ICS SECURITY

2017 IN REVIEW

POSITIVE TECHNOLOGIES

CONTENTS

INTRODUCTION

Manufacturing facilities and critical infrastructure, such as energy and transportation, have fallen victim to more and more cyberattacks in recent years. Loss of USD $300 million by shipping giant Maersk,[1] interruptions in production at Renault and Nissan plants,[2] and a ransomware attack on the San Francisco public transit system[3] are only a few recent examples that have made headlines.

Securing industrial control systems (ICS) is a critical factor in ensuring the overall information security of critical facilities and infrastructure. Many efforts have been made to promote ICS security: governments are developing regulatory frameworks, computer emergency response teams (CERT) are issuing bulletins, and ICS vendors are gaining awareness that vulnerabilities in their products can cause loss of lucrative contracts[4] and even lives.

Despite these efforts—and in the face of mounting incident costs and concern—security at most industrial facilities has shown minimal improvement since the Stuxnet attacks of 2010, as illustrated in this report.

The problem is worsened by the tendency to connect ICS equipment to the Internet, which is likely to intensify with the advent of the Fourth Industrial Revolution. Such connections set the stage for attacks by hackers from anywhere in the world, even without direct physical access to target equipment.

Nowadays, almost any advanced Internet user can look up the IP addresses of network equipment used on ICS networks (such as switches, interface converters, and gateways) with the help of publicly available search engines. When this equipment is hacked, building systems and operations are at high risk. In 2017, we found that vulnerabilities in such equipment are becoming an increasingly common occurrence.[5]

This report, our fourth on the subject, describes findings by Positive Technologies regarding vulnerabilities in ICS components and their prevalence on Internet-connected systems, and how this situation has evolved over recent years.

ABBREVIATIONS USED

DCS—distributed control systems

HMI—human–machine interface

ICS—industrial control system

LAN—local area network

PLC—programmable logic controller

RAP—remote access point

RTU—remote terminal unit

SCADA—supervisory control and data acquisition

1 bloomberg.com/news/articles/2017-08-16/maersk-misses-estimates-as-cyberattack-set-to-hurt-third-quarter

2 businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5

3 theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

4 In December 2017, oil transporter Transneft announced that it would cease use of Schneider Electric equipment due to multiple vulnerabilities jeopardizing the company's cybersecurity

5 Examples of attacks leveraging network equipment will be described in a separate report, which will be released at a later date on ptsecurity.com

VULNERABILITIES IN ICS COMPONENTS

Research methodology

Information was drawn from publicly available sources, such as vulnerability knowledge bases, vendor advisories, exploit databases and packs, research papers, and posts on security websites and blogs.[6]

The following vulnerability knowledge bases were used:

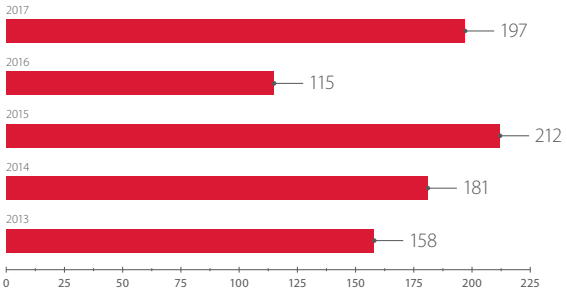
+ ICS-CERT (ics-cert.us-cert.gov)
+ NVD (nvd.nist.gov), CVE (cve.mitre.org)
+ Positive Research Center (securitylab.ru/lab)
+ Schneider Electric Cybersecurity Support Portal[7]
+ Siemens Product CERT (siemens.com/cert)

The severity of vulnerabilities in ICS components was assessed based on the Common Vulnerability Scoring System (CVSS) version 3 (first.org/cvss).

Our assessment of disclosed vulnerabilities did not attempt to cover every single vendor of industrial automation equipment, instead focusing on larger and more prominent companies.

Trends

The number of new vulnerabilities disclosed in 2017 increased compared to the prior year. As of publication of this report, information about 197 vulnerabilities of major manufacturers had been published. However, this number could still increase due to responsible disclosure policies, since vulnerabilities often are not published until after they have been fixed. For example, 30 vulnerabilities in Moxa equipment were detected in 2016 but disclosed only in 2017.

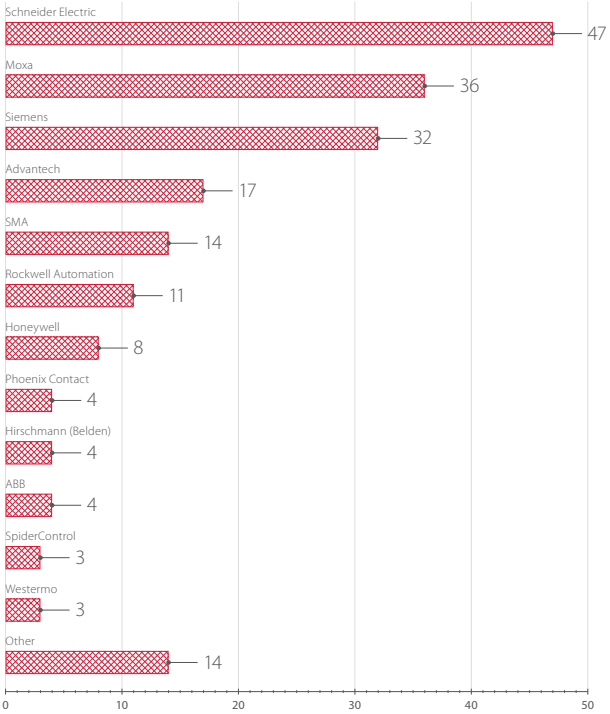


Number of new vulnerabilities found in ICS components

Vulnerabilities by vendor

The top spots saw a reversal of positions. The previous leader, Siemens, yielded first place to Schneider Electric, whose 47 component vulnerabilities disclosed in 2017 exceeded the company's total for 2016 (5) by almost ten times. Also notable is the increased number of security flaws in Moxa industrial network equipment, with twice as many (36) as in the previous year (18).

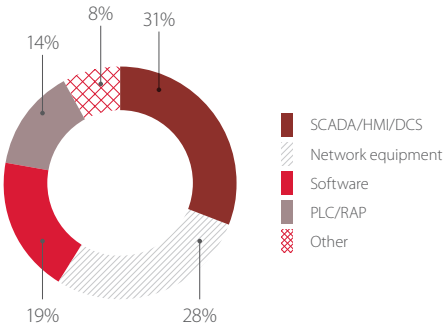
6 digitalbond.com, scadahacker.com, immunityinc.com/products/canvas, exploit-db.com, rapid7.com/db
7 schneider-electric.com/b2b/en/support/cybersecurity/report-an-incident.jsp



Number of vulnerabilities disclosed in 2017 by major ICS vendors

Vulnerabilities by component type

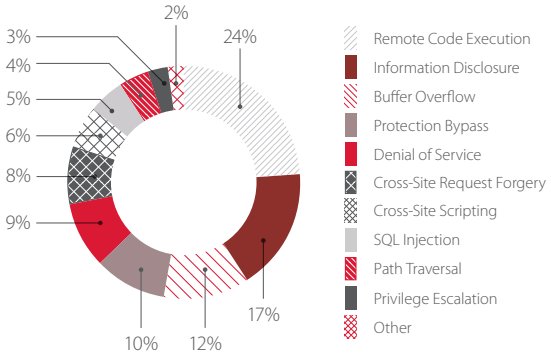
The core trend we see is the growing number of new vulnerabilities in industrial network equipment. Security flaws were detected in Moxa (36), Hirschmann (4), and Phoenix Contact (4) products. While the number of vulnerabilities in network equipment disclosed in 2016 was a third less than in SCADA/HMI/DCS devices,[8] the subsequent 12 months narrowed that gap.



Localization of new vulnerabilities in ICS components

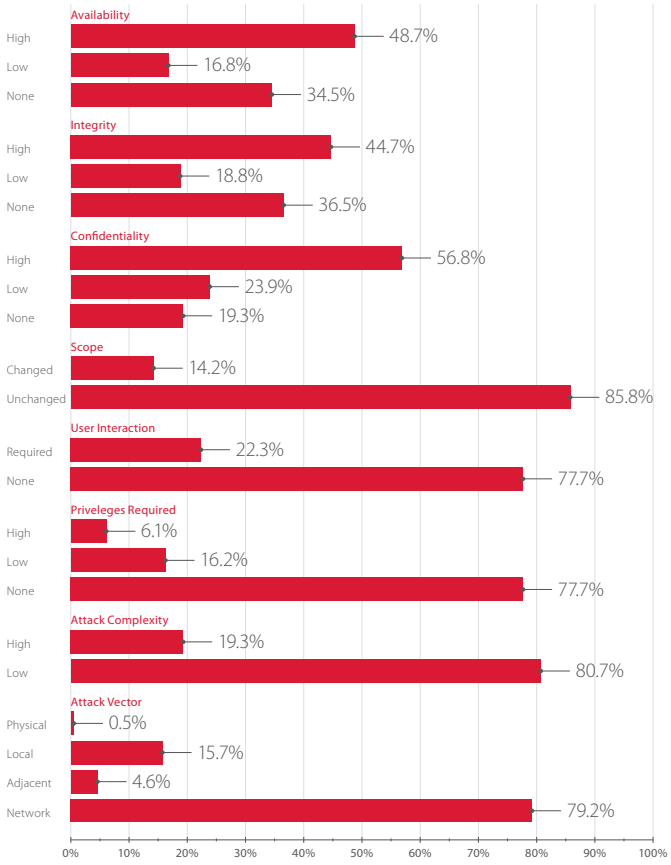
8 ICS components for supervision and monitoring

The most common types of vulnerabilities were Information Disclosure, Remote Code Execution, and Buffer Overflow. In 2016, the first two also topped the list, and the third one was Denial of Service.



Types of vulnerabilities in ICS components

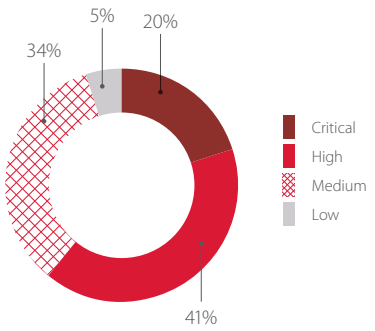
According to CVSS v3 metrics, the situation remained almost unchanged as compared with 2016. Most vulnerabilities detected in 2017 can be exploited remotely without needing to obtain any privileges in advance.



CVSS scores of vulnerabilities

Severity of new vulnerabilities

More than half of the newly reported vulnerabilities are of critical and high severity, based on CVSSv3 scoring. The share of critical vulnerabilities increased by 3% compared with 2016.



Vulnerabilities by severity level

INTERNET ACCESSIBILITY OF ICS COMPONENTS

Research methodology

To collect information on the online accessibility of ICS components, Positive Technologies used passive methods only. To obtain the research materials, we scanned ports of Internet-accessible components using publicly accessible search engines: Google, Shodan (shodan.io), and Censys (censys.io).

Passive techniques for gathering data about the Internet accessibility of ICS components have several limitations:

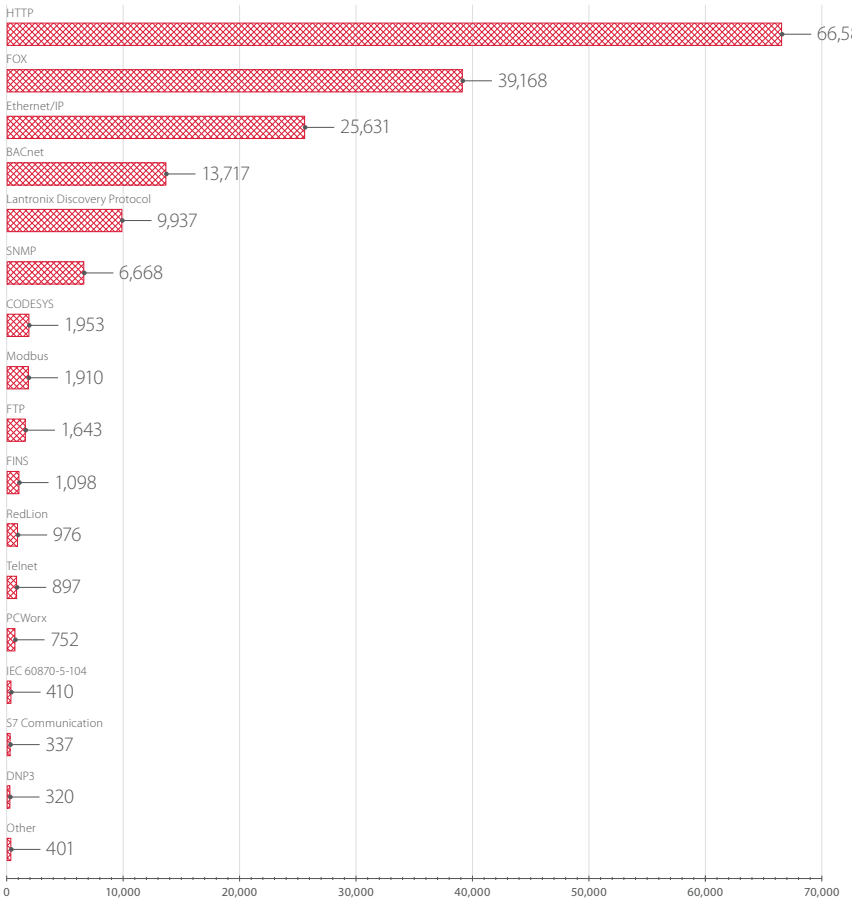
+ Shodan scans a limited number of ports and performs scanning of the Internet from specific IP addresses, which are blacklisted by some firewall vendors and administrators. Therefore, data from Google and Censys was used to expand the scope of assessment.
+ In many cases, it was not possible to determine product versions, because the necessary information was not given in the banners returned by host servers.

This data was then specially analyzed to identify which results corresponded to ICS equipment. Our experts created a database of ICS identifiers for determining product and vendor based on a device's banner.

Prevalence

The research revealed 175,632 ICS components accessible online.

Looking at the protocols used by the detected ICS components, the most common protocol was HTTP, which is consistent with recent years. The Fox protocol was also very popular: it is used in Niagara Framework products and most commonly seen in automation systems for buildings, facilities, and data centers. These systems control air conditioning, power supply, telecommunications, alarms, lighting, security cameras, and other important building systems. Such automation systems often contain vulnerabilities[9] and have already been attacked in the wild.[10]

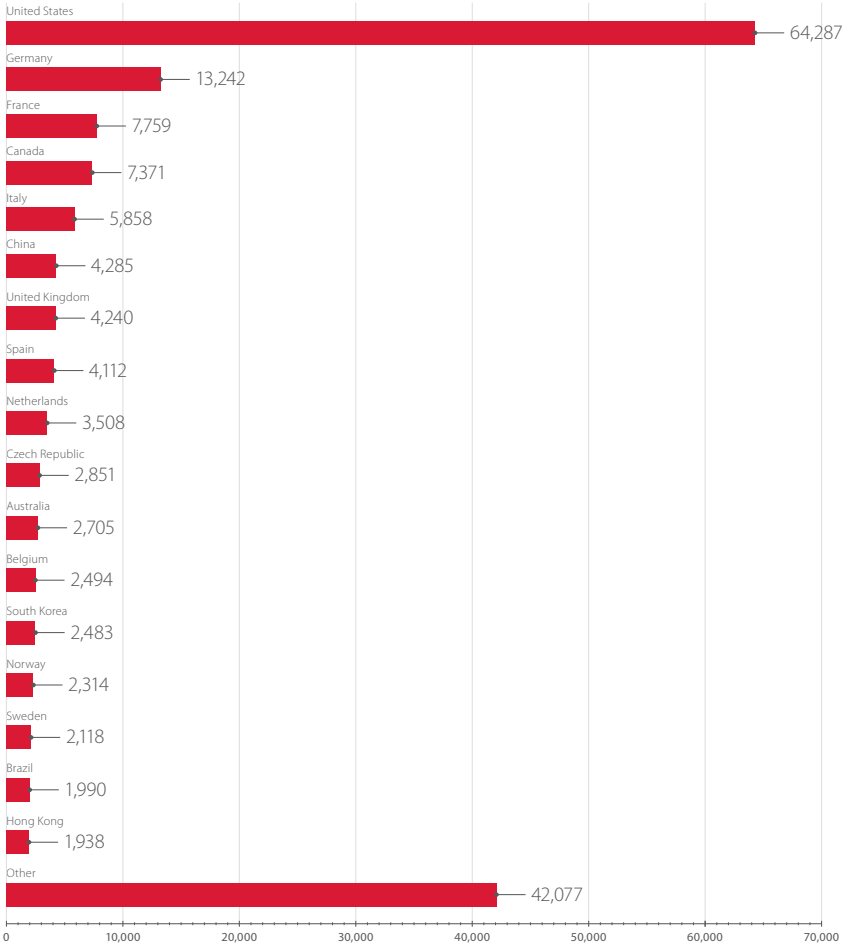


Number of Internet-accessible ICS components, by protocol

9 ics-cert.us-cert.gov/advisories/ICSA-12-228-01A
10 info.publicintelligence.net/FBI-AntisecICS.pdf

Geographic distribution

The U.S. has held the top spot for some years now, increasing its commanding lead of Internet-accessible components by 10% in the last year to around 42% of the total. Germany took second place (6%), the same as in the previous year. Rounding out the top three is France (5%); China fell from third to sixth place.



Number of Internet-accessible ICS components, by country

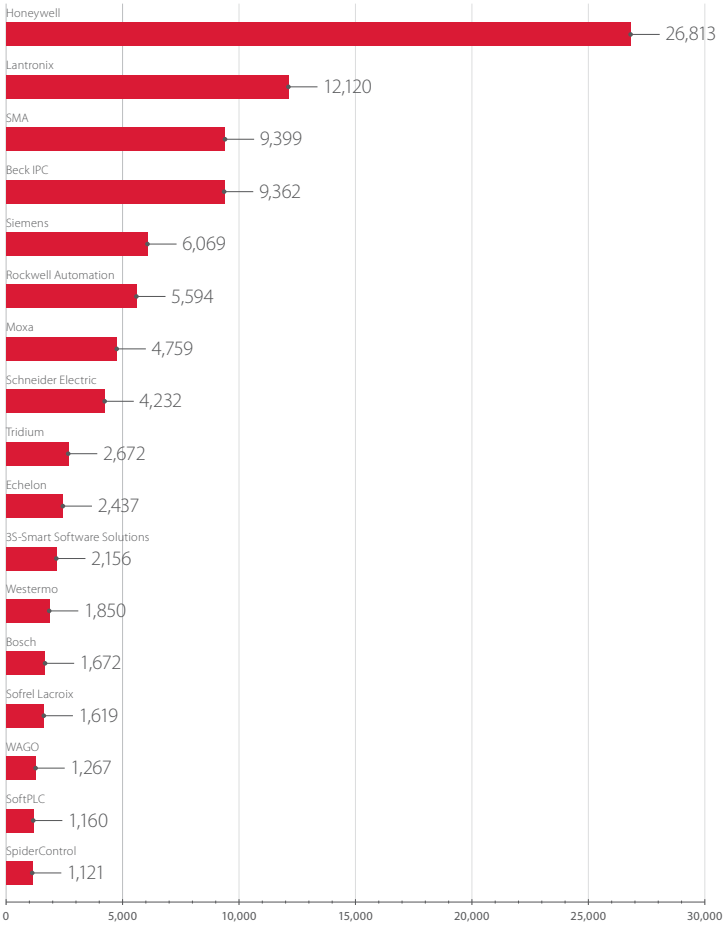
Changes in Russia

In 2017, Russia jumped up three positions to number 28 in the list of countries. The number of detected ICS components grew from 591 in 2016 to 892 in 2017. These changes suggest a growing danger caused by an increasing number of Internet-accessible ICS components located in Russia.

Statistics: vendors and products

First place is occupied by Honeywell, the owner of Tridium and Niagara Framework. Some Niagara products retain their old brand, which is why Tridium is listed separately from Honeywell in this report.

The second most popular vendor is Lantronix. This California-based company manufactures devices designed to provide remote access to equipment via the Internet.



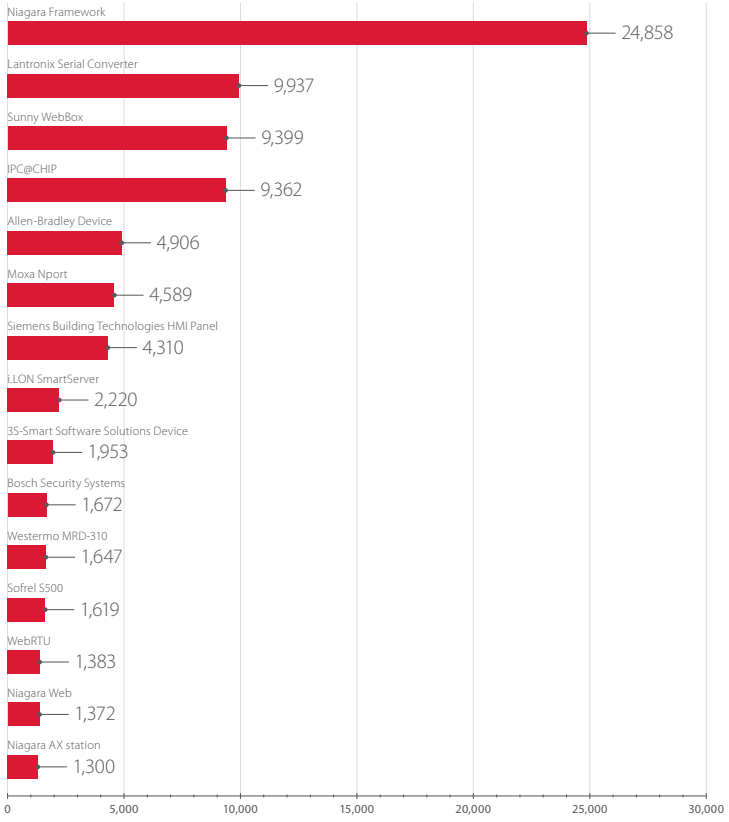
Number of Internet-accessible ICS components, by vendor

According to recent research,[11] several thousand Lantronix interface converters are accessible on the Internet. Almost half of these devices expose passwords that could be used to connect via Telnet. Our research confirms this fact: we detected 12,120 accessible Lantronix devices in total, a number of which were vulnerable.

Despite their auxiliary role, these devices can pose a significant hazard to operations when connected to the Internet. Interface converters connect ICS components to each other, so any malfunction or failure on their part can cause loss of remote control and management. For example, during a cyberattack on the Ukrainian energy grid,[12] the attackers remotely disrupted the functioning of Moxa converters. As a result, utility operators could no longer connect to field devices at substations or remotely control substation switches.

As in prior years, Niagara Framework is the software most commonly found on Internet-accessible equipment. Apart from Lantronix interface converters, which hold second place, Moxa converters are also close to the top.

11 bleepingcomputer.com/news/security/thousands-of-serial-to-ethernet-devices-leak-telnet-passwords/
12 boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf



Internet-accessible ICS components, by product

Types of ICS components

The distribution of Internet-accessible components by types remained almost the same. The only difference from 2016 is a significant increase in the share of network equipment.

Share of ICS components accessible on the Internet, by type

Type of ICS component	Share in 2017	Share in 2016
SCADA/DCS/HMI and/or PLC/RAP (RTU)[13]	14.2%	13.6%
PLC/RAP (RTU)	13.2%	12.9%
Network equipment	12.9%	5.1%
SCADA/DCS/HMI	7.1%	7.8%
Electrical measuring equipment	6.3%	5.2%
Other	46.5%	55.5%

13 This type includes components that can be classified under multiple types, such as Niagara Framework multifunction products.

CONCLUSION

The 2017 data shows an increasing number of vulnerabilities publicly acknowledged by major ICS vendors. More than half of the detected vulnerabilities are of critical or high severity.

The number of Internet-accessible ICS components is growing. The majority of them were detected in the countries with the highest levels of industrial automation (U.S., Germany, France, Canada, Italy, and China).

An increase in the number of known vulnerabilities and Internet-accessible ICS components allows attackers to conduct a wider range of attacks, which can cause very tangible impacts. Responding to sophisticated attacks on ICS components requires large amounts of preparation and planning. Before the first line of code is ever written, ICS developers must design the security mechanisms necessary to protect ICS components from attacks.

To identify potential attack vectors and develop an effective protection system, companies should perform regular ICS security audits and deploy industrial cybersecurity incident management solutions.

As always, observing the following basic security guidelines goes a long way toward ensuring protection:

+ Segregate ICS operational networks from the enterprise LAN and external networks.
+ Limit physical access to ICS networks and components.
+ Enforce a strict password policy.
+ Properly configure network equipment and firewall filtering rules.
+ Protect privileged accounts.
+ Minimize privileges of users and services.
+ Use antivirus software.
+ Regularly install updates to operating systems and applications.

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