KUSH BORIKAR

borikarkush@gmail.com (408)-460-0243 in/kush-borikar kushb98.github.io/

EDUCATION

Master's in Cybersecurity
New Jersey Institute of Technology • Newark, New Jersey • Sep 2022 - May 2024

Bachelor's in Information Technology
Nagpur University • India • Aug 2016 - June 2020

CERTIFICATIONS

CompTIA Security+ | CCNA | ISC2 CC | IBM CySA | Security Blue Team - BTL1 | Udemy Splunk Architect

SKILLS

Security Inforamtion & Event Management : Log Analysis, Alert Monitoring, Alert Triaging, Detection, Root Cause Analysis, IOCs, YARA
Networking: TCP/IP, OSI, Network Topology, Network Security, Firewalls, Network Monitoring, Wireshark, Nmap, Snort, Intrusion Detection & Prevention systems (IDS/IPS) | Incident Response: Detection, Analysis, Eradication, Case Management, DeepBlue CLI
Threat Intelligence: MITRE ATT&CK, MISP, OWASP, OSINT, TTPs| SIEM Query Languages: SPL, KQL, Kusto
Operating Systems: Windows, Linux, Unix | Others: Vulnerability Assessment, Phishing Analysis, Endpoint Protection, Kali Linux

PROJECTS

Security Monitoring & Intrusion Detection using ELK Stack
- Configured Elasticsearch, Logstash, and Kibana to aggregate and analyze 1000+ logs.
- Configured honeypots to simulate network environments, capturing a diverse array of attack data which fed into Elasticsearch.
- Developed custom dashboards and alerts within Kibana to monitor indicators of compromise(IOC) that point towards network intrusion.
- Conducted regular audits of network rules, using insights from honeypot traffic to adjust firewall policies and improve security controls.

SIEM Implementation - Splunk
- Conducted root cause analysis and performed alert monitoring across multiple data sources on Splunk Enterprise SIEM.
- Improved alert fidelity by refining detection rule logic and implementing automated incident response workflows.
- Integrated threat data from multiple security tools (firewalls, IDS/IPS) to enhance detection capabilities.

Security Operations Center Design (Azure Cloud)
- Built a security monitoring environment using Azure Sentinel and Log Analytics for intrusion detection.
- Created detection rules using KQL, successfully identifying 11,000+ security incidents.
- Integrated threat intelligence feeds and MITRE ATT&CK framework to profile adversary tactics and techniques.

EXPERIENCE

Information Security Analyst
Rebecca Everlene Trust Company **August 2024 - Present, Chicago. IL**
- Implemented enterprise-wide data loss prevention controls through Access Control policies and Identity & Access Management.
- Conducted security assessments detect vulnerabilities and suggest remediation strategies to improve application security.
- Drafted and reviewed standard operating procedures and security policies for critical applications.

Networks Support Assistant
New Jersey Institute of Technology **September 2023 - May 2024, Newark, NJ**
- Resolved network security issues and configuration issues for 100+ devices in lab environments.
- Deployed and maintained network security infrastructure by configuring switches, routers, firewalls and other network equipment.
- Conducted network security monitoring using Wireshark and Nmap, identifying and remediating 150+ security vulnerabilities.

Data Analyst
FirstCry.com **March 2021 - May 2022, Pune, India**
- Performed complex data analysis and root cause analysis of campaign performance, improving operational efficiency by 35%.
- Generated real-time performance metric reports, saving marketing team 40 hours monthly and enhancing data-driven decision making.
- Analyzed patterns and trends across 5000+ user datasets using advanced analytical tools, to discern complex user behavioral patterns.

Cyber Security Intern
V3 Data Solutions **January 2020 - June 2020, Nagpur, India**
- Implemented security monitoring solutions across 75+ endpoints, enhancing intrusion detection capabilities.
- Participated in security assessments and vulnerability assessments.
- Assisted in developing security alerts and SIEM rules to enhance and detect network instrusions.
- Created incident response documentation and tailored security awareness materials to enhance development team's secure coding practices.