IRMA® BEDROHUNGSLEVEL

IRMA®
SO EINFACH. SO SICHER!

CYBERSECURITY IN INDUSTRIELLEN NETZWERKEN FÜR MANAGER & AUDITS AUF DEN PUNKT GEBRACHT

KOSTENLOSE IRMA® DEMO ANFORDERN

Eindeutiger Wert. Klare Information.

Als Intrusion Detection System erkennt IRMA® Teilnehmer und Anomalien in OT Netzwerken – rein passiv. Dabei lautet das Grundprinzip: Alle Teilnehmer im OT Netzwerk müssen validiert sein – denn alles Unbekannte stellt ein potenzielles Risiko dar. IRMA® handelt entsprechend: Zu jedem Asset wird ein Bedrohungswert gebildet und die einzelnen Werte zu einem zentralen Bedrohungslevel aufsummiert. Je geringer der Bedrohungslevel, desto mehr ist im Netzwerk validiert und damit bekannt. Als eindeutiger Wert ist der Bedrohungslevel somit der einfache Indikator für das unbekannte, und damit risikobehaftete, Verhalten im Netzwerk.

Der Bedrohungslevel steht aber nicht nur im IRMA® Dashboard zur Verfügung – er kann über verschiedene Schnittstellen von anderen Systemen abgefragt werden.

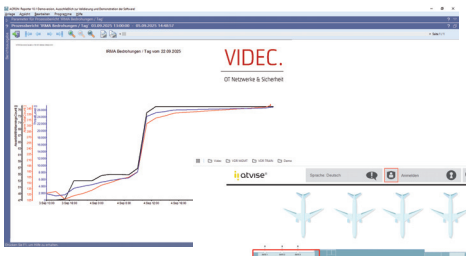

Abb.: Beispiel 1 - acron Reporter mit Prozessbericht "IRMA® Bedrohungen"

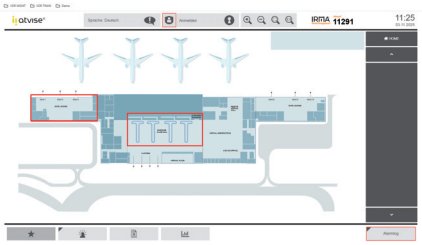

Abb.: Beispiel 2 - Anbindung an SCADA (atvise®)

FORENSIK & ALARME

Packet Capture (PCAP) für tiefe Analysen, Offline-Updates, Relais-Kontakte für Überwachung und Alarme, SysLog Event, Mail, IRMAGuard, uvm.

ACRON: SICHTBARE CYBERSICHERHEIT

acron Anwender sind mit Berichten und Anlagenwerten bestens vertraut. Diese Berichte können jetzt um den Faktor Cybersicherheit erweitert werden. Dank der OPC Anbindung werden der IRMA® Bedrohungslevel und weitere Kennzahlen erfasst und können in Berichten managementgerecht aufbereitet werden. Ideal für Industrie- und KRITIS-Umgebungen (NIS2/CRA-konform).

Ergebnis: Ihr Netzwerk wird transparent, die Awareness steigt, Gesetzesvorgaben werden eingehalten. So gibt IRMA® Ihnen in Zeiten steigender Cyberbedrohungen die Kontrolle über Ihr Netzwerk zurück – so einfach, so sicher.

Sie möchten IRMA® im acron Alltag erleben?
Vereinbaren Sie einen unverbindlichen Info-Termin.

KENNZAHLEN OPC UA

Bedrohungslevel, Asset mit Warnungen, Anzahl ungelesene Alarme, uvm.

COMPLIANCE-HIGHLIGHTS

Erfüllung von BSI IT-Grundschutz (KRITIS), NIS2, IT-SiG 2.0, SzA Reifegrad 3 und 4

BRÜCKE ZWISCHEN OT UND IT

SIEM Integration per Syslog Forwarder, Kennzahlen per OPC UA für SCADA / BDE/ Managementsysteme

IT SECURITY MADE IN GERMANY

In Deutschland entwickelt – seit 2015 im Einsatz

VIDEC.

Fordern Sie Ihre kostenlose IRMA® Demo an: Tim Karnau · Phone +49(0)170 – 9772264 · tim.karnau@videc.de · www.videc.de

BRÜCKE ZWISCHEN IT & OT

EIN FIKTIVER BLICK IN DIE PRAXIS

NEULICH AUF DER GESELLSCHAFTERVERSAMMLUNG
Aus der Sicht eines fiktiven Geschäftsführers

In den Räumen des Firmensitzes am Rande von Bremen tagte die Gesellschafterversammlung der ABC GmbH. Als das Protokoll zur Cybersicherheit kam, wurde es spannend.

"Herr Müller", fragte der Vorsitzende, "was konkret tun Sie als Geschäftsführer gegen die unsichtbaren Bedrohungen? Unsere Produktion ist KRITIS-relevant – NIS2 und der neue CRA verlangen mehr als bloße Versicherungspolicen. Wie stellen Sie sicher, dass wir nicht der nächste Opferfall sind?" Müller nickte - er war auf diesen Moment vorbereitet.

"Sehr geehrte Gesellschafter, Cybersicherheit ist kein Buzzword mehr, sondern unser täglicher Begleiter in der Produktion. Vor Monaten haben wir IRMA® als Kernsystem installiert – es erkennt Assets in Echtzeit und trackt Details wie neue Verbindungen oder verdächtige Aktivitäten. Darauf aufbauend liefert acron monatliche Management- berichte, die den Bedrohungslevel übersichtlich zusammen- fassen. Lassen Sie mich Ihnen den letzten acron Bericht zeigen." Kurz darauf erschien die acron Oberfläche auf der Leinwand: Klare Grafiken, farbcodierte Levels von 1 bis 20, mit einem stabilen Durchschnitt von 15 im vergangenen Monat. "Kein Alarmismus – volle Transparenz. acron fasst die IRMA® Daten zu einem Level zusammen, NIS2-konform dokumentiert – und für den CRA zeigt es unsere Resilienz in der Supply Chain, indem es Lücken in Assets aufzeigt".

Die Gesellschafter lehnten sich vor. "Aber wie läuft das im Alltag? Wer kümmert sich um die Details?" Müller lächelte. "Lassen Sie mich Ihnen von Hans und Mona erzählen. Hans ist unser Elektriker-Veteran mit 30 Jahren Fabrikerfahrung – er kennt jede Schraube in Halle B. Mona leitet die IT-Sicherheit, kompetent, findig, mit SIEM im Blut. Neulich blinkte bei Hans im Leitstand in IRMA® ein Bedrohungslevel 22 auf: 'Neue Verbindung, unbekanntes Gerät'. Hans ist beileibe kein Technikfreak, aber IRMA® ist so einfach gehalten – große Schriften, intuitive Farben – dass er sich direkt gekümmert hat. Er rief Mona an, sie checkte die IRMA® Logs: Eine Modbus-Verbindung über Port 502 zu einem neuen Sensor am Förderband, plus ein altes Relikt in Halle C, das Pings verschickte. Gemeinsam validierten sie es – Hans nannte es 'Förderband-Sensor 3', Mona prüfte auf Angriffe. Level runter auf 15, der acron Bericht notierte es sauber, Fall erledigt. Teamwork pur."

Müller scrollte durch den acron Bericht: "Sehen Sie hier die Timeline? Vorher-Nachher. Das ist keine Silo-Arbeit mehr – Produktions-OT und IT sind eine Brücke, die wir gebaut haben. Hans und Mona? Die sind ein Team: Lokales Know-how trifft auf smarte Tools." Und die Gesellschafter? Sie nicken jetzt zustimmend. 'Entlastet', hieß es am Ende der Runde. 'Machen Sie weiter so.' Müller lehnte sich zurück. IRMA® und acron waren mehr als Systeme – sie waren sein Sicherheitsnetz.

HINWEIS: Diese Erzählung wurde mit der Hilfe von KI erstellt und dient zur Veranschaulichung der Nutzung von IRMA® und acron im industriellen Umfeld. Die Personen und Handlungen sind fiktiv, die Darstellung der IRMA® und acron Features entsprechen jedoch der Realität.

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

VIDEC Data Engineering GmbH · Contrescarpe 1 · DE-28203 Bremen · www.videc.de
OTNetSec: Tim Karnau · +49(0)170 - 9772264 · tim.karnau@videc.de

V25.10-D