4.0 Post-Incident Activity / Lessons Learned

This incident was a strong reminder that even a single click on a malicious document can open the door to system compromise and resource hijacking. While our response was swift and effective, the process revealed some gaps and areas we must tighten up as we prepare for the next incident response cycle.

One major takeaway is the importance of stronger web control policies. The malware came from a URL that was accessed through a web browser, likely without any restrictions or real-time URL filtering in place. Moving forward, stricter web access controls—such as blocking known malicious domains and preventing access to uncategorized or suspicious sites—should be implemented organization-wide.

Another critical insight is the need for enhanced macro detection and blocking. The infection was made possible because the user downloaded and opened a Word document containing a malicious macro that executed silently. We need to enable security tools and GPO settings that can automatically detect, block, or warn users about documents with embedded macros—especially those from untrusted sources.

On the monitoring front, while our tools like EDR, SIEM, IDS, and IPS helped during containment, we realized that having real-time alerting tied directly to process behavior anomalies (like sudden CPU spikes or unusual registry changes) would improve detection speed. We plan to tune our SIEM rules and create use cases around known crypto mining behaviors.

Finally, continuous user awareness training remains key. The end user downloaded a suspicious file without verifying its source. We're reinforcing our training modules to help users recognize phishing attempts, unsafe downloads, and how to report them early.

In all, this incident served as both a challenge and a checkpoint. We’re walking away with clear strategies—web filtering, macro defense, tighter monitoring, and better user education—that we’ll carry into the next preparation phase of our incident response cycle.