www.atmicnetworks.com

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

www.atmicnetworks.com

Question: 1

How will Roadway solutions typically start?

A. secure multi-service infrastructure

B. best in breed solutions

C. resilient industrial security

D. DMZ

Answer: A

Explanation:

In the context of roadway solutions, "secure multi-service infrastructure" typically refers to the foundational framework that integrates multiple services, such as traffic management, safety systems, and communications networks, in a secure and robust manner. This infrastructure is essential for enabling advanced roadway systems that can adapt to varying conditions and demands, ensuring efficient and safe transportation environments.

Reference:

The answer is derived from common practices and conceptual understanding within the domain of industrial and roadway infrastructure solutions, where security and multi-service capabilities are crucial.

Question: 2

In the industrial security sales play, which stakeholder is typically tasked with choosing the ICS security solution?

A. CSO

B. Field technician

C. IT

D. OT

Answer: D

Explanation:

In the industrial security sales play, the stakeholder typically tasked with choosing the Industrial Control Systems (ICS) security solution is the Operational Technology (OT) team. The OT team is directly responsible for the continuity, efficiency, and safety of the industrial processes. Their deep understanding of the operational requirements and the critical nature of the systems makes them the primary decision-makers for security solutions that impact production and operational environments.

Reference:

This conclusion is based on industry standards and roles where OT teams are primarily engaged in managing and securing operational technologies within industrial setups.

Question: 3

Which types of devices are able to be connected in an Extended Enterprise solution?

A. Data centers, desk phone

B. Webex, sensors

C. IP cameras, sorters

D. Smart meters, actuators

Answer: D

Explanation:

In an Extended Enterprise solution, the types of devices that can be connected typically include those that extend the functionality of the enterprise beyond its traditional boundaries. Smart meters and actuators are examples of such devices. Smart meters provide critical data for utility management and optimization, while actuators play a key role in automating processes and systems, both crucial for expanding the enterprise's operational capabilities into more distributed and dynamic environments.

Reference:

The answer reflects an understanding of extended enterprise architectures, where the integration of various IoT devices like smart meters and actuators supports extended operational efficiency and data-driven management.

Question: 4

Which equipment consistently needs connectivity in a port use case?

A. baggage scanning system and IP phones

B. video surveillance and conveyors

C. auxiliary power systems and crane systems

D. scanners and digital signage

Answer: B

Explanation:

In port use cases, maintaining continuous connectivity for equipment such as video surveillance and conveyors is essential. Video surveillance systems are crucial for security monitoring and safety throughout the port, while conveyors are integral to the operation of moving goods efficiently.

Consistent connectivity ensures that these systems operate without interruption, which is vital for maintaining the flow

of operations and security within the port environment.

Reference:

The answer aligns with common industrial practices in ports where the continuity of surveillance and conveyor operations are critical for daily activities.

Question: 5

What are Cisco's primary areas of focus for a connected factory?

A. Connected Factory, Connected Inventory, Factory Cloud

B. Smart Plant, Smart Security, Smart Automation

C. Connected Factory, Factory Wireless, Factory Security

D. Smart Factory, Connected Periphery, Cisco IND

Answer: C

Explanation:

Cisco's primary areas of focus for a connected factory include "Connected Factory," "Factory Wireless," and "Factory Security." These areas are designed to enhance the connectivity, flexibility, and security of manufacturing operations. The Connected Factory integrates various manufacturing devices and systems onto a common network platform. Factory Wireless enables robust and flexible wireless connectivity for mobile and fixed assets. Factory Security addresses the cybersecurity and physical security needs of manufacturing environments.

Reference:

This understanding is based on Cisco's strategic approaches to industrial IoT, focusing on enhancing connectivity, mobility, and security within manufacturing environments.

Question: 6

What is a pillar in Cisco's IoT strategy?

A. monitor the network

B. contain all threats

C. differentiate with security

D. expand IT relationships

Answer: C

Explanation:

A key pillar in Cisco's IoT strategy is to "differentiate with security." Cisco emphasizes the importance of integrating advanced security features into their IoT solutions to provide a distinct advantage over competitors. This approach not only ensures the protection of networked devices and data but also positions Cisco as a leader in secure IoT deployments. By prioritizing security, Cisco aims to address the significant concerns businesses have regarding the vulnerability of IoT systems.

Reference:

This answer reflects Cisco's strategic emphasis on enhancing the security capabilities of their IoT offerings, as outlined in their IoT and security documentation.

Question: 7

What is the primary value proposition of Cisco Cyber Vision?

A. securely run authenticated IoT applications at the edge on Cisco's IOx-hosted infrastructure

B. embedded small form factor solves size, weight, and power challenges

C. manage operations of the network of geographically distributed assets

D. discover industrial assets, protocols, and communication patterns to provide operational insights

Answer: D

Explanation:

Cisco Cyber Vision is primarily designed to offer visibility and security for industrial control systems. Its key value proposition lies in its ability to discover and monitor industrial assets, protocols, and communication patterns, providing crucial operational insights into the industrial network. This enables better security management by identifying vulnerabilities and anomalies in network behavior, thus helping maintain the integrity and efficiency of industrial operations.

Reference:

This understanding is based on Cisco's documentation for Cyber Vision, which highlights its capabilities in asset visibility and network monitoring to ensure robust security in industrial environments.

Question: 8

Which Catalyst IE switch acts as an SD-Access (SDA) Extension Policy Extended Node?

A. IE2000

B. IE3400

C. IE4010

D. IE5000

Answer: B

Explanation:

The Cisco Catalyst IE3400 Rugged Series Switches act as SD-Access Extended Nodes. These switches are part of Cisco’s Industrial Ethernet product line and are designed to support the extension of Software-Defined Access (SDA) features. This capability allows the IE3400 to integrate seamlessly with Cisco’s policy-based network architecture, providing enhanced security, automation, and simplification at the network edge in rugged environments.

Reference:

This information is supported by Cisco's official product descriptions and technical specifications that detail the role and capabilities of the IE3400 as part of Cisco’s extended enterprise networking solutions.

Question: 9

Which valuable resources has Cisco created for each of the focus industries?

A. CRD - Cisco Reference Design

B. DVD - Digital Validated Design

C. DAD - Digital Acceleration Design

D. CVD - Cisco Validated Design

Answer: D

Explanation:

Cisco has created Cisco Validated Designs (CVDs) for each of its focus industries. CVDs provide detailed architectural overviews, setup, and deployment guidelines specifically tailored to industry needs. These designs are tested and validated to ensure reliability and reduce the complexity of deployments. The resource helps customers build and manage networks based on Cisco's best practices and proven configurations.

Reference:

The answer is based on Cisco's approach to providing customers with comprehensive, tested, and validated design guides that help in simplifying and ensuring successful deployments across various industries.

Question: 10

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

A. FND, IND, loT Operations Dashboard

B. ISE, Firepower, Stealthwatch

C. vManage, DNA-Center, Webex

D. Industrial Asset Vision, Umbrella, Duo

Answer: B

Explanation:

Cisco Cyber Vision is integrated with Cisco ISE (Identity Services Engine), Cisco Firepower, and Cisco Stealthwatch. This integration enhances the security capabilities of network systems by providing extensive visibility into network activities and threats, thus allowing for better threat detection, response, and policy enforcement across an organization's network.

Reference:

This information aligns with Cisco's documentation on Cyber Vision, which highlights its integration capabilities with these security products to offer a robust defense against cyber threats in industrial environments.

Question: 11

Who is the typical buyer for Extended Enterprise Solutions?

A. CSO

B. OT

C. IT

D. Industrial Systems Integrators

Answer: C

Explanation:

The typical buyer for Extended Enterprise Solutions within organizations is often the IT department. IT professionals are responsible for ensuring the seamless integration and management of enterprise solutions that extend beyond the traditional office space into areas like remote locations, branch offices, and other off-campus environments. They handle the oversight of deploying, managing, and securing the extended network to support the organization's operational needs.

Reference:

This answer is derived from understanding the roles within organizations where IT departments are typically tasked

with overseeing and implementing technology solutions that support broader business operations, including extended enterprise environments.

Question: 12

Where are Utilities currently focused?

A. reduce OpEx, grid modernization, renewables, safety and security

B. maintain grid reliability, air gap grid connectivity, move OpEx to CapEx

C. clean coal, leverage existing assets, connected vehicle

D. reduce power coverage, Smart appliances, electric vehicle

Answer: A

Explanation:

Utilities are currently focused on reducing operational expenditures (OpEx), modernizing the grid, integrating renewable energy sources, and enhancing safety and security measures. These priorities aim to improve efficiency, sustainability, and resilience in utility operations, addressing the increasing demands for cleaner energy and more reliable service amidst growing environmental and economic

challenges.

Reference:

This understanding is based on industry trends and strategic focuses commonly observed in the utilities sector, aiming to adopt more sustainable and efficient practices while ensuring robust infrastructure security.

Question: 13

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

A. 1552H

B. IW6300

C. IW3702

D. MR20

Answer: A

Explanation:

The Cisco Aironet 1552H Outdoor Access Point is specifically designed for hazardous environments and is Class 1 Division 2 certified. This makes it suitable for areas where explosive gases, vapors, or liquids might exist under abnormal conditions, providing reliable wireless connectivity in potentially hazardous industrial settings.

Reference:

This information is detailed in Cisco's product specifications for the Aironet 1552H, highlighting its design and certification for use in hazardous locations.

Question: 14

What are the focal points for Oil and Gas opportunities?

A. gas station automation and fixing corroded pipelines

B. automation of back-office processes

C. ensure Oil and Gas exploration and midstream are connected

D. improve operations, leverage data and insights, and pervasive security

Answer: D

Explanation:

In the Oil and Gas sector, the focal points for opportunities include improving operational efficiencies, leveraging data and insights for better decision-making, and ensuring pervasive security across all operations. These priorities are crucial for optimizing production, reducing downtime, and protecting assets from increasing cyber and physical threats, thus

enhancing overall business performance and safety in the Oil and Gas industry.

Reference:

This response is derived from the strategic objectives often pursued in the Oil and Gas industry to maximize efficiency and security, which align with Cisco's solutions tailored for these sectors.

Question: 15

What does Cisco Edge Intelligence provide?

A. a dashboard for visualizing security vulnerabilities in the network

B. a holistic solution for the delivery of IoT data to multi-cloud destinations

C. the ability to configure industrial network devices quickly and easily

D. low-latency wireless backhaul for mission-critical applications

Answer: B

Explanation:

Cisco Edge Intelligence provides a holistic solution that simplifies the extraction, transformation, and delivery of data from IoT devices to various multi-cloud destinations. This platform enables organizations to effectively manage their IoT data at the edge, ensuring efficient data processing and transmission to the cloud, facilitating seamless integration with enterprise applications and analytics tools.

Reference:

This response is based on Cisco's documentation on Edge Intelligence, which describes its capabilities to streamline the flow of data from edge devices to the cloud, enhancing IoT operations and cloud integration.

Question: 16

What are Cisco's full-stack sensors, LoRaWAN gateway, and dashboard solution called?

www.atmicnetworks.com

A. Industry Monitoring Insight

B. Sensor to Cloud Stack

C. Industrial Asset Vision

D. Complete Condition Visibility

Answer: C

Explanation:

Cisco's full-stack sensors, LoRaWAN gateway, and dashboard solution are called "Industrial Asset Vision." This solution is designed to provide comprehensive monitoring and management of industrial assets through advanced sensors and connectivity technology, enabling enhanced visibility and control over industrial operations.

Reference:

This information is detailed in Cisco's offerings for industrial IoT solutions, where Industrial Asset Vision plays a key role in asset management and operational efficiency.

Question: 17

Which use case involves extending Intent-Based Networking to the Extended Enterprise?

A. parking lot connectivity

B. substation automation

C. first-response vehicles

D. oil and gas pipeline

Answer: A

Explanation:

Extending Intent-Based Networking (IBN) to the Extended Enterprise, particularly in use cases like parking lot connectivity, involves deploying advanced networking solutions that extend the intelligence and management capabilities of core networks to remote or outdoor environments. This application of IBN supports efficient connectivity and smarter management of resources in distributed locations such as parking lots.

Reference:

This answer is based on the application of Cisco's IBN technologies, which are designed to extend robust network functionalities to edge and remote locations, enhancing connectivity and control.

Question: 18

What is a key benefit of the roadways connectivity solution?

A. protected against security risks and improved productivity

B. increased operational efficiency

C. reduced costs and bridged gaps between IT and OT

D. improved driver experience and safer roads

Answer: D

Explanation:

A key benefit of the roadways connectivity solution is the improvement in driver experience and the enhancement of road safety. These solutions deploy various technologies like connected traffic systems, smart lighting, and more to provide real-time information, reduce accidents, and improve overall traffic flow, thereby significantly enhancing the safety and driving experience on the road.

Reference:

This understanding is derived from Cisco's focus on IoT solutions for smart cities and transportation, which emphasize improving public safety and user experiences through advanced connectivity and smart infrastructure.

Question: 19

What is the primary business outcome for an outdoor connectivity use case?

A. improved safety by connecting surveillance cameras

B. improved emergency services with onboard vehicle connectivity

C. improved data offloading from machines

D. improved operational efficiency via real-time process visibility

Answer: D

Explanation:

The primary business outcome for outdoor connectivity use cases, such as in industrial sites or large outdoor facilities, is improved operational efficiency achieved through real-time process visibility. By enabling connectivity in outdoor environments, organizations can monitor processes in real-time, receive timely data, and make informed decisions that optimize operations and reduce downtime.

Reference:

This conclusion is supported by the general benefits of IoT connectivity in enhancing visibility and control over operations in various industries, particularly in extensive outdoor settings.

Question: 20

Which two services are in IoT Operations Dashboard? (Choose two.)

A. Edge Intelligence

B. Cross Operational Viewer

C. Industry Monitoring Insight

D. Secure Equipment Access

E. Network Troubleshoot Tool

Answer: AD

Explanation:

In the IoT Operations Dashboard, two of the services included are Edge Intelligence and Secure Equipment Access. Edge Intelligence allows for the management and processing of data at the edge, facilitating local decision-making and reducing latency. Secure Equipment Access provides secure remote access to devices, which is critical for maintaining security while managing devices from a central location.

Reference:

These services are part of Cisco's IoT Operations Dashboard offerings, as detailed in Cisco's IoT solutions documentation, which highlights the integration of various services to manage and secure IoT deployments effectively.

Question: 21

Which feature of the warehouse connectivity solution results in significant operational cost savings?

A. placement does not require air conditioning

B. provides web server capabilities

C. helps bridge adjacent networks

D. performs data analysis

Answer: A

Explanation:

A significant operational cost saving in the warehouse connectivity solution comes from the fact that the placement of network equipment does not require air conditioning. This is particularly beneficial in large warehouse environments where the cost and logistics of cooling can be substantial. By eliminating the need for air conditioning for the network equipment, companies can significantly reduce operational expenses related to energy consumption and maintenance.

Reference:

This benefit is based on the design and deployment strategies of industrial networking equipment that are optimized for environments with minimal infrastructural support, reducing overall operational costs.

Question: 22

Which Industrial Routing device is purpose-built for remote and mobile deployments such as first responders and mass transit vehicles?

A. IG30R

B. IR1800

C. IR7200

D. IR8100

Answer: C

Explanation:

The Cisco Industrial Router 7200 (IR7200) series is purpose-built for remote and mobile deployments, making it well-suited for applications like first responders and mass transit vehicles. This device is designed to provide reliable, secure, and robust connectivity in mobile or remote settings, ensuring continuous communication and data transfer essential

for critical operations in these environments.

Reference:

The information is derived from Cisco's product literature on the IR7200, which specifies its capabilities and intended use cases, particularly emphasizing its suitability for challenging and mobile deployments.

Question: 23

Why is the Industrial Network Director (IND) a clear added value in OT applications?

A. IND can provide asset visibility for Modbus, Profinet, and Bacnet automation devices.

B. IND enables app hosting in field routers IR8XX.

C. IND improves industrial asset visibility and network troubleshooting.

D. IND can work as a universal SCADA for automation systems.

Answer: C

Explanation:

The Industrial Network Director (IND) is particularly valuable in Operational Technology (OT) applications due to its ability to improve industrial asset visibility and network troubleshooting. IND is designed to manage and monitor industrial networks, helping OT professionals gain comprehensive visibility into their network assets and streamlining the troubleshooting process. This capability enhances operational efficiency and minimizes downtime in industrial environments.

Reference:

The role of IND in enhancing network management and troubleshooting in OT environments is highlighted in Cisco's documentation and marketing materials for IND, which emphasize its benefits in industrial settings.

Question: 24

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:

In connected factory use cases, the key Cisco products include IE Switches, Cyber Vision, and the Industrial Network Director (IND). These products work together to provide robust connectivity, security, and management for industrial environments. IE Switches ensure reliable network connections in harsh factory settings, Cyber Vision offers security and visibility for industrial control systems, and IND provides centralized management and monitoring capabilities.

Reference:

This combination of products is integral to Cisco's connected factory solutions, as detailed in Cisco's industrial solutions portfolio, where they are described as essential components for achieving

comprehensive connectivity and security in manufacturing environments.

Question: 25

Which IE product is a rack mount switch?

A. E3300

B. IE3400

C. IE4000

D. IE5000

Answer: D

Explanation:

www.atmicnetworks.com

The Cisco IE5000 is a rack mount switch designed for industrial environments. This product is ideal for applications that require ruggedized switches with high-density connectivity and advanced network management features in a rack mount form factor. It is particularly suited for use in industrial, energy, and transportation sectors where rack mount equipment is often necessary.

Reference:

The specification of the IE5000 as a rack mount switch is well-documented in Cisco's product descriptions, highlighting its design and utility in industrial network setups.

Question: 26

Which products are a key component of a port or container terminal connectivity use case?

A. Catalyst 3800

B. FND

C. CGR8140

D. Cisco Ultra-Reliable Wireless Backhaul

Answer: D

Explanation:

In port or container terminal connectivity use cases, Cisco Ultra-Reliable Wireless Backhaul is a key component. This technology provides high-capacity, low-latency wireless connectivity that is essential for the real-time data transfer required in port operations. It supports the seamless movement of containers by ensuring constant communication between cranes, vehicles, and control stations, thereby enhancing operational efficiency and reducing delays.

Reference:

Cisco's solutions for ports and container terminals often emphasize the importance of reliable, highspeed wireless connections to cope with the extensive area and mobility demands typical of such environments.

Question: 27

What are the main use cases that connected roadways and intersections enable?

A. connecting both serial and ethernet field devices, and remote and mobile asset connectivity

B. connectivity for traffic signal controller, video surveillance, and digital signage

C. public safety fleet monitoring, and predictive maintenance for rail

D. alternate routing of vehicles, and counting the number of passengers on public transportation

Answer: B

Explanation:

Connected roadways and intersections primarily enable the connectivity for traffic signal controllers, video surveillance, and digital signage. These technologies are integrated to manage traffic flow more efficiently, enhance road safety, and provide real-time information to drivers and pedestrians. This integration supports smart city initiatives by improving traffic management, reducing congestion, and increasing safety and information dissemination at roadways and intersections.

Reference:

This answer reflects common smart roadway solutions that leverage connectivity to optimize traffic management and enhance public safety, as outlined in various Cisco smart city and IoT deployments.

Question: 28

Which wireless technology is ideal for a customer requiring a low cost of ownership and high control over networks and SLAs?

A. LoRaWAN

B. 5G

C. 4G

D. Cisco Ultra-Reliable Wireless Backhaul

Answer: A

Explanation:

LoRaWAN (Long Range Wide Area Network) is ideal for customers requiring a low cost of ownership and high control over networks and Service Level Agreements (SLAs). This wireless technology offers low-power, wide-area network solutions that are cost-effective and provide deep penetration in dense urban or indoor environments. It allows for long-range communications at a low power which ensures extended battery life and minimal operational costs, making it suitable for a wide range of IoT applications.

Reference:

LoRaWAN's benefits in terms of cost-effectiveness and network control are widely recognized in the IoT community, including in Cisco's IoT and networking solutions.

Question: 29

What are the two primary areas of IoT hardware investment in Oil and Gas? (Choose two.)

A. automation of back-office processes

B. scheduling for truck deliveries and maintenance

C. gas station automation

D. improve operational excellence, health, safety, and environmental control

E. cybersecurity threat prevention, detection, and response

Answer: DE

Explanation:

In the Oil and Gas sector, two primary areas of IoT hardware investment are improving operational excellence, health, safety, and environmental control (HSE), and cybersecurity threat prevention, detection, and response. Investment in IoT technologies in these areas is critical to enhance overall operational efficiencies, ensure compliance with safety and environmental regulations, and protect infrastructure from cyber threats, which are increasingly prevalent in the

industry.

Reference:

These focus areas align with industry trends where enhancing operational safety and securing critical infrastructure are prioritized to mitigate risks and improve performance in the volatile environments typical of oil and gas operations.

Question: 30

What is the primary purpose of utility substations?

A. monitor the reliable and efficient delivery of power into the distribution grid

B. FLISR: fault isolation, recovery, and service restoration

C. Volt-VAR reactive power control

D. provide physical security for the grid

Answer: A

Explanation:

The primary purpose of utility substations is to monitor and ensure the reliable and efficient delivery of power into the distribution grid. Substations play a crucial role in transforming voltage levels between high transmission voltages and lower distribution voltages, and in managing the flow of electrical power in various directions, ensuring stability and efficiency in the power supply to residential, commercial, and industrial users.

Reference:

This explanation is based on the fundamental functions of substations within electrical grids, as described in basic electrical engineering principles and utility operation standards.