CHECK POINT + ICS²
ADVANCED INTRUSION DETECTION FOR SCADA

BENEFITS

- Comprehensive cyber-protection for SCADA systems
- Real-time cyber-intrusion alerts
- Zero-day attack detection
- Insider cyber-attack detection
- Passive non-intrusive operation

A NEW BREED OF CYBER-ATTACKS

More organized, better financed and more sophisticated than ever before, today's cyber criminals continuously seek new types of vulnerabilities to exploit. Over the past few years, a new breed of cyber -attack has emerged and is now a major concern to industrial companies. Traditional cyber-attacks gain unauthorized access to data. Now, cyber -attacks target SCADA (Supervisory Control and Data Acquisition) systems that manage and automate industrial processes to gain unauthorized access and sabotage the physical processes. A successful cyber-attack of this sort on a power or water utility could be devastating, resulting in not only financial loss and customer dissatisfaction, but also safety and environmental hazards. Industrial plant security managers need a solution that can effectively detect these harmful intrusions in their control systems. Due to the "always- on" operation of SCADA systems, the solution needs to be one that does not interfere with the plant's industrial processes.

PROTECTING INDUSTRIAL PROCESSES

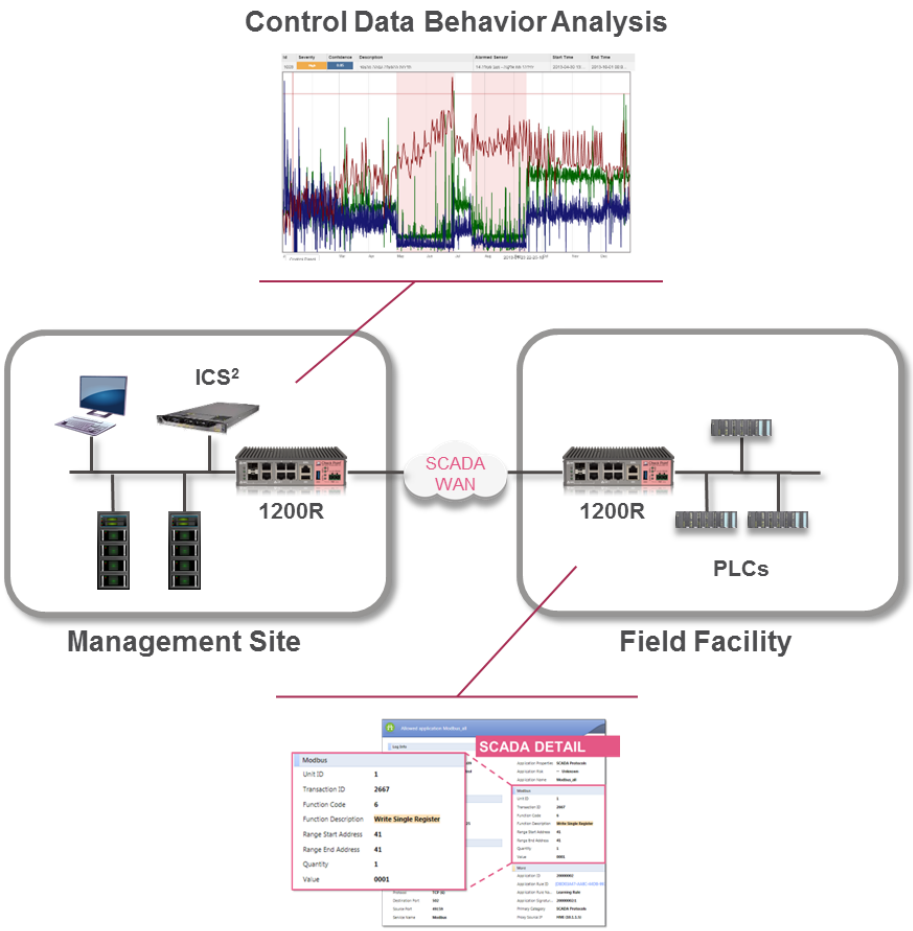
The Check Point SCADA-aware threat detection and prevention system combined with the ICS² Industrial Intrusion Detection System (IIDS) enables your industrial plant security teams to detect sophisticated cyber-attacks on SCADA systems.

- Data Collection – Our joint solution collects the plant's network data (SCADA protocols) and operational data (pressure, temperature, valves status, flow values, etc.), creating a baseline of the normal process operation.
- Analysis – The system then analyzes the plant operational behavior patterns. It creates plant-specific signatures that reflect the unique characteristics of each end device and the relationships between different parts of the system (e.g. between a flow sensor, a valve, and a pressure sensor).
- Detection – Continuously tracking plant operation data and comparing this data to the plant signatures, it searches for anomalous or suspicious behavior.
- Alerts & Forensics - Once it detects an anomaly, the system logs a description, raises an alarm to the security team, and shows a graphic analysis of the anomalous process.

Our joint solution detects sophisticated cyber-attacks designed to be hidden as well as insider attacks made by personnel or partners that have authorized access to the system. Because the system can create its own plant-specific behavior signatures, it can detect cyber-attacks that exploit previously unknown vulnerabilities (zero-day attacks). In addition, it can detect unintentional human errors and misconfigurations that impact plant productivity.

DETECTION INTRUSIONS USING MULTIPLE SOURCES

By monitoring the SCADA network and the operational process data, the Check Point ICS² joint solution (XIDS) can deliver increased accuracy in detecting sophisticated cyber-intrusions. By finding correlations between SCADA network and process anomalies, the system is able to provide cybersecurity teams with detailed information about the field devices affected by a cyber incident and about the nature of the attack.



Advanced detection of cyber-attacks on SCADA systems

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT ICS²

ICS² is a cybersecurity company that develops innovative solutions for protecting critical infrastructure assets from advanced cyber-attacks. Our products and solutions are designed to address the operational needs of companies in energy, water, chemicals and manufacturing industries. ICS² is led by team of experienced professionals with unique expertise in the areas of OT, IT, cyber security, machine learning and big data analysis. For more information, visit www.ics2.com.

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com