Payatu

Payatu Casestudy

A Renowned Fintech Company Gets SOC Expertise Onboard

Payatu Security Consulting Pvt. Ltd.

Project Overview

Fintech cyberattacks are not just an impact on money, but also a massive blow to the thin trust of customers and breach of compliance standards.

This well-recognized Australian fintech understood the criticality of being in the fintech arena and its responsibility toward its customers' data. The company came to Payatu with a clear mindset of monitoring, protecting, detecting, investigating, and responding to cyber threats, if any, around the clock.

Leveraging the expertise of its SOC professionals, Payatu armored up to monitor and protect the client's assets that consisted of personnel data, customer data, business systems, intellectual property, and brand integrity.

For the Payatu SOC team, it was important to get a complete overview of the client's threat landscape including various endpoints, software, and servers along with third-party services and traffic flowing between all the devices.

The team designed a detailed plan and carried it out meticulously.

The Scope

The scope of the project comprised of round-the-clock monitoring of -

1. Devices allotted to employees such as mobile and laptops
2. Applications installed on all devices
3. Device activities such as login from an unexpected user agent, IP, application, etc.
4. Cloud services such as Azure and AWS
5. In Azure, monitoring of Outlook, One Drive, and audit logs services to detect, and respond to phishing and bruteforce
6. Access of files shared outside the client's organization
7. All operational-infrastructure devices (mobiles, laptops, AWS Servers – whenever applicable) logging data to CrowdStrike
8. Salesforce, Fortinet, Sentinel, O365
9. AWS devices / application logging data to Splunk
10. Proactive monitoring (automatically and manually) of logged data
11. WordPress sites logging data to Splunk
12. Honeypots deployment and alert setup on the client's on-prem and AWS infrastructure
13. 24x7 availability of staff to respond to emergencies
14. Alerts investigated and closed within SLAs

CHALLENGES

01 No existing SOC infrastructure meant everything needed to be developed from scratch

02 Each element in the scope required a different setup, this led to a drastic increase in the overall scope of the project

03 Limited time to get the setup done proved to be a constraint

04 Regulations on permissions

Actions Implemented

Services and Infrastructure Monitored

AZURE SENTINEL

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.

WHAT IS MONITORED?

01 The suspicious activity of any user

02 Phishing mails alerts

03 Malware in Azure environment

04 High usage of Microsoft apps

05 Unfamiliar login location

06 New OAuth Application attached to an account

07 Scanning activity on client websites

AWS CLOUDTRAIL

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account.

Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.

WHAT IS MONITORED?

01 Virtual Machines Activity

02 IAM & Root User logins

03 New Account creation

04 Cost Factor of AWS S3 Bucket access

05 S3 Bucket activities

06 Source & Destination of Activities and API Calls

07 Roles and Users access the secret manager

08 Error codes & Events

SALESFORCE

Salesforce is a popular CRM tool for support, sales, and marketing teams worldwide. Salesforce services allow businesses to use cloud technology to better connect with partners, customers, and potential customers.

WHAT IS MONITORED?

01 Browser login history

02 Logins by geography

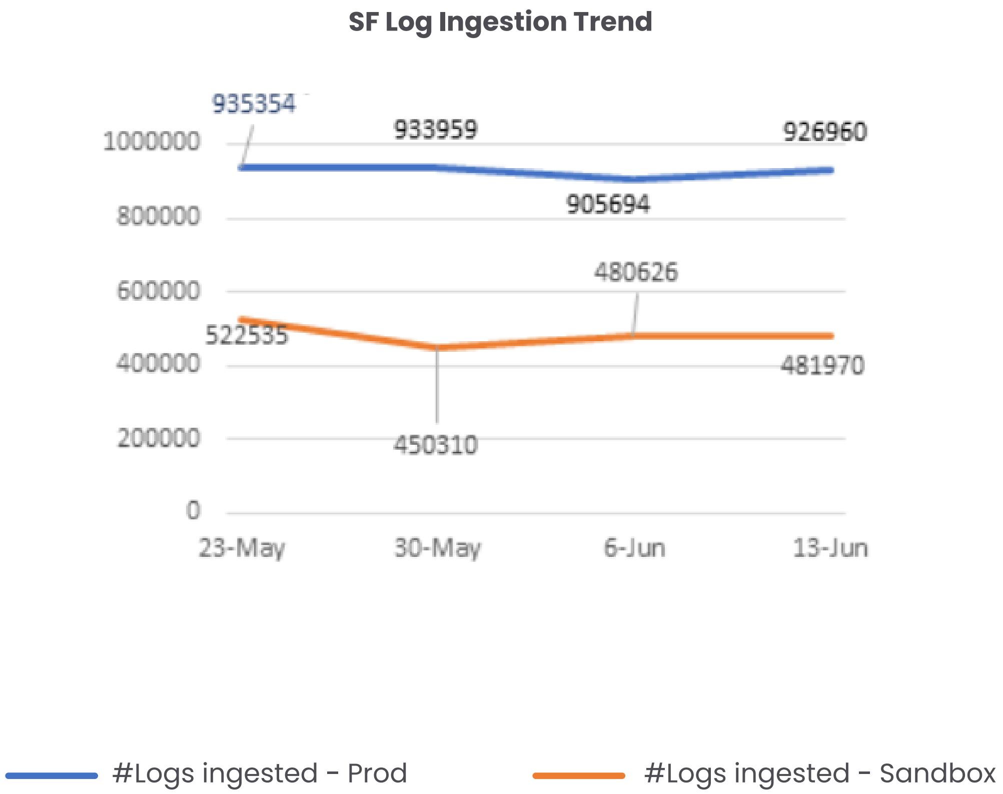
03 Most active users & IPs

04 Browser & Platform used

05 Account Lockouts Source IPs

AVERAGE WEEKLY SALESFORCE MONITORING STATISTICS

- Salesforce Prod logs entries monitored – **926,960**
- Salesforce Sandbox logs entries monitored – **481,970**



MICROSOFT OFFICE 365

Microsoft Office 365 is a modern collaboration platform that provides a full-featured email system with web access, integrated calendaring, a campus contacts directory, support for mobile device access, email storage, and document storage.

WHAT IS MONITORED?

01 Management Activity

02 Service Health & Communications

03 Mailbox

04 Office 365

05 One Drive

06 SharePoint

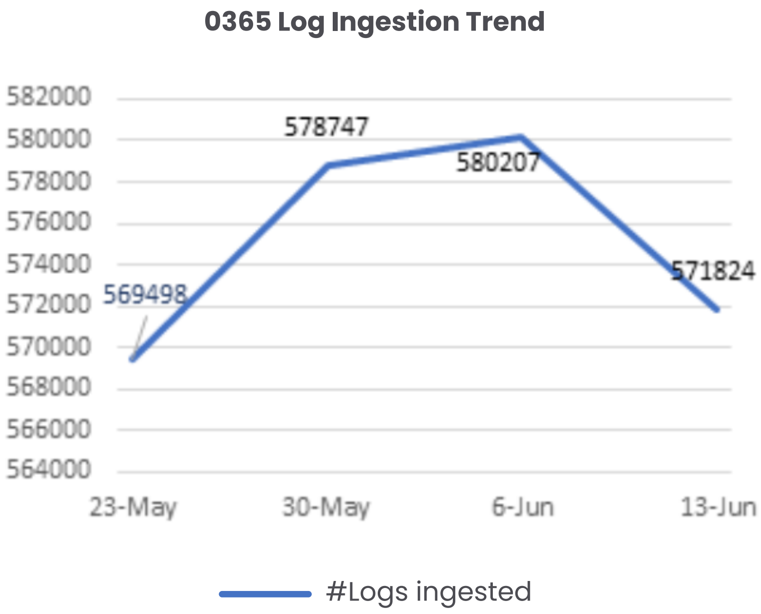
07 Audit Logs

08 Teams

AVERAGE WEEKLY 0365 MONITORING STATISTICS

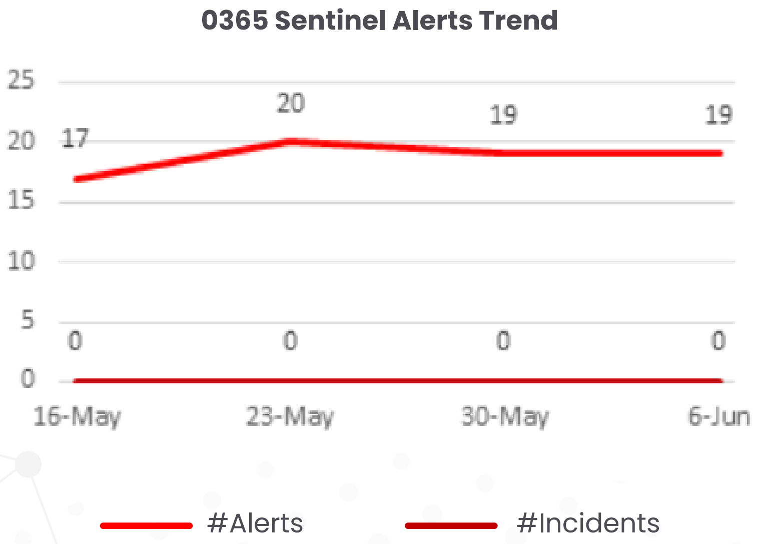
0365 logs monitored - **571,824**

- **Logins from AUS – 23,069**
- **Logins outside AUS – 3,766**



ALERT DETAILS

- Alerts triggered - 19
- Alerts investigated -19



FORTINET

FortiGate NGFWs deliver industry-leading enterprise security for any edge at any scale with full visibility and threat protection. Organizations can weave security deep into the hybrid IT architecture and build security-driven networks to achieve:

01 Ultra-fast security, end to end

02 Consistent real-time defense with FortiGuard services

03 Excellent user experience with security processing units

04 Operational efficiency and automated workflows

WHAT IS MONITORED?

01 The Traffic

- 01 Source & Destination IPs
- 02 Applications generating traffic
- 03 Protocols

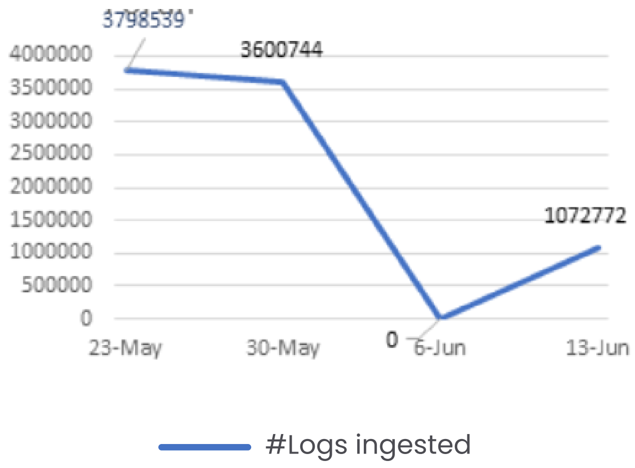
02 Threats identified by Fortinet

03 Devices connected to the Fortinet

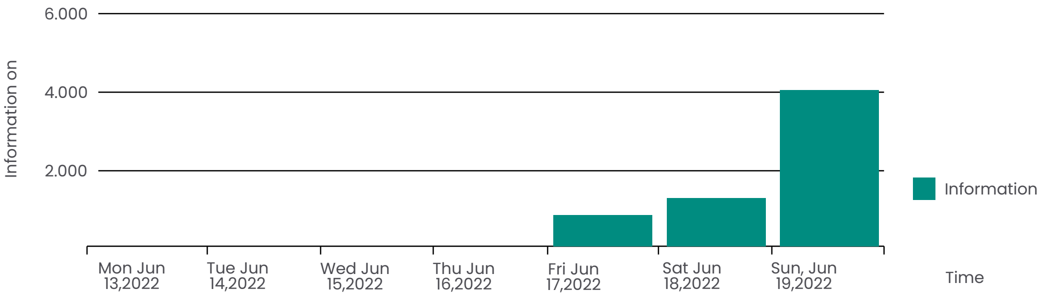
AVERAGE WEEKLY FORTINET MONITORING STATISTICS

1,072,772 Fortinet - logs monitored

Fortinet Log Ingestion Trend



Fortinet Threat By Severity



CROWDSTRIKE

CrowdStrike is a global cybersecurity leader with an advanced cloud-native platform for protecting endpoints, cloud workloads, identities, and data.

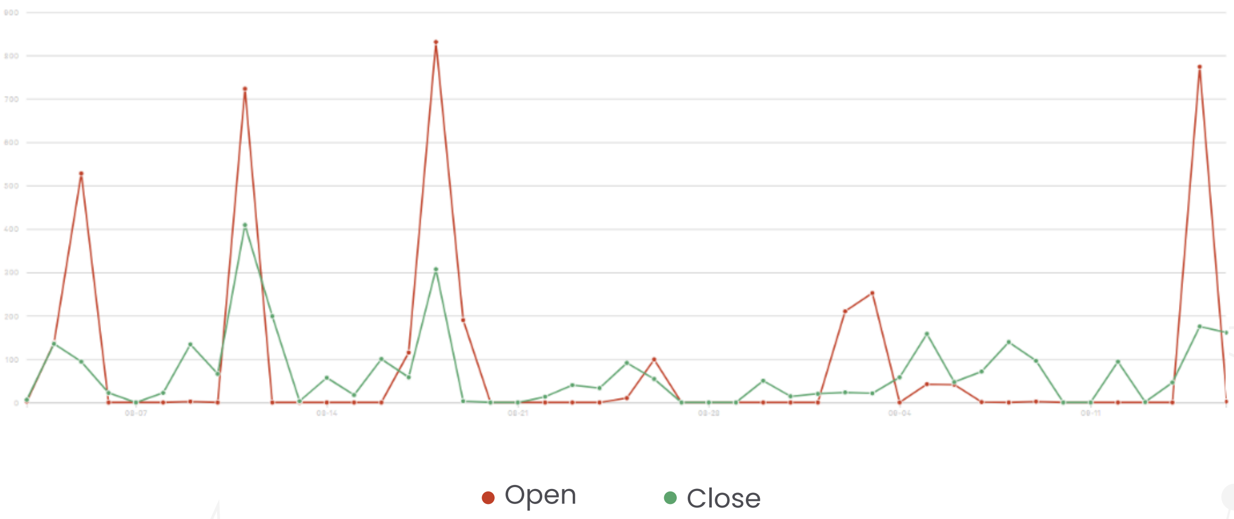
WHAT IS MONITORED?

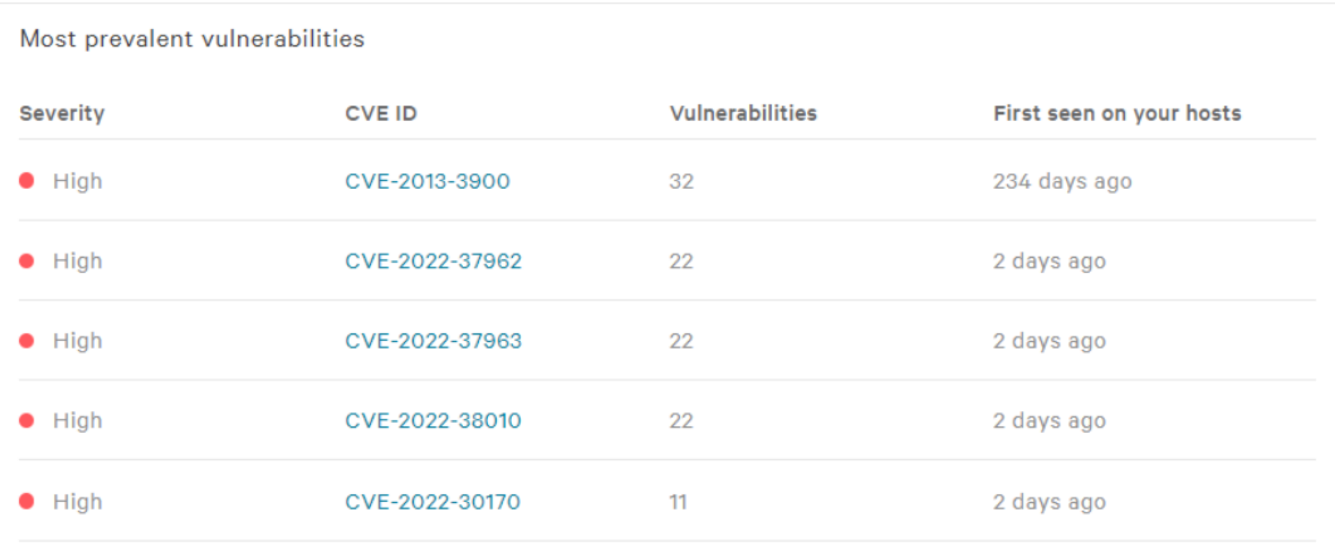
01 Mobiles: Monitoring apps installed, checking for the outdated software's, checks to latest CVEs

02 Laptops: Complete EDR prevention policy applied. Ex: checks the executed scripts, installed apps, defense evasion. Checks for the latest CVEs & outdated apps.

03 Servers [Cloud PC]: Same as laptops

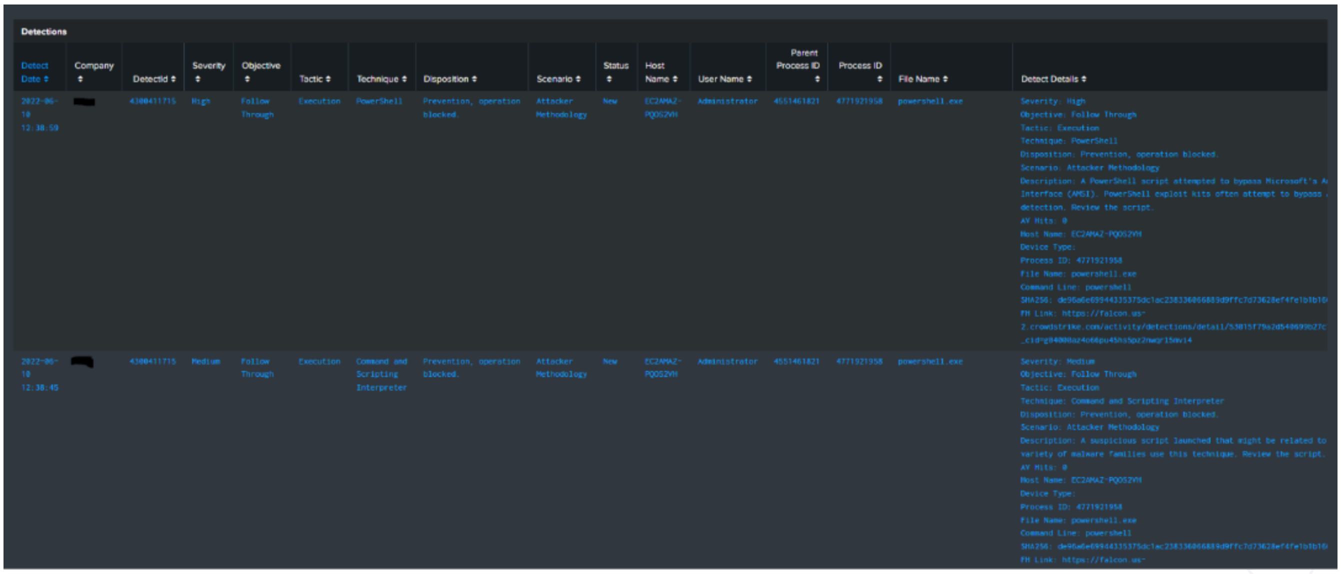
Open and closed vulnerabilities by day (last 45 days)





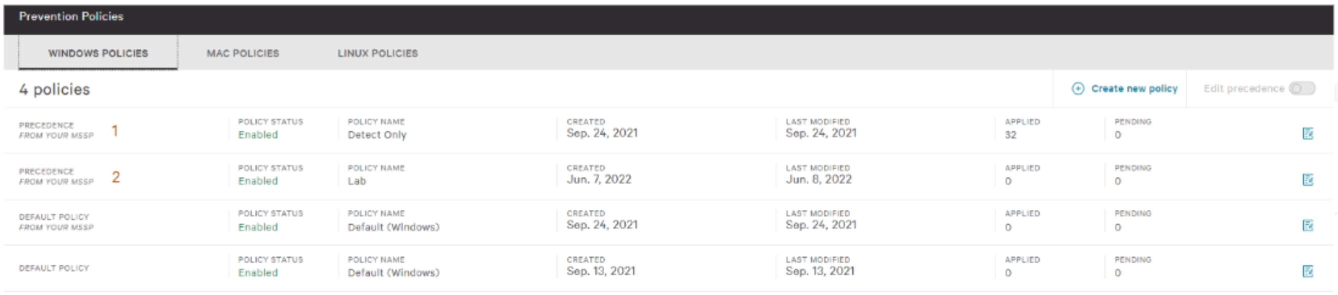
Most prevalent vulnerabilities

Severity	CVE ID	Vulnerabilities	First seen on your hosts
● High	CVE-2013-3900	32	234 days ago
● High	CVE-2022-37962	22	2 days ago
● High	CVE-2022-37963	22	2 days ago
● High	CVE-2022-38010	22	2 days ago
● High	CVE-2022-30170	11	2 days ago



Detections

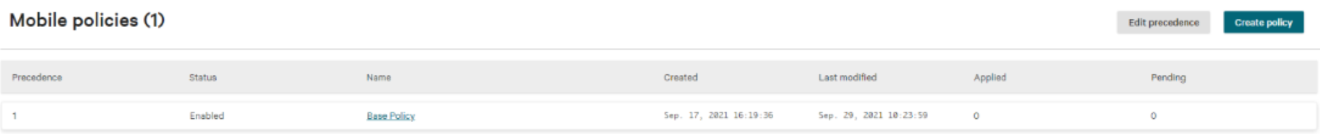
Detect Date ⇕	Company ⇕	DetectId ⇕	Severity ⇕	Objective ⇕	Tactic ⇕	Technique ⇕	Disposition ⇕	Scenario ⇕	Status ⇕	Host Name ⇕	User Name ⇕	Parent Process ID ⇕	Process ID ⇕	File Name ⇕	Detect Details ⇕
2022-06-10 12:38:50	[redacted]	4300411715	High	Follow Through	Execution	PowerShell	Prevention, operation blocked.	Attacker Methodology	New	EC2AMAZ-PQOS2VH	Administrator	4551461821	4771921958	powershell.exe	Severity: High Objective: Follow Through Tactic: Execution Technique: PowerShell Disposition: Prevention, operation blocked. Scenario: Attacker Methodology Description: A PowerShell script attempted to bypass Microsoft's A Interface (AMSI). PowerShell exploit kits often attempt to bypass detection. Review the script. AV Hits: 0 Host Name: EC2AMAZ-PQOS2VH Device Type: Process ID: 4771921958 File Name: powershell.exe Command Line: powershell SHA256: de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b16 FH Link: https://falcon.us- 2.crowdstrike.com/activity/detections/detail/53015f79a2d548699b27c _cid=g84000az4o66pu45hs5pz2nwgr15mv14
2022-06-10 12:38:45	[redacted]	4300411715	Medium	Follow Through	Execution	Command and Scripting Interpreter	Prevention, operation blocked.	Attacker Methodology	New	EC2AMAZ-PQOS2VH	Administrator	4551461821	4771921958	powershell.exe	Severity: Medium Objective: Follow Through Tactic: Execution Technique: Command and Scripting Interpreter Disposition: Prevention, operation blocked. Scenario: Attacker Methodology Description: A suspicious script launched that might be related to variety of malware families use this technique. Review the script. AV Hits: 0 Host Name: EC2AMAZ-PQOS2VH Device Type: Process ID: 4771921958 File Name: powershell.exe Command Line: powershell SHA256: de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b16 FH Link: https://falcon.us-



Prevention Policies

4 policies

	POLICY STATUS	POLICY NAME	CREATED	LAST MODIFIED	APPLIED	PENDING
PRECEDENCE *FROM YOUR MSSP* 1	Enabled	Detect Only	Sep. 24, 2021	Sep. 24, 2021	32	0
PRECEDENCE *FROM YOUR MSSP* 2	Enabled	Lab	Jun. 7, 2022	Jun. 8, 2022	0	0
DEFAULT POLICY *FROM YOUR MSSP*	Enabled	Default (Windows)	Sep. 24, 2021	Sep. 24, 2021	0	0
DEFAULT POLICY	Enabled	Default (Windows)	Sep. 13, 2021	Sep. 13, 2021	0	0



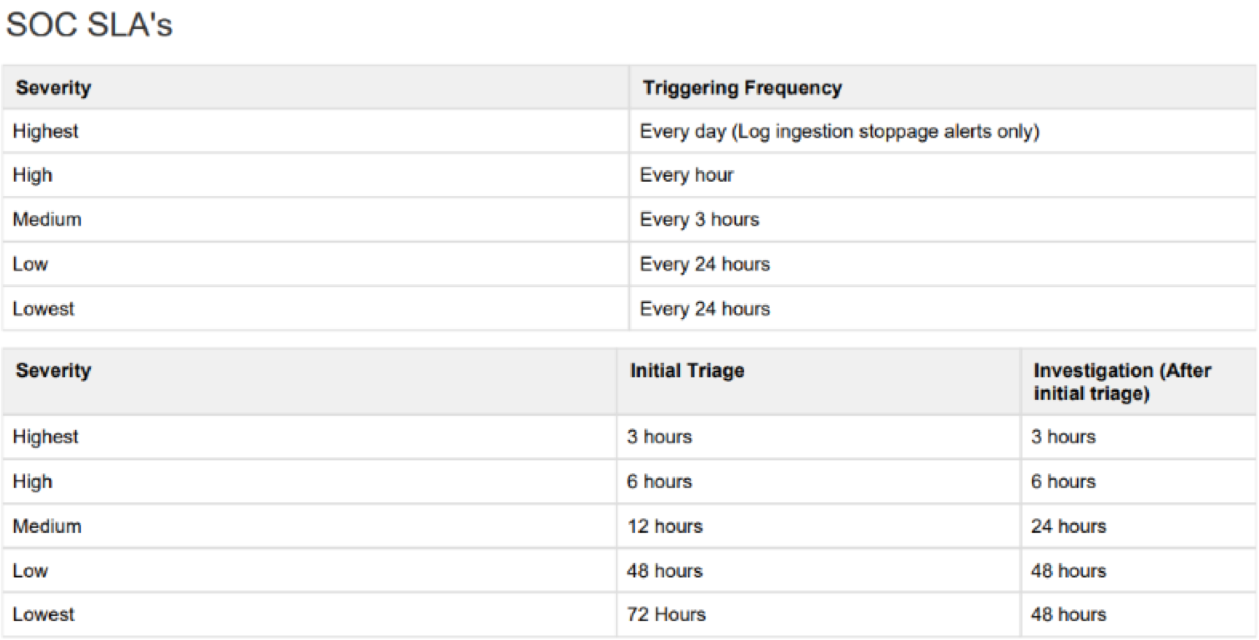
Mobile policies (1)

Precedence	Status	Name	Created	Last modified	Applied	Pending
1	Enabled	Base Policy	Sep. 17, 2021 16:19:36	Sep. 29, 2021 10:23:59	0	0

TICKETING SYSTEM

Jira is a Project Management Software for Bug Tracking and Agile Project Management. Since it supports languages like English, French, German, Japanese, and Spanish, Jira is a multilingual tool.

EXECUTION OF ALL SLAs

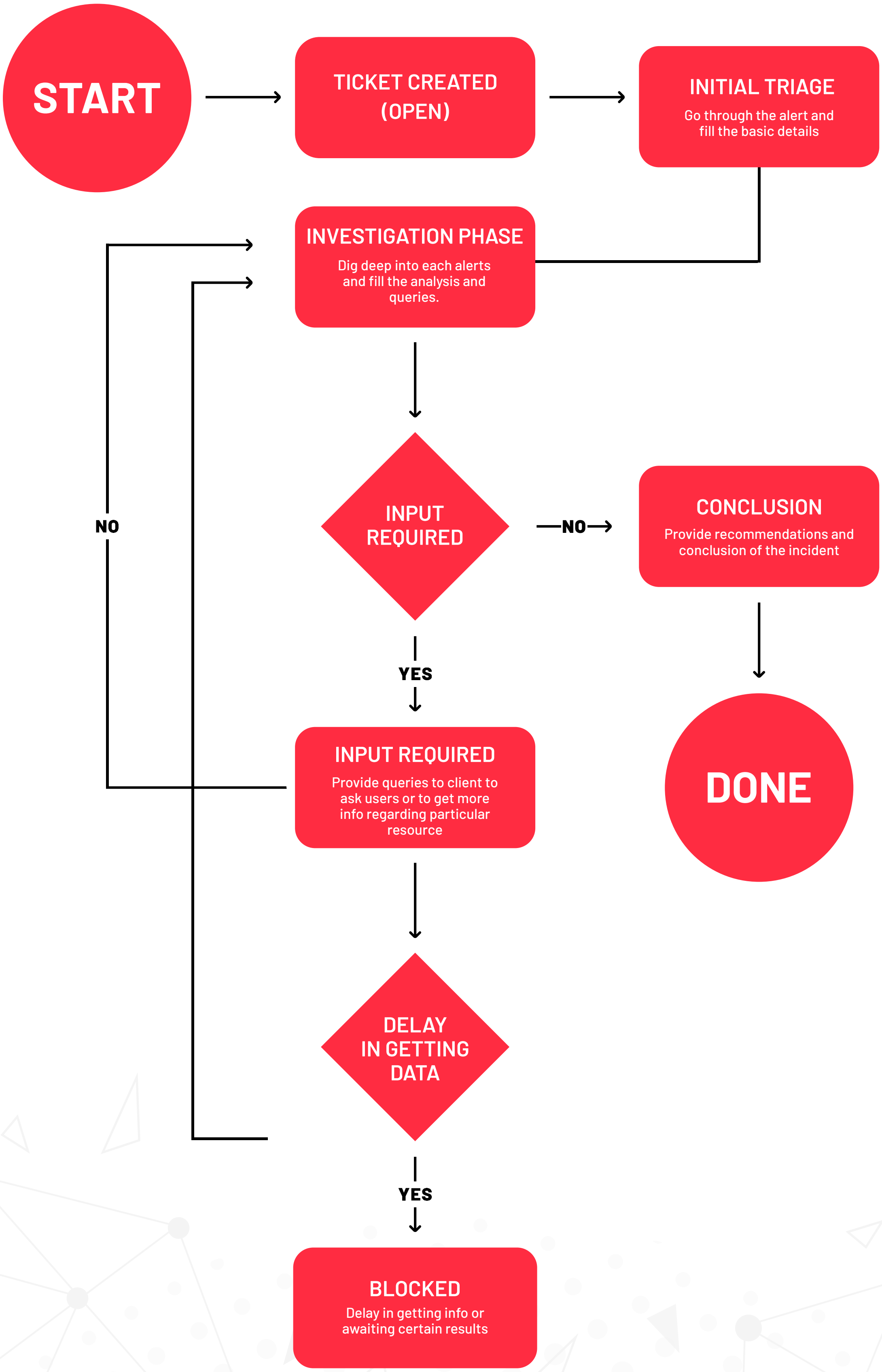


SOC SLA's

Severity	Triggering Frequency
Highest	Every day (Log ingestion stoppage alerts only)
High	Every hour
Medium	Every 3 hours
Low	Every 24 hours
Lowest	Every 24 hours

Severity	Initial Triage	Investigation (After initial triage)
Highest	3 hours	3 hours
High	6 hours	6 hours
Medium	12 hours	24 hours
Low	48 hours	48 hours
Lowest	72 Hours	48 hours

WORKFLOW EXECUTION AS PER AGREEMENT



START

TICKET CREATED (OPEN)

INITIAL TRIAGE

Go through the alert and fill the basic details

INVESTIGATION PHASE

Dig deep into each alerts and fill the analysis and queries.

INPUT REQUIRED

CONCLUSION

Provide recommendations and conclusion of the incident

DONE

INPUT REQUIRED

Provide queries to client to ask users or to get more info regarding particular resource

DELAY IN GETTING DATA

BLOCKED

Delay in getting info or awaiting certain results

The SOC Team Goes an Extra Mile

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

- They shared a detailed report about the latest CVE exploiting in the wild and how to secure from it and a result of analysis in client environment. [E.g., sharing of the Follina report by the Payatu team]
- They shared the defense techniques so that client will be safe from threat actors. [E.g., how to keep users safe from malware delivered by ISO, known USB devices block, blocking the Powershell scripts/ restricting access to cmd & Powershell, etc.]

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.

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 🔗