VinCSS
Trusted Cybersecurity Pioneer

RED TEAMING

Trusted Cybersecurity Pioneer

DESCRIBE

Red team is a service that simulates targeted and sophisticated attacks (APT - Advanced Persistent Threat) against organizations and enterprises with the goal of detecting and mitigating potential exploitable attack vectors early on. It also evaluates the effectiveness of existing network defense measures from the perspective of adversaries.

When provided in a continuous manner, "Continuous Red Teaming" service can help organizations detect and alert early on to threats that are often overlooked by defensive measures and procedures, or non-technical security threats.

Trusted Cybersecurity Pioneer

FUNCTION

SIMULATING TARGETED ATTACKS

The Red Team service can simulate the tactics, techniques, andprocedures (TTPs) of APT groups or mimic a purposeful sophisticated attack. This helps businesses conduct real-world testing and gain a practical understanding of how security vulnerabilities can be exploited to target their business operations.

PROACTIVE THREAT HUNTING

When provided in a continuous form (Continuous Red Teaming), the Red Team service helps organizations proactively hunt for potential security threats from external sources that could be leveraged against the organization. It also identifies and addresses security weaknesses from within that adversaries could exploit to achieve their objectives, expanding their impact within the organization.

MONITORING AND ALERTING FOR DATA LEAKS

With the assistance of a Data Leak Intelligence system that tracks information about data leaks on the internet, the Red Team service actively monitors and alerts when it detects data related to the business being leaked or offered for sale on the internet.

ASSESSING NETWORK DEFENSE CAPABILITIES

The Red Team service can be used to assess network defense capabilities, physical security at offices, headquarters, facilities, and factories. Enterprise organizations can also use the Red Team service to conduct experiments and simulations in coordination with the Blue Team to evaluate effectiveness and improve the quality of network defense solutions (Purple Teaming).

VinCSS
Trusted Cybersecurity Pioneer

PROCEDURE

01 TARGET IDENTIFICATION

VinCSS engages in discussions with the client to pinpoint specific objectives the client aims to achieve through the service. For example, assessing the capability of bad actors to infiltrate the internal network from the internet and demonstrating their ability to access financial data.

02 METHODOLOGY AND EXECUTION TIMELINE ALIGNMENT

After establishing the objectives, VinCSS advises the client on the methods to achieve those objectives and the timeline for execution. This includes which operational measures to implement, tools to use, and tactical approaches to choose. It also involves deciding whether to deploy Continuous Red Teaming or conduct a Red Team Campaign, including the duration.

03 DETERMINING ENGAGEMENT RULES

VinCSS collaborates with the client to define the rules that need to be adhered to during the service execution. For instance, specifying which operational measures should not be taken or outlining the coordination mechanisms between VinCSS and the client during the service period.

04 EXECUTION

VinCSS conducts activities according to the agreed-upon timeline.

05 REPORTING

For single campaign engagements, VinCSS provides detailed result reports and scripts for issue preproduce (if necessary) after the campaign concludes. In the case of Continuous Red Teaming, VinCSS reports security threats as they are detected and successfully exploited by experts, while also providing regular progress reports. For single campaign engagements, VinCSS provides detailed result reports and scripts for issue preproduce (if necessary) after the campaign concludes. In the case of Continuous Red Teaming, VinCSS reports security threats as they are detected and successfully exploited by experts, while also providing regular progress reports.

06 VERIFICATION OF REMEDIATION STATUS

VinCSS assists the client in advising on and verifying the remediation of identified security vulnerabilities until they are successfully addressed. Confirmation reports are provided after remediation.

Trusted Cybersecurity Pioneer

RESULT

Through Red Team reports, organizations will gain the most realistic insight into the security issues that exist within their environment.

Specifically, these reports will detail how these security issues are interconnected and chained together forex-ploitation.

They will also assess whether adversaries have successfully achieved their objectives to create significant impacts on the organization.

Additionally, Red Team reports provide recommendations to organizations on how to remediate security issues and address vulnerabilities of concern to minimize the risk of becoming a target of a sophisticated targeted attack.

Trusted Cybersecurity Pioneer

BENEFIT

MINIMIZE REAL-WORLD ATTACK VECTORS

Red Team activities help organizations reduce the impact of actual attack vectors that could be exploited to significantly affect business operations.

PROACTIVELY DETECT AND MITIGATE SECURITY ISSUES

Red Team engagements actively detect and mitigate security issues, particularly latent security problems that could form part of an exploitation chain in reality or newly emerging issues during continuous organizational operations.

ASSESS EFFECTIVENESS OF DEFENSE SOLUTIONS

Red Team assessments evaluate the effectiveness of defense solutions and minimize the chances of overlooking security issues that may be missed by other security measures.

Trusted Cybersecurity Pioneer

ADVANTAGE

EXPERIENCED TEAM

VinCSS's Red Team comprises experienced professionals who have earned reputable security certifications in the industry, such as SANS and Offensive Security certifications. The Red Team at VinCSS undergoes continuous training in various environments within a leading diversified corporation in Vietnam, spanning industries such as Automotive, Healthcare, Retail, Real Estate, Mobile Device Manufacturing, Technology, and Education.

DIVERSE TECHNICAL APPROACHES

VinCSS's Red Team campaigns are typically organized with a variety of technical approaches, without limitations on methods. These may include simulating Phishing, Vishing, Wireless Testing, Physical Testing, among others. Technical methods are selected and proposed to suit the specific challenges presented by each client.

TRANSPARENCY

All Red Team activities by VinCSS are closely monitored by VinSOC, allowing clients to monitor or audit the team's activities and data whenever necessary.

MAXIMUM SUPPORT IN POST-REPORT REMEDIATION

VinCSS closely supports and collaborates with clients during the post-report remediation process, offering guidance and assistance to verify the status of remediation until all reported issues have been addressed.

VinCSS
Trusted Cybersecurity Pioneer

THANK YOU!

VINCSS INTERNET SECURITY SERVICES JSC

• Floor 20A, Vincom Center Dong Khoi Building, No 45A Ly Tu Trong Street, Ben Nghe Ward, Dist. 1, HCMC, Vietnam.

• Email: sales@vincss.net • Website: www.vincss.net