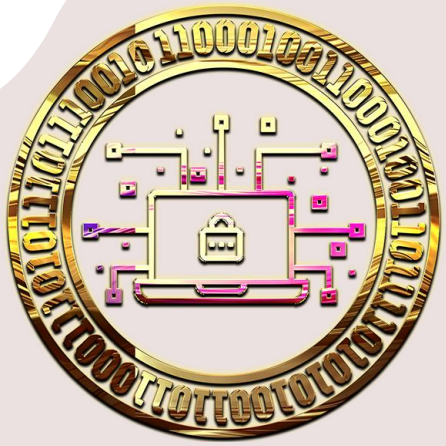

# Industrial Control Systems Security

## INDUSTRIAL CONTROL SYSTEM SECURITY

The growing threat of advanced cyber attacks on critical infrastructure and industrial control systems is a unique challenge for organizations. Government spies, terrorists, and organized crime increasingly target industrial systems, resulting in physical disruption of commercial operations and theft of intellectual property. Disruption of industrial control systems, in addition to destroying expensive equipment, can also lead to interruption of critical operations. These attacks, in turn, can lead to widespread costs and a loss of public confidence in society.

## CONTACT

Phone:
026 368 06249

Website:
unk9vvn.com

Email:
info@unk9vvn.com

## ARCHITECTURAL STUDY

In the first step, the IT and OT architecture of the industrial complex should be thoroughly studied and visualized. Software and management systems, communication protocols and Programmable logic controller (PLC) should also be examined and monitored so targeted penetration tests are implemented on them in terms of cyber security and vulnerable areas are identified, in which all communication arrangements and connected devices should be identified and examined under a magnifying glass.

## VULNERABILITY ASSESSMENT OF DEVICES AND APPLICATION

Software and hardware technologies used in industrial spaces must be thoroughly evaluated for cybersecurity, including operating systems, port-enabled services, databases, and controllable management software. Accurate expertise is the discovery of zero-day vulnerabilities that can occur in both binary and web layers.

### SYSTEMIC CHALLENGES

Industrial control systems include technologies such as data monitoring and data acquisition (SCADA) and distributed control systems (DCS), which are at the core of day-to-day operations in chemical processing, oil and gas production infrastructure and other industries.

These programs include rail switches, SCADA monitors, and programmable logic controllers (PLCs). Infrastructure organizations that are critical to the economy and national security use similar technologies, from banking data centers to power grids and rail transportation.

Many of these systems are increasingly connected to IT networks, exposing them to cyber attacks.

### IT TECHNOLOGY AND OT TECHNOLOGY

IT and OT technology is a custom combination of technology, information, and consulting services from cybersecurity experts that can enable industrial and manufacturing organizations to identify hazards and actively reduce threats. We provide a comprehensive, non-invasive security solution for your entire IT and operational technology (OT).

Our offensive team has extensive experience and knowledge of control systems and is familiar with the ICS and OT space, our experts who are familiar with Threat Intelligence and have unparalleled knowledge of attackers behavior, Perform advanced security tests and help you identify and restrain threats in industrial networks.

### AIR-GAP NETWORK ATTACKS

the Air-Gap network due to its separation from the World Wide Web, has its own range of attacks, which are widespread and dangerous, attacks based on Physical Media, Acoustic Electromagnetic, Magnetic, Electric, Optical and Thermal, which has greatly increased the cyber risks to industrial control systems. these attacks are implemented on the basis of industrial and military networks and have a special secrecy.

Human factors are also the driving force behind Physical Media attacks, so informing human resources in the field of cyber security will be a principle. Also, if the hardware used is not in the right structure, they can form the factors of forming an attack scenario.

## ASSESS NETWORK VULNERABILITIES

The evaluation of the communication network of industrial spaces alone has a list of vulnerabilities that must be thoroughly investigated. For example, in the architecture of Air-Gap networks, there are always unique scenarios and threats that must be addressed separately. Communication protocols that are constantly interacting with sensors and operating devices must also be fully inspected for cyber security.

## INDUSTRIAL PENETRATION TESTING

In industrial penetration testing, the team of experts always try to examine all vulnerabilities in two methods, black box and white box. Here, the focus is on detecting vulnerabilities, not evaluating them. In this regard, the penetration testing process provides more comprehensive and complete vulnerability detection that allows all devices and operating systems, including IoT devices, to be tested.

## RED TEAM SUMULATION

But the highest level of cyber security assessment of industrial complexes can be considered as red team simulation, the red team always tries to fully implement the operational method of all cyber attack teams that have ever attacked industrial complexes, and Makes the problem areas appear and has suitable conditions for the attacker, One of these simulations is the Stuxnet industrial cyber attack.