Secureworks®

Ransomware Attack Simulation

How would your organization detect, defend, and respond to a ransomware attack?

Overview and Benefits

The Secureworks® Adversary Group helps test the security and resiliency of your organization by simulating real-world threat actors aiming to compromise your data.

The Secureworks® Ransomware Attack Simulation is a live-fire testing engagement using our Internal Penetration Testing methodology* to test your network defenses, detections and response capabilities, to answer the question: "Could we defend against a threat actor attempting to deploy ransomware in our environment?" or "Would we know if an attacker was in our environment and attempting to gain elevated privileges? And how quickly?"

We leverage lessons learned from thousands of adversarial testing and incident response engagements to design tests that leverage the same TTPs used by real-world threat actors.

For maximum impact, ransomware threat actors target and attempt to disable backup servers, moving on to gain elevated permissions on as many systems as possible before deploying ransomware. Therefore, our Ransomware Simulation has two main goals; compromise as many systems as possible, and compromise critical backup infrastructure.

Pre-Test Planning & Validation

- Kick-off to define rules of engagement
- Technical scoping call with an SME from the Adversary Group
- Identify targeted systems, services, and data security strategies

Execution

- Identify exploitable internal systems, networks, and policies
- Attempt to gain control of key accounts, backup infrastructure, devices and potentially cloud environments
- Option to deploy a mock ransomware executable to prove code execution on a sampling of systems

Final Report

- Executive Summary
- Detailed findings
- Extensive technical narrative
- Delivered within three weeks of test execution

Watch the Methodology Video

The standard Ransomware Attack Simulation starts internally, focusing on how a threat actor might move through the environment to gain elevated controls. To further enhance your understanding of a ransomware threat actor's ability to compromise your environment, consider additional Secureworks Adversary Group services.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com

About Secureworks
Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.