Kushal Badodekar

(312) 451-1041 | kushalbadodekar001@gmail.com | LinkedIn | Portfolio

SUMMARY

Security Engineer with 3+ years' experience in security operations, network security, and endpoint protection. Skilled in threat modelling, detection engineering, and incident response, focusing on automating workflows using Python, PowerShell to boost triage speed and minimize risks. Proficient in tuning SIEM and EDR platforms (CrowdStrike, Splunk, Microsoft Defender) to improve threat visibility. Passionate about AI-driven security, red/blue team simulations enhancing organizational resilience.

EDUCATION

Master of Science, Cyber Forensics and Security - Illinois Institute of Technology, Chicago, IL, USA — May 2025

Bachelor of Engineering, Computer Science - Visvesvaraya Technological University, Karnataka, India — June 2019

SKILLS

Tools & Platforms: CrowdStrike Falcon, Splunk, Microsoft Defender, Tenable, Wireshark, AWS, Azure Entra ID, YARA
Technical Skills: Incident Response, Threat Hunting, Vulnerability Management, SOAR, SQL, IDS/IPS, Python, PowerShell
Frameworks: MITRE ATT&CK, NIST-800, ISO 27001, SOX, Zero Trust, OWASP

WORK HISTORY

Security Analyst | *James Hardie Building Products – Chicago, USA* — June 2024 – Dec 2024

- Implemented **20+** custom EDR rules in **CrowdStrike Falcon** & **Defender**, increasing actionable threat detections by **10%** and strengthening enterprise security posture.
- Developed and tuned **10+ detection** rules in **Splunk** mapped to **MITRE ATT&CK**, reducing false positives by **20%**.
- Identified and remediated **15+ Azure Entra ID** misconfigurations, eliminating privilege escalation risks and securing **10+** business-critical applications.
- Automated **20+ SOAR** workflows in **Python/PowerShell,** to streamline incident response and reducing triage time.
- Led **10+** STRIDE **threat modeling** sessions for production environments, identifying and mitigating **15+ security** risks.
- Executed **vulnerability management** and compliance audits on **5,000+** endpoints using **Tenable**.

Cybersecurity Engineer II | *ATOS – India* — April 2022 – Aug 2023

- Led and mentored a team of **5+** analysts to strengthen security operations and incident response, conducted **10+** tabletop exercises that identified gaps and reduced containment time by **30%**.
- Conducted advanced threat hunting across **2,000+ endpoints** and diverse log sources using **IOC/IOA** analysis, uncovering **15+** undetected attack patterns.
- Reverse-engineered **10+ malware** samples to generate IOCs, improving detection accuracy & reduce undetected threats.
- Developed **25+ SOC incident response** playbooks, improving triage efficiency and standardizing processes.

Cybersecurity Engineer I | *ATOS – India* — Feb 2020 – March 2022

- Modernized **firewall policy** management and optimized **IDS/IPS** configurations, boosting threat prevention effectiveness by **40%** and reducing false positives by **25%**.
- Conducted forensics on breaches, analyzing **Splunk** logs and endpoints to determine RCA and recommend mitigations.
- Implemented Abnormal Security to design custom phishing detection rules, reducing successful phishing attacks by 15%
- Automated patching for **1,000+** assets with **Ansible**, reducing SLA breaches for critical vulnerabilities by **30%**.

CERTIFICATIONS AND COMPETITIONS

Certifications:

- CompTIA Security+
- AWS Certified Cloud Practitioner
- SOC Detection Engineering - Antisyphon
- Practical Malware Analysis & Triage

Competitions:

- CyberTruck, CyberTractor 2025 – Pen-testing
- Collegiate Penetration Testing Competition 2024
- Cyber Force 2023 – CTF and anomaly detection.
- NCAE Cyber Games - Regionals and Nationals.

PROJECTS

Malware Analysis - Performed hands-on malware analysis and triage of real-world samples, identifying persistence, C2, and evasion techniques, and developed custom **YARA detection rules** and automated scripts to accelerate threat response.

Product Security - Performed firmware analysis/hardening on PLC/RTU devices, led red team OT attacks (Wireshark, J1939/Modbus/Ethernet/IP), and remediated ICS vulnerabilities in a segmented Purdue Model environment.

Active Directory Security: Designed domain controller lab improving logging, threat detection, and attack surface reduction, simulated Kerberoasting/LLMNR/relay attacks to strengthen domain defenses and logging.