IRMA

GANZHEITLICHER SCHUTZ VOR CYBERANGRIFFEN IN PRODUKTIONSANLAGEN

- Kognitive Anomalieerkennung und sofortige IT-Visualisierung
- Kontinuierliche Überwachung
- Einfache Handhabung – Umgehender Nutzen

VIDEC.

NEUE BEDROHUNGEN ERFORDERN NEUE LÖSUNGEN

Ganzheitliche IT-Sicherheit auf dem neuesten Stand der Technik

Die Herausforderung

Mit hoher Geschwindigkeit hält die Vernetzung und übergreifende Kommunikation von IT-Systemen Einzug in die Produktionen. Basis dafür ist das Industrial Ethernet. Strikt getrennte Netze für den Datenaustausch in Produktionsanlagen sind nicht mehr vorhanden. Diese Vernetzung von Produktionsanlagen und ihrer Steuerungseinheiten mit der Büro-IT oder über das Internet bietet den Unternehmen nicht nur Vorteile durch eine kontinuierliche Optimierung und Flexibilisierung der Fertigung – sie birgt auch viele Gefahren.

Etablierte Sicherheitselemente wie Antivirenschutz, Intrusion Detection oder Prävention Systeme erkennen nur bekannte traditionelle Schadsoftware wie Malware oder Trojaner. Für die neuesten Vorgehensweisen und Technologien heutiger Cyberangriffe ist dies nicht mehr ausreichend.

Deshalb stellt die effiziente Angriffserkennung und somit Absicherung von Produktionsanlagen gegen Cyberangriffe, interne Manipulationen oder fehlerhafte Konfigurationen eine zunehmende Herausforderung dar.

Ihr Anspruch

Sie wollen jederzeit den aktuellen Sicherheitsstatus Ihres IT-Netzes kennen? Die relevanten IT-Risiken sollen bekannt und bewertet sein? Auch im Falle eines Sicherheitsvorfalls, z. B. durch einen Cyberangriff, muss die Handlungsfähigkeit gewahrt bleiben.

Nur ein kontinuierliches Monitoring der Kommunikation in der Produktionsanlagen-IT entdeckt die neuartigen Cyberangriffe und Manipulationen. Um unmittelbar reagieren zu können und Schäden zu vermeiden braucht es eine intelligente Echtzeit-Analyse mit aussagekräftigen Alarmmeldungen, die priorisiert verteilt werden können.

Mit IRMA® haben wir für diese Herausforderungen eine IT-Sicherheitslösung auf dem aktuellsten Stand der Technik entwickelt.

Der Nutzen

- Erhöhung der Cybersicherheit durch Erkennen von Anomalien sowie der Industrial-IT Visualisierung ohne Security-Expertenwissen.
- Compliance – Erfüllung der wesentlichen Rechts- bzw. Unternehmens-Vorgaben & Branchenstandards.
- Aufwandsarme Betriebsführung durch einfachste Installation und Einrichtung sowie umgehende kontinuierliche Überwachung mit Alarmierung.

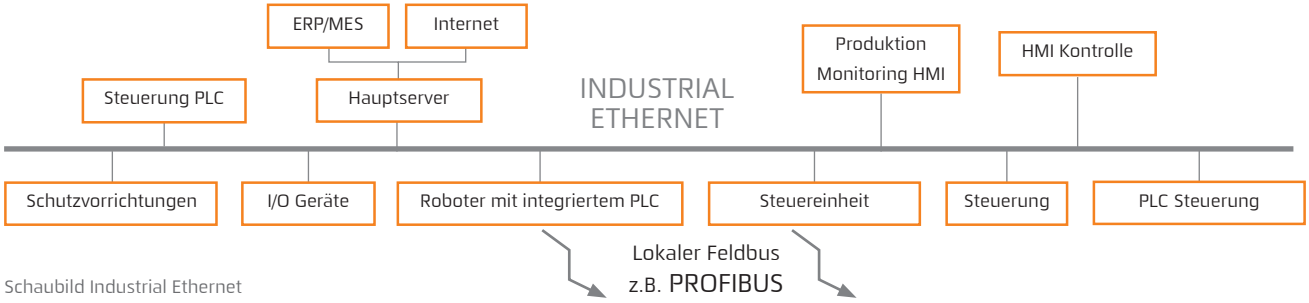


Schaubild Industrial Ethernet

Die Lösung: IRMA®

Mit IRMA® können Sie auf ein leistungsfähiges Industrie-Computersystem zurückgreifen, mit dem Cyberangriffe schnell identifiziert und abgewehrt werden können.

Ohne jegliche Aktivitäten im IT-Netz überwacht IRMA® kontinuierlich Ihre Produktionsanlagen, liefert Informationen zu Cyberangriffen und ermöglicht die risikobasierte Analyse sowie die intelligente Alarmierung mittels einer übersichtlichen Management-Konsole. So können Risiken frühzeitig bewertet und Aktionen verzögerungsfrei gestartet werden, um einen Angriff zu stoppen oder seine Folgen wirkungsvoll zu entschärfen.

IRMA® wurde als innovative IT-Lösung auf dem Stand der Technik entwickelt und gewährleistet damit Ihre anhaltende Handlungsfähigkeit im Falle eines Cyberangriffs.

Ihre Vorteile

- Optimale IT-Sicherheit auf dem neuesten Stand der Technik
- Unmittelbare Erkennung von Anomalien im IT-Netz
- Passive Überwachungsautomation
- Absicherung von nicht patchbaren Systemen, wie z. B. Windows NT/2000/XP, alte SPS, OPC Classic
- Absicherung von zertifizierten Produktionsanlagen und Prozessen ohne Re-Zertifizierung (z. B. Pharma, Chemie, Nahrungsmittel)
- Sofortige Einsatzbereitschaft durch einfache Installation und herstellerübergreifendes Konzept

IRMA® bietet Ihnen

- Vollständige Übersicht und Sicherheit Ihrer IT-Systeme, Netzwerk- und Datenverbindungen
- Integriertes Alarmmanagement für Cyber-Sicherheitsvorfälle
- Kontinuierliche Überwachung, Angriffserkennung und Reporting in Echtzeit
- Methodisches Werkzeug für eine zielgerichtete Risikoanalyse

MODULE + FUNKTIONEN

Kontinuierliche Überwachung

IRMA® erfasst und analysiert alle Systeme und Verbindungen ohne jegliche Aktivität im Netzwerk der Produktionsanlage.

Sofort nach der Validierung bzw. der Beurteilung im integrierten Risikomanagement überwacht IRMA® kontinuierlich Ihre IT-Infrastruktur und zeigt in Echtzeit Manipulationen oder Cyberangriffe an. Entscheidungen über maßgebliche Aktionen, die den Angriff stoppen oder die Auswirkung entschärfen, können so verzögerungsfrei getroffen werden.

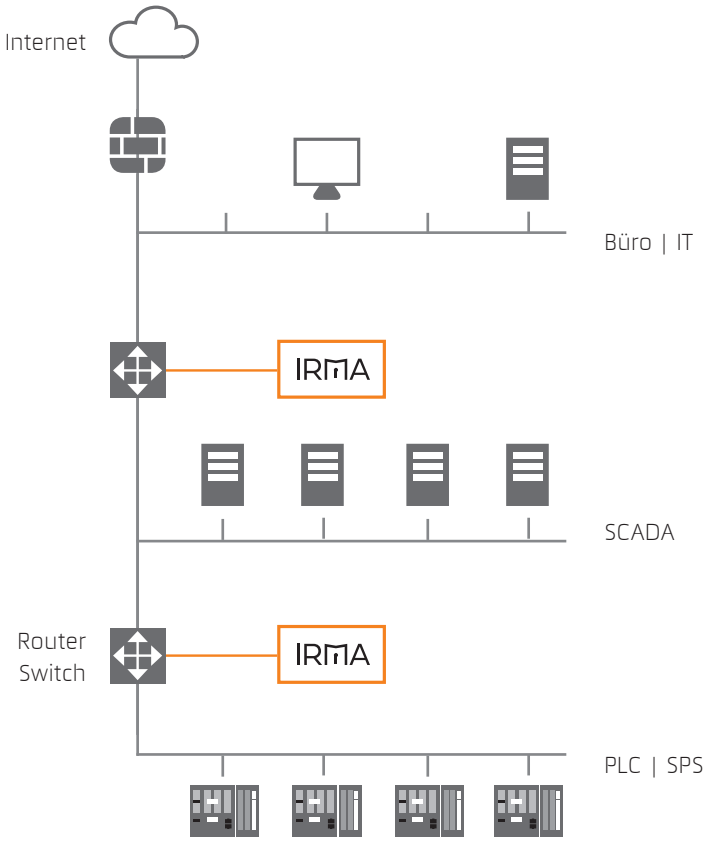
Intelligente Alarmierung

Alarmmeldungen werden in IRMA® priorisiert, angezeigt, verteilt und können auch online in ein Alarmmanagement überführt werden. Das Alarmmanagement hat eine Schlüsselfunktion an der Mensch-Maschine-Schnittstelle im Betrieb. Alarmierungen sind nur hilfreich, wenn die Häufigkeit und die Qualität der Informationen geeignet sind, die Betriebsverantwortlichen zu unterstützen.

Mit IRMA® erfolgt die Priorisierung von Alarmmeldungen wahlweise automatisch oder in effizienter Weise über das integrierte Risikomanagement. Die Alarmhäufigkeit ist dabei auf ein handhabbares Maß beschränkt und die Aussagekraft der Alarme ist sehr hoch.

Durch die bereitgestellten Informationen werden Cyberangriffe sofort erkannt. So werden umgehende Gegenmaßnahmen ermöglicht, die einen Angriff stoppen oder seine Folgen wirkungsvoll entschärfen.

IRMA® überwacht kontinuierlich Ihre Produktionsanlagen, liefert Informationen zu Cyberangriffen und ermöglicht die Analyse und intelligente Alarmierung mittels einer übersichtlichen Management-Konsole.



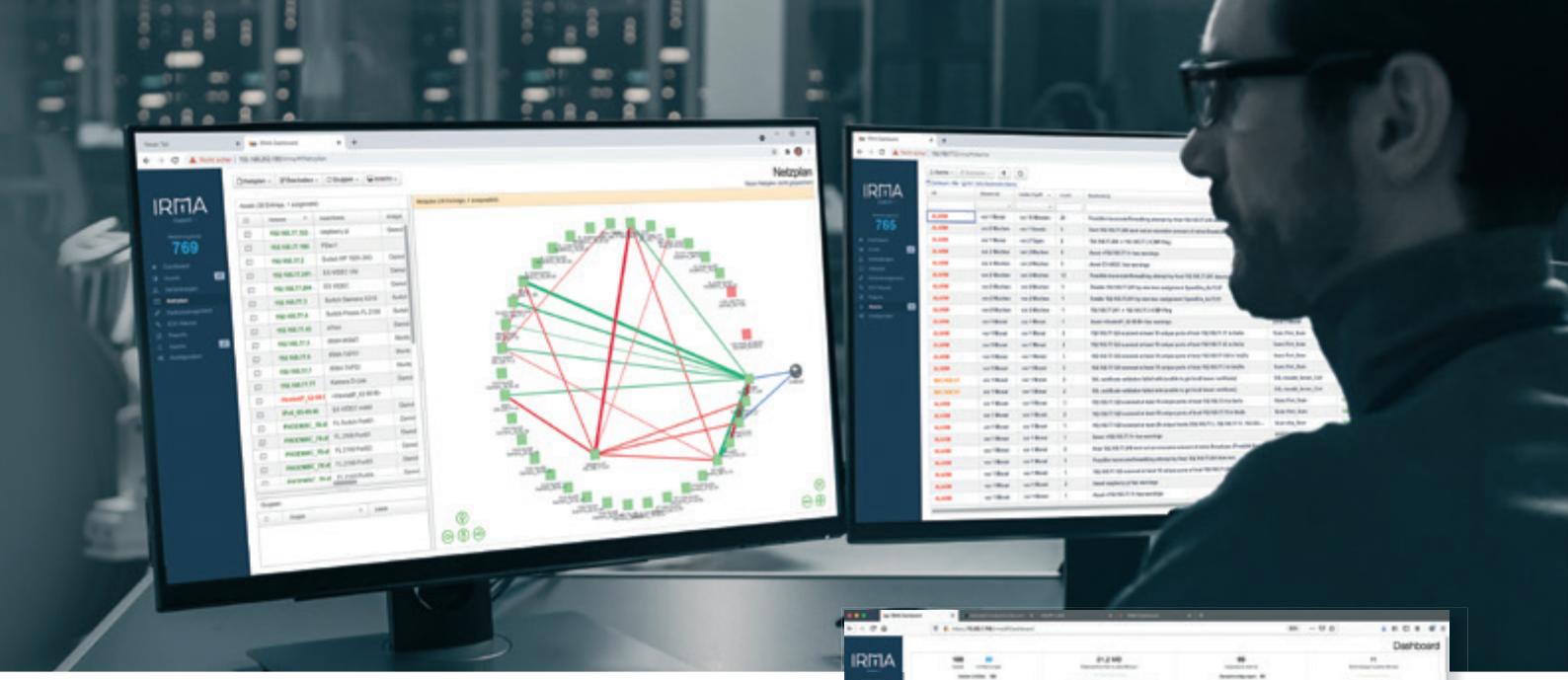
Effektive Analyse

Basierend auf diesen Erkenntnissen lassen sich notwendige und zielgerichtete Anpassungen der Sicherheitsarchitektur im Rahmen des Sicherheitsmanagementprozesses effektiv vornehmen.

Optional kann IRMA® Angriffsszenarien erkennen, Anomalien der Nutzung eigenständig identifizieren und durch Priorisierung im Risikomanagement die Alarmierung effizient steuern.

Übersichtliches Reporting

Mit komfortablen Reporting- und Exportfunktionen gewährleistet IRMA® jederzeit eine umfassende Übersicht. Durch die direkte Kopplung mit ihrem Alarmmanagement wird so eine effiziente Gefahrenabwehr und die Instandhaltung Ihrer IT-Infrastruktur gesichert.

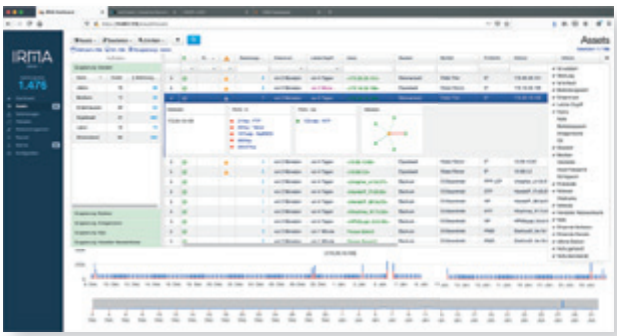


Module im Basissystem

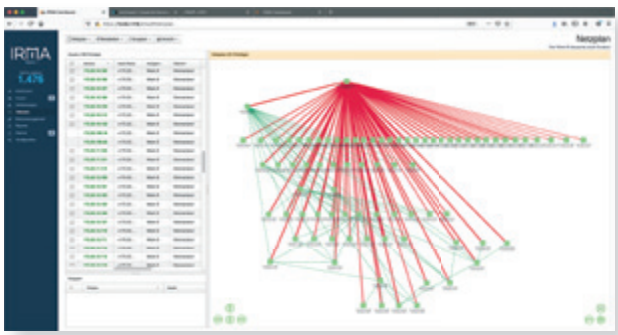
- Überwachung bestehender und neuer Produktionsanlagen und deren Systeme durch Soll-Ist-Vergleich der identifizierten Systeme und Datenverbindungen
- Überwachung insbesondere von Systemen, für die es aktuell keine Schutzmöglichkeit gibt bzw. aufgrund der hohen Betriebslaufzeit nicht mehr geben wird
- Alarmierungen
- Beurteilung aller identifizierten Informationen im Risikomanagement-Prozess in Bezug auf mögliche Betriebsrisiken, z. B. Ausfall, Produktionsqualität, Datenschutz
- Analysedaten zur Erstellung einer angepassten Sicherheitsarchitektur und Sicherheitstechnik in der Produktion
- Automatisierte Reports für Auditierungen

Optionale Module

- Zusätzliche Branchenstandards für KRITIS
- Erweiterung des Risikomanagements
- Zusätzliche Client TAPs für weitere Netzsegmente
- Strukturierung der IT-Komponenten im Produktionsprozess



IRMA® IT-Asset Detail



Darstellung eines Netzplans

EINBINDUNG + SCHNITTSTELLEN

Schutz vor neuen Gefahren

Einfache Installation

IRMA® ist das erste Überwachungssystem, das sich störungsfrei in den Produktionsprozess implementiert. In wenigen Schritten ist IRMA® bereit, ihr Produktionsnetzwerk zu überwachen – ohne zeit- und kostenintensive Implementierungsprozesse und Konfigurationen.

Sofortiger Nutzen

Für den Anschluss an das Netzwerk der Produktionsanlage erfolgt die Auslieferung im Passiv-Mode. Das System beginnt sofort mit dem Identifizieren, lernt ihr Produktionsnetzwerk kennen und zeigt es übersichtlich an. Auch bei segmentierten Netzwerken wird dabei die ganzheitliche Überwachung durch den Einsatz von IRMA®-TAP-Clienten gewährleistet.

Damit stehen Ihnen die Überwachungs- und Schutzfunktionen von IRMA® sofort zur Verfügung. Sie erhalten unmittelbar Informationen zu manipulierten System- und Datenverbindungen sowie zu Cyberangriffen.

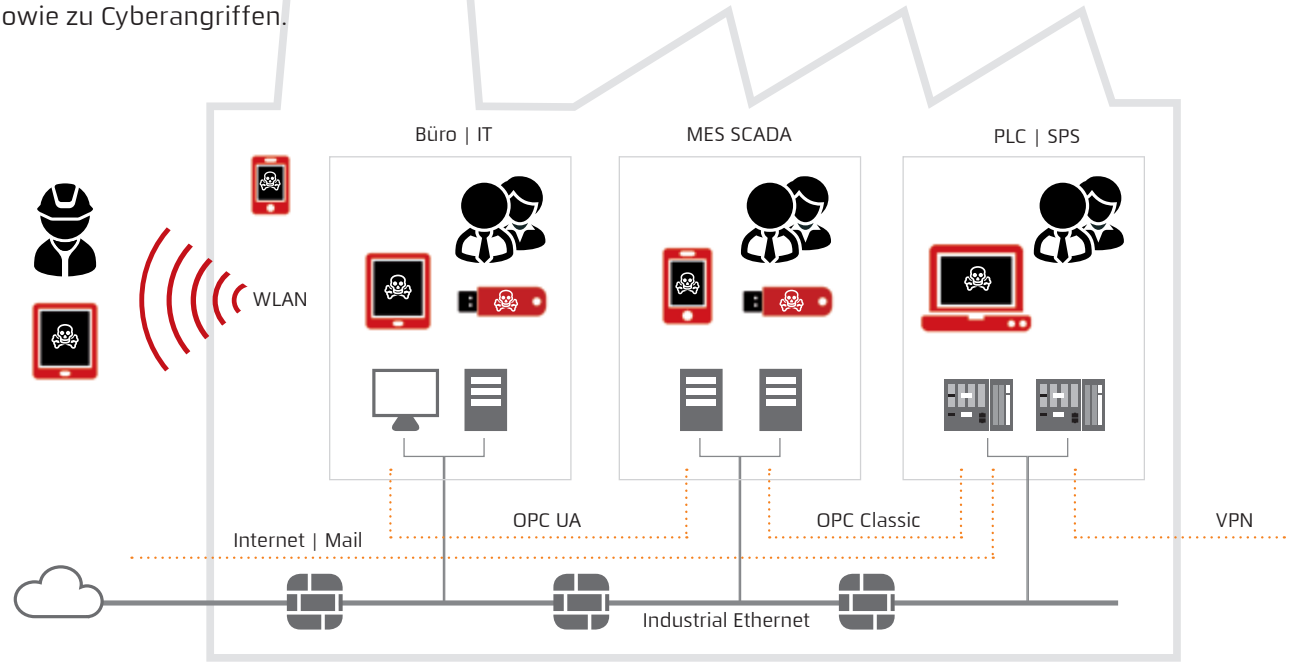
Intelligente Überwachung

IRMA® ermöglicht Ihnen, sämtliche Informationen nahtlos im Risikomanagement zu nutzen. Es lernt das kontinuierliche Überwachen und steuert die Alarmierung angepasst an die Schutzklassen in ihrem Risikomanagement-Prozess.

IRMA® liefert Ihnen alle notwendigen Daten, um Angriffe abzuwehren und Manipulationen umgehend zu beseitigen.

Herstellerübergreifende Einbindung

Egal, welche Hersteller in ihrer Produktionsanlage eingesetzt werden: IRMA® arbeitet auf technologischen Standards und damit herstellerunabhängig.



Neue Herausforderungen

Vorhandene IT-Sicherheitsvorkehrungen in Produktionsanlagen werden überwiegend nach dem Prinzip der Perimetersicherheit mit Firewalls und VPNs realisiert. Dies bedeutet, es werden wie mit einem Zaun oder Graben einzelne Bereiche voneinander abgetrennt, die untereinander nur zulässige Kommunikationsverbindungen erlauben.

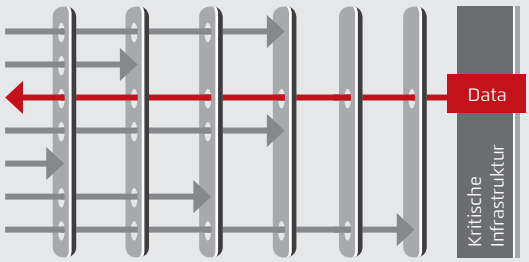
Solche Sicherheitselemente sind jedoch heute nicht mehr ausreichend. Viele Angriffsmethoden umgehen inzwischen die vermeintliche Sicherheit von Firewalls und VPNs gezielt, z.B. durch „drive by“. Dabei wird der Schadcode quasi „huckepack“ in zugelassenen Verbindungen mittransportiert und kann die vermeintlich sicheren Grenzen ungehindert passieren.

Mobile Gefahrenquellen

Außerhalb des Unternehmens genutzte Laptops der Mitarbeiter und Servicetechniker sowie Smartphones und Tablets werden oft schnell und unbemerkt während der Benutzung im Internet infiziert. Zum Beispiel nimmt der Servicetechniker, der am Vorabend im Hotel-WLAN seine Mails abruft und im Internet surft, am nächsten Tag das gleiche, jetzt infizierte Gerät – z.B. den Laptop, einen USB-Stick oder eine vorkonfigurierte Komponente – mit in den geschützten Bereich und verbindet es zum Datenaustausch mit der Produktionsanlage.

Angriffe von innen

Mit solchen infizierten mobilen Endgeräten gelangen die Werkzeuge der Angreifer dann unbemerkt von den Firewalls oder innerhalb der VPNs in die IT-Infrastruktur Ihrer Anlage und können sich dort unbeobachtet ausbreiten.



Wirkung von Sicherheitselementen eingehend/ausgehend

Sicherheit mit IRMA®

Mit IRMA® können neue Systeme und Verbindungen zu mobilen Endgeräten sofort identifiziert und analysiert werden. Für Firewalls und VPNs in der klassischen Perimetersicherheit ist eine solche Erkennung mobiler Geräte nicht möglich. IRMA® dagegen ermöglicht eine umgehende Beurteilung, ob die Verbindungen zulässig oder – z.B. infolge eines Cyberangriffes – unzulässig sind.

Überwachung in Echtzeit

Überwachung und Reporting in Echtzeit sind die Voraussetzungen für das Erkennen von Cyberangriffen, die Ihre Produktionsanlage bereits erreicht haben. Die von den Angreifern genutzten Werkzeuge und Datenverbindungen müssen kontinuierlich beobachtet, kontrolliert und analysiert werden, um die Ausbreitung und damit auch den Cyberangriff selbst zu stoppen.

Verlässlicher Schutz

Mit IRMA® ist diese kontinuierliche Überwachung aller Systeme und Datenverbindungen in ihrer Produktionsanlage gewährleistet. Cyberangriffe oder Ausfälle sind sofort sichtbar und können detailliert analysiert werden.

FUNKTIONSÜBERSICHT

IRMA

IRMA® bietet Ihnen

- Vollständige Übersicht und Sicherheit Ihrer IT-Systeme, Netzwerk- und Datenverbindungen
- Integriertes Alarmmanagement für Cyber-Sicherheitsvorfälle
- Kontinuierliche Überwachung, Angriffserkennung und Reporting in Echtzeit
- Methodisches Werkzeug für eine zielgerichtete Risikoanalyse

Das sagen unsere Kunden

- „Der Einsatz von IRMA® bietet eine sehr gute Möglichkeit, unsere hohen Ansprüche an die Prozess- und IT-Sicherheit und damit an die Versorgungssicherheit langfristig sicherzustellen."
- „Neben der Erhöhung des allgemeinen Sicherheitsniveaus werden wesentliche Controls der DIN ISO/IEC 27001 erfüllt."
- „Das Zertifizierungsverfahren nach § 11 Abs. 1a EnWG wird mit IRMA® deutlich erleichtert."
- „Es erfolgt damit ein zunehmender Anstieg der Organisationssicherheit für die Stadtwerke."

Ihre Vorteile

- Optimale IT-Sicherheit auf dem neuesten Stand der Technik
- Unmittelbare Erkennung von Anomalien im IT-Netz
- Passive Überwachungsautomation
- Absicherung von nicht patchbaren Systemen, wie z. B. Windows NT/2000/XP, alte SPS, OPC Classic
- Absicherung von zertifizierten Produktionsanlagen und Prozessen ohne Re-Zertifizierung (z. B. Pharma, Chemie, Nahrungsmittel)
- Sofortige Einsatzbereitschaft durch einfache Installation und hersteller übergreifendes Konzept
- Verfügbar in Deutsch und Englisch, weitere Sprachen auf Anfrage

Unterschiedliche Hardware-Varianten

SecurITy made in Germany

Weitere Informationen zu IRMA® finden Sie auf unserer Webseite www.videc.de.

VIDEC Data Engineering GmbH
Contrescarpe 1 · DE-28203 Bremen · Phone +49(0)421 – 33 950-0 · info@videc.de · www.videc.de
Niederlassungen und internationale Vertretungen entnehmen Sie bitte unserer Webseite.

VIDEC.

Es gelten die AGB der VIDEC Data Engineering GmbH | IRMA® ist ein Produkt der ACHTWERK GmbH & Co KG. Alle Rechte vorbehalten.

design: www.blaukontor.de
V23.12-D