protect. transform. nurture.

Level 15, Aldar HQ
PO BOX 111787
Abu Dhabi, United Arab Emirates

Operational Technology Cybersecurity FAQ

What are the factors driving the need for OT cybersecurity assessment?

1

Industrial control systems (ICS) are used as an integral part of critical infrastructures industries such as utilities and manufacturing to automate or remotely control product production, handling or distribution and are often installed with a lifespan of several years. These ICS equipment are designed on the notion that they would communicate within small, dedicated networks, disconnected from the public internet and protected by the same physical security controls as the sites and plants where they are located. Even the newly built ICS systems tend to incorporate software principles which have similar underlying assumptions.

With the recent IT/OT Convergence and ubiquitous internet connectivity or often referred to as the fourth industrial revolution characterised by a blend of technologies blurring the lines between physical, digital, and biological spheres. Industrial control systems may still run on independent networks, but true physical isolation is becoming the exception rather than the norm.

Even without a direct connection, malware are bridging airgaps between external and the ICS network. The threat landscape has changed dramatically, placing greater focus on OT Security in organisations that experienced breaches in the recent past. Government and regulators have been quick to react and have started emphasising on compliance with the security standards.

Can we apply the IT cybersecurity concepts and strategies to cover OT environment?

2

One of the fundamental difference between IT as against OT cybersecurity approach is the decentralised nature of the OT environment as against the more convergent centralised nature of the IT environment. A large utility provider, for example, could have control functions distributed over a large geographic area in multiple power generation plants and distribution centres.

The second significant difference is the motivation, objectives and intents of attackers in an ICS environment as against a traditional IT environment. The main goals in an ICS environment are to obtain access to specialised hardware unique to the OT field and to hinder the operational process and disrupt production, public health and safety and in many installations cause physical damage to the equipment.

Lastly, the stages, terminologies and life cycles of a cybersecurity attack on the OT environment are different from traditional IT security. Here, the primary objective of the adversary is to hinder the operational process involving additional stages that include the manipulation of operational and safety factors. In terms of the CIA triad, for ICS environment, the 'Availability' principle plays a more critical role than the other two principles.

Hence, the mitigation strategies need to guide how to tailor traditional IT security controls to accommodate unique ICS performance, reliability and safety requirements to help industry reduce the vulnerability of computer-controlled systems to malicious attacks, equipment failures and other threats. The ICS environment is very resistant to policy changes that might impact the process, and hence cybersecurity strategies developed for data-centric information technology are not necessarily the best fit for protecting operational technology.

What are the types of incidents affecting ICS environments?

3

Possible incidents[1] an ICS may face include the following:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.
- Unauthorised changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorised changes or to cause the operators to initiate inappropriate actions, which could have various negative effects.
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various adverse effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the process of safety systems, which could threaten human life

[1] *Source: NIST Special publication 800-82: Guide to Industrial Control Systems (ICS) Security*

What are the primary security objectives needed to achieve ICS cybersecurity transformation?

4

The requirements that ICS must operate in high-availability, high-capacity modes make the implementation of some common security countermeasures difficult. Special care must be taken to ensure the countermeasures does not impact operations. ICS security professionals in discussion with equipment operators and business must balance security with functionality requirements and creatively apply best security practices while enabling ICS operators to perform their duties unimpeded.

Major security objectives[2] for an ICS implementation should include the following:

- A comprehensive inventory of ICS assets
- Restrict logical access to the ICS network and network activity.
- Restrict physical access to the ICS network and devices.
- Protect individual ICS components from exploitation.
- Restrict unauthorised modification of data.
- Detect security events and incidents.
- Maintain functionality during adverse conditions.
- Restore the system after an incident.

[2] *Source: NIST Special publication 800-82: Guide to Industrial Control Systems (ICS) Security*