PRABHU PERUMAL

Cybersecurity | DevSecOps | Cloud | On-Premise
Castle Rock, CO | +1 (720) 305-6402 | prabhu312p@icloud.com
LinkedIn: https://www.linkedin.com/in/prabhu-perumal/ | Blog : https://www.praboo.in

SUMMARY

Cybersecurity and DevSecOps Engineer with over **4 years** of experience protecting financial organizations data, specialized in setting up, securing, and monitoring IT systems across AWS cloud and on-premises infrastructures which includes business-sensitive data, application data, logs, servers, physical network devices and user endpoints as desktops and laptops. Expertise in **Vulnerability Management, AWS security, Penetration Testing, SIEM (Security Information and Event Management), Endpoint Protection, CASB, DLP (Data Loss Prevention), Firewalls, Governance Risk Compliance (GRC) and Programming Languages.**

SKILLS & TOOLS

AWS Security & Governance:

- Data protection and IAM access reviews in S3 Buckets
- Setting up Compliance standards in EC2 servers
- Monitoring Logs through CloudTrail, Threat detection using GuardDuty
- Implement API Gateway security rules and Access controls
- Sensitive data discovery using Amazon Macie

AWS Penetration Testing:

- IAM privilege escalation testing
- S3 misconfiguration abuse testing
- EC2 metadata exposure (IMDS) testing
- EKS RBAC and Container security testing

Data Security, DLP & Shadow IT:

- Enforce data loss prevention rules, monitor file upload activity, and the Shadow IT Process using behavioral analysis (Symantec CloudSOC)
- Secure internet and private application access policies to protect remote users(Zscalar ZPA/ZIA)
- Good exposure on Cyera and Varonis

Programming & Scripting:

- Python, C++, Basic Java & Shell, Bash Scripting

Network Security:

- Palo Alto Networks NGFW Configuration in AWS
- Rule Auditing, ACL Optimization and Port/Protocol Abuse detection
- CCNA Skills (Subnets, Routing), Wireshark

Vulnerability Management:

- Tenable.io and Nessus: Vulnerability and Hardening Scanning
- Risk Analysis: Patch prioritization using CVSSv3, EPSS, and KEV

Governance, Risk & Compliance (GRC):

- CIS Benchmarks, NIST 800-53, OWASP Top 10, MITRE ATT&CK, CVSS, EPSS, KEV.

DevSecOps & Automation:

- CI/CD Pipeline Security, SAST/DAST (Synk and Prisma cloud), Container Image Scanning, IaC Security

Endpoint Security & Forensics:

- Antivirus: Agent Deployment and policy validation (CrowdStrike Falcon), EDR Bypass Testing
- Exploitation testing using Kali Linux, Metasploit, Burp Suite, and Digital Forensics tools
- Splunk/Kibana SIEM log analysis

EDUCATION

- Master of Science in Cybersecurity | University of Denver, USA | Sept 2023 – Aug 2025
- Bachelor of Engineering in Computer Science | Anna University, India | June 2015 – April 2019

CERTIFICATION

- AWS Certified AI Practitioner – Jan 2026
- AWS Certified Solutions Architect – Associate - Nov 2025
- Certified Ethical Hacker (CEH v12) – EC-Council - Jan 2025
- Purdue Certified in Applied Cybersecurity Essentials - Feb 2021
- First Aid Responder (CPR/AED)-American Red Cross-Feb 2024

EMPLOYMENT HISTORY

#	Role	Duration	Company	Location
1	Technology Analyst – Cybersecurity	Jan 2023 – Aug 2023	Infosys (3 years) Client: Temasek	Bengaluru, India
2	Senior Systems Engineer – Cybersecurity	Feb 2022 – Dec 2022		
3	Systems Engineer – Cybersecurity	Aug 2020 – Jan 2022		
4	Intern and Junior SOC Analyst	Jul 2019 – Jun 2020	Comodo CA (1 year)	Chennai, India

ACHIEVEMENTS, AWARDS & LEADERSHIP

- **Cyberforce Competition 2024** – U.S. Dept. of Energy: Secured ICS turbine systems against cyberattacks during live challenges.
- **Rise Insta Awards (x2) – Infosys Limited (2022):** Recognized for clearing 10,000+ critical vulnerabilities and cross-project problem-solving with different projects.
- **Cybersecurity Professional Skill Tag – _Infosys Limited (2021) -** In recognition of my skills and experience that contribute to the company's future readiness, I have been awarded this skill tag.
- **Student Innovator Award (2019)** – ICT Academy and **Smart India Hackathon Finalist** – AICTE, Govt. of India.
- **Student Chairman, Dept. of CSE (2019)** and Organizer of **SINTACS 2018** national-level technical symposium.

PROFESSIONAL EXPERIENCE

Infosys | Aug 2020 – Jan 2023| Client Overview – Temasek: **Temasek** is the parent company of global investments. **Seviora (Asset Management Hub)** and **Fullerton** operate under Seviora to provide specialized Asia-Pacific investment strategies in Singapore. Each company manages its IT infrastructure and operations separately.

Project 1: Data Loss Prevention and Endpoint Security (DLP-ES) | Jan 2023 – Aug 2023 | Temasek: Safeguards internal sensitive data from being shared outside the organization across laptops, desktops, and cloud storage used by both business users and IT users. Enforces data protection rules and secures devices with falcon antivirus and endpoint controls for all the users.

Roles & Responsibilities:

- **Achieved 100% from 13% true-positive DLP detection** eliminating false positives through strict DLP rule tuning in Symantec CloudSOC.
- **Blocked 62 Public cloud storage,websites** reducing data exfiltration risk through behavioral Shadow IT analysis.
- **100% true-positive detection**, implementing AWS Macie with precision-tuned rules for PII and financial data in S3.
- **1200+ User endpoints onboarded**,implementing Falcon agent EDR with continuous threat monitoring and response.
- **Reduced IAM attack surface**, removing excessive S3 permissions and enforcing least-privilege access.

Project 2: Vulnerability Assessment and Compliance – On-prem | Jan 2023 – Aug 2023 | Fullerton: Secures on-premises Windows servers used by IT and application users by reducing weaknesses that could be exploited to steal data or cause harm. Protects servers from breaches caused by software flaws, unauthorized access, misconfigurations, and risky user behavior by discovering assets, assessing weaknesses, limiting privileges, strengthening authentication & enabling continuous monitoring.

Roles & Responsibilities:

- Improved **65% patch turnaround time** and sustained 100% remediation SLAs, discovering and remediating vulnerabilities across 60+ on-prem servers **(Tenable.sc).**
- Improved **CIS hardening from 58% to 96%,** validating secure windows server baselines to support AWS cloud migration.
- Ensured **100% audit readiness** by completing **internal GRC audits** (**MAS TRM,CIS,NIST**)and closing all security gaps prior to external audit assessment.

Project 3: Cloud Vulnerability Management(VM) and Firewall Management(FM) | Feb 2022 – Dec 2022 | Seviora: Enable and manage the end-to-end vulnerability lifecycle for all IT assets in the AWS environment including cloud servers, network devices, and employee laptops. Automate patch management, secure cloud network traffic, enforce least-privilege firewall rules, block suspicious activity in real-time and maintain the compliance.

Roles & Responsibilities:

- Onboarded endpoints, network devices (Switches/Routers/AccessPoints), and new AWS servers into Tenable.io and Nessus, enabling enterprise-wide visibility and continuous vulnerability scanning.
- Stabilized AWS vulnerability posture within 4 months post on-prem migration by remediating 400K+ vulnerabilities (10K critical); earned two Infosys Rise Insta Awards.

- Executed **risk-based vulnerability assessments (CVSS v3)** across SAP servers, network devices, .NET, and Log4j; tiered assets, validated true risk, and **governed security exceptions at scale**.
- Contained **zero-day threats (e.g. log4j) within 2–5 days** through rapid risk assessment and prioritized remediation
- Scaled **automated remediation**, accelerating patch rollout and fix verification with **Python-driven workflows**.
- **Reduced firewall rule conflicts-30%**, strengthening AWS network security and blocking malicious IOCs (Palo Alto NGFW).

Project 4: DevSecOps and Network Security | Aug 2020 – Jan 2022 | Temasek: Implement shift-left security to identify and remediate issues early in code before release for development team. Routinely review cloud access and system exposure, servers, and applications are not accessible to public. Ensures that cloud applications and systems are protected by allowing safe access for employees through an internal VPN.

Roles & Responsibilities:

- **Hardened 20+ cloud and container workloads** by closing open ports, tightening permissions, and fixing vulnerable images (Prisma Cloud / Twistlock) in the code repository
- **Remediated 6+ projects code releases** by fixing application vulnerabilities during the build process (Snyk SAST/DAST).
- Secured remote user access by **replacing VPN exposure** with identity-based access controls (Zscaler ZIA/ZPA).
- **Hardened 8+ AWS resources,** reducing cloud attack surface by correcting over-permissive IAM roles, exposed APIs, and public EC2/S3 access (AWS).

Comodo CA (Sectigo) | July 2019 – June 2020: Comodo CA (now Sectigo) is a global provider of computer security software and SSL certificates.

Project: Security Monitoring & Web Application Protection: Proactively detected and remediated threats by monitoring system and web logs for anomalies (failed logins, suspicious activity) and conducting web security checks to fix common weaknesses, safeguarding servers, websites, and user data.

Roles & Responsibilities:

- **Enabled SIEM-driven incident alerts** for XSS, brute-force, and access anomalies in Splunk, accelerating detection and response.
- **Hardened 10+ web apps** by eliminating SQLi/XSS, authentication flaws, and Apache/Nginx misconfigurations.

SCHOOL PROJECTS (https://www.praboo.in/my-projects)

- **AWS Penetration Testing Lab (CloudStrike-X, 2025):** Built a multi-module AWS attack lab (IAM, EC2, S3, Lambda, API Gateway, Cognito, EKS) to simulate real-world exploits, uncover misconfigurations and validate mitigations aligned with CIS & AWS best practices.
- **Digital Forensics Investigation – Innovize Inc. (2025):** Performed full Linux forensic investigation-persistence mechanisms, backdoors, user misuse, and network traces, documenting timelines and IR recommendations.
- **Blockchain-Based Ransomware-Proof Backup (2025):** Built a decentralized backup architecture using IPFS + Ethereum smart contracts to ensure ransomware-resistant file storage with cryptographic integrity validation.
- **Capture The Flag (CTF) Lab Development (2025):** Designed and deployed “CypheriaGame” and “KubeGoat” ,a 23-challenge CTF platform covering web, binary exploitation, container attacks, privilege escalation, and Kubernetes misconfigurations
- **AWS CI/CD Deployment – Tetris Game on ECS, Multi-Cloud Kubernetes (2024):** Engineered a full CI/CD pipeline using ECS Fargate, ECR, ALB, and CodePipeline to automate Docker image builds and enable zero-downtime deployments with CloudWatch monitoring.
- **Honeypot Deception in OSINT & SOCMINT (2024):** Designed honeypot traps to divert attackers using decoy servers and fake data. Deployed deception-based honeypots with realistic decoy data to study attacker behavior, divert threats, and strengthen red-team/blue-team intelligence workflows.
- **Augmented Reality Plant Disease Detection (Jul 2019):** Used Python OpenCV and CNN to detect leaf diseases with AR visualization.
- **AI-Based Bank Statement System (May 2018):** Automated bank subsidy eligibility and claims through Python AI integration with MSME.