Payatu

Payatu Case Study

Securing Over 1,600 Assets Across Web, Mobile, and Infrastructure for a Digital Health Insurance Leader

Payatu Security Consulting Pvt. Ltd

Project Overview

In today's hyperconnected world, trust and security form the backbone of digital healthcare. One of India's most prominent private health insurance companies renowned for its expansive reach and customer-first policies has been at the forefront of this transformation.

With over **17 crore** lives insured since inception, the organization plays a critical role in ensuring healthcare access across the country.

As the company scaled its digital footprint through mobile apps, web platforms, and modern infrastructure, it recognized the growing importance of cybersecurity. A seamless digital experience was no longer enough, security needed to be embedded at every layer.

To strengthen its digital defenses, the leadership engaged Payatu to conduct a multi-faceted security assessment covering mobile applications, web platforms, network architecture, and internal Wi-Fi systems.

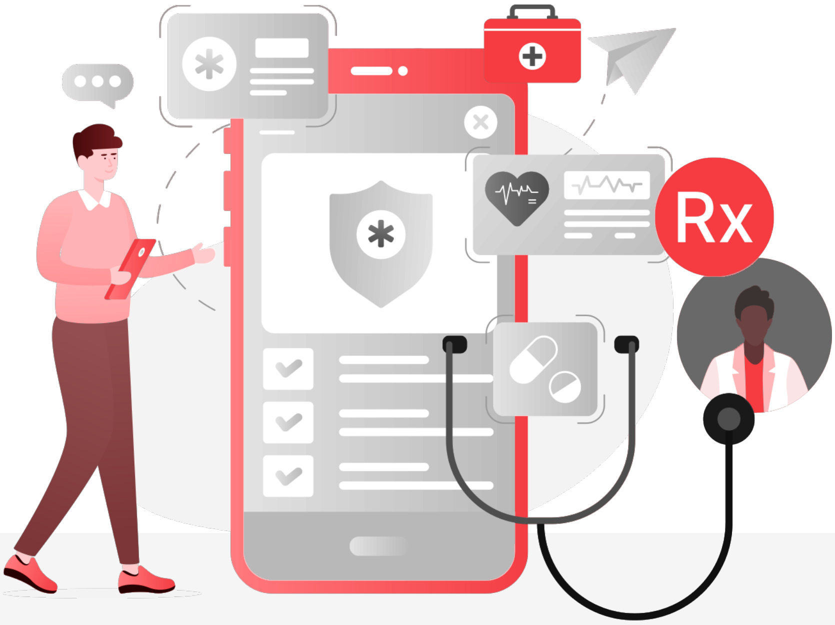
The goal: **identify hidden vulnerabilities and build a resilient, secure environment** that supports the company's mission of delivering accessible, high-quality healthcare**.**

Here's how Payatu helped turn that vision into action.

The Scope

- Penetration Test of 10 Mobile Applications
- Security Assessment of 35 Web Applications
- Infrastructure Penetration Test
  - External Network Penetration Test of 40+ subdomains
  - Internal Network Penetration Test of 1570 IPs Wireless
  - Wireless Penetration Testing

Mobile Penetration Testing Process



1. Discovery

The discovery process begins with information gathering, which is one of the most critical stages in a security assessment. This involves identifying the application platform, the frameworks and technologies used, API routes, and third-party integrations within the application.

2. Understanding the Platform

The Payatu Bandits invest time in understanding the mobile application from an external perspective. This includes studying the company behind the app, its business model, and the stakeholders involved. This context helps frame the security assessment in terms of real-world business impact.

3. Assessment

Mobile application testing requires a distinct approach, evaluating the app both pre- and post-installation to uncover hidden security flaws.

A. Static Analysis

Static analysis involves examining the application's source code without executing it. This phase includes decompiling the application using tools such as JADX, APKtool, etc. Once decompiled, the source code is reviewed for sensitive information like hardcoded secrets and access tokens. Key configuration files such as Android Manifest and info.plist are also analyzed to understand the app's components. This helps testers build a detailed view of the attack surface and identify potential vulnerabilities.

B. Reverse Engineering

In this phase, the Bandits aim to understand the internal workings of the application without executing it. The APK or IPA files are extracted from the device and decompiled using tools like Apktool, Jadx, Hopper, etc. The resulting code is analyzed for hardcoded secrets, API keys, and logical flows. If Runtime Application Self-Protection (RASP) mechanisms are implemented, their configuration and robustness are examined to identify potential bypass opportunities.

C. Local File Analysis

Once the application is installed on the device, the Bandits log in using provided credentials and interact with the app as a typical user would. During this interaction, the app writes data to its sandbox environment. The contents of this sandbox such as database files, shared preferences or plist files, cached data, logs, and temporary files are analyzed for insecure data storage practices or exposure of sensitive information like tokens, credentials, or personally identifiable information (PII).

D. Dynamic Analysis

Dynamic analysis is conducted while the application is running. This includes monitoring local I/O operations during runtime and analyzing network traffic between the app and its backend services. This phase helps uncover runtime vulnerabilities that may not be visible through static inspection alone.

4. Exploitation

Building on the insights gathered in earlier stages, the exploitation phase involves safely leveraging identified vulnerabilities. The Bandits attempt to gain unauthorized access or bypass security controls such as root/jailbreak detection or certificate pinning to perform restricted actions via the app's APIs. The objective is not just to confirm the existence of a vulnerability but to validate its real-world impact, while staying within the boundaries of the agreed testing scope.

5. Reporting

This is the final phase, where all findings are consolidated into a clear and structured document for stakeholders. The report includes an executive summary that highlights the overall security posture, key risks, and business impact for non-technical audiences, followed by a detailed technical section for developers and security teams. Each finding is documented with supporting evidence, and all exploitable vulnerabilities in the target system are recorded with associated CVSS v3.1 scores and reported to the client.

Web Penetration Testing Process

1. Understanding the Application

It's important to first understand the web application's architecture, user roles, and workflows because most logic flaws stem from how the app is intended to function. That's why the Bandits focus heavily on grasping the application's design and intended behavior before diving into exploitation.

2. Reconnaissance

To uncover meaningful vulnerabilities, it's essential to first expand the attack surface. That's why the Bandits start by identifying all possible exposure points, this includes subdomains, legacy URLs, IP ranges, hidden endpoints, publicly exposed git directories, open S3 buckets, vulnerable Jira instances, and even leaked credentials.

3. Vulnerability Assessment

After getting a better understanding of application functionality and getting all the necessary information, the actual vulnerability assessment phase begins.

A. Manual Testing and Business Logic Validation

With a solid understanding of the app and its common issues identified, the focus shifts to manual testing. This is where the Bandits attempt to uncover vulnerabilities that scanners often miss such as broken access control, privilege escalation, insecure direct object references (IDOR), and flaws in multi-user workflows. This phase relies heavily on human intuition, context awareness, and creative thinking to identify high-impact issues.

B. Automated Vulnerability Scanning

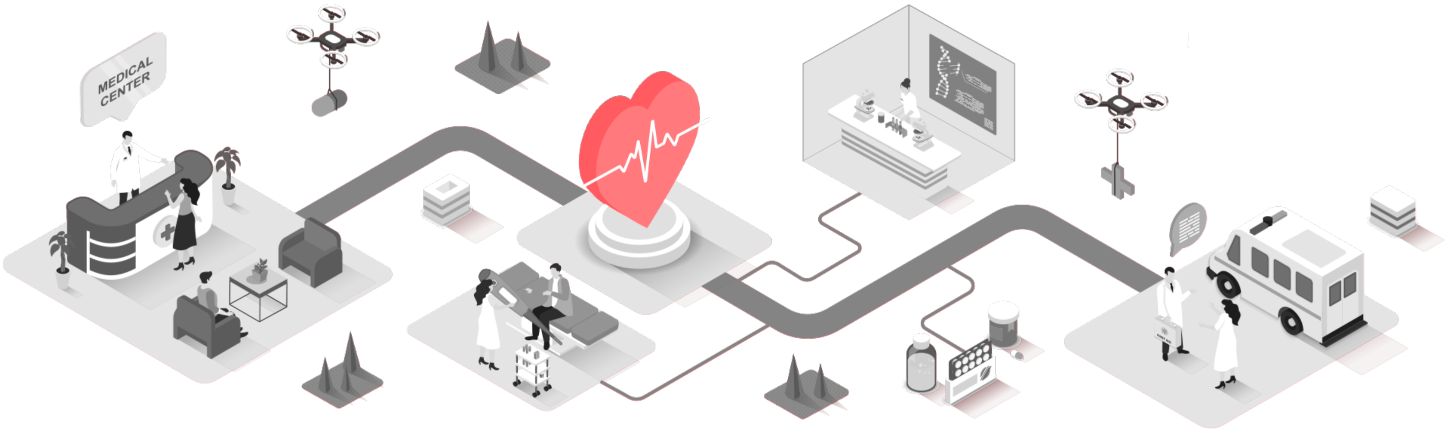
To identify baseline issues, industry-grade scanners are used to detect common and well-known vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS, and misconfigurations. These tools help surface low-hanging risks and provide initial insights into the security hygiene of the application.

4. Reporting

This is the presentable outcome of the security assessment exercise. All exploitable security vulnerabilities in the target system were recorded and reported to the client.

In the report, the details of the vulnerabilities, attacks, and proof of vulnerability were captured along with recommendations on how to mitigate those vulnerabilities.

Infrastructure Testing Process



1. Test Plan Development

Every assessment begins with creating a detailed test plan document. This includes analyzing the client's network architecture, identifying potential threat vectors, and defining testing milestones with clear timelines. Pre-requisites such as the IP address range, SSIDs, and any scope exclusions are finalized and documented. This phase ensures transparency and alignment before testing begins.

2. Reconnaissance and Information Gathering

The discovery process includes comprehensive information gathering which serves as the foundation for identifying attack vectors. The Bandits perform extensive reconnaissance to map the client's external footprint through domain enumeration, subdomain discovery, DNS analysis, and OSINT techniques. This black box approach helps identify all externally accessible resources that could serve as potential entry points.

3. External Network Assessment

The testing phase begins with comprehensive scanning of externally facing network assets. Both open-source and commercial tools, along with proprietary Payatu utilities, are used to discover services, open ports, and associated configurations on public-facing infrastructure.

A. Service Enumeration

Service enumeration is performed to identify running versions, exposed ports, and configuration anomalies on external assets. These findings are cross-checked against known vulnerability databases and enriched through manual probing to uncover weak points in the network perimeter.

B. Vulnerability Identification

External vulnerabilities are systematically identified through automated scanning combined with manual verification. Special attention is given to web services, mail servers, VPN endpoints, and other critical external services that could provide initial access.

4. Internal Network Penetration Testing

Through provided internal access, comprehensive internal network assessment is conducted. Large IP ranges are divided into manageable batches to avoid overwhelming the network infrastructure.

Network segmentation, lateral movement opportunities, and privilege escalation paths are thoroughly evaluated. Both authenticated and unauthenticated perspectives are tested to understand the full scope of internal exposure.

5. Wireless Network Assessment

Wireless infrastructure assessment covers both unauthenticated and authenticated attack scenarios. The Bandits evaluate wireless security protocols, encryption implementations, and access control mechanisms.

A. Unauthenticated Assessment

Testing includes identifying weak encryption, rogue access points, and wireless misconfigurations that could allow unauthorized network access.

B. Authenticated Assessment

Once connected to wireless networks, lateral movement opportunities and network segmentation effectiveness are evaluated from a wireless client perspective.

6. Exploitation and Post-Exploitation

For every confirmed vulnerability, controlled proof-of-concept (PoC) exploits are developed, ensuring that testing remains safe and non-disruptive. No exploits that could cause Denial of Service (DoS) or system crashes are executed without prior written approval. During critical stages like exploitation and post-exploitation, explicit client consent is mandatory, always obtained via email to maintain a verifiable communication trail.

The exploitation phase may use individual vulnerabilities or combine multiple findings to demonstrate complex attack chains and real-world impact scenarios.

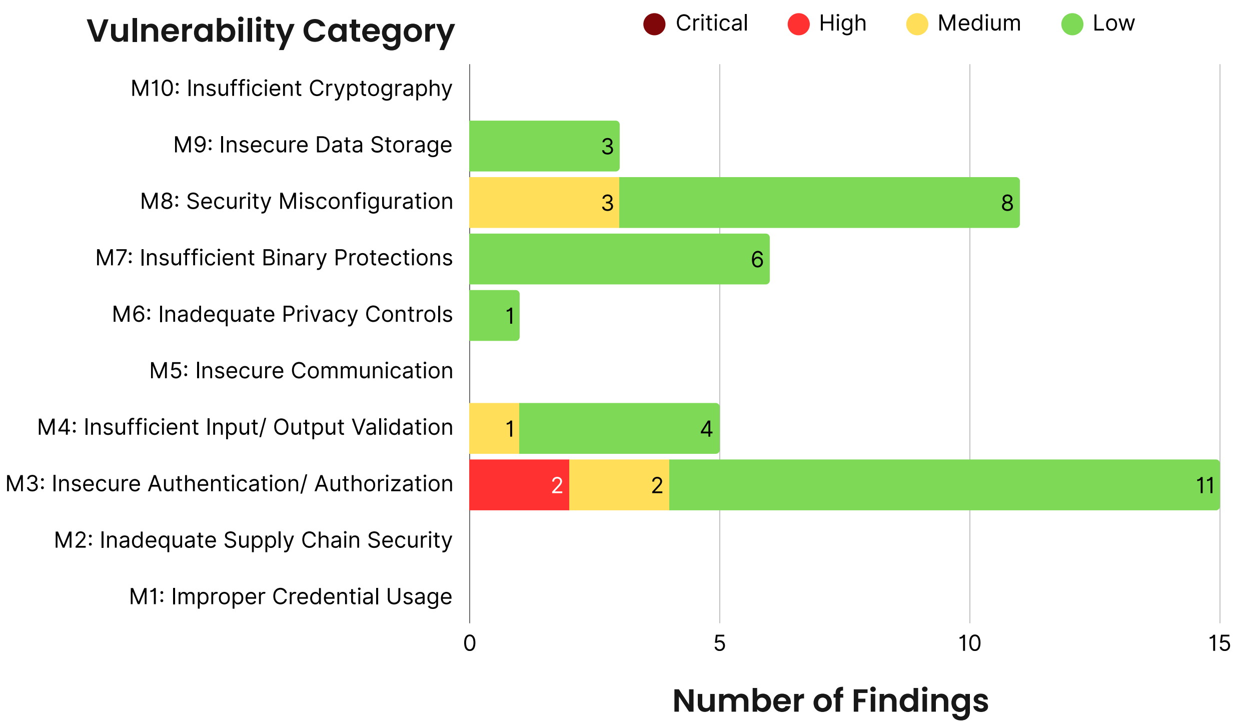
7. Reporting and Documentation

Throughout the engagement, test case status is tracked within the test plan document. All valid findings include step-by-step PoCs, screenshots, and remediation suggestions tailored to the client's environment. The final report serves as a comprehensive guide detailing vulnerabilities across external, internal, and wireless infrastructure while providing actionable recommendations to strengthen overall network resilience.

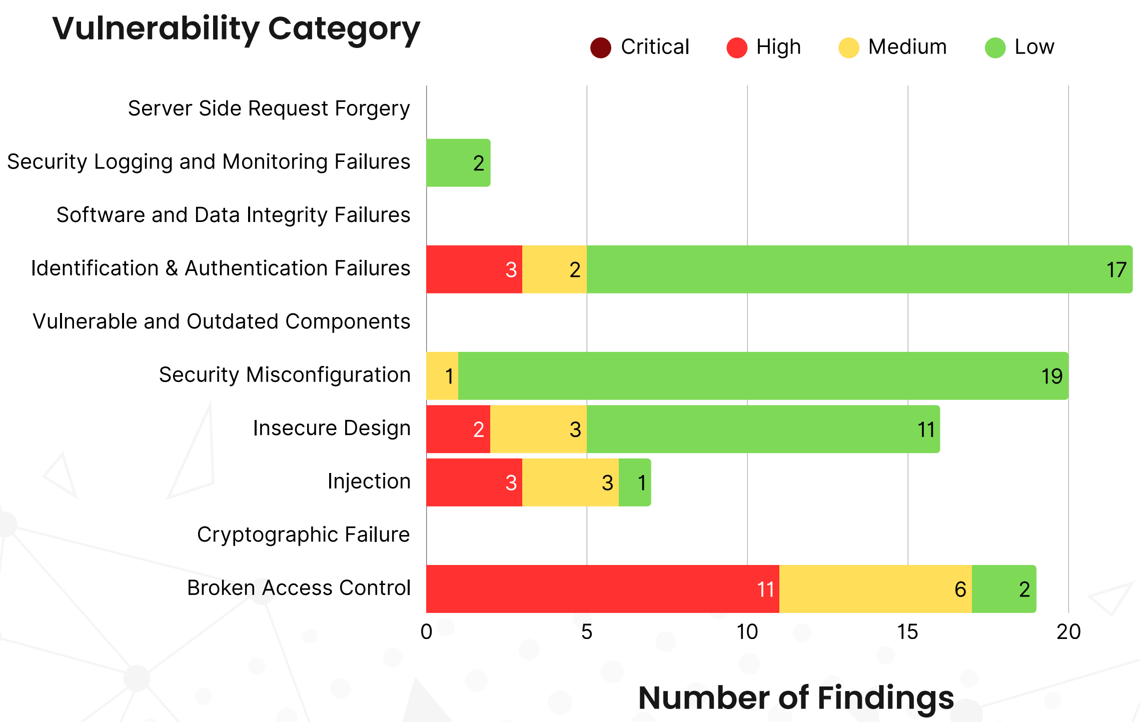
Findings

- Missing foundational access and authentication controls
- Overreliance on client-side encryption exposes underlying vulnerabilities
- Unsafe file handling and upload validation missing
- Lack of abuse prevention and activity control mechanisms
- Lack of secure input validation and output encoding
- Fundamental security controls missing
- Patch management failures - critical vulnerabilities (Eternal-Blue, Zero Logon) remain unpatched despite being years old
- Network segmentation was inadequate – unrestricted sub-net access indicated a poor network architecture
- Legacy systems present - SMBv1 and outdated SSH indicate older infrastructure without security updates

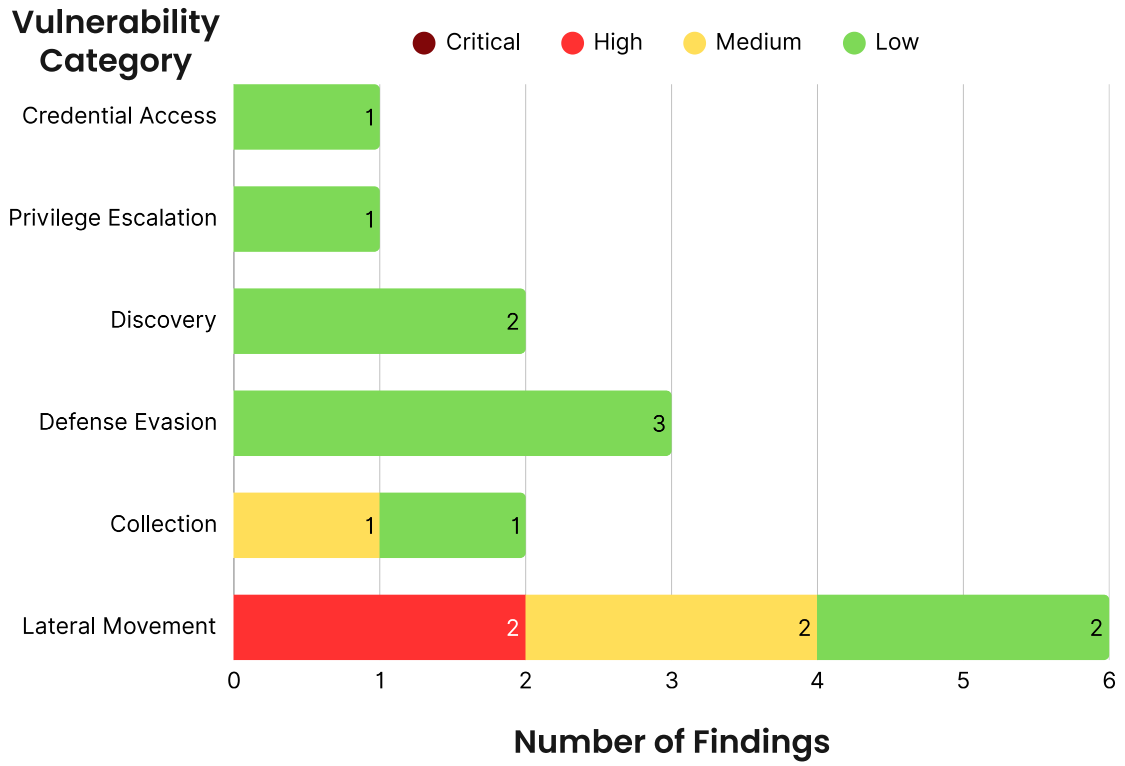
OWASP Mobile Top 10: 2024 Findings



OWASP Web Top 10: 2021



MITRE ATT&CK Framework: Network Assessment



Recommendations

Web Application Security

- Enforce strict server-side access control for all sensitive operations.
- Use parameterized queries or prepared statements to prevent injection attacks.
- Validate uploaded files with MIME type and scan using antivirus tools.
- Implement output encoding and avoid using user input in file paths.

Mobile Application Security

- Avoid storing sensitive data in AsyncStorage; use the iOS Keychain for encrypted, device-protected storage.
- Implement strong server-side access controls for all requests and use UUIDs or other hard-to-guess identifiers instead of sequential IDs.
- Use secure random tokens with short expiry, store refresh tokens safely, and revoke them on logout, password reset, or new login.
- Enforce restrictions and proper scoping for all API keys used in the application, regularly monitor their usage, and rotate them on a timely basis.

Infrastructure

- Patch critical vulnerabilities (e.g., EternalBlue, Zero Logon) and disable outdated protocols like SMBv1.
- Implement network segmentation and harden SSH, LDAP, and SMTP configurations.
- Enforce certificate-based authentication across wireless and critical services (e.g., EAP-TLS, admin access).
- Enable MFP and prevent plaintext credential transmission over Wi-Fi.
- Establish automated patching, regular vulnerability assessments, TLS hardening, and continuous network monitoring.

Business Impact

With the help of Payatu, the client was able to achieve -

Reduced financial risk by preventing data breaches that could lead to legal penalties, compensation payouts, and revenue loss

Protected brand reputation by avoiding security incidents that erode customer trust

Improved customer retention by ensuring a safer and more reliable user experience across digital platforms

Enabled faster go-to-market for digital products by removing compliance and security blockers early

Lowered operational downtime by proactively mitigating threats that could disrupt business continuity

Strengthened compliance posture for regulations like IRDAI, HIPAA, or GDPR, reducing audit friction and penalties

Optimized security spends by focusing resources on high-impact areas and avoiding expensive post-incident responses

Enhanced decision-making with greater visibility into infrastructure risks and remediation priorities

Decreased dependency on legacy systems, improving agility and reducing maintenance overhead

Improved partner and stakeholder confidence, enabling smoother collaborations and third-party integrations

Before Vs After

AREA	BEFORE ✕	AFTER ✓
Risk Exposure & Operational Resilience	Flat network, anonymous services, and unpatched CVEs exposed the organization to high-risk breaches and system-wide compromise.	Network segmentation, strict access control, and patch management reduced the attack surface by over 90% and limited incident impact.
Customer Data Security & Privacy	Sensitive user and internal data were exposed through SQLi, XSS, weak encryption, and insecure APIs.	Data is now encrypted, properly scoped, and excluded from exposure aligned with privacy best practices.
Access & Account Control	Broken access controls and insecure session management enabled privilege escalation and account takeovers.	Role-based access, MFA, and secure session handling protect against unauthorized access and account hijacking.
Revenue & Business Logic Protection	Price manipulation and flawed transaction logic risked direct financial loss and reputational impact.	Business-critical logic is now secured, preventing fraud, unauthorized changes, and revenue leakage.
Compliance & Stakeholder Trust	Lack of server-side validation, outdated protocols, weak access controls, and exposure of backend logic made the application vulnerable to multiple OWASP Top 10 risks, resulting in erosion of partner trust.	Alignment with OWASP improves audit performance and reinforces customer confidence.

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.

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.

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.

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.

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

- AI/ML Security Audit
- Trainings

More Products Offered

- EXPLIoT
- CloudFuzz

Payatu

Payatu Security Consulting Pvt. Ltd.
www.payatu.com
info@payatu.io
+91-20-47248026
+91-8319812123 (SALES)