Praveen Dollin

Bengaluru India +919483942027 praveendollin4@gmail.com

PROFESSIONAL SUMMARY

4+ Years of hands-on Experience in Security Operations. Incident Response, Endpoint Security, Phishing analysis, Threat Intelligence, Network Security. Good understanding of log formats of various devices such as Web sense, Vulnerability Management Products, IDS/IPS, EDR, Firewalls, WAF, Proxy, Routers, Switches, OS, DB Servers, and Antivirus. Experience in Information Security with emphasis on security operations, Log monitoring, Log management, incident management, and security event analysis through Sentinel & Splunk SIEMs. Analyzing the detections and incidents from EDR solutions like Crowdstrike, MS defender and containing the machines and providing real-time response. Having experience in handling incident response in Linux OS and troubleshooting accordingly. Having experience in developing Security content like rules, reports, dashboards in SIEM. Experience in generating Daily, Weekly & Monthly Reports from Sentinel and Splunk and communicating to stakeholders. Agile in investigating security threats such as Malware Outbreaks, DDOS, OWASP T-10 and Phishing Analysis on the network. Having knowledge in integrating log sources along with SIEM and parser creation. Performing the effective phishing analysis and performing phishing campaign using Knowbe4.

WORK HISTORY

SECURITY ANALYST

10/2022 to 01/2025

TEAL IND Pvt Ltd | Bengaluru

- Perform incident response analysis to uncover attack vectors involving a variety, of malware, data exposure, phishing, and social engineering methods
- Monitor security alerts received from SIEM or other security tools like EDR, DLP, email gateway, proxy, IDS/IPS, firewall, threat intelligence, etc.
- Carry out Level 2 triage of incoming incidents (initial IR assessment of the priority of the event, initial determination of incident nature to determine risk and damage, or appropriate routing of a security or privacy data request)
- Providing threat/vulnerability analysis and security logs from larger number of security devices In addition to investigate Incident Response support when there is a threat Investigating and monitoring Network traffic / IDS / Firewall / Endpoint security logs using IBM Qradar and Splunk Insider threat and APT detection or Understanding/ differentiation of intrusion attempts& false alarms
- Composing security alert notifications raising ticket to higher officials in ticketing tool Advise incident responders/ other teams on threat and providing evidence and information and tracking the threat resolution Email analysis using various open source tools such as MX Toolbox,

redirectdetective.com

- Perform malware analysis technique such as static and dynamic to understand and mitigate the effect of worms and virus detected by the end point security and isolate them by creating lab environment sand box and too Identifying and prioritizing vulnerabilities in the network Analysis of notables triggered and taking necessary actions Based on the request related to incident, searching, fetching and sharing the logs to the concerned team
- Basic search in Splunk and using the fields, using the tags in Splunk and Have knowledge on creating the dashboards and use cases Monitoring the logs from end devices and investigate offenses or any malicious traffic is observed, then taking an appropriate action involving respective tower (if necessary) based on analysis
- Log source integration (Windows, Linux and Network devices) to QRadar Analysing and Troubleshooting the issues related to web content filtering
- Allowing, Whitelisting or blocking the URL, domain or IP's based on the request Monitoring the dashboards related to health monitoring of the Log database, log server, Filtering service and Directory service, database updates
- Fetching, sharing the logs using for analysis and if requested respectively
- Investigating the suspicious mail and taking necessary actions such as blocking the IP's, URL's, source, sender's mail ID etc by coordinating with different teams
- Malicious URL's and domains, Bad Reputed Ip's, Suspicious Email ID and Domain, malicious attached documents hash values details updating in Trustar and integrated the same with SIEM to identify the malicious traffic entering into the network.

SECURITY ANALYST

10/2020 to 09/2022

DXC Technology | Bengaluru

SKILLS

SIEM : Splunk, AZURE Sentinel, Qradar

EDR/XDR : Crowdstrike, Defender

Email Gateway : Microsoft o365, Proofpoint

Malware Analysis : Joe Sandbox, Wildfire

Vulnerability Assessment : Qualysgaurd, Nessus.

ITSM : Service Now, Jira

IDS/IPS : Cisco Firepower, PaloAlto

Phishing Campaign : KnowBe4

Data loss prevention : Symantec DLP

Packet Analyzer : Wireshark, TCPDump

Cloud : AWS Cloudwatch, Cloudtrial, VPC, Azure, defender for Cloud

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

EDUCATION

Bachelor of Computer Applications | Computer Science *09/2020*

Kle, Hubballi

CERTIFICATIONS

- CEH
- Fortinet NSE
- Qualysgaurd
- Splunk

LANGUAGES

English

Bilingual or Proficient (C2)

kannada

Bilingual or Proficient (C2)