

Meet the Intrusion Detection Systems: A Growing Family that is Protecting Critical Infrastructure

Authors:

Anis Bishara, Application Engineer (U.S)

Gil Kroyzer, Founder & CEO

Today's cybercriminals are more organized and more sophisticated than ever before. With every passing day, we are learning of new variants of cyber-attacks that are capable of bypassing traditional security defenses. According to published information, over 50% of such attacks target the Energy Sector, with the number and severity of attacks growing as they are financed by hostile countries, crime organizations or commercial entities.

In the energy sector, the main target for such attacks is the Supervisory Control and Data Acquisition (SCADA) system. A successful infiltration of a SCADA can allow the cyber attacker to gain control of the physical processes of a power plant, which can have a wide variety of consequences. An attack can be subtle, stealing information or performing minor changes in process logic that degrades efficiency and thus has an impactful cost over time. Alternatively, an attack can be direct, controlling equipment with malicious intent and leading to physical damage and a process shutdown.

For example, when an ex-employee of the company that installed radio-controlled sewage equipment for the Maroochy Shire council in Australia accessed the sewage control system via wireless connection and issued false commands, it caused 800,000 liters of sewage to spill into local parks and rivers. The Estimated cost of this cyber-attack is \$1 Million.

Many solutions exist that prevent such intrusions of the OT network. From Firewalls to Demilitarized Zones (DMZs) to Diodes, the principle idea is to create an impenetrable virtual wall that prevents all undesired access from the external world. Unfortunately, no single solution provides absolute protection. Furthermore, to rely exclusively on such protection means one is completely vulnerable once access is obtained. To make matters worse, one may not be aware of the intrusion.

Therein lies the value of an Intrusion Detection Systems (IDS). It does not exist to prevent an intrusion, but to raise a flag when it occurs. An IDS operates by monitoring the organization's various computer systems and identifying anything out of the ordinary, whether through white/black-listing or anomaly detection mechanisms. It is commonly accepted to group Intrusion Detection Systems into one of two categories: Network-based (NIDS) and Host-based (HIDS).

NIDS are typically Firewalls or Passive Probes that are connected to the network at specific locations to allow the monitoring and inspection of network traffic, and content analysis of individual packets that traverse the network. Conversely, HIDS are typically software-based solutions installed on hosts that analyze the host itself and any inbound and outbound network traffic on the host. While the location of these systems is different, they both operate from an IT perspective with a technical understanding of the communication protocols of the OT world.

More recently, a third category is now emerging: Industrial Intrusion Detection Systems (IIDS). This category is fundamentally different from the others in that it operates through an OT perspective. This approach does not rely on the IT definition of suspicious network traffic, but rather observes whether the plant is operating as expected. This is done through a software-based big-data analysis mechanism that connects directly to the SCADA system and looks for anomalies in the process behavior.

An IIDS can also operate in conjunction with NIDS providing anomaly detection for the plant's physical process and for the plant's network traffic. This is known as XIDS (Cross-platform Intrusion Detection System).

With the growing cyber-threat on critical infrastructures, security teams are realizing that they not only require IDS solutions for their IT systems such as NIDS and HIDS, but also solutions for their OT systems such as IIDS and XIDS.