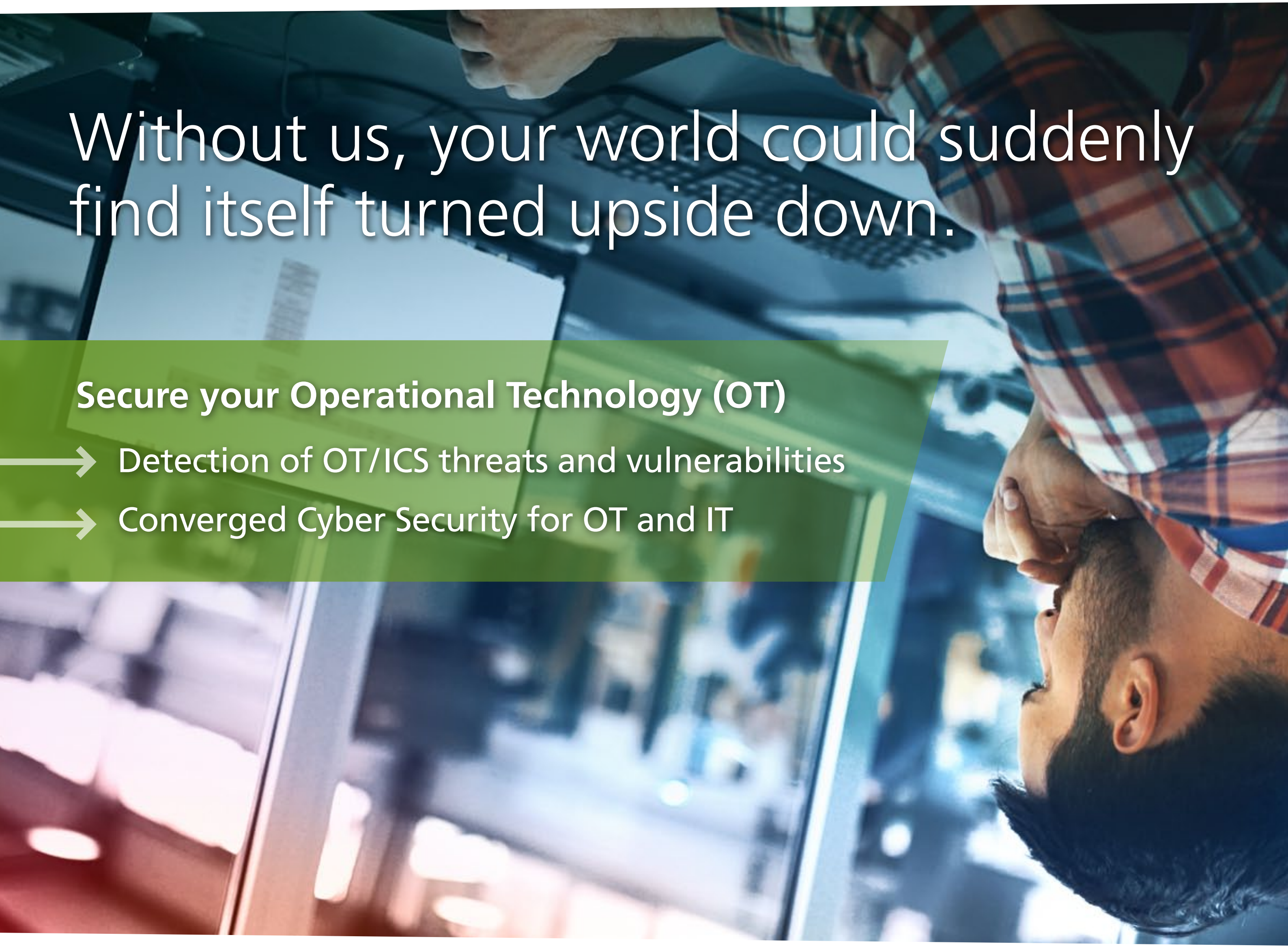
RADAR
CYBER SECURITY



Without us, your world could suddenly find itself turned upside down.

Secure your Operational Technology (OT)

- Detection of OT/ICS threats and vulnerabilities
- Converged Cyber Security for OT and IT

IT Security
made in Europe

OT and IT Security

The learnings from Petya & WannaCry

OT (Operational Technology) is highly interconnected nowadays – both within OT and with IT (Information Technology). Embedded systems communicate independently with one another, plant operators monitor and control remotely, cloud planning systems calculate job steps and machine scheduling, maintenance personnel gain access and make changes to configurations from all over the world.

Nowadays, protective mechanisms for OT and IT are at least just as important as the physical measures taken to protect a factory. Threats can penetrate and manipulate systems via network connections. Malware can completely paralyse vast areas and also cause immense physical damage, as well as putting life in danger.
It was clear that factories and plants were the targets of cyber attacks long before the numerous production failures experienced by the multinationals in 2017.

Particular constraints are applicable to OT and IT security in industrial production. Production plant control technology has real-time requirements that make it difficult if not impossible to modify the systems. This means, for instance, that software patches on the systems, malware scanners and antivirus programs can impair functionality. There is also the fact that hardware and software are used for comparably long periods in production, in stark contrast to other applications.

Sophisticated security concepts have to be found for the production environments so that OT and IT security can be put into practice both for new systems and old equipment.

The latest incidents

Petya & NotPetya ransomware paralysed brand-name chocolate and cosmetics manufacturers, shipping companies, other multinationals and authorities.
The attacks were designed to cause chaos and achieved their aim in a number of multinational groups and national infrastructures worldwide. The ransomware spread quickly through the organisations and paralysed many areas by exploiting vulnerabilities in the Microsoft Windows operating system. As soon as their computers were affected, users received a ransom demand, payable in bitcoins. Petya & NotPetya have caused losses running into millions for these affected companies, mostly due to production stoppages sometimes lasting a week, or by bringing other critical business processes to a standstill.

WannaCry ransomware infected 230,000 devices across all industries in more than 150 countries.
One of the biggest ransomware attacks so far initially started in older Windows systems (Windows XP and Windows Server 2003). The malware apparently used a security flaw in Microsoft's SMB protocol. The loophole also goes by the name "EternalBlue", and was exploited by the American NSA for its own purposes for more than five years. After a security incident at the NSA, the hacker group known as the "Shadow Brokers" found out about "EternalBlue" and revealed the vulnerability. Organisations from all industries were paralysed, especially critical infrastructures, car manufacturers, logistics and telecommunications groups.

APT attack on a steel works
Using a combination of social engineering (Scenario 3) and email data theft (spear phishing attack), intruders gained access to the office network of a steel works. From there, they worked their way into the production networks. They disabled control systems and parts of the plant. A blast furnace could not be shut down as normal and remained in an "undefined" state. The furnace suffered massive damage.

Attack on production networks by Dragonfly
Dragonfly is a group that has already attacked several dozen companies in Germany. One of their attack campaigns targeted manufacturers of industrial control system software. They inserted the malware program Havex into the installation files on the download servers. This allowed them to gather specific information about the industrial control systems sector, including details of the devices and systems used in production networks. The Federal Office for Information Security (BSI) expects the perpetrators to make use of this information in further attacks and is following the attack campaign together with Germany's Federal Criminal Police Office (BKA).

Risk scenarios

Scenario 1
Attackers install malicious programs and block all production and logistics operations. Production and capacity utilisation data are inspected, and application and system data manipulated. In a worst-case scenario, a misdirected machine could cause physical damage in its vicinity.

Scenario 2
Commands to industrial robots are sent via embedded systems, which are usually connected to a programmable logic controller. The control components are linked to the Internet. An attacker can therefore read application and system data, install data packets designed to sabotage the production lines, related systems or even the entire corporate IT infrastructure.

Scenario 3
Social engineering: attackers exploit human characteristics, such as helpfulness, trust, curiosity or fear, to manipulate employees and gain access to data, to circumvent security precautions or to install malicious code on their computers. Their objective is to spend time undisturbed inside the company's network.

Industry 4.0 = Security 4.0?

Industry 4.0 is the term used to describe the fourth industrial revolution, the future of industrial production based on the "Internet of Things". Its characteristics include a high level of product individualisation and an ability to simultaneously take account of the requirements of dynamic (high-volume) production. Factories are turning into smart factories. Processes are being controlled and coordinated in real time across national and corporate boundaries. To succeed, it will require the standardisation and modularisation of the individual process steps and the programming of virtually editable models of these modules. Product individualisation enables companies in many industries to produce a large number of product variants at low cost, and in doing so, to satisfy individual customer needs. Companies can react flexibly to market developments, to rapid changes in product requirements or fluctuating commodity prices. This high level of adaptability is accompanied by an improved utilisation of production capacities, whilst the flexible management of resources serves to improve overall operating efficiency. More accurate calculations mean that less material is needed, which reduces inventory and manufacturing costs.

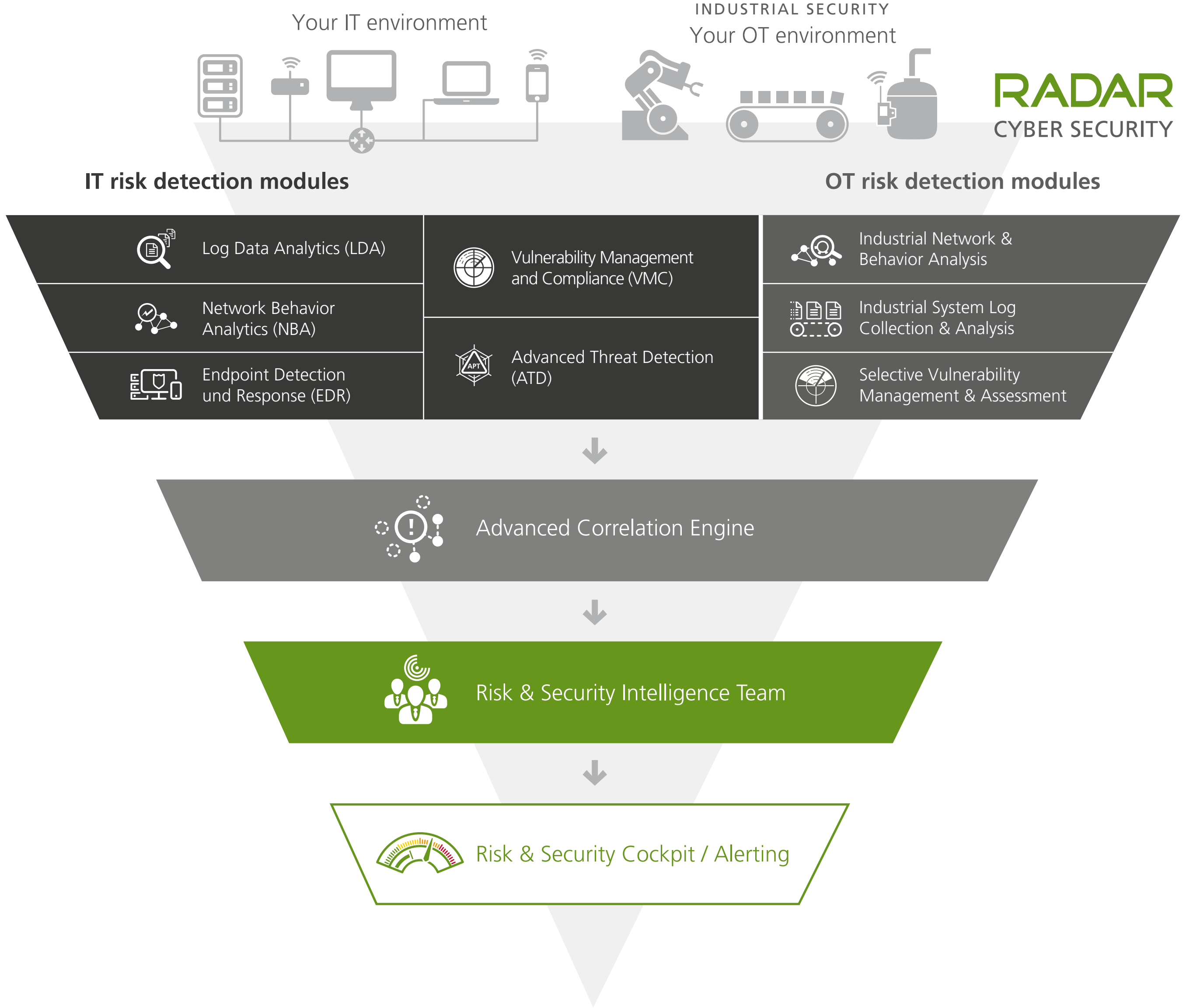
Industry 4.0 means opportunities and challenges. Integrating the concept within an organisation means opening up the company's IT infrastructure, making it more susceptible to errors and more vulnerable to attack. Unfortunately, intruders will not stop trying to find new ways of breaking into business networks. Attacks specifically designed to penetrate industrial control systems present a threat to production facilities. Infected computers can be controlled remotely and their data stolen. Other linked or built-in devices such as microphones, keyboards and monitors can also be spied on. As the malware exploits unknown security holes, firewalls and network monitoring software are unable to detect it.

OT and IT security nowadays: the concept of converged cybersecurity for OT and IT

To secure OT and IT, manufacturing companies must establish an effective and efficient security management system for their "smart factories". Traditional protection strategies such as firewalls, antivirus software and network monitoring software only ever protect specific, small parts of the IT infrastructure from potential attacks. Attackers, on the other hand, focus on detecting new and unknown security holes.

A broad-based protection strategy counteracts this. A wide array of risk identification modules correlates millions of security events and remains constantly on the lookout for new threat scenarios. The results of the correlations are then analysed by a team of experts with constantly updated specialist knowledge and skills. The analyses must be able to provide a readily available overview of the critical information that would quickly reveal the presence of a real attack.

The concept of converged cybersecurity for OT and IT comprises three components: (1) Detection tools for the automated collection and analysis of all data potentially relevant to security from the entire OT and IT landscape, and for correlating this data to acquire knowledge about its relevance to a possible security risk; (2) analysis and assessment work carried out by security experts; and (3) preparing the information for further, customised processing, such as in risk elimination, or also possibly as a source of information for different internal target groups regarding the current status quo of OT and IT security in an organisation.


Your IT environment
INDUSTRIAL SECURITY
Your OT environment
RADAR
CYBER SECURITY
IT risk detection modules
OT risk detection modules
Log Data Analytics (LDA)
Network Behavior Analytics (NBA)
Endpoint Detection und Response (EDR)
Vulnerability Management and Compliance (VMC)
Advanced Threat Detection (ATD)
Industrial Network & Behavior Analysis
Industrial System Log Collection & Analysis
Selective Vulnerability Management & Assessment
Advanced Correlation Engine
Risk & Security Intelligence Team
Risk & Security Cockpit / Alerting

Component 1: excellent detection tools

Comprehensive protection for the OT and IT infrastructure requires the use of automated risk detection modules and an Advanced Correlation Engine.

IT risk detection modules

Automated IT risk detection modules include:

» Log Data Analytics (LDA): creating an alert in the event of security issues or potential risks through the collection, analysis and correlation of logs from various sources.

» Network Behavior Analytics (NBA): High performance analysis of the network traffic is used for signature- and behaviour-based detection of dangerous malware, anomalies and other network traffic risks.

» Vulnerability Management and Compliance (VMC): a 360-degree overview of potential security flaws in operating systems and application software, and the monitoring for anomalies of all data flows on the network.

» Advanced Cyber Threat Detection (for Email and Web, ATD): the deployment of next-generation sandbox technologies to detect “advanced malware” in emails and web downloads.

» Endpoint Detection and Response (EDR): the collection, analysis and correlation of server and client logs as well as rapid alerting when attacks, misuse or errors are detected.

» Software Compliance (SOCO): automated monitoring of adherence to compliance regulations and the immediate reporting of breaches to minimise compliance risks.

OT risk detection modules

Automated OT risk detection modules include:

» Industrial network & behaviour analysis: Identifying protocols and applications in network traffic, analysing extracted data and visualising anomalies to create clarity regarding the ongoing situation. The DPI (deep packet inspection) solution R&S®PACE 2 classifies and decodes the data streams down to the content layer. Authorised protocols are thus also checked for hidden attacks. Security problems originating from infected machines, incorrect configuration or potential cyber attacks are detected.

» Industrial system log collection & analysis: Collection, analysis and the correlation of logs from different sources in the OT environment, for warning when there are security problems or potential risks.

» Selective vulnerability management & assessment: Vulnerability scans (vulnerability management and assessment, VMC) are run in selected areas and environments. Scanning does not cause any data availability or integrity problems.

State of the art Advanced Correlation Engine

Signature-based intrusion detection is often ineffective on the types of attack being carried out today. Traffic is therefore not tested based on patterns but on behaviour within the IT system. Unusual behaviour becomes visible when all security events are correlated with each other on two levels: at the level of a risk identification module and at the level of cross-correlation of the information from different modules.

Advanced correlation is also a necessary requirement for recognising the suspicious behaviours of concealed or as yet unknown forms of attack.

To ensure the success of the Advanced Correlation Engine in detecting risks and warning of critical situations, rules, policies and self-taught algorithms and statistical models must be applied and updated regularly.

Component 2: expert analysis and evaluation

Automatically collected security information must be assessed by highly specialised experts. They analyse, evaluate and prioritise the results and, using the very latest information and knowledge, are responsible for the ongoing development of automated mechanisms. All the results should be seen as part of a big picture, and the analysis should take into account events in the particular IT and OT infrastructure as well as the latest developments inside and outside the industry.

Teams of experts must also act quickly to provide precise instructions on troubleshooting and they must constantly adapt all the policies and rules used by the risk identification modules and advanced correlation engines to identify and eliminate vulnerabilities and new types of attack without delay.

Component 3: information processing

Intelligence on the latest OT and IT security situation within the company should be presented centrally and in the form of detailed, easy-to-understand reports and statistics for both the internal security teams as well as for senior management. Information should focus on the most critical events to ensure that remedial work is targeted specifically at what matters. In urgent scenarios, an alert must be sent to defined recipients.

The early warning system for your OT and IT – as a solution or a manged service?

The automated collection and analysis of security data, the correlation of all the information, the continuous tailoring of rules and models and the interpretation of the information collected requires time as well as personnel and financial resources. This investment might pay off for very large organizations. However, many companies are not in a position to make such efforts over the long term in addition to their normal business operations. This is where the expertise and tools of an external specialist are worth looking at.

Radar Cyber Security is the European market leader for proactive OT and IT security monitoring and risk detection as a solution and as a managed service. We offer businesses a complete package for implementing continuous security monitoring across their OT and IT infrastructure.

Companies who outsource their OT and IT security services do not have to transfer security-related and therefore highly sensitive information to the outside. Radar Cyber Security provides an on premise hardware appliance, including all modules and the Advanced Correlation Engine. It collects and analyses all automatically obtained information. The hardware appliance operates within the network, making sure that no security-sensitive data ever physically leaves the company. Radar Cyber Security continuously configures and maintains all the modules. The rules governing risk detection and correlation are constantly updated.

All important information, free from false positives and false negatives, is ultimately sent to the Risk & Security Cockpit. Reports and statistics are made available in the desired depth of detail. In urgent cases, alerts are sent via the Cockpit, via email and even as a push message to mobile phones. The internal IT security teams can contact the experts at any time via a messaging and feedback system. A built-in Business Process Risk View highlights those business processes that are most vulnerable to OT and IT security threats, adding the finishing touch to this fully-featured and resource-saving solution.

RADAR
CYBER SECURITY | Safeguard your digital journey.

Radar Cyber Security is Europe's leading technology company in the field of Detection & Response. In focus: The early detection of IT and OT security risks for corporations and public authorities offered as a Solution or a Managed Service. The cutting-edge, inhouse-developed technology platform is the basis used for building up a client's Cyber Defense Center (CDC) or it is used in combination with our expert analysts, documented processes and best practices as CDC as a Service. The result: Highly effective and efficient improvement of IT security and IT risk management, continuous IT and OT security monitoring and an overview of security-related information throughout the entire IT and OT landscape of an organization.

Radar Cyber Security HQ
Zieglergasse 6
1070 Vienna
Austria

Phone: +43 (1) 929 12 71-0
Fax: +43 (1) 929 12 71-710
Email: sales@radarcs.com
Web: www.radarcs.com

Radar Cyber Security Deutschland
Taunustor 1
60310 Frankfurt am Main
Germany

Phone: +49 (69) 2443424 655
Fax: +49 (69) 2443424 150
Email: sales_germany@radarcs.com
Web: www.radarcs.com/de

Radar Cyber Security Schweiz/Liechtenstein
Schaanerstrasse 1
9490 Vaduz
Liechtenstein

Phone: +423 237 90 90
Fax: +423 237 74 99
Email: sales_switzerland@radarcs.com
Web: www.radarcs.com/ch

Coverbild: istock.com/gilaxia

PUBLIC