Shaping the future of IT security

Radar Cyber Security – THE EARLY WARNING SYSTEM FOR YOUR IT.

Cyber Defense Center (CDC)
IT and OT Security Monitoring
Advanced Cyber Threat Detection
IT and OT Risk Detection

TECHNOLOGY — SOLUTIONS — MANAGED SERVICES
Next Generation Cybersecurity

Safeguard your digital journey.
Solutions
Our technology. Your experts.

For large organizations
- Building your own CDC (Cyber Defense Center)

For Managed Security Services Provider
- Building your CDC for your clients

Managed Services
The all-round service from a single provider.

- CDC as a Service
- IT and OT Security Monitoring
- Log Data Analytics (LDA)
- Advanced Cyber Threat Detection
- IT and OT Risk Detection

On-Premise, cloud or hybrid.
Radar Cyber Security offers you the technology and support you need for your efficient and comprehensive inhouse Cyber Defense Center (CDC).

Radar Cyber Security provides support at all stages: from planning and implementation to integration into your organisation and continuous improvement – whether you want to establish or expand your CDC.

The RadarPlatform is the core that makes it possible to create the technological basis tailored to your needs. Regular updates, integrated threat intelligence and continuous improvements are included. Big Data is proceeded and analysed and finally results in customized reports, alarms and a central source for information: the Risk & Security Cockpit. Everything is state-of-the-art at any time and following Radar Cyber Security's reliable procedures for detection and risk assessment, including the advanced correlation engine.

In addition, we support you with our CDC Empowerment Services: we tailor the platform to your specific needs, conduct trainings for your CDC team and jointly work out the right processes and best practices for your organisation. The goal always in mind: maximum effectivity and efficiency regarding detection & response. Our experience is always available to you.

White labelling or franchising – Radar Cyber Security offers various options to providers of managed security services so that they can supply their customers with services based on the RadarPlatform, the leading Cyber Security Detection technology developed in Europe.

Solutions for Managed Security Services Provider
Building your CDC for your clients

White labelling or franchising – Radar Cyber Security offers various options to providers of managed security services so that they can supply their customers with services based on the RadarPlatform, the leading Cyber Security Detection technology developed in Europe.
Managed Services
Your all-in-one solution: Hardware, software and expert know-how. Radar Cyber Security offers all tools and manages the operations.

CDC as a Service
Radar Cyber Security sets up a Cyber Defense Center (CDC) in your company and manages its continuous operation. Quickly up and running, using tried and tested principles and based on cutting-edge technology developed in Europe. Personal contact in your local language, clear rules and documented processes for structured procedures and easy communication with your company. Choose your ideal service hours up to 24/7, including incident response and real-time alerting.

IT und OT Security Monitoring
Increasing interconnectedness of IT and OT systems leads to new vulnerabilities for attacks from both the inside and outside. Continuous and central IT Security Monitoring of IT and OT infrastructure and its components is essential. Radar Cyber Security continuously monitors the entire IT and OT infrastructure and applications and evaluates all data results, specifically searches for weaknesses in systems and their configuration and intelligently analyses the network traffic.

Log Data Analytics (LDA)
The collection and analysis of logs from various sources of a network (server, clients, network devices, firewalls, applications, etc.) is essential in order to get information about security-relevant events. Out of millions of events Radar Cyber Security effectively and efficiently identifies those, which indicate abuse of IT and applications, internal or external attacks or other threats.

Advanced Cyber Threat Detection
New types of malware, Advanced Persistent Threats (APTs) and trojans find their way into companies via web downloads or e-mail attachments as they are not detected by signature-based systems alone. In addition there is the risk of insider threats whereby unauthorized access is obtained to specifically targeted information. Radar Cyber Security uses a multitude of systems for signature- and behavior-driven analyses of network traffic and next-generation sandbox technologies for the analysis of all incoming e-mail attachments as well as web downloads and analyses all findings centrally. In addition, suspicious email traffic is detected and blocked.

IT Risk Detection
Companies and organizations need up-to-date risk information every day. Radar Cyber Security collects and analyses risk in the IT infrastructure considering parameters such as the importance of IT infrastructure components, establishes the legally required Internal Control System for your IT and supplies documentation for your compliance & regulatory demands. A clear illustration of effects of security-relevant issues on IT services and business processes as well as an IT risk management workflow is included.

Professional Services
Radar Cyber Security is your partner for all topics concerning cybersecurity and risk management. The portfolio comprises professional services such as strategic IT and OT security and risk consulting, the support in case of immediate threats (Fire Fighting), Incident Response, Incident-Workflow management as well as special incident remediation and forensics. All services are available 24/7.

Included Modules:
- NBA
- LDA
- VMC
- ATD
- EDR

Professional Services:
- Incident Response and Forensics

Included Modules:
- NBA
- LDA
- VMC
- ATD

Professional Services:
- IT Risk Consulting; (Service Risk View, Business Process Risk View)
- Incident Response
- Incident-Workflow management
- Special incident remediation and forensics
Our technology for your safety.

Products and services for the future.
The approach

- 24/7 automated IT security monitoring and risk detection: correlation, cross-correlation and aggregation of events from Log Data Analytics (LDA), Network Behavior Analytics (NBA), Vulnerability and Compliance Management (VMC), Endpoint Detection and Response (EDR) and Advanced Threat Detection (Email & Web/ATD).
- Customer-specific requirements are considered through detection scenarios.
- The Risk & Security Intelligence Team, our experts for risk and security analysis, analyses the automatically obtained findings in predefined intervals (daily/weekly/monthly) as part of our managed services.

The result

- The consolidated and verified IT risk and security information is immediately applicable for remediation processes.
- No false positives, no false negatives.
- All IT risk and security information are presented centrally in the Risk & Security Cockpit. Customised and easy to understand reports and statistics are available on the push of a button.
- Real-time alerts are generated based on dynamically set thresholds.
- The Risk & Security Intelligence Team gradually takes over the development of customised detection scenarios as part of our managed services.
- A structured IT risk management process is established and leads to transparency.

Managed Services comprise all areas, including the work of the Radar Cyber Security Risk & Security Intelligence Team. Solutions comprise the RadarPlatform which is the technological basis for the work of your internal analysts. Radar Cyber Security supports you by establishing processes and by providing technical trainings for your team.
Excellence in detection.
The modules at a glance.
Log Data Analytics (LDA)

The collection, analysis and correlation of logs from various sources results in alerts in case of security flaws or potential risks.

- numerous common log formats are understood out of the box
- information and events from all areas are aggregated
- risk is identified through the state-of-the-art correlation engine with continuously updated, enhanced and always customised correlation rules and policies

Network Behavior Analytics (NBA)

High performance analysis of the network traffic is used for signature- and behavior-based detection of dangerous malware, anomalies and other network traffic risks.

- more than 19,000 continuously updated (matched with IP reputation data) signatures and rules
- additional behavior-driven analyses for zero-day exploits and other unknown attacks without signatures as well as the detection of protocols even if varying ports
- identification of thousands of file types via MD5 checksums and possible file extraction to let documents stay out or not get out

Endpoint Detection and Response (EDR)

Analysis, monitoring and detection of anomalies on hosts lead to active response and immediate alerts.

- collection, analysis and correlation of logs of a server or client, alerts in case of the detection of an attack, fraudulent use or error
- file integrity checks of the local system
- rootkit detection identifies hidden actions by attackers, trojans, viruses, etc. when system changes occur

Vulnerability Management und Compliance (VMC)

Continuous internal and external vulnerability scans with comprehensive detection, compliance checks and tests deliver results with zero false positives and full vulnerability coverage.

- continuous and highly accurate internal and external vulnerability scans for a 360° view
- authenticated or non-authenticated vulnerability scans, open ports and potential unsecure or unnecessary services on these ports are detected
- compliance- and password-checks spot configuration problems with regard to applications as well as password- and user-policies, detection of standard and missing passwords
- vulnerabilities are categorized in high, medium or low risk as well as the possibility of exploitation

Compliant software per server / server groups is assessed according to policies and a continuous analysis of the current status.

- management of the full software inventory for Windows- and Linux systems
- policies can be defined for software compliance rules
- alerts point to software with known vulnerabilities
- licence management is included

Advanced Threat Detection (Email & Web/ATD)

Next generation sandbox technologies are used for the detection of advanced malware in e-mails and web downloads.

- best-in-class detection of advanced malware specifically designed to detect and stop advanced and evasive malware
- next-generation sandbox technologies powered by full-system emulation and with deep understanding of malware behavior to measure its impact
- continuously updated feed for advanced threats
- productive email traffic – detect and block suspicious emails
Advanced Correlation Engine

Correlation within a module as well as cross-correlation of information from various modules results in superior detection of risks and security flaws and a rich view of enterprise activity.

- analysis of extensive amounts of security- and risk-relevant data
- correlation of logs with network flows, vulnerabilities, IDS events, SIEM findings and other data presents all relevant information in one big picture
- correlation and cross-correlation based on rules, policies and machine learning
- differentiation of normal and abnormal behavior within the IT infrastructure
- continuous enhancement of rules and statistical models
- alerts in critical situations

Risk & Security Intelligence Team

The Risk & Security Intelligence Team analyses, consolidates and assesses all data delivered by the automated monitoring and detection modules as part of our managed services to form superior risk and security information. False positives and false negatives are eliminated.

- the Team focuses exclusively on risk analysis for clients. Highly valuable analogies may be drawn across industries
- findings are used to continuously enhance policies and rules of the automated risk detection
- each reported risk description is enriched with clear instructions for remediation
- highly experienced and well-trained team with deep subject matter expertise in security audit, penetration testing, white-hat hacking and social engineering continuously transfers knowhow to the client
- on demand: experts for fire fighting and forensics, the role of an external CERT team

Drawing the right conclusions.

Data analysis: automated and by experts.
The big picture.

One source for all IT and OT risk- and security-relevant information.

Risk & Security Cockpit

The Risk & Security Cockpit is the central source for risk and security information. Customised and easy to understand reports and statistics are available on the push of a button.

- reports and statistics are provided in the preferred level of detail
- alerts in case of urgent information on risk or security flaws provided in the Cockpit, via email and even via push message on mobile phones if requested
- overall risk remediation workflow within the Cockpit
- messaging / feedback system for the communication with the Intelligence Team
- business process risk view presents the current threats of the IT security flaws to IT services and in turn to business processes
- asset management functionalities provide an overview about what is really running in the network
What distinguishes us.

EFFECTIVENESS
- Award-winning technology made in Europe
- The largest Cyber Defence Centre in Europe
- Highest European data protection security standards

PRODUCTIVITY
- Focus on core business
- Improvement of IT and OT processes
- Ease of use

EFFICIENCY
- Return on investment
- Perfection in in-depth analysis
- Complete coverage regarding a wide range of events
- Your early warning system for IT and OT is always state-of-the-art
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