Incident report analysis

Real-World Example

Summary	An event notification for a process from the executable Advanced_Port_Scanner_2.5.3869.exe was triggered by the SIEM. It was authorized IT staff running the executable but Sentinelone immediately killed and quarantined the process. The team needs the ability to safely use this tool so I created a custom portable version of the executable and whitelisted the hash of only that version of the executable for operation in the organization.
Identify	In review of the incident I discovered through conversation with the Engineering Team that the software was obtained from https[:]//download.advanced-port-scanner[.]com/download/files/Advanced_Port_Scanner_2.5.3869[.]exe. The reputation of the executable in VirusTotal was clean and this website was the appropriate location to download the executable from. I identified that a procedure for acquiring and approving software was needed.
Protect	I created and received management approval for a “Software Acquisition and Approval” policy that detailed the purpose of the policy, the required communications and approvals, the required sandbox analysis method, and modification of the executable to customize the hash for whitelisting. Further, I utilized a HEX editor in VSCode to modify the portable version of the “Advanced Port Scanner” software to generate a custom hash for use within our organization and added it to all tooling.
Detect	To detect future malicious use of this application while allowing approved use, all personnel have been trained to utilize the newly customized executable located on an internal secure storage. Furthermore, I created a custom

	Elastalert rule that ignored the hash of our customized version of the executable. This way, any attacker who uses the software maliciously would have acquired it from the public website and our tools would continue to deny and alert but any authorized and trained personnel would use the customized version successfully without generating false-positive alerts.
Respond	Sentinelone automatically killed and quarantined the executable and no further action was required to prevent malicious activity. Leadership was informed of the event as per company policy and approved the recommended actions to enable continued safe operation.
Recover	The action required two hour's time to approve and generate a customized tool so the Engineering Team was able to continue safe operations with minimal delay.
