Exam

ITI42220-1 23V Security in Information Systems and Software Engineering

**Question 1 (10 points)**

Give a short description of:

1. What is Operational Technology (OT)?
2. What is Information Technology (IT)?
3. 3 differences between OT security and IT security?

**Question 2 (20 points)**

You are the security advisor of a large hydropower plant company. The company uses a legacy OT system that is 15 years old, and you know that it has several vulnerabilities and is not secure. Your company performs maintenance once in a year during summer, where production is stopped for 2 weeks. If planned for, patching is normally performed during this maintenance period.

You have the following risk response options to improve the security posture of the system.

Option 1: Apply available patches on a test system, and plan for patching the operational system during the next maintenance cycle.

Option 2: Strengthen monitoring, intrusion detection and logging capabilities around the system.

Option 3: Replace the legacy system with a new/modern system.

Option 4: Immediately shutdown the system and the production until patching is done.

Elaborate in short, in what order you will prioritise the options above. Give rationale for your choice. Feel free to make any assumptions to come to your decisions but do write your assumptions in the answer.

**Question 3 (20 points)**

In DevSecOps paradigm, security is a shared responsibility of development, operations, and security teams. Explain from the security team perspective, in what way you can support development and operation teams during the DevSecOps process.

Give 1 example of an activity/task you will perform or support during 4 different stages (e.g., code, build, as shown in the figure below). Limit yourself to one short paragraph per stage.

 

**Question 4 (50 points)**

Halden Battery Plant (HBP) develops and produces electric vehicle batteries. HBP has major car companies as its clients - Audi, Jaguar, and Porsche. HBP’s battery technology is highly advanced and energy efficient when compared to its competitors. Continuous operation of the plant is business critical for HBP, as disruption in production can result in loss of 1 million kroners per day. The plant is also safety critical, as release of chemicals could lead to harm to people and environment.

The production process consists of 3 stages as below.

1. raw materials necessary for making batteries are mixed and processed;
2. battery cells are manufactured;
3. battery cells are packaged and stored.

**Raw materials processing**

**Battery packaging & storage**

**Battery cell manufacturing**

Battery production is a complex process. The quality of the batteries produced depends on precise handling of raw materials (quantities of materials, mixing duration, etc.) and precise manufacturing of battery cells (electrode fabrication, cell sealing, etc). Any deviations within the process will lead to manufacturing poor quality batteries and will be rejected during quality inspections.

(Question continues on the next page)

The industrial control system used for monitoring and controlling the plant processes is supplied by a company called ElectroX. The control system consists of several components – e.g., PLC, sensors, actuators, HMI – from different vendors such as Siemens and ABB.

You are the security manager of HBP and have been asked to perform a risk assessment of the plant and elicit security requirements. You are going to apply NIST 800-30 based risk assessment.

Identify 4 threats and assess their risks. Identify 1 security requirement for each threat.

You can document your results in the following format, or in any format of your preference.

|  |
| --- |
| **ID:** <number 1 to 4> |
| **Threat source:** <your text> |
| **Threat event:** <your text> |
| **Vulnerability:** <your text> |
| **Impact:** <your text> |
| **Likelihood:** <your text> **Severity:** <your text> **Risk:** <your text> |
| **Security requirement:** <your text> |
| **Assumptions (if any):** <your text> |

Use the risk table below for classifying likelihood, severity, and risk.

