Girish Vanamadi

9666654204 / 8498959465 | girishvanamadi1996@gmail.com | Kakinada, Andhrapradesh

Summary

- 4.6 years of deep experience in IT and IT security operations with a broad exposure on infrastructure/network/IT security tools, Security incident response.
- Experience with multiple Endpoint Security (EDR) and Next generation Antivirus (NGAV) tools like VMware Carbon black ,Cybereason,Crowd strike, McAfee EPO, Windows Defender(Microsoft ATP)
- Having knowledge of OSI and various network protocols such as TCP/ IP, DNS, DHCP, HTTPS, FTP, SMTP,SSH.
- Having knowledge in PCI DSS.
- Experience with SIEM tools – Splunk.
- Familiar with PowerShell and PHP scripting.
- Having Knowledge in Cryptography algorithms & application security.
- Experience in Incident Management & Change management.
- Experience in Vulnerability Management.

Education

Computer Science & Engineering (M.tech) | University College of Engineering (JNTU-K) | 09/2019 | Kakinada, Andhra Pradesh

Percentage : 73.2%

Computer Science & Engineering (B.Tech) | Pragati Engineering College | 05/2017 | Surampalem, Andhra Pradesh

Percentage : 70.81%

Intermediate | Sri Chaitanya Junior college | 04/2013 | Kakinada, Andhra Pradesh

Percentage: 87%

SSC | Aditya Public school | 04/2011 | Kakinada, Andhra Pradesh

Percentage : 86%

Skills

EDR, Cybereason, Qualys, Crowdstrike, Splunk, Endpoint Security, Malware Analysis, Phishing email Analysis, Security Alerts review, Compliance Management, Access Management, Scripting, ServiceNow, Security Incident management, loganalysis, Vulnerability Management, Threat hunting, Microsoft Defender for endpoint (ATP), carbon black

Experience

Security Engineer | 04/2023 - Present | COGNIZANT | Hyderabad, Telangana

- **Automated Reporting**: Implemented automation for generating device reports across 17 companies, reducing report generation time from one hour to 5 minutes using Carbon Black's APIs.
- **Ticket Management**: Managed Carbon Black and CrowdStrike tickets, ensuring timely resolution within SLAs.
- **Exclusion Management:** Handled exclusion requests for Carbon Black and CrowdStrike, validating and whitelisting legitimate applications.
- **RFM & Bypass Devices** : Fixing devices running in RFM & bypass mode in Crowdstrike & Carbonblack
- **Policy Management**: Proficiently managed security policies in Carbon Black and CrowdStrike.
- **Investigations**:Conducted investigations on high severity alerts in Carbon Black and CrowdStrike.
- **Agent Compliance and Virus Scan:** Responsible for agent compliance checks and working on non-compliant machines. Performed scans on virus or malware-infected endpoints and ensured clean scan results. Isolated critical endpoints when necessary.
- **IOC Blocking:** Blocked IOCs in EDR consoles based on advisories received from SOC, validating reputation in open-source security intelligence portals like VirusTotal.

- **Collaboration with SCCM:** Collaborated with SCCM team for managing EDR agent installation through deployment tools.
- **Dynamic Host Groups:** Designed dynamic host groups in CrowdStrike for enhanced operational efficiency.
- **USB Device Exclusions**:Managed approval and implementation of USB device exclusions in CrowdStrike and Carbon Black.
- **Performance Optimization**:Resolved performance issues in Carbon Black and CrowdStrike, including high CPU and memory usage due to EDR agents
- **Vendor Collaboration**: Collaborated with Carbon Black vendors to address interoperability issues and other challenges.
- **Sensor Coverage /Compliance** : Ensured comprehensive sensor coverage by deploying Carbon Black agents on all relevant devices.
- **Threat Detection**:Created custom threat detection rules in Carbon Black. (watch list)
- **Agent Connectivity issues** : Resolved sensor connectivity issues, ensuring uninterrupted security coverage.
- **Email Security:** Knowledge in email security tools such as Proofpoint TAP, TRAP, and Proofpoint URL isolation.

Automations

- Automated the McAfee DAT(signature version) and DLP compliance reports by using PHP as Backend language and SQL as database.
- Developed a script which accepts machine names as input and will provide the ping status of the machines if the machines are connected our client network.
- Restrict app execution automation in Microsoft Defender for endpoint.
- Automation Demo Videos
- Successfully automated the generation of onboarded devices reports for 17 operating companies, utilizing APIs to extract data from the Carbon Black console. Reduced the report generation time from one hour to just 5 minutes.

Information Security Analyst | 04/2022 - 04/2023 | Deloitte | Hyderabad, Telangana

- Reviewing security alerts triggered by Security tools like CrowdStrike and taking necessary action.
- Supervise the configuration, monitoring, and execution of vulnerability scans. (Qualys)
- Working with different teams in the organization to fix the vulnerabilites that were vulnerabilites that were identified on the endpoints.
- Reviewing and approving of the Firewall rules (to open ports in Network firewall) tickets and ensuring all the data is encrypted during the transit.
- Analyzed suspicious emails for phishing and malware attacks.
- Significantly reduced attack surface by providing data on inactive user & service accounts and implementing account retirement procedures.
- Handling Netskope (web proxy) incidents like recategorization and whitelisting of the URL's up on the requirement.
- Monitoring of the High severity alerts triggered by Stealthwatch (IDPS) and taking necessary actions. & Fine tuning the policies up on the requirement.
- Service Account management & Password compliance.
- DB access management requests review.

Security Analyst | 10/2019 - 04/2022 | Tata Consultancy Services | Hyderabad, Telangana

- Worked on deploying Cybereason sensor on Windows and Linux Machines. Deployed Cybereason on 13000 machines (Linux & Windows) by collaborating with different teams in our organization as part of EDR Project.
- Worked on onboarding the devices to Defender for endpoint (MDE)
- Whitelisting & block listing of hashes in MDE
- Offboarding of Devices from MDE when devices are decommissioned.
- Handling Smart screen related issues in MDE
- Having Knowledge in ASR Rules.(MDE)
- Troubleshooting the issues related to MDE.
- Automated Restrict App execution in MDE
- Hands-on experience in analyzing the logs of sensor & handling sensor connectivity issues when an EDR agent on an endpoint not connecting to the Cybereason console.
- Reviewing security alerts triggered by Cybereason and CrowdStrike and taking necessary action.

- Responsible for taking a lead in identifying in false positive detection alerts & identifying indicators of threat activity, and executing actionable recommendations.
- Responded to, handled, and remediated security incidents.
- Trouble shooting and resolving the Incidents of Cybereason without breaching SLA.
- Capable of tracking, analyzing, escalating and resolving IT Security issues.
- Having knowledge in Malware analysis and allow listing/ Block listing the file hashes, IP's in EDR solutions up on the requirement.
- Hands on experience in Creating the custom detection rules in EDR solutions.
- Creating folder exclusions in AV policy by considering vendor requirements.
- Involved in creating and maintaining Security Operational process and procedure document.
- Worked on upgradation of EDR agents on all the endpoints in the organization.
- Facilitated policy changes and console Monitoring in EDR solutions.
- Preparing weekly compliance report and sharing with the client and worked on defects to improve the compliance.
- Contacting and closely working with Cybereason support engineers for resolving the challenges if we face any.
- Tagging sensors and dividing in to groups based on the Organization requirement.

Certifications

- Qualys Certified specialist.
- Splunk Fundamentals.
- AZ 900 Azure fundamentals

Awards

- On the Spot Award. (TCS)
- Applause Award.