Knowledge Check Quiz Related Topic Week 10 (IoT Devices)

Due Mar 27 at 11:59pm   **Points** 10   **Questions** 10
Available until Mar 27 at 11:59pm   **Time Limit** None

Instructions

Answer the following questions on the related topic material this week.

Attempt History

	Attempt	Time	Score
LATEST	**Attempt 1**	21 minutes	9 out of 10

Score for this quiz: **9** out of 10
Submitted Feb 14 at 10:27am
This attempt took 21 minutes.

Question 1   1 / 1 pts

An IoT device has at least one transducer that acts as a sensor or actuator. What is the purpose of this transducer?

○ Define a core baseline

Correct!   ◉ Interact directly with the physical world

○ Establish an authorization boundary

○ Update IoT software

Question 2

1 / 1 pts

An IoT device has at least one network interface such as a WiFi, Bluetooth, or Zigbee. What is the purpose of this network interface?

○ Characterize an enabling system

○ Provide cybersecurity

Correct! ◉ Interface with the digital world

○ Implement compensating controls

Question 3

1 / 1 pts

When should an IoT device be characterized as an enabling system?

○ Device lacks key cybersecurity requirements

Correct! ◉ Device is managed in a different authorization boundary

○ Device interferes with system reliability or resiliency

○ Device introduces privacy or safety risks for people

Question 4

0 / 1 pts

What is the term that defines high-level device cybersecurity capabilities and non-technical supporting capabilities?

○ Threat source

○ Predisposing conditions

orrect Answer   ○ IoT core baseline

ou Answered   ◉ Federal profile

Question 5   1 / 1 pts

What is the term for the things that the IoT device must posses and/or manufacturers must provide in order for the device to be integrated in the system?

○ Password-based authentication

○ Predisposing conditions

○ Likelihood of occurrence

Correct!   ◉ Key device cybersecurity requirements

Question 6   1 / 1 pts

Which considerations help an organization understand the specific use case for an IoT device?

○ Likelihood of occurrence and magnitude of impact

○ Security control mapping and profile

○ Threat source effects

Correct!

◉ Data collection, storage, and transfer

Question 7   1 / 1 pts

What is the term for a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source?

○ Profile

○ Cybersecurity

Correct!

◉ Vulnerability

○ Element

Question 8   1 / 1 pts

What is the term for characteristics of the environment, organization, or system that contribute to the likelihood that once initiated, threat events

will result in undesirable consequences or impacts?

Correct!

○ ◉ Predisposing conditions

○ Non-technical supporting capabilities

○ Device cybersecurity requirements

○ Compensating controls

Question 9   1 / 1 pts

What is the term for a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability?

○ Core baseline

○ Vulnerability disclosure

○ Capabilities catalog

Correct!

◉ Likelihood of occurrence

Question 10   1 / 1 pts

What is the term for the level of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system aviailability?

Correct!

- ⦿ Magnitude of impact

- ○ Enabling system

- ○ Authorization boundary

- ○ Non-technical capability

Quiz Score: **9** out of 10

Correct!

- ⦿ Magnitude of impact