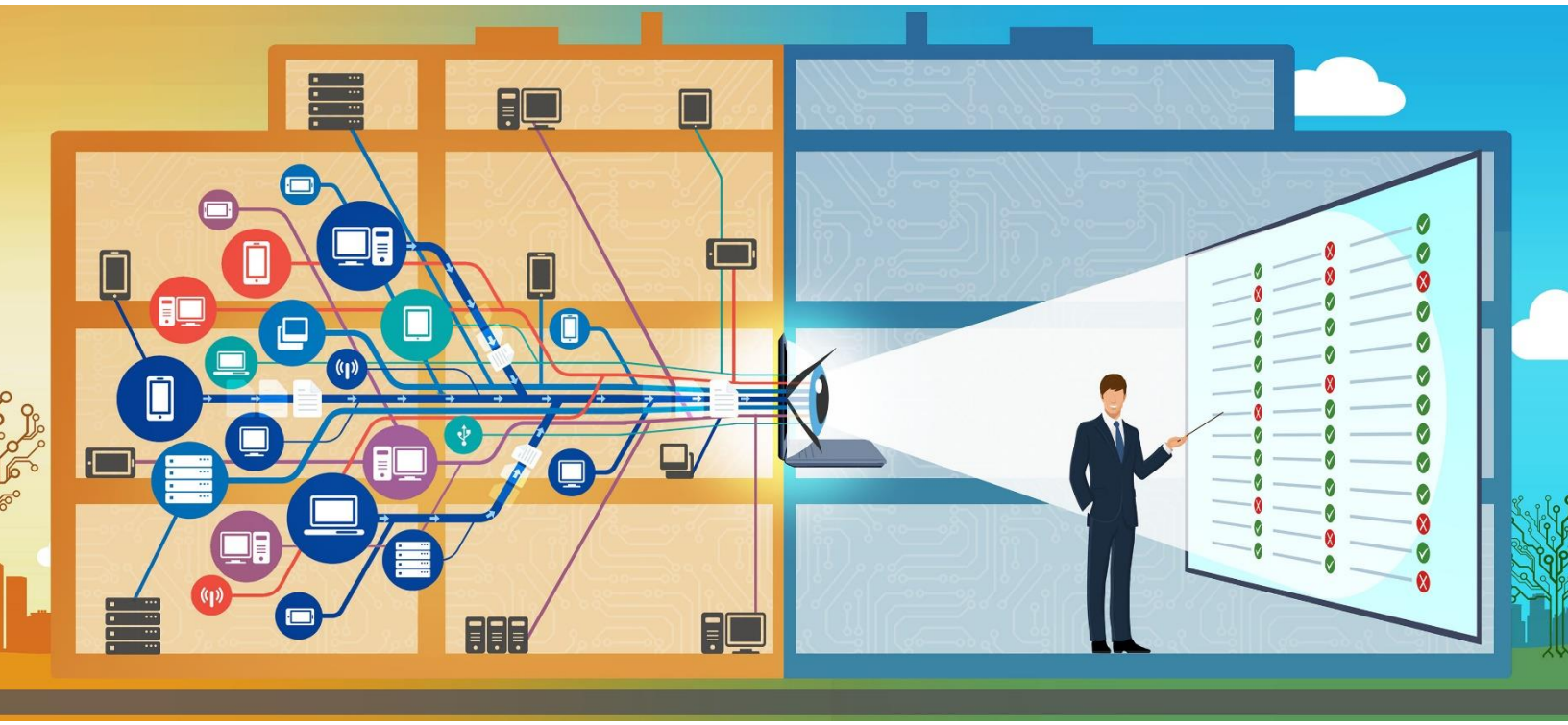
CSAT

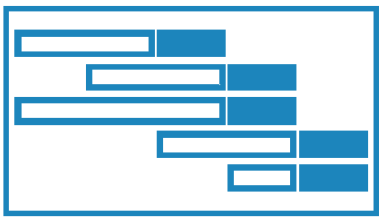
QS solutions



Faktencheck zur Optimierung Ihrer Sicherheit

In Zeiten dramatisch anwachsender Cyberkriminalität wollen Organisationen Ihren Sicherheitsstatus schnell und einfach überprüfen. Schwachstellen in der Inhouse-IT und in Cloud-Services wie Office365 müssen aufgedeckt und geschlossen werden. Das Cyber Security Assessment Tool (CSAT) von QS solutions gibt Ihnen ein vollständiges Bild Ihrer Situation durch automatische Scans und parallele Datenerhebungen per Interview. CSAT bewertet Ihren Sicherheitsstatus im Detail und liefert Ihnen Empfehlungen für einen konkreten Aktionsplan. Damit weist Ihnen CSAT den Weg zur Optimierung Ihrer Sicherheit, zur damit verbundenen Stärkung des Vertrauens Ihrer Geschäftspartner sowie zur Erfüllung der entsprechenden gesetzlichen Anforderungen der Datenschutzgrundverordnung (DSGVO).

Machen Sie Ihre IT sicher – worauf es ankommt



Definieren Sie Ihre Cyber Security Roadmap
Machen Sie Ihren Sicherheitsstatus transparent. CSAT liefert Ihnen alle notwendigen Informationen durch automatisierte Scans und Analysen. Diese Daten bilden die Grundlage für die Definition von Prioritäten und geben Ihnen die relevanten Informationen für eine Roadmap zur Verbesserung Ihrer Sicherheit.

Erkennen Sie Ihre "Technologielücken" Rechtliche Regelungen machen sowohl organisatorische Prozesse als auch ergänzende Technologien erforderlich. CSAT definiert, welche technischen Maßnahmen Sie ergreifen können, um die Anforderungen der DSGVO zu erfüllen. Sie können CSAT auch verwenden, um regelmäßig den Status zu überprüfen, um damit festzustellen, ob die ergriffenen Maßnahmen wirksam sind. (DSGVO Art. 32).

Empfehlungen
CSAT identifiziert die Bereiche, die Ihre Aufmerksamkeit erfordern, und empfiehlt konkrete Maßnahmen, die ergriffen werden sollten. Wenn CSAT z. B. herausfindet, dass vertrauliche Informationen mit Personen außerhalb Ihrer Organisation geteilt werden, sollten die Maßnahmen zur Dokumentensicherheit auf den Prüfstand kommen.

Wie arbeitet CSAT?

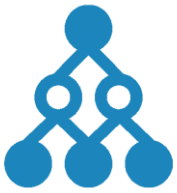
CSAT sammelt automatisiert sicherheitsrelevante Fakten durch

- Scannen aller Endpunkte und anderer Systeme im Netzwerk
- Durchsuchen von Active Directory und Azure Active Directory
- Scannen von Inhalten in Office 365, SharePoint und Fileshares.

Die Erfassung der relevanten Informationen erfolgt durch einen maschinellen Scan. Dabei kommen Agenten zum Einsatz, die sich nach dem Scan der Endpunkte selbst löschen. Dadurch wird der Aufwand für die interne IT-Abteilung auf ein Minimum reduziert

Endpunktscan

CSAT sammelt Informationen über Konten, Firewall-Regeln, installierte Anwendungen, Betriebssysteme mit Service Packs, über Fileshares und die Registry



Active Directory und Azure AD

CSAT erhebt Benutzer- und Gruppeninformationen, identifiziert externe Benutzer und (nicht verwendete) Konten (einschließlich Administratorenkonten) und kennzeichnet verdächtige Konten.

Office 365, SharePoint und Fileshares

CSAT durchsucht Inhalte von Office 365, SharePoint und Fileshares nach personenbezogenen Daten (PII). Der Zugriff auf SharePoint-Sites und Dokumente wird ebenfalls dokumentiert. Es erfolgt ein Abgleich mit den Konten des Active Directory zur Identifikation nicht autorisierter Zugriffe.

CSAT – in vier Schritten zum Erfolg

Vorbereitung & Installation (½ Tag)

- Prüfung der technischen Infrastruktur
- Prüfung von Endpunkten und Netzwerkzugriff
- Installation CSAT auf einem Windows- Server
- Konfiguration CSAT

Scannen (½ Tag)

- Scan der Endpunkte
- Scan von Active Directory und Azure AD
- Scan Office 365, SharePoint-Sites und Fileshares

Reporting und Empfehlungen (1½ Tage)

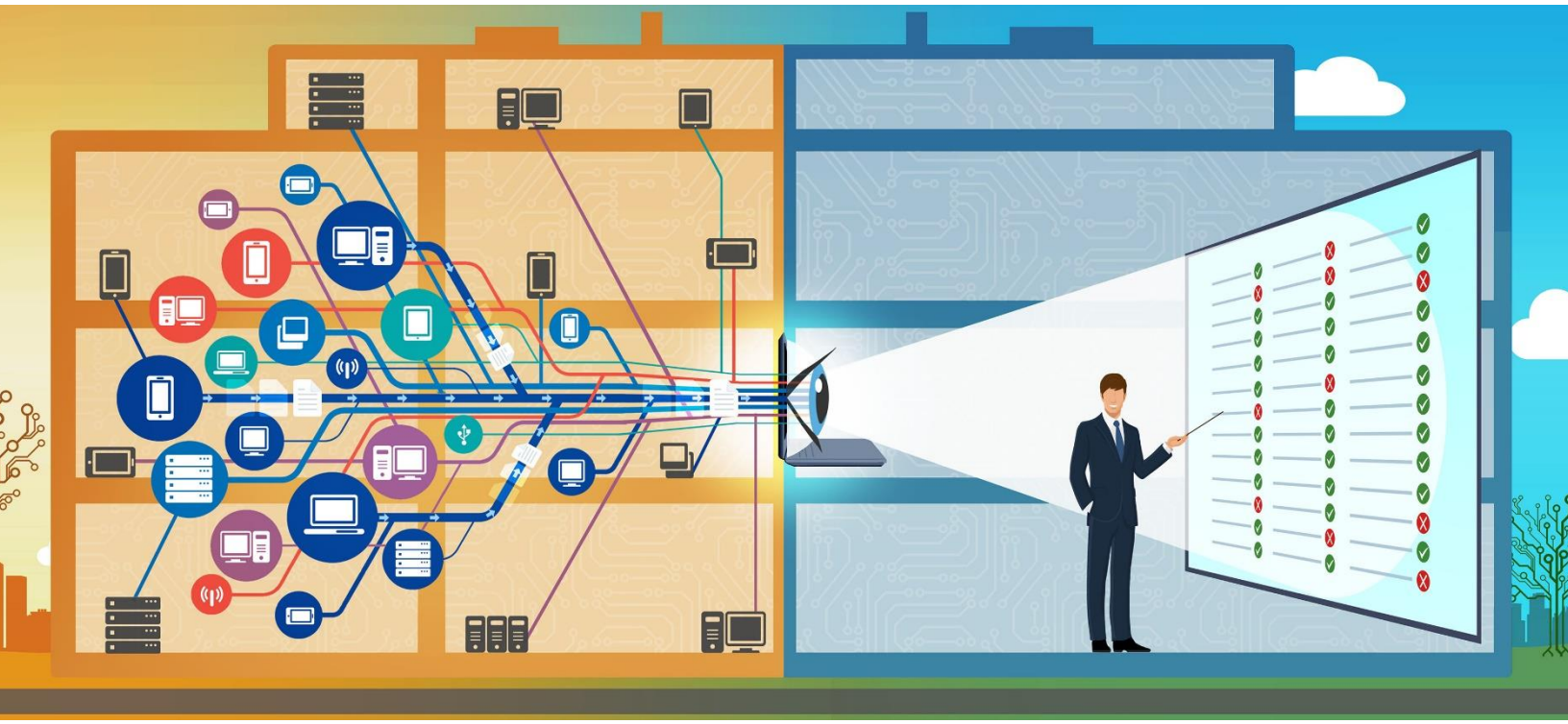
- Analyse der gewonnenen Daten durch QS
- Erstellung Ergebnisbericht

Präsentation der Ergebnisse (½ Tag)

- Präsentation und Diskussion von Ergebnissen, Schlussfolgerungen und Empfehlungen

Möchten Sie mehr über CSAT erfahren?

Besuchen Sie unsere Website.



Video anschauen

Kontakt
+49 (0)2234 69000 / csat@qssolutions.de / www.qssolutions.de