Handbuch für das Security Analyse Tool "SecCheck"

V0.5 vom 01. März 2024

Inhaltsverzeichnis

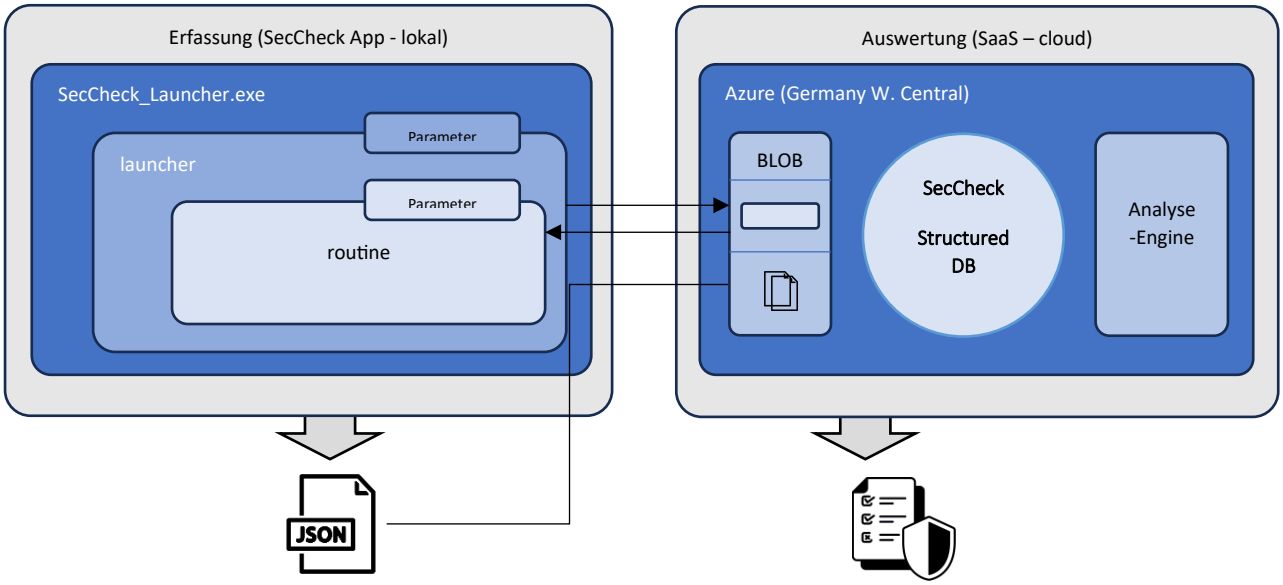
Legende:

Um die Lesbarkeit und Benutzerfreundlichkeit des Handbuchs zu verbessern, haben wir alle Optionen, die eine spezifische Anpassung an individuelle Kundenanforderungen ermöglichen, mit einem speziellen Symbol hervorgehoben. Bitte beachten Sie, dass solche Anpassungen in der Regel einen erhöhten Konfigurationsaufwand mit sich bringen.

1. Einleitung

Das Security Analyse Tool "SecCheck" bietet eine umfangreiche Lösung für Unternehmen, um Sicherheitsaspekte ihrer Windows-Systeme zu überprüfen und zu bewerten. Es setzt sich zusammen aus einer SecCheck-App, die Daten vom Client-System sammelt, und einer Analyse-Engine, die diese Daten auswertet und in einem detaillierten SecCheck-Report zusammenfasst.

Die SecCheck-App benötigt keine Installation auf dem Ziel-System und kann manuell oder im Rahmen automatisierter Prozesse ausgeführt werden. Sie liest lediglich Daten aus, ohne Änderungen am System vorzunehmen. Sie interagiert mit den von Hersteller bereitgestellten Komponenten in der Cloud. Sollten spezielle Anforderungen eine direkte Kommunikation nicht erlauben, so können spezielle Enterprise-Einstellungen getroffen werden.



2. Systemanforderungen

Das Tool unterstützt derzeit folgende Betriebssysteme:

Windows 10 1809 oder höher

Windows 11 21H2 oder höher

Windows Server 2019 (1809 LTSC) oder höher

Windows Server 21H2 oder höher

Für den Standardbetrieb wird Folgendes benötigt:

- Internetzugriff für Uploads und Downloads via HTTPS auf https://storagesecccheckqagwc.blob.core.windows.net (Port 443)
- Eine gültige E-Mail-Adresse für den Versand des Berichts

Falls eine Internetverbindung zum genannten Ziel nicht verfügbar oder nicht gewünscht ist, bietet das Collector-Tool eine alternative "Offline"-Funktion. Mit dieser Option können Datensätze generiert und auf einem internen Speicher oder einem Netzwerkfreigabeort abgelegt werden. Um diese Daten anschließend zu analysieren, ist eine manuelle Übermittlung an unsere Analyse-Engine erforderlich. Um das geeignete Verfahren hierfür zu besprechen, bitten wir Sie, sich mit unserem Kundensupport in Verbindung zu setzen.

3. Datensammlung

Die Collector-App ist unter folgendem Link erhältlich: https://storagesecchecckqagwc.blob.core.windows.net/SecCheck_Launcher.exe. Für eine umfassende Analyse ist es empfehlenswert, die App mit Administratorrechten zu starten. Die App unterstützt diverse Parameter, um eine Anpassung an spezifische Bedürfnisse und eine automatisierte Ausführung ohne Benutzerinteraktion zu ermöglichen.

Verfügbare Parameter:

EmailResponse: E-Mail-Adresse für den Berichtversand.

EULAaccepted: Zustimmung zur Endbenutzer-Lizenzvereinbarung für die Automatisierung.

SkipTestConnection: Unterlässt die Überprüfung einer Internetverbindung beim Start.

ServiceProviderLogoURL: URL für das Logo des Dienstanbieters.

SkipWUA: Überspringt die Sammlung von Windows Update-Daten.

HideUserData: Anonymisiert Benutzerdaten vor dem Versand zur Analyse.

CompressOutput: Erzeugt eine komprimierte JSON-Datei zur Reduzierung der Uploadgröße.

SaveLocalReport: Speichert das Analyseergebnis lokal ab.

NoUpload: Verhindert den Upload der Daten zum Analyse-Server.

BLOBdirectUpload: Pfad zum eigenen Azure BLOB-Speicher für die Datenspeicherung.

CustomerBlobUrl: URL zum kundenspezifischen BLOB-Speicher.

CustomerSASwriteToken: SAS-Token für den Schreibzugriff auf den BLOB-Speicher.

ReportLanguage: Sprache des Berichts (derzeit unterstützt: "de-DE", "en-US").

AccessToken: Token zur Erweiterung des Leistungsumfangs.

LicenseToken: Token zur Verifizierung einer gültigen Lizenz.

GPresult: Steuert die Durchführung eines GPresult auf dem Client.

NoValidation: Deaktiviert die manuelle Prüfung bei Analysefehlern.

Beispielaufruf über CMD:

perl

Copy code

.\SecCheck_Launcher_QA_ADMIN.exe -EmailResponse "jon.doe@example.com" -EULAaccepted -LicenseToken "ixlF-cV3F" -SkipTestConnection

4. Datenanalyse und Berichterstattung

Nach der Datensammlung werden die Daten zur Analyse-Engine übertragen, die einen ausführlichen Bericht im HTML-Format erstellt. Dieser Bericht wird an die angegebene E-Mail-Adresse gesendet. Bitte überprüfen Sie auch Ihren Junk-Mail-Ordner und fügen Sie die Adresse report@securitybaselinecheck.com zu Ihren vertrauenswürdigen Absendern hinzu.

5. Häufig gestellte Fragen (FAQ)

Frage: Ich erhalte einen Bericht, aber einige Details fehlen.

Antwort: Dies tritt auf, wenn kein gültiger Lizenz-Token angegeben wurde. In solchen Fällen wird ein verkürzter Bericht erstellt. Für eine vollständige Analyse erwerben Sie bitte einen Lizenz-Token über den Azure Marketplace oder unter https://www.securitybaselinecheck.com.

6. Support und Kontakt

Bei weiteren Fragen oder für Unterstützung kontaktieren Sie bitte das ITManager SecCheck Team:

E-Mail: support@securitybaselinecheck.com

Telefon: +49 178 178 178