

Bitdefender Offensive Services: Red Teaming

A shifting attack surface means increased demand for new technologies and services that identify and prioritize threat exposure across internal and external environments. For most organizations, cybersecurity validation – the convergence of techniques, processes, and tools used to validate how potential attackers would actually exploit an identified threat exposure, and how protection systems and processes would react – is now more necessary than ever.

Bitdefender now offers customized Red Team Exercises that simulate real-life threat actors to demonstrate how attackers would attempt to compromise the critical functions and underlying systems of your organization. It identifies security vulnerabilities (physical and digital) in the organization to help your security team improve detection and response capabilities.

Bitdefender Red Teaming utilizes MITRE ATT&CK®, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations, to perform realistic adversarial simulations. Two versions of the red team service are offered, designed at providing fulfilling different outcomes and objectives, depending on the requirements of the engagement. An organization can either take a scenario-based or a complete black-box approach.

Both versions follow the same execution methodology, but every environment is unique, so our Red Team Testers customize their methods and attack vectors to each engagement. We ensure best-in-class service delivery, with a team of CREST-accredited cybersecurity consultants who start every engagement with methodical, objective-focused scoping. Our rigorous standards and experienced team ensure your business has the most comprehensive and sophisticated detection and response capabilities in the face of increasingly sophisticated threats.

Bitdefender delivers red teaming engagements using a variety of methods dependent on the customer and objectives, such as:

- ↳ Network assessment and segmentation building to evaluate security controls, lateral movement, domain trust and firewall controls.
- ↳ Social engineering through malware or credential phishing to assess the level of security staff's awareness and response.
- ↳ Endpoint security evasion through obfuscation and modern techniques to execute malicious code.

At-a-Glance

Bitdefender Offensive Services ensure our customers have the most comprehensive and sophisticated detection and response capabilities in the face of increasingly sophisticated threats.

We empower you to find potential security blind spots, while also gaining knowledge and becoming better prepared in the case of a future attack.

Key Benefits

- ↳ Understand the true impact of a sophisticated targeted attack using a real-world attack simulation
- ↳ Improve prioritisation of your security investment
- ↳ Recognize threat exposures across internal and external environments
- ↳ Uncover hidden vulnerabilities using comprehensive assessments that go beyond a typical penetration test - before attackers do
- ↳ Meet regulatory and/or compliance mandates
- ↳ Prioritize security investments and resource allocations
- ↳ Provide in-depth reporting on cybersecurity posture to customers and partners

- ↳ Assessment of user groups and access control and abuse of low-level user privileges to escalate and emulate insider threat attacks.
- ↳ Exploitation of low-hanging fruit vulnerabilities, such as outdated software versions, default credentials or weak passwords.
- ↳ Abuse of Active Directory attacks and cloud security, depending on the environment.

Key Features:

- ↳ Assessment of the potential damage of a successful attack – before it occurs.
- ↳ Real results stemming from actual exploitation of internal and external security gaps.
- ↳ End-to-end project management to provide the utmost visibility and help you track progress.
- ↳ Support of internal audits for compliance certification acceptance or renewal.
- ↳ A CREST-accredited team of cybersecurity consultants who tailor red teaming to your unique environment, ensuring the exercises provide relevant and practical recommendations to resolve issues.
- ↳ Contextualized findings detailing results and observations for each phase of assessment, including techniques executed and an assessment of your prevention, detection, and response capabilities.
- ↳ Analysis and recommendations across the prevention, detection, and response spectrums.

Learn more about Red Teaming at [Bitdefender Offensive Services](#).

Contact Us

For more information on Bitdefender Red Teaming by, please reach out to [us](#).

Learn more about how **Bitdefender Offensive Services** can help your organization [here](#).