RADAR
SMART SOLUTION

Ersparen Sie sich so einen Morgen!

PLUG & DETECT

Kontinuierliches IT Security Monitoring für Unternehmen mit bis zu 500 Mitarbeitern

Das Erfolgskonzept von RadarServices

Speziell für Unternehmen mit bis zu 500 Mitarbeitern.

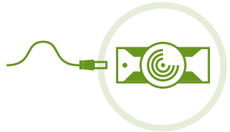
PLUG & DETECT

Kontinuierliches IT Security Monitoring leicht gemacht

RadarServices ist Europas führender Anbieter für kontinuierliches IT Security Monitoring. Das Portfolio wurde für die zeitnahe IT-Risikoerkennung – ursprünglich bei großen Unternehmen und Behörden – entwickelt. Es wurde über Jahre hinweg getestet, verbessert und perfektioniert.

Die Experten in Europas größtem Kompetenzzentrum für IT-Sicherheit haben auch die Sicherheit von kleinen und mittleren Unternehmen im Blick. Für diese Organisationen – mit ungefähr bis zu 500 Mitarbeitern - wurde Radar Smart Solution entwickelt.

Plug & Detect umfasst:



Plug

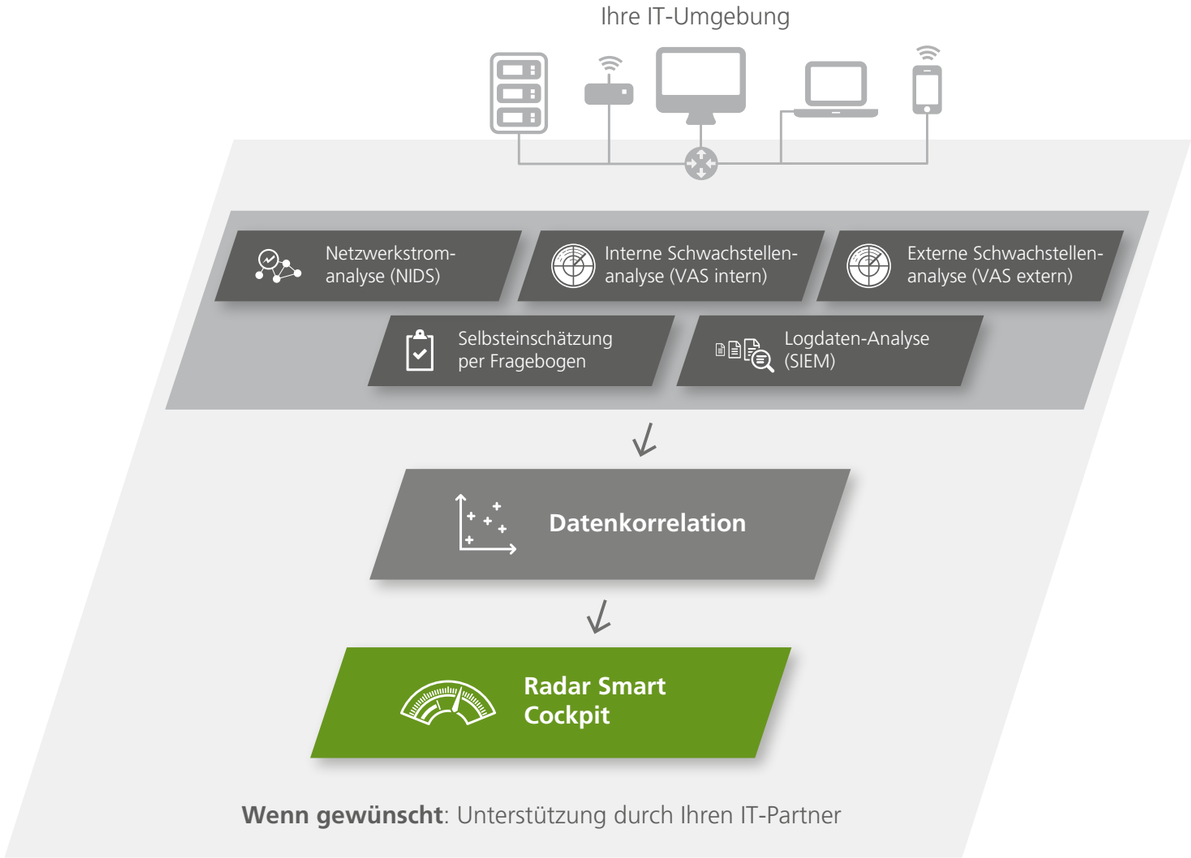
Radar Smart Solution besteht aus einer Hardware, der „Radar Smart Box“, die für die Datensammlung da ist. Die Verbindung der Radar Smart Box zu Ihrem Unternehmensnetzwerk ist einfach herzustellen.

Detect

Nach der Implementierung der Radar Smart Box werden Daten, die potenziell auf Sicherheitsrisiken hindeuten können, aus mehreren Quellen innerhalb des Netzwerks und auch von extern automatisiert gesammelt und analysiert. Im Radar Smart Cockpit bekommen Sie den Überblick über die gewonnenen Erkenntnisse: Wo gibt es Sicherheitsprobleme? Wurden unautorisierte Zugriffe auf Ihr Netzwerk erkannt? Und: Was konkret müssen Sie tun, um erkannten Problemen entgegenzuwirken und Ihre IT-Sicherheit insgesamt zu erhöhen?

RADAR SMART SOLUTION

Das System.



Ihre Vorteile

Wissen Sie heute, welche sicherheitsrelevanten Vorgänge in Ihrem Netzwerk gerade passieren?

WELCHE IT-SICHERHEITSMASSNAHMEN TREFFEN SIE AKTUELL?

Firewalls und Antivirussoftware gehören heute zum Standard.

DIE SCHLECHTE NACHRICHT:

Angreifer konzentrieren sich genau darauf, was herkömmliche Sicherheitsmaßnahmen nicht als Gefahr erkennen. Sie erkennen nämlich nur das, was man ihnen vorab als Muster mit auf den Weg gegeben hat und das reicht heute nicht mehr aus. So ist der globale Trend im Bereich der IT-Sicherheit zu erklären: Weg von der Gefahrenabwehr, hin zur Gefahrenerkennung und der Reduktion der tatsächlichen statt der fiktiven Risiken.

Radar Smart Solution erkennt die aktuellen Gefahren – Angriffe oder Schwachstellen in Ihrer IT – und berichtet Sie Ihnen in einer strukturierten, priorisierten und mit Hilfestellungen für die Behebung versehenen Reihenfolge.

Daten schützen, Patchen, Risiken erkennen, einschätzen und managen – wie priorisieren Sie die zahlreichen Aufgaben der IT-Sicherheit?
Zeitliche Ressourcen sind ein sehr knappes Gut. Das trifft besonders für den IT-Sicherheitsbereich in Unternehmen zu. Die Aufgaben sind zahlreich und vielfältig. Die Komplexität ist hoch und erfordert tiefes Expertenwissen aus verschiedenen Disziplinen. **Wie können Sie die vielfältigen Aufgaben so managen, dass Ihr IT-Sicherheitsniveau insgesamt bestmöglich erhöht wird?**

Radar Smart Solution ordnet die Aufgaben der IT-Sicherheit für Sie. Ausschlaggebend ist eine Priorisierung nach der geschätzten Höhe des Risikos. So wissen Sie genau, welche Prioritäten zu setzen sind und wo Sie Ihre zeitlichen Ressourcen am effektivsten einsetzen sollten, um Ihre IT-Sicherheit bestmöglich zu erhöhen.

Einzigartig

State of the Art Security in einer schlanken Form.

Radar Smart Solution wurde speziell für kleine und mittelständische Unternehmen entwickelt.

Das kontinuierliche IT Security Monitoring erfasst die wichtigsten Quellen für sicherheitsrelevante Informationen.

Die Cloud-Basis und die standardisierten, voll automatisierten Leistungsbestandteile ermöglichen die schlanke Form eines bisher nur für große Organisationen leistbaren IT Security Monitorings.

Das Radar Smart Cockpit, inklusive Behebungsanleitungen für Sicherheitsprobleme, ist in Ihrer Landessprache und in einer leicht verständlichen Form verfasst

Die Auswahl an verschiedenen Leistungspaketen erlaubt eine maximal mögliche Abdeckung des IT Security Monitorings je nach Ihren Budgetvorgaben.

Die je nach Ihren Bedürfnissen punktuelle oder dauerhafte Einbeziehung eines IT-Partners bietet Ihnen Flexibilität für die tatsächlich von Ihnen benötigte Expertenunterstützung und die Möglichkeit der Zusammenarbeit mit einem von Ihnen präferierten Partner.

Netzwerkstromanalyse (NIDS)

Gefährliche Malware und andere Risiken im Netzwerkverkehr werden signatur- und verhaltensbasiert analysiert.

Daten werden ständig aus dem Internet empfangen und an das Internet gesendet. Das betrifft nicht nur die von Ihnen bewusst gesendeten und empfangenen Daten. Auch Angreifer nutzen diesen Austausch. Radar Smart Solution erkennt verdächtige Muster und Anomalien wie z.B. Malware, Command and Control Server, Bots, Spyware, Drive-by Sources, DDoS Ziele und Quellen.

Signaturbasierte Erkennung erfolgt aufgrund von vorgegebenen Mustern. Angreifer nutzen aber vermehrt Wege in Ihr Netzwerk, die vorher noch nicht bekannt sind. Die verhaltensbasierte Erkennung ist genau auf diesen Bereich spezialisiert.

Je nach dem von Ihnen gewählten Paket ist eine maximal zu analysierende Datenmenge inkludiert.

Externe und interne Schwachstellenanalyse (VAS extern und VAS intern)

Kontinuierliche externe und interne Schwachstellen-Scans erkennen bestehende Schwachstellen in Ihrer IT und berichten sie, sodass Sie sie strukturiert beheben können.

Externe und interne Schwachstellen-Scans (in der Fachsprache Vulnerability Management and Assessment genannt) bieten Ihnen den Überblick über aktuell bestehende Schwachstellen in Ihrem Netzwerk. Das Resultat sehen Sie in Ihrem Radar Smart Cockpit: Eine klare Prioritätenliste für die Abarbeitung.

Neben den schnellen und effizienten authentifizierten oder nicht-authentifizierten Schwachstellen-Scans werden durch Compliance- und Passwort-Checks Konfigurationsprobleme in Bezug auf Anwendungen und Passwörter sowie User-Policies erkannt. Standard- oder fehlende Passwörter werden festgestellt. Veraltete Patch-Versionen bei installierter Software und Services werden bei Windowssystemen mit Registry und dll-Checks aufgedeckt.

Schwachstellen werden in hohes, mittleres und geringes Risiko und die Möglichkeit ihrer Ausnutzung kategorisiert. Das Ergebnis ist ein leicht verständlicher Überblick über die aktuellen Schwachstellen mit fertig aufbereiteten Informationen zur Erfüllung von Compliance Anforderungen. Mitarbeiterschulungen sind nicht notwendig.

Die Anzahl der Geräte, die für die Scans entscheidend sind, variiert je nach dem von Ihnen gewählten Paket. Je nach dem von Ihnen gewählten Paket werden entweder eine oder beide Arten der Scans durchgeführt.

Logdaten-Analyse (SIEM)

Logs sind eine wichtige Quelle, um sicherheitsrelevanten Ereignissen auf die Spur zu kommen. Deshalb werden sie gesammelt, analysiert, korreliert und resultieren gegebenenfalls in Alarmierungen.

Logs aus verschiedenen Quellen in einem Netzwerk (Server, Clients, Netzwerkgeräte, Firewalls, Anwendungen, etc.) geben entscheidende Hinweise auf sicherheitsrelevante Ereignisse. Die Kunst besteht darin, die wirklich relevanten Informationen aus Millionen von Ereignissen herauszufiltern. In der Fachsprache nennt man dieses IT-Risikoerkennungsmodul Security Information and Event Management (SIEM).

Zahlreiche gängige Log Formate werden unterstützt. Legen Sie aus einer Liste an standardisierten Log-Quellen fest, welche daraus für Ihr Unternehmen relevant sind. Je nach dem von Ihnen gewählten Paket ist eine maximale Anzahl an Logquellen inkludiert.
Informationen und Ereignisse aus diesen Logdateien werden aggregiert. Durch eine State of the Art Correlation Engine mit kontinuierlich erweiterten und maßgeschneiderten Regeln und Policies werden potenzielle Risiken identifiziert.

Selbsteinschätzung per Fragebogen

Neben Erkenntnissen aus der automatisierten Risikoanalyse werden Rahmenfaktoren Ihrer IT-Sicherheit miteinbezogen.

Wie groß ist aktuell die Gefahr, dass Ihr Unternehmen Schäden durch einen Cyberangriff erleiden könnte? Radar Smart Solution ermöglicht Ihnen den Überblick über die Fakten, die Ihrem aktuellen IT-Risiko zugrunde liegen. Dazu gehören nicht nur die Erkenntnisse, die aus der automatisierten Risikoanalyse mithilfe unserer Werkzeuge gezogen werden. Auch Rahmenfaktoren, die Ihre IT-Sicherheit bestimmen, sind entscheidend. Organisatorische Details innerhalb und außerhalb Ihres Unternehmens werden regelmäßig im Rahmen einer einfachen und verständlichen Selbsteinschätzung abgefragt und in die Risikoanalyse einbezogen.

Datenkorrelation

Sicherheitsrelevante Daten werden mithilfe einer umfassenden Korrelation aus der großen Datenmasse herauskristallisiert. Korreliert werden Daten dabei sowohl innerhalb eines Risikoerkennungsmoduls als auch übergreifend über mehrere Module hinweg.

Eine einzelne Information innerhalb einer Datenmasse weist oftmals noch nicht auf ihre Sicherheitsrelevanz hin. Erst durch die Kombination von Informationen entstehen die wertvollen Puzzlestücke, die notwendig sind, um einem Angreifer auf die Spur zu kommen. Eine Korrelation von Logs mit Schwachstellen, IDS-Daten oder SIEM Erkenntnissen lässt einen Gesamtüberblick über sicherheitsrelevante Daten zu.

Korrelation und Cross-Korrelation basieren auf Regeln, Policies und selbstlernenden Algorithmen: Regeln werden vordefiniert, um Muster zu erkennen. Sie werden kontinuierlich erweitert. Policies werden verwendet, um festzustellen, ob spezifische Aktionen zur richtigen Zeit und am richtigen Ort stattfinden. Selbstlernende Algorithmen umfassen die Lernfähigkeit der Correlation Engine, zwischen normalem und abnormalem Vorkommen unterscheiden und Verhaltensveränderungen bei Applikationen, Servern und in anderen Netzwerkbereichen erkennen zu können. Eine Verwendung außerhalb der Geschäftszeiten, eine übermäßige Verwendung von Anwendungen oder anderen IT-Services sowie Muster im Netzwerkverkehr über die Zeit und im Vergleich zu vergangenen Perioden (unter Berücksichtigung von täglichen, wöchentlichen, monatlichen und saisonalen Schwankungen) sind Beispiele für die Erkennung von Anomalien.

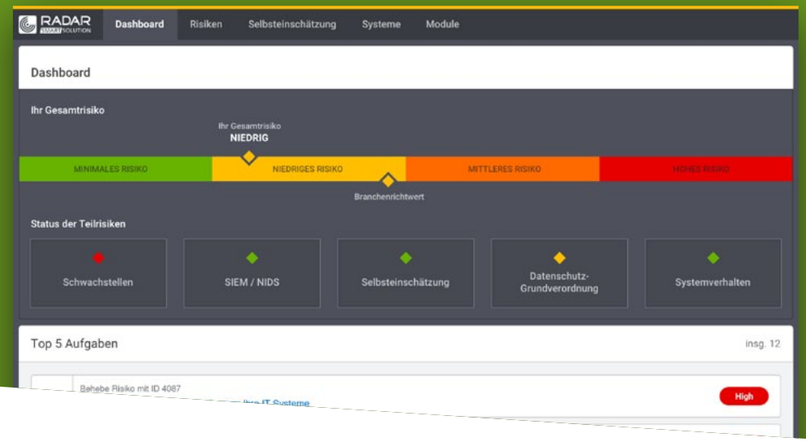
Threat Intelligence

Bringt die aktuellen sicherheitsrelevanten Informationen zusammen.

Threat Intelligence Informationen werden aus zahlreichen internen und externen, weltweit führenden, kommerziellen als auch Open Source-Quellen miteinbezogen. Mit ihnen wird schädliches Verhalten schneller erkannt – seien es zum Beispiel Verbindungen von oder zu verdächtigen IPs aus der internen IT-Infrastruktur.

Zu diesen Informationen gehören neben den IP-Adressen mit schlechter Reputation auch ebensolche URLs, für Phishing verwendete E-Mail-Adressen und für Schadsoftware verwendete Dateinamen, Dateipfade oder User Agents.

Die von RadarServices umfassend gesammelten und verarbeiteten sicherheitsrelevanten Daten gepaart mit den umfangreichen Threat Intelligence Informationen aus verschiedenen Quellen ermöglichen RadarServices unvergleichliche Schnelligkeit bei Detection & Response.



Radar Smart Cockpit

Alle gewonnenen Erkenntnisse werden zentral, verständlich und übersichtlich im Radar Smart Cockpit präsentiert. Sie sind priorisiert und mit Behebungshinweisen versehen. So wissen Sie, was wann zu tun ist.

Das Cockpit beinhaltet Ihren individuellen Überblick über die sicherheitsrelevanten Informationen, die die automatisierte Erkennung geliefert hat. Die Ergebnisse werden mit den festgestellten, klassifizierten und priorisierten Sicherheitsproblemen dargestellt.

Die Übersicht über die vorhandenen Geräte bietet die Möglichkeit auszuwählen, welche Geräte in die Überprüfung mit einbezogen werden sollen.

Sie wissen, was in welcher Reihenfolge erledigt werden sollte und halten bereits die Informationen in den Händen, die Sie für die nächsten Schritte der Behebung oder Risikominimierung benötigen. Ersparen Sie sich ein langes Suchen auf den Webseiten von einzelnen Herstellern. Radar Smart Solution liefert die wichtigsten Informationen gleich mit.

Expertenunterstützung auf Wunsch

Wie Sie ein IT-Partner im weiteren Vorgehen unterstützen kann.

Je nachdem wie viel Kapazität Ihnen in Ihrem Unternehmen für die IT-Sicherheit zur Verfügung steht, kann es sinnvoll sein, einen IT-Partner in die Aufgaben rund um das kontinuierliche IT Security Monitoring mit einzubeziehen.

Er kann Sie zum Beispiel in den folgenden Bereichen unterstützen:

- Tiefere Expertenanalyse der automatisiert erlangten Ergebnisse
- Unterstützung bei der Behebung von Risiken und/oder Schwachstellen
- Hilfe in dringenden Notfällen / akuten Angriffsfällen
- Ansprechpartner für weitergehende Fragen oder beim Handling der Risikoerkennungswerkzeuge
- Beratung bei Fragen rund um Ihre laufende IT-Sicherheit oder
- Durchführung von IT-Sicherheits- und Mitarbeiterschulungen

Übersicht über die Leistungspakete

Ihre Unternehmensgröße*	**1–50** Mitarbeiter	**50–100** Mitarbeiter	**100–250** Mitarbeiter	**250–500** Mitarbeiter
RADAR SMART SOLUTION Starter	NIDS (50 MBit) VAS Extern (2 IPs)	NIDS (100 MBit) VAS Extern (5 IPs)	NIDS (150 MBit) VAS Extern (10 IPs)	NIDS (200 MBit) VAS Extern (25 IPs)
RADAR SMART SOLUTION Basic	NIDS (100 MBit) VAS Extern (2 IPs) VAS Intern (50 IT-Geräte) Risikofragebogen	NIDS (200 MBit) VAS Extern (5 IPs) VAS Intern (100 IT-Geräte) Risikofragebogen	NIDS (300 MBit) VAS Extern (10 IPs) VAS Intern (250 IT-Geräte) Risikofragebogen	NIDS (500 MBit) VAS Extern (25 IPs) VAS Intern (500 IT-Geräte) Risikofragebogen
RADAR SMART SOLUTION Plus	NIDS (100 MBit) VAS Extern (2 IPs) VAS Intern (50 IT-Geräte) SIEM (5 Logquellen) Risikofragebogen	NIDS (200 MBit) VAS Extern (5 IPs) VAS Intern (100 IT-Geräte) SIEM (10 Logquellen) Risikofragebogen	NIDS (300 MBit) VAS Extern (10 IPs) VAS Intern (250 IT-Geräte) SIEM (25 Logquellen) Risikofragebogen	NIDS (500 MBit) VAS Extern (25 IPs) VAS Intern (500 IT-Geräte) SIEM (50 Logquellen) Risikofragebogen

* Die Unternehmensgröße erlaubt einen ungefähren Schluss auf die Anzahl der IT-Geräte in Ihrem Unternehmen/die Anzahl der IT-Geräte, die von der Risikoerkennung erfasst werden sollen. Die Anzahl der IT-Geräte ist die Basis für die Preiskalkulation.

RADAR SERVICES

The European Experts
in IT Security Monitoring
and IT Risk Detection

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

Radar Smart Solution ist die Plug & Detect Lösung für das IT Security Monitoring in Unternehmen mit bis zu 500 Mitarbeitern.

RadarServices
Zieglergasse 6
1070 Wien
Österreich

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

RadarServices Deutschland
Taunustor 1
60310 Frankfurt a. M.

T: +49 (69) 2443424 655
E: sales_germany@radarservices.com