Life Is On | Schneider Electric

Enhancing Cyber Security in Industrial Control Systems and Critical Infrastructure with Dynamic Endpoint Modeling

by Daniel Paillet

Executive summary

Cyber attacks against Industrial Control Systems (ICS) are on the rise, putting nations' critical infrastructure at risk. In a paradigm shift from the traditional network security systems, a new approach — Dynamic Endpoint Modeling — learns and models the behavior of all devices on the network and triggers alerts when algorithms detect changes in learned behavior.

Introduction

As the barriers between Information Technology (IT) and Operations Technology (OT) disappear, Industrial Control Systems (ICS) environments are increasingly exposed to cyber attacks. The U.S. Department of Homeland Security's ICS Cyber Emergency Response Team noted a 20% increase in ICS-related attacks in 2015, across a wide range of industry sectors. See **Figure 1.** As supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control systems become connected to the Internet to allow greater business efficiency (remote process monitoring, system maintenance, process control and production data analysis), they also make the business more vulnerable to threats. with the potential to seriously affect a nation's critical ICS and power infrastructure.[1]

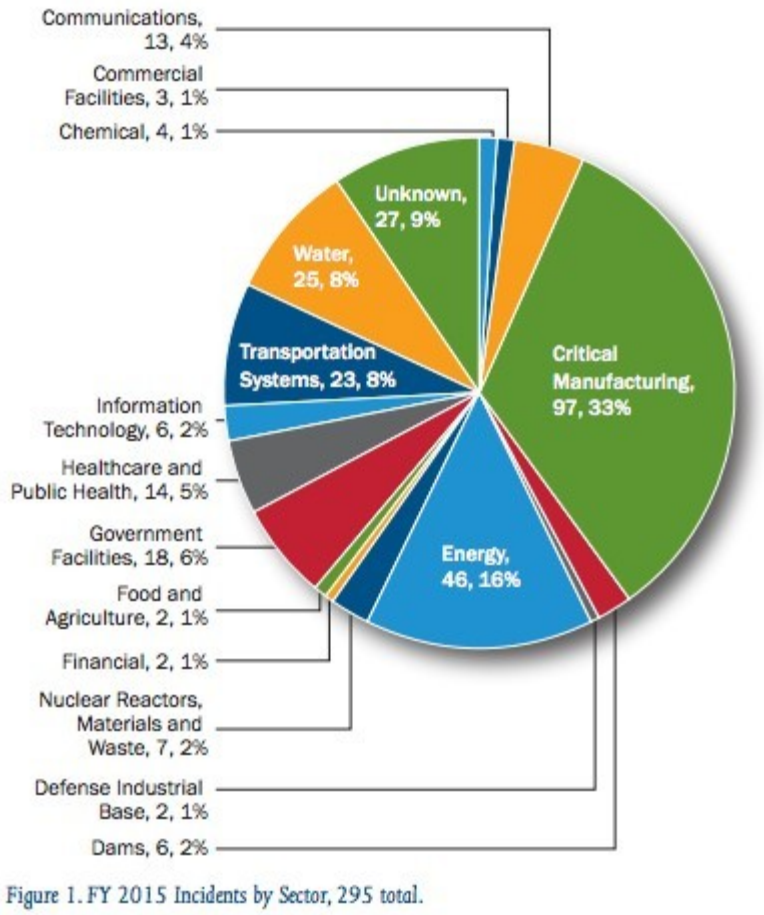

Figure 1. FY 2015 Incidents by Sector, 295 total.

Figure 1

Breakdown by sector of ICS cyber attacks in the United States in 2015

This paper discusses a newly emerging technology that could be of great benefit in adding a layer of cyber security as well as a cost-effective solution in securing critical infrastructure networks: Dynamic Endpoint Modeling.

[1] http://www.reuters.com/article/us-usa-cybersecurity-infrastructure-idUSKCN0UR2CX20160113
http://www.claimsjournal.com/news/national/2016/01/20/268254.htm
http://www.v3.co.uk/v3-uk/news/2399334/us-industrial-control-systems-attacked-245-times-in-12-months

Dynamic End-point Modeling explained

Dynamic Endpoint Modeling is a unique technology that constructs a software-based model of a network and its devices, learning the roles and behaviors of all the endpoints on the network. Dynamic Endpoint Modeling is a paradigm shift from the traditional network security systems. Dynamic Endpoint Modeling is **not:**

- a firewall protecting the network perimeter
- a signature or anomaly-based Intrusion Detection System
- a web application (Layer 7) firewall filtering network flows
- reliant on host agents

Dynamic Endpoint Modeling performs a passive collection of IP (Internet protocol) "metadata," which includes IP addresses, ports, and other flags, from the network. Typically, network Dynamic Endpoint Modeling has sensors connected to a switch or a stack of switches. These switches are configured, depending on the vendor, with a port set to spanning or mirroring to provide data flows from the switches to the sensors. Importantly, this is a one-way data connection. Once the data is received by the sensor, it extracts the metadata and forwards it to the modeling analysis and subsequently to a dashboard for user analysis. To allow for these communications, one network port on the sensor is configured in promiscuous mode for collecting data, while the other port is configured for forwarding this data to a dashboard residing in the cloud.

Dynamic Endpoint Modeling learns and models the behavior of all devices on the network, including how the device connects, to where, what and to whom a connection is made. It establishes a baseline behavioral model, and any changes that divert from the baseline will alert that a possible compromise or malicious activity has occurred on the endpoint. Dynamic Endpoint Modeling does not depend on payloads or known signatures to determine anomalies. Therefore, it is not hampered by encryption, unlike traditional Intrusion Detections Prevention Systems (IDPS) and Next-Generation Firewalls.

Dynamic Endpoint Modeling sends real-time alerts when a system or systems diverge from learned roles or when suspicious traffic is detected, and uses the following five analysis dimensions when building its behavioral models:

1. **ROLE** Dynamic algorithms are used to recognize device roles to analyze and detect activities that divert from the learned baseline.
2. **GROUP** Algorithms assess the devices for known learned behavior by comparing them to other like devices.
3. **CONSISTENCY** Algorithms detect when a device has changed from its known behavior, including traffic streams and access.
4. **RULES** Algorithms detect changes in known patterns by endpoints such as protocols, ports, and blocklisting communications.
5. **FORECAST** Algorithms forecast learned behavior from past behavior and analysis. An assessment is performed against the learned systems for predictive forecasting.

The aforementioned security dimensions allow the Dynamic Endpoint Modeling system to know when a new device appears on the network or accesses the Internet for the first time. It also alerts if a device behaves outside the learned behavior patterns on the network. This can be important especially if an ICS device is accessible from the Internet, since legacy ICS devices are susceptible to attacks

Related resource

For more information on network intrusion detection systems, see the Schneider Electric white paper Network Intrusion Detection Systems for Critical Infrastructure

due to their lack of cyber security robustness. Figure 2 shows the placement of the endpoint modeling sensors in an Industrial Control System Network.

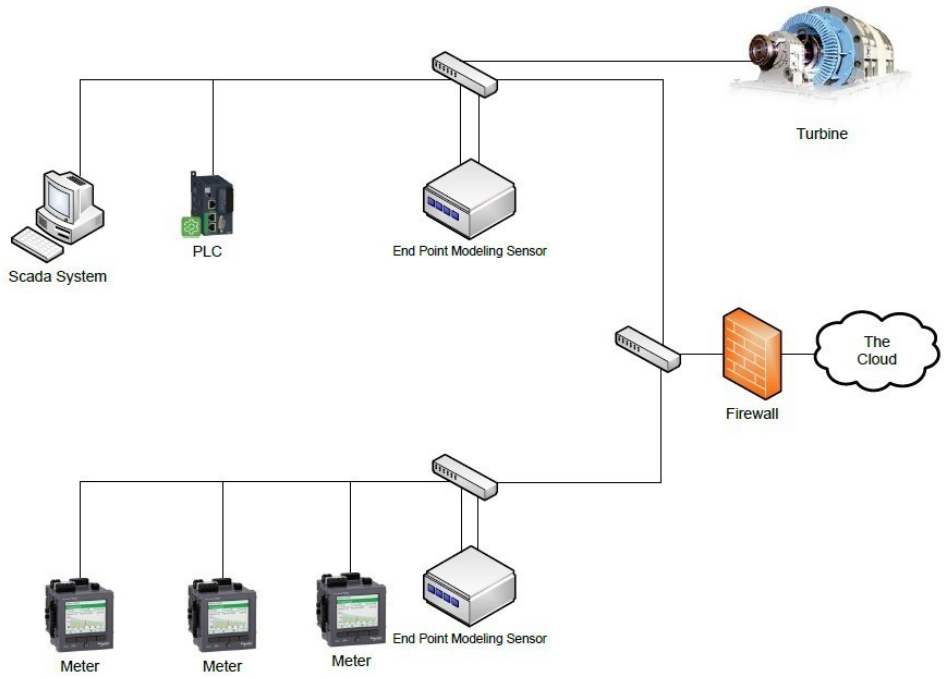

Figure 2

Placement of the endpoint modeling sensors in an ICS network.

Conclusion

Endpoint Modeling offers a quick and cost-effective deployment in a passive mode without any impact to network performance. Unlike traditional Intrusion Detection Preventions Systems, the skill sets needed to deploy and maintain such a solution are not demanding, and the costs for implementing are extremely cost effective. Also unlike these legacy security approaches, endpoint modeling is very low noise, thereby minimizing distraction. This solution provides another dimension to a well-planned defense-in-depth strategy.

About the author

Daniel Paillet is currently Cyber Security Lead Architect within the Schneider Electric, Partner Business. His background includes working in the US Department of Defense on various security projects. He has over 15 years of security experience in Information Technology, Operational Technology, Retail, Banking and Point-of-Sale. He holds the CISSP, CEH and other agnostic and vendor specific certifications. His current role is to architect, improve, and develop secure solutions and offerings within Schneider Electric.