

# Ajay PB

Chennai, Tamil Nadu, India

(+91) 97898 19091

[ajaypb1192@gmail.com](mailto:ajaypb1192@gmail.com)

[www.linkedin.com/in/ajaypb](https://www.linkedin.com/in/ajaypb)



## Summary

Experienced Information Security professional with around 9 years of experience in leading the development, operations, and daily management of the various components of Managed Security Services. Expertise in managing network and endpoint security, threat detection, mitigation, and management. Eager to contribute in a senior-level IT security role.

---

## Skills

Security Engineering, Software Development, Network Security, Cloud Security, Endpoint Security, Vulnerability Assessment.

---

## Technical Expertise

Next-gen Firewalls, Site-to-Site & SSL VPN, Security Information and Event Management (SIEM), Log Management (Elastic Stack), Cloud Access Security Broker (CASB), Endpoint security and EDR, Rapid7 Nexpose.

---

## Experience

### Assistant Manager

Tata Communications Limited • Chennai • Tamil Nadu

Role: MSS Engg. - Project Manager

Jan-2019 – Present

- Co-ordinated with the senior management to design business objects dashboards in Single Pane of Glass portal for our Managed Security Services for optimizing security views and developed professional dashboards across Threat Management.
- Performed predictive analysis and ticket reduction evaluations by investigating logs and triggered security events using the elastic stack for analysis.
- Developed and managing multiple security services, dashboards, and in-house automation solutions such as Security, Orchestration, Automation, and Response (SOAR), FortiGate Automated Policy Configuration, and Automated Patch Management.
- Played a major role in enhancing the operations efficacy by strengthening and automating the incident handling and response process and improving the automation efficiency by 80%.
- Maintained effective communications and collaborated across multiple teams and vendor to evaluate, develop, and implement new features/services.

- Collaboratively work with the selected vendor and internal staffs to implement and integrate a CASB solution based on the requirements and provide technical assistance, solution design, and assist in developing security controls.

### **Senior Security Analyst**

**Role: SOC Operations - Shift Lead**

**Comodo Cybersecurity • Chennai • Tamil Nadu**

**Oct-2016 • Jan-2019**

- Monitor, evaluate, and maintain systems and security configurations to protect the customer infrastructure to identify potential threats and respond to reported security violations.
- Design and implement SOC operating procedure (SOPs) documentation and train the team members on the incident handling process.
- Performed research on recent security malware, vulnerability, and breaches and provided tailored recommendation to secure their infrastructure.
- Devised long terms plans for customer's drivers by reviewing their requests for improvement and enhancements of both process and the services.
- Collaborated with the customer's internal team to evaluate the network flow to identify gaps in the logs to uncover missing information which are required to improve the identification of overarching security incidents.

### **Senior Analyst**

**Role: Client Support - Sr. Security Engineer**

**HCL Technologies • Chennai • Tamil Nadu**

**Aug-2014 • Oct-2016**

- Responsible for managing the customers endpoint security and network level security devices such as Firewalls, IDS/IPS, VPN, and Two-Factor Authentication.
- Performed migration of firewall security policies from legacy firewalls to next-gen Palo Alto Firewalls.
- Defined the network flow and deployed the Palo Alto firewalls with the fine-tuned security configuration from the migration activity based on the existing communications established with the legacy firewalls.
- Maintained and monitored the IDS/IPS security alerts and incidents through our internal SIEM tools and create tickets for investigation to the concerned teams for action.
- Played major roles in increasing the firewall performance by refactoring and periodically reviewing the security configurations and keeping security devices update to dates based on the vendor discussion.

---

## **Certifications**

- **Certified Information Systems Security Professional (CISSP)**  
[Credential ID: 610233 | Expires on: March 2025]
- **Microsoft Certified: Azure Fundamentals**

---

## **Education**

- **Bachelors in Electronics and Communication Engineering**  
S A Engineering College • Chennai • Tamil Nadu • April 2014
- **Diploma in Electronics and Communication Engineering**  
S A Polytechnic College • Chennai • Tamil Nadu • April 2011