# SSResearch Paper: Thinking Critically About Careers

Gabriel Leslie

Department of Information Systems Technology, Northern Virgina Community College

ITE 152: Introduction to Digital and Information Literacy and Computer Applications

Professor Walter Pehrsson

April 7, 2025

The estimated annual cost of cybercrime committed around the globe is projected to reach 30 billion USD per year by 2025, and 265 billion USD per year by 2031 (eSentire & Cybersecurity Ventures, 2022)[1]. The demand for skilled cybersecurity professionals has surged, making the career path one of the most sought-after fields in technology. The two career paths that I am most interested in are SOC analyst and a security consultant. I chose these career paths based on the parameters of how hard it is to break into these careers, the cost and pay, and finally an insight from employees talking about their experiences. What brought up the interest in choosing these careers is from the show "Mr. Robot" (2015) and as well as just meeting people that told me about their jobs in cybersecurity.

## SOC Analyst

### Job Description

SOC (Security Operations Center) analysts monitor threats, identify vulnerabilities, and respond to incidents. Key tasks include:

- Analyzing alerts from SIEM (Security Information and Event Management) tools.
- Investigating malware/phishing attacks.
- Collaborating with IT teams to patch vulnerabilities (Muntean, 2024).

### Education/Training Requirements

- Education: Most employers prefer a bachelor's degree in computer science or related fields, though some accept certifications + experience (Muntean, 2024).

[1] Cobos, E. V., & Cakir, S. A Review of the Economic Costs of Cyber Incidents.

- Certifications: CompTIA Security+ or CySA+ are entry-level requirements. Advanced certs (e.g., CEH, CHFI) improve prospects.
- Licenses: None required.

**Salary**

- Virginia: 59,000–59,000–75,000 (entry-level).
- National: 72,000–72,000–135,000 (median: $97,000) (Payscale, 2024).
- Education Impact: Bachelor's degrees increase earning potential by 15–20%.

**Benefits & Drawbacks**

- Benefits: High demand, remote work options, skill development.
- Drawbacks: Shift work (including nights), high stress during breaches.

**Advancement Opportunities**

- Next Roles: Senior SOC Analyst → Threat Hunter → SOC Manager.
- Requirements: Certifications (e.g., CISSP), leadership training.
- Continuing Education: Annual training to stay current with threats.

**Typical Day**

- Morning: Review overnight alerts.
- Afternoon: Investigate suspicious activity, document incidents.
- Evening: Hand off unresolved issues to next shift.

## Security Consultant

### Job Description

Security Consultants assess client systems, design security solutions, and advise on compliance (e.g., GDPR, HIPAA). Tasks include**:**

- Conducting penetration tests.
- Writing risk assessment reports.
- Training staff on security protocols (ISC², 2023).

### Education/Training Requirements

- Education: Bachelor's degree in cybersecurity or IT (master's preferred for senior roles).
- Certifications: CISSP, CISM, or OSCP required for most positions.
- Licenses: None, but some firms require clearance (e.g., DoD Secret).

### Salary

- Virginia: 85,000–85,000–120,000 (entry-level).
- National: 90,000–90,000–180,000 (median: $125,000) (BLS, 2024).

### Benefits & Drawbacks

- Benefits: High pay, project variety, autonomy.
- Drawbacks: Travel requirements, client pressure.

### Advancement Opportunities

- **Next Roles: Senior Consultant → Security Architect → CISO.**

- **Requirements: MBA for executive roles, PMP certification.**

**Typical Day**

- Morning: Client meeting to discuss audit results.
- Afternoon: Simulate attacks on a client's network.
- Evening: Draft remediation plan.

Conclusion

The cybersecurity field presents two distinct but equally vital career pathways through the SOC analyst and security consultant roles. SOC analysts serve as essential operational defenders, working in dynamic environments to detect and neutralize immediate threats. Their work demands technical precision, rapid response capabilities, and the ability to function effectively in team-based security operations. In contrast, security consultants operate at a more strategic level, assessing broader organizational vulnerabilities and developing comprehensive protection frameworks. While both roles require continuous learning and certification maintenance, they offer different professional experiences and growth trajectories.

My personal interest in these careers stems from their critical importance in today's digital landscape and the intellectual challenges they present. The SOC analyst role appeals to my preference for hands-on technical work and immediate problem-solving, while the security consultant path aligns with my long-term interest in strategic planning and organizational leadership. Both positions offer strong compensation, job security, and opportunities to make meaningful impacts in protecting digital assets and infrastructure. As cyber threats continue to

evolve in sophistication and scale, these roles will only grow in importance, making them excellent choices for technology professionals seeking challenging, rewarding careers with long-term growth potential.

## References


- Bureau of Labor Statistics. (2024). *Occupational outlook handbook: Information security analysts*. U.S. Department of Labor. https://www.bls.gov/ooh/
- eSentire & Cybersecurity Ventures. (2022). *Cybercrime economic impact report*.
- (ISC)². (2023). *2023 Cybersecurity workforce study*.
- Muntean, R. (2024, January 15). *How to become a SOC analyst*. Springboard Blog. https://www.springboard.com/blog/
- Payscale. (2024). *SOC analyst salary data*. https://www.payscale.com/