SPECTEROPS
Creators of BloodHound

SERVICES

Purple Team Assessments

Understand How Effectively Your Detection and Response Capabilities Operate Against Current Attack Methodologies

Why SpecterOps

Our passion is to demystify adversary tradecraft. We love diving into TTPs to fully understand what is going on under the hood. That level of understanding allows us to tell you exactly what to evaluate and which actions an attacker MUST do in order to execute an attack.

By evaluating those bottlenecks in the attack path, your organization will be confident in its ability to detect malicious activity.

Why Now

Validate that your Security Operations Center is operating at the level you expect.

Benefits

- **Confidently stand behind your detection and response results**
- **Actionable and specific recommendations to close any gaps in the capability**
- **Educate security operations staff with how attacks really work**
- **Create a roadmap to enhance your detection and response capabilities**
- **When you accept risk, confidently understand the risk that you are accepting**

You will understand the effectiveness of your current preventative and detection controls for the most common attack techniques.

The SpecterOps delivery approach is focused on evaluating the existence and efficacy of security controls for one attack technique or behavior per day throughout the course of the exercise. These techniques will be established during the client kick off call and will be formally agreed upon in the assessment plan. Control validation is accomplished via dynamic testing whereby a selection of tool variations (test cases) is executed on the designated system(s). Results are then assessed in three ways:

- **Prevention:** Did the control stop the test case?
- **Detection:** Did the control alert on the test case?
- **Perception:** Was relevant telemetry generated and captured?

Test case selection is critical. SpecterOps selects test cases which offer a representative sampling of the range of variation that exists within the technique itself. This set of test cases allows for triangulation of control efficacy. **The assessment team will determine how much change is necessary before a control fails to achieve its goal.** Additionally, the assessment will help grow the organic competency of the client's information security team to understand adversary tradecraft.

To facilitate this, the exercise includes multiple presentations that are open to the entire team. The presentations will outline a technique per day to include:

- What the technique is
- How it works
- Why attackers might want to use it
- The different implementation variations that are possible
- The test cases we selected
- Why we selected those cases

Email info@specterops.io ›

Learn more at specterops.io ›

Real Results

- 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 internally developed controls.
- Clear ways forward to close immediate issues and a roadmap for long-term improvement.
- Enough detail to allow you to recreate test cases and findings.
- Executive Summaries for senior-level management.
- Exposure to a framework for continuous detection capability improvement.