RADAR SERVICES

# RADAR PLATFORM

## Cyber Security Detection Technology for your Security Operations Centre

**IT Security**
made in Europe

# Customized IT security.

Our services.

# Solutions

Our technology. Your experts.

For large organisations

**Building your SOC (Security Operations Centre)**

For Managed Security Services Provider

**Building your SOC for your clients**

On-Premise, cloud or hybrid.

# Managed Services

Next Generation Managed Security Services.

**SOC as a Service**

**IT Security Monitoring**

**Security Information & Event Management (SIEM)**

**Advanced Cyber Threat Detection**

**IT Risk Detection**

On-Premise, cloud or hybrid.

# Solutions

Our technology. Your experts.

## The Cyber Security Detection Technology
for large organisations

RadarServices offers you the technology and support you need for your efficient and comprehensive inhouse Security Operations Center (SOC).

RadarServices 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 SOC.

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 RadarServices' reliable procedures for detection and risk assessment, including the advanced correlation engine.

In addition, we support you with our **SOC Empowerment Services**: we tailor the platform to your specific needs, conduct trainings for your SOC 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.

## Our offer for
## Managed Security Services Provider

**White labelling or franchising** – RadarServices 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.

# Systematically accessing the decisive information.

The multi-level principle.

# Risk detection modules

» **24/7 automated IT security monitoring and risk detection**: correlation, cross-correlation and aggregation of events from Security Information & Event Management (SIEM) and Logging, Network-based Intrusion Detection (NIDS), Host-based Intrusion Detection System (HIDS), Vulnerability Management and Assessment (VAS), Software Compliance (SOCO) and Advanced Threat Detection (Email & Web/ATD).

» **Possibility to consider customer-specific requirements** through detection scenarios.

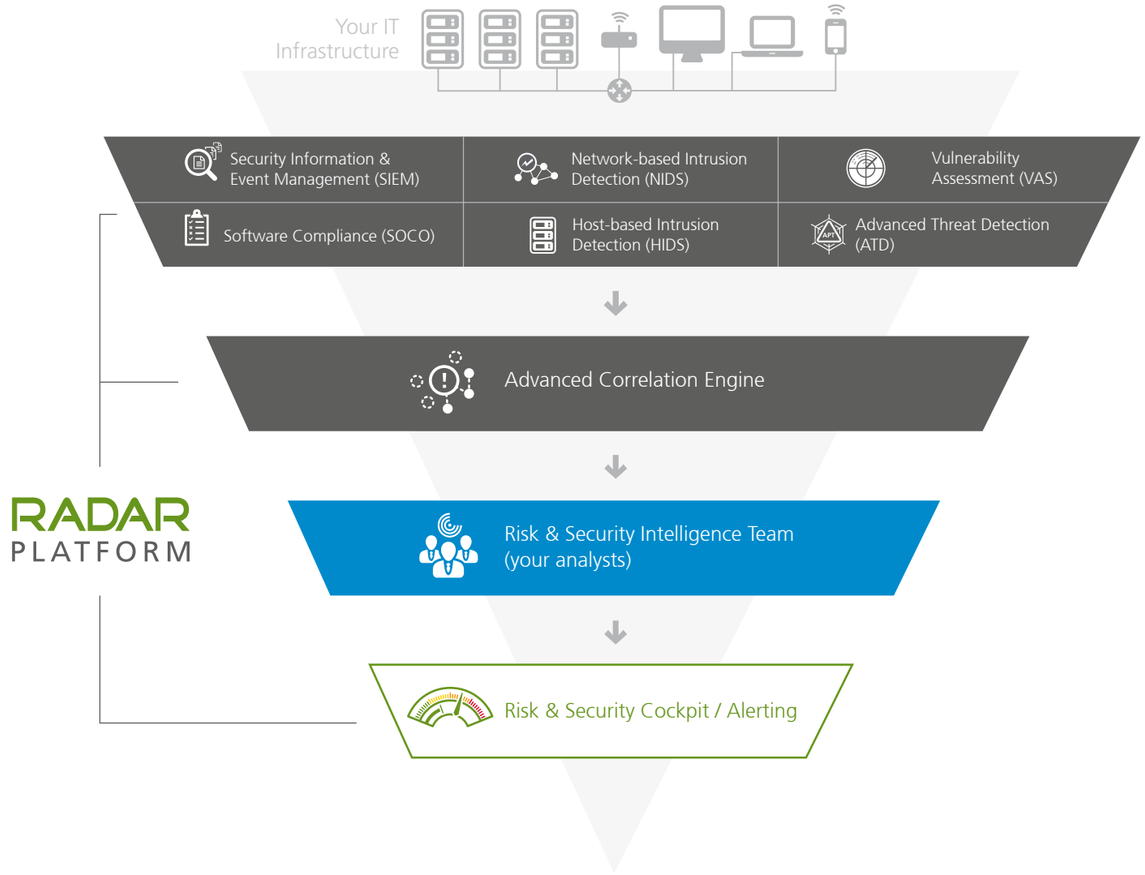
# The result

✔ **Correlation and cross-correlation** of IT risk and security information**.**

✔ **Reduction of false positives und false negatives to the maximum possible extent.**

✔ **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.



# Excellence in detection.

The modules.

## Security Information & Event Management (SIEM)

**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-based Intrusion Detection (NIDS)

**High performance analysis of the network traffic is used for signature- and behaviour-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 behaviour-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

## Vulnerability Management and Assessment (VAS)

**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



## Software Compliance (SOCO)

**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

## Host-based Intrusion Detection System (HIDS)

**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

## 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** behaviour to measure its impact
- **continuously updated feed** for advanced threats

# Drawing the right conclusions.

Data analysis: automated and by experts.


## 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.**

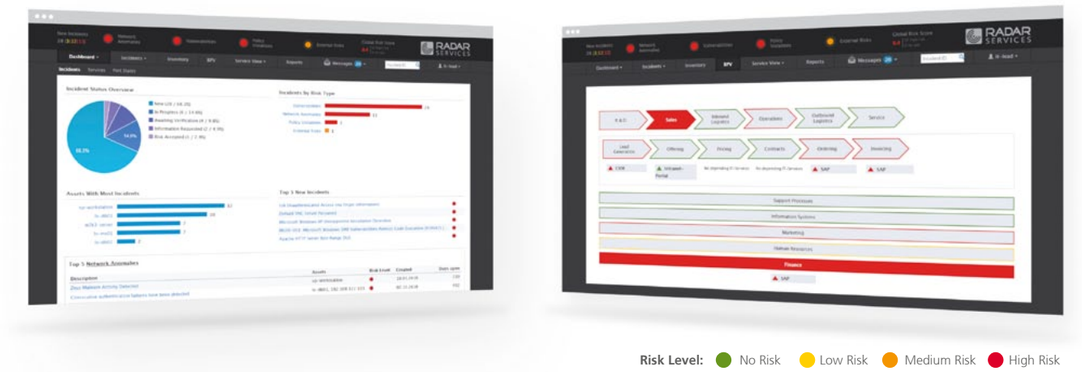
- analysis of extensive amounts of security- and risk-relevant data
- **correlation** of logs with network flows, vulnerabilities, IDS events, SIEM findings and other data **presents all relevant information in one big picture**
- correlation and cross-correlation based on **rules, policies and machine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

## Risk & Security Intelligence Team

**Your Risk & Security Intelligence Team analyses, consolidates and assesses all data delivered by the automated monitoring and detection modules to form superior risk and security information. False positives and false negatives are eliminated.**

# The big picture.

One source for all 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

RADAR SERVICES

**The European Experts**
in IT Security Monitoring
and IT Risk Detection

**RadarServices is Europe's leading technology company in the field of Detection & Response.** In focus: The early detection of IT 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 Security Operations Center (SOC) or it is used in combination with our expert analysts, documented processes and best practices as SOC as a Service. The result: Highly effective and efficient improvement of IT security and IT risk management, continuous IT security monitoring and an overview of security-related information throughout the entire IT landscape of an organization.


**RadarServices**
Zieglergasse 6
1070 Vienna
Austria

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

**RadarServices Germany**
Taunustor 1
60310 Frankfurt a. M.

Phone: +49 (69) 2443424 655
Email: sales_germany@radarservices.com

**RadarServices Middle East**
A110-1, DSO HQ Building
Dubai, VAE

Phone: +971 (4) 501 5447
Email: sales_me@radarservices.com