Mathan Subbiah

7200780670 mathan1702@gmail.com

Profile

Experienced SOC Analyst proficient in designing, implementing, and maintaining efficient SIEM solutions for comprehensive threat detection and incident response. Skilled in leveraging XDR platforms for advanced threat hunting and correlation across endpoints, networks, and cloud environments. Demonstrated expertise in utilizing a wide range of SOC security tools for log analysis, vulnerability assessment, threat hunting and incident management. Adept at identifying and mitigating security risks to ensure the confidentiality, integrity, and availability of critical information systems.

Work experience

08/2021 – present
Chennai, India

Senior Security Engineer - IT
Toppan Merrill

- Provided expert-level support and administration for Splunk, XDR, Cofense, and other security tools, creating alerts, reports, and dashboards to enhance visibility and detection capabilities.
- Led and coordinated responses to complex security incidents, including root cause analysis, containment, eradication, and recovery.
- Developed and executed advanced threat hunting strategies to proactively identify and mitigate sophisticated threats.
- Contributed to the design and implementation of security architectures and controls.
- Stayed abreast of the latest threat intelligence and incorporated it into security operations.
- Developed and maintained comprehensive documentation for security incidents, investigations, and procedures.
- Utilized tools to identify and prioritize vulnerabilities in the organization's attack surface.
- Provided expert-level analysis and remediation for Azure/O365 security incidents.
- Collaborated with other security teams to address complex security issues and ensure a holistic approach to security.
- Assessed and prioritized security risks across the organization, collaborating with relevant teams to develop and implement mitigation strategies.
- Mentored junior engineers, fostering a culture of continuous learning and professional growth within the team.

10/2017 – 08/2021
Bangalore

Technology Security Analyst
Accenture

- Monitored security events in real-time, identified and prioritized threats
- Triage and investigate security alerts to determine their validity and potential impact
- Follow established incident response procedures to contain and remediate security incidents.
- Investigated and escalated security incidents, contained threats, and minimized impact
- Analyzed security data, generated comprehensive reports, and communicated findings effectively
- Documented security events, procedures, and findings
- Developed and refined standard operating procedures for security processes
- Identified and reported bugs to clients
- Generated weekly and monthly production reports.

Work experience

07/2017 – 10/2019
Chennai

Information Security Engineer
Sify Technologies Ltd

- Led vulnerability management, security incident and event management, and patch management services for clients in BFSI, Telecom, Manufacturing, and Healthcare sectors, utilizing expertise in ArcSight.
- Collaborated with cross-functional teams to assess Vulnerability programs and deliver Endpoint Detection & Response (EDR) service to over 250 customers.
- Contributed to the 24x7 Security Operations Center (SOC) by providing Security Incident Detection & Response (SIDR) service to more than 25 customers, leveraging experience with Nessus and Nexpose.
- Supported the monitoring of Endpoint Security Services for over 250 cloud customers and 25 dedicated customers, covering 15,000 endpoints, with proficiency in Trend Micro OfficeScan and DeepSecurity.
- Assisted in ensuring the timely delivery of Fortknox service for 25 cloud customers, utilizing knowledge of Symantec Endpoint Protection, McAfee EPO, and Trend Micro Vulnerability.
- Implemented 10+ product log sources and designed Regex Parser files for 10+ products in ArcSight.
- Successfully implemented TrendMicro OfficeScan XG, Application Control, and Endpoint Encryption products for over 10,000 devices.

Skills

Security Information and Event Management ●●●●●	XDR ●●●●●	Email Security ●●●●●	Threat Intelligence Analysis ●●●●●
Incident Response Management ●●●●●	Regex Log Parsing ●●●●●	Cloud Security ●●●●○	Vulnerability Assessment ●●●○○
Firewall Configuration and Management ●●○○○	Penetration Testing Skills ●●○○○	Malware Analysis and Reverse Engineering ●○○○○	

Tools Handled

Splunk | Arcsight | Cortex XDR | Cofense | Defender for Cloud | Immuniweb | Qualys | SocRadar | Arcsight Regex | Trend Micro OfficeScan | Trend Micro DeepSecurity | Trend Micro Application Control | Trend Micro Endpoint Encryption | Nessus | Nexpose | Symantec Endpoint Protection | McAfee EPO

Strengths

Teamwork | Innovation | Coordinating | Strong analytical skills | Attention to detail | Technical proficiency | Problem-solving abilities | Incident response experience

Education

01/2019 – 12/2020
Chennai

Cyberforensics And Information Security | Master of Science
Madras University

Education

06/2013 – 03/2017
Chennai

Electronics And Communications Engineering | Bachelor of Engineering
Sri Sai Ram Engineering College

Certificates

06/2017 **RHCSA**

06/2017 **RHCE**

02/2018 **Red Hat Certified Specialist in Ansible Automation**

03/2018 **CEH**

01/2019 **CCNA**

05/2019 **Red Hat Certified OpenShift Administrator**

07/2021 **Splunk Core User**

Hobbies

Feeling the music

Playing sport

PC Gamer

Film enthusiast