Automatisiertes Security Risikomanagement mit SECIRA©

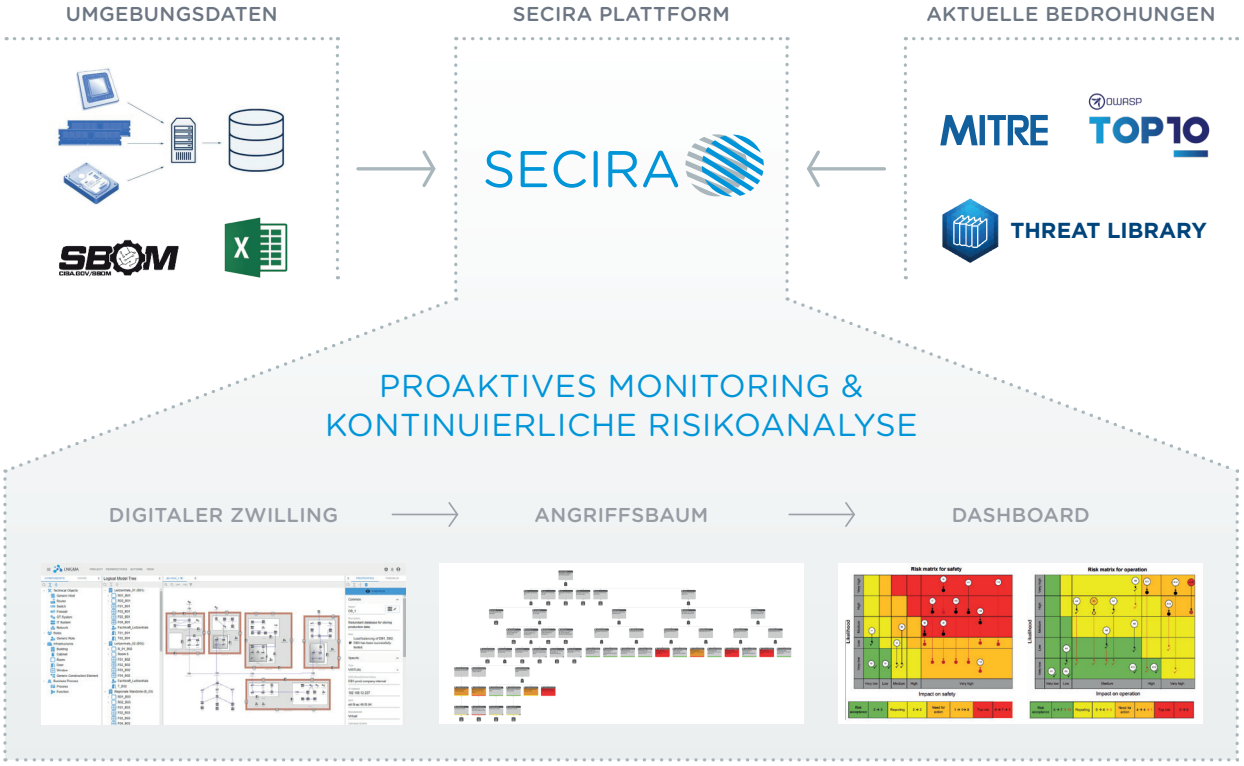
Kontinuierliche, ganzheitliche Analysen für Technik, Infrastruktur & Rollen

DIE AKTUELLE LAGE:

Die Häufigkeit und die Komplexität von Angriffen steigt, Infrastrukturen werden immer vernetzter und abhängig von Interoperabilität. Die Herausforderungen an CISO und andere Sicherheitsverantwortliche steigen kontinuierlich.

DIE LÖSUNG:

Um die Situation beherrschbar zu machen, braucht es ein ganzheitliches Security Risikomanagement, das räumliche Infrastruktur, technische Systeme (IT, OT, Cloud) sowie Rollen und Prozesse gleichermaßen berücksichtigt. Ein dauerhaft etabliertes Risikomanagement zeigt blinde Flecken auf, unterstützt im Tagesgeschäft und in der Security-Strategie.



Mit SECIRA© schaffen wir ganzheitliches Risikomanagement auf allen Ebenen, in einer dauerhaften, automatisierten Form. Der Digitale Zwilling bildet die aktuelle Situation ab. Der Angriffsbaum zeigt uns tagesaktuell, wo Risiken bestehen und wie sich diese auf Geschäftsprozesse auswirken.

RISIKOMANAGEMENT LEBENSZYKLUS

SECIRA© ist die einzige Web-Plattform auf dem Markt, die in der Lage ist, ein ganzheitliches Risikomanagement als Service durchzuführen.

Spezialisten der ICS GmbH etablieren den Lebenszyklus gemeinsam mit den Verantwortlichen beim Kunden und sorgen damit für eine qualitativ hochwertige, dauerhafte und allumfassende Risikoanalyse mit dem Ziel, diese automatisch zu aktualisieren.

Das Risikomanagement wird auf Basis eines Digitalen Zwillings aufgebaut, in dem alle für die Security relevanten Informationen über alle OSI-Layer hinweg beschrieben werden. Der Lebenszyklus über die Phasen „Sammeln“, „Modellieren“, „Überwachen“ und „Risikomanagement“ legt den Grundstein für eine defense-in-depth Security Architektur. Dabei werden alle notwendigen Daten möglichst automatisiert durch Importe und bidirektionale Schnittstellen zusammengetragen und im Digitalen Zwilling visualisiert.

Das so entstandene Logikmodell wird kontinuierlich auf Sicherheitslücken, Schwachstellen und strukturelle Schwächen hin überwacht. Die Bewertung der Sicherheitslücken im Kontext gibt Aufschluss über die Bedrohungslandschaft und zeigt Auswirkungen neu aufgekommener Exploits. Die Risikoanalyse findet entweder zyklisch oder bei Bedarf statt und gibt 24/7 Auskunft über den aktuellen Risikostatus des reellen Kundensystems.

THINK SAFE. THINK ICS

Informatik Consulting Systems GmbH
Sonnenbergstr. 13 · 70184 Stuttgart, Deutschland · Telefon +49 711 21037-00 · info@ics-gmbh.de
secira.eu · think-safe-think-ics.de