

OT Security Practitioner (810-115 OTSEC) v1.0

Exam Description: OT Security Practitioner (810-115 OTSEC) v1.0 is a 60-minute exam that validates your knowledge and skills related to the cybersecurity of industrial control systems and operational technology environments, with the ability to support OT security operations under guidance in sectors such as manufacturing, mining, utilities, and critical infrastructure. Passing this exam earns you the Cisco Certified OT Security Practitioner certification.

The following topics serve as a general guide for the exam. Please note that additional related topics may be included in any given exam version. These guidelines are subject to change at any time without notice to ensure they remain accurate and relevant.

25% 1.0 OT Security Fundamentals

- 1.1 Describe the differences between OT and IT
- 1.2 Describe cyber threats to OT environments, such as ransomware and attacks on critical infrastructure
- 1.3 Describe the Purdue Reference Model
 - 1.3.a Levels
 - 1.3.b ICS/SCADA components (PLCs, RTUs, HMIs, DCS)
- 1.4 Describe the characteristics (including use-cases) of industrial communication protocols
 - 1.4.a DNP3
 - 1.4.b EtherNet/IP
 - 1.4.c IEC 61850
 - 1.4.d MODBUS
 - 1.4.e MQTT
 - 1.4.f OPC UA
 - 1.4.g PROFINET
- 1.5 Describe the core principles of OT security frameworks
 - 1.5.a IEC 62443
 - 1.5.b NIS2
 - 1.5.c NIST CSF

25% 2.0 Secure Network Infrastructure

- 2.1 Configure secure baseline hardening on industrial switches such as Cisco Industrial Ethernet (IE) switches by disabling unused ports and services
- 2.2 Configure port security and MAC limiting on industrial switches such as Cisco IE switches to establish a secure operational baseline
- 2.3 Configure management VLANs and enforce secure access using SSH and role-based credentials on industrial switches such as Cisco IE switches

- 2.4 Configure network segmentation using VLANs and access control lists (ACLs) to separate OT levels and the OT/IT boundary
- 2.5 Describe security implications of deploying wireless services in OT
- 2.6 Describe the role and function of security devices such as firewalls and data diodes in industrial infrastructure

- 20% 3.0 Authentication and Access Control**
 - 3.1 Describe characteristics and importance of access control in industrial networks
 - 3.2 Describe controlled remote access to OT assets such as engineering workstations and HMIs
 - 3.3 Select the process to access OT assets following zero-trust principles including least-privilege access and explicit authorization based on a scenario
 - 3.4 Troubleshoot OT connectivity and access issues by verifying interface, VLAN, and ACL configurations

- 30% 4.0 Visibility and Risk Assessment**
 - 4.1 Describe characteristics and importance of an OT visibility tool
 - 4.2 Identify issues such as anomalous behavior, unauthorized devices, and protocol deviations using OT visibility tool feedback
 - 4.3 Interpret an event generated by OT visibility tools such as Cisco Cyber Vision
 - 4.4 Interpret the risk profile of an OT asset based on the output of an OT visibility tool
 - 4.5 Select the remediation option for vulnerable OT devices, weighing the risks based on a scenario