Hemanth Kokanti

hemanth02824@gmail.com +91 9381802824 Gurugram, India linkedin.com/in/xxyyzzaabb

Profile

Cybersecurity Professional with expertise in incident response, threat detection, and security operations. Skilled in optimising security workflows, analysing threats, and enhancing defence strategies. A proactive problem-solver and driven team player, passionate about continuous learning, security innovation, and delivering results.

Skills & Expertise

Cybersecurity Engineering: Incident Response, SIEM Engineering (Splunk, Microsoft Sentinel, AWS GuardDuty), Threat Detection Rule Development (MITRE ATT&CK, IDS/IPS, AV/AD, Proxy, VPNs), Vulnerability Management & Exploit Mitigation (Qualys, Nessus, Burp Suite).

Security Tools: Splunk, Microsoft Sentinel, MS Defender XDR, Microsoft 365 Security & Compliance, AWS, Qualys, ServiceNow, Acunetix, Security Scorecard, HackerOne, CyberAngel, RiskWatch, Burp Suite, Fortify, Sophos AV, Bitdefender AV.

Penetration Testing & Offensive Security: Red Teaming & Threat Emulation (Kali Linux, Metasploit, Burp Suite), Malware Analysis & Reverse Engineering (Cuckoo Sandbox, IDA Pro).

Programming & Automation: Python, PowerShell, Bash

Compliance & Security Auditing: ISO 27001, GDPR, PCI-DSS, Security Scorecard Optimization

Professional Experience

Giesecke Devrient, *Cyber security Analyst* Apr 2023 – present | Gurugram, India

- Investigated L1 & L2-level security incidents and alerts using a full incident management lifecycle and forensic analysis, ensuring comprehensive documentation and resolution.
- Engineered advanced SIEM detection rules leveraging MITRE ATT&CK, IDS/IPS, Antivirus (AV), Active Directory (AD), Proxy, VPNs, and other security sources, reducing false positives by 40%.
- Integrated and analyzed external threat intelligence feeds (IOCs, CVEs, exploit data) into Splunk and Microsoft Sentinel, improving detection of emerging cyber threats and enhancing root cause analysis.
- Led multiple security projects, including integrating diverse log sources into SIEM and managing SOC architecture enhancements, reducing false positives in detection use cases.
- Strengthened vulnerability management using Qualys, reducing remediation time for critical vulnerabilities by 40%. Analyzed 300K+ vulnerabilities per month, prioritizing remediation based on risk assessment and business impact.
- Elevated the security scorecard from 74 to 93 by collaborating with developers on secure code analysis using SAST tools and enhancing the HackerOne bug bounty program.
- Led penetration testing assessments and supported ISO 27001, GDPR, and PCI-DSS compliance across 17 countries. Managed audit preparations and security audits.
- Developed custom Python scripts to automate threat-hunting processes and redundant SOC tasks, improving efficiency and detection accuracy.
- Led and mentored a team of 3 cybersecurity interns, delivering training from fundamental security concepts to advanced SOC practices. Created technical presentations to simplify complex security topics.

Giesecke Devrient, *Cyber security Intern* Sep 2022 – Apr 2023 | Gurugram, India

- Monitored and analyzed security alerts using SIEM tools like Splunk and Microsoft Sentinel, identifying potential threats and escalating incidents as needed. Assisted in developing and fine-tuning detection rules and use cases, contributing to the SOC's ability to detect and respond to emerging threats.
- Conducted malware analysis and IOC identification, supporting senior analysts in the development of effective remediation strategies. Researched, documented, and integrated external threat intelligence from feeds into monitoring tools, including relevant IOCs and vulnerabilities.
- Assisted in maintaining compliance with ISO 27001 and GDPR, supporting audit preparations and documenting security policies.
- Assisted in integrating threat intelligence into the organization's security monitoring systems, including the identification of vulnerabilities and indicators of compromise (IOCs) related to third-party suppliers.

Technical Projects

Integrated Vulnerability Data into SIEM for Real-Time Insights

- Automated the integration of vulnerability data into SIEM, reducing 90% of manual effort in report sharing and data correlation.
- Enabled real-time visibility of vulnerabilities for stakeholders, improving incident investigation efficiency by providing immediate insights into affected assets.

Integrated Third-Party Security Tools with SIEM

- Connected external threat intelligence sources such as "Have I Been Pwned" (HIBP) and dark web monitoring tools to SIEM (Splunk & Microsoft Sentinel) to automate the correlation of leaked credentials and exposed data with enterprise security events.
- Created detection rules and alerts in SIEM to trigger automated responses when user credentials matched known breach databases, improving incident response efficiency.

Awards

Security Champion, *Giesecke Devrient*

Recognized for exceptional contributions across various security domains including Incident Response, Threat Hunting, Vulnerability Management, External Attack surface management and Third-party Risk Assessments.

Spot Award for identifying and mitigating a critical vulnerability targeting C-Level Executives., *Giesecke Devrient*

Identified and prevented a phishing attack targeting C-level executives from the initial stage, successfully stopping it before it could impact the organization. Recognized with the Spot Award for this proactive effort in securing the organization's leadership.

Education

Siddhartha Institute of Science and Technology, Jul 2018 – Sep 2022 | Tirupati, India

Bachelors of Technology - Electronics and communications Engineering

- Simulated Phishing Attack for Security Awareness: Conducted a controlled phishing simulation among college students and faculty to assess email security awareness. Analysed click-through rates and provided training on phishing identification, reducing engagement with malicious links.
- Web Application Security Testing: Performed penetration testing on a college web portal using Burp Suite to identify security vulnerabilities. Prepared a security report with mitigation recommendations for the college IT team.

Certifications & Training

Static/Dynamic Malware Analysis - Udemy, Cyber Attacks and Mitigation Techniques, Vulnerability Management: Assessing the Risks with CVSS v3.1 - LinkedIn, PCI Compliance – Qualys, Vulnerability Management Detection& Response – Qualys, Evolution of Cybersecurity – Fortinet

Personal Traits

- Excellent Documentation Skills Known for creating clear, precise, and well-organized documentation, ensuring that all processes, procedures are comprehensively captured and easily accessible for teams and stakeholders.
- Takes the initiative in team settings, driving collaboration and ensuring that team efforts align with the overall goals. Recognized for contributing innovative ideas and solutions while encouraging team participation and fostering a collaborative environment.
- Highly capable of managing multiple tasks and projects simultaneously, effectively prioritizing based on business needs, security risks, and deadlines, while maintaining a high level of performance and focus on critical objectives.
- Able to think critically and creatively when faced with complex or unexpected challenges, finding effective solutions and ensuring minimal disruption to workflows or security operations.