Symantec

CASE STUDY

Business

- Partner: KORAMIS
- Website: http://www.koramis.de
- Sector: Industrial Security
- Headquarters: Saarbrücken, Germany
- Employees: 35

Challenge

A key partner of Symantec in the growing market for IoT security, KORAMIS is one of the leading systems integrators in the field of industrial security and is considered a renowned specialist for the protection of IIoT environments against malware and cyber attacks.

Solution

- Symantec Critical System Protection
- Symantec Industrial Control System Protection

Services

- Holistic consulting for protection of critical industrial environments
- Signature-free protection of historically grown, heterogeneous production environments against advanced threats and cyber attacks
- Malware analysis, monitoring and policy enforcement for secure integration of removable media in IIoT environments
- Extension of the EOL/EOB of critical control systems

KORAMIS

Security for the Industrial Internet of Things (IIoT)

How KORAMIS uses Symantec technology to protect demanding industrial networks

Digitalization of industrial environments is advancing rapidly: Those who want to hold their ground in today's global competition must harness the power of open, networked infrastructures and flexible, increasingly cloud-based technologies. IIoT (Industrial Internet of Things) allows businesses to seamlessly integrate production facilities, web-enabled endpoints and highly complex embedded systems.

This is a positive development in terms of the companies' productivity, efficiency and competitiveness. However, from a security point of view, the opening-up and expansion of networks is quite problematic: Each new system increases the companies' attack surface, as well as the complexity of their infrastructures.

The consequence: Industrial environments are becoming increasingly targeted by cybercriminals worldwide. Attackers sabotage production systems via multi-stage attacks, zero-day exploits and advanced persistent threats, attempting to steal critical know-how, to crash sensitive systems or to extort companies with threats of damage.

Securing IIoT environments often proves a considerable challenge for even experienced security integrators. While traditional companies' business IT can usually be protected with proven enterprise security best practices, production networks obey their own rules: Historically grown, they combine a wide variety of hardware and software platforms with a colorful mix of more or less exotic operating systems: from Windows NT to various Linux derivatives to proprietary, non-serviceable embedded systems.

From ICS developer to Ilot security specialist

Symantec partner KORAMIS has been specializing in the protection of IIoT environments for over a decade, and belongs to a small circle of the world's leading experts in this field. Among the most important distinguishing features of Saarbrücken-based KORAMIS is that it was originally founded as an integrator and programmer of industrial control systems (ICS) and can thus now best assess the circumstances, requirements and priorities of manufacturing companies.

Michael Krammel, Managing Director of KORAMIS, explains: "As former ICS integrators we have a comprehensive knowledge of our customers' processes and understand the importance of the stability and availability of IT in industrial environments. In Symantec we have found an important strategic partner for this demanding market. Their host-based systems reliably protect our customers' production plants without disrupting operations, and prevent targeted attacks and dynamic threats in the process."

"In Symantec we have found an important strategic partner for this demanding market. Their host-based systems reliably protect our customers' production plants without disrupting operations, and prevent targeted attacks and dynamic threats in the process."

—Michael Krammel, Managing Director of KORAMIS

KORAMIS supports customers from the industry with a broad solutions and consulting portfolio to protect their infrastructures. In addition to protection against internal and external attacks, the focus is increasingly upon reliable adherence to legal compliance provisions, such as the German IT-Sicherheitsgesetz, the KRITIS specifications and the European NIS directive.

"Our projects usually begin with a detailed assessment of the existing systems and applications. In doing so, we also get an overview of their vulnerabilities and carry out penetration tests in order to locate all possible points of attack", says Daniel Buhmann, Business Unit Manager Security Solutions at KORAMIS. "We thus provide the prerequisites for a sound risk management right at the start of the project – and can decide upon viable technical and organizational measures to protect the systems."

The key component of the IIoT security architectures developed by KORAMIS is Symantec Critical System Protection (CSP). This compact, host-based security solution combines innovative sandboxing for applications with integrated intrusion detection & prevention, and powerful malware filters to harden industrial systems and protect against all prevalent threats.

"CSP is optimized for ICS, SCADA and embedded systems with low computing power and works independently of the operating system, without signatures, updates or internet connection", explains Olaf Mischkovsky, IIoT expert at Symantec. "This solution protects twenty-year-old Windows NT servers just as reliably as it does the latest embedded systems in a smart car, without affecting the operation in any way."

Isolation of applications and application whitelisting

To help prevent compromised applications from causing damage to the ICS, Symantec CSP supports granular, policy-based whitelisting. This ensures that only approved applications run on the host at all times, and only in the prescribed manner. Symantec CSP automatically moves unknown services and applications to an isolated sandbox with minimal privileges. Thus they have no access to the code or functions of other applications, nor will they be able to pervade the network or download malicious code from the Internet.

Integrated IDP functionalities

In addition to application control, KORAMIS uses Symantec CSP as a powerful intrusion detection and prevention solution for customers in order to reliably identify and proactively prevent suspicious activity on the host. "CSP comes with thousands of predefined rules by default and constantly monitors files, settings, logs, events and application behavior on the host system," Daniel Buhmann explains. "In the event of anomalies and policy violations, the system automatically triggers an alert and prevents all corresponding activity. This way common attacks can be stopped reliably."

The combination of hardening, sandboxing and whitelisting allows KORAMIS to control network access in a customer's network, to close backdoors and minimize inbound and outbound traffic. Even zero-day exploits and targeted malware attacks can be reliably prevented by means of restrictive application control in order to protect customers' ICS hosts and network environments.

> “CSP comes with thousands of predefined rules by default and constantly monitors files, settings, logs, events and application behavior on the host system.”
>
> —Daniel Buhmann, Business Unit Manager Security Solutions at KORAMIS

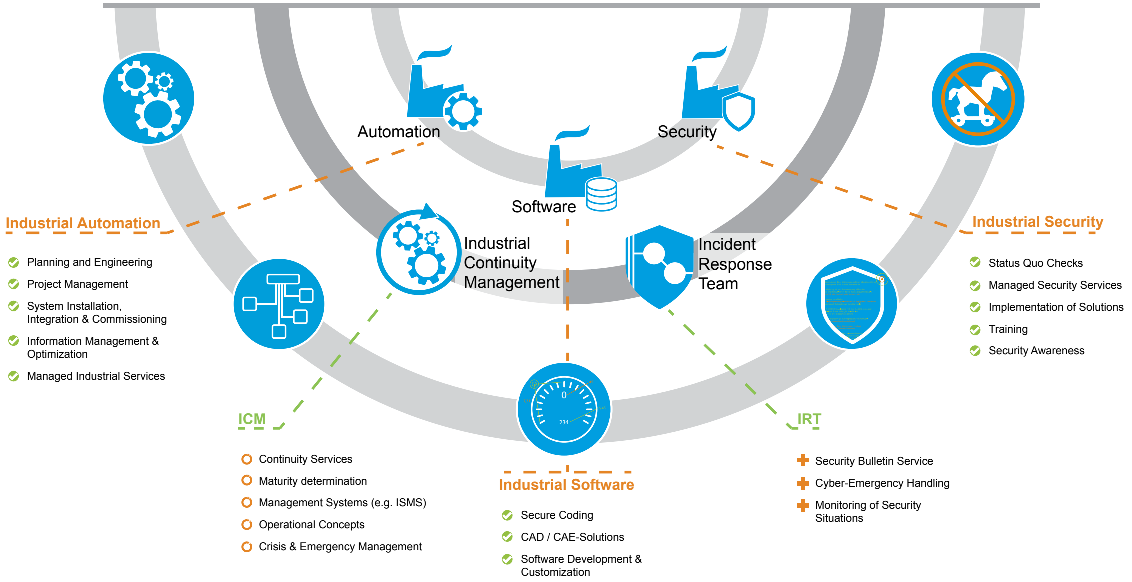
This is all the more important as signature-based filters are not a viable alternative in industrial environments: Most industrial control systems already reach their limits due to the high CPU requirements. In addition, the often outdated operating systems cannot reliably be protected by signatures, as many manufacturers weed out old patterns after a few years in order to prevent the pattern files from becoming too large.

Attack vector removable storage devices

In addition to Symantec CSP, KORAMIS experts typically recommend that their customers use a data lock, such as the Symantec ICSP (Industrial Control System Protection). This compact and robust station allows users to make a quick security check of their USB removable storage devices before connecting to the network. The data storage device is scanned within seconds with a number of powerful technologies: The ICSP Station combines traditional signature-based methods with reputation analysis, machine learning and innovative sandboxing to reliably identify malware and advanced threats.

“Because most production networks are not connected to the Internet, infected USB sticks are among the most dangerous entry points for malware in the industry,” explains Olaf Mischkovsky. “The ICSP allows reliable control of this attack vector. In particularly critical environments, customers have the option to install a small agent on their production systems to ensure that only ICSP-certified media can be used. This provides operators with an extra measure of security and prevents employees from simply forgetting to have their sticks checked.”

As forgetful, careless or simply uninformed employees are among the most important risk factors, customised awareness and security trainings are a fixed component of most KORAMIS projects. KORAMIS CEO Michael Krammel explains: “Until a few years ago, the cyber security was not on many industrial companies’ agenda and they didn’t sensitize their employees to the dangers. But with security now increasingly focused upon due to the growing number of attacks and ever stricter legal requirements, this attitude has changed significantly, and the willingness to invest in state-of-the-art technology is higher than ever.”


Automation
Security
Software
Industrial Continuity Management
Incident Response Team
Industrial Automation
Planning and Engineering
Project Management
System Installation, Integration & Commissioning
Information Management & Optimization
Managed Industrial Services
Industrial Security
Status Quo Checks
Managed Security Services
Implementation of Solutions
Training
Security Awareness
ICM
Continuity Services
Maturity determination
Management Systems (e.g. ISMS)
Operational Concepts
Crisis & Emergency Management
Industrial Software
Secure Coding
CAD / CAE-Solutions
Software Development & Customization
IRT
Security Bulletin Service
Cyber-Emergency Handling
Monitoring of Security Situations

KORAMIS – a success story in the truest sense

As a renowned specialist in the protection of Industry 4.0 environments, KORAMIS has grown rapidly in recent years. While the focus in the first few years in the security business was on energy providers and chemical companies in the DACH region, the Saarbrücken-based company is now operating on a global scale and serves big and small manufacturing companies across all sectors. In addition to securing ICS and SCADA systems, KORAMIS is also very successfully involved in the booming IoT security market – another segment where Symantec's host-based solutions can be exploited to the full.

To learn more about Symantec Critical System Protection, please visit
https://www.symantec.com/products/embedded-security

To learn more about Symantec Industrial Control System Protection, please visit
https://www.symantec.com/solutions/industrial-control

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.