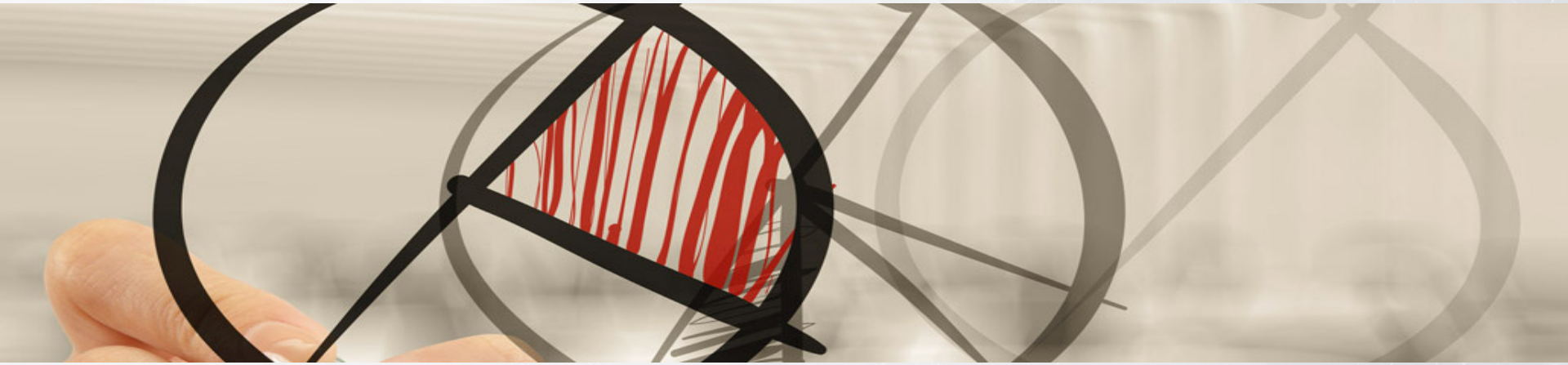
KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.



Teilautomatisierte Risikoanalyse nach ISO 27005 durch Integration mit securiCAD

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.

UNTERNEHMENSRESILIENZ. INFORMATIONSSICHERHEIT. MEHR.

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.

Unternehmensresilienz:
Ihr starkes „Immunsystem“

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.

Wir bieten Ihnen:

- **Optimierung der Widerstandskraft** der Organisation
  - Stärkung der Belastbarkeit durch die Fähigkeit einer schnellen und zielgerichteten Ausrichtung an prognostizierte externe und interne Veränderungen

- **Integrative Betrachtung** der Teildsziplinen

Immunsystem stärken

„Grippeimpfung“ auf den Bedarf abstimmen

Steigerung der Effizienz

durch Integration von Management-systemen

Schaffung neuer Prognose-fähigkeiten

- **Framework CHARISMA** als Kern

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.

Beratungs- und Lösungsanbieter

- Etablierter Anbieter von **Beratung, Lösungen und Wissenstransfer**
- Lösungen für **anspruchsvolle Anforderungen**
- **Spezialistenpool** qualifizierter und kompetenter Berater
- Umfangreiches **Kompetenznetzwerk**

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.

Grundlagen der ISO 27005

Kurzeinführung in die ISO 27000-Reihe

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO INTELLIGENT. EINFACH. PREMIUM.

Begriffe und Grundlagen

- ISO/IEC 27000
  Überblick und Vokabular

Normativ

Anforderungen

- ISO/IEC 27001
  ISMS
- ISO/IEC 27006
  Anforderung an Zertifizierer

Normativ

Empfehlungen

- ISO/IEC 27002
  Anwendung der Controls
- ISO/IEC 27007
  Leitfaden zur Durchführung von ISMS Audits
- ISO/IEC 27003
  Leitfaden zur Implementierung eines ISMS
- ISO/IEC 27005
  Risikomanagement
- ISO/IEC 27004
  Messungen

Informativ

Branchenspezifisch

- ISO/IEC 27011
  Richtlinien für Informationssicherheit der Telekommunikation
- ISO/IEC 27799
  Gesundheitswesen
- ISO/IEC 27019
  Energieversorger

Informativ

Grundlagen

- ISO 27005 stellt genaue Anleitung zur IT Risikoanalyse und zum Risikomanagement im IT Bereich dar
- Beinhaltet Beschreibung des kompletten Risikomanagement-Prozesses + genaue Beschreibung der einzelnen Schritte des Risikomanagement und der Risikoanalyse
- Anhänge liefern Informationen zur Etablierung eines Risikomanagement im Bereich Informationssicherheit
- Erfüllung von Forderungen der ISMS Norm ISO 27001

Risikomanagement Bedeutung

- Erreichen eines **angemessenen Risikoniveaus** (Einbeziehung u.a. von Art der Daten und Assets, Branche, Größe der Organisation) durch eine **systematische, geplante** und **organisierte** Vorgehensweise

- **Planungs-, Kontroll- und Lenkungsaufgabe**

- Notwendige Einbettung in die **Managementstruktur**

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.

Zweck und Nutzen

- Systematischer, unternehmensweiter Prozess zur **Früherkennung**, **Vermeidung** und **Bewältigung** von Gefahren
- Erreichung einer größeren Planungssicherheit zur wahrscheinlicheren **Erreichung der Unternehmensziele**
- Optimierung des unternehmerischen **Risikoprofils**
- Verbesserung des **Unternehmenserfolgs**
- Sicherung von **Wettbewerbsvorteilen**

Schrittfolge für Risikoanalyse

- Schritt 1: Definition
  - systematischen Ansatz für den Umgang mit Risiken definieren
- Schritt 2: Beschreibung
  - geeignete Methode zur Analyse, Bewertung und Behandlung von Risiken (Risikomanagementhandbuch) beschreiben:
    - Festlegung der Schutzklassen und Kriterien (Schadenshöhe, Eintrittswahrscheinlichkeit, Risikoakzeptanz)
    - Festlegen der Verantwortlichkeiten
    - Festlegen der Review-Zyklen
- Schritt 3: Verfahrensanweisung
  - Für IT-Risikomanagement

Schrittfolge für Risikoanalyse

- Schritt 4: Erfassen
  - Alle bedrohten Objekte und deren Wert erfassen
- Schritt 5: Erfassen der Daten und Informationen
  - Daten und Informationen durch IT-Risikoanalyse erfassen
- Schritt 6: Erfassen der Bedrohungen und Schwachstellen
  - Systematische Erfassung + Bewertung der Bedrohungen + Schäden im Zuge der IT-Risikoanalyse + Bewerten von möglichen Schäden durch Verlust, Veränderung oder Ausfall

Schrittfolge für Risikoanalyse

- Schritt 7: Bewertung
  - Eintrittswahrscheinlichkeit bewerten
- Schritt 8: Erstellung einer Risikomatrix
  - Risikomatrix bestehend aus Eintrittswahrscheinlichkeit pro Schaden + zu erwartende Schadenshöhe

Risikomatrix

		Schadensausmaß		
		Gering	Mittel	Hoch
Eintrittswahrscheinlichkeit	Häufig	Mittleres Risiko	Hohes Risiko	Hohes Risiko
	Gelegentlich	Geringes Risiko	Mittleres Risiko	Hohes Risiko
	Selten	Geringes Risiko	Geringes Risiko	Mittleres Risiko

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO INTELLIGENT. EINFACH. PREMIUM.

Herausforderungen

- Regelmäßige / stetige Änderungen (regelmäßige Prüfungen und Neubewertungen)
- Unzureichendes Wissen, unzureichende Qualifizierung, fehlende Erfahrung (permanente Weiterbildung)
- Was nicht bekannt ist, kann nicht identifiziert, analysiert und/oder bewertet werden
- Identifizierung der Prozesse mit höchster Wertschöpfung (Geschäfts-/ Produktionsprozessdefinition)
- Besondere Sorgfalt bei der Schutzbedarfsfeststellung (nicht nur drei Abstufungen, Evaluierung regelmäßiger Ergebnisse)

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.

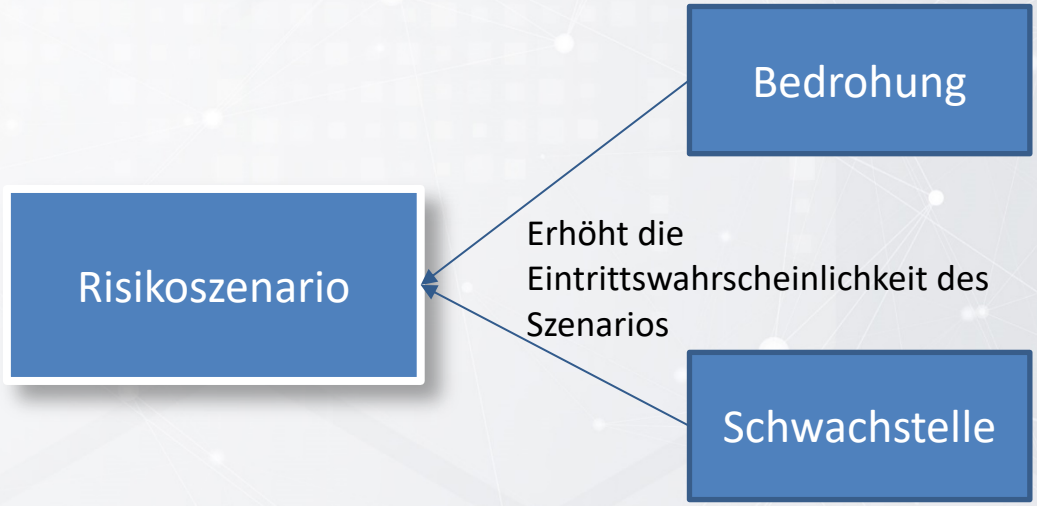
ISO 27005 Risikoanalyse in verinice

Risikoanalyse in ISM-Perspektive

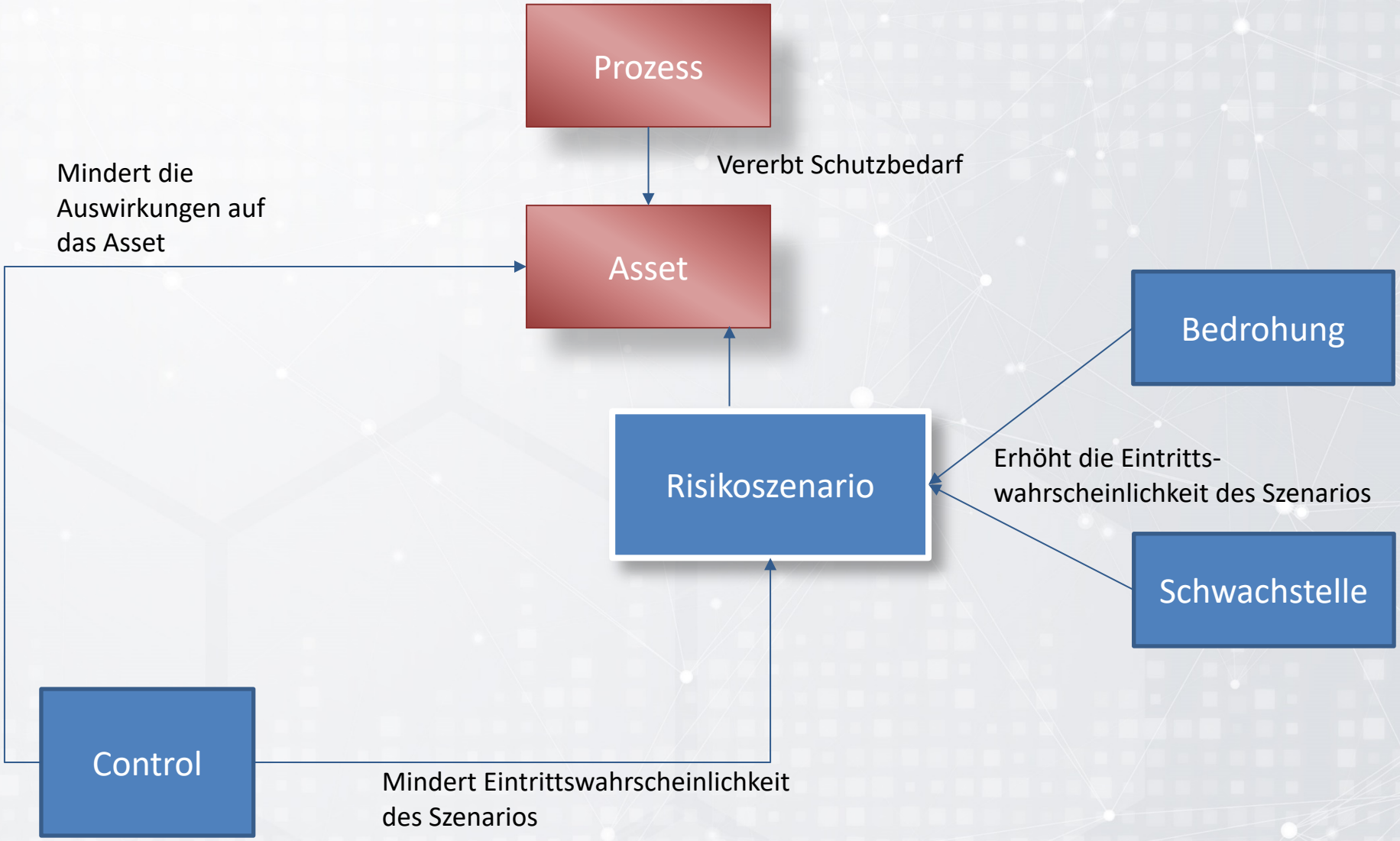
- Risiken werden als Risikoszenario beschrieben
  - Kombinierte Wirkung aus Bedrohung und Schwachstelle

- Beteiligte Objekttypen
  - Prozesse
  - Assets
  - Controls
  - Bedrohungen
  - Schwachstellen

Risikoszenario



- Eintrittswahrscheinlichkeit des Szenarios ergibt sich aus
  - Bedrohungshäufigkeit und
  - Ausnutzbarkeit der Schwachstelle.


Prozess
Vererbt Schutzbedarf
Mindert die Auswirkungen auf das Asset
Asset
Bedrohung
Risikoszenario
Erhöht die Eintritts-wahrscheinlichkeit des Szenarios
Schwachstelle
Control
Mindert Eintrittswahrscheinlichkeit des Szenarios

KOOPERATIONS PARTNER TÜV HESSEN

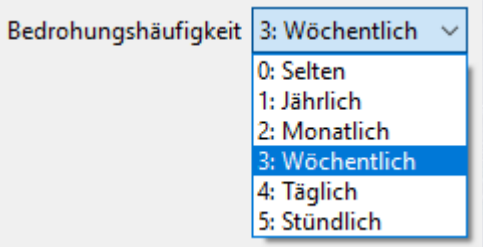
CARMAO
INTELLIGENT. EINFACH. PREMIUM.

Voraussetzungen der Risikoanalyse

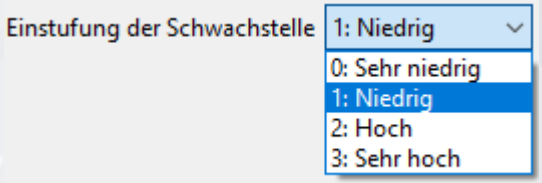
- Bestimmung und Bewertung der Assets (Informationswerte)
  - Eigentümer und Zugehörigkeit zu Geschäftsprozess
  - Business Impact (Schutzbedarf) vollständig erfasst
- Bestimmung und Bewertung der Bedrohungen
  - Qualifizierte Beschreibung
  - Bedrohungshäufigkeit
- Bestimmung und Bewertung von Schwachstellen
  - Qualifizierte Beschreibung
  - Einstufung der Schwachstelle

Risikoberechnung

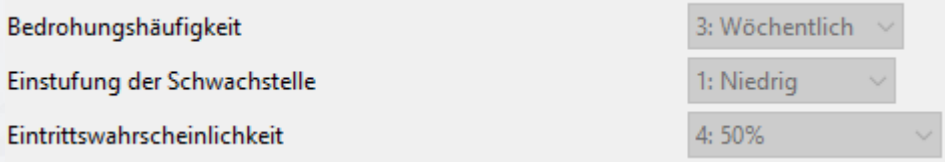
- **Problem:** Einschätzung der Eintrittswahrscheinlichkeit subjektiv
  - Bedrohungshäufigkeit:



  - Einstufung der Schwachstelle:



  - Eintrittswahrscheinlichkeit: Bedrohungshäufigkeit + Schwachstelle

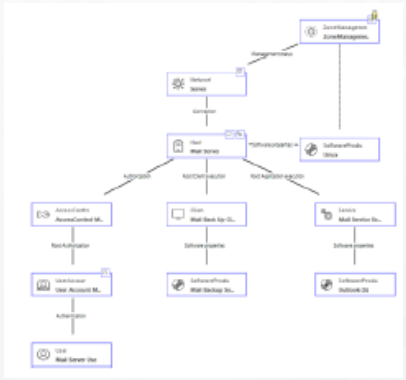


KOOPERATIONS PARTNER TÜV HESSEN

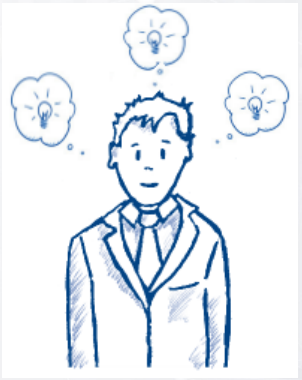
CARMAO
INTELLIGENT. EINFACH. PREMIUM.

Reproduzierbare, objektive Eintrittswahrscheinlichkeit mit **securiCAD**

securiCAD – Eine innovative Technologie



CAD-System für die Modellierung von IT-Architekturen



Hinterlegtes Wissen über Angriffsbäume und Wahr-scheinlichkeitsnetze

Intelligente Analysen zur Weiter-entwicklung der IT-Infrastruktur

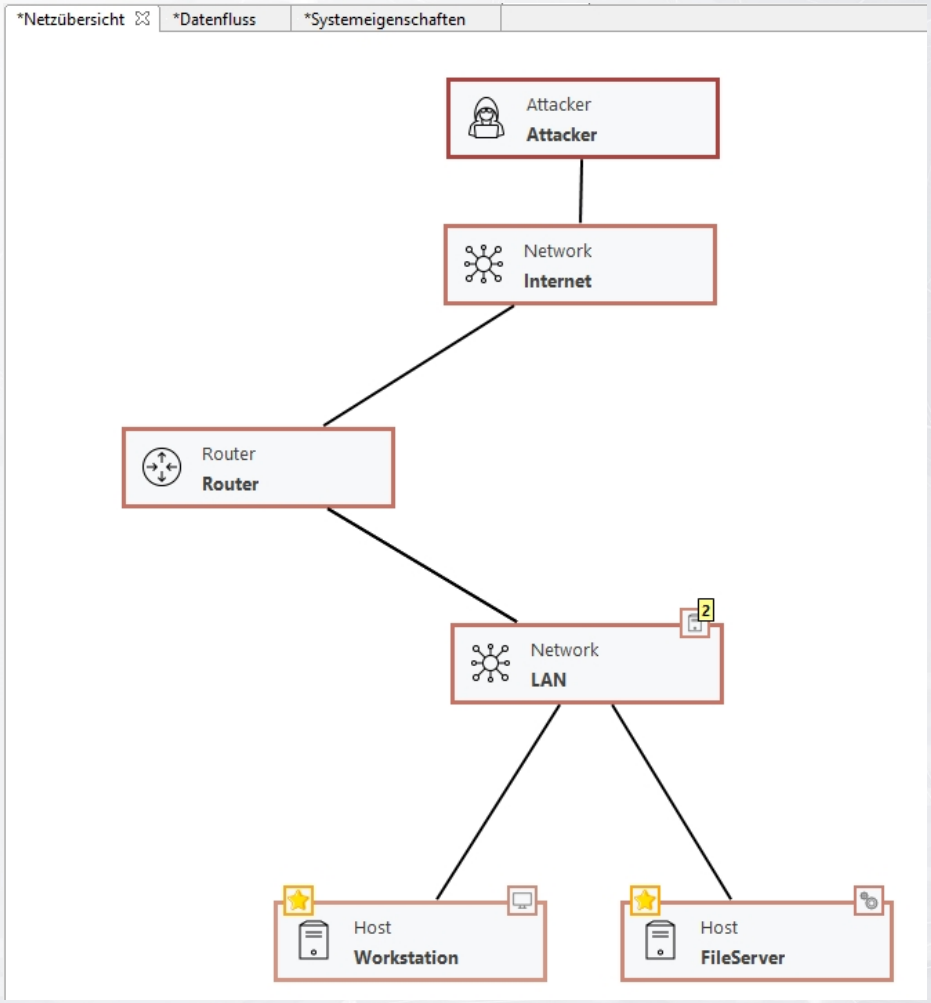
KOOPERATIONS PARTNER TÜV HESSEN

CARMAO INTELLIGENT. EINFACH. PREMIUM.

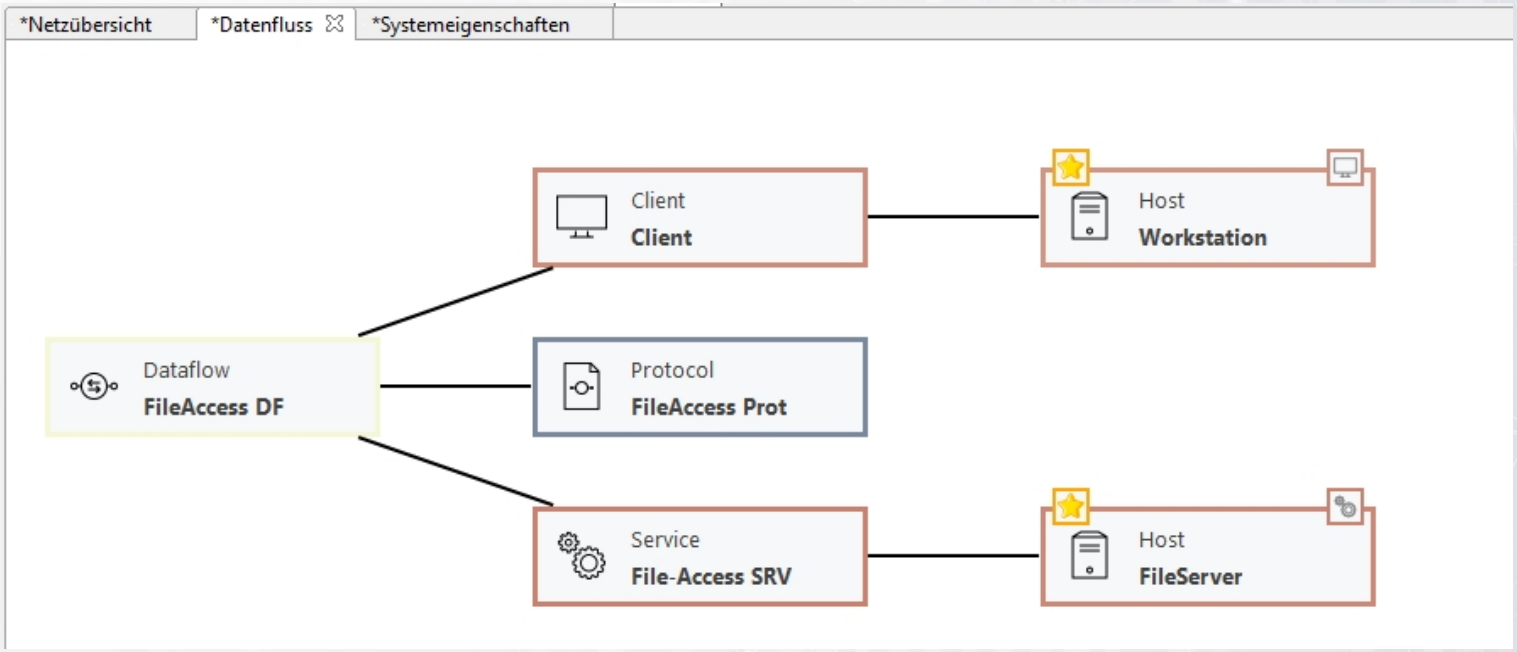
securiCAD im Überblick

- modelliert und visualisiert Netzwerke
- simuliert Cyber-Angriffe und deren Auswirkung auf das gesamte Netzwerk
- prognostiziert die Zeit TTC (time to compromise), wie lange ein Netzwerk Angriffen standhält
- kann Auswirkungen von Veränderungen vorhersagen, bevor diese tatsächlich umgesetzt werden
- liefert eine „ Heat map “ über Schwachstellen

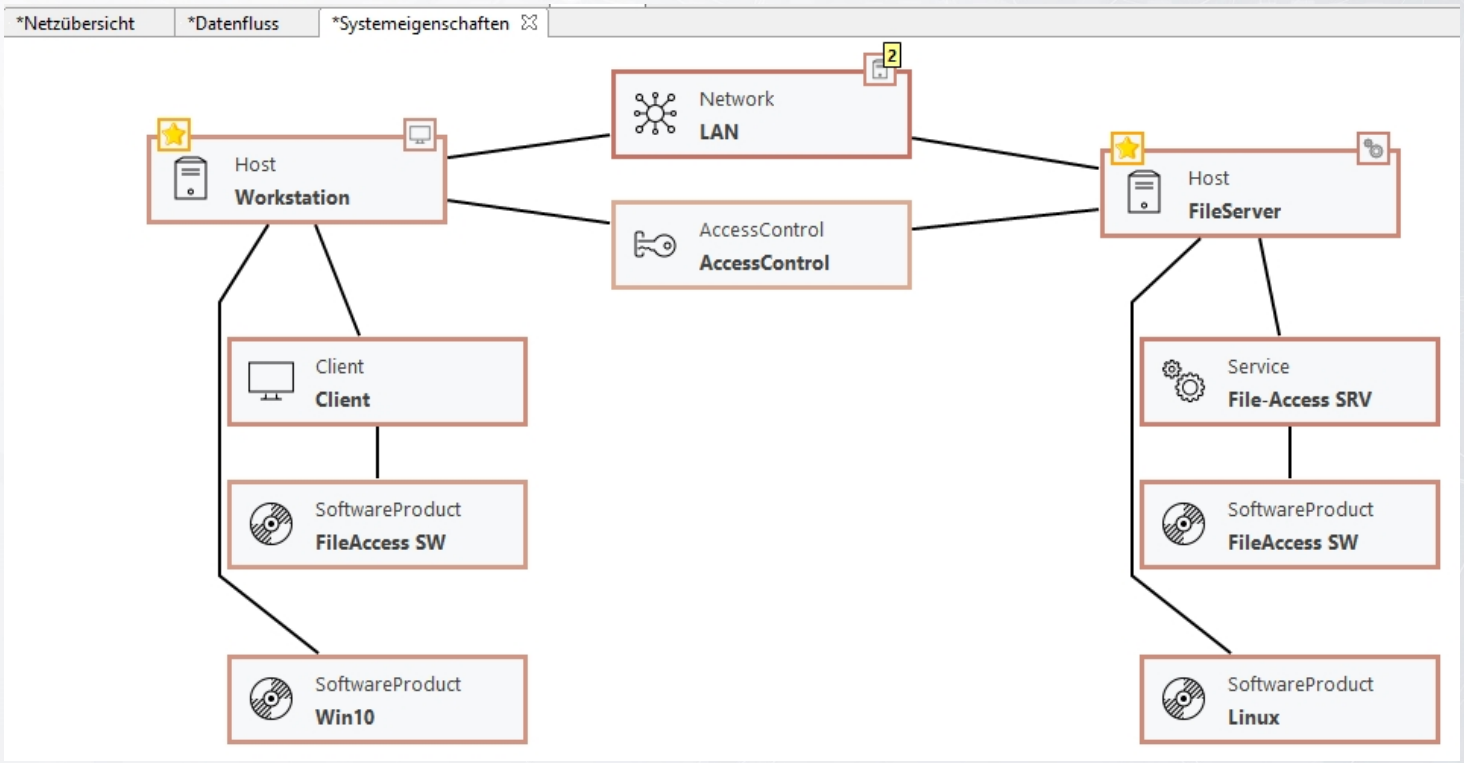
Netzübersicht



Datenfluss


*Netzübersicht
*Datenfluss
*Systemeigenschaften
Client
Client
Host
Workstation
Dataflow
FileAccess DF
Protocol
FileAccess Prot
Service
File-Access SRV
Host
FileServer

Systemeigenschaften



KOOPERATIONS PARTNER TÜV HESSEN

CARMAO
INTELLIGENT. EINFACH. PREMIUM.

Schnittstelle zwischen **verinice** und **securiCAD**

Schnittstelle

- Notwendige Vorbereitungen
  - Hinzufügen von Tags zu den Assets
  - Präfix „SC-“ + spezifischer Asset-Typ aus securiCAD
  - z.B. „SC-Host“

- Export der Organisation aus verinice als VNA-Datei

KOOPERATIONS PARTNER TÜV HESSEN

CARMAO INTELLIGENT. EINFACH. PREMIUM.

Schnittstelle

- Import in securiCAD
  - Unterscheidung der verschiedenen Asset-Typen durch vorher gesetzte Tags
- Berechnung der Eintrittswahrscheinlichkeiten durch securiCAD
  - quantitativ stochastischer Ansatz mit dem Ziel der Reproduzierbarkeit und Vergleichbarkeit

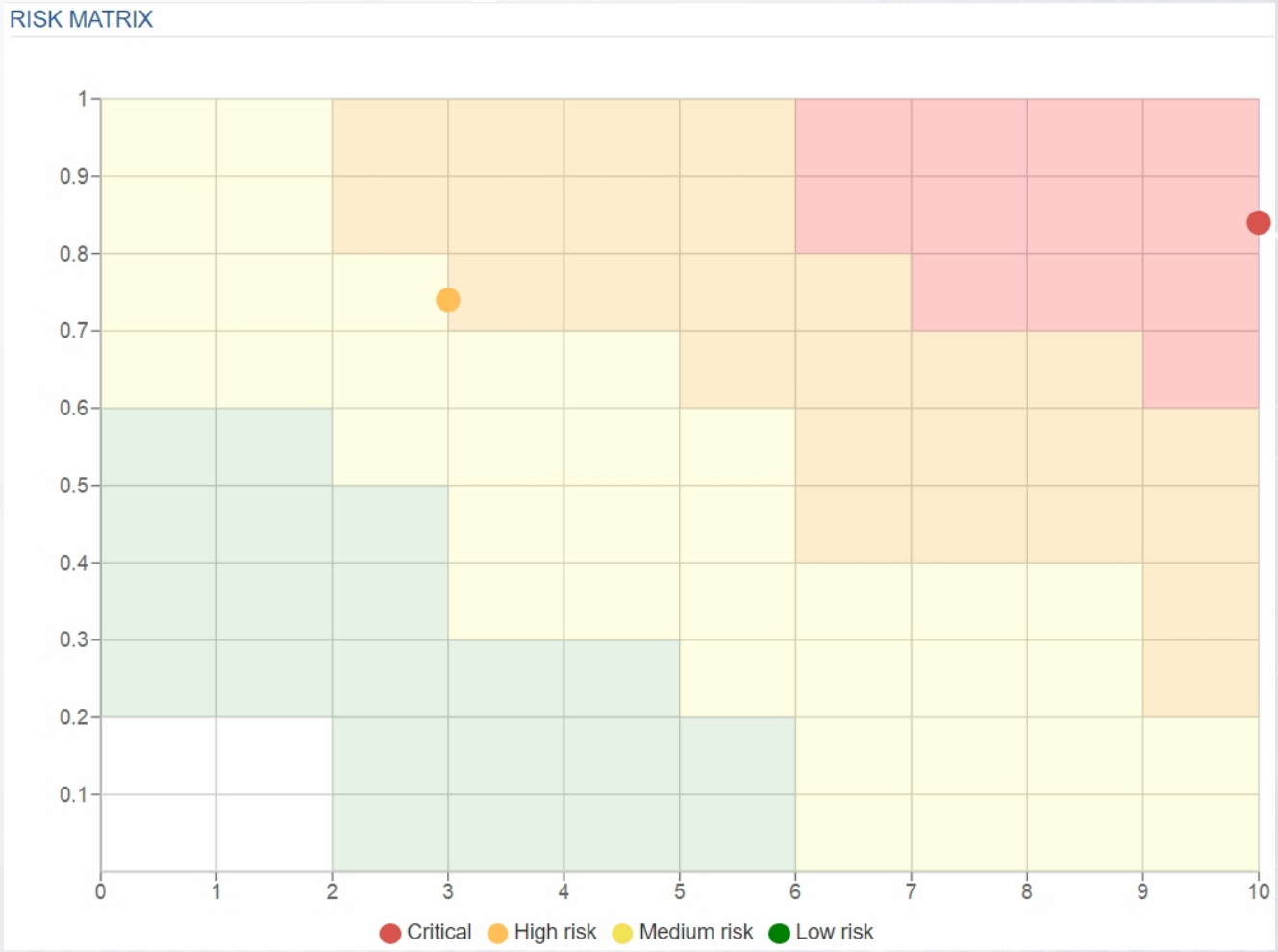
Ergebnisse in securiCAD

Risks

Each column contains a summary for all high value assets of a selected simulation. The high value assets are grouped by object type. Click on the object types to see details for each object type

	Initial simulation Feb 11 2019, 12:46	**AV+PW-Policy** Feb 11 2019, 12:47	**Initial simulation** Feb 11 2019, 12:48
Host			
FileServer.Compromise			
Time to compromise	8 day(s)	23 day(s)	100 day(s)
Consequence	10	10	10
Probability	0.84	0.64	0.16
Risk	Critical	Critical	Medium
Workstation.Compromise			
Time to compromise	12 day(s)	50 day(s)	100 day(s)
Consequence	3	3	3
Probability	0.74	0.47	0.14
Risk	High	Medium	Low

Ergebnisse in securiCAD



Vielen Dank für Ihre Aufmerksamkeit

Sie haben noch Fragen?

Ich stehe Ihnen gerne zur Verfügung.

Ulrich HEUN

Geschäftsführender Gesellschafter

Telefon: +49 6431 2196-0

E-Mail: ulrich.heun@carmao.de

CARMAO GmbH | Walderdorffer Hof | Fahrgasse 5 | 65549 Limburg