Knowledge Check Quiz Case Study Week 4 (Natanz)

Due Feb 13 at 11:59pm **Points** 15 **Questions** 15
Available until Feb 13 at 11:59pm **Time Limit** None

Instructions

Answer the following questions on the case study material this week.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	23 minutes	15 out of 15

Score for this quiz: **15** out of 15
Submitted Jan 21 at 1:44pm
This attempt took 23 minutes.

Question 1

1 / 1 pts

What was the **target of the attack**?

Correct!

● Fuel Enrichment Plant

○ Power Grid

○ Bank

○ Water Services

Question 2

1 / 1 pts

Where did the attack occur?

○ Estonia

Correct! ● Iran

○ Australia

○ Ukraine

Question 3

1 / 1 pts

When was the attack **discovered**?

Correct! ● June 2010

○ April 2014

○ December 2015

○ April 2000

Question 4

1 / 1 pts

What was the **duration** of this attack?

○ Months

○ Days

Correct! ● Years

○ Weeks

Question 5

1 / 1 pts

What was the **impact** from the attack?

○ Credit card information stolen

Correct!

● Centrifuges were damaged

○ Widespread power outages

○ Raw sewage was spilled

Question 6

1 / 1 pts

What makes this case study **significant**?

○ Supply chain attack on industrial control systems

○ Denial of service attack on critical infrastructure

Correct!

● Cyber physical attack

○ Insider attack on industrial control systems

Question 7

1 / 1 pts

How did the attack occur?

○ Hackers stole credentials from HVAC vendor

○ Phishing campaign to gain credentials

Correct!

● Malware introduced to manipulate control systems to damage equipment

○ Distributed denial of service attack on government websites

Question 8

1 / 1 pts

What **technical concerns** contributed to this incident?

Correct!

● Malware designed to impose damage

○ Adobe Flash vulnerability used to inject malicious code

○ SCADA system insecure

○ PING flood and botnets

Question 9

1 / 1 pts

What **human behavior** contributed to this incident?

Correct!

● Contractor USB sticks used to install malware

○ Security team ignored warnings from anti-intrusion system

○ Disgruntled employee sabotaged operations

○ Employees open attachment on phishing email

Question 10

1 / 1 pts

What **business decisions** contributed to this incident?

○ Old versions of Office and Windows

○ Server did not receive two-factor authentication update

Correct! ● Contractors allowed access to networks

○ Security patch not installed

Question 11

1 / 1 pts

Which **malware** was used in the attack?

○ Poison Ivy

Correct! ● Stuxnet

○ Black Energy

○ Black POS

Question 12

1 / 1 pts

Which **2 attack routines** were used to **manipulate the centrifuge rotors**?

○ Cascade Protection System and fieldbus

○ SCADA and Step7

Correct! ● Over-pressure and over-speed

○ Product and tails

Question 13

1 / 1 pts

Which layer of a cyber-physical attack spreads the **malware**?

Correct! ● Information Technology

○ Communications

○ Physical

○ Industrial Control System

Question 14

1 / 1 pts

What was the **goal** of the Natanz cyber attack?

○ Zero-day attack on the uranium enrichment servers

○ Destroy more centrifuges than were available for replacement

Correct! ● Damage that would appear as a reliability issue

○ Catastrophic failure in the Cascade Protection System

Question 15

1 / 1 pts

What is a **fieldbus**?

○ Computer that is used to configure the industrial controllers

○ Category of computer programs used to display and analyze process conditions

○ Signals that are passed between peripherals and program logic by attack code

Correct! ● Realtime micro-network for connecting automation peripherals

Quiz Score: **15** out of 15