Manoj Kumar M

sogimanu@gmail.com 6360417051

SUMMARY

Detail-oriented Incident Responder and SOC Analyst with over 2.3 years of cybersecurity experience. Proficient in using SIEM tools like Seceon, and ArcSight for threat detection and incident management. Skilled in preparing reports, conducting health checks, and troubleshooting technical issues, with a strong commitment to enhancing security posture and client support.

Profile

- Over 2.3 Years of experience in Security Operation Center
- Good understanding common network services and protocols
- Hands on experience on SIEM called ArcSight and Seceon for monitoring and analysis
- Solid understanding of network concepts: OSI Model, TCP/IP Model, DNS,DHCP, TCP, UDP, 3Way handshake, ARP etc.
- Familiar with types of Cyber-attacks like Phishing, DOS/DDOS, Cyber Kill Chain, Brute force, MITM, Miter Attack etc.
- Good understanding of various SOC processes like monitoring, analysis, log analysis, SLAs, client meetings
- Keep updated with the latest developments in cyber security
- Identify the false positive and false negative cases withthe help of standard proceduresand open-sourcetools

EXPERIENCE

Executive-SOC analyst L1

Tata Advanced Systems Limited, on-site.
Noida, Uttar Pradesh. **April 2024 – Present,**

- 24*7 Eyes on glass monitoring logs and investigating suspicious activities using SIEM solution called Arc-Sight and Seceon
- Analyze threats by taking the events from firewall, Endpoints Serves, IPS/IDS etc
- Identification of incidents and respond according to the SLAs
- Preparing Daily, Weekly and Monthly report and sending an onsite team to publish it
- Raising the tickets after analysis that includes all the information about the offence
- Preparing SOP (Standard Operations Procedures) and sharing it with customers and internal Teams for the resolved issues
- Contacting the customers directly in case of high priority incidents and helping the customers in the process of mitigating the cyber attacks
- Advising or updating the Customers about the findings and recommendations of the alrets
- Preparing Security Advisory for the new vulnerabilities released and informing the customers
- Maintain keen understanding of evolving internet threats to ensure the security of client networks
- Willingness to work in any shifts in a job that involves 24*7 Security Operation Center environment

SOC analyst L1

Neptune Information Solutions Limited, hybrid.
Bengaluru, Karnataka **November 2022 -March 2024,**

- Monitoring and managing the real time events for the security devices using the SIEM tools: IBM QRadar
- Responsible for 24/7 Enterprise Network and System Security Surveillance
- Incident Analysis and Management in the Security Operations Center
- Escalation Single Point of contact for Client Query and work proposals.
- Preparing Daily, Weekly and Monthly report and sending an onsite team to publish it.
- Creating or implementing queries for triggering auto generated reports to customers on a weekly or Daily basis as per customer requirement.
- Identification of incidents and respond according to the SLAs
- Preparing SOP (Standard Operations Procedures) and sharing it with customers and internal Teams for the resolved issues
- Raising implementation request and fine-tuning the request, preparing knowledge base for all the incidents, changes and problems resolved.
- Advising or updating the Customers about the findings and recommendations
- Preparing Reports Weekly/Monthly for the entire customer. Which includes the Top Virus infected machines
- Preparing Security Advisory for the new vulnerabilities released and informing the customers
- Analyzing the Events and providing details and solutions to the next level
- Follow up with respective teams on raised incidents and give necessary inputs on remediation actions to be taken

SKILLS

Skills:
Incident Response
SOC Analysis
Client meeting
Log Analysis

Tools Used:
SIEM- ArcSight, Seceon
Email Gateway–Proofpoint
Proxy–Zscaler
Firewall – Palo Alto
Ticketing Tool: Summit AI ITSM
Sandbox– Threat stream Joe Sandbox
Endpoint Security/Remediation: Microsoft Defender
Automation: Siemplfy SOAR
Open-Source Tools: Virus Total
IPVoid .com
Abuse IPDB

EDUCATION

VSKUB University
Bachelor of Science • Karnataka • 2018-2021

GOVT GB PU College
Karnataka • 2018

CERTIFICATIONS

Certificate of Professional SECEON INC
Seceon • 2024

Cyber Threat Management
Cisco • 2023

Cyber Threat Intelligence-101
ArcX • 2023

LANGUAGES

English
Hindi
Telugu
Kannada