NANDINI CHENNUPATI

CYBER SECURITY ANALYST

linkedin.com/in/nandini-chennupati

naganandini.chennupati@gmail.com

+1 331-222-7737

PROFESSIONAL SUMMARY

Cyber Security Analyst with over two years of hands-on experience and a Master's Degree in Information Technology. Expertise in identifying and analyzing suspicious activities, managing sensitive information, and utilizing a wide range of security tools for comprehensive log and packet analysis. Proficient in conducting vulnerability assessments, penetration testing, and malware analysis to ensure the confidentiality, integrity, and availability of systems, networks, and data. Dedicated to safeguarding organizational assets and enhancing security posture through proactive threat detection and mitigation strategies.

TECHNICAL SKILLS

Programming Languages: Python, Java, SQL, C, C++, Ruby

Scripting and Automation: PowerShell, Bash (Linux scripting)

Operating Systems: Linux, Windows, Ubuntu, Kali Linux

Productivity Tools: Microsoft Excel, Microsoft Word

Networking:

- **Protocols:** OSI Model, TCP/IP, DHCP, DNS, UDP, SSH, SSL, RDP
- **Tools:** Wireshark, pfSense, Network Protocol Analysis, ICS/IDS
- **Firewalls & Security:** Firewalls, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Snort (for network intrusion detection and prevention)

Cybersecurity Tools:

- **Network Scanning & Reconnaissance:** Nmap, Recon-ng, Ettercap
- **Penetration Testing:** Meterpreter, Armitage, Metasploit, Burp Suite
- **Vulnerability Management:** Nessus, Vulnerability Assessment Tools
- **Security Automation:** SOAR, Splunk, VMware
- **Cryptography:** OpenSSL, Brute Force Tools (John the Ripper, XHydra)
- **Data Security:** Data Loss Prevention (DLP) Tools

Cloud Security: Microsoft Azure, AWS, Google Cloud Platform (GCP)

Endpoint Security: Sophos Endpoint Security, Endpoint Detection & Response (EDR)

Security Practices:

- Identity & Access Management (IAM)
- Privileged Access Management (PAM)
- **Risk Management:** Risk Analysis, Vulnerability Management, Security Best Practices

EDUCATION

Governors State University - University Park, Illinois Aug 2022 - May 2024

Master of Information Technology GPA: 3.923/4

VR Siddhartha Engineering College - Vijayawada, India June 2017 - May 2021

Bachelor of Electronics and Instrumentation Engineering CGPA: 7.72/10

CERTIFICATIONS

- CompTIA Security+
- Google Cyber Security Professional

PROFESSTIONAL EXPERIENCE

Teaching Assistant - Cyber Security

Governors State University - University Park, Illinois Sep 2023 - May 2024

- Assisted professors in delivering coursework on Information Security, Cyber Security Fundamentals, and Wireless Penetration Testing, providing guidance and support to students in understanding complex security concepts.
- Developed and graded assignments and projects related to Cyber Security, ensuring alignment with current industry practices and academic standards.
- Facilitated laboratory sessions and practical exercises, including real-time network security simulations and forensic analysis, to enhance students hands-on learning experiences.
- Provided one-on-one mentoring and tutoring to students, helping them with research topics and coursework, including projects on Cloud Integrity Assurance and Social Engineering.
- Contributed to the design and development of course materials and examinations, incorporating up-to-date security practices and emerging threats to maintain the relevance and rigor of the curriculum.

Programmer Analyst Trainee

Cognizant Technology Solutions - Bangalore, India Sep 2021 - Aug 2022

- Investigated anomalies and suspicious activities to assess potential threats to the organization’s assets.
- Conducted security scans for internal applications, identified and remediated vulnerabilities, and configured Single Sign-On (SSO) to enhance data protection.
- Performed detailed forensic analysis of security incidents to determine the root cause and extent of any compromises.
- Collaborated with threat intelligence teams to identify emerging threats and indicators of compromise (IOCs) for proactive threat detection.
- Managed and maintained security tools, including EDR platforms, ensuring proper configuration, tuning, and integration with other security systems.
- Identified and addressed security events that posed risks to the confidentiality, availability, and integrity of information, ensuring compliance with federal laws and HHS policies.

- Continuously assessed and strengthened security controls based on industry standards, regulatory requirements, and best practices, including NIST Cybersecurity Framework and ISO/IEC 27001.
- Demonstrated expertise in incident response and effective communication during security events.
- Applied deep knowledge of intrusion analysis techniques to enhance threat detection and mitigation strategies.
- Utilized skills in security incident investigation and log analysis to promptly identify and respond to breaches.
- Demonstrated experience in investigating security incidents, threats, and vulnerabilities, leveraging extensive knowledge of cyber threats and attack vectors.
- Proficient in identity federation protocols, including SAML, OAuth, and OpenID Connect, to ensure secure authentication and authorization processes across multiple systems and applications.
- Developed and maintained comprehensive documentation of security and network alerts, and reviewed suspicious emails submitted by staff.
- Created detailed technical and procedural documentation for the vulnerability management program, designed reports and metrics, and communicated areas of concern to management.
- Expertly analyzed system data, including security event logs, system logs, and firewall logs, to accurately identify security incidents and trends.
- Applied the MITRE ATT&CK framework for in-depth threat analysis and utilized CrowdStrike for threat hunting and incident response.
- Acted as a subject matter expert on security-related matters, providing clients with guidance on risk management strategies, incident response planning, and security architecture design.
- Proficient in deploying and managing security monitoring tools such as SIEM, IDS/IPS, and endpoint detection and response (EDR) systems.
- Participated in the on-call rotation to provide 24/7 support for critical security incidents, demonstrating a commitment to maintaining the organization's security posture.
- Assisted in the development and execution of security awareness training programs for employees, promoting a culture of cybersecurity awareness and best practices.

Cyber Security Analyst Intern

Hindustan Shipyard LTD - Vizag, India **May 2019 - Jun 2020**

- Monitored and analyzed security alerts from various sources, investigating potential security incidents to assess their nature and scope.
- Executed real-time incident detection and response activities, ensuring rapid containment and mitigation of security threats.
- Conducted incident triage to evaluate the accuracy, scope, urgency, and impact of security incidents.
- Coordinated incident response efforts and provided updates to OpDiv Incident Response Teams (IRTs) and HHS, following CSIRC methodologies.
- Informed CSIRC management and HHS IRT members of suspected incidents, detailing event history, status, and potential impact.

- Skilled in implementing and managing identity and access control systems.
- Experienced in deploying authentication and authorization mechanisms to secure access to resources.
- Analyzed and responded to previously undetected threats or potential security risks.
- Conducted in-depth analysis of security events using SIEM tools, IDS/IPS, and other security technologies to identify malicious activities.
- Supported and maintained organizational identity governance initiatives and managed the firm's Privileged Access Management (PAM) platform, ensuring proper access controls and regulatory compliance.
- Ensured that the identity and access management program protected the entire environment, including cloud services and high-performance computing environments.
- Triaged alerts and incidents to identify potential threats and operational issues.
- Monitored network infrastructure to ensure maximum uptime and promptly addressed any degradations or outages.
- Managed agency-wide event and incident tracking using a ticket management system.
- Tracked and reported ongoing cybersecurity incidents to the primary incident handler.
- Responded to verified incidents using a wide range of tools to mitigate active threats.
- Collaborated with the security team to conduct tests and identify network vulnerabilities.
- Worked with cross-functional teams to coordinate and implement security measures, ensuring compliance with established policies and procedures.
- Developed and maintained comprehensive documentation of incident reports, response activities, and post-incident analysis for continuous improvement.

PROJECT DETAILS

Fortifying Cloud Ecosystems - Navigating the Multi-Layered Security Paradigm

- Includes network security, data encryption, IAM, application security, and incident response.
- Each layer addresses specific security challenges for robust threat protection.
- Uses machine learning-based anomaly detection and real-time monitoring for quick response.
- Correlates data from various sources for a comprehensive cloud security view.

Virtual Telepresence Robot for Secure Remote Monitoring

- Utilized Python for precise control of robot movements and hardware integration.
- Implemented encryption to secure video feed, control commands, and sensor data.
- Connected to a cloud-based platform for remote access and control via a secure web interface or mobile app.
- Incorporated authentication mechanisms, IDS, and firewalls to protect against unauthorized access and cyberattacks.
- Equipped with HD cameras for real-time video, with cloud processing and storage ensuring low latency.