IRMA®
SO EINFACH. SO SICHER!

IRMA®
SYSLOG EVENT MANAGER

SO EINFACH. SO SICHER.

- Passive Anomalieerkennung kombiniert mit aktiver Syslog-Protokollierung
- SIEM Funktionen für die Automatisierung
- Protokollierung und Detektion für Systeme zur Angriffserkennung IT-SiG2.0
- Kontrolle über das Netzwerk der Automatisierungen, Anlagen und Maschinen

INDUSTRIAL AUTOMATION

IRMA® SYSLOG EVENT MANAGER

IRMA® Syslog Event Manager ist die kostengünstige Lösung für Betreiber kritischer Infrastrukturen, Produktionsunternehmen sowie Anlagen- und Maschinenbauer. Syslog-Meldungen von OT-Geräten (SPS, Steuerungen, Gateways usw.), Netzwerkgeräten (Router, Switches, Firewalls usw.), Windows® und Linux®/Unix®-Hosts können mit IRMA® einfach angezeigt und analysiert werden. Die eingehenden Meldungen und Informationen lassen sich nach Zeit, Gerät / Asset, Schweregrad usw. filtern und bearbeiten. Zusätzlich lassen sich benutzerdefinierte Alarmierungen einfach einrichten.

Der IRMA® Syslog Event Manager verfügt über integrierte Aktionen, um angemessen auf kritische Syslog-Meldungen zu reagieren. Darüber hinaus gibt es Funktionen zur Archivierung, die Sie bei der Einhaltung von gesetzlich vorgeschriebenen Sicherheitsrichtlinien unterstützen.

Das Besondere …

Durch die Korrelation der Syslog-Meldungen mit der Anomalieerkennung im IRMA® System erhalten Sie zentral Systemmeldungen der Geräte und zeitgleich mögliche Änderungen im Verhalten innerhalb der Produktionsanlagen.

So sehen Sie auf einen Blick ob kritische Manipulationen erfolgt sind. Damit verbinden Sie Protokollierung und Detektion an einem Punkt. IRMA® unterstützt damit die schnelle Reaktion, um Ausfälle und Schäden zu verhindern.

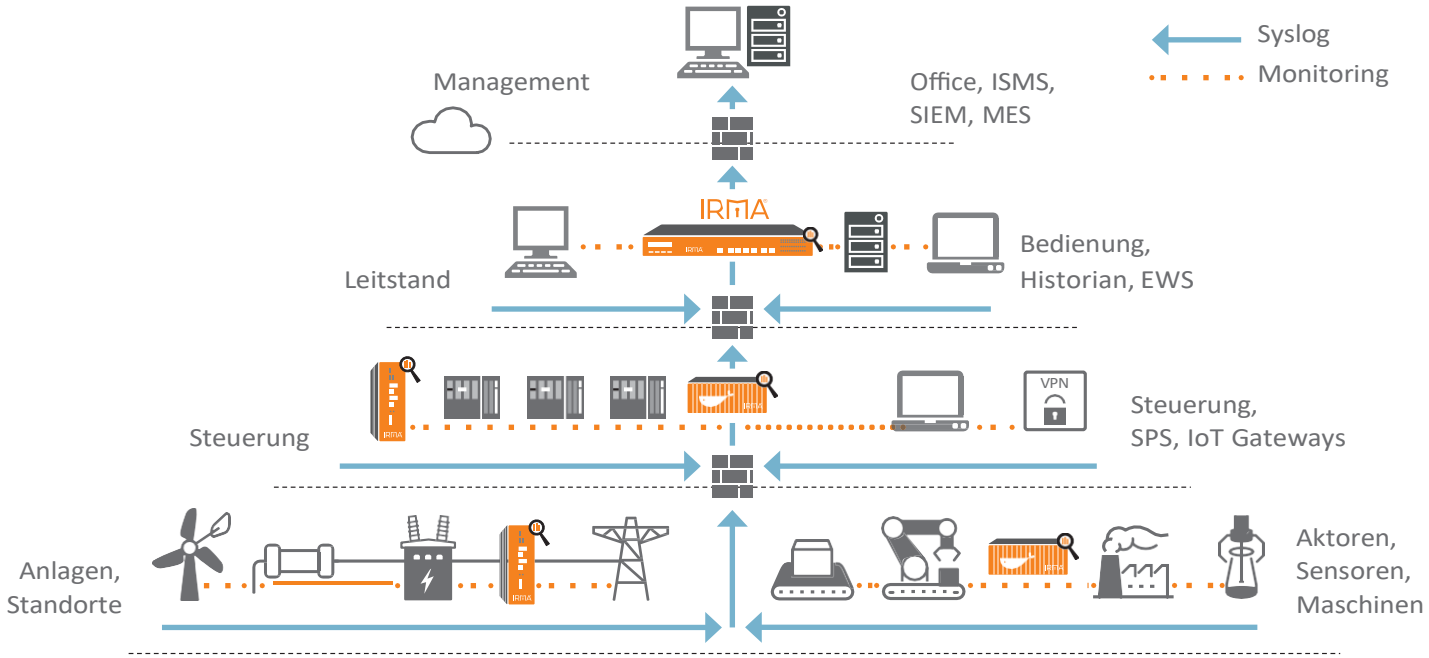
… für KRITIS

Ein Vorteil ist die schnelle Einführung oder Erweiterung der umfangreichen Protokollierungsinfrastruktur für Meldungen von Geräten in der Anlage der kritischen Dienstleistung. Außerdem können Vorgaben zur Umsetzung der Protokollierungen für Systeme zur Angriffserkennung sowie Compliance Vorgaben im Unternehmen hinreichend erfüllt werden.

… für Produktionsunternehmen, Anlagen- und Maschinenbauer

- Erhöhung der Verfügbarkeit
- Schnellere Instandhaltung und Serviceeinsätze
- Zustand des OT-Netzwerkes auf einen Blick

Dies ist ein wesentlicher Schritt zur Erfüllung der Anforderungen der EU-NIS Richtlinie.



Die Funktionen

- Zentralisierte Überwachung von Syslog-Meldungen und Windows®-Ereignisprotokollen
- Intuitive Webkonsole zum Anzeigen, Filtern und Bearbeiten
- Setzen von Filtern und Regelwerken für bestimmte Meldungen
- Reagieren auf Meldungen: Generieren von Alarmen, Senden von E-Mail-Warnungen
- Korrelation mit Verhaltensanomalien, die über passives OT-Netzwerkmonitoring analysiert werden
- Integrierte Archivierung zur Einhaltung von Vorschriften der Protokollierungen

Durch die einfache und strukturierte Darstellung der Ansichtsfilter und Regelwerke wird eine schnelle Einführung mit geringem Aufwand gewährleistet. Somit erhält der Nutzer eine schnelle Analyse bei auftretenden Anomalien bzw. einem Vorfall.

- Kombinierter Syslog-Empfang und passives Netzwerk-Monitoring
- Flexibel skalierbar – auch in großen segmentierten Netzwerken
- Entwickelt für die besonderen Anforderungen von OT-Geräten
- Unterstützt die Protokollerfassung von IPv4- und IPv6-Geräten

Erweiterte Syslog-Warnungen und Alarmierung

Systemweit oder per Gerätegruppe / Geräte lässt sich die Severity (Schweregrad) für den Empfang der Meldungen auswählen. Der IRMA® Syslog Event Manager enthält eine Vielzahl integrierter Aktionen, um im Falle eines Vorfalls automatisiert zu Alarmieren:

- Auslösen von E-Mail-Benachrichtigungen
- Alarmierung per RestAPI oder MQTT an ein SIEM oder den Leitstand
- Schaltung potentialfreier Kontakte

Die intelligente Warnfunktion des IRMA® Syslog Event Manager benachrichtigt Sie, wenn die vordefinierten Kriterien erfüllt sind. Diese Funktion ist basierend auf Zeit, Typ der Syslog-Nachricht, Syslog-Quelle usw.

Der IRMA® Syslog Event Manager benötigt keine Installation und ist somit sofort einsatzbereit. Die Lizenzierung erfolgt nach der Anzahl der Geräte, von denen Meldungen empfangen werden. Die Funktionserweiterung ist ab 1.250 € erhältlich.

Die Bedienelemente und die Philosophie sind identisch. Bestehende Nutzer des IRMA® Systems als reines passives OT-Monitoring sind somit innerhalb kürzester Zeit arbeitsfähig.

IRMA® – SO EINFACH, SO SICHER

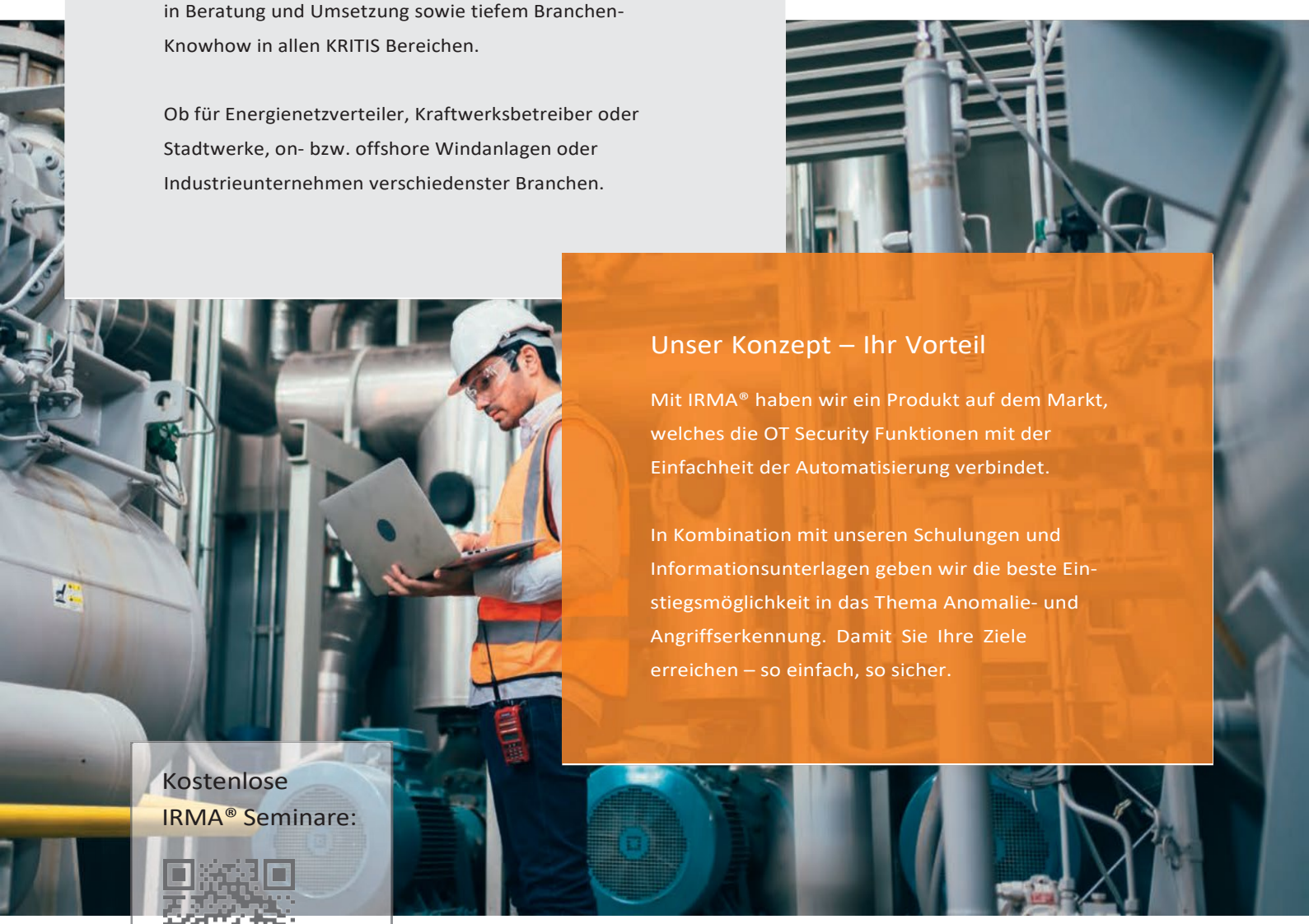
IRMA®

SO EINFACH. SO SICHER!

Einfach. Sicher. Kompetent

Wir bieten 30 Jahre Expertise im Bereich Automatisierung, gepaart mit umfassendem Erfahrungswissen in Beratung und Umsetzung sowie tiefem Branchen-Knowhow in allen KRITIS Bereichen.

Ob für Energienetzverteiler, Kraftwerksbetreiber oder Stadtwerke, on- bzw. offshore Windanlagen oder Industrieunternehmen verschiedenster Branchen.



Unser Konzept – Ihr Vorteil

Mit IRMA® haben wir ein Produkt auf dem Markt, welches die OT Security Funktionen mit der Einfachheit der Automatisierung verbindet.

In Kombination mit unseren Schulungen und Informationsunterlagen geben wir die beste Einstiegsmöglichkeit in das Thema Anomalie- und Angriffserkennung. Damit Sie Ihre Ziele erreichen – so einfach, so sicher.

Kostenlose
IRMA® Seminare:

Melden Sie sich hier an!
www.videc.de

Österreich:

Industrial Automation GmbH
Technikerstrasse 1-3 · A-6020 Innsbruck
Telefon +43 512 272271 - 0
Telefax +43 512 219921 - 3586
info@industrial-automation.at · www.scada.online

Schweiz:

Industrial Automation (Suisse) S.à.r.l.
Rue du Village 5 · CH-1052 Le Mont sur Lausanne
Telefon +41 21 5605400
Telefax +41 21 5880048
info@industrial-automation.ch · www.scada.online

INDUSTRIAL AUTOMATION

V2109-D