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

Exam Information

Candidate Eligibility:
The Certified Internet of Things Security Practitioner™ (CloTSP) 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:

- CertNexus 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

**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:

<table>
<thead>
<tr>
<th>Domain</th>
<th>% of Examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Securing IoT Portals</td>
<td>29%</td>
</tr>
<tr>
<td>2.0 Implementing Authentication, Authorization, and Accounting</td>
<td>14%</td>
</tr>
<tr>
<td>3.0 Securing Network Services</td>
<td>14%</td>
</tr>
<tr>
<td>4.0 Securing Data</td>
<td>14%</td>
</tr>
<tr>
<td>5.0 Addressing Privacy Concerns</td>
<td>12%</td>
</tr>
<tr>
<td>6.0 Securing Software/Firmware</td>
<td>10%</td>
</tr>
<tr>
<td>7.0 Enhancing Physical Security</td>
<td>7%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
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
  - SQLi
  - Second order SQLi
  - LDAP injection
  - XSS
- 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
  - Strong passwords
  - Change default username and password
  - Password expiration policies
  - Secure password recovery mechanisms
  - 2FA where possible
- 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
  - FTP, DNS, SNMP, Telnet
- 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
  - Public data cellular network
  - Dedicated/Custom APN setting
  - Unsecured network ports

Objective 3.2  Implement countermeasures used to provide secure network services.

- Port control
  - Access control list
- Secure memory spaces
  - Fuzzing
  - Buffer overflow
- DoS mitigation/DDoS
  - Endpoints
  - Cloud
- Secure network nodes
  - Cloud
  - Gateway
  - Edge
- Secure field devices
- Secure network pathways
  - Physical
  - Logical

Domain 4.0  Securing Data

Objective 4.1  Identify common threats used to exploit unsecure data.

- Vulnerable data in motion
  - Internet
  - Local network
  - Poorly implemented SSL/TLS
  - Misconfigured SSL/TLS
  - M2M
Objective 4.2 Implement countermeasures used to secure data.

- Encrypt data in motion, at rest, and in use
  - SSL/TLS
  - SSH
  - IPSec
  - S/MIME
  - PKI
    - Symmetric
      - AES, 3DES
    - Asymmetric
      - RSA, DH, ECC

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
  - Anonymize
  - Encrypt
  - De-identify
- 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
  - Embedded sensors, actuators, and communication modules
  - Applications/software (programming, etc.)
  - System integration (API)
  - Microservice architectures (container security)
- 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
  - Hardened update server
  - Secured download and installation
  - Failsafe option to revert to previous bootloader/firmware
  - Method to modify certificates within endpoints after deployment
- 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 (CiTSP)* 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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expanded Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>2FA</td>
<td>two-factor authentication</td>
</tr>
<tr>
<td>3DES</td>
<td>Triple Data Encryption Standard</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>API</td>
<td>application program interface</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
</tr>
<tr>
<td>CSRF</td>
<td>Cross-Site Request Forgery</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DH</td>
<td>Diffie-Hellman</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>ECC</td>
<td>elliptic curve crytography</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>M2M</td>
<td>machine-to-machine</td>
</tr>
<tr>
<td>OT</td>
<td>operational technology</td>
</tr>
<tr>
<td>OTA</td>
<td>Over-the-Air</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>PHI</td>
<td>personal health information</td>
</tr>
<tr>
<td>PII</td>
<td>personally identifiable information</td>
</tr>
<tr>
<td>PKI</td>
<td>public key infrastructure</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest-Shamir-Adleman</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SQLi</td>
<td>Structured Query Language Injection</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UPnP</td>
<td>Universal Plug and Play</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-Site Scripting</td>
</tr>
</tbody>
</table>