8. Impact Assessment and Countermeasure Execution Support Technology

NEC corporation

Automatic risk assessment without operator's security knowledge. Provide countermeasure plans based on attack simulations automatically.

Application Area

Semiconductor / Packaging | IoT | ICT vendor
Manufacturer | Infrastructure | Distribution
Local Government | Building / Smart City

Technology Features

■ Automatic risk assessment using attack simulations

Analyze both system impacts and affected devices automatically in case of a cyber-attack. Translate risk assessment results into a guideline format* and support operators to deal with the guideline. *)IPA "Security risk analysis guide for control systems"

■ Provide countermeasure plans against the cyber attack

Evaluate countermeasure plans using attack simulations automatically and support operator to execute them.

Effects

■ Perform the risk assessment in a short time without security knowledge

Operators can evaluate cyber-attacks and effective countermeasures for their system without security knowledge by using attack simulations. It can decrease the evaluation time as 1/4.

■ Perform the risk assessment easily that is recommended by security guideline

Automatic risk assessment can be performed with input device list, device information and network configurations (*for high accuracy, additional information is required)

Use case

Target

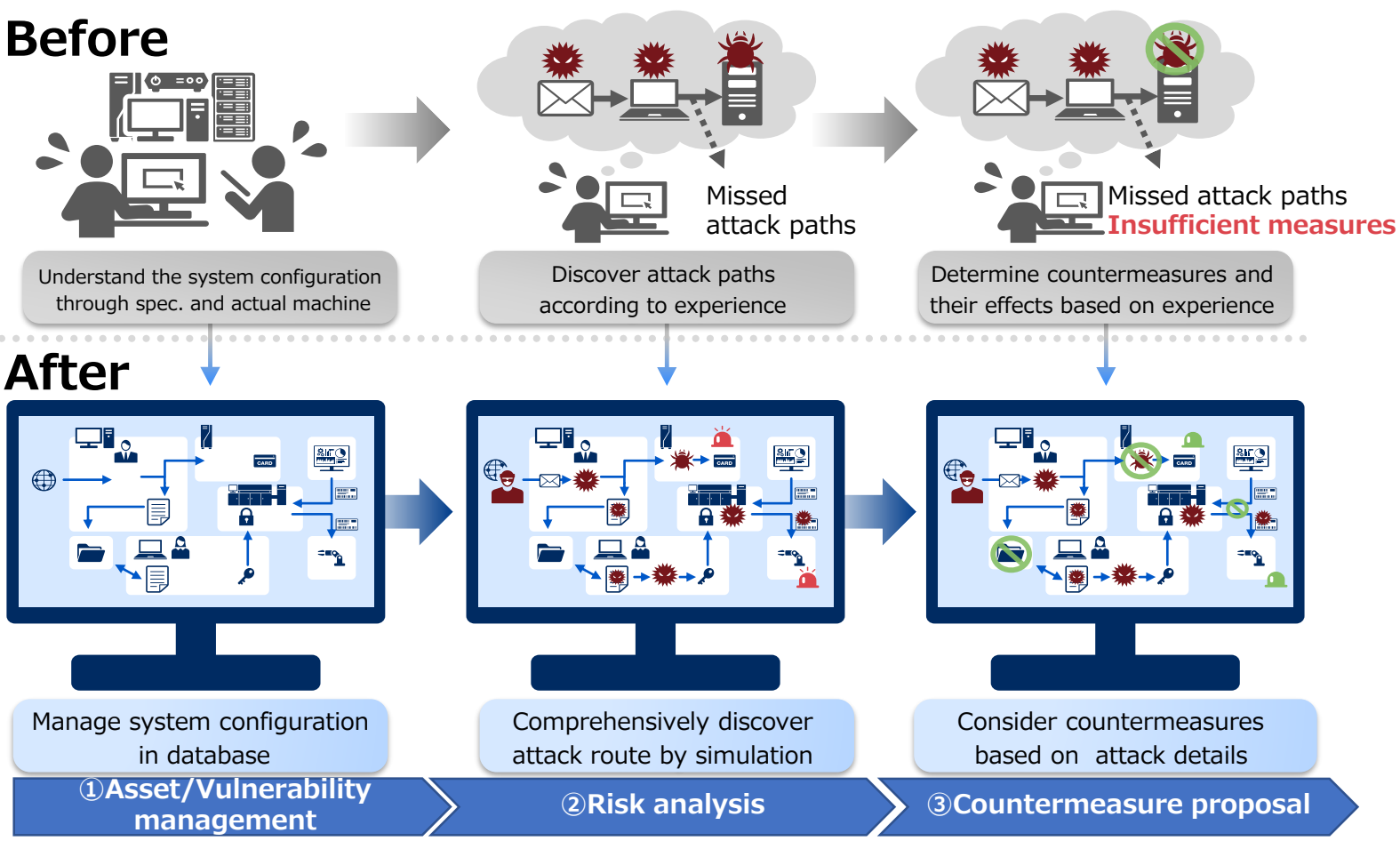
IoT systems of manufacturing (plants), distribution, smart building and so on.

Use case

Risk assessment, Perform risk assessment on a daily basis and countermeasures

Required info.

OS info., Installed software, IP address

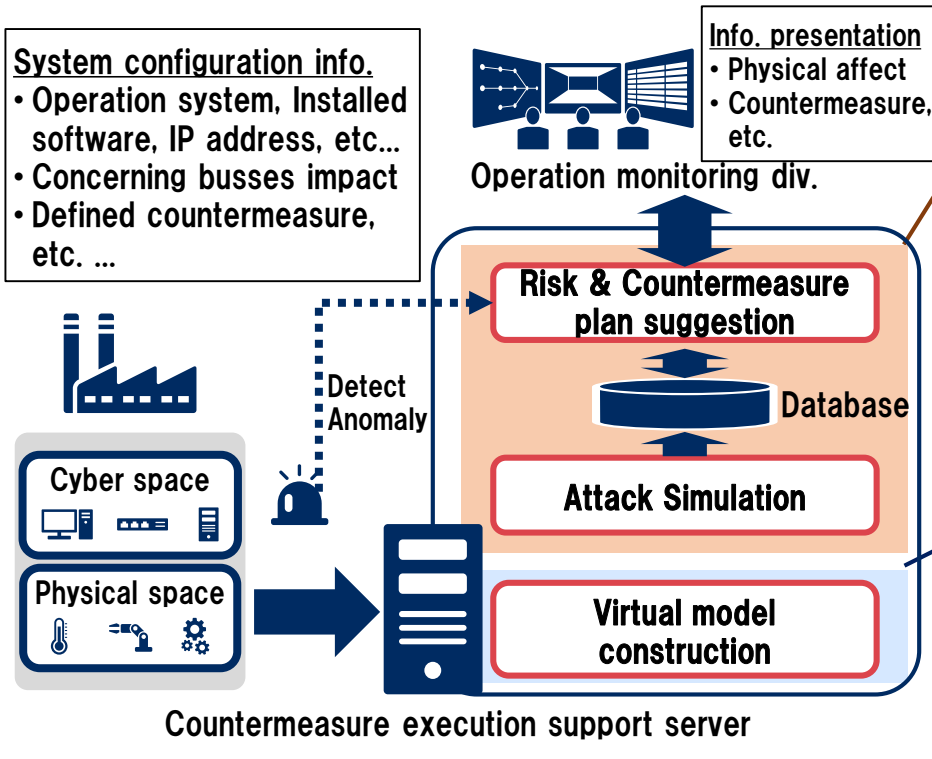


8. Impact Assessment and Countermeasure Execution Support Technology

NEC corporation

Technology Description

Overview of R&D Technologies



■ **Countermeasure execution support technology**

Perform attack simulations and evaluate effectiveness of countermeasure plans on the virtual model. When an anomaly is detected, the technology suggests applicable countermeasure from evaluated plans.

■ **Virtual model construction technology**

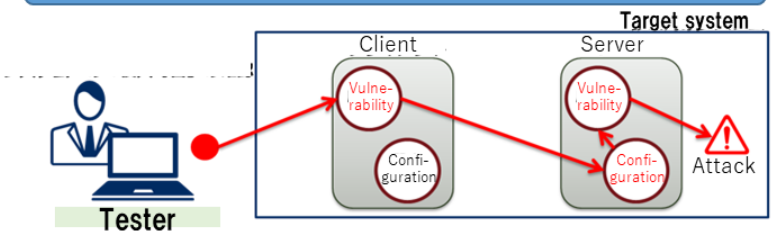
Create the model which is used to analyze cyber-attack risk without using actual systems.

Problems to be solved

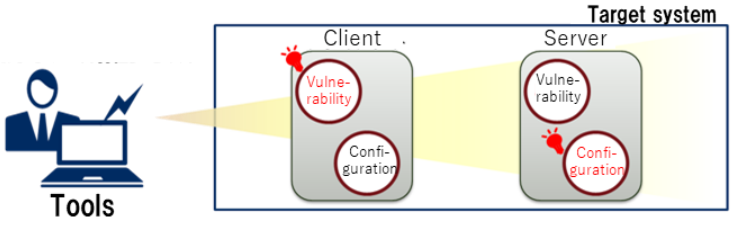
■ **Guidelines recommends risk assessment for considering countermeasures**

It is difficult to perform risk assessment because there are hundreds to thousands of equipment

Manual assessment requires a lot of time



Existing tools do not show system damage



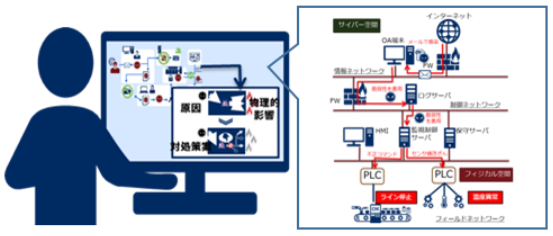
Support for large-scale environment

Easy to understand damage

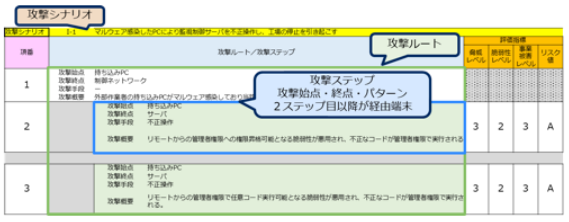
■ **Our technology supports risk assessment and reduces it's cost**

Supports thousands of units to make it adaptable to any environment

Large-scale attack simulations



Reports according to guidelines



Contact

NEC Corporation
Email: nec-sip2-ac2@secl.jp.nec.com