ACHT:WERK GmbH & Co. KG · Am Mohrenshof 11a · D-28277 Bremen

Verteiler:
Kunden, Partner, Support

Bremen, 10.03.2025

Sehr geehrte Damen und Herren,

dieses Dokument beschreibt die zusätzlichen Funktionen des IRMA® Systems in dem genannten Release. Rechtliche Hinweise:


Alle Inhalte, insbesondere Texte, Fotografien und Grafiken dieses Dokuments sind urheberrechtlich geschützt und dürfen nur im Einklang mit der Achtwerk GmbH & Co. KG abgeschlossenen Lizenzen kopiert oder offengelegt werden. Sollten Sie Teile hiervon verwenden wollen, wenden Sie sich bitte an den Vertrieb des IRMA®Systems. Für den Einsatz eines Netzwerk-Monitoringsystems und die Aufzeichnung von Kommunikationsdaten sind länder- und unternehmens-spezifische rechtliche Rahmenbedingungen zu beachten.

Wichtige Hinweise: Dieses Dokument, Begleittexte und Marketing-Dokumente wurden mit größter Sorgfalt erstellt. Fehler können jedoch nicht ausgeschlossen werden. Die in diesem Handbuch enthaltenen Informationen können jederzeit ohne Vorankündigung geändert werden und sind nicht als Zusage oder Verpflichtung seitens Achtwerk GmbH & Co. KG zu interpretieren. Daher kann eine Garantie oder juristische Haftung nicht übernommen werden.
Für Nutzer des IRMA® Systems wird ein gesonderter Vertrag abgeschlossen, der Weiteres regelt.

Wir behalten uns vor, Benutzerhandbücher und andere Dokumente sowie die Spezifikation des IRMA® Systems jederzeit und ohne Vorankündigung zu ändern. Änderungen können in zukünftigen Benutzerhandbüchern berücksichtigt werden; es besteht jedoch keine Verpflichtung zu einer zeitnahen Überarbeitung und Bereitstellung weiterer Benutzerdokumente.

Beim Release V25.02 handelt es sich um einen Major-Release.

DAS VERFAHREN DES OFFLINE UPGRADES (HANDBUCH: KAPITEL „SYSTEM UPDATE“) IST ZWEIMAL DURCHZUFÜHREN.

Erstellen Sie zuvor ein Backup der Daten vom IRMA® System.

Während des Upgrades wird empfohlen die Monitoring Netzanschlüsse zu trennen oder deaktivieren.

Das Upgrade der Software der IRMA® Geräte erfordert eine kontinuierliche Stromversorgung, Verfügbarkeit der Netzwerkinfrastruktur und Verbindung der Client TAPs zur Zentrale.

1. Durchgang:

Starten Sie mit der Achtwerk Upgradeseite https://office.acht-werk.de/upgrade-stable21 wie in der Bedienoberfläche angezeigt. Es werden das bestehende Betriebssystem und die vorhandenen Softwaremodule aktualisiert und für das Upgrade vorbereitet.

Führen Sie danach einen Warmstart aus und prüfen Sie die Version der IRMA® Zentrale. Es muss [stable25] angezeigt werden:

IRMA Version v24.06 [stable25]
Release Zeit 27.09.2024, xx:xx:xx
Geräteversion: 24.06~250xxxxxxx

2. Durchgang:

Hier nutzen Sie die Achtwerk Upgradeseite https://office.acht-werk.de/upgrade-stable25
(NICHT .../upgrade-stable21 wie in der Bedienoberfläche angezeigt!)

Das Upgrade wird ca. 600-700 MB (Paketreply-Datei) zum Download zur Verfügung stellen. Die Aktualisierung dauert 30-60 Minuten an. Es werden dabei das bestehende Betriebsystem und die vorhanden Softwaremodule aktualisiert.
Dieses Upgrade enthält einen Kaltstart der Geräte.

Prüfen Sie danach im Menü Konfiguration / Info und der Systemübersicht:

IRMA Version v25.02 [stable25]
Release Zeit 05.03.2025, xx:xx:xx
Die Geräteversion der IRMA® Geräte muss mindestens 25.02~250xxxxxxx sein.

Neue Funktionen:

- SYSLOG-Weiterleitung: Syslog-Meldungen und Ereignisse der Anomalieerkennung des IRMA® Systems können (automatisch) per Syslog weitergeleitet werden:
  - Weiterleitung der empfangenen und analysierten Syslog-Meldungen aus dem Syslog Event Manager
  - Ereignisse der Anomalieerkennung des IRMA® Systems
  - Audit Log Ereignis des IRMA® Systems
    Alle Syslog-Meldungen des IRMA® Systems werden mit Facility: User und Severity: Info versendet.

- OPC UA DA Server zum Austausch der Detektion-Metriken
  - Bedrohungslevel des IRMA® Systems
  - Anzahl Ereignisse mit Art „Alarm“ und „Info“
  - Anzahl der Assets mit Status Warnung
  - Server Security Mode ist "SignAndEncrypt" mit Zertifikaten und Standard Port TCP/4880

- REGELWERKE:
  - Erweiterung der Mailvorlage für die Aktion eMail senden
  - Erstellung individueller Mailtexte
  - Variablen: %(count) - Trefferanzahl, %(rule) – Name der Regel, %(time) – Zeitstempel, %(table) - Tabelle der Asset mit Detaildaten.

- OT-ASSETMANAGEMENT:
  - Erweiterung der Eigenschaftenfelder / Attribute eines Assets wie z.B. Produkt, Gehäuse, Seriennummer, Firmware, Status, Lifecycle, Durchstarten und freie Textfelder.

- VORAB-Import von Assets
  - Assets können vorab aus Projektierung oder CMDB importiert werden.
  - Abgleich mit den vorhandenen Assets erfolgt primär anhand der MAC-, alternativ per IPv4 Adresse.
  - Wird das Asset im Monitoring erkannt, wird das Feld „letzter Zugriff“ entsprechend aktualisiert. Initial ist das Feld leer.

- IM- und EXPORT der Netzwerke
  - Einfacher Im- und Export der IPv4-Netzwerke, die das IRMA® System überwacht und entsprechend Assets erzeugt
    HINWEIS: Mit dem Import können auch Netzwerkbereiche im öffentlichen IPv4-Bereich hinzugefügt werden.

- NOTIZEN:
  - Notizfeld zur Kommentierung von Alarmen
  - Erstellen von individuelle Texthinweise in den PCAP Dateien im Downloads

- RISIKOMANAGEMENT:
  - Mehrfachauswahl von Assets (Gruppen) zur Zuweisung zu Bedrohungen
  - Dedizierte Wahl der Schutzziele je identifizierter Bedrohung

- Erweiterung der Erkennung und Analyse der Layer 3 Protokolle
  - IPv4 (non-tcp, non-udp, non-icmp)
  - IPSEC (AH/EPS)
    HINWEIS: Diese Verbesserung wird ggf. neue Assets oder Verbindungen erkennen und anzeigen. Der Bedrohungslevel ändert sich!

- Verbesserung der Heuristik und Bestätigung der Verbindungsrichtung
  - zusätzliche Spalte Port(2) bei fehlendem Handshake
  - Manuelle Änderung der Richtung ohne erkanntem Handshake

- Benutzerrecht Syslog
  - Berechtigung für das Syslogmenü (Syslog Event Manager)

- LDAP / ADS Benutzerauthentifizierung
  - Abfrage Suchbasis im AD verbessert
  - Standardmäßig per User Principal Name (UPN). Fehlende Domäne im Benutzernamen wird automatisch die Standarddomäne genutzt (z.B. Username@domain.com).
  - Bei mehreren Domänen Eingabe des NetBIOS-Domänennamens das NTLM-Format (DOMAIN\Username)

Aktualisierung und Erweiterung der Security Parameter und Funktionen:


- TLS 1.3 ist default, Migration des HTTPS Zertifikat mit 3072 Länge
- SFTP mit PPKey
- OPC UA SecurityMode „SignAndEncrypt“ mit Zertifikaten
- De-/Aktivierung Supportzugang (SSH)
- Kennzeichnung der Funktionen und Konfigurationen für den sicheren Betrieb und sicherem System nach IEC62443-4-x (Handbuch)
- Aktualisierung der Opensource Software-Komponenten und Betriebssystem

Fehlerbehebungen:

- (Alarme) TTL Analyse Fehler, FalsePositive bei Traceroute / Firewalking Alarm [5690]
- (System) Performance - Debian10 CryptSetup Fix (intern) [5721]
- (System) Steuerung der Prozesse für die Verbindungen der Client TAPs [1016]
- (System) Performance für 10Gb Monitoring Netzanschlüsse [1016]
- (Assets) Behandlung ICMP Type 3 reply geändert – Es wird kein Asset erzeugt [5641]
- (Regelwerke) Fehler beim Synchronisierung der Regelwerke und Aktualisierung der Endpunkte Alarm der RestAPI behoben [5721]
- (System) Pcap Export Filter Verhalten [6295]
- (System) Falsche Darstellung Verbindung gleicher SRC / DST Port [5862]
- (System) Verbindungsrichtungen / Heuristik [3943] [3944] [5465] [5466] [5417]
- (Alarme) CONN::SWAP bei Drehung einer Verbindung (vormals auch CONN::DEL)
- (System) Suchbasis-Abfragen/LDAP funktioniert nicht [5055]