Information Security Analysts

SOC: 15-1212 • Career Profile Report

■ Key Facts

$124,910	**182,800**	**+29.0%**
Median Salary	Employment	Growth Rate

■ Requirements & Salary Range

Education: Bachelor's degree

■ Automation Risk Assessment

Low Risk - 12.0% probability of being automated in the next 10-20 years.

This job is relatively safe from automation due to its creative, social, or complex problem-solving requirements.

■■ Work-Life Balance

7.8/10 - Good work-life balance

■ Personality Fit (RIASEC)

Higher scores indicate better personality fit for this career type.

Realistic	7.4/10	**Investigative**	9.2/10
Artistic	4.6/10	**Social**	5.4/10
Enterprising	5.6/10	**Conventional**	6.8/10

■ Top Skills Required

Analytical skills, Communication skills, Creative skills, Detail oriented, Problem-solving skills

✓ Strengths

- High Demand
- Flexible Work
- Continuous Learning

■ Challenges

- Burnout Risk
- Rapid Technological Change

■ What They Do

Information Security Analysts typically perform the following tasks: • Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs. • Monitor current reports of computer viruses to determine when to update virus protection systems. • Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers. • Perform risk assessments and execute tests of data processing system to ensure functioning of data processing activities and security measures. • Modify computer security files to incorporate new software, correct errors, or change individual access status. • Review violations of computer security procedures and discuss procedures with violators to ensure violations are not repeated. • Document computer security and emergency measures policies, procedures, and tests. • Confer with users to discuss issues such as computer data access needs, security violations, and programming changes. • Monitor use of data files and regulate access to safeguard information in computer files. • Coordinate implementation of computer system plan with establishment personnel and outside vendors. • Train users and promote security awareness to ensure system security and to improve server and network efficiency.