Secureworks®

DATA SHEET

Red Team Testing

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

Measuring Yourself Against the Adversary

You may believe your security defenses are prepared for any threat. But to be truly sure, you need to run a real-world scenario that's designed to measure how well your organization's defense and response capabilities will withstand social, physical, network and application attacks from a simulated adversary.

How Secureworks® Helps

The Secureworks Adversary Group tailors every Red Team test for each organization. Our methodology is performed by the industry's top security testers, based on thousands of global engagements across more than 4,000 customers, yet customized for individual scope. Each Red Team test leverages artificial and human intelligence, and unmatched visibility into the threat landscape from the Secureworks Counter Threat Unit™ (CTU™). These blended attacks combine various techniques to avoid detection and prevention including open source intelligence, phishing, wireless, covert physical and network attack methods. We enable customers to tune their existing devices to detect advanced threat tactics, so they can predict and prevent certain threats altogether.

What Does Red Team Testing Help Me Answer?

- How would my network stand up to a group of highly skilled
- adversaries with minimal limitations?
- How 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?
- Can my IR team track down an actual attack?

Customer Benefits

- Be confident in the assessment knowing that the latest Threat Intelligence was utilized
- 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 Prediction and Prevention capability of existing devices
- Improve response capabilities and processes

Who Should Use a Red Team Engagement?

Organizations that:

- Have implemented response and detection teams, and want to test them
- Rely heavily on physical and personnel security measures to protect their networks
- Are concerned that current attacks may be going undetected
- Powerful Defensive and Blocking Capabilities
- Want to simulate an actual attack where the attackers can use various methods of entry and attempt to remain covert throughout the engagement
- Have completed several Penetration Tests with positive results

What to Expect in Your Report

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

Engagement summary: Brief description of what testers carried out during the engagement.

Summary of findings & recommendations: Conveyed in a way suitable for non-technical audiences, describes systemic issues and high-risk findings, and our recommendations to remedy issues or reduce risk.

The Detailed Findings is 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 & recommendations: Describes any findings, webpage links for further reading, and recommendations for remediation or risk reduction. Evidence of the findings is supplied where applicable, and if possible, sufficient information is supplied to replicate the findings using publicly available tools. Descriptions of the techniques used and the causes of success or failure are included.

Solution Features

- Performed by the industry's top security testers, on-site or remotely
- Real-world scenario leveraging the latest Threat Intelligence from The Secureworks Counter Threat Unit
- Customized engagement goals
- Blended, covert test that can encompass network testing, phishing, wireless, and physical attacks
- Repetition performed until goal is met
- Manual testing to simulate attacker methods and techniques
- Wireless, Physical testing and drop box placement as necessary
- OSINT to gather additional targets

Our Testers

From our in-depth technical hiring process, to our continued investment in our consultants through generous training programs, we seek and cultivate technical excellence. Our consultants advise global government agencies, law enforcement, and the media, and are often first to market with cutting-edge security solutions.

Proven Methodology

Secureworks has performed thousands of Assessments and Tests for a wide array of companies, from small business to Fortune 500. We combine proven, public industry methodology (NIST and PTES), with our experts' advice and experience. Our focus on security and combination of artificial and human intelligence gives us a lens into the threat landscape across any technology, any industry, any environment, anywhere.

Next Steps

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

If your organization needs immediate assistance call our **Global Incident Response Hotline (24x7x365).**
+1-770-870-6343

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.