Prem Madishetty

+1 (369) 210 7491 | San Diego, CA | pmadishetty7420@sdsu.edu | LinkedIn

EDUCATION

San Diego State University, San Diego, USA — August 2024 – May 2026
Master of Science in Cybersecurity Management — GPA: **3.97/4**

EXPERIENCE

AI Security Researcher — Oct 2024 – May 2026

AI4Business Lab, San Diego State University — San Diego, CA

- Fine-tuned **GPT-2** to summarize **Cyber Threat Intelligence Reports** and to identify actionable **IOC** for a 40% improved efficiency.
- Developed a novel system to reduce LLM hallucinations by 14%, using **RAG**, Agentic **AI** Systems and frameworks like **AutoGen**.
- Designed an **NLP** model to detect phishing emails by analyzing patterns, improving **email threat detection** accuracy by 30%.
- Built an AI Anomaly Detection System to identify network patterns, enhancing **DDoS** and data exfiltration detection by 25%.

Incident Response Analyst

TCS — **May 2023 – July 2024**

- Achieved 100% SLA compliance by **Incident Management**: creating dashboards & documenting findings of Incidents.
- Designed, Updated, and Optimized **SOAR** playbooks to automate tasks and enhance incident response efficiency by 40%.
- Resolved 20+ high-priority **ZScaler** incidents by analyzing traffic (**Wireshark**) & collaboration with partners to restore BAU.
- Automated **Phishing** alert workflow using **UI Path**, notifying stakeholders in real-time, reducing incident response time by 40%.
- Implemented a robust **Business Continuity Program** (BCP) ensuring 100% uptime for critical infrastructure and operations.
- Enhanced operational efficiency by creating 12+ **SOP** s to standardize processes and to promote security awareness in team.

SOC Analyst

TCS — **May 2021 – April 2023**

- Fine-tuned **SIEM** alerts and enhanced log correlation by reducing false positives and accelerating threat detection by 35%.
- Ensured 100% compliance with **IPS/IDS** signature updates through proactive change control and change tickets.
- Delivered **Cyber Threat Intelligence** with attack vectors, IOC & mitigation strategies for accelerating threat detection by 30%.
- Accelerated Policy Enforcement through **GRC** driven risk assessments, ensuring timely approvals and 100% compliance.
- Used CrowdStrike for sandbox-based **Malware Analysis** on 50+ phishing emails to strengthen email threat protection setup.
- Managed Zscaler **WAF** by handling incidents and liaised between customer and vendor to ensure 100% firewall uptime.
- Led **Forensic** investigations on **Tanium** alerts to identify & mitigate incidents and document findings to refine flow by 25%.
- Drove **Vulnerability Management** by scans, ServiceNow tickets, remediation & GRC requests to maintain 100% compliance.
- Reported 7 data exfiltration efforts using **EDR** by tracking RSD, print, and emails to thwart reputation and financial losses.
- Enforced **IAM** key rotation policy every 90 days on **AWS** servers to boost **Cloud Security** posture & ensure 100% compliance.
- Ensured 100% **NIST** & **ISO 27001** compliance for nuclear and renewable sites by enforcing contractual security controls.

PROJECTS

VPN Server Setup on AWS Cloud

- Deployed a t2.micro **EC2** instance with Ubuntu & OpenVPN Access Server to route traffic securely for mobile VPN connectivity.
- Configured AWS **IAM** roles, **S3** buckets for log storage, and **Security Groups** to enforce inbound and outbound traffic rules.
- Applied **ZTA** principles to ensure access control, continuous monitoring, optimized performance and 100% privacy of traffic.

Honeypot Deployment on AWS Cloud

- Configured AWS Cloud infrastructure (**EC2, VPC, IAM** roles) to deploy the **T-Pot** honeypot for threat monitoring.
- Captured Attack Vectors and **IOC**s like Malicious Payloads & Malicious IPs for making automated **threat intelligence** reports.
- Analyzed and visualized data using graphs and **heat maps**, to detect environment-specific emerging attacks and plan defenses.

IoT Device Penetration Testing and Exploit Analysis

- Performed **Network Reconnaissance** with Bettercap to discover IoT devices & captured unencrypted traffic with **Wireshark**.
- **Exploited** smart bulbs using Python and Bettercap via Telnet sessions leveraging lack of authentication and encryption.
- **Documented** security weaknesses in IoT ecosystems, outlining threat vectors, network exploits, and mitigation strategies.

SKILLS

- ***Operating Systems:*** Linux, Windows Server, Ubuntu
- ***Scripting Languages:*** Python, Bash, PowerShell, R, JAVA, SQL
- ***Protocols:*** ZTA, PQC, SSL/TLS, IPsec
- ***Compliance Standards:*** GDPR, HIPAA, SOC 2, NIST, ISO 27001
- ***Soft Skills:*** Attention To Detail, Critical Thinking, Problem-Solving, Effective Communication, Collaboration and Teamwork

CERTIFICATIONS

- Certified Ethical Hacker (***CEH***) from *EC-Council*
- ***CompTIA Security +*** from *CompTIA*
- ***Generative AI Fundamentals*** from *Data Bricks*