# Configurazione di Secure Malware Analytics Appliance con Umbrella

## Sommario



## Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi alle integrazioni di terze parti supportate con Secure Malware Analytics Appliance (in precedenza Threat Grid).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Malware Analytics
- Cisco Umbrella

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

- Umbrella
- Appliance Secure Malware Analytics

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Per fornire ulteriori informazioni analitiche su un campione inviato, ad esempio il punteggio di rischio Umbrella, l'appliance Malware Analytics si integra con Umbrella tramite la chiave API.

## Configurazione

---

> Suggerimento: nelle operazioni di cluster TGA ogni nodo TGA è configurato singolarmente. La mancata configurazione di ogni nodo TGA può causare risultati incoerenti.

---

> Nota: le integrazioni provengono dall'interfaccia dirty dell'accessorio; l'interfaccia dirty deve essere collegata e deve essere consentito l'accesso in uscita per il corretto funzionamento.

---

Passaggio 1. Accedi al dashboard Umbrella e fai clic su Amministrazione > Licenze nel menu di navigazione a sinistra. Il tipo di pacchetto corrente verrà visualizzato.

Passaggio 2. Accertarsi di disporre della licenza per il corso SIG https://umbrella.cisco.com/products/umbrella-enterprise-security-packages

Passaggio 3. Nel dashboard Umbrella fare clic su Indaga > Chiavi API > Copia token di accesso API

Passaggio 4. Accedere all'interfaccia Opadmin (Admin) di Malware Analytics Appliance.

Passaggio 5. Selezionare Configurazione > Integrazioni.

Passaggio 6. Configurare il TGA con i token di accesso API.

Una volta configurati, fare clic su Save (Salva), quindi su Reconfigure (Riconfigura).

Passaggio 7. Utilizzare RASH per l'appliance del cliente per eseguire

systemctl: tg-supervisor con riavvio senza blocco

Passaggio 8. Verificare che la licenza disponga del livello API appropriato:

curl —include —request POST —header "Authorization: Bearer 12345678910" —data-binary "["cnn.com"]" https://investigate.api.umbrella.com/domains/categorization

---

> Nota: per aggiornare la licenza, è necessario contattare l'account manager del cliente. Impossibile completare l'azione desiderata perché la licenza di livello 1 non ha accesso agli endpoint in blocco. È quindi necessario aggiornare la licenza al livello 2 o al livello 3.

---

Passaggio 1. Inviare un esempio di URL per l'analisi.

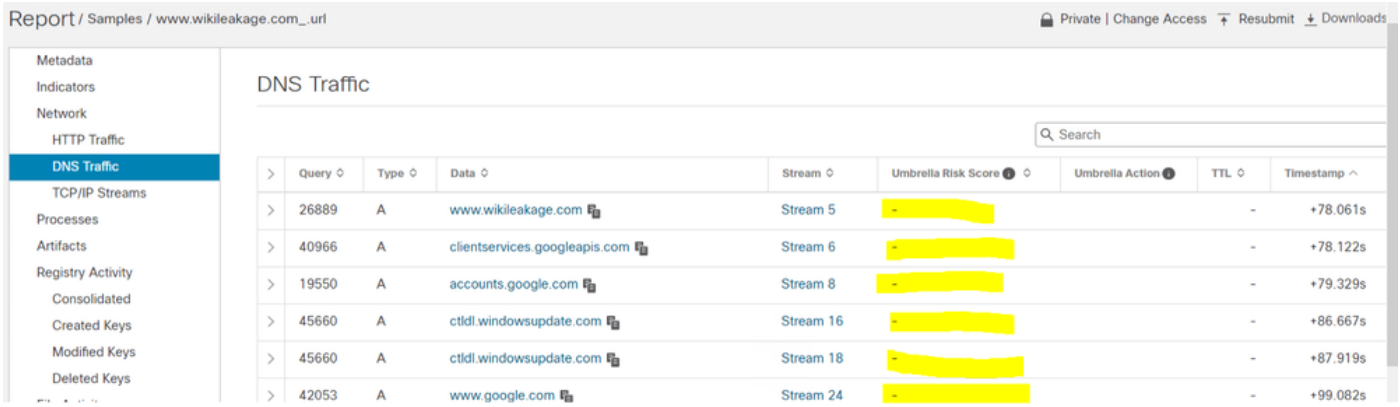
Passaggio 2. Dopo il completamento dell'esempio, visualizzare gli esempi>traffico DNS.

Passaggio 3. Passare al punteggio Umbrella Risk.

# Risoluzione dei problemi

1. Il punteggio di rischio complessivo non è presentato nel campione di appliance di analisi malware nel traffico DNS

Accertarsi di non ricevere l'errore HTTP 403 nel passaggio 8. Verificare che la licenza disponga del livello API appropriato.




Per risolvere questo problema, i clienti devono contattare lo specialista della sicurezza e l'account team per aggiornare le licenze Umbrella. Non è compito né responsabilità del GATE aiutare con la licenza Umbrella.

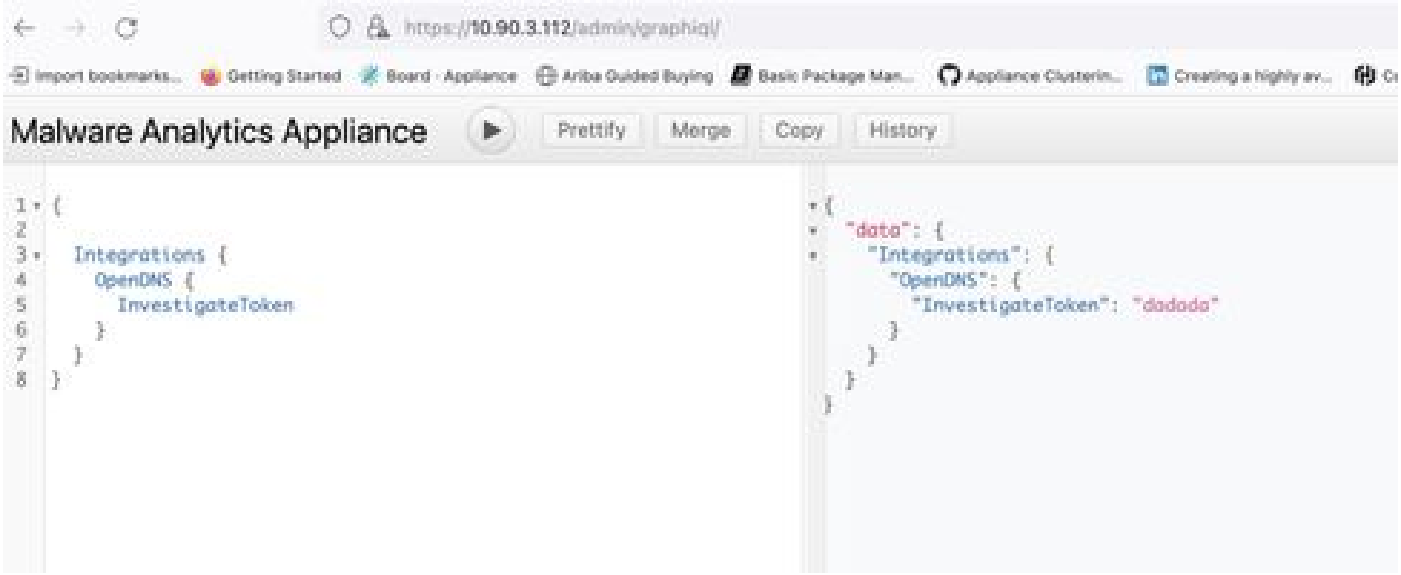
2. Il token Umbrella non viene salvato nell'appliance Malware Analytics

Per verificare che il token API Umbrella sia hardcoded correttamente nell'accessorio, è possibile utilizzare graphiql per eseguire una query sul file di configurazione. La risposta deve essere il token Umbrella API corretto ottenuto dal dashboard Umbrella.

---

> Suggerimento: sostituire <IP> con il nome host corrispondente della TGA, cancellare i valori predefiniti e digitare esattamente ciò che è sullo schermo a sinistra, quindi premere il pulsante play.

---


https://10.90.3.112/admin/graphiql/
Import bookmarks...
Getting Started
Board · Appliance
Ariba Guided Buying
Basic Package Man...
Appliance Clusterin...
Creating a highly av...
Malware Analytics Appliance
Prettify
Merge
Copy
History
{
Integrations {
OpenDNS {
InvestigateToken
}
}
}
{
"data": {
"Integrations": {
"OpenDNS": {
"InvestigateToken": "dadada"
}
}
}
}

graphiql

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).