iQ.Suite Watchdog Sandbox

Abwehr von neuen Bedrohungen durch Sandbox-Verhaltensanalyse

Merkmale

- Dynamische Verhaltens-analyse von Dateien & Dokumenten mit ausführ-barem Inhalt
- Unterstützung verschiedener Betriebssysteme *(Windows, Mac OS X, Android)*
- Aufdeckung von Malware-Verschleierungstechniken
- Auswahl zu analysierender Dateitypen
- Unterstützte Dateiformate
  - *Ausführbare Dateien z.B. EXE, COM und DLL*
  - *MS Office Dokumente inkl. Makros, z.B. XLSX, DOCM und RTF*
  - *PDF-Dokumente*
  - *Archive, z.B. ZIP, RAR, & CAB*
- Nahtloses Zusammenspiel mit Virenscannern

Malware-Verhalten unter der Lupe

In Zeiten hochentwickelter Angriffe bedarf es innovativer Technologien um neuartige Bedrohungen abzuwehren. Sandbox-Lösungen setzen dort an, wo die Möglichkeiten traditioneller Virenscanner enden: Sie erkennen dank dynamischer Verhaltensanalyse auch Schadcode, der sich unter dem Radar herkömmlicher Sicherheitslösungen bewegt.

Als Bestandteil unserer mehrstufigen Sicherheitslösung, steht Ihnen mit der Sandbox-Technologie in iQ.Suite Watchdog eine solche Lösung zur Verfügung. Dateien und Dokumente werden in einer abgesicherten Cloud-Umgebung unter realen Bedingungen auf schadhaftes Verhalten untersucht. Es wird auch Malware erkannt, die ihr bösartiges Verhalten verschleiert oder nur nach einer bestimmten Zeit aktiv wird. Sie haben dabei die volle Kontrolle, welche Dateien in die Cloud hochgeladen und analysiert werden. Auch aktuelle Bedrohungen, wie Krypto-Trojaner, die sich in Makros von Office Dokumenten verstecken, werden zuverlässig erkannt.

iQ.Suite Watchdog Sandbox

Cloud-basierte Abwehr von Cyberattacken

Vorteile

- Schutz vor unbekannter Malware
- Bereitstellung umfangreicher Bedrohungsinformationen
- Schnell einsatzbereit aus der Cloud
- Keine kostenintensive lokale Sandbox-Installation
- Einfache Verwaltung
- Hohe Performance
- Umfangreiche Reports

Über GBS

GBS ist führender Anbieter von Lösungen und Services für die Microsoft und IBM Collaboration Plattformen.

Weltweit vertrauen mehr als 5.000 Kunden und 4 Millionen Anwender auf die Expertise von GBS.

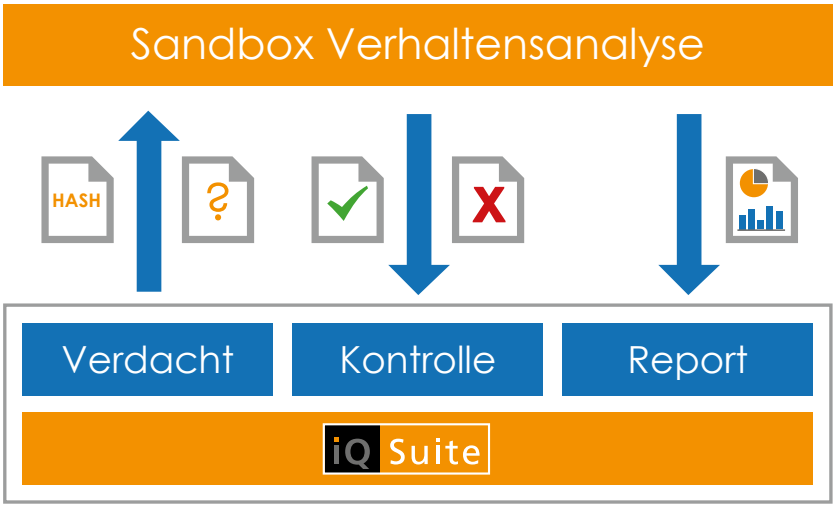
Stark im Zusammenspiel

Um bestmögliche Ergebnisse bei gleichzeitig hoher Performance zu erzielen, empfiehlt sich zunächst der Einsatz eines mehrstufigen Viren- und Spamschutzes, wie er in iQ.Suite Watchdog und Wall verfügbar ist. Im nächsten Schritt werden dann die verbleibenden, unbekannten Bedrohungen an die Sandbox geschickt und einer umfassenden Analyse unterzogen.

Diese mehrstufigen Sicherheitsmechanismen arbeiten nahtlos mit der Sandbox-Analyse zusammen und bieten das Rückgrat einer durchdachten Sicherheitsstrategie.

Die 4 Schritte der Sandbox-Analyse

1. Hashwerte der verdächtigen Dateien werden mit denen bekannter Malware verglichen (lokal/Cloud).
2. Ist die Datei bekannt, wird sie bei positiver Rückmeldung zugestellt oder bei negativer Rückmeldung in der Quarantäne platziert.
3. Bei unbekannten Dateien wird eine anonymisierte Kopie der verdächtigen Datei an die Sandbox gesendet, in einer sicheren Cloud-Umgebung ausgeführt und analysiert. Je nach Einstufung erfolgt die Zustellung bzw. Ablehnung der Datei.
4. Im letzten Schritt werden forensische Reports zu jedem Bedrohungsereignis bereitgestellt, die tiefere Einblicke und Kontextinformationen liefern.



Ob unter Microsoft Exchange/SMTP, Office 365 oder IBM Domino: Mit der flexiblen Cloud-basierten Sandbox für iQ.Suite Watchdog sind Sie bestens vor den neuesten Bedrohungen geschützt.