Payatu

Payatu Casestudy

Leading Australian Fintech Gets a 360° Security Reformation with a New MSSP

MSSP – Managed Security Services Provider

This is a tale of how a game-changer organization was actually able to up its game by getting Payatu onboard as its Managed Security Services Provider.

In this scenario, Payatu became the outsourced partner of the client, and would look after the monitoring and management of the cybersecurity of the company as a whole.

What makes this case study even more fascinating is the fact that it shows the partnership between the two firms demonstrating excellence from one end and consistent trust from the other.

The client of Payatu here, a leading Australian cashflow funder and small business transaction financer realized that it needs an end-to-end security services provider that would help in safeguarding not just the infrastructure, but also everything ranging from devices, assets, and applications.

Project Overview

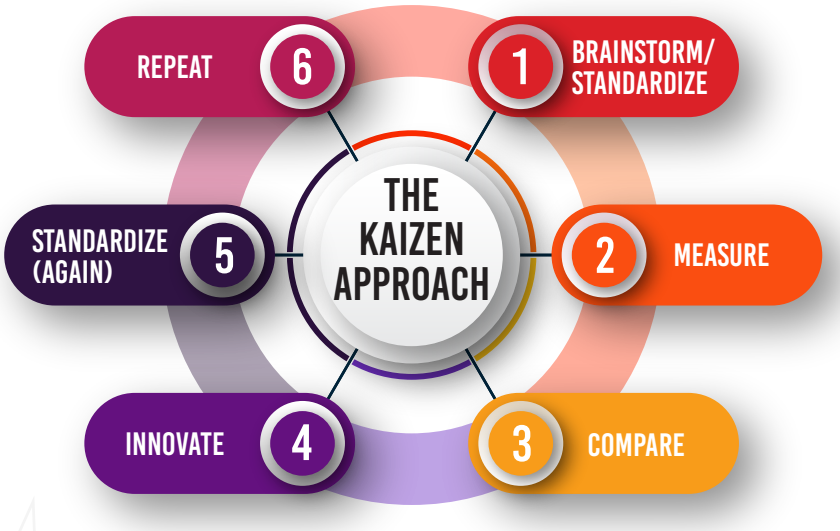
One of the most talked about and utilized services of Payatu is it becoming an MSSP for its clients.

In this role, Payatu steps into the shoes of the protector against a variety of security threats, by constructing a foundation that has experts on it throughout, to oversee and inspect activities that can impose any kind of menace to the organization.

Followed here is something on the lines of Kaizen – continuous improvement.

As an MSSP, Payatu takes on the responsibility of monitoring the organization's everyday tasks for any malicious activity and consistently improving the security posture of its client.

The MSSP, Payatu makes it a point to follow in the steps of -



The umbrella of services that are covered by the MSSP are -

1. SOC

With the aim of detecting, analyzing, and responding to the cybersecurity incidents happening in an organization, the SOC team utilized a garnished combination of technology solutions and a robust set of strategies and processes.

SOC monitors and analyzes activities on servers, networks, endpoints, applications, websites, databases, and other systems for malicious activity that can hint at a compromise or a security breach.

Under SOC, Payatu was able to establish certain success criteria -

1. All operational-infrastructure devices (mobiles, laptops, AWS Servers – whenever applicable) logging data to CrowdStrike
2. Salesforce application logging data to Splunk
3. Honeypots deployment and alert setup On-Prem and AWS infrastructure
4. AWS devices / application logging data to Splunk
5. 24x7 availability of staff to respond to emergencies
6. Proactive monitoring (automatically and manually) of logged data

These criteria helped the service provider in establishing a standard for techniques and parameters for identifying and mitigating risks.

2. Policy Validation

Organizations are supposed to have certain security policies in place that act as the basic guidelines for the operations of the company and what to do in case of any discrepancies that may pave the way for a security breach.

Once the policies are drafted and formulated, it can be a critical task to get through any constraints. Hence, it is highly imperative to validate such policies at the point when being decisive enables the mitigation of any non-compliance scenarios.

Under policy validation, Payatu was responsible for verifying the operational process of the company keeping in mind the formulated policies with the intention of making them more applicable and secure.

With an increase in the governmental regulation status as well as the number of breaches across domains, policy validation is a necessity and not an option.

Thus, the client asked Payatu to validate its security policies and ensure maximum efficiency and fruitful functionality.

Under policy validation, Payatu was able to establish certain success criteria -

- Each policy is validated via technical checks
- Identify any gaps in the policies and procedures
- Initiate policy revision after the gap analysis
- Documentation done in detail for each validation point / check

These criteria helped the client in significantly developing its IT structure by eliminating any foreseeable shortcomings. It instills a sense of confidence in the company as well as its customers by elevating its cyber and IT hygiene.

3. Backup & Restoration Testing

Data, today, has become one of the most significant assets any company can possess. The dynamic and ever-growing nature of this asset makes it highly prone to fall prey to several types of attackers and cyber criminals. Keeping in mind digital transformation and an increase in the amount of data, backup and restoration must be performed in a timely and consistent fashion.

Data that is not backed up and has not been set for restoration can lead to catastrophic losses.

According to the National Archives & Records Administration in Washington, 93% of companies that lost their data center for 10 days (about 1 and a half weeks) or more due to a disaster, filed for bankruptcy within one year of the disaster.

Being a leading fintech, this client of Payatu set its mind to protect all its data and information resources by having Payatu take the lead in creating and organizing its backup and restoration processes.

Under this project, Payatu ensured that its client had a proper backup policy that is designed after thorough testing of how to create a backup that would best suit the client, what should be the backup schedule, and what are the restoration practices in case of any emergencies.

Payatu made sure that all these things are well-documented along with the testing in motion. What was done here is that the Bandits ran multiple tests and asked the client to try restoring from a particular backup. The client was asked to perform a particular test case to ensure that the backups are in proper order and synchronization, making it a smooth process in case of emergencies.

Multiple systems of the client were targeted for backup and restoration, including but not limited to, the client's infrastructure and almost all the critical systems.

The success parameters for this project were -

1 **Backups validated against policy for:**

1. Operational Infrastructure
2. Web Application
3. SF Application (including full system restore done and functionally checked to ensure DRP compliance)
4. AWS/Azure infrastructure
5. O365 suite
6. Mobile devices

2 **Confluence pages created for backup progress tracking and test cases**

These criteria helped the client in safeguarding its sensitive information and keeping a strategy ready to cope with any kind of disaster.

4. DevSecOps

Following the practice of consistency, DevSecOps is an approach that integrates security as a shared responsibility, starting from the initiation of the development process, and continuing throughout the entire IT lifecycle.

Development, security, operations – DevSecOps requires the security teams to think on the lines of application and infrastructure security from the very beginning.

The client here had two major applications that came under the purview of DevSecOps

- The company's Salesforce application
- The company's proprietary application (under development)

Payatu created a set of policies and tools that contained a detailed list of applications that the client can use for implementing DevSecOps and how to implement them in the most efficient manner.

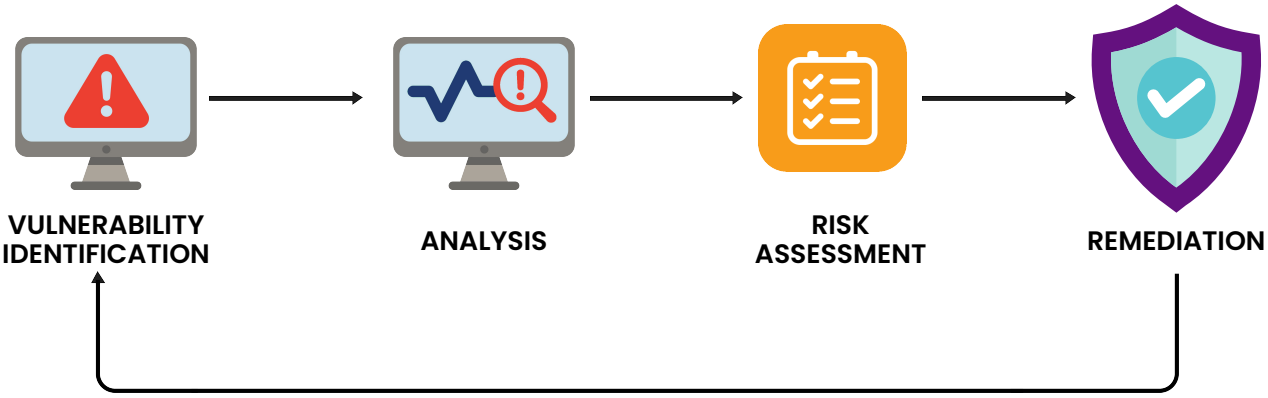
To finalize the best set of practices there was a considerable evaluation and integration of suggestions.

Under DevSecOps, Payatu was able to establish certain success criteria:

1. Security testing embedded into build/deployment process
2. Monitoring and alerting embedded into the DevOps pipeline
3. Vulnerability management solution embedded into the DevOps pipeline

These criteria played a crucial role in formulating the most effective DevSecOps plan for the client.

5. Vulnerability Assessment



Conducting a systematic review of the weaknesses in terms of security across the IT infrastructure of an organization is known as vulnerability assessment.

Investigating a broad array of probable causes and related issues across multiple networks and systems within the IT environment is a notion deeply integrated into vulnerability assessment.

Modern-day organizations understand the gravity of losses that can come with security threats if associated vulnerabilities are not found and mitigated in time. It is now significantly critical to ensure that not just identification, but also classification and prioritization of vulnerabilities is done in the most efficient manner.

For this client, Payatu mainly focused on running scans on websites, internal networks, and public-facing assets and services.

Activities conducted to get the most out of these assessments were -

Under Vulnerability Assessment, Payatu was able to establish certain success criteria -

1. Vulnerability assessment performed weekly
2. Resolving all the identified vulnerabilities
3. Ensuring we keep the systems to be scanned list up to date

With the help of these activities and criteria, the client was able to keep its networks, digital assets, and its IT ecosystem intact and safe, which is all part of a much broader threat mitigation strategy.

6. Cyber Threat Intelligence (CTI)

Understanding and identifying existing and emerging threats in an organization is one of the best ways to prevent a grave attack.

In times like these, when data is a powerful weapon and a high-value asset altogether, intelligent tools that can offer evidence-based information should be the go-to resources for making informed decisions.

Cyber Threat Intelligence is the approach of using automation to analyze data in order to deliver context of the threats.

This helps organizations in producing action-oriented advice to be proactive in fighting these threat actors.

Payatu utilized such tools to detect any possible attacks that can happen or have happened in the company. The team scanned through multiple forums to spot any stolen data or anything that is attributed to or belongs to the client.

When it comes to CTI, the Bandits browse through a number of data leaks that have taken place in the previous weeks, evaluate user accounts of the client, and identify all the ways that can be useful in mitigating any threat activities.

The success criteria for Cyber Threat Intelligence were -

1. Proactive search for management team data in leaked datasets
2. Detect Password spraying attacks against public accounts
3. Identify breached usernames
4. Spot all the publicly scrapped information related to the client

With the help of these activities and criteria, Payatu stepped on the pedal of proactiveness in securing its client in all ways possible.

7. Proprietary Application Security Review

This was the client's proprietary application that was hosted on the Azure environment.

The Payatu team was asked to conduct a security assessment for the application infrastructure.

This activity required the team to go through the application in a very granular manner to identify any issues, develop a report, compile it, and share it with the client.

The success criteria established for the application security review of this proprietary application were-

These criteria played a vital role in protecting the proprietary application of the client.

Present Day Scenario

Payatu is still the MSSP for this fintech leader and strives diligently towards protecting its infrastructure every single day.

The client is not just happy but also delighted with the work that the Bandits are doing to create a secure environment and make cybersecurity omnipresent in this organization.

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.

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.

Payatu

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.

More Services Offered by Payatu

- IoT Security Testing
- AI/ML Security Audit
- DevSecOps Consulting
- Critical Infrastructure
- Trainings

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com
info@payatu.com
+91 20 41207726