Configurar integrações da terceira parte do dispositivo de ThreatGrid

Índice

Introdução

Este original descreve como configurar e pesquisar defeitos integrações da terceira apoiadas com o dispositivo de ThreatGrid (TGA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivo de Cisco ThreatGrid
- Guarda-chuva de Cisco

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A fim fornecer a informação analítica adicional de uma amostra submetida, o dispositivo da grade da ameaça (TGA) integra com serviços de terceira parte. Estes serviços incluem atualmente VirusTotal e o guarda-chuva investiga.

Configuração

Dica: Em operações do conjunto TGA cada nó TGA é configurado individualmente. A falha configurar cada nó TGA pode conduzir aos resultados inconsistentes.

Nota: Fonte das integrações da relação suja do dispositivo; a relação suja deve ser conectada e permitiu o acesso externo para operações apropriadas.

Etapa 1. Entre à relação de **Opadmin (Admin) do** TGA.

Etapa 2. Navegue aos **>Integrations da configuração.**

Etapa 3. Configurar o TGA com os ajustes exigidos.

```
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)
```

Etapa 4. **A salvaguarda** uma vez configurada do clique e clica então **aplica-se.**

Nota: Quando você clica a **salvaguarda,** TGA aplica a configuração e pode ser não disponível processar amostras por até 20 minutos. As amostras submetidas estão processadas na ordem recebida uma vez que o procedimento do aplicativo da configuração é terminado.

Verificar

Etapa 1. **Submeta uma** amostra (arquivo ou URL) para a revisão.

Etapa 2. Após conclusão da amostra; Veja o relatório gerado do Sample Analysis.

Etapa 3. Navegue ao **indicador comportável.**

Etapa 4. A integração bem sucedida indica a detecção pelo serviço do Antivirus. Sem integração de VirusTotal, esta detecção não ocorre. Um exemplo bem sucedido da integração é mostrado na imagem.

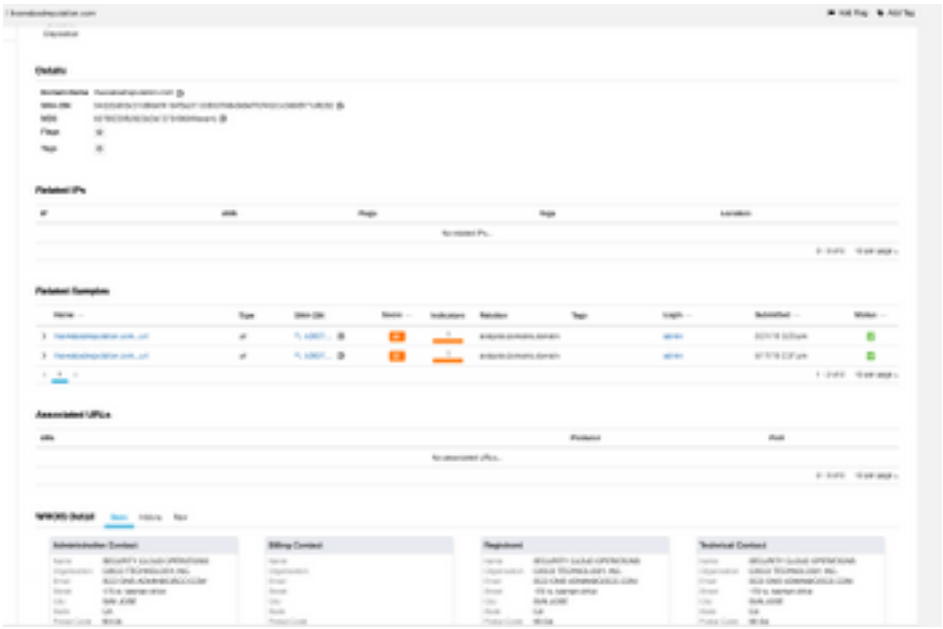
Etapa 1. **Submeta uma** amostra (arquivo ou URL) para a revisão.

Etapa 2. Após conclusão da amostra; Veja o relatório gerado do Sample Analysis.

Etapa 3. Navegue ao **domínio extraído.**

Etapa 4. Selecione uma URL.

Etapa 5. A integração bem sucedida indica detalhes adicionais da URL selecionada. Um exemplo é mostrado na imagem.



Troubleshooting

A fim verificar que a chave API está correta, você pode terminar o procedimento da pesquisa de defeitos de todo o dispositivo que tiver o sibilo e a onda instalados.

> Dica: Substitua o **<key>** com a chave correspondente API como obtido na seção de configuração para a operação apropriada.

VirusTotal

```
Query Example
curl --request GET --url
'https://www.virustotal.com/vtapi/v2/file/report?apikey=<key>&resource=<sha256>'

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/7943e9a19548a94f481f9dfdf448c835789a462ccb6740ebabda901ed5e909a2/analysis/1558548981/",
"verbose_msg": "Scan finished, information embedded", "total": 72, "positives": 50,
"sha256": "7943e9a19548a94f481f9dfdf448c835789a462ccb6740ebabda901ed5e909a2", "md5":
"327684f9c54b2785b7b67510c3aed372"}

Guarda-chuva/OpenDNS

Query Example
curl --interface dirty -H "Authorization: Bearer <key>"
"https://investigate.api.umbrella.com/domains/categorization/<URL>"

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

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