RYAN BERTULFO

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

Security Operations Analyst (SOC) | Threat Detection & Incident Response

Security Operations Analyst with 6+ years supporting Singapore government environments, specializing in SIEM monitoring, malware investigation, IOC validation, and incident escalation within regulated cloud and on-prem infrastructure. Experienced across Splunk, Google Chronicle, Elastic SIEM, and Trend Micro Vision One. Skilled in malware alert analysis, hash-based validation, false-positive reduction, IR reporting, and coordination with L2 SecOps, pen testers, and agency CISO/SIRO stakeholders. Strong foundation in network, endpoint, and cloud security monitoring, with proven reliability in 24/7 operations.

Core Skills and Technical Competencies

Security Operations & IR: IOC validation • alert triage • Threat verification • IR reporting • Malware Inv • Inc Escalation
Detection & Monitoring: Elastic SIEM • Sysmon pipelines • Detections • Dashboards • Telemetry interpretation
Cloud & Infrastructure: AWS CloudWatch • WAF • Shield • EC2 monitoring • CloudFormation onboarding automation
Networking & Access: Cisco • VLANs • TCP/IP • RSA SecurID • VPN
Tools: Splunk • Chronicle • Elastic • Trend Vision One • Qualys • Nessus • ServiceNow • Linux • Python (basic) • SolarWinds
Soft Skills: Incident communication • Analytical thinking • Cross-team coordination • Reporting • Shift leadership

Professional Experience

Senior Infra Executive, Network – Team Lead **Jul 2018 - Present**
NCS Group Singapore / APBA TG Human Resource Pte Ltd
(*Security and Network Operations*)

Malware Investigation & IOC Validation

- Investigated malware detections via Trend Micro Vision One, reviewing event metadata, file hashes, execution paths, and endpoint/process activity.
- Conducted hash-based IOC validation, comparing new alerts against historical detection patterns to identify reused files vs. new unknowns.
- Verified alerts against pentest activity and maintenance/patching/Nessus scan windows to eliminate noise and false positives.
- Identified real threats from GCC cloud workloads and escalated qualified incidents to L2 SecOps with supporting evidence.
- Notified and coordinated with agency SIRO/CISO for high-impact or repeated detections, summarizing findings and status.

SIEM Monitoring & Security Analysis

- Reviewed alert metadata and event context across Splunk, Elastic, and Chronicle for security detections involving endpoint, network, and cloud telemetry.
- Performed preliminary security investigations, validating alert criticality and determining escalation requirements.
- Contributed to monthly IR and incident trend reports, highlighting patterns, repeated detections, and risk observations.

Cloud & Infra Security Monitoring

- Monitored AWS workloads using CloudWatch, WAF, and Shield logs to identify anomalous traffic, brute-force attempts, and suspicious patterns.
- Automated EC2 onboarding/offboarding for security alerting using AWS CloudFormation and integrated CW alarms.
- Supported security monitoring and availability for 2,000+ endpoints, servers, and network devices.

Operations Leadership

- Team lead for an 8-member 24×7 monitoring team; improved SOP adherence and reduced incident resolution time by 30%.
- Ensured SLA compliance, accurate incident documentation, and alignment with ITIL processes.

PROJECT PORTFOLIO:

- Elastic SIEM plus Sysmon logs: Log pipelines, dashboards, detections.
- Google Chronicle SIEM Lab – Rule testing and alert workflows
- Splunk EC2 Monitoring Lab – AWS Log detection, brute force detection.
- Cloud Resume Challenge – Terraform, CI/CD, S3, CloudWatch
- Nessus & Qualys Labs – Vulnerability scanning & validation.

NCS Group 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

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

Certifications

CompTIA Security + Certified

ITIL v4 Foundation in IT Service Management

ISC2 Certified in Cybersecurity (CC)

IBM Cybersecurity Fundamentals

Qualys Vulnerability Management Foundation (eLearning)

Splunk Security Operations and the Defense Analyst (eLearning)

Cisco Certified Network Associate (**CCNA**)

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

Cisco Verified Level 200 – Understanding of Cisco Network Devices

Cisco Linux Unhatched

ADDITIONAL INFORMATION

• 6+ years in regulated Singapore government environments.

• Experienced in SOC workflows, pen test coordination, and IR reporting.

• Active SIEM/detection engineering labs across Elastic, Chronicle, Splunk.