PassQueen
a.k.a dumpsqueen.com

Cisco IoT Essentials for Account Managers

Cisco 700-826

Version Demo

Total Demo Questions: 5

Total Premium Questions: 50

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which class 1 div 2 Industrial Wireless Access Point is purpose-built for hazardous environments?

A. 1552H

B. IW6300

C. IW3702

D. MR20

ANSWER: B

Explanation:

IW6300 is correct because the Cisco Catalyst IW6300 Heavy Duty Series is Cisco's purpose-built industrial wireless platform for demanding and potentially hazardous deployments, such as oil and gas, mining, manufacturing, and utility environments. The platform is designed with a ruggedized enclosure and environmental protections appropriate for industrial operations, rather than the conditions expected of conventional enterprise indoor wireless access points. Cisco specifies hazardous-location certifications for applicable IW6300 models, including Class I, Division 2 and ATEX/IECEx Zone 2 certifications. Class I, Division 2 denotes locations in which flammable gases or vapors are not normally present in ignitable concentrations but may be present under abnormal conditions. This certification enables organizations to extend secure wireless connectivity to field equipment, mobile workers, sensors, and operational-technology applications in these environments while aligning the access-point selection with site safety requirements. The IW6300 series also provides modern industrial wireless capabilities, including Wi-Fi 6, to support high-density and latency-sensitive industrial use cases. Cisco's product documentation describes the IW6300 as a heavy-duty access-point family for hazardous locations and lists its relevant certifications: Cisco Catalyst IW6300 Heavy Duty Series Data Sheet. Cisco's industrial wireless portfolio context is available at Cisco Industrial Wireless.

QUESTION NO: 2

With which products does Cisco Cyber Vision have a built-in integration?

A. FND, IND, IoT Operations Dashboard

B. ISE, Firepower, Stealthwatch

C. vManage, DNA-Center, Webex

D. Industrial Asset Vision, Umbrella, Duo

ANSWER: B

Explanation:

ISE, Firepower, Stealthwatch is correct. Cisco Cyber Vision is designed to extend industrial-network visibility and context into Cisco's broader security architecture. Its integration with Cisco Identity Services Engine enables Cyber Vision to share industrial asset and communication information that can support identity-based access controls and segmentation policies. Integration with Cisco Firepower, now generally positioned within the Cisco Secure Firewall portfolio, allows industrial context and asset intelligence to improve security-policy decisions and threat investigation. Cyber Vision also integrates with Cisco Stealthwatch, now Cisco Secure Network Analytics, to enrich network telemetry and detections with operational-technology asset context. Together, these integrations help security and operations teams identify industrial devices, understand their communications, apply appropriate access controls, and investigate threats across information-technology and operational-technology environments. Cisco's Cyber Vision product information describes its role in providing industrial visibility and sharing context with the Cisco security ecosystem; see Cisco Cyber Vision. Cisco also documents the continuing Secure Network Analytics portfolio, the current product naming for Stealthwatch, at Cisco Secure Network Analytics.

QUESTION NO: 3

A service organization needs to centrally govern remote technician sessions to industrial equipment and also prepare selected OT data for delivery to cloud applications. Which two services in Cisco IoT Operations Dashboard address these needs? (Choose two.)

A. Secure Equipment Access

B. Edge Intelligence

C. Industrial Network Director

D. Cisco Cyber Vision

E. Industrial Asset Vision

ANSWER: A B

Explanation:

Secure Equipment Access enables controlled remote access to equipment for authorized personnel and third parties, helping avoid direct exposure of industrial assets. **Edge Intelligence** collects, transforms, filters, and delivers IoT data from the edge to appropriate cloud or enterprise destinations.

Industrial Network Director manages industrial network infrastructure, while Cisco Cyber Vision provides OT asset and communication visibility. Industrial Asset Vision is an integrated sensor-to-cloud asset-monitoring solution rather than one of the two requested dashboard services.

QUESTION NO: 4

A plant security team is preparing an industrial security proposal. The customer will not accept a solution that disrupts production systems, and it needs sufficient context to isolate device groups according to operational risk. Which two outcomes should be emphasized? (Choose two.)

A. visibility into industrial assets and communications

B. policy-based segmentation of device groups

C. replacement of the existing SCADA system

D. direct public internet access to industrial controllers

E. management of all OT devices as standard office endpoints

ANSWER: A B

Explanation:

Visibility into industrial assets and communications is essential because the customer must understand the OT environment before making security changes. **Policy-based segmentation of device groups** helps reduce exposure and lateral movement while allowing the organization to separate systems according to operational requirements.

Replacing the SCADA system is outside the role of an industrial security solution. Directly exposing controllers to the public internet increases risk. Treating all OT devices as standard office endpoints ignores the availability and operational constraints of industrial environments.

QUESTION NO: 5

What are the key products in the connected factory use cases?

A. Catalyst IE 3800, Catalyst 9000, IR829

B. IE Switches, Cyber Vision, Industrial Network Director

C. IW6300, AP1572, MR210

D. CGR2010, CGR1240, IR510

ANSWER: B

Explanation:

IE Switches, Cyber Vision, Industrial Network Director is correct because these products address the fundamental networking, visibility, security, and operations requirements of a connected factory. Cisco Industrial Ethernet switches are designed for industrial environments and provide resilient connectivity between manufacturing assets, controllers, machines, and the broader enterprise network. They form the network foundation needed to collect and transport operational data reliably.

Cisco Cyber Vision adds industrial asset discovery and deep visibility into industrial control-system communications. This enables organizations to understand connected assets and network behavior, supporting segmentation, risk assessment, and the protection of operational technology environments without requiring disruptive changes to production processes. Cisco Industrial Network Director provides centralized configuration, monitoring, and lifecycle management for industrial network infrastructure, helping operations teams manage distributed industrial switching environments consistently.

Together, these capabilities support the connected-factory outcome: securely connecting production assets, gaining meaningful visibility into operational networks, and managing industrial infrastructure at scale. Cisco describes Cyber Vision's industrial visibility and security capabilities at Cisco Cyber Vision and provides Industrial Network Director product information at Cisco Industrial Network Director.