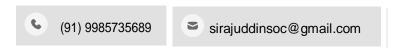
Sirajuddin Mohammed

Cyber Security Analyst



CAREER OBJECTIVE

As a Security Analyst, I managed escalations reported through monitoring tools, including Splunk as a SIEM, collaborating with Physical Security, Network Teams, L1 Analysts, and customers. Leveraging IDS/IPS and AV, EDR, & XDR solutions for network monitoring, I handled over 200 tickets weekly, enhancing operational efficiency by 25%.

By proactively monitoring IOCs and blocking malicious traffic, I ensured efficient containment of security incidents. My role encompassed threat analysis, system monitoring, incident response, team collaboration, and customer support.

WORK EXPERIENCE

BlueVolerum Solutions Inc.

Systems Security Analyst

Oct 2023 - Dec 2024

- Collaborate with existing Security Operations Center (SOC) provider to support investigation of escalated threats. Provide on-call support on a scheduled rotation with existing cyber security team.
- Analyze and investigate escalated security incidents, determine their impact, and take necessary containment and remediation actions.
- Proactively identify threats by analyzing network traffic, endpoint logs, and security alerts to detect advanced persistent threats (APTs).
- Leverage threat intelligence sources (MITRE ATT&CK, VirusTotal, Open Threat Exchange) to enhance threat detection and response strategies.
- Assist in conducting security awareness sessions, educating employees on phishing attacks, social engineering, and cybersecurity best practices.

SYNCHRONY INTERNATIONAL SERVICES

Threat Detection and Response Analyst

July 2018 – Sept 2023

- Responsible for monitoring, detecting, investigating, and responding to cybersecurity threats and incidents to protect an organization's IT infrastructure and data..
- Manage security incidents, carry out forensic investigations, and formulate incident response strategies.
- Analyze malware in suspicious files identified by antivirus software and perform sandbox testing when necessary.
- Track and analyze user behavior, including actions like executed processes, location shifts, failed logins, privileged process execution, and TOR IP address interactions.

- Regularly monitoring of network and systems for possible security threats, utilizing tools such as SIEM to identify suspicious activity in real-time.
- Monitor Remote Phishing and Customer Mailboxes for malicious phishing links, analyze spam emails, and log incidents into the ticketing system if any threats are detected on the network.
- Proactively identify malicious websites from daily IDS event logs and block these sites on proxies to prevent further virus downloads if accessed by users.
- Analyze security events and alerts to determine the severity of incidents and provide actionable insights for further action or investigation.

EDUCATION

Master In Business Administration Bachelor of Computer Application

SKILLS & TOOLS

Vulnerability Assessment			Process Improvements		Log Analysis		c Cloud	DFIR
SIEM Administration E		Basic	Basic Pen testing Knowledge		Incident Response		Email Security	
SIEM Monitoring		Exabeam AWS Cloud Securit		curity	CrowdStr	ike EDR	& XDR	Qradar
Akamai WAF	Servi	iceNow	OWASP- Web Application		n Security DLP		Proof Point DLP	
Proof Point TA	P,	Windows	AWS					

TRAINING AND CERTIFICATIONS

CompTIA Security+ | CompTIA Splunk Certified User | Splunk ITIL Foundation Level | EXIN CISM- Certified Information Security Manager | ISACA

Certified Ethical Hacker (CEH) | EC-Council

AZ-900 - Azure Fundamentals | Microsoft

Amazon Web Services Cloud Practitioner | Amazon Web Services (AWS)

Microsoft Certified Systems Engineer (MCSE) | Microsoft

Akamai Kona Site Defender & Bot Manager Foundations | Akamai University

Qualys Certified Specialist - Vulnerability Management certified | Qualys