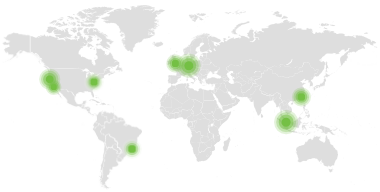
REPORT



2021

Industrial Internet Security Trend Report

Inspired by the rapid growth of the industrial Internet, many countries have included the development of the industrial Internet in their national strategies and set forth laws and regulations to push the industry further into wider areas. For this industry to develop soundly, a complete security system is a prerequisite.

Table of Contents

Key Findings:

- The number of exposed ICS assets was basically proportional to the industrial development of a country or region.
- A significant majority (72%) of exposed assets were using the protocol MODBUS.
- The number of ICS vulnerabilities is increasing year by year. Vulnerabilities in products of large vendors have attracted much attention. Vulnerabilities that have not yet provided patches or practical mitigation advice are more danger than others in published vulnerabilities.
- Attacks affecting the operations of infrastructures are frequent. Ransomware is the most commonly used vector as attackers are becoming more aggressive.

Key Insights:

- To cope with unknown cybersecurity threats to the industrial Internet, cyber ranges can be introduced for cyberattack and protection emulation, cybersecurity trend deduction, personnel training, new technology demonstration and experiments, and emergency response exercises. Cyber ranges are expected to evolve stage by stage from physical sand tables to virtual ranges, to a hybrid of the two, and finally to the digital twin.
- The deception techniques for the industrial Internet are expected to play an important role in the security of the industrial Internet in the years to come.
- For the industrial Internet, security products should be characterized by ease of use and able to conduct accurate, fine-grained, multidimensional detections in real time and make all-round evaluations without having any negative impact on the business.
- Industrial Internet security services should cover security consulting, security training, security assessment and security operations.
- Effective and efficient industrial Internet security operations can ensure that security risks are identifiable, manageable, and controllable for enterprises and organizations with limited resources.

Security Posture of the Industrial Internet

Global Exposure of ICS Assets

Over the period from January to September 2021, our monitoring of industrial control system (ICS) devices around the world found that the number of exposed ICS assets was basically proportional to the industrial development of a country or region. The top 3 countries with the largest number of exposed assets were the USA (15%), Germany (9%), and China (7%). The exposed assets in top 10 countries together accounted for about 66% of the total number of such assets.

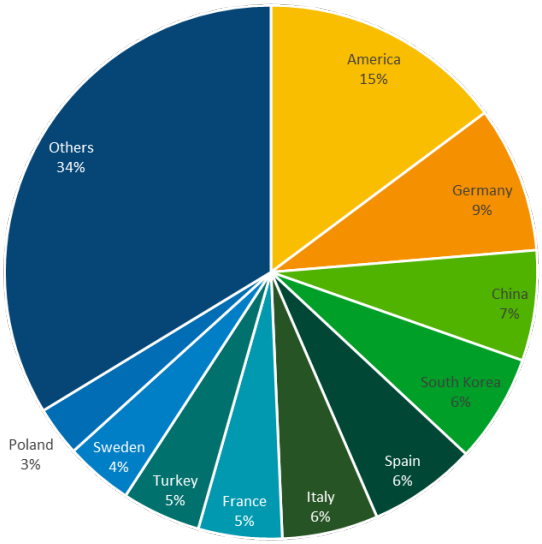


Figure 1 Global exposure of ICS assets by country (Source: NTI)

Global Exposure of Common Industrial Protocols

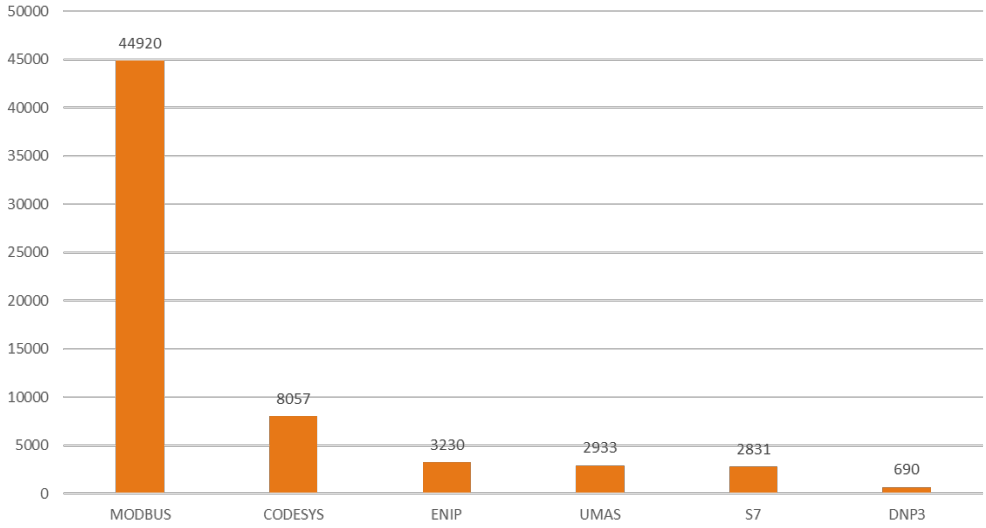


Figure 2 Global exposure of common industrial protocols (Source: NTI)

As for industrial protocols, MODBUS, CODESYS, EtherNet/IP (ENIP), Unified Messaging Application Services (UMAS), S7, and Distributed Network Protocol 3 (DNP3) were the top 6 protocols most commonly used. MODBUS alone was found on 72% of exposed assets.

Vendors of Exposed ICS Asset

Exposed ICS assets are from Schneider Electric, Siemens, Rockwell, CONPOWER, and Solare Datensysteme GmbH, among others. The top 3 vendors were Schneider Electric (37%), Siemens (13%), and Rockwell (13%), together contributing 63% of the total exposed assets.

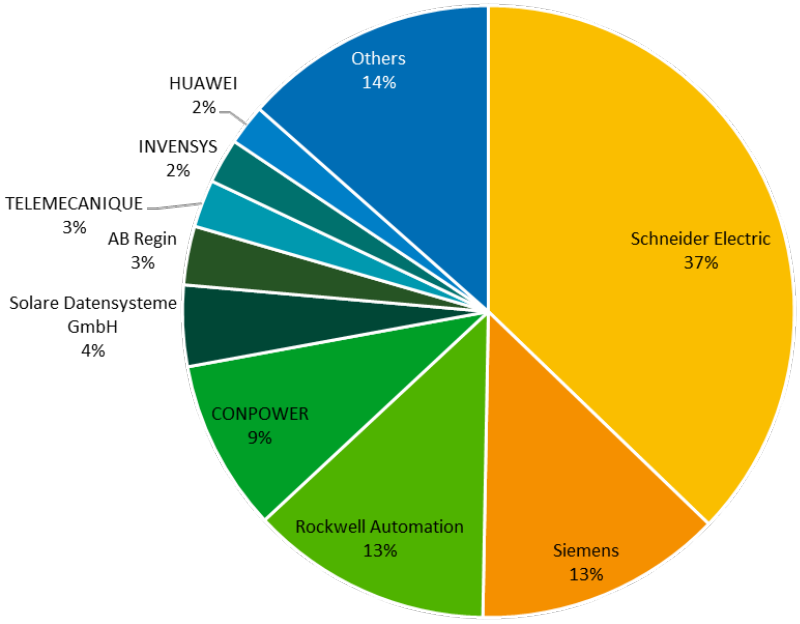


Figure 3 Vendors of exposed ICS assets (Source: NTI)

Vulnerabilities in the Industrial Internet

The number of vulnerabilities found in ICSs is increasing year by year. The following chart was drawn based on data from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

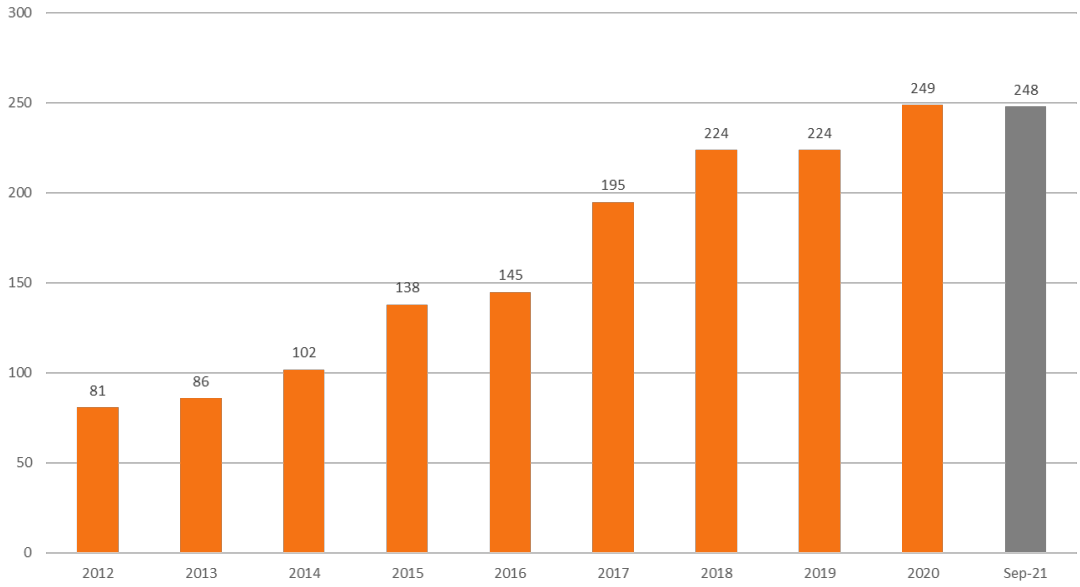


Figure 4 Number of security advisories released by ICS-CERT in the past 10 years

The Dragos team analyzed 703 ICS/OT vulnerabilities in 2020 and found that 78% of advisories had a patch. 64% of the rest advisories with no patch had no practical mitigation advice. [1]

[1] 2020 ICS Year in Review Vulnerability Webinar 04-15-21.pdf (dragos.com)

Sources of Security Risks to the Industrial Internet

Devices

When it comes to the industrial Internet, smart device software is usually not up to date, vulnerabilities are underestimated, and developers are not well aware of security issues.

Smart devices exposed on the Internet are large in quantities, providing opportunities for malicious samples to spread and scan for vulnerable devices for launch of distributed denial-of-service (DDoS) attacks.

Networks

The nodes, data, access controls, business continuity, and authentication of the identity resolution system for the industrial Internet bring in cybersecurity risks to the industrial Internet. The adoption of 5G technology also contains the risk of DDoS attacks from massive traffic detection, vulnerable devices with insufficient computing power, and a very large number of links as well as the risk of bypassing centralized monitoring made possible by edge clouds, device-to-device (D2D) communication, and the like.

ICSs

Thanks to the industrial Internet, previously hierarchical, closed, and local production controls are flattening, becoming more open and global. In this context, if ICS vulnerabilities are improperly managed and protections are insufficient at the technology level, insider and outsider threats will become a reality.

Data

Many ICSs use protocols that transmit messages in plaintext. Besides, they usually work on universal operating systems and are not updated in time. Worse still, industrial data sources are varied, adhering to different formats and standards. And there is no authentication or real-time access control for data access and uses.

Platforms

- The industrial infrastructure as a service (IaaS) is exposed to the risks of virtual machine (VM) escape, cross-VM side channel attacks, image tampering, and other emerging attacks.
- The industrial platform as a service (PaaS) is prone to such security risks as software and hardware resource theft and access, DoS, and malicious code injection.
- The industrial software as a service (SaaS) is scenario-specific, incorporating multiple industrial microservice components that are loosely coupled. Intended to implement complicated functions, the industrial SaaS has no security design standard to follow, plagued with security issues, such as vulnerabilities in industrial apps, insecure communication over application programming interfaces (APIs), improper user controls, and developers' malicious code injection.
- At the access stage, a platform is at the risk of data being monitored, intercepted, tampered with, lost, or stolen. At the operational stage, stored data may be breached. At the end-of-life stage, the platform is exposed to the risk of data leaks and no backup.

Statistics on Attacks in the Industrial Internet

Since January 2021, the number of ICS attacks has soared, affecting the operations of critical information infrastructure. Manufacturing, electric power, pipeline, water treatment, national defense, aerospace, petrochemical, medical apparatus, energy, and healthcare industries as well as utilities have been major targets of hackers. We analyzed samples collected from 59 attacks and found that about 59% of attacks used ransomware. Of all identified ransomware families, Revil made up the largest proportion.

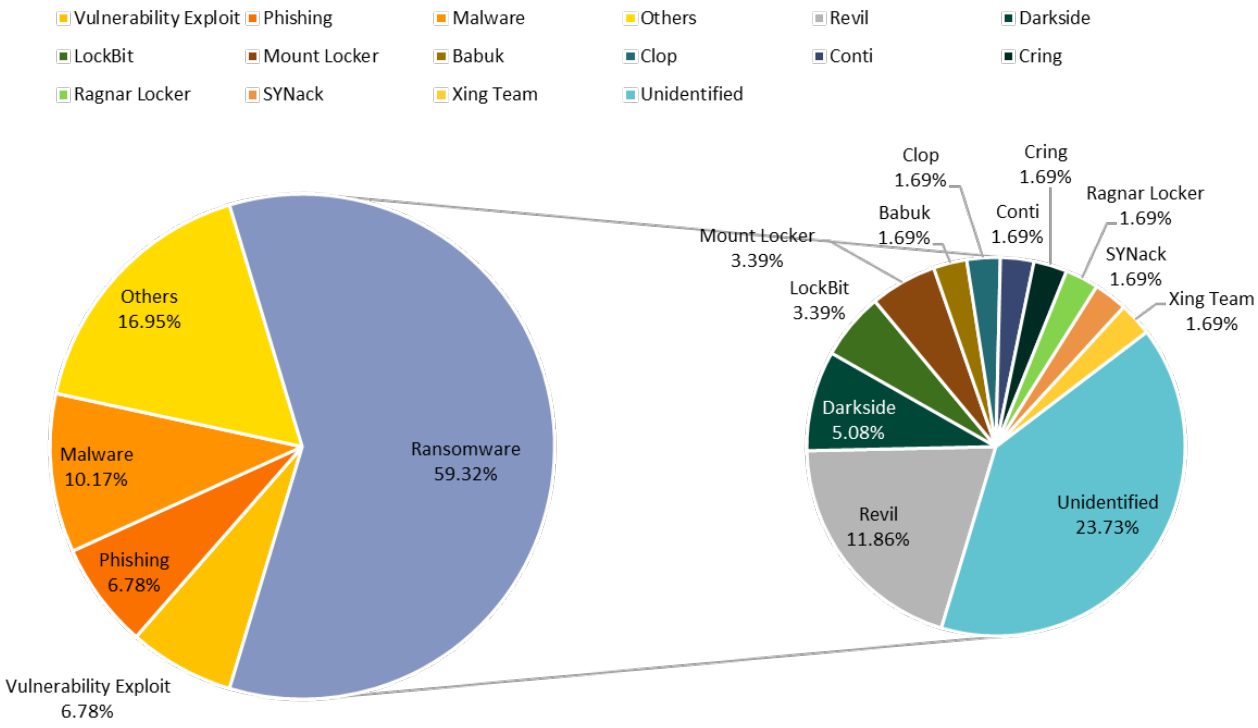


Figure 5 Proportions of attack types

Technical Trend of Protections for the Industrial Internet

To cope with unknown cybersecurity threats to the industrial Internet, cyber ranges can be introduced for cyberattack and protection emulation, cybersecurity trend deduction, personnel training, new technology demonstration and experiments, and emergency response exercises. Cyber ranges are expected to evolve stage by stage from physical sand tables to virtual ranges, to a hybrid of the two, and finally to the digital twin.

Figure 6 Photo of a sand table

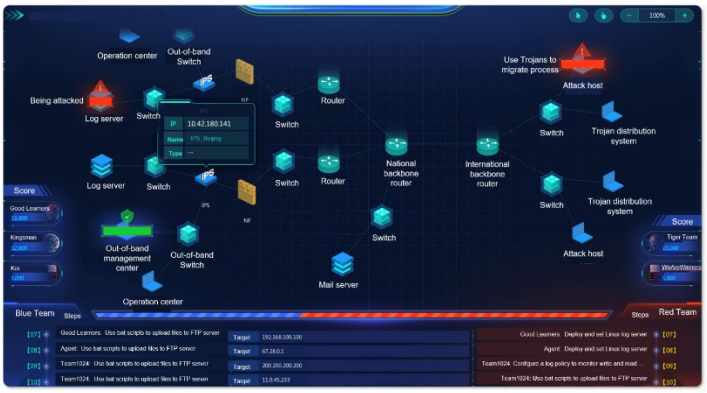


Figure 7 Virtual range

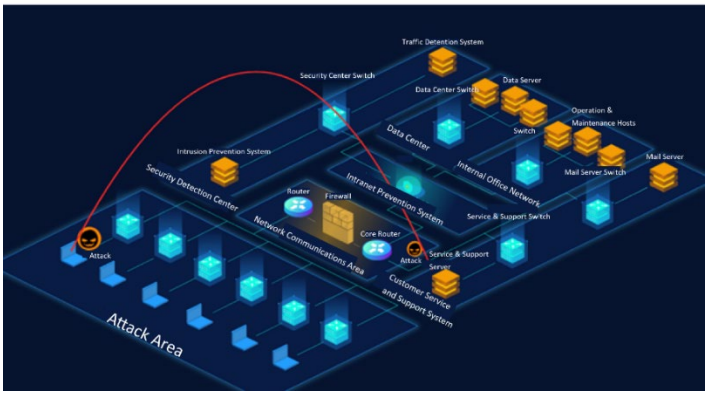


Figure 8 Hybrid of a sand table and a virtual range

Figure 9 Digital twin scenario

In this era when hackers repeatedly target the industrial Internet, how can enterprises promptly capture attacks, preventing them from disrupting the business? The deception techniques for the industrial Internet, which have emerged in these two years, are expected to play an important role in the security of the industrial Internet in the years to come.

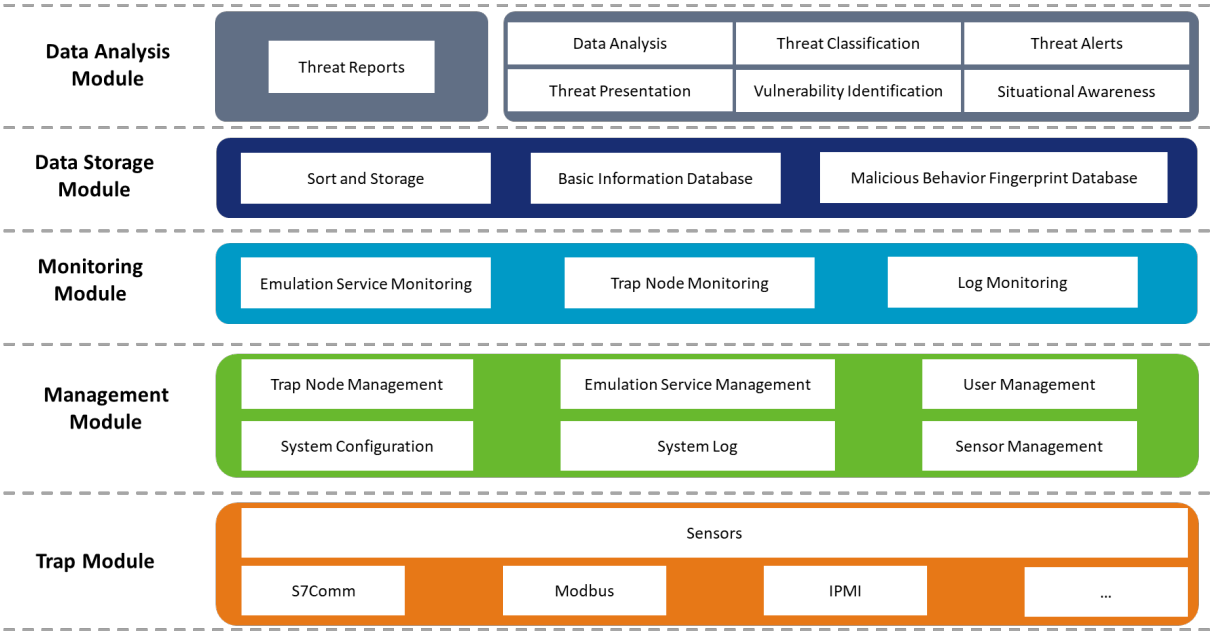


Figure 10 Architecture of the deception system for the industrial Internet

To effectively protect the industrial Internet, we should make bold assumptions and then verify their possibilities. A main method of detecting loopholes in offensive and defensive strategies is to make deductions from a business-specific sand table, providing solutions and technical support for business continuity assurance.

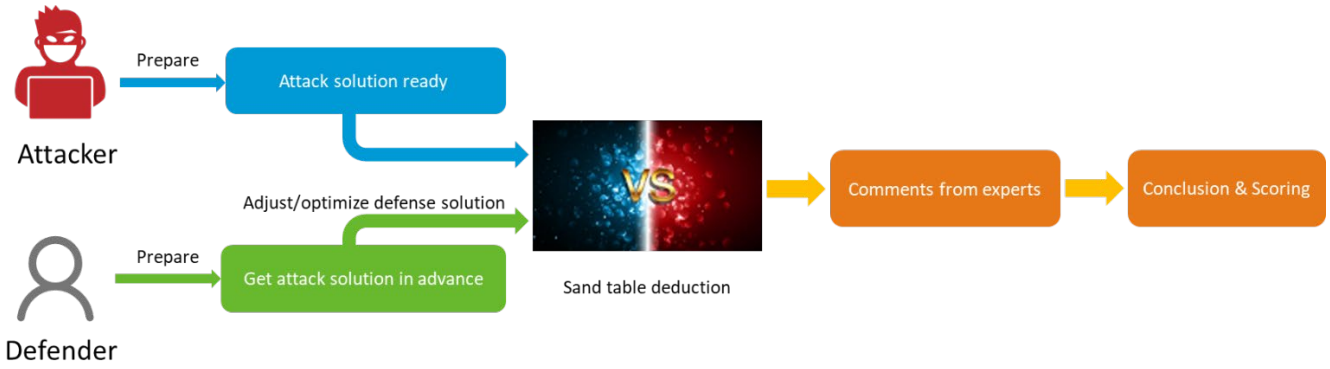


Figure 11 Simulated attack/defense deduction process

What to Expect About Industrial Internet Security Products

- Device manufacturers should not only attach importance to the security of functions but also add security techniques to their solutions and products.
- For the industrial Internet, security products should be characterized by ease of use (EOU) and able to conduct accurate, fine-grained, multidimensional detections in real time and make all-round evaluations without having any negative impact on the business.

- The security of the industrial Internet should take the entire ecosystem into account. For this purpose, a defense-in-depth system featuring a layered architecture should be developed and a border protection system be deployed to secure the business.
- Artificial intelligence (AI) are accelerating the development of industrial Internet security products. Security orchestration and automated response techniques, when applied, will be more conducive to control and presentation of threats facing the future dynamic system architecture. The ecosystem of the industrial Internet will gradually become autonomous and controllable.
- Security products will be compatible with the next-generation Internet over time. IPv6 is pivotal to the next-generation Internet technology and Internet of things (IoT) technology. For IoT where IPv4 and IPv6 coexist, security products will evolve towards enhanced support for transitional techniques and higher capacity for processing mixed traffic in such new environments.

What to Expect About Industrial Internet Security Services

Security Consulting

Industrial Internet security consulting is changing from focusing on individual issues to having the big picture in mind and from information security to convergent security.

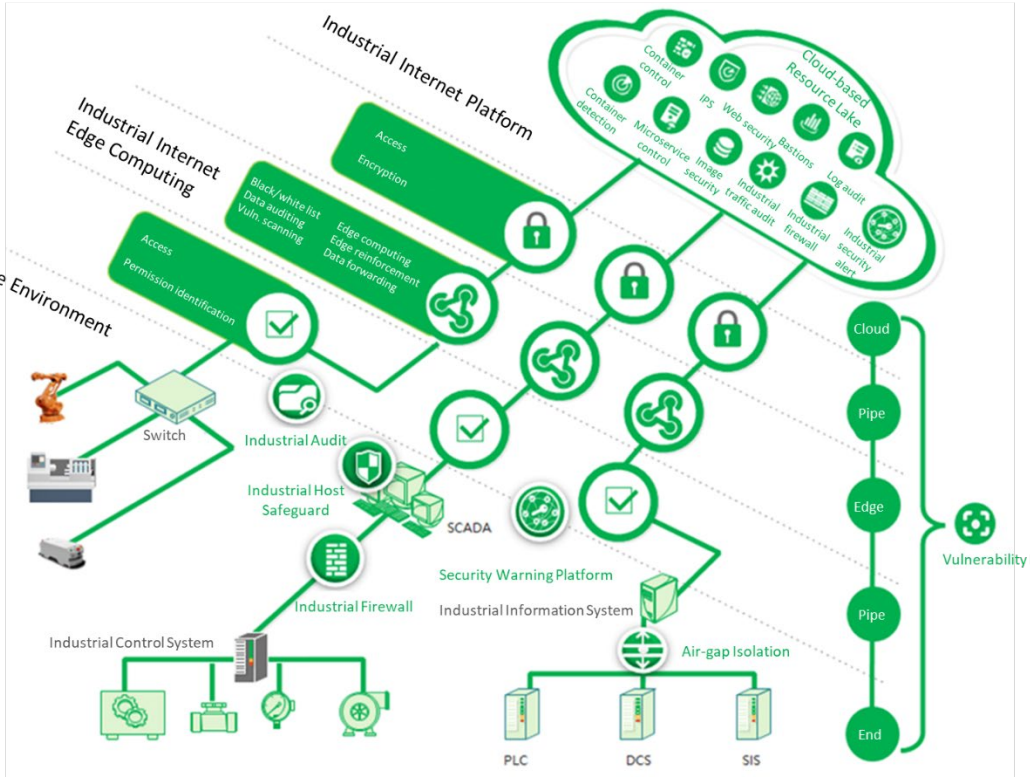


Figure 12 Security consulting service for the industrial Internet

Security Training

Cybersecurity of the industrial Internet calls for an organic system instead of a large number of security products deployed at random. In other words, the system will be a collection of multiple elements, including the management, people, policies, and protection devices, working in unison. Personnel of low security awareness may become the largest loophole in a cybersecurity system, as is the shortest plank for a bucket.

- Industrial Control Fundamentals
- Information Security Basics
- Industrial Control Security Basics
- Industrial Control Attack Testing and Practice
- Industrial Control Prevention System
- Vulnerabilities in Industrial Control System
- Industrial Laws and Standards
- Solutions for Industrial Control System
- Emergency Response System
- Cutting-edge Technologies

Figure 13 Security training courses for the industrial Internet

Security Assessment

In the initial scores of years of development, ICSs were completely independent, isolated from an enterprise's management system. Subsequently, with the fast advancement of IT transformation, information, network, and IoT technologies have seen increasingly broad applications in the industrial control field represented by the smart grid, smart transportation, and industrial production system. For collaboration and information sharing with other systems, ICSs cannot be isolated any more. They have begun to adopt standard, universal communication protocols and hardware/software systems and some even connect to public networks, such as the Internet, in one way or another. This exposes ICSs to viruses, trojans, hacks, and DoS, which were typical threats to traditional information systems. Moreover, as ICSs are mostly used in critical industries like electric power, transportation, petrochemical, and nuclear industries, a security incident on an ICS will cause a greater social impact and financial loss than on an information system.

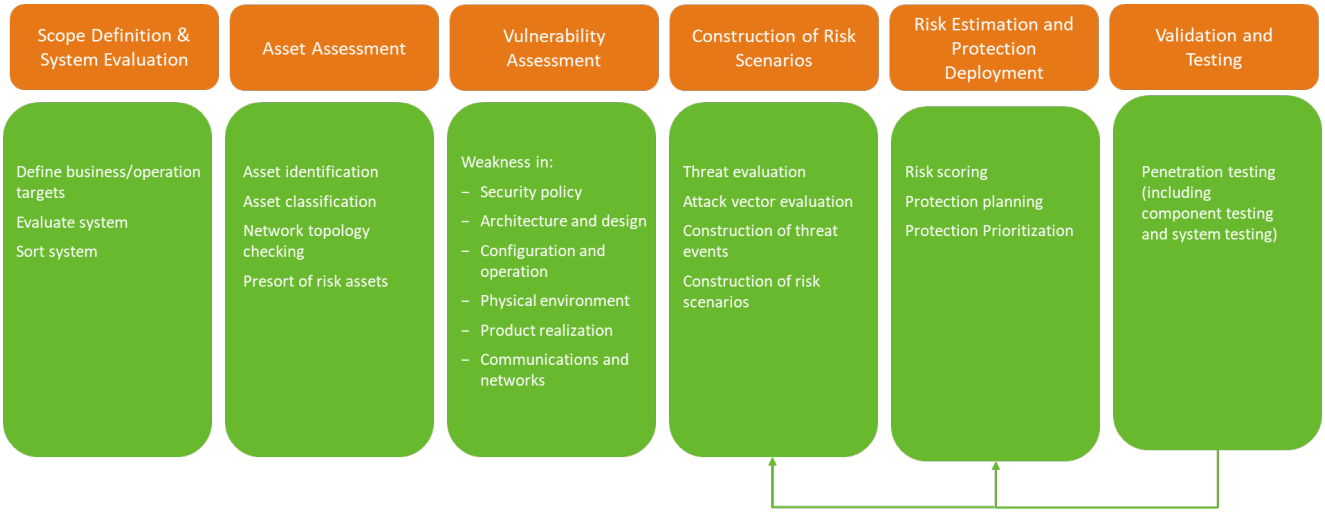


Figure 14 Security assessment process for the industrial Internet

Security Operations

Through extensive analysis of industrial enterprises, we found that their security operations were encumbered with insufficient effective inputs, as demonstrated in:

- Lack of professionals and techniques
- Large number of security vulnerabilities that are difficult to fix
- No deep integration of business processes and cybersecurity
- Weak links found in business security, such as risks brought in by lower-level assets and edge assets
- Underestimation of the criticality of incidents and low capability of closed-loop management, leading to the possibility of legal violations
- Low cost efficiency

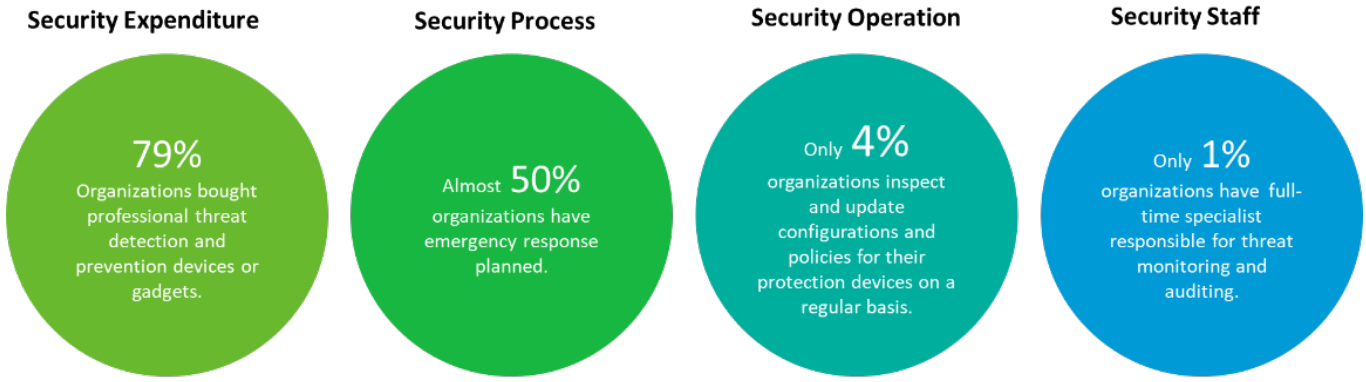


Figure 15 Security operation status of nearly 400 organizations
(Source: NSFOCUS's security services during critical events in 2019 and 2020)

Effective and efficient industrial Internet security operations can ensure that security risks are identifiable, manageable, and controllable for enterprises and organizations with limited resources.

Recommendations on Security Operations of the Industrial Internet

1. Establish an asset management process and mechanism for end-to-end security management of industrial enterprises' intranet and extranet assets throughout the lifecycle, in a bid to minimize the attack surface of business systems and reduce cybersecurity risks.
2. Use a dedicated ICS vulnerability scanning system to discover risks in business systems and perform closed-loop management of vulnerabilities from vulnerability detection to assessment, remediation, and finally to verification. Develop security configuration baselines as the minimum requirements for enterprises to protect their business.
3. Build processes on big data analytics and visualization techniques to optimize platform policies, and develop and improve the capabilities of ongoing monitoring, analysis, and handling of threats in the industrial Internet.
4. Security enterprises, based on years of experience in the cybersecurity realm, provide 24/7 security solutions for industrial Internet enterprises, including not only traditional security software for asset surveys, virus removal, firewalling, intrusion detection, traffic audits, or security monitoring but also

security capabilities in the form of SaaS to help customers create virus, vulnerability, and protection tool databases on the industrial Internet platform.

5. Establish a security operations center (SOC) for the industrial Internet to provide all-round protections 24/7 for industrial Internet enterprises through a complete process covering threat identification, protection, detection, response, alerts, and handling.

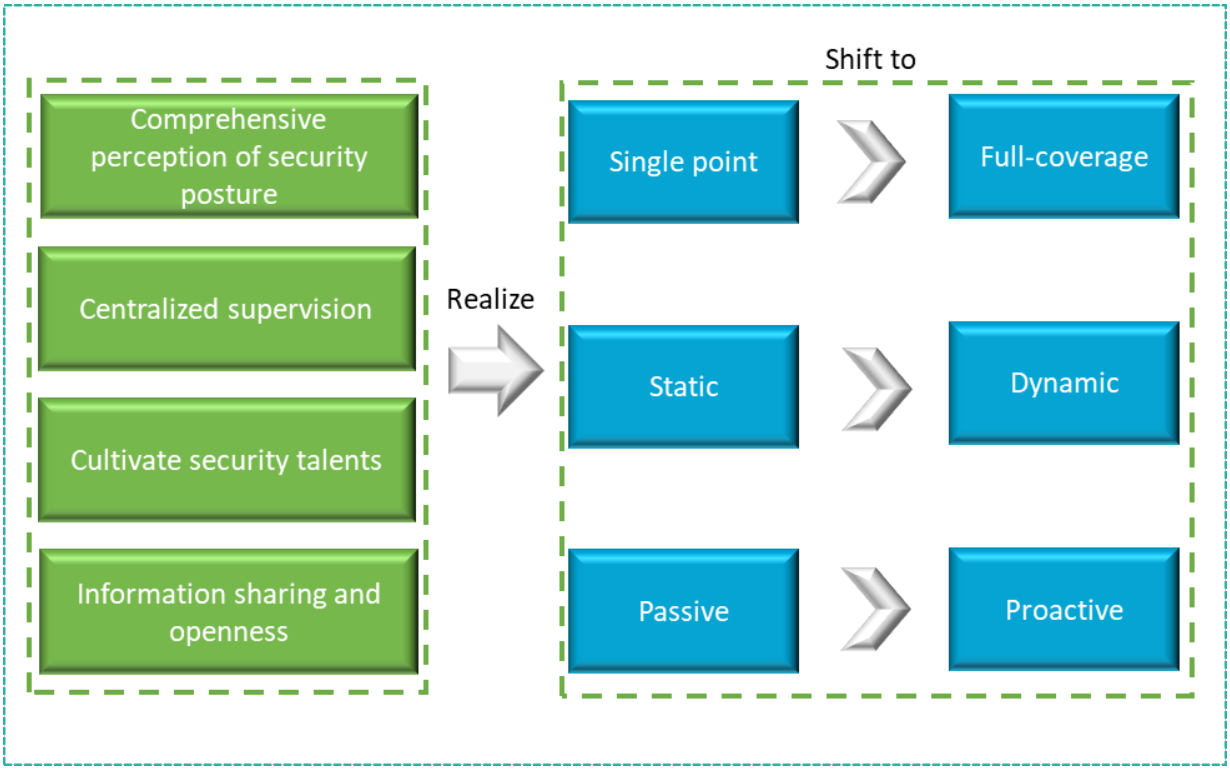


Figure 16 SOC development roadmap

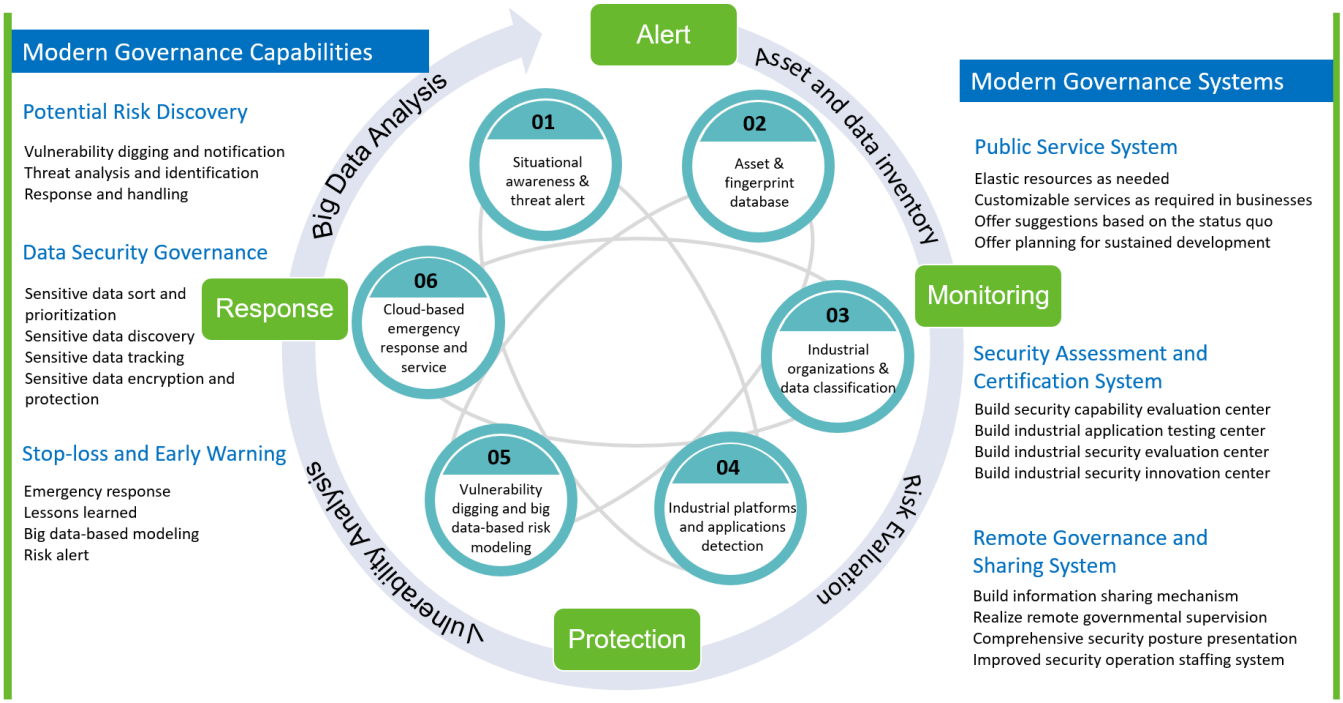


Figure 17 SOC for the industrial Internet

Conclusion

The industrial Internet is a new type of infrastructure that features deep integration of the next-generation ICT and the industrial economy. As a cornerstone of the fourth industrial revolution, it is an inevitable path for industries to become digital, interconnected, and intelligent. Built on networks, the industrial Internet pivots around platforms, with data as key elements and security as the top concern. It not only serves as the infrastructure for the transformation to digitalized, networked, and intelligent industries but also represents a pattern of deeply integrating the Internet, big data, and artificial intelligence with the real economy.

The industrial Internet is crucial to people's livelihood and is of great significance to the national economy and social development. For this reason, it becomes a target of the adversaries, hostile groups, and hackers at home and abroad. Immediate measures must be taken to secure the networks for the sound development of the industrial Internet.