ENGINSIGHT

DAS FAHRER-ASSISTENZSYSTEM für Ihre VDA-ISA (TISAX®)*-Zertifizierung

TECHNISCHE MASSNAHMEN DES VDA ISA-KATALOGS MIT ENGINSIGHT AUTOMATISIEREN

Als Auftragnehmer für die Automobilindustrie müssen Sie festgelegte **Qualitäts-, Informationssicherheits- und Datenschutz-Standards** erfüllen, um mit Automobilherstellern zusammenzuarbeiten. Die TISAX®*-Anforderungen sind vergleichbar mit denen der ISO 27001, beinhalten jedoch Unterschiede bezüglich der Prüfziele und Assessment-Levels. Sie müssen unter anderem nachweisen, dass sie über ein **etabliertes und zuverlässig funktionierendes Informationssicherheits-Managementsystem (ISMS)** gemäß ISO 27001 verfügen.

Informationssicherheit erfüllen und deren Einhaltung regelmäßig nachweisen

Der **VDA ISA-Katalog** zur Überprüfung der Informationssicherheit unterscheidet **organisatorische und technische Schutzmaßnahmen**.

Viele technische Vorgaben setzen Sie mit Enginsight einfach, nämlich automatisiert, um und sorgen darüberhinaus **dauerhaft für mehr Cybersicherheit in Ihrem Unternehmen**.

Ist die Norm einmal erfüllt, heißt es: Dran bleiben. In dreijähigem Abstand wird überprüft, ob die Anforderungen aufrechterhalten wurden.

So können bei möglichen Fehlentwicklungen schnell entsprechende Gegenmaßnahmen eingeleitet werden. Wichtig ist hierbei, dass die wiederholten **Risikobeurteilungen** stets konsistente, gültige und vergleichbare Ergebnisse liefern.

Automation schont Ressourcen und Nerven

Enginsight bietet enorme Potenziale, um zentrale Elemente der Audits zu automatisieren. Assetmanagement und Betriebssicherheit sind hier besonders hervorzuheben.

Enginsight bietet viele weitere **Automationsmöglichkeiten, die den Alltag von IT-Admins und CISOs erleichern**. Sie können Vorlagen für automatische Penetrationstest erstellen, die wiederkehrend zum Wunschzeitpunkt durchgeführt werden. Als Datengrundlage für die Zielsysteme dient die automatisierte IT-Inventarisierung. Sie sammelt und kategorisiert alle IP-Adressen im Firmennetzwerk.

Ein eindeutiges **Scoring** der Ergebnisse ermöglicht es Ihnen, die aufgespürten Sicherheitsrisiken zu bewerten und Maßnahmen zur Risikobehandlung zu priorisieren. Nichtkonformitäten erkennen Sie so einfach und können umgehend Korrekturmaßnahmen einleiten.

Zu Dokumentationszwecken und als Nachweis, lassen Sie sich die Ergebnisse jederzeit als PDF-**Report** ausgeben.

Wir zeigen Ihnen wie all' das und noch viel mehr im Detail funktioniert. Mit Sicherheit!

Mehr Sicherheit durch Automation

Scanergebnisse bleiben unabhängig von der Tagesform des Testenden.

- ✓ Arbeitsaufwand und Kosten werden deutlich reduziert.
- ✓ Neue IT-Assets werden inventarisiert, damit keine Schatten-IT entsteht.
- ✓ Alarme halten Sie stets auf dem Laufenden, so dass Sie im Bedarfsfall schnell handeln können.
- ✓ Sie bekommen jederzeit einen Live-Zustand zur IT-Sicherheit.

ZIELE NACH VDA-ISA (TISAX®)* MIT ENGINSIGHT UMSETZEN

Der TISAX®*-Fragenkatalog ist lang. Die technischen Anfoderungen sind nur ein Teil davon, doch lassen sie sich teilweise automatisiert umsetzen oder unterstützen, mit der richtigen Lösung – Enginsight. Nachfolgend eine Übersicht, welche technischen Anforderungen Sie mit Enginsight in den Griff bekommen.

VDA ISA Control	Relevanz/ Erfüllung	So erfüllen SIe die Vorgabe mit Enginsight
Asset Management		
1.3.1 Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?	unterstützend	Inventarisierung von IP-Adressen mit Hacktor
Incident Management		
1.6.1 Inwieweit werden Informationssicher-heitsereignisse verarbeitet?	unterstützend	Logging (IDS/Systemevents/File Integrity Mo-nitoring) + entsprechende Alarmszenarien
Physikalische Sicherheit und Business Continuity		
3.1.2 Inwieweit ist in Ausnahmesituationen die Informationssicherheit sichergestellt?	unterstützend	Forensik über Logs (IDS), Beweismittelsiche-rung, IPS
Identity & Access Management		
4.2.1 Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt?	unterstützend	Alarm: Versuchter Zugriff auf Objekte
IT Security / Cyber Security		
5.1.1 Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?	unterstützend	(wie A10 27001) Zertifikatverwaltung
5.2.3 Inwieweit werden IT-Systeme vor Schadsoftware geschützt?	✓	Pulsar zusammen mit GDATA
5.2.4 Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?	unterstützend	Logerfassung
5.2.5 Inwieweit werden Schwachstellen erkannt und behandelt?	✓	CVS Scoreing, Patchmanagement, Systeme ermitteln
5.2.6 Inwieweit werden IT-Systeme technisch überprüft (Systemaudit)?	✓	Pentests, Hacktor

ZIELE NACH VDA-ISA (TISAX®)* MIT ENGINSIGHT UMSETZEN

VDA ISA Control	Relevanz/ Erfüllung	So erfüllen SIe die Vorgabe mit Enginsight
5.2.7 Inwieweit wird das Netzwerk der Organisation gemanagt?	unterstützend	Netzwerk Überwachung, Mirkosegmentierung
5.3.2 Inwieweit wird das Netzwerk der Organisation gemanagt?	unterstützend	IDS, IPS + Alarme

Mit Enginsight lösen Sie vielfältige technische Anforderungen in einer Plattform

- ✓ IT-Inventarisierung (Asset Management)
- ✓ IT-Monitoring
- ✓ Schwachstellenmanagement
- ✓ Automatisierte Pentests
- ✓ Intrusion Detection und Intrusion Prevention
- ✓ Patch Management
- ✓ Mikrosegmentierung
- ✓ Endpoint Detection / Antivirus
- ✓ Websecurity
- ✓ Risikomanagement
- ✓ Security Configurations
- ✓ Security Automation

Trust Seal
www.teletrust.de/itsmig

SecurITy made in Germany

Zertifiziert durch TÜV THÜRINGEN
ISO 27001 / ID:15 121 21169
www.tuev-thueringen.de

ISMS nach ISO 27001 erfolgreich umsetzen! Wir machen es.

Jetzt Termin vereinbaren

*TISAX® ist eine eingetragene Marke der ENX Association.
Enginsight GmbH und die ENX Association führen keine geschäftliche Beziehung hinsichtlich der vorstehend beschriebenen Lösung. Mit der Nennung der Marke TISAX® ist keine Aussage des Markeninhabers zur Geeignetheit der hier beworbenen Leistungen verbunden.

ENGINSIGHT GmbH
Leutragraben 1
07743 Jena

+49 3641 271 49-66
hello@enginsight.com

enginsight.com - Machen Sie Unsichtbares sichtbar und Unsicheres sicher!