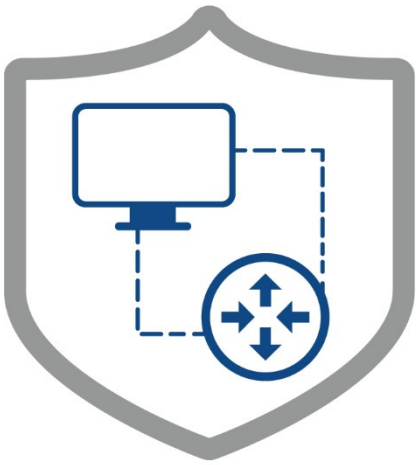
Power and Water Cybersecurity Suite – Network Intrusion Detection

Features

- Detects sophisticated network intrusion attempts
- Monitors data traffic through routers on the electronic security perimeter
- Provides deep-packet inspection capabilities
- Displays current system status on dashboard
- Optionally aggregates data in the security incident & event management module for further analysis and correlation



Overview

Direct attacks on control systems from malicious software can originate from networks as well as endpoints. Additional techniques that work in conjunction with firewalls and malware prevention applications need to be deployed for effective protection against possible network attacks originating from outside the control system and for system misuse or attacks originating from inside the control system.

Network-based intrusion detection identifies unauthorized, illicit and anomalous behavior based solely on network traffic. A detection system collects packets that traverse a given network and flag any suspicious traffic.

Network intrusion detection systems gather, identify, log and alert users of potentially harmful incidents. A few of the most commonly detected network events include protocol-based reconnaissance and attacks, unexpected application services or policy violations.

In a trusted environment, such as distributed control systems, perimeter control takes precedence over inner network control. While both can be monitored, data traffic across the electronic security perimeter is considered more vulnerable than the data contained within the perimeter.

Solution

Network intrusion detection is a Power and Water Cybersecurity Suite module and appliance that protects against network attacks. The module employs best practices by using routers to connect the control system to the enterprise LAN and field devices. This deployment provides both network isolation and access control. Only authorized sources or destination IP addresses can communicate with the designated nodes.

The network intrusion detection module inspects communication contents between the control system and outside devices through intelligent packet-filtering and policy-based discovery capabilities. Each communication packet is analyzed to determine the presence of malicious entries that could result in a denial-of-service.

The module's event database aggregates and correlates intrusion, discovery, connection and performance data. It also provides device, license and policy management as well as notifications (or alerts) and custom template-based reporting.

Intrusion events can be optionally forwarded to the Power and Water Cybersecurity Suite's security incident & event management module for further analysis.

Typical deployment of the network intrusion detection module includes a virtualized management console and a hardware appliance which is typically located in the Power and Water Cybersecurity Suite's cabinet.

The hardware appliance provides a physical connection to control system's routers. Additional hardware appliances can be added when the number of targeted networks exceeds eight. Data collected from all networks is aggregated in the virtualized portion of the module.

Operation

The Power and Water Cybersecurity Suite's network intrusion detection dashboard provides current system status information including data regarding generated system events. The dashboard also shows the status and overall health of deployed applications. The dashboard includes the following network intrusion detection functions:

- **Overview:** Shows important network intrusion data used for generating reports and graphs
- **Analysis:** Drills down to the context explorer level for gaining insight to or searching for connection data and for viewing data on intrusion events, hosts, vulnerabilities and correlation
- **Policies:** Enables rule configuration for access control to managed devices, policies for intrusions, correlations, network-based malware detections and actions for remediation.
- **Devices:** Configures the physical appliances within the intrusion detection system that are connected to and monitoring the network
- **Objects:** Creates and manages objects with IP addresses, networks, ports, VLAN tags, URLs application lists, file lists and security zones. These objects are used in other parts of the network intrusion detection system such as policies, rules, searches, reports, or dashboards. All objects can be grouped for convenience.

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-005-5 R1 Part 1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications	Both inbound and outbound communication traffics are closely inspected
CIP-007-6 R3 Part 3.1	Deploy method(s) to deter, detect or prevent malicious code	Deep packet inspection can detect malicious code in packets across the electronic security perimeter

EMERSON