SOC Analyst

Name - DHANUSH GOWDA

Phone- 9663295311

Mail - dhanushgowdadg5311@gmail.com

Professional Summary:

Accomplished Cybersecurity Analyst with experience in SOC monitoring, incident response and threat hunting. Proficient in SIEM platforms such as Splunk, QRadar, AlienVault, DNIF and Securonix. Proven track record in developing playbooks, optimizing correlation rules and reducing false positives. Skilled in log analysis, malware detection and automation, with a strong focus on improving security operations and threat detection capabilities.

Skills:

Technical Skill:

Incident Response/Threat Hunting: NIST, Cyber Kill Chain, Malware & Phishing Analysis, DDoS Analysis
SIEM/SOAR Platforms: Splunk, IBM QRadar, Elastic ELK, Forti SOAR, Playbook Development, Linux
Endpoint/EDR Security: Microsoft Defender (ATP), McAfee ePO, Sophos, CrowdStrike, Cisco AMP
Network/Perimeter Security: IDS/IPS, Zscaler, Cisco Firewall, F5 WAF, Infoblox DDI, Allot, Riverbed
Cloud & Email Security: Microsoft 365 Security & Compliance, AWS Security, Kubernetes Security
Networking/Traffic Analysis: TCP/IP, Wireshark, PCAP, Syslog & NMap
Malware Analysis: Sandbox, CyberChef, OllyDbg, IDA Pro, Process Explorer &Flare VM
Ticketing tools: ServiceNow

Soft Skills: Communication **|** Teamwork **|** Adaptability **|** Problem solving **|** Time Management

Work Experience:

XANTT Technologies pvt ltd From July 2023 to Till date

Roles and Responsibilities

- Managed shift operations for security alert monitoring and investigations, implementing playbooks to reduce manual tasks.
- Monitored and analyzed security events from multiple sources using **Splunk and SIEM** to detect potential threats.
- Performed **incident response** including triage, containment, eradication, and recovery of malware, ransomware, phishing, and insider threats.
- Conducted **endpoint investigations and remediation** using **EDR tools** (Microsoft Defender, Sophos) and **Malwarebytes**.
- Performed **network traffic analysis** with **Wireshark**, intrusion detection with **Snort**, and vulnerability scanning with **Nessus** and **Nmap**.
- Conducted **penetration testing and web application security assessments** using **Metasploit, Burp Suite, and SQLmap**.
- Integrated **threat intelligence feeds and IOCs** into the SIEM platform to support proactive threat hunting.
- Developed and fine-tuned **SIEM dashboards, alerts, and custom correlation rules** to improve detection accuracy.
- Prepared **incident reports, vulnerability reports, and compliance documentation** for senior management

and audit purposes.

- Coordinated with IT and application teams to **remediate vulnerabilities and strengthen security controls**.
- Authored and maintained **SOPs and playbooks** for SOC operations to streamline incident handling and knowledge sharing.
- Served as the primary point of contact between clients and management, handling all queries from stakeholders and ensuring effective communication.
- Worked with SOC managers and clients to enhance processes and address requirements.
- Performed alert analysis with SIEM, managed high-severity incidents and investigated emerging security threats.
- Oversaw and mentored senior L1 analysts/Junior security analysts, assisting with incident escalation and resolving their queries.
- Conducted threat hunting with the MITRE ATT&CK framework, produced incident reports following industry standards and created new detection rules to improve security operations.
- Reduced alert volume by 40% through optimized detection rules.
- Managed SOC monitoring and incident response for various clients, utilizing SIEM platforms (Qradar, Splunk, Securonix, DNIF) to track security events and incidents.
- Authored forensic incident reports, engaged in proactive threat hunting using the Cyber Kill Chain.
- Developed innovative automation scenarios using SOAR for improved incident response efficiency.
- Created weekly, monthly and quarterly reports, providing insights into security trends and incidents across client environments, while leveraging Microsoft Defender for enhanced endpoint detection and response.
- Performed comprehensive security monitoring and alert investigations using Splunk SIEM and analytics tools, ensuring thorough incident triage and root cause determination. Additionally, created multiple dashboards in Splunk to enhance visibility and streamline security operations.
- Conducted proactive threat hunting to identify and mitigate malicious activities and suspicious behaviors.
- Developed detailed playbooks for various security alert categories, enhancing investigation quality, standardizing responses, and improving team efficiency.
- Analyzed SPAM and phishing threats, including email analysis and identification of malicious tactics, to strengthen cyber defense measures.
- Monitored security alerts generated by Splunk SIEM, focusing on TCP/IP traffic, OSI layers, firewall logs and OWASP guidelines.
- Conducted in-depth analysis using runbooks and SOC tools, leveraging threat intelligence and firewall configurations.
- Generated daily, weekly and monthly reports on security incidents.
- Troubleshoot critical laptop issues and installed drivers, ensuring prompt resolution and optimal performance.
- Collected and verified details of critical vulnerabilities, cross-checking available patch information and updating software packages.

Education:

BE - Government engineering college
PUC - Hassan public pu college
SSLC - Max muller public school

Declaration

I hereby declare that the information provided above is true to the best of my knowledge and belief. I take full responsibility for the authenticity of the details mentioned and affirm that I have not withheld any relevant information.