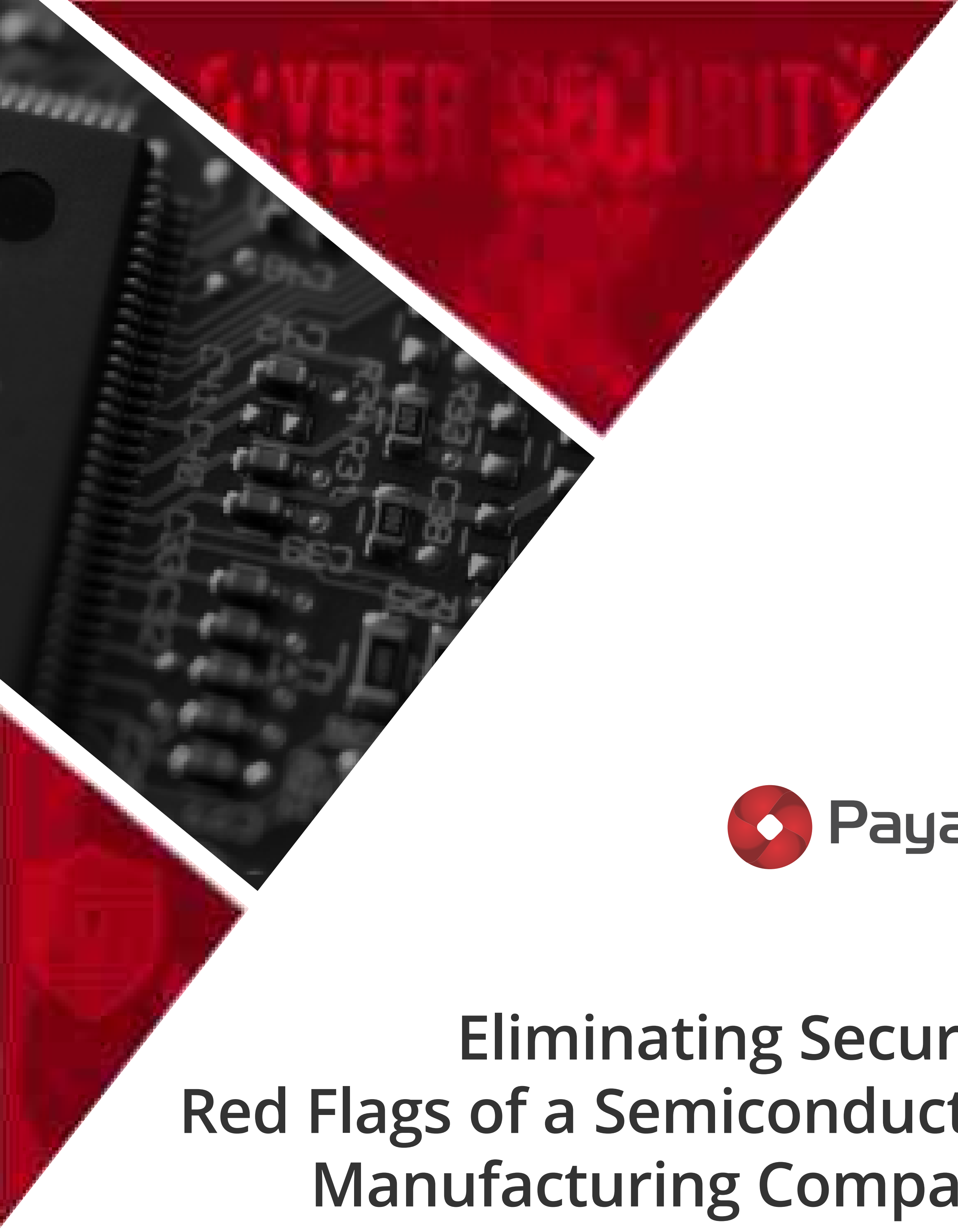


Payatu

# Eliminating Security Red Flags of a Semiconductor Manufacturing Company

Payatu Casestudy

# Table of Content

# Project Overview

The client is a semiconductor manufacturer and a sister concern of one of our most prestigious and returning customers. Payatu was pleased to have this client onboard for red team assessment and made it a point to deliver beyond what was expected.

The current world problems extend far and wide, where cybersecurity concerns are some of the most pressing issues of all times. Hence, to secure the infrastructure of its organization, Payatu's client wanted to conduct a red team assessment to identify and analyze the gaps and the gravity thereof.

# The Scope

To conduct a red team assessment of the entire infrastructure of the organization in tasks such as

**Replicating the type of attacks that could be initiated from the Internet on the client's infrastructure and applications including but not limited to**

1. Web Servers and/or Applications
2. Mobile Application
3. Network
4. Servers
5. Cloud Assets

**To identify vulnerabilities which can be exploited to**

01 Bypass the security controls implemented

02 Enumerate accounts

03 Gain privileged access to the infrastructure/ network/applications in scope

04 Gain access to internal network

05 Copy/Access data

06 Gain access to emails

**All types of social engineering attacks like phishing, impersonation etc. to extract credentials or other sensitive information from employees.**

# Challenges

These are some of the challenges and roadblocks that were faced by the Payatu team while conducting this assessment

1. Phishing employees in the client's infrastructure
2. Entire infrastructure sitting behind a VPN
3. Entering internal exchange server used by client for exchanging emails
4. Bypassing email filters
5. Lack of concurrent logins
6. Bypassing the antivirus/firewall
7. Bypassing MFA
8. Compromising servers with open RDP in the network
9. Time constraint
10. Performing malware attack on users.

# Process

Knowing how to carry out an activity when there are multiple aspects to a project is an art mastered by the Bandits of Payatu. The process to identify the gaps, infiltrate the system, and compromise the infrastructure was carried out rather sophisticatedly and in the below mentioned steps

01 Enumerating internal network

02 Compromising the internal server

03 Sending phishing emails to the smtp server hosted by the client

04 Logging into the emails of the client

05 Logging to the portals run internally

06 Compromise database server containing user information of the client

07 Exploiting web vulnerabilities identified

08 Accessing credentials of the employees and getting their sessions

09 Malware email campaigns for installation of infected links

10 Identifying the VPN used to get access to the server via social engineering

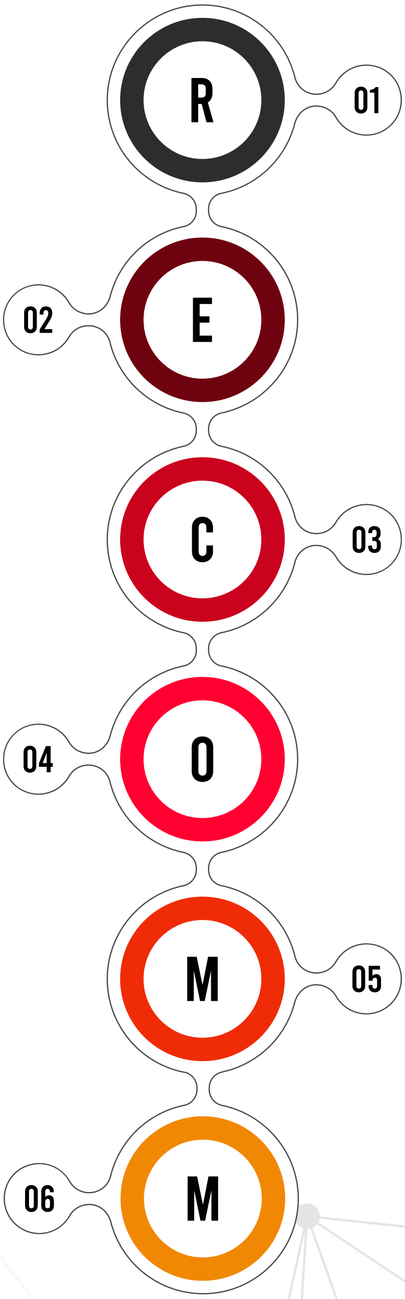
# Findings

The Payatu team found several vulnerabilities, the severity of which varied. They were able to identify these vulnerabilities and make a note of it to report back to client for fixing the same.

1. Web Application Security - SQL injection to gain access to organization's user data
2. Arbitrary file upload to PHP shell access
3. Network Exploitation - SMTP Open relay Server
4. Host Exploitation - Privilege Escalation to root user
5. Social Engineering - Phished the client's users and logged in to Microsoft O365, bypassing MFA
6. Web Application Security – Cross-Site Scripting Reflected in the client's Ecard
7. Web Application Security – Directory Listing Enabled
8. Network Exploitation- Anonymous FTP Login

# Recommendations

Being experts in the field of cybersecurity, the Bandits knew exactly what measures should be taken by the client to fix the issues and vulnerabilities identified. Below is the list of all the recommendations made by the Payatu team -



01 Improvements to the SOC team

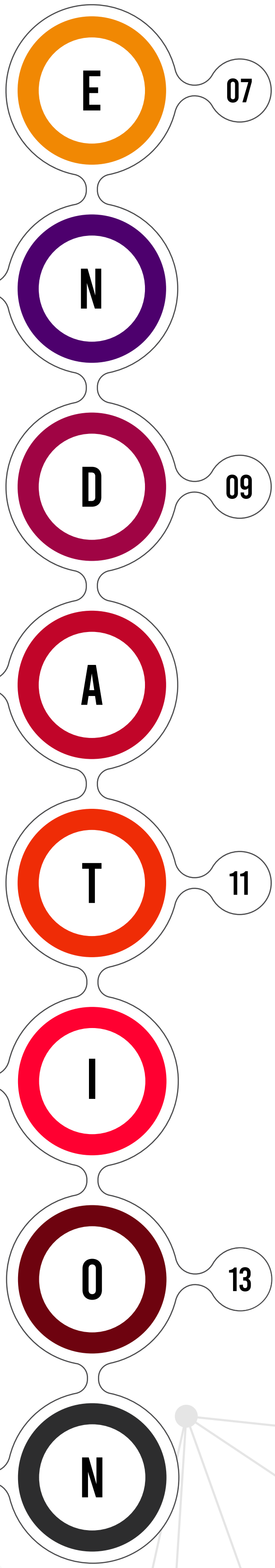
02 Use of parameterized query for mitigating SQL injection attacks

03 Character Escaping to mitigate cross site scripting

04 Securing the external facing web applications

05 The file types allowed to be uploaded should be restricted to only those that are necessary for business functionality

06 The application should perform filtering and content checking on any files which are uploaded to the server.



07 All the control characters and Unicode ones should be removed from the filenames and their extensions without any exception.

08 Use Cross-Site Request Forgery protection methods.

09 Use an anti-malware and scanner on the Linux servers and the servers should be scanned consistently.

10 Implement Azure Conditional Access that blocks MITM servers like Evilginx which can be used to perform a sophisticated phishing attack.

11 Install all the security updates released from the vendor in all systems and servers in the organization.

12 Elevate the amount of red team assessments conducted

13 Provide security awareness training to employees of the organization

14 The organization should perform regular penetration tests of internal and external web applications

# The Takeaway

With the help of Payatu's recommendations, this client of theirs was made aware of its actual security posture and the gaps that needed to be filled by the SOC team. The client was glad to apprehend the fact its external facing application and servers needed to be worked on, in order to make them intrusion-free from any attackers.

The result of all these activities, findings, and quality of output was that the client decided to conduct consistent red team assessments with Payatu. It is a matter of pride for the Payatu Bandits to ensure that each and every client of theirs leaves with utmost satisfaction and an improved security structure.

# 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.

Our deep technical security training and **state-of-the-art** research methodologies and tools ensure the security of our client's assets.

At Payatu, we believe in following one's passion, and with that thought, we have created a world-class team of researchers and executors who are willing to go above and beyond to provide best-in-class security services. We are a passionate bunch of folks working on the latest and cutting-edge security technology.

**Payatu Security Consulting Pvt. Ltd.**

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