Konfigurieren der Integration von ThreatGrid-Appliances mit Drittanbieterlösungen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie unterstützte Drittanbieter-Integrationen mit der ThreatGrid-Appliance (TGA) konfiguriert und Fehler behoben werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ThreatGrid-Appliance
- Cisco Umbrella

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die Threat Grid Appliance (TGA) kann mit Services von Drittanbietern integriert werden, um zusätzliche Analysedaten für eine eingesendete Stichprobe bereitzustellen. Zu diesen Services gehören derzeit VirusTotal und Umbrella Investigate.

Konfiguration

Tipp: In TGA Cluster Operations wird jeder TGA-Knoten einzeln konfiguriert. Wenn die einzelnen TGA-Knoten nicht konfiguriert werden, können inkonsistente Ergebnisse erzielt werden.

Hinweis: Integrationen, die von der verschmutzten Schnittstelle der Einheit stammen; Die schmutzige Schnittstelle muss angeschlossen und für einen ordnungsgemäßen Betrieb ausgehender Zugriff zugelassen werden.

Schritt 1: Melden Sie sich bei der **Admin-**Schnittstelle der TGA an.

Schritt 2: Navigieren Sie zu **Configuration>Integrations.**

Schritt 3: Konfigurieren Sie die TGA mit den erforderlichen Einstellungen.

```
  Virus Total
    URL: http://www.virustotal.com/vtapi/v2/
    Key: (Obtained API key from the Virus Total Website)

Umbrella/OpenDNS Configuration Details
    Investigate API Key (Obtained from Umbrella Console)
```

Schritt 4: Klicken Sie nach der Konfiguration auf **Speichern** und dann auf **Übernehmen.**

Hinweis: Wenn Sie auf **Speichern** klicken**,** übernimmt TGA die Konfiguration und kann für die Verarbeitung von Beispielen für eine Dauer von bis zu 20 Minuten nicht verfügbar sein. Eingesendete Stichproben werden in der Reihenfolge verarbeitet, in der sie empfangen wurden, sobald die Konfigurationsanwendung abgeschlossen ist.

Überprüfen

Schritt 1: **Senden Sie** ein Beispiel (Datei oder URL) zur Überprüfung.

Schritt 2: Nach Abschluss der Probe; Zeigen Sie den erstellten Beispielanalysebericht an.

Schritt 3: Navigieren Sie zu **Verhaltensindikator.**

Schritt 4: Erfolgreiche Integration bedeutet Erkennung durch Antivirus Service. Ohne VirusTotal-Integration tritt diese Erkennung nicht auf. Im Bild wird ein Beispiel für eine erfolgreiche Integration angezeigt.

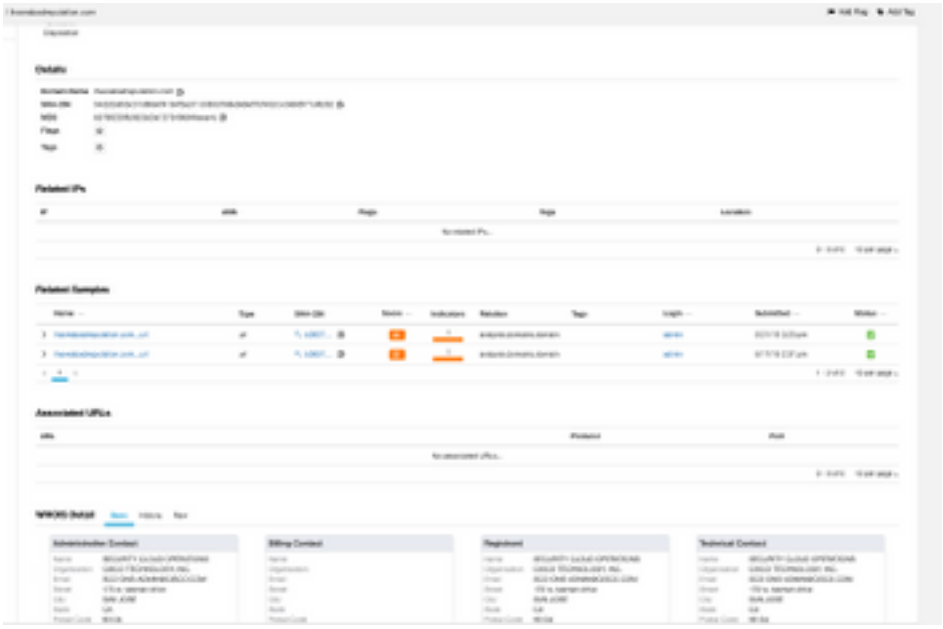
Schritt 1: **Senden Sie** ein Beispiel (Datei oder URL) zur Überprüfung.

Schritt 2: Nach Abschluss der Probe; Zeigen Sie den erstellten Beispielanalysebericht an.

Schritt 3: Navigieren Sie zu **Extracted Domain (Extrahierte Domäne).**

Schritt 4: Wählen Sie eine URL aus.

Schritt 5: Die erfolgreiche Integration zeigt zusätzliche Details der ausgewählten URL an. Im Bild wird ein Beispiel angezeigt.



Fehlerbehebung

Um zu überprüfen, ob der API-Schlüssel korrekt ist, können Sie die Fehlerbehebung auf jedem Gerät durchführen, auf dem Ping und Curl installiert sind.

> **Tipp**: Ersetzen Sie **<key>** durch den entsprechenden API-Schlüssel, wie er im Konfigurationsabschnitt für den ordnungsgemäßen Betrieb angegeben ist.

VirusTotal

Query Example
curl --request GET --url 'https://www.virustotal.com/vtapi/v2/file/report?apikey= &resource=

Success Response
{"scans":
{"Bkav": {"detected": true, "version": "1.3.0.10239", "result": "W32.FamVT.RorenNHc.Trojan", "update": "20190522"},
"MicroWorld-eScan": {"detected": true, "version": "14.0.297.0", "result": "Trojan.CryptZ.Gen", "update": "20190522"},
"CMC": {"detected": false, "version": "1.1.0.977", "result": null, "update": "20190321"},
"CAT-QuickHeal": {"detected": true, "version": "14.00", "result": "Trojan.Swrort.A", "update": "20190522"},
"McAfee": {"detected": true, "version": "6.0.6.653", "result": "Swrort.i", "update": "20190522"},
"Cylance": {"detected": true, "version": "2.3.1.101", "result": "Unsafe", "update": "20190522"},
"VIPRE": {"detected": true, "version": "75204", "result": "Trojan.Win32.Swrort.B (v)", "update": "20190522"},

"Qihoo-360": {"detected": true, "version": "1.0.0.1120", "result":
"HEUR/QVM20.1.5BD9.Malware.Gen", "update": "20190522"}},
"scan_id": "7943e9a19548a94f481f9dfdf448c835789a462ccb6740ebabda901ed5e909a2-1558548981",
"sha1": "936c9a7a5c92d2987569f3dbe1a8bddee80e98e7",
"resource": "7943e9a19548a94f481f9dfdf448c835789a462ccb6740ebabda901ed5e909a2", "response_code":
1, "scan_date": "2019-05-22 18:16:21",
"permalink":
"https://www.virustotal.com/file/7943e9a19548a94f481f9dfdf448c835789a462ccb6740ebabda901ed5e909a
2/analysis/1558548981/",
"verbose_msg": "Scan finished, information embedded", "total": 72, "positives": 50,
"sha256": "7943e9a19548a94f481f9dfdf448c835789a462ccb6740ebabda901ed5e909a2", "md5":
"327684f9c54b2785b7b67510c3aed372"}

Umbrella/OpenDNS

Query Example
curl --interface dirty -H "Authorization: Bearer

https://investigate.api.umbrella.com/domains/categorization/

Success Response
{"example.com":{"status":0,"security_categories":[],"content_categories":["54"]}}

Invalid API Key Example
{"error":"unauthorized"}