Harsha V

Sagarvh0066@gmail.com

EDUCATION

Indiana Wesleyan University, United States *(Master of Science, Information Technology Management; GPA 3.6)* **Jan 2023 - Present**

EXPERIENCE

Amazon, India **Aug 2019 – Dec 2022**

Threat Analyst, Strategic Planning Team

- Implemented Splunk Enterprise Security version 7.3 to aggregate and correlate security logs from Cisco ASA firewalls, Snort IDS/IPS, EDR, and custom applications, for threat detection and incident response.
- Used Splunk User Behavior Analytics (UBA) to detect IOCs of insider threats, unusual data access patterns, privilege escalation, data exfiltration.
- Utilized IDS/IPS systems, Snort and Suricata for network traffic analysis and threat detection.
- Configured custom alert rules and signatures for YARA and Snort.
- Engaged in threat hunting exercises using ELK stack and Sysmon APTs detection.
- Integrated Splunk with Palo Alto Networks Cortex XSOAR to automate response actions, alert triage, threat containment, forensic data collection.
- Conducted deep packet inspection (DPI) and Network Traffic Analysis using Wireshark and Zeek to analyze network traffic.
- Created custom scripts using Python and PowerShell for advanced log analysis and automated detection of specific threats or anomalies.
- Monitored Twitter, Reddit, and specialized forums for threat intelligence.
- Leveraged tools like TweetDeck and custom scripts to track hashtags and keywords related to emerging threats.
- Employed CTI frameworks such as NIST, MITRE ATT&CK, Cyber Kill Chain, Diamond Model to standardize documentation and ensure thoroughness.
- Collaborated with incident response team, to gather threat information from various open-source platforms.
- Leveraged Passive DNS data from Farsight Security DNSDB for threat intelligence feeds to identify actors associated with threats.
- Utilized sandbox environments like Cuckoo and FireEye to safely execute and analyze suspicious files and payloads.
- Conducted comprehensive research across various sources including internal logs, network traffic data, threat intelligence feeds, OSINT, and external reports to gather relevant security data.
- Developed and documented monitoring processes to ensure effective utilization of tools, including defining KPIs and alerts.
- Employed disk imaging and hashing techniques to create forensic images of storage media.
- Configured AWS CloudWatch, Azure Monitor, and Google Cloud Logging, to collect and analyze logs from cloud services and resources.
- Performed cross-functional operations including network and endpoint data investigation.

Cognizant **Jul 2018 – Jul 2019**

SOC Analyst, Blue Team

- Integrated data firewalls, intrusion detection systems (IDS), endpoint protection platforms (EPP), and network traffic logs, into a centralized SIEM.
- Worked extensively with SIEM tools such as Splunk and ELK stack to monitor and detect potential security threats.
- Analyzed phishing emails, websites to identify TTPs used by threat actors, enabled a 25% improvement in threat detection.
- Developed deployment and integration plans for new security tools, including testing, validation, and configuration of the tools to meet the organization's needs.
- Leveraged CTI frameworks like Phishing Kill Chain model to understand the lifecycle of attacks, led to 20% enhancement in attack detection rates.
- Implemented EDR solutions like Microsoft Defender and Sysmon to monitor endpoint activity and detect anomalies.
- Monitored security blogs like Medium, Krebs on Security, Threatpost, FireEye, Palo Alto Networks' Unit 42 to stay informed about the latest threats.
- Maintained knowledge base of known TTPs mapped to the MITRE ATT&CK framework, ensuring comprehensive tracking and easy reference.
- Deployed Symantec Data Loss Prevention (DLP) version 15.5 to prevent unauthorized data exfiltration.
- Maintained an up-to-date log of all incident-related activities, ensuring accurate and complete records for audit and post-incident review purposes.
- Deployed Maltego version 4.2 for threat actor profiling.
- Conducting link analysis and visualization of relationships between domains, IP addresses, email addresses, and social media accounts associated with cyber threats.
- Conducted in-depth analysis of exploited vulnerabilities Nessus and Qualys to identify open patches in systems and applications.
- Reverse-engineered malware samples using Sandbox environment.
- Worked with incident responders and threat hunters to confirm the presence of malicious activity, ensuring accurate alert triage and prioritization.

SKILLS

- **Networking**: TCP/IP protocols, LANs, WANS, VPNs, Routers, Firewalls, Cloud, Virtualization.
- **Operating Systems:** Windows, Unix-Based Systems (Solaris, Linux).
- **Scripting Languages:** Python, PowerShell, Bash.
- **CTI Frameworks:** MITRE ATT&CK, NIST, Cyber Kill Chain, Diamond Model.
- **Security Tools:** Wireshark, tcpdump, Symantec Endpoint, McAfee Endpoint Protection, Microsoft Defender ATP, Nessus, Nmap, SOAR, Metasploit, Snort, Suricata, SIEM(Splunk, ELK).
- **Other Skills**: MS Office (Word, Excel, Outlook, Access, PowerPoint)

PROJECTS

SOC Home Lab

- Created a personal Virtualized SOC home-lab using VirtualBox. Played the role of both a cyber security attacker and defender.
- Configured a C2 server using Metasploit and dropped a C2 payload on a Windows VM.
- Simulated attacks with Kali Linux against Windows environment and monitored network traffic to generate alerts for attacks and write analysis.
- Implemented SIEM tools, EDR solutions, and IDS/IPS to monitor the virtual IT environment.
- Employed deception techniques such as honeypots and honeytokens to lure and identify malicious actors.
- Conducted network analysis using Zeek and Wireshark to detect anomalous network traffic patterns.
- Developed custom dashboards and visualizations within the SIEM platform to track security events and incidents.
- Maintained expertise in cybersecurity domains such as network security, endpoint security, cloud security, and threat intelligence, staying abreast of industry trends, emerging threats, and new technologies.
- Engaged in coursework and participated in Capture the Flag (CTF) challenges on TryHackMe platform, developing practical cyber security skills and enhancing knowledge in offensive and defensive techniques.