



Payatu Case Study

A Fintech Frontier Entrusts Payatu's Precision in SOC Services

Project Overview

Given the current cyber atmosphere, a top audit recovery services and source-to-pay automation provider decided to undergo the process of strengthening its security posture.

Being a fintech company, it is important that the digital infrastructure of the organization is safeguarded. Fintech companies have a lot of sensitive customer data, which needs to be protected at all costs. And the first step to safeguard anything is to identify the gaps.

When Payatu was approached by the client to help it with its cybersecurity practices, the team quickly understood what the best service for this client would be. The answer was Security Operations Center – SOC!

SOC is a function of cybersecurity that is responsible for monitoring, preventing, detecting, investigating, and responding to cyber threats 24x7. Because there is round-the-clock monitoring and detection, catching cyber threats in their tracks becomes faster.

Thus began the process of setting up and utilizing a Security Operations Center for this fintech client.

The Scope

Set up a SOC ensuring that the client receives:



24*7 Monitoring Support



Ticketing



Reporting



Response

- Weekly Advisory (Blocking/unblocking)
- Daily updates for Emergency alerts



Actions Implemented

Monitoring and Analysis of everything under scope.

1. Email Archiving Platform

This platform is a powerful email archiver and compliance solution for mail systems. It has an easy-to-use query builder and uses powerful query language to find emails with ease.

What is monitored?



Bruteforce login



Login from a foreign country



Persistence using adding groups, users



New packages installed



Defense Services stopped



Audit Logs ingestion pipeline monitoring



New service created

2. SFTP Servers

SFTP is a network protocol for securely accessing, transferring and managing large files and sensitive data.

What is monitored?



Bruteforce Login



Login from a foreign country



Persistence using adding groups, users



New packages installed



Defense Services stopped



Audit Logs ingestion pipeline monitoring



New service created



Sudo commands executed

3. Microsoft Azure AD

Microsoft Azure AD is a cloud identity and access management solution that connects employees, customers, and partners to their apps, devices, and data.

What is monitored?



Privilege role assigned



PowerShell activity



Malicious links clicked



Forward rule creation



OAuth application added for authentication



Impossible travel activity



New resources, subscriptions, VM creation



DLP alerts

4. Azure Virtual Desktop

Azure Virtual Desktop is a Microsoft Azure-based system for virtualizing its Windows operating systems, providing virtualized desktops and applications securely in the cloud using the Remote Desktop Protocol.

What is monitored?



Login from outside the country

5. Microsoft 365

Microsoft 365 is a product family of productivity software, collaboration and cloud-based services.

What is monitored?



Data exfiltration using secure link, downloading files, anonymous links in SharePoint and OneDrive



User anomalous behavior



User added



Device added



OneDrive and SharePoint files accessed outside the country



Single-factor login



Bruteforce monitoring



Same IP used by multiple users



User account login failed



Successful logins outside the country

6. Cloud Data Platform

This platform, hosted in the cloud, enables organizations to store and analyze substantial amounts of data efficiently and economically.

What is monitored?



New user, user role created



User role assigned



Successful login outside the country



Same IP used by multiple users



Failed login

7. AzureDevOps

Azure DevOps is a Microsoft product that provides version control, reporting, requirements management, project management, automated builds, testing and release management capabilities.

What is monitored?



Actions from outside the country



Audit stream activity



Repository creation

8. Project and Work Management Platform

This platform in the cloud enables users to develop their own applications and project management software.

What is monitored?



Deleted board



User created

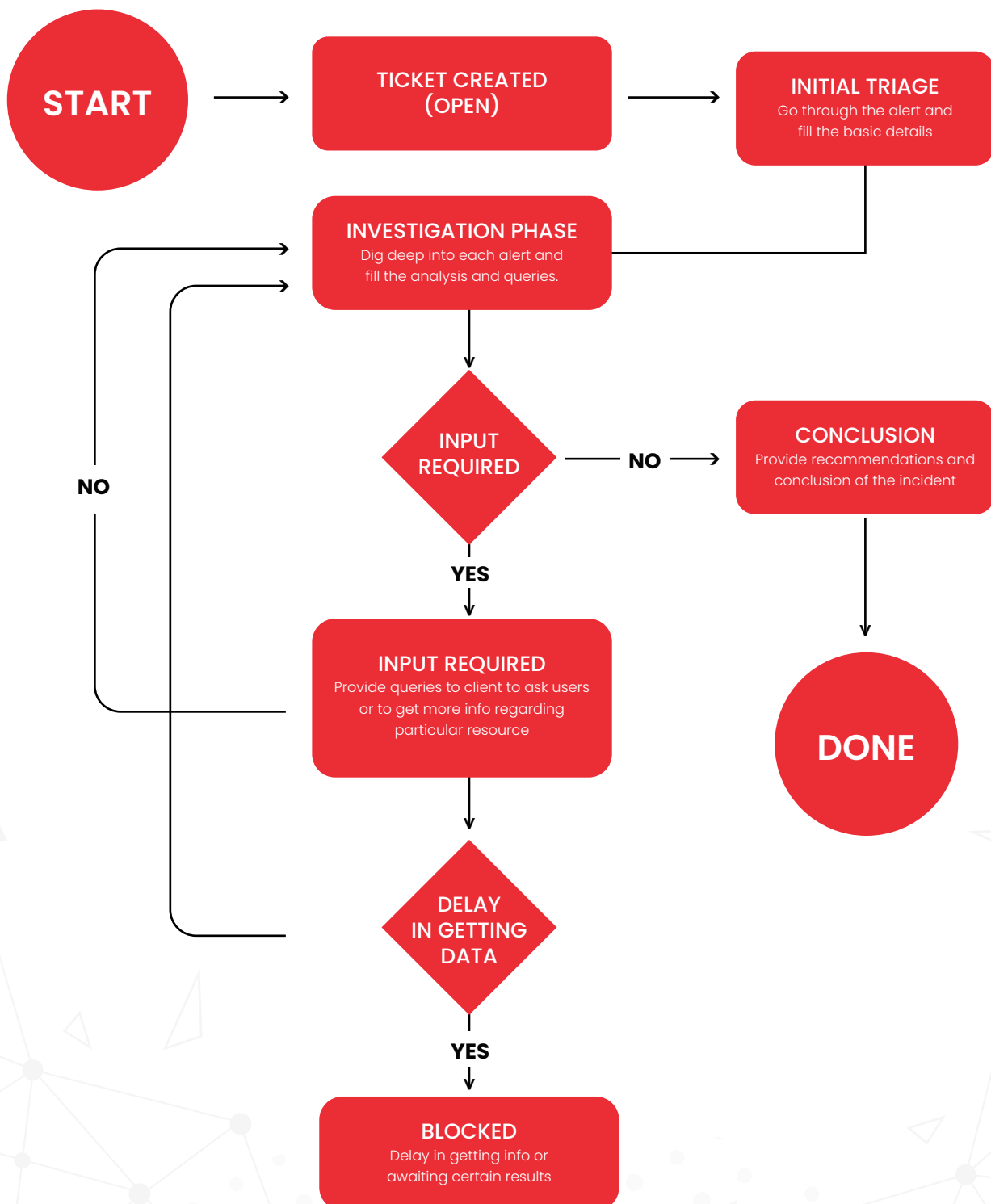


Download activity by user



Login from outside the country

Workflow as per Agreement



The SOC Team Goes an Extra Mile

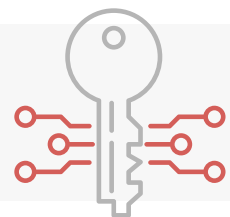
The Bandits in the SOC team provide regular recommendations based on the threat's trends -

Address the identified gaps in the Email Security policies by implementing the suggested improvements outlined.



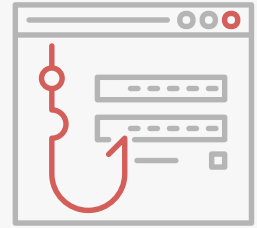
It's advisable to establish a network diagram to identify unmanaged devices within your system.

Consider developing robust Conditional Access policies specifically tailored for Entra ID to enhance security measures effectively.



It is strongly advised to enforce Multi-Factor Authentication (MFA) across all applications, including the project management platform and Entra ID, to bolster authentication security.

Educate users on recognizing and reporting phishing emails is crucial. It is suggested to provide comprehensive training on identifying phishing attempts and establish protocols for reporting suspicious emails after analyzing user interaction.



Regularly review user accounts to identify any inactive or departed employees and promptly remove or disable their accounts to maintain security hygiene.

Establish a security baseline as a fundamental framework for security measures to ensure consistency and effectiveness across your organization.



Developing clear and efficient security processes for reporting, alerting, and responding to security incidents is imperative. This will streamline incident management and enhance your overall security posture.

Before and After

BEFORE

❗ There was no established security baseline.

❗ There were no network diagrams, and devices were unidentified and unmanaged.

❗ Exchange and email policies were improperly configured.

❗ There were no Standard Operating Procedures (SOP) for incidents and alerts.

❗ There were no weekly reports for the SOC and security.

AFTER

✅ A proper baseline has been established and is continuously updated.

✅ A SOC Network Diagram has been created, and assistance is provided to the team in building the network diagram. Additionally, new hosts and devices that were previously not under monitoring are being identified.

✅ Exchange and email policies have been audited to identify gaps, resulting in a reduction in spam and phishing emails.

✅ Standard Operating Procedures (SOP) have been developed for handling incidents and alerts.

✅ Weekly reports are now generated for the management and team regarding SOC and security matters.

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.



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.



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 Security Consulting Pvt. Ltd.

 www.payatu.com

 info@payatu.com

 +91 20 41207726

