RADAR
CYBER SECURITY

Trusted cybersecurity from a European source

FOR IT AND OT

Cyber Defense Center (CDC) as a Service

Cyber Defense Center solutions for setting up:

– In-house CDC

– MSSP providership

Part of MATERNA
Information & Communications

IMPRINT

Published by:
RadarServices Smart IT-Security GmbH, Zieglergasse 6, 1070 Vienna
FN371019s, Chamber of Commerce Vienna.

Credits: p.14 NicoElNino/Shutterstock.com, p.19 istock.com/xijian, p.20 Arnold Mike, p. 24 istock.com/yoh4nn, Back cover: TZIDO SUNS/Shutterstock.com

Safeguard your digital journey.

Your cyber resilience, our solution

YOUR BENEFITS

- ✓ Risk mitigation: Real-time mapping of the extent where your IT/OT infrastructure is at risk, including specific recommendations for response
- ✓ Cost optimization: Cost transparency while strengthening your cyber resilience
- ✓ Compliance: Adherence to legal requirements and compliance rules
- ✓ Focus on your core business
- ✓ Return on (Security) Investment

OUR PRODUCT

- ✓ One of the largest Cyber Defense Centers (CDC) in Europe, based on state-of-the-art inhouse developed technology
- ✓ Over 10 years of experience in the development and operation of our CDC
- ✓ Integration of proprietary technology experience for our customer organizations

OUR PROCESSES

- ✓ Converged presentation of your IT and OT security situation within central interface
- ✓ Data remains in your company at all times: compliance with highest standards of data protection without software backdoors

OUR TEAM

- ✓ In-depth expertise coupled with state-of-the-art technology

OUR PRODUCTS

RADAR SERVICES

All-in-one service from a single source.

CDC as a Service

RADAR SOLUTIONS

Our technology. Your experts.

Setting up a Cyber Defense Center
to protect your organization

Setting up a Cyber Defense Center
to offer Managed Security Services

RADAR SERVICES

All-in-one service from a single source.

CDC as a Service

RADAR Cyber Security establishes a Cyber Defense Center (CDC) in your company and takes charge of its ongoing operation. It is ready made in no time - aligned with trial and error principles and based on the latest RADAR developed technology. Service managers in your national language, clear regulations and documentation facilitate the creation of structures and procedures as well as communication between your company and RADAR Cyber Defense Center.

Recommended core modules:

LDA NBA VMC

Recommended add-on modules:

ATD EDR

The competencies of our Cyber Defense Center

- ✓ Exclusive focus on threat detection
- ✓ Advantage of cross-sectoral analogies and use cases
- ✓ Analysis findings modify policies and rules of automated risk detection on a frequent basis
- ✓ Each incident description comes with a recommendation from analysts for risk elimination

IT and OT detection at a glance

RADAR Cyber Security collects and analyzes risks in the IT and OT infrastructure, taking the importance of components into account, representing internal control systems (ICS) and mapping compliance and legal requirements. Clear information on business processes and risk management of IT/OT services is available.

Your benefits:

Define your service hours – including incident response and alert intervals

RADAR SOLUTIONS

Our technology. Your experts.

Joint forces for your Cyber Defense Center (CDC)

RADAR Cyber Security stands for a comprehensive offering of hardware and software for setting up and operating a Cyber Defense Center. We supervise and support you during each and every phase – from planning to implementation, through integration into your organization and continuous improvement.

RADAR Platform is a state-of-the-art cyber security detection platform technology and represents the core of RADAR Solutions, tailored to your CDC environment and individual needs. It includes a modular design, continuous updates, integrated threat intelligence as well as optimization upgrades. Your analysts and operations managers work with modern technology – from Big Data Analytics to customized reports in the Risk & Security Cockpit (RSC). RADAR Cyber Security roots on the holistic model of threat detection and risk assessment based on an advanced correlation engine.

We also provide your team with CDC empowerment services:

- ✓ Training lessons with your security and operations team
- ✓ Compilation of processes and best practices for your organization

Our goal is your security with the highest possible degree of Detection and Response effectiveness. We provide you with our experience and knowledge from more than 10 years of first-hand Managed Security Services.

The concept

Around-the-clock automated security monitoring and risk detection
Correlation, cross-correlation and aggregation of events from:

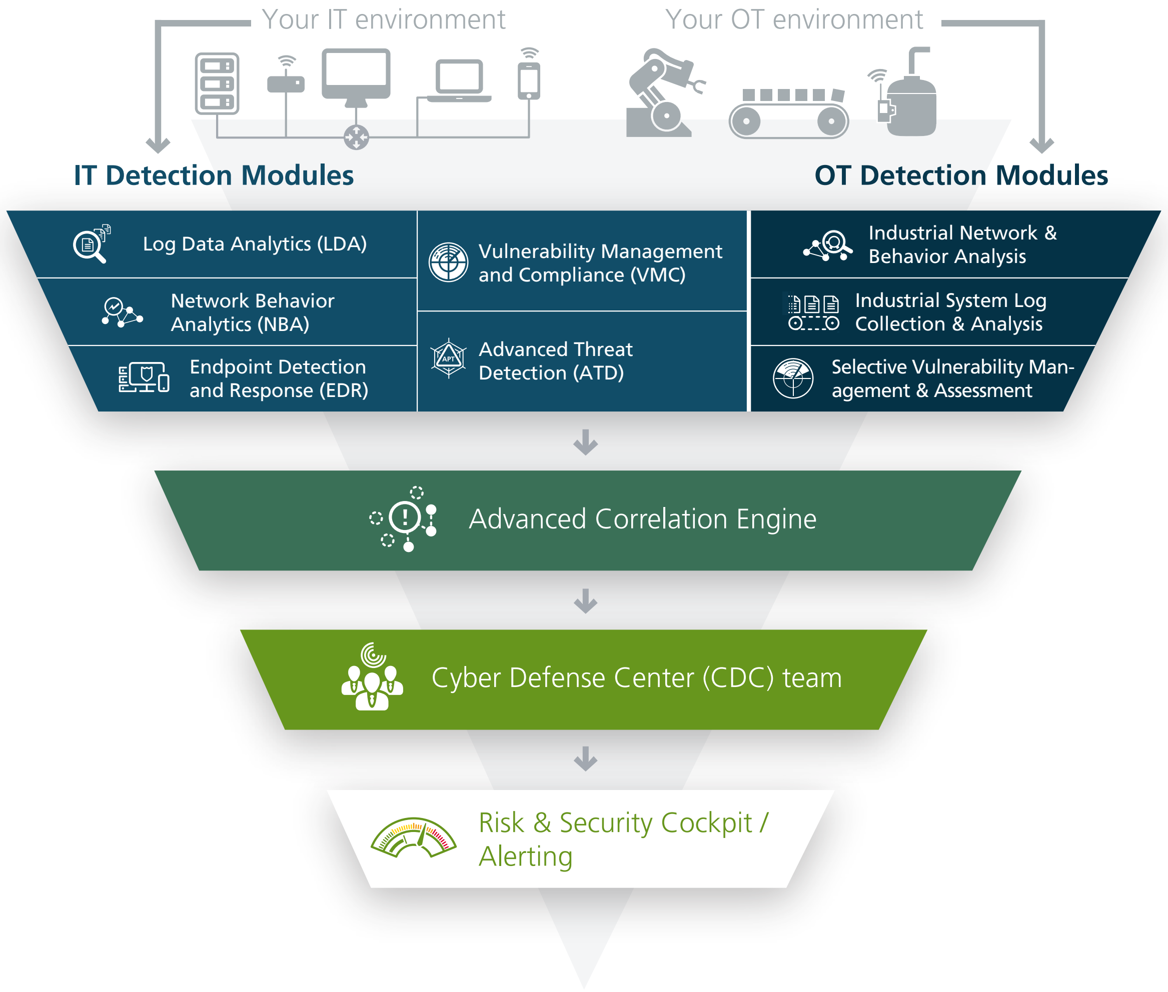
Log Data Analytics (LDA), Network Behavior Analytics (NBA), Vulnerability Management & Compliance (VMC), Endpoint Detection and Response (EDR) und Advanced Threat Detection (E-Mail & Web/ATD)

Customer-specific requirements are being processed as detection scenarios

The Result

- ✓ Consolidated and verified IT and OT risk information can be accessed for immediate mitigation.
- ✓ Reduction of false positives and false negatives
- ✓ All IT and OT security information is presented centrally in the Risk & Security Cockpit (RSC). Customized risk reports and statistics are easy to understand and can be obtained at the press of a button
- ✓ Real-time alerts are issued by means of dynamic threshold values
- ✓ The Cyber Defense Center team takes over the successive development of detection scenarios
- ✓ A structured risk management process is established and creates transparency

Consolidated IT and OT security



Your IT environment

Your OT environment

IT Detection Modules

OT Detection Modules

Log Data Analytics (LDA)

Network Behavior Analytics (NBA)

Endpoint Detection and 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

Cyber Defense Center (CDC) team

Risk & Security Cockpit / Alerting

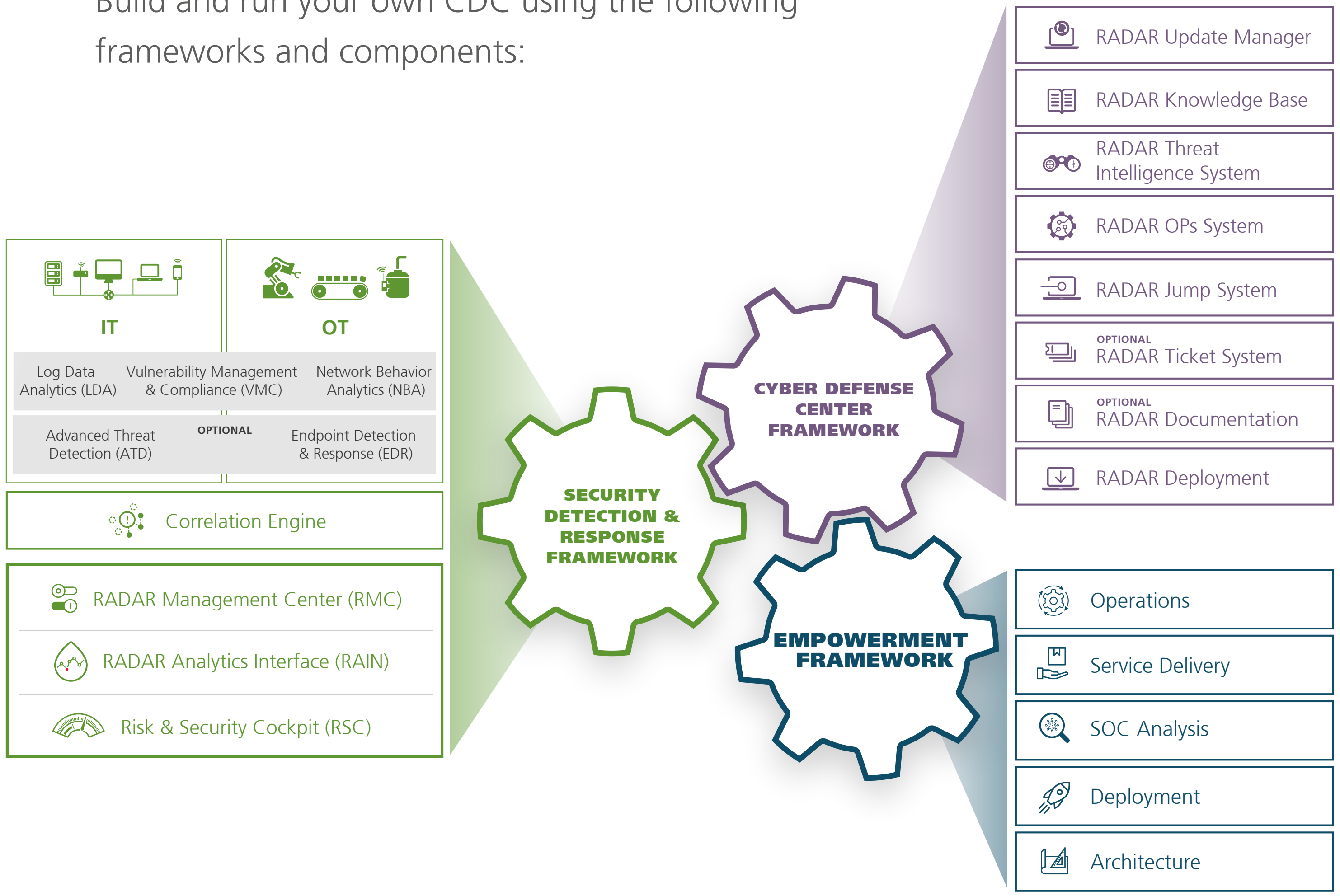
RADAR Services cover all areas, including the operations of RADAR Cyber Security's Cyber Defense Center team. With **RADAR Solutions**, the work is done by your internal experts. RADAR Cyber Security provides you with the technology, helps you establish the necessary processes and trains your employees.

Our technology for your security

RADAR Platform and its frameworks

The Detection and Response solution for your CDC in detail

Build and run your own CDC using the following frameworks and components:


IT
OT
Log Data Analytics (LDA)
Vulnerability Management & Compliance (VMC)
Network Behavior Analytics (NBA)
Advanced Threat Detection (ATD)
OPTIONAL
Endpoint Detection & Response (EDR)
Correlation Engine
RADAR Management Center (RMC)
RADAR Analytics Interface (RAIN)
Risk & Security Cockpit (RSC)
SECURITY DETECTION & RESPONSE FRAMEWORK
CYBER DEFENSE CENTER FRAMEWORK
EMPOWERMENT FRAMEWORK
RADAR Update Manager
RADAR Knowledge Base
RADAR Threat Intelligence System
RADAR OPs System
RADAR Jump System
OPTIONAL
RADAR Ticket System
OPTIONAL
RADAR Documentation
RADAR Deployment
Operations
Service Delivery
SOC Analysis
Deployment
Architecture

Cyber Defense Center Framework (CDCF)

The CDCF provides the entire range of RADAR Solutions technologies to manage the processes and operations of inhouse cyber defense professionals and with end customers. You receive the license to use our CDC technology “Made in Europe” (RADAR Platform) to process and analyze IT and OT security information for your own operations or for a business model (Managed Security Services).

RADAR Update Manager

Component to integrate the latest updates for the entire software stack, threat intelligence data, detection use cases, signatures and knowledge base.

RADAR Jump System

Component to ensure a secure connection to the CDC with RADAR technology in the RADAR Solutions user environment using thin clients, screen recording and secure sign-in

RADAR Knowledge Base

Component to store all use cases as well as alerts and incident descriptions with a clear summary and recommended actions

RADAR Ticket System

Central tool for CDC support cases, coordinating CDC service tasks and performing internal tracking by means of alert system interface

RADAR Threat Intelligence System
Component for analyzing, managing and integrating indicators of compromise, data enrichment (closed/open source) and detection rules

RADAR Documentation
Components for knowledge sharing within your CDC team and for storing playbooks, runbooks, etc.

RADAR Operations System
All aspects needed to operate RADAR Platform (e.g. monitoring, backup, recovery)

RADAR Deployment
Deployment in end customer environments

Security Detection & Response Framework (SDRF)

This framework comprises all components needed to detect, analyze and subsequently process security information. Data from the detection modules is collected and processed in user-friendly dashboards. Notifications on security incidents in the end customer's environment are captured.

- ✓ **RADAR Analytics Interface for CDC security analysts**
- ✓ **Risk & Security Cockpit for decision-makers**
- ✓ Workflow cockpits for managing all administrative tasks within a CDC are integrated into **RADAR Management Center (RMC)**.

Empowerment & Training Framework

RADAR Cyber Security provides training programs to CDC teams to handle the various tasks involved in using RADAR Solutions. The empowerment program covers:

- ✓ **Training lessons covering all relevant positions in and around CDC operations**
- ✓ **Service delivery**
- ✓ **Technical sales**

Technology.
Processes.
Experts.

Our success is your security

RADAR Cyber Security is driven by the powerful combination of human expertise and experience, coupled with the results of our own research. We bring together cyber security experts and our European technology to provide you with the solutions you need today to meet security challenges of tomorrow, making us a unique Cyber Security Trusted Advisor in the heart of Europe.

RADAR Cyber Security provides a range of security detection modules for various needs:

Log Data Analytics

Log data analysis with machine learning and use case research

Collecting, analyzing and correlating log data from a variety of sources is considered a core discipline of IT security. This type of detection is in many cases applied as an entry level product (also called Security Information & Event Management SIEM). The result: Security-relevant information and indicators of compromise in real-time, in order to take necessary countermeasures in the case of security incidents.

- ✓ Support and integration of common log formats
- ✓ Aggregation of information and events from all areas
- ✓ Identification of potential risks with our state-of-the-art correlation engine incorporating continuously enhanced and tailor-made rules and policies

Network Behavior Analytics (NBA)

Detection of malware, anomalies and other risks in the network traffic based on signature and behavior-based detection engines.

- ✓ Over 19,000 continuously extended signatures and rules are compared with IP reputation data
- ✓ Behavioral analysis of Zero-day events and other types of attacks not yet known as well as detection of protocols and ports
- ✓ Identification of different file types based on MD5 checksums and further file extraction to prevent documents from being transferred inside or outside the network (if applicable)

Vulnerability Management & Compliance (VMC)

Internal and external vulnerability scans with comprehensive detection, compliance checks and tests to cover all vulnerabilities

- ✓ Continuous internal and external vulnerability scans for a 360-degree overview
- ✓ Authenticated or non-authenticated vulnerability scans
- ✓ Detection of open ports and the use of potentially insecure or redundant services on those ports
- ✓ Compliance/password checks to detect configuration issues that are related to application, password and user policies
- ✓ Identification of norms or missing password rules with vulnerability classifications High, Medium or Low Risk, along with the likelihood of exploits

Advanced Threat Detection (E-Mail & Web/ATD)

Next-generation sandbox technologies are used to detect advanced malware in emails and downloads.

- ✓ State-of-the-art detection methods to identify sophisticated malware
- ✓ Next-generation sandbox technologies with full system emulation and deep learning mechanism of malware behavior
- ✓ Productive email traffic: detect and block suspicious messages
- ✓ Continuous updates on advanced threat feeds

Endpoint Detection & Response (EDR)

The analysis, monitoring and detection of anomalies in hosts trigger active responses and immediate alerts.

- ✓ Collection, analysis, and correlation of logs from a server or client sends incident alerts whenever attacks, misuse or errors are detected
- ✓ Verification of the local systems's file integrity
- ✓ Root kit detection identifies events such as hidden attacks, trojans or viruses based on system modifications

OT: Monitoring production networks

Safeguarding industrial control systems

This is what OT monitoring looks like

Operational technology (OT) and industrial control systems are network parts within IT infrastructure. A holistic overview and converged view of IT and OT systems ensure an optimum of protection against daily cyber threats. All data is synchronously analyzed and processed by the same procedure.

The following modules are available for OT detection:

Industrial network behavior analysis

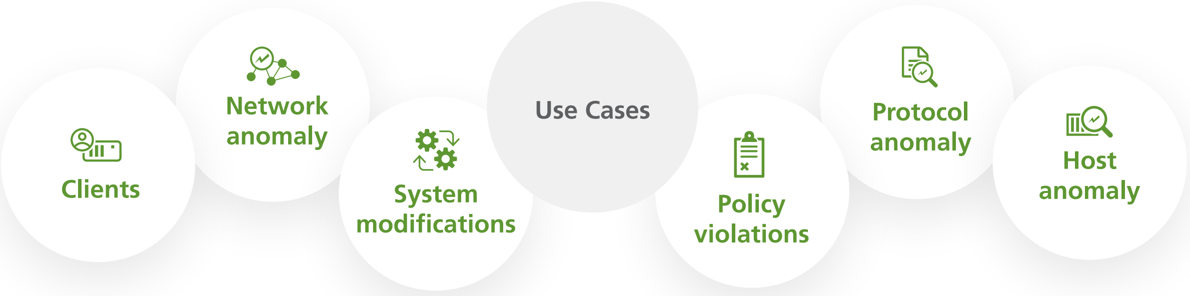
- ✓ Detection using protocol and flow data
- ✓ Metadata extraction from industrial logs
- ✓ Automatic analysis through machine learning

Industrial system log collection and analysis

- ✓ Detection of security-critical operations and anomalies based on defined use cases
- ✓ Collection, normalization and correlation of OT logs
- ✓ Advanced correlation with integrated IT and OT log data analysis

OT vulnerability management and assessment

- ✓ OT vulnerability scans
- ✓ Vulnerability assessment based on asset data
- ✓ OT threat intelligence and knowledge transfer on threat types



Clients

Network anomaly

System modifications

Use Cases

Policy violations

Protocol anomaly

Host anomaly

Drawing the right conclusions

Advanced Correlation Engine

Correlation within a module and cross-correlation of information from different modules ensure high-quality detection of risks and security issues. The engine enables a comprehensive view on security incidents within IT/OT infrastructures.

- Security overview and all relevant data
- Inclusion of logs, vulnerabilities, anomalies, asset information and more
- Correlation and cross-correlation are based on rules, policies, and self-learning algorithms
- Differentiation between normal and abnormal behavior in the IT and OT infrastructure
- Ongoing expansion of rules and statistical models
- Alerting modes in critical situations

Dashboards for analysis and decisions

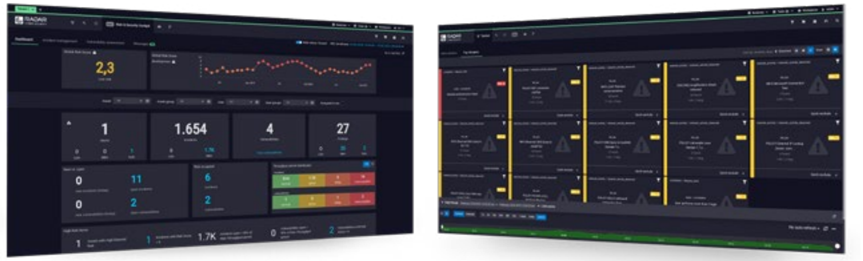
Our range of technological equipment for your CDC workers or end customers includes user interfaces that provide a quick and easy overview of key security indicators from consolidated IT and OT data.

RADAR Analytics Interface (RAIN)
For independent analysis, evaluation of alerts and rule adjustment of the automated security detection system

Risk & Security Cockpit (RSC)
Presenting security analysis and assessment results to IT decision makers – serves as a basis for forensic experts and for determining countermeasures in the event of reported cyber attacks

The needle in the digital haystack

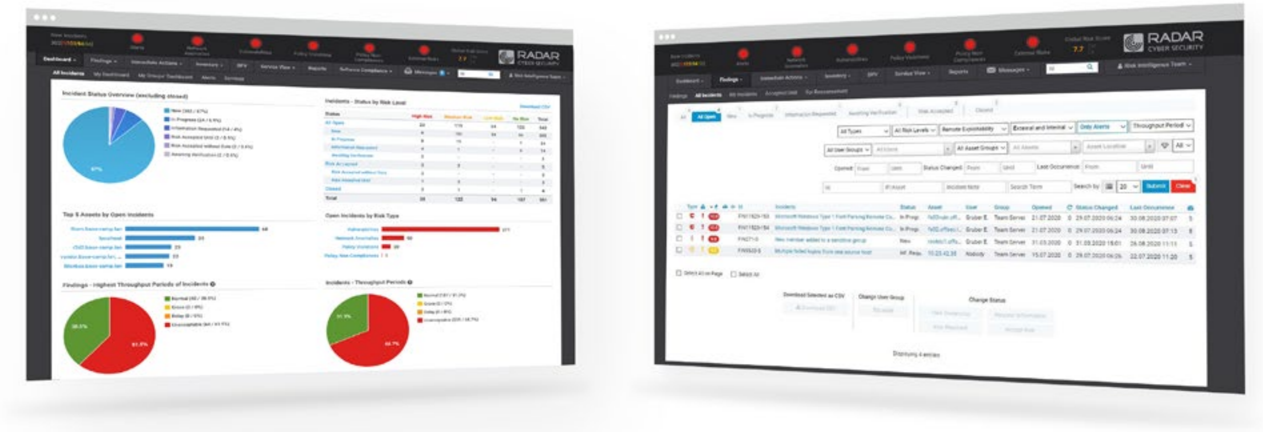
All relevant IT and OT security information at a glance



RAIN – RADAR Analytics Interface

RAIN is the ideal cyber security analytics and detection tool. Complex data is simplified and interpretation is facilitated. CDC analysts, threat hunters and incident response experts can analyze alerts, drill down underlying data from different perspectives and deliver further analysis results, which are being displayed in the Risk & Security Cockpit for end customers. For subsequent analysis, processes can be automated by conversion into rules that allow future alerts. Threat types and categories are visualized on dashboards. Relations between security events can be derived due to the size of the database in IT and OT infrastructures.

✓ Finding the needle in the haystack	**Big Data Analytics** ✓ **Combination of historical and recent risk data** ✓ **Reduction of administrative workload**
✓ Working with huge data volumes	
✓ Time-consuming and complex ✓ Extensive data processing	✓ **Contextualizing data** ✓ **Flexibilization of data access** ✓ **Seamless convergence** ✓ **Efficient orchestration**
✓ Identifying meaningful data patterns	



Risk Level: 🟢 No Risk 🟡 Low Risk 🟠 Medium Risk 🔴 High Risk

RSC – Risk & Security Cockpit

Analyzed risk and security alerts are presented in the Risk & Security Cockpit. Tailor-made and easy-to-understand risk reports and statistics are available at the push of a button.

- ✓ Risk level assessment with four levels
- ✓ Reports and statistics with the required level of detail
- ✓ Alert notifications in urgent cases
- ✓ Consistent and traceable risk elimination workflow within the Cockpit
- ✓ Messaging and feedback communication with the Cyber Defense Center team
- ✓ Integrated business process view shows business processes at risk due to security issues
- ✓ Asset management function that tracks all assets in the network

RADAR
CYBER SECURITY | Safeguard your digital journey.

As part of the Materna Group, RADAR Cyber Security operates one of the largest cyber defense centers in Europe in the heart of Vienna, based on its inhouse developed Cyber Detection Platform technology. Driven by the strong combination of human expertise and experience, coupled with the latest technological developments from more than 10 years of research, the company combines comprehensive solutions to the challenges of IT and OT security in its RADAR Services and RADAR Solutions products. The best-of-breed cyber detection platform, the RADAR Platform, monitors the infrastructure of market leaders in all industries as well as in the public sector. It follows a holistic approach covering both IT and OT landscapes. This makes RADAR Cyber Security a unique cyber security know-how hub in Central Europe.

Contact us

RADAR Cyber Security
Zieglergasse 6
1070 Vienna
Austria

P: +43 (1) 929 12 71-0
F: +43 (1) 929 12 71-710
E: sales@radarcs.com
www.radarcs.com

Get informed

Subscribe to our newsletter: **newsletter-subscribe.radarcs.com**

CYBERSECURITY MADE IN EUROPE™
Initiated by ECSO. Issued by eurobits e.V.

ECS EUROPEAN CYBER SECURITY ORGANISATION

MSSP Alert Top 250 MSSPs

ISO 27001 CERTIFIED