JABEZ DANIEL

+919483127179 | jabezds@gmail.com| https://www.linkedin.com/in/jabez-daniel-982637132/ | Bengaluru

SIEM ENGINEER | CYBER SECURITY ENGINEER

Accomplished and dedicated **Splunk and QRadar certified engineer** with over 7 years of experience in **configuring**, **integrating**, and supporting SIEM environments, including **administration** of QRadar and Splunk, as well as **developing** addons, apps, and conducting **threat hunting**. Skilled in creating dynamic dashboards, parsers, app extensions, log source integrations, and automated alerts. Proficient in **automating** security content using **Splunk SOAR** to enhance operational efficiency and improve threat detection.

SKILLS

- **Programming & Databases**: Powershell, Bash, Python, SQL, HTML, CSS, JavaScript
- **Security Tools & Platforms**: Splunk, Splunk SOAR, IBM QRadar, ServiceNow, Wireshark, Nmap, Burp Suite, Cribl
- **Cybersecurity & Detection Engineering:** Threat Detection, Vulnerability Analysis, Network Scanning, OS Detection, Web Application Security, Cryptographic Analysis, Incident Response Automation
- **Networking & SIEM:** Network Protocols, SIEM Architecture, Log Ingestion & Normalization, Event Correlation
- **Data & Analytics**: Data Cleaning, Data Transformation, Exploratory Data Analysis (EDA), Correlation Search Development, Dashboard Creation
- **Project & Delivery Skills:** Requirement Gathering, Solution Design, Project Planning, Implementation

CAREER HIGHLIGHTS

- Worked on **Splunk SOAR automation** which resulted in cutting down of the processing time by over 1 month leading to a saving in manpower and resource cost.
- Demonstrated **proactive involvement** in creating **correlation searches** in Splunk ES based on requirements from SOC team and Threat intel, contributing to effective threat detection and incident response.
- Collaborated with the Sales and Delivery team to deliver product **demos**, successfully **securing** numerous new projects and contract renewals.

PROFESSIONAL EXPERIENCE

NOVO NORDISK — Sep 2024- Nov 2025

Role: Content Management – SIEM Engineer

Work as a member of the Content Management Team in the Internal Firm Service to manage threat detection

- Strengthened enterprise threat detection by designing and implementing correlation searches in **Splunk Enterprise Security (ES) aligned** with the **MITRE ATT&CK framework**.
- Improved operational efficiency by automating repetitive security workflows through **Splunk SOAR** playbooks.
- Administered and optimized **Splunk ES and SOAR** environments, managing user permissions, system health, and performance tuning.
- Partnered with the Security Operations Center (SOC) to fine-tune notable events, significantly reducing false positives and alert fatigue.
- Developed and maintained incident response documentation and integrated ServiceNow SecOps for automated alert handling and ticket resolution.
- Developed custom Python scripts in Splunk SOAR to meet specific operational requirements, enhancing automation and streamlining security workflows.

NUSUMMIT CYBERSECURITY (FORMALLY AUJAS CYBERSECURITY LTD) — Oct 2018- Aug 2024

Senior Consultant — **(Jan 2024- Aug 2024)**

Role: SIEM Admin/ Threat hunter (Banking Client)

Served in a dual role as SIEM (QRadar) Administrator and Threat Hunter, supporting a banking environment.

- Managed end-to-end **QRadar administration**, including rule creation, log source integration, data onboarding, system performance monitoring, and issue resolution.
- Led proactive **threat hunting** to identify hidden adversaries and anomalous behaviors using **behavioral analytics, threat intelligence integration, and detection engineering.**
- Developed and executed **AQL-based queries** to uncover potential security incidents and enrich threat-hunting investigations.

- Fine-tuned **correlation rules and alerts**, collaborating with the SOC team to minimize false positives and enhance detection accuracy.
- Partnered with the **CISO** to present and operationalize key threat-hunting findings

Senior Consultant **(April 2019- Dec 2023)**

Role: Security Developer / SIEM (Splunk/QRadar) Integration Engineer
Progressed from the role of Associate Consultant to Senior Consultant over a period of 4 years.

Worked with the security development teams to develop app and addon in **QRadar** and Splunk for various security vendors like Cisco and CarbonBlack and Cybereason. Also collaborated with DevOps team to assist with **AWS cloud security**.

- Integrated multiple Cisco products like Cloud security, ISE, ESA, Firepower, TG, Carbon Black ThreatHunter and Cybereason to QRadar and Splunk
- Managed the setup and integration with proxy server
- Worked on AWS environment security remediation
- Developed custom parsers and Dynamic dashboards
- Created SPL and AQL to support the dashboards
- Defined Splunk configuration files, CIM compatibility
- Worked on product release validation and testing
- Worked with developers to ensure the app functions meet client expectation, provided comprehensive evaluation of overall application security posture.

- Proactively identified and mitigated cyber threats impacting business and network environments, improving overall detection and response capabilities.
- **WireGuard -Trading Encryption Solution Key** : Setup and configured Wireguard on the client environment and established end-to-end encrypted communication.

SOC Analyst **(Oct 2018- Mar 2019)**

Role : SOC Monitoring Analyst

- Investigated security incidents, tagged and classified offenses based on severity
- Reported security incidents to customers and did RCAs and created supporting reports.
- Monitored and detected threats, created proper shift handovers and kept all stakeholders informed.

EDUCATION

Bachelor in Engineer (Computer Science & Engineering) | VTU University, 2014–2018

TRAININGS/CERTIFICATIONS

- Splunk Core Certified Power User, Splunk (Jul 2023)
- CEH Practical, EC-Council(Oct,2021)
- IBM Certified Associate Analyst - Security QRadar SIEM V7.2.6, IBM (Nov,2018)
- Splunk 7.x Fundamentals, Splunk (Jan,2020)
- Splunk Infrastructure Overview, Splunk (Jan,2020)
- Oracle Cloud Infrastructure Foundations 2020 Certified Associate, Oracle (Jul,2020)
- Microsoft Certified: AZ-900, Microsoft (Oct,2020)
- Microsoft Certified: Security, Compliance, and Identity Fundamentals SC-900 (Apr,2022)
- CNSS Certified Network Security Specialist, ICSI UK (May,2020)
- CEHv10, EC-Council(Nov,2019)

AWARDS / RECOGNITIONS

- Nominated as a Beta tester for Nokia smartphones by Nokia (Jan,2019).
- Awarded Aujas ACE award for commitment and dedication in project contribution (2020,2021,2022,2023,2024)
- Was recognized in Aujas Wall of Fame for resolving customer issues(May,2021)
- Awarded CEH Master designation by EC_Council for completing both CEH ANSI and CEH Practical Certification.