CARO-Suite

CARO bereinigt automatisch die Zugriffsrechte auf Ihren IT-Systemen

- Risikobewertung von Experten für Ihre IT-Sicherheit
- Berechtigungskonzepte erkennen und bewerten
- Automatisierte Bereinigungsprozesse
- Einfach integrierbar und leicht zu bedienen

CARO-Analysis©

Für Ihren Durchblick

Die Fehler in Ihren Berechtigungen werden übersichtlich dargestellt und nach Risiken bewertet.

CARO-Automation©

Für Ihre Entlastung

Ihre Zugriffsrechte werden automatisch sauber gehalten. Sie sind befreit von stupiden Arbeiten und können einer erhöhten Sicherheit vertrauen.

CARO-Reporting©

Für Ihre Kontrolle

Nach jedem der durchgeführten Änderungsschritte protokolliert CARO revisionssicher alle Details für Sie.

CUSATUM

CUSATUM Service GmbH

Hauptsitz
Wiesenweg 16
16548 Glienicke / Nordbahn

E-Mail: info@cusatum.de
www.cusatum.de

SECURITY MADE IN GERMANY

CARO-Suite

3 Module für Ihre IT-Sicherheit

Mit der CARO-Suite können Sie Berechtigungsfehler und Risiken von Zugriffsrechten analysieren und automatisiert bereinigen. Sparen Sie Zeit und Geld durch saubere Berechtigungsstrukturen mit optimierten Zugriffsrechten.

Die CARO-SUITE bietet für Ihre IT-Sicherheit:

CARO-ANALYSIS©

- Risiko-Dashboard
- Berechtigungsanalyse

CARO-AUTOMATION©

- Risikobewertung von Experten
- Handlungsempfehlungen
- Automatisiertes Bereinigen

CARO-REPORTING©

- Revisionssichere Reporte
- Compliance-konform

SECURITY MADE IN GERMANY

CARO-Suite

Risikobewertung von Experten

Mit dem neuen Risiko-Dashboard erkennen Sie auf einen Blick, wo genau bei Ihnen die größten Risiken zu finden sind und wie Sie diese mit wenigen Klicks automatisiert bereinigen.

Risiko-bewertung	Bereinigungsbausteine	Erklärung	Analysen
kritisch	VASS, ARCA, RAPA, DUKE, DARS, BAKS	Diese Analysen finden Berechtigungsfehler, die von unseren Experten als kritisch eingestuft werden. Kritische Fehler entstehen durch unzulässige Zugriffsrechte und sollten vorrangig bereinigt werden.	✓ Erlaubte Besitzer-Analyse ✓ Direkte Benutzerberechtigungen ✓ Redundante Zugriffsrechte ✓ Unterbrochene Vererbung ✓ Inaktive Computer ✓ Kennwort läuft nie ab
Wichtig	ERBE, MARS, VASS, ARCA, LARS	Diese Analysen finden weitere als wichtig eingestuften Probleme in Ihrem System. Solche relevanten Probleme sollten zeitnah behoben werden.	✓ Ersteller-Besitzer ✓ Mindest-Berechtigungen ✓ Verschobene Verzeichnisse ✓ Ungewollte Konten ✓ Inaktive Benutzer ✓ Listgruppenanalyse
auffällig	TEUS, ARCA	Es werden Sicherheits-auffälligkeiten in den Zugriffsrechten gefunden. Diese Auffälligkeiten sollten nach unserer Erfahrung durch Ihre Administratoren überprüft werden.	✓ Verwaiste Kontoreferenzen ✓ Veraltetes Kennwort ✓ Deaktivierter Benutzer ✓ Leere Gruppen ✓ Gruppen ohne Beschreibung

Analyse- und Bereinigungsbausteine

Standardmäßig werden 11 Bereinigungs- und Analysebausteine mit der CARO-Suite ausgeliefert.

BAKS

Besitzer-**A**nalyse- und **K**orrektur-**S**oftware

Besitzer korrigieren

- Stellt zulässige Besitzer sicher, damit administrative Konten Ihre Berechtigung behalten, z.B. damit Backup-Tools funktionieren
- Analysiert Sicherheitsrisiken durch das Entfernen von unerlaubten und unkontrollierbaren Zugriffs-Berechtigungen

LARS

Listgruppen **A**nalyse- und **R**estrukturierungs-**S**oftware

Fehler in Listgruppen analysieren

- Analyse der Berechtigungen in Ordner-Hierarchien
- Verwalten von List-Berechtigungen in übergeordneten Ordnern

TEUS

Tool zur **E**ntfernung **u**nbekannter **S**IDs

Verwaiste SIDs entfernen

- Entfernt tote SIDs und macht die Dokumentation Ihrer Berechtigungen wieder leichter lesbar und verständlich
- Reduziert die Nachfragen Ihrer Revision und dokumentiert, dass Sie die volle Kontrolle haben
- Bietet mehr Sicherheit, da weniger Angriffsfläche für SID History Injection

DARS

Direktzugriff **A**nalyse- und **R**estrukturierungs-**S**oftware

Direkte Berechtigungen prüfen

- Identifiziert Direktberechtigungen von Usern
- Korrigiert effizient diese Einträge

RAPA

Redundant **A**ccount **P**ermission **A**nalysis

Redundante Berechtigungen beseitigen

- Identifiziert redundante Berechtigungen
- Überprüfen von Gruppenmitgliedschaften mit gleichzeitiger Direktberechtigung

CARO-Suite

Analyse- und Bereinigungsbausteine

Standardmäßig werden 11 Bereinigungs- und Analysebausteine mit der CARO-Suite ausgeliefert.

DUKE

Direktzugriffsrechte **U**ngewollter **K**onten **E**ntfernen

- Identifiziert alle Zugriffsrechte der konfigurierten ungewollten Konten und entfernt diese
- Reduziert Sicherheitsrisiken durch das Entfernen von unbekannten und unkontrollierbaren Zugriffsberechtigungen

Direkte ungewollte Berechtigungen entfernen

VASS

Vererbung-**A**nalyse- und **S**anierungs-**S**oftware

- Identifiziert veränderte Berechtigungen in Ordner-Hierarchien
- Angleichung der Berechtigungen durch Vererbung oder andere systemspezifische Werkzeuge

Aufgebrochene Vererbungen wiederherstellen, Verschobene Verzeichnisse finden

ARCA

Account **R**isk- und **C**ompliance-**A**ssessment

- Analysiert Konto-basierend auf Best Practice-Kriterien
- Inaktive Benutzer- oder Computerkonten
- Deaktivierte Benutzerkonten
- Konten mit nie ablaufenden Kennwörtern oder zeitlich lange nicht geänderten Kennwörtern
- Leere Gruppen und Gruppen ohne Beschreibung

Risk- und Compliance Dashboard

ERBE

ERsteller-**B**esitzer auf Dateisystemen **E**ntfernen

- Entfernt den Ersteller-Besitzer und verhindert das Entstehen von neuen toten SIDs
- Erlaubt damit eine saubere Migration, z.B. in die Cloud

Ersteller-Besitzer entfernen

MARS

Mindestberechtigungen **A**nalyse und **R**estrukturierungs-**S**oftware

- Prüft alle Dokumente und Ordner auf erforderliche Zugriffsrechte für Konten und berücksichtigt dabei sowohl direkte als auch indirekte Zugriffsrechte
- Setzt fehlende Berechtigungen

Mindest-Berechtigungen überprüfen

Berechtigungen anzeigen und dokumentieren

Mit dem Module EBIS zeigt CARO eine globalen Ressourcenansicht mit der IST-Berechtigungssituation an. Sie können Berechtigungs- und Use-Case-Reporte erstellen, einfach an Ihre Corporate Identity anpassbar durch Microsoft-Word-Office-Vorlagen.

EBIS

Erfassung der **B**erechtigungs-**I**st-**S**ituation

- Zeichnet die Berechtigungslage auf Fileservern auf
- Analysiert u.a. auf unterbrochenen Vererbungshierarchien, verschobene Verzeichnisse oder Null-DACL in den ACEs
- Anzeige von fehlenden Besitzereinträgen
- Zeigt im Detail geänderte Berechtigungen unterhalb an, wie hinzugekommene oder entfernte Zugriffsrechte
- Zeigt Gruppenmitgliedschaften mit direkten und indirekten Mitgliedschaftsbeziehungen
- Reporte für die IST-Berechtigungssituation „Wer hat wo Zugriff?"
- Reporte über geänderte Berechtigungen unterhalb
- Differenz-Reporte für eine Verzeichnisstruktur
- Report „Wo hat ein Benutzer Zugriff?"

IST-Situation erfassen und Berechtigungen reporten

Best Practices

Für das Bereinigen ist es sinnvoll, bestimmte Analysen gemeinsam zu nutzen. In unserem Flyer *Best Practices und Anwendungsfälle zum Bereinigen* erfahren Sie mehr über eine empfohlene Reihenfolge und sinnvolle Kombinationen von CARO-Analysen für ein effizientes Bereinigen.

Ebenfalls werden zu jedem Bereinigungsbaustein Anwendungsfälle beschrieben.

Herr L., System-Administrator*
„Ich will gar nicht so euphorisch sein, dass wir so viele Fehler gefunden haben. Aber nun bin ich wirklich froh, dass hier die CARO-Suite so schnell aufgeräumt hat!

**Namen und Firmeninformation sind aus Datenschutzgründen gekürzt. Gerne geben wir Ihnen in einem persönlichen Gespräch diese Referenzen weiter.*

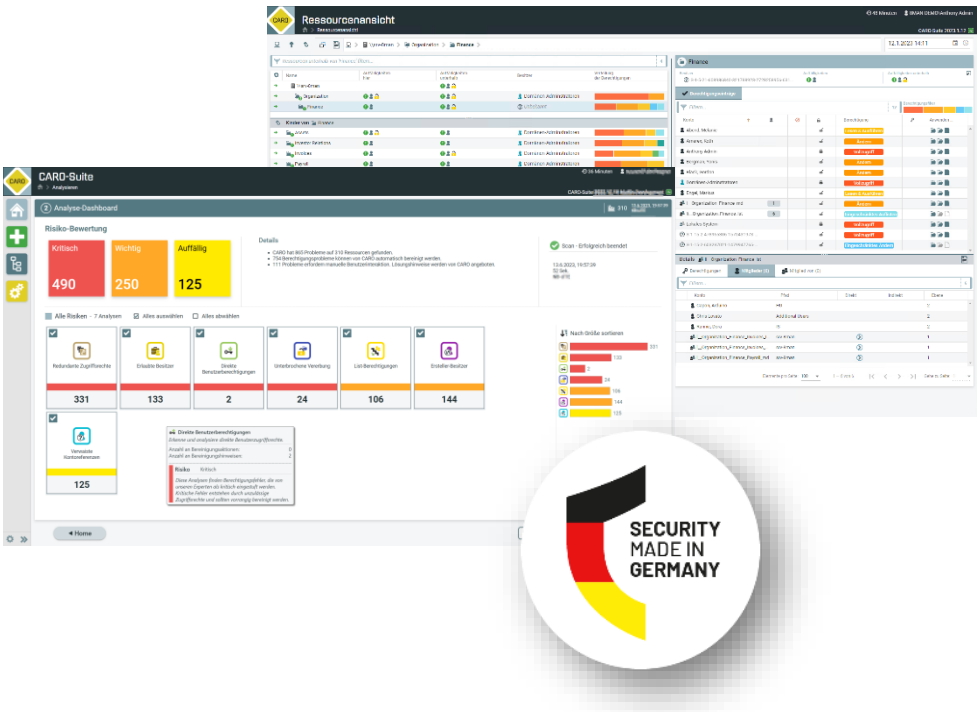
CARO-Suite

CARO-Suite - Zugriffsrechte sicher im Griff!

Historisch gewachsene Berechtigungsstrukturen gehören mit CARO der Vergangenheit an. Sicherheitslücken werden beseitigt und automatisch reduziert. CARO sorgt in Ihren IT-Strukturen für Ordnung!

DIE CARO-SUITE IM DETAIL

- Risikobewertung im Analyse-Dashboard mit Expertenwissen
- Detaillierte Analysen für Berechtigungsfehler enthalten
- Umfangreiche Handlungsempfehlungen zum Bereinigen
- Globale Ressourcen-Ansicht der Zugriffsrechte mit Gruppenmitgliedschaften
- Hoch performante Scans und umfangreiche Analysen zur Änderung Ihrer problematischen Zugriffsrechte
- Planbarkeit von Scans und Änderungen für einen beliebigen Zeitpunkt
- Für Filesystem und Active Directory
- Integration in andere Systeme über Rest-API
- Automatisierung von Mitarbeiterprozessen mit dem Zusatzmodul C-MAN
- Basis-Reporte im PDF-Format, durch Word-Office-Report-Vorlagen einfach an eigene Corporate-Identity anpassbar
- Revisionssichere Protokollierung aller durchgeführten Änderungen
- Mehrsprachiger WebClient mit Multi-User-Support
- Datenspeicherung in MS-SQL-Datenbank
- Einfaches Lizenzmodell



CARO-Suite

CUSATUM – Gemeinsam für mehr Sicherheit!

Die CUSATUM Service GmbH am Standort Berlin/Brandenburg ist ein Software- und Beratungsunternehmen mit dem Fokus auf Berechtigungsmanagement und Automatisierung von Mitarbeiterprozessen.
Als „Macher der ersten Stunde" haben wir den 8MAN von Protected Networks entwickelt. Dieser heißt jetzt SolarWinds-ARM und ist bis heute ein großer Erfolg im deutschsprachigen Raum.

Unsere Erfahrungen aus eineinhalb Jahrzehnten im Berechtigungsmanagement haben wir heute in unserer CARO-Suite vereinigt. Sie ist die notwendige Ergänzung zum ARM, die bisher gefehlt hat! Die CARO-Suite unterstützt Unternehmen im Berechtigungsmanagement zur Erfüllung gängiger Sicherheits- und Compliance-Richtlinien.

Mike Wiedemann, CEO
Seine Leidenschaft ist Kundenzufriedenheit. Für zufriedene Kunden geht er auch die „extra Meile"!

Ute Wagner, CDO
Ein User Interface muss nicht nur einfach zu bedienen sein, es muss auch Freude machen, es zu nutzen!

Christian Schönfeld, CEO
Meine Erfahrungen direkt umwandeln in CARO - das ist mein Anspruch! Für alles gibt es eine Lösung. Packen wir es an!

CUSATUM

Herausgeber

CUSATUM Service GmbH

Hauptsitz
Wiesenweg 16
16548 Glienicke / Nordbahn

E-Mail: info@cusatum.de
www.cusatum.de

Support

Telefon: +49 30 94 86 3401
Mobile: +49 175 221 11 04

E-Mail: support@cusatum.de

Stand: September 2023

SECURITY MADE IN GERMANY