Jose Enquito

10197 Caminito Zar, San Diego, CA • +1 858-610-6635 • jhei.enquito@gmail.com
• linkedin.com/in/jose-enquito-5a4b05a8/ • https://jenquito.github.io

Cybersecurity Engineer

6 Years of experience focusing on cybersecurity risks, threat analysis and detection, and vulnerability assessment. Reduced risks of data exploitation and malicious attacks by 45% in 6 months using cyber defence frameworks, threat intelligence, network security and traffic analysis, endpoint security monitoring, digital forensics, cryptography, incident responses, and SIEM.

WORK EXPERIENCE

Abbott Diagnostics • 11/2021 - Present
Cyber Security Engineer

- Conducted weekly security operations for phishing alerts, Security Operations Center (SOC) tier 2 alerts, and 40+ security events. Managed the company's DNS, email, VPN and firewall infrastructure achieving uptime for SaaS offering with 200+ users.
- Executed firewalls, IDS/IPS, SIEM, DLP, XDR, and endpoint security solutions to reduce malicious attacks by 66% up to date
- Performed penetration testing on devices to remediate vulnerabilities, improving security posture by 57%
- Conducted security awareness training for 200+ employees, improving security awareness of the workforce.
- Designed security solutions to protect the company's IT infrastructure against cyber-attacks, reducing the number of security incidents by 70%.

Dexcom Inc. • 02/2019 - 04/2021
SOC Analyst I

- Performed threat analysis in a 24/7 environment, mitigating, and managing all threats and risks to a company using Splunk (SIEM) to achieve 90% security in data in conjunction with detecting real-time threats, and analyzing recorded traffic files while identifying anomalies using Snort.
- Knowledge of Kali Linux VM to assess vulnerabilities and security of company without compromising company host computers.
- Decreased cyber security risks by 25% in through proactive threat detection and response techniques incorporating Unified Kill Chain methodology, CIA Triage, and using OSINT resources to identify any potentially malicious files, urls, and hashes.
- Implemented MITRE ATT&CK Framework and D3FEND to discover, mitigate, and report potential attacks on the system and the network as well as contribute to MISP to reverse engineer potential malwares and better protect the system from any malicious attacks.
- Conducted vulnerability assessment and inspection of malicious files using Loki with knowledge reference with Valhalla.
- Conducted CIRT after penetration testing using GVM and Armitage/Metasploit, sending payload to the system to measure the vulnerability of the system to report the integrity of the security and its network.

Hewlett Packard • 03/2013 - 08/2015

Security Analyst

- Scanned local computers and websites for malware and security risks regularly, saving more than 200 computers and laptops from unwanted threats and vulnerabilities.
- Quarantined and removed unwanted programs and issues found to establish and ensure security
- Performed regular packet analysis using Wireshark to ensure network traffic flowing between client and server is encoded, tracing connections, and identifying any potential bursts of network traffic that may raise suspicion of a potential attack.
- Updated security plans to meet NIST 800.53 security standard as a team.

EDUCATION

Bachelor Of Science In Information Technology Polytechnic

Arizona State University

Associate Degree In Computer Science

Southwestern College

CERTIFICATIONS

AWS Certified Cloud Practitioner

Amazon Web Services

SKILLS

Cryptography, Cyber Kill Chain, Cyber Threat Intelligence, Endpoint Security, Extended Detection Response, Kali Linux, Linux, Metasploit, Microsoft Sentinel, Nessus, Network Mapper, OSINT, Penetration Testing, Performance Improvement, PowerShell, Python, Risk Analysis, Security Information and Event Management, Snort, Threat Detection, Threat Modeling, Unified Kill Chain, Vulnerability Assessment, Wireshark