Jayanthsai.Dhanapuram

jayanthsaidhanapuram@gmail.com|91-9493629715

Objective

SOC Analyst with over 3.5 years of expertise in cybersecurity who is results-driven and highly trained. competent in doing technical analysis, spearheading incident response initiatives, and tracking and reducing risks to IT infrastructure. In search of a demanding role as SOC Analyst where I can apply my knowledge of threat detection, incident management, and security technologies to improve an organization's cybersecurity posture.

Professional Experience

- 3.5 years of experience in Security Operations Center with expertise in SIEM tools including Azure Sentinel, Elastic & hands-on experience on Splunk.
- Extensive knowledge of security methodologies, procedures, and technical solutions, encompassing firewalls, intrusion detection/prevention systems, endpoint security, and email security.
- In-depth understanding of security vulnerabilities, risks, and threats.
- Skilled in analyzing emails and malware, along with incident management, reporting, and alerting.
- Proficient in network security, including TCP/IP protocols and network security applications, with a strong foundation in network capture analysis tools and protocols.
- Knowledgeable in Windows and Linux OS environments, particularly in event logging and security monitoring.
- Experienced in analyzing security incidents, assessing risk levels, and coordinating responses effectively.
- Demonstrated interpersonal, coordination, and communication skills, facilitating effective collaboration across teams.
- Strong grasp of networking and application security principles, with hands-on technical expertise in malware analysis, incident response, and threat detection.
- Adept at providing technical analysis and insights in collaboration with internal stakeholders and customer teams to enhance security postures.
- Proficient in implementing automated workflows within SOAR platforms to streamline repetitive security tasks and reduce response times.
- Skilled in leveraging SOAR tools for real-time threat detection, investigation, and incident response.
- Experienced in designing and implementing custom playbooks to handle security incidents like phishing, malware analysis, and vulnerability patching.
- Adept at integrating SOAR solutions with various security tools such as SIEMs, firewalls, and endpoint protection systems for enhanced threat visibility.
- Hands-on experience in managing and resolving security incidents using SOAR platforms, ensuring minimal business impact.

Professional Qualification

- Bachelor’s from Acharya Nagarjuna University - 2020

Technical Skills

- **Cybersecurity SIEM** : Azure Sentinel, IBM QRadar, Splunk
- **Remote Monitoring** : Datto RMM & N-Sight
- **Endpoint Security** : SentinelOne, Microsoft 365 defender.
- **Vulnerability Tools** : Nessus
- **Security Skills** : Cyber Kill Chain, Incident Response Lifecycle
- **Ticketing Tools** : Jira, Servicenow
- **Operating Systems** : Windows Server, Linux
- **Other Monitoring Tools** : VirusTotal, AbuseIPDB, IP Void, URL Void, Hybrid Analysis

Work Experience

- Organization : Relay Human cloud private limited.
- Role : SOC Analyst
- Experience : 1+ year (February 2024 To March 2025)

Responsibilities

- Proficient in using Azure Sentinel to gather and analyze security logs from a variety of sources, including Azure Active Directory, Security Events, AWS, Office 365, and syslog, along with on-premises environments utilizing Proofpoint.
- Experienced in investigating alerts to detect malicious activities within Azure Sentinel SIEM, employing tools such as VirusTotal, AbuseIPDB, IP Void, URL Void, URL Scan, MX Tool, and Hybrid-Analysis.
- Capable of designing alerts customized to align with business needs.
- Skilled in conducting cyber threat intelligence operations, which encompass gathering IOCs, tracking threat actors, and monitoring potentially harmful infrastructure.
- Able to manage project activities autonomously as well as collaboratively within a team environment.
- Experienced in an Offshore SOC team, focusing on monitoring SOC events and preventing intrusion attempts.
- Adept at collecting and analyzing logs from network devices to identify unusual activities.
- Proficient in incident response for cybersecurity, including event analysis and investigations, validating SIEM reports, collaborating with team members to resolve incidents, determine root causes, and implement preventive actions within set SLAs.

Work Experience

- Organization : Accenture.
- Role : SOC Analyst
- Experience : 2 Years (January 2022 To January 2024)

Responsibilities

- Utilized Elastic SIEM for log collection and analysis, creating custom queries and dashboards to enhance incident detection.
- Managed remote monitoring with Datto and N-Sight, responding to alerts to prevent critical issues.
- Configured and managed SentinelOne as an EDR solution, analyzing alerts and conducting proactive threat hunting.
- Performed regular vulnerability assessments using Qualys, collaborating with IT teams to prioritize and remediate security weaknesses.
- Performed R&D project on Zabbix, Snort & suricata designing a monitoring solution to improve system performance tracking.
- Oversaw the deployment of SentinelOne and Elastic agents, providing training to IT staff on management and troubleshooting.
- Actively participated in the incident response lifecycle, maintaining detailed reports and coordinating with external partners as needed.
- Fostered collaboration across teams, delivering regular updates to management on security initiatives and incidents.
- Prepare weekly and monthly reports summarizing security events, incident trends, key performance indicators (KPIs), and notable findings for management, stakeholders, and regulatory compliance purposes.
- Generate firewall reports using SIEM tools like Elastic to review and analyze firewall logs, rule violations, traffic patterns, and access control lists (ACLs) for compliance, security policy enforcement, and anomaly detection.
- Contributed to the development of security policies and procedures to enhance the organization's security posture.
- Stayed updated on industry trends and participated in security drills to improve incident response capabilities.

Certifications

- Fortinet: NSE 1 and NSE 2 Certifications
- Cisco Network Academy
- TryHackMe L1 & L2
- Fortinet Certified Associate

- FCF Cybersecurity
- Elastic Fundamentals

Languages Known

- English
- Telugu
- Kannada
- Hindi

Conclusion

Motivated cybersecurity professional with experience in security operations and incident response. Eager to leverage my skills in a dynamic organization focused on enhancing security.

Jayanth sai.Dhanapuram