Exercise Week 7: Supply Chain Lifecycle Vulnerabilities

Due Mar 6 at 11:59pm   **Points** 7   **Questions** 7
Available until Mar 6 at 11:59pm   **Time Limit** None

Instructions

In this exercise we will follow a hardware assembly with firmware through its lifecycle from design to disposal. At each stage, a supply chain vulnerability is described. Select the ICT SCRM security control that can mitigate this vulnerability.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	31 minutes	5 out of 7

Score for this quiz: **5** out of 7
Submitted Jan 27 at 3:14pm
This attempt took 31 minutes.

Question 1   1 / 1 pts

During design, the attacker is able to infiltrate the engineering network for the supplier to find the design documents for the hardware assembly and its firmware. The attacker alters its functionality so that it will not behave as intended in the deployed system.

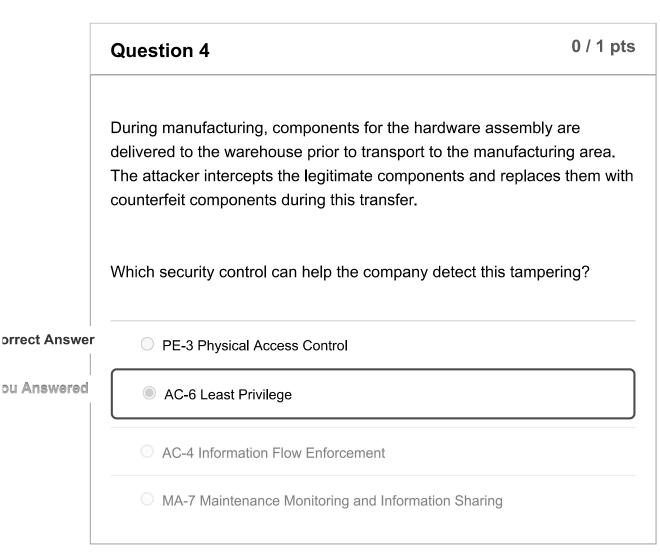Which security control can mitigate this supply chain vulnerability?

○ PE-18 Location of Information System Components

○ MA-2 Controlled Maintenance

Correct!

◉ AC-17 Remote Access

○ AC-22 Publicly Accessible Content

Question 2

1 / 1 pts

During design, an insider creates a backdoor that would allow the attacker to remotely cause the system to fail. Fortunately, the backdoor is discovered during design verification testing.

Which security control can help to identify the insider so that they can be removed from the supplier company?

○ MA-5 Maintenance Personnel

Correct!

◉ AC-2 Account Management

○ AC-19 Access Control for Mobile Devices

○ PE-17 Alternative Work Site

Question 3

0 / 1 pts

During preparations for manufacturing, the attacker inserts malware into the fixture that will be used to install the firmware.

Which security control can mitigate this supply chain vulnerability?

○ AC-21 Collaboration and Information Sharing

○ AC-5 Separation of Duties

○ MA-3 Maintenance Tools

◉ PE-2 Physical Access Control

Question 4

0 / 1 pts

During manufacturing, components for the hardware assembly are delivered to the warehouse prior to transport to the manufacturing area. The attacker intercepts the legitimate components and replaces them with counterfeit components during this transfer.

Which security control can help the company detect this tampering?

○ PE-3 Physical Access Control

◉ AC-6 Least Privilege

○ AC-4 Information Flow Enforcement

○ MA-7 Maintenance Monitoring and Information Sharing

Question 5

1 / 1 pts

During preparations for system deployment, the end user orders spare parts. The attacker advertises a spare part that is less expensive than the original manufacturer with faster delivery. The attacker's part has faulty logic that will disrupt the system behavior during operation.

Which security control can mitigate this supply chain vulnerability?

○ PE-20 Asset Monitoring and Tracking

○ AC-18 Wireless Access

○ AC-3 Access Enforcement

Correct!

◉ MA-6 Timely Maintenance

Question 6   1 / 1 pts

During sustainment, the attacker poses as part of the repair crew in the depot. When no one is looking, the attacker replaces the hardware assembly with a compromised assembly that contains malware in the firmware.

Which security control can mitigate this supply chain vulnerability?

Correct!

◉ PE-6 Monitoring Physical Access

○ AC-24 Access Control Decisions

○ MA-4 Nonlocal Maintenance

Question 7

1 / 1 pts

During sustainment, the failed hardware assembly is replaced during a repair operation and the failed unit is discarded. The attacker retrieves the discarded hardware assembly. Even though the failed unit is broken, there is significant information on the working part of the assembly that is valuable to the attacker to design future attacks.

Which security control can mitigate this supply chain vulnerability?

Correct!

⦿ PE-16 Delivery and Removal

○ AC-1 Access Control Policy and Procedures

○ MA-1 System Maintenance Policy and Procedures

○ AC-6 Least Privilege

Quiz Score: **5** out of 7