

Why Cyber Security Specialist?

A HIGHLY DEMANDED JOB IN THE IT MARKET



Security Foundations

Application Security Specialist

Security Intelligence Analyst



Salaries

\$157,000

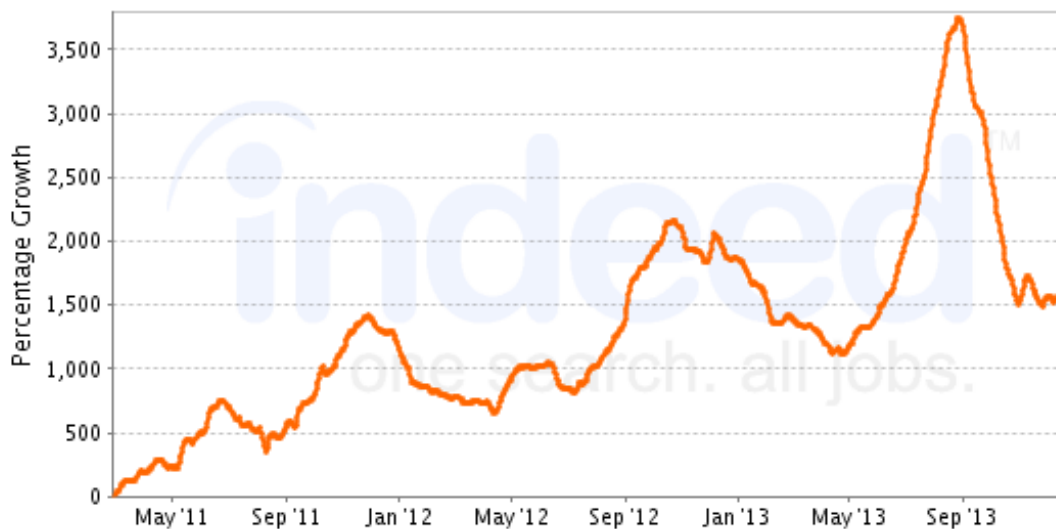
156% higher than average salaries

Job Description:

- Address the challenges of securing people, data, applications and infrastructure.
- Develop security measurements on various applications on devices such as PCs, Laptops, Mobile Devices and Systems.
- Recognize and protect against intrusions and abnormal activities.
- Implement security improvements on existing platforms

Job Trends from Indeed.com

— cybersecurity specialist



Application Security – Why IBM?

IBM is a Market Leader in the Application Security Space

GARTNER Magic Quadrant – Application Security Testing

IBM MARKET POSITION



IBM SOLUTION

IBM® Security AppScan®

Enables organizations to assess the security of **web and mobile applications**, strengthen application security program management and achieve regulatory compliance by identifying vulnerabilities and generating reports with intelligent fix recommendations to ease remediation.

Appropriate Use:

- Proactively protect vulnerable applications
- Reduce the cost of remediating vulnerabilities by detecting them earlier in the development cycle and enhancing security awareness within development teams
- Actively monitor database transactions to help block attacks
- Facilitate effective incident response through enhanced real-time threat identification

Security Intelligence – Why IBM?

IBM is a Market Leader in the Security Intelligence Space

GARTNER Magic Quadrant – Security Information and Event Management

IBM MARKET POSITION



IBM SOLUTION

IBM® QRadar® Security Intelligence Platform

Provides log management, event management, reporting and behavioral analysis for networks and applications.

QRadar includes the release of weekly threat intelligence feeds from **X-Force** and Network Anomaly Detection, designed to complement **SiteProtector IDS**, adding the collection and processing of NetFlow data, deep packet inspection (DPI), anomaly detection and behavior analysis for all supported event sources.

QRadar is integrated with InfoSphere BigInsights (IBM's commercialized Hadoop offering) and also with IBM's analytics and data visualization technologies.

Appropriate Use: QRadar is a good fit for midsize and large enterprises that need general SIEM capabilities, and also for use cases that require behavior analysis and NetFlow analysis.

IBM Cyber Security Specialist – *Academic Roadmap*

Cyber Security Specialist

Complete Academic Certification Track Overview



Cyber Security Foundations

Content: Understanding threats and security risks in the society and in the enterprise. Security Domains (People, Data, Application and Infrastructure).

Application Security Specialist - Tool: IBM Security AppScan Standard

Courses: Essentials of Application Security. Application Security Fundamentals with IBM AppScan Standard.

Security Intelligence Analyst - Tool: IBM Security QRadar SIEM

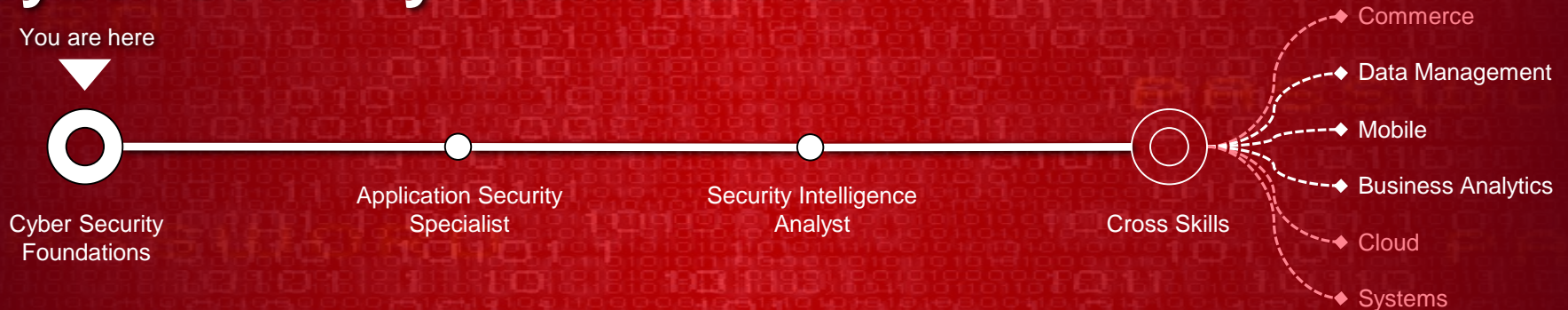
Courses: Foundations of Security Intelligence and Advanced Concepts for SIEM

Security Cross Skills

Mobile Apps security, Security Data Access, concepts of Security in the Cloud space.

IBM Cyber Security Specialist – *Academic Roadmap*

Cyber Security Foundations



Foundations (4 hs instructor-led)

Cyber Security Foundations Course

- IBM Security Overview
- Past, Present and Future
- Trends
- Enterprise Security
- Industry Domains:
 - Healthcare
 - Telco
 - Banking
 - Government
- Case Studies in Africa
- IBM Research in Security
- Cross-skills
- Links and additional resources

Pre-requisite Skills (10 hs self-paced)

ZU370 - Introduction to HTML5 and JavaScript Programming

- HTML5 development support for cross-platform applications
- Code JavaScript functions, and use the form elements of HTML5

DEV452 – Database Academic Associate e-learning Course

- Relational database concepts, DB2 and Data Studio overview
- SQL and database objects, data concurrency and locking
- Database Security and troubleshooting
- DB2 pureXML and Application Development
- The Next IM Frontier – Big Data

XF2015 X-Force 2015 Trend and Risk Security Report

<http://www-03.ibm.com/security/xforce/downloads.html>

This report is an analysis of the security landscape, designed to help individuals better understand the latest security risks.

IBM Cyber Security Specialist – Academic Roadmap

Application Security Specialist



IBM Official Courses (24 hs instructor-led)

RT330 - Essentials of Web Application Security

- Web Application Basics
- Hacking 101 - Introduction to Web Application Security
- OWASP Top 10 Web Application Security Vulnerabilities
- WASC threat classifications
- 7 coding principles that will help secure Web applications
- Common Vulnerabilities such as SQL Injection & Cross-site scripting
- Describe best practices for integrating security in the SDLC
- Threat Modeling & Application Security Testing

TK400 - IBM Security AppScan Standard Fundamentals

- Use advanced techniques to scan web applications
- Describe potential risks of conducting automated security scans
- Review scan results, filter false positives, prioritize issues and communicate them to stakeholders
- Use Glass box and malware scanning.

- Create reports that are based on discovered security issues
- Security AppScan SDK and eXtensions Framework (AXF)

IBM Textbooks

Redbook: REDP-4530-00 - Improving Your Web Application SDLC Security Posture with IBM Rational AppScan

<http://www.redbooks.ibm.com/abstracts/redp4530.html?Open>

IBM Exams

IBM Academic Certificate - IBM Application Specialist

www.ibm.biz/meauniversity

IBM Certified Specialist – IBM AppScan Standard Edition

Test C2150-139 - AppScan Standard Edition

<http://www-03.ibm.com/certify/certs/38003501.shtml>

IBM Cyber Security Specialist – Academic Roadmap

Security Intelligence Analyst



IBM Official Courses (32 hs instructor-led)

BQ101 - IBM Security QRadar SIEM 7.2 Foundations

- Network Security
- Dashboard
- Analyzing Log Activity, Network Activity and Advanced Filtering
- Asset and Vulnerability Assessment
- Offense Investigation, Rules and Tuning
- Reporting and Customer Support

BQ120 - IBM Security QRadar SIEM 7.1 Advanced

- Manage the QRadar administration functionality
- Create and customize network and remote hierarchies
- Create Reference Sets
- Create user security profiles and custom properties
- Create and deploy a Universal DSM
- Create event, flow and anomaly rules

IBM Textbooks

Redbook: REDP-4956-00 - - Realizing Efficient Enterprise Security Intelligence by Using IBM Security Intelligence Solutions
<http://www.redbooks.ibm.com/abstracts/redp4956.html?Open>

IBM Exams

IBM Academic Certificate - IBM Security Intelligence Analyst
www.ibm.biz/meauniversity

IBM Certified Associate - Security QRadar

Test C2150-195 - IBM Security Qradar
<http://www-304.ibm.com/jct03001c/certify/certs/47000502.shtml>

IBM Cyber Security Specialist – *Academic Roadmap*

Security Cross Skills



Mobile Application - Secure your mobile applications

With the explosive growth in the mobile ecosystem, mobile application security is a huge concern. New mobile application designs require new ways of testing to ensure data safety. In this article, explore different aspects of mobile application security. With hands-on examples, learn to use IBM® Security AppScan® Standard with mobile user agents and with emulators and actual devices for Android and iOS.

Data Management - IBM InfoSphere Guardium Technical Training (Course Code: GU201)

This course offers a balanced mix of lectures, hands-on lab work, case studies, and testing. You will learn how to create reports, audits, alerts, metrics, compliance oversight processes, and database access policies and controls. You will also learn about system administration, archiving, purging, and back-ups.

Business Analytics - IBM Business Analytics Proven Practices: IBM Cognos BI Authentication and Single Sign-On.

Implement seamless authentication between security systems and IBM Cognos BI, using these guidelines. This document contains important information about the technical concepts and backgrounds involved and the design of authentication and single sign-on (SSO) functionality in IBM Cognos BI. It also discusses setting expectations regarding supported vs unsupported environments and information that must be gathered for troubleshooting the IBM Cognos BI side of things. This document is intended for security architects and administrators designing authentication for a system includes Cognos BI.