JAYASRI DEVARAKONDA

Cyber Security Analyst

📱 9515120044 | ✉ js9148395@gmail.com

Professional Summary

Experienced and detail-oriented professional with a strong background in Security Information and Event Management (SIEM) administration, architecture, and troubleshooting. Proficient in utilizing tools such as Qradar and Splunk to create playbooks, automate processes, and ensure the efficient operation of SOC tools. Skilled in building parsers, creating custom profiles, and fine-tuning use cases and rules to enhance threat detection capabilities. Strong communicator with a commitment to maintaining the integrity and confidentiality of sensitive information.

Experience

Accenture

Hyderabad

Cyber Security Analyst

09/2021 - Present

- Led network traffic analysis efforts to identify compromised systems, mitigate denial of service attacks, and detect resource abuse. Utilized advanced tools and techniques to monitor network traffic and identify anomalous behavior indicative of security threats.
- Integrated threat intelligence feeds into Microsoft Sentinel, enhancing threat detection and response capabilities. Incorporated external threat intelligence sources to enrich security monitoring and improve the organization's ability to identify and respond to emerging threats.
- Developed and implemented security automation scripts and playbooks in Microsoft Sentinel to streamline security operations. Automated repetitive tasks and standardized incident response procedures, resulting in increased efficiency and reduced response times.
- Created comprehensive reports and documentation related to security incidents, investigations, and overall security posture. Ensured accurate and timely reporting of security incidents to stakeholders, enabling informed decision-making and proactive risk management.
- Provided expert support for priority incident investigations and threat intelligence discoveries, leveraging hunting expertise to identify the extent of potential compromises. Collaborated with cross-functional teams to contain, eradicate, and recover from security incidents using Microsoft Defender's tools and features.
- Educated users and colleagues about cybersecurity best practices and the use of Microsoft Defender. Conducted training sessions and workshops to increase awareness of security threats and promote a culture of security awareness within the organization.
- Conducted investigations using Endpoint Detection and Response (EDR) tools and live response techniques. Identified and analyzed security issues, documented findings, and reported on incident response activities to contribute to continuous improvement efforts.
- Monitored the threat and vulnerability landscape, staying informed about security advisories and emerging trends. Proactively identified potential threats and vulnerabilities, taking appropriate action to mitigate risks and protect the organization's assets.
- Collaborated closely with technical, vulnerability management, incident management, intelligence analyst, and forensic personnel to develop a comprehensive understanding of cyber threat actors and improve the organization's overall security posture.
- Notified appropriate business stakeholders about serious security events, implemented security improvements based on assessment and market trends, and contributed to incident response efforts by investigating, documenting, and reporting all security issues.
- Demonstrated advanced knowledge of Qradar and Splunk SIEM platforms, including architecture and configuration. Utilized expertise to create SIEM playbooks and automate security processes, improving efficiency and response times.
- Conducted thorough audits of SIEM deployments in customer environments, ensuring compliance with security standards and best practices.
- Built parsers for SIEM using regex and DSM validation techniques, creating custom profiles as needed to optimize log parsing and analysis.
- Developed and fine-tuned SIEM use cases and rules to enhance threat detection capabilities, troubleshooting issues with SIEM and other SOC tools as they arise.
- Managed the onboarding of log sources to SIEM monitoring, resolving issues with non-reporting devices to maintain optimal device reporting status.
- Proficient in traditional log search methods and AQL (Advanced Query Language), capable of hunting for threats by monitoring logs from various sources.
-

Possessed extensive experience in SIEM administration and event flow architecture, managing different types of logs generated by devices such as Windows, proxies, network devices, databases, and applications.

- Ensured the health of SOC tools remained in optimal condition, resolving internal incident tickets and vendor tickets for SOC tools promptly.
- Provided assistance to L2 and L1 teams with required knowledge base details and basic documentation, coordinating with SOC monitoring teams to troubleshoot issues and escalate as needed.
- Maintained high ethical standards and protected confidential information, troubleshooting anomalies reported by other teams and building incident reports and advisories.
- Updated and maintained the SOC knowledge base for new security incidents and documentation, created daily status report sheets for review by SOC managers.
- Reviewed advisories and made necessary detection measures, provided analysis and trending of security log data from a large number of security devices.

Mold Tek technologies

Hyderabad

IT Support Specialist

08/2010 - 09/2021

- Responded to requests for IT assistance directly from corporate and field users, addressing issues promptly and effectively to minimize disruption to workflow.
- Troubleshot and resolved escalated issues from the Service Desk, providing advanced technical support and guidance to resolve complex IT issues.
- Provided escalated support for Tech:Bar, assisting users with hardware and software issues in person and ensuring timely resolution of technical problems.
- Assisted with call support as dictated by volume or need, maintaining a flexible approach to meet the demands of IT support services.
- Delivered onsite support for local buildings and customers, including desk visits, printer troubleshooting, meeting support, and audit support, ensuring optimal functionality of IT resources.
- Provided remote support using a flexible schedule when not onsite, addressing technical issues remotely to maintain uninterrupted IT services.
- Managed IT request tickets in a Service Management System, ensuring compliance with IT department processes and timely resolution of user inquiries and issues.
- Installed business-supported applications using IT software distribution technologies, ensuring proper configuration and compatibility with user systems.
- Addressed network services and related issues such as port configuration and IP Phone configuration as needed, ensuring smooth operation of network infrastructure.
- Resolved identified security issues as required, taking proactive measures to mitigate security risks and safeguard corporate systems and data.

Education

Nagarjuna University, K.L.C

Vijayawada

B.Tech

06/2005 - 05/2009

Tools

- SIEM: **Azure Sentinel, Alien vault, Qradar, Splunk**
- EDR: **Carbon Black, falcon crowdstrike, defender for endpoint, Cybereason**
- Phishing Email Analysis, &**Digital Guardian (USB and Print Logs).**
- VMT: **Qualys, Nessus**
- Anti-Virus tools: **Trendmicro, (McAfee preferred) Device management.**
- Email gateway: **Mimecast, Proofpoint, Cofense, Iron Port, 0365**
- Cloud: **AWS, Azure**
- Firewall: **Cisco, Palo Alto**
- Ticketing Tools: **Trend Micro, ServiceNow.**
- Other Tools:**IDS, IPS, DLP**

Technical Skills

- **SIEM Administration (Qradar, Splunk):** Proficient in the administration of Security Information and Event Management (SIEM) systems, specifically Qradar and Splunk. This includes configuration, maintenance, and optimization to ensure effective threat detection and response capabilities.
- **Playbook Creation and Automation:** Experienced in developing SIEM playbooks and automating repetitive tasks to streamline incident response processes. This involves creating standardized procedures and automated workflows for common security incidents.
- **SIEM Audit and Troubleshooting:** Skilled in conducting audits of SIEM systems in customer environments to ensure compliance with security policies and standards. Capable of identifying and resolving issues, troubleshooting errors, and optimizing SIEM performance.
- **Log Source Onboarding and Management:** Proficient in onboarding new log sources to SIEM monitoring, configuring log collection, and managing log sources effectively. This includes troubleshooting non-reporting devices to maintain a consistent flow of log data.
- **Incident Response and Ticket Resolution:** Experienced in responding to security incidents, managing incident tickets, and resolving issues in a timely manner. This involves collaborating with internal teams and external vendors to address security threats and ensure prompt incident resolution.
- **Threat Analysis and Trending:** Skilled in analyzing security log data from various sources to identify and assess potential security threats. Capable of detecting patterns and trends in security incidents, conducting threat intelligence research, and proactively mitigating emerging threats.
- **Change Management and Documentation:** Proficient in raising change management tickets for SOC administration activities, such as patch upgrades and log source onboarding. Experienced in maintaining documentation and knowledge base materials to support SOC operations and facilitate knowledge sharing.
- **MITRE Tactics and Techniques:** Knowledgeable about MITRE ATT&CK framework, including common tactics and techniques used by adversaries during cyber attacks. Capable of leveraging this knowledge to enhance threat detection capabilities and improve incident response processes.

Declaration

I hereby Jayasri declare that the above-mentioned information is correct up to my knowledge and I bear that responsibility for the correctness of the above-mentioned.

(Jayasri)