BUREAU VERITAS 1828

Secura
A BUREAU VERITAS COMPANY

OT Perimeter Assessment

Boundaries between Information Technology (IT) and Operational Technology (OT) are fading. Protecting the link between IT and OT networks is now crucial to secure the OT attack surface. The OT Perimeter Assessment can help you keep your OT systems secure.

The OT Perimeter Assessment gives you:

Insight into threats

You gain insight into potential cyber attack entry points and into vulnerabilities.

Actions you can take

You receive concrete recommendations , so that you can protect your systems.

Advice from OT specialists

OT security requires expertise: you can rely on our OT security specialists to help you.

Why choose the OT Perimeter Assessment?

IT and OT networks are increasingly linked - for automation, efficiency, and instant data analysis. This IT/OT convergence is a result of Industry 4.0, the fourth revolution in industrial manufacturing. It makes your systems more vulnerable to cyber attacks - particularly if they are also connected to the internet and the cloud. The **OT Perimeter Assessment** checks these three things: your OT-network design, the flow of data traffic and vulnerabilities in the network. We focus on systems in the IT and OT networks that need to communicate with each other. This includes IT systems that interact with dual-homed IT/OT systems or cross the Demilitarized Zone (DMZ). The OT Perimeter Assessment is an excellent place to start with OT security. The results of this assessment can give you an idea of potential next steps to take.

How the OT Perimeter Assessment works

Each OT Perimeter Assessment consists of 3 main elements.

Understanding the network design

Analyzing firewall configuration

Scanning for vulnerabilities

1. Understanding the network design

After studying drawings, asset registers and technical info, we draw up a network diagram. Your experts and ours then review this, to pinpoint all possible entry points, including remote UPS management, physical access controls, or HVAC and BMS (building management system). Your IT and OT experts are also involved in a high-level Threat Modeling session, to map potential threats.

2. Analyzing the firewall configuration

The traffic between your IT and OT is probably filtered by one or more firewalls or other boundary protection devices. We analyze the firewall settings thoroughly. The goal is to:

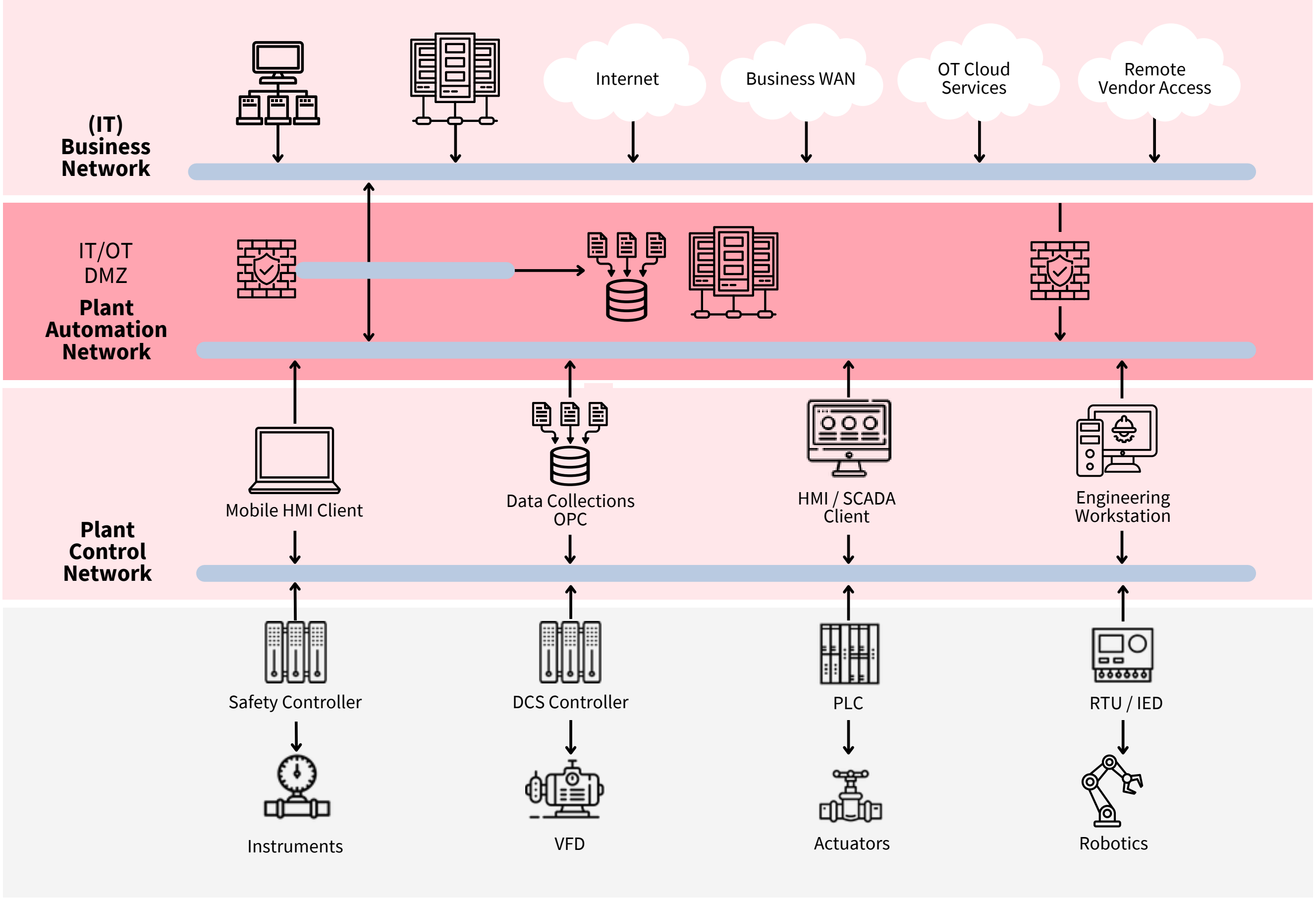
- Verify that only the minimum amount of required traffic is allowed through and all other traffic is denied.
- Verify that allowed traffic only flows between authorized endpoints.
- Correlate the allowed traffic to the security configurations of the endpoints.

3. Scanning for vulnerabilities

Based on the analyzed network diagrams and firewall configuration, you can expect additional OT network scans to get a more in depth insight into the actual network traffic. We use two different techniques:

Passive scanning. This is a “read-only” technique that uses a copy of already existing network traffic. method can expose vulnerabilities like weak protocols, poor configuration or outdated firmware.

Active scanning. These queries are tailored to a single host or a selected part of the network. This way we can discover weak or unencrypted protocols, weak or unsecure software applications or services, unknown IT/OT communication flows, unknown systems or poorly configured systems and known security vulnerabilities (CVEs).



This graphic shows the focus of the assessment. The main focus, in red, is the perimeter between IT and OT. However, we also check relevant parts of the OT or IT systems, shown in pink.

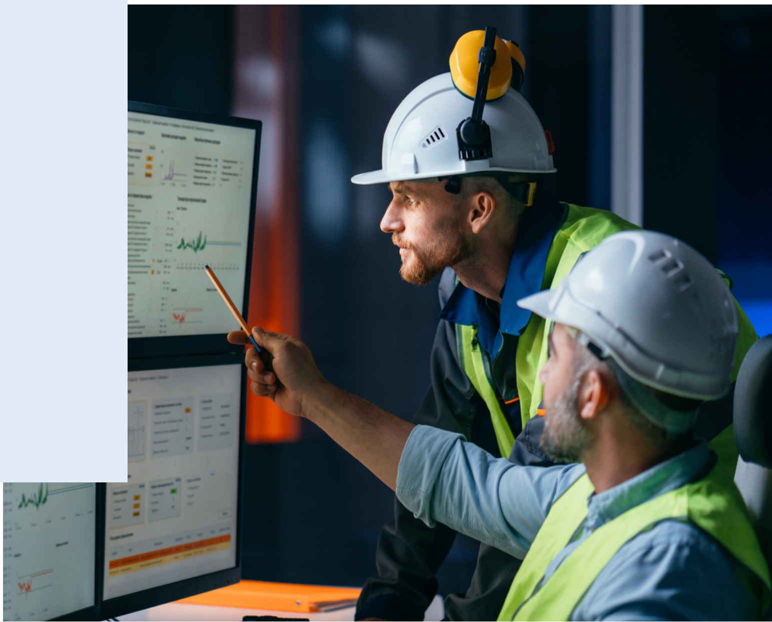
Taking action

All the findings from these three steps are then combined and analyzed. The result is a report with actionable points of improvement, so you can take direct action.

What our customers say

"This was a real eye opener"

> *"We have only just gotten started with our security. The OT Perimeter Assessment showed us how many misconfigurations there actually were in our network. This was a real eye opener for us."*



Related Services

NIS2 Services

Chances are high that your company is covered by the European NIS2 directive. We offer Gap Assessments and Implementation Support to help you reach full NIS2 compliance.

OT Site Assessment

The OT Site Assessment involves site visits, system architecture reviews, and expert consultations to identify and address security weaknesses. With this assessment you can optimize your OT security.

Industrial pentesting

Vulnerability assessments and penetration testing are ways to discover weak spots in the security of your OT systems. We have specialized OT pentesters that can help you with this.

Secura
A BUREAU VERITAS COMPANY

About Secura / Bureau Veritas

Secura is a leading cybersecurity company. We help customers all over Europe to raise their cyber resilience. Our customers range from government and healthcare to finance and industry. We offer technical services, such as vulnerability assessments, penetration testing and red teaming, but also provide audits, forensic services and awareness training.

Secura is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80.000 employees and is active in 140 countries.

Example case | OT Perimeter Assessment

Which problem did the customer have?

A large manufacturer with multiple global facilities wanted to know for each of their facilities how secure the boundaries were between IT and OT. They lacked company wide policies for their OT security.

Result

During the OT Perimeter Assessment we found multiple issues. For instance, we found that if an attacker had gained access to one facility, they were able to reach other facilities. Because we had tested all facilities we were able to help this customer prioritize the risks and advise them on improvement.

BUREAU VERITAS 1828

Interested?

Contact us today to start raising your cyber resilience.

info@secura.com

+31 (0) 88 888 3100

secura.com