JERRY PAUL ACOSTA CSA+|VCA-DCV|VCA-Cloud

Mobile: +6594296100
Email: fellowjerry@gmail.com

Experienced 6 years in technical and operational Information Technology Cyber Security. Specializing in technical and administrative controls. Combining system security engineering and analysis skills which I have learned through different projects deployments and trainings. As of now I have solely focused on CyberSecurity landscape and reinforcing it with industry standard vendor-neutral cybersecurity certification from Comptia.

Network Security Analyst:

Security Operations Center(SOC) analyst for Singapore's top stocks trading and financial institution with Singapore Exchange(SGX).
Works closely with Symantec(MSS) SOC team to prevent cyber attacks.
Analyse logs for security incidents, escalate and prevent further threats.
Handles security tools such as McAfee SIEM/NIPS/ATD, FireEye HX endpoint, Symantec Endpoint Protection Manager and Messaging Gateway, F5 Silverline anti-DDOS, Zscaler Web Proxy.
Contribute Incident Handling Playbooks in Phishing, Web-defacement and more.

Experience
Network Security Analyst at Intersoft KK
February 2017 - Present
ProjectDetails:
Deployed as Cybersecurity analyst for the top investment holding company in Singapore(Singapore Exchange). To work in their Enterprise Command Center office which managed by leading Cybersecurity solutions provider(HCL), in a 24/7 environment.
Role:
Acting as Tier 2 Security Analyst and Incident Handler
Handling threat prevention and analysis
SIEM(IntelSecurity/Mcafee) incident/offense monitoring and investigation. Alyse threats for signature base blocking.
Collaborates with Symantec's MSS analyst on escalated offenses and alerts.
Monitors NIPS(IntelSecurity/Mcafee) for threats to counteract like Network anomalies and intrusions.
Validating Advanced Persistent Threats for deeper analysis for preparation, detection, containment, eradication and recovery.
Web security analysis for real threat mitigation on web traffic from Spyware and malware detections.
Monitors DDOS event in real-time with F5 silverline cloud solutions, as well as web application proxy configurations.
Investigating and detecting IoC from reviewed logs from multiple sources.
Collaborates with direct employees for immediate response and mitigation on real threats detected.
Collaborates with Infrastructure/Network team to suppress threats detected for remediation and recovery.

Network and Security Engineer
Flow Traders Asia
August 2016 - December 2016 (5 months project)

Performing 2 roles in a High frequency trading organization as Network and Security engineer.
Daily network and security operations tasks.
Monitors real-time network connectivity and security incidents
Security Incident handling and response
Vulnerability Management and remediation
Network connectivity troubleshooting
Wireless LAN setup with WLAN controller
Administering endpoint protection(Symantec) and email email gateway(Ironport)
Formulates Security Playbooks and procedures
Document and Update security policies
Document and Update network design and configurations

IT Security Senior Analyst - Security Operations Center at Fairchild
April 2015 - July 2016 (1 year 4 months)
As an IT Security Analyst I am part of the global Enterprise Information Security team tasked with the responsibility of protecting and securing 24/7 on-premise and cloud-based Fairchild's systems, applications, networks and information/data through the effective use of technologies and processes.

IT Security Analyst - Attack Surface Management at UnitedHealth Group
October 2013 - April 2015 (1 year 7 months)
As an IT Security Analyst, I would support information security policies, standards and procedures to secure and protect data residing on systems. Work directly with user departments to implement procedures and systems for the protection, conservation and accountability of proprietary, personal or privileged electronic data. Generally my work is self-directed and not prescribed. Works with less structured, more complex issues. Serves as a resource to others.
Primary Responsibilities:
- Conducts penetration testing to web and applications to identify certain vulnerabilities
- Administer and maintain user and group security to company wide applications with a high degree of accuracy including: Processing of Requests, Service Restoration and Support of Entitlement Reviews and remediation of exceptions
- Participation in Quality Reviews
- Understand and enforce General Computing Controls
- Communicate with end users through multiple intake requests systems
- Develop and maintain procedure documentation.
- Identify security administration deficiencies, recommend improvements, and assist to implement corrective action
- Execution of month end reporting
- Secondary On-call responsibilities when assigned

Systems Engineer - Security and Optimization at Trends and Technologies Inc.
April 2012 to October 2013 (1 year 7 months)

As a Systems Engineer for Security and Optimization products, I work closely with clients on project-based solutions.
Designing and deploying solutions with Security products like Bluecoat, McAfee, Solarwinds, Riverbed, Fortigate, Checkpoint.

For full details check my LinkedIn profile:
https://www.linkedin.com/in/jerry-paul-acosta-comptia-csa-vca-dcv-vca-cloud-0899b119