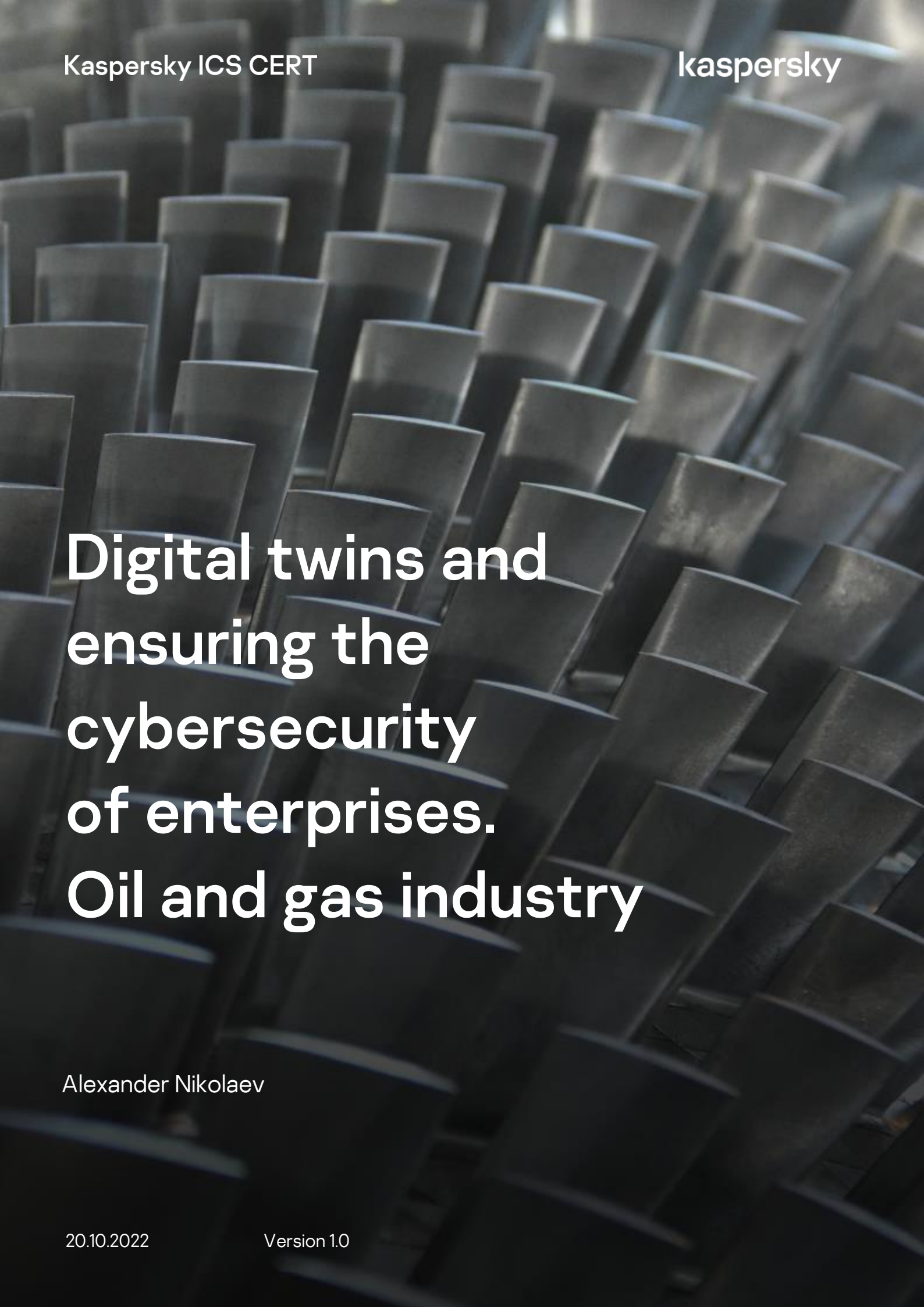
kaspersky



Digital twins and ensuring the cybersecurity of enterprises. Oil and gas industry

Alexander Nikolaev

20.10.2022 Version 1.0

An important aspect of the oil and gas industry is the huge variety of unit and industrial process types. During its lifetime, each enterprise or facility becomes unique, unlike any other, due to various adaptations, refurbishments, and upgrades. For example, oil refining or hydrotreatment units based on the same original design and installed in different refineries at the same time, will be significantly different from each other after a few decades of operation. This is also true of oil well equipment. Even if the same oil production method is used, there are many factors that affect system development. These include oil well locations, oil quality and composition, oil pool characteristics, output, etc. Ultimately, these differences between facilities lead to differences in production process organization, which in turn affect support equipment, the software used, IT and cybersecurity related processes. The evolution of the economic situation and competitive pressure often require further upgrading enterprises and facilities, including their cybersecurity systems. Importantly, the upgrades should not be overly complicated or expensive and should be based on unified, standard designs wherever possible.

Digital twins

A digital twin is a virtual copy of an object, which can be a system (such as a diesel fuel hydrofining system), unit (such as an electric desalting plant), shop (such as an oil and gas production shop), field, or refinery, which accurately reproduces all processes taking place at the original object in real time, so that at any moment in time, parameters of the digital twin's state match the relevant parameters of the physical object's state.

In such a system, all data is converted to digital products, which begin to help choose and compute optimal operating modes, predict operating parameters, and conduct various experiments with minimal risk to expensive physical assets of the company and to people.

Digital twins can vary widely depending on the goals that the company wants to achieve. The complexity level of a digital twin is defined individually in each case, depending on the level of detail, visualization type, functionality, and the depth of analysis.

Digital twins offer additional optimization capabilities, both in terms of controlling an enterprise's production assets and in terms of ensuring its cybersecurity.

It is well known that the main emphasis in ensuring the cybersecurity of enterprises in the oil and gas industry is made on operational tasks, including vulnerability management, attack monitoring and detection, incident response, and restoring systems to normal operation after failures caused by incidents. All of these processes can be optimized using digital twins.

Thus, a digital twin designed in a certain way can help identify equipment that should be the first in line for upgrades, assess possible risks and consequences

of an upgrade in order to make the right plans for upgrades of real-world systems and minimize equipment idle time and the time it takes to perform the upgrade.

Security monitoring and incident detection and investigation can also be optimized using digital twins, for example, to conduct personnel training and cyber maneuvers, to analyze possible consequences of an attack identified, including during the investigation on a real-world object, using information about the attack details identified.

Digital twins are an important development driver for technology enterprises. However, it should be kept in mind that, like any new information technology, digital twins themselves bring new information security and cybersecurity threats to enterprises. The fear of new cyberattacks and data leaks is a sufficiently strong constraining factor for enterprise managers, which holds back production digitalization.

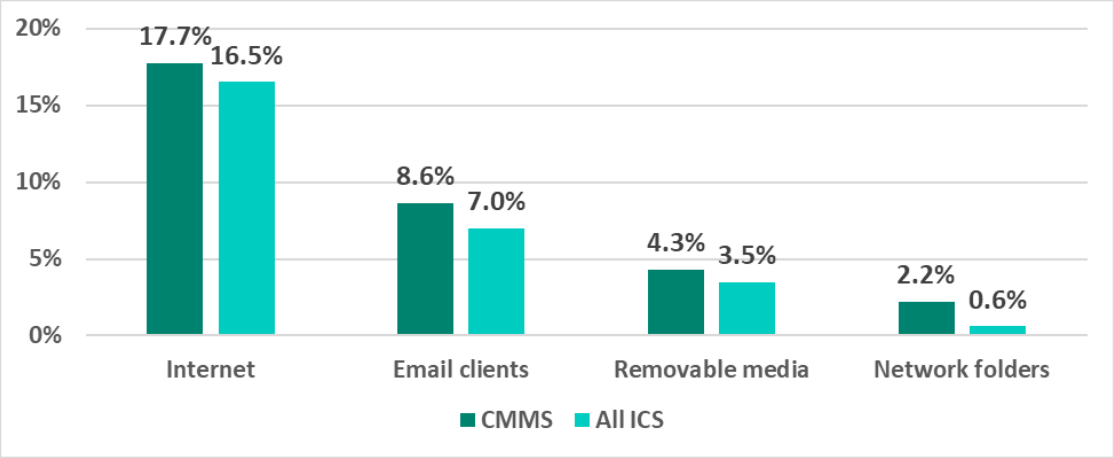
Threats associated with enterprise digitalization

New advanced technologies always come with new vulnerabilities, threats and risks, which have to be neutralized "on the spot". Digitalization using time-tested, proven technologies offers the chance for a more secure implementation of these technologies based on previous experience, even if that experience is negative or irrelevant. In the latter case, we get a chance to correct the situation.

The fear of new technologies is not unfounded. Specifically, our research on the ICS threat landscape shows that implementing new types of systems increases an enterprise's attack surface. This is particularly relevant to systems that require both internet access and access to ICS systems.

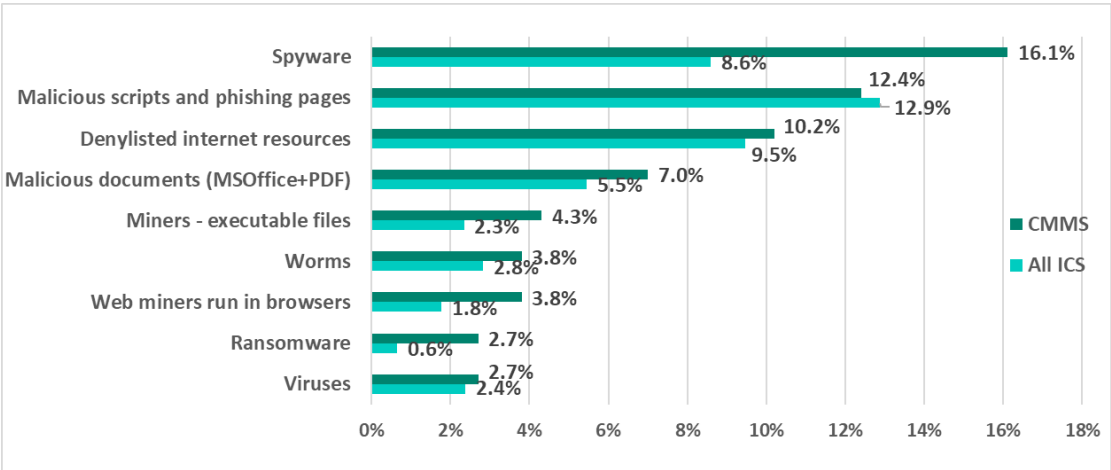
For example, let's look at statistics on computerized maintenance management systems (CMMS). According to our research, 38.2% of such systems were attacked at least once in the first half of 2022.

The percentages of CMMS on which threats from different sources were blocked were as follows:



It can be seen in the above diagram that the majority of attacks are associated with access to internet resources. Email (phishing) attacks rank second, and attacks via removable media (USB flash drives, external hard drives, etc.) are in third place.

The ranking of blocked threats is led by spyware, as well as phishing (phishing pages and malicious documents from phishing emails), which, in most cases, is also ultimately used to install spyware. Next come banker Trojans, ransomware, and self-propagating malware (worms and viruses):

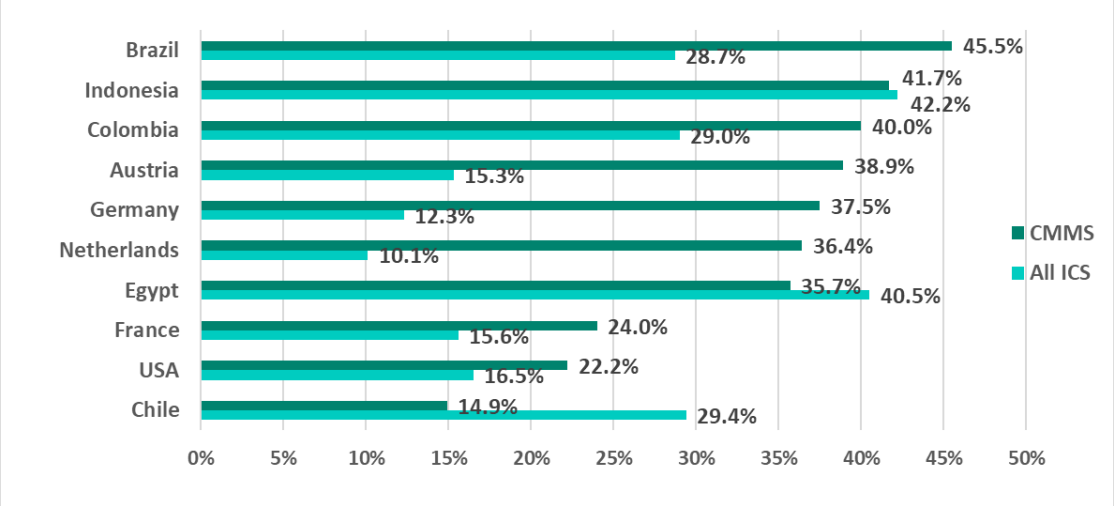


As in the case of other types of IT and OT systems, most blocked threats are random attacks. Their success can be explained primarily by the poor cybersecurity awareness of employees and contractors. Another important factor is mistakes and omissions by IT, OT and information security staff, whose job it is to ensure the enterprise's security. This includes flaws in network architecture and topology, network device configuration, unpatched firmware, operating system and software vulnerabilities, remote access tools left unattended and forgotten, insufficient enforcement of information security

policies related to the use of portable and mobile devices and removable media, and the lack or improper configuration of security solutions.

Sloppy and unprofessional actions of employees allow most random threats to reach the enterprise's OT network and create the conditions for successful targeted attacks.

Tellingly, the TOP 10 ranking based on the percentage of CMMS attacked in H1 2022 includes countries that have traditionally been rated as secure. These countries are not included in the TOP 10 ranking based on the overall percentage of attacked ICS computers in each country:



This demonstrates that using new, "advanced" technologies such as CMMS at industrial enterprises can noticeably increase the attack surface and the relevant cybersecurity risks.

Digital twin security: cyber immunity

The operation of a digital twin requires "live" data from the OT network. Therefore, when deploying digital twins, a high-priority objective is to ensure security – not so much of the digital twin itself as of the object modeled by it. The security of the technical solution used to set up, deploy and connect a digital twin is crucial.

Such solutions should have "innate" security, known as cyber immunity. Cyber immunity is achieved by dividing an IT system into isolated parts and controlling communication between these parts in such a way as to prevent an adversary from developing an attack in ways that are incompatible with system security goals, even if individual components are compromised.

Specifically, the gateway used to receive data from the ICS network and transfer it to internet-facing systems (such as the digital twin's components) should reliably separate the industrial environment from the corporate environment, preventing attacks from getting through to ICS equipment. This means that the gateway should have the relevant cyber immunity property: if any of its components facing the external network is compromised (for example, if a network stack or network interface driver vulnerability is exploited), this should not enable the attacker to gain access to the network interface connected to the protected OT network. A gateway with this cyber immunity property can be based on an operating system that guarantees security domain separation (a "secure OS"). Driver instances, network stacks, file systems and application level software should be separated into different security domains for different network interfaces. The Kaspersky IoT Secure Gateway is an example of such solutions.

Additional security measures and tools may be required to ensure the security of a digital twin. These could include setting up the digital twin in a separate network segment isolated from the corporate network, using classical security solutions (such as antivirus software) and dedicated tools, such as virtualization environment protection tools, as well as other security tools. The specific list of measures and tools will vary from case to case.

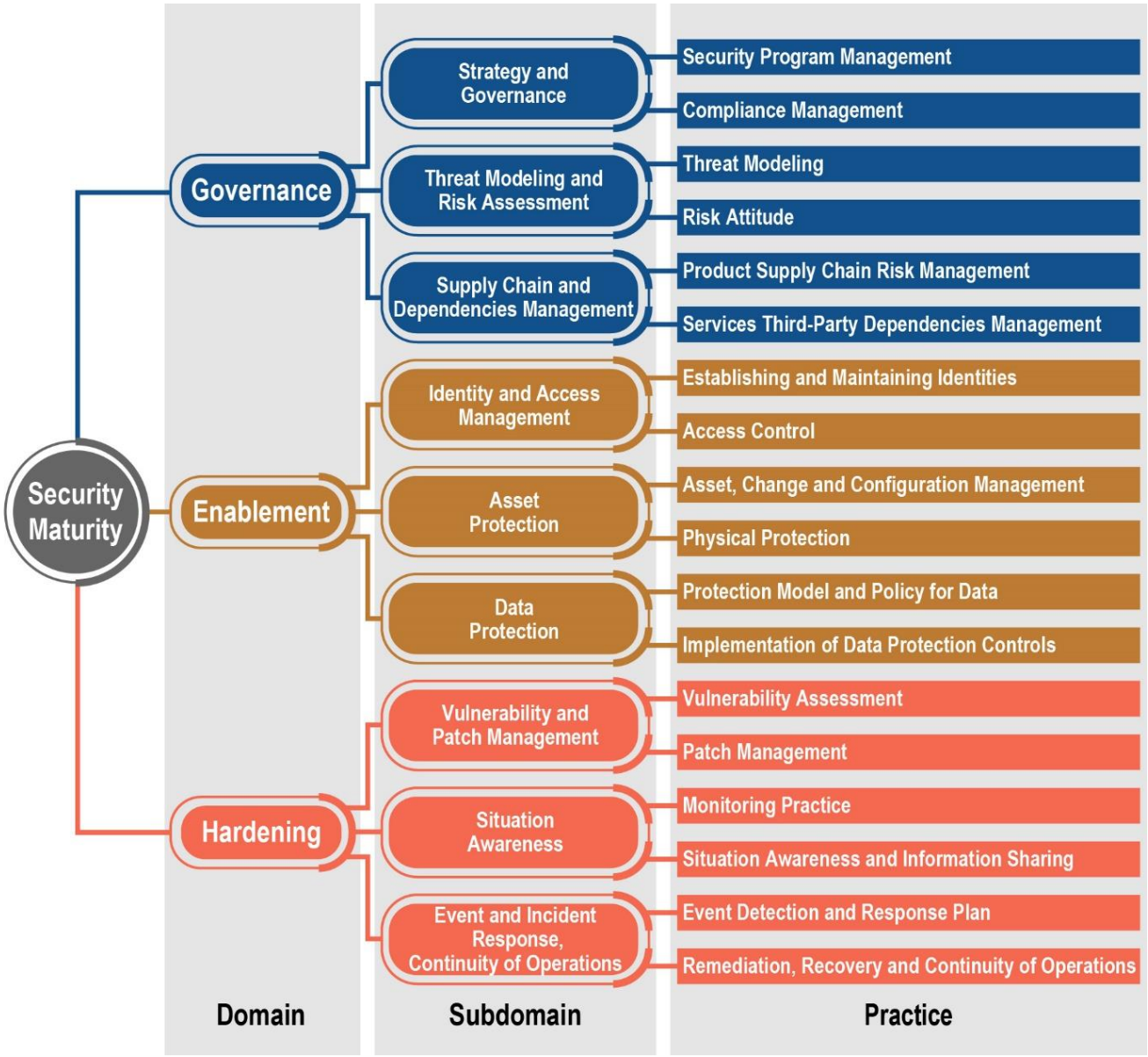
An IoT security maturity model and a security maturity profile based on it provide a tool for developing information security and cybersecurity requirements and can help define the "sufficient security" level for each case.

Security maturity models

Internet of things security maturity model practices are very helpful in setting priorities when planning and organizing cybersecurity processes and assessing the implementation quality of all measures planned as part of these processes.

The goal of an internet of things security maturity model (IIC IoT Security Maturity Model, IoT SMM) is to ensure the choice of methods for protection against cyberthreats that meet the real business needs of the organization. An internet of things security maturity model can equally well be used with more or less sophisticated devices, components of IoT devices and infrastructures, and the infrastructures themselves.

The hierarchy of security practices is the architecture of choice and the nucleus of an internet of things security maturity model:



In terms of an internet of things security maturity model (IIC IoT SMM), as well as a digital twin security maturity model (IIC Digital Twin Consortium IoT SMM), these are practices in the Security Hardening domain. The cost of implementing these practices at oil and gas industry enterprises can vary, depending on the category of the enterprise. Implementing security updates for enterprises in the industry can take a long time, particularly given outdated equipment and outdated IT/OT products. In addition, given the transfer of responsibility (between ICS engineers and information security engineers), these processes can continue ad infinitum.

A digital twin's security maturity level should correlate with the purpose, physical limitations, and the specifics of the enterprise's operation, as well as the security maturity level of the system being modeled. It isn't always worthwhile to build an

expensive digital twin of the entire oil or gas production enterprise. For example, the system's overall security maturity level (covering ICS, different units, etc.) could be too low for this work to be done, or it could be easier to reach a certain location physically by car, or a unit might not be an important or critical facility (such as a booster pump station in a field with low production figures). In such cases, it makes sense to consider designing digital twin functions selectively, implementing only the necessary and sufficient functions.

It's also the same with defining the levels of information security and cybersecurity. The "sufficient security" level must be explicitly defined. That level will be different for each facility and will depend on many factors. It is unacceptable to sacrifice the facility's performance to achieve a sufficient security level. It is also essential to correlate the costs associated with information security services with the future benefits of using them.

Using a security maturity model can help optimize the formulation of the internet of things security objective, that is, define the "sufficient security" level, assess and plan the scope of work that needs to be done to achieve it, with the necessary level of detail, starting from the security domain level and through to specific practices.

Security maturity profile

The "IoT Security Maturity Model Digital Twin Profile" is an industry-specific extension of the document "Security Maturity Model: Practitioner's Guide".

The profile defines maturity parameters that are specific to digital twins. For example, for the Patch Management practice, the minimum maturity level does not require correlation between a security update and the asset (equipment) in the digital twin representation. For the second and third levels, this correlation is defined, and the fourth and highest maturity level requires general representation, correlation, and coordination of installed updates between the digital twin and the physical production process. This means that using the digital twin technology to improve cybersecurity becomes relevant starting from the second maturity level, making it suitable for most industrial enterprises.

It follows that the IoT security maturity profile for digital twins can be used to coordinate requirements for security processes when designing services, for example, at MES level. Such things as geographic distribution, physical protection, technical parameters of the production process can be accounted for to optimize these processes in the future. It should also be noted that process maturity requirements will be different for different types of enterprises (exploration and production, processing and sales, transportation and logistics).

Conclusion

In modern technology-intensive production, IT and large-scale digitalization, and therefore new cybersecurity technologies, are essential to remaining competitive, reducing costs associated with maintaining the existing infrastructure, and increasing net profits.

Digital twins can be among the technologies that offer significant advantages. Examples of new cybersecurity technologies that are necessary for their integration can include cyber immune systems based on secure operating systems, specifically communication equipment offering the necessary security guarantees.

The selection of sufficient security measures and tools can be made easier by using the SMM (Security Maturity Model) methodology. This methodology for making decisions related to ensuring the security of industrial internet of things systems is rapidly evolving in line with the evolution of IT. Specifically, a framework for creating digital twin security profiles has already been developed.

Implementing secure digital twins can in turn open up new opportunities in the future – not only for optimizing the management of the enterprise's production assets, but also for addressing information security issues, specifically vulnerability management for software and hardware-based components of OT systems. This makes the technology particularly valuable for modern enterprises in the oil and gas industry.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com