CIPHER SECURITY

CIPHER SECURITY SCADA/ICS SERVICES

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) are systems that are used to control the Operational Technology (OT) aspect of an industrial process.

There are many sectors using ICS and SCADA systems, the most common of which are the Industrial sector, and the Critical Infrastructure sector.

Due to the special nature of ICS and SCADA networks, a different approach than the common IT-security approach is required to secure such networks.

Cipher Security offers a variety of SCADA/ICS services adjusted to the unique requirements and limitations of the industrial and critical sectors enabling safe, yet effective, SCADA/ICS Penetration Tests.

Such services fall into two major categories: Offensive and Defensive services.

The Offensive service involves several Penetration Tests, while the Defensive offering varies between SCADA APT Risk Assessments, and SCADA Forensics Investigations.

SCADA PENETRATION TESTS

Cipher Security offers a variety of Penetration Tests specially structured for the unique limitations of an industrial/critical infrastructure

FROM LAN TO SCADA

In this test, the Cyber Attacker will demonstrate an intrusion attempt scenario from the corporate LAN to the SCADA/ICS network.

The attacker will endeavor exploiting network separation and defense mechanisms exists between networks, and will attain access to the critical SCADA/ICS network.

The test is considered as very safe to carry out on production networks, and could be concluded with minimal essential communications between the client and the tester.

MAINTENANCE WINDOW SCADA PENETRATION TEST

This sensitive Penetration Test is carried within the SCADA/ICS production network while on prescheduled maintenance window.

The attacker will attempt to gain control over several critical nodes on the network, demonstrating SCADA/ICS Takeover scenario.

The test must be carefully scheduled to the tight maintenance-window restrictions, allowing it to be performed effectively within the allotted time.

Due to the nature of this test, most of Offensive activities are approved per-task, and carried with extreme cautionary measures.

This test is carried out with constant communication between the tester, and client's point of contact.

PRODUCTION SCADA PENETRATION TEST

This sensitive Penetration Test is carried within the SCADA/ICS production network out of maintenance window, in a live production environment.

The attacker will try to gain control over several critical nodes on the network, demonstrating SCADA/ICS Takeover scenario, while carefully considering the sensitive environment and the critical conditions such a test dictates.

Due to the sensitive and delicate nature of this test, all activities are pre-approved, and executed with extreme cautionary measures.

The Production SCADA Penetration Test involves usually longer testing periods, due to extensive communication between the tester and client's point of contact, and the supreme cautionary measures must be taken to ensure a Zero-Risk approach.

COMPLEMENTARY SERVICES

Cipher Security offers a set of Complementary Services to allow a comprehensive SCADA protection suit

SCADA/ICS CODE OF PRACTICE

A complete reference guide structured from Industry Best-Practices, enabling company CISO to instruct business units to secure SCADA infrastructure.

Cipher Security Code of Practice had been implemented in Power Plants and factories worldwide.

SCADA/ICS FORENSICS.

This unique service offers SCADA networks forensic investigation. The investigation is usually conducted to verify whether external and malicious factors exist in the network. Cipher Security had successfully conducted SCADA forensic investigations in power plants and factory facilities.

COMPLETE HARDENING PLAN FOR ENTIRE SCADA AND ICS INFRASTRUCTURE.

The Cipher Security Hardening plan is a set of guidelines calibrated to fit SCADA networks, and dramatically reduce the potential attack surface unhardened components suffer from .

SCADA RISK ASSESSMENTS.

A complete and thorough birds-eye view on current security snapshot of the infrastructure, to help identify risks in an early phase. The assessment does not involve any logical engagement by an external entity, therefore can be carried in any environment.

SCADA SECURE ARCHITECTURE DESIGN.

This service helps CISOs and network architects to securely design a SCADA infrastructure. Using Cipher Security best-practices, the service helps assist the CISO with designing and implementing industrial infrastructure.

All of Cipher Security services are conducted under supreme cautionary measures, to ensure minimal risk or exposure to the Infrastructure Under Test