Sujith Kumar Navva

Email: navv0001@e.ntu.edu.sg | LinkedIn: SujithNavva | Phone: +65 98854920 | GitHub: SujithNavva |Singapore

Professional Summary

Cybersecurity Engineer with expertise in enterprise security engineering, threat detection, and privileged access management across on-premises and cloud environments. Proven success in deploying Trend Micro XDR, BeyondTrust PAM (dual-control), and WAF/IPS technologies (Imperva, DOSarrest, TippingPoint). Experienced in SIEM operations, cloud compliance, and automation using Python and Java. Currently driving hybrid security modernization at Network for Electronic Transfers (Singapore) while pursuing an MSc in Cybersecurity at NTU. Dedicated to building secure, compliant, and resilient infrastructures aligned with MAS TRM and ISO 27001 standards.

Core Competencies

Security Operations & Monitoring: LogRhythm SIEM, Amazon Security Lake, ELK Stack, Grafana, AppDynamics
Endpoint & Network Defense: Trend Micro XDR, Imperva WAF, DOSarrest WAF, TippingPoint IPS, Tripwire FIM, XyGate
Privileged Access Management: BeyondTrust (Dual-Control, Audit Management, External Audit Support)
Vulnerability Management: Tenable, Patch Management, Security Baseline Enforcement
Incident Response & Threat Detection: MITRE ATT&CK, Attack Navigator, Autopsy
Cloud Security & Compliance: AWS, Azure, GCP | AWS Macie | Security Lake
Security Automation & Scripting: Python, Bash, PowerShell, Java
Secure Software Development: React.js, Spring Boot, OWASP Secure Coding
DevOps & CI/CD: Docker, Jenkins, Git
Governance & Risk Management: MAS TRM, PII Detection, ISO 27001 Controls, PCI-DSS

Professional Experience

Cybersecurity Engineer

Network for Electronic Transfers (Singapore) | *Present*

- Deployed and integrated **Trend Micro XDR** across on-prem and cloud environments, enhancing SOC visibility and detection accuracy.
- Implemented **BeyondTrust PAM** with dual-control access enforcement and managed periodic internal/external PAM audits.
- Optimized and hardened **Imperva and DOSarrest WAFs** and **TippingPoint IPS**, reducing false positives and improving web application protection.
- Conducted advanced **LogRhythm troubleshooting** and tuning for improved event correlation, alerting, and dashboard optimization.
- Managed **Tripwire FIM** and **XyGate** for server integrity monitoring and audit compliance.
- Automated security operations and patch compliance workflows using **Python and Java** scripts.
- Integrated **Amazon Security Lake** with ELK for centralized SIEM visibility and alert analytics.
- Deployed **AWS Macie** for automated PII detection and compliance reporting.
- Led **vulnerability assessments using Tenable** and enforced security baselines across hybrid workloads.
- Supported incident response exercises aligned with **MAS TRM** and enterprise security governance frameworks.

Application Security – L2 Analyst

Development Bank of Singapore (DBS) | *Jul 2022 – Aug 2024*

- Supported L2/L3 production incidents during MAS resilience pauses, reducing downtime by 15%.
- Delivered features used by thousands of active customers, ensuring security and reliability.
- Managed **security incident triage and escalation** during MAS resilience events, ensuring 24/7 coverage and reducing downtime by 15%.
- Reviewed and remediated **application-level vulnerabilities** in coordination with developers and SOC teams.
- Supported **forensic investigations and access control audits**, ensuring alignment with internal and regulatory security controls.
- Contributed to implementation of **secure coding guidelines**, encryption libraries, and data protection measures for customer-facing systems.

Key Projects

- **Hybrid XDR Deployment:** Integrated Trend Micro XDR telemetry into LogRhythm SIEM for unified cloud-on-prem monitoring.
- **PAM Transformation:** Migrated from manual access control to **BeyondTrust dual-control PAM** with automated audit reporting.
- **Cloud Honeypots:** Built and analysed Azure/GCP honeypots via ELK and Sentinel for real-time threat intelligence.
- **OAuth Phishing PoC:** Simulated token theft and implemented countermeasures for secure authentication.
- **IoT Cryptography:** Researched lightweight ciphers (ASCON, PRESENT) for embedded device protection.

Education

Master of Science (MSc) in Cybersecurity
Nanyang Technological University (NTU), Singapore
Bachelor of Technology in Computer Science Engineering
SRM Institute of Science and Technology, Chennai | 2018 – 2022 |

Certifications

- Advanced Cyber Threat Intelligence – *May 2025*
- Automation with Python and PowerShell for IT & Cybersecurity
- Penetration Testing Professional Certificate – *Cybrary*
- Application Security Titan – *Bronze Level*
- Front-End Developer – *React.js*

Achievements

- Reduced **service downtime by 15%** through proactive monitoring during MAS incidents.
- Onboarded **100+ assets** to **BeyondTrust PAM**, achieving full dual-control compliance.
- Enhanced **SOC visibility** by deploying Trend Micro XDR across hybrid workloads.
- Improved compliance posture via **Tripwire and XyGate** integrations for file integrity and audit readiness.
- Strengthened cloud privacy with scalable **PII detection using AWS Macie**.