RADAR
CYBER SECURITY

Mit Sicherheit in die Zukunft.

Radar Cyber Security – DAS FRÜHWARNSYSTEM FÜR IHRE IT.

Cyber Defense Center (CDC)

IT und OT Security Monitoring

Advanced Cyber Threat Detection

IT und OT Risk Detection

TECHNOLOGY — SOLUTIONS — MANAGED SERVICES

IT Security
made in Europe

FT 1000 Europe's Fastest Growing Companies 2019
statista

ISO 27001
CERTIFIED

Maßgeschneiderte Cybersecurity der nächsten Generation

Safeguard your digital journey.

IMPRESSUM

Herausgeber
RadarServices Smart IT-Security GmbH, Wien
FN371019s, Handelsgericht Wien.

Bildrechte: Cover istock.com/mbbirdy, S.10 Arnold Mike, S.14, S.18, S.22-23 Stanislav Jenis

Solutions

Unsere Technologie. Ihre Experten.

Für große Unternehmen

Ein eigenes CDC (Cyber Defense Center) bauen

Für Managed Security Services Provider

Ein CDC für Kunden bauen

On-Premise, Cloud oder Hybrid.

Managed Services

Das Rundum-Service aus einer Hand.

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

On-Premise, Cloud oder Hybrid.

Solutions

Unsere Technologie. Ihre Experten.

Lösungen für große Organisationen

Bauen Sie Ihr eigenes CDC

Radar Cyber Security bietet Ihnen ein Gesamtpaket aus Hardware, Software und Training, das Sie für Ihr effizientes und umfassendes Cyber Defense Center (CDC) benötigen.

Wir unterstützten Sie **in allen Phasen – von der Planung und Implementierung, bis hin zur Integration in Ihre Organisation und der laufenden Verbesserung**. Egal ob Sie Ihr CDC auf- oder ausbauen möchten.

Die **RadarPlatform** ist dabei das Herzstück, die einen an Ihre Bedürfnisse angepassten Einsatz erlaubt. Ständige Updates, integrierte Threat Intelligence und laufende Verbesserungen sind inklusive. Von Big Data Analytics bis zu maßgeschneiderten Berichten im Risk & Security Cockpit und Alarmierung – alles immer State-of-the-Art und nach dem bewährten Radar Cyber Security Ansatz der Erkennung und Bewertung inklusive Advanced Correlation Engine.

Darüber hinaus unterstützen wir Sie durch unsere **CDC Empowerment Services**: Wir passen die Plattform an Ihre speziellen Bedürfnisse an, führen Trainings für Ihr CDC-Team durch und stellen gemeinsam mit Ihnen die für Ihre Organisation passenden Prozesse und Best Practices auf. Das Ziel immer vor Augen: höchste Effektivität bei Detection & Response. Unsere Erfahrung ist für Sie immer zugänglich.

Lösungen für Managed Security Services Provider

Bauen Sie ein CDC für Ihre Kunden

White-Labeling-Option oder Franchising – Radar Cyber Security bietet Managed Security Services-Anbietern verschiedene Möglichkeiten, Kunden Dienstleistungen auf Basis der RadarPlatform, der führenden und in Europa entwickelten Cyber Security Detection Technologie anzubieten.

Managed Services

Das Gesamtpaket aus Hardware, Software und Experten-Know-how.
Radar Cyber Security stellt alle Werkzeuge bereit und managt den laufenden Betrieb.

CDC as a Service

Radar Cyber Security etabliert ein Cyber Defense Center (CDC) in Ihrem Unternehmen und übernimmt dessen laufenden Betrieb. **In kürzester Zeit ist es einsatzbereit, nach bewährten Prinzipien** und basierend auf **modernster, in Europa entwickelter Technologie**. **Persönliche Ansprechpartner** in Ihrer Landessprache, klare Regelungen und dokumentierte Prozesse ermöglichen **strukturierte Abläufe und einfache Kommunikation** mit Ihrem Unternehmen. Wählen Sie die für Sie passenden **Servicezeiten bis zu 24/7** aus. **Incident Response und Echtzeit-Alarmierung** ist dabei natürlich inklusive.

Inkludierte Module:

LDA NBA VMC ATD EDR

Professional Services:
Incident Response und Forensik

IT und OT Security Monitoring

Umfassende Vernetzung von IT- und OT-Systemen führt zu ständig neuen Einfallstoren für Angriffe von innen und außen. Ein kontinuierliches und zentrales Monitoring der IT- und OT-Infrastruktur und ihrer Komponenten ist unabdingbar. Radar Cyber Security **überwacht laufend die gesamte IT- und OT-Landschaft und Applikationen, bewertet alle Ereignisdaten, sucht gezielt nach Schwachstellen** in Systemen und deren Konfiguration und **analysiert intelligent den Netzwerkverkehr**.

Inkludierte Module:

LDA NBA VMC

Log Data Analytics (LDA)

Die Sammlung und Analyse von Logs aus verschiedenen Quellen in einem Netzwerk (Server, Clients, Netzwerkgeräte, Firewalls, Anwendungen, etc.) erfolgt zentral, um Informationen über sicherheitsrelevante Ereignisse zu erlangen. Radar Cyber Security kristallisiert **aus Millionen von Ereignissen effektiv und effizient diejenigen heraus, die auf einen Missbrauch der IT, OT und Applikationen, auf interne oder externe Angriffe oder auf andere Sicherheitsbedrohungen hinweisen**.

Inkludierte Module:

LDA

Advanced Cyber Threat Detection

Neuartige Malware, Advanced Persistent Threats (APTs) und Trojaner gelangen durch Web Downloads oder E-Mail-Anhänge in Unternehmen, da sie durch signatur-basierende Systeme allein nicht erkannt werden. Hinzu kommt das Risiko von Insider-Threats, wodurch gezielt wichtige Informationen unberechtigt erlangt werden. Radar Cyber Security setzt **mehrere Systeme zur signatur- und verhaltensbasierten Analyse von Netzwerkverkehr und Sandbox-Technologien der neuesten Generation zur Analyse aller eingehenden E-Mail-Anhänge sowie Downloads** ein und wertet die Erkenntnisse zentral aus. Zusätzlich wird verdächtiger E-Mail-Verkehr erkannt und blockiert.

Inkludierte Module:

NBA ATD

IT Risk Detection

Unternehmen und Organisationen benötigen eine tagesaktuelle Sicht auf ihre Risiken. Radar Cyber Security **erfasst und analysiert Risiken in der IT- und OT-Infrastruktur unter Einbeziehung der Wichtigkeit von Komponenten**, stellt das gesetzlich vorgeschriebene **Interne Kontrollsystem (IKS)** für Ihre IT dar und beinhaltet **Nachweise für Compliance & regulatorische Anforderungen**. Klare Darstellungen über Auswirkungen auf IT- und OT-Services und Geschäftsprozesse sowie ein Risikomanagement-Workflow sind ebenfalls enthalten.

Inkludierte Module:

LDA

Professional Services:
IT-Risikoberatung (Service Risk View, Business Process Risk View)

Professional Services

Radar Cyber Security ist Ihr Ansprechpartner rund um das Thema Cybersecurity und Risikomanagement.

Das Portfolio umfasst Professional Services wie die strategische IT- und OT-Security und Risikoberatung, die Unterstützung im akuten Angriffsfall (**Fire Fighting**), **Incident Response**, Incident-Workflowmanagement sowie spezielle **Incident-Behebung und Forensik**. Alle Services stehen auch 24/7 auf Abruf bereit.

Unsere Technologie für Ihre Sicherheit.

Produkte und Services für die Zukunft.

Vorgehensweise

» **Automatisierte IT-Sicherheitsüberwachung und Risikoerkennung rund um die Uhr**: Korrelation, Cross-Korrelation und Aggregation von Ereignissen aus Log Data Analytics (LDA), Network Behavior Analytics (NBA), Vulnerability und Compliance Management (VMC), Endpoint Detection und Response (EDR) und Advanced Threat Detection (E-Mail & Web/ATD)

» **Kundenspezifische Anforderungen** werden in Erkennungsszenarien abgebildet

» Das **Risk & Security Intelligence Team**, unsere Experten für die Risiko- und Sicherheitsanalyse, analysiert im Rahmen unserer Managed Services die automatisiert erlangten Erkenntnisse **in vorab definierten Intervallen** (täglich/wöchentlich/monatlich)

Ergebnis

✔ Die **konsolidierten und verifizierten IT-Risiko- und Sicherheitsinformationen** sind sofort für den Behebungsprozess verwendbar

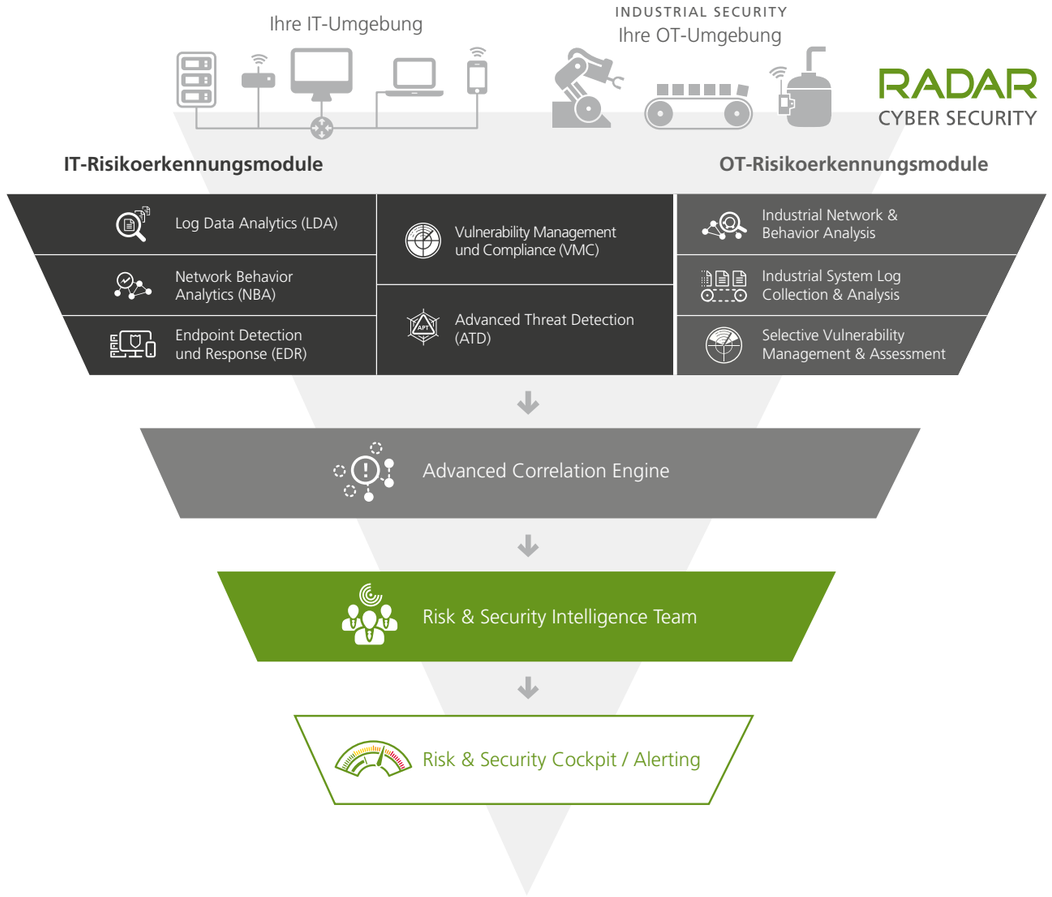
✔ **Keine False Positives, keine False Negatives**

✔ **Alle IT-Risiko- und Sicherheitsinformationen** werden **zentral** im Risk & Security Cockpit präsentiert. Maßgeschneiderte und leicht verständliche Risikoberichte und Statistiken sind auf Knopfdruck verfügbar

✔ **Echtzeit-Alarmierung** wird auf Basis von dynamisch festgelegten Schwellwerten ausgelöst

✔ Das Risk & Security Intelligence Team übernimmt im Rahmen unserer Managed Services sukzessive die **Weiterentwicklung der kundenspezifischen Erkennungsszenarien**

✔ Ein **strukturierter IT-Risikomanagementprozess** wird gelebt und schafft Transparenz



Managed Services umfassen alle Bereiche, inklusive der Tätigkeit des Risk & Security Intelligence Teams von Radar Cyber Security. Bei **Solutions** werden die Leistungen dieses Teams durch Ihre internen Experten erbracht – Radar Cyber Security stellt Ihnen die Technologie zur Verfügung, etabliert die notwendigen Prozesse und schult Ihre Mitarbeiter.

Exzellenz in der Erkennung.

Die Module im Überblick.

Log Data Analytics (LDA)

Die Sammlung, Analyse und Korrelation von Logs aus verschiedensten Quellen resultieren in Alarmierungen bei Sicherheitsproblemen oder potentiellen Risiken.

- Unterstützung **zahlreicher** gängiger **Log-Formate**
- Aggregation von Informationen und Ereignissen aus **allen Bereichen**
- Identifizierung potentieller Risiken durch unsere **State-of-the-Art Correlation Engine** mit kontinuierlich erweiterten und maßgeschneiderten Regeln und Policies

Network Behavior Analytics (NBA)

Erkennung von gefährlicher Malware, Anomalien und anderen Risiken im Netzwerkverkehr auf Basis von signatur- und verhaltensbasierten Detection Engines.

- Mehr als 19.000 **kontinuierlich erweiterte**, mit IP-Reputationsdaten verglichene, **Signaturen und Regeln**
- **Verhaltensbasierte Analysen** für Zero-Day-Exploits und andere noch nicht bekannte Angriffsarten, Erkennung von **Protokollen**, unabhängig von Ports
- **Identifizierung tausender verschiedener Dateitypen** anhand der MD5-Prüfsummen und weitergehender Dateiextraktion, um Dokumente gegebenenfalls nicht in oder aus dem Netzwerk transferieren zu lassen

Endpoint Detection und Response (EDR)

Die Analyse, Überwachung und Erkennung von Anomalien bei Hosts führen zu aktiven Reaktionen und sofortiger Alarmierung.

- **Sammlung, Analyse und Korrelation** von Logs eines Servers oder Clients und **Alarmierung** bei der Erkennung von Angriffen, Missbrauch oder Fehlern
- Überprüfung der **Dateiintegrität** des lokalen Systems
- **Rootkit-Erkennung** identifiziert z.B. versteckte Angriffe, Trojaner oder Viren anhand von Systemveränderungen

Vulnerability Management und Compliance (VMC)

Kontinuierliche, interne und externe Schwachstellen-Scans mit umfassender Erkennung, Compliance Checks und Tests für eine komplette Abdeckung zu allen Schwachstellen.

- Kontinuierliche **interne und externe** Schwachstellen-Scans für einen 360-Grad-Überblick
- **Authentifizierte** oder **nicht-authentifizierte** Schwachstellen-Scans, Erkennung von offenen **Ports** und der Nutzung von potentiell unsicheren oder überflüssigen Services auf diesen Ports
- **Compliance- und Passwort-Checks** zur Erkennung von Konfigurationsproblemen in Bezug auf Anwendungen und Passwörter- sowie Benutzerrichtlinien, Feststellung von Standard- oder fehlenden Passwörtern
- Empfehlungen zur **Schwachstellen-Kategorisierung** in hohes, mittleres und geringes Risiko und die Möglichkeit ihrer Ausnutzung

Compliant Software pro Server / Server-Gruppe wird mit Hilfe von Policies und einer kontinuierlichen Analyse des aktuellen Status festgestellt.

- **Management des kompletten Software-Inventars** für Windows- und Linuxsysteme
- Definition von **Policies für Software Compliance**-Regeln
- **Alarmierung** bei der Auffindung von Software mit bekannten Schwachstellen
- **Lizenzabgleich und -management** inklusive

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

Sandbox-Technologien der nächsten Generation werden für die Erkennung von „Advanced Malware“ in E-Mails und Downloads eingesetzt.

- **Modernste Erkennungsmethoden** für hochentwickelte und getarnte Malware
- **Sandbox-Technologien der nächsten Generation** mit vollständiger Systememulation und tiefgreifendem Verständnis von Malware-Verhalten
- **Produktiver E-Mail-Verkehr** – verdächtige Mails erkennen und blockieren
- **Kontinuierliche Updates** des Feeds für Advanced Threats

Die richtigen Schlüsse ziehen.

Datenanalyse automatisiert und durch Experten.

Advanced Correlation Engine

Korrelation innerhalb eines Moduls und Cross-Korrelation von Informationen aus verschiedenen Modulen führen zu einer hochqualitativen Erkennung von Risiken sowie zu Sicherheitsproblemen und einem umfassenden Blick auf die sicherheitsrelevanten Vorkommnisse im Unternehmen.

- **Gesamtüberblick** über sicherheitsrelevante Daten
- Miteinbeziehung von **Logs, Schwachstellen, Anomalien, Asset-Informationen** und vielem mehr
- Korrelation und Cross-Korrelation basieren auf **Regeln, Policies und selbstlernenden Algorithmen**
- Unterscheidung zwischen **normalem und abnormalem Verhalten** in der IT- und OT-Infrastruktur
- **Laufende Erweiterung** der Regelwerke und statistischen Modelle
- **Alarmierung** in kritischen Situationen

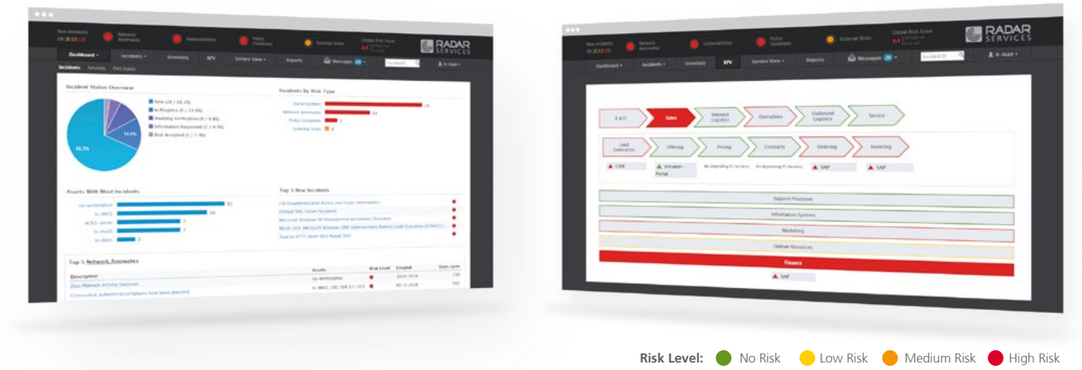
Risk & Security Intelligence Team

Das Risk & Security Intelligence Team von Radar Cyber Security analysiert und konsolidiert im Rahmen unserer Managed Services alle im Rahmen der automatisierten Risikoerkennung gesammelten Daten, um hochqualitative Risiko- und Sicherheitsinformationen zu erreichen. False Positives und False Negatives werden bearbeitet.

- Team mit ausschließlichem Fokus auf die Risikoanalyse bei Kunden, **Analogien** können **über Branchengrenzen hinweg** gezogen werden
- Erkenntnisse **verbessern laufend die Policies und Regeln** der automatisierten Risikoerkennung
- **Anreicherung jeder Risikobeschreibung** mit einer **Empfehlung für die Risikobehebung**
- Ständiger **Wissenstransfer** zum Kunden: jeder Mitarbeiter verfügt über tiefgreifendes Spezialisten-Know-how in den Bereichen Security Audit, Penetration Testing, White-Hat-Hacking und Social Engineering
- Auf Abruf: sofort einsatzbereite Experten für Fire Fighting und Forensik, Einnahme der Rolle eines externen **CERT-Teams**

Immer alles im Blick.

Eine Übersicht für alle IT- und OT-Risiko- und Sicherheitsinformationen.



Risk & Security Cockpit

Alle Risiko- und Sicherheitsinformationen werden zentral im Radar Risk & Security Cockpit präsentiert. Maßgeschneiderte und leicht verständliche Risikoberichte und Statistiken sind auf Knopfdruck verfügbar.

- **Berichte und Statistiken** in der gewünschten Detailtiefe
- **Alarmierung** in dringenden Fällen über das Cockpit – via E-Mail oder auch als Push-Mitteilung auf das Mobiltelefon
- Durchgehender und nachvollziehbarer **Risikobehebungs-Workflow** im Cockpit
- **Nachrichten- und Feedback-System** für die Kommunikation mit dem Risk & Security Intelligence Team
- Integrierter **Business Process Risk View** zeigt die durch die IT-Sicherheitsprobleme gefährdeten Geschäftsprozesse auf
- **Asset Management** – Funktionen für den Überblick über alles, was sich tatsächlich im Netzwerk befindet

Was uns auszeichnet.

EFFEKTIVITÄT

Prämierte Technologie made in Europe

Das größte Cyber Defence Centre in Europa

Höchste europäische Datenschutzsicherheitsstandards

PRODUKTIVITÄT

Fokus aufs Kerngeschäft

Verbesserung der IT- und OT-Prozesse

Benutzerfreundlichkeit

EFFIZIENZ

Return on Investment

Perfektion in der Analysetiefe

Komplettabdeckung in der Ergebnisbreite

Ihr Frühwarnsystem für IT und OT ist immer State-of-the-Art

RADAR CYBER SECURITY | Safeguard your digital journey.

Radar Cyber Security ist Europas führendes Technologieunternehmen im Bereich Detection & Response. Im Mittelpunkt steht die zeitnahe Erkennung von Risiken für die Sicherheit der IT und OT von Unternehmen und Behörden als Solution oder als Managed Service. Basis dafür ist eine hochmoderne, eigenentwickelte Technologieplattform mit der Kunden ihr Cyber Defense Center (CDC) aufbauen können oder die in Kombination mit Security-Analyseexperten, bewährten Prozessen und Best Practices als CDC as a Service zur Verfügung steht. Das Ergebnis: Eine besonders effektive und effiziente Verbesserung von IT-Sicherheit und -Risikomanagement, kontinuierliches IT und OT Security Monitoring und ein auf Knopfdruck verfügbarer Überblick über die sicherheitsrelevanten Informationen in der gesamten IT- und OT-Landschaft einer Organisation.

Radar Cyber Security HQ
Zieglergasse 6
1070 Wien
Österreich

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

Radar Cyber Security Deutschland
Taunustor 1
60310 Frankfurt am Main
Deutschland

T: +49 (69) 2443424 655
F: +49 (69) 2443424 150
E: sales_germany@radarcs.com
www.radarcs.com/de

PUBLIC

B_CORP_DE_v1