Payatu

Payatu Casestudy

Web, Mobile and Cloud Security Assessment of a Thriving HR Product!

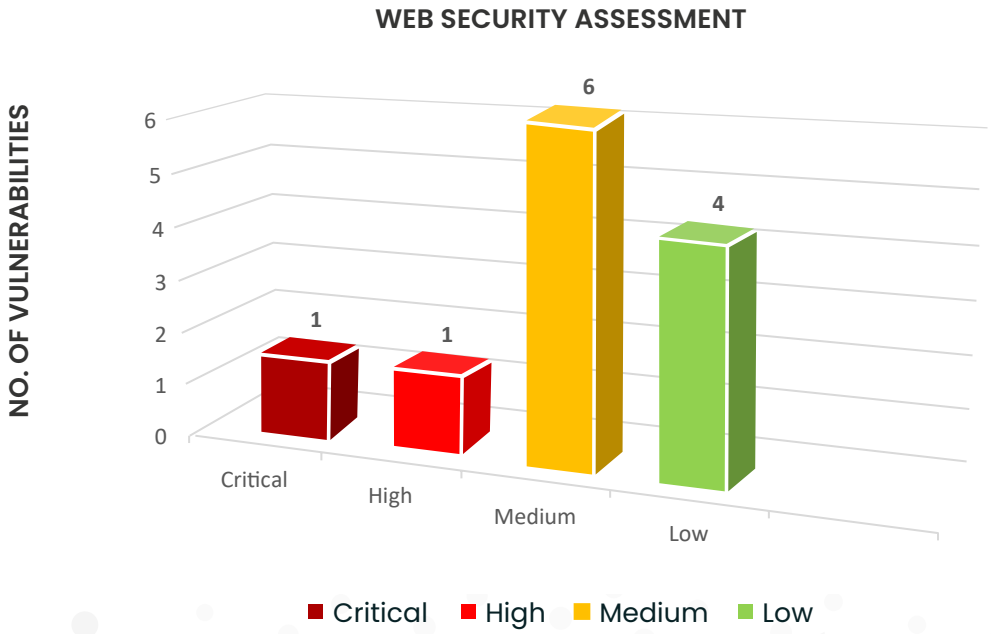
Payatu Security Consulting Pvt. Ltd.

Project Overview

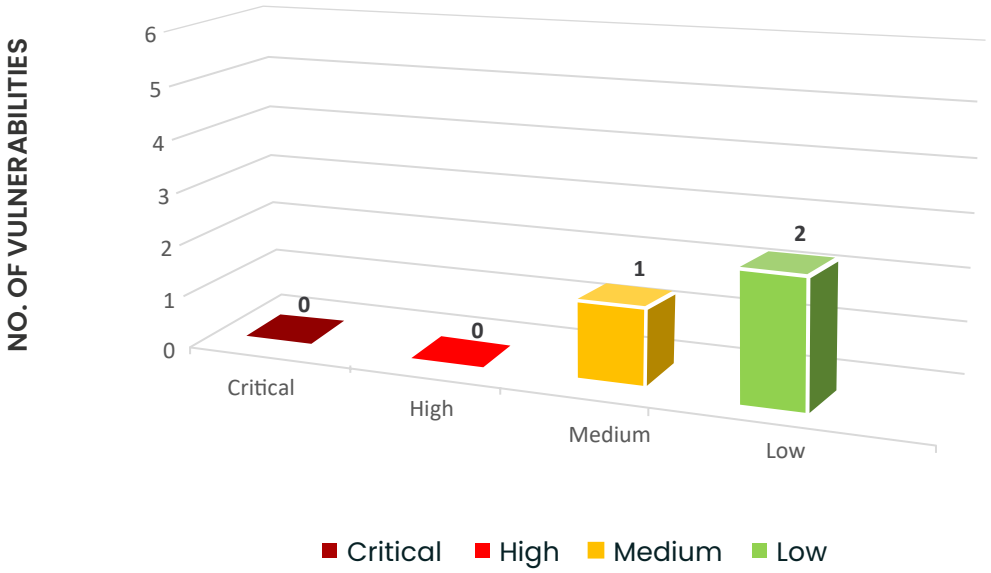
The product is committed to changing how businesses deal with talent and hiring by enhancing the experience for employers, recruiters, and applicants. The product has a large influence and is revolutionising an entire industry.

It was crucial to assess the product's Ecosystem Security Posture before launch, keeping its compliance and security timelines in mind. Payatu was tasked with conducting the following assessment:

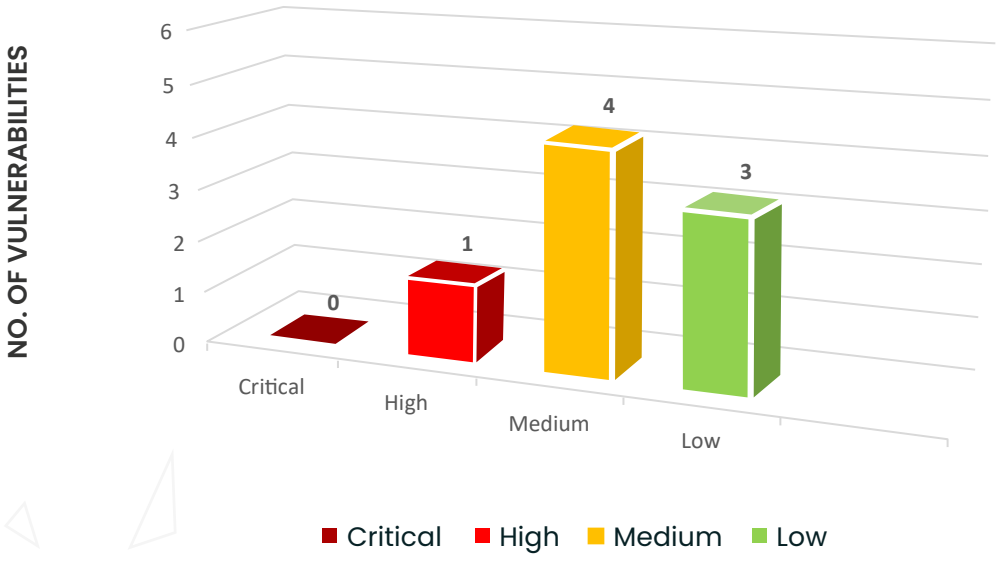
1. Web Security Assessment
2. Mobile Security Assessment (Android/iOS)
3. Cloud Configuration Review

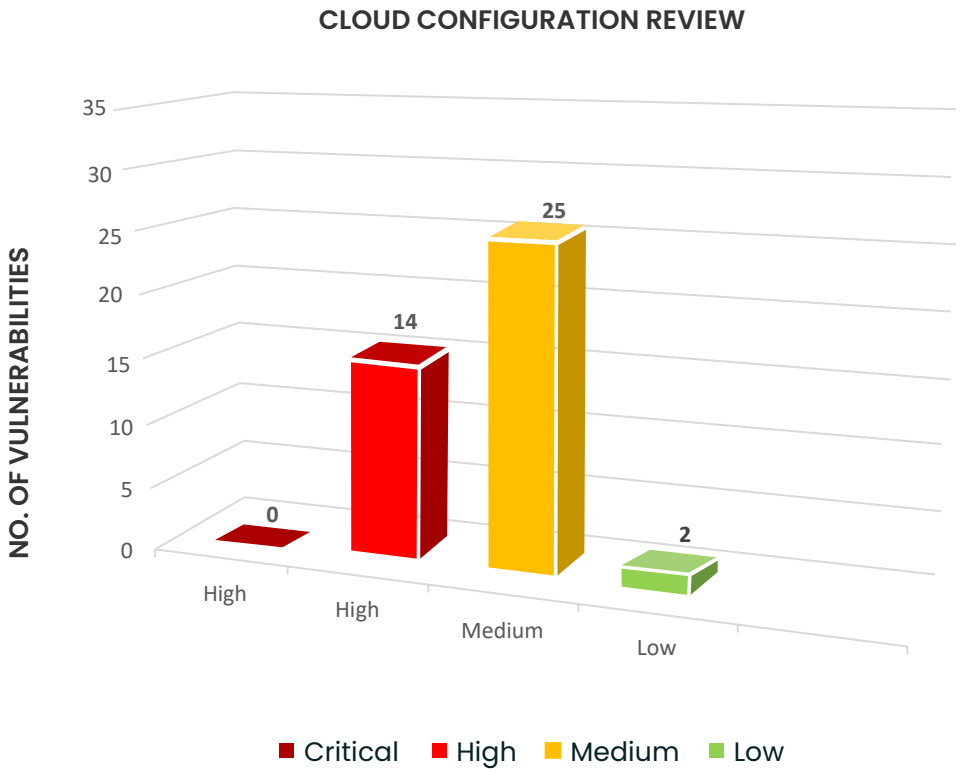


MOBILE SECURITY ASSESSMENT(ANDROID)



MOBILE SECURITY ASSESSMENT(iOS)





In this role, Payatu Bandits safeguard the product against various security threats by identifying all security flaws in their diverse infrastructure, explaining the impact and risks associated with the issues discovered, and making recommendations for prioritisation and remediation steps.

The Payatu Bandits stood out in this case for their expert evaluation of the product under time constraints and delivery of a thorough report customised to the Client's preferences.

1. Web Application Assessment

Scope of the study

Web Application Assessment of the product has been performed, considering below common security issues:

01 Proper access control is implemented across the application.

02 Proper authorization & authentication system is implemented.

03 Proper error handling is done to avoid exposing sensitive information.

04 The user is input handled properly or not?

05 Any other security related issue pertaining to the web applications.

Business Impact Summary

The following business impacts were identified:

1. An attacker can take over a user's account before creating the invitation link and change the email id to take over another user's account without any verification and invitation associated with the victim's email.
2. An attacker can read over fetched sensitive data received from API requests/responses.
3. An attacker can get access to the confidential/sensitive information, which was not intended to be visible by the lower privileged users.
4. An attacker can gain access to a user's system and thus compromise sensitive data on the victim's system, damaging their system and thus affecting the availability of resources.
5. The overall business impact of all the vulnerabilities found in the web applications can impact the confidentiality, integrity and availability of the system, which not only create service disruption but also loss in business.

Technology Impact Summary

The following technology impacts were identified:
The Payatu security team performs security assessments on the web application. These assessments aim to uncover any security issues in the assessed web application, explain the impact and risks associated with the found issues, and provide guidance in the prioritization and remediation steps.

It was identified that the web application did not implement access control features, especially 'User Invite Link' and 'API Endpoints'.

Testing Environment

To perform the platform's portal assessment, the Bandits set up the BurpSuite proxy tool and another automation tool for reconnaissance getting low-hanging vulnerabilities, which intercepts the HTTP/HTTPS traffic originating from the browser to the web application's server.

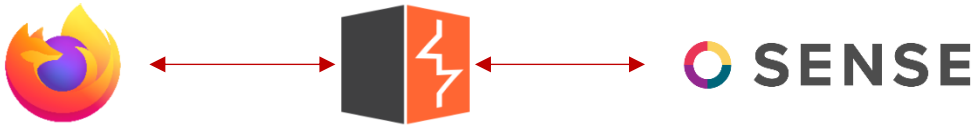


Table of Findings

VULN ID	FINDING	SEVERITY	STATUS
PY-SHQ-001	Pre-auth account takeover	CRITICAL	FIXED
PY-SHQ-002	Privilege escalation in setting module	HIGH	NA
PY-SHQ-003	CSV injection	MEDIUM	NA
PY-SHQ-004	User's invite code shared with third party	MEDIUM	NA
PY-SHQ-005	Arbitrary file upload	MEDIUM	FIXED
PY-SHQ-006	Old session does not expire after password change	MEDIUM	NA

2. iOS Mobile Application Assessment

Scope of the study

Security Assessment of the product has been performed, considering Payatu standards and globally recognized OWASP testing guidelines.

Overall security posture of the application is moderate, though some of the security controls/measures have not been properly thought of/implemented during the design and coding of the application, the exploitation is not very likely due to randomness in identifiers.

The security assessment revealed **0 critical** severity security issues, **1 high** severity security issue, **4 medium** severity issues, **3 low** severity issues in this application. Additional information is contained within the Technical Findings section of this report.

Based on the revalidation and comments from the client, the Bandits closed all the issues reported in the report. They marked these as Fixed or NA based on the revalidation by the Payatu Team or comments from the client's team respectively.

Business Impact Study

The following business impacts were identified:

1. Screenshots are cached, which can reveal sensitive information to attackers and lead to loss of customer data.
2. CSRF tokens and device tokens are stored in an unencrypted format which can be fetched by the attacker to chain different vulnerabilities resulting in high impact.
3. Unencrypted database file stored in the application data directory, which reveals sensitive information.
4. Use of potentially dangerous function in iOS application, which allows the attacker to extract customer data from the application.
5. Logs are saved in cleartext in the application data directory, which exposes users' information and leads to users' data loss.
6. As jailbreak detection is not implemented, the application can be installed on a jailbroken device, which will allow the attacker to extract more (not intended) information from the phone related to the application, like tokens, logs, etc.

Technology Impact Summary

The following technology impacts were identified:

- CSRF token and device token are stored in plist files, which can be viewed and modified easily on both the Jailbroken and non-Jailbroken iPhones.
- If an application allows storing cache data in a cleartext file and the application also uses some vulnerable hashing algorithms.

Testing Environment

To perform the iOS application assessment, the testing environment was setup using a jailbroken device and different automation tools for reconnaissance getting low hanging vulnerabilities.

Table of Findings

VULN ID	FINDING	REMEDIATION	SEVERITY	STATUS
PY-SHQ-001	Insecure communication: SSL pinning not Implemented	Implement SSL certificate pinning in the application.	MEDIUM	NA
PY-SHQ-002	Application is running on rooted device	Implement checks in the application to detect whether the application is installed on a rooted device.	Low	NA
PY-SHQ-003	Partially code obfuscation	Obfuscate string tables as well as methods. Use tools like proguard to obfuscate source code.	Low	NA

3. Android Mobile Application Security Assessment

Security Assessment of the product has been performed, considering Payatu standards and globally recognized OWASP testing guidelines.

Overall security posture of the application is **high,** though some of the security controls/measures have not been properly thought of/implemented during the design and coding of the application, the exploitation is not very likely due to randomness in identifiers.

The security assessment revealed 0 critical severity security issue, **0 high** severity security issue, **1 medium** severity issue, **2 low** severity issues in this application. Additional information is contained within the Technical Findings section of this report.

After the revalidation, the client's team evaluated the vulnerabilities and took the on decision of not implementing a fix for business reasons, disruption of service or the issue does not possess any threat to the business. As per the revalidation status, Payatu team is marking all the vulnerabilities as Not Applicable.

Scope of the study

Payatu Bandits conducted the security audit following the methodology mentioned in SOW and adhering to OWASP Mobile Top 10 – 2016.

The security assessment lasted three days.

Business Impact Summary

The following business impacts were identified:

1. An attacker can perform a MITM attack and sniff the traffic between the mobile device and the server. (Data Theft)
2. An attacker can read the application's logic from the decompiled source code if the application is not obfuscated. (Intellectual Property Theft)
3. An attacker can understand the workflow of the application if the application is running on a rooted device. (Intellectual Property Theft)

Technology Impact Summary

The following technology impacts were identified:

- During the assessment it has been identified that the application did not implement root detection and SSL pinning.
- An attackers can create a malicious fake application as code is partially obfuscated, which will allow the attacker to inject malicious code into the application's logic.

Testing Environment

To perform android application assessment, the testing environment was setup using a rooted device or any Android Emulator.

There are many android emulators like Android Studio, Genymotion, etc.

The BurpSuite proxy tool was also setup, which intercepts the HTTP/HTTPS traffic originating from the mobile application installed on the android device to the server.

Apart from BurpSuite, a few more tools like MobSF, Objection, Frida, Drozer, APK tool, Android Debug Bridge (adb), Dex2jar, and Jdgui were also setup.

Table of Findings

VULN ID	FINDING	REMEDIATION	SEVERITY	STATUS
PY-SHQ-001	Insecure communication: SSL pinning not implemented	Implement SSL certificate pinning in the application.	MEDIUM	NA
PY-SHQ-002	Application is running on rooted device	Implement checks in the application to detect whether the application is installed on a rooted device.	LOW	NA
PY-SHQ-003	Partially code obfuscation	Obfuscate string tables as well as methods. Use tools like proguard to obfuscate source code.	LOW	NA

4. Cloud Configuration Security Assessment

Scope of the study

Security Assessment has been performed, considering, but not limited to, the below common security issues:

01 Appropriate access control mechanisms and user rights management is in place.

02 Proper logging and monitoring have been incorporated in the infrastructure or not.

03 Encryption of data both in transit and at rest is configured.

04 If there are resources or users with excessive permissions.

The security assessment was performed as detailed in the SOW and Payatu Cloud Security Methodology v2.0.
The following services were part of the scope:

SERVICES		
ElasticLoadBalancer	DLM	SNS
Glue	ECR	APIGateway
S3	ElasticFileStystem	ES
SecretsManager	Transfer	Kinesis
SQS	ACM	Cloudwatch
SSM	ECS	Events
ElastiCache	Lambda	IAM
EC2	ElasticMapReduce	
RDS	States	
CloudFormation	Kafka	

Business Impact Summary

The following business impacts were identified:

1. Successful exploitation will allow an attacker to gain higher privileges. This privilege escalation will enable the attacker to access unauthorized AWS.
2. If there is no key rotation policy or unused keys are present, an attacker can use a compromised set of access keys without admin knowledge to access AWS services.
3. Users should not use root accounts for administrative operations. If it is compromised, it can damage the whole AWS infrastructure setup, which can damage the entire business.
4. If the AWS instances are not upgraded regularly, it may leave the database instances unpatched for vulnerabilities. It may be possible for an attacker to exploit these vulnerabilities and get access to sensitive data.
5. If the backup is not properly configured, it may lead to a loss of data in the event of failure.
6. In case of any breach, conducting a forensic investigation would not be possible as logging is not configured for most of the services.
7. It might be possible for an attacker to access the sensitive data stored in AWS resources which may result in sensitive information disclosure, loss of customer data and privacy violations.

Technology Impact Summary

The following technology impacts were identified:

- Payatu identified that the IAM roles were misconfigured, leading to privilege escalations.
- The credentials have been unused for more than 90 days, leading to an account takeover if the credentials get leaked. If an attacker gains access keys, they can access the AWS services without the administrator's knowledge.
- Allowing communication using HTTP will create a possibility of man-in-the-middle attacks.
- Logging is disabled for multiple services. If there is a compromise, there will be no evidence of the incident to investigate.
- Encryption of data is disabled for various services; if an attacker gets access to the underlying hardware or performs MiTM attacks, it may be possible to gain access to sensitive data in cleartext.
- Allowing weaker SSL/TLS protocols can allow an attacker to get back cleartext from cipher text. Services should be regularly updated to apply the latest features and security patches.

Testing Environment

To perform the cloud configuration review assessment:

Payatu Bandits used AWS command-line Interface (AWS CLI) and tools like scout suite, pacu and other in-house developed tools to perform a configuration review of the AWS infrastructure..

Table of Findings

VULN ID	FINDING	SEVERITY	STATUS
1	**RDS**		
1.1	Instance storage not encrypted	HIGH	NOT FIXED
1.2	Short or no backup retention period	HIGH	NOT FIXED
1.3	Auto-minor version upgrade	MEDIUM	NOT FIXED
1.4	Multi-AZ disabled	MEDIUM	NOT FIXED
2	**2 S3**		
2.1	Buckets with weak permissions	HIGH	NOT FIXED
2.2	Buckets access logging disabled	MEDIUM	NOT FIXED
2.3	Buckets allowing clear text (HTTP) communication	MEDIUM	NOT FIXED
2.4	Buckets without MFA delete	LOW	NOT FIXED
2.5	Buckets without MFA delete	LOW	NOT FIXED
3	**EC2**		
3.1	EBS volume not encrypted	HIGH	NOT FIXED
3.2	Instance metadata service V1 is used	HIGH	NOT FIXED
3.3	EBS snapshot not encrypted	MEDIUM	NOT FIXED
3.4	Default security groups in use	MEDIUM	NOT FIXED
4	**SNS**		
4.1	IAM actions authorized to all principals	HIGH	NOT FIXED
5	**SQS**		
5.1	IAM actions authorized to all principals	HIGH	NOT FIXED
6	**ELBv2**		
6.1	Load balancer allowing clear Text (HTTP) communication	HIGH	NOT FIXED
6.2	Access logging not configured	MEDIUM	NOT FIXED
6.3	Lack of deletion protection	MEDIUM	NOT FIXED
6.4	Drop invalid headers not enabled	MEDIUM	NOT FIXED

VULN ID	FINDING	SEVERITY	STATUS
7	**EMR**		
7.1	Encryption in-transit not enabled	HIGH	NOT FIXED
8	**ElastiCache**		
8.1	Encryption not enabled for cluster	HIGH	NOT FIXED
8.2	Redis version not updated	MEDIUM	NOT FIXED
9	**ECR**		
9.1	Image scanning not enabled	MEDIUM	NOT FIXED
9.2	Image tags mutability	MEDIUM	NOT FIXED
10	**ECS**		
10.1	ECS task log driver not used	HIGH	NOT FIXED
11	**ES**		
11.1	Encryption at-Rest not enabled	MEDIUM	NOT FIXED
11.2	Node-to-node traffic not encrypted	MEDIUM	NOT FIXED
11.3	Logging not configured	MEDIUM	NOT FIXED
11.4	HTTPS not enforced	MEDIUM	NOT FIXED
11.5	ElasticSearch version not updated	MEDIUM	NOT FIXED
12	**MSK**		
12.1	Encryption in-transit not enforced	HIGH	NOT FIXED
12.2	Outdated kafka version used	MEDIUM	NOT FIXED
13	**IAM**		
13.1	IAM policy too permissive	HIGH	NOT FIXED
13.2	Root account used recently	HIGH	NOT FIXED
13.3	Unused credentials not removed	MEDIUM	NOT FIXED
13.4	Lack of key rotation	MEDIUM	NOT FIXED
13.5	Users with multiple access keys	MEDIUM	NOT FIXED
14	**SecretsManager**		
14.1	Secrets should use CMKs	MEDIUM	NOT FIXED
15	**Lambda**		
15.1	TraceConfig is not active	MEDIUM	NOT FIXED

VULN ID	FINDING	SEVERITY	STATUS
16	**ACM**		
16.1	Transparency logging not enabled	MEDIUM	NOT FIXED
17	**Kinesis**		
17.1	Encryption in-transit not enabled	MEDIUM	NOT FIXED

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.

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.

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.

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.

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 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.

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.

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. pipeline to increase the visibility of security threats.

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.

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.

More Services Offered by Payatu

- AI/ML Security Audit
- Trainings

More Products Offered by Payatu

- EXPLIoT
- CloudFuzz

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.com

+91 20 41207726