Threat Profiling

Check Point Incident Response Team's Threat Profiling service conducts a comprehensive and tailored evaluation of the threat landscape your environment faces. It is designed to deepen understanding of the tactics, techniques, and procedures employed by potential adversaries. By highlighting specific (sub-)techniques used by perpetrators, and providing informed recommendations, we empower your organization with actionable security configurations and strategies to strengthen security measures and effectively mitigate risks. This strategic approach ensures ongoing vigilance and adaptation to the evolving cyber threat environment.

Aim: Providing a comprehensive evaluation of the threat landscape the environment is facing, helping to understand the (sub)techniques used by potential perpetrators, to identify potential vulnerabilities or weaknesses in the environment, and to make informed decisions to strengthen security measures and mitigate risks.

Deliverables: Priority List of most likely and most dangerous MITRE ATT&CK techniques and their associated Mitigations, Detections, Validations, safeguard implementations and Check Point Coverage.

Methodology: The identification of the most likely and most dangerous MITRE ATT&CK Techniques is focused on the organisation's industry and country and is derived from Check Point's Telemetry and other data sources. It also benefits from a previously conducted or including ASMA and CP<R> evaluation and/or includes a Top ATT&CK Techniques assessment.

Benefits:

Improved Threat Awareness: Creating a threat profile provides a consolidated analysis of various threat intelligence sources, including anti-virus telemetry, open-source information, and adversary tactics and (sub)techniques. This enhanced threat awareness helps to understand the specific threats the environment may face.

Targeted Security Measures: A threat profile allows to develop appropriate countermeasures and proactive security strategies to address the specific threats identified. This focused approach enhances the overall effectiveness of security measures and reduces the risk associated with successful attacks.

Proactive Risk Mitigation: With a threat profile in place, it is possible to proactively identify and mitigate potential risks before they can be exploited by attackers. By staying ahead of existing threats and understanding their specific characteristics the likelihood of successful attacks can be reduced.

Enhanced Security Posture: By analysing attacker tactics and techniques, organizations can anticipate the potential impact of attacks and develop appropriate response strategies. Creating a threat profile aids in the development of an improvement roadmap, including but not limited to the development of robust incident response plans, preparing for Tabletop Exercises, preparing for a Ransomware/Breach Readiness Assessment, or preparing for a Penetration Test.

Hands-on Implementation recommendations of Best-Practices Security Configurations: tap into actionable, hands-on guidance with our prioritised selection of the CIS Benchmark configuration recommendations. These recommendations provide you with ready-to-implement security configuration enhancements tailored for your environment. Steer your security strategy from reactive to proactive with clear, practical steps that yield immediate, measurable improvements in your defence capabilities.