Payatu

Payatu Case Study

50+ Applications, 2 Years, 1 Goal: Scaling Continuous Security for a Leading Global Travel Company with Payatu

Payatu Security Consulting Pvt. Ltd

Company Profile

As the travel and tourism industry is soaring to higher levels, supporting it with advanced technology has become paramount. Making the travel cycle seamless from start to finish is the need of the hour. Hence, more and more companies in this industry are now looking at expanding their horizons by integrating technology into their offerings.

Empowering these companies is an organization that offers products and solutions ranging from search engines to hotels, airports, and travel agencies. This organization is one of the reasons that global travel and hospitality has become more responsive and creative.

Being a multi-million-dollar organization, the goal for this company is to strive and be better every single day. With growing security threats, this organization wanted to be proactive and enhance its security ecosystem. Since the time was ripe, the management decided to partner with Payatu to get a better view of its security posture by identifying gaps and uncovering problem areas continually.

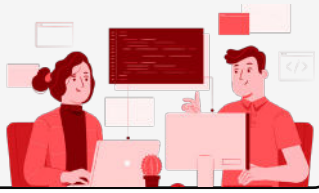
Keeping in mind the goal of achieving a robust security environment, the company hired Payatu for a 2-year long recurring assessment of different solutions, ensuring identification of all vulnerabilities and timely resolution of the same.

Let's take a step back and take a look at the client's security picture before the initiation of the project.

With millions of customers relying on its platforms for seamless travel experiences, the organization had invested heavily in security measures. Their approach included:

Periodic pentesting by external security vendors, ensuring compliance and vulnerability assessments.

A dedicated internal security team, responsible for conducting security reviews and responding to threats.



However, as the company continued its rapid expansion—onboarding new services, integrating third-party vendors, and handling larger transaction volumes—a crucial question emerged:

"Are we secure enough to handle the next wave of cyber threats?"

The leadership team knew that cyberattacks were evolving faster than traditional security methods could keep up with. While the company had never suffered a major breach, relying solely on scheduled security assessments and reactive responses no longer felt like a sustainable strategy.

The Security Management Team's Perspective: The Need for Proactive Security

The Security Management team, tasked with ensuring that the company's security posture remained ahead of the curve performed great, but was growing increasingly concerned about hidden vulnerabilities within the organization's ecosystem.

During an internal risk review, a critical insight emerged—while security tests were conducted periodically, there were gaps in continuous security validation. With 50+ applications and a complex infrastructure, even a minor vulnerability left undetected could be a potential entry point for attackers.

The team outlined two primary security concerns:

1. Strengthening Security for Business-Critical Applications

- The company's flight ticket booking applications and underlying infrastructure processed sensitive customer and financial data.
- A single vulnerability in these applications could lead to data breaches, fraud, and reputational damage.

2. Shifting from Periodic to Continuous Security Assessments

- One-time testing was no longer enough.
- The organization needed ongoing security assessments of all its applications in bulk.

The Top-Level Strategic Management's Tactical Decision: A Security-First Mindset

The top-level management had always viewed security as a business enabler, not just an IT function. They knew that in the travel and tourism industry, customer trust was everything. They understood that a single security breach could cause:

Massive financial loss due to fraud and data breaches.

Regulatory penalties for failing compliance standards.

Erosion of customer trust, leading to brand reputation damage

Recognizing that waiting for a breach to happen was not an option, the management greenlit a continuous two-year-long strategic security initiative—one that would take the company from reactive security to a fully integrated, proactive cybersecurity model.

After evaluating several security firms, the company chose Payatu as its trusted security partner.

The Security Assessment Process: A Proactive Approach

To align with the company's new security-first strategy, Payatu structured a multi-layered assessment process to uncover and remediate security gaps continuously.

1. Addressing the Challenges in the Existing Pentesting Process

One of the biggest challenges the company faced was that its pentesting process was unorganized. To address this, Payatu provided structured guidance and operational support:

Streamlined the pentesting process by establishing a predefined checklist of prerequisites, ensuring smooth execution.

Provided advisory on team structuring, ensuring optimized workload distribution and improved response times.

2. Security Testing Across 50+ Applications and Infrastructure (Continuous Testing)

With a structured recurring security assessment model, Payatu performed:

Web & Mobile Application Penetration Testing (PT):

Identified injection flaws, broken authentication, and business logic vulnerabilities in customer-facing applications.

Ensured secure API integrations for seamless communication between airlines, payment gateways, and third-party travel services.

Infrastructure Security Testing:

Conducted extensive network and cloud security testing to uncover misconfigurations, weak access controls, and exposed services.

Ensured secure hosting environments for customer data in compliance with industry standards.

Conducted an assumed breach exercise on individual services like k8s, Jenkins, databases, etc.

API Security Testing:

Validated authentication mechanisms and authorization models to prevent data leaks and unauthorized access.

Ensured robust API rate limiting to prevent brute-force attacks and abuse.

3. Establishing a Structured Remediation Strategy

Identifying vulnerabilities is only half the battle—remediating them efficiently is the key to reducing security risk.

Annual or Bi-Annual Pentesting Based on Criticality

Payatu recommended a structured approach where critical applications underwent security assessments annually or bi-annually, ensuring ongoing security validation.

Defined SLAs for Vulnerability Remediation

Implemented a clear SLA (Service-Level Agreement) framework for fixing vulnerabilities:

Critical issues: Immediate remediation within 24 hours.

High-risk vulnerabilities: Fix within 5 days.

Medium-risk issues: Address within 15 days.

Low-risk vulnerabilities: Documented and fixed based on business

This structured approach significantly improved risk management and reduced security incidents over time.

Vulnerabilities Found

Some significant vulnerabilities found during the span of 2 years under different assessments are -

- User impersonation
- Admin Credentials in Config File
- Compromise of latest credentials
- Broken Access Controls
- Payment Bypass
- Privilege Escalation to Root
- Hardcoded Data
- HTTP Verb Tampering Leads to Deletion of Critical Data

Avoided Potential Impact

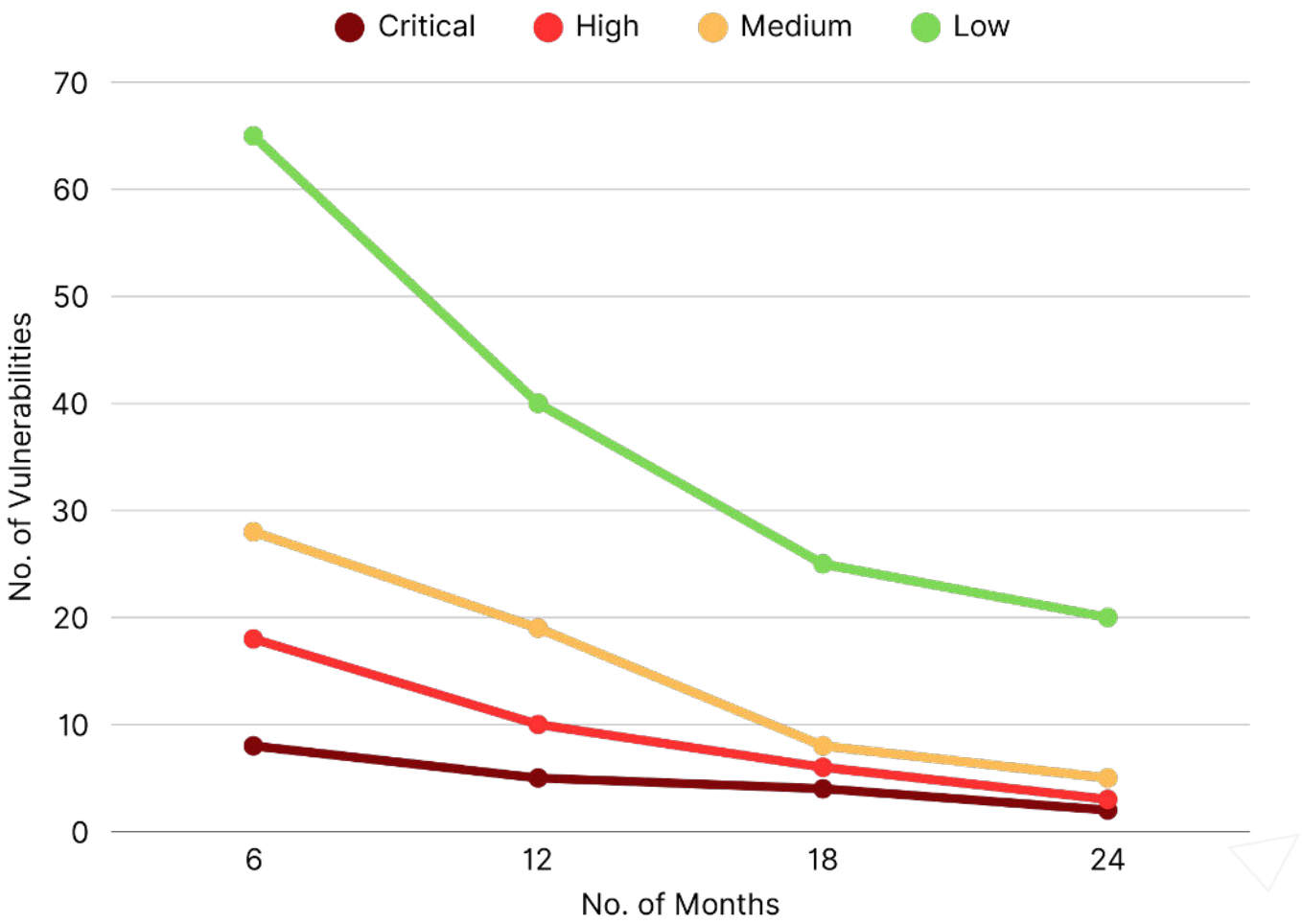
Potential Business Impact of Security Weaknesses that were avoided because of timely identification of vulnerabilities -

Issues in the flight booking flow could lead to poor user experience, ultimately resulting in customer attrition.

Seat selection conflicts—where multiple travelers were assigned the same seat—create confusion and could negatively impact the organization's reputation.

Allowing cab bookings at zero cost could result in direct revenue loss for the business.

Findings



Data shows that there was a steep decline in the number of vulnerabilities due to timely identification and fixation of the same.

Current Scenario

The engagement has been renewed by the client for several more assessments and is still ongoing.

Payatu continues to help this and many other such clients in evaluating the security strengths and weaknesses of their products, applications, infrastructure.

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.

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.

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.

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.

Security Operations Center

Cyber threats are everywhere, often operating in the shadows. Their goal: to breach networks, compromise systems, and steal critical data. With Payatu's SOC service, you can uncover these hidden threats, bolster your defenses, and protect your data from relentless cyber attacks.

Payatu

AI / ML Security Audit

Incorrectly implemented AI/ML systems can lead to security and privacy issues. The severity of which depends on how critical the use case is. The repercussions of the same include misclassification of unauthorized entities, theft of intellectual property such as application train models, etc. With a dedicated team capable of effectively assessing and strengthening AI/ML systems, we can provide specific methods to prevent potentially damaging threats before they potentially derail your project.

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.

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.

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

- Trainings

More Products Offered

- EXPLIoT

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.io

+91-20-47248026