POSITIVE TECHNOLOGIES

SCADA

Global initiatives such as the OPC Foundation's unified architecture, open SCADA and operational technology (OT) platform convergence, are driving automation forward, in an effort to improve efficiencies and management, enrich customer service and reduce operating costs. While these advancements help improve quality of service, productivity and profitability, they also dramatically increase the risk of critical services falling victim to cyberattack.

How we can help

+ Expert audit of ICS security
+ Research & security analysis on ICS components including ERP, MES, SCADA, HMI, PLC and RTU
+ Implementation of ICS vulnerability & compliance management based on MaxPatrol
+ Automated security analysis of Siemens SIMATIC, Invensys Wonderware, ABB, etc.

ICS Risks on the Rise

For decades, supervisory control and data acquisition (SCADA) management systems (part of the industrial control systems environment), have played critical roles automating production for industrial sectors and critical infrastructure.

Attacks like Stuxnet, Shamoon and Flame are only a few examples of a new breed of cyber threat that companies can expect and must be ready for. Consider this: a 2012 study by Positive Research found the number of ICS vulnerabilities had increased 10 times in just 2 years.

Pioneering SCADA Security

Since 2009, Positive Technologies has been working with leading Manufacturing, Petrochemical, Utilities and Transportation companies to improve the security of their automated control systems. Through this collaboration we have acquired a comprehensive understanding of how to protect ICS/SCADA systems developed by leaders such as ABB, Emerson, Invensys (Schneider Electric) and Siemens. In fact, our deep inspections have revealed over 1/3 of all known SCADA vulnerabilities.

Our experience tells us that successfully securing SCADA systems, programmable logic controllers (PLC) and remote terminal units (RTU), requires close cooperation with ICS vendors. At Positive Research, we have more than 200 of the most advanced researchers in the industry – one of the largest teams of its kind in Europe. Last year alone, working alongside ICS leaders like Schneider Electric and Siemens, our experts discovered over 100 new ICS vulnerabilities. This close partnership allows for the rapid development of patches and interim workarounds – giving you confidence that your security risks can be resolved quickly.

Critical Systems Require Critical Thinking

Many of the same technologies and techniques used to protect traditional IT systems can be applied to securing industrial control systems. However, since the business continuity plans, threat models and breach implications associated with these automated systems are quite unique, they require different security approaches for auditing and penetration testing. Some unique considerations for industrial security include:

+ Continuous & multi-level security monitoring: from the network level to applications; from RTU to ERP; from vulnerabilities to human error & fraud
+ ICS/SCADA specific security assessments: different security assessment goals; threat models; operational procedures & organizational complexity

What Others Are Saying:

SIEMENS

"We value the IT security expertise of Positive Technologies. Their research and experience has helped us improve the security of our automation products and better protect our customers' facilities."

David Heinze,
Manager for Industrial Security,
Siemens

MOSENERGO

"The results from several security assessments, completed by Positive Technologies, will allow us to improve security of our power generation company, re-evaluate stability and continuity of the main production processes and focus on the key risk areas."

Network Security Team,
Mosenergo

Enel

"The research provided by Positive Technologies changed our view of cyber security and helped us redefine our strategic direction for securing SCADA infrastructure."

Francesco Ceccarelli
Head of Security Governance and Business Intelligence,
Enel

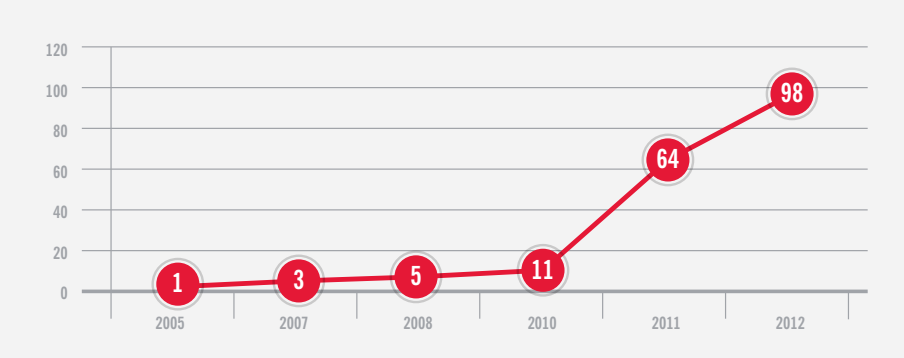

Figure 1: SCADA Vulnerabilities 2005-2012

Maxpatrol for Security Analysis of Industrial Control Systems

Securing industrial automation and industrial process control systems requires the use of both traditional IT security techniques and non-traditional operational technology methods. MaxPatrol's defense in depth approach delivers security automation and compliance management for your entire network; from routers and ERP systems to the electronic instruments, sensors and other intelligent endpoints that collect data and control your physical operations.

MaxPatrol features built-in checks for specialized networking equipment such as Cisco Connected Grid and industrial protocols like Modbus, S7, DNP3 and IEC104. Its extensive database of more than 90,000 security and configuration checks including leading PLC and SCADA solutions from ABB, Schneider Electric and Siemens, and leading ERP solutions SAP and Oracle, ensures that both your IT and OT security risks are identified and resolved quickly and completely.

In addition to supporting mature regulations such as ISO and SOX, MaxPatrol can also automate compliance with international security regulations such as the North American Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) and guidelines such as those proposed by the European Network and Information Security Agency (ENISA) or by specific countries involving the protection of their critical infrastructures.

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit www.ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of $20M+.

SCADA_SB_A4.ENG.0008.01.DEC.29.2014

POSITIVE TECHNOLOGIES