ANDREAS TOH

An **innovative engineer** with experience in **cybersecurity** and **automation** who is eager to take on opportunities in the rapid pace of technological change.

andreastyh@gmail.com
+65-91597698
Singapore, SG
linkedin.com/in/andreastoh

WORK EXPERIENCE

IT Security Engineer
Partners Group FEB 2020 - PRESENT

- Accelerated the firm's patch and remediation resolution time to achieve a higher security posture - Hardening of ciphers and protocols, Zero-day patching
- Implemented the rollout of Crowdstrike EDR agents to a total of 3000 devices
- Deployed the Vectra NDR solution across global office locations to monitor and respond to network traffic for on-premise and cloud environment
- Tested and set up Microsoft 365 Security: Exchange Online Protection, Advanced Threat Protection, Cloud App Security, Insider Risk Management
- Conducted phishing campaigns and remedial training as part of the employee cybersecurity awareness program
- Oversaw Tenable.io vulnerability scanning and the development of SNOW SecOps VR for end-to-end vulnerability management lifecycle

Security Engineer, Networks Security Operations Center
Singtel JUL 2019 - JAN 2020

- Performed Tier 1 & 2 support, event monitoring, triage, analysis, investigation and escalation of real-time security events of multiple business units
- Built a JIRA server as a project management tool, CMDB, KMDB and Service Desk to correlate CVEs with assets for company-wide vulnerability management
- Ensured the timely remediation of security weaknesses identified during VAPT
- Conducted updates of SecOps manuals, playbooks, and documentation
- Implementing, managing and onboarding servers to the SIEM inclusive of development, tuning and optimization of use-cases and correlation rules
- Mentored two junior staff to take on security monitoring and analyst roles

Engineer, Service Operations (Networks)
Singtel JUL 2017 - JUN 2019

- Responsible for Value-Added Services (location-based & eSIM-related) and security-related Operations Support Systems (TPAM, Firewalls and 2FA VPN)
- Provided 24/7 remote and on-site support, security hardening and resolution
- Administered 100+ Linux servers, Windows servers, Fortinet and Cisco network devices with 99.95% uptime
- Increased productivity by identifying and automating processes using Automation tools and Microsoft Visual Basic for Applications
- Cybersecurity Representative, Incident Secretariat and Change Leader

EDUCATION

Bachelor of Engineering (Hons) in Electrical & Electronic Engineering with Minor in Business
Nanyang Technological University AUG 2014 - JUL 2017

QUALITIES

Adaptable | Analytical | Driven | Curious | Focused | Ownership

CERTIFICATIONS

Red Hat Certified System Administrator

Red Hat Certified Specialist in Ansible Automation

Cisco Certified Network Associate

Lean Six Sigma Yellow Belt

ITIL Foundation Certified in IT Service Management by Axelos

EC-Council Certified Ethical Hacker

UiPath RPA Developer Advanced

LANGUAGES

English	●●●●●
Chinese	●●●●○
German	●●○○○

INTERESTS

Cybersecurity
Attend regular meetups for education and networking in Singapore cybersecurity community Div0

Web Development & Design
https://michaeltohphotography.com
Designed static website using HTML, CSS and JS and hosted on AWS

Machine Learning
Set-up home lab using Tensorflow for image classification

TECHNICAL SKILLS

Cyber Security	Trustwave, Splunk + ES, Fortinet, One Identity PAM, Vectra, Crowdstrike, CyberArk, Kudelski, Tenable, Microsoft 365, Open Systems
System Administration	Linux, Cisco IOS, Juniper OS, FortiOS, Windows, Atlassian Jira, ServiceNow
Programming Languages	Unix Shell Scripting/ Bash, SQL, Python, HTML, CSS, JavaScript, YAML, Powershell
Automation	Ansible, UiPath, Microsoft VBA, Powershell + Task Scheduler
Methodologies	Agile, ITIL
Cloud Platforms	Amazon Web Services, VMWare, Huawei OpenStack
Monitoring	Grafana, Nagios, Cacti