pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

IT Analyst

Location	Rosslyn, VA
Security Clearance	Secret Required to Start. (TS Preferred)
Years of experience	4+ in the information technology or security field
Education	Bachelor's Degree or Advanced Degree in Computer Science, Law, English, Communications, History, or other related technical or liberal art discipline.
Certifications	Preferred, but not required: • CompTIA Security+ • CompTIA Network+ • Oracle SQL • CISSP • CEH • GCFE
Duties	Project Overview: The Operational Threat and Analysis (OTA) branch of Cyber Threat Analysis Division performs user activity auditing of computer networks (OTA Audit Team) and provides investigative support to counterintelligence and law enforcement elements utilizing industry standard system and network monitoring tools within the State Department and to external agencies (OTA Investigations Team). Job Description: The OTA Analyst conducts in-depth analysis of user activity data employing technical and non-technical disciplines to transform data into actionable information. The primary area of responsibility for the analyst is to examine and analyze data, prioritize significant events for further investigation, correlate information with other information sources to establish context, and to compile noteworthy information into analytic reports for working groups and senior management. Additional queries to be performed include reviewing sensitive electronic and hard copy investigative and intelligence community reporting, collaborating with internal and external entities via working groups, conferences, or task forces, and preparing summary documents, briefings, assessments, graphical representations of data, and other written products. Audit Analyst Role: The audit analyst will conduct trend and anomaly analysis of user activity data and will use data analytic and visualization tools to discern and display potential threat indicators, while also conducting limited inquiries to solidify hypotheses leading to threat resolution. The individual will also support partnering business areas with ad-hoc data reporting, and will perform hands-on quantitative, statistical, and operational analysis to determine and communicate meaningful and actionable patterns, trends, insights and recommendations.

pillarsystems CORPORATION
"Supporting Our Clients Through Pillars Of Excellence"

IT Analyst

Duties

Daily Responsibilities:

Perform network monitoring, analysis and reporting of information security events

- Identify malevolent indicators of system and network activity data, define a source for the data, create policy to produce normalized daily auditable data
- Identify, prioritize, and track relevant cyber events, potential security and policy violations, incidents, and other anomalous activity
- Perform statistical analyses of data for the development of new data management techniques and operational improvements
- Prepare and review threat reports, assessments, briefings, and other written products
- Establish baselines of normal endpoint behavior to support outlier detection
- Core work hours are 9:00am – 3:00pm (8.5 work day), Rosslyn, VA

Investigative Analyst Role:

Daily Responsibilities:

The Investigative analyst will perform user activity monitoring, analysis, and reporting, employing technical and non-technical disciplines to transform data into actionable information; The individual will be responsible for conducting in-depth analysis of user activity data and performing data acquisitions from live hosts located worldwide using various Windows and forensics tools, and ensuring chain of custody and control procedures.

- Responsible for the analysis and reporting of technical and intelligence information to provide indications, analysis, and trends identified through behavioral analysis of data
- Perform assessments of malicious or suspicious activities to determine potential security risks
- Prepare comprehensive and detailed court-ready case documentation and written notes and reports regarding findings.
- Develop Operational Threats and Analysis program policies, processes, and procedures, provide user support, conduct group training sessions, and provide one-on-one tool training services to case agents and supporting personnel.
- Core work hours are 9:00am – 3:00pm (8.5 work day), Rosslyn, VA

Qualifications

Required: Basic Requirements

- At least 2 years experience in a research analyst or data analyst role; preferably in a cyber-security setting
- Knowledgeable of Database systems (Oracle and MS SQL)
- Experience in behavioral, audit, security, and/or policy compliance analysis
- Ability to work well with and accept challenges in a fast paced, dynamic, team-based environment
- Proficiency with MS Office Suite products (Excel, Word, Outlook, Visio, PowerPoint, etc.) and Server
- Strong quantitative and analytic abilities to analyze and validate data
- Ability to demonstrate effective organizational and technical skills
- Detail-oriented and have a strong delivery performance (ability to meet deadlines and requests efficiently, and multi-task and establish priorities)
- Ability to quickly learn and understand various company systems

Qualifications

Desired Skills: Preferred but not required

- Ability to write and execute SQL queries
- Experience with Powershell, Splunk, IBM SPSS platform using the Modeler module
- Experience with designing and implementing data models to drive threat analysis
- Knowledge of cyber threat indicators
- Ability to prepare and present briefings
- Technical knowledge of Microsoft Operating Systems