Yogeesh Kumar *Threat Analyst*

Bengaluru, India 560066
yogeeshkumarshetty@gmail.com
+916363785459
Yogeesh Kumar Shetty - Sophos | LinkedIn

Profile

A highly motivated and enthusiastic professional with a passion for **Cyber Security and Information Security** with **4 years** of experience. Proficient in **Threat Hunting**, Investigating, analyzing **security incidents** and providing suitable counter measures. Experienced in **Vulnerability Assessments** and **Managed Risk** reporting to clients with the detailed report of mitigation, remediation strategies and security best practices.

Skills

- Programming Languages: Python
- Security Tools: SOAR, Sophos MDR, CrowdStrike, Nessus, MS Defender.
- Email Security & Awareness: Proof Point, Knowbe4
- SIEM: Splunk, ArcSight.
- Ticketing Tools: Jira, ServiceNow
- Cloud: AWS
- AI Tool: Amazon Bedrock, ChatGPT
- Operating System: Linux, Windows

Professional Experience

2023/06 – present

Threat Analyst
SOPHOS.

- Work as a member of both the **SOC team and the Managed Risk** activity, responsible for conducting **security assessments**, including VA (infrastructure, network devices, public facing servers).
- Performing Threat Hunting based on both threat models driven approach and hypothesis based on Managed detection and response (Sophos MDR) platform. Involves collecting and analyzing data from various data sources including
  - Identify threats not identified by SOC monitoring.
  - Monitoring Indicator of compromise **IOC's and IOA's.** Creating
  - exclusions policy at endpoint, servers and firewalls perimeter level.
- Full understanding and utilization of **Microsoft-related security** tools, including **Defender** for various incident analysis and creating report.
- Conducting Health Check for Sophos MDR Central environment assesses its configuration against best practices, helping to ensure optimal protection.
- Performing the 3rd party vendor device integration with SOPHOS MDR platform and ensure accurate configuration and transmission of telemetry data to Sophos DataLake.
- Identifying potential security threats or vulnerabilities and prioritizing detections ensures critical threats are addressed promptly, bolstering overall security.
- Managed and triaged all security incidents stemming from triggered detections. Provided thorough analysis and actionable recommendations to stakeholders, ensuring swift and effective responses to mitigate risks and enhance security posture.
- Experience in regular vulnerability assessments and Attack surface Management to identify vulnerabilities in network devices, public facing servers and sharing the VA report with the Stakeholders.
- Conduct **phishing campaigns** on a global level to raise awareness among employees about the latest phishing tactics.

2021/06 – 2023/06

Associate Engineer – Security (SOC)

Atos Global IT Solution

- Monitoring and investigating security events, alerts and logs from multiple log sources through ArcSight Logger/MDR tool AIsaac.
- Hands on working experience on Log Analysis of different vendors and products like EDR, XDR, Firewalls, Gateway, DLP, VPN, Microsoft windows, Linux, Azure AD, VPC, IDS/IPS, NGFW, WAF, Proxy.
- Performed advanced threat analysis by correlating events from diverse log sources, crafting comprehensive investigation reports includes possible risks, conclusions and actionable recommendations to enhance security posture.
- Hands on experience and better knowledge effectively using multiple Threat Intel platforms like Virus Total, Abuseipdb, Hybrid analysis, Cyberchef, Any. Run.
- Whitelisted false positives, raised validated incidents and engaged in weekly SOC meetings, facilitating client discussions on raised incidents.
- Proficient in utilizing the MITRE ATT&CK framework to conduct security analysis, automation, fine-tuning, mitigation strategies, and reporting within Security SOAR and SIEM operations.

Education

2012 – 2016
Mangalore, India

Batchelor of Engineering (B.E)
Visvesvaraya Technological University
Percentage: 7.3 CGPA

Certificates

Splunk
Splunk Enterprise Certified Administrator (Cybrary)

Vulnerability Management
Fundamental of Vulnerability Management (Cybrary)