Juan Jimenez
(510) 375- 4468
Juan.F.Jimenez88@gmail.com

Summary

Self-motivated professional seeking new opportunities in Cyber Security.
Programming, digital security and Networks have always been my passion, and I am looking to make the next steps into a position which utilizes and develops the skills I have gained in school, work and through active self-study. I am currently working on Pen testing, UNIX, Linux, and windows in my home lab and checking log data for anomalies. I also have working knowledge on how to find threats using Palo Alto servers; this includes going through data sets and daily reports from Palo Alto. Setting up rules on the firewalls to fill many different needs that arise. Verifying anomalies with log ingestion tools such as Splunk.

Skills

● Proficiency in database management

● Threat analysis, and research

● Extensive experience in building and maintaining computer and network environments.

● Software: Deployinator, Security Monkey, Nmap, Wireshark, Maltigo, PagerDuty, Docker, Kubernetes, Opsgenie, and a variety of log ingestion and parsing tools.

● Monitoring Tools: Datadog, PagerDuty, OpsGenie, AlienVault, Sumo Logic, PRTG, NodePing, Splunk and a variety of networking tools.

● Hardware: A10, F5, PaloAlto Networks, Cisco, AWS, VMWare

● OS: CentOS and Windows (All) Experience

Education

Laney College: 2011-Present
Art Institute of Portland: 2007-2008

Experience

Whil Concepts
April 2019 - Present
Lead SOC Analyst

● Create documentation on new policies

● Collect evidence of current policies being followed for SOC 2 compliance and GDPR

● Fill holes found by log analysis and updated security groups securing our AWS infrastructure

● Change over the ISP for more cost effective and secure internet use saving over 20% overall cost

● Create Security Education material

Blend
October 2018 - February 2019
Security Analyst

●Worked across teams, to maintain a secure Infrastructure.

●Researched vulnerabilities and finding solutions to any found issues across company infrastructure.

●Answered any security inquiries from teams about new technologies after assessing the potential impact and weighing the pros and cons of new services.

●Investigated Possible phishing attacks.

●Configured AWS, AWS-config, and leveraging CloudTrail to watch our cloud infrastructure

●Compiled how to guides for new services, and applications

●Created documentation and alerting on security issues.

Tunein
May 2016 - July 2018
Senior Network Operation Center Technician

●Monitored and patched local datacenter and Cloud environments.

●Created, maintained and implemented monitoring integrations for a hybrid environments including AWS, and windows/ Unix.

●Worked across departments to assist with our Virtual and Physical environments .

●Worked with the primary security engineer in assessing external and internal threats. Evaluating new technologies and understanding the risk vs reward of adding them to the environment. Setting up DUO authentication and helping employees understand the value of 2FA

●Created Postmortems, Runbooks, and guides for major service interruptions.

●Linux environment maintenance

●Linux bash scripting.