Building Cyber Resilience in Operational Technology

Introduction

Many industries in Africa rely on Operational Technology (OT) to run physical systems such as manufacturing plants, energy systems, transportation networks, and water treatment facilities. Unlike traditional IT systems, OT environments control real-world processes, meaning that cyberattacks can cause physical disruption, safety risks, and economic damage.

Recent global incidents such as SolarWinds, Colonial Pipeline, and NotPetya have shown that cyber threats can spread through trusted software updates, third-party suppliers, and poorly protected networks. These attacks demonstrate that cybersecurity must focus not only on protecting data but also on ensuring operational resilience and business continuity.

Tasks and Objectives

You are working with a large industrial company that operates several production facilities across Africa. The company depends on many vendors, software providers, and equipment suppliers to keep its systems running.

Your task is to help them strengthen their cyber resilience and protect their operational technology systems from cyber risks.

4 Key Questions to Consider:

- How can companies identify cyber risks in their OT environment before they cause disruptions?
- What security practices should suppliers and technology partners follow to reduce risk?
- How can organizations protect both IT and OT systems without disrupting operations?
- What should companies do if a cyberattack shuts down critical systems?

Key Tasks

Your 3-minute video proposal must cover the following:

Create a Cyber Resilience Plan to help the company protect its operational technology and maintain business continuity. Your plan should include:

1. Risk Identification

Explain how the company can identify cyber risks in its OT environment and supply chain.

Examples may include:

- Vendor risk assessments
- Network vulnerability scanning
- Monitoring for unusual system activity

2. Security Requirements

Define basic cybersecurity requirements that suppliers and partners must follow.

Examples may include:

- Secure software updates.
- Access control and authentication.
- Patch management.
- Security certifications or compliance standards

3. Monitoring and Protection

Describe how the company can continuously monitor its systems and vendors to detect threats early.

Examples may include:

- Network monitoring tools
- Incident reporting procedures
- Regular security reviews for suppliers

4. Incident Response and Recovery

Explain what the company should do if a cyberattack disrupts operations.

Your response plan should include:

- Immediate response actions
- Communication procedures
- System recovery and backup strategies
- Steps to prevent the attack from happening again

Final Requirement

Your plan should be simple, practical, and realistic, helping the company protect its systems while ensuring that operations remain safe and uninterrupted.

April 7th, 12:00PM CET/SAST is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

DataGr8 is a South African-based company providing comprehensive cybersecurity and compliance solutions to customers across Africa. Founded in 2009, their journey began with compliance email and data archiving services, soon expanding to include data migrations. As technology and threats evolved, so did DataGr8. Today, DataGr8 stands at the forefront of the cybersecurity industry, dedicated to safeguarding their clients' data and ensuring compliance with regulatory standards. DataGr8's innovative solutions encompass cloud backup, managed detection and response, vulnerability management, cyber awareness training, and email and domain security. By aligning cutting-edge cybersecurity solutions with clients' business objectives, DataGr8 enhances overall security posture and protects data in an ever-changing threat landscape. At DataGr8, they are committed to excellence, continuous improvement, and fostering long-term partnerships to meet the diverse and evolving needs of their clients.