NATIONAL SECURITY AGENCY
CYBERSECURITY REPORT

HARDENING SIEM SOLUTIONS

A TECHNICAL REPORT FROM NETWORK INFRASTRUCTURE SECURITY

Date of Report 29 October 2019

DOCUMENT CHANGE HISTORY

DATE	VERSION	DESCRIPTION
10/08/19	1.0	

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

ADDITIONAL DISCLAIMER

For more specific or step-by-step instructions on how to implement these security methods, please seek documentation or consultation with the SIEM provider. Not all security measures may be relevant or available for certain vendors. When purchasing a SIEM solution, keep security features in mind. The recommendations included in this paper are not an exhaustive list.

CONTACT INFORMATION

For general cybersecurity inquiries and reporting, contact the NSA Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov .

For media inquiries, contact Press Desk: 443-634-0721 Email: MediaRelations@nsa.gov

Contents

WHAT ARE SIEM SOLUTIONS?

Security Information and Event Management (SIEM) solutions make investigating large amounts of data easier and faster for administrators. SIEM solutions collect logs and traffic from across the enterprise and format the data to allow for efficient searching and correlation. Additionally, SIEMs can provide alerting, basic incident response (IR), dashboards, and reporting, and integrations for data enrichment. Without a SIEM solution, analysts would have to log in to multiple devices to manually search and correlate hundreds of logs and events. But SIEM solutions oversee an organization's most critical network and host data, and a compromised SIEM allows a threat actor to monitor defenders in order to stay in. As a critical nerve-center of the network, a SIEM must be properly secured.

RISK

Although SIEMs are great for log aggregation and correlation, threat detection, and incident response, they can also pose a security risk if not properly hardened. A 2018 report from Carbon Black reported that 72% of IR professionals saw log destruction—such as deletion of antivirus and security logs—during attacks [1]. While a SIEM can help mitigate log destruction by exporting logs from their original locations, if poorly secured it can be an attractive target for an attacker looking to delete critical logs to cover their tracks.

If an attacker gains access to an organization's SIEM solution or collects unencrypted traffic from it, then the organization's critical network information is exposed. This critical network information can be IP addresses and domain names of critical assets, usernames, operating systems (OS), services running, etc. Many SIEMs integrate with vulnerability scanners to import and correlate device vulnerability data with event data. The attacker will know what attacks are most likely to work because the SIEM has told them what assets the organization has, the location of each asset, and what vulnerabilities it may have. Additionally, they may cover their tracks by deleting certain logs or events. They will also be privy to any actions in the SIEM indicative of incident response actions such as evictions, allowing them to take evasive action. Advanced attackers are very difficult to prevent, detect, and evict. Each security measure taken can be circumvented in one way or another, therefore, one security measure is not enough to protect against an attacker. Securing an organization's SI EM solution is important to protect the organization and its assets.

SECURING THE SIEM

An attacker may try to gain physical or remote access to an organization's SIEM solution. Possible goals include stealing information about the organization to plan an attack and preventing administrators from detecting the attack. SIEM administrators must take security measures to protect the SIEM hardware, software, and data from any angle of attack.

Secure the Physical Hardware

If an attacker gains access to an organization's SIEM appliance, they may be able to connect removable media such as a USB device to exfiltrate data or install malware such as a keystroke logger. While unlikely, they may even try to destroy evidence by physically stealing, or damaging the hardware, thus preventing security personnel from using the SIEM to see the attacker's actions. Ensure the hardware is in a locked server rack in a locked room. Limit room and rack access to only authorized personnel.

Secure the Operating System

Vulnerabilities in the OS running a SIEM product could provide attackers a way into the SIEM. Ensure the host-based firewall is on and blocking unnecessary ports. Limit Internet access into the SIEM appliance. If 3rd party integration (such as cloud reputation lookup or other services) is required, then closely constrain connections from the SIEM to known services. Remove unnecessary programs and turn off unnecessary services. Utilize patch management to ensure the OS and software are getting regular security updates. Run anti-malware software on the OS. Enforce applicable OS security policies. Furthermore, ensure accounts on the OS are secure (see password account suggestions in the *Secure the Instance* section). Take a baseline of the OS to identify unauthorized changes and maintain a configuration back up.[1]

[1] These suggestions above are not an exhaustive list. Consult the Center for Internet Security (CIS) Benchmarks at https://learn.cisecurity.org/benchmarks for more specific and thorough operating system configuration guidance.

Secure the Downloaded Package and Installation

When downloading SIEM software from the Internet, ensure that the software has not been tampered. One way to check the integrity of the package is to see if the package is digitally signed and verify the signature is valid. Another way is to compare the hash value of the download to the hash value from the vendor using a secure algorithm such as SHA-512. If the SIEM utilizes third party packages, the packages should be signed by the third party and the SIEM solution should verify the authenticity of the signatures.

Install the software in a directory that is protected. For example, the Windows® Program Files directory is protected by file/folder permissions and User Account Control (UAC).

Configure the enterprise Network Access Controls (NAC) to only allow policy-compliant workstations to connect to the SIEM. NACs implement control policies and user access controls to protect the network.

Secure the Instance

The SIEM solution itself may contain vulnerabilities either in the software or in the way it was configured. This includes authentication settings, software and its features, and connections and communications.

Authentication

Utilize multi-factor authentication (MFA). MFA provides extra security by adding protection in layers. NSA generally recommends utilizing the combination of token-based and knowledge-based authentication (e.g. PKI smart card and PIN).[2] A SIEM is a critical and relatively easy location to implement MFA, since relatively few users have access to SIEMs (compared to the general population). Always change default passwords or remove these accounts entirely. Attempting to log in with default credentials is one of the first things an attacker will try. Enforce policies to ensure multi-factor authentication is mandatory for all accounts. Avoid shared accounts wherever possible. When one account is used by multiple people, it makes it difficult to hold people accountable for configuration changes. Additionally, shared accounts are more likely to be compromised. If passwords alone must be used then enforce strict requirements on length, complexity, reuse, expiration, and lockout.

Practice the principle of least privilege. Restrict access rights to the minimum accesses the user or account needs to do the job. Implement access controls to restrict user access to sensitive data and critical administrative functions. Most SIEMs offer a variety of account roles that allow for customizing those accounts at a granular level. In larger organizations, most analysts looking at logs only need read access to data and perhaps to take certain actions. Even for small “jack-of-all-trades” teams, separate accounts can be used for administering the features of the SIEM.

Many SIEM solutions integrate with external directories such as Lightweight Directory Access Protocol (LDAP). When using LDAP, configure LDAP over TLS (LDAPS), which encrypts LDAP communications. Many SIEM solutions support Single-Sign-On (SSO) with Kerberos or New Technology LAN Manager (NTLM) and Active Directory®. One downside of using this SSO approach is the risk of hashed passwords or Kerberos tickets being stolen and replayed in “pass-the-hash” or “pass-the-ticket” attacks.

Run software on an unprivileged service account instead of a root or administrator account, if possible. Secure service accounts by locking down settings. Service accounts are more powerful than user accounts and therefore should be used by as few processes as possible. For more guidance with service accounts, see “Securing Windows Service Accounts” published by the SANS Institute [2].

Software and Configurations

To ensure the SIEM software is secure, immediately update the software (including both the SIEM and the OS and applications on it) whenever security updates are available. Check the vendor’s website regularly for vulnerability announcements such as the release of new Common Vulnerabilities and Exposures (CVE) or sign up for vulnerability announcement newsletters or data feeds. The CVE list by MITRE provides an email newsletter and social media data

[2] For more information, please refer to “Transition to Multi-Factor Authentication” an NSA Cybersecurity Top 10 Mitigation.

feeds for vulnerability announcements [3]. The National Vulnerability Database by National Institute of Standards and Technology (NIST) provides many data feed options to receive vulnerability announcements including Rich Site Summary (RSS), JavaScript Object Notation (JSON), and Extensible Markup Language (XML) [4].

Disable unnecessary features or components as these could pose security risks. Check with the SIEM vendor to see if security add-ons are available.

An attacker may try to change the configurations on the SIEM solution to evade detection. Ensure change management is in place to identify unauthorized changes. Ways to accomplish this include: using a configuration management tool to provide version control, integrating SIEM configuration changes into an existing change management framework, or configuring the SIEM to monitor its own configuration files (if possible). Ensure high-risk changes trigger alerts which are sent to authorized administrators using a channel like email or phone call.

Connections and Communications

An attacker may try to intercept traffic not only for authentication information but also for information about the organization's network and assets. Such information can be used to speculate what vulnerabilities an organization might have. Using this information, an attacker can choose an exploit that is likely to succeed. Several communications/connections to protect include:

- Users and administrators accessing the SIEM web interface over the internet
- Administrators accessing the SIEM host remotely
- Logs and events getting forwarded over the network to the SIEM solution
- Integrations with third party services

Browsers. When connecting to the web interface over the internal network, use the latest version of a supported internet browser. Block JavaScript® and Flash®, if possible. If JavaScript or Flash is necessary, use the latest version.

Encryption and Certificates. Use TLS encryption to protect authentication and log traffic. Access the site using HTTPS, which requires the SIEM web interface to be configured with TLS. Ensure that TLS 1.2 or better is used to prevent vulnerabilities associated with weaker TLS versions.

Do not use default certificates, either for the web-based interface on the server, or for securing communications with agents, log servers, databases, and other components integrated with the SIEM. Use certificates signed by a trusted Certificate Authority (CA). If purchasing certificates from a CA is not possible, then replace default certificates with certificates signed by the organization's root CA. To further strengthen, use common name checking. The browsers of dedicated management workstations connecting to the SIEM web interface must be configured to trust the CA that signed the SIEM's certificate. By trusting the CA, the browsers will trust the SIEM's certificate.

TLS also provides encryption which can help prevent an attacker from viewing potentially sensitive data, such as SIEM administrator credentials, traversing the network. If an attacker compromises the SIEM's private key, the attacker could decrypt traffic from the SIEM solution. Protect the private key by utilizing privilege and permission restrictions on the folders where the private key sits. Certain products also support variants of on-disk encryption on the folders where the private key sits.

If it is suspected that a SIEM solution's private key(s) is compromised, revoke the SIEM certificate and generate a new certificate and corresponding private key. This depends on the certificate being revocable (including being tied to a certificate authority) beforehand.

Avoid sending logs in plaintext, especially security critical logs and bulk log forwarding where the impact of exposure is particularly high. Avoid using native syslog which sends data in plaintext.

Some products may have a Federal Information Processing Standard (FIPS) mode that ensures the product complies with US Government standards for cryptographic software. This setting prevents the product from using known weak encryption.

Remote Access. Remote access introduces an additional opportunity for attackers to get into the network. If possible, block remote access to the SIEM server and services. If utilizing remote access, ensure that a secure protocol using TLS or SSH is used. This will encrypt the traffic, verify to the client that the SIEM is who it claims to be, and protect the data from prying eyes. Limit shell/command line access to SIEM servers and services to allow only authorized users access. Set an appropriate timeout for remote sessions and preferably do not allow more than one concurrent connection using the same account. If allowing remote access, the systems allowed to connect should preferably only be owned and managed by the organization, rather than unsecured and unmanaged personally-owned systems. One possible practice is to provide organization-owned equipment such as laptops where users do not have administrative rights, only authorized software is allowed to be installed, and soft or hard PKI credentials are used to connect in via encrypted VPNs.

Third Party Integrations. SIEM solutions often integrate with third party products (e.g. threat reputation services, app providers, analytic providers, providers of other parts in a stack, etc.). Only integrate with trusted third parties. To request third party services, the SIEM may make outbound connections to the third party Internet servers. Make sure these connections occur over secure channels such as TLS and flow through the security devices protecting the enterprise network. Be wary of sending data from the SIEM solution to third parties, particularly non-anonymized data.

Network Segregation. Segregate network traffic on a separate VLAN from management traffic and protect all the traffic with a network firewall. On the firewall, follow a deny-by-default policy. Make a list of ports necessary for the SIEM solution to work properly and open only those ports. Connections may include a port for accessing the web interface, a port to listen for incoming data, and a port for management. Use network Access Control Lists (ACL) to limit the IP addresses that can access various parts of the organization's networks.

Other Settings. The SIEM solution may offer its own additional security settings such as IP whitelisting, IP blacklisting, web session timeout, and the maximum size of data accepted. Utilize such features if available. Consider implementing denial of service countermeasures such as rules blocking IPs which open large numbers of partial connections.

Protecting Data at Rest

Back up data and configurations regularly and test them periodically. Backups should be kept on a separate network or at least a separate server. Backups kept on the same server or network as the log data are susceptible to the same risks as the log data. Off-line off-site backups are the most secure. Both original data and backup data should be protected by file system Access Control Lists (ACL) (not to be confused with network ACLs). File system ACLs restrict access to objects (e.g. files, folders, etc.) which prevents unauthorized actors from accessing the log data on the disk.

Enable on-disk encryption for servers holding logs. This will protect the data if it is physically stolen out of a data center. If necessary, utilize Data Integrity features which compute hash values on every slice of data and separately store those hashes for verification of the data's integrity.

Turn on alerts for risky commands such as deleting or exporting data. An attacker may try to clear logs to cover their tracks. Logs should not be deleted outside of the age-off schedule. If an administrator receives an alert that local logs have been deleted before the defined age-off, it should be considered a high priority security concern.

Logs and other data forwarded to the SIEM solution may contain sensitive data. Utilize the SIEM solution's masking feature to protect data such as credit card information or social security numbers. Make sure there are no plain text passwords visible. Information gained such as usernames and passwords can be used by an attacker to traverse the network.

AUDITING AND COMPLIANCE

Regularly perform audits to keep track of activity in a system. Perform a periodic review of: SIEM access and audit logs; SIEM server audit and security logs; SIEM users and roles. Follow vendor security guidance on how to implement their product in a secure way.

Some laws and policies may determine how long certain types of data, such as Personally Identifiable Information (PII) can be retained. Determine if any laws and policies apply to the logs and data the organization collects and set data age-off to an appropriate amount of time on the data source and any servers/devices containing this data. In the case of a compromise, this limits the amount of data an attacker gains access to. Know what information the organization keeps, retain only what is necessary, protect what is kept, and properly dispose of what the organization doesn't need [5].

CONCLUSION

SIEM solutions can help analysts detect threats but, if not secured properly, can introduce vulnerabilities. Security professionals need to plan security measures not only for their SIEM software but also for the hardware, OS running the software, and data collected. An attacker's work is made more difficult if an organization properly secures its SIEM solution.

REFERENCES

[1] "Global Incident Response Threat Report," Carbon Black, November 2018. [Online] Available: https://www.carbonblack.com/global-incident-response-threat-report/november-2018/

[2] G. Rice, "Securing Windows Service Accounts," SANS Institute, 03 March 2005. [Online] Available: https://cyber-defense.sans.org/resources/papers/gsec/securing-windows-service-accounts-107116

[3] "CVE Data Updates and RSS Feeds," CVE, MITRE Corporation. [Online] Available: https://cve.mitre.org/cve/data_updates.html

[4] "NVD Data Feeds," National Vulnerability Database, National Institute of Standards and Technology. [Online] Available: https://nvd.nist.gov/vuln/data-feeds

[5] "Protecting Personal Information: A Guide for Business," Federal Trade Commission, October 2016. [Online] Available: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business