Sridevi P

Bengaluru, India | +91 9346813363 | pedapati.sridevi98@gmail.com

Summary

Cybersecurity professional with 4.8 years of experience in threat analysis, incident response, and vulnerability management. Adept at implementing security protocols, conducting risk assessments, and ensuring compliance with industry standards. Strong problem-solving skills and focus on maintaining secure and stable IT environments.

Skills

- Endpoint Security – MS Defender 365
- Cloud Security- Azure Sentinel
- Incident Response - ServiceNow
- Email Security – Office 365
- Antivirus - McAfee ePO
- Vulnerability Management - Rapid7
- SIEM - Splunk ES
- IDS, IPS alert investigation
- Windows Server management
- WAF, MCAS
- DLP - MS Purview
- MS Intune Administrator

Experience

SECURITY ANALYST | 09/2020 - Current

DSV Logistics (Adrola software Technologies) - Hyderabad, India

- Experience in a 24/7 SOC environment, as part of a team or independently, to analyse alerts and log data promptly and effectively. Assess the severity and impact of potential threats to accurately prioritise alerts and incidents.
- Experience in maintaining the team and hiring members, providing services to stakeholders, and attending daily calls with clients.
- Monitor and analyse security information and event management (SIEM) tools, and other security monitoring systems to identify potential security incidents and anomalies.
- Conduct in-depth analysis of security events, collaborating directly with customers to escalate and thoroughly investigate incidents.
- This involves understanding the scope, impact, and root cause of incidents to tailor the response effectively.
- Execute swift containment and remediation measures for identified security incidents, employing predefined response strategies to isolate affected systems and prevent further compromise.
- Proactively participate in the creation and enhancement of processes and procedures, such as Security Playbooks.
- Expertise in Splunk enterprise architecture such as search heads, indexers, deployment server, licence master, and heavy or universal forwarders.
- Good knowledge of troubleshooting the MDE agent connectivity using the MDE client analyser files.
- Experience in creating log analytic workspaces and policies in Azure Sentinel, with good hands-on experience in creating automation rules to auto-close incidents.
- Perform health checks for AV infrastructure and distribute reports regularly.
- Experience in analysing advanced system-based threats using EDR Defender for Endpoint.
- Experience in monitoring, responding to, and analysing trends in workstations, servers, and security-related events. Perform daily, weekly, and monthly scheduled tasks for MS 365 Defender.
- Monitor, respond to, and analyse trends in workstations and servers for security-related events. Perform daily, weekly, and monthly scheduled tasks for Microsoft 365 Defender.
- Implementation of use cases using KQL, with complex correlation across different data sources in Azure Sentinel and Defender 365.

- Experience in handling technical administration and troubleshooting activities related to the M365 Defender suite.
- Experience in creating, tracking, and responding to support cases raised with Defender ATP Support.
- Experience in managing the DLP agents' installations on servers, and the creation of use cases to monitor alerts by using Microsoft Purview.
- Responding to in-house queries and guiding users with threat remediation strategies, best security practices, and incident response.
- Experience in adding and deploying a client onboarding configuration file; Configuration Manager can monitor deployment status, and Microsoft Defender ATP agent health.
- Experience in the Rapid7 Vulnerability Management tool to perform vulnerability scanning and reporting.
- Experienced in creating and fine-tuning use cases with respect to KQL and SPL languages.
- Experience in creating runbooks, SOPs, and documents supporting Security Operations.
- Strong experience in managing Endpoint Agents over Windows and Linux operating systems, Active Directory integrations, and Windows Event Logs.
- Experience with system security concepts, tools, implementation, DLP, CASB, and integration with various data sources and application stacks.
- Experience in writing correlation rules and monitoring the Enterprise Security Application.
- Experience in working on host isolation and advanced threat analysis using EDR, MS 365 Defender.
- Prepare Endpoint Compliance reports and initiate the remediation activities wherever required.
- Experience in configuring the ServiceNow ticketing tool with Defender and Splunk to automatically create a ticket in ServiceNow for work notes, and to maintain records.
- Experienced in creating runbooks and playbooks using Logic Apps in Azure Sentinel.
- Strong knowledge and working experience with Office 365 email gateway solutions; completely own, manage, monitor, and administer the email security stack and policies for both on-premises and cloud environments, which include Office 365 email security solutions.
- Experienced in creating PIM roles and managing the RBAC roles using Sentinel.
- Investigating suspicious mail and taking necessary actions, such as blocking IPs, URLs, sources, and the sender's mail ID by coordinating with different teams.
- Experience in handling and creating AWS workspaces, deploying ISO files, and onboarding them into Defender 365.
- Providing threat and vulnerability analysis, security logs from a large number of security devices, and investigating incident response support when there is a threat.
- Investigating and monitoring network traffic, IDS, firewall, and endpoint security logs using IBM QRadar and Splunk. Insider threat and APT detection, or understanding and differentiation of intrusion attempts and false alarms.
- Good hands-on experience in the integration of AWS and Azure security, implementing policies, and fine-tuning the rules.
- Performed folder exclusion policies, other device-based policies, and tags in Defender for Endpoint.
- Good knowledge of MITRE ATT&CK, the diamond model, and other cyber threat kill chains.
- Strong knowledge and working experience of Office 365 Email gateway solutions, completely owning, managing, monitoring, and administering the email security stack and policies for both on-premises and cloud environments, which include Office 365 Email security solutions.
- In-depth understanding of the latest techniques used by attackers for persistence, privilege escalation, defence evasion, and lateral movement.
- Experience in configuring and tuning ASR policies in the Microsoft 365 Defender portal.
- Good experience in ticketing tools (ServiceNow, Jira).
- Creating custom detection rules using KQL language in Defender ATP.
- Monitor, respond to, and analyse trends in workstations, servers, and security-related events. Perform daily, weekly, and monthly scheduled tasks for Defender ATP.
- Analysis of phishing emails reported by users to identify the type of attack and take immediate remediation.
- Strong experience in managing Endpoint Agents over Windows and Linux operating systems, Active Directory integrations, and Windows Event Logs.

Certifications

- SC -200 MS security operational analyst.

- AZ900 - Azure fundamentals
- Splunk power user.
- MD 101- MS Intune administrator

Education

Kakinada Institute of Engineering and Technology - Kakinada, AP | B.Tech
C.S.E, 2020