ANWENDERBERICHT

Automobilbranche setzt hohe Sicherheitsstandards

macmon secure unterstützt den Zulieferer JOYSONQUIN maßgeblich bei der Zertifizierung

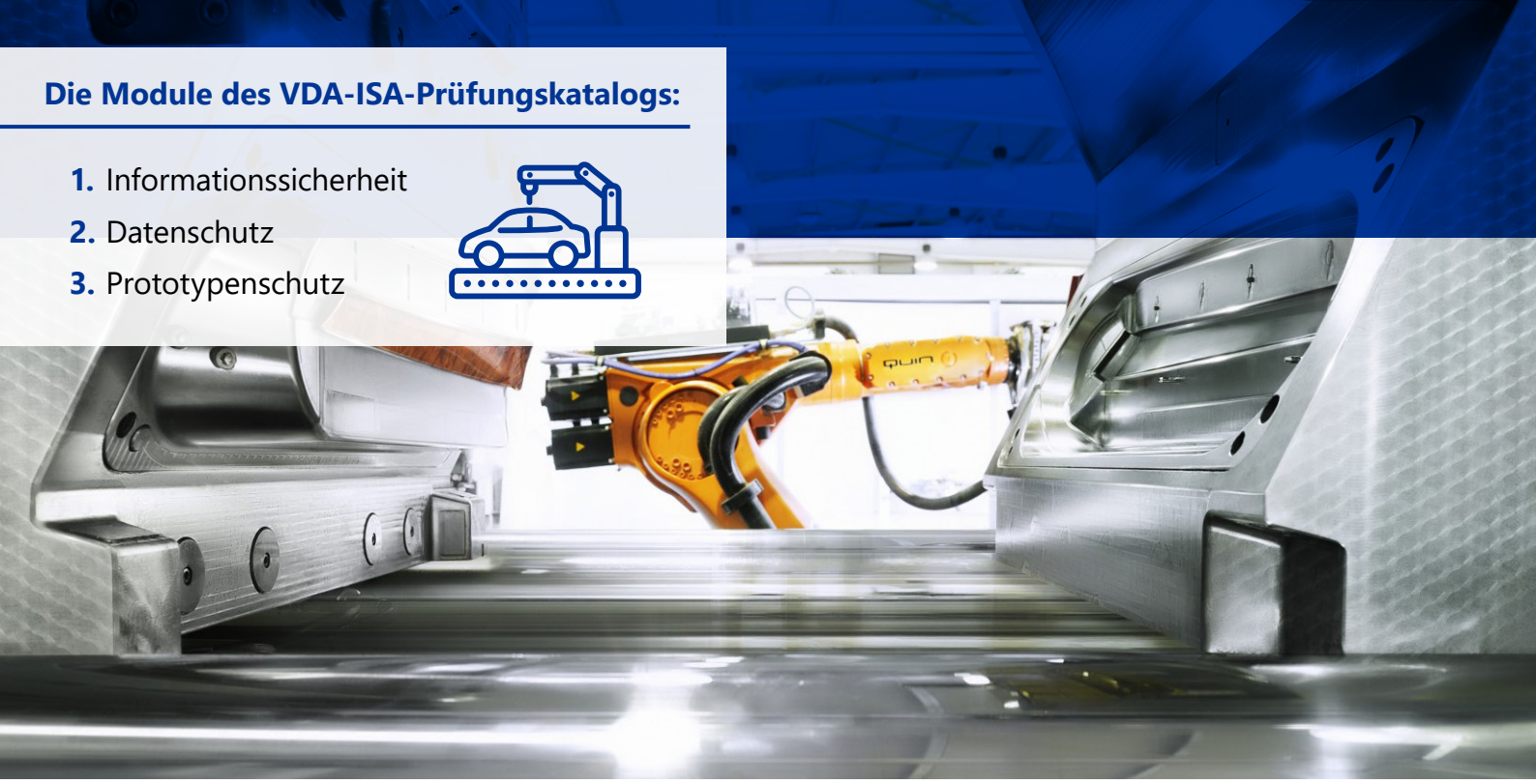
JOYSONQUIN Automotive Systems, ein gemeinsames Investment von SENSSUN und JOYSON Electronics ist ein globaler Automobilzulieferer mit rund 4.200 Mitarbeitern. JOYSONQUIN ist derzeit einer der drei führenden globalen Anbieter für hochwertige Innenraumausstattung für namhafte OEMs wie beispielsweise Mercedes-Benz, BMW, Porsche, VW/Audi, Tesla und GM. Darüber hinaus hat JOYSONQUIN einen großen Marktanteil bei Luftmanagementsystemen, Motorluftansaugsystemen und Waschsystemen im chinesischen Markt. Mit Standorten für Entwicklung und Produktion in China, den Vereinigten Staaten, Mexiko, Deutschland, Polen und Rumänien bedient JOYSONQUIN seine Kunden global. Durch die erfolgreiche Implementierung des **macmon Premium Bundle** konnte das Unternehmen die Zertifizierungsanforderungen seiner Kunden, in Rekordzeit erfüllen.

> *„Die Einführung des macmon Premium Bundle erwies sich als problemlos und einfach, wir erzielten sofort wichtige Mehrwerte für unsere IT-Sicherheit, die Implementierung fand nur wenige Wochen nach dem ersten Kontakt statt."*
>
> **Adriano Vasile** | Teamleiter IT-Infrastruktur | JOYSONQUIN

Adriano Vasile, Teamleiter IT-Infrastruktur, unter anderem verantwortlich für die IT-Sicherheit, ergänzt: „Wir haben den für uns notwendigen „Assessment Level 2 (AL2)" der TISAX®-Zertifizierung mit einem externen Datenschutzbeauftragten und unserem **IT-Systemhaus Luithle+Luithle GmbH** in nur wenigen Monaten mit einem Spitzenwert bestanden. Die Einführung des **macmon Premium Bundle** erwies sich als problemlos und einfach, wir erzielten sofort wichtige Mehrwerte für unsere IT-Sicherheit, die Implementierung fand nur wenige Wochen nach dem ersten Kontakt statt."

Die Module des VDA-ISA-Prüfungskatalogs:

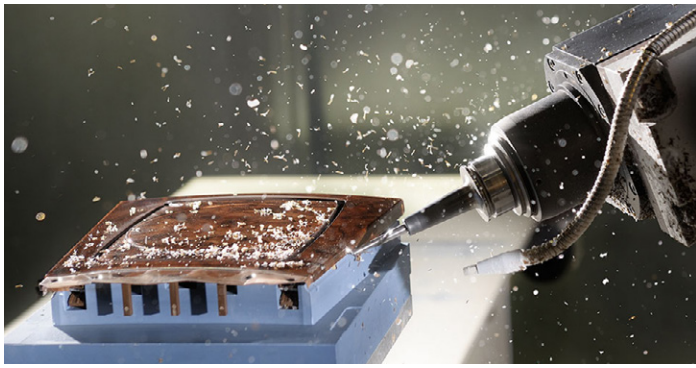
1. Informationssicherheit
2. Datenschutz
3. Prototypenschutz



Die Produktentwicklung in der Automobilindustrie unterliegt strengen Sicherheitsanforderungen – Innovationen müssen umfassend geschützt werden

TISAX® – standardisierte Sicherheit für die arbeitsteilige Automobilindustrie

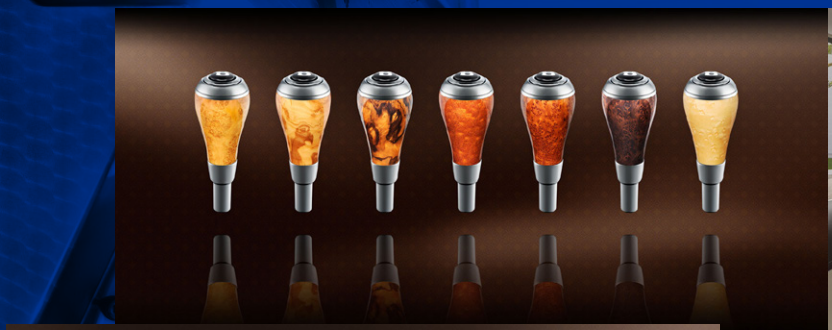
Der **Verband der Automobilindustrie** (VDA) hat mit TISAX® einen Standard für Informations- und Cybersicherheit geschaffen, der speziell an die Anforderungen der Automobilbranche angepasst ist. Ziel ist eine sichere Verarbeitung und ein vertrauensvoller Austausch von Informationen zwischen Zulieferern und Automobilherstellern. Mit TISAX® wird für Automobilzulieferer eine **Zertifizierung für Informationssicherheit** im Unternehmen geschaffen, die sich speziell an die Bedürfnisse der Branche richtet.

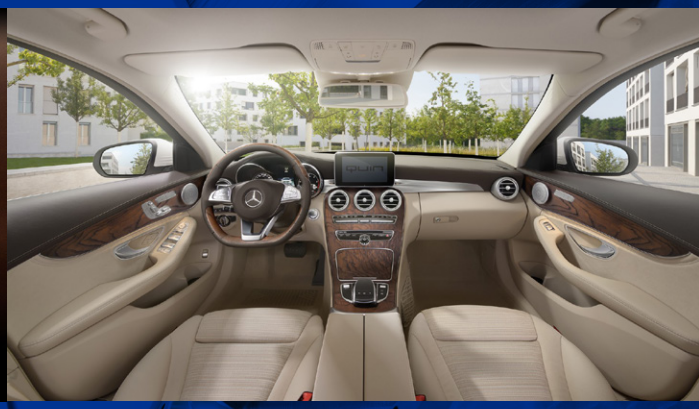


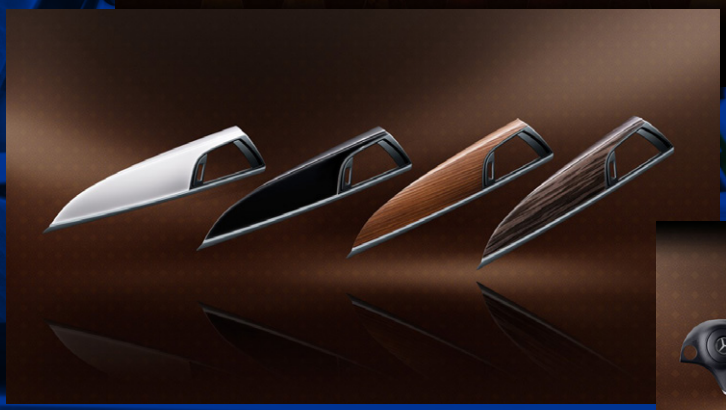
Die Produktion von JOYSONQUIN ist hoch präzise – die Security-Lösung von macmon ebenso

Der **Anforderungskatalog für die TISAX®-Zertifizierung** (VDA ISA) baut auf der internationalen Industrie-Norm ISO 27001 auf, enthält aber noch weitergehende Anforderungen. So sind beispielsweise speziell für die Automobilbranche die Bereiche Einbindung von Partnern in die eigene IT-Infrastruktur, Datenschutz und Prototypenschutz aufgenommen worden. Um die Zertifizierung zu erlangen, müssen Unternehmen die Anforderungen erfüllen, die im **VDA-ISA-Prüfungskatalog** festgelegt sind. Dieser besteht aus drei Modulen: **1. Informationssicherheit, 2. Datenschutz und 3. Prototypenschutz.**

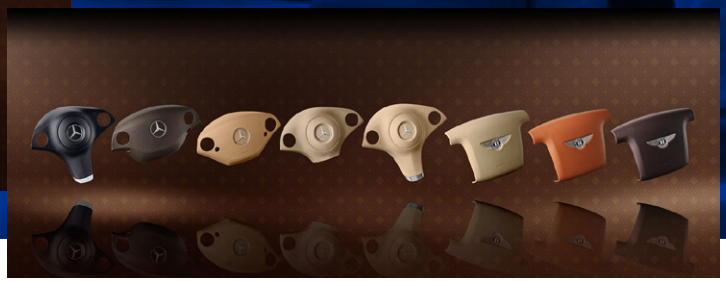
Die Informationssicherheit ist das Hauptmodul, basierend auf ISO 27001, das bei jedem Assessment geprüft wird. Die drei Sondermodule werden dem Assessment je nach Bedarf hinzugefügt. Ziel des **Moduls „Informationssicherheit"** der TISAX®-Zertifizierung ist es, dass die IT-Sicherheit in einem Unternehmen geplant, überwacht, geprüft und laufend verbessert wird. Dies setzt im Wesentlichen drei Dinge voraus: Standardisierte Prozesse, automatisierte Workflows und revisionssichere Reports. Hier greift **macmon Network Access Control** als IT-Security-Lösung ein.







Höchste Produktqualität „Made in Germany" – gesichert durch macmon secure aus Berlin



Schnell zur umfassenden Netzwerk-Übersicht und -Kontrolle

Das Asset Management im Sinne der TISAX®-Anforderungen beschäftigt sich zum einen mit Informationswerten (Daten/Informationen) und zum anderen mit Informationsträgern (IT/OT-Systeme jeglicher Art). Dabei ist es elementar, ein zentrales Verzeichnis über alle vorhandenen Assets sowie die zuständigen Personen zu führen. Durch den Einsatz von **macmon NAC** besteht bei **JOYSONQUIN** eine vollständige Transparenz über alle mit dem Netzwerk verbundenen Geräte. Gerätetypen können nach diversen Kriterien, wie dem Standort, dem Netzwerkzugang, dem Gerätetyp, dem Informationsgehalt und vielen anderen Eigenschaften gruppiert, und im Netzwerk verwaltet werden. **macmon NAC** erstellt damit ein Verzeichnis sämtlicher mit dem Netzwerk verbundenen Assets und liefert zudem ergänzende Informationen, wie den Lebenszyklus oder den aktuellen Standort der Geräte. Dazu Adriano Vasile: „Seit der Einführung von **macmon NAC** haben wir endlich die volle Kontrolle über alle Endgeräte, die Verwaltung der Switche läuft zentral über die macmon Konsole, und das mit nur wenigen Klicks – das war für uns am Anfang der absolute Wow-Effekt."

> *„Seit der Einführung von macmon NAC haben wir endlich die volle Kontrolle über alle Endgeräte, [...] und das mit nur wenigen Klicks – das war für uns am Anfang der absolute WOW-Effekt."*
>
> **Adriano Vasile** | Teamleiter IT-Infrastruktur | JOYSONQUIN

Langjährige Partnerschaften schaffen Vertrauen

Adriano Vasile beschreibt den Auswahlprozess für seine NAC-Lösung: „Nachdem die Forderungen unserer Kunden nach einer TISAX®-Zertifizierung deutlich formuliert wurden, haben wir uns an unseren Systemhaus-Partner gewandt. Es ist von großem Vorteil, einen kompetenten Partner an der Seite zu haben, der uns bei der Auswahl, Implementierung und Optimierung unserer Hard- und Software-Struktur unterstützt. **Luithle+Luithle GmbH** sind **Silber-Partner von macmon secure** und kennen seit vielen Jahren deren erprobte Lösungskompetenz. Nachdem ich an einem Webinar über den erfolgreichen Einsatz von **macmon NAC** bei einem anderen Unternehmen teilgenommen hatte, konnte ich schnell die richtige Entscheidung treffen."

Schadensbegrenzung durch Ereignisverarbeitung und situative Reaktion

Das Incident Management einer Organisation stellt die geordnete Verarbeitung von Informationssicherheits-Ereignissen dar und hat das Ziel, möglichen Schaden zu begrenzen und ein wiederholtes Eintreten zu verhindern. **macmon NAC** bietet neben der Kontrolle der Netzwerkzugänge und dem zugehörigen Regelwerk eine separate Ereignisverarbeitung, mit der individuell auf jede Situation reagiert werden kann. So werden die im Netzwerk ermittelten Informationen zu Endgeräten und Netzwerkgeräten verarbeitet und analysiert, um Angriffsereignisse wie ARP-Spoofing, MAC-Spoofing, informelle Ereignisse zu Network-Session-Started, aber auch Warnungen wie Endpoint-Almost-NonCompliant oder Network-Device-Changed zu generieren.

Auf Basis dieser Ereignisse (circa 50 verschiedene) wurden bei **JOYSONQUIN** diverse Reaktionen definiert, wie das Isolieren eines Endgerätes zur Schadenabwehr. Dabei können sämtliche Umgebungsvariablen wie Standort, zuständige Person und Uhrzeit als Bedingungen einbezogen werden, um individuell das Incident Management aktiv zu unterstützen.

Die Netzwerke von JOYSONQUIN werden rund um die Uhr vor kriminellen Zugriffen geschützt

Adriano Vasile ist begeistert von der macmon NAC-Performance: „Versucht sich ein nicht-autorisiertes Gerät im Netzwerk anzumelden wird das Gerät sofort geblockt und somit der Zugriff auf das Netzwerk automatisch unterbunden. Soll der Zugriff eines neuen Gerätes erlaubt werden, können wir das direkt in der macmon-Konsole konfigurieren und mit einem Klick innerhalb von wenigen Sekunden am entfernten Switch-Port das richtige Netzwerk (VLAN) aktivieren und somit den Zugriff gewähren. Dieser Prozess ist sehr komfortabel und spart wichtige Zeit und Nerven bei der IT-Administration."

„Versucht sich ein nicht-autorisiertes Gerät im Netzwerk anzumelden wird das Gerät sofort geblockt, und somit der Zugriff auf das Netzwerk automatisch unterbunden.

Adriano Vasile | Teamleiter IT-Infrastruktur | JOYSONQUIN

Sicherheitsrichtlinien für mobile Endgeräte geprüft und realisiert

macmon NAC unterstützt die Durchsetzung von Sicherheitsrichtlinien für mobile Endgeräte indem zum einen die Überprüfung der umgesetzten Sicherheitsmaßnahmen, wie Virenschutz, Windows Firewall oder installierte Patches geprüft werden und zum anderen, direkte Maßnahmen eingeleitet werden können. Mobile Endgeräte, die längere Zeit nicht im **JOYSONQUIN** Unternehmensnetzwerk angemeldet waren, werden in einem separaten Quarantänenetz überprüft, und falls nötig aktualisiert oder rekonfiguriert, um erst nach bestandener Sicherheitsprüfung wieder Zugriff zum Unternehmensnetzwerk zu erhalten. Die Integrität dieser Endgeräte wird durch Sicherheitsmaßnahmen aus den Bereichen des Fingerprinting, des WMI und SNMP sowie des Footprinting individuell verifiziert.

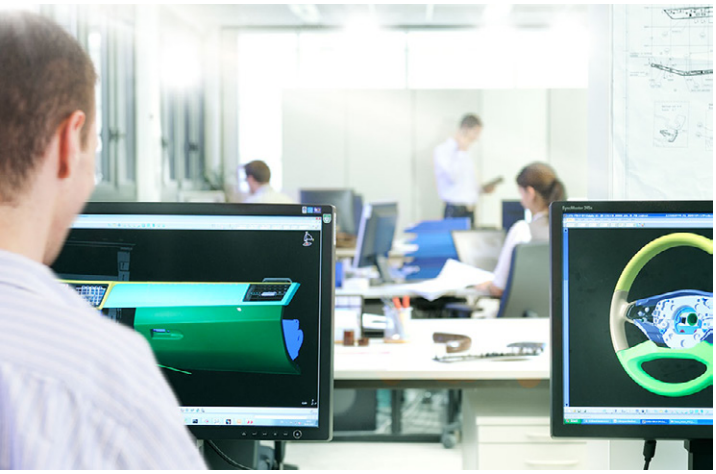
Einlass nur für vertrauenswürdige Endgeräte

Das Identity Management einer Organisation regelt die Identifizierung von vertrauenswürdigen Quellen für die Authentifizierung mit dem Ziel, nur berechtigten Personen und Geräten den Zugriff auf Unternehmensressourcen zu ermöglichen. Des Weiteren wurden im Rahmen der Zertifizierung von **JOYSONQUIN** Maßnahmen und Verfahren zur Protokollierung definiert, die die nachhaltige Dokumentation zum Auffinden von Sicherheitsverstößen ermöglichen.

macmon Network Access Control ist sowohl in der Lage Endgeräte und Benutzer zu authentifizieren als auch eine Kombination aus beiden Identitäten zu erkennen. Zum einen wird so sichergestellt, dass nur Geräte Zugang zum Netzwerk erhalten, die vertrauenswürdig sind und den Sicherheitsvorgaben entsprechen, und zum anderen kann in der Kombination mit Benutzeridentitäten geregelt werden, dass bestimmte Geräte nur von bestimmten Benutzern im Netzwerk betrieben werden dürfen. Auf diese Weise lassen sich Sicherheitszonen in Abhängigkeit der verfügbaren Ressourcen und Informationen definieren und mittels **macmon NAC** vor unbefugter Nutzung schützen. Dabei können, neben der Verwaltung der Zugänge und der Steuerung der Segmentierung, diverse Drittanbieter-Lösungen wie Firewalls oder IPS-Systeme integriert werden. Somit trägt macmon signifikant zur Verbesserung der IT-Sicherheit bei, was vor dem Hintergrund von Cyberkriminalität und Industriespionage in der Automobilindustrie besonders wichtig ist

Steuerung, Segmentierung und Management aller Endgeräte der JOYSONQUIN Netzwerkinfrastruktur

Die Operations Security einer Organisation regelt Verfahren zur Absicherung der IT-Netzwerkinfrastruktur mit dem Ziel, Aspekte der Informationssicherheit bei Änderungen der Geschäftsprozesse zu betrachten. Das geschieht ständig in Unternehmen mit globalen Lieferketten. Ferner soll sichergestellt werden, dass Zuverlässigkeit, Vertraulichkeit und Integrität der Daten gewährleistet sind. Denn allein für die komplette Entwicklung eines neuen Fahrzeugs investiert ein Automobilhersteller mehrere Milliarden Euro und befindet sich in ständiger Innovationskonkurrenz mit anderen Herstellern.



Nur autorisierte Mitarbeiter haben Zugang zu sensiblen Daten

> *„Die Segmentierung des Netzwerks ist eine grundlegende Funktion und gleichzeitig ein großer Mehrwert von macmon NAC."*
>
> **Adriano Vasile** | Teamleiter IT-Infrastruktur | JOYSONQUIN

Die Verwaltung und Steuerung der Netzwerke samt sämtlicher darin befindlichen Endgeräte und Netzwerkgeräte bildet das Grundprinzip von **macmon NAC**.

Adriano Vasile erklärt: „Wir sichern hochkritische Netzwerkbereiche durch interne Firewalls, während die Kommunikation durch die Firewalls nur für Endgeräte und Benutzer zugelassen wird, welche vorher durch **macmon NAC** eindeutig identifiziert wurden und die entsprechende Sicherheitsfreigabe haben. Die Segmentierung des Netzwerks ist eine grundlegende Funktion und gleichzeitig ein großer Mehrwert von **macmon NAC**, da wir neue Netzwerke auch leichter erstellen und schnell ausrollen können, das reduziert wiederum den Administrationsaufwand." Dabei können durch das interne IT-Infrastruktur Team die Grenzen zwischen Segmenten durch virtuelle Netzwerke (VLANs) oder auch Access Control Listen (ACLs) definiert werden, um so sicherzustellen, dass immer nur die berechtigten Personen und Geräte zu den jeweiligen Informationsdiensten und Informationssystemen Zugang erhalten.

Stand: 03/2023

Optimierung der IT-Sicherheit in der Automobilindustrie – ein kontinuierlicher Prozess

Das Unternehmen **JOYSONQUIN** optimiert kontinuierlich die Sicherheit und Performance seiner IT-Infrastruktur. In Zusammenarbeit mit dem **IT-Systemhaus Luithle+Luithle GmbH** werden nach der ersten zufriedenstellenden Phase der Implementierung die Erfahrungen mit **macmon NAC** gesammelt und bewertet. Zusätzliche Funktionen werden schrittweise implementiert, um die Netzwerksicherheit stets in bestmöglicher Art und Weise zu verbessern. Da **macmon NAC** auch interessante Schnittstellen zu seinen zahlreichen Technologie-Partnern anbietet, erwartet Adriano Vasile noch weitere Synergieeffekte. Auch die Betrachtung der globalen Netzwerkinfrastruktur, das Thema Sicherheit der OT-Netzwerke und die strategische Nutzung von Cloud-Diensten stehen auf der umfassenden Agenda des engagierten IT-Infrastruktur Experten.

Das macmon Premium Bundle bietet dem Automobilzulieferer JOYSONQUIN Übersicht, Compliance und Zugangskontrolle. Durch die Akquisition durch **Belden** erweitert **macmon secure** seine Expertise auf OT-Netzwerke, was in Kombination zu weiteren Optimierungen, Ergänzungen und Erweiterungen für Unternehmen der Automobilbranche führen wird.

FAZIT von Adriano Vasile, Teamleiter IT-Infrastruktur, JOYSONQUIN

Die Anforderungen an die Informationssicherheit in der Automobilbranche wachsen exponentiell. In diesem komplexen, globalen Wertschöpfungsprozess setzt IT-Security im Wesentlichen drei Dinge voraus: standardisierte Prozesse, automatisierte Workflows und revisionssichere Reports. Für die **TISAX®-Zertifizierung** wurde **macmon Network Access Control** (NAC) als **IT-Security-Lösung** schnell und einfach eingesetzt.

macmon secure GmbH | Alte Jakobstraße 79 - 80 | 10179 Berlin | Tel.: +49 30 23 25 777 - 0 | nac@macmon.eu | www.macmon.eu