SKILL INFINITY
(1296874-M)

COURSE OVERVIEW

Organizational Systems Security Analyst (OSSA)

The Organizational Systems Security Analyst™ (OSSA) is an international Enterprise-level, IT-Security Certification designed by experienced IT Security practitioners especially for the following groups of people:

- IT-Security Professionals looking for practical and hands-on technical enterprise-level IT-security training & certification.
- IT Professionals who are looking to get into the IT-Security industry.
- Technical staff who are interested in learning more about real-world, practical IT-Security from technical, procedural and legal standpoints, who are responsible for the security of their organization's infrastructure or who are interested in a career in IT-Security.
- Those looking for an Enterprise-relevant technical-level IT-Security course which uses practical lab-based hands-on training and a practical hands-on certification examination that will not devalue over time.

With its emphasis on the use of practical methodologies and technical tools to achieve the objective of network, server and web-application security for organizations, the **Organizational Systems Security Analyst™** teaches a vendor independent approach to practical issues surrounding IT security and is geared towards equipping participants with the knowledge and skills necessary to secure their organizations from both internal and external threats.
Unlike those who focus on IT-Security tools which can become ineffective very fast in the real world, the **Organizational Systems Security Analyst™** first looks at security from a methodological perspective and draws lessons from Sun Tzu's "Art of War", introducing the practicalities of IT-Security and not just theory. It then populates the framework with resources and tools by which various security aims and objectives can be met. For these technical portions, although there is practical coursework, the aim is not to teach about the tool itself but about the category of usefulness that the tool falls into so that the course attendees can select, on their own, the “best-of-breed” for the task at hand. Give a man a tool and he’ll protect himself for a day. Give him methodology in conjunction with resources and he’ll be able to protect his organization for a lifetime.

And, of course, because IT-Security does not exist in a vacuum, the **Organizational Systems Security Analyst™** covers legal and operational issues that will be faced both locally and in a multinational setting. Programme participants will come away with the following:

- A top-to-bottom practical understanding of the real-life issues facing the IT-Security Professional today, augmented by workbook-based lab work setting up a complete enterprise defensive network overlay.
- The ability to advise their organizations about the various IT-Security risks and how to mitigate them.
- An understanding of the need to ensure that policies, procedures, people and platforms are executed and established in a secure manner.
- The ability to conduct incident response and basic computer forensics.
- An appreciation of the legal framework in which all organizations operate in and its impact on the organization.

This course is extremely heavy on practical labs and includes a practical lab-based certification exam, which is held on the last day of the course.

SKILL INFINITY
(1296874-M)

COURSE OVERVIEW

Target Student

- IT-Security Practitioners and Technical Professionals
- IT-Security Penetration-Testers and/or Technical Auditors
- IT Network Designers
- IT Network Administrators / Engineers
- IT System Administrators / Analysts / Engineers
- Application Designers / Specialists and anyone who needs or wants to know how to secure their organization's infrastructure, information and assets against internal and external threats.

Methodologies & Tools

- The 8-Step Security Gameplan™
- The 5E Attacker Methodology™
- The Threat-Liability-Disruption-Potential (TLDP) Matrix™
- Wireshark
- IPtables
- FWbuilder
- Snort
- Tripwire
- Honeyd
- GPG
- Nmap
- Nessus
- Ettercap-ng
- Achilles
- Metasploit
- Exploit code
- Netcat
- Ophcrack
- Disk Investigator

Suggested Prerequisites

- Understand networking protocols and principles such as TCP/IP, 802.3, HTTP, etc, and how they work in detail.
- Understand basic IT-security principles and concepts such as CIA, defence-in-depth, etc.
- Attendees should preferably be in technical and/or practitioner roles/positions/jobs.
- Strong interest in IT-security

SKILL INFINITY
(1296874-M)

COURSE OVERVIEW

Course Outline

Practical coursework is interspersed throughout the course and the following is a brief course module outline:

What is Information Security
- Sun Tzu's Guiding Principle
- Cybertacks
- Cybertack Origins
- Defining Security: Key Terms
- The CIA Triad
- The SOB Troika
- Trust & Verify / Ask The Oracle
- The 8-Step Security Gameplan™

Defending your Turf & Security Policy Formulation
- Sun Tzu's Guiding Principle
- The 4Ps of Defence
- Security Policies: Due Diligence
- Building A Policy
- This LAND Is Mine

Network 101
- Sun Tzu's Guiding Principle
- Sniff Me If You Can: Why Sniff?
- How A Sniffer Really Works
- Networking Protocols From A Security Viewpoint
- Attacker POV: Frames, IP and ICMP
- Attacker POV: ARP, DNS & Routing
- Packet Dump / Sniff Log Analysis

Defensive Tools & Lockdown
- Sun Tzu's Guiding Principle
- Firewalls
- Lab Network Firewall Deployment and Configuration
- NIDS (Network-based Intrusion Detection System)
- Lab Network NIDS Deployment and Configuration
- HIDS & FICs (Host-based IDS and File Integrity Checkers)
- Lab Network HIDS/FIC Deployment and Configuration
- Honeypots
- Lab Network Honeypot Deployment and Configuration
- Cryptography: VPNs, Digital Signatures & GPG
- Using GPG

The 5E Attacker Methodology™: Attacker Methods/Exploits
- Sun Tzu's Guiding Principle
- Attack Anatomy : The 5E's
- Preparation & Tool Repositories
- Sandboxing
- Checking Tool Authenticity
- The 5E Attacker Methodology™

- Social Engineering, Dumpster Diving & Physical Violation
- Browsers, WHOIS & DNS as attack tools
- War Driving, Network Mapping & Port Scanning
- OS Determination & Fingerprinting
- Vulnerability & Web Scanning (network & web based)
- Spoofing, Session Hijacking, MITM
- DoS & DDoS: Botnets & Zombies
- Buffer Overflow, Shell Code & Heap Overflow
- Format String Vulnerability
- Metasploit Framework
- Exploit Code compilation
- Web Application Vulnerabilities
- OWASP Top 10
- Web Application Exploitation
- Password Cracking
- Backdoors & Covert Channels
- Trojans & Rootkits
- File Hiding, Log Modification & Executable Removal

Wireless (In)Security Introduction

- Sun Tzu's Guiding Principle
- WLAN Security Basics: Open, WEP, WPA-PSK, WPA/WPA2
- Warchalking & Wardriving
- Typical WLAN Deficiencies

Incident Response & Computer Forensics

- Sun Tzu's Guiding Principle
- Incident Response Framework
- The Need for Incident Response
- The TLDP Matrix™
- Incident Response Policy
- Incident Response Team Structure & Services
- Incident Response Phases
- Case Study Part I: Incident Response
- Computer Forensics Introduction
- Sun Tzu's Guiding Principle
- The Role of a CFI
- Chain of Custody
- Data Acquisition
- Information Gathering: Browser Forensics
- Information Gathering: Malware Forensics
- Information Gathering: Email Forensics
- Case Study Part II: Computer Forensics

SKILL INFINITY
(1296874-M)

COURSE OVERVIEW

The Impact Of Law

- Sun Tzu's Guiding Principle
- Why You Need To Know
- Permissable Actions
- Harmonization
- The State Of Cybercrime Law
- Clearing up SarBox FUD
- S.E. Asian Law Examples
- Legal Tradition Comparisons
- Problems with Enforcement
- When To Enforce?
- Computer Misuse Act: Law Enforcement Rights
- Computer Misuse Act: What Is An Offence?