Unit 5E Cityland Herrera Tower Makati City
info@peopleplustech.com
www.peopleplustech.com

JOB DESCRIPTION

JOB TITLE:	**Cyber Defense Incident Specialist**
LOCATION:	**Makati (Hybrid)**
Responsibilities	Joining a collaborative team of CyberSecurity experts from US and PH for a client project, as a Cyber Defense Incident Specialist you will be responsible for investigating, analyzing, and responding to cyber incidents within the organization's technological environment or enclave. Ensures that the security requirements to protect the organization's mission and business processes are protected. • Coordinate and provide expert technical support to organization-wide cyber defense technicians to resolve cyber defense incidents. • Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. • Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security. • Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. • Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. • Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). • Track and document cyber defense incidents from initial detection through final resolution. • Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies. • Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. • Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. • Coordinate with intelligence analysts to correlate threat assessment data.

Qualifications and Requirements	• 5+ years of experience in the security field in Cyber & Information Security, Cyber or IT Risk, Security Operations Center, Incident and Problem Management. • Knowledge of ISO 27001/2700, GDPR, ITIL, COBIT and NIST CSF and NIST RMF Frameworks. • Knowledge of cyber and information security assurance, third party auditing and cloud risk assessment methodologies. • Cyber Security or IT Security certifications at any level • Fluency in English required.