Compromise Assessment

A Compromise Assessment (CA) looks for signs of compromise across all endpoints in the network when a breach has already occurred. The aim is to identify any and all points of presence of an attacker in the wider environment by pivoting on both incident specific (e.g., indicators identified during Active Incident Handling or a RCA) and generic indicators originating from Check Point's Thread Cloud and other bespoke threat intelligence feeds. A Compromise assessment restores trust in the remaining and rebuild portions of the network, by assuring that any left-over artefact of an attacker is detected and removed. There exists a strong synergy with a RCA. A RCA gives case specific IoC's and takes additional endpoints in scope that have been identified by the CA. A compromise assessment without a pre-existing breach is in most cases referred to as a threat hunt.

Aim: Restoring trust in the remaining and rebuilt sections of the network. Identifying candidate endpoints to take into scope of the RCA.

Deliverables: A comprehensive CPIRT written report and a list of assets at risk.

Methodology: CPIRT works preferably with dedicated endpoint agents and a cloud-based collector. However, when the visibility in the environment is sufficient (e.g., the presence of another compromise assessment tool) CPIRT might leverage the existing tooling depending on the situation.

Benefits:

Identification of breached systems: A compromise assessment's output is a list of assets that have traces of nefarious activity. This allows for swift isolation of these systems and if deemed necessary addition to the scope of a RCA.

Restoring Trust in the infrastructure: Once a breach has materialized the trust relationship between the business and the IT infrastructure is broken. A Compromise assessment aims to restore trust in the infrastructure.

Identification of shadow IT: In many cases a CA reveals shadow IT in a network. These range from older remote assistance and access tools, to software assets that are unwanted, outdated, or unneeded. Once identified the IT team can work to address these entries.

No whack-a-mole: By actively hunting for all points of presence of an attacker in a network, CPIRT avoids playing a game of whack a mole with the attacker where the attacker can keep forcing access into the network as one backdoor on a system has remained unseen.