Kushal Badodekar

(312) 451-1041 | kushalbadodekar001@gmail.com | linkedin.com/in/kushal-badodekar

SUMMARY

Cybersecurity analyst with 3+ years' experience in SOC operations, cloud security (Azure/AWS), and endpoint protection. Skilled in threat modelling, detection engineering, and incident response, with a focus on automating workflows (Python, PowerShell) to improve efficiency and reduce risk. Proficient with CrowdStrike, Splunk, and Microsoft Defender; experienced in SIEM tuning and compliance (NIST, MITRE ATT&CK) and conducting red/blue team simulations against advanced threats.

EDUCATION

Master of Science, Cyber Forensics and Security - Illinois Institute of Technology, Chicago, IL — 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, OAuth, YARA
Technical Skills: Incident Response, Threat Hunting, Vulnerability Management, SOAR, SQL, IDS/IPS, Python, PowerShell
Frameworks: MITRE ATT&CK, NIST-800, ISO 27001, PCI-DSS, SOX, Zero Trust, OWASP

WORK HISTORY

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

- Orchestrated advanced detection strategies in **CrowdStrike Falcon** & **Microsoft Defender** (EDR), boosting detection precision by **10%** and reducing response time to threats.
- Developed and tuned **threat detection rules** in **Splunk** leveraging **MITRE ATT&CK**, reducing false positives by 20%.
- Identified and remediated cloud misconfigurations, access controls in **Azure Entra ID**, preventing potential privilege escalation and data exposure incidents.
- Automated response and remediation workflows in **Python/PowerShell**, reducing **triage time** and analyst workload.
- Performed **vulnerability management** and compliance audits with **Tenable** ensuring **NIST** CSF adherence.
- Performed **threat modeling** using the **STRIDE** framework to identify and mitigate application and infrastructure risks.

Senior Consultant | *ATOS – India* — April 2022 – Aug 2023

- Led a team of 5+ analysts to optimize security operations, refined incident response plans, and conduct tabletop exercises boosting threat readiness company-wide.
- Conducted advanced **threat-hunting** investigations using log aggregation, **IOC/IOA** analysis, and behavioral analytics, successfully uncovering stealthy attack patterns.
- Developed **20+ SOC incident response** playbooks, increasing triage efficiency and standardizing processes.
- **Reverse-engineered** malware and reconstructed phishing attack chains to produce actionable **threat intelligence**.

Associate Consultant | *ATOS – India* — Feb 2020 – March 2022

- Performed forensics on breaches, analyzing network logs and endpoints to determine RCA and recommend mitigations.
- Reduced successful phishing incidents by **15%** leveraging **Abnormal Security** tools and strategies.
- Automated **vulnerability scanning** and patch deployment with **Python** and **Ansible**, cutting manual workload by 30%.
- Configured firewalls and **endpoint access controls** to enforce **least privilege**, reducing unauthorized access incidents.

CERTIFICATIONS AND COMPETITIONS

Certifications:

- CompTIA Security+
- AWS Certified Cloud Practitioner
- RedHat Linux Enterprise 9
- Practical Malware Analysis & Triage

Competitions:

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

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.