VINOD POLAROWTHU

SOC Analyst

vinodpolarowthu182@gmail.com

+91 8088476182

CAREER OBJECTIVE

SOC Analyst with proficient and thorough experience and a good understanding of information technology. Specialized in proactive network monitoring of SIEM (Splunk and QRadar), EDR (Crowdstrike Falcon), DLP (Forcepoint). Able to use various security tools to perform logs and packet analysis. Finally, can perform malware analysis with the overall objective to ensure confidentiality, integrity and availability of the systems, networks, and data.

PROFESSIONAL SUMMARY

- Overall, **3.5 years** of experience into Cyber Security as Security Analyst (SOC).
- Skilled SOC Analyst with **3 years** of experience in monitoring threats, unauthorized access, viruses, and a wide range of threats and attacks.
- Experience in using SIEM tool Splunk and Q-radar.
- Experience in understanding the logs of various network devices, operating systems Expertise in defining resources like Dash Boards, Data Monitors, Active Channels, threats, open vas, etc.
- Investigating and creating a case for the security threats and forwarding it to the Onsite SOC team for further investigation and action.
- Performing Log analysis & analyzing the crucial alerts on an immediate basis.
- Recognizing attacks based on their signatures.
- Monitoring and carrying out second-level analysis incidents.
- Take immediate remediation on the Bad Threat Intel IOC's includes IP'S, URLs, etc.
- Demonstrated experience in Blacklisting the required countries and IOC in the firewalls, Email Security, EDR, etc.
- Identify and prioritize current vulnerabilities in client environments based on analysis from security instrumentation.
- Maintain state on current cyber threat actor techniques, tactics, and procedures.
- Proactively work with vendors on P1 issues and finding the Root cause also excel in taking Remediation's in the client Environment.
- Perform quality assurance functions to ensure client satisfaction.
- Participate in client service calls to assist in successful client outcomes.

TECHNICAL SKILLS

- Security Operation Center **(SOC)**
- **SIEM Tool**: Splunk and Q-radar
- **Ticketing Tool**: Service Now
- **End point security**: Symantec & Trend Micro
- **DLP, Crowd Strike, Carbon Black**
- **Vulnerability Management**: Nessus & Qualys
- **Email Security**: Proof point & Symantec

WORK HISTORY

MICROLAND, Bangalore, India
SOC Analyst, OCT 2021 to Till Date

Roles & Responsibilities:

- Monitoring the incoming security alerts in Q-radar & Splunk.
- Monitoring alerts triggered from sentinel and by analyzing logs and by taking necessary actions with respect to alerts and remediate the alerts by meeting SLA
- Worked on SNOW incidents creation to closing and Updating IOC's In Threat Intelligence in Sentinel.
- Performed Use Cases query development in Azure Sentinel for Internal and Client Engagements
- Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Maintain keen understanding of evolving internet threats to ensure the security of client networks.
- Regarding security incidents mitigation which in turn makes the customer business safe and secure.
- Determine the scope of security incident and its potential impact to Client network.
- Filling the Daily health checklist.
- Installation of Application Software and Antivirus software.
- Installing the Operating Software such as Windows.
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP etc.
- Good understanding of security solutions like Firewalls, DLP, Anti-virus, IPS, Email Security etc.
- Experience on performing log analysis and analyzing the critical alerts at immediate basis through Antivirus.
- Handling and analyzing suspicious executions through EDR Crowd strike.
- Analyzed phishing emails and associated payloads to identify trends, tactics, and techniques used by threat actors.
- Implemented anti-phishing controls and security awareness training programs to educate employees on phishing threats and best practices for email hygiene.
- Led incident response efforts for phishing incidents, coordinating with stakeholders to contain, investigate, and remediate affected systems.
- Troubleshooting SIEM dashboard issues when there are no reports getting generated or no data available.
- Determine the scope of the security incident and its potential impact on the client network.
- Filling the Daily health checklist and Installation of Application Software and Antivirus software.
- Installing the Operating Software such as Windows.
- Preparing daily, weekly, and monthly report as per client requirement.
- Recommend steps to handle the security incident with all information and supporting evidence of security events.
- Creation of reports and dashboards and rules fine tuning.
- Using components with known vulnerabilities, Insufficient logging and monitoring.
- Maintain & Document the application support strategy.

EDUCATION

B.TECH from sathyabama university in **2020.**

DECLARATION

I Here declare that the above given information is correct to the best of my knowledge and belief.

VINOD POLAROWTHU