Version 1.4 September 16, 2022 Brett McFadden	**Use Case**	**Low** *These tasks are usually items that can be accomplished during normal workflow.*	**Medium** *These tasks require some urgency and should take precedence over non-business critical work.*	**High** *These tasks are very important and must be completed ASAP.*	**Critical** *These tasks are time-sensitive, and teams are expected to stop what they're doing and attend to the immediate task at hand.*
SOC-INFO *No Action Required*	Providing facts, knowledge, or a **general message** of interest. Commonly sent to the TUMs wider audience.	N/A	N/A	N/A	N/A
SOC-ADVISORY *Recommended Action*	Providing facts, knowledge, and details for a **security concern/event** of general interest. Commonly sent to the TUMs wider audience.	**Necessary actions should be taken during your normal workflow.** **Recommended Action Steps:** 1. Notify your constituents. 2. Verify that Western's devices are not under any threat. 3. Complete any necessary corrective actions.	**Necessary actions should take precedence over non-business critical work.** **Recommended Action Steps:** 1. Notify your constituents. 2. Verify that Western's devices are not under any threat. 3. Complete any necessary corrective actions.	**Necessary actions should take precedence over all non-disaster recovery work.** **Recommended Action Steps:** 1. Notify your constituents. 2. Verify that Western's devices are not under any threat. 3. Complete any necessary corrective actions.	N/A
SOC-NOTICE *Requested Action*	A formal notice, request, or signal for action, sent to an individual or group.	**Requested actions should be completed during your normal workflow.** **Requested Action Steps:** 1. Determine if this issue is expected 2. If not, or unsure, engage with necessary parties to determine validity 3. Discuss results with Security Analyst 4. Remediate issue or implement approved changes	**Requested actions should take precedence over non-business critical work.** **Requested Action Steps:** 1. Determine if this issue is expected 2. If not, or unsure, engage with necessary parties to determine validity 3. Discuss results with Security Analyst 4. Remediate issue or implement approved changes	**Requested actions should take precedence over all non-disaster recovery work.** **Requested Action Steps:** 1. Engage with necessary parties to investigate the issue. 2. Determine if this issue is expected 3. Discuss results with Security Analyst 4. Remediate issue or implement approved changes	N/A
SOC-ALERT *Required Action*	A warning of danger, threat, or risk, typically with the intention of having it avoided or dealt with vigilantly	**Required actions should be completed during your normal workflow.** **Required Action Steps:** 1. Engage with necessary parties to investigate the issue. 2. Determine if this issue is expected 3. Remediate the issue 4. Discuss results with Security Analyst	**Required actions should take precedence over non-business critical work.** **Required Action Steps:** 1. Engage with necessary parties to investigate the issue. 2. Determine if this issue is expected 3. Remediate the issue 4. Discuss results with Security Analyst	**Required actions should take precedence over all non-disaster recovery work.** **Required Action Steps:** 1.Engage with necessary parties to investigate the issue. 2. Determine if this issue is expected 3. Remediate the issue 4. If necessary lock down the device(s) to prevent spread 5. Discuss results with Security Analyst	**Required actions must take precedence over everything and be implemented immediately.** **Required Action Steps:** 1. Stop whatever you are working on and engage with necessary parties and the security team. 2. If necessary lock down the device(s) to prevent spread. 3. Investigate the identified issue.

* For all SOC-Notify and SOC-Alert communications, we require a response in a timely manner, remediation timeline can be discussed based on severity of the issue.