OWEN H MAKIN

619-385-1439 | Email: OwenMakin@gmail.com | Imperial, CA 92251 | LinkedIn

CYBER SECURITY ANALYST

An ambitious and results-driven graduate of Flatiron School.Possesses strong skills in troubleshooting and research that help technology focused companies drive improvements in their security systems. Experienced in mechanical and electrical systems, and programming and a background in CNC robotics.

TECHNICAL & LANGUAGE SKILLS

- Programming languages: Python 3, Java (DrJava), PLC (Fagor), LabView (NI)
- Computer Networking Protocols: TCP/IP IPv4 and IPv6, UDP, OSI Model
- Proficient in Linux (Kali-Linux), Windows (7,10), MacOS, iOS
- Understanding of both LogRhythm and Splunk SIEM consoles: initiated logging on the systems and integrating the logs with each console. Deployed both consoles on different VMs.
- Installed Windows Servers, Linux Servers, and virtual machines running Kali-Linux and Ubuntu.

AREAS OF SPECIALTY

- **Business Management:** Client management; Engagement with C-Suite Leadership including briefings; Project management including budgeting and timeline development.
- **Information Management:** Usage of SPLUNK for reporting, alerting, threat hunting, and digital forensics; Monitoring of logs to determine if and when breaches have occurred by using features in SPLUNK such as regex.
- **Security Management:** Network Security across the OSI Model with firewalls, honeypots,and DMZ's; Experience installing and maintaining Endpoint Security and Endpoint Antivirus software; Use of protocols with encryption such as SSH.
- **Penetration Testing & Threat Intelligence:** NMAP, NetCat/Ncat, and Wireshark to identify vulnerabilities; Knowledge of various APT's and their TTP's.

CYBERSECURITY ANALYSIS PROJECTS

CAPSTONE PROJECT

Acme Company (fictitious entity) suffers a severe cyber attack. As a result of the initial evaluation, the existing SOC team is released & a new time is hired. As a member of the new SOC team, we were tasked with determining the extent of the breach and with securing the machines from future breaches by using tools to find and patch vulnerabilities. Gained hands-on experience handling security incidents, including review of raw log files, data correlation, analysis, and conducting security investigations. Hunted for and dissected previously unidentified threats. Differentiate between potential intrusion attempts and false alarms. Recommended usage of intrusion detection and intrusion prevention systems in order to secure the network from future attacks.

- Monitored and analyzed SPLUNK logs exported from machines on the network
- Developed Incident Response Plan and strategy for detecting and responding to security breaches
- Utilized Nmap and Wireshark to perform network discovery, packet capture and traffic analysis.
- Conducted an in depth security investigation of the network to determine the extent of the attack.
- Prepared daily briefs with teammates that were presented to the CISO to monitor progress.
- Presented our findings on breaches and needed patches to secure machines to our CISO.

GOVERNANCE RISK AND COMPLIANCE PROJECT

As a member of a company that designs and manages data centers we were tasked with constructing a plan that fulfilled the growth strategy of the client while also complying with all relevant laws and regulations.

- Developed Security Plan and strategy for maintaining a data center during the project
- Presented our findings on different security controls to the clients management.

OWEN H MAKIN

619-385-1439 | Email: OwenMakin@gmail.com | Imperial, CA 92251 | LinkedIn

CYBER SECURITY ANALYST

PROFESSIONAL EXPERIENCE

CNC Service Technician, **CNC Parts Department**, San Diego, CA 11/2014 - Present

- Traveled to manufacturing facilities all over North America to install and retrofit CNC machines in manufacturing industries such as aerospace, plastics, composites, wood, and medical equipment.
- Worked with upper management of various companies to improve their manufacturing processes by upgrading and installing machines in their factories.
- Trained clients on operating, maintaining, and aligning their machines in house as well as on-site.

PROFESSIONAL TRAINING, EDUCATION, & CERTIFICATIONS

Cybersecurity Analytics Program: Flatiron School **GRAD:** Nov 2020

- More than 450 hours of classroom and lab experience in: hunt analysis, network security, systems security, governance, risk and compliance (GRC), strategy/analysis, threat intelligence and log detection

Western Governors University, Salt Lake City, UT **Expected:** Oct 2021
Bachelors of Science in Cybersecurity and Information Assurance

CompTIA Security+ **Earned:** Mar 2021