KEY BENEFITS

- **Safe for production network.** Passive monitoring means no interference for mission-critical operations. Unlike other ICS security solutions, PT ISIM™ is installed outside the industrial control network in a way that doesn't involve the risk of downtime or incoming data connections.
- **Network integrity monitoring.** PT ISIM™ automatically inventories the network, including ICS components, and performs constant monitoring of network integrity.
- **Incident visualization.** Convenient tools in PT ISIM™ combine network topology with production workflows for an eagle-eye view of security. Security incidents can be visualized at the level of business logic.
- **Event correlation.** PT ISIM™ detects long-term, multi-stage attacks by analyzing security events and intelligently chaining these events together. The event chain shows at a glance how an incident has progressed over time, helping to take preventive measures before it's too late.
- **Rapid reaction to security incidents.** If an incident occurs, PT ISIM™ provides staff with the information they are authorized to see, via role-based access control. Monitoring staff are given only the tools they need to perform their role. Those with investigator roles have full access to information for incident forensics.
- **Site-specific flexibility.** PT ISIM™ can watch for the attack vectors that are unique to a specific site or facility. This protection is customized based on information from a site ICS audit.
- **Built for industrial conditions.** Conditions in the field, or on the factory floor, can be physically demanding. PT ISIM™ is made to withstand the demands of industry without skipping a beat.

PT INDUSTRIAL SECURITY INCIDENT MANAGER™: TAKING INDUSTRIAL CYBERSECURITY TO A WHOLE NEW LEVEL

Today's industrial infrastructure is more automated than ever before. Transportation, manufacturing, utilities, mining, and other industries are active all around the clock. Cybersecurity is critical, since attacks can damage expensive equipment, halt operations, and even hurt people and property.

Corporate IT systems and production systems have tended to converge, but in this process, cybersecurity has been severely neglected. As a result, a security breach anywhere on the network can cause the downfall of a company's entire infrastructure. In early 2017, Positive Technologies researchers found that over 160,000 industrial control system (ICS) components were connected directly to the Internet, making them accessible to anyone. And as Positive Technologies found in ICS security audits in 2016, pentesters in the vast majority of cases could obtain full control over a mission-critical production network by leapfrogging from a corporate network or external networks. The difficulty of hacking industrial systems is decreasing and even low-skilled hackers can wreak havoc.

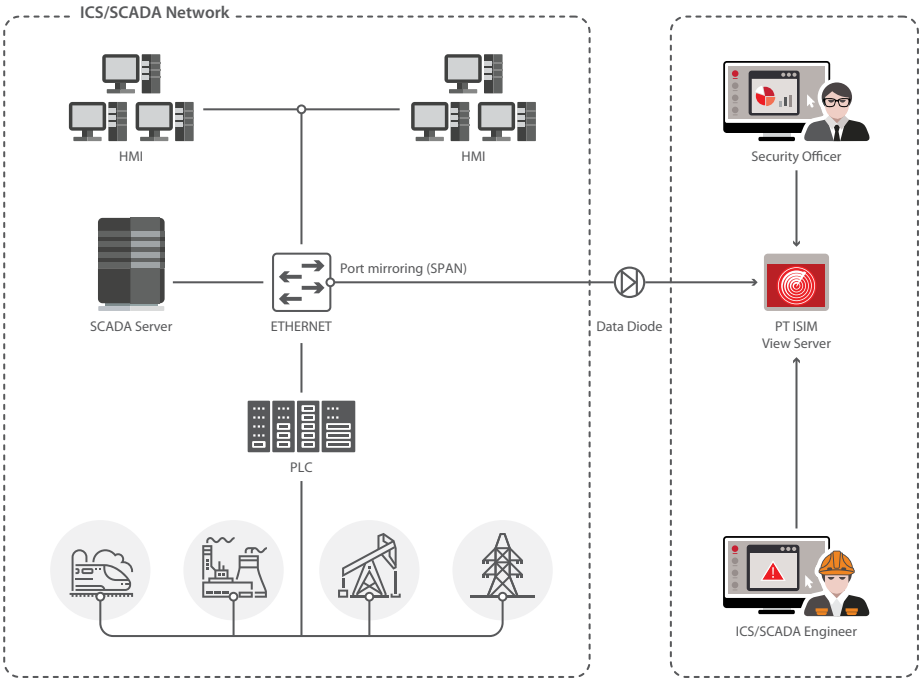
As seen for many years now, ICS components are consistently vulnerable to cyberattacks. Positive Research reports that over 75 percent of vulnerabilities published in 2016 were found in ICS components from leading manufacturers such as Siemens, Schneider Electric, Advantech, and Moxa. Over half of the discovered vulnerabilities were of high or critical importance. And to make things worse, manufacturers' response is far from ideal: over 50 percent of known vulnerabilities have either not been patched at all or no timing for a future patch has been announced.

That's why Positive Technologies has developed PT Industrial Security Incident Manager—to take industrial cybersecurity to a whole new level.

PT ISIM™ HELPS TO:

+ **Detect and prevent attacks.** PT ISIM™ uniquely presents each incident as part of a chain of events and visualizes attack progression using network topology and production workflows. This enables detecting and cutting off an attack before any harm to operations, equipment, or people.
+ **Investigate incidents without interrupting operations.** PT ISIM™ saves a copy of traffic recorded on the industrial control network. With this forensic archive, security staff can perform retrospective analysis and investigate incidents at any moment without causing any downtime.

SAMPLE DEPLOYMENT SCHEME



HOW PT ISIM™ WORKS

PT ISIM™ performs non-stop monitoring of network activity in order to identify vulnerabilities and hacker attacks on industrial control networks. It does not interfere with operations, network infrastructure, or equipment. PT ISIM™ is connected to the industrial control network by a unidirectional gateway, which physically blocks incoming data.

PT ISIM™ analyzes a copy of traffic from an industrial control network, detects security events, and intelligently correlates these events. Smart event chaining enables the software to pinpoint actions of concern, visualizing them in a chain step by step even before an attack has taken place. With this intuitive visualization of incidents, security staff can quickly review attacks that have taken place at different times and contextualize them based on network infrastructure and production workflows. In addition, the archive of network traffic can be used at any time for retrospective analysis and incident forensics.

PT ISIM™ combats a wide array of threats: unauthorized network connections, bruteforcing of system passwords, sending of unauthorized commands, and attempts to alter PLC programming or equipment firmware. Protection extends to internal threats, including staff actions (whether intentional or unintentional) and configuration errors.

Components included with PT ISIM™ facilitate setup of a security operations center (SOC), the industry standard for security management and response.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com