**Description**

Insufficient Logging and Monitoring is a rather broad category encompassing substandard installation and configuration of security tools and defensive tactics, resulting in inherent deficiencies in the ability to identify anomalies and/or intrusions within an environment. The problem is pervasive, so much so that in 2017, this rather broad category of risk was listed in the OWASP Top 10 for the first time. Indeed, malicious actors effectively rely on the absence or lack of effective monitoring to evade detection long enough to deploy the tools that will lead to compromise.

Insufficient Logging and Monitoring differs to other categories in the OWASP Top 10 as it is not a technically exploitable vulnerability per se; rather, it is more a set of (or as its namesake suggests, a lack of) detection and response implementations and best practices which when combined, could coalesce in a failure to detect a breach, a prolonged delay in breach identification, and an added complexity when performing post-breach digital forensics.

A primary issue faced by security and administration teams is that the amount of logs generated in an environment can be so vast in number and spread across different technology components within the overall environment, that effective monitoring can become... rather less effective than optimal.

Ensuring effective logging and monitoring is crucial within any IT infrastructure environment; without these mechanisms in place, it is very difficult for an organization to gauge its security status.

Insufficient Logging and Monitoring occurs when:

* Security Information and Event Management (SIEM) systems are not configured correctly and thus are unable to process and flag relevant events.
* Logs of applications, devices, and/or APIs are not monitored for anomalous behavior.
* Warnings that are generated serve to confuse, rather than clarify, threats.
* Logs are not adequately protected and may be at risk of tampering/deletion by malicious actors covering their tracks.
* Logins, failed logins, and high-value transactions are not logged due to misconfiguration or non-configuration, leading to difficulties in auditing processes.
* Logs are only stored locally with no redundancy.

**Impact**

If logging and monitoring systems are both installed and properly configured in a manner suitable for their environment, anomalous events occurring in a network or against a web application have a greater chance of being flagged and potentially halted.

The genesis of most successful attacks begins with reconnaissance and vulnerability probing. If, during this initial phase of assessment, the probes go unnoticed due to insufficient logging and monitoring, the chance of stopping the attack early is missed, thus increasing the probability of a successful exploitation.

In addition, the time to identify that a breach had even occurred in an environment in 2017 was, on average, [191 days](https://www.ibm.com/downloads/cas/ZYKLN2E3). Thus, highlighting a specific example of the ramifications of poorly implemented logging and monitoring tools, teams, and processes, is a fairly moot point since virtually *all* successful attacks were successful in some way as a result of insufficient monitoring, or ineffective actioning of monitoring output.

**Prevention**

Determining which systems to bolster and which to compromise on due to resource constraints is an important choice faced by teams responsible for an organization's security. As a general rule, the higher value the data possesses, the more security controls, in this case, logging and monitoring, should be implemented to sound the alarm. Importantly, logging for logging-sake is not a solution; too many logs are part of the problem.

Administrators must:

* Log application errors, runtime errors, connectivity issues, file system errors, and configuration alterations.
* Log server-side input validation, login, and access control failures, with sufficient detail of the user.
* Log high-risk functionality, including access to payment cardholder data, key changes, data-encrypting key use, all actions by administrative user accounts, token addition or deletion etc.
* Ensure inter-departmental collaboration and clarity concerning legal and compliance needs within the organization, and the relevant logging and monitoring required to comply with any regulatory frameworks, such as Sarbanes-Oxley, PCI-DSS, or HIPAA.
* Converge the log streams to an auditable and centralized logging system with adequate redundancy.
* Ensure audit trails, and additional security provisions, are implemented to prevent log tampering.
* Create an incident response plan that ensures logs can be furnished in the event of a post-breach audit.

**Testing**

Ensure that the application's logs are clear and can be easily monitored and analyzed either locally or log shipped to a remote monitoring system.

* **OWASP ASVS**: [7.2](https://github.com/OWASP/ASVS/releases/download/v4.0.2_release/OWASP.Application.Security.Verification.Standard.4.0.2-en.pdf)
* **OWASP Testing Guide**: [Test Application Platform Configuration](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/02-Test_Application_Platform_Configuration)

**References**

[OWASP - Insufficient Logging and Monitoring](https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A10-Insufficient_Logging%252526Monitoring)

[MITRE - CWE-778 Insufficient Logging](https://cwe.mitre.org/data/definitions/778.html)