

DealerTrack® *JOB POSTING*

Information Security Analyst, Senior

Responsibilities:

Works under the guidance of Corporate Security to ensure adoption of DealerTrack security standards.

Documents, manages and provides operational support of security procedures for the DT DPS locations (e.g., malware procedures, separation procedures, firewall review procedures, physical or application access procedures, patching procedures).

Implements and maintains business continuity plans and procedures for back-office and assists with disaster recovery efforts for customer-facing systems.

Identifies, implements and manages risk mitigation efforts for operational, physical, network and application security.

Provides security guidance for new business and technical projects to ensure compliance with corporate security standards.

Meets as scheduled, or as needed, with various departments (e.g., IT, HR, Internal Audit, Legal and Compliance); provides updates and information on security issues and responds to requests for information to support compliance initiatives.

Performs security monitoring to identify and resolve issues uncovered by various internal application and network security monitoring tools; escalates to Corporate Security if appropriate.

Performs application security assessments and coordinates remediation efforts for internal or third party applications.

Facilitates and manage customer security audits and requests. Escorts customers to various DealerTrack and vendor facilities.

Qualifications (education, prior work experience, specialized skills and knowledge):

Bachelor's Degree

5-7 years related experience

Expert knowledge and hands-on experience in enterprise security.

Ability to multi-task and work independently.

Ability to apply security principles to business needs.

Knowledge of networking and systems administration.

Understanding of complex Web-based architecture.

Ability to work in a fast-paced environment; ability to work in a team and independently to fix issues with little or no supervision.

Excellent project management skills; ability to build effective working relationships at all levels of the organization; excellent communications skills.

Ability to perform vulnerability assessments/penetration testing using various vulnerability assessment tools.

Knowledge of risk management frameworks and security best practice guidelines (ISO 27001). Exposure to SAS 70 and Sarbanes Oxley audit controls. Familiarity with US laws regarding consumer data.

CISSP, CISM, CISA or GIAC certification required.