Aurora Health Care

Profile Title:	Job Code(s):	Job Title(s):	FLSA Status:
IT Security Analyst Sr.	111085	IT Security Analyst Sr.	Exempt

Aurora Health Care is looking for an experienced, energetic Sr. Security Analyst for our Security Operations Center (SOC). Qualified candidates will lead monitoring for security events, help manage security incident response and conduct forensic examinations.

Major Responsibilities:

Monitor security events via the Security Incident Event Manager (SIEM) system. Assist in enhancing/tuning SIEM rules.

Hunt for potential security events using a variety of tools and methods.

Oversee remediation of security events discovered by the SOC. Collaborate with other teams to ensure proper and timely remediation.

Assists in developing and enhancing SOC responses to incidents (procedures/run books).

Help manage security incidents. Help orchestrate and participate in Security Incident testing.

Conduct forensic investigations using advance technologies and equipment.

Maintains awareness of trends in IT Security, technology and regulatory requirements.

Knowledge, Skills & Abilities Required:

Experience working in an IT Security Operations Center or Incident Response role.

Experience with SIEMs, system and network security and forensic tools.

Extensive knowledge of networks, systems, devices and applications.

Strong troubleshooting, reasoning and problem solving skills.

Team Player with strong customer service, prioritization and time management skills.

Organizational skills and the ability work autonomously with a strong attention to detail and processes.

Ability and experience in writing clear and concise technical documentation.

Strong verbal communication skills and the ability to effectively interact with all levels.

Ability to manage multiple priorities with tight deadlines in a dynamic work environment.

Ability to adapt to changing technologies and learn new technologies.

Aurora Health Care

Physical Requirements and working conditions:

Position may require travel. May be exposed to road and weather hazards.

Exposed to normal office environment.

Operates all equipment necessary to perform the job.

Experience required:

5 years plus of experience in IT Security preferred.

Certifications:

None required. CISSP, CISA or CISM preferable.

This job description indicates the general nature and level of work expected of the incumbent. It is not designed to cover or contain a comprehensive listing of activities, duties or responsibilities of the incumbent. Incumbent may be required to perform other related duties.

To apply, visit http://www.aurorahealthcarecareers.org/