Cheerla Dharmendar

SOC Analyst

9398909594◇ Cheerla.dharmendar@outlook.com◇ Gachibowli, Hyderabad, Telangana, India◇

linkedin.com/in/cheerla-dharmendar-36a50a194

SUMMARY

Experienced with 3.2 years as an Information Security operation Center (SOC) Analyst with hands-on expertise in SIEM tools like IBM QRadar, Azure Sentinel and Claroty for real-time monitoring, analyzing, and responding to security incidents across IT and OT environments. Skilled in threat detection, incident response, frameworks as MITRE ATT&CK and managing a variety of vulnerabilities with strong critical thinking, communication, and interpersonal skills. Capable of effectively administering security infrastructure operations in fast-paced, challenging environments.

EXPERIENCE

SOC Analyst Mar '22 — Present

Hyderabad, India

Tata consultancy Services

- Managed 24x7 Security Operations Centre, utilizing IBM QRadar, Azure sentinel and Claroty (OT SOC) for real-time security monitoring, analysis, and incident detection.
- Monitored and triaged security events originating from devices such as Firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS), analysis tools, Operating Systems level logs and O365 logs.
- Responding to inbound security monitoring alerts and Email security.
- Having experience in Global SOC operations for potential security threats, identify and act on anomalous network activity with IBM QRadar and Azure sentinel as a Security Information and Event Management (SIEM) Platforms, and endpoint protection solutions with more than 200+ use cases with In-depth Analysis of alerts arising from tools, and inputs on fine-tuning, whitelisting, and optimization of security systems.
- Promptly detecting and responding to security incidents, such as malware infections, DOS and DDOS attacks, and unauthorized access attempts, Investigate malicious.
- Phishing emails, domains and IPs using Open-Source tools and recommend proper blocking based on analysis.
- Utilized sandboxing tools to monitor for a wide range of threats and malicious emails, effectively minimizing security risk.
- Working on shared SOC handling multiple clients in Incident Analysis, Investigation and Response using available security tools within the defined SLA (Service Level Agreement)
- Generated comprehensive reports for weekly and Monthly Metrics and provided valuable training and imparted technical knowledge to junior team members.
- Contributed significantly to the continuous improvement of security processes and procedures within a 24x7 cyber security operations environment at a Managed Security Services Provider (MSSP).
- Proper knowledge in understanding cyberattacks and methodologies, Phishing, Incident Handling and Incident Response.
- Ability to work well in ticketing system (Service Now)

PROJECTS

Provided shared Support for Projects related to Insurance, Finance, Petroleum and Pharmaceutical companies.

- Conducted thorough reviews of security alerts escalated from Level 1 analysts within the SOC.
- Created regular, weekly and Monthly reports and updated Standard Operating Procedures (SOPs).
- Collaborated with cross-functional teams to identify and develop use cases.
- Monitored and identified suspicious security events within the environment.
- Utilized sandboxing tools to enhance proactive threat detection capabilities.

OT SOC operations for food manufacturing company

• Continuously monitor OT systems PLCs (Programmable Logic Controllers), and other industrial control systems, for anomalies, intrusions, and suspicious activities.

SKILLS

Security Operations: Incident Response, Log Analysis, Phishing Analysis, Malware Analysis, Endpoint Security.
SIEM Tool: IBM QRadar, Azure Sentinel, Claroty.
Ticketing Tools: Service now.
Microsoft Office: Excel, Power point.
Microsoft Defender: Microsoft Defender (Endpoint Detection and Response), CrowdStrike (Extended Detection and Response).

CERTIFICATIONS AND ACHIEVEMENTS

SC 200: Microsoft Certified security operation Analyst Associate.
On The Spot Award given by client for handling phishing analysis

EDUCATION

B.E in Electronics and Communication Engineering from MCET under Osmania University in the year 2020. Jul '16 — Sep'20