RAVI VARMA

Hyderabad, IN
+91-7382459045| ravi.varma2298@gmail.com

CAREER OBJECTIVE

Seeking a dynamic and challenging role as a SOC Analyst within an organization that values my capabilities and offers ample opportunities for professional development. Leveraging my **4+ years of experience as an Information Security Analyst**, I aim to contribute my expertise in **SIEM tools** utilization for effective log **monitoring** and **analysis** in the realm of **Security Monitoring and Operations (SOC)** and **Security Information and Event Management (SIEM)** comprehensive reports tailored to meet client Requirements.

PROFESSIONAL SUMMARY

- Proficient in using SIEM tools like **Microsoft Azure Sentinel, Splunk, IBM Qradar, and Device Management to monitor real-time events and analyze security issues.**
- Expertise in **email security threats and controls**, with experience in **scrutinizing email headers, attachments, and URLs.**
- Created and handled formal **incident reports** to resolve current threats to prevent future ones.
- Utilized various security **tools to monitor and analyze** security events, ensuring **risks and threats** were identified within agreed-upon service standards.
- Recognized successful and attempted cyber intrusions by **reviewing and analyzing** relevant event details in **logs**.
- Distinguished between **false alarms** and **real intrusion attempts**, taking action to **prevent and remediate**.
- Collaborated closely with stakeholders and provided timely responses to **security incidents, offering root cause analysis.**
- Documented all actions taken during **incident investigations for a clear record**.
- Responded **consistently and systematically** to common alerts from multiple sources.
- Actively kept up with the **latest security issues** and informed clients when necessary.
- Worked with Windows/Unix Security Logs and **logs** from **IDS/IPS, Palo Alto Panorama, Next Generation Firewalls, Anti-Virus/Malware Analysis,** and **Active Directory Integration**.
- Possessed a fundamental understanding of enterprise-grade technologies, **including operating systems, databases, and web applications**.
- Collaborated with other teams to support the **Incident management process** effectively.
- Applied knowledge of **OSI layers** and protocols to enhance **network security**.
- Proficient in implementing and managing **Firewalls, VPN, and other security products**.
- Responsible for evaluating alerts related to **malware and phishing attempts**.
- Monitored client networks using our **SIEM platforms**, ensuring **infrastructure availability.**

WORK EXPERIENCE

Information Security Analyst L2 *Nov 2020–To date*
ValueLabs – Hyderabad, IN

- Experience in a **24/7 Security Operations Center (SOC)** involving:
- Monitoring SOC events and promptly **detecting and preventing intrusion attempts**.
- **Real-time monitoring** of various **network security devices** like **Firewalls, Endpoint Security, Operating Systems, and Email Security** to align with client requirements and ensure **uninterrupted log monitoring.**
- **Identifying successful** and attempted cyber intrusions through **in-depth log analysis**.
- **Kusto Query Language (KQL)** with Complex Correlation of Different data sources in **MS Sentinel.**
- Conducting **Vulnerability Assessment (VA)** on both **web applications and servers**.
- **Recognizing attacks** based on their **unique signatures**.
- Proficient understanding of the **event lifecycle** and associated processing stages.
- Employing antivirus and other analysis tools for **Malware Analysis** and thorough malware removal from client environments and establishing metrics to support **Key Performing Indicators (KPIs).**
- Distinguishing **false positives** from **actual intrusion attempts** and aiding in their resolution.
- Collaborating with stakeholders and supporting escalation procedures.
- Maintaining detailed documentation of actions taken during **incident investigations**.
- Coordinating with other teams to facilitate **incident management processes**.
- Providing engineering teams with recommendations for **tuning and filtering**.
- Fulfilling data requests from customers and other teams, Preparing **RCA documents** and **daily, weekly, and monthly reports,** and Creating **Dashboards** in **Azure Sentinel, Splunk, and IBM Qradar.**
- Conducting **research, analysis, and alert responses**, including **log retrieval and documentation**.
- Monitoring and conducting **secondary-level analysis of incidents.**
- Analyzing SOC monitoring tool alerts to report **abnormal behaviours, suspicious activities, traffic anomalies, and more.**
- Performing analysis of **network traffic and host activity** across various technologies and platforms.
- Assisting in **incident response activities,** such as **host triage, malware analysis, remote system analysis, end-user interviews, and remediation efforts.**
- Expertise in **recognizing cyber-attacks** based on their **signatures** and aiding in **remediation and prevention.**
- **Developing advanced queries and alerts** to detect adversary actions.
- Analyzing **malicious campaigns and evaluating** the effectiveness of security technologies.
- Leading **response and investigation** efforts for **advanced/targeted attacks**.
- **Identifying IT infrastructure gaps** by simulating attacker behaviours and responses.
- Offering **expert analytic support** for large-scale and complex **security incidents**.
- Demonstrated proficiency with **core security technologies, including SIEM, firewalls, IDS/IPS, proxies, Incident Lifecycle, Vulnerability scanners, and antivirus solutions.**

CERTIFICATIONS

- Certified **CompTIA CySA+** certification
- Certified **SECURITY ENGINEER CERTIFICATE** by **Pro5**

EDUCATION

B-Tech (Computer Science & Engineering) ***OCT 2020***
Andhra University College of Engineering

TECHNICAL SKILLS

- **SOC** (**Security Operation Centre**) Experience
- **SIEM** (**Security Information and Event Management**) Proficiency
- Expertise in **Azure Sentinel, Splunk, IBM Qradar Tools**
- Ticketing Tool- **ServiceNow**
- EDR Tools- **Falcon Crowd Strike, MS Defender**
- Firewall- **Palo Alto Panorama**
- Anti-Virus Tools and Device Management (Preferably **McAfee**)
- Email Gateway Security **– MS O365 Defender**
- Vulnerability Scanners Tools – **Qualys and Nessus**
- Mail Security Monitoring Skills**-Phishing Email Analysis, Spam emails and Malicious Emails**
- Cyber and Technical Threat Analysis, **Threat Hunting, Threat Intelligence**, and **Malware Analysis.**
- In-depth Knowledge of **Networking Protocols, Primarily TCP/IP Protocol, OSI Layers, Subnetting, DNS, DHCP, Ports, Network Access Control, Network Configuration and Segmentation, Firewall monitoring, Content filtering, and Cryptography.**
- Microsoft Advanced Threat Protection- **ATP Microsoft O365 security**
- Good Understanding of **WAF, Anti-Virus, Proxy, DLP, Firewall, OSINT.**

DECLARATION

I hereby declare that the details furnished above are true and correct to the best of my knowledge and belief.

(RAVI VARMA UPPALAPATI)