

ICF - Enterprise Cybersecurity & Resilience

Security Information and Event Management (SIEM) Engineer- Req. 1600004543

Atlanta, GA

\$5000k Sign-on Bonus and relocation assistance available

Job Description:

The SIEM engineer is responsible for the configuration, deployment, and management of the customer's SIEM solution in a 24 X 7 X 365 environment. The engineer is responsible for monitoring, configuration changes, accounts, managing log sources, and software updates for the client SIEM solution. The engineer must be able to analyze, troubleshoot, and remediate issues with the SIEM. The engineer will work closely with other teams to ensure that the SIEM is performing to standard with all necessary logging sources.

Qualifications

Key Responsibilities:

- Act as the subject matter expert for the customer's SIEM solution.
- Maintain SIEM operations and document current environment.
- Work with external teams to ensure all necessary logging sources are reporting to the SIEM.
- Creation of technically detailed reports on the status of the SIEM to include metrics on items such as number of logging sources; log collection rate, and server performance.
- Incorporate change management into all system changes.
- Assist in troubleshooting and problem solving a wide variety of client issues.

Basic Qualifications:

- Ability to maintain a DoD clearance.
- Bachelor's Degree in Computer Science or related technical discipline, or the equivalent combination of education, professional training, or work experience.
- DOD 8570 Compliance, or the ability to quickly obtain the security certifications: Security+, and CEH.
- Minimum of eight years managing/utilizing a SIEM solution.
- Experience in performing infrastructure support at an enterprise level.
- Ability to demonstrate strong knowledge of computer security concepts.
- Demonstrated ability to document processes and procedures.

Preferred Skills/Experience:

- Initiative and a personal interest in Information Technology Security.

- People skills, and the ability to communicate effectively with various clients with the ability to explain and elaborate on technical details.
- Experience with industry recognized SIEM solutions such as ArcSight, Splunk, LogRhythm, AlienVault, etc.
- Relevant IT certifications such as CCNA, CCNP, JNCIA, etc.
- Vendor certification in a SIEM technology.
- Experience with change control policy and procedures.
- An understanding of DOD information assurance policy and regulations.

Professional Skills:

- Excellent verbal, interpersonal and written communication skills
- Strong analytical, problem-solving and decision making capabilities

About ICF:

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with more than 5,000 professionals focused on making big things possible for our clients. We are business analysts, policy specialists, technologists, researchers, digital strategists, social scientists and creatives. Since 1969, government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success. Come engage with us at icf.com.

Point of contact: **Thomas W. Houston** | **Cyber Security Recruiter** | **+1.770-826-5329 mobile** | Tom.Houston@icf.com

ICF | Bldg 3, Corporate Square, Suite 370, Atlanta, GA