Title: Log Events and Response
Author: Hunter Celeste

Log Events and Response

Editor:	Date:	Notes
Hunter Celeste	5/26/2023	Creation of Documentation Event Priority and Response Defined 7 Events added to table

---

Event Priority: Based on the severity of the threats the logs will be ordered based on their priority. These being High, Moderate, Low, and None. Below are listed these events.

- **High:** These are events that could be critical attacks on the system. Examples of these include SQL attacks or use of a USB on an unauthorized device.
- **Moderate:** These events may pose a threat but aren't as critical or severe to damaging systems or acquiring information. Examples include (Finish)
- **Low:** These events may be a sign of a threat or just user error/failure. Such logs should be noted and responded to but at a lower priority.
- **None:** These events will be recognized by the system but there is usually no follow-up response afterward due to their severity. An example of this is entering a wrong password once.

Event:	Priority:	Action:	Response:
Wrong Passcode (Once)	None	Warning Message	None
Illegal Characters for Field (Once)	None	Warning Message	None
Wrong Passcode (Multiple)	Low	Lock Account Log into the Low Priority Section	Account must be recovered by talking to the security admin or IT.
Account is logged-in past work hours	Low	Log into the Low Priority Section	Log Reviewed to see if the employee stayed late.
Illegal Characters for Field (Multiple)	Moderate	Log into Moderate Priority Section	Review event and Access Device it was done on
SQL Injection Attack	High	Log Event in High Priority Notify the Administrator Immediately	Review Log and assess if there is any damage.
Attempt to extract large amount of data from database	High	Log Event in High Priority Notify the Administrator Immediately Lock User*	Review Log and assess database security. User is investigated and interviewed.
Attempt to plug-in USB into non-authorized device	High	Log Event in High Priority Notify the Administrator Immediately	Review Log and Assess Device. If device was logged in, interview the account holder

Response: All logs should be reviewed on a minimal or weekly basis for low priority and daily for high priority. High priority logs will immediately be displayed as a notification both on the security administrators computer and/or authorized device.

Note: *Failure to review logs may lead to failure to address a vulnerability in the system and lead to a further attack or compromised data. Logs will be reviewed on the basis described above or the employee will be at risk of termination.*