P Venkatesh

Bengaluru, India
+91-9550989937
pvenkateshwara225@gmail.com

Personal Summary

Experienced Information Security Engineer with 4.5 years of expertise in incident response, digital forensics, and malware analysis. Adept at leading and managing investigations, identifying and mitigating security threats, and fortifying systems against cyber attacks. Skilled in collaborating with executive leadership to develop and implement robust security strategies that enhance organizational resilience.

Skills

- Endpoint Security: MS Defender 365, CrowdStrike Falcon
- SIEM: Splunk [ES], QRadar
- SOAR: Azure Sentinel
- Antivirus: Symantec
- Email Security: Office 365, Proof Point
- AWS Cloud Security
- Incident Response: ServiceNow, Auto Task
- Windows Server Management
- MS Intune Administrator
- Vulnerability Management: Rapid 7

Work History

TCS March 2021 to Current

Security Engineer

Bengaluru, India

- Expertise in Splunk enterprise architecture such as search heads, indexers, deployment server, licence master, and heavy/universal forwarders.
- Provides regular monitoring, triage, and incident response to automated security alerts using security tools like SIEM, Splunk, and Azure Sentinel. EDR, antivirus, and email security.
- 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 Defender ATP.
- Implementation of use cases using KQL with complex correlation across different data sources in Azure Sentinel.
- Hands-on experience in analysing phishing emails and malware emails, performing soft deletes and hard deletes of malicious emails from the email cluster, and adding indicators to the tenant allow list, block list, and based on analysing the IOCs.
- Knowledge of Group Policy Objects, Active Directory security and compliance configurations, and migrating to the Intune administrator console.
- Experienced in examining suspicious emails for malicious content and providing recommendations on remediation actions using Office 365.
- Experience in running policies and software deployment in antivirus, anti-malware, and endpoint detection and response solutions.
- Handling spam and phishing email submissions from end-users, taking containment steps by further investigating domains and IPs to recommend proper blocking, and creating SPF, DKIM, and DMARC records for the domains to protect against spoofing.
- Experience in handling and deploying the Defender agents onto servers to onboard into Defender, and troubleshooting agent connectivity issues using the MDE Client Analyser.
- Experienced in creating conditional access policies and fine-tuning the ASR rules in Defender 365 and in Intune.
- Escalating security incidents based on the client's SLA and providing meaningful information related to security incidents by conducting an in-depth analysis of events, which makes the customer's business safe and secure.
- Performed root cause analysis for the incidents reported at the security operations centre.
- Experience in working on host isolation and advanced threat analysis using EDR, Microsoft

Defender ATP.

- Experience in creating group policies and initiating remote wipe-outs on end devices by using the Intune administrator console.
- Implemented conditional access policies and integrated Intune with Azure Active Directory for enhanced security and user authentication.
- Configured and optimised Microsoft Defender for Endpoint to enhance protection against malware, ransomware, and advanced threats.
- Implemented security policies and automated remediation processes using Microsoft Defender across enterprise environments.
- Hands-on experience in creating playbooks, notebooks, runbooks, and in creating automation roles using Azure Sentinel.
- Experience in creating Log Analytics workspaces, creating conditional access policies, and detection rules using Defender 365 and Azure Sentinel.
- Creating and fine-tuning use cases and custom detection rules by using the SPL and KQL languages in Defender and Splunk portals.
- Good hands-on experience in creating virtual machines, deploying endpoint agents on them, and managing IAM roles in an AWS environment.
- Knowledge of Group Policy Objects, Active Directory security and compliance configurations, and migrating to the Intune administrator console.
- Expertise in using SOAR technologies such as Logic Apps, implementing playbooks, and creating automation rules using Microsoft Sentinel SOAR.
- Monitoring, analysing, and responding to infrastructure threats, vulnerabilities, and risks. Collecting the logs of all the Windows, Linux, and network devices and analysing the logs to find suspicious activities.
- Taking the appropriate action based on advisories, IOCs, identifying threat actors using Mitre ATT&CK, and coordinating with the respective team to block the IOCs.
- Experience in handling and deploying the Defender agents onto servers to onboard into Defender, and troubleshooting agent connectivity issues using the MDE Client Analyser.
- Good hands-on experience in managing the P1 bridge call, involving the stakeholders, and experience in creating the incident response report for critical incidents.
- Experience in AIR (Automated Investigations and Remediation) policies and their implementation.
- Configure and manage dashboards, notebooks, data connectors, and playbooks in Azure Sentinel. Hunt security threats using Azure Sentinel.
- Good knowledge in analysing different malicious executables and documents. Good understanding of Azure Active Directory, Azure MFA, and conditional access.
- Experience in supporting, fine-tuning, and troubleshooting correlation searches in Splunk SIEM.
- Good hands-on experience in creating the SOPs, playbooks, and runbooks using Splunk and Defender, as well as hands-on experience in creating and managing the endpoint health check reports and vulnerability reports to reduce the exposure score.
- Good hands-on experience in providing KT sessions, training, and assigning tasks to juniors.
- Experience in creating and maintaining the daily, weekly, and monthly reports of device health status by using Defender ATP.
- Experience in initiating vulnerability scans on end devices and servers for automated reports using Rapid7.
- Knowledge of Group Policy Objects, Active Directory security and compliance configurations, and migrating to the Intune administrator console.
- Experienced in creating or managing virtual machines, deploying ISO files, and managing snapshots/images.
- Experience with compliance tickets and advisory for the blacklisting of IOCs, and processes using Endpoint Security.
- Conducted investigations on infrastructure through forensic analysis to identify Indicators of Compromise (IoCs).
- Extensive experience working with SIEM, log aggregators, and incident response management solutions.
- Expert in installing and using Splunk apps and add-ons.

- Experience in creating, tracking, and responding to support cases raised with Defender ATP support.
- Experience in providing end-to-end support to enterprise counterparts, identifying the root cause of sophisticated enterprise initiatives, and implementing endpoint security solutions such as Microsoft Defender ATP.

Certifications

- SC200- Security operational analyst.
- SC300- Identity and access management administrator
- AZ900- Azure fundamentals