|  |
| --- |
| Agnihothram Rangagopal (security Researcher)  Hyderabad, Telangana, India |+91-8790395439 | [agnihothramrangagopal@gmail.com](mailto:agnihothramrangagopal@gmail.com) | <https://www.linkedin.com/in/agnihotram-gopal-a893a115a/> |

# Profile

* Experienced as Security Analyst with 3 years of experience in EDR Detection writing, Threat Hunting, Incident response, Endpoint Security, SOC, Email Security.
* Extensive knowledge on **OWASP**-10, **SANS**-25 programming errors.
* Understanding of Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).
* Extensive knowledge in Malware Analysis (Static & Dynamic Analysis) and firewalls, VPNs, IDS/IPS, and other network security tools.
* Experience analyzing malicious files, memory dumps, and logs.
* Ability to triage and investigate alerts to determine their severity and scope.
* Knowledge of common adversary tactics and techniques, e.g., obfuscation, persistence, Defence evasion, etc. and attack vectors and techniques (e.g., phishing, DDoS, ransomware).
* Solid understanding of current cyber-attack tactics/techniques and mitigation solutions.
* Knowledge of incident response procedures.

# Experience

## Microosft Defender ATP (edr)| Ltimindtree | 26th March 2023 – 17th February 2025

* Working with various stakeholders for streamlining day-to-day tasks/Activities in the project.
* Utilize IOCs fed by Microsoft’s Threat Intelligence to hunt for active threats.
* Creating new EDR Alerts/Detections for recent undetected suspicious/malicious threat campaign.
* Analyzing the recently developed EDR Alerts to determine its detection quality before moving to production.
* Working on Customer/Global escalations related to Product.
* Correlated machine logs and data to enhance accuracy of threat detection, reducing false positives.
* Analyzing FP alerts triggered by EDR and fine-tuning False Positive detectors by writing Suppression rules.
* Wrote tactical detection rules for unidentified alerts, customizing rules for customer environments.
* Monitoring Network and Endpoint Exfiltration Alerts. Monitored Phishing Email Analysis on and Office365.
* Finetuning the EDR detector logics based on the behavioral perspective and threshold of the Alerts.
* Conducted machine state analysis using KQL to support threat investigations.
* Creating automations for Known FP & TP alerts based on threshold & legitimacy.
* Working on various stages of IR which involves in-depth analysis and RCA submission on security incidents.
* Proactively emulated APT group behavior for threat hunting, identifying gaps in EDR detection.

## Microosft Defender ATP (soc)| Ltimindtree | 25th MARCH 2022 – 25th MARCH 2023

* Experienced SOC analyst in – Microsoft O-365, IBM QRADAR & Azure Sentinel.
* Performed security event monitoring of heterogeneous networks such as firewalls, IDS/IPS & DLP devices using QRADAR
* Working experience in SOC environment with hands on experience using SIEM Qradar tool which includes log analysis finetuning exiting correlation rules to reduce false positive and responding to incidents.
* Monitoring of external cyber threats leveraging threat intelligence provided by IBM XForce feed integrated into IBM QRadar.
* Creation and Modification of reference sets, Security Operations Procedures (SOPs) and use-cases.
* Use case fine-tuning suggestions to mitigate false positives.
* Escalation and Coordination with other domains for unresolved incidents.
* Working on Real time network traffic by analyzing the logs from IDS and Firewalls through SIEM Tool.
* Handle the complete incident management framework cycle right from incident identification, incident containment, performing root cause analysis, suggestion and implementation of preventive and corrective controls and perform network analysis as needed on a case-to-case basis.
* Filtering the events by defining & Applying Filters at different levels of an events.
* Updating all the trackers & trends regularly.
* Investigating the events based on criteria by creating an Active Channel.
* Raising Incidents if found any suspicious or illegitimate & notifying to Client.
* Displaying the event data in different layouts by defining Dash Boards & Data Monitors.
* Checking Connectors health status & Reporting to the Admin team.
* Monitoring AV logs in QRadar & raising case for malware infections.

# Education

## Vkr vnb & agk Engineering college[jntuk] | June 2017-september 2021 | B. Tech(cse)

# Skills & Abilities

* **Threat Research Tools:** Visual Studio, Kusto Explorer, Cyber Explorer, MTE, IcM , KQL
* **Malware Static Analysis:** PE studio, CFF Explorer, ExeinfoPE, Hex Editor, Bin Text
* **Malware Dynamic Analysis:** ProcMon, Process Explorer, RegShot.
* **IP Reputation & analysis:** IP Void, Cisco Talos, MX Toolbox, Virus total, Abuse IPDB
* **URL Reputation & Analysis:** URL void, URL scan, Researcher Studio, Cisco Talos Intelligence, Alien Vault
* **SIEM Tools:** Azure Sentinel, IBM QRADAR, Crowd strike.
* **Email Gateway:** Office365

# Accomplishments

* Honored as Best Performer of the Quarter for Q2 2023, Q1 2024 for outstanding project contributions.
* Recognized by the Leadership team for writing detections related to security threat campaign FN’s.

# Certifications:

Certified Ethical Hacker (CEH)