IRMA® SYSLOG EVENT MANAGER

IRMA®
SO EINFACH. SO SICHER!

SOFTWAREERWEITERUNG FÜR IRMA® SYSTEME

Zentralisierte Syslog Übersicht

Der IRMA® Syslog Event Manager ist eine Erweiterung in der Webkonsole des IRMA® Systems zum Managen und Archivieren von empfangenen Syslog-Meldungen für die zentrale Alarmierung.

Empfang und Analyse von Syslog-Meldungen erfolgt durch eine Erweiterung des IRMA® Monitoring Systems.

BESTANDTEILE

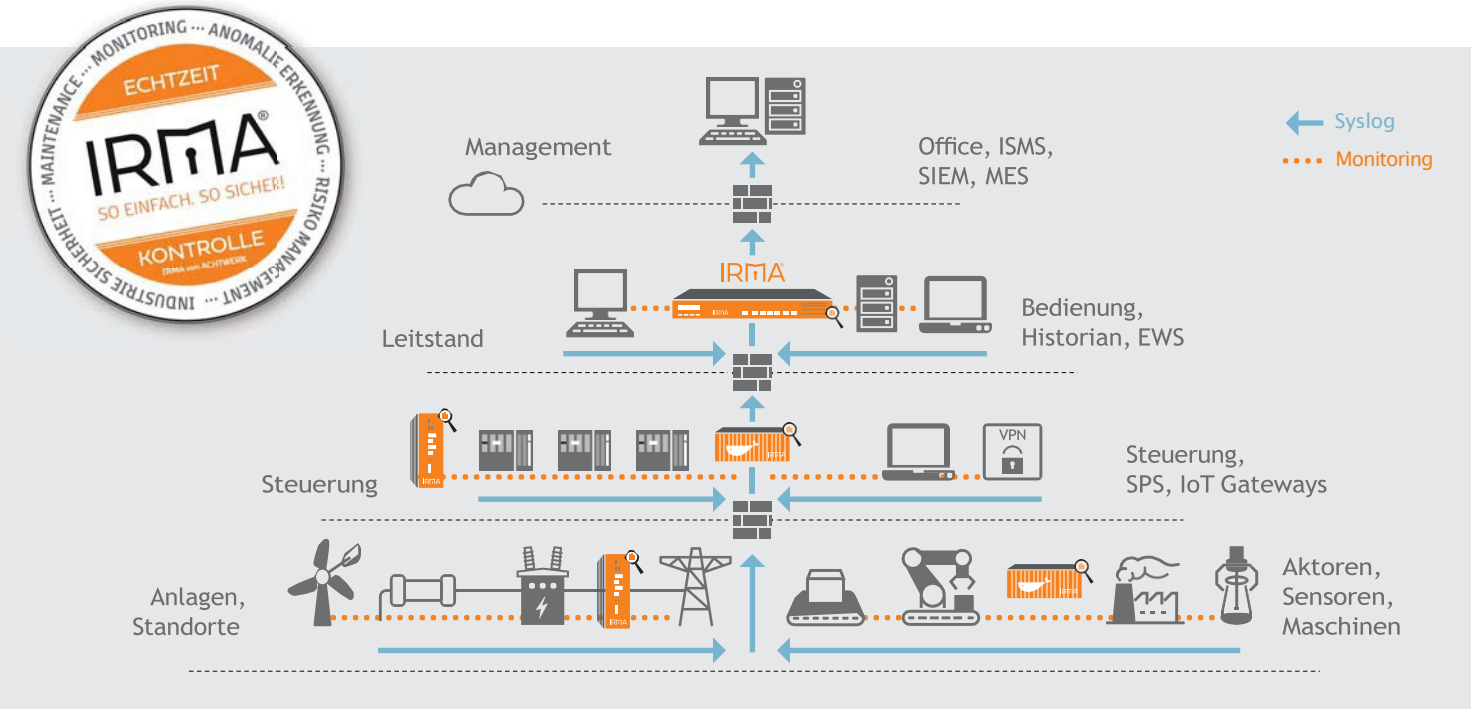
- Integrierter IRMA® Syslog Event Manager in der IRMA® Zentrale
- Lizenzierung des IRMA® Logdaten Empfängers

Der Vorteil: Die Meldungen werden durch das passive Monitoring des IRMA® Systems erfasst und analysiert - ohne die bestehende Syslog-Infrastruktur zu ändern.

Die Besonderheit mit IRMA® ist die Korrelation der Syslog-Meldungen mit den Informationen des passiven Netzwerkmonitorings zum aktuellen Verhalten der Assets und Kommunikationsverbindungen. So wird auf einen Blick erkennbar, ob kritische Manipulationen erfolgt sind.

HINWEIS: Für die Nutzung ist eine Lizenzerweiterung des IRMA® Systems zur Aktivierung des IRMA® Logdaten Empfängers notwendig.

IRMA® ist ein Industrie-Computersystem, welches passiv in einem Netzsegment die dort kommunizierenden Geräte und Verbindungen erkennt und analysiert.



Weitere Informationen zu IRMA® finden Sie auf unserer Webseite.

TECHNISCHE DATEN

FUNKTIONEN & PARAMETER

EMPFANG / IMPORT
Priority Severity: Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug, Unspecified - Konfigurierbar via IRMA® System, per Asset / Gerät

FILTERUNG
Priority: Facility, Zeit, Asset / Gerät, IP-Adresse, Schweregrad, Inhalte des Messagefelds (Texte, Wörter, u.w.)

SYSLOG PROTOKOLL
IPv4, IPv6, udp, port 514

REGELWERKE AKTIONEN
Mail, Kontakt, Alarm, Löschen

ALARMIERUNG
Mail, potentialfreie Kontakte, RestAPI, MQTT

DATENSICHERHEIT
Datenspeicherung erfolgt verschlüsselt. Administrative Änderungen werden im Auditlog gespeichert.

SOFTWARESCHNITTSTELLEN
RestAPI, SFTP, MQTT

MELDESCHWALL
Limitierung per Asset / Gerät, Zeiteinheit, systemweit

PARTITIONIERUNG / SPEICHERUNG
Stunde, Tag, Monat

ANZEIGE
Nach RFC3164, RFC5424 sowie properitären Strukturen

HINWEIS
Der maximale Durchschnittsdatenverkehr des eingesetzten IRMA® Hardware-Geräts ist zu beachten.

Einfach. Sicher. Kompetent.

Ein wesentlicher Schritt zur Anforderungserfüllung der EU-NIS Richtlinie: Mit der Kombination von Syslog-Meldungen und der Anomalieerkennung im IRMA® System verbinden Sie Protokollierung und Detektion an einem Punkt. IRMA® unterstützt damit die schnelle Reaktion, um Ausfälle zu verhindern.

Unser technischer Support stellt Ihnen gerne Anwendungsbeispiele verschiedener Komponenten (z.B. Server, Switche, usw.) zur Aktivierung der Syslog Funktionalität bereit. Übrigens: Termine für unsere IRMA® Syslog Event Manager Schulungen erhalten Sie auf Anfrage. Sprechen Sie uns an.

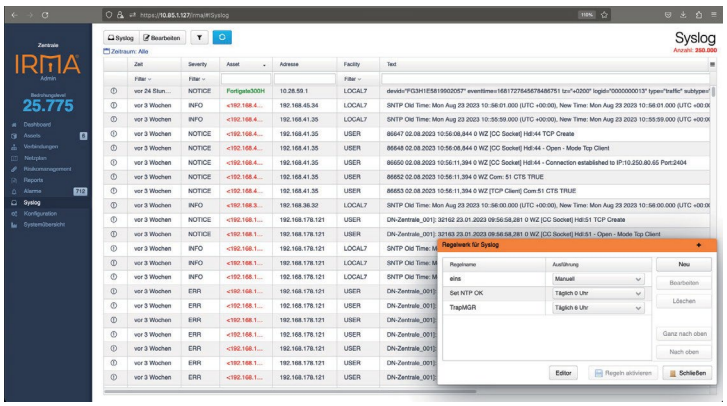


Abb.: IRMA® Syslog Menü Anzeige / Übersicht Regelwerke

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

design: www.blaukontor.de
V23.09-D