Jocelyn Khuu

Security Engineer | linkedin.com/in/jocelynkhuu | github.com/jocelynkhuu | khuuj.com

EXPERIENCE

AMERICAN SPECIALTY HEALTH **REMOTE, CA**

Info Security Engineer II *January 2024 - Present*

- Managed Crowdstrike Falcon and implemented host firewall policies, sensor updates, exclusions, and created SOAR workflows to automate incident response
- Collaborated with GRC team with providing evidence for HITRUST requirements and audits
- Submit change requests and present production changes to Change Advisory Board (CAB)
- Manage SIEM and ensure logs are ingested, filtered, and parsed according to requirements
- Assist IT with Jamf and MacOS management, troubleshooting policies and configuration profiles

CLOVER NETWORK, INC. **REMOTE, CA**

Security Engineer *January 2022 - December 2024*

- Enabled privileged access management for over 300 users by implementing Britive through Terraform
- Streamlined user access and configured SAML SSO for over 100 SaaS applications using Forgerock IDP
- Managed Google Cloud Platform (GCP) IAM and server permissions through Terraform and Puppet
- Automated OpenLDAP attribute, user, and group management with Python scripts
- Spearheaded and launched an IT asset management system (Snipe-IT) in Terraform, tracking 1300+ IT assets
- Implemented CIS benchmarks and oversaw endpoint security for over 1,200 MacOS devices
- Led incident response and reduced Falcon EDR detection mean time to respond (MTTR) by 70%
- Oversaw Crowdstrike sensor updates and detection/prevention settings for over 1200 devices
- Investigated phishing reports by analyzing URLs, attachments, email headers, and DNS records for threats

PETAL CARD, INC. **NEW YORK, NY**

IT Support Specialist *June 2021 - January 2022*

- Oversaw IT operations by onboarding and offboarding users, administering JAMF, Google Workspace, Okta, GitHub, Slack, Zoom, Zendesk, JIRA, Confluence, and JAMF Pro as sole IT support for over 150 Mac users
- Managed Okta SSO integrations for over 30 SaaS applications and automated tasks in Okta Workflows
- Patched software updates and tracked vulnerabilities in Tenable and JAMF Protect
- Worked cross-functionally to secure IT operations to address issues to meet SOC2 compliance in Vanta

FACEBOOK, INC. **MENLO PARK, CA**

Enterprise Support Tech *April 2019 – June 2021*

- Acted as escalation and on-call for configuration management and client security issues relating to endpoint management by troubleshooting from stack traces and logs and tracking trending issues
- Collaborated with Client Security and Internal Detection and Response Team (IDR) on malware removal and troubleshooting security software such as Santa (binary authorization), MDATP, Carbon Black, and Osquery
- Drove incident response with cross-functional teams from identification to remediation and completed incident reports by querying dashboards to gather logs, identify IOCs, and discover impact

- Spearheaded deployment of Go2Chef (a Chef bootstrapper) to use chef-solo (Chef local mode) for off-corp Linux provisioning, enabling over 2,000 Fedora users to provision systems from home
- Developed Python tool for automated Chef upgrades on Linux systems by dynamically generating JSON config files, bootstrapping Chef with Go2Chef, and querying Chef's Omnitruck API for package downloads

STANFORD UNIVERSITY SCHOOL OF MEDICINE **PALO ALTO, CA**

Computing Support Analyst 2 *April 2018 – April 2019*

- Provided tier 2 desktop support for over 2,000 faculty and staff at Stanford University School of Medicine
- Imaged and deployed Windows 10 and MacOS systems and ensured devices were HIPAA-compliant
- Troubleshot endpoint management software (IBM BigFix) and security software (SCEP) for systems
- Collaborated with InfoSec teams on isolating systems, VLAN migrations, and maintaining system compliance
- Created and modified network database entries for systems and assigned IPs and changed VLANs for systems

FUTUREWEI TECHNOLOGIES, INC. **SANTA CLARA, CA**

IT Support Engineer (Contracted through Intellipro Group, Inc.) *April 2017 – April 2018*

- Provided front-line helpdesk support for multiple locations including over 800 local and remote users
- Lead, created, and presented in weekly IT orientation and served as the point of contact for all new hires
- Educated users on security policies through orientation and reported security incidents to management
- Tracked and triaged tickets through Track-IT, resolving an average of 500 tickets per month
- Created and maintained images, configured user profiles, and deployed Windows 7, 10, and MacOS systems
- Provisioned Avaya VoIP phones by updating VLAN settings and completing firmware updates
- Configured and managed network patch panels, activating ethernet ports and ensuring proper connectivity between switches and end-user devices

EDUCATION AND CERTIFICATES

University of California, Irvine *B.A., Business Economics*
Jamf Certified Expert (Jamf 400) Issued February 2023
Jamf Certified Endpoint Security Admin (Jamf 370) Issued April 2023
Jamf Certified Admin (Jamf 300) Issued November 2022
Jamf Certified Tech (Jamf 200) Issued September 2022