MOHAMMAD HASSAN

Cyber Security Analyst

CONTACT

azmihassan55@gmail.com

+971 561819518

Dubai, UAE

Key Skills

- **SIEM** - Q-radar, Sentinel, Splunk.
- **SOAR** – Cortex X-SOAR.
- **EDR & AV** - Symantec, Trend Micro.
- **Mail Gateway** – Symantec.
- **Threat Intelligence** – Eclectic IQ.
- **Anti DDOS** – Huawei ATIC.
- **DLP** – Force Point.
- Security Incident Handling and Response.
- MITRE ATT &CK Framework
- Intrusion Detection and Prevention
- Content/Playbook Management
- Security Automation

Profile

Cyber Security Professional with 7+ years of experience in cyber security operation and center. Skilled in Various security tools like SIEM, SOAR, EDR etc. 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.E** in Computer Science & Engineering - RGPV University
- CEH – EC Council
- IBM Cyber Security Analyst
- Cortex X-Soar: Analyst
- Chronicle Certified SOAR Analyst
- Microsoft Certified: Security Operations Analyst Associate (SC-200)
- Microsoft Certified: Azure Fundamentals (AZ-900)
- ITIL V4 Foundations
- CCNA (R&S)

Experience

Cyber Security Analyst

EITC (Du Telecom) – Dubai, UAE

August 2021 – Present

- Conduct triage and analysis of security incidents to resolve or escalate for further investigation.
- Utilized Palo Alto Cortex XSOAR to design, implement, and optimize security automation workflows.
- Integrated security tools and system with Cortex SOAR Platform to create efficient incident responses.
- Develop and customize playbooks to automate repetitive tasks, reducing manual intervention and improving efficiency.
- Configuring, fine tuning and creating new rules in SIEM as per client requirements.
- Implemented the threat intelligence management playbook which basically performs enriching indicators, adding IOC's to SIEM or external dynamic lists (EDL) and custom requirements.
- Actively investigating/preparing the latest security, vulnerabilities, advisories, incidents notify to the clients.
- Analysis and Mitigation for DDoS attacks with appropriate counter measures.

- Create/Review Security Standard Operating Procedures (SOPs).
- Review weekly, monthly report and present to the clients.
- Perform upgradation and patching of security appliances.

SOC Analyst

Alpha Data Abu Dhabi, UAE
Jan 2020 - July 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

Media Nucleus India Pvt. Ltd. – Mumbai, India
Dec 2016 - Oct 2019

- 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.
- 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.
- 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.

Personal Details

Nationality – Indian
Languages Known – English and Hindi.

Reference

Available upon request.