Abbu Bakar Siddiq

Cyber Security Analyst

abbubakarsiddiq200111@gmail.com 9535809127 Bengaluru,India Abu Bakar Siddiq

Career Objective

To associate with an innovative and vibrant organization, allowing me to put my competencies to the best use to add value to the organization and contribute to my overall growth as an individual.

Professional Summary

SIEM Tools: Splunk Enterprise and Enterprise Security

- **Vulnerability Management: Nessus**
- **Incident Analysis Tools: CISCO Talos, Mx Toolbox, Virus Total, IBM-Xforce etc.**
- **Ticketing Tool: Service Now**
- **Certification: SIEM XPERT- WORLDSEC TECHNOLOGIES Pvt ltd.**

- **Soc Analyst- intern in 8 months of experience in WORLDSEC TECHNOLOGIES Pvt ltd.**
- **Cyber Security Analyst with proficient and thorough experience and a good understanding of information technology. Specialized in proactive network monitoring of SIEM**
- **Good understanding of security solutions like Anti-virus, Firewall, IPS/IDS, Email Gateway, Proxy etc.**
- **Hands on experience with Splunk SIEM tool for logs monitoring and analysis, using Service Now ticketing tool for incidents response**
- **Good knowledge on networking concepts including OSI Model, Subnetting, TCP/IP, ports, DNS, DHCP etc.**

LANGUAGES

English
Kannada
Hindi

CERTIFICATES

SIEM-XPERT WORLDSEC TECHNOLOGIES Pvt ltd.

Organizational Experience

Soc Analyst - JUN 2024 - Till date in WORLDSEC TECHNOLOGIES Pvt ltd as

Job Responsibilities:

- **Working in a 24x7 Security Operations Center**
- **Monitoring the customer network using Splunk SIEM**
- **Analyzing Realtime security incidents and checking whether its true positive or false positive**
- **Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.**
- **Raising true positive incidents to the respective team for further action**
- **Creating tickets on service now and assigning it to the respective team and taking the follow-up until closer**
- **Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.**
- **Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks.**
- **Work closely with business units to ensure that they know what and how to feed data into the SIEM**
- **Co-ordinate with networking teams to maintain and establish communication to remote ArcSight Connectors**
- **Investigate malicious phishing emails, domains, and IPs using Open-Source tools and recommend proper blocking based on analysis**
- **Good knowledge of Splunk Distributed cluster Architecture**
- **Detail knowledge of the working functionality of various components of Splunk such as Indexer, Search head, Heavy forwarder, deployment server etc.**
- **Experience in onboarding of data sources with Splunk such as Windows, Linux, Fortinet Firewall etc.**
- **Installing Splunk apps and Addon on the Splunk**
- **Experience in installation of Universal forwarder on the servers for logs collection**
- **Responsible for upgrading the Forwarders to the newer versions**
- **Doing the troubleshooting incase any device is not reporting to the Splunk**
- **Knowledge of Creating dashboard, Reports in Splunk**
- **Knowledge and experience in creating Correlation Searches/Rules in Splunk**

EDUCATION

: Bca at Davangere University, 2024 Aug

: CGPA: 7.2 / 10 , 72%