



Compliance Manager

## Compliance Manager

### Die Unterstützung bei der Erfüllung von Normen / Richtlinien

Konzernübergreifend stehen Anlagenbetreiber durch alle Branchen hindurch zunehmend vor der Herausforderung, ihre technische IT und Automatisierungsumgebungen nachhaltig gegen interne wie externe Bedrohungen abzusichern.

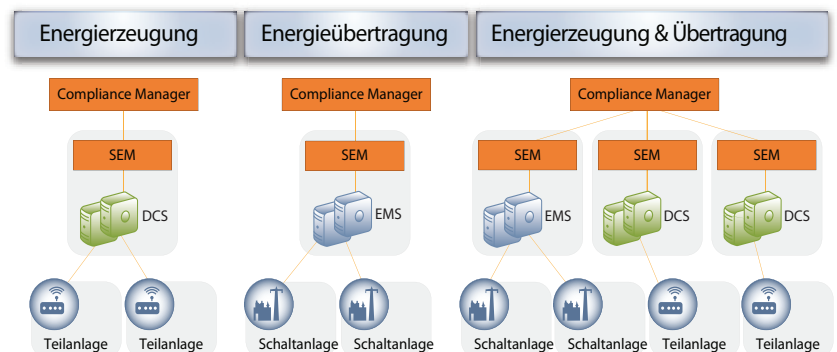
Industrial Defender, als führender Hersteller von IT-Security für kritische Infrastrukturen, bietet auf Basis einer konsequenten Defense-in-Depth™ Security-Strategie ein skalierbares Lösungskonzept an.

Der Compliance Manager von Industrial Defender ermöglicht den Betreibern, den Compliance- und Audit-Anforderungen von Richtlinien und Normen erfolgreich nachzukommen, ohne die Verfügbarkeit der Systeme zu beeinträchtigen. Die Compliance Manager Applikation erweitert die Funktionen Protokollierung und Warnmeldungen der Industrial Defender Security Event Manager (SEM) Konsole, indem sie zur Unterstützung des Audit-Prozesses, Erfassungs-, Archivierungs- und Reporting-Prozesse automatisiert. Der Compliance Manager erfasst und archiviert sowohl Auditeinstellungen als auch Konfigurationen von leittechnischen Systemen und Komponenten sicher. Somit steht Unternehmen ein integriertes, automatisiertes System zur Verfügung, von dem aus sie Audit-Reporting, Systemkonfiguration und Benchmarking verwalten können.

Zurzeit sind die Compliance Audits nach NERC CIP integriert. Eine Anpassung an weitere Normen und Richtlinien wird gerade durchgeführt.

### Entscheidende Vorteile

- Automatisierte Datenerfassung, Datennormalisierung, Archivierung und Reporting zur Unterstützung von Auditanforderungen
- Integriert und optimiert den Compliance-Prozess zur Verwaltung von unterschiedlichen leittechnischen System- und Softwareständen, transparent in einem Gerät
- Verwendet offene, standardbasierte Frameworks, um jährlich wiederkehrende Audit-Prozesse effizient zu gestalten
- Prüft kritische Infrastrukturen auf Bedrohungen unter Beachtung von Compliance-Anforderungen
- Automatisches Reporting optimiert zeitaufwändige manuelle Datenerfassung
- Verbessert leittechnisches Konfigurations- und Patchmanagement
- Ermöglicht Benchmarking von leittechnischen Systemkonfigurationen
- Speziell entwickelt für Compliance-Anforderungen von leittechnischen Systemen und Komponenten



## Anforderungen eines NERC CIP Audits

Organisationen mit NERC CIP Compliance Audits, stellen fest, dass dieser Prozess heutzutage meistens manuell abläuft, oft fehleranfällig und zudem zeitaufwändig und teuer ist. Der Compliance automatisiert und optimiert nicht nur einen Großteil dieses Prozesses, er geht auch die besonderen Herausforderungen an, die ein NERC CIP Audit-Prozess mit sich bringt, wie beispielsweise:

- Zusammenstellung notwendiger Daten, Berichte und Dokumentationen für ein Audit
- Sammlung und Archivierung aller relevanten Log- und Compliance-Daten
- Nutzung von Informationen unterschiedlicher leittechnischer Systemlieferanten
- Verifizierung von Korrekturmaßnahmen nach Richtlinienabweichungen
- Sicherstellung der ausgewählten Normencompliance auch bei zusätzlicher Einführung weiterer Unternehmens- bzw. Branchenrichtlinien
- Zeitersparnis durch Automatisierung der manuellen Prozesse

## Features

Unterstützung bei Audits / Analysen

- Umfassendes Audit-Reporting durch Automatisierung, Interpretation und Integration von Log-Events vieler verschiedener Anbieter von leittechnischen Systemen und Komponenten
- Sichere und zentrale Erfassung und Archivierung sowohl von Audit-Einstellungen als auch von Konfigurationen aus PLS, SCADA, HMI Workstations, und anderen kritischen Anlagen auch bei geringen Netzwerkbandbreiten und performancebeeinträchtigten Systemen
- Konfigurierbare NERC CIP Protokolle zur Erleichterung des Audit-Prozesses

Patch Management Support

- Aktuelle und umfassende Übersicht sämtlicher Patches, von Betriebssystemen und leittechnischer Softwareapplikationen, für einfacheres und schnelleres Patch Management
- Deltalisten zeigen Unterschiede zwischen Systemen auf und erleichtern den Abgleich mit Richtlinien und dokumentierten Soll-Zuständen
- Zentralisiertes Reporting für bessere Planung der Patch Management Strategie

Configuration Management Support

- Aktuelle und umfassende Auflistung der Konfigurationsparameter von leittechnischen Systemen und Komponenten
- Harmonisierung bestehender Konfigurationen mit Richtwerten für effizientere Durchsetzung von Standards und Normen
- Warnmeldung bei Änderungen oder Abweichungen nicht konformer Konfigurationen

Software-Inventarisierung

- Aktuelle und umfassende Auflistung von installierten Software-Applikationen
- Aktuelle und umfassende Auflistung von Betriebsmitteln und Bestandsinformationen

## Hardwareübersicht

Merkmale	Standard
Rack Konfiguration	2 HE
Prozessor	Intel Quad Core Xeon
Arbeitsspeicher	16 GB
Speicherkapazität	5 x 300 GB SATA Festplatten
Back Up-Speicherkapazität	2 x 1 TB SATA Festplatten
Speicherverfahren	Raid 10
Festplattenwechselstrategie	Hot-Swap
Energieversorgung	zweifach 230V DC, hot-swap fähig
Leistung	600 Watt
Wärmeabgabe	3264 BTU/h
Kühlung	redundanter Lüfter
Maße (BxHxT)	442 x 747 x 89 mm
Gewicht	29.5 KG

## KORAMIS GmbH

Kompetenzzentrum

Automatisierungstechnik & IT-Sicherheit

Neumühler Weg 32.1

D - 66130 Saarbrücken-Güdingen

Tel. +49 (0)681 - 968 191 - 30

Fax +49 (0)681 - 968 191 - 930

## KORAMIS – Ihr Partner für IT-Security

Als innovatives Unternehmen adressiert KORAMIS seit 1985 die Prozess- und Versorgungsindustrie und bietet Lösungen und Tools im technischen Umfeld von kritischen Infrastrukturen an. Im Bereich IT-Security ist KORAMIS Partner von Industrial Defender und bietet von der Risiko-Analyse über Lösungsimplementierung bis zum Support komplette Sicherheitslösungen aus einer Hand.