Dhina M A S

+91 8925609059 | dhina.mas11@gmail.com | https://www.linkedin.com/in/dhina-s-399226220/

Objective

To monitor and respond to security threats, ensuring the safety of an organization's networks and systems. Aiming to detect and resolve cyber risks quickly, improve security measures, and contribute to a strong and secure IT environment.

Experience

L1 SOC Engineer **Jul 2023 – Mar 2025**

Secure Traces | Bengaluru, Karnataka

- Monitored and analyzed security events, alerts, and logs in the LogRhythm SIEM tool to identify, investigate, and respond to potential security threats. This included correlating data from multiple sources, identifying suspicious activity, conducting in-depth analysis of incidents, and escalating critical threats to ensure rapid mitigation and continuous improvement of the organization's security posture.
- Assigned to investigate and assess security alarms to identify potential threats, performing thorough analysis to determine the severity and validity of each incident. Responsible for closing low-level or false positive alarms promptly, while escalating high-priority or complex alarms to the L2 SOC Analyst for further investigation and resolution. This process ensures the effective prioritization of security incidents & helps minimize the overall risk to the organization's endpoints.
- Mitigate the advanced threats and identify potential weakness in the security infrastructure, aligning with standards.
- Utilized the MITRE ATT&CK Framework to identify and analyze cyberattack tactics and techniques, enhancing threat detection and response strategies. Applied advanced security techniques based on the MITRE ATT&CK Framework to proactively discover vulnerabilities and mitigate potential risks.
- Collaborated with L2 SOC analysts by proposing new use cases for improving threat detection capabilities, recommending new use case scenarios to enhance the effectiveness of the SIEM platform.
- Conducted knowledge transfer (KT) sessions for new SOC analysts, providing structured training on SIEM operations, threat hunting methodologies, and security best practices to accelerate their onboarding and effectiveness.
- Fine-tuned detection to minimize false positive alerts, ensuring that only genuine security threats were flagged and reducing unnecessary noise for efficient threat management. Refined security systems to enhance the accuracy of threat detection, improving the reliability and effectiveness of the alert system.
- Ensured adherence to Service Level Agreements (SLAs) by promptly investigating, responding to, and resolving security incidents within defined timeline.

Junior SOC Analyst **Apr 2023 - Jul 2023**

Necurity Solutions | Chennai, Tamil Nadu

- Monitored and analyzed security events using SIEM tools & other monitoring systems [WAZUH, ALIENVAULT].
- Implemented new DQL use-cases in Wazuh.

Education

Master of Computer Applications (MCA) | Pursuing **2024 - Present**

Jain (Deemed-to-be University) | Bengaluru, Karnataka

BCA specialized in CLOUD TECHNOLOGY & INFORMATION SECURITY **Jul 2019 – Jun 2022**

Vels Institute of Science Technology & Advanced Studies | Chennai, Tamil Nadu

TECHNICAL SKILLS

- **SIEM Tools:** LogRhythm, Wazuh & AlienVault.
- **Incident Response:** Root Cause Analysis.
- **Network Security:** Intrusion Prevention Systems (IPS), Firewalls, Packet Analysis.
- **Email Phishing Analysis:** Header Analysis (SPF, DKIM, DMARC), URL & Attachment.
- **Security Monitoring & Incident Handling**: Log Analysis, Event Correlation, Malware Analysis
- **Endpoint Security:** EDR, AV, Behavioral Analysis.
- **Threat Intelligence & Analysis:** MITRE ATT&CK, TTP Detection

ADDITIONAL TECHINCAL DEVELOPMENT

Elastic Stack SIEM Configuration and Management: Successfully set up and configured Elastic Stack SIEM in a home lab environment. Demonstrated proficiency in deploying a Kali Linux VM, configuring Elastic Agents for log collection, and forwarding data to the SIEM for effective security event monitoring.

Security Event Simulation and Analysis: Acquired hands-on experience in generating and analyzing security events using Nmap on Kali Linux. Proficient in querying Elastic SIEM to identify and investigate security incidents, enhancing skills in network security monitoring and threat detection.

Visualization and Alerting in SIEM: Developed a custom dashboard in Elastic SIEM to visualize security events, demonstrating skills in data interpretation and pattern recognition. Successfully created and tested alert rules for detecting specific security events, showing competency in proactive incident response and alert management.

CERTIFICATIONS

- **Offensive Security Defense Analyst (OSDA) SOC-200**
  Offensive Security | Pursuing
  The certification is primarily based on hands-on experience in a live lab environment where candidates must identify and respond to simulated cyberattacks.

- **LogRhythm Security Analyst - LRSA (LogRhythm)**
  This certification validates proficiency in areas like searching log data, creating custom rules and filters, correlating events, analyzing threat intelligence, and managing security incidents within the LogRhythm environment.

- **Linux Fundamentals for IT professionals (Udemy)**
  IT professionals with the essential knowledge and skills needed to understand and effectively use the Linux operating system

- **Build responsive website using HTML5, CSS3, JS & Bootstrap (EDUCBA)**
  The primary focus is on creating websites that adjust their layout and content to fit different screen sizes, which is crucial in today's multi-device web landscape.