RYAN BERTULFO

+65 81219509 • ryanbertulfo@gmail.com • Singapore • LinkedIn • Github

IT Operations Specialist with 6+ years of experience in **Network Operations (NOC)** and **first-level Security Monitoring (SOC)** within enterprise and government environments. Proven ability to operate in 24x7 shifts, adhering to ITIL best practices and compliance standards, expertise in infrastructure monitoring, incident response, threat detection, and cloud security operations. Hands-on experience with Cisco network devices, AWS security tools, and various observability platforms. Adept at collaborating with cross-functional teams to resolve incidents, ensure compliance, and maintain high service uptime. Certified in ***AWS Solutions Architect***, ***CCNA***, ***ITILv4, ISC2 CC*** *and* ***IBM Cybersecurity Fundamentals***.

PROFESSIONAL EXPERIENCE

NCS Group Singapore, Singapore **Jul 2018 - Present**
Infrastructure Executive, Network – Assistant Infra Lead
(Equivalent to Network\Security Operations Specialist)

Leadership & Team Management: Lead 5 NOC Engineers, strict documentation and implementation of SOP, managed onboarding/training, unconventional shift and schedule adherence with optimized workflows, and ensure project efficiency.

Server/Network Monitoring, Observability Operations & 1st level Cybersecurity Threat Detection:

- Operate within a **24x7 NOC/SOC environment**, ensuring availability and security of enterprise systems through proactive monitoring and structured **shift scheduling adherence**.
- Monitor **AWS\AMS Cloud Services, Server and Network Infrastructure,** includes wireless access points, security controllers, security devices and switches with SolarWinds, CA Spectrum, eG Monitoring and AWS CloudWatch.
- Monitor and analyses **security events** using **Splunk**, **AWS Log Insights, WAF & Shield**, and **CloudWatch**; escalate Indicators of Compromise (IOC) to Tier 2 analysts following defined SOPs.
- Serve as ***Agency Admin Point of Contact*** for **GCSOC** (Govt Cyber Security Operations Center) using **Google SecOps**, **GASSP** (Govt Agency Self Service Portal), and **WOGAA** (Whole of Govt Application Analytics), coordinating on government cybersecurity compliance for websites and device security and availability.
- Perform **IOC searches** on network login logs, DB utilization patterns, and bandwidth activities; analyses vulnerabilities and raise alerts using **Splunk**.
- Utilize ticketing systems such as **ServiceNow** for accurate incident tracking, documentation, escalation, root cause, resolution and closure aligned with **ITIL best practices**.
- Investigate **WAF** alerts breach with **CW Log Insight**, government website placement leveraging **Regex patterns**, and document actions with full traceability.
- Automate **AWS EC2 alarms** (onboarding/offboarding) with **CloudFormation** for CloudWatch monitoring. GCC **CyberArk** device and users' management Process Improvement:
- Generate Spectrum **availability** and **AWS EC2 reports**, streamlined comprehensive documentation, and updated leadership on alerts.
- Generate **GCSOC** Monthly reporting of Incidents (formerly **CTP**) for agency compliance and audit.
- Collaboration: Partnered with Network/SysOps (Support Operations) Teams and Support vendors to reduce resolution times and optimize cloud infrastructure.
- Manage **RSA Admin Console** for user/device onboarding, monitor network routers, and troubleshoot VPN routing issues.
- Collaborate with internal teams and external vendors to reduce Mean Time to Resolution (**MTTR**) and enhance security postures.
- Generate **GCSOC** Monthly reporting of Incidents (formerly **CTP**) for agency compliance and audit.

Professional Development: Cybersecurity Training | Self-Study and Home Lab Practice – 2025

- Actively studied ***MITRE ATT&CK, SANS Incident Response Framework, and Cyber Kill Chain***, applying concepts in home labs to simulate threat detection and incident response scenarios.
- Developed practical skills through online security platform challenges, focusing on bridging theoretical knowledge of security frameworks with real world application.
- Created home lab environments to practice cybersecurity techniques, preparing for hands-on roles in SOC.
- Demonstrated commitment to continues learning by engaging with platforms like HTB, THM and other free resources to enhance practical expertise.

NCS Group Singapore, Singapore **Jun 2012 - Jun 2018**
Help Desk Specialist (Assistant Team Lead)

- Provided first-level technical support for 500+ employees, resolving hardware /software, and network issues with a 98% satisfaction rate.
- Administered user accounts, VPN, Citrix, and SharePoint access, ensuring smooth onboarding and offboarding processes for 200+ new hires annually.
- Generated weekly reports on incident resolution and critical root cause analysis, achieving 95% SLA compliance.

EDUCATION

Southwestern University, City of Cebu, Philippines, Bachelor of Science in **Information Technology**

CERTIFICATIONS

AWS Certified Solutions Architect – Associate (**AWS -SAA**)

Cisco Certified Network Associate (**CCNA**)

Cisco Verified Level 200 – Understanding of Cisco Network Devices

ITIL v4 Foundation in IT Service Management

IBM Cybersecurity Fundamentals

Certified Data Center Facilities Operations Manager (**CDFOM**)

Cisco Linux Unhatched

ISC2 Certified in Cybersecurity (CC)

Core Competencies

Security Operations: DDoS Mitigation, Access Control, SOC Monitoring, CyberArk, GASSP, WOGAA, RSA Admin
Incident Management: ServiceNow ITSM, BMC Helix, ITIL v4, Documentation, SOP Compliance, Ticket and Escalation
Security Frameworks: Knowledge of MITRE ATT&CK, SANS Incident Response Framework, and Cyber Kill Chain
Network Operations: Cisco Devices, VLAN Configurations, TCP/IP Model, OSI Layer Analysis
Monitoring & Analytics: eG Monitoring, CA Spectrum, Cloud Watch, SolarWinds, Splunk
SIEM Tools: Google SecOps (Chronicle), Splunk, Elastic Stack
Scripting/Automation: Basic Python, Bash, Linux PowerShell & *familiar with* Solidity
Soft & Cognitive Skills: Critical Thinking, Problem Solving, Attention to Detail, Creative Thinking, Communication & Collaboration, Adaptability, Threat Analysis

Additional Information

Employment Status in Singapore: S Pass

Citizenship: Filipino