Secureworks

DATA SHEET

ADVERSARY EXERCISES

Measure Defense and Response Capabilities Against a 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 by using various methods to gain entry and escalate in your environment, and to test internal incident response capabilities, 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 exercises 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 goals. These exercises help measure how well your organization's security controls and security team perform against each step in the cyber kill chain and assist in closing any identified visibility gaps.

The Secureworks Adversary Exercises service line offers a holistic approach for cultivating and enriching your Blue Team's capabilities, testing assumptions about security controls, and identifying gaps in detection. We use three different exercises at various junctures of a customer's security maturity journey or points in the security improvement cycle:

- Collaborative Adversary Exercise
- Adversary Emulation Exercise
- Adversary Simulation Exercise

CUSTOMER BENEFITS

- Identify detection and prevention gaps in security controls
- Measure response capabilities and timing
- Boost the skill level of defense personnel
- Test assumptions of security controls against both common and unique tactics, techniques and procedures

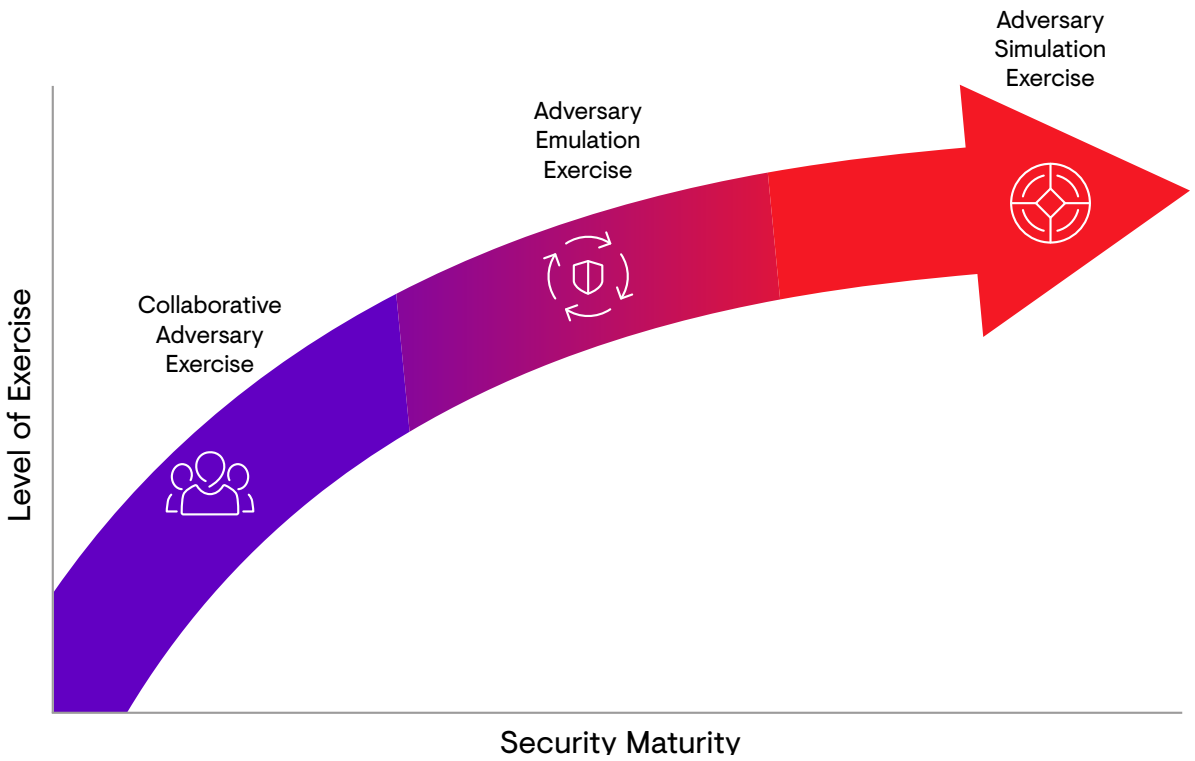
SERVICE FEATURES

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

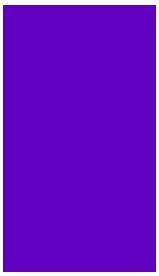
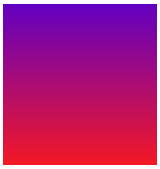
While the methodologies and maturity level required for the three exercises differ, each one shares the common overarching goal of assessing detection, prevention and response capabilities, and can help answer questions such as:

- 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?

ADVERSARY EXERCISES: ENGAGE. RESPOND. IMPROVE.



With exercises for different points in an organization's security maturity journey, Secureworks helps identify an appropriate exercise that will yield the best results and effects. The following table gives a high-level overview of each exercise to examine how they differ:

SERVICE	EXERCISE COLOR GAUGE	DESCRIPTION	KEY USE CASES AND DETAILS
Collaborative Adversary Exercise		Secureworks performs a pre-defined playbook of tactics, techniques and procedures, based on common threat actor techniques, alongside your organization's Blue Team within a dedicated communication channel.	• A starting point to assess if detections and preventions are effective. • Examine tactics, techniques and procedures together with Secureworks, with explanations and insight into attacks. • Tune detections in a controlled setting that also permits attack replay. • Blue Team is aware of Red Team activities and participates in the exercise.
Adversary Emulation Exercise		Secureworks mimics the tactics, techniques, and procedures of a real-life threat actor that is known to target your organization based on threat intelligence.	• Test assumptions for detection, prevention, and response to known threat actors and their TTPs. • Except for key personnel, Blue Team is unaware of Red Team activities. • Focuses on "known bads."
Adversary Simuation Exercise		Secureworks simulates a real-life adversary by using unique and unattributable tactics, techniques, and procedures.	• Assess maturity of security controls and personnel to respond to an unknown threat. • Except for key personnel, Blue Team is unaware of Red Team activity. • Focuses on "unknown bads."

NEXT STEPS

Threat Hunting Assessment

Secureworks Taegis™ XDR

Incident Management Retainer

Secureworks Taegis™ VDR

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