|  |  |  |  |
| --- | --- | --- | --- |
| RYAN FORTRESS | | 3150 Collingswood Dr.  El Dorado Hills, CA 95762  530.918.8886  [ryan.fortress@gmail.com](mailto:ryan.fortress@gmail.com) <https://www.the4tress.com/> | |
| **PROFESSIONAL OBJECTIVE** | | | |
| To obtain a position that will capitalize on my experience and interests in the following areas:   * Security Operations and Administration * Troubleshooting/Monitoring of Network Security Infrastructures * Development of analysis tools in JavaScript, PHP, and Python | | | |
|  | | | |
| **PROFESSIONAL EXPERIENCE** | | | |
|  | **ThreatConnect Inc.** | | 2015 – Present |
|  | *Sr. Sales Engineer*   * Delivering demos, trials, and workshops based on ThreatConnect’s Cyber Threat Intelligence and Orchestration Platform to the top threat intel teams for some of the largest energy, finance, health and retail customers in the world. * Working with new and existing customers to provide guidance on developing and automating Cyber Threat Intelligence programs. * Authored multiple field integrations to support complex sales which directly lead to exceeding annual sales quota every year.   *Customer Success Engineer*   * Interpreted customer pains and prodvide creative solutions. This included writing custom integrations between ThreatConnect and other security software (SIEMs, firewalls, HBSS, etc.) in Python. * Interfaced with customers to bring their security operations to a higher level by incorporating their analytical process into ThreatConnect and automate many time consuming tasks and lowering MTTR. * Provided training to customers on threat intelligence methodologies/best practices and how to use the advanced features in ThreatConnect to get the most accurate and detailed information on existing intelligence to help lower risk and expedite attribute of attacks.  Managed some of the most difficult customer's expectations, feature requests, and bug reports. | | |
|  | **NSSPlus** | | 2013 – 2015 |
|  | *Sr. Developer*   * Developed a tool (Phoenix) that replaced ArcSight for the Military Health Systems NSOC and saved the organization over $1.2 million per year. * Phoenix enabled analysts to quickly obtain information from multiple sources (IDS/IPS, HBSS, OSINT, etc.) and integrated existing tools (Splunk, ticketing, wiki, etc.) into a single easy to use interface. * Increased analyst productivity by 80% and lowered event and incident response time by 70%. * Enabled analysts to easily communicate each event between shifts with tight nit logging and notification systems. * Application was written in JavaScript, PHP, Python and MySQL.   ***NSSPlus continued…***  *Cyber Threat Analyst*   * Provided support for the ongoing analysis of threats capable of impacting resources being serviced by the NSOC NCD SP activity based on review of programmatic, technical, and daily review of open source intelligence (OSINT) as well as classified threat warnings and bulletins. * Performed daily reviews of cyber threat warnings, bulletins, alerts, and incident reporting documentation and databases produced by the director of National Intelligence (DNI), National Intelligence Council (NIC), Defense intelligence Agency (DIA), National Security Agency (NSA), United States Strategic Command (USSTRATCOM), Joint Task Force Global Network Operations (JTF-GNO), United State Cyber Command (USCYBERCOM), Central Intelligence Agency (CIA), Department of Homeland Security (DHS), and US Computer Emergency Response Team (US CERT). * Coordinate and deconflict threat analysis activities and reporting with existing NSOC IAVM program infrastructure. | | |
|  | **ITT Systems** | | 2009 – 2013 |
|  | *GBS Network Technician*   * Ensure our dedicated network meets DOD-CERT IAVA security standards to provide secure downloads for the US ARCENT G2 Intelligence team. * Install and operate the Global Broadcast System which enables the US ARCENT Command Group and G2 Intelligence/Security to view and analyze UAV feeds from throughout South West Asia. * Completed over 360 maintenance actions and 12 real world missions to provide over 26,800 hours of secure and non-secure communications capability at 99% availability. * Troubleshoot satellite, data, and radio networks as well as Linux and Windows systems when any problems occur. | | |
|  | **General Dynamics IT** | | 2008 - 2009 |
|  | *Network Technician*   * Responsibilities include installation, operation and maintenance of tactical satellite radio equipment for the Coalition Forces Land Component Command (CFLCC). * Network Control Station for six sites which provide a contingency network for all of Third Army’s military posts in Kuwait. * Equipment handled includes AN/PSC 5, ANCD, and Simple Key Loader. | | |
|  |
| **EDUCATION/CERTIFICATIONS** | | | |
| Bachelors of Science in Management of Information Systems, Wester Governor’s University | | | **2015** |
| GIAC Certified Incident Handler (GCIH) | | | **2012** |
| Windows Server 2008 Active Directory, Configuring | | | **2011** |
| ECCouncil Certified Ethical Hacker (CEH) | | | **2011** |
| CompTIA Security+ & Network+ | | | **2010** |
| Associates in Management of Information Systems, University of Phoenix | | | **2010** |
| Radio Systems Operator/Maintainer Certification (Honor Graduate) | | | **2005** |