Securing IoT Infrastructure in Smart Cities Training Course



19 - 23 Oct 2026

Sharm El-Sheikh

4100 € (Per Person)

Ref: #CYB8052_272596

Course Introduction / Overview:

The rapid evolution of smart cities, powered by the Internet of Things (IoT), promises unprecedented efficiency and quality of urban life. However, this interconnectedness introduces a complex and expansive attack surface, making smart city cybersecurity a critical priority. This course provides a comprehensive exploration of the strategies and technologies required to secure IoT ecosystems within urban environments. It moves beyond theoretical concepts to deliver practical, actionable knowledge for protecting critical infrastructure, from smart grids and intelligent transportation systems to public safety networks. As highlighted by cybersecurity expert Dr. Kim-Kwang Raymond Choo, the convergence of physical and digital realms in IoT necessitates a multi-layered security approach. This program, offered by BIG BEN Training Center, is meticulously designed to equip professionals with the skills to design, implement, and manage robust IoT security frameworks. Participants will delve into threat modeling, vulnerability assessment, and incident response, ensuring they can safeguard the data, devices, and citizens that define the smart city of the future.

Target Audience / This training course is suitable for:

- IT and Cybersecurity Professionals.
- Urban Planners and City Managers.
- IoT Solution Architects and Developers.
- Network Engineers and Administrators.
- Government and Public Sector Technology Leaders.
- Security Consultants and Auditors.
- Critical Infrastructure Operators.
- Technology Policy and Compliance Officers.

Target Sectors and Industries:

- Government and Public Administration.
- Energy and Utilities.
- Transportation and Logistics.
- Telecommunications.
- Real Estate and Smart Building Management.
- Public Safety and Emergency Services.
- Healthcare and Public Health.
- Engineering and Construction.

Target Organizations Departments:

- Information Technology (IT) and Information Security.
- Operations Technology (OT).
- Urban Planning and Development.
- Research and Development (R&D).
- Risk Management and Compliance.
- Public Works and Infrastructure Management.
- Corporate Security.
- Innovation and Smart City Project Teams.

Course Offerings:

By the end of this course, the participants will have able to:

- Analyze the unique threat landscape and vulnerabilities of smart city IoT ecosystems.
- Develop a comprehensive security strategy for the entire IoT device lifecycle.
- Implement robust security protocols for IoT networks, including 5G and LPWAN.
- Design and enforce data privacy and protection policies for smart city data.
- Conduct IoT-specific vulnerability assessments and penetration testing.
- Create an effective incident response plan for security breaches in a smart city context.
- Evaluate and apply international IoT security standards and frameworks.
- Integrate security into the design of smart city applications and services.
- Manage risks associated with third-party vendors in the IoT supply chain.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and directly applicable to real-world challenges. This course combines expert-led presentations with hands-on labs and collaborative workshops to ensure a deep understanding of IoT security principles. Participants will engage with detailed case studies of actual smart city security incidents, analyzing both successful defenses and critical failures. Team-based exercises will focus on practical skills such as threat modeling for a new smart traffic system or developing a risk mitigation plan for a public utility's IoT network. Interactive sessions encourage peer-to-peer learning and knowledge sharing, allowing participants to discuss challenges specific to their own organizations. The instructor will provide continuous feedback and facilitate discussions that bridge technical details with strategic governance. This blended approach ensures that participants not only learn the theory but also gain the confidence and competence to implement effective IoT security measures in their professional roles.

Course Agenda (Course Units):

Unit One: Foundations of Smart City and IoT Security

- Introduction to Smart City Architecture and Ecosystems.
- The Role of IoT in Urban Infrastructure.
- Understanding the IoT Security Threat Landscape.
- Key Vulnerabilities in Connected Devices and Systems.
- Common Attack Vectors against Smart Cities.
- Principles of Secure IoT Architecture Design.
- Introduction to IoT Security Frameworks and Standards (NIST, ETSI).

Unit Two: Securing the IoT Device and Hardware Layer

- The IoT Device Lifecycle Management.
- Hardware Security Fundamentals (Secure Elements, PUFs).
- Secure Boot and Trusted Execution Environments.
- Firmware and Software Update Security Mechanisms.
- Device Identity, Authentication, and Provisioning.
- Physical Tampering Detection and Response.
- Managing Security for Legacy and Resource-Constrained Devices.

Unit Three: Network, Communication, and Edge Security

- Securing IoT Communication Protocols (MQTT, CoAP, LwM2M).
- Wireless Network Security (Wi-Fi, LoRaWAN, NB-IoT).
- Security Considerations for 5G in Smart Cities.
- Introduction to Edge and Fog Computing Security.
- Implementing Network Segmentation and Micro-segmentation.
- Intrusion Detection and Prevention Systems for IoT Networks.
- Securing VPNs and APIs for IoT Communications.

Unit Four: Data Privacy, Cloud, and Application Security

- Data Protection and Privacy Regulations in Smart Cities (GDPR).
- End-to-End Data Encryption Strategies.
- Securing IoT Data at Rest, in Transit, and in Use.
- Cloud Platform Security for IoT Data Aggregation.
- Secure Software Development Lifecycle (SSDLC) for IoT Applications.
- API Security and Access Control Management.
- Blockchain Technology for Enhancing IoT Security and Trust.

Unit Five: Governance, Risk Management, and Incident Response

- Developing an IoT Security Governance Framework.
- Conducting IoT Risk Assessments and Management.
- Building a Smart City Security Operations Center (SOC).
- IoT Incident Response and Forensics.
- Developing and Testing a Cyber-Resilience Strategy.
- Ethical Considerations and Public Trust in Smart City Technology.
- Future Trends and Challenges in Smart City Cybersecurity.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Beyond technical safeguards, what societal and ethical frameworks are necessary to build true trust in a fully connected smart city ecosystem?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by adopting a holistic, ecosystem-wide perspective on smart city security, moving beyond the protection of individual devices to address the complex interplay between hardware, networks, data, and urban governance. Unlike programs that focus narrowly on technical exploits, this training integrates strategic risk management, regulatory compliance, and policy development, providing a complete framework for building cyber-resilient cities. Its curriculum is uniquely structured around the entire IoT lifecycle, from secure device provisioning to end-of-life decommissioning, ensuring no security gaps are overlooked. Furthermore, the course content is deeply rooted in practical application, using real-world case studies from municipal transportation, public utilities, and emergency services to illustrate key principles. Participants will not just learn about security standards; they will learn how to apply them within the unique political, social, and economic constraints of an urban environment. This strategic, lifecycle-based, and practical approach equips leaders to build secure, trustworthy, and sustainable smart cities for the future.