KUSH BORIKAR

Cyber Security Analyst

SAN JOSE, CA • + 1 (408) 460-0243 • borikarkush@gmail.com • LinkedIn • Portfolio

SUMMARY

Cyber Security Analyst with 3+ years of experience in **Blue-Team Security Operations, Incident response and Vulnerability management. CompTIA Security+ & Security Blue Team** certified, with proven success in reducing critical vulnerabilities by 45% and streamlining SOC operations.

EDUCATION

Master's in **Cyber Security**, New Jersey Institute of Technology (**GPA: 3.9/4**) 2022 - 2024
Bachelor's in **Information Technology**, Nagpur University **(GPA: 3.1/4)** 2016 - 2020

SKILLS

Security Tools: Splunk, Azure Sentinel, Wireshark, Snort IDS, Suricata IPS, Burp Suite, Metasploit, Nmap, Nessus, OpenVAS, YARA, TheHive, DeepBlue CLI, Autopsy, Volatility, VirusTotal, VMWare, Strings, Ghidra, IDA Free
Networking: TCP/IP, OSI, DNS, HTTP, SMTP, VPN, SSL/TLS, Routers, Switches, Firewalls(Palo Alto, Fortinet), Cloud Security
Programming/Scripting: Python, PowerShell, Bash, JavaScript
Core Security Skills: **SIEM** - Log Analysis & Monitoring | Security Operations, Incident Response, Vulnerability Assessments, Digital Forensics, Endpoint Security (EDR), Dynamic Malware Analysis, Email Security, Incident Triage, Regex
Threat Intelligence: MITRE ATT&CK, MISP, OWASP, OSINT, TTPs, Cyber Kill Chain| SIEM Query Languages: SPL, KQL(Kusto)
Operating Systems: Windows, Windows Server, Linux Distributions, MacOS, Unix
Other Tools: Git, GitLab, Microsoft 365, Google Suites, Slack, JIRA, ServiceNow

CERTIFICATIONS

CompTIA Security+ | (ISC)2 CC | Security Blue Team - BTL1 | LetsDefend SOC Analyst | AWS Cloud Practitioner

WORK EXPERIENCE

Information Security Analyst Remote - Chicago, IL
Rebecca Everlene Trust Company Aug 2024 - Present

- Led organization wide Security operations to implement policies, mitigate vulnerabilities and prevent security incidents.
- Developed and implemented AWS security policies using AWS IAM, Config, and CloudTrail, enhancing cloud infrastructure security posture.
- Configured AWS Security Hub, Cloud Watch and GuardDuty to monitor and detect potential security threats across cloud environments.
- Implemented least privilege access controls using AWS Identity Center, reducing unauthorized access risks by 35%.

Networks Support Assistant Newark, NJ
New Jersey Institute of Technology Apr 2023 - May 2024

- Developed Python scripts for automated network forensics, using Wireshark and Nmap to analyze 100+ endpoints, reducing vulnerability detection time by 40%.
- Engineered network security assessment workflows integrating packet capture tools to map infrastructure vulnerabilities and streamline incident response.
- Created custom automation solutions for proactive threat detection, identifying and mitigating 125+ network security risks with advanced scripting techniques.

Cyber Security Analyst Pune, IN
FirstCry.com Mar 2021 - May 2022

- Conducted quarterly security assessments of FirstCry's web application platform, identifying and mitigating 75+ vulnerabilities, including SQL injection, cross-site scripting (XSS), and broken authentication, using tools like OWASP ZAP, Nikto, and manual testing, which reduced exploitable attack vectors by 40%.
- Collaborated with development teams to integrate secure coding practices through code reviews and security training, decreasing the occurrence of critical vulnerabilities in production by 30% and improving deployment timelines by 15%.
- Performed monthly penetration tests on APIs and web application endpoints, ensuring secure data transmission, enhancing compliance with OWASP Top 10 standards, and reducing the risk of data breaches by 35%.

Cyber Security Intern - Incident Response Nagpur, IN

V3 Data Solutions Jan 2020 - Jun 2020

- Served as a member on the Cyber Incident response team to produce and maintain detailed reports summarizing lessons learned, trends, and strategic insights for leadership
- Deployed EDR solutions across 75+ systems, conducting detailed vulnerability assessments using OpenVAS, and achieving a 90% compliance rate with security standards.
- Contributed to cross-functional incident response process optimization, developing standardized playbooks that enhanced team collaboration and reduced incident resolution time by 20%.

PROJECTS

Network Intrusion Detection System - SNORT IDS

- Deployed and configured Snort in a vulnerable network environment to detect real-time threats, including port scans and brute-force attacks.
- Developed and tested custom Snort rules to identify malicious traffic, enhancing detection accuracy and response capabilities.
- Analyzed intrusion alerts and integrated Snort logs with a visualization platform to streamline monitoring and improve threat analysis.

Malware Analysis Lab - FlareVM

- Performed static and dynamic analysis of malware samples using tools such as PE Studio, Regshot, and Wireshark to identify malicious behavior and persistence mechanisms.
- Extracted and analyzed Indicators of Compromise (IOCs), including file hashes, IP addresses, and domains, to aid in threat intelligence and detection.
- Documented findings in comprehensive incident reports, providing actionable insights to improve security monitoring and response capabilities.

SIEM Implementation - Splunk

- Enhanced alert fidelity by refining 50+ detection rules, increasing SOC efficiency and implementing automated incident response workflows to reduce response times by 30%.
- Streamlined integration of threat data from firewalls, IDS/IPS into Splunk ES, enhancing detection capabilities and reducing manual log analysis by 40%.