Payatu

Payatu Casestudy

MNC Catches Impersonator in Action with Payatu's CTI

(Cyber Threat Intelligence)

Payatu Security Consulting Pvt. Ltd

Project Overview

A pioneering Indian MNC identified that with a rapid growth in smartphone penetration, there was an increase in the adoption of digital services by businesses as well as consumers. To help businesses with their digitization to address the market needs, this MNC has set up a digital arm.

This new entity has been building digital businesses for a while now and has already created a holistic presence across various touchpoints. This has resulted in the new company soaring to great heights in a short time.

Now, for a company like this, it is critical to proactively take measures that will get them ahead of any threat actors' dirty tricks.

So, to ensure that, this company got in touch with Payatu and asked the service provider to be its CTI partner and help strengthen the security defense of the company.

Let's see how things unfolded for the client on the CTI landscape!

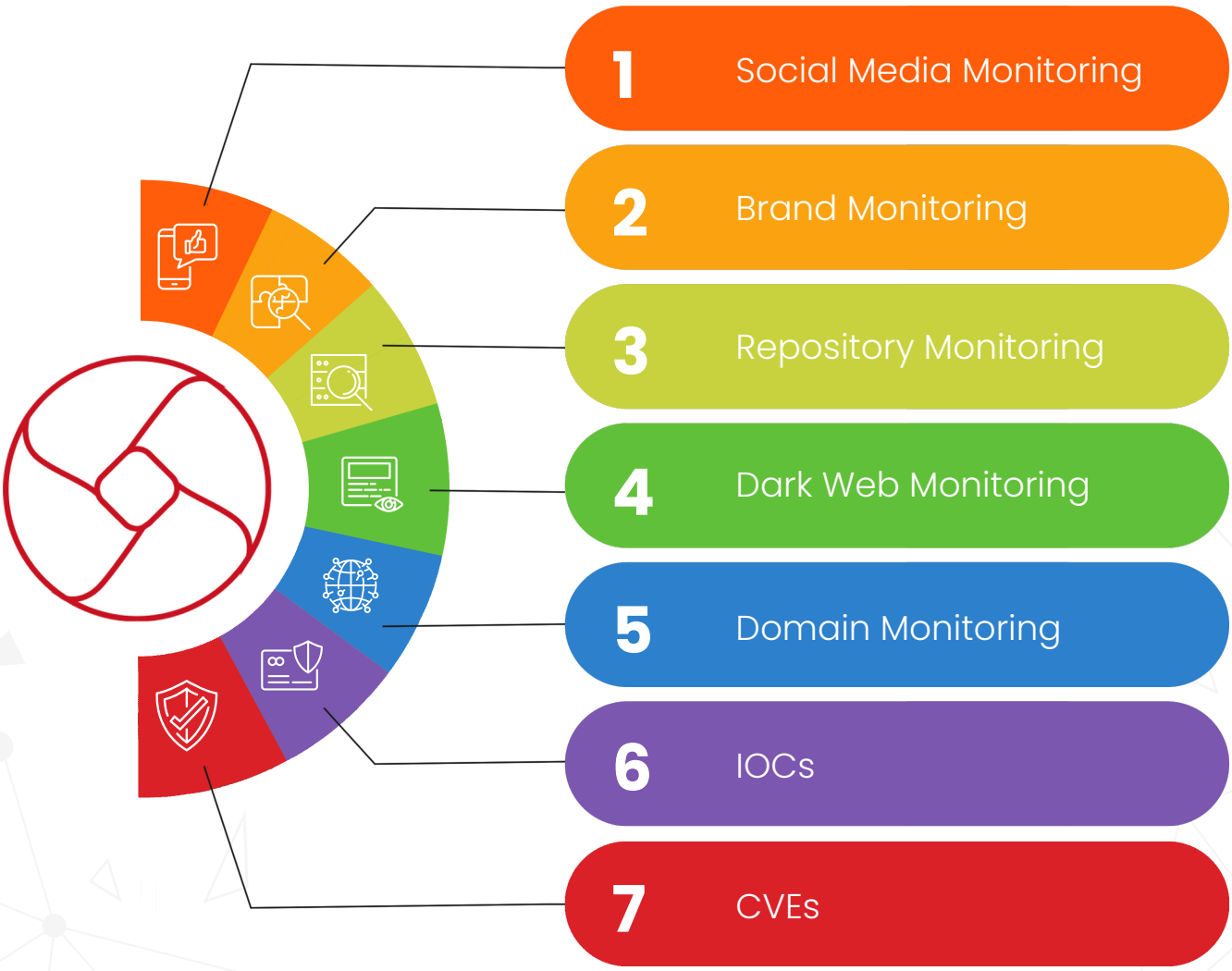
Scope

1. Collect any and all data available on the internet that involves the client
2. Monitor the dark web very minutely to spot any mention of the client
3. Periodic monitoring of the client's domain
4. Periodic monitoring of the client's social media
5. Brand monitoring
6. Update the client about any new vulnerabilities that make their way to the threat landscape
7. IOCs
8. Updates on the latest active malware family
9. Updates on the latest active APT group

Payatu's Action Items

Payatu's CTI deliverables can be divided into 7 top-level categories, that again can be divided into different steps.

The 7 top-level categories of the CTI service offered by Payatu are -



1. Social Media Monitoring

Social Media monitoring is required in order to identify fake accounts that might be created in the company's name, or any senior employee's name to scam the general public and/or the customers.

Why is there a need for monitoring social media?

It can help in identifying -

Fake company or high-level employees' profiles used to influence the followers and damage the reputation of the company

Fake messages to followers and connections asking for sensitive information to commit fraud

Fake job openings from the company leading to financial or other frauds

Fake videos posted by fraudsters ruining the reputation of the company

Suspicious videos or threads with the intent of scamming the public

Platforms monitored

Facebook

LinkedIn

YouTube

Twitter

Instagram

2. Brand Monitoring

More and more cybercriminals are now becoming extremely sophisticated and launching direct attacks on the brand name of an organization. They create fake pages, impostor domains, and rogue applications that are bound to ruin the name of the brand in the industry. Brand monitoring can help in identifying, analyzing, and responding to such cyber criminals by following an intelligence-driven approach.

Payatu offers brand monitoring by -

- Keeping an eye out for any similar newly created domains
- Navigating the digital space to identify any misleading information about the client
- Keeping a check of the client's complete brand presence

3. Repository Monitoring

With the world embracing the internet and the open-source community, it is unfortunately not uncommon for the employees of an organization to accidentally (or on purpose) make a repository public that should and needs to be kept private.

This can result in sharing of the source code of an upcoming application, sensitive internal tools data, and custom defined tools data with adversaries and competitors.

To ensure that this does not happen, Payatu -

- Monitors certain sources very closely
- Identifies any sensitive information pertaining to the client
- Specifically looks for any application or internal tools containing company's internal components

Sources Monitored

GitHub

GitLab

SOURCEFORGE

4. Dark Web Monitoring

This category is highly important since data leaks in case of an attack can be identified on the Dark Web.
The stolen or hacked data is more often than not shared on the Dark Web by the attacker, and identifying it is the first step towards damage control.

Actions taken -

1. Deep Web Crawling

Deep Web crawling refers to the problem of traversing the collection of pages in a Deep Web site, which is dynamically generated in response to a particular query that is submitted using a search form.

2. Deep/Dark Web Forums and Marketplaces Monitoring

A Dark Web forum is a platform where users can discuss things like drug trafficking, hacking, data leaks, etc. These forums offer different types of memberships for users such as VIP, Premium, or Moderator.

Marketplaces, on the other hand, are sites where different vendors offer different kinds of products for sale. For instance, Dark Web marketplaces have vendors that offer drugs, compromised accounts, databases, credit cards, and more. Users on Dark Web marketplaces fall into one of two categories:

Vendors who sell the product and **buyers who buy the product**.

Monitoring these can help in offering useful information to stop these cyber criminals in their tracks.

Sources Monitored

- Nulled Forums
- xss.is
- Breached Forums

5. Domain Monitoring

With techniques like DGA (Domain Generation Algorithm), threat actors have been creating fake/phishing domains which are generally look-alike domains, or in most cases have random domain names and website look-alike which can be identified by monitoring the logo of the company/app used.

Ngrok is a service frequently used by threat actors to host pages for phishing.

Actions taken -

- Checking what sort of trouble users can get in trying to type the client's domain name
- Finding look-alike domains that adversaries can use to attack the client
- Detecting typosquatters, phishing attacks, fraud, and brand impersonation
- DNS twist – Identifying domains not created by the client

6. IOCs

IOCs or Indicators of Compromise is a forensic term that serves as evidence of potentially malicious activity on a network or system. IOCs can be extremely helpful when studied thoroughly to better understand malware's behavior or techniques.

Actions taken -

Collecting and delivering the latest IOCs to the client on a weekly basis

Specifying the type of IOC, attributes, and the value

This value is then used by the client to simply ingest into its security solutions to look out for this value and create alerts if found

	A	B	C	D	E	F	G	H
1	type	attribute_	value					
2	url	gootloade	https://www.lenovob2bportal.com/test.php					
3	ip-dst|por	Mirai	107.182.128.29|1791					
4	ip-dst|por	Mirai	194.31.98.17|9375					
5	ip-dst|por	RedLineSt	3.131.207.170|14544					
6	url	Loki	http://qtd8gcdoplav737wretjqmaiy.ga/basement/fre.php					
7	ip-dst|por	Mirai	185.174.136.71|81					
8	url	LokiBot	http://lokaxz.xyz/fc/bk/ss.php					
9	url	ArkeiSteal	http://selousgame.com/					
10	url	LokiBot	http://45.133.1.20/healthone/five/fre.php					
11	url	LokiBot	http://198.187.30.47/p.php?id=7124741524802130					
12	url	LokiBot	https://cqmio.com/cj/loki/fre.php					
13	ip-dst|por	emotet	107.22.159.198|7774					
14	ip-dst|por	emotet	108.158.100.139|6752					
15	ip-dst|por	emotet	108.159.107.249|48268					
16	ip-dst|por	emotet	17.20.148.183|8907					
17	ip-dst|por	emotet	18.229.236.50|18850					
18	ip-dst|por	emotet	28.49.84.29|23589					
19	ip-dst|por	emotet	45.230.140.156|22366					

7. CVEs

CVEs or Common Vulnerabilities and Exposures is a list that classifies vulnerabilities and security-related threats. This list is publicly shared and made available in a very convenient way to exchange information about issues in the cyber world.

Actions taken -

- Delivering a weekly report containing a list of new CVEs
- Highlighting CVEs and breaches related to any third-party system of solution used by the client
- Making recommendations on how to patch the said vulnerabilities

8. Challenges

Restrictions to information sharing on the client's side made collecting relevant data a little challenging

Self-creation of the knowledge base turned out to be time consuming

Newer additions were made to the scope in the later stages of the project

Crunched timelines

Payatu's Everyday CTI Process

1. Aggregation of Indicators of Compromise, Articles and News Bits regularly from a vast number of sources.

2. Categorization of the aggregated threat intel data into two - 'Targeted' and 'Generic'.

a. Generic intel data is not directly associated with the client but is of significant relevance.
Eg. The client uses Microsoft Defender and a bypass technique for the same was being used by some malware campaigns in the wild.

b. Targeted intel data is directly associated with the client.
Eg. A 0-day exploit surfaced in one of the client's products.

3. Prioritization of the intel data into three - 'Current', 'Daily', and 'Weekly'.

a. Current intel data is any critical intel data point that is supposed to be reported immediately to the client.

b. Daily intel data is of higher priority and a collective summary of the same is supposed to be delivered every morning through a communication channel like email.

c. Weekly intel data is of lower priority and is supposed to be delivered weekly, i.e., every Monday.

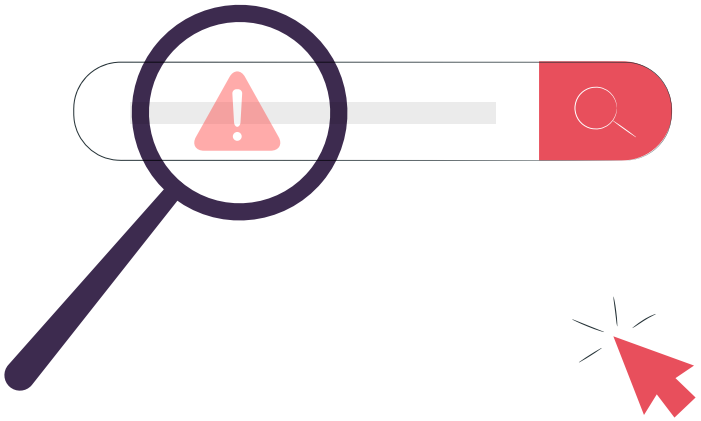
4. Periodic monitoring of social media platforms, newly registered Typosquat Domain Names and Dark Web for appearances of keywords relevant to the client. Any finding is supposed to be reported to the client with minimum delay from the time it is observed.

5. Planning and acting upon any explicit request from the client for targeted intel against any threat group or/and malware campaign and reporting back the findings with minimum delay from the time it is observed.

The Most Significant Finding of the Project

Payatu Bandits were able to independently identify an impersonator domain, that could very well be mistaken for the client's actual website.

This not only helped this MNC in catching hold of a website disguising itself as the client, but also played an extremely critical role in taking timely action and saving the brand name and customer trust.

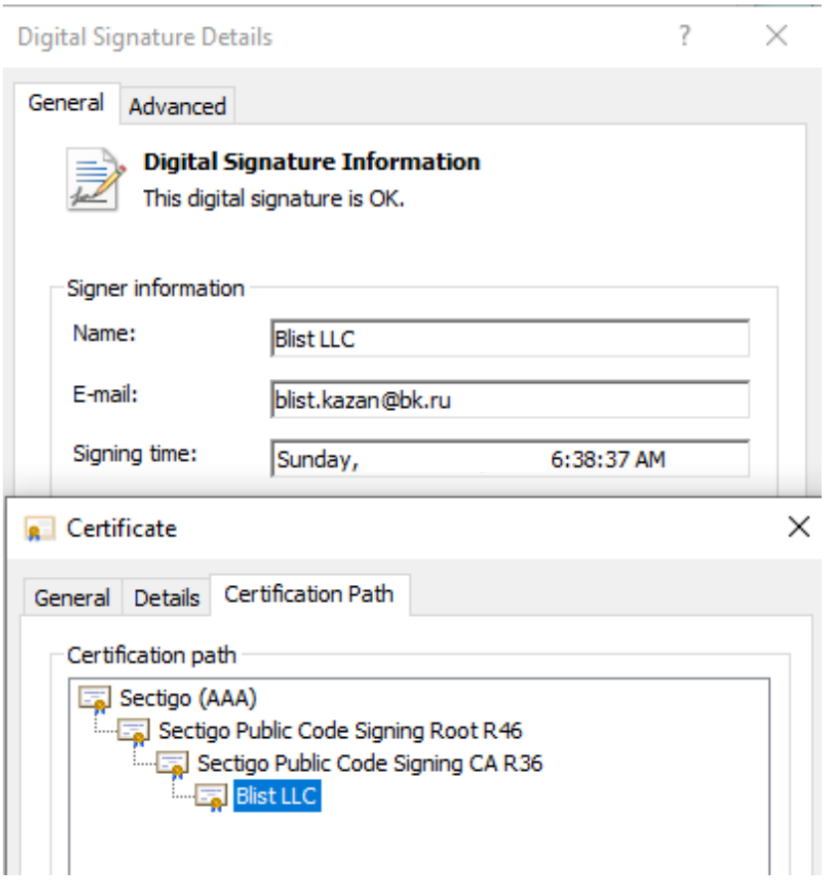


What Payatu CTI Deliverables Look Like?

2.1 Threat Intelligence regarding Blister Malware Campaign

Blister in its true sense acts as a loader for other malware and appears to be a novel threat that enjoys a low detection rate. This is due to the fact that it relies on a valid code-signing certificate to disguise malicious code as legitimate executables.

Blister uses a code-signing certificate issued by digital identity provider Sectigo for a company called Blist LLC with an email address from a Russian provider Mail.Ru.



Issuer: Sectigo Public Code Signing CA R36
Issued to: Blist LLC
Serial number: 2f4a25d52b16eb4c9dfe71ebbd8121bb
Valid from: Monday, 4:00:00 PM
Valid to: Wednesday, 3:59:59 PM

2.1.1 Detection

2.1.1.1 Registry Hives

Look for a base64 encoded Run key in the following:

2.1.1.1.a Machine Hive

"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run"*

"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run"*

"HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\Shell"*

2.1.1.1.b User Hive

"HKEY_USERS\\Software\\Microsoft\\Windows\\CurrentVersion\\Run*"*

"HKEY_USERS\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run*"*

"HKEY_USERS\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\Shell*"*

2.1.1.2 Startup Folders

Look for unwanted shortcut (.lnk) files in the following:

2.1.1.2.a Registry Path

"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User Shell Folders\\Common Startup"

"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Shell Folders\\Common Startup"

"HKEY_USERS\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User Shell Folders\\Startup"*

"HKEY_USERS\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Shell Folders\\Startup"*

2.1.1.2.b Startup Path

"?:\\Users\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs*"*

2.1.1.3 YARA Rule

YARA can be utilized to implement the following rule to detect Blister:

```
rule Windows_Trojan_Blister{
   meta:
      author = "Elastic Security"
      creation_date = "                "
      last_modified = "                "
      os = "Windows"
      category_type = "Trojan"
      family = "Blister"
      threat_name = "Windows.Trojan.Blister"
      reference_sample = "0a7778cf6f9a1bd894e89f282f2e40f9d6c9cd4b72be97328e681fe32a1b1a00"

   strings:
      $a1 = {8D 45 DC 89 5D EC 50 6A 04 8D 45 F0 50 8D 45 EC 50 6A FF FF D7}
      $a2 = {75 F7 39 4D FC 0F 85 F3 00 00 00 64 A1 30 00 00 00 53 57 89 75}
condition:
      any of them
}
```

2.1 Threat Intelligence regarding Enemybot Botnet

2.1.1 Introduction

Enemybot, a new DDoS **Linux-based** botnet attributed to Keksec was discovered in mid-March. Keksec is a threat group that specialises in cryptomining and DDoS attacks.

This botnet is mostly based on Gafgyt's source code, however some modules from Mirai's original source code have been spotted.

It also connects to a command-and-control (C2) server concealed within the Tor network, making it more difficult to take down.

Enemybot has been found infecting Seowon Intech and D-Link routers, as well as using a recently discovered iRZ router vulnerability.

Enemybot targets the following architectures:

- arm
- arm5
- arm64
- arm7
- bsd
- darwin
- i586
- i686
- m68k
- mips
- mpsl
- ppc
- ppc-440fp
- sh4
- spc
- x64
- x86

2.1 Threat Intelligence on Log4j Exploitation

The timeline for Log4j vulnerabilities discovered

CVE	AFFECTS	FIXED IN	DETAILS
CVE-2021-44228	Log4j2 2.0-beta9 through 2.12.1 2.13.0 through 2.15.0	2.15.0	An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled
CVE-2021-4104	1.2	EOL (August 2015)	Affects when specifically configured to use JMSAppender, which is not the default.
CVE-2021-45046	2.15.0	2.16.0	Message lookup substitution is disabled by default. But in certain non-default configurations, this could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments.
CVE-2021-45105	2.0-alpha1 through 2.16.0 (excluding 2.12.3)	2.17.0	No protection from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted.

2.1 Business Threat

- A malicious Python package (pymafka, similar to PyKafka) has been spotted in the PyPI registry performing supply chain attacks to drop Cobalt Strike beacons and backdoors on Windows, Linux, and macOS systems. It only reached a download count of 325 before it got removed. However, it could still cause significant damage to those affected as it allows initial access to the internal network of the developer. [1 2]

- Multiple security vulnerabilities in NETGEAR BR200 and BR500 routers have been acknowledged by the vendor as 'unable to fix'. In order to be exploited, these vulnerabilities require the computer managing the router to visit a malicious website or click a malicious link while accessing the router's management GUI. [1]

- Cisco has rolled out fixes for a medium-severity vulnerability (CVE-2022-20821) affecting IOS XR Software that it said has been exploited in real-world attacks. [1 2]

- The U.S. government is warning that the DPRK (North Korea) is dispatching its IT workers to get freelance jobs at companies across the world to obtain privileged access that is sometimes used to facilitate cyber intrusions. [1 2]

- A joint security advisory issued by multiple national cybersecurity authorities revealed the top 10 attack vectors most exploited by threat actors for breaching networks. [1 2]

Recommendations:

- Network related IOC(s) pertaining to various threat actors and malware families observed in the wild for the last 7 days are included in the corresponding *weekly-iocs-23-05-22.csv*. These can be used in identifying the corresponding threat actors and malware families.

- According to NETGEAR, it is unable to fix the disclosed vulnerabilities due to technical limitations outside of their control. However, NETGEAR has provided a list of security controls to remediate the risk. [1]

- The advisory, jointly released by agencies from the United States, Canada, New Zealand, the Netherlands, and the United Kingdom, includes guidance to mitigate the routinely exploited weak security controls, poor security configurations, and bad practices. [1 2]

Payatu

About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

CTI

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting – social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platform monitoring done for their brand.

IoT Security Testing

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

Payatu

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components “fit” together in your mega-product.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared. As long as cloud servers live on, the need to protect them will not diminish.

Both cloud providers and users have a shared responsibility to secure the information stored in their cloud Payatu’s expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Code Review

Payatu’s Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Red Team Assessment

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization’s crown jewels and test its readiness to detect and withstand a targeted attack.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Critical Infrastructure Assessment

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation systems etc. and can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure.

DevSecOps Consulting

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.

More Services Offered

- AI/ML Security Audit
- Trainings

More Products Offered

- EXPLIoT
- CloudFuzz

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.com

+91 20 41207726