PURPLE TEAM ASSESSMENTS

Understand Efficacy of Detection Capabilities

WHY SPECTEROPS

Our experience across hundreds of government, defense industry, financial, and healthcare environments has taught us that the most vital component of a robust security posture is understanding how adversaries will operate against the organization's enterprise environment. Our objective, across all engagements, is to train and arm our clients with the knowledge of how the effective use of the interlocking components of their security program provide a robust security posture and readiness against sophisticated attacks.

At SpecterOps, we have found that dynamic evaluation is the best way to evaluate the efficacy of security controls, whether preventative or detective in nature. To do this, we select an adversary technique or behavior, design test cases, execute the test cases, and evaluate the results relative to existing security controls. This dynamic approach is especially important given that a preponderance of security controls are vendor supplied and thus the analytic itself is opaque. While dynamic evaluation with test cases is a standard for Purple Teaming as many know it, we believe that the "devil is in the details" with respect to test case selection to represent each behavior.

BENEFITS

Understand the ROI of security initiatives

Reduce assumptions in understanding cyber risk acceptance

Receive actionable results to drive immediate improvements

Educate security operations staff in adversary tradecraft

Develop roadmaps for increasing detection coverage

WHAT YOU GET

- In-depth testing of detection coverage for the most widely used adversary techniques
- Transparency throughout the engagement so that methodologies utilized may be built into internal programs
- Evaluation of vendor-supplied and organic controls
- Tactical and strategic recommendations for short-term and long-term improvements
- Technical details that allow you to recreate test cases and findings
- Summary for executives and senior- level management
- Invaluable experience learning a framework for continuous detection

OUR APPROACH

Demystify Adversary Tradecraft
There is often a divergence between the perceived threat posed by an attacker behavior and the actual threat. SpecterOps leverages its deep technical experience in threat research, tradecraft analysis, and tool development to demonstrate the nuances of tradecraft that must be considered during security operations.

Assess the Comprehensiveness of Technique Coverage
We implement a diverse set of test cases for each technique to provide a representative sampling of the attack variations that could be encountered.

Evaluate Preventative and Detective Controls
Security controls can be split into two primary categories. Preventative controls are those that focus on blocking the execution of a behavior. Detective controls are those that identify when a behavior has occurred in the monitored space even when it cannot be addressed automatically. Our methodology is built to understand the scope of both types of controls.

Evaluate Raw Telemetry Available for Improvement
Many security programs are equipped with raw data, logs, or technology that is not currently used to its full potential. Our method helps to illuminate this under-utilized capability.

Educational
Our Purple Team approach is built to facilitate an educational environment where adversary tradecraft is taught for all members of the client's security staff.

Learn more at **www.specterops.io**

SPECTEROPS