Power and Water Cybersecurity Suite – Rogue System Detection[1]

Features

- Detects and remediates rogue systems through Trellix ePolicy Orchestrator®
- Provides full visibility of all assets on the network
- Converts identified rogue systems into managed clients

Overview

All network-integrated devices must be identified as network assets so they can be properly monitored and controlled. Unprotected or rogue systems are often a weakness within security strategies, creating entry points that viruses and other potentially harmful programs can use to access a network.

Networks are connecting to an increased number of devices or systems, collectively known as the Internet of Things (IoT). Most IoT devices or systems have limited processing and memory to support security management agents; therefore, only a small fraction of IoT components are managed. Those outside of security management tools are considered “rouge.”

Security software focuses on assets that are known and permitted within the network environment. Often, they are not designed to detect and control network-connected rogue systems or devices.

Consequently, rogue systems pose a unique threat to organizations by presenting vulnerabilities and allowing sensitive data to be exposed or stolen. Since rogue devices are external to the security management framework, they are not part of any standards, policies, security controls, or patch updates. Unmanaged assets are vulnerable to attack, not only to the specific system but to other systems on the network. Furthermore, unprotected systems that join the network can also create compliance issues.

Attackers can use the assets’ legitimate data and access rights to extract sensitive information or to distribute malware. Rogue systems that are detected on the network can indicate physical malicious activity within the corporate network and can create unprotected wireless access points that bypass firewalls.

Security risks increase as more undetected and unmanaged systems or devices are connected to a network.

Solution

The Power and Water Cybersecurity Suite Rogue System Detection application provides near real-time discovery of rogue systems by using sensors installed throughout a network. The sensors employ passive discovery techniques to detect network-connected systems. New systems identified by the sensors are checked by the dashboard for installed active agents. If the detected system is unknown to the server, the Rogue System Detection application provides information to the dashboard for immediate action. Remediation steps include alerting administrators to deploy an agent to the rogue system for conversion into a managed system. The Rogue System Detection application is included in the PWCS Trellix dashboard application.

Dashboard

The Rogue System Detection application provides expanded reporting and monitoring capabilities through a dashboard powered by Trellix ePolicy Orchestrator (ePO). An overall system status monitor shows the system's condition as a percentage of compliant systems. Systems are separated into the following categories:

- **Exceptions** – Systems that do not need an agent, including routers and printers, as well as those systems that do not need to be monitored and reported anymore. A system can be marked as an exception only when it does not represent a vulnerability in the environment.
- **Inactive** – Systems that have gone dormant for a certain time and are considered inactive. These are systems that are likely shut down or disconnected from the network such as a laptop, retired system, or another device.
- **Managed** – Managed systems have an active Trellix agent that has communicated with the Trellix ePO server in a specified time.

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-002-5.1a R3	Bulk Electric System Cyber System Categorization	Identifies network present assets.
CIP-005-7 R1.1	Electronic security perimeter	Electronic security perimeter (R1.1)