Security information and event management

Security information and event management (**SIEM**) is a field within the field of computer security, where software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware. Vendors sell SIEM as software, as appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes.[1] The term and the initialism SIEM was coined by Mark Nicolett and Amrit Williams of Gartner in 2005.[2]

History

Monitoring system logs has grown more prevalent as complex cyber-attacks force compliance and regulatory mechanisms to mandate logging security controls within a Risk Management Framework. Logging levels of a system started with the primary function of troubleshooting system errors or debugging code compiled and run. As operating systems and networks have increased in complexity, so has the event and log generation on these systems. In comparison,

the logging of system, security, and application logs is not the only way to perform incident response. They do offer the capability to trace the activities of nearly any system or user-related movement throughout a given period. From the late 1970s, there was a formation of working groups to help establish the criteria for the management of auditing and monitoring programs and what and how system logs can be used for insider threat, incident response, and troubleshooting. This also established a base discussion for many of the concepts still used in modern cybersecurity. See, Basis for Audit and Evaluation of Computer Security from National Institute of Standards and Technology (NIST) Special Publication 500-19 published in 1977.[3]

With Risk Management Frameworks (RMF) being implemented worldwide in nearly all industry sectors, auditing and monitoring are core elements of information assurance and information security. Information assurance personnel, cybersecurity engineers, and analysts can use logging information to perform critical security functions in real-time. These items are driven by governance models that integrate or use auditing and monitoring as a basis for that analytical work. As information assurance matured in the late 1990s and moved into the 2000s, system logs needed to be centralized. This allows records to be centrally located and viewed and provides centralized management as a 'nerve center' for all machines on a given network.

This centralization and consolidation of system data would provide significantly more than just a holistic view. Still, now organizations could use the logging data for operational use cases and help with performance and networking-based communication troubleshooting. Security Information and Event Management (SIEM) is now commonplace, and there are apparent variations of the same acronym in this article. The word SIEM is primarily a moniker forcing all logs into a single place to provide a single pane of glass for security and network operations to perform analysis.

The National Institute of Standards and Technology provides the following definition for Security Information Event Management (SIEM): "Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface."[4] Information assurance has become a forcing function for system logging. System logging can enable traceability for an account on a system used to perform system actions. In combination with the operating system, the SIEM can index and parse system logs and be made available for searching.

On May 17, 2021, United States President Joseph Biden signed Executive Order 14028 Improving the Nations Cybersecurity.[5] This Executive Order mandates endpoint protection, further defining logging requirements, implementing audit logging in a unified way, and enhancing the

capabilities to provide further insight into system and account actions. Audit logs were identified in three separate technical areas, all relating to incident response and knowing what is happening on a system at a given time. This Executive Order responds to an increase in cyber-attacks that use ransomware to cripple critical infrastructure components related to national security and the public. Enhancing existing information assurance security controls as part of a Risk Management Framework is a suitable mechanism to force compliance and justify funding based on these Presidential requirements.

Security Information and Event Management (SIEM) & Information Assurance

Published in September 2006, NIST SP 800-92 Guide to Computer Security Log Management is the primary document used in the NIST Risk Management Framework for what should be auditable. While not definitive or exhaustive as there have been significant changes in technology since 2006, this guidance anticipated industry growth as the document is still relevant. This document pre-dates many modern SIEM technologies that are well known today, as evident by no reference to the term "SIEM.[6][7] NIST is not the only guidance for a regulatory mechanism for auditing and monitoring that are encouraged to use SIEM solutions instead of de-centralized individual host-based checks. NIST identifies several public and private entities with their logging guidance that may enforce its requirements; Federal Information Security Management Act of 2002 (FISMA),[8] Gramm-Leach-Bliley Act (GLBA),[9] Health Insurance Portability and Accountability Act of 1996 (HIPAA),[10] Sarbanes-Oxley Act (SOX) of 2002,[11] Payment Card Industry Data Security Standard (PCI DSS),[12] and International Organization for Standardization (ISO) 27001.[13] It is not uncommon for NIST documents to be referenced in public and private organizations.

NIST SP 800-53 AU-2 Event Monitoring is a core security control for enabling logging functionality to support the information assurance process for all auditing throughout a system.[14] AU-2 Event Monitoring also serves as a critical basis for continuous monitoring for information assurance and cybersecurity engineering efforts throughout a network. It is expected that the SIEM solution is used as a core tool or suite of tools to support this effort. Depending on the system categorization concerning the impact on the Confidentiality, Integrity, and Availability (CIA) of a system are generally five specific requirements needed to satisfy the base logging requirements of a federal system (AU-2, a-e).[15][16] It is essential to understand the security control requirements about the SIEM infrastructure and operation. Below are the security control requirements for AU-2.

> The [Assignment: organization-defined...] is left blank to determine what is appropriate for its enterprise. Executive Order 14028 seeks to unify the inputs across all federal agencies.[17]
>
> a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
>
> b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
>
> c. Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
>
> d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
>
> e. Review and update the event types selected for logging [Assignment: organization-defined frequency].[14]

Events on a system could include and are not limited to credential changes, failed access attempts, role base or attribute changes to accounts, token-based use, access attempts, and failures, etc. While logging every system action to the system is possible, it is often not advised based on the volume of logs and actionable security-relevant data. Organizations can use AU-2 a through e, as the basis to build from while adhering to other controls that may require or call out specific security auditing requirements in more granular detail. NIST SP 800-53 SI-4 System Monitoring is the security control that specifies the monitoring of the system.[18][7] This monitoring is focused on monitoring systems that monitor the system. This can include hardware and software in unison to detect events and anomalies, malware, connections, and any other pertinent mechanism that is used to detect attacks or indicators of potential attacks.[18]

> a. Monitor the system to detect:

> - 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and
> - 2. Unauthorized local, network, and remote connections;
>
> b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];
>
> c. Invoke internal monitoring capabilities or deploy monitoring devices:
>
> - 1. Strategically within the system to collect organization-determined essential information; and
> - 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
>
> d. Analyze detected events and anomalies;
>
> e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
>
> f. Obtain legal opinion regarding system monitoring activities; and
>
> g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].[18]

NIST SP 800-53 RA-10 Threat Hunting is a new base security control added to NIST 800-53 with the latest Revision 5 edit and publication.[19][7] Threat hunting is the proactive defense of a network by combining all security information and actively looking for threats. To execute the operation, the analysts and engineers need a repository of information, and a SIEM solution is often used as a hub because all system logs would typically be sent to this centralized location. A threat hunting team is not limited to this approach. However, the SIEM solution should provide significant amounts of security-relevant data.[20]

> a. Establish and maintain a cyber threat hunting capability to:
>
> - 1. Search for indicators of compromise in organizational systems; and
> - 2. Detect, track, and disrupt threats that evade existing controls; and
>
> b. Employ the threat hunting capability [Assignment: organization-defined frequency].

NIST SP 800-53 R5 and the brief descriptions of AU-2, SI-4, and RA-10 depict how individual controls are all used as critical elements of the event, alerting and monitoring via a SIEM.[21] These controls, combined with other technical security controls provided by NIST, weave together an in-depth defense system. The assurance of the system security is enforced with various risk assessments and continuous monitoring - often enhanced or streamlined with a SIEM product used across entire cybersecurity teams. There are many more technical controls that outline specific items that must be monitored. The controls identified are a cursory overlook of controls directly related to the event and audit gathering functionality and use in a SIEM tool.

Terminology

The acronyms *SEM*, *SIM* and *SIEM* have sometimes been used interchangeably,[22] but generally refer to the different primary focus of products:

- *Log management*: Focus on simple collection and storage of log messages and audit trails[23]
- *Security information management* (SIM): Long-term storage as well as analysis and reporting of log data.[24]
- *Security event manager* (SEM): Real-time monitoring, correlation of events, notifications and console views.
- *Security information and event management* (SIEM): Combines SIM and SEM and provides real-time analysis of security alerts generated by network hardware and applications.[1][25]
- *Managed Security Service:* (MSS) or *Managed Security Service Provider:* (MSSP): The most common managed services appear to evolve around connectivity and bandwidth, network monitoring, security, virtualization, and disaster recovery.
- *Security as a service (SECaaS)*: These security services often include authentication, anti-virus, anti-malware/spyware, intrusion detection, penetration testing and security event

management, among others.

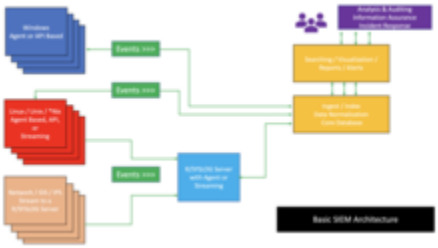
In practice many products in this area will have a mix of these functions, so there will often be some overlap – and many commercial vendors also promote their own terminology.[26] Oftentimes commercial vendors provide different combinations of these functionalities which tend to improve SIEM overall. Log management alone doesn't provide real-time insights on network security, SEM on its own won't provide complete data for deep threat analysis. When SEM and log management are combined, more information is available for SIEM to monitor.

A key focus is to monitor and help manage user and service privileges, directory services and other system-configuration changes; as well as providing log auditing and review and incident response.[24]

Capabilities

- **Data aggregation:** Log management aggregates data from many sources, including networks, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.
- **Correlation:** Looks for common attributes and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information. Correlation is typically a function of the Security Event Management portion of a full SIEM solution[27]
- **Alerting:** The automated analysis of correlated events
- **Dashboards:** Tools can take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern.
- **Compliance:** Applications can be employed to automate the gathering of compliance data, producing reports that adapt to existing security, governance and auditing processes.[28]
- **Retention:** Employing long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements. The Long term log data retention is critical in forensic investigations as it is unlikely that the discovery of a network breach will be at the time of the breach occurring.[29]
- **Forensic analysis:** The ability to search across logs on different nodes and time periods based on specific criteria. This mitigates having to aggregate log information in your head or having to search through thousands and thousands of logs.[28]

Components



Basic SIEM Infrastructure

SIEM architectures may vary by vendor; however, generally, essential components comprise the SIEM engine. The essential components of a SIEM are as follows:[30]

- A data collector forwards selected audit logs from a host (agent based or host based log streaming into index and aggregation point) [31][32]
- An ingest and indexing point aggregation point for parsing, correlation, and data normalization [33]
- A search node that is used for visualization, queries, reports, and alerts (analysis take place on a search node) [34]

A basic SIEM infrastructure is depicted in the image to the right.

Use cases

Computer security researcher Chris Kubecka identified the following SIEM use cases, presented at the hacking conference 28C3 (Chaos Communication Congress).[35]

- SIEM visibility and anomaly detection could help detect zero-days or polymorphic code. Primarily due to low rates of anti-virus detection against this type of rapidly changing malware.
- Parsing, log normalization and categorization can occur automatically, regardless of the type of computer or network device, as long as it can send a log.

- Visualization with a SIEM using security events and log failures can aid in pattern detection.
- Protocol anomalies that can indicate a misconfiguration or a security issue can be identified with a SIEM using pattern detection, alerting, baseline and dashboards.
- SIEMS can detect covert, malicious communications and encrypted channels.
- Cyberwarfare can be detected by SIEMs with accuracy, discovering both attackers and victims.

Correlation rules examples

SIEM systems can have hundreds and thousands of correlation rules. Some of these are simple, and some are more complex. Once a correlation rule is triggered the system can take appropriate steps to mitigate a cyber attack. Usually, this includes sending a notification to a user and then possibly limiting or even shutting down the system. According to UTMStack (https://utmstack.com/siem-correlation-rules/) , these are some of the most important ones.

Brute Force Detection

Brute force detection is relatively straightforward. Brute forcing relates to continually trying to guess a variable. It most commonly refers to someone trying to constantly guess your password - either manually or with a tool. However, it can refer to trying to guess URLs or important file locations on your system.

An automated brute force is easy to detect as someone trying to enter their password 60 times in a minute is impossible.

Impossible Travel

When a user logs in to a system, generally speaking, it creates a timestamp of the event. Alongside the time, the system may often record other useful information such as the device used, physical location, IP address, incorrect login attempts, etc. The more data is collected the more use can be gathered from it. For impossible travel, the system looks at the current and last login date/time and the difference between the recorded distances. If it deems it's not possible for this to happen, for example traveling hundreds of miles within a minute, then it will set off a warning.

Many employees and users are now using VPN services which may obscure physical location. This should be taken into consideration when setting up such a rule.

Excessive File Copying

If you think about your day-to-day activities, you most likely don't copy or move a lot of files around on your system. Therefore any excessive file copying on a system could be attributed to someone wanting to cause harm to your company. Unfortunately, it's not as simple as stating someone has gained access to your network illegally and wants to steal confidential information. It could also be an employee looking to sell company information, or they could just want to take home some files for the weekend.

DDoS Attack

A DDoS (Distributed Denial of Service) Attack would cause an issue for pretty much any company. A DDoS attack can not only take your web properties offline, it can also make your system weaker. With suitable correlation rules in place, your SIEM should trigger an alert right at the start of the attack so that you can take the necessary precautionary measures to protect your systems.

File Integrity Change

File Integrity and Change Monitoring (FIM) is the process of monitoring the files on your system. Unexpected changes in your system files will trigger an alert as it's a likely indication of a cyber attack.

Models

Alongside correlation rules, it's also possible for SIEM to have models. Models differ somewhat from correlation rules but if implemented correctly can be just as useful. Instead of using a one-to-one correlation, a model requires a number of steps to happen in order to trigger an alert. This usually means a first-time rule followed by an anomalous behavior. This can be as simple as a user logging in from a different location than usual and then carrying out a large file transfer.

This can be extremely useful as a single event does not necessarily mean a compromise of an organization's servers or network, it could just be a team member working from a café for a

change in scenery.

Handling False Positives

Unfortunately, false positives appear in all walks of life, and this holds true for SIEM. All tools and systems have the possibility to produce a false-positive result. For example, too many failed login attempts can just be an employee forgetting their password and not someone trying to break into the system. It's important that for any triggered events the steps taken are justifiable and of an appropriate measure as you wouldn't want employees getting locked out for hours in such scenarios.[36]

Alerting examples

Some examples of customized rules to alert on event conditions involve user authentication rules, attacks detected and infections detected.[37]

Rule	Goal	Trigger	Event Sources
Repeat Attack-Login Source	Early warning for brute force attacks, password guessing, and misconfigured applications.	Alert on 3 or more failed logins in 1 minute from a single host.	Active Directory, Syslog (Unix Hosts, Switches, Routers, VPN), RADIUS, TACACS, Monitored Applications.
Repeat Attack-Firewall	Early warning for scans, worm propagation, etc.	Alert on 15 or more Firewall Drop/Reject/Deny Events from a single IP Address in one minute.	Firewalls, Routers and Switches.
Repeat Attack-Network Intrusion Prevention System	Early warning for scans, worm propagation, etc.	Alert on 7 or more IDS Alerts from a single IP Address in one minute	Network Intrusion Detection and Prevention Devices
Repeat Attack-Host Intrusion Prevention System	Find hosts that may be infected or compromised (exhibiting infection behaviors)	Alert on 3 or more events from a single IP Address in 10 minutes	Host Intrusion Prevention System Alerts
Virus Detection/Removal	Alert when a virus, spyware or other malware is detected on a host	Alert when a single host sees an identifiable piece of malware	Anti-Virus, HIPS, Network/System Behavioral Anomaly Detectors
Virus or Spyware Detected but Failed to Clean	Alert when >1 Hour has passed since malware was detected, on a source, with no corresponding virus successfully removed	Alert when a single host fails to auto-clean malware within 1 hour of detection	Firewall, NIPS, Anti-Virus, HIPS, Failed Login Events

See also

- IT risk

- Log management
- Security event manager
- Security information management

References

1. *"SIEM: A Market Snapshot" (http://www.drdobbs.com/197002909)* . *Dr.Dobb's Journal. 5 February 2007.*
2. *Williams, Amrit (2005-05-02). "Improve IT Security With Vulnerability Management" (https://www.gartner.com/doc/480703/improve-it-security-vulnerability-management)* . *Retrieved 2016-04-09. "Security information and event management (SIEM)"*
3. *Ruthberg, Zella; McKenzie, Robert (1977-10-01). "Audit and Evaluation of Computer Security" (https://csrc.nist.gov/publications/detail/sp/500-19/archive/1977-10-01)* . *doi:10.6028/NBS.SP.500-19 (https://doi.org/10.6028%2FNBS.SP.500-19)* .
4. *Johnson, Arnold; Dempsey, Kelley; Ross, Ron; Gupta, Sarbari; Bailey, Dennis (October 2019). "Guide for security-focused configuration management of information systems" (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf) (PDF). Gaithersburg, MD: NIST SP 800–128. doi:10.6028/nist.sp.800-128 (https://doi.org/10.6028%2Fnist.sp.800-128)* . *S2CID 63907907 (https://api.semanticscholar.org/CorpusID:63907907)* .
5. *"Improving the Nation's Cybersecurity" (https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity)* . *Federal Register. 2021-05-17. Retrieved 2021-07-28.*
6. *Kent, Karen; Souppaya, Murugiah (2006-09-13). "Guide to Computer Security Log Management" (https://csrc.nist.gov/publications/detail/sp/800-92/final)* . *doi:10.6028/NIST.SP.800-92 (https://doi.org/10.6028%2FNIST.SP.800-92)* . *S2CID 221183642 (https://api.semanticscholar.org/CorpusID:221183642)* .
7. *Computer Security Division, Information Technology Laboratory (2016-11-30). "Release Search - NIST Risk Management Framework | CSRC | CSRC" (https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search)* . *CSRC | NIST. Retrieved 2021-06-13.*
8. *Computer Security Division, Information Technology Laboratory (2016-11-30). "NIST Risk Management Framework | CSRC | CSRC" (https://csrc.nist.gov/Projects/Risk-Management)* . *CSRC | NIST. Retrieved 2021-07-23.*
9. *"Understanding the NIST cybersecurity framework" (https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework)* . *Federal Trade Commission. 2018-10-05. Retrieved 2021-07-23.*
10. *Rights (OCR), Office for Civil (2009-11-20). "Summary of the HIPAA Security Rule" (https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html)* . *HHS.gov. Retrieved 2021-07-23.*

11. *"The Role of Information Security in Sarbanes-Oxley Compliance" (https://doi.org/10.48009/2_iis_2005_124-130)* . *Issues in Information Systems. 2005. doi:10.48009/2_iis_2005_124-130 (https://doi.org/10.48009%2F2_iis_2005_124-130)* . *ISSN 1529-7314 (https://www.worldcat.org/issn/1529-7314)* .
12. *"Mapping PCI DSS v3_2_1 to the NIST Cybersecurity Framework v1_1" (https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf?agreement=true&time=1627059974846)* *(PDF). July 2019.*
13. *"NIST SP 800-53, Revision 5 Control Mappings to ISO/IEC 27001" (https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r5-to-iso-27001-mapping.docx)* . *10 December 2020.*
14. *Computer Security Division, Information Technology Laboratory (2016-11-30). "Release Search - NIST Risk Management Framework | CSRC | CSRC" (https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search)* . *CSRC | NIST. Retrieved 2021-07-18.*
15. *"Risk management framework for information systems and organizations" (https://doi.org/10.6028/NIST.SP.800-37r2)* . *Gaithersburg, MD. December 2018. doi:10.6028/nist.sp.800-37r2 (https://doi.org/10.6028%2Fnist.sp.800-37r2)* .
16. *"Guide for conducting risk assessments" (https://doi.org/10.6028/NIST.SP.800-30r1)* . *Gaithersburg, MD. 2012. doi:10.6028/nist.sp.800-30r1 (https://doi.org/10.6028%2Fnist.sp.800-30r1)* .
17. *"Improving the Nation's Cybersecurity" (https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity)* . *Federal Register. 2021-05-17. Retrieved 2021-07-18.*
18. *Computer Security Division, Information Technology Laboratory (2016-11-30). "Release Search - NIST Risk Management Framework | CSRC | CSRC" (https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search)* . *CSRC | NIST. Retrieved 2021-07-19.*
19. *"Security and Privacy Controls for Information Systems and Organizations" (https://doi.org/10.6028/NIST.SP.800-53r5)* . *2020-09-23. doi:10.6028/nist.sp.800-53r5 (https://doi.org/10.6028%2Fnist.sp.800-53r5)* . *S2CID 238185691 (https://api.semanticscholar.org/CorpusID:238185691)* .
20. *Mavroeidis, Vasileios; Jøsang, Audun (2018-03-16). "Data-Driven Threat Hunting Using Sysmon" (https://doi.org/10.1145/3199478.3199490)* . *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy. ICCSP 2018. Guiyang, China: Association for Computing Machinery: 82–88. arXiv:2103.15194 (https://arxiv.org/abs/2103.15194)* . *doi:10.1145/3199478.3199490 (https://doi.org/10.1145%2F3199478.3199490)* . *ISBN 978-1-4503-6361-7. S2CID 49864578 (https://api.semanticscholar.org/CorpusID:49864578)* .
21. *Force, Joint Task (2020-12-10). "Security and Privacy Controls for Information Systems and Organizations" (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)* . *doi:10.6028/NIST.SP.800-53r5 (https://doi.org/10.6028%2FNIST.SP.800-53r5)* . *S2CID 238185691 (https://api.semanticscholar.org/CorpusID:238185691)* .

22. Swift, David (26 December 2006). "A Practical Application of SIM/SEM/SIEM, Automating Threat Identification" (http://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781) (PDF). SANS Institute. p. 3. Retrieved 14 May 2014. "...the acronym SIEM will be used generically to refer..."

23. Kent, Karen; Souppaya, Murugiah (September 2006). "Guide to Computer Security Log Management" (https://csrc.nist.gov/publications/detail/sp/800-92/final) . Computer Security Resource Center, NIST. doi:10.6028/NIST.SP.800-92 (https://doi.org/10.6028%2FNIST.SP.800-92) . S2CID 221183642 (https://api.semanticscholar.org/CorpusID:221183642) . SP 800-92.

24. Jamil, Amir (29 March 2010). "The difference between SEM, SIM and SIEM" (http://www.gmdit.com/NewsView.aspx?ID=9IfB2Axzeew=) .

25. The Future of SIEM - The market will begin to diverge (http://techbuddha.wordpress.com/2007/01/01/the-future-of-siem-%E2%80%93-the-market-will-begin-to-diverge/)

26. Bhatt, S.; Manadhata, P.K.; Zomlot, L. (2014). "The Operational Role of Security Information and Event Management Systems" (https://ieeexplore.ieee.org/document/6924640) . IEEE Security & Privacy. **12** (5): 35–41. doi:10.1109/MSP.2014.103 (https://doi.org/10.1109%2FMSP.2014.103) . S2CID 16419710 (https://api.semanticscholar.org/CorpusID:16419710) .

27. Correlation (http://securityinformationeventmanagement.com/security-event-management.php) Archived (https://web.archive.org/web/20141019131638/http://securityinformationeventmanagement.com/security-event-management.php) 2014-10-19 at the Wayback Machine

28. "Compliance Management and Compliance Automation – How and How Efficient, Part 1" (https://web.archive.org/web/20110723002943/http://www.accelops.net/blog/?p=149) . accelops.net. Archived from the original (http://www.accelops.net/blog/?p=149) on 2011-07-23. Retrieved 2018-05-02.

29. "2018 Data Breach Investigations Report | Verizon Enterprise Solutions" (http://www.verizonbusiness.com/about/events/2012dbir/) . Verizon Enterprise Solutions. Retrieved 2018-05-02.

30. Kotenko, Igor; Polubelova, Olga; Saenko, Igor (November 2012). "The Ontological Approach for SIEM Data Repository Implementation" (https://ieeexplore.ieee.org/document/6468405) . 2012 IEEE International Conference on Green Computing and Communications. Besancon, France: IEEE: 761–766. doi:10.1109/GreenCom.2012.125 (https://doi.org/10.1109%2FGreenCom.2012.125) . ISBN 978-1-4673-5146-1. S2CID 18920083 (https://api.semanticscholar.org/CorpusID:18920083) .

31. Kotenko, Igor; Chechulin, Andrey (November 2012). "Common Framework for Attack Modeling and Security Evaluation in SIEM Systems" (https://ieeexplore.ieee.org/document/6468300) . 2012 IEEE International Conference on Green Computing and Communications: 94–101. doi:10.1109/GreenCom.2012.24 (https://doi.org/10.1109%2FGreenCom.2012.24) . ISBN 978-1-4673-5146-1. S2CID 15834187 (https://api.semanticscholar.org/CorpusID:15834187) .

32. Karl-Bridge-Microsoft. "Eventlog Key - Win32 apps" (https://docs.microsoft.com/en-us/windows/win32/eventlog/eventlog-key) . docs.microsoft.com. Retrieved 2021-07-18.

33. *Kotenko, Igor; Polubelova, Olga; Saenko, Igor (November 2012). "The Ontological Approach for SIEM Data Repository Implementation" (https://ieeexplore.ieee.org/document/6468405) . 2012 IEEE International Conference on Green Computing and Communications: 761–766. doi:10.1109/GreenCom.2012.125 (https://doi.org/10.1109%2FGreenCom.2012.125) . ISBN 978-1-4673-5146-1. S2CID 18920083 (https://api.semanticscholar.org/CorpusID:18920083) .*

34. *Azodi, Amir; Jaeger, David; Cheng, Feng; Meinel, Christoph (December 2013). "Pushing the Limits in Event Normalisation to Improve Attack Detection in IDS/SIEM Systems" (https://ieeexplore.ieee.org/document/6824575) . 2013 International Conference on Advanced Cloud and Big Data: 69–76. doi:10.1109/CBD.2013.27 (https://doi.org/10.1109%2FCBD.2013.27) . ISBN 978-1-4799-3261-0. S2CID 1066886 (https://api.semanticscholar.org/CorpusID:1066886) .*

35. *"28c3: Security Log Visualization with a Correlation Engine" (https://www.youtube.com/watch?v=j4pF9VUdphc) . YouTube. December 29, 2011. Archived (https://ghostarchive.org/varchive/youtube/20211215/j4pF9VUdphc) from the original on 2021-12-15. Retrieved November 4, 2017.*

36. *"Essential SIEM Correlation Rules for Compliance" (https://utmstack.com/siem-correlation-rules/) . UTMStack. 17 November 2020.*

37. *Swift, David (2010). "Successful SIEM and Log Management Strategies for Audit and Compliance" (https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528) . SANS Institute.*

Last edited 7 days ago by 73.244.173.204

WIKIPEDIA