Srikanth Pepakayala

SOC ANALYST

Mumbai | +91 7032194868 | srikanthpepakayala@gmail.com | LinkedIn: www.linkedin.com/in/srikanthpepakayala

Career Objective

Seeking a challenging and rewarding position within a leading high-tech organization. Eager to contribute as a key player in a dynamic and innovative environment, collaborating with committed and dedicated professionals. Aim to fully explore and realize my potential while contributing significantly to the organization's success.

Work Experience

Talakunchi Pvt Ltd | Security Analyst L1 **OCT 2022 – Till**

Title: Altisource

Role: Security Analyst

Tools: QRadar, Office 365, and others

Description:

- Executed real-time monitoring and investigation of security events using QRadar and additional tools, ensuring proactive threat detection and response.
- Administered the release of Office 365 quarantine emails, aligning actions with user needs and business objectives.
- Conducted in-depth analysis of phishing emails and malware, implementing effective risk mitigation strategies.
- Reviewed and interpreted daily, weekly, and monthly security reports to identify trends and drive process optimization.
- Adhered to Service Level Agreements (SLAs) for handling service requests, incidents, work orders, and problem records, while preparing comprehensive Root Cause Analyses (RCAs).

Title: Tenable AD (Identity Exposure) | Zscaler Deception

Client: Leading Bank Sector

Role: Tenable Administrator

Tools: Splunk, Tenable AD, Zscaler Deception

Description:

- Conducted real-time monitoring and investigation of security events using Splunk and other platforms, enhancing threat detection capabilities.
- Managed and resolved issues with Tenable Identity Exposure, identifying and addressing identity-based vulnerabilities and misconfigurations.
- Compiled and analyzed monthly User Access Management (UAM) reports, utilizing insights to refine and enhance security processes.
- Performed daily Tenable health assessments to identify discrepancies and ensure system integrity.
- Continuously monitored for emerging threats, contributing to a strengthened security posture.

Key Contributions:

- Collaborated effectively with clients during high-priority incidents, offering support and devising mitigation strategies.
- Developed detailed root cause analysis reports and customized dashboards to meet client-specific requirements.
- Adapted to various shifts within a 24/7 Security Operations Center environment, demonstrating flexibility and commitment.

Summary

- Over all 2+ years of experience in Security Operation Center Analyst (SOC) and Information risk management.
- Proficient in SIEM tools like QRadar and Splunk for real-time monitoring and analysis of security alerts.
- Familiar with types of cyber attacks like phishing, Malware, DOS/DDOS, Brute force attack, MITM, Sniffing etc.
- Skilled in phishing email analysis, malware detection, log correlation, and troubleshooting cybersecurity incidents.
- Good Understanding of various SOC processes like monitoring, analysis, playbook, SLAs client meetings, reports walk through etc.
- Adept at generating client-focused reports, dashboards, and conducting in-depth root cause analyses.
- Proactive in escalating high-priority incidents with actionable recommendations aligned with SLA requirements.
- Good Knowledge on Microsoft Word, Microsoft Excel and PowerPoint skills.

Academic Details

Adikavi Nannaya University, B.sc MPC	**2021**
Intermediate, MPS Jr College	**2018**
SSC, Mandapeta Public School	**2015**

Technical Skills

- **SIEM:** QRadar, Splunk
- **EDR and XDR:** TrendMicro Apex Central
- **Web Application Firewall:** Imperva, Cloudflare
- **Antivirus:** Trend Micro
- **Firewall:** Palo Alto
- **DLP:** Force point
- **Email Gateway:** Microsoft 0365
- **Ticketing Tool:** Symphony Summit, ServiceNow
- **Exposure Management Tool:** Tenable AD (Identity Exposure), Zscaler Deception

Key Achievements

- Improved detection rates by fine-tuning SIEM configurations, reducing false positives by 15%.
- Successfully managed identity security configurations, enhancing overall security posture.
- Ability to work independently or as a collaborative or in a challenging environment.

Certifications

- Certified SOC Analyst (CSA) – EC-Council
- NSE 1 & NSE 2 – Fortinet
- Threat Intelligence Analyst – arcX
- Network Defense Essentials (NDE) – EC-Council