Secureworks®

DATA SHEET

Red/Purple Team Exercises

Measure Defense and Response Capabilities Against a Simulated Real-Life Adversary

Measuring Yourself Against the Adversary

Threat actors are continuously evolving their tactics, techniques and procedures, finding new and creative ways to bypass existing security programs and defense strategies. To increase cyber resilience and incident readiness, organizations must go beyond testing for vulnerabilities by running real-world scenarios and simulated attacks. This requires mimicking adversaries using various methods to gain entry and escalate in your environment to test internal incident response capabilities and detection and prevention tools.

How Secureworks® Helps

The Secureworks Adversary Group is a dedicated team of top security testers leveraging a goal-based methodology honed by years of testing. All engagements leverage tactics and tools commonly used by threat actors and defensive and offensive research from the Secureworks Counter Threat Unit™ (CTU™), including lessons from thousands of incident response and testing engagements performed annually. To help your Blue Team practice and train for real-world events, Secureworks provides different types of exercises based on your organization's incident response process maturity and engagement goals. These tests help measure how well your organization's defense and response capabilities will withstand attacks, and enable action including tuning of existing devices to detect advance threats and proactive improvement of response capabilities.

Red Team Test

The Secureworks Red Team Test is a stealthy test designed to achieve specific goals and shine a light on gaps in an organization's response and detection capabilities. Our methodology uses blended attacks that combine various techniques to avoid detection and prevention. These include open-source intelligence, phishing/social engineering, wireless, covert physical and network attack methods.

It answers questions such as:

- How would my network stand up to a group of highly-skilled adversaries with minimal limitations?
- How well are my security controls protecting my critical data?
- Is my Alerting/Monitoring system tuned to catch a stealthy adversary?
- Are my IT Administrators making good security choices?
- If a user is compromised, how will the rest of my network withstand an internal attacker?

Customer Benefits

- Gain actionable insights to strengthen your organization's security posture against the most likely cyber threats
- Validate protections and monitoring of high-value systems
- Improve detection and prevention capabilities of existing devices
- Improve response capabilities and processes

Service Features

- Performed by the industry's top security testers, on-site or remotely
- Real-world scenarios and common attack methods based on the latest Intelligence from the Secureworks Counter Threat Unit™
- Customized engagement goals
- Manual testing to simulate attacker methods and techniques
- Wireless tests, physical testing and drop box placement as necessary
- OSINT to gather additional targets

What to Expect in Your Red Team Testing Report

The report consists of two sections.

The **Executive Summary** is written for a non-technical audience — senior management, auditors, Boards of Directors, and other concerned parties.

Engagement Summary

Brief description of what testers carried out during the engagement.

Summary of Findings and Recommendations

Suitable for non-technical audiences, the Summary describes systemic issues and high-risk findings, and our recommendations to remedy issues or reduce risk.

Detailed Findings

Written for technical staff and provides detailed findings and recommendations.

Engagement Methodology

Contains details of what was performed during the engagement.

Attack Timeline

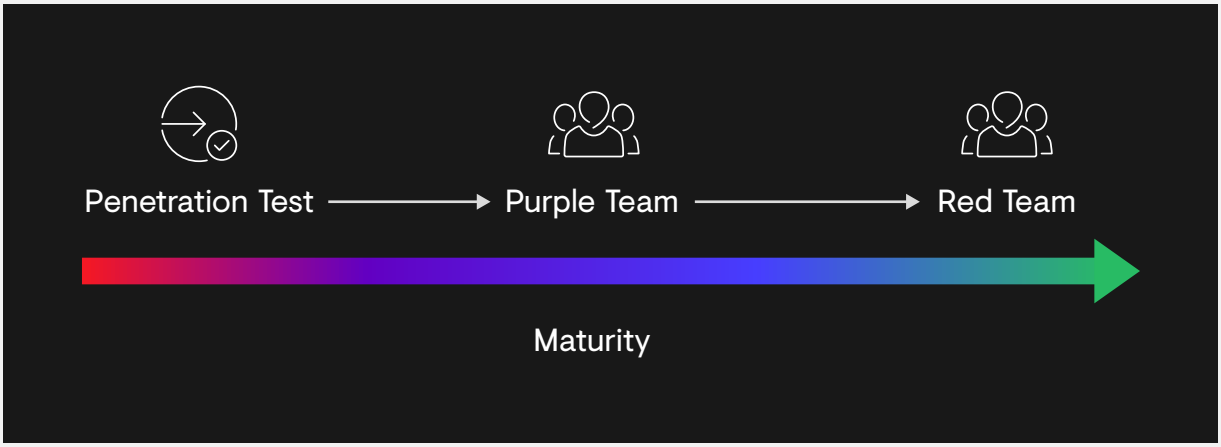
Describes the sequence of events to assist in understanding blended threats and/or dependent phases.

Detailed Findings and Recommendations

Describes any findings, further resources, and recommendations for remediation or risk reduction. Evidence of findings is supplied and, if possible, sufficient information is provided to replicate the findings using publicly available tools. Descriptions of the techniques used and the causes of success or failure are included.

Next Steps

- Threat Hunting Assessment
- Secureworks Taegis™ XDR
- Incident Management Retainer
- Secureworks Taegis™ VDR



Purple Team Testing: Exercise. Respond. Improve.

A Purple Team Test leverages the Secureworks Red Team and offers a collaborative approach through exposure to offensive security consultants, or the optional addition of a Secureworks IR Blue Team consultant, as attacks are performed. Unlike a traditional Red Team exercise, a Purple Team uses defined scenarios that cover different aspects of the kill chain providing actionable events for your Blue Team to help answer questions such as:

- Do I have appropriate response processes in place?
- How quickly does my security team respond to an attack?
- How does my Blue Team responds to common attacks and where can I improve?
- Am I ready for a highly customized Red Team test?

The Purple Team test reports are geared towards providing metrics to baseline and track progress. In addition to an executive overview and high-level description of the overall engagement and actions performed, the report detail provides:

- MITRE Attack Heatmap: Maps actions performed to MITRE Attack Framework.
- Scenario Playbook & Methodology: Description of playbook actions and methodology used.
- Actions Performed: Detailed description of actions performed including start/stop times, detection and response times (where provided by the defender), and MITRE techniques used.

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.

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