Solution brief

Red Team Operations.

Understand your vulnerabilities.

Evolving cyber threats create a dynamic risk environment.

How well prepared are you to meet these new challenges? First, you need to understand where your weakest points are and the limits of your visibility.

A Red Team Operation is a cybersecurity assessment that uses simulated attacks to gauge the effectiveness of your threat detection, response and containment capabilities. It also serves as a training exercise for your defensive teams as they contend with what seems to be an advanced adversary operating in your environment.

How it works.

The attack scenario starts with a simulated system breach on your network. After securing an initial foothold on a trusted system, our operators will seek to achieve one or more objectives by gaining situational awareness, escalating privileges, moving laterally, collecting sensitive information and exfiltrating data from your environment. We use similar advanced techniques, tactics and procedures that real-world attackers are deploying in order to effectively simulate a threat.

During an operation, we maintain detailed attack logs and Indicators of Compromise (IOCs) in order to provide your defensive teams with an operational view of an advanced threat as it unfolds. This allows them to gauge how effective current detection and response systems and processes are.

To create realistic testing scenarios, we work with you to identify objectives that threat actors may want to seek out. These could include:

- Sensitive data (credit card or Social Security numbers, Personally Identifiable Information (PII), source code, or intellectual property (IP)
- Access to critically sensitive areas of a target environment

All testing activities are coordinated with you and any vulnerabilities identified will be confirmed by our team to help ensure no false positives. Every effort will be taken during testing to demonstrate potential business impacts without harm to systems.

Reporting.

After analyzing the data collected during the operation, we provide you a written report detailing attack chains and findings, and a prioritized list of recommendations for improved mitigation and detection.

In addition to the written report, we offer customers the option to participate in a live call to review the findings and discuss how to remediate any security gaps that may have been identified.

Why Verizon?

We are not in the practice of one-size-fits-all consulting but instead tailor our services to meet the specific needs of your organization. Through our team of dedicated Threat and Vulnerability Management (TVM) security consultants, we are an active member of the international security community and well-respected in the fields of IT security research, vulnerability discovery, metrics development and secure development.

Learn more.

Red Team Operations can help improve your security posture by gauging how effective your defensive capabilities are. For more information, speak to your account representative.

verizon