Naveen Kumar Golla Akkulappa

+91-9100964467 | naveengolla1898@email.com | Linkedin

Professional Summary

- Manage 24/7 Shared Security Operations Center (SOC) operations, including log monitoring using Azure Sentinel and Microfocus ArcSight SIEM tools.
- Conduct incident response activities, including malware analysis, brute-force attack analysis, and phishing email analysis.
- Oversee the full incident lifecycle, from detection to resolution, ensuring compliance with SLAs and organizational policies.
- Create and maintain Standard Operating Procedures (SOPs) and runbooks for effective alert management based on dashboard alerts.
- Perform advanced analytical queries and investigations to identify security incidents, focusing on Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).
- Collaborate with external stakeholders and vendors to resolve security incidents and ensure effective threat mitigation.
- Implement Endpoint Detection and Response (EDR) strategies to proactively detect and respond to emerging cybersecurity threats.
- Prepare and deliver Weekly Status Reports (WSR) and Daily Status Reports (DSR) to the CISO and relevant teams, ensuring clear communication of security status and updates.
- Troubleshoot performance and availability issues with security devices, including IDS, IPS, UTM, content filtering, data loss prevention, antivirus, encryption, VPN, and SSL/TLS.
- Provide L1 support to resolve alerts generated from complex network, endpoint, and log analysis performance.
- Analyze network traffic from firewalls, IDS/IPS events, and logs, evaluating the effectiveness of existing security controls.
- Perform continuous monitoring and threat analysis, reviewing logs and network traffic for abnormal patterns and potential threats.
- Escalate security incidents as necessary and ensure proper documentation and incident management throughout the lifecycle.
- Mentor and lead first-level security analysts, ensuring effective knowledge transfer, team support, and training.
- Expertly use Microsoft Excel to create lookups, pivot tables, and detailed data analysis to support security investigations and reporting.

Skills

- **SIEM Tools:** Azure Sentinel, Microfocus ArcSight
- **OS :** Windows, Linux
- **Threat Intelligence Tools:** Virustotal, Mxtoolbox, AbuseIPDB, Hybrid Analysis
- **Vulnerability Scanning:** Nessus
- **Networking & Protocols:** VIPs, DNS, NAT, OSI
- **Directories:** Active Directory, LDAP
- **Analysis & Investigation Tools:** Wireshark, NMAP, ProcessMonitor, IPVoid
- **Ticketing & Incident Management:** ServiceNow, CRM
- **Security Controls:** IDS, IPS, UTM, APT, DLP, Antivirus, Encryption, VPN, SSL/TLS

Education

Bachelor of Technology, Jain University | Bangalore, Karnataka

Work Experience

Security Operations Center (Security Engineer)

Worked on Microsoft Azure sentinel and ArcSight which helps to analyze the User Behavior (UBA) and determining whether any user credentials or accounts had been compromised or any suspicious malware activity occurred in the environment.

- Played a Vital role in SOC team as L1 Analyst. Worked with core teams to investigate the false and true positive alerts.
- Primary focus on the analysis of Phishing/Spam mail campaigns. To identify, contain and remediate the spam incidents.
- Working on Azure sentinel dashboards by collecting IOC things to determine True positive or False Positive.
- Experience in creating SOP Runbooks by taking detailed Triage.
- Responsible for following all the steps in Incident Response Process.
- Responsible for monitoring infrastructure health, security and capacity, and make decisions on the security incidents that occurs in the environment.
- Responsible for preparing and submitting the Weekly Security Metrics Report and Weekly SLA Metrics to the client.
- Monitoring and identify positive security events from Microsoft Azure sentinel dashboards, Orion during the shift hours and take necessary action for the critical events that is seen during each shift's hours with deviations for all the environments that we support.
- Served as Analyst in SOC operations for real-time monitoring, analyzing logs from various security/Industrial appliances.
- Handling multiple customers globally analyzing the customer networks for potential security attacks.
- Scheduling and performing Vulnerability Scans on client networks to identify the vulnerabilities exist if any and coordinate till closure.
- Support security incident response processes in the event of a security breach by providing incident reporting
- Experience in creating the Preparing project status report in MS Excel.

Information Security Analyst **August 2021 –till date**
CBS Bangalore, Karnataka

- Skilled communicator with strong verbal and written language abilities, enabling effective collaboration with peers and senior management.
- Proficient in managing Priority 1 and Priority 2 incidents within the SIEM dashboard, ensuring timely and efficient resolution of critical alerts.
- Hands-on experience in malware analysis and phishing/spam email investigations to identify and mitigate security threats.
- Conducted thorough root cause analysis of malware and other security threats, implementing proactive solutions to mitigate risks.
- Served as the Single Point of Contact (SPOC) for the client for over 2 years, ensuring seamless communication and consistent service delivery.
- Performed detailed incident analysis and responded immediately to crucial alerts to protect systems and data.
- Expertise in vulnerability scanning using the Nessus tool to identify and address information security vulnerabilities, including SQL Injection, Cross-site Scripting (XSS), and directory traversal.
- Well-versed in implementing tools for comprehensive Web Application Vulnerability Assessments to strengthen security frameworks.
- Analyzed phishing and spam activities, notifying users and providing guidance to mitigate future risks.
- Prepared daily, weekly, and monthly reports and dashboards on security threats, trends, and vulnerabilities, meeting client requirements effectively.

Trainings Attended

ServiceNow Ticketing Tool • Splunk SIEM • Rapid7/NexPose MetaSploit Vulnerability Assessment