KUSH BORIKAR

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

SUMMARY

Results-driven Cybersecurity Professional with hands-on experience in SIEM implementation, log analysis, and threat detection. Proficient in tools like Splunk, ELK stack, and Azure Sentinel, with a strong foundation in network security, incident response, and compliance frameworks. Demonstrated ability to automate security processes, triaging and conduct root cause analysis.

EDUCATION

Master's in Cybersecurity

New Jersey Institute of Technology • Newark, New Jersey • Sep 2022 - May 2024 • 3.90

Bachelor's in Information Technology

Nagpur University • India • Aug 2016 - June 2020 • 3.0

CERTIFICATIONS

CompTIA Security+ | IBM CySA | CCNA | Udemy AWS Security Certified | Udemy Splunk Architect | ISC2 CC

SKILLS

Security Inforamtion & Event Management : Log Analysis, Configuration, Maintenance, Rule Creation, Correlation
Networking: TCP/IP, OSI, Network Topology, Network Security, Firewalls, Network Monitoring, Snort, Wireshark, Intrusion Detection/Prevention systems (IDS/IPS) | **Device Security**: Endpoint Protection (EDR/XDR), Device Hardening
Scripting Languages: PowerShell, Python, BASH, Perl | **SIEM Query Languages**: SPL, KQL, YARA-L, Kusto.
Threat Intelligence: MITRE ATT&CK, OWASP, OSINT | **Incident Response**: Detection, Resolution strategies, Incident Management
Compliance Frameworks: NIST, ISO27001, PCI-DSS, HIPAA, SOC | **Operating Systems**: Windows, Linux, Unix

PROJECTS

Splunk SIEM Implementation for Security Operations

- Integrated logs from 5 multiple sources, including firewalls and EDR systems, to streamline security monitoring and incident detection.
- Developed and fine-tuned 50+ SPL queries to create custom dashboards and alerts, enhancing visibility into potential threats.
- Participated in security incident investigations and root cause analysis, contributing to the development of mitigation strategies.

Honeypot Deployment and ELK Integration for Cyber Threat Detection

- Implemented and managed a honeypot platform with ELK stack integration, enabling real-time threat detection and data visualization for more than 10 sources.
- Configured Elasticsearch, Logstash, and Kibana to aggregate and analyze 1000+ logs, developing use cases and actionable insights.
- Enhanced incident response capabilities by utilizing Kibana Query Language (KQL) to create advanced queries and correlations.

Azure Cloud Detection Lab

- Designed a cloud-based security detection environment using Azure Sentinel, Log Analytics Workspace, and 5 Virtual Machines.
- Implemented data ingestion and analysis pipelines to identify potential security threats using Kusto Query Language (KQL) and custom analytic rules, detecting over 11000 security incidents.
- Mapped detected threats to the MITRE ATT&CK framework to understand adversary tactics, techniques, and common procedures.

EXPERIENCE

Networks Support Assistant

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

- Provided expert support in diagnosing and resolving network configuration and security issues in lab environments for 100+ end devices.
- Employed Python scripts for automation of deploying servers and analysis to streamline troubleshooting processes.
- Conducted training sessions for 200+ students on network security best practices and tools, including Wireshark for traffic analysis.

Data Analyst

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

- Increased operational efficiency by 35% through analyzing complex data sets using Excel, delivering actionable insights.
- Developed real-time performance metrics reports, saving marketing team 40 hours monthly and revolutionizing efficiency and ROI.
- Leveraged advanced Excel functions and formulas to analyze complex data sets, identifying buying trends for 5000+ users.

Cyber Security Intern

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

- Secured more than 75 orgranization end devices through system configurations and device hardening.
- Conducted code reviews, security testing and implemented Access management for 10+ organization projects.
- Communicated complex and secure coding practices to the developement team to enhance web application security.