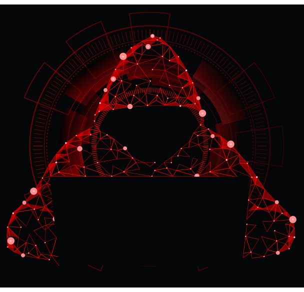
Payatu

Red Team Datasheet



OVERVIEW OF THE SERVICE

Traditional security measures, such as firewalls, antivirus software, and access controls, are no longer sufficient to protect against different types of attacks. With the ever-evolving and sophisticated nature of cyber threats faced by organizations, there is a rise in the need for a proactive and comprehensive approach to security. Red teaming is one such approach.

Red teamers simulate a potential adversary and use their expertise to challenge and test an organization's security measures. The goal of a red team is to identify and exploit vulnerabilities by simulating real-world attacks and testing an organization's defenses. This helps in providing actionable recommendations for improvement. By conducting realistic and thorough security assessments, a red team helps organizations strengthen their security resilience against real-world threats and stay one step ahead of attackers.

Payatu's red team experts are one to beat. These experts aka the Bandits, are highly skilled professionals who know how to curate and conduct this intelligence-led security assessment.

KEY ATTRIBUTES

Payatu's objective is to expose vulnerabilities associated not only with the client's security infrastructure (Network, Servers, Routers, Switches, etc.) but also with people and physical locations.

A combination of realistic and abstract approach

Having substantial experience and understanding of red team tactics paired with learning the organizations' crown jewels conceptually helps Payatu Bandits to define a process and roadmap specific to the client.

End-to-end defining of the scope

It is important for Payatu to address all types of potential attacks and gaps in the client's systems, which is why its scope covers everything from mirroring the conditions of a genuine cyber-attack to utilizing the same tactics, techniques, and procedures (TTPs) used by criminal adversaries.

Ultramodern tech integrations

Payatu strives to widen the testing surface to ensure the identification of all vulnerabilities, and it does so by integrating modern third-party tools and software for executing a game-changing red team assessment.

Reports that go beyond reporting

Generalized reporting is a drawback that can make any red team assessment futile. With Payatu, clients get a detailed report consisting of the findings, criticality ratings, granular breakdown of the vulnerabilities, failed testcases and even recommendations.

The Payatu Extra Mile

Payatu goes an extra mile by offering guidance to the in-house security team of the client on the mitigation and recovery plan, getting the compliance of the systems with the mandated standards, and a lot more.

KEY BENEFITS

It is important for clients to identify issues and risks that threaten the integrity, reliability, and performance of their organization, and it is equally important for Payatu to deliver on the same.

01 Identify Exposed Assets with Reconnaissance

To protect the assets from being compromised, it essential, first to identify where and how they are exposed over the internet. With active and passive reconnaissance, the target environment is analyzed, and the clients are given a more thorough and accurate picture of their assets' security posture.

02 Secure the Organizations from Physical Break-ins

By assessing their physical security posture, clients can understand better how to secure their organizations from attackers that try to physically break-in into their premises. Physical threats include but are not limited to lock picking, RFID cloning, etc.

03 Assessment of Team's Efficiencies Against Social Engineering Attacks

More often than not, the employees of the organization fall prey to fraudulent messages and are tricked into entering their credentials to the attacker's server/click on the malicious link. With Payatu's red team assessment, clients can assess the knowledge of their team against social engineering attacks such as phishing. The result of this assessment can be used to better train the employees.

04 Protection Against Infiltration in the Infrastructure

Payatu Bandits excel at uncovering the type of vulnerabilities and security issues that can be exploited. For the clients to protect their infrastructure and network from being infiltrated, it is critical to identify the ways in which infiltration and exploitation is possible.

05 Prevention of Attacks in Internal Networks Post-Exploitation

Once the attacker achieves an initial foothold in the internal network, clients must know how to prevent further attacks. With post-exploitation clients can know not just how to detect but also prevent attacks in the internal network.

06 Granular Understanding via Extensive Documentation

In the documentation, the details of the test cases, scan results, vulnerabilities found, and proof of vulnerabilities are captured along with an overview of the current security state of the target and how the customer can improve it.

07 Build Brand Confidence for Users

Clients can make security their value proposition in the competitive digital market by establishing trust within their users/clients by offering security as their brands' proposition.

08 High-Quality Testing

9 out of 10 industry leaders have made it a point to recommend Payatu's services to other pioneers because of the experiences they had while getting their organization tested. This has been made possible because of the best-in-class hires who have proved their mettle by going beyond their scope of work, even before they're hired.

Top Customers

NXP TATA DIGITAL ssmc tcs TATA CONSULTANCY SERVICES

ENGAGEMENT MODELS

You choose what works best for you!

Payatu offers different engagement models to let the client decide what floats their boat when they avail themselves of the red team assessment service. They can choose from

01

Time-boxed Approach,

where the client shares the details of the scope of assessment with Payatu and the service provider evaluates the time and investment required to execute the project. This goes both ways, the time can be decide by either client or Payatu.

Weeks	Coverage
4	Digital Infrastructure
5	Digital Infrastructure + Social Engineering of Employees
6	Digital Infrastructure + Social Engineering of Employees + 1 Location Physical Red Team