KUSH BORIKAR

San Francisco, CA • (408) 460-0243 • borikarkush@gmail.com • LinkedIn • Portfolio

CORE SKILLS

Security Operations | Incident Response | Threat Detection | Vulnerability Management | SIEM Administration | Cloud Security | Network Security | Malware Analysis | Security Automation & Scripting | Penetration Testing | Risk Assessment | Security Compliance | Threat Intelligence | Policy Development | Application Security | Log Analysis | Security Frameworks | API Security | Network Protocols | Security Controls | Remediation Planning | Data Analysis

WORK EXPERIENCE

Information Security Analyst | Rebecca Everlene Trust Company | Remote - Chicago, IL **Aug 2024 - Jan 2025**

- Orchestrated comprehensive vulnerability management programs, conducting 55+ assessments using Nessus, Qualys & OpenVAS, reducing critical vulnerabilities by 45% through risk-based remediation strategies
- Established organization-wide security policies and procedures, including secure SDLC guidelines and incident response playbooks, achieving 90% compliance across development teams
- Led security awareness program targeting phishing and social engineering, resulting in 40% improvement in phishing detection rates and 50% reduction in successful attacks

Teaching Assistant - Network Security | New Jersey Institute of Technology | Newark, NJ **Apr 2023 - May 2024**

- Instructed and mentored 200+ students in network security labs, guiding hands-on exercises with Wireshark and Nmap for traffic analysis and vulnerability scanning
- Facilitated practical workshops on deploying secure cloud environments in GCP(Google Cloud Platform), implementing network security controls, and following security best practices
- Developed Python-based network traffic analysis tools to demonstrate packet inspection, protocol analysis, and anomaly detection techniques to students

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

- Led application security program conducting quarterly security assessments using OWASP ZAP and Nikto, identifying and remediating 75+ vulnerabilities including SQLi and XSS, reducing attack surface by 40%
- Implemented secure code review process and developer security training, decreasing critical vulnerabilities by 30% and improving deployment efficiency by 15%
- Executed monthly penetration testing of APIs and web applications, ensuring OWASP Top 10 compliance and reducing high and critical vulnerabilities by 35% through systematic remediation of vulnerabilities

Cyber Security Intern - Incident Response | V3 Data Solutions | Nagpur, IN **Jan 2020 - Jun 2020**

- Deployed and configured EDR solutions across 75+ endpoints, enhancing threat detection capabilities by 90% and improving incident response time
- Developed standardized incident response playbooks that reduced resolution time by 20% and improved cross-team collaboration
- Created detailed incident analysis reports and metrics dashboards for executive leadership, enabling data-driven security decisions

PROJECTS

SOC Automation & Incident Response Lab (Wazuh, TheHive, Shuffle SOAR) **Feb 2025**

- Designed and deployed a SOC lab integrating Wazuh (SIEM/EDR), TheHive (Incident Response), and Shuffle (SOAR) for automated security operations
- Engineered automated playbooks in Shuffle to enrich alerts, correlate threat intelligence, and trigger response actions such as IP blocking and notifications
- Configured Wazuh to ingest logs from Windows and Linux endpoints, forwarding critical security alerts to TheHive for streamlined triage and investigation

Cloud-Native SOC Design | Azure Sentinel **Jan 2025**

- Implemented an Azure Sentinel-based SOC environment processing 100000+ events, achieving 20% reduction in false positives through ML-powered analytics
- Built custom KQL queries and analytics rules based on MITRE ATT&CK framework, enabling real-time detection and response to 11,000+ security threats
- Integrated OSINT feeds and implemented automated threat hunting playbooks, reducing mean time to detect (MTTD) for critical incidents to under 12 hours

Network Security Monitoring Infrastructure | SNORT Intrusion Detection System **Dec 2024**

- Engineered comprehensive IDS solution using Snort in high-traffic environment, implementing 10+ custom rules for detecting advanced threats
- Created automated alert triage system integrating Snort with Splunk, improving alert correlation and reducing analysis time by 35%
- Developed custom threat signatures and implemented automated response actions for common attack patterns, achieving 90% accuracy in threat detection

EDUCATION

IBM Cyber Security Analyst Professional Certificate 🔗 10/2023- 03/2024
IBM Security Learning

Master's in Cyber Security 09/2022 - 05/2024
New Jersey Institute of Technology, NJ
GPA: 3.9/4.0
Relevant Coursework: Network Security, Security Operations, Vulnerability Management, Application Security

Bachelor's in Information Technology 08/2016 - 05/2020
Nagpur University, India
Relevant Coursework: Computer Networks, Database Management, Programming, Data Analytics, Operating Systems

TOOLS & TECHNOLOGIES

SIEM: Splunk, Wazuh, QRadar, Sentinel, LogRhythm, ELK
IDS/IPS: Snort, Suricata, Wireshark
Vulnerability Management: Nessus, Qualys, OpenVAS
Forensics: Autopsy, Volatility, DeepBlue CLI, Chainsaw
Malware Analysis: YARA, VirusTotal, Ghidra, Regshot, IDA
Frameworks: MITRE ATT&CK, OWASP, Cyber Kill Chain, NIST
Pentesting: Burp Suite, Metasploit, Nmap, Kali Linux
Incident Response: TheHive, Endpoint Security - EDR/XDR
Operating Systems: Windows, Linux, MacOS, Unix
Compliance: NIST, ISO 27001, SOC2, HIPAA, PCI DSS
Network Protocols: TCP/IP, DNS, HTTP, SMTP, SSL/TLS
Infrastructure: Active Directory, VPN, Routers, Switches, Firewalls (PFSense, Fortigate), Virtualization, Containers
Cloud Platforms: AWS, Azure, GCP
Programming & Automation: Python, PowerShell, Bash
Databases & Queries: SQL, SPL, KQL(Kusto), Lucene, WQL
Version Control: Git, GitLab
Documentation: Technical Writing, Incident Reports, Playbooks, Security Policy Development
Other: JIRA, ServiceNow, MS O365, Google Workspace

CERTIFICATIONS

- CompTIA Security+ 🔗
- (ISC)² Certified in Cyber Security 🔗
- Security Blue Team - Blue Team Level 1 (BTL1) 🔗
- Splunk SOC Essentials
- LetsDefend SOC Analyst 🔗
- LetsDefend Malware Analyst 🔗
- LetsDefend Programming for Cyber Security 🔗
- AWS Certified Cloud Practitioner (IP)