Sarp Parmaksiz

in www.linkedin.com/in/sarp-parmaksiz ☎ +1 (669) 254 6946 📍 San Jose ✉ sp.sarpp@gmail.com

Core Competencies

- SIEM
- OWASP Top 10
- Awareness Training
- Security Protocols
- ELK Stack
- Secure Development Lifecycle

Experience

Cyberpulse Inc.

May 2020 – Present

SOC Security Analyst

- Performing security monitoring, incident response and vulnerability management activities in a 24x7x365 SOC environment
- Analyzing, investigating and escalating security alerts from security information and event management (SIEM) system
- Developing and analyzing dashboards, and reporting anomalous/suspicious activities
- Contributing the development of security monitoring and incident response processes

Winslow Automation Inc. / Six Sigma

CGA Process Engineer

May 2018 – Present

- Creating curriculum and increasing awareness of cyber threats for the company (CMMC Requirement)
- Designing and implementing a test method which reduced misalignment rework rates from 20% to under 7%
- Leading various teams in closing 17 CAPAs as leader and worked on numerous CAPAs as a team member to contain and mitigate current problems, and prevent possible future problems
- Directed and supervised physical dimensions testing, CMM programming, XRF operations, pull and shear tests
- Trained Test Services personnel on concepts and procedures, and authored the certification tests to continuously educate and assure competency

Education

San Jose State University

- M.S. Software Engineering – Cybersecurity (3.8/4.0 GPA) September 2019 – October 2021
- B.S. Industrial Technology – Manufacturing Systems Concentration (3.0/4.0 GPA) August 2014 – May 2018
- Minor – Business Management
- ASQ Internal Auditing Basics Certificate

Projects

September 2019 – Present

Parsing .tlv

Goal: Successfully extract signed certificate file with parsing program and perform SDL activities

- Established a security baseline to comply with CIA triad requirements
- Initiated gap analysis to identify areas that are non-compliant with the security baseline
- Created a threat model using OWASP Threat Dragon to identify possible threats
- Performed static analysis (SAST) using Bandit and PyLint to determine and mitigate any security vulnerabilities and code style violations
- Implemented Fuzzing using Peach Fuzzer to find and patch bugs

Malware Obfuscation

Goal: Reverse engineer the given malware, modify the malware and elude firewall signature detection

- Reverse Engineered the "Eicar" malware using IDA disassembler
- Embedded "dead code" into malware body and reassembled.
- Before the dead code, the "Eicar" was detected by 65 out of 66 engines, after the dead code, only 6 engines were able to detect it

Tools & Skills

- Python
- SAST
- Splunk
- DAST
- Cryptography
- Kali Linux
- Owasp ZAP
- Wireshark
- Metasploit
- Nmap

Achievements

Epsilon Pi Tau Honor Society Member

December 2017 – Present