ABUL FAZAL SAJU

Cyber Security Analyst

CONTACT

abulfazal.s@outlook.com

+971 505053710

Dubai, UAE

LinkedIn

https://www.linkedin.com/in/abul-fazal-saju-a6180b42/

Key Skills

- Security Incident Handling and Response
- Forensic Analysis
- SIEM, EDR Administration
- Soar Playbooks
- MITRE ATT&CK Framework
- Anti DDOS Protection
- Vulnerability Assessment
- Intrusion Detection and Prevention
- Cyber Threat Intelligence
- Log Analysis
- Cloud security

Solutions

- **SIEM** – Sentinel, Qradar, Splunk, ArcSight.
- **EDR/XDR** -Microsoft Defender, Symantec, Carbon Black, Trend Micro.
- **Soar** – Cortex XSOAR
- **Threat Intelligence** – Eclectic IQ, Cyware
- **Mail Gateway** – Symantec, McAfee
- **Firewall** – Palo Alto, Fortinet, Cisco
- **Anti DDOS** – Huawei Atic
- **IDS** – Fortinet, Trend Micro
- **DLP** – Force Point.
- **Ticketing** - HPSM, Manage Engine.

Profile

Cyber Security Professional with 13 years of experience in cyber security incident handling and response. Skilled in Various security tools like SIEM, SOAR, EDR, Cloud security. Experience in SOC Processes Development and Security Incident Management, Cyber Threat Intelligence, Cyber Threat Hunting, SOAR Automation for CSOC to build for Cyber Security as Service to various regional customer.

Education & Certifications

- **B. Tech** in Computer Science & Engineering - Cochin University, Kerala 2012
- CEH – EC Council
- IBM Cyber Security Analyst
- Cortex XSoar Administrator
- Microsoft Certified: Azure Security Engineer Associate (Az-500)
- Microsoft Certified: Security Operations Analyst Associate (SC-200)
- Microsoft Certified: Azure Fundamentals (Az-900)
- ITIL V4 Foundations
- VMware Carbon Black App Control Administrator
- CCNA (Routing & Switching)

Experience

Cyber Security Analyst

EITC (Du Telecom) – Dubai, UAE

March 2021 - Present

- Handling Critical and Major incidents and create detailed Incident report with preventive measures.
- Managing and Administration of Qradar, Azure Sentinel.
- Integration of log sources with IBM Qradar, Splunk (Onboarding Customers) and parsing.
- Conduct in depth analysis of cyber threats including malware, phishing campaigns, APT actors and other cyber-attack techniques, identify patterns to ensure optimum incident resolution including the ownership of escalated incidents.
- Analysis and Mitigation for DDoS attacks with appropriate counter measures.
- Creating Use cases, playbooks, reports, dashboards in SIEM, SOAR.
- Managing and Administration of Qradar, Azure Sentinel.
- Monitor, Collect and analyze threat intel feeds from various sources and other open feeds and publish reports with threat mitigation recommendation.
- Create/Review Security Standard Operating Procedures (SOPs)
- Actively investigating/preparing the latest security, vulnerabilities, advisories, incidents notify to the clients
- Review weekly, monthly report and present to the clients.
- Identify improvements in automation, investigation procedures and adhere to SLAs for security investigations.

Senior SOC Analyst

Alpha Data Abu Dhabi, UAE
April 2020 - March 2021

- Perform deep Analysis of security events/devices logs using SIEM Tool.
- Configuring, fine tuning and creating new use cases as per client requirements.
- Analysis to identify the origin of threats, initiation of measures to prevent recurrence.
- Revising and enhancing the SIEM configuration and contents as per the best practices.
- Preparing Soc Monthly, Weekly, Daily reports.
- Perform on-going optimization, configure additional use-cases, suggest improvements as a continuous process.
- Creating new SOP, Generating Reports, Managing backup plans, Daily Health Check-ups etc.
- Monitoring threats across all network endpoints using Symantec EDR.
- Investigate and remediate threats/malicious activities.
- Monitoring and fine-tuning Symantec Email Gateway.
- Real time monitoring and log analysis using Symantec Endpoint Protection.
- Provide support to data protection programs, including insider threat Management and Data Loss Prevention (DLP).

SOC Analyst

Elitser Technologies – Abu Dhabi, UAE
March 2018- March 2020

- Monitoring and deep analysis of security events/devices logs using SIEM Tool.
- Recognize potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information.
- Review and Analyze the security breaches and determine their root cause and respond in the timely manner and coordinate with the L3's for the remedies on the escalated incidents.
- Creating Reports, Filters, Dashboard, AQL Queries etc.
- Monitoring local traffic rates, CPU, Memory, Threats, Attacks etc. and informing corresponding Team.
- Configuring on demand scan on client machines using **Symantec Endpoint Manger**
- Ensure the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of vulnerability scanning devices.
- Annotating security alerts, Raising tickets with SLA.
- Blocking/unblocking phishing URLs and thorough analysis of websites.
- Updating new signatures and engines for client machines.
- Monitoring top dashboards, finding out major threat events and informing users.
- Active monitoring network and server health using **Nagios Monitoring Tool.**
- Analyzing attacks reported from multiple sources both internal and external.

IT Network Security Engineer

Steel Wood Industries FZCO - Dubai-UAE.
Oct 2015 - Feb 2018

- Managing Windows Server and AV solutions.
- Managing Cisco ASA Firewall, VPN Connectivity's and Security Appliances.
- Monitoring HP Network monitoring tool.
- Primary level configuration in cisco router, Cisco ASA and Catalyst switches.
- Perform regular backup of network devices and daily health check-ups.
- Creating network infrastructure using Microsoft Visio.
- Managing Active Directory Domain Services, DNS, Group Policy, Hyper V, DHCP Server, WDS, WSUS.
- Creating virtualization client for virtual machines, snapshot, restoring.
- Managing AVAYA IP Phones, Network Printers and Scanners.
- Configuring on demand scan on client machines, Updating new signatures and engines for client machines.
- Analyze, test and apply Microsoft Windows server service patches and hotfixes.

IT Security Engineer

Mind Media Innovations Pvt Ltd -Kerala, India
June 2012 - June 2015

- Monitoring and deep analysis of security events/devices logs using ArcSight SIEM Tool.
- Perform L1 analysis of incident/Events.
- Perform analysis on quarantined mails in email gateway for enhancements of rules.
- Monitoring local traffic rates, CPU, Memory, Threats, Attacks etc. and informing corresponding Team.
- Monitor, Analyze and security issues and vulnerability. Initiate escalation procedure to counteract potential threats.
- Determine the cause of security incidents and take corrective measures to resolve the issues. Monitoring the email gateway.
- Network and Log Analysis.
- Updating new EDR signatures and engines for client machines.

Personal Details

Nationality – Indian
Languages Known – English, Malayalam, Tamil and Hindi

Reference

Available upon request.