SIEMENS
Ingenuity for life

Article

New early-warning cybersecurity system

Adds extra hardening safeguards to Oil and Gas industrial control networks

As the potential for cyber attacks against the energy sector grows, a revolutionary early-warning system designed to protect the industrial control systems of the oil and gas industry has emerged to complement highly recommended defense-in-depth strategies.

Few people outside the oil and gas industry and its regulatory frameworks appreciate the vast nationwide infrastructure that brings fuel to their corner gas stations and, for many, to their homes. But for criminals, terrorists, and so-called hacktivists, this mostly invisible infrastructure is rich with targets for cyber attacks.

After all, any big disruptions to the nation's intricate network of oil and gas facilities used in exploration, production, distribution, storage and refining, could be spectacular – and potentially devastating to the economy, environment, and quite possibly life safety.

In fact, the U.S. Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) considers the energy sector's infrastructure a prime cyber-attack target. In 2015, for the second consecutive year, it ranked second out of 16 categories behind critical manufacturing for the number of significant cyber attacks reported against it. For this reason, both the U.S. and the European Union are enacting new cybersecurity regulations for the oil and gas industry as mandatory safeguards against such attacks.

This attack frequency has only grown in recent years. That's because the industry continues to deploy increasing numbers of industrial control systems (ICSs) in networks along the entire value chain – upstream, midstream, and downstream – so operators can realize the quantum gains in operational efficiency, visibility, and safety that other industries like manufacturing have long enjoyed. They then connect their ICSs to their enterprise IT networks to gain much more operational visibility and business insights. That's when trouble's door can open.

The most insidious cyber threats to the oil and gas industry are advanced persistent threats, also known as "low-and-slow" attacks.

Special vulnerabilities of ICS networks
Although historically operated in isolation, ICS networks pose special cybersecurity challenges to those trying to protect them from intruders. To understand what those challenges are, it helps to compare ICS networks to enterprise IT networks.

IT networks arose to connect shared office printers, servers, and eventually to provide interoffice communications and external Internet access –all relatively simple compared to the typical complexities and availability requirements of an ICS. However, once connected to the Internet, enterprise networks became open prey for hackers, making precautions such as perimeter defense, firewalls, intrusion detection, anti-virus software and patch management necessary. These measures led to today's defense-in-depth, layered security model that's also deployed across ICS networks.

While that model will remain a best practice to secure both network types, ICS networks can require even greater security when used within critical infrastructure applications for these three reasons:

- First, they must operate within a varied, often intricate context of different vendors' offerings, different versions and configurations, and different levels of cybersecurity maturity – all with numerous interdependencies. That's why making a change to any one of the components in an ICS, including security, without conducting offline system tests could have unintended (and sometimes unknown) rippling effects.

- Second, ICS networks manage supervisory control and data acquisition (SCADA) sub-nets. These connect field-level industrial sensors, drives, motors, controllers and switches to the higher-level ICS, which increasingly links to enterprise IT networks. The IT networks external-facing vulnerabilities can open doors for hackers, who are intent on attacking the ICS. At the same time, wireless SCADA systems, often operating from remote locations using public IP addresses, are also vulnerable to attacks, accessible via their wireless media, whether cellular, 900MHz radio, satellite or microwave.

- Third, ICS networks must run predictably and deterministically 24x7x365. ICS software will typically control sophisticated process automation steps that require precise execution to within milliseconds and sometimes microseconds. Should a cyber attack disrupt an ICS network, the operational impacts can be much more dire to oil and gas operations than for an enterprise IT network, as critical fail-safe features in an unprotected ICS network can be disabled.

Combating "low-and-slow" cyber attacks
The most insidious cyber threats to the oil and gas industry are advanced persistent threats (APTs), also known as "low-and-slow" attacks. These are hard to detect before an attack fully executes, because they operate under the radar of most conventional IT cybersecurity tools.

Without disrupting network or ICS operations, an APT will execute a series of small events that may not constitute an actual cyber attack, but these events could still be anomalous and indicate malevolent intent. Examples include the appearance of new, copycat or forked processes or forked memory usage that occur outside of normal and prior observed ICS or network behaviors.

New safeguards
To combat these types of sophisticated threats, Secure-NOK has combined their unique Network Anomaly Detector with the Siemens RUGGEDCOM platform. The result is SNOK®, a well-known anomaly-based, intrusion detection system (IDS) can now be hosted on the Siemens RUGGEDCOM RX1500 Multi-Service Platform.

The Siemens RUGGEDCOM RX1500 offers a rich set of modular WAN, serial, switching and routing options with enhanced security appliance capability. This allows for hassle-free upgrades in the field, and the flexibility to adapt to changing network architectures and cybersecurity requirements. SNOK® provides an early-warning network monitoring system to identify and isolate cyber threats that may be undetectable by conventional IT security tools. In effect, it adds critical, extra hardening to the defense-in-depth cybersecurity umbrella already protecting ICS networks and any enterprise IT networks to which they're connected.

Plug-and-play installation
The Siemens/Secure-NOK SNOK® Network Anomaly Detection solution differentiates itself by running on the RX1500 Application Processing Engine (APE) module. The APE is an x86-based computer designed to occupy a single-line module slot in a Siemens RUGGEDCOM RX1500 device. The APE is able to host a variety of cyber security solutions including Next Generation Firewalls and identity based cloaking solutions. With the addition of the SNOK® Network Anomaly Detection solution, the Siemens RUGGEDCOM RX1500 adds another critical layer to its security appliance capability.

This solution is compatible with new and legacy ICS networks, designed and specifically tailored to operate in SCADA environments with plug-and-play simplicity. In addition, it requires no changes in the existing network topology or hardware and can be seamlessly dropped into the existing infrastructure thus preserving current investment. Uniquely, the SNOK® platform has virtually no operational load or other impacts on the ICS or SCADA networks and doesn't require signature updates.

How it works
SNOK® works quietly behind the scenes, using software agents to collect deep low-level information that, analyzed over time, can identify anomalous behavior patterns in the network or any of its devices that might indicate a low-and-slow cyber threat before an actual attack and disruption can occur. SNOK® then alerts a compromised ICS network's operators to the attack. It also provides sufficient data to help them make informed decisions about an effective response and corrective action.

Currently, the Siemens/Secure-NOK® SNOK® Network Anomaly Detection solution is in its early deployment stages within the oil and gas industry, with interest coming from other parts of the energy sector such as the power utility industry. Clearly the energy sector is starting to realize that ICS networks need more hardening and early-warning safeguards in addition to conventional, defense-in-depth cybersecurity approaches. It's an idea whose time has come – and Siemens/Secure-NOK SNOK® Network Anomaly Detection solution is specifically designed to address it.

For more information, please contact:
Siemens Industry, Inc.
Davinder Harcharan
davinder.harcharan-singh@siemens.com

Secure-NOK
Siv Hilde Houmb
sivhoumb@securenok.com

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity

Published by
Siemens Industry, Inc. 2016.

Siemens Industry, Inc.
5300 Triangle Parkway
Norcross, GA 30092

For more information, please contact our Customer Support Center.
Phone: 1-800-241-4453
E-mail: info.us@siemens.com

usa.siemens.com/oilandgas

Order No: NTAR-OGSNK-0816
Printed in U.S.A.