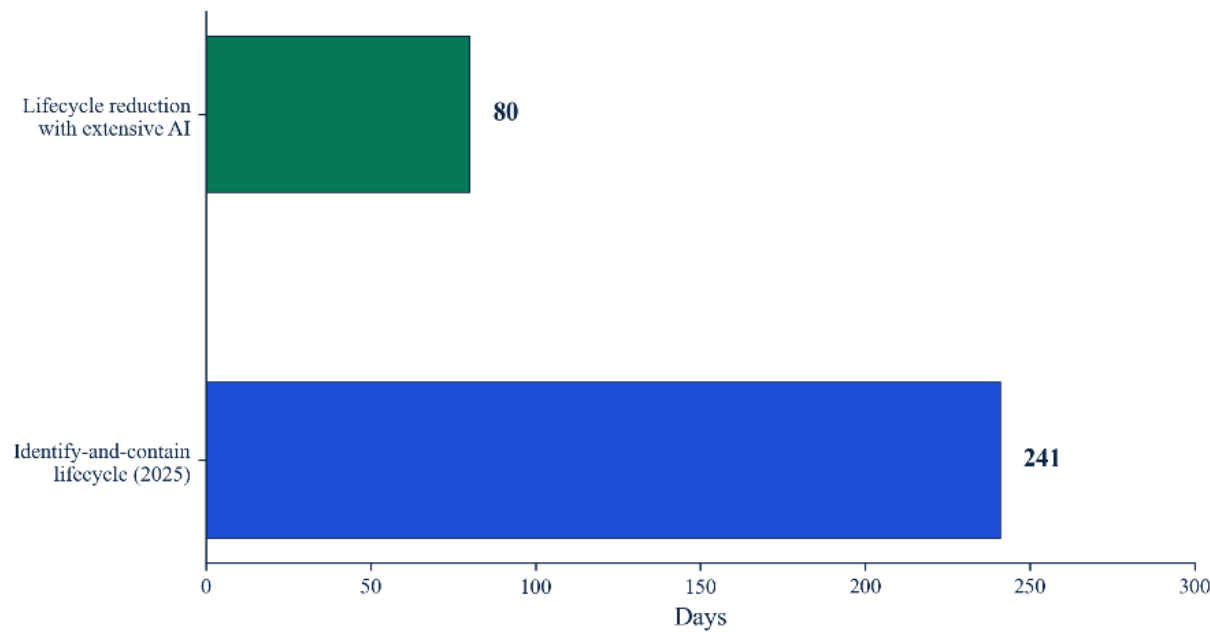


Figure 2. Breach lifecycle in days and the effect of automation according to IBM 2025 [4]

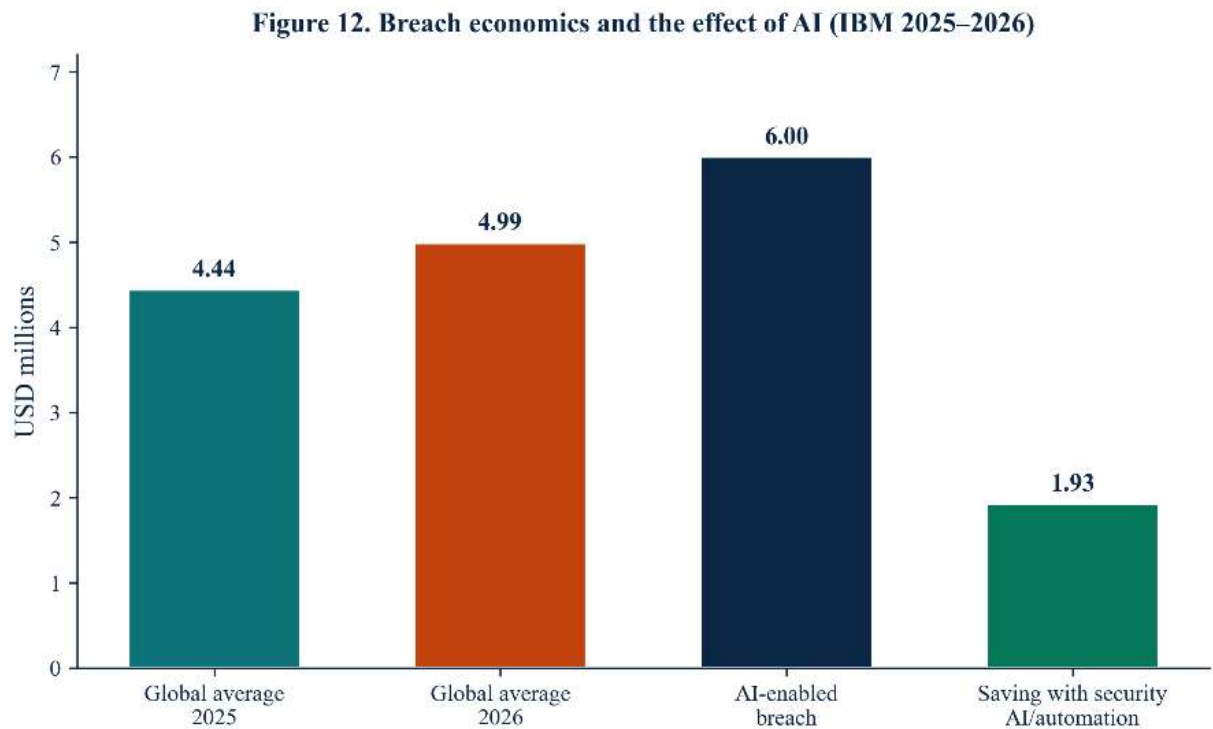


Figure 12. Breach economics and the effect of AI according to IBM 2025–2026 [4][5]

4.2 Breach structure according to Verizon DBIR 2025

If IBM answers the cost question, Verizon answers the how question. Credential abuse accounted for 22% of initial access; vulnerability exploitation rose to 20%; and edge devices and VPNs represented 22% of exploitation actions after growing nearly eightfold from the previous year. Median time to full remediation of those edge vulnerabilities was 32 days, and only about 54% were fully

remediated during the year [6]. Third-party breaches approximately doubled to 30%, the human element appeared in about 60% of cases, and ransomware was present in 44% [6].

Edge devices are especially significant for data centers because they form the boundary of customer, cloud, and supplier connectivity. Delay in patching a VPN concentrator or an application firewall converts the perimeter into a silent entry point. The doubling of third-party breaches likewise implies that a SOC that monitors only internal assets leaves the supply chain outside its field of view. Figure 3 summarizes these indicators.

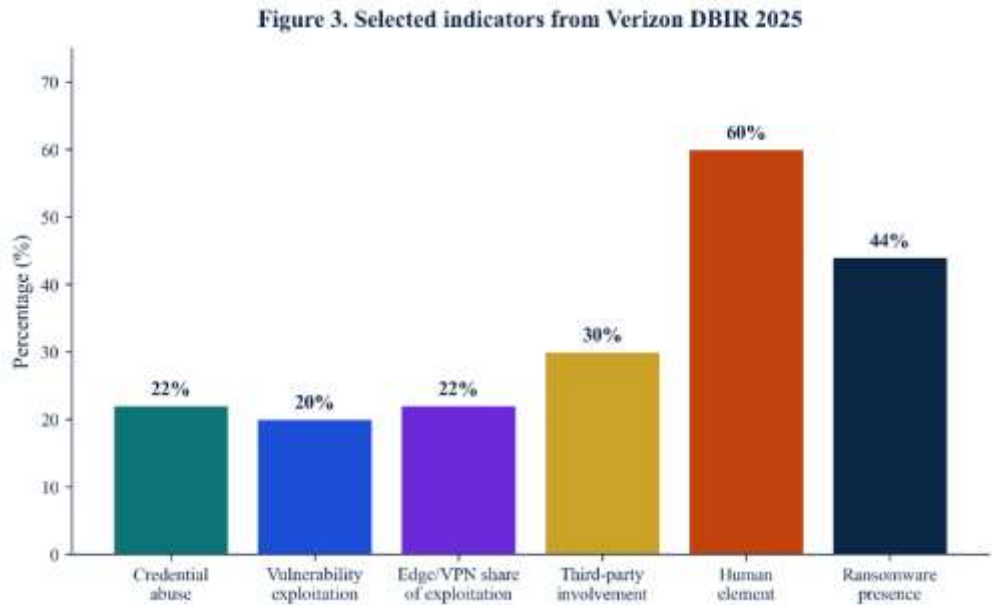


Figure 3. Selected indicators from the Verizon 2025 Data Breach Investigations Report [6]

4.3 The European landscape and the NIS 2 Directive

ENISA's 2024 report found that DDoS and ransomware together accounted for more than half of observed incidents. Public administration represented 33% of DDoS events, followed by transport (21%), banking (12%), and digital infrastructure (6%) [7]. Ransomware was relatively concentrated in business services (18%), manufacturing (17%), and health (8%) [7]. In the 2025 report, DDoS dominance rose to approximately 76.7% of recorded cases, intrusions accounted for 17.8%, and ransomware represented 81.1% of cybercrime activity within the sample [8].

Frequency does not equal destructiveness. DDoS is the most visible threat in open sources and is often driven by politically motivated groups, whereas intrusion and ransomware remain more damaging to data confidentiality and long-term service availability. NIS 2 imposes explicit risk-management, reporting, and response obligations on digital-infrastructure entities [18]. A data-center SOC is therefore no longer an optional improvement; it is simultaneously a compliance instrument and an operational capability. Figure 4 shows the DDoS distribution.

Figure 4. DDoS events by sector (ENISA 2024)

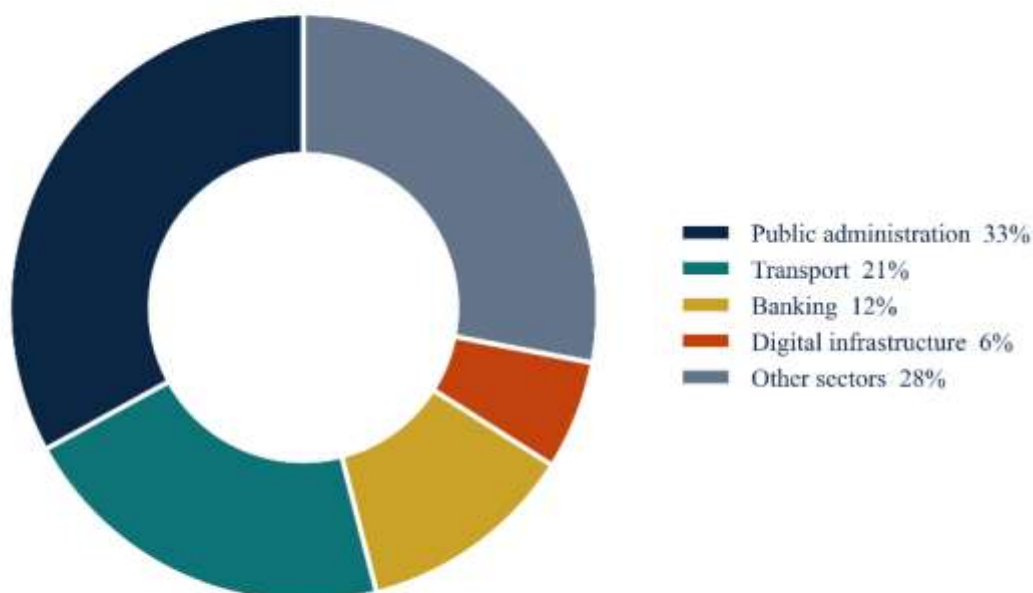


Figure 4. Distribution of DDoS events by sector according to ENISA 2024 [7]

4.4 Incident characteristics inside data centers

The Uptime Institute 2025 survey, with more than 980 respondents, found that most operators had experienced a cyber incident; that IT software and network-configuration issues lead the causes; and that 54% cited patch management, 38% default configurations, and 24% weak access-control separation as common causes of cybersecurity-related network incidents [19]. The survey also reported that 2025 was the first year in which some

operators stated that the cost of their most impactful incidents exceeded USD 50 million, and that fewer than half of operators have a dedicated cybersecurity team [19].

These findings indicate that data centers suffer a governance gap, not merely a hardware gap. The absence of a dedicated team means that signals from building-management systems, power-distribution units, or cooling plants may be treated as facility faults rather than as cyber-physical incidents. The model proposed in this study addresses that gap explicitly. Figure 5 ranks the causes.

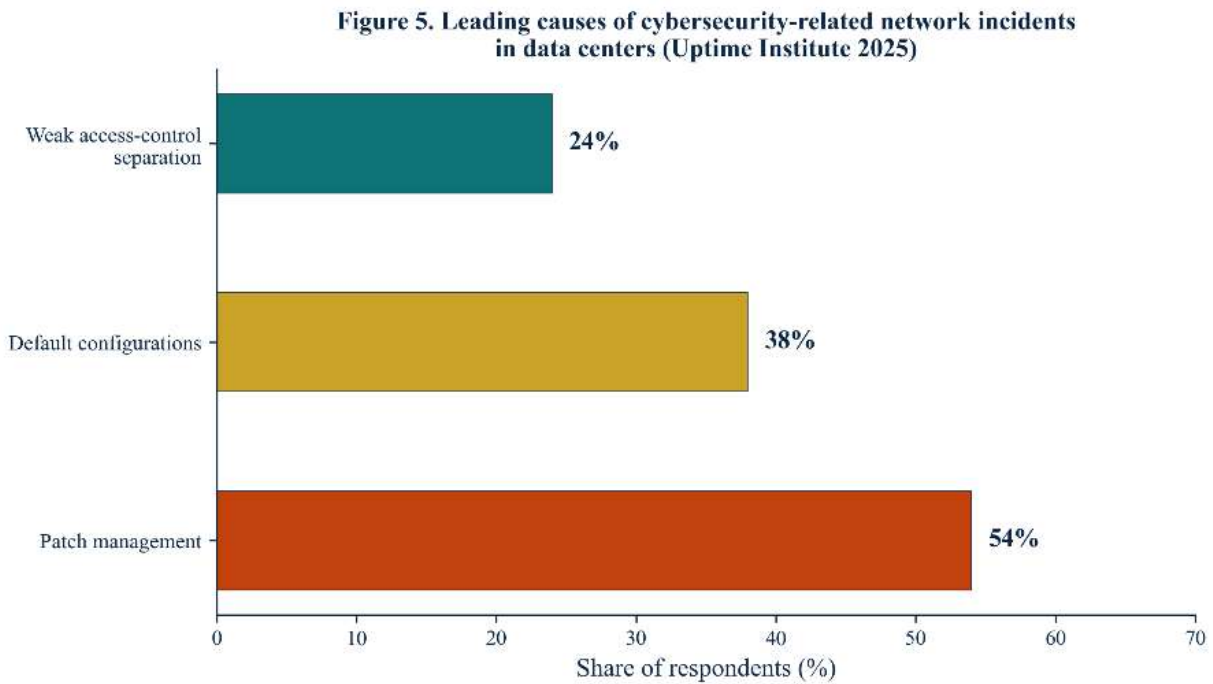


Figure 5. Leading causes of cybersecurity-related network incidents among data-center operators [19]

Table 1. Selected threat and cost indicators from official sources used in this study

Indicator	Value	Source
Global average breach cost, 2024	USD 4.88 million	IBM 2025 [4]
Global average breach cost, 2025	USD 4.44 million	IBM 2025 [4]
Global average breach cost, 2026	USD 4.99 million	IBM 2026 [5]
Mean time to identify and contain	241 days	IBM 2025 [4]
Saving from AI/automation	approx. USD 1.9–1.93 million	IBM 2025–2026 [4][5]
Incidents analyzed / confirmed breaches	22,052 / 12,195	Verizon 2025 [6]
Ransomware presence in breaches	44%	Verizon 2025 [6]
Third-party breaches	approx. 30%	Verizon 2025 [6]
Observed incidents (Europe, 2024)	11,079 incidents	ENISA 2024 [7]
DDoS share of 2025 EU sample	approx. 76.7%	ENISA 2025 [8]
Operators with a dedicated security team	fewer than half	Uptime Institute 2025 [19]

Table 1. Selected indicators from official reports (2024–2026)

5. Architectural construction of a SOC-based protection system

5.1 The SOC as a system, not a monitoring room

A SOC should be understood as a socio-technical system. Technology aggregates telemetry and generates hypotheses; process determines when an alert is escalated

to an incident; and people judge ambiguity and learn from cases. A defect in any one of the three sides degrades the other two: a context-poor tool exhausts the analyst, an undocumented process renders the tool ineffective, and a burned-out analyst ignores a valid signal [1][14][15].

In a data-center environment the system expands to a fourth layer: the physical-operational asset. Availability is not merely server uptime; it is continuity of power,

cooling, connectivity, and access control. Figure 6 therefore proposes a layered construction that begins with assets, then telemetry sources, platforms, processes,

and people, and terminates in governance aligned with the Govern function of NIST CSF 2.0 [2].

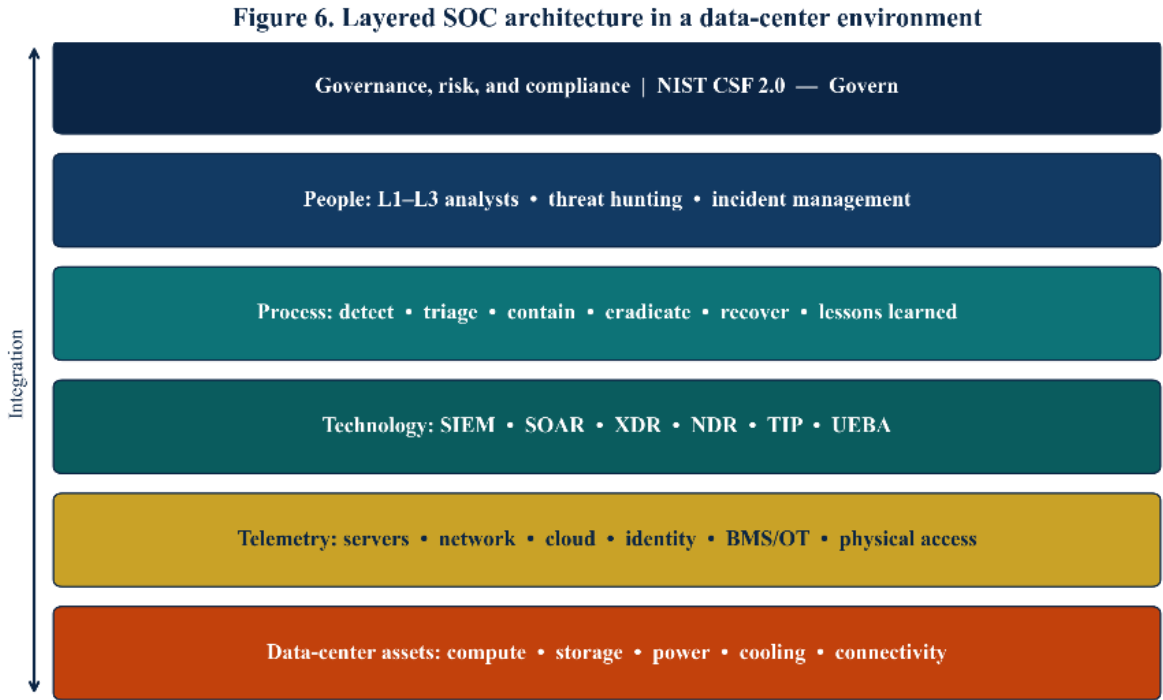


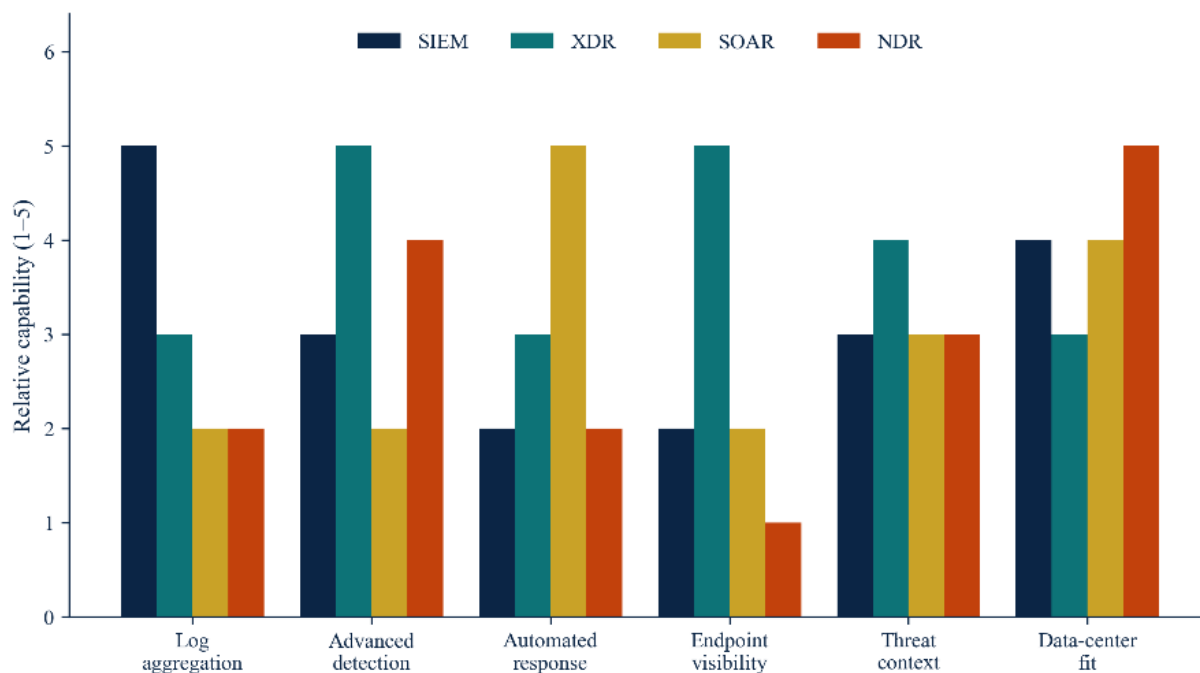
Figure 6. Layered SOC architecture in a data-center environment (author synthesis based on [1][2][19])

5.2 Technology layers: from log to decision

Security information and event management (SIEM) remains the backbone of log aggregation and historical correlation. Extended detection and response (XDR) widens visibility across endpoints, email, and identity. Security orchestration, automation, and response (SOAR) executes playbooks and reduces repetitive manual work. Network detection and response (NDR/NIDS) reveals patterns in flow and packets inside data centers, where host agents cannot be installed on

every asset [16][22]. The stack is completed by a threat-intelligence platform (TIP) and user and entity behavior analytics (UEBA).

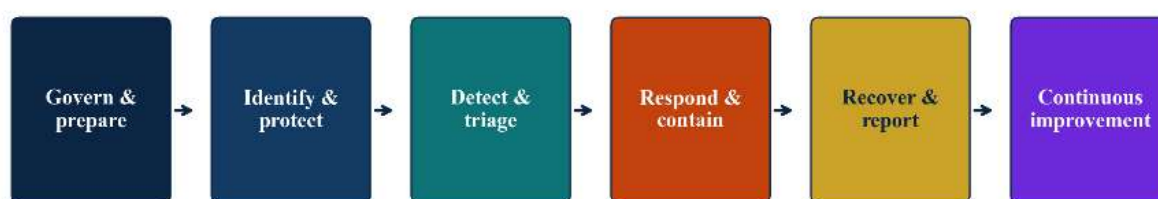
A multiplicity of platforms is itself a risk if the telemetry bus is not unified. The problem is rarely the absence of a product; it is the duplication of a single event in four incompatible formats. A data path should therefore be designed explicitly: collect, normalize, enrich with context (asset, owner, classification, ATT&CK mapping), correlate, then decide—humanly or through conditional automation [21][22]. Figure 9 shows that no platform dominates every dimension; integration is the rule, not the exception.

Figure 9. Comparative capabilities of core SOC platforms**Figure 9.** Comparative capabilities of core technical platforms (analytical comparison based on [16][22][15])

5.3 The incident cycle under NIST SP 800-61 Revision 3

NIST recast incident response as an activity distributed across framework functions rather than as a closed loop after damage has occurred [3]. Govern, Identify, and Protect are preparatory risk-management activities that

reduce incident likelihood and impact, whereas Detect, Respond, and Recover constitute the direct response. Continuous improvement remains a cross-cutting principle [2][3]. This view is consistent with ISO/IEC 27035, which treats preparation and lessons learned as explicit phases rather than administrative afterthoughts [11][12]. Figure 11 translates the cycle into an operational path for a data center.

Figure 11. DC-SOC incident cycle aligned with NIST SP 800-61r3 and CSF 2.0**Figure 11.** Incident-handling cycle in the proposed model according to NIST SP 800-61r3 and CSF 2.0 [2][3]

5.4 Zero trust inside the data center

Zero Trust Architecture assumes that network location confers no implicit trust and that authentication and authorization are re-evaluated before every session to a resource [9]. In a data center this implies east-west segmentation among compute, storage, and management

zones; continuous verification of operator identities and service accounts; prevention of lateral movement from the building-management network into production; and privileged-account monitoring as a high-value control. The SOC is not a passive observer; it is the primary consumer of policy and telemetry signals produced by the zero-trust layer.

6. Systematic comparisons

6.1 Operating models: in-house, hybrid, and managed service

No operating model is universally optimal. An in-house SOC provides the highest control, contextual knowledge, and privacy protection, but it is slow to build, expensive to run, and difficult to staff for genuine 24/7 coverage [1][17]. A managed service or SOC-as-a-Service accelerates capability and supplies full-shift coverage, but it may weaken business-context depth and data sensitivity. The

hybrid model occupies the middle ground: the organization retains governance and critical escalation, while continuous monitoring or night shifts are assigned to a partner [17].

Governmental, banking, and healthcare data centers have a well-founded preference for in-house or tightly controlled hybrid models because of data sovereignty and reporting requirements. Mid-sized commercial facilities may find hybrid operation more realistic. Figure 7 presents this comparison on a relative 1–5 scale derived from the literature, not from a new survey.

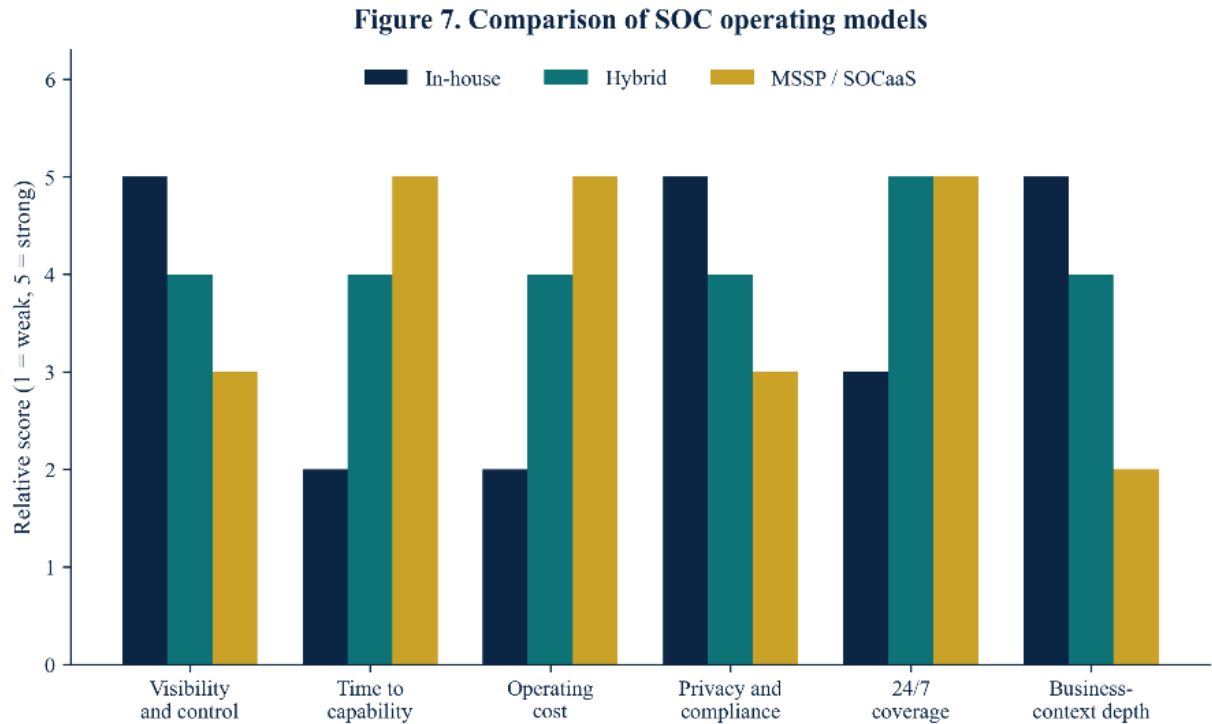


Figure 7. Comparison of SOC operating models (comparative analysis based on [1][17])

Table 2. Comparison of SOC operating models

Dimension	In-house	Hybrid	MSSP / SOCaaS
Data control	High	Medium–high	Medium
Time to capability	Long	Medium	Short
Annual operating cost	High	Medium	Contract-dependent
24/7 coverage	Difficult without depth	Feasible	Usually strong
Business-context knowledge	High	Good	Relatively limited
Fit for a sovereign data center	High	High with conditions	Contract-conditional

Table 2. Operating-model comparison (author synthesis based on [1][17][18])

6.2 Comparison of relevant normative frameworks

These frameworks are complementary, not substitutes. NIST CSF 2.0 supplies a shared outcome language and explicit governance [2]. NIST SP 800-61r3 translates that

language into response priorities [3]. ISO/IEC 27001 and 27002 provide a certifiable management system [10][23]. ISO/IEC 27035 structures the incident from preparation to lessons learned [11][12]. NIST SP 800-53 details technical and managerial controls [20]. MITRE ATT&CK converts the adversary into a measurable behavior matrix [21][22]. NIS 2 imposes a legal minimum on European Union entities and those who deal with them [18]. The SOC's function is to be the operational projection point of these frameworks, not to replace them.

Confusing a framework, a control, and a tool is among the most common design errors. A framework answers what outcome must be achieved; a control answers which protection is implemented; a tool answers by which means the outcome is observed. An organization that purchases a SIEM and then claims completion of CSF 2.0 has reduced a risk-management system to a log collector. Table 3 clarifies the distinctions.

Table 3. Comparison of frameworks and standards relevant to data-center protection

Framework / standard	Reference year	Unit of focus	Role of the SOC
NIST CSF 2.0	2024	Risk-management outcomes	Map services onto the six functions
NIST SP 800-61r3	2025	Incident response	Operate detect, respond, and recover
ISO/IEC 27001:2022	2022	ISMS requirements	Operationalize controls and monitoring
ISO/IEC 27035:2023	2023	Incident management	Incident policy and response team
NIST SP 800-53 r5	2020	Control catalog	Bind monitoring to specified controls
NIST SP 800-207	2020	Zero trust	Consume continuous-verification signals
NIS 2 Directive	2022	EU legal obligation	Reporting and entity risk management
MITRE ATT&CK	Continuously updated	Adversary behavior	Detection coverage and rule gaps

Table 3. Map of normative frameworks used in this study [2][3][9][10][11][18][20][21]

6.3 Open-source versus commercial stacks

Bassey and colleagues demonstrated that an open-source stack combining Wazuh, TheHive, and Suricata can detect and handle common scenarios in an experimental environment that scales horizontally—a path suitable for small and medium organizations or national laboratories

[16]. Large data centers with heavy regulatory obligations, however, typically require a mixture: an enterprise-grade correlation core, reliable automation, and contractual support, while retaining open tools for hunting and experimentation. The scientific criterion of choice is not the slogan “open” or “commercial,” but the ability to normalize data, integrate APIs, demonstrate alert compression, and withstand audit.

Table 4. Brief comparison of open-source and commercial stacks

Comparison criterion	Open stack (e.g., Wazuh/TheHive/Suricata)	Integrated commercial stack
License cost	Low	High
Human operating cost	Relatively high	Medium to high
Speed of proof of concept	High	Medium
Contractual support	Community / partners	Direct vendor contract

Fit for a large data center	Complementary or hybrid	Common as a core
Transparency and auditability	High	Vendor-dependent

Table 4. Technical-stack comparison (based on [16][17])

7. The proposed DC-SOC model

7.1 Design rationale

The DC-SOC model proceeds from the hypothesis that data-center protection requires four concurrent conditions: comprehensive visibility over cyber and

physical telemetry; risk governance that binds incidents to business impact; disciplined automation that does not execute destructive isolation on critical paths without a human condition; and a maturity path that is measured rather than asserted. The model is vendor-independent, implementable in-house or in hybrid form, and aligned with the CSF 2.0 functions [2], the 800-61r3 cycle [3], and zero-trust principles [9].

Figure 8. Proposed DC-SOC model for data-center protection

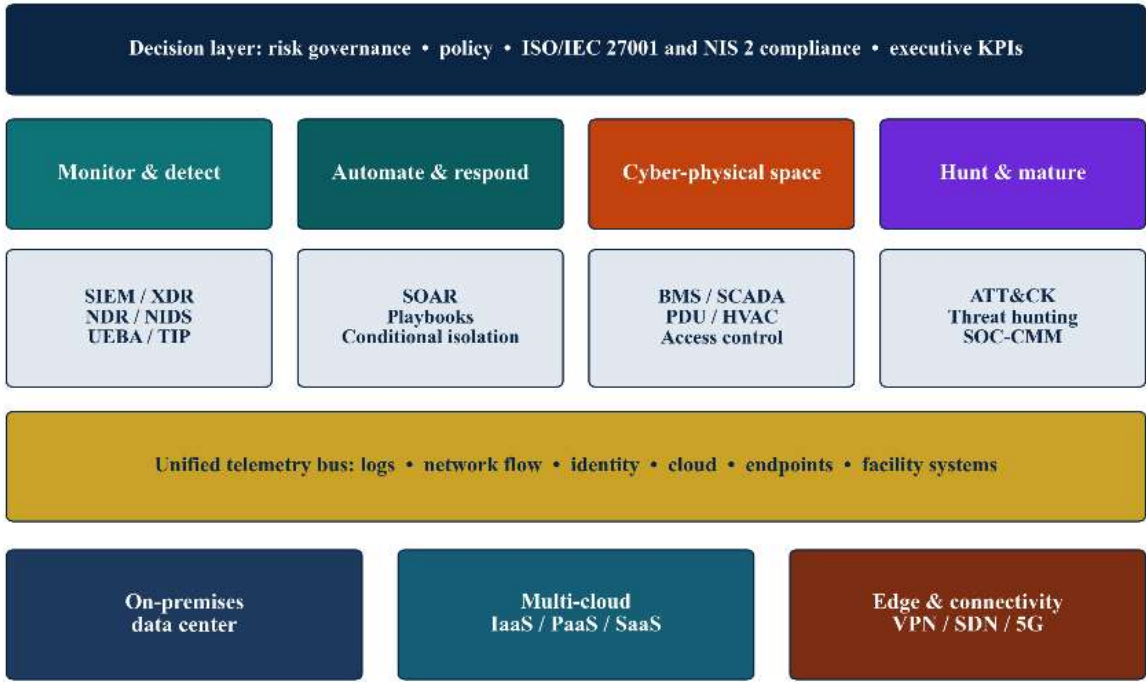


Figure 8. Proposed DC-SOC model for data-center protection (author contribution)

7.2 The six layers of the model

The first layer is the decision layer. It comprises risk policy, asset classification, escalation thresholds, compliance with ISO/IEC 27001 and NIS 2 where applicable, and an executive dashboard that does not reduce performance to alert counts [10][18]. The second layer is monitor-and-detect, comprising SIEM/XDR, NDR/NIDS, and UEBA with intelligence enrichment. The third layer is automate-and-respond, using SOAR and written, tested playbooks, with conditional automated isolation that is not applied to cooling or power systems except through a dual-approval path. The fourth layer is the cyber-physical space—the distinguishing contribution of the model: the integration of BMS, PDU, HVAC, and access-control systems into

the same telemetry bus that serves the servers [19]. The fifth layer is hunt-and-mature, binding rules to the ATT&CK matrix and measuring gaps periodically [21][22]. The sixth layer is the unified telemetry bus that serves three environments: on-premises, multi-cloud, and the edge.

7.3 Rules for cyber-physical integration

A rise in aisle temperature or the loss of one power path must not be treated as a facility alarm alone. An adversary capable of manipulating a building-management system can halt row cooling, an effect that exceeds many conventional malware incidents. Conversely, analysts must not be flooded with every facility alarm. Shared use cases should be defined: a hall-door opening coincident with an unusual privileged session; a PDU setting change outside a maintenance window; or sensor loss while the management-network

path remains active. These cases are hybrid incidents, and investigation is jointly owned by security and facility operations.

7.4 Maturity path

The model adopts the logic of the SOC Capability Maturity Model (SOC-CMM) across business, people, process, technology, and services, without claiming that

this study executed a new field assessment with the tool. Figure 10 illustrates a gap commonly reported in the literature: relatively higher technology maturity against weaker people and process maturity [1][13][15]. The model proposes analytic targets at level four and above in each domain, while recognizing that reaching them is a multi-year path.



Figure 10. Maturity domains: a common picture in the literature versus the target of the proposed model [1][13]

8. Analytical results and performance indicators

8.1 Indicators that should be measured—and those that should be abandoned

The market commonly uses misleading indicators such as “alerts handled per day” or “closure rate under fifteen minutes.” These metrics reward formal speed and may push analysts toward immature closure [13][14]. Indicators consistent with the literature and with cost reports are: mean time to detect (MTTD); mean time to respond or contain (MTTR/MTTC); the ratio of true incidents to normalized alerts; incident-report quality; coverage of

ATT&CK techniques relevant to the data center; the share of safe automation (automated execution with human review on catastrophic paths); and time to remediate edge assets [4][6][13][22].

If IBM’s findings are projected onto these indicators, an approximately 80-day reduction in the breach lifecycle through AI and automation translates into a saving approaching USD 2 million per major incident on average [4][5]. This is not an original calculation by the author; it is a direct reading of the relationship announced by the source. Generalizing the figure to every data center would be scientifically unwarranted because sectors, jurisdictions, and log volumes differ.

8.2 Results of the synthetic comparison

The comparative analysis yields six propositions. First, the most frequent threat (DDoS) is not necessarily the most costly; ransomware, intrusion, and third-party breaches are heavier economically and regulatorily [6][7][8]. Second, edge devices and VPNs have become a primary exploitation theater, and a 32-day median patch interval is too long for a data center [6]. Third, the absence of a dedicated security team among a large share

of operators explains part of the detection gap [19]. Fourth, alarm quality matters more than rule quantity [14][15]. Fifth, contemporary frameworks impose explicit governance, not merely technical monitoring [2][3][18]. Sixth, the hybrid model is the most generalizable if data sovereignty and automation boundaries are tightly specified.

Table 5. Proposed DC-SOC performance indicators and analytical cautions

Indicator	Operational definition	Desired direction	Measurement hazard
MTTD	Time from first reliable signal to recognition	Decrease	Ignoring weak signals
MTTR / MTTC	Time from recognition to containment	Decrease	Formal, incomplete containment
Triage accuracy	Share of correctly classified alerts	Increase	Cosmetic relabeling
Report quality	Completeness of context, impact, and action	Increase	Long reports without a decision
ATT&CK coverage	Share of relevant techniques covered	Directed increase	Formal coverage without data
Edge remediation	Median days to close a perimeter CVE	Decrease below 32 days	Service disruption from haste
Safe automation	Share of tested playbooks with a human condition	Gradual increase	Unconditional catastrophic isolation

Table 5. DC-SOC performance indicators (author synthesis based on [4][6][13][15][22])

8.3 Projection onto data-center scenarios

Scenario 1: exploitation of an edge-device vulnerability. According to Verizon, this path is a rising share of initial access [6]. In DC-SOC, vulnerability intelligence is bound to a mandatory ticket, monitoring is raised on the adjacent zone, and a playbook reviews accounts created after the suspected exploitation. Scenario 2: ransomware arriving through a third party that manages backups. Internal server monitoring is insufficient; backup paths, service accounts, and repository-permission changes must be observed [6][10]. Scenario 3: cyber-physical tampering with the cooling system. A conventional SIEM will not see it unless BMS telemetry is ingested and coupled to change-control policy [19]. Scenario 4: a DDoS campaign against customer-facing interfaces. Coordination among the SOC, the network team, and the connectivity provider is required, which explains the dense presence of DDoS in ENISA reports [7][8].

9. Discussion

The results of this analysis are consistent with the early conclusion of Vielberth and colleagues: a SOC remains incomplete if research or investment is confined to technology or to hiring without binding processes [1]. The present study adds a data-center-specific dimension: physical-operational telemetry is not an ornamental extra but a visibility condition. This is consistent with Uptime Institute's finding that many operators still lack a dedicated security team despite rising incident cost [19].

IBM's figures also support the hypothesis that directed automation has a tangible economic return, but they do not justify a discourse in which artificial intelligence replaces the analyst [4][5][15][24]. Qualitative studies show that analysts suffer more from missing context and explainability than from a shortage of algorithms [14]. The smarter investment in a data center is therefore signal quality: log normalization, asset tagging, identity binding, and the distinction between a benign trigger and a true incident.

The third-party problem raises a governance issue that crosses contractual boundaries. If approximately 30% of

breaches pass through an external relationship [6], a SOC that has no monitoring right over the supplier—or at least a right to an audit log and alert integration—operates with partial blindness. This is consistent with the emphasis of NIS 2 and ISO/IEC 27001 on supply-chain and supplier management [10][18].

The limits of the discussion follow from the nature of the sources. The IBM, Verizon, and ENISA reports are not random samples of every data center in the world; they are incident collections or surveys with disclosed biases (organization size, willingness to disclose, geographic coverage). They were therefore used as directional indicators, not as physical constants. Likewise, the relative scores in Figures 7, 9, and 10 are analytical syntheses and should be recalibrated in the field before a final investment decision is taken.

10. Recommendations

On the basis of the preceding analysis, the study recommends the following:

1. Adopt the SOC as an operational protection system for data centers and bind it directly to risk governance rather than to device administration alone [2][3].
2. Integrate building-management, power, cooling, and physical-access systems into the telemetry bus, with clearly defined hybrid use cases [19].
3. Select the operating model according to data sovereignty rather than lowest price, preferring a tightly controlled hybrid model for organizations that cannot staff genuine 24/7 coverage internally [17][18].
4. Treat the patching of edge devices and VPN paths as a weekly, measured program in response to Verizon's evidence [6].
5. Redesign performance indicators around MTTD, MTTR, analysis quality, and ATT&CK coverage, and abandon raw-volume metrics that feed fatigue [13][14][15].
6. Introduce artificial intelligence as an augments of triage and enrichment, not as a substitute for judgment on catastrophic paths, and retain a human condition for isolation that affects physical availability [5][15][24].
7. Contractually require cloud, backup, and support suppliers to grant a monitoring right or to deliver a correlatable audit log into the SOC [6][10].
8. Conduct an annual maturity assessment across business, people, process, technology, and services, and report gaps to senior management in the language of business impact rather than product names [1].

11. Conclusion and research outlook

This study has shown that a data-center protection system is not completed by an advanced firewall or a logging platform alone, but by a Security Operations Center designed as a socio-technical system with a cyber-physical layer. The analysis rested on authentic recent sources and showed that breach cost remains in the multi-million-dollar range, that dwell time is still measured in months rather than hours despite improvement, and that ransomware, third parties, edge devices, and alert fatigue constitute the most urgent quartet [4][5][6][15].

The paper offered DC-SOC as a comparative architectural framework that binds governance, telemetry, detection, automation, physical assets, and maturity. It is a design contribution that is testable, not a final field-experimental result. Future work should include case studies in sovereign and hybrid data centers, measurement of the effect of BMS-signal integration on MTTD, laboratory-safe testing of conditional playbooks on cooling systems, and the development of a unified SOC-maturity scale that incorporates local compliance requirements.

In conclusion, protecting a data center is simultaneously a sovereignty decision and an operational decision. The closer the center moves from the logic of “collect more logs” to the logic of “improve decision quality in time,” the closer it comes to the purpose for which it exists: the preservation of confidentiality, integrity, and availability as conditions for the continuity of public and private service.

Declaration of competing interests

The author declares no financial or institutional conflict of interest that influenced the findings of this study or the selection of references.

Funding

This research received no dedicated external funding.

Author contribution

The author designed the method, collected the sources, conducted the comparative analysis, formulated the proposed model, and wrote the manuscript in full.

References

- [1] Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, 8, 227756–227779. <https://doi.org/10.1109/ACCESS.2020.3045514>

- [2] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>
- [3] National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61 Rev. 3). <https://doi.org/10.6028/NIST.SP.800-61r3>
- [4] IBM. (2025). Cost of a data breach report 2025. IBM Corporation.
- [5] IBM. (2026). Cost of a data breach report 2026. IBM Corporation.
- [6] Verizon. (2025). 2025 data breach investigations report. Verizon Business.
- [7] European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- [8] European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- [9] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
- [10] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022).
- [11] International Organization for Standardization. (2023). Information technology – Information security incident management – Part 1: Principles and process (ISO/IEC 27035-1:2023).
- [12] International Organization for Standardization. (2023). Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response (ISO/IEC 27035-2:2023).
- [13] Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2022). A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers & Security*, 124, Article 102959. <https://doi.org/10.1016/j.cose.2022.102959>
- [14] Alahmadi, B. A., Axon, L., & Martinovic, I. (2022). 99% false positives: A qualitative study of SOC analysts' perspectives on security alarms. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 2783–2800). USENIX Association. <https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi>
- [15] Tariq, S., Baruwat Chhetri, M., Nepal, S., & Paris, C. (2025). Alert fatigue in security operations centres: Research challenges and opportunities. *ACM Computing Surveys*, 57(9), 1–38. <https://doi.org/10.1145/3723158>
- [16] Bassey, C., Chinda, E. T., & Idowu, S. (2024). Building a scalable security operations center: A focus on open-source tools. *Journal of Engineering Research and Reports*, 26(7), 196–209. <https://doi.org/10.9734/jerr/2024/v26i71203>
- [17] da Silva, D. A., Costa, J. L., & Almeida, J. R. (2024). Infrastructural challenges and good practices in a security operation center. In 13th Symposium on Languages, Applications and Technologies (SLATE 2024) (Open Access Series in Informatics, Vol. 120, Article 13). Schloss Dagstuhl – Leibniz-Zentrum für Informatik. <https://doi.org/10.4230/OASIS.SLATE.2024.13>
- [18] European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union*, L 333, 80–152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- [19] Uptime Institute. (2025). Uptime Institute data center security survey 2025 (UII Data Report 185). Uptime Institute Intelligence.
- [20] Joint Task Force. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [21] The MITRE Corporation. (2024). MITRE ATT&CK®. <https://attack.mitre.org/>
- [22] Chamkar, S. A., Maleh, Y., & Gherabi, N. (2024). Security operations centers: Use case best practices, coverage, and gap analysis based on MITRE adversarial tactics, techniques, and common knowledge. *Journal of Cybersecurity and Privacy*, 4(4), 777–793. <https://doi.org/10.3390/jcp4040036>
- [23] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022).

- [24] Baruwat Chhetri, M., Tariq, S., Singh, R., Jalalvand, F., Paris, C., & Nepal, S. (2024). Towards human-AI teaming to mitigate alert fatigue in security operations centres. *ACM Transactions on Internet Technology*, 24(3), 1-22. <https://doi.org/10.1145/3670009>