Nitin Maurya

New Delhi, India | (+91) 9013306829 | nitin_maurya@outlook.com | linkedin.com/in/maurya-nittin/

PROFESSIONAL SUMMARY

Cyber Security Architect and Automation Consultant with 10+ years of experience across banking and telecom sectors, specializing in security architecture, SOC modernization, and large-scale security automation. Proven ability to translate business requirements into technical deliverables and engage C-level stakeholders and Indian banking regulators (RBI, CERT-In) to drive enterprise security implementations across on-premises and hybrid cloud environments (Azure, AWS).

CORE COMPETENCIES

Security Architecture

- Security roadmaps, enterprise architecture design, SOC amalgamation for PSU banks (Punjab National Bank, Oriental Bank of Commerce, Union Bank of India)

Cloud Platforms

- Microsoft Azure, Amazon Web Services (AWS), hybrid cloud environments

Security Operations & Automation

- **SIEM**: RSA NetWitness, Microsoft Sentinel, Elastic SIEM
- **SOAR**: Palo Alto Cortex XSOAR (Demisto), Tines, Splunk SOAR — design strategy, architecture, playbook development
- **XDR/EDR**: CrowdStrike Falcon, Microsoft Defender ATP
- MITRE ATT&CK-aligned detection engineering, incident response automation, Zero Trust Network Access (ZTNA)

Automation & Scripting

- Python, N8N, Backbox (network device patching and automation)

Network & Endpoint Security

- **Proxy**: Zscaler Internet Access (ZIA), Cisco IronPort
- **Micro-segmentation**: Zscaler Private Access (ZPA), CrowdStrike ZTNA
- **Firewalls**: Check Point, Cisco, FortiGate, Palo Alto Networks, Prisma SASE, pfSense

Other Security Tools

- Security Onion, Metasploit, Wireshark, Caldera (Breach & Attack Simulation), Wazuh

PROFESSIONAL EXPERIENCE

British Telecom eServe India Pvt. Ltd. — Cyber Security Architect & Automation Consultant Apr 2023 – Present

Leading design, implementation, and optimization of enterprise-grade security automation solutions for managed security service customers across banking, telecom, and enterprise verticals.

Key Achievements:

- **Automated Incident Response:** Introduced ZeroOps IR processes eliminating manual intervention for 90% of alerts, reducing mean time to acknowledge (MTTA), respond, and resolve (MTTR).
- **SOAR Optimization:** Consolidated 10+ playbooks into modular automations, reducing SOAR resource consumption by 30% and improving operational efficiency.
- **MITRE ATT&CK Alignment:** Designed 20+ detection rules mapped to MITRE tactics and techniques, enhancing cross-platform threat visibility.
- **SIEM EPS Optimization:** Reduced SIEM Events Per Second (EPS) load by 30% through log filtering and normalization.
- **AI-Powered Threat Intelligence:** Integrated OpenAI to auto-enrich incidents with contextual insights, improving analyst decision-making accuracy.
- **Threat Mitigation Automation:** Developed advanced threat response approval workflows enabling customer-authorized automated remediations for critical incidents.
- **Red Team Simulation:** Implemented Caldera-based adversary emulation to validate detection rules and reduce security coverage gaps.
- **Shadow AI Security:** Architected detection and auto-remediation solution for shadow AI usage within customer development environments (OpenRouter/QwenCode LLM + CrowdStrike).

Responsibilities:

- Architect and lead delivery of SIEM, SOAR, firewall, proxy, and incident response automation solutions for enterprise customers.

- Develop custom integrations including Proofpoint Threat Response (SaaS), Zscaler Private Access, Sonatype Nexus Repository, and Palo Alto Strata Cloud Manager (contributed 2 new out-of-the-box integration features).
- Support presales engagements by designing and delivering high-impact technical proof-of-concept demonstrations.
- Implement phishing detection and auto-remediation workflows for high-volume spam environments.
- Conduct real-time automated forensic collection through CrowdStrike Real Time Response (RTR).
- Build and maintain internal knowledge management systems (Confluence) to streamline operational efficiency.
- Collaborate with Product Management and Portfolio teams to evaluate and onboard open-source security tools as new service additions.

Integrated Technologies:

- AI/ML: OpenAI (context enrichment)
- EDR/XDR: CrowdStrike Falcon, Microsoft Defender ATP
- Threat Intel: Anomali ThreatStream, VirusTotal, MITRE ATT&CK, Unit 42
- Cloud Security: Prisma Access, Zscaler ZIA, Zscaler ZPA
- Red Teaming: Caldera
- Data Ingestion: Syslog, Webhook

Punjab National Bank — Senior Manager IT (Cyber Security) July 2016 – Apr 2023

Led cybersecurity operations, SIEM implementation, and SOC transformation for one of India's largest public sector banks, including post-merger SOC consolidation following the Government of India's PSU bank amalgamation initiative.

- **SOC Leadership:** Led SOC amalgamation of three PSU banks (PNB, Oriental Bank of Commerce, Union Bank of India), managing a 10+ member SOC team and significantly improving SIEM integration capabilities.
- **SOAR Implementation:** Implemented Palo Alto Cortex SOAR platform for automated incident response workflows.
- **Detection Engineering:** Delivered new detection use cases across critical banking applications — Internet Banking, Mobile Banking, UPI, IMPS, SWIFT, Core Banking Solution (CBS), Cheque Truncation System, RTGS, NEFT, and more.
- **Regulatory Compliance:** Managed RBI audits and regulatory compliance tasks; presented security metrics and posture reports to CXO-level strategy committees.
- **Incident Response:** Provided 24/7 on-call support for critical security incidents, maintaining 100% SLA compliance.
- **Email Security:** Administered Messaging Gateway for inbound/outbound email security — spam filtering, policy enforcement, SPF/DKIM monitoring, blacklist/whitelist management.
- **IPS Monitoring:** Monitored Intrusion Prevention System (IPS), took actions against DDoS attacks, and maintained threat intelligence in SIEM.
- **Threat Intel & Advisories:** Actioned advisories from CERT-In and other government cyber bodies; shared threat intelligence on scanning, probing, malware, and spam detected on security devices.
- **Automation:** Automated incident management using Python, reducing need for dedicated automation servers and lowering operational costs.
- **Red Team / Blue Team activities:** Deployed infrastructure for RED teaming exercises conducted by CERT-In (India's national cyber nodal agency).

Canara Bank — Single Window Operator – Grade A Aug 2015 – Jun 2016

- Monitor and respond quickly to incoming requests relate to IT issues.
- Maintain computer systems and act as support if any system goes down.
- Responsible for PC's, Printers, Servers and related equipment.
- Maintain user PCs, including upgrades and configuration as needed.

LICENSES & CERTIFICATIONS

- **Palo Alto Networks Certified Security Automation Engineer (PCSAE)** | ID: 0274924b0bed40c4b3d89dc0fa9faeb0
- **Tines Advanced Certification** | ID: aRRRGj89nA
- **EC-Council Certified Ethical Hacker (CEH)** | ID: ECC7598431026
- **CompTIA Security+** | ID: 5139CJNNTLFQQT35

EDUCATION

Master of Technology (M.Tech.) — University School of Information Technology Aug 2012 – May 2014

Post Graduate Program in Artificial Intelligence and Data Science — MIT xPRO **(In Progress)** Sept 2025 – Aug 2026