Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

The Evolution of Security Information and Event Management: From Log Management to AI-Driven Security Operations

Jini Fernandez

Independent Researcher, Riyadh, Saudi Arabia

DOI: https://doi.org/10.63363/aijfr.2026.v07i06.8885

Abstract
Security Information and Event Management (SIEM) is a class of software that collects security-relevant logs and events from across an organization's systems, normalizes and stores them, analyzes them to detect threats, and supports investigation, reporting and compliance. The term, introduced by industry analysts in 2005, joined two earlier product categories: security information management, focused on long-term log storage and reporting, and security event management, focused on real-time correlation and alerting. Since then, SIEM has moved from on-premises appliances running fixed correlation rules, through search-centric and big-data platforms, to cloud-native services that combine detection with automation, behavior analytics and, most recently, large language models. This entry traces that evolution from the late 1990s to 2026, explains the technical, regulatory and economic forces behind each change, and summarizes what has remained constant.

Keywords: SIEM, Security Operations, Log Management, Security Analytics, Cloud Security, History of Computing, XDR, SOAR

1. Introduction

SIEM has been rebuilt several times since the early 2000s, and each rebuild was driven less by new detection ideas than by changes in data volume, regulation and computing economics. Understanding those drivers helps explain the design of today's platforms and the problems they still share.

SIEM sits at the center of most security operations centers (SOCs), where it aggregates telemetry and turns it into alerts for analysts [1]. Recent surveys describe its current capabilities, deployment trends and use in critical infrastructure [2, 3], and its role within the wider SOC [4]. These works describe what SIEM is today. Less attention has been given to how it reached its present form, even though many of its persistent problems, such as alert volume [5], normalization effort and licensing cost, are legacies of earlier design choices.

This entry describes the evolution of SIEM in four overlapping periods: the origins of log management and its two precursor categories (Section 2); the convergence into SIEM and its compliance-driven adoption (Section 3); the shift toward big data, search and behavior analytics (Section 4); and the move

to cloud-native platforms, extended detection and AI assistance (Section 5). Section 6 compares the periods across five dimensions, and Section 7 discusses open challenges. Product and company events are cited to contemporary press releases and news reports; they illustrate broad shifts and do not imply an assessment of any vendor.

2. Origins: Log Management, SIM and SEM (1990s–2004)

Before SIEM existed as a category, organizations dealt with security logs through two separate needs: keeping records for later review, and spotting attacks while they happened.

2.1. Logs as the Raw Material

The common transport for log data was syslog, a simple protocol from the Unix world in which devices send short text messages to a collector. Its de facto behavior was documented by the IETF in 2001 as the BSD syslog protocol [6], and later standardized with structured fields and timestamps [7]. Syslog's simplicity made it universal, but it also left message content unstructured and inconsistent across vendors. That inconsistency became the parsing and normalization problem that every later SIEM generation has had to solve.

As networks grew, firewalls, intrusion detection systems, servers and applications each produced their own logs in their own formats. Administrators reviewed them device by device, if at all. US federal guidance later summarized the resulting problems: log volume outpacing analysis capacity, inconsistent formats, protection of log integrity, and the cost of retention [8].

2.2. Two Precursor Categories

Two product categories emerged to address these problems [9]:

- **Security information management (SIM)** centralized and stored logs over the long term, indexed them, and produced reports. Its main users were auditors and compliance teams who needed to show what had happened.
- **Security event management (SEM)** processed events in real time, normalized them, correlated events from different sources, and displayed alerts on an operator console. Its main users were security operators who needed to know what was happening now.

The distinction mirrored a split inside organizations between compliance and operations. It also mirrored a technical trade-off: storing everything cheaply favored simple, write-optimized storage, while real-time correlation favored keeping a small, normalized working set in memory.

2.3. Early Correlation Research

Detection research began well before commercial log products. Anderson's 1980 study proposed using audit trails to detect misuse of computer systems [10], and Denning's intrusion-detection model formalized the idea of profiling normal behavior and flagging deviations from it [11]. By the late 1990s, intrusion detection had an established taxonomy of approaches [12]. Researchers had also shown that, because attacks are rare compared with normal events, even small false-alarm rates overwhelm operators, a problem known as the base-rate fallacy [13].

The research community responded with alert correlation: combining low-level alerts from multiple sensors into higher-level descriptions of attacks and removing duplicates and false alerts [14], and reconstructing multi-step attack scenarios from the prerequisites and consequences of individual alerts [15, 16]. These ideas later became core features of commercial correlation engines.

2.4. Regulation as a Driver

Regulation turned log management from good practice into an obligation. US rules for health data, financial reporting, financial privacy, payment cards and federal systems, among others, all imposed requirements for collecting, protecting and reviewing logs [8]. Compliance gave organizations a budget line for log collection, and it gave SIM vendors a market well before advanced threat detection did.

3. Convergence: The First SIEM Generation (2005–2011)

In 2005, Gartner analysts Mark Nicolett and Amrit Williams introduced the term SIEM for products that combined SIM's storage and reporting with SEM's real-time correlation [9]. The name described a market that was already merging: buyers wanted one system to satisfy auditors and support operators.

3.1. Architecture and Detection

First-generation SIEMs shared a recognizable design. Collectors or agents gathered events and parsed them at ingest into a fixed, vendor-defined schema. A correlation engine then evaluated rules against the normalized event stream in real time, keeping state in memory for patterns such as thresholds and sequences. Normalized events were written to a relational or proprietary database for reporting and investigation. Many products shipped as hardware appliances or appliance-like software sized to an expected event rate.

Detection meant rules. Vendors supplied libraries of correlation rules and compliance reports, and customers tuned and extended them. This made detections explainable and fast, but every new attack pattern needed a new rule, and every new log source needed a new parser before any rule could use it.

3.2. Market Recognition

By the end of the period, SIEM had become strategic for large technology vendors. HP completed its acquisition of ArcSight, a security and compliance management company, in October 2010 at an enterprise value of US$1.5 billion [17]. In 2011, IBM announced its acquisition of Q1 Labs, whose QRadar product combined log, threat and compliance management with analysis of network flow data [18]. These acquisitions placed SIEM inside the broad security portfolios of large IT companies.

3.3. Limitations

Three limitations of this generation, several of them also described in operational accounts of SIEM [1], shaped what came next:

- **Fixed schemas at ingest.** Data that did not fit the vendor's schema was dropped or poorly parsed, and changing the schema was costly.
- **Scaling limits.** Relational storage and in-memory correlation struggled as event volumes grew, so organizations filtered data before collection and kept short retention periods.

- **Rule maintenance.** Rule libraries required constant tuning, and poorly tuned rules produced large volumes of false positives. Compliance-driven deployments were often switched on to pass audits rather than tuned for detection.

4. Big Data and Analytics: The Second Generation (2011–2018)

The second generation responded to the scaling and schema limits of the first by storing more data in rawer form and analyzing it in more ways. Detection began to move beyond hand-written rules toward search, statistics and shared intelligence.

4.1. Search-Centric Platforms and Schema-on-Read

Search-centric platforms indexed events largely as received and extracted fields at query time rather than at ingest. This schema-on-read approach meant new or unusual log sources could be collected immediately and interpreted later, and analysts could ask questions the original designers had not foreseen. Detections increasingly took the form of scheduled searches rather than stateful, real-time rules. The trade-offs were higher storage and compute needs and some loss of real-time immediacy. Splunk, whose Enterprise Security application provides SIEM functions on top of its general machine-data platform, is a widely used example of this model.

Distributed storage and processing frameworks from the big-data movement allowed similar designs at very large scale. Research showed what this made possible: Beehive mined large volumes of heterogeneous enterprise logs to surface suspicious host behavior that existing tools had missed [19], and later work detected early-stage infections by mining large-scale DNS and web proxy logs [20].

4.2. Behavior Analytics

User and entity behavior analytics (UEBA) applied anomaly-detection techniques [21] to build baselines of normal behavior for users, hosts and peer groups, and flagged deviations such as unusual logins or data transfers. It drew on a wider body of machine-learning research for intrusion detection [22], tempered by warnings that anomaly detection behaves differently in security than in other domains, because errors are costly and representative attack data is scarce [23]. Later research modeled system logs as event sequences with deep learning [24, 25] and detected lateral movement by modeling internal login paths [26].

In operational SOCs, machine learning was used more often to prioritize alerts and reduce false positives than to raise alerts on its own [27]. UEBA began as separate products and was gradually absorbed into SIEM platforms, often as a risk score added to alerts rather than as a standalone alert source.

4.3. Threat Intelligence and Shared Frameworks

SIEMs began to ingest threat-intelligence feeds automatically, matching indicators such as malicious IP addresses and domains against incoming events. Surveys documented the growth of intelligence sharing [28] and the limits of technical indicators, which adversaries can change quickly [29]. Practitioners reported persistent data-quality problems in shared intelligence [30], and researchers proposed models and taxonomies to describe intelligence more consistently [31].

Correlation increasingly followed models of attack progression. The intrusion kill chain described an intrusion as a sequence of stages from reconnaissance to actions on objectives [32]. Researchers applied it to SIEM log analysis and to the aggregation of SIEM alerts [33, 34], and later systems correlated suspicious information flows into high-level stages of advanced attacks [35].

Two shared frameworks changed how detections were described. MITRE ATT&CK provided a common vocabulary of adversary tactics and techniques against which detection coverage could be mapped [36, 37], and the Sigma project offered a vendor-neutral rule format that could be converted into different SIEM query languages [38].

4.4. Orchestration and Automation

As alert volumes grew, response became the bottleneck. Security orchestration, automation and response (SOAR) tools emerged to run playbooks that enrich alerts, query other tools and take containment actions automatically. Gartner first used the acronym SOAR in 2015 for a different phrase and redefined it in 2017 with its current meaning [39]. A multi-vocal review of the field described how orchestration tied together the many tools in a SOC [40]. Like UEBA, SOAR began as a separate category and was later integrated into SIEM platforms.

5. Cloud-Native Platforms: The Third Generation (2018–2026)

The third generation moved SIEM into the cloud and folded neighboring tools into single security operations platforms. Its defining changes were elastic storage and compute, new pricing models, open data schemas, consolidation of the vendor market, and AI assistance.

5.1. SIEM as a Cloud Service

Cloud-native SIEMs run as managed services on hyperscale infrastructure, removing the need for customers to size and operate their own clusters. In March 2019, Alphabet's Chronicle launched Backstory, a security telemetry platform built on Google infrastructure that could retain petabytes or years of data, with pricing explicitly not based on data volume [41]. In September 2019, Microsoft made Azure Sentinel, later renamed Microsoft Sentinel, generally available as a cloud-native SIEM after more than six months of public preview [42]. Cloud delivery also aligned SIEM with where data increasingly originated: cloud control planes, software-as-a-service applications and identity providers.

5.2. Platform Convergence and Extended Detection

Vendors began combining SIEM, SOAR, UEBA, endpoint detection and threat intelligence into unified platforms. Extended detection and response (XDR) products approached the same goal from the endpoint side, correlating telemetry across endpoints, networks, cloud and identity. In October 2022, Palo Alto Networks made Cortex XSIAM generally available, describing it as an autonomous security operations platform that changes how data, analytics and automation are used in the SOC [43]. In this model, the boundaries between SIEM, XDR and SOAR became largely a matter of packaging.

5.3. Open Schemas

Normalization, a problem since syslog, gained an open industry response. In August 2022, AWS and Splunk launched the Open Cybersecurity Schema Framework (OCSF) with Symantec's schema work as

its foundation and 15 further initial members, to provide a vendor-agnostic taxonomy for security data [44]. The schema itself is published openly [45]. Open schemas aim to make data portable between tools and reduce the parsing work that every SIEM generation has repeated.

5.4. Market Consolidation

The mid-2020s saw rapid consolidation. Cisco completed its acquisition of Splunk in March 2024 for approximately US$28 billion in equity value [46]. In September 2024, Palo Alto Networks closed its acquisition of IBM's QRadar software-as-a-service assets, offering eligible customers migration to Cortex XSIAM [47]. In July 2024, Exabeam and LogRhythm completed their merger [48]. Consolidation turned platform migration into a common, large-scale task for SOCs.

5.5. AI Assistance

Generative AI arrived in SIEM through natural-language assistants that summarize incidents, explain alerts, write queries and suggest response steps. Microsoft Copilot for Security, for example, became generally available in April 2024 [49]. Research on large language models in security has grown rapidly [50, 51]. An empirical study in a commercial SOC found that analysts used an LLM mainly as an on-demand aid for understanding and writing commands, rather than for high-stakes decisions [52]. The reliability of AI-generated detection logic and investigation conclusions remains an open question (Section 7).

Figure 1 places the milestones cited in Sections 2–5 on a single time axis. Four of the fourteen events fall within six months of 2024, which shows how sharply consolidation accelerated in the third generation. Year-only events are placed mid-year.

Figure 1: Timeline of SIEM Milestones, 2001–2026



6. Cross-Cutting Shifts

Across three generations, SIEM moved from structure-first to collect-first, from rules alone to layered analytics, and from owned infrastructure to consumed services, while the core tasks of collection, normalization and detection stayed the same. Table 1 compares the generations across five dimensions.

Table 1: Comparison of SIEM Generations

Dimension	First generation (2005–2011)	Second generation (2011–2018)	Third generation (2018–2026)
Architecture	Appliances; relational or proprietary storage; real-time correlation engine	Distributed indexing and big-data clusters, mostly self-managed	Managed cloud services with elastic storage and compute
Data model	Fixed vendor schema applied at ingest	Schema-on-read; fields extracted at search time	Vendor data models plus open schemas such as OCSF
Detection	Correlation rules and compliance reports	Scheduled searches, UEBA, threat-intelligence matching, ATT&CK-mapped content	Built-in analytics and models, detection-as-code, AI assistants
Response	Manual triage in the console	SOAR playbooks as separate tools	SOAR and XDR integrated into one platform
Economics and deployment	Hardware and licenses sized to events per second	Licensing commonly based on ingested data volume	Subscriptions, with tiered storage and some models not tied to data volume

Three observations follow from the comparison.

Normalization never went away. Each generation moved where normalization happens, at ingest, at search time, or through open schemas, but none eliminated it. The effort of understanding diverse log formats is a constant cost of SIEM, and it has shifted rather than shrunk.

Economics shaped detection. Data volume has consistently set the limits of what an organization could afford to collect and keep. Pricing tied to events per second or ingest volume encouraged filtering before collection, while cloud models with tiered or volume-independent pricing encouraged keeping more data. What a SIEM could detect depended as much on these commercial choices as on its analytics.

Integration, then separation, then re-integration. SIM and SEM merged into SIEM; UEBA and SOAR then emerged as separate products; the third generation absorbed them again into platforms. Each cycle reflected the same tension between specialized tools that innovate quickly and unified platforms that reduce operational overhead.

7. Outlook and Open Challenges

The next stage of SIEM is likely to be defined less by new storage technology than by whether automation and AI can be trusted with decisions that people now make. Five challenges carry over from earlier generations or are new to this one.

- **Alert fatigue persists.** Each generation promised fewer, better alerts, yet analysts still report that false positives dominate their queues [5, 53]. A four-year measurement in one SOC found that only about 0.01% of network alerts were associated with true attacks [54], and sustained alert volume contributes to analyst burnout [55]. Research approaches such as provenance-based triage [56] and contextual analysis of event sequences [57] aim to reduce this burden.
- **Detection quality.** Rules remain open to evasion. A study of widely used Sigma rules found that adversaries could evade nearly half of them easily [58]. Studies of production rulesets show that a small fraction of rules generates most alerts [59] and that rule design choices strongly affect noise [60], while claimed ATT&CK coverage does not consistently mean the same detection capability [61].
- **Migration after consolidation.** Market consolidation forces many organizations to move years of detection content between platforms. Translating and validating that content is costly, and errors are often silent.
- **Trust in AI assistance.** AI assistants can speed up investigation and query writing, but they also produce plausible output that is wrong, as code-generating models do when they recommend software packages that do not exist [62]. A study of LLM-based alert triage found that every approach tested missed at least 40.4% of attack-related alerts [63]. Methods for validating AI-generated detections and conclusions are not yet mature.
- **Data sovereignty and regulation.** Cloud delivery collides with national requirements for data residency and security monitoring. Frameworks such as Saudi Arabia's Essential Cybersecurity Controls [64] set monitoring obligations that SIEM deployments must meet, influencing whether organizations choose cloud, local-cloud or on-premises options.

8. Conclusions

SIEM evolved from two narrow tools, one for keeping logs and one for watching events, into cloud platforms that combine collection, analytics, automation and AI assistance. Each generation answered the scaling and cost limits of the one before: fixed schemas gave way to schema-on-read, self-managed clusters to cloud services, and separate tools to unified platforms. Throughout, the same core problems remained: making diverse data usable, keeping detections accurate, and limiting the volume of alerts that people must review. The newest generation adds a further question: how far AI-produced detections and conclusions can be trusted. How SIEM answers it will likely define its next stage.

Conflict of Interest

The author declares no conflicts of interest.

Acknowledgement

This research received no external funding. During the preparation of this manuscript, the author used Claude (Anthropic) for the purposes of drafting text, structuring the paper, and identifying and verifying

references. The author has reviewed and edited the output and takes full responsibility for the content of this publication.

References

1. S. Bhatt, P.K. Manadhata, L. Zomlot, "The operational role of security information and event management systems", IEEE Security & Privacy, 2014, 12, 35–41. https://doi.org/10.1109/MSP.2014.103
2. G. González-Granadillo, S. González-Zarzosa, R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures", Sensors, 2021, 21, 4759. https://doi.org/10.3390/s21144759
3. J.M. López Velásquez, S.M. Martínez Monterrubio, L.E. Sánchez Crespo, D. Garcia Rosado, "Systematic review of SIEM technology: SIEM-SC birth", International Journal of Information Security, 2023, 22, 691–711. https://doi.org/10.1007/s10207-022-00657-9
4. M. Vielberth, F. Böhm, I. Fichtinger, G. Pernul, "Security operations center: A systematic study and open challenges", IEEE Access, 2020, 8, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514
5. F.B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, G.-J. Ahn, "Matched and mismatched SOCs: A qualitative study on security operations center issues", Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS), London, UK, 2019, pp. 1955–1970. https://doi.org/10.1145/3319535.3354239
6. C. Lonvick, "The BSD syslog Protocol", RFC 3164, Internet Engineering Task Force: 2001. https://doi.org/10.17487/RFC3164
7. R. Gerhards, "The Syslog Protocol", RFC 5424, Internet Engineering Task Force: 2009. https://doi.org/10.17487/RFC5424
8. K. Kent, M. Souppaya, "Guide to Computer Security Log Management", NIST Special Publication 800-92, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2006. https://doi.org/10.6028/NIST.SP.800-92
9. Palo Alto Networks, "What Are Security Information and Event Management (SIEM) Tools?", Accessed 10 November 2026. https://www.paloaltonetworks.com/cyberpedia/what-are-siem-tools
10. J.P. Anderson, "Computer Security Threat Monitoring and Surveillance", Technical Report, James P. Anderson Co.: Fort Washington, PA, USA, 1980.
11. D.E. Denning, "An intrusion-detection model", IEEE Transactions on Software Engineering, 1987, SE-13, 222–232. https://doi.org/10.1109/TSE.1987.232894
12. H. Debar, M. Dacier, A. Wespi, "Towards a taxonomy of intrusion-detection systems", Computer Networks, 1999, 31, 805–822. https://doi.org/10.1016/S1389-1286(98)00017-6
13. S. Axelsson, "The base-rate fallacy and the difficulty of intrusion detection", ACM Transactions on Information and System Security, 2000, 3, 186–205. https://doi.org/10.1145/357830.357849
14. F. Valeur, G. Vigna, C. Kruegel, R.A. Kemmerer, "A comprehensive approach to intrusion detection alert correlation", IEEE Transactions on Dependable and Secure Computing, 2004, 1, 146–169. https://doi.org/10.1109/TDSC.2004.21
15. F. Cuppens, A. Miège, "Alert correlation in a cooperative intrusion detection framework", Proceedings of the 2002 IEEE Symposium on Security and Privacy, 2002, pp. 202–215. https://doi.org/10.1109/SECPRI.2002.1004372

16. P. Ning, Y. Cui, D.S. Reeves, “Constructing attack scenarios through correlation of intrusion alerts”, Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, 2002, pp. 245–254. https://doi.org/10.1145/586110.586144
17. TechCrunch, “HP Closes $1.5 Billion Acquisition of ArcSight”, 22 October 2010. Accessed 10 November 2026. https://techcrunch.com/2010/10/22/hp-closes-1-5-billion-acquisition-of-arcsight
18. TechCrunch, “IBM Buys Network Security Intelligence Company Q1 Labs”, 4 October 2011. Accessed 10 November 2026. https://techcrunch.com/2011/10/04/ibm-buys-network-security-intelligence-company-q1-labs/
19. T.-F. Yen, A. Oprea, K. Onarlioglu, T. Leetham, W. Robertson, A. Juels, E. Kirda, “Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks”, Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC), New Orleans, LA, USA, 2013, pp. 199–208. https://doi.org/10.1145/2523649.2523670
20. A. Oprea, Z. Li, T.-F. Yen, S.H. Chin, S.A. Alrwais, “Detection of early-stage enterprise infection by mining large-scale log data”, Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2015, pp. 45–56. https://doi.org/10.1109/DSN.2015.14
21. V. Chandola, A. Banerjee, V. Kumar, “Anomaly detection: A survey”, ACM Computing Surveys, 2009, 41, 15. https://doi.org/10.1145/1541880.1541882
22. A.L. Buczak, E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection”, IEEE Communications Surveys & Tutorials, 2016, 18, 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
23. R. Sommer, V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection”, Proceedings of the 2010 IEEE Symposium on Security and Privacy, 2010, pp. 305–316.
24. M. Du, F. Li, G. Zheng, V. Srikumar, “DeepLog: Anomaly detection and diagnosis from system logs through deep learning”, Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2017, pp. 1285–1298. https://doi.org/10.1145/3133956.3134015
25. M. Landauer, S. Onder, F. Skopik, M. Wurzenberger, “Deep learning for anomaly detection in log data: A survey”, Machine Learning with Applications, 2023, 12, 100470. https://doi.org/10.1016/j.mlwa.2023.100470
26. G. Ho, M. Dhiman, D. Akhawe, V. Paxson, S. Savage, G.M. Voelker, D. Wagner, “Hopper: Modeling and detecting lateral movement”, Proceedings of the 30th USENIX Security Symposium, 2021, pp. 3093–3110.
27. C. Feng, S. Wu, N. Liu, “A user-centric machine learning framework for cyber security operations center”, Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017, pp. 173–175. https://doi.org/10.1109/ISI.2017.8004902
28. T.D. Wagner, K. Mahbub, E. Palomar, A.E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions”, Computers & Security, 2019, 87, 101589.
29. W. Tounsi, H. Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks”, Computers & Security, 2018, 72, 212–233. https://doi.org/10.1016/j.cose.2017.09.001
30. C. Sillaber, C. Sauerwein, A. Mussmann, R. Breu, “Data quality challenges and future research directions in threat intelligence sharing practice”, Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security (WISCS), 2016, pp. 65–70.

31. V. Mavroeidis, S. Bromander, “Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence”, Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC), 2017, pp. 91–98. https://doi.org/10.1109/EISIC.2017.20
32. E.M. Hutchins, M.J. Cloppert, R.M. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains”, Proceedings of the 6th International Conference on Information Warfare and Security (ICIW), Washington, DC, USA, 2011, pp. 113–125.
33. B.D. Bryant, H. Saiedian, “A novel kill-chain framework for remote security log analysis with SIEM software”, Computers & Security, 2017, 67, 198–210. https://doi.org/10.1016/j.cose.2017.03.003
34. B.D. Bryant, H. Saiedian, “Improving SIEM alert metadata aggregation with a novel kill-chain based classification model”, Computers & Security, 2020, 94, 101817. https://doi.org/10.1016/j.cose.2020.101817
35. S.M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar, V.N. Venkatakrishnan, “HOLMES: Real-time APT detection through correlation of suspicious information flows”, Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 1137–1152. https://doi.org/10.1109/SP.2019.00026
36. B.E. Strom, A. Applebaum, D.P. Miller, K.C. Nickels, A.G. Pennington, C.B. Thomas, “MITRE ATT&CK: Design and Philosophy”, Technical Report, The MITRE Corporation: McLean, VA, USA, 2018.
37. B. Al-Sada, A. Sadighian, G. Oligeri, “MITRE ATT&CK: State of the art and way forward”, ACM Computing Surveys, 2025, 57, 12. https://doi.org/10.1145/3687300
38. SigmaHQ, “Sigma: Generic Signature Format for SIEM Systems”, Accessed 10 November 2026. https://github.com/SigmaHQ/sigma
39. TechTarget, “What is SOAR (security orchestration, automation and response)?”, Accessed 10 November 2026. https://www.techtarget.com/searchsecurity/definition/SOAR
40. C. Islam, M.A. Babar, S. Nepal, “A multi-vocal review of security orchestration”, ACM Computing Surveys, 2019, 52, 37. https://doi.org/10.1145/3305268
41. SecurityWeek, “Alphabet's Chronicle Launches Security Telemetry Platform”, 5 March 2019. Accessed 10 November 2026. https://www.securityweek.com/alphabets-chronicle-launches-security-telemetry-platform/
42. Dark Reading, “Microsoft's Azure Sentinel SIEM Now Generally Available”, 25 September 2019. Accessed 10 November 2026. https://www.darkreading.com/cloud-security/microsoft-s-azure-sentinel-siem-now-generally-available
43. Palo Alto Networks, “Palo Alto Networks Ushers in the Next-Generation Security Operations Center with General Availability of Cortex XSIAM”, Press Release, 12 October 2022. Accessed 10 November 2026. https://www.paloaltonetworks.com/company/press/2022/palo-alto-networks-ushers-in-the-next-generation-security-operations-center-with-general-availability-of-cortex-xsiam---the-autonomous-security-operations-platform
44. Help Net Security, “Open Cybersecurity Schema Framework Project Helps Organizations Detect and Defend from Cyberattacks”, 11 August 2022. Accessed 10 November 2026. https://www.helpnetsecurity.com/2022/08/11/open-cybersecurity-schema-framework/

45. "Open Cybersecurity Schema Framework (OCSF)", Accessed 10 November 2026. https://schema.ocsf.io
46. Cisco, "Cisco Completes Acquisition of Splunk", Press Release, 18 March 2024. Accessed 10 November 2026. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cisco-completes-acquisition-of-splunk.html
47. Dark Reading, "Palo Alto Networks Closes Acquisition of IBM's QRadar SaaS Assets", 5 September 2024. Accessed 10 November 2026. https://www.darkreading.com/cybersecurity-operations/palo-alto-networks-closes-acquisition-of-ibm-s-qradar-saas-assets
48. Exabeam, "Exabeam and LogRhythm Complete Merger and Announce New Company Details", Press Release, 17 July 2024. Accessed 10 November 2026. https://www.exabeam.com/press-releases/exabeam-and-logrhythm-complete-merger-and-announce-new-company-details/
49. Microsoft, "Microsoft Copilot for Security Is Generally Available on April 1, 2024, with New Capabilities", Microsoft Security Blog, 13 March 2024. Accessed 10 November 2026. https://microsoft.com/en-us/security/blog/2024/03/13/microsoft-copilot-for-security-is-generally-available-on-april-1-2024-with-new-capabilities
50. H. Xu, S. Wang, N. Li, K. Wang, Y. Zhao, K. Chen, T. Yu, Y. Liu, H. Wang, "Large language models for cyber security: A systematic literature review", ACM Transactions on Software Engineering and Methodology, 2025, arXiv:2405.04760. https://arxiv.org/abs/2405.04760
51. I. Hasanov, S. Virtanen, A. Hakkala, J. Isoaho, "Application of large language models in cybersecurity: A systematic literature review", IEEE Access, 2024, 12, 176751–176778. https://doi.org/10.1109/ACCESS.2024.3505983
52. R. Singh, S. Tariq, F. Jalalvand, M.B. Chhetri, S. Nepal, C. Paris, M. Lochner, "LLMs in the SOC: An empirical study of human-AI collaboration in security operations centres", arXiv, 2025, arXiv:2508.18947. https://arxiv.org/abs/2508.18947
53. B.A. Alahmadi, L. Axon, I. Martinovic, "99% false positives: A qualitative study of SOC analysts' perspectives on security alarms", Proceedings of the 31st USENIX Security Symposium, Boston, MA, USA, 2022, pp. 2783–2800.
54. L. Yang, Z. Chen, C. Wang, Z. Zhang, S. Booma, P. Cao, C. Adam, A. Withers, Z. Kalbarczyk, R.K. Iyer, G. Wang, "True attacks, attack attempts, or benign triggers? An empirical measurement of network alerts in a security operations center", Proceedings of the 33rd USENIX Security Symposium, Philadelphia, PA, USA, 2024, pp. 1525–1542.
55. S.C. Sundaramurthy, A.G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, S.R. Rajagopalan, "A human capital model for mitigating security analyst burnout", Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), Ottawa, ON, Canada, 2015, pp. 347–359.
56. W.U. Hassan, S. Guo, D. Li, Z. Chen, K. Jee, Z. Li, A. Bates, "NoDoze: Combatting threat alert fatigue with automated provenance triage", Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 2019. https://doi.org/10.14722/ndss.2019.23349
57. T. van Ede, H. Aghakhani, N. Spahn, R. Bortolameotti, M. Cova, A. Continella, M. van Steen, A. Peter, C. Kruegel, G. Vigna, "DeepCASE: Semi-supervised contextual analysis of security events", Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), 2022, pp. 522–539.

58. R. Uetz, M. Herzog, L. Hackländer, S. Schwarz, M. Henze, “You cannot escape me: Detecting evasions of SIEM rules in enterprise networks”, Proceedings of the 33rd USENIX Security Symposium, Philadelphia, PA, USA, 2024, pp. 5179–5196.
59. M. Vermeer, M. van Eeten, C. Gañán, “Ruling the rules: Quantifying the evolution of rulesets, alerts and incidents in network intrusion detection”, Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security (ASIA CCS), 2022, pp. 799–813. https://doi.org/10.1145/3488932.3517412
60. K.T.W. Teuwen, T. Mulders, E. Zambon, L. Allodi, “Ruling the unruly: Designing effective, low-noise network intrusion detection rules for security operations centers”, Proceedings of the 20th ACM Asia Conference on Computer and Communications Security (ASIA CCS), Hanoi, Vietnam, 2025, pp. 1428–1441. https://doi.org/10.1145/3708821.3710823
61. A. Virkud, M.A. Inam, A. Riddle, J. Liu, G. Wang, A. Bates, “How does endpoint detection use the MITRE ATT&CK framework?”, Proceedings of the 33rd USENIX Security Symposium, Philadelphia, PA, USA, 2024, pp. 3891–3908.
62. J. Spracklen, R. Wijewickrama, A.H.M.N. Sakib, A. Maiti, B. Viswanath, M. Jadliwala, “We have a package for you! A comprehensive analysis of package hallucinations by code generating LLMs”, Proceedings of the 34th USENIX Security Symposium, Seattle, WA, USA, 2025, pp. 3687–3706.
63. S.A. Tsegai, A. Kantchelian, D. Yao, P. Gao, “From investigation failures to reliable SOC agents: Understanding and improving LLM-based alert triage”, arXiv, 2026, arXiv:2610.10608. https://arxiv.org/abs/2610.10608
64. National Cybersecurity Authority, “Essential Cybersecurity Controls (ECC-2:2024)”, National Cybersecurity Authority: Riyadh, Saudi Arabia, 2024. Accessed 10 November 2026. https://nca.gov.sa/en/regulatory-documents/controls-list/ecc/