Nagaraju Katreddy

Email:katreddy9696@gmail.com Ph:+(91)-9652619016

Professional Summary

Experienced Security Analyst with over 3+ years of experience in Information security. Excellent hands-on experience in Splunk SIEM, EDR, Endpoint security, and Phishing email analysis.

Skills:

- SIEM : Splunk , Azure Sentinel
- EMAIL: O365, Mimecast
- Antivirus Sophos AV
- EDR : MS Defender ATP
- Malware Sandbox: Any.Run
- Vulnerability Assessment: Qualys
- Networking protocols.
- Phishing Email Analysis
- Data Security DLP (Force point, Endpoint DLP)

Skills Summary

- Provides regular monitoring, triage, and incident response to automated security alerts using Security tools (like SIEM Splunk, Azure Sentinel. EDR, Antivirus, and Email Security).
- Experience in Analyzing phishing/malicious email campaigns to identify IOCs and contain those IOCs & on an Email Fraud defense to secure environment from hackers and fraudsters.
- Experience in writing correlation rules and monitoring Enterprise Security Application.
- Experienced in writing correlation rules with respective to KQL & SPL languages.
- 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, Network and Host based firewalls.
- Extensive knowledge of Splunk architecture and various components. Passionate about Machine data and operational Intelligence.
- Good knowledge & working experience on central logging, log management, Splunk SIEM architecture.
- Good knowledge on MITRE ATT&CK, diamond model, or other cyber threat kill chains.
- Experience in analyzing advanced system-based threats using EDR CrowdStrike falcon.
- Experience with log analysis and incident management with Splunk enterprise security.
- Experience removing email threats that are weaponized post-delivery, as well as unwanted emails from compromised internal accounts automatically.
- Analyze, contain, and eradicate malicious activity detected from real-time alerts and

manual threat hunts.

- Experience in performing Root Cause Analysis for data from SIEM
- Knowledge of email security threats and security controls, including experience analyzing email headers
- Experience with advanced persistent threats and human adversary compromises.
- Good experience in Security threat investigations using Endpoint & Network Security Tools.
- In-Depth knowledge of End Point Protection (AV, HIPS, and DLP)
- Excellent understanding of concepts of Vulnerability Assessment, Management, and patching.
- Experience in Qualys Vulnerability management tool.
- Having good verbal and written communication skills
- Enthusiastic for the email threat space, and willing to learn from mentors.
- Experience in Supporting on-call activities and rotation.
- Hands-on on Maintaining policies and procedures documentation and communicating needed enhancement.

IT Experience:

- Currently Worked as Security Analyst with Insta Global Source Pvt. Ltd., Hyderabad
- Past working as Information Security Analyst with HAYS Business Solutions, Noida
- Position: Information Security Analyst
-

Academic Overview:

- Bachelor Of Science ,Andhra University

Technical Strengths:

- Certified Splunk user
- Well-trained & Experienced in IT Security Professional.
- ExperienceinTechnicalSupport&Servicing.