



Information Security Analyst – Financial Services

SALARY RANGE (2017): \$74,000–\$95,000

It's up to me to protect my company's computer networks and systems from cyber-attacks. I constantly plan and carry out security measures to keep things safe, and monitor and assess all networks for possible leaks. If a violation is detected, I am the one to investigate and enact backup security systems and sweeps until I am confident that things are secure.

The Tip: Do a work-term experience. This forces you to get out of a classroom and apply yourself. It will open your world and expose you to corporate realities.

PRIORITY KNOWLEDGE AND SKILLS:

<p>Technical Knowledge & Skills</p> <ul style="list-style-type: none"> • Data & information management • Security risk management • Security policies & procedures • Security testing & auditing • Penetration & vulnerability testing • Anti-virus & anti-malware systems • TCP/IP, routing and switching • Firewall/intrusion detection and prevention protocols • Network protocols & packet analysis tools • Cloud computing • Security information & event management (SIEM) 	<p>Tools and Environment</p> <ul style="list-style-type: none"> • Windows, UNIX and Linux operating systems • Utility software • C, C++, C#, Java or PHP programming languages • SaaS models <p>Certifications</p> <ul style="list-style-type: none"> • Certified Ethical Hacker (CEH) • EC-Council Certified Security Analyst (ECSA) • Certified Information Security Manager (CISM) • Certified Information Systems Security Professional (CISSP)
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

BUILDING BLOCK EXPERIENCES

<p>Education & Learning:</p> <ul style="list-style-type: none"> • Bachelor of Information Technology (IT) • Completed certifications in Certified Ethical Hacker (CEH) 	<p>What gets me up in the morning is knowing it falls on me to ensure that all our corporate data is safe. As a cybersecurity professional, I identify opportunities to enhance information protection. My IT degree exposed me to various ways of protecting the individual and organizations from cyber-attacks and reducing system vulnerabilities. I took several short courses in IT security while studying for my CEH certification, which is highly respected in the industry.</p>
<p>Employment Experiences:</p> <ul style="list-style-type: none"> • Had a system administrator internship position at a local IT security company. Hired as a full-time system administrator at graduation. • Moved to a junior system security analyst 	<p>My internship as a system administrator exposed me to various aspects of system vulnerabilities. I consolidated on this knowledge in my role as system administrator and junior system security analyst. Moving into the role of senior security analyst was easy, having worked</p>

<p>position at a large financial services company.</p> <ul style="list-style-type: none"> • Promoted to system security analyst after three years. 	<p>with people and systems, and being involved in the development and implementation of the organization's security policy.</p>
<p>Community Experiences:</p> <ul style="list-style-type: none"> • In high school, I volunteered as a “good shepherd,” protecting kids that were bullied. This opened my mind to the vulnerability that exists despite institutions’ protective structures. • I later developed an interest in traveling abroad, and understood more about individual and corporate vulnerabilities. • Currently, I sponsor two high school kids on an annual educational visit to Silicon Valley where they can experience simulated cyber security scenarios and how they could lead to the collapse of businesses 	<p>A passionate professor in university introduced me to this field school program where we spent three weeks in an IT firm in China. We were exposed to their security structures and training sessions that simulated cyber-attacks from another country. It was an eye-opening experience for me.</p>
<p>Contextual Experiences:</p> <ul style="list-style-type: none"> • I consider myself a risk-taker, but that wasn't always the case 	<p>Balance requires discipline and perspective. I've become a better security analyst because I understand the relationship between security and risk. I take risks but always think about the risk of not protecting myself.</p>
<p>Relationships:</p> <ul style="list-style-type: none"> • I have developed a diverse team of mentors inside and outside of IT. This includes senior people in cyber security. I follow top information security specialists on LinkedIn. 	<p>Social media is a very good source of connection with potential mentors. Follow them on Twitter and join them on LinkedIn.</p>