Senior Security Operations Center Analyst Senior Security Operations Center Analyst Senior Security Operations Center Analyst - Cargill Apple Valley, MN A highly experienced military all source intelligence analyst with operational leadership experience supporting  worldwide combat operations. Considerable cyber security experience working in command centers for Fortune  companies and cloud environment organizations. Authorized to work in the US for any employer Work Experience Senior Security Operations Center Analyst Cargill - Wayzata, MN November 2017 to Present   Perform real-time proactive security monitoring, detection and response through the use of LogRhythym   Handle incident escalations from L1 analyst conducting a more in-depth analysis of findings   Investigate escalated alerts, triage and forward to CSIRT team for additional investigation   Monitor DLP solution for potential exfiltration of sensitive data   Interact with various business units in an effort to build relationship aimed at improving security posture   Conduct ad-hoc and strategic threat searches based upon tactical and strategic reporting with Tanium   Partner with cyber intelligence team in building internal threat intelligence program   Develop and maintain automation and ticketing systems within Phantom   Work with security specific teams to provide lessons learned and tuning of various tools Senior Intelligence Analyst (1N071) - E7/MSgt Air National Guard - Minneapolis, MN January 2014 to Present   Analyze and evaluate data from multiple sources to gain awareness of potentially suspicious activity   Continuously evaluate and conduct intelligence analysis form ambiguous and vetted sources   Process classified and open source intelligence products and sources   Create and maintain security documentation and standard operating procedures in support of team  responsibilities, including but not limited to security risk assessments and threat management   Maintain an understanding and awareness of the overall threat landscape (cyber, geo-political, terrorism)   Analyze threat system effectiveness against established tactics, countermeasures, and defenses   Identify and communicate ad-hoc request and intelligence data changes with partner teams   Provide tactical and strategic intelligence briefings to support partner teams and operational assets   Brief executive level leadership and large groups on operating environment threat picture to include local and deployed areas   Compose critical reports and provide recommendations on potential adversary courses of action Security Analyst III Patterson Companies - Mendota Heights, MN August 2016 to November 2017 Interfaced with infrastructure team to provide operational input for applicable security policies Developed, tested and implemented incident response playbooks Reviewed information security trends and news sources for emerging threats and vulnerabilities Functioned as NGAV (Cylance) administrator for endpoints and server infrastructure Monitored QRadar and systems for potential occurrences of security incidents and respond using established response playbooks Researched solutions and technologies that provide analysis of network systems to ensure regulatory and internal compliance measures Managed the relationship with security personnel and other teams to provide statistic and metric data Performed multiple assigned technical tasks including research, analysis, and root cause analysis of cyber threats and compromises related to the same Developed and maintain listing of Indicators of Compromise from intelligence feeds and log source information Provided SIEM tuning feedback from log analysis to engineering team reducing white noise Composed incident response event reports for senior leadership review IT Security Consultant United Health Group/Optum Technology - Chaska, MN July 2015 to August 2016 Monitored SIEM (ArcSight) and IDS/IPS (FireEye) feeds to identify possible enterprise threats Investigated, responded to and remediated security incidents Used investigative tools to validate security events such as: consoles for anti-virus, firewalls and IDS/IPS Investigated potential PII, HIPAA and intellectual property violations through the use Symantec DLP software Developed and documented processes and procedures to aid in incident detection and escalation Developed and updated policies and procedures for the general operation of the IT Security Played in an advisory role in application development or other related projects to assess security requirements and controls and to ensure that security controls are implemented as planned Followed detailed operational processes and procedures to appropriately analyze, escalate, and assist in remediation of critical information security incidents Provided technical assistance on enterprise-wide security incident war-room calls, participate in operational exercises Cargo Supervisor US Air Force - North Carolina Air National Guard - Charlotte, NC August 2002 to January 2014 C-130H3 Loadmaster Quality Assurance Analyst M1 Support Services March 2010 to March 2012 Education M.A. in

Intelligence Studies & Terrorism American Military University 2015 US Air Force Non-Commissioned Officers Academy 2012 B.A. in Psychology & Political Science University of North Carolina Charlotte - Charlotte, NC 2008 Skills IDS (4 years), risk assessments (5 years), root cause analysis (7 years), Security (6 years), solutions (10+ years) Additional Information CORE COMPETENCIES  Security Operations (SOC)  IDS/IPS  Teamwork / Support  Intelligence Analysis  Risk Assessments / Security  Cyber Defense Operations  Root Cause Analysis  Intelligence Research  NGAV & EDR Solutions  Disciplined and experienced Military Veteran Intelligence Analyst skilled in all facets of collecting, disseminating, monitoring, and processing actionable intelligence  Resourceful, focused and analytical professional proficient in automated data processing systems, and US government intelligence databases  Real world working experience in 24/7 cyber security operations center monitoring enterprise-wide threat streams utilizing leading edge technologies including cloud-based solutions  Active TS/SCI TK-G Security Clearance

Name: James Rivera

Email: jordan09@example.org

Phone: +1-802-253-7394x702