Secure Logging Standards

Contents

Secure Logging Standards

Logging Standards

These security logging standards from the GE Digital Platform & Product Cybersecurity (GED P&P Cybersecurity) team define the security events to be logged by tenant applications. GED P&P Cybersecurity recommends that tenant application land/or service logs contain adequate amount of information to identify, investigate and resolve adverse security events. Standards may evolve from periodic assessments.

Logging Attributes

The GED P&P Cybersecurity team requires the following attributes to be included in the logs:

Table 1:

Attributes	Description
What	Type of event that occurred
Where	Source of the event (source, destination and protocol details)
Who	System user or device identification associated with the event
When	Time event occurred (i.e. date and timestamp)
Outcome	Success or failure of the event

Log generating sources must be configured to alert respective system or service owners of log capturing and processing failures, such as:

- When a system is shutting down
- When a system is overwriting its oldest log records
- When the log capturing mechanism has failed
- When the storage capacity for the logs has reached or exceeded its limit

Security Events Identified in Logs

The following security events may apply to tenant applications and services based on the design and development of the application and/or service. It is the application developer's responsibility to identify which event categories will apply to their own applications and/or services, and provide the corresponding logs to GED P&P Cybersecurity for review, ingestion and monitoring.

Table 2:

No.	Event Category	Security Event Types
1	Audit and Accountability	• Shutdown or unavailability of the "logging function" to gather, store or analyze logs • Deletion, deactivation or modifications of log files on an application and application monitoring tools
2	Security Operations	• Startup and shutdown of an application • Serious failure errors (e.g. device crash or failure to restart), application unavailability and exception events such as communication error

No.	Event Category	Security Event Types
3	Security Administration	• Changes (successful and failed) to security configurations of an application (e.g. enable/disable security policies, change in user rights, log settings, certification services etc.) • Addition of an administrative or a group • Alteration (success and failure) in account privileges • Attempts (success and failure) to change login password
4	Authentication	• Login attempts (success and failure) to gain access to the application including any remote logins • Account lockouts and other authentication failure events on a privileged account
5	Authorization	• Attempts to alter critical application files or folders (e.g. configuration files, installation directories etc.) and other resources • Actions performed by privileged accounts
6	System Administration	Application component installation and changes (e.g. installing or deleting modules)
7	API Calls	• Successful and unsuccessful API requests • Identity of the API caller • Time of the API call • Source IP address • Request parameters • Response elements