RADAR
CYBER SECURITY

Bewährte Cybersicherheit aus europäischer Hand

FÜR IT UND OT

Cyber Defense Center (CDC) as a Service

Cyber Defence Center Solutions für den Aufbau von:

– für Inhouse CDC

– für MSSP

Part of MATERNA
Information & Communications

Safeguard your digital journey.

IMPRESSUM

Herausgeber
RadarServices Smart IT-Security GmbH, Zieglergasse 6, 1070 Wien
FN371019s, Handelsgericht Wien.

Bildrechte: S.14 NicoElNino/Shutterstock.com, S.19 istock.com/xijian, S.20 Arnold Mike,
S.24 istock.com/yoh4nn, Rückseite TZIDO SUNS/Shutterstock.com

Ihre Cyber-Resilienz, unsere Lösung

IHRE VORTEILE

- Risikominimierung: Echtzeit-Abbildung der Bedrohungslage Ihrer IT und OT Infrastuktur inkl. konkreter Handlungempfehlungen
- Kostenoptimierung: Kostentransparenz bei der Stärkung Ihrer Cyber Resillience
- Konformität: Einhaltung von gesetzlichen Vorgaben und Compliance Regeln
- Fokussierung: Ihr verstärkter Fokus auf das Kerngeschäft
- Return on (Security) Investment

UNSER PRODUKT

- Betrieb eines der größten Cyber Defense Centers (CDC) in Europa, basierend auf modernster Eigentechnologie
- Mehr als 10 Jahre Erfahrung in der Entwicklung und dem Betrieb unseres Cyber Defense Centers
- Einbindung der eigenen Technologieerfahrung für unsere Kundenorganisationen

UNSERE PROZESSE

- Konvergierte Darstellung Ihrer IT und OT Sicherheitslage über eine Benutzeroberfläche
- Alle Daten verbleiben in Ihrem Unternehmen, höchste Datenschutzstandards ohne Software Hintertüren

UNSER PERSONAL

- Fundiertes Wissen und menschliche Expertise gepaart mit dem neuesten Stand der Technik

UNSERE PRODUKTE

RADAR SERVICES

Das Rundum-Service aus einer Hand.

CDC as a Service

RADAR SOLUTIONS

Unsere Technologie. Ihre Expert:innen.

Ein Cyber Defense Center (CDC) im eigenen Unternehmen aufbauen

Ein CDC für die Erbringung Ihrer Managed Security Service-Leistungen etablieren (MSSPs)

RADAR SERVICES

Das Rundum-Service aus einer Hand.

CDC as a Service

RADAR Cyber Security etabliert sich als Cyber Defense Center (CDC) in Ihrem Unternehmen und übernimmt den laufenden Betrieb. In kürzester Zeit ist es einsatzbereit, operiert nach bewährten Prinzipien und basiert auf modernster, eigenentwickelter Technologie. Persönliche Ansprechpartner:innen in Ihrer Landessprache, klare Regelungen und dokumentierte Prozesse ermöglichen strukturierte Abläufe und einfache Kommunikation zwischen Ihrem Unternehmen und unserem CDC im Herzen Europas.

Empfohlene Kernmodule:

Empfohlene Zusatzmodule:

Die Kompetenzen unseres Cyber Defense Centers

- Team mit Fokus auf die Risiko- und Angriffserkennung
- Analogien/Use Cases können über Branchengrenzen hinweg weitergenutzt werden
- Analyseerkenntnisse modifizieren laufend die Richtlinien und Regeln der automatisierten Risikoerkennung
- Ergänzung jeder Vorfallsbeschreibung mit einer Empfehlung zur Risikobehebung durch Analyst:innen

IT- und OT-Detection auf einen Blick

RADAR Cyber Security erfasst und analysiert Risiken in der IT- und OT-Infrastruktur unter Einbeziehung der Wichtigkeit von Komponenten, stellt das interne Kontrollsystem (IKS) dar und bildet Compliance sowie Gesetzesanforderungen ab. Klare Informationen zu Geschäftsprozessen und Risikomanagement der IT-/OT-Services sind abrufbar.

Ihr Vorteil:
Legen Sie die für Sie passenden Servicezeiten fest – inklusive Incident Response und zeitnaher Alarmierung.

RADAR SOLUTIONS

Unsere Technologie. Ihre Expert:innen.

Gemeinsam für Ihr Cyber Defense Center (CDC)

RADAR Cyber Security bietet für Aufbau und Betrieb eines Cyber Defense Centers ein Gesamtpaket aus Hardware und Software. Wir unterstützen Sie in allen Phasen – von der Planung und Implementierung, bis hin zur Integration in Ihre Organisation und der laufenden Verbesserung.

Die RADAR Platform ist eine hochmoderne Cybersecurity Detection-Technologie und bildet das Herzstück von RADAR Solutions. Diese wird an Ihre CDC-Umgebung und individuellen Anforderungen angepasst. Modularer Aufbau, laufende Updates, integrierte Threat Intelligence und Optimierungen sind inkludiert. Von Big Data Analytics bis zu maßgeschneiderten Berichten im Risk & Security Cockpit – Ihre Analyst:innen und Operations Manager:innen arbeiten auf dem neuesten Stand der Technik. RADAR Cyber Security setzt auf das ganzheitliche Modell der Angriffserkennung und Risikobewertung, die auf einer bewährten Advanced Correlation Engine basieren.

Darüber hinaus unterstützen wir Ihr Team durch unsere CDC Empowerment-Leistungen:

- ✔ Trainings mit Ihren Security und IT/OT Operations Teams
- ✔ Zusammenstellung von Prozessen und Best Practices für Ihre Organisation.

Unser Ziel ist Ihre Sicherheit mit der höchstmöglichen Effektivität im Bereich Detection and Response. Wir stellen Ihnen unsere Erfahrungen und Erkenntnisse aus mehr als 10 Jahren direkter Arbeit mit unseren Kund:innen zur Verfügung.

Vorgehensweise

Automatisierte IT-Sicherheitsüberwachung und Risikoerkennung rund um die Uhr: Korrelation, Cross-Korrelation und Aggregation von Ereignissen aus

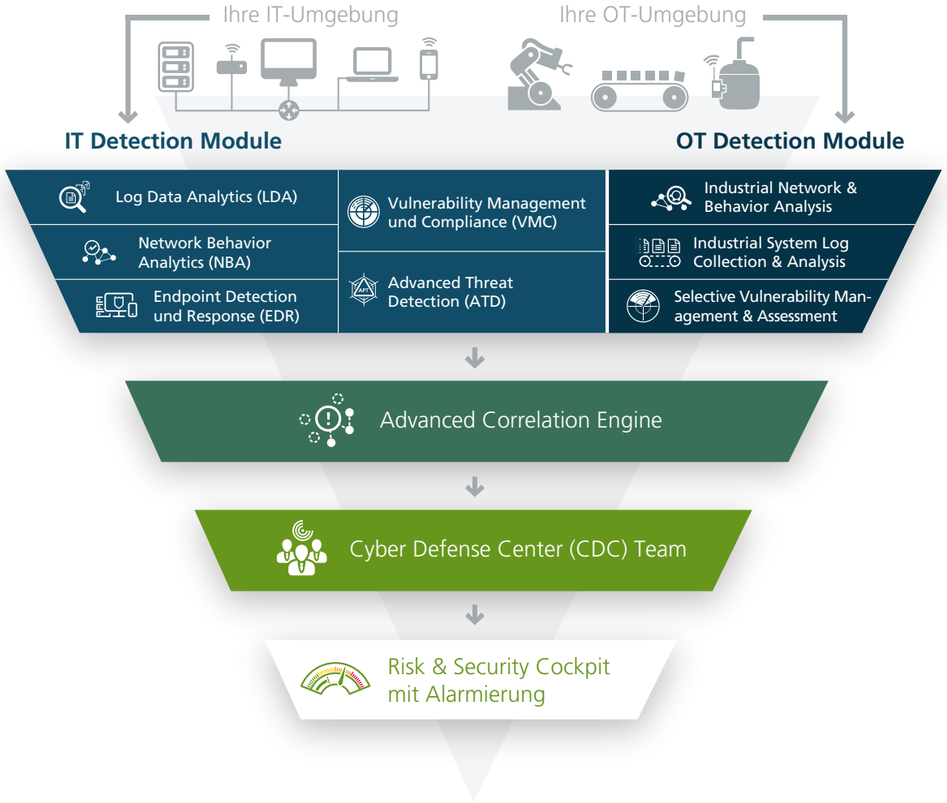
Log Data Analytics (LDA), Network Behavior Analytics (NBA), Vulnerability Management & Compliance (VMC), Endpoint Detection and Response (EDR) und Advanced Threat Detection (E-Mail & Web/ATD)

Kundenspezifische Anforderungen können in Erkennungsszenarien abgebildet werden

Ergebnis

- Die konsolidierten und verifizierten IT- und OT-Risikoinformationen sind sofort für den Behebungsprozess abrufbar
- Reduktion der False Positives und False Negatives
- Alle IT- und OT-Sicherheitsinformationen werden zentral im Risk & Security Cockpit präsentiert. Maßgeschneiderte und leicht verständliche Risikoberichte und Statistiken sind auf Knopfdruck abrufbar
- Echtzeit-Alarmierung wird auf Basis von dynamisch festgelegten Schwellenwerten ausgelöst
- Das Cyber Defense Center Team übernimmt eine sukzessive Weiterentwicklung der Erkennungsszenarien
- Ein strukturierter Risikomanagement-Prozess wird etabliert und schafft Transparenz

Konsolidierte IT und OT Security



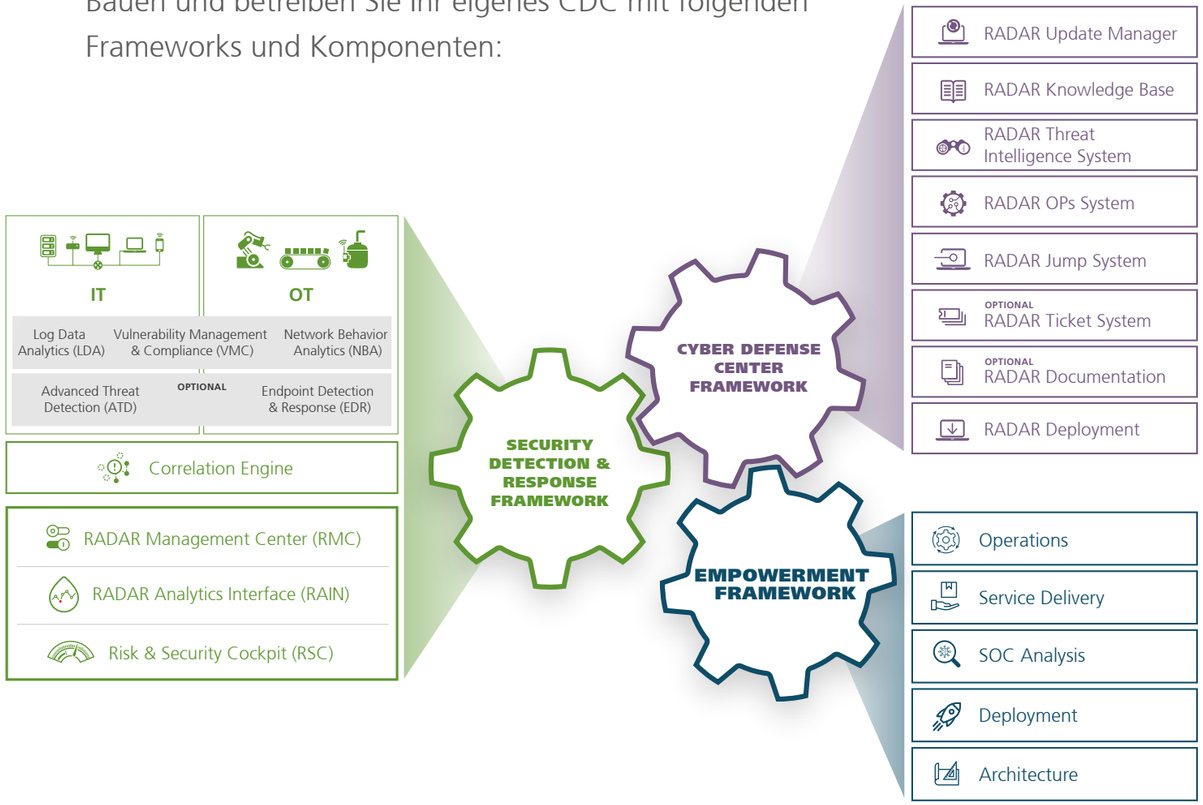
RADAR Services umfasst alle Bereiche, inklusive der Tätigkeit des Cyber Defense Center Teams von RADAR Cyber Security. Bei **RADAR Solutions** wird die Leistung dieses Teams durch Ihre internen Expert:innen erbracht. RADAR Cyber Security stellt Ihnen die Technologie zur Verfügung, unterstützt bei der Etablierung der notwendigen Prozesse und schult Ihre Mitarbeiter:innen.

Unsere Technologie für Ihre Sicherheit.

Die RADAR Platform und ihre Rahmenbedingungen

Die Detection and Response-Lösung für Ihr CDC im Detail

Bauen und betreiben Sie Ihr eigenes CDC mit folgenden Frameworks und Komponenten:



Cyber Defense Center Framework (CDCF)

Das CDCF stellt alle Technologien im Rahmen von RADAR Solutions zur Verfügung, um die Prozesse und Abläufe im SOC und zu Endkund:innen zu managen. Sie erhalten die Lizenz zur Nutzung unserer CDC-Technologie „Made in Europe“ (RADAR Platform), um IT- und OT-Sicherheitsinformationen für Ihren Eigenbetrieb bzw. für ein Geschäftsmodell (Managed Security Services) aufbereiten und analysieren zu können.

RADAR Update Manager

Komponente zur Integration der neuesten Updates für den gesamten Software-Stack, Threat Intelligence-Daten, Detection Use Cases, Signaturen und Knowledge Base.

RADAR Jump System

Komponente zur Gewährleistung einer sicheren Verbindung zum SOC mit RADAR-Technologie am Standort des RADAR Solutions Anwenders mit Hilfe von Thin Clients, Bildschirmaufzeichnungen und sicheren Anmeldeprozessen

RADAR Knowledge Base

Komponente zur Speicherung aller Use Cases sowie Warnmeldungen und Vorfallsbeschreibungen mit klarer Zusammenfassung, Beschreibung und Handlungsempfehlungen

RADAR Ticket System

Zentrales Tool für SOC-Supportfälle, Koordination von CDC-Serviceaufgaben und interne Nachverfolgung mit Schnittstelle zur zentralen Alarmierung

RADAR Threat Intelligence System
Komponente zur Analyse, Verwaltung sowie Integration von Indicators of Compromise, Data Enrichment (Closed/Open Source) und Erkennungsregeln

RADAR Documentation
Komponenten für den Wissensaustausch innerhalb Ihres CDC-Teams sowie für die Ablage von Playbooks, Runbooks, etc.

RADAR Operations System
Alle notwendigen Komponenten für den Betrieb der Plattform (z.B. Monitoring, Backup, Wiederherstellung)

RADAR Deployment
Deployment zu Installationen für Endkund:innen

Security Detection & Response Framework (SDRF)

Dieses Framework umfasst alle Komponenten, welche für die Erkennung und Analyse und in Folge zur strukturierten Aufarbeitung der angezeigten Sicherheitsvorfälle notwendig sind. Die Daten aus den Erkennungsmodulen werden gesammelt und in übersichtlichen Dashboards aufbereitet. Sicherheitsvorfälle der Endkund:innen-Umgebung können erfasst werden.

- **RADAR Analytics Interface für Cyber Defense Center-Analyst:innen**
- **Risk & Security Cockpit für Entscheidungsträger:innen**
- Darüber hinaus sind Workflow-Cockpits für die Verwaltung aller administrativen Aufgaben innerhalb eines CDC in das **RADAR Management Center** integriert.

Framework: Empowerment & Training

RADAR Cyber Security bietet CDC-Verantwortlichen Schulungsprogramme für die unterschiedlichen Aufgaben bei der Anwendung von RADAR Solutions. Dazu zählen Schulungen für:

- **alle relevanten Positionen im und rund um den CDC-Betrieb**
- **Servicebereitstellung**
- **Technischer Vertrieb**

Technologie.
Prozesse.
Experten.

Unser Erfolg ist Ihre Sicherheit

RADAR Cyber Security wird von der starken Kombination aus menschlicher Expertise und Erfahrung angetrieben, gepaart mit den Ergebnissen unserer eigenen Forschungs- und Entwicklungsarbeit. Wir vereinen Cyber Security Expert:innen und unsere europäische Technologie, um Ihnen genau die Lösungen anzubieten, die man heute benötigt, um den Herausforderungen von morgen entgegen zu treten. Das macht uns zu einem einzigartigen Cyber Security Trusted Advisor inmitten Europas.

RADAR Cyber Security stellt eine breite Palette an Security Detection-Modulen für unterschiedliche Bereiche bereit:

Log Data Analytics

Logdatenanalyse mit Machine Learnung und Use-Case-Forschung

Die Sammlung, Analyse und Korrelation von Logdaten aus verschiedensten Quellen gilt als Kerndisziplin der IT-Sicherheit. Diese Art der Erkennungsleistung kommt in vielen Fällen als Einstiegsprodukt (auch SIEM genannt) zur Anwendung. Das Resultat: Sicherheitsrelevante Informationen und Indicators of Comprise in Echtzeit, um schnellstmöglich Schritte und Maßnahmen bei einem Sicherheitsvorfall setzen zu können.

- 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 und Ports
- Identifizierung verschiedener Dateitypen anhand der MD5-Prüfsummen und weitergehender Dateiextraktion, um Dokumente gegebenenfalls nicht in oder aus dem Netzwerk transferieren zu lassen

Vulnerability Management & 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

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 Nachrichten erkennen und blockieren
- Kontinuierliche Updates des Feeds für Advanced Threats

Endpoint Detection & 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
- 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

OT: Vernetzte Produktion überwachen

Schutz für Industrie-Kontrollsysteme

So sieht OT-Monitoring aus

Operational Technology (OT) und industrielle Kontrollsysteme sind mit der IT-Infrastruktur vernetzt. Ein ganzheitlicher Überblick und eine konvergente Sicht auf IT- und OT-Systeme gewährleisten einen optimalen Schutz vor Cyberbedrohungen. Alle gesammelten Daten werden durch den gleichen Ablauf synchron analysiert und weiterverarbeitet.

Folgende Module stehen für die OT Detection zur Verfügung:

Industrielle Netzwerkverhaltensanalyse

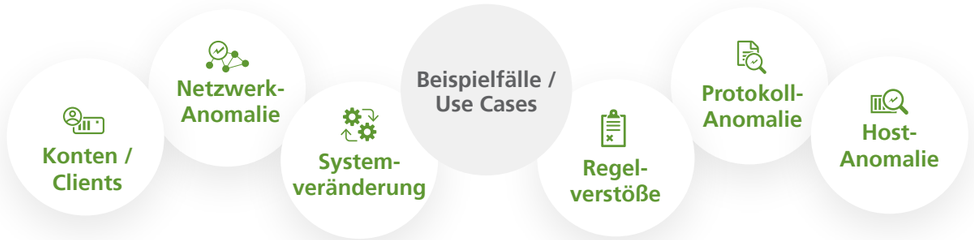
- Erkennung aus Protocol- und Flow-Daten
- Metadaten-Extraktion aus industriellen Protokollen
- Automatische Analyse durch Machine Learching

Industrielle System-Protokollsammlung und Analyse

- Erkennung von sicherheitskritischen Vorgängen und Anomalien auf der Grundlage von definierten Use Cases
- Sammlung, Normalisierung und Korrelation von OT-Logs
- Erweiterte Korrelation mit integrierter IT- und OT-Protokolldatenanalyse

Gezieltes OT-Schwachstellenmanagement und Bewertung

- OT-Schwachstellenscans
- Bewertung von Schwachstellen basierend auf Asset-Daten
- OT Threat Intelligence und Wissensaufbau zu Bedrohungsarten



Die richtigen Schlüsse ziehen.

Advanced Correlation Engine

Die Korrelation innerhalb eines Moduls und die Cross-Korrelation von Informationen aus verschiedenen Modulen führen zu einer hochqualitativen Erkennung von Risiken und Sicherheitsproblemen. Dies ermöglicht einen umfassenden Blick auf die sicherheitsrelevanten Vorkommnisse innerhalb eines Unternehmens.

- 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

Dashboards für die eigene Analyse und Entscheidungen

Unsere Technologie-Ausstattung für Ihre Mitarbeiter:innen bzw. Endkund:innen umfasst Benutzeroberflächen, die schnell und unkompliziert einen Überblick zu wesentlichen Sicherheitsfragen aus konsolidierten IT- und OT-Daten geben.

RADAR Analytics Interface (RAIN)
Zur eigenständigen Analyse, Bewertung von Alarmierungen und Regelanpassung der automatisierten Sicherheitserkennung

Risk & Security Cockpit (RSC)
Zur Darstellung von Ergebnissen aus der Sicherheitsanalyse und -bewertung für IT-Entscheidungsträger:innen - dient als Grundlage für Forensiker:innen und für die Festlegung von Gegenmaßnahmen im Fall von gemeldeten Cyberangriffen

Die Nadel im digitalen Heuhaufen

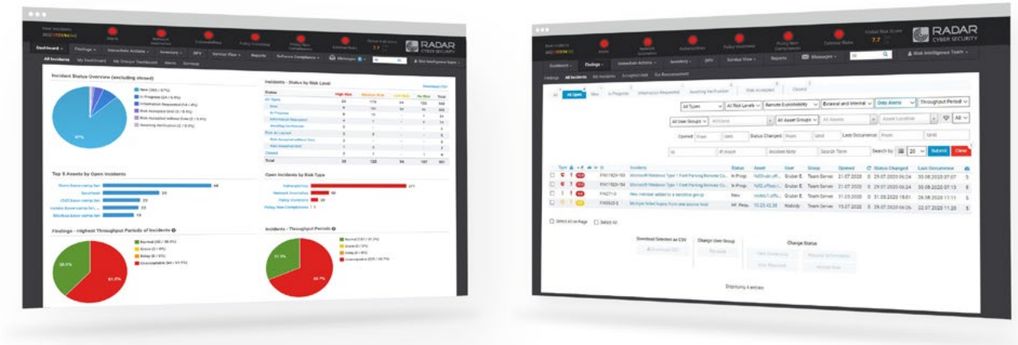
Alle relevanten IT- und OT-Sicherheitsinformationen im Blick

RAIN – RADAR Analytics Interface

RADAR Analytics Interface ist ein ideales Cybersecurity-Analysewerkzeug. Komplexe Daten werden vereinfacht und können so leichter interpretiert werden. CDC Analyst:innen, Threat Hunter sowie Incident Response Verantwortliche können Alarmmeldungen entsprechend analysieren, mittels Drill Downs die dahinterliegenden Daten aus verschiedenen Perspektiven beleuchten und damit weitere Analyseergebnisse liefern, welche wiederum im Risk & Security Cockpit ausgeworfen werden. Für spätere Analysen können Abläufe in Regeln überführt und damit automatisiert werden, um dazu laufend weitere Alarmierungen zu erhalten. Aufgrund der breiten Datenbasis aus der gesamten IT- und OT-Infrastruktur können die vielfältigen Bedrohungen anschaulich auf Dashboards visualisiert und Beziehungen zwischen Sicherheitsereignissen veranschaulicht werden.

- ✓ Nadel im Heuhaufen finden
- ✓ Arbeit mit riesigen Datenmengen
- ✓ Zeitintensiv und komplex
- ✓ Umfangreiche Datenverarbeitung
- ✓ Sinnvolle Datenmuster erkennen

- ✓ **Big Data Analytics**
- ✓ **Kombination aus historischen und aktuellen Risikodaten**
- ✓ **Reduktion von administrativen Aufwänden**
- ✓ **Ansicht von Daten im Kontext**
- ✓ **Flexibilität beim Zugang zu Daten**
- ✓ **Nahtlose Konvergenz**
- ✓ **Effiziente Orchestrierung**



Risiko-Levels: Kein Risiko · Geringes Risiko · Mittleres Risiko · Hohes Risiko

Risk & Security Cockpit

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

- ✓ Risikolevel-Bewertung mit 4 Stufen
- ✓ Berichte und Statistiken in der gewünschten Detailtiefe
- ✓ Alarmierung in dringenden Fällen
- ✓ Durchgehender und nachvollziehbarer Risikobehebungs-Workflow
- ✓ Nachrichten- und Feedback-System für die Kommunikation mit dem Cyber Defense Team
- ✓ Integrierter Business Process View zeigt die durch die Sicherheitsprobleme gefährdeten Geschäftsprozesse auf
- ✓ Asset Management – Funktion für den Überblick zu allen Assets, die sich tatsächlich im Netzwerk befinden

RADAR CYBER SECURITY | Safeguard your digital journey.

RADAR Cyber Security betreibt als Teil der Materna-Gruppe im Herzen Wiens eines der größten Cyber Defense Center Europas auf Basis der eigenentwickelten Cyber Detection Platform Technologie. Angetrieben von der starken Kombination aus menschlicher Expertise und Erfahrung, gepaart mit den letzten technologischen Entwicklungen aus mehr als zehn Jahren Forschung vereint das Unternehmen in seinen Produkten RADAR Services und RADAR Solutions umfassende Lösungen für die Herausforderungen in Bezug auf IT- und OT-Security. Kern ist die Best-of-Breed Cyber Detection Platform, die RADAR Platform, welche mit Orchestration, Automation und Response täglich die Infrastruktur von Marktführern in allen Branchen sowie im öffentlichen Dienst überwacht. Verfolgt wird dabei ein holistischer Ansatz, der sowohl IT- als auch OT-Landschaften von Unternehmen und Behörden abdeckt. Das macht RADAR Cyber Security zu einem einzigartigen Cyber Security Know-how Hub inmitten Europas.

Kontaktieren Sie uns:

RADAR Cyber Security
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

Informieren Sie sich:

Jetzt Cyber Security News anmelden unter **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