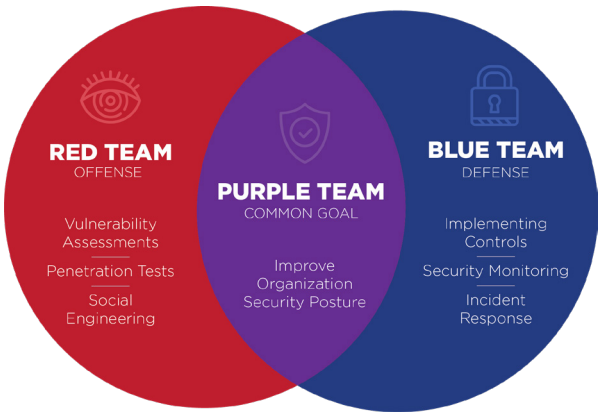
SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Purple Team Assessments

A Schneider Downs Purple Team exercise provides clients with the unique opportunity to view a simulated attack in real-time from the perspective of both the threat actors (red teamers) and the defense teams (blue teamers).

Our red teamers and blue teamers come together onsite and work with your team to demonstrate how to prevent and detect specific offensive techniques from the MITRE ATT&CK framework and other hacker tools, techniques and procedures.



How a Purple Team Assessment Works

The Purple Team exercise will match the hacker toolsets and mentality of our red team experts with the incident responder and defensive thinking of our blue team experts in a way that encourages, engages and sparks knowledge transfer.

1 Acclimation

To maximize the effectiveness of a Purple Team exercise, we begin by gaining a deep understanding of your environment. During this phase, we familiarize ourselves with your alerting and detection capabilities, network architecture and other pertinent details. The more we understand your environment, the more valuable and accurate the exercise will be.

2 Threat Mapping

Using the full MITRE ATT&CK framework, we collaborate with your team to select a tailored set of tactics and techniques that are risk-based, industry-appropriate and meaningful to your organization. This highly flexible process can emphasize a specific theme of offensive techniques or ensure a well-balanced baseline. We also cross-reference your threat intelligence with the framework to identify likely threat actors and incorporate their typical behaviors into your custom threat map. This allows us to anticipate additional attack vectors and create a realistic attack scenario.

3 Execution

With the threat map defined, our red team executes each technique in a transparent environment. This encourages an "over-the-shoulder" learning experience, giving your security team the opportunity to observe and even assist with activities such as enumeration, exploitation, lateral movement, post-exploitation and exfiltration. Throughout execution, our red team provides expert guidance on modern offensive strategies and the mindset of an attacker.

4 Impact Analysis

We closely monitor the success or failure of each technique to understand its impact within your environment. Ideally, existing controls prevent execution or block the intended outcome; if not, we may test alternate methods. When a technique succeeds, we assess its full impact and identify additional mitigation opportunities. Because no environment can prevent every technique, this analysis supports appropriate prioritization and informed decision-making.

5 Detection

As offensive techniques are executed, our blue team works alongside your team to monitor logs and systems in real time. When a technique is successful, we help your team use existing capabilities to prevent or detect it; if those capabilities are insufficient, we guide the development of new ones. Throughout this phase, our blue team provides expert insight into modern defensive strategies and real-world threat actor behavior.

6 Reporting

At the conclusion of the exercise, you receive a comprehensive report that includes a detailed threat map, the execution status of each technique, analysis from both red and blue teams and a clear guide for implementing any defensive enhancements not fully addressed during the engagement.

24x7x365 Network Incident Hotline

If you suspect your organization is under attack, the Schneider Downs Incident Response Team is available 24x7x365 at 1-800-993-8937.

Ready to Get Started?

Contact the team at contactsd@schneiderdowns.com or learn more at www.schneiderdowns.com/cybersecurity.

About Schneider Downs?

The Schneider Downs cybersecurity practice consists of experts offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team.