KUSH BORIKAR

borikarkush@gmail.com (408)-460-0243 in/kush-borikar

SUMMARY

Dedicated Security Engineer with expertise in SIEM systems, vulnerability assessment, and incident response. Experienced in implementing DevSecOps processes and integrating security measures throughout the development lifecycle. Skilled in utilizing various security tools and frameworks with a strong focus on continuous learning.

EDUCATION

Master's in Cybersecurity & Privacy

New Jersey Institute of Technology • Newark, New Jersey • 2024

Bachelor's in Information Technology

Nagpur University, India • 2020

CERTIFICATIONS

*** CompTIA Security+ * IBM CySA * CCNA * Udemy AWS Security Certified * Udemy Splunk Architect**

SKILLS

* Security Monitoring * Incident Response * Malware Analysis * Log Analysis * SIEM (Splunk/Sentinel) * IDS/IPS * Threat Intelligence *Network Security * Firewall Management *Cloud Security (AWS/GCP) * Endpoint Security (EDR/XDR) * Vulnerability Assessment * Antivurs Software * Python/PowerShell/Bash *Security Frameworks (NIST, ISO 27001, PCI, DSS) * Networking Concepts - TCP/IP/DNS/VPN * CI/CD * Gitlab Nmap/Metasploit * Linux/ Windows Operating Systems* Docker/Kubernetes * Security Integration *

PROJECTS

Implementation of Splunk SIEM Security Monitoring & Log Analysis

- Implemented Splunk SIEM lab, integrating logs from firewalls, IDS/IPS, and EDR systems, reducing threat detection time by 15%.
- Engineered custom Splunk dashboards and alerts, enhancing security monitoring and enabling proactive threat analysis.
- Optimized alert mechanisms, resulting in a 10% decrease in false positives during simulated security scenarios.

Application Security Analysis

- Executed threat hunting and vulnerability assessments on 22 Android applications using MobileAudit, identifying critical security flaws.
- Engineered a custom MobileAudit Docker container to streamline the security scanning process and enhance threat detection capability.
- Identified security lapses in audited applications, prioritized risks, and proposed development process improvements, delivering comprehensive reports with empirical assessment data and risk analysis.

Endpoint Security with Xcitium OpenEDR

- Deployed Xcitium OpenEDR across 10 lab endpoints, improving malware defense, remote monitoring, and patch management processes in a controlled environment.
- Optimized endpoint protection by implementing and testing security policies, leveraging Xcitium's features, which resulted in a 20% reduction in malware attacks and a 5% improvement in system performance on test machines.

EXPERIENCE

Computer Networks Teaching Assistant

New Jersey Institute of Technology **September 2023 - May 2024, Newark, NJ**

- Assisted in troubleshooting network lab environments, helping students resolve network configuration and security issues.
- Led sessions on secure network practices, aligning with best practices for cybersecurity and threat analysis.
- Facilitated learning on network monitoring tools, akin to those used in security monitoring and incident response in SOC environments.

Data Analyst

FirstCry.com **March 2021 - May 2022, Pune, India**

- Increased operational efficiency by 40% through analyzing complex data sets using Excel, delivering actionable insights for strategic decision-making.
- Developed real-time performance metrics reports, saving marketing team 40 hours monthly and revolutionizing efficiency and ROI.

Cyber Security Intern

V3 Data Solutions **January 2020 - June 2020, Nagpur, India**

- Configured security tools for vulnerability assessments, code reviews, and security testing; implemented best practices to enhance web application security.
- Implemented antivirus software across 50+ company devices, achieving a 95% reduction in malware incidents within 6 months using advanced detection tools and regular system scans.