Iverson Associates Sdn Bhd (303330-M)
Suite T113 – T114, 3rd Floor, Centrepoint, Lebuh Bandar Utama
Bandar Utama, 47800 Petaling Jaya, Selangor Darul Ehsan
Tel: 03-7726 2678      Fax: 03-7727 9737      Website: www.iverson.com.my

Course Outline :: CySA+::

| Module Title | : | **CompTIA Cybersecurity Analyst (CySA+)** |
|---|---|---|
| **Duration** | : | **5 days** |

## Description

The CySA+ training  will teach you the fundamental principles of using threat and vulnerability analysis tools plus digital forensics tools. It will prepare you to take the CompTIA CySA+ CS0-001 exam by providing 100% coverage of the objectives and content examples listed on the syllabus.

After reading this study guide, you will be able to:

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

## Pre-requisite

To get the most out of the CompTIA CySA+ Study Guide and be able to prepare for your exam you should have successfully earned the CompTIA Network+ certification and CompTIA Security+ certification or have equivalent knowledge. Specifically, it is recommended that you have the following skills and knowledge before starting this course:

- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools
- Identify network attack strategies and defenses.
- Know the technologies and uses of cryptographic standards and products
- Identify network- and host-based security technologies and practices.
- Describe the standards and products used to enforce security on web and communications technologies.

## Course Outline

Lesson 1: Explaining the Importance of Security Controls and Security Intelligence
Lesson 2: Utilizing Threat Data and Intelligence
Lesson 3: Analyzing Security Monitoring Data
Lesson 4: Collecting and Querying Security Monitoring Data
Lesson 5: Utilizing Digital Forensics and Indicator Analysis Techniques
Lesson 6: Applying Incident Response Procedures
Lesson 7: Applying Risk Mitigation and Security Frameworks
Lesson 8: Performing Vulnerability Management

Lesson 9: Applying Security Solutions for Infrastructure Management

Lesson 10: Understanding Data Privacy and Protection

Lesson 11: Applying Security Solutions for Software Assurance

Lesson 12: Applying Security Solutions for Cloud and Automation

Appendix A: Mapping Course Content to CompTIA Cybersecurity Analyst+ (Exam CS0-002)

Appendix B: Security Resources

Solutions

Glossary

Index