



Certified Internet of Things Security Practitioner™ (ITS-110) Exam Blueprint

Date Issued: 1/15/2019

Date Modified: 9/20/2022

Version: 1.5

Approved by: Scheme Committee



CIoTSP

Introduction to CertNexus

CertNexus is a vendor-neutral certification body, providing emerging technology certifications and micro-credentials for business, data, developer, IT, and security professionals. CertNexus' mission is to assist closing the emerging tech global skills gap while providing individuals with a path towards rewarding careers in Cybersecurity, Data Science, Data Ethics, Internet of Things, and Artificial Intelligence (AI)/ Machine Learning (ML).

We rely on our Subject Matters Experts (SMEs) to provide their industry expertise and help us develop these credentials by participating in a Job Task Analysis, Exam Item Development, and determining the Cut Score. We also depend upon practitioners in the field to participate in a survey of the Job Task Analysis and beta testing to ensure that our certifications validate knowledge and skills relevant to the industry.

Acknowledgements

CertNexus was honored to have the following Subject Matter Experts contribute to the development of this exam blueprint.

Stephen Denman	Sandia National Laboratories	https://www.sandia.gov	
Christopher Gregory	Hobart and William Smith Colleges	https://www.hws.edu	
Mark Szewczul	Digital.ai	https://digital.ai	
John Hackmeyer	CyberCrocodile, LLC	https://cybercrocodile.com	
Usman Minhas	IBM	https://www.ibm.com/	

Exam Information

The *Certified Internet of Things Security Practitioner™ (CIoTSP)* is an industry-validated certification which helps professionals differentiate themselves from other job candidates by demonstrating their ability to put security concepts related to IoT into practice. This calls for a robust workforce of professionals who have the skills and ability to defend your networks and respond when needed. In addition, it will validate the knowledge and skills to secure network environments for IoT devices, analyze vulnerabilities and determine reasonable controls against threats, and effectively monitor IoT devices and respond to incidents.

Candidate Eligibility

The *Certified Internet of Things Security Practitioner™ (CIoTSP)* exam requires no application fee, supporting documentation, or other eligibility verification measures for you to be eligible to take the exam. An exam voucher will come bundled with your training program or can be purchased separately [here](#). Once purchased, you will receive more information about how to register for and schedule your exam through Pearson Vue. You can also purchase a voucher directly through Pearson Vue. Once you have obtained your voucher information, you can register for an exam time [here](#). By registering, you agree to our Candidate Agreement included [here](#).

Exam Prerequisites

While there are no formal prerequisites to register for and schedule an exam, we strongly recommend you first possess the following knowledge:

- Understanding of the fundamental benefits and challenges of securing IoT systems.
- Understanding of an IoT ecosystem, including the physical elements, edge/fog computing elements, network and connectivity elements, cloud and cloud platform elements, and the applications and “Things” within various market sectors.
- Understanding of common IoT security and privacy threats and countermeasures.
- Understanding of common IoT safety and risk management approaches.
- Understanding of the IoT system/software development life cycle.

You can obtain this level of skill and knowledge by taking the following courseware, which is available through training providers located around the world, or by attending an equivalent third-party training program:

- *Certified Internet of Things (IoT) Security Practitioner™ (Exam ITS-110)*

Exam Specifications

Number of Items: 100

Passing Score: 60%

Duration: 120 minutes (**Note:** Exam time includes 5 minutes for reading and signing the Candidate Agreement and 5 minutes for the Pearson VUE testing system tutorial.)

Exam Options: In person at Pearson VUE test centers or online with Pearson OnVUE online proctoring

Item Formats: Multiple Choice / Multiple Response

Exam Description

Target Candidate:

This certification exam is designed for practitioners who are seeking to demonstrate a vendor-neutral, cross-industry skill set that will enable them to design, implement, operate, and/or manage a secure IoT ecosystem.

Exam Objective Statement:

This exam will certify that the candidate has the foundational skill set of secure IoT concepts, technologies, and tools that will enable them to become a capable IoT Security practitioner in a wide variety of IoT-related job functions.

To ensure exam candidates possess the aforementioned skills, the *Certified Internet of Things Security Practitioner™ (CIoTSP)* exam will test them on the following domains with the following weightings:

Domain	% of Examination
1.0 Securing IoT Portals	29%
2.0 Implementing Authentication, Authorization, and Accounting	14%
3.0 Securing Network Services	14%
4.0 Securing Data	14%
5.0 Addressing Privacy Concerns	12%
6.0 Securing Software/Firmware	10%
7.0 Enhancing Physical Security	7%
Total	100%

The information that follows is meant to help you prepare for your certification exam. This information does not represent an exhaustive list of all the concepts and skills that you may be tested on during your exam. The exam domains, identified previously and included in the objectives listing, represent the large content areas covered in the exam. The objectives within those domains represent the specific tasks associated with the job role(s) being tested. The information beyond the domains and objectives is meant to provide examples of the types of concepts, tools, skills, and abilities that relate to the corresponding domains and objectives. All of this information represents the industry-expert analysis of the job role(s) related to the certification and does not necessarily correlate one-to-one with the content covered in your training program or on your exam. We strongly recommend that you independently study to familiarize yourself with any concept identified here that was not explicitly covered in your training program or products.

Objectives

Domain 1.0 Securing IoT Portals

Objective 1.1 Identify common threats used to compromise unsecure web, cloud, or mobile interfaces.

- Account enumeration
- Weak default credentials
- Injection flaws
- Unsecure direct object references
- Sensitive data exposure
- CSRF
- Unvalidated redirects and forwards
- Session Management
- Malformed URLs
- Session replay
- Reverse shell
- Misconfiguration
- Weak account lockout settings
- No account lockout
- Unsecured credentials
- Lack of integration credentials on Edge devices

Objective 1.2 Implement countermeasures used to secure web, cloud, or mobile interfaces.

- Change default passwords
- Secure password recovery mechanisms
- Secure the web interface from XSS, SQLi, or CSRF
- Protect credentials
- Robust password policies
- Account lockout policies
- Protect against account enumeration
- 2FA if possible
- Granular role-based access

Domain 2.0 Implementing Authentication, Authorization, and Accounting

Objective 2.1 Identify common threats used to exploit weak authentication/authorization schemes.

- Lack of password complexity
- Poorly protected credentials
- Lack of 2FA
- Unsecure password recovery
- Privilege escalation
- Lack of RBAC
- Unsecure databases and datastores
- Lack of account lockout policy
- Lack of access auditing
- Lack of security monitoring
- Lack of security logging

Objective 2.2 Implement countermeasures used to provide secure authentication, authorization, and accounting.

- Granular access control
- Password management
- Ensure re-authentication is required for sensitive features
- Event logging and IT/OT admin notification
- Security monitoring

Domain 3.0 Securing Network Services

Objective 3.1 Identify common threats used to exploit unsecure network services.

- Vulnerable services
- Buffer overflow
- Open ports via UPnP
- Exploitable UDP services
- DoS/DDoS
- DoS via network device fuzzing
- Endpoint (address) spoofing
- Packet manipulation/injection
- Networking, protocols, radio communications

Objective 3.2 Implement countermeasures used to provide secure network services.

- Port control
- Secure memory spaces
- DoS mitigation/DDoS
- Secure network nodes
- Secure field devices
- Secure network pathways

Domain 4.0 Securing Data

Objective 4.1 Identify common threats used to exploit unsecure data.

- Vulnerable data in motion
- Vulnerable data at rest
- Vulnerable data in use

Objective 4.2 Implement countermeasures used to secure data.

- Encrypt data in motion, at rest, and in use

Domain 5.0 Addressing Privacy Concerns

Objective 5.1 Identify common threats used to compromise privacy.

- Collection of unnecessary personal or sensitive information (PII, PHI, metadata)
- Unsecured data in transit or at rest
- Unauthorized access to personal information
- Lack of proper data anonymization
- Lack of data retention policies

Objective 5.2 Implement countermeasures used to ensure data privacy.

- Only collect critical data
- Protect sensitive data
- Comply with regulations/laws
- Authorize data users
- Data retention policies
- Data disposal policies
- End-user notification policies (GDPR)
- Enable courtesy notifications to end users
- Enable notifications as required by law

Domain 6.0 Securing Software/Firmware

Objective 6.1 Identify common threats used to exploit unsecure software/firmware.

- Poorly designed/tested software/firmware
- Unsecure updates/patches
- Firmware contains sensitive information
- Lack of OTA updates
- Constrained devices with non-existent security features
- Lack of end-to-end solution
- Software/firmware not digitally signed
- Unsecure bootloader/boot
- Unsecure key storage

Objective 6.2 Implement countermeasures used to provide secure software/firmware.

- Digitally signed updates
- Remote update capability for, e.g., bootloader, firmware, OS, drivers, application, certificates
- Secure updates/digitally signed updates
- Root-of-trust/secure enclave
- Secure bootloader/boot, measured boot

Domain 7.0 Enhancing Physical Security

Objective 7.1 Identify common threats used to exploit poor physical security.

- Access to software/configuration via physical ports
- Access to or removal of storage media
- Unprotected shell access for accessible ports
- Unrestricted physical access to vulnerable devices
- Easily disassembled devices

Objective 7.2 Implement countermeasures used to ensure physical security.

- Protect data storage medium
- Encrypt data at rest
- Protect physical ports
- Tamper-resistant devices
- Limit physical access when possible
- Hardened security for shell access
- Limit administrative capabilities and access

Recertification Requirements

The *Certified Internet of Things Security Practitioner™ (CIoTSP)* certification is valid for 3 years from the time certification is granted. You must retake the most up-to-date version of the exam prior to the 3-year period's end to maintain a continuously valid certification.

Certified Internet of Things Security Practitioner™ (CIoTSP) Acronyms

Acronym	Expanded Form
2FA	two-factor authentication
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
API	application program interface
APN	Access Point Name
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name Server
DoS	Denial of Service
ECC	elliptic curve cryptography
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
IoT	Internet of Things
IPSec	Internet Protocol Security
IT	information technology
LDAP	Lightweight Directory Access Protocol

M2M	machine-to-machine
OT	operational technology
OTA	Over-the-Air
PHI	personal health information
PII	personally identifiable information
PKI	public key infrastructure
RBAC	Role Based Access Control
RSA	Rivest-Shamir-Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SQLi	Structured Query Language Injection
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPnP	Universal Plug and Play
UDP	User Datagram Protocol
XSS	Cross-Site Scripting



CertNexus offers personnel certifications and micro credentials in a variety of emerging technology skills including Cybersecurity, Cyber Secure Coding, the Internet of Things (IoT), IoT Security, Data Science, Artificial Intelligence, and Data Ethics. For a complete list of our credentials visit <https://certnexus.com/certification/>.

CERTNEXUS[®]

1150 University Ave, Suite 20, Rochester, NY 14607

1-800-326-8724 | info@certnexus.com

certnexus.com