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 are cybersecurity professionals who protect **computer systems, networks, and sensitive data from digital threats**. They design, implement, and monitor security measures that safeguard organizations against hacking, malware, data breaches, and other cyber risks. Their work is critical to maintaining trust, privacy, and operational continuity in an increasingly digital world.

This career is well suited for individuals who enjoy problem-solving, technology, and staying ahead of constantly evolving cyber threats.

What Do Information Security Analysts Do?

Information security analysts plan and maintain an organization’s cybersecurity defenses.

Common responsibilities include:

- Monitoring networks and systems for security breaches
- Investigating and responding to cyber incidents
- Implementing security tools such as firewalls and intrusion detection systems
- Conducting vulnerability assessments and penetration testing
- Developing security policies, procedures, and best practices
- Training staff on cybersecurity awareness
- Keeping systems compliant with security standards and regulations

Key Areas of Cybersecurity

Information security analysts may focus on specific security domains:

- Network Security: Protecting internal and external network traffic.
- Application Security: Securing software and web applications.
- Cloud Security: Protecting cloud-based infrastructure and data.
- Incident Response: Detecting, analyzing, and responding to cyberattacks.
- Governance, Risk, and Compliance (GRC): Ensuring adherence to laws and standards.

Skills and Abilities Needed

Information security analysts combine deep technical knowledge with analytical thinking.

Core Professional Skills

Personal Qualities That Matter

Education and Career Pathway

Entering this field typically requires formal education and technical experience:

- Bachelor’s Degree (common): Cybersecurity, computer science, information systems, or related fields
- IT or Network Experience: Often gained through systems administration or support roles
- Professional Certifications (common): Cybersecurity or information assurance credentials
- On-the-Job Training: Learning organization-specific security systems
- Continuous Skill Development: Staying current with emerging threats and technologies

Where Do Information Security Analysts Work?

Information security analysts are employed across nearly every industry:

- Technology and Software Companies
- Financial Services and Banking
- Healthcare and Insurance Organizations

- Government and Defense Agencies
- Consulting and Cybersecurity Firms

Many roles offer remote or hybrid work options.

How Much Do Information Security Analysts Earn?

Earnings vary by experience, industry, and specialization:

- Entry-Level Analysts: Typically earn strong IT salaries
- Experienced or Senior Analysts: Often earn significantly higher compensation
- Specialized or Leadership Roles: May earn more in high-risk or regulated industries

Compensation commonly includes bonuses and robust benefits.

Is This Career Difficult?

This career is intellectually demanding and fast-paced. Analysts must constantly adapt to new attack methods, technologies, and compliance requirements. The challenge lies in staying ahead of threats while maintaining secure, usable systems for organizations.

Who Should Consider Becoming an Information Security Analyst?

This career may be a strong fit if you:

- Enjoy technology and cybersecurity challenges
- Like investigating problems and threats
- Are detail-oriented and analytical
- Can handle responsibility and pressure
- Want a high-impact, in-demand tech career

How to Prepare Early

- Learn networking, operating systems, and basic programming
- Practice cybersecurity fundamentals and ethical hacking
- Study data protection and privacy principles
- Participate in cybersecurity labs, competitions, or internships
- Explore degree programs or certifications in cybersecurity

Information security analysts defend the digital backbone of modern society—anticipating threats, strengthening systems, and ensuring data remains secure, trusted, and resilient in an ever-evolving cyber landscape.

*Generated by StartRight • Data from U.S. Bureau of Labor Statistics & O*NET*

Source: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm