STACKTITAN

TACTICAL ASSESSMENT CATALOG

ENDPOINT RESILIENCY ASSESSMENT:

A breach of network, compromise of assets, and theft of data can often be attributed to the initial point of host-level entrenchment. The ability for an adversary to obtain initial compromise, escalate privileges, extract meaningful data, and penetrate further within the network from a workstation or similar point of singularity should be assumed. Acting upon this assumption, the Endpoint Resiliency Assessment (ERA) evaluates system, network, and application capabilities relative to these endpoint or host-level attack patterns.

STACKTITAN

ENDPOINT RESILIENCY ASSESSMENT:

THREAT MODELING

A variety of criteria such as industry vertical, incentive, capability, and opportunity cost, for example, can enable a motivated adversary. Therefore, the significance of understanding the overall objective in conjunction with a relevant threat actor is paramount to establishing threat models that will replicate actual venerable attack patterns and courses of action. The output of this exercise will establish a viable approach to further resiliency testing, while aligning test cases with the industry-curated MITRE ATT&CK adversary knowledge base.

PAYLOAD DELIVERY RESILIENCY TESTING

Payload Delivery Resiliency Testing uses a variety of common and unique techniques to evaluate the network and endpoint's ability to identify and prevent delivery of malicious or weaponized payloads. These techniques are executed systematically, utilizing a spectrum of obfuscation, encryption, and bypass tactics to identify the effectiveness of security controls intended to block such delivery, allowing the organization to fully understand its susceptibility to initial penetration via various remote channels and protocols.

ENDPOINT RESILIENCY ASSESSMENT:

LOCALIZED RESILIENCY TESTING

The resiliency of an endpoint to withstand localized attacks is paramount in preventing widespread network compromise. Adversarial attack patterns commonly include payload execution, persistence, escalation, credential harvesting, and memory manipulation. Localized Resiliency Testing emulates these tactics to critique the effectiveness of next generation endpoint security software, antivirus deployments, system hardening and group policy, and system patching practices, giving visibility into an endpoint's ability to withstand direct exploitation.

NETWORK AND EGRESS RESILIENCY TESTING

Rarely do adversarial attack patterns (i.e., kill-chains) end with the compromise of a single endpoint; attackers pursue lateral network movement, data exfiltration, and redundant command-and-control (C2) as a means to escalate privileges, pursue targets of interest, and maintain network presence. Network and Egress Resiliency Testing examines these techniques using common and proprietary variations, measuring the probability of these security controls to detect and mitigate network-based attack patterns.

ENDPOINT RESILIENCY ASSESSMENT:

EVIDENCE COLLECTION AND REPORTING

Documentation and evidence is compiled into a professional, quality-assured report format appropriate for distribution to executives, technical staff, and risk owners. The document contains executive summary and assessment details as well as a comprehensive listing of test cases, categorized by phase and intent, with clearly annotated test outcomes.