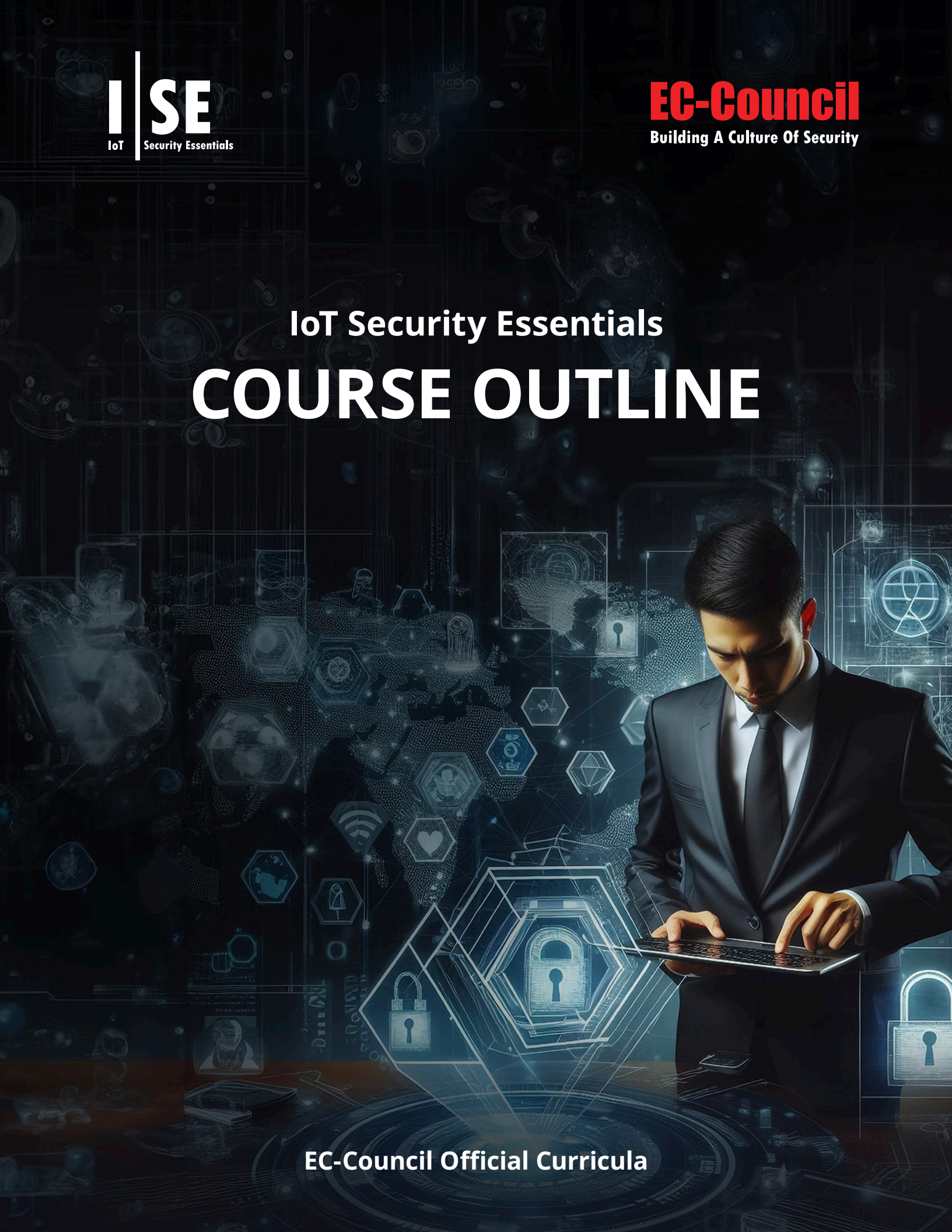
IoT | SE
IoT Security Essentials

EC-Council
Building A Culture Of Security

IoT Security Essentials
COURSE OUTLINE



EC-Council Official Curricula

IoT Security Essentials (ISE)

Course Outline

(Version 1)

Module 01: IoT Fundamentals

- Definitions
- IoT
- IoT Beginnings
- The IoT Paradigm
- IoT Characteristics
- What's Smart?
- Smart Technology
- IoT in Power Grids and Home
  - Smart Homes
  - Smart Grid
  - Smart Grid Case Study
  - Smart Grid – Why?
  - Smart Grid – Smart City
  - Smart Agriculture
- Internet of Military Things
  - IoT Architecture
  - IoT Application Areas and Devices
  - IoT Technologies and Protocols
  - IoT Communication Models
- Industrial IoT basics

- SCADA
- NIST 800-82 – SCADA
- DCS
- Smart City
  - Smart City Framework
- Health IoT
  - Remote Patient Monitoring
  - Medical IoT wearable devices
  - Medical IoT internal devices
  - Medical IoT Under Skin Devices
- IoT Platforms
  - IoT Platforms – Xively
  - IoT Platforms – AWS IoT
  - IoT Platforms - GE Predix
  - IoT Platforms - Google Cloud IoT
  - IoT Platforms - Microsoft Azure IoT
  - IoT - Technical Basics
- Nodes and Applications in Wireless Sensor Networks
  - Types of Nodes
  - Types of Applications
- The Future of IoT

Module 02: IoT Networking and Communication

- Basic Concepts – MAC Address
- EUI-64
- Network Concepts– IP Addresses (IPV4)
- Private Vs. Public
- Private IP Address
- OSI Model - Open Systems Interconnect
- TCP Model
- IP Addresses and Subnet Masks

- IPv4 Subnetting Techniques
- Custom IP Addresses
- CIDR
  - CIDR Address
- IP Address Services
- APIPA
- IPv6
- Network Concepts - Wi-Fi
- Narrowband, Broadband, and Spread Spectrum Signals
- Frequency Hopping Vs. Direct Sequence
- Spread Spectrum Details
- 802.11 Broadcast Methods
- 802.11 Channels
- IoT Protocols
- Bluetooth
  - 802.15
  - Bluetooth Protocols
  - Simplified Bluetooth Stack
- ANT+
- IPv6 Over Low Power Wireless Personal Area Networks (6LowPAN)
- 6LowPAN
- NFC
- RFID
- ZigBee
- IEEE 802.15.4 Physical Layer
- Operating Frequency Bands
- PHY Frame Structure
- IEEE 802.15.4 MAC Layer
- IEEE ZigBee Network Topologies MAC Layer
  - ZigBee Network Topologies
  - ZigBee and Bluetooth Comparison

- Z Wave
- LoRa
- RuBee
- WirelessHART
- MiWi
- MQTT
- TR-069
- OMA-DM
- XMPP
- DDS
- Constrained Application Protocol (CoAP)
- Cellular Networks
- 5G
- Windows IoT
- Power System Communication Technologies
- Power Line Carrier Communication (PLCC)
  - Coupling Types in PLCC System
  - PLCC---Uses
  - PLCC---Fiber Optic
- Tele-Control Protocols
- IEC–60870–5-101
- ICCP Protocol
- IEEE Standards
- Distributed Network Protocol 3 (DNP3)
- IEEE IoT Standards List
- Building Information Model

Module 03: IoT Processors and Operating Systems

- PCB
- NAND
- UART

- JTAG
- CPU Internal Structure
- Interrupts
- Operating Systems
- Features of the OS in Embedded Systems
- Operating System Kernel
- Kernel Types
- Firmware
- Real-Time Operating System (RTOS)
- Type of Real-Time Systems
- Performance Evaluation
- Four Main Tasks of an OS
- RTOS – VxWorks
- What is VxWorks?
- Differences Between Traditional UNIX and VxWorks
- VxWorks Architecture
- VXWorks Networking Support
- RTPS QNX
- RTOS – LINUX
- Contiki
- The Contiki OS
- Contiki Protothreads and Dynamic Linking
- RIOT
- TinyOS
  - TinyOS Design
  - TinyOS Tools
  - TinyOS Scheduler
- MagnetOS
- FreeRTOS
- Apache Mynewt
- BeRTOS

- Zephyr
- Linux & Android
  - History of Linux
  - Linux
  - Linux Shells
  - Basic Shell Command Summary
  - Run Levels
  - Android Linux Kernel
  - Android OS
  - Android App Priority and Processes
  - Linux Kernel and Storage Management
  - Android Architecture
  - Android Versions
  - Android Automotive
  - Android TV
  - Android Things

Module 04: Cloud and IoT

- What is Cloud Computing?
- NIST
- Cloud Characteristics
- Types of Cloud Computing Services
- Cloud Deployment
- Basic Cloud Concepts
- Cloud Computing
- Cloud Types
- Multi-cloud
- HPC Cloud
- Virtualization
- Virtual Systems
- IaaS

- PaaS
- SaaS
  - Example SaaS: Google Docs
- Variations
- Characteristics of Virtualization
- Virtual Components
- Distributed Systems Issues
- Terms
- Uses of Cloud Computing
- IoT Cloud Commercial Solutions
- AWS IoT
- AWS IoT Components
- Oracle Cloud
- Grid Computing
- Fog Computing
- Future Trends

Module 05: IoT Advanced Topics

- IoT Software
- Web Applications
- Hybrid Model
- Embedded Device Web App
- Web Communications
- Mobile Applications
- Hybrid
- Native Applications
- IoT Identity Management
- IoT Protocols
- What is Machine Learning?
- IoT and Machine Learning
- Types of Learning

- Supervised vs. Unsupervised Learning
- Classification
- Neural Networks
- Terminology
- Hebb's Rule
- ANNs – The Basics
- Topologies of Neural Networks
- Multi-Layers
- Recurrent Networks
- Elman Nets
- Neural Network Function
- K-Nearest Neighbor
- Echo State Network
- Naive Bayes
- Block Chain IoT
- What is a Block?
- What is a Transaction?
- Block Chain IoT
- How to Achieve Convergence?
- Structure of a Block Chain
- Consensus Algorithms

Module 06: IoT Threats

- List of Common IoT Attacks
- IoT Vulnerable
- How Bad is the Problem?
- Mirai
- BrikerBot
- Other Notable IoT Attacks
- Definition of Sybil Attack
- Sybil Attack

- Sinkhole Attack
- TinyOS Beaconing
- Geographical Attacks and Attackers
- Spoofed, Altered, or Replayed Routing Info
- Wormhole Attack
- Blackhole Attack
- Rushing Attacks
- HELLO Flood Attack
- Smart Heating Shutdown
- Access Internal State
- Modify Internal State
- Clone TAP
- IoT Expands Security Needs
- OWASP IoT Top 10
- Dark Reading Top 8 Attacks
- IoT Attack Surface
- IoT Goat
  - Example DOS – Syn Flood
  - Example DOS – Smurf
  - Example DOS – Fraggle
- DHCP Starvation
- Amplification
- Other DoS Attacks
- Bluetooth Attacks
- Wireless Attacks
- IoT Hacking
- IoT Attacks
- IoT Privacy Issues
- Malware
- Virus Types
- Hiding Techniques

- Ransomware
- Smart Thermostat Ransomware
- Other New Attacks
- Hacking Medical Devices
- Hacking Cars
- Hacking Homes
- IoT Hacking
- Metasploit and IoT
- SCADA - Poor Authentication and Authorization
- SCADA Unpatched Systems
- E-passport Threats
- Security Threats of RFID-Enabled Supply Chain

Module 07: Basic Security

- The CIA Triangle
- Other Security Concepts/Terms
- Best Practices for Protecting Embedded OSs
- WLAN Security Goals
- Basic WLAN Security Mechanisms
- Open System Authentication
- Shared Key Authentication
- WEP
- WPA
- WPA2
- WPA3
- MAC Address Filtering
- Disabling SSID Broadcast
- Changing the Default Login
- Bluetooth Security Modes
- Authentication Summary
- Zigbee Security

- RuBee Security
- IoT Checklist
- IoT Security Measures
- IoT Security Tools
- Firmware Security Testing Methodology
- ByteSweep
- Stanford Secure IoT project
- System Hardening
- Symmetric Block Cipher Algorithms
- Symmetric Encryption
- DES & AES
- Blowfish
- Asymmetric Encryption
- How Does Public/Private Key Encryption Work?
- RSA & Diffie-Helman
- Digital Signature Basics
- Hashes
- What is a Collision?
- History of SSL
- TLS v 1.3
- Remote Access Security - TLS
- SSL/TLS Handshake
- Certificate Store
- Basics of Defending SCADA/ICS
- SCADA Security Basics
- SCADA Security Standards
- RTU Security - Serial Port
- Current Grid Environment
- Threats to the Grid
- NISTIR 7628
- Medical Device Standards

- EMC Terminology
- IoT Privacy
- IoT Security Compliance Framework 1.1
- Industrial IoT Security Framework
- IETF
- NIST
- NISTIR 8228
- IEEE Standards
- Security in the SDLC
- Legal, Regulatory, and Rights Issues
- Aircrack
- Wireless tools
- Other Wifi tools
- Bluetooth tools
- Security Protocols For Wireless Sensor Networks
- SNEP: Sensor Network Encryption Protocol
- TINYSEC
- MINISisEC
- LEAP: Localized Encryption And Authentication Protocol
- ZigBee Security
- ZigBee Security Trust Center
- ZIGBEE

Module 08: Cloud Security

- State of Cloud Security
- Cloud Threats On the Rise
- Cloud Vulnerabilities
- Issues
- Critical Security Areas in Cloud Computing (CSA)
- Top 10 Customer Issues Eroding Cloud Confidence (from CSA)
- Privileged Access

- Data Segregation
- Cloud Security Alliance - Guidance
- CloudAudit & the A6 Deliverable
- ISO 27017
- ISO 27018
- NSA Guidance
- Cloud Computing Attacks
- Man in the Cloud
- Cloudbleed
- Secure Cloud Computing
- Infrastructure Security
- Compliance
- Cloud Computing Also Relies on the Security of Virtualization
- Sample Hypervisor Security Issues
- Security Issues
- Virtualization Security Guidance
- Cloud Provider Employees
- Mobile Cloud
- IRM
- Privacy & Personal Information
- U.S. Privacy Law
- GDPR
- Cloud Security Policies
- Procedures, Standards, and Guidelines
- Policy Types
  - NIST 800-14
  - NIST 800-14 - Principles
  - NIST 800-14 – Practice Areas
- Investigative Support
- Forensic Issues

Module 09: Threat Intelligence

- National Vulnerability Database
- US Cert
- Shodan
- IoT Sploit
- Alien Vault
- Threat Crowd
- Phishtank
- STRIDE
- DREAD
- PASTA
- CVSS
- Common Vulnerability Exposure (CVE)
- Risk Determinations
- Risk Assessment Standards
- Addressing Risk
- Residual Risk
- Find Web Cams
- Web Cams Default passwords
- NIST 800-115
- NIST 800-53 A
- National Security Agency (NSA) Information Assessment Methodology (IAM)
- NSA-IAM Overview
- IAM
- PCI Penetration Testing standard
- PCI Highlights
- PTES
- Cyber Kill Chain
- CEH Lifecycle
- Vulnerability
- TCPdump

- FLAGS
- Packet Flags
- Nmap
  - Nmap (ZenMap the GUI Version)
- NMAP Flags

Module 10: IoT Incident Response

- Standards
- Processes
- Procedures
- Impact
- IoT and the Cloud
- Indicators of Compromise
- Tools
- Forensic Tools

Module 11: IoT Security Engineering

- Methodologies
- 12 Practices
- Threat Modeling
- Dread
- Stride