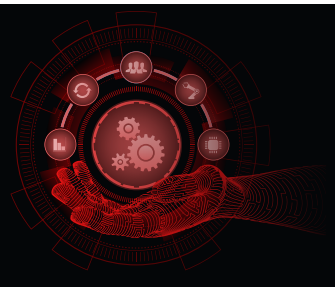
Payatu

IoT Security Datasheet



OVERVIEW OF THE SERVICE

Designing and delivering an embedded/IoT device is one thing but developing and offering a secure embedded/IoT product is altogether a different ballgame. With the fast-paced adoption of smart devices, hackers have elevated their attacking skills as well. The only way to fix any gaps in these devices and ecosystems is by actually identifying them first. That is when IoT security assessment comes into the picture.

Payatu is an industry-leader in delivering class-A IoT security assessment that has helped a number of reputed clients and big names in the IoT field in evaluating all kinds of threats and vulnerabilities. This service company is highly appreciated for its capability to provide one-of-a-kind security assessment that covers everything from hardware, firmware, Radio/RF, IoT protocols, cloud pentest, mobile app pentest, threat modeling, and fuzzing.

KEY ATTRIBUTES

Payatu's objective is to perform controlled attack and penetration activities to assess the overall level of security of the IoT/embedded devices and ecosystem, and what sets this service provider apart is -

A combination of realistic and abstract approach

Having substantial experience in this arena paired with learning the client's product 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 on the client's IoT products, which is why its scope covers everything ranging from embedded/hardware systems, network services, applications, firmware, any and all device-specific requirements, etc.

Ultramodern tech integrations

Payatu strives to widen the attack surface to ensure identification of all vulnerabilities, and it does so by integrating different internal, external, and modern third-party tools and software.

Compliance-driven assessment

Payatu's IoT assessments incorporate domain and technology-specific compliance standards, guidelines, and best practices to enable the clients to get clear visibility into any compliance violations and actions to become compliant via Payatu's mitigation strategies and recommendations.

Reports that go beyond reporting

Generalized reporting is a drawback that can make any IoT security assessment futile. With Payatu, clients get a detailed report of the test cases that worked, breakdown of the vulnerabilities, failed test cases, mitigation strategies, and recommendations.

The Payatu Extra Mile

Payatu goes an extra mile to retest and revalidate the products, offer guidance to the in-house security team of the client on the mitigation plan, get the compliance of the IoT products with the mandated standards, and a lot more.

Payatu

KEY BENEFITS

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

01 Finding Vulnerabilities with Device Hardware and Firmware Reconnaissance

To identify different vulnerabilities, reconnaissance is performed, which is the process of collecting as much information as possible about the target product ecosystem to find vulnerabilities and ways to penetrate into the device. Information such as electronic components, bus communication, interfaces, RTOS/BareMetal firmware metadata, and OS attack surface is collected.

02 Spot Weak Points with Radio and Network Protocol Scanning

Clients can spot different weak points in their devices, with scanning, which is the process of analyzing the communication mechanism and technologies used. Payatu Bandits use a combination of automated and manual scanning to identify vulnerabilities and weaknesses of a target device and its communication interface in order to determine how it can be exploited.

03 360° Attack Surface Coverage

When assessing a system, it is important to identify both software and hardware vulnerabilities that can compromise a device as well as the whole ecosystem including software applications, cloud, device firmware, and hardware. Payatu Bandits utilize tools and techniques to identify the entire attack surface of the target system, right from hardware to the cloud, which gives a complete threat landscape of the system.

04 Compliance and Risk Assessment

It is the process to conduct risk profiling of the target system based on the impact as well as the domain-specific compliance violations from the identified vulnerabilities.

05 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.

06 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.

07 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 IoT products 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

stryker ESPRESSIF Binatone Johnson Controls

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 IoT security 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.

S. No.	IoT Module	Scope Coverage	Timeline
1	Hardware Security Assessment	01	2-4 Weeks
2	Firmware Security Assessment	01	2-4 Weeks
3	Radio Security Assessment	01	2-3 Weeks
4	Cloud Security Assessment	01	1-2 Weeks
5	Web/Mobile Application Assessment	01	1-2 Weeks

02

Master Services Agreement

Minimum duration & projects commitment,

where Payatu conducts a T-shirt sizing of the client-proposed minimum scope and classifies each project as per complexity.

Minimum T&M effort commitment,

where Payatu proposes investment mapped with resource skill, resource experience, duration of T&M engagement, based on the client-proposed minimum commitment.