Mustafa Ozpay

Cyber Security Analyst

San Antonio, United States, 78253, Fully Work Authorized · No Visa Sponsorship Required · Remote, 8328961434, mr.ozpay@gmail.com

Professional summary

Cyber Security Analyst with 7 years of experience specializing in incident response, vulnerability assessment, and threat hunting. Demonstrated expertise in utilizing custom platforms and OSINT tools to enhance security measures across various operating systems. Committed to advancing security compliance and risk management through innovative solutions and continuous improvement.

Employment history

Cyber Security Analyst, Aug 2020 - Present

HPS, San Antonio

- Led investigations on endpoint devices, by using Uptycs Inc. custom platform.
- Investigated file integrity monitoring system to detect potential Indication of Attacks/Compromises.
- Monitoring endpoint users to search/find Vulnerabilities.
- Threat hunting using custom platform to investigate security opening in different operating system, environments such as Windows, Linux, MacOS, Containers.
- Handled the offenses, analyzed the logs, collected/correlated, Threat Intelligence.
- Conduct analysis to determine the legitimacy of files, domains and emails using OSINT and sandbox tools.
- Improved service level agreement of provided solutions to the customers.
- Created tickets for escalation to IR/Engineering when necessary by Jira.
- Created tickets for communicating internally within different teams, using Jira.

IT Manager, Aug 2017 - Jun 2020

SST, Houston

- Led IT team, ensuring smooth operation and maintenance of school's IT infrastructure.
- Oversaw Cisco phone setup and management, ensuring reliable communication.
- Managed networking infrastructure, supporting a connected school environment.
- Administered print and file servers, ensuring seamless access for staff and students.
- Provided hands-on support for complex technical issues, minimizing disruption.

Skills

Vulnerability Assessment, Network Security, Data Encryption, Security Compliance, Malware Analysis, Risk Management, Threat Hunting, OSINT Analysis, Log Analysis, Endpoint Security, Incident Management, Penetration Testing, Cloud Security, Data Loss Prevention, Identity Management, Security Automation, SIEM Management, Threat Intelligence, Cryptography, Access Control, Incident Simulation, Digital Forensics, Security Policy, Threat Modeling, Security Awareness, Firewall Management, Data Privacy, Security Training, System Hardening, IoT Security, Security Architecture, Vulnerability Management, Social Engineering, Incident Response Planning, Network Forensics, Security Monitoring, User Access Management, linux, system admin, CrowdStrike, FireEye, Splunk, QRadar, Nessus, Qualys, Nmap, Kali Linux, Malware Analysis, Phishing Analysis, Email Analysis, TCP/IP & OSI layers, Network Protocols, Wireshark, Java, Python, JavaScript, SQL, Unix, Linux, Windows, MacOS.

Education

Master of Science in Computer Science, May 2022 - Aug 2023

North American University, Houston

- **Cybersecurity Assessments:** Conducted comprehensive assessments involving PfSense installation on VMware, Security Onion, and Splunk.
- **Vulnerability Detection:** Identified and addressed vulnerabilities in Linux and Windows machines.
- **Threat Analysis:** Detected and analyzed threats and Nmap scans using Security Onion.