Threat Exposure Checks Explained

A threat exposure check is when an analyst uses multiple tools such as a SIEM and EDR to look for the presence of any indicators of compromise they have retrieved from intelligence vendors, information sharing partners, government alerts, or from OSINT sources. This activity is considered a tactical task, as it requires a deep technical understanding to analyse the results from several different tools to determine if any exposure has been detected, and then assessing exactly what's been observed so it can potentially be passed to security analysts for investigation. To help you understand when and how threat exposure checks are conducted, we will walk you through a scenario based on real-world practices.

EXAMPLE WALKTHROUGH

The threat intelligence team receive an email alert from US-CERT stating that "Vulnerability X" has seen a spike in exploitation activity across the internet. This report includes a list of IP addresses that US-CERT and partners have observed scanning the internet for vulnerable devices. The threat intelligence team would now retrieve that list of indicators of compromise and search for them in their SIEM platform, where the perimeter firewalls send their logs, so they can all be queried at once. The assigned analyst will search for the source IP equal to the values provided in the report and do a historic search, typically for the previous 7 days. Once the search has completed the analyst will be able to see if any of the mentioned scanning IPs have scanned the organisations public IP range in the past 7 days.

If there is a recorded presence of the malicious IPs performing any kind of scanning or enumeration activity then IP blocks can be considered, depending on the nature of the IPs. Alerts can also be setup to trigger if these IPs begin scanning again, so that defenders can closely monitor exactly what the IPs are scanning.

In an organisation that has a team working on vulnerability management, it is likely that they will work closely with the threat intelligence team, as context around vulnerabilities is extremely important. A high-rated vulnerability might never be exploited, but a medium-rated vulnerability could be exploited on a mass-scale. If malicious actors are actively exploiting a vulnerability, then this can provide justification for immediate patching.