CDW Professional Services

Simulate real-world attack scenarios for maximum security.

Red Teaming Services

While the motivations of cyber criminals can vary, they will stop at nothing and break in by whatever means necessary to achieve their malicious objectives. But even though you've bolstered your cyber defenses and matured your security posture, how can you be sure your organization is truly ready to defend against the relentless attacks of an intruder? With CDW's Red Teaming services, our Offensive Security practice conducts covert, real-world attack simulations against your organization to establish the effectiveness of your security systems and evaluate if and how your security team would detect and respond to a targeted attack.

Red Teaming Services can help you achieve:

Operational Efficiencies **Reliability** **Reduced Risk**

Finding the Right Solution

The most effective method for ensuring an organization's security team is prepared to protect critical assets is to run a realistic attack scenario within the organization. CDW's Red Teaming Services use sophisticated techniques to simulate a real-world cybersecurity attack to accurately assess a company's defensive posture and incident response.

While our Offensive Security experts may use many of the same tools and techniques used in penetration tests, the primary goal of a Red Team engagement is different. Our aim is to gain undetected access to your organization's network and, if detected, continue to act as an adversary to evaluate your response team. Your organization's security team is typically unaware of the planned attack, which allows us to assess their real-time responses to these active threats. An effective security team will be able to identify that an attack is in progress and deploy the necessary controls to stop it before sensitive systems and data are compromised. If an attack is missed, the Blue Team needs to identify the gap in their alerting tools.

Red Teaming is a vital element in accurately assessing a company's prevention, detection and response capabilities, and with CDW's Red Teaming services, we can help ensure that your organization's defenses are strengthened against future attacks

CDW + RED TEAM

CDW's Offensive Security practice has been helping thousands of global customers improve their cybersecurity posture through the identification of vulnerabilities and weaknesses since 1998.

- **Unparalleled Experience:** CDW's Offensive Security team is built on the extraordinary technical experience of its team members. CDW's penetration testing and technical security assessment methodologies have been developed and refined over 20 years and are backed through thousands of technical assessments.
- **Proven Methodologies:** As the cyber threat landscape has changed, CDW's pen testing approach has evolved to meet the dynamic needs of our customers. We have incorporated industry standards like PTES, OSSTMM, OWASP and NIST SPs to align with the leading edge of the market.
- **Certified Experts:** CDW's penetration methodologies are backed by skilled engineers who are regularly trained in the latest attacks and are equipped with the best tools available. Our team members hold more than 100 certifications, including CISSP, GCIH, OSCP and CRTO.
- **Dedicated Project Management:** Every CDW engagement has a dedicated security project manager (PM). This ensures your team and ours have a consistent project experience from end to end. This PM also ensures you are aware of activities and progress and providing you the updates and feedback you need.

CDW's full lifecycle of Services can support your organization no matter where you are on your journey

Design → Orchestrate → Manage   On-Premises → On-Journey → Cloud-Based

CDW

Services Overview

The following features are included as part of the CDW Red Teaming engagement:

Service	Available
Scoping Calls • Assess and define the roles and expectations of all stakeholders and determine the appropriate escalation paths.	✓
Planning Sessions • Evaluate the overall state of your current cybersecurity posture, including relevant security processes or controls and organizational structure, to determine which assets to exfiltrate along with any additional target-based objectives of the Red Team engagement.	✓
Active Attack Simulations • Conduct covert attack simulations to assess the detection and response capabilities of your organization’s Blue Team in the event of a targeted attack. Attempt to gain access to your internal network through various attack vectors while subverting your organization’s current defenses.	✓
Remediation Planning • Recommendations for improvements to security controls and best practices to guide mitigation efforts and help prioritize and address security risks based on their severity to your organization.	✓

Certifications

Our team of Offensive Security experts has earned the following certifications:

- CISSP: Certified Information Systems Security Professional
- CEH: Certified Ethical Hacker
- CRISC: Certified in Risk and Information Systems Control
- OSCP: Offensive Security Certified Professional
- GSEC: GIAC Security Essentials Certification
- GDAT: GIAC Defending Advanced Threats
- GCIH: GIAC Certified Incident Handler

To learn more about our Red Teaming Services,
contact your CDW Account Team or call 800.800.4239.