EDUCATION

Western Governors University | Salt Lake City, UT

BS, Cybersecurity and Information Assurance Anticipated Graduation: April 2022

EXPERIENCE

UNIVERSITY OF CALIFORNIA, DAVIS | Davis, CA

Service Desk Supervisor 2020 – 2021

- Identified an issue with account permission revocation and implemented an account audit which ensured that 100% of these accounts were revoked within 24 hours of termination.
- Administered hundreds of Zoom accounts and several dozen appliances, educating employees on secure communications and ensuring full HIPAA compliance within the context of Zoom. Critical security patches for Zoom appliances were applied within 24 hours.
- Developed a process to create secure accounts for student employees with access to sensitive data, which enforced 100% enrollment in multifactor authentication.
- Created an improved asset management and inventory control procedure using ServiceNow reports and dashboards. Investigation via BigFix revealed an 8% inventory error rate over the previous two years prior to implementation of the new procedure.
- Refined onboarding process leading to more accurate assignment and documentation of user security groups, better conforming to the principle of least privilege.
- Monitored potential cybersecurity incidents such as Sophos Endpoint Security alerts and user reported phishing attempts; critical alerts were addressed within 30 minutes and phishing attempts within 1 hour. As a result of the quick response, no phishing attempts were successful.
- Generated workflows, forms, dashboards, and reports in ServiceNow to track employee metrics and deliver data to stakeholders.
- Managed departmental workload, improving response times by 10%, while also expanding the technical skills of the service desk team.

TRIMBLE NAVIGATION | Folsom, CA

Product Lead 2016 – 2020

- Assigned to key clients to migrate data from their on-site servers to Trimble SaaS product. Directed them in the use and difference to ensure user acceptance.
- Created technical documentation both for clients and analysts. Conducted training of analysts using this documentation to introduce them to new SaaS offerings.
- Monitored Splunk for client issues, error logs, and other information within the SaaS environment to correct performance and connectivity issues for end users.
- Analyzed complex issues, recreating client environments within a virtual lab, fixing the issue if possible, or escalating to development when required.
- Handled software product releases, including verification of the checksum of the final software package.
- Worked closely with partner companies delivering custom implementation solutions to clients, including changes to SQL views and advanced software configurations.
- Managed client expectations, and coordinated client, support, and development meetings to ensure that critical issues were resolved within stated SLA.
- Developed the technical interview test for support analyst candidates, the test covers the analysts ability to follow directions, use multiple sources of information, and solve moderately technical problems. This led to hiring three skilled and versatile employees.

Applications Specialist 2012 – 2016

- Acted as an escalation point for analysts, solving issues with Windows Server, IIS, SQL, DNS, TLS and other technologies. Worked with development to deliver solutions to analysts and clients.
- Set priorities for issues and enhancement requests requiring code changes, enabling development to implement changes based on the actual impact and severity of the item.
- Performed quality-assurance testing, including regression testing and ensuring that product testing was completed before deadlines.
- Worked directly with clients on complex web issues, using tools such as Fiddler to examine web traffic and locate issues within their network or IIS configuration.

Support Analyst 2011 – 2012

- Acted as the single point of contact for high sensitivity and high priority clients. Served as the client advocate.

SIEMENS IT SOLUTIONS | Sacramento, CA
IT Technician 2006 – 2011

- Developed a knowledge base of over 200 items specific to the support of Siemens Mobility Inc, and coordinated and trained three large classes of 50 international employees each on the knowledge items and on remote support for Siemens employees.
- Configured active directory permissions for users, files, and folders, ensuring users only had access required by their job roles, and all accounts were correctly handled during transitions or separations.
- Created PKI cards for employees, enabling multi factor authentication for key employees, encrypted mail, and non-repudiation.
- Conducted physical security audits, finding and correcting 1-4 non-compliance issues each audit and working with the users to correct them. 90% of users did not repeat the same incident.

SUREWEST | Sacramento, CA
Advanced Technical Support 2000 – 2006

- Provided second tier support for video, internet, and telephony.

CERTIFICATIONS

● ITIL 4 Foundations	GR671336120BB
● Security +	4G6Z2B7P0LV41GW5
● CySA+	TEW7HP8NVKREQRGV

COMPUTER LANGUAGES AND TOOLS

- ServiceNow
- SQL, Python, Powershell
- Nessus, Nmap, Wireshark, Fiddler, Metasploit, Kibana, Splunk

PROJECTS

- Home Lab running Rocky with Python, Django, and MySQL. Ubuntu for general use. Kali to test homelab and home network for vulnerabilities, using Nessus to scan IOT devices, Nmap to scan the entire network, and Metasploit exercises.
- Red team exercise, using Netdiscover to find hosts on the network, then scanned with Nmap, finding vulnerability with Wordpress implementation, using WPScan. Compromised password using Hydra and retrieved flags. Connected to MySQL and able to query databases.
- Blue team exercise, using Kibana and establishing baselines. Mapped network to locate target operating systems, and ELK stack system. Set appropriate thresholds and created HTTP error notification to alarm from brute force attacks or DDoS. Created HTTP request size monitor at the appropriate threshold to find request sizes over 3500/1 minute, alerting for DDoS or HTTP request smuggling. Finally, set a CPU usage monitor which sets an alarm for high CPU usage, 50%, over a period of 5 minutes, both to monitor server health and watch for indicators of compromise.

ADDITIONAL

- Trimble Navigation: Support Person of the Year 2014, Commitment to Trimble PPM Success 2020
- WGU Excellence Awards: Data Management Applications, Communications