Securing your operation

Cybersecurity solutions from Schneider Electric

schneider-electric.com

Life Is On | Schneider Electric

Client references

“Qatargas had recently utilized the services of the Schneider Electric global cybersecurity team for three recent projects. They were found to be knowledgeable in this field, will discuss and come up with new or custom solutions, and benefit the end user (Qatargas). The solutions have already been implemented and are working well. Overall, Qatargas is satisfied with the services provided by the cybersecurity team of Schneider Electric.”

—Ahmed Hassan Al-Sulaiti,
Head of Project Execution (On-plot & Off-plot),
Qatargas, Qatar

“The Schneider Electric cybersecurity team was engaged to perform a Vulnerability Risk Assessment based on IEC62443/ISA99 standards at three refinery sites at HELPE in Greece. They performed the Risk Assessment successfully utilizing a defense-in-depth approach, categorizing the criticality and subsequent risk levels based on each system class.

The team then defined their appropriate best practices, recommendations, and controls to meet our cybersecurity needs as clearly defined in the Policy. We're appreciative of the effort that the Schneider Electric cybersecurity team put into this project, and look forward to possible implementation services.”

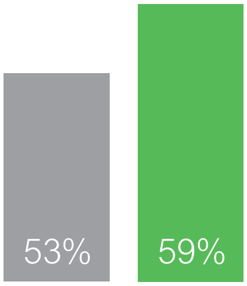
—Kovaios Leonidas, Group IT Director,
Hellenic Petroleum, Greece

The cybersecurity challenge in a connected world

We are in the midst of a technology revolution, and the world as we know it is more connected than ever. But with great connectivity comes great threats. The digitization of every aspect of our lives means that there is a growing reliance on technology not just in our homes but across businesses and industries too. A dependence that will leave us all vulnerable if our connected systems are breached.

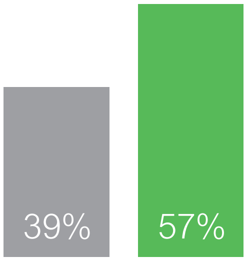
The past decades have seen businesses across the board from Oil & Gas to manufacturing, finance, and data industries embrace the digital revolution. Emergence of new technologies such as cloud computing and the Internet of Things (IoT) has brought down barriers, enabling industries to grow and advance like never before. But these open platforms and interconnected systems have also created more opportunities for cyber criminals, leading to a rise in the frequency of cybersecurity attacks.

Cyber-intrusions don't just disrupt industrial operations, but can affect people's lives, a country's economy or even trigger ecological calamities. Attacks like the Struxnet virus of 2010 and the 2017 WannaCry outbreak have highlighted the urgent need for organizations to upgrade their safety measures and rethink traditional cybersecurity approaches. The necessity for a comprehensive security strategy is now being acknowledged by more and more sectors as an integral part of standard operational risk management.



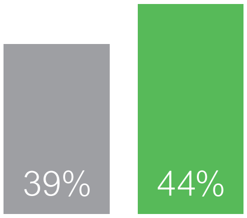
59%

of respondents see criminal syndicates as the most likely source of an attack today, compared with 53% in 2014.



57%

of respondents say the lack of skilled resources is challenging information security's contribution and value to the organization today, compared with 39% in 2014.



44%

of respondents see phishing as a top threat today, compared with 39% in 2014.

88%

of respondents do not believe their information security fully meets the organisation's needs.

*Source: Global Security Survey 2015, Ernest & Young

What makes Schneider Electric the perfect choice?

Cybercrime is ever evolving, with attackers constantly developing advanced technology and skills to compromise your data and systems. The disruption of your operational systems can have a far-reaching and potentially catastrophic impact. Special skills are needed to fortify your defenses while keeping your plant running smoothly.

As a global technology solutions leader, Schneider Electric™ has vast industrial experience working with both Information Technology (IT) and Operational Technology (OT). This experience works to your advantage, as it enables us to collaborate with IT departments and third-party security solutions providers to develop precise and effective cybersecurity solutions that secure your systems without hampering operational efficiency.

Managing cybersecurity requires experts to be well versed with foundational knowledge of the systems they are working to protect. Having worked closely with clients to help plan and set up many of these control systems, our cybersecurity team has gained deep knowledge and insight into what it takes to protect the safety, reliability, and confidentiality of these OT systems. Their familiarity with the system architecture enables quicker identification of security risks and implementation of more targeted solutions, thus preventing wastage and plant downtime. Schneider Electric's cybersecurity professionals are truly the best the industry has to offer.

The Schneider edge:

Cybersecurity Expertise	Technical Expertise	Consulting Expertise
Industry Specific Knowledge: ISA99/IEC62443 – Cybersecurity Specialist	Microsoft®, McAfee®, Symantec®, VMware®	Information Systems Consultancy Practice (BCS Practitioner)
Holistic Knowledge: (ISC)² CISSP, ISACA CISM	Dell®, HP®, Magellis	Enterprise & Solutions Architecture (BCS Practitioner)
Auditing: ISACA CISA, ISO27001 Lead Auditor	GFI LanGuard®, Nessus, Nipper	Project Management: Prince2
Certified Ethical Hacking (CEH): EC Council	Juniper®, Cisco®, Enterasys®, SolarWinds®, Fortinet®, Checkpoint®, Palo Alto®	ITIL v3: Foundation
Certified Penetration Tester (Offensive Security)		Symantec Authorized Consultants

Defense in depth: The Schneider approach

Inspired by the military tactic of delay rather than fighting a single battle, Schneider has adopted a ‘defense in depth’ strategy to prevent or minimize cyberattacks. This multi-pronged defense system adheres to IEC62443 standards, and involves the creation of a multi-layered and multi-technology strategy to safeguard critical systems.

The defense in depth strategy is not just an implementation tool, but a holistic security approach. We don’t just safeguard, but assess, manage and monitor your systems with the help of Schneider Electric’s Portfolio Life Cycle Methodology.

Cybersecurity Portfolio Life Cycle Method

Assess:

Our cybersecurity consultants help you assess and review your systems to detect gaps, risks, uncover any security malpractices, assess your staff's security competencies, provide emergency response services, and more.

Design:

Based on suggestions and reports from the assessment, the system architecture will then be designed, incorporating all the elements and components in keeping with the latest industry standards.

Implement:

We help you design, develop, and maintain your critical infrastructure through a 'defense in depth' based security platform that offers you:

- A central authentication, authorization, and auditing system
- Protection against malware through advance functions like data loss prevention, device control and whitelisting
- Scheduled backups and encryptions of files and folders
- Network and system performance monitoring

Monitor:

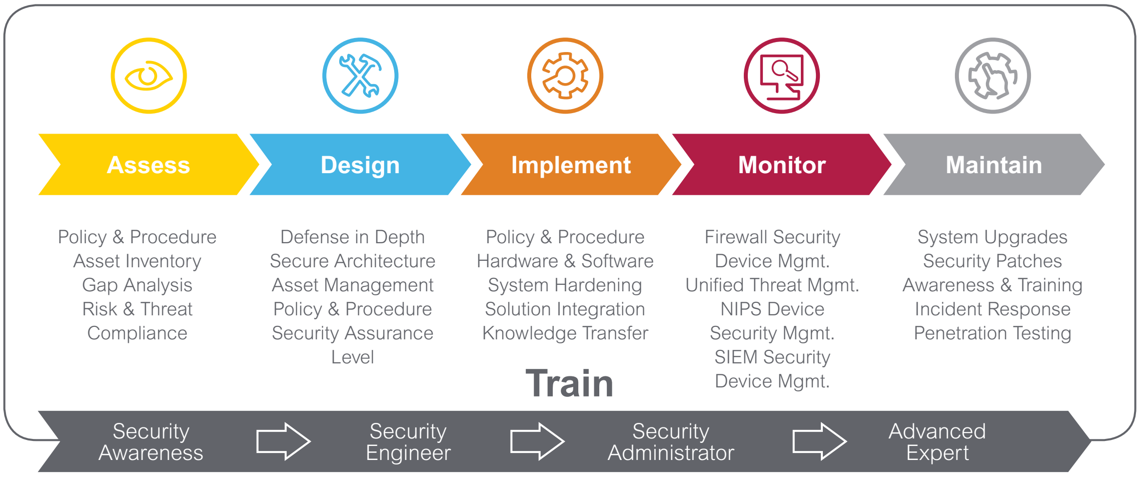
The cybersecurity solutions will be monitored to detect threats, apply solutions as well as to ensure smooth functioning of devices and the system as a whole.

Maintain:

It is critical to continually review and update your cybersecurity protection. We work with your team to ensure that your systems and skills are up-to-date and tested regularly to maximize your security and peace of mind.

Train:

Schneider Electric offers basic to advanced level training programs specifically customized for your security teams. Our courses are designed to educate your team about security practices and introduce a security culture that leads to quick threat response and business continuity.



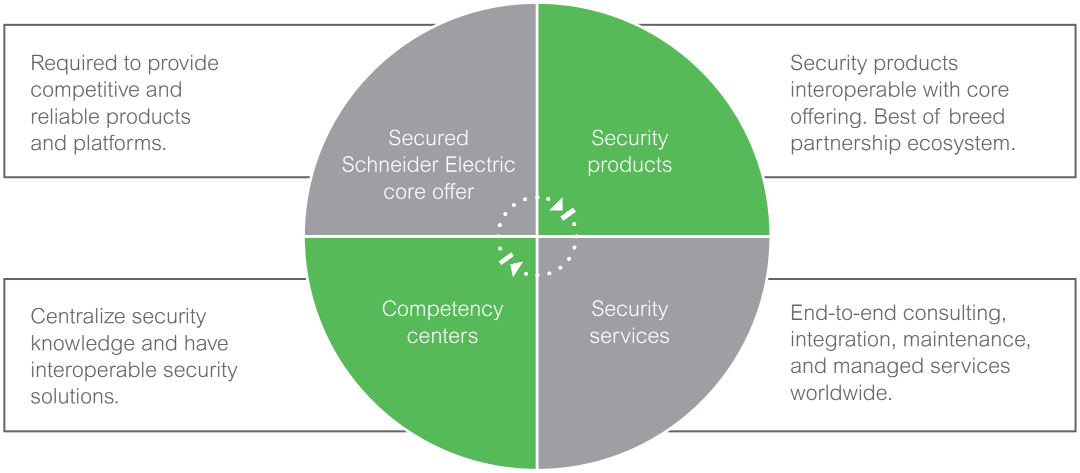
Assess	Design	Implement	Monitor	Maintain
Policy & Procedure Asset Inventory Gap Analysis Risk & Threat Compliance	Defense in Depth Secure Architecture Asset Management Policy & Procedure Security Assurance Level	Policy & Procedure Hardware & Software System Hardening Solution Integration Knowledge Transfer	Firewall Security Device Mgmt. Unified Threat Mgmt. NIPS Device Security Mgmt. SIEM Security Device Mgmt.	System Upgrades Security Patches Awareness & Training Incident Response Penetration Testing

Train

Security Awareness ⇨ Security Engineer ⇨ Security Administrator ⇨ Advanced Expert

Cybersecurity

Our 360* Cybersecurity Solutions



Required to provide competitive and reliable products and platforms.

Security products interoperable with core offering. Best of breed partnership ecosystem.

Centralize security knowledge and have interoperable security solutions.

End-to-end consulting, integration, maintenance, and managed services worldwide.

Our solutions include:

- A dynamic ecosystem of partnerships and platforms including governments, universities, and suppliers that help drive research, policy, and collaborative projects to produce a holistic, security-conscious offering.
- An ISO conformant vulnerability management process that is activated upon external notification, vulnerability disclosure, or customer report.
- An advanced Global Threat Intelligence Center that actively monitors cyberspace for threats to our products and customers.
- 150+ products that are cybersecurity standards certified for electrical and process installations.
- An excellent team of cybersecurity experts who understand your process requirements, enterprise needs, and business environment.

Schneider Electric has earned the industry's first ISA Secure Security Development Lifecycle Assurance conformance certificate.

Life Is On | Schneider Electric

Consider Schneider Electric to simplify your cybersecurity challenges.
schneider-electric.com

Schneider Electric Industries SAS
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex

• 998-20119182_GMA-US