The CISSP Bootcamp is a fast-paced, highly condensed, “11th hour” crash course for those students who are getting ready to take the CISSP exam in the next few weeks. It is also an excellent course for those who want to discover the depth and breadth of the exam and build their security knowledge foundation for the real world. The course will cover the objectives, high-points and more difficult topics of all CISSP domains.

The instructor for this bootcamp will be Michael J Shannon. Mr. Shannon began his IT career when he transitioned from recording studio engineer to network technician for a major telecommunications company in the early 1990’s. He soon began to focus on security and was one of the first 10 people to attain the HIPAA Certified Security Specialist. Throughout his 30 years in IT he has worked as an employee, contractor, and consultant for several companies including Platinum Technologies, Fujitsu, IBM, State Farm, MindSharp, Thomson, Pearson, and Skillsoft among others. Mr. Shannon has authored several books, training manuals, blog articles, and CBT modules over the years as well. He has attained the CISSP, CCSP, Security+, CCNP Security, Palo Alto PCNSE7, ITIL 4 Managing Professional, and OpenFAIR security-related certifications, as well as other various cloud- based certifications.

Course Syllabus

Session 1

- **Introduction to CISSP 2021**
  - The (ISC)² organization
  - (ISC)² Code of Ethics
  - The (ISC)² Code of Ethics Preamble and Canons
  - The CISSP exam and certification
- **Fundamental Concepts and Principles**
  - The CIA triad, DAD, and the Parkerian Hexad
  - The OSI reference model
  - The TCP/IP reference model
- **Secure Design Principles**
  - Least Privilege and Need-to-Know
  - Defense-in-Depth (DiD)
  - Separation-of-Duties (SoD) and Keep it Simple
  - Zero Trust, Secure Defaults, and Fail Securely
  - Privacy by Design and Trust but Verify
- **Security Governance Principles**
  - Aligning Security with Business
  - Organizational Roles, Responsibilities, and Processes
  - Data and Asset Ownership
  - Due Diligence and Due Care
  - Security Governance
  - Privacy Governance
  - Security Control Frameworks
  - Cybercrime issues and conducting investigations
- **Security Policy**

    - Policy Development and Implementation
    - Acceptable Use Policy (AUP)
    - Employment Policies
    - Agreements and third-party factors
    - Security Awareness Education and Training

Session 2

- **Asset Classification and Lifecycle**
    - Data States
    - Data and Asset Classification
    - Configuration Management Database (CMDB)
    - Asset Inventory and Management
    - Data Handling Roles
    - Data Lifecycle Management
- **Risk Management**
    - Inherent vs. Residual Risk and Risk Treatment
    - Assessing Vulnerability and Vulnerability Information Gathering
    - Risk Assessment Documents
    - Qualitative, Semi-quant, and Quantitative Analysis
    - Control Categories and Types
    - Risk Management Frameworks
    - Countermeasure Selection and Implementation
    - Risk Monitoring and Reporting
    - Supply Chain Risk Management (SCRM)
- **Practical Cryptography**
    - Symmetric and Asymmetric Key Algorithms
    - Diffie-Hellman Key Exchange
    - HMAC for Integrity and Origin Authentication
    - Digital Signatures and Certificates
    - Elliptic Curve Cryptography and Quantum Computing
    - Key Management and HSMs
    - Public Key Infrastructure
    - OCSP Stapling and Certificate Pinning
    - Cryptanalysis Methods
- **Identity and Access Management Principles**
    - Controlling Physical and Logical Access
    - Access Security Models and Architectures
    - Deploying Identity and Access Management

Session 3

- **Deploying Identity and Access Management (IAM)**
    - RADIUS and TACACS+
    - SAML and SSO Vulnerabilities

    - Oauth and OIDC
    - Kerberos
    - Provisioning and Deprovisioning
    - IAM and IdM
    - NAC and 802.1X Solutions
    - Accounting and Session Management
    - Identity Registration and Proofing
- **Architecture, Design, and Solutions Vulnerabilities**
    - Client-side vs. Server-side
    - Database Security
    - SCADA Security
    - Virtualization and Hypervisor Vulnerabilities
    - Cloud Service Types and Deployment Models
    - MSSPs and CASBs
    - Securing Distributed Systems
    - Mobile Device Security
    - Internet of Things (IoT)
    - Containers, Microservices, and Serverless Technology
    - Embedded Systems, TPM and Memory Protection
    - HPC and Edge Computing Systems
- **Site and Facility Security**
    - Primary and Secondary Loss
    - Physical Defense-in-Depth
    - Perimeter Barriers
    - Cameras and Lighting
    - Industrial Camouflage
    - Security Guards, Sensors, and Alarms
    - Locking Mechanisms
    - Power and Environmental Controls
    - Distribution Frames, Wiring Closets, and Datacenters
    - Secure Enclosures
    - Fire Controls

Session 4

- **Communication and Network Security**
    - Secure Protocols
    - Software-Defined-Networking
    - Secure Switches and Routers
    - Firewalls and IPS Systems
    - Active Defense
    - Wireless Devices and Security
    - Other Communication Systems and Security
    - Content Delivery Networking (CDN)
    - Endpoint Security

  - IPsec and Transport Layer Security (TLS)
- **Security Operations: IT Service Management, Incident Response, and Forensics**
  - Configuration, Change, and Patch Management
  - Vulnerability Assessment and Management
  - Logging and Monitoring Activities
  - Incident Response and Management
  - Forensic Investigations

Session 5

- **Security Operations: Business Continuity Planning**
  - Business Impact Analysis
  - Business Continuity Planning (BCP)
  - Backup Storage Strategies
  - Implement Recovery Strategies
  - Personnel Safety and Security Concerns
  - Testing Disaster Recovery Plans
- **Security Assessment and Testing**
  - Assessment, Test, and Audit Strategies
  - Security Control Testing
  - Collect Security Process Data
  - Analysis and Report Generation
- **Application Development Security**
  - Development Methodologies
  - Maturity Models
  - Integrated Product Teams (IPT)
  - Identify Security Controls
  - Software Configuration Management (SCM)
  - Application Security Testing
  - Assess Software Security Effectiveness
  - Cloud Development Deployment
  - Source-code Weaknesses
  - Application Programming Interface (API) Security
  - Secure Coding Practices
  - Software-defined Security