ANDREAS TOH

Cybersecurity Engineer

Singapore, SG

✉ andreastyh@gmail.com

linkedin.com/in/andreastoh

andreastoh.com

PROFILE

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

Andreas is equipped with deep technical knowledge in systems & network, complemented with excellent project management skills, specialising in security solutions implementation and operations.

He is naturally curious, and is currently learning AWS, Machine Learning and German.

EDUCATION

Bachelor of Engineering (Hons) in Electrical & Electronic Engineering with Minor in Business

Nanyang Technological University

2014 - 2017

Diploma, Engineering with Business

Singapore Polytechnic

2009 - 2012

SKILLS

- Cybersecurity
- SysAdmin
- Automation
- Integrity
- Analytical
- Adaptable

LANGUAGES

English	Chinese
Native	Native

EXPERIENCE

IT SECURITY ENGINEER

Partners Group — Feb 2020 - Present

- Developed and implemented an end-to-end vulnerability management solution to manage vulnerability lifecycles
- Accelerated the firm's patch and remediation resolution time to achieve a higher security posture - Hardening of ciphers and protocols, 0-day patching
- Deployed Endpoint & Network Detection & Response solution across global offices to monitor network traffic and respond to threats for on-premise and cloud environment
- Main Subject Matter Expert for email security architecture and operations
- Conducted the employee cybersecurity awareness program including internal phishing campaigns and training
- Plan and review of penetration testing & red teaming on internal systems
- Analyze security gaps and evaluate next-generation security tools to close the gaps

SECURITY ENGINEER, NSOC

Singtel — Jul 2019 - Jan 2020

- Performed Tier 1 & 2 support, incident response and investigation of real-time security events for multiple business units using Splunk and SIEM tools
- Self-deployed a project management tool, CMDB, KMDB and Service Desk to correlate CVEs with assets for company-wide cybersecurity management
- Ensured the timely remediation of security weaknesses identified during VAPT
- Conducted updates of SecOps manuals, playbooks, and documentation
- Implemented, managed and onboarded 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

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+ servers and network devices with minimum 99.95% uptime
- Monitored system performance and metrics using open-source tools such as Telegraf, InfluxDB and Grafana and Elasticsearch, Logstash and Kibana.
- Increased productivity by identifying and automating processes using Automation tools such as Ansible and Microsoft Visual Basic for Applications
- Cybersecurity Representative, Incident Secretariat and Change Leader

CERTIFICATES

- AWS Certified Solutions Architect Associate
- Microsoft 365 Certified: Security Administrator Associate
- Red Hat Certified System Administrator
- Red Hat Certified Specialist in Ansible Automation
- Cisco Certified Specialist - Enterprise Advanced Infrastructure Implementation
- Cisco Certified Network Associate
- Lean Six Sigma Yellow Belt
- ITIL Foundation Certified in IT Service Management
- EC-Council Certified Ethical Hacker
- UiPath RPA Developer Advanced

INTERESTS

Cybersecurity   Technology   Fitness   Music