GIAC Security Leadership (GSLC)

Length: 5 Days

About this course: The GIAC Security Leadership Certification (GSLC) is an intermediate skill level certification for individuals with managerial or supervisory responsibility for information security staff.

Target Audience: Security Professionals with managerial or supervisory responsibility for information security staff.

COURSE CONTENT

1. **Change Management and Incident Handling for Managers:** The candidate will understand the risks of incidents and unplanned changes, identify requirements for effective change management and incident response programs, and demonstrate understanding of the basic legal issues in incident and evidence handling

2. **Common Attacks and Malware:** The candidate will be able to identify common network attack methods, types of malicious code, and strategies used to mitigate those threats

3. **Managing Access Control:** The candidate will demonstrate an understanding of the fundamental theory of access control, secure authentication and authorization, and threats to account credentials and system access

4. **Managing Defense in Depth and Security Policy**: The candidate will demonstrate an understanding of the terminology and concepts of Defense-in-Depth, assessing security posture, and using security policy to meet the security needs of the organization

5. **Managing Disaster Recovery and Contingency Planning**: The candidate will demonstrate familiarity with the theory and techniques of cyber warfare. The candidate will be able to lead Business Continuity and Disaster Recovery teams, and understand the risk posed by natural disasters, large scale disruptions, and cyber warfare

6. **Managing Employees and Total Cost of Ownership**: The candidate will demonstrate an understanding of effective communication and negotiation tactics, managing employee priorities, use TCO analysis for proposed solutions and projects, and applying due diligence to reduce legal liability and the risk of fraud

7. **Managing Operational Security**: The candidate will demonstrate an understanding of operational security (OPSEC) principles, as well as offensive and defensive OPSEC techniques

8. **Managing Physical Security and Facility Safety**: The candidate will demonstrate the ability to advocate for and integrate security requirements into facility, safety and procurement processes, including physical access and dealing with vendors

9. **Managing Privacy and Web Security**: The candidate will demonstrate an understanding of the privacy concerns of individuals, strategies for maintaining data privacy on private and public networks, and understand the risks posed to data by steganography, web applications, and Internet communications

10. **Managing Risk and Ethics**: The candidate will demonstrate the ability to evaluate and manage risk and will be familiar with ethical issues pertaining to IT/Information Security

11. **Managing Security Awareness and Protecting Intellectual Property**: The candidate will be able to identify and protect intellectual property and intangible assets, including an understanding of secure software development processes, honeypots and honeytokens, and managing an organizational security awareness program

12. **Managing the Network Infrastructure**: The candidate will demonstrate an understanding of common LAN and WAN technologies, including network infrastructure, virtualization, MAC and IP addressing, VoIP, DNS, and common threats to network services

13. **Managing the Quality and Growth of the Security Organization**: The candidate will demonstrate an understanding of hiring and managing a global security team and achieving sustainable growth, including the principles of cultural awareness, quality, and continuous process improvement

14. **Managing the Use of Cryptography**: The candidate will demonstrate an understanding of symmetric, asymmetric and hashing algorithms, PKI and key management, and understand the common uses of cryptography in securing network data and communications

15. **Managing Vulnerabilities**: The candidate will demonstrate an understanding of common approaches, methods, and tools used to gather information externally and internally, and how to effectively prioritize and remediate vulnerable systems and devices

16. **Managing Wireless Security**: The candidate will demonstrate an understanding of wireless networking technologies and risks, including security considerations for 802.11 and Bluetooth devices

17. **Network and Endpoint Security Technologies:** The candidate will demonstrate an understanding of security technologies and devices used to prevent and detect network and endpoint threats, including filtering, IPS/IDS, virtualization, logging, and correlation

18. **Network Protocols for Managers:** The candidate will demonstrate understanding of the terminology and concepts of network protocols and how to assess competent network engineers

19. **Project Management and Business Situational Awareness:** The candidate will demonstrate familiarity with the terminology, concepts and phases of project management as well as identifying and modeling effective business situational awareness

20. **Selling and Managing the Mission:** The candidate will demonstrate an understanding of how to use mission statements and security frameworks to align security with the business, and how to effectively promote security within an organization

Learnsoft
ENTERPRISE TRAINING

Detailed List Of Course Objectives:

Certification Objective	Expanded Topic Areas
802.11	• Airborn viruses (ie. Cabir) • Securing and Protecting wireless best practices • Security Technologies (WPA, 802.11i, 802.1x, and EAP) • Types of wireless and their frequencies • WEP Weaknesses • Wireless Threats (Eavesdropping, Wardriving, Masquerading, DoS, Rogue AP)
Access Control and Password Management	• Access control models (DAC, MAC, RBAC) • Best Practices (implicit deny, least privilege, separation of duties, job rotation) • Centralized Access Control Technologies (Active directory, RADIUS) • Fundamentals of Biometrics • Password cracking • Passwords, Hashes and limitations of windows hashes • Strong Password Policy (what it is and why it's needed) • Terminology (identity, authentication, authorization, least privilege, need to know, separation of duties, rotation of duties, data owner, single sign on,)
Building a Security Awareness Program	• General approach to training • Know what NIST SP 800 - 50 is • Metrics for Security Awareness Programs • Security Awareness Goals (changing user behavior)
Business Situational Awareness	• Budgeting Approaches (top down, bottom up, negotiated, devolving) • Factors that reduce business situational awareness

	• Several important objectives: employees with 20 objectives are not accountable • Temet Nosce: know your strengths and weaknesses • Time Management • To align security with the needs of the business, you must know company financials and products, you must know the business
Change Management and Security	• Implementing change management • Indicators of change management problems • Relationship between undocumented changes and network instability • Repeatable builds • Tracking unplanned work
Computer and Network Addressing	• Broadcast addresses • CIDR Addressing • IP addresses and Subnet masks (network and host portion) • MAC Addresses and OUIs (MACs built into NIC, only last for one hop) • Private Addresses Strongly Recommended
Cryptography Algorithms and Concepts	• AES • Concepts in crypto (computational complexity, intractable problems, public scrutiny) • Crypto Attacks (known plaintext, chosen plaintext, adaptive chosen plaintext, ciphertext only, chosen ciphertext, chosen key) • DES (56 bit key space considered insecure, symmetric block cipher) • ECC usage and vulnerabilities • Quantum cryptography concepts • RSA vs. DES (asymmetric vs. Symmetric) characteristics

Cryptography Applications, VPNs and IPSec	• Client and Server Side Certificate uses • Encrypting and Decrypting email with PGP • IPSEC Headers (AH and ESP) • IPSEC modes (transport and tunnel) • Key Management (public key distribution, private key storage) • PKI CA Hierarchy • PKI Problems (revocation is biggest issue) • PPP Basics • VPN components and placement issues • VPN technologies (SSL, SSH) • VPN types (site to site, client VPN) • Web of Trust (such as Linkedin, Facebook or people you know)
Cryptography Fundamentals	• Depend on secrecy of the key NOT the algorithm • Key management is weakest link • OPSEC problems (ie. Enigma Purple defeated by poor operations) • ROT-13 • Stream and block cipher characteristics • Techniques must be combined carefully to produce strong crypto (substitutation, permutation, hybrid) • XOR operations
Defense-in-Depth	• Architectural Process, zones, checkpoints • Information-centric DiD • Protected Enclaves DiD • Risks Associated with Connecting USB or Portable Devices or Using Them as Copying Devices • Role Based Access Control • Security Architect • Terminology (risk, threat, attack surface) • Uniform Protection DiD (least important type) • Vector Oriented DiD
Defensive OPSEC	• 3 key laws of OPSEC • Employee issues (monitoring, screening, agreements, need to know, least privilege) • OPSEC Defined • Sensitive information (labeling, handling, and access)

Disaster Recovery / Contingency Planning	• BCP (definition and components) • Business Impact Analysis • DRP (definition and components) • Key Elements of continuity planning • Top BCP/DRP Planning Mistakes
DNS	• Cache Poisoning - dangers of attacker controlling namespace • Cybersquatting • Domain Hijacking -- procedural and technical controls to prevent • gethostby name and gethostbyaddr • Hierarchy • Host Table (how it can be used against you or to protect you) • Nslookup forward and reverse lookups • Protecting Domain Names • Uses and misuses of the HOSTS table
Endpoint Security	• 3rd party applications - ie. Secunia PSI • Anti-virus has reached its limit • Browser defense, plugins, testing • Endpoint White list • Risks associated with connecting USB or Portable devices, or using them as copying devices
Facilities and Physical Security	• Cooling, Hot Spots • Detection of unauthorized access • Lock types (traditional, cipher lock, magnetic cards, smart cards, biometric) • Physical Security basics • Power Basics • Smoke and Fire basics - detective and suppressive controls
General Types of Cryptosystems	• Goals of each type of crypto system (CIA + non-repudiation) • One way hash functions • Public Key Crypto (Asymmetric/two key crypto) • Secret Key Crypto (symmetric/one key crypto)

Honeypots, Honeynets, Honeytokens, Tarpits	• Benefits and Drawbacks of using Honeypots • Honeypots defined and types (host, network, service, honey token) • Legal Issues • Technologies (Virtualization, honeynet project, labrea tarpit)
Incident Handling and the Legal System	• Chain of Custody • Evidence collection (real, direct, best, relevant, reliable, integrity, sign and seal) • Search and Seizure (with and without a warrant) • Types of laws (regulatory, criminal, civil) • US Title 18 Section 30
Incident Handling Foundations	• Common Incident Handling Mistakes • Containment Phase - how to contain the incident in detail (make a backup) • Detecting and recognizing incidents (if you detect zero, maybe you are not recognizing incidents) • Identification Phase - steps to recognize an incident in detail • Incident Handling and Incidents defined • Preparation Phase - how to in detail • Six Step Incident Handling Process Defined
Information Warfare	• Asymmetry • Currency Destabilization • Cybermilitia • Malicious Code Blitz • Perception Management • Predictable Response
IP Terminology and Concepts	• Application Layer Security Protocols • Encapsulation • ICMP • IP and Important Fields • Packets vs Frames • Ping, Traceroute/Tracert and their uses • Server and Client Ports • Sniffers

	• TCP 3 Way Handshake and connection establishment • UDP • What is a network protocol
Logging	• Raid 5, raid 10 • Syslog • Thin and fat events, referential data
Malicious Software	• Malicious Browser Content and Hybrid Threats (browser was never designed to be a security gateway) • Malware Defense Techniques • Propagation techniques • Trojan Horse characteristics • Virus types and characteristics (require user action to spread) • Worm characteristics (does not require user action to spread)
Manager's Guide to Assessing Network Engineer	• Ask them about embedded protocol and to read the fields • Done at job interview • Give them the handout and sample packet • You have the "teacher's edition" to check their work
Managerial Wisdom	• Key Concepts from Good to Great (First Who, then What, Hedgehog Concept, Flywheel, Level 5 leader) • Know the 7 Habits of Highly Effective People
Managing Ethics	• 48 laws of power (concept of amorality: win at any cost) • Ethical Leadership (managers) • Ethics Terminology (Ethics, Morals, Policy, Laws, Culture) • Seven Signs of Ethical Collapse

Managing Intellectual Property	• Attacks on IP (insider threats, cybersquatting) • Copyrights (defined, fair use, attacks, defenses) • Digital Rights Management (Sony XCP, CSS) • DMCA • How to protect IP (NDA, non-compete, need-to-know, control publicly released info, label information, monitor outgoing traffic, watermarks, Internet searches, best practices) • Intellectual Property Valuation • IP defined • Patents • Trade secrets and know how (defined, how to identify) • Trademarks and Service marks (defined, registration, attacks)
Managing IT Business and Program Growth in a Globalized Marketplace	• 2050 largest economy • 5 specific cultural points (such as shaking hands) • Four Ps of Marketing (product, price, promotion, position) • Key Business Concepts (continuous process improvement, strategic and disruptive innovation) • Location (physical and virtual) • Potential barriers to global communication and business • Three Cs (customer, cost, community) • Value Added Tax (VAT defined and benefits)
Managing Legal Liability	• Best Practices for Managing Liability • Common Damages • Downstream liability and contributory negligence (related to DiD and due diligence) • Indicators of Fraud • Types of Fraud (internal, customer, credit card, accounting, telecom, etc) • Zublake standard and eDiscovery
Managing Negotiations	• Negotiation Keys (internalization, change, authority, price vs value, speed, walking away) • Distributive Bargaining (BATNA, ZOPA, claiming value, anchoring point) • Good negotiation is win-win. • Integrative Bargaining (principled, mutual gains, win-win)

Managing PDA Infrastructure	• Centralized Management versus Individual Device Management • Security Threats • Synchronization
Managing Privacy	• OECD Privacy Principles • Personally Identifiable Information (PII) • Privacy Certifications as proof of due diligence (TRUSTe, WebTrust, BBB Online Privacy Seal) • Significant privacy cases
Managing Security Policy	• Issue-specific policy • Policy assessment -SMART • Policy Benefits • Policy development tools (standards, guidelines, frameworks, mission statement) • Security Posture and Culture
Managing Software Security	• Architectural Issues • Best Practices (safe defaults, modular code, user accountability, error handling) • Code Review (Manual, Automated, Hybrid, SDLC Integration) • Understand basics of common implementation flaws at a high level
Managing Technical People	• E-mail (business record, retention policy, when to use other comms) • Encouraging Closure of projects • Integrity • Listening to and understanding technical people • Meeting best practices • Understand the power dynamic between technical staff and management • Value of Metrics

Managing the Mission	• Doctrine • Goals • Mission Statement • Vision Statement
Managing the Procurement Process	• Difference between price and value • Negotiating with vendors (vendor honesty and key negotiating points) • Product Support and Outsourcing • Trade Show Tips • Vendor and Product Selection, Ricochet Response
Managing the Total Cost of Ownership	• Direct costs and Indirect costs • Depreciation (straight line, sum of years) • SDLC disposal phase (grave costs) • TCO (defined, how to calculate)
Methods of Attack	• Browsing, Enumeration, and Traffic Analysis • Buffer Overflow key concepts • Denial of Service (centralized p2p, distributed, physical) (basic forms: resource exhaustion , unexpected value, physical disruption, configuration disruption) • Google hacking database and Goolag • Infrastructure attacks (satellite, undersea cables, fiber optic trunks) • Logic bombs and the Duronio case • Malicious Code (Trojan horses and trapdoors) • MITM and Replay attacks • Phishing and spear phishing • Physical Attacks • Race conditions (timing attackes) • Rootkits • SPAM and e-mail flooding
Mitnick-Shimomura	• IP address spoofing • Disable defenses • DoS so legitimate IP does not alert

	• Sequence number prediction
Offensive OPSEC	• Competitive intel tools and features (whitepages.com, whois.net, nslookup, tracert, geobytes, wayback machine, Dun and Bradstreet) • Differentiate between espionage and competitive intelligence • Info on Individuals (google, intelius, credit reporting) • Key Google searching techniques (ext, intitle, site, link, cache, related, inanchor, info) • Limiting publicly available info (email and web) • Sources for researching corporate information • Using press releases
Project Management For Security Leaders	• Closing out • Monitor, Control, Conflict Resolution, Change Management • Phases of project management • Project Management Terms • Staying on top of execution is key to bringing tasks to close
Quality	• Deming out of crisis • DemingÕs 14 points • Process Improvement
Risk Management and Auditing	• Acceptable Risk (who decides) • Acting on the risk (accept, mitigate, transfer, avoid) • Analysis types (SWOT, Cost Benefit, Weakness Gap, Threat Gap) • Best Practices (templates, group policy, hotfixes, www.cisecurity.org, etc.) • Briefing Management • Calculating Annualized Loss Expectancy (ALE) • Calculating Single Loss Expectancy (SLE) • Difference between qualitative and quantitative approaches • Terminology (Risk, threat, vulnerability, SDLC) • Types of Risk

Safety	• Evacuation preparation and procedures • Safety first, security second • Safety walkthrough
Security and Organizational Structure	• Capacity analysis and methods for increasing capacity • Employee discipline and termination • Employee performance (measuring, diagnosing causes of failure) • Employee retention, compensation, and promotion • Filling positions (requirements, hiring, interviews, 1099) • Potential conflict of interest for CISO/CSO to report to CIO
Security Frameworks	• Cobit • ISO 27001/27002 (formerly ISO 17799) defined • Understand security's relationship to the organizations mission
Selling Security	• Selling A Security Program to upper management • Strategic Information Systems Plan
Steganography	• Differences between steganography and cryptography and why detection is more difficult • Methods (injection, substitution, file generation) • Steganalysis
The Intelligent Network	• Basic troubleshooting (troubleshooting UTM) • Data Normalization • Firewall types and the default rule • HIPS and NIPS basics • Ingress/Egress filtering • IPS and IDS basics, alert types, and importance of detection • Managing NIDS Costs (deployment and maintenance) • Signature Analysis, Anomaly Analysis, and Application/Protocol Analysis • Type 1 and Type 2 Virtualization

	• Unified Threat Management (features, drawbacks, selection criteria)
The Network Infrastructure	• Logical and physical topologies • Network Components • Network segmentation • TCP Model • The OSI Model (frequently used in troubleshooting) • VLANs and how they support Defense In Depth • VOIP Basics, Security Implications, availability issues, and threats
Vulnerability Management - Inside View	• CISecurity.org • Inside view, tools, approach
Vulnerability Management - Outside View	• Basic Hacker Process • Exploitation tools versus vulnerability scanners • How to do a scan, process, dos and don'ts • Inside view, outside view, user view • Manager's role in prioritizing remediation • Risk of not remediating after knowing about vulnerability • Role of penetration testing in vulnerability management • Scanning techniques (port, stealth, tcp/udp, passive) • Threat Concerns • Threat Vectors - relation to DiD • Why war dialing is still important, tools
Vulnerability Management - User View	• Awareness and Inoculation • P2P and IM dangers and controls • Social Engineering

Web Communications and Security	• CGI and State/Cookie basics • Cross Site Scripting • HTTPS security misconceptions • JavaScript Object Nation • Protocol basics (HTTP and HTTPS) • Proxy modification of cookies • SOA (Exposes business logic) • SQL Injection (stored procedures and input validation to mitigate)
Wireless Advantages and Bluetooth	• Attacks (bluesnarf, bluejack, sniffing) • Bluetooth defenses (non-discoverable mode, auditing, pairing in trusted environment, strong PINS) • Bluetooth protocol fundamentals (PIN, discovery mode) • Wireless Advantages