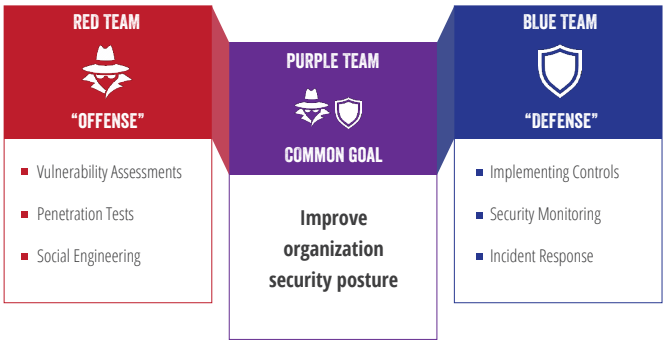
SCHNEIDER DOWNS

Big Thinking. Personal Focus.

Cybersecurity Services

A Schneider Downs Purple Team exercise provides clients 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.



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.

OUR APPROACH

1. Acclimation

The more we understand about your environment, the more valuable the exercise, which is why our team starts with becoming familiar with your current alerting/detecting capabilities, your network architecture and other critial details.

2. Threat Mapping

Our team will leverage every category of the MITRE ATT&CK framework and work with you to map a custom set of tactics and techniques that are risk-based, industry-appropriate and meaningful to your organization. This selection process is highly flexible and can either steer the exercise toward a specific theme of offensive techniques or it can ensure a well-balanced exercise for a stronger baseline.

3. Execution

Once threat mapping is complete, our red team will execute each of the techniques in a transparent environment that your team can observe, learn from, and even get a hands-on assist in the execution of a variety of typical hacker activities. Throughout this process, our red team will serve as an expert resource to transfer valuable knowledge regarding modern offensive strategies and offer insights into the mind of a hacker.

4. Impact Analysis

The success or failure of each technique is closely monitored to ensure complete understanding of its impact within the environment. If a technique is successful, we analyze the results to determine its full impact and identify additional mitigating factors. With the understanding that it's not always possible to prevent every technique, impact analysis for successful techniques allows for appropriate prioritization and accurate decision-making.

5. Detection

As our red teamers try to breach your systems, our blue teamers will be alongside your team simultaneously monitoring your information flow. If a technique is successful, we'll help your team leverage current capabilities to prevent/detect each technique. If current capabilities are insufficient, we'll help your team develop improvement plans. The blue team will serve as an expert resource to transfer valuable knowledge regarding modern defensive strategies and offer insights into their real-world threat actor encounters.

6. Reporting

After the exercise, your team receives a comprehensive report, including a detailed threat map of each technique's execution status and analysis from both our red and blue teams, as well as a detailed guide for the implementation of any defensive items that were not fully addressed during the exercise.

SOFTWARE SOLUTIONS

Schneider Downs is an authorized reseller for a number of software solutions, including Carbon Black®, Mimecast®, Guardicore and Sophos.

WHY SCHNEIDER DOWNS?

Schneider Downs can help your organization be better prepared. We offer a comprehensive set of information technology security services, including network penetration assessments, network vulnerability assessments, web application security testing and IT security maturity assessments. Our expert team includes application configuration specialists, implementation consultants and certified information system auditors who can assist your organization with an objective assessment, identify crucial information and key security risks, and assist with the implementation of industry best-practice security standards to mitigate these risks. For more information visit our website at www.schneiderdowns.com/cybersecurity or contact us at cybersecurity@schneiderdowns.com.

EXPERIENCING OR SUSPECT A NETWORK INCIDENT?

Contact the Schneider Downs Incident Response Team 24x7x365 at 1-800-993-8937.

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

www.schneiderdowns.com

TAX

AUDIT AND ASSURANCE

CONSULTING

WEALTH MANAGEMENT

PITTSBURGH
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

COLUMBUS
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

WASHINGTON, D.C.
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003