NuSummit Cybersecurity

DATASHEET

Red Teaming Services

The Enterprise Threat Landscape: Risks and Adversaries

With the rising global average cost of a data breach, organizations face a compelling need to bolster their security. To stay ahead of cyber threats, organizations must evaluate their security measures across internal, external, and physical domains, strengthen their defenses, and proactively identify vulnerabilities. To effectively defend against cyberattacks, it's crucial to understand the current threat landscape. Here are some key high-risk scenarios, attack vectors, and adversary groups your organization should be aware of:

Top Risk Factors

- Data Breaches
- Malware Targeting Company Assets
- Ransomware Holding Applications Hostage
- Non-Compliance With Regulatory Bodies and Standards

Top Attack Vectors

- Phishing Attacks
- Malware Infiltration
- Ransomware Attacks
- Disruption of Communications (Ddos Attacks)
- Botnet Operations
- Exploit Kit Utilization

Top Adversary Groups

- Organized Crime Syndicates
- Corporate Espionage Networks
- Insider Threats
- Lone Wolf Cybercriminals

Red Teaming Services for Elevated Cyber Defense

See Threats in Action

Immediate insights into attacker methodologies.

Prepare for the Worst

Insights into potential attack strategies for improved response.

Test your defenses

Evaluation of your ability to detect, respond to, and recover from threats.

Actionable Intelligence

Detailed reports with concrete recommendations for your security team.

Key Highlights

Our red team assessment service adheres to the industry-standard MITRE ATT&CK framework, developed by Mitre Corp., encompassing Tools, Tactics, and Procedures (TTP) similar to those observed in millions of enterprise network attacks leading to cyber breaches.

1 MITRE ATT & CK Aligned

Leverages the industry-standard framework for in-depth attack simulation.

2 Multi-Phased Targeted Attacks

Simulates real-world attacker tactics, techniques, and procedures (TTP) across multiple phases.

3 Breach Scenario Definition

Creates realistic scenarios to highlight the current security posture.

4 Exhaustive Component Evaluation

Scrutinizes every infrastructure asset for vulnerabilities.

5 Hidden Risk Identification

Uncovers previously undetected critical security risks

6 Threat Impact Analysis

Measures the potential consequences of exploited vulnerabilities.

7 Tailored Remediation Strategies

Provides actionable recommendations and solutions aligned with your specific business needs.

8 Assess Effectiveness

Evaluate the efficacy of existing security measures and protocols in preventing, detecting, and responding to attacks.

Our Approach

Our end-to-end red team assessments put your defenses to the test by leveraging multi phased simulated attacks. We meticulously target every component of your infrastructure - exposing hidden vulnerabilities and identifying potential security gaps. We offer a thorough analysis of your security posture, providing actionable insights and solutions to:

Simulate Real-World Attacks to Reveal Security Gaps

We create realistic breach scenarios that pinpoint weaknesse in your existing security posture.

Unmask Hidden, High-Impact Vulnerabilities

Our security services uncover hidden, high impact vulnerabilities and critical security risks, mitigating potential threats before attackers can exploit them.

Gauge the Potential Consequences of Threats

Our assessment of potential consequences of a breach helps prioritize remediation efforts.

Tailor Solutions to Your Specific Needs

Our customized security services and solutions address and identify vulnerabilities and strengthen your overall defenses.

Our Capabilities

With the rising global average cost of a data breach, organizations face a compelling need to bolster their security. To stay ahead of cyber threats, organizations must evaluate their security measures across internal, external, and physical domains, strengthen their defenses, and proactively identify vulnerabilities.

To effectively defend against cyberattacks, it's crucial to understand the current threat landscape. Here are some key high-risk scenarios, attack vectors, and adversary groups your organization should be aware of:

Post Exploitation And Persistence

Gain higher-level access, navigate horizontally, and establish an enduring presence within a network using cutting-edge methodologies upon infiltration.

Asset Access

Gain access to user accounts, identify vulnerabilities, and advance to higher access levels by controlling additional devices and systems.

Probe And Attack

We leverage recon intelligence findings to simulate targeted attacks, pinpointing vulnerable areas and exploring potential attack paths.

Security Control Evasion

Deflect security events by identifying weaknesses, modifying configurations, disabling services, establishing control privileges, moving between systems, and modifying logs.

Thorough Reconnaissance

We gather holistic information about your systems, policies, and configurations, simulating real-world attacker methods.

What sets us apart?

Our team of cybersecurity experts leverages extensive experience and cutting-edge expertise to protect your valuable assets from sophisticated threats. Our experienced advisors offer support to enable you to make well-informed decisions. Following industry best practices we provide remediation strategies covering both prevention and detection to enhance your overall cybersecurity posture. With extensive experience in managing high-risk threats and advanced cyber combat expertise, we can safeguard your valuable business assets and offer customizable security solutions in the following ways.

Vulnerability Neutralization

Proactive identification and neutralizing of vulnerabilities across data, software, and processes, fortifying your defenses against potential attacks.

Integrated Solutions Control

A unified and resilient security architecture built by seamlessly integrating security controls to safeguard critical assets from everyday threats and advanced attacks.

Advisory Support for Informed Decisions

Informed decision-making with the guidance of our expert advisors. We offer best practices and remediation strategies to elevate your cybersecurity posture.

Attack and Defense Readiness

Elevated security preparedness to mitigate the impact of threats and respond swiftly to breach attempts

Security Team Collaboration And Awareness

Empowered security team and other business functions through attack simulations and awareness training. We enable you to enhance collaboration and impart knowledge to effectively repel and respond to cybersecurity threats.

Detection and Response Optimization

We help fine-tune your detection mechanisms and response strategies, significantly reducing the time to detect and respond to actual attacks.

Success Stories

NuSummit Cybersecurity offers end-to-end security testing services to shield your organization from real-world cyber threats. Our highly skilled team of experts employs cutting-edge intelligence-based security testing methodologies to analyze and replicate the tactics employed by malicious actors, delivering unparalleled insights and strategic recommendations to enhance your security posture. Through a thorough assessment of your current security infrastructure, we offer readiness assessment, leveraging simulated multi-layered attacks to help you defend against specific cyber threats and achieve maximum protection.

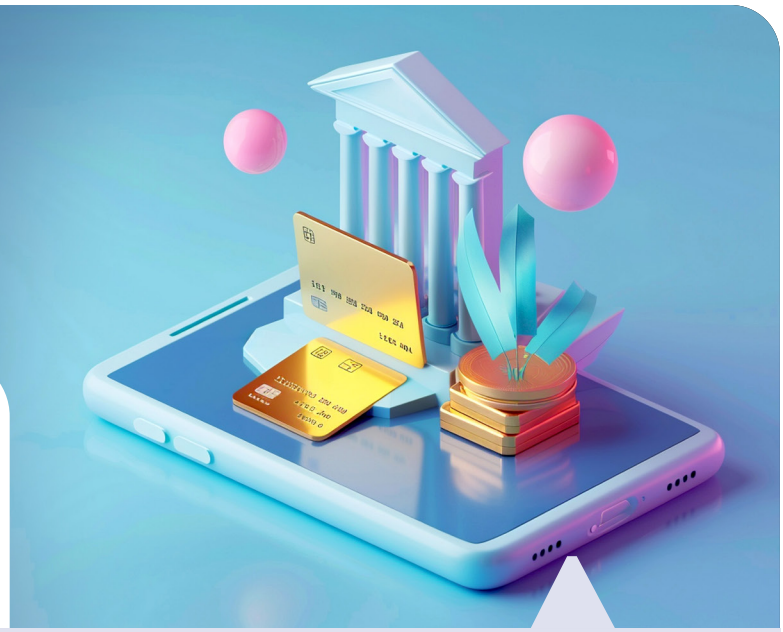
One of the Largest Banks in India

Business Challenge

The bank, as per RBI regulations, needed to conduct a Red Team Assessment over VPN to assess the effectiveness of existing security controls in its Annual Information Security Program. They sought a security partner to document remediation requirements for identified gaps and provide advisory support to non-security teams.

Business Impact/ Benefits Delivered

Our red team campaign successfully met most objectives, starting with accessing a domain joined VDI as a regular user and using stealthy methods to bypass network filters. We transferred offensive tools, elevated privileges, disabled security solutions, and gained access to core banking servers, VPC administrative consoles, and customer details after successfully bypassing the 2FA mechanisms. With our assistance, the bank identified defense control gaps and implemented recommendations to enhance prevention and detection capabilities, improving overall security posture and maximizing security investments.



One of the Largest Banks in Miidle East

Business Challenge

The bank, per SAMA regulations, required a Red Team Assessment to gauge its security controls against real-world attacks. Seeking a CREST certified company, they aimed to evaluate their overall security posture and detection/response capabilities. They needed a security partner to document remediation requirements for identified gaps and provide advisory support to non-security teams.

Business Impact/ Benefits Delivered

We are a CERT-In empaneled and CREST Approved Organization. We created threat profiles and scenarios to assess specific objectives and goals outlined by the bank, aiding in the identification of security vulnerabilities. We were able to perform various techniques to attack and bypass the security controls implemented within the bank's network. We worked closely with the bank to implement recommendations for addressing these gaps, ultimately enhancing their overall security posture. This collaboration aimed to maximize the effectiveness of security investments and improve incident detection, prevention, and response capabilities.

One of the Largest IT Outsourcing Companies in India

Business Challenge

The client, with an internal Vulnerability Assessment and Penetration Testing (VAPT) team, wanted to test their security against real internal threats. They needed a CREST-certified company for Red Teaming and advisory support, especially due to their European client base.

Business Impact/ Benefits Delivered

We identified new network vulnerabilities overlooked by the client's prior assessments. Through our internal Red Team assessment, we successfully accessed critical systems, providing advisory support to address issues and improve overall security posture.

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at **cybersecurity.nusummit.com** or write to us at **cybersales@nusummit.com**

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai Mumbai I New Delhi I Bangalore

Follow us at: