Jaavid Malette

jaavid.malette@gmail.com | (919)-946-5993

WORK EXPERIENCE

Triangle Ecycling **Durham, NC**

Information Technology Analyst *Jun 2015 - Present*

- Implemented and managed security patches, OS updates, and system monitoring to mitigate risks and ensure compliance.
- Led incident response efforts, conducting security risk assessments and developing security plans.
- Conducted in-depth troubleshooting, analyzed system performance, and provided recommendations.
- Trained and supported new IT interns, fostering teamwork in complex, data-driven environments.

Lead, Tech Sales *Jan 2017 - Present*

- Managed sales processes, including customer relations and negotiations.
- Analyzed sales data to improve performance, similar to analyzing data in Splunk to identify trends.
- Automated pricing and optimized data management using AI, boosting sales efficiency.
- Collaborated with the IT team to customize client solutions, showcasing communication skills.

EDUCATION

Durham Technical Community College **Durham, NC**

Associate's Degree - Computer/Information Technology Administration and Management *Graduation Date: Jun 2018*

CERTIFICATIONS

Google Cybersecurity Certificate (November 2023)
CompTIA Security+ Certificate (July 2024)

PROJECT EXPERIENCE

TryHackMe

Advanced Splunk Dashboards and Reports

- Completed the Advanced Splunk module on TryHackMe, focusing on advanced Splunk features for analyzing cybersecurity incidents.
- Set up and configured a Splunk instance with a forwarder to ingest logs from various sources.
- Designed complex search queries and applied regex to filter logs, enhancing incident investigation and threat-hunting.
- Generated comprehensive reports from log data, identifying security trends and potential threats.
- Developed interactive dashboards to visualize log data, improving the efficiency of security operations and accelerating incident response.

Splunk

BOTS 1-3 (Boss of the SOC)

- Participated in Splunk's BOTS competitions, focusing on detection and analysis using Splunk ES.
- Analyzed cybersecurity incidents with diverse log sources (cloud, firewall, endpoint) through real-time threat detection and incident reporting.
- Utilized advanced search queries, regex, and dashboards in Splunk to detect anomalies and enhance threat detection.
- Applied proactive threat-hunting techniques, improving overall security posture.
- Gained hands-on experience in comprehensive security operations with Splunk, including incident management and continuous monitoring.

SKILLS & INTERESTS

Skills: Splunk, Incident Detection and Response, EDR Tools, SOAR, MITRE ATT&CK, NIST CSF, IDS/IPS Systems, Vulnerability Assessment, Wireshark, TCPDump, Communication, Team Collaboration.