MANOJ DODDASIRIGERE

Bengaluru India | 7760788354 | manojgoudar07@gmail.com

Professional Summary

A demonstrated Information Security Analyst with 5 years of experience in information security, Endpoint Security, Network Security with a focus on system security monitoring, Incident response, Threat Intelligence, Threat hunting, Content development. An accomplished analyst with over five years of experience in assessing information security risks and coordinating remediation efforts.

Skills

SIEM : Splunk, AZURE Sentinel, Qradar

EDR/XDR : Crowdstrike, Defender

Email Gateway : Microsoft o365, Proofpoint

Malware Analysis : Falcon Sandbox, Wildfire

Vulnerability Assessment : Qualysgaurd, Nessus.

ITSM : Service Now, Jira

IDS/IPS : Cisco Firepower, PaloAlto

Data loss prevention : Symantec DLP

Packet Analyzer – Wireshark, BRIM

Cloud : AWS Cloudwatch, Cloudtrial, VPC, Azure

OSINT Tools: MxToolbox/Abuse IPDB/VT/URL Void/Any Run/ Cyber Chef, Sysinternals, PE studio

Work History

Security Analyst - SOC 07/2019 to Current

DXC Technology – Bengaluru

- Provide Information Security Operations Center (ISOC) support.
- Experience working with global teams across multiple time zones, cultures, and languages and mostly supported MNC clients.
- Analyzing the phishing Emails which are reported by the employees and performing phishing campaign.
- Analyzing the DLP related incidents and identifying any possible data leakage, taking the quick actions to mitigate data leakage.
- I have actively participated in the POC of FortiSOAR solution
- Monitoring and responding to Cloud infrastructure logs AWS Cloud trail, Cloudwatch, Defender for Cloud etc
- Having experience in analyzing the raw logs, PCAPS and writing the regular expressions to extract fields out of it

- Track and respond to all incoming alerts from the SOC, the MSSPs, and the systems monitored directly by the Security Operations team
- Perform tier 2 triage of all escalations from the SOC & MSSPs, tier 1 triage of all alerts that are directly monitored, and work with Security Engineering for all escalations beyond the Security Operations team
- Monitor multiple security alert sources, eliminate false positives from Splunk, Sentinel SIEM, based on the impact and nature of the Security incident triage significant security events, and escalate according to the established procedures.
- Review automated daily security events, identify anomalies and escalate critical security events to the appropriate IT Team and follow up as required.
- Investigate the root cause of the incident from different logs.
- Monitor security devices log delay alarm to keep the device in a healthy state using SIEM
- I have good experience managing the incidents from Crowdstrike, MS defender EDR
- Good understanding of MITRE ATT&CK framework -Threat Hunting, Incident Detection and Response, use case engineering, Designing and implementing IR Playbooks, Curating Threat Intelligence.
- SECURITY INCIDENT RESPONSE SPAM EMAIL ANALYSIS EDUCATION Analyze event/alert patterns to properly interpret and prioritize threats with available DLP tools and other devices
- Identify trends and derive requirements aimed at improving and enhancing existing data loss prevention and detection policies
- Creating the incident report and send across to the management.
- Conduct thorough investigative actions based on security events (Real-time incidents: SQL injection, cross-site scripting, Trojan, server attacks, etc.) and remediate as dictated by standard operating procedure
- Dashboards, reporting, & KPIs Perform routine (daily, weekly, monthly, quarterly, & yearly) reporting on our security events, trends, and system hygiene & posture, such as on our IaaS environments & critical SaaS environments
- Build the system & configuration components needed to capture the metrics by which security hygiene, monitoring & alerting health, and security program effectiveness are measured
- Presenting daily status report to the customers and completing the action items requested by the customers
- Track our KPI elements over time such that KPI trends can be determined & used as feedback to the security program design
- Having good experience in analyzing the traffic in Panorama and Wildfire for file analysis

Education

Bachelor of Commerce 07/2019

KSEDC College - Bengaluru, India

Certifications

- CEH
- Fortinet NSE
- Qualysgaurd
- Splunk
- AZ-900