Dhalavari Swetha

CYBER SECURITY CONSULTANT

CONTACT

+91 9944660193

swetha.dhalavari@gmail.com

Bangalore, India

SKILLS

Microsoft Sentinel
RSA Netwitness
IBM QRadar, MDE
AWS, Azure
Windows OS, Linux OS
MITRE ATT&CK Framework
SIEM Threat Detection, Threat Hunting
Log Analysis, Phishing Analysis
Wireshark, Network Analysis
OWASP
Cyber Kill Chain
C, Python, SQL, KQL

EDUCATION

Vellore Institute of Technology - Sep 2019

M.Tech Software Engineering (Integrated) - 8.14

CERTIFICATIONS

Certified by Purdue University in Applied Cyber Security Essentials

PROFILE

Passionate Cyber security professional with 5+ years of experience in managing threat content like Threat detection, threat hunting using SIEM solutions QRadar, Netwitness, Microsoft Sentinel.

WORK EXPERIENCE

Societe Generale GSC - Tecplix Technologies (Payroll) | Cyber Security Consultant | Jul 2024 - Present

- Development of Cloud Detection Content in Microsoft Sentinel based on current environment.
- Dedicatedly worked on Azure services like Azure Kubernetes, Azure Key vault , Entra ID etc.
- Analyzing the current security posture, identifying security gaps.
- Detection Use case creation from MITRE, Using Mitre for gap analysis.
- Managing and maintaining detection content through GitHub, Jira
- Responding to Alerts and Continuous Fine Tuning of SIEM Rules.
- Incident Response Plan creation and SOC Procedures for created detection content.
- Closely working with Analysts to help with Investigations
- Validation of existing detection rules.
- Exposure to Splunk

RSA Security | Software Engineer 1 | Feb 2022 - Jul 2024

- Creating and implementing new threat detection content, rules and use cases to deploy in Netwitness SIEM platform
- Created multiple App Rules, ESA Rules for different mediums like log, packet and Endpoint.
- Developing custom content based on threat intelligence and threat hunting results.
- Deep understanding of cybersecurity frameworks such as MITRE ATT&CK and its tactics, techniques. Also mapping threat detection content to the MITRE ATT&CK framework to help display product coverage.
- In depth understanding on Threat research, Attack Scenarios, APT, Malware Analysis, Packet Analysis, log Analysis.
- Performed attack simulation on different operating systems to test created rules on Netwitness. Exposure to AttackIQ, Atomic Red Team.
- Posting blogs related to Threat research content.
- knowledge of collaboration tools such as JIRA and Confluence
- Basic experience with Github source control tool, AWS Cloud, Scripting.
- Basic level Knowledge on parsing of logs being ingested into the SIEM Platform.

Infosys | Senior Systems Engineer | Aug 2020 - Feb 2022

- Worked on IBM QRADAR SIEM and was Part of Content Management Team.
- Performed Threat detection, threat hunting and log analysis to identify malicious activities using IBM QRadar.
- Use case development based on multiple log source types, attack scenario, MITRE Framework using TTPs and client requirements.
- Use cases are created for each client based on log sources integrated, Payload information, Events generated.
- Creation of Building Blocks, Custom Event Properties, Event Mapping on QRadar.
- Monitoring and analysis of security alerts, Network Traffic, Phishing Header Analysis.
- Incident Response Plan document creation.
- Assist customers to fully optimize the SIEM system capabilities.
- Work with the customer designated personnel to provide continual correlation rule tuning
- Involved in discussions with client for review of finalized Use case, threshold, reference set, make recommendations to meet client requirements.
- Mapping Use case created to MITRE Framework and Cyber Kill Chain Phases.
- Using MITRE Framework for SOC Procedures.
- Working with Analysts to help with Incident investigations to identify root cause analysis and remediation planning.
- Exposure to Playbook Creation on Cortex XSOAR for the Use cases

Infosys | Systems Engineer Trainee | Jan 2020

Trained in fundamentals of Cyber Security, Identity and Access Management Fundamentals, Application Security, Vulnerability Management, Enterprise Security and Fundamentals of Python Programming, DBMS.