Identifying Root Cause and Recovery

Once an incident has been contained, evidence collected, and any malicious artifacts have been removed, it's time to identify the root cause if it's still unknown by this stage, and perform remediation activities so that systems can be returned to production environments, allowing the business to operate at the same capacity as before the incident. Below we will cover how organizations can work to identify the root cause, and what actions are typically conducted during the recovery stage.

IDENTIFYING THE ROOT CAUSE

For some incidents the root cause will be immediately present, such as a user informing the security team that they opened an attachment in an unusual email, then their laptop started doing strange things. But in some cases it may take a lot of analysis work to discover how the incident started, referring to the Cyber Kill Chain or ATT&CK Framework to map the stages observed during an incident, potentially helping to identify the cause by using similar attack paths and investigating hypothesis about the initial infection.

By taking forensic images of any affected systems, analysts can spend time analyzing the data with the goal of uncovering the actions taken by the malicious actor during the attack. It's important to identify the root cause if recovery efforts are to be effective, as rushing this stage could result in the initial entry point being left open, potentially allowing the attacker to regain access.

INCIDENT RECOVERY

Now that the incident has concluded, it's time to fix any systems that were affected by the incident or display similar weaknesses. If an incident was caused because of a vulnerability in a program, this should be patched to prevent it from being exploited again in the future. If the incident was the result of human error, the individual or individuals should be given training and/or support so that a similar incident doesn't happen in the future. When considering recovery actions, the below list summarises common responses:

- **Patching systems with program, operating system, and security updates to ensure that any vulnerabilities are fixed. Manual testing should be conducted after patching to ensure the fix has worked.**
- **Disabling services that are not needed on a system.**
- **Update endpoint detection and response (EDR), anti-virus (AV), intrusion detection and prevention system (IDPS), and SIEM rules to allow for monitoring and alerting of similar activity that occurred during the incident.**
- **Share intelligence regarding the incident, such as indicators of compromise, with other organizations to allow them to improve detection and perform threat exposure checks across their environments.**