Val-Ed™

Valiant Technologies Education & Training Services

Workshop for aspirants of Security+

Welcome to Valiant Technologies. We are a specialty consulting and training organization that focuses on information security at the strategic and operational levels. With significant strength also in information security assurance services, Valiant CISSTech, as we were formerly known, has been serving clients across many countries - Bahrain, Hong Kong, India, Kuwait, Malaysia, Maldives, Saudi Arabia, Sri Lanka, South Africa, Sultanate of Oman, Thailand, United Arab Emirates, and Zambia.

Val-Ed™, our educational services division offers a variety of ready-packaged and tailor-made educational and training programs in the area of information security. This catalogue provides detailed information on one of the educational and training offering to clients in the area of information security technology, management and assurance.

We have a full range of services that we offer covering the full spectrum of information security and our services catalogue provides details of the following services that we provide to clients. Please ask for a services catalogue for more details on these services:

- Testing and hardening of information system defenses:
  - Vulnerability assessment
  - Penetration testing
  - Application security testing
  - Hardening of servers and network components
  - Periodic evaluation of network security
- Information Security Management Services
  - Security Policies, Procedures and Guidelines
  - Security Awareness Program
  - Risk Assessment and Analysis
  - Executive Management briefings on Security
  - Vendor selection for security products
  - Computer Forensics Investigation\
  - ISO-27001 preparatory services
  - Fill-in Security Manager program
- Control and Assurance Services
  - Gap analysis against ISO-27001, COBIT, ISSAF
  - Information security controls review
  - Information Systems Security Audit
  - Control assessment for SOX compliance
- Business Continuity and Disaster Recovery Management

We look forward to being of service to you and look forward to hearing your interest.

- Valiant Team

List of regular programs offered by Valiant Technologies

	Course Name	Duration (days)
1	Workshop for CISSP Aspirants	4
2	Workshop for CISA Aspirants	5
3	Workshop for CISM Aspirant	4
4	Workshop on BCP and DRP	2
5	Workshop on Change Management	1
6	Workshop on Information Security Policies	3
7	Information Security for Senior Management	½
8	Security Awareness for IT user management	2
9	Security Plus Certification of CompTIA	6
10	Sarbanes Oxley Act – Structure and Implementation	2
11	Digital Evidence for IT / IS Auditors	1

CV of principal instructor, Dr Rama K Subramaniam is found on the last page

Thought Leadership...
Valiant Technologies

Training program for aspirants of Security Plus Certification of CompTIA

Background:

CompTIA Security+ certification tests for security knowledge mastery of an individual with on-the-job networking experience, with emphasis on security. The exam covers industry-wide topics, including communication security, infrastructure security, cryptography, access control, authentication, external attack and operational and organization security. Security+ is taught at colleges, universities and commercial training centers around the globe. Security+ is an elective or prerequisite to advanced security certifications, some of which are discussed later in this proposal.

Security+ certification is recognized around the world as the benchmark for foundation-level security professionals. Incorporating a comprehensive range of security knowledge areas, Security+ was developed with input from industry, government, academia and front-line practitioners, so you can be assured of its relevance.

CompTIA and Related Certifications

CompTIA certifications often apply towards advanced certifications, such as Microsoft's MSCA and IBM's Advanced Tivoli Deployment Professional certification, apart from meeting requirements for some of Symantec's certifications. By taking a CompTIA exam as an elective towards advanced certifications like these, you benefit by having a dual certification - an important distinction in today's job market. CompTIA certifications are either prerequisites or electives for other well known certifications as follows:

Security+ certification can be used as electives or equivalents to several of Microsoft's advanced certifications. A CompTIA certification will not only apply as an elective, but is also a separate and distinct credential. If you're working towards your MCSE and MCSA certification, you might want to get there with two certifications on your resume. Some options are presented in the following paragraphs.

1. MCSA Security on Windows Server 2003 and MCSA on Windows 2000

   This specialized MCSA certification has an emphasis on security. The MCSA: Security exam tests candidates on the Microsoft Windows 2000 and Windows 2003 tracks. You must pass three core exams and two security specialization exams, one of which may be CompTIA's Security+ exam.

2. MCSE Windows Server 2003 and Microsoft Windows 2000

   Microsoft accepts CompTIA's Security+ certification as an alternative to passing an elective exam in the MCSE on Microsoft Windows 2000 and in the MCSE Windows Server 2003 certification programs.

3. MCSE Security on Windows Server 2003 and MCSE on Windows 2000

   This specialized MCSE certification has an emphasis on security. The MCSE: Security candidates taking the MCSE Security Windows 2000 track or the MCSE Security Windows 2003 track, must pass four core exams three security specialization exams, one of which may be the CompTIA Security+.

4. Symantec Certified Technology Architect (SCTA)

   A Symantec Certified Technology Architect (SCTA) focuses on a single security segment and how to design, plan, deploy and manage effective security solutions. CompTIA's Security+ certification can be used to fulfill a requirement for this certification.

5. IBM Certified Advanced Deployment Professional – Tivoli Security Management Solutions 2003

   CompTIA Security+ certification is required for this IBM certification. CompTIA Security+ certification is also recommended for all IBM Tivoli Software Sales and Security staff.

What does this certification cover?

It covers five essential domains of knowledge of Information Security and the relative weightage of coverage of these domains of knowledge is as follow:

	Domain	Weightage %
1	General Security Concepts	30
2	Communication Security	20
3	Infrastructure Security	20
4	Cryptography	15
5	Operations / Organizational Security	15

Duration: Six days of approximately seven to eight hours of class room instructions and exercises in the form of quiz, on-line tests using Valiant's proprietary question bank and group exercises.

Assessments

Pre-Assessment: The client would be requested to identify the number of candidates who are to be trained and send as many or more numbers of potential candidates for a half day pre-assessment workshop to be conducted by Valiant. The workshop would present the concepts for about an hour and half and all participants would take a pre-assessment test administered on-line. Valiant would provide the results of this assessment with domain-wise grades of all candidates enabling the client to choose the number of people to be ultimately selected for the course.

Post Assessment: This has two components:

Firstly all candidates would be assessed internally by Valiant through an on-line examination on the second half of the last day of the program. Domain wise rating of the candidate's understanding of the areas of knowledge imparted to them will be made available to the candidates as also the sponsoring organization.

Secondly, candidates will write the on-line examination conducted by CompTIA in any of the Prometric or Vue testing centers across the world to attain the Security+ certification if they make the passing grade.

On the basis of the first assessment, Valiant would be in a position to report to the sponsoring organization the degree of assimilation of the each of the domains of knowledge covered in the program.

Detailed Course Content

The details of the course contents in respect of each of these domains of knowledge would be as follows:

Domain 1 – General Security Concepts

1.0 Understand the basic security paradigms

- The CIA triad and its limitations in open networked systems
- The concept of the four phase cycle of logical access Identification – Authentication – Authorization and Accountability
- Fundamentals of network topologies, Internet, Intranet and Extranet from a security perspective
- MAC (Mandatory Access Control)
- DAC (Discretionary Access Control)
- RBAC (Role Based Access Control)

1.2 Recognize and be able to differentiate and explain the following methods of authentication

- Kerberos
- CHAP (Challenge Handshake Authentication Protocol)
- Certificates
- Username / Password
- Tokens
- Multi-factor
- Mutual
- Biometrics

1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols

1.4 Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk

- DOS / DDOS (Denial of Service / Distributed Denial of Service)
- Back Door
- Spoofing
- Man in the Middle
- Replay
- TCP/IP Hijacking
- Weak Keys
- Mathematical
- Social Engineering
- Birthday
- Password Guessing
  - Brute Force
  - Dictionary
- Software Exploitation

1.5 Recognize the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk

- Viruses
- Trojan Horses
- Logic Bombs
- Worms

1.6 Understand the concept of and know how reduce the risks of social engineering

1.7 Understand the concept and significance of auditing, logging and system scanning

Domain 2 – Communication Security

2.1 Recognize and understand the administration of the following types of remote access technologies

- 802.1x
- VPN (Virtual Private Network)
- RADIUS (Remote Authentication Dial-In User Service)
- TACACS (Terminal Access Controller Access Control System)
- L2TP / PPTP (Layer Two Tunneling Protocol / Point to Point Tunneling Protocol)
- SSH (Secure Shell)
- IPSEC (Internet Protocol Security)
- Vulnerabilities

2.2 Recognize and understand the administration of the following email security concepts

- S/MIME (Secure Multipurpose Internet Mail Extensions)
- PGP (Pretty Good Privacy) like technologies
- Vulnerabilities
  - SPAM
  - Hoaxes

2.3 Recognize and understand the administration of the following Internet security concepts

- SSL / TLS (Secure Sockets Layer / Transport Layer Security)
- HTTP/S (Hypertext Transfer Protocol / Hypertext Transfer Protocol over Secure Sockets Layer)
- Instant Messaging
  - Vulnerabilities
  - Packet Sniffing
  - Privacy
- Vulnerabilities
  - Java Script
  - ActiveX
  - Buffer Overflows
  - Cookies
  - Signed Applets
  - CGI (Common Gateway Interface)
  - SMTP (Simple Mail Transfer Protocol) Relay
- SSL / TLS (Secure Sockets Layer / Transport Layer Security)
- LDAP (Lightweight Directory Access Protocol)

2.5 Recognize and understand the administration of the following file transfer protocols and concepts

- S/FTP (File Transfer Protocol)
- Blind FTP (File Transfer Protocol) / Anonymous
- File Sharing
- Vulnerabilities
  - Packet Sniffing
  - 8.3 Naming Conventions

2.6 Recognize and understand the administration of the following wireless technologies and concepts

- WTLS (Wireless Transport Layer Security)
- 802.11 and 802.11x
- WEP / WAP (Wired Equivalent Privacy / Wireless Application Protocol)
- Vulnerabilities
  - Site Surveys

Domain 3 Infrastructure Security

3.1 Understand security concerns and concepts of the following types of devices

- Firewalls
- Routers
- Switches
- Wireless
- Modems
- RAS (Remote Access Server)
- Telecom / PBX (Private Branch Exchange)
- VPN (Virtual Private Network)
- IDS (Intrusion Detection System)
- Network Monitoring / Diagnostics
- Workstations and Servers
- Mobile Devices
- Coaxial Cable
- UTP / STP (Unshielded Twisted Pair / Shielded Twisted Pair)
- Fiber Optic Cable
- Removable Media

3.3 Understand the concepts behind the following kinds of Security Topologies

- Security Zones
- DMZ (Demilitarized Zone)
- Intranet
- Extranet
- VLANs (Virtual Local Area Network)
- NAT (Network Address Translation)
- Tunneling

3.4 Differentiate the following types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system

- Network Based
  - Active Detection
  - Passive Detection
- Host Based
  - Active Detection
  - Passive Detection
- Honey Pots
- Incident Response

3.5 Understand the following concepts of Security Baselines, be able to explain what a Security Baseline is, and understand the implementation and configuration of each kind of intrusion detection system

- OS / NOS (Operating System / Network Operating System) Hardening
  - File System
  - Updates (Hotfixes, Service Packs, Patches)

- Network Hardening
  - Updates (Firmware)
  - Configuration
    - Enabling and Disabling Services and Protocols
    - Access Control Lists

- Application Hardening
  - Updates (Hotfixes, Service Packs, Patches)
  - Web Servers
  - E-mail Servers
  - FTP (File Transfer Protocol) Servers
  - DNS (Domain Name Service) Servers
  - NNTP (Network News Transfer Protocol) Servers
  - File / Print Servers
  - DHCP (Dynamic Host Configuration Protocol) Servers
  - Data Repositories
    - Directory Services
    - Databases

Domain 4 Basics of Cryptography

4.1 Be able to identify and explain the of the following different kinds of cryptographic algorithms

- Hashing
- Symmetric
- Asymmetric

4.2 Understand how cryptography addresses the following security concepts

- Confidentiality
- Integrity
  - Digital Signatures
- Authentication
- Non-Repudiation
  - Digital Signatures
- Access Control

4.3 Understand and be able to explain the following concepts of PKI (Public Key Infrastructure)

- Certificates
  - Certificate Policies
  - Certificate Practice Statements
- Revocation
- Trust Models

4.4 Identify and be able to differentiate different cryptographic standards and protocols
4.5 Understand and be able to explain the following concepts of Key Management and Certificate Lifecycles

- Centralized vs. Decentralized
- Storage
  - Hardware vs. Software
  - Private Key Protection
- Escrow
- Expiration
- Revocation
  - Status Checking
- Suspension
  - Status Checking
- Recovery
  - M-of-N Control (Of M appropriate individuals, N must be present to authorize recovery)
- Renewal
- Destruction
- Key Usage
  - Multiple Key Pairs (Single, Dual)

Domain 5 Operational / Organizational Security

5.1 Understand the application of the following concepts of physical security

- Access Control
  - Physical Barriers
  - Biometrics
- Social Engineering
- Environment
  - Wireless Cells
  - Location
  - Shielding
  - Fire Suppression

5.2 Understand the security implications of the following topics of disaster recovery

- Backups
  - Off Site Storage
- Secure Recovery
  - Alternate Sites
- Disaster Recovery Plan

5.3 Understand the security implications of the following topics of business continuity

- Utilities
- High Availability / Fault Tolerance
- Backups

5.4 Understand the concepts and uses of the following types of policies and procedures

- Security Policy
  - Acceptable Use
  - Due Care
  - Privacy
  - Separation of Duties
  - Need to Know
  - Password Management
  - SLAs (Service Level Agreements)
  - Disposal / Destruction
  - HR (Human Resources) Policy
    - Termination (Adding and revoking passwords and privileges, etc.)
    - Hiring (Adding and revoking passwords and privileges, etc.)
    - Code of Ethics
- Incident Response Policy

5.5 Explain the following concepts of privilege management

- User / Group / Role Management
- Single Sign-on
- Centralized vs. Decentralized
- Auditing (Privilege, Usage, Escalation)
- MAC / DAC / RBAC (Mandatory Access Control / Discretionary Access Control / Role Based Access Control)

5.6 Understand the concepts of the following topics of forensics

- Chain of Custody
- Preservation of Evidence
- Collection of Evidence

5.7 Understand and be able to explain the following concepts of risk identification

- Asset Identification
- Risk Assessment
- Threat Identification
- Vulnerabilities

5.8 Understand the security relevance of the education and training of end users, executives and human resources

- Communication
- User Awareness
- Education
- On-line Resources

5.9 Understand and explain the following documentation concepts

- Standards and Guidelines
- Systems Architecture
- Change Documentation
- Logs and Inventories
- Classification
  - Notification
- Retention / Storage
- Destruction

Principal Instructor

Dr. Rama K Subramaniam

MBA(UK), PHD, FCA, CISA, CISM, CISSP, CEH, CHFI, CSQP, MCSE, Security+

He is Director of Valiant Technologies Pvt Ltd and Tejas Brainware Systems Pvt Ltd. He has been an information security consultant, trainer and educator for over a decade now. He has trained experts in many information security domains across Gulf nations, India, Far East and Africa. He has also been a consultant to a number of organizations in the commercial, government, armed forces, judiciary and law enforcement segments in these countries.

He is a certified and experienced professional in the areas of creating and implementing secure information security architecture; internal controls systems and processes; conceptualization, creation, testing and maintenance of business continuity and disaster recovery plans; security audits and certification of network infrastructure; conceptualization and implementation of multi-factor authentication processes (including PKI and X.509 compliant certification infrastructure); creation, assessment and certification of CoBIT, ISO-17799, BS-7799 and ISO-15408 compliant information security management systems.

He served earlier as Global Chair of the Education and Awareness Principles Expert Group of Globally Accepted Information Security Principles (GAISP), based in the United States and is currently Global Chair of the Accreditation Process committee of Open Information Systems Security Group (OISSG), based in the UK where he overseas their certification and accreditation processes. He is the charter President of the first chapter of ISSA (Information Systems Security Association) in Asia and served on the boards of Dubai and Chennai chapters of ISACA. He is past Co-Chairman of the Information and Communication Technologies Expert Committee of the Hindustan Chamber of Commerce and charter President of Institute of Internal Auditors, Zambia.

He was formerly Managing Director of Thewo Corporate Services based in Lusaka, Zambia; Group Operations Director or Benetone Group of Companies based in Bangkok, Thailand and Commercial Director of Dynaspede Integrated Systems Ltd, based in Mumbai.