Bengaluru | +91 9492145188 | venkatjuluri4@gmail.com

VENKAT JULURI

SUMMARY

Security Analyst with around 5 years of expertise in **Mphasis** in incident response and forensics. Skilled at leading investigations, mitigating threats, and securing systems against attacks. Proven ability to collaborate with executives to develop and implement effective security strategies.

SKILLS

- Endpoint Security: Crowd Strike, MS Defender 365.
- SIEM: Splunk [ES], Q-Radar.
- Soar: Azure Sentinel, Google Chronicle
- Antivirus: Symantec
- Vulnerability Management: Rapid 7
- Azure Security Engineer
- DLP : MS purview
- WAF : MCAS
- Email Security: Office 365
- MS Intune Administrator.
- Endpoint security engineer.

CERTIFICATIONS

- Splunk advanced power user.
- Azure Fundamentals AZ900
- SC300 - MS identity and access management administrator
- MD101 - Exploring and managing Modern desktops.

EXPERIENCE

SECURITY ANALYST 08/2020 to Current
Mphasis, Bengaluru

- Good knowledge and working experience in central logging, log management, and Splunk SIEM architecture.
- Experience in writing correlation rules and monitoring Enterprise Security Application.
- In-depth knowledge of endpoint protection (AV, HIPS, and DLP).
- 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 handling and deploying the Defender agents onto servers to onboard into Defender, and troubleshooting agent connectivity issues using the MDE Client Analyzer.
- Expertise in using SOAR technologies such as Logic Apps, implementing playbooks, and creating automation rules using Microsoft Sentinel SOAR.
- Experience in creating the group policies and initiating the remote wipe-outs on the end devices by using the Intune administrator console.
- Knowledge of Group Policy Objects, Active Directory security and compliance configurations, and migrating to the Intune administrator console.
- Strong experience in managing Endpoint Agents over Windows and Linux operating systems, Active Directory integrations, and Windows Event Logs.
- Prepare Endpoint Compliance reports and initiate the remediation activities wherever required.
- Experience in adding and deploying a client onboarding configuration file; Configuration Manager can monitor deployment status, and Microsoft Defender ATP agent health.

- Experience in working on host isolation and advanced threat analysis using the EDR Microsoft Defender ATP.
- Experienced in creating log-analytics rules based on the client's requirements by configuring different data tables using KQL language.
- Experienced in creating various automation rules for closing incidents and alerts to reduce false positives.
- Provides regular monitoring, triage, and incident response to automated security alerts using security tools (such as SIEM, Splunk, and Azure Sentinel). EDR, antivirus, and email security.
- 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.
- Experienced in migrating the agents and tools from McAfee EPO to Defender ATP.
- Experienced in handling true positive incidents, remediating in a timely manner, and preparing the Incident Response (IR) Reports.
- Experience in analysing advanced system-based threats using EDR Defender for Endpoint. Managed the SPLUNK SIEM and created new alerts for security use cases. Integration of log sources into the SIEM solution.
- Experience in AIR (Automated Investigations and Remediation) policies and their implementation.
- In-depth understanding of the latest techniques used by attackers for persistence, privilege escalation, defence evasion, and lateral movement. Expertise in building use cases around the NIST and MITRE ATT&CK frameworks to enable detection at various stages of a cyber-attack.
- Experienced in examining suspicious emails for malicious content and providing recommendations on remediation actions using Office 365.
- Experience in creating, tracking, and responding to support cases raised with Defender ATP Support. Responding to in-house queries and guiding users with threat remediation strategies and best security practices.
- Performed root cause analysis for the incidents reported at the security operations center.
- Experience in creating runbooks, SOPs, and documents supporting the Security Operations.
- Experience in providing end-to-end support to enterprise counterparts, identifying the root cause of sophisticated enterprise initiatives with endpoint security solutions, such as Microsoft Defender ATP.
- Hands-on experience in analysing the device timeline logs and pulling reports by using advanced hunting in KQL.
- Expert in installing and using Splunk apps and add-ons.
- Knowledge of email security threats and security controls, including experience in analysing email headers.
- Prepare and deliver reports and metrics on vulnerability assessment outcomes, remediation progress, and the overall vulnerability landscape to senior management and other relevant stakeholders.
- Managing the reporting of AV migration and compliance reports.
- Good understanding of Azure Active Directory, Azure MFA, and conditional access.
- Knowledge of a breadth of security technologies and topics such as Security Information and Event Management (SIEM), IDS/IPS, Data Loss Prevention (DLP), Proxy, Web Application Firewall (WAF), Enterprise Anti-Virus, Sandboxing, and network and host-based firewalls.
- Designed, implemented and maintained security systems and controls.

EDUCATION

GVVIT College of Engineering And Technology., Bhimavaram, AP
B-Tech, E.E.E, 2015