Akshay Koshti

Ahmedabad, Gujarat | Akshaykoshti97@gmail.com | +91 9624123473 | LinkedIn | GitHub

PROFILE SUMMARY

Experienced SOC Analyst with a strong background in cyber threat monitoring, incident response, and security operations across diverse industries. Proven expertise in threat detection, cyber threat intelligence, and phishing simulation. Skilled in managing SIEM platforms (ArcSight, Splunk, Seceon, Securonix), EDR solutions (CrowdStrike, MDATP, Bitdefender, SentinelOne, Seqrite), and cloud security tools like Prisma. Adept at handling mail security (O365, Area1), brand monitoring, and security posture assessments (BitSight, Secure Scorecard, Cycognito). Proficient in ticketing systems (ServiceNow, BMC) and security tool management, with a focus on optimizing SOC workflows and response strategies.

KEY SKILLS

- Incident Response
- Cyber Threat Intelligence
- SIEM Management (ArcSight , Splunk, Seceon, Securonix)
- Threat Detection & Analysis
- Brand Monitoring
- Cloud Security (Prisma)
- Phishing Simulation
- Security Tool Management
- Mail Security (O365 & Area1)
- Ticketing System (service Now & BMC)
- Security Postures (BitSight, Secure score card & Cycognito)
- EDR Solutions (CrowdStrike, MDATP, Bitdefender, Sentinel One, Seqrite)

WORK EXPERIENCE

Deputy Manager, Techd Cybersecurity Ltd. — May 2025 – Present

- Lead the Product Support Group, overseeing deployment and support projects for cybersecurity solutions including Seqrite, SentinelOne, Bitdefender, and CrowdStrike.
- Manage the Seceon XDR team, handling onboarding, troubleshooting, and ongoing client support.
- Conducted Cyber Drills and Table top exercise as per client requirement in various sectors.
- Actively manage the Security Operations Center (SOC), driving continuous improvements and implementing future-ready updates.
- Implemented GoPhish to conduct phishing simulation exercises for clients, enhancing their email security awareness and response readiness.

Deputy Manager, Adani Enterprise Ltd. — Dec 2021 – May 2025

- Skilled in SIEM analysis, utilizing ArcSight to parse logs from network devices and endpoints.
- Proficient in Microsoft Defender ATP's EDR tool, conducting threat investigations and deploying advanced hunting queries for proactive threat detection. Experienced in CrowdStrike management.
- Expertise in crafting tailored detection rules with KQL queries in Defender ATP.
- Effective management of phishing campaigns, blocking IOCs, and providing O365 Email Protection recommendations.
- Hands-on incident investigation with Falcon CrowdStrike and threat analysis using Recorded Future.
- Monitoring OT security threats with RAM2-Otorio and proactive takedown of suspicious domains.
- Conducted MDATP testing for Migration Activity.
- Generating comprehensive EDR coverage reports and utilizing ServiceNow for ticket creation.

SOC Analyst, TechDefence — Jul 2021 – Oct 2021

- Monitored and triaged incidents, delivering daily reports to multiple clients.
- Crafted threat advisories for clients, leveraging up-to-date research and trends.
- Managed vendors, documented processes, and Deployed SIEM for clients.
- Scripted new rules and hunts for Splunk, enhancing security protocols.

SOC Analyst Intern, Colgate-Palmolive **Jan 2021 – Jul 2021**

- Conducted daily security activities, monitoring SIEM and OT systems.
- Supported senior team members in refining Splunk Use Cases and automating XSOAR.
- Contributed to security measures like BitSight and Cycognito.
- Utilized threat intelligence tools such as Anomaly and Insight.

Technical Consultant, REESS GmbH (Switzerland) **Jun 2018 – Jan 2019**

- Conducted research on new trends and products.
- Prepared presentation and research materials for clients.
- After project approval, acted as a liaison between clients and the development team.

Cyber Security Intern, Gurugram Cyber Cell **Jun 2017 – Jul 2017**

- Worked as a research intern at Gurugram cyber cell and worked on Social Media Crime.

EDUCATION

Master Of Science – Cyber Security **2019 – 2021**

National Forensics Sciences University • Gandhinagar, Gujarat

Bachelor Of Engineering – Computer Engineering **2014 – 2018**

Gujarat Technological University • Ahmedabad, Gujarat

AWARDS & CERTIFICATIONS

- AZ-900 Certification
- Certified Ethical Hacking
- Basis Technology: Autopsy Basics Hands-on
- Black Bag Technology: Certified Mobilyzer Operator
- Microsoft Student Ambassador (Twice)

ADDITIONAL INFORMATION

During my academic journey, I explored key cybersecurity domains including juice jacking, Docker container security, and Active Directory hardening during my Master's, and led development projects like an attendance management system and an online comic book platform during my Bachelor's. Professionally, I've gained hands-on experience at Adani, where I led **EDR migration**, **optimized NMS configurations**, and enhanced **Office 365 security**. Currently at TechDefence, I manage the Product Support Group, overseeing deployments of solutions like **Seqrite, SentinelOne, Bitdefender**, and **CrowdStrike**. I also lead the **Seceon XDR** team for onboarding and troubleshooting, manage SOC operations for continuous improvement, and have implemented an open-source ticketing system (**GLPI**) to track SLA metrics. Additionally, I conduct phishing simulation exercises using **GoPhish** to strengthen client security awareness.