ADRIANNE SORIANO

11 Sin Ming Rd Singapore, 575629
☎ +6582509867 | ✉ adrianne.soriano24@gmail.com | adrianne-soriano-20a599146 | adriannesoriano24

SUMMARY

Cybersecurity and IT professional with over 7 years of experience in network security, system administration, and threat detection across both government and private sectors. Skilled in managing security solutions, analyzing threats, and leading incident response. Expertise in SIEM, endpoint protection, malware analysis, and vulnerability management. Strong analytical skills, attention to detail, and a commitment to ongoing learning.

TECHNOLOGY SKILLS

Certifications:
GCIH | eJPT | ISC2 CC | Splunk Power User | CCNA Security | CCNA R&S | Licensed Electronics Engineer

Core Defensive Security Competencies:
Security Monitoring • Threat Hunting • Incident Response • Digital Forensics • Malware Analysis • Vulnerability Management • SIEM Engineering & Analysis (Splunk, QRadar) • SOC Operations • Log Analysis • Network Security • Endpoint Detection & Response (EDR) • Security Automation • Cloud Security

Security Tools & Technologies:

- **SIEM:** IBM QRadar • Splunk • Google Chronicles • Crowdstrike Falcon • LogRythm • ELK Stack • Wazuh
- **Endpoint & Network Security:** FireEye CM NX HX • Trend Micro • McAfee NIPS • Cisco ASA • Fortinet • Sophos • Palo Alto • Zscaler
- **Threat Detection & Analysis:** Suricata • Snort • Wireshark • YARA • Sysmon • Zeek (Bro)
- **Vulnerability & Risk Management:** Nessus • OpenVAS • Qualys • Nmap
- **Digital Forensics & Malware Analysis:** Volatility • Autopsy • FTK Imager • Ghidra • IDE Pro • Cyberchef • Binwalk
- **Incident Response Tools:** TheHive • Cortex • GRR Rapid Response • Velociraptor • RITA • MISP
- **Infrastructure & Platforms:** Windows Server • Linux (RedHat, Ubuntu, CentOS, Kali, etc.) • macOS • On-prem • Virtualization • AWS • Azure

Programming & Scripting:
Python • Bash • PowerShell • JavaScript • C/C++ • PHP • Go • HTML • MySQL

PROFESSIONAL EXPERIENCE

Ensign Information Security - Singapore | August 2022 to Present (2 yrs 10 mos)
Security Analyst

- Conduct in-depth investigations and triage of security events, correlating threat intelligence with real-time alerts.
- Perform enrichment on high-value assets and threat indicators to assess exposure and potential breach impact.
- Lead root cause analysis and post-incident reviews to improve detection and response strategies.
- Analyze suspicious files using static and dynamic methods, supporting malware triage and reverse engineering.
- Assist in ad hoc security operations tasks and cross-team collaboration.

GIC Private Ltd - Singapore | July 2019 to July 2022 (3 yrs 2 mos)

IT Security Engineer

- Deployed and maintained security technologies including firewalls, DLP, antivirus, proxy, and endpoint solutions.
- Administered and supported platforms such as Splunk ES/UBA, Trend Micro Deep Security, FireEye, Cisco ASA, Palo Alto, Zscaler, and Fortinet.
- Performed regular patching, signature updates, vulnerability scans, and compliance checks.
- Managed BAU security operations, ensuring high availability of critical defense systems.
- Conducted weekly agent reconciliation, system health checks, and resolution of security-related incidents.
- Collaborated across teams using tools like JIRA and diagnostic platforms to resolve issues efficiently.

Centrics Networks - Singapore | September 2017 to June 2019 (1 yr 10 mos)
Network Security Engineer

- Implemented and supported firewall and proxy systems across enterprise environments.
- Deployed appliances including Sophos UTM/XG, Palo Alto, Juniper SRX, and Fortinet solutions.
- Configured and troubleshot routing/switching on Cisco, Dell, HP, and Extreme Networks devices.
- Utilized PRTG and Netgain for proactive network monitoring and performance optimization.

Caspo Inc. - Philippines | February 2017 to July 2017 (6 mos)
Network Security Engineer

- Supported network and security technologies including VPN, IAM, DLP, and antivirus platforms.
- Conducted vulnerability assessments and penetration tests using approved tools and methodologies.
- Reviewed firewall rules for compliance and minimized unauthorized access risk.
- Worked with solutions like CyberArk, RSA, Websense, McAfee, and F5 APM/LTM.

Comscentre - Philippines | November 2015 to January 2017 (1 yr 3 mos)
Network Engineer

- Delivered VoIP support across 50+ regional sites using Cisco Unified Comms Suite (CUCM, CUC, IM&P, etc.).
- Managed incidents related to LAN/WAN connectivity and telephony (Jabber, WebEx, HCS, SIP, ISDN).
- Executed enterprise network changes: ACLs, VPNs, routing (static/dynamic), and firewall configurations.
- Performed IOS/firmware upgrades, system backups, and on-call escalations in collaboration with Cisco TAC.

Novare Technologies Inc. - Philippines | February 2015 to November 2015 (10 mos)
Solutions Engineer

- Supported migration of critical applications to cloud infrastructure (Tier 1–3).
- Decommissioned legacy systems and performed secure data backup/scrubbing.
- Provided operational support across both cloud and on-prem environments.

EDUCATION

Bachelor of Science in Electronics Engineering
Mapúa Institute of Technology, Philippines
2007 – 2013