

Configurazione dell'app Cloud Security per IBM QRadar

Sommario

[Introduzione](#)

[Panoramica](#)

[Requisiti](#)

[Requisiti di Cisco Umbrella](#)

[Requisiti SIEM per IBM Security QRadar](#)

[Installazione di Cisco Cloud Security App per IBM QRadar](#)

[Configurazione app Cisco Cloud Security: Aggiunta dell'origine del log](#)

[Generazione del token di autenticazione](#)

[Configurazione dell'app Cisco Cloud Security](#)

[Indicizzazione in QRadar](#)

Introduzione

In questo documento viene descritto come configurare l'app Cisco Cloud Security con IBM QRadar per l'analisi dei log.

Panoramica

QRadar di IBM è un popolare SIEM per l'analisi dei log. Fornisce una potente interfaccia per l'analisi di grandi blocchi di dati, ad esempio i registri forniti da Cisco Umbrella per il traffico DNS della tua organizzazione. Cisco Cloud Security App per IBM QRadar offre informazioni dettagliate su più prodotti di sicurezza (Investigate, Enforcement e CloudLock) e li integra con QRadar. Consente inoltre all'utente di automatizzare la sicurezza e contenere le minacce in modo più rapido e diretto da QRadar.

Quando si configura l'app Cisco Cloud Security per QRadar, integra tutti i dati della piattaforma Cisco Cloud Security e consente di visualizzare i dati in formato grafico nella console QRadar. Dall'applicazione, gli analisti possono:

- Analizza domini, indirizzi IP, indirizzi e-mail
- Bloccare e sbloccare i domini (imposizione)
- Visualizzare le informazioni di tutti gli incidenti della rete.

Questo articolo descrive le procedure di base per la configurazione e l'esecuzione di QRadar in modo che possa estrarre i registri dal secchio S3 e utilizzarli.

Requisiti



Nota: Il supporto per QRadar deve provenire da IBM, in quanto Cisco non è in grado di supportare direttamente hardware o software di terze parti. Per qualsiasi problema di collegamento del dashboard Umbrella al secchio S3, Dell può fornire assistenza. Molte delle informazioni reperibili qui sono reperibili anche sul sito web di IBM:

https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umbrella.html

Requisiti di Cisco Umbrella

In questo documento si presume che il bucket S3 di Amazon AWS sia stato configurato in Umbrella (Impostazioni > Gestione log) e sia visualizzato in verde con i log recenti caricati.

Per ulteriori informazioni su come configurare questa funzione, vedere: [Gestione dei log](#).

Requisiti SIEM per IBM Security QRadar

L'amministratore deve disporre di diritti amministrativi per gli accessori QRadar, la configurazione Amazon S3 e il dashboard Umbrella. In base a queste istruzioni, l'amministratore QRadar ha

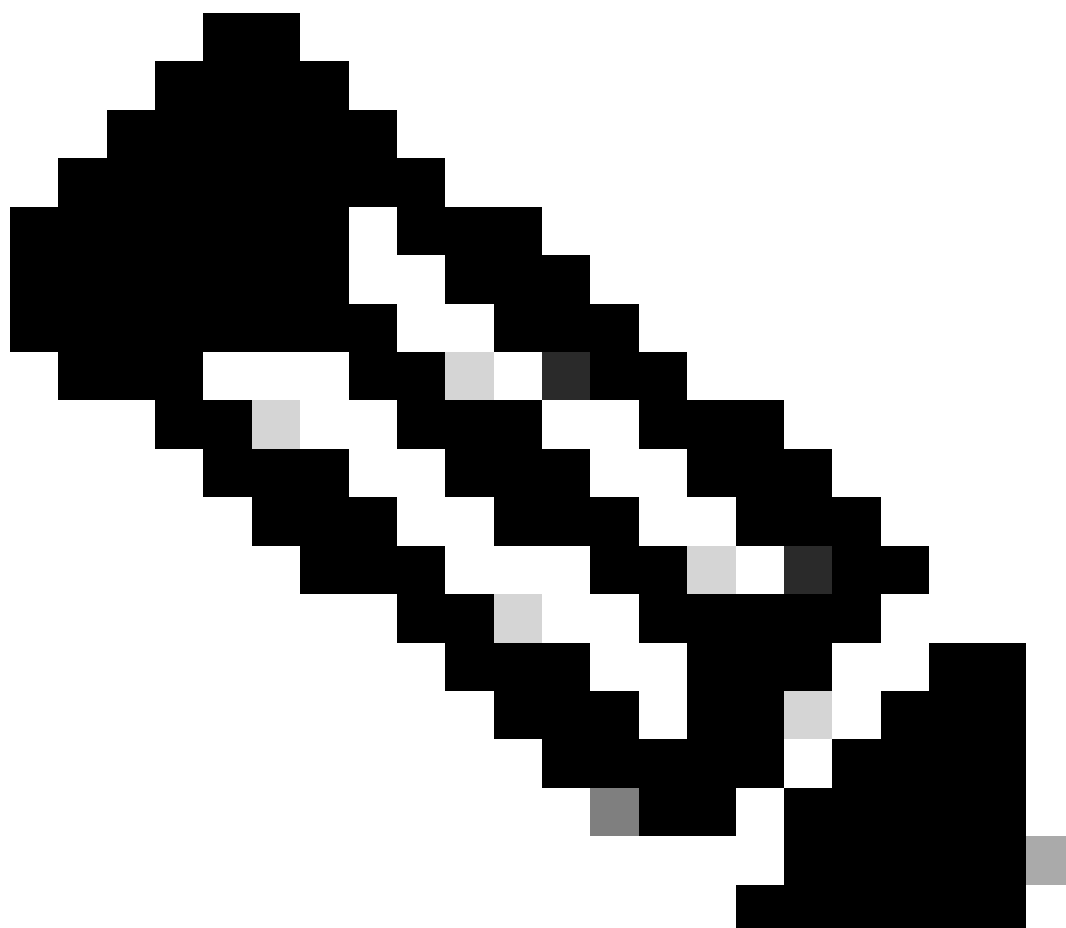
familiarità con la creazione di file LSX (Log source Extension).

Tenere presente che Cisco Cloud Security App v1.0.3 funziona solo con IBM QRadar 7.2.8. La nuova versione, v1.0.6, funziona con l'attuale versione QRadar dalla 7.4.2 e successive.

Installazione di Cisco Cloud Security App per IBM QRadar

1. Scaricare e installare Cisco Cloud Security App per IBM QRadar, disponibile qui: [Cisco Cloud Security App v1.0.3](#) (per IBM QRadar v7.2.8) o [Cisco Cloud Security App v1.0.6](#) (per IBM QRadar v7.4.8).
2. Dopo l'installazione, distribuire le modifiche in QRadar.

Configurazione app Cisco Cloud Security: Aggiunta dell'origine del log



Nota: In S3 è possibile visualizzare altri log, ad esempio Audit e Firewall, ma questi non

sono supportati. Impostare solo i tre elencati qui. Qualsiasi tentativo di configurare gli altri registri genera un errore.

Per aggiungere un'origine registro, fare clic sulla scheda Admin sulla barra di navigazione QRadar, scorrere verso il basso e fare clic su QRadar Log Source Management, quindi fare clic sul pulsante +New Log Source:

- Nome origine log (i nomi delle voci devono corrispondere esattamente a quelli elencati):
 - Registri DNS Cisco: log_ombrello_dns_cisco
 - Log IP di Cisco Umbrella: cisco_umbrella_ip_logs
 - Registri proxy Cisco Umbrella: log_ombrello_proxy_cisco
- Formato evento: Cisco Umbrella CSV
- Tipo origine registro: Cisco Umbrella
- Configurazione protocollo: API REST Amazon AWS S3
- Modello file: .*?\.\csv\.\gz
- Estensione origine registro: Cisco Umbrella_ext **
- Selezionare i gruppi di cui si desidera che l'origine registro sia membro:
gruppo_origine_log_ombrello_cisco

Per ulteriori informazioni, vedere Aggiunta guidata singola origine log:

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Select a Log Source type

Search: umbre

Cisco Umbrella

Step 2: Select Protocol Type

4404306773524

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Select a protocol type

Look up Protocol Type

Amazon AWS S3 REST API

Forwarded

☐ Show Undocumented Protocol Types

Step 1: Select Log Source Type

Step 3: Configure Log Source Parameters

4404306773268

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Configure the Log Source parameters

Name *
The name of the log source.

cisco_umbrella_dns_logs

Description
An optional description of the log source.

Enabled
Indicates whether the log source should be enabled.

☒ On

Groups *
The groups that this log source will belong to.

cisco_umbrella_logsource_group

Q

+ Add Group

Extension
Log Source Extensions perform post-processing of events after default parsing has occurred.
[+ Show More](#)

CiscoUmbrella_ext

X

▼

Step 2: Select Protocol Type

Step 4: Configure Protocol Parameters

4404313505300

Configure the protocol parameters

^ [AWS Authentication Configuration]

Log Source Identifier *

cisco_umbrella_dns_logs

Authentication Method *

- Access Key ID / Secret Key: Standard Access Key authentication

[+ Show More](#)

Access Key ID / Secret Key

Access Key ID *

The Access Key ID that is required to access the AWS S3 bucket.

XXXXXXXXXXXXXXXXXXXX

Secret Key *

The Secret Key that is required to access the AWS S3 bucket.

XXXXXXXXXXXXXXXXXXXX

^ [AWS S3 Collection Configuration]

S3 Collection Method *

Use a Specific Prefix - Single Account/Region Only

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

4404306774164

IBM QRadar Log Source Management - Add a Single Log Source

☒ Select Log Source Type

☐ Select Protocol Type

☐ Configure Log Source Parameters

☒ Configure Protocol Parameters

☐ Test Protocol Parameters

Configure the protocol parameters

^ [AWS S3 Collection Configuration]

S3 Collection Method *

Choose how to collect the data.

[+ Show More](#)

Use a Specific Prefix - Single Account/Region Only

Bucket Name *

The name of the AWS S3 bucket where the log files are stored.

cisco-managed-eu-west-2

Directory Prefix *

The root directory location on the AWS S3 bucket from which the files are retrieved.

[+ Show More](#)

:3_51f2a158aad51ec7a68449a10400ba027acc00c3/dnslogs/

Region Name *

The Region the SQS Queue or S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3

eu-west-2

Event Format *

Choose the format of the events that are contained in the files.

[+ Show More](#)

Cisco Umbrella CSV

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

4404306897556

Test Protocol Parameters



[Restart](#)

Results (4):

- ✓ Testing DNS resolution of [s3.amazonaws.com]
- ✓ Testing TCP connection to [s3.amazonaws.com:443]
- ✓ Testing SSL connection to [s3.amazonaws.com:443]
- ✓ Testing access to S3 Bucket [cisco-managed-eu-west-2]

Events (5):

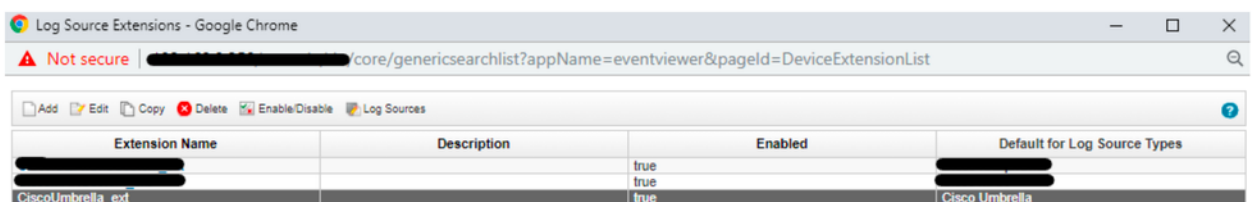
Log Source Identifier	Payload
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-44ea.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-a6fd.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-cb6f.csv.gz"}

Step 4: Configure Protocol Parameters

Finish

4404306881812

Nota: Se l'estensione dell'origine del log non è mappata a "CiscoUmbrella_ext", scegliere il nome dell'origine del log dall'elenco:



Extension Name	Description	Enabled	Default for Log Source Types
[REDACTED]		true	[REDACTED]
[REDACTED]		true	[REDACTED]
CiscoUmbrella_ext		true	Cisco Umbrella

360071157752

Edit a Log Source Extension

Name

CiscoUmbrella_ext

Description

Log Source Types

Available

3Com 8800 Series Switch

APC UPS

AhnLab Policy Center APC

Akamai KONA

Amazon AWS CloudTrail

Amazon AWS Security Hub

Amazon GuardDuty

Ambion TrustWave ipAngel Intrusion Prevention Sy

Apache HTTP Server

Application Security DbProtect

Set to default for

Cisco Umbrella

Upload Extension:

Choose file

No file chosen

Upload

Extension Document

```
<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
<pattern id="UserName-Pattern-1">"MostGranularIdentity":(.*)"</pattern>
<pattern id="EventName-Pattern-1">(.*)</pattern>
<match-group device-type-id-override="431" order="1">
  <matcher order="1" enable-substitutions="true" capture-group="1" pattern-id="UserName-Pattern-1" field="UserName" />
  <matcher order="1" capture-group="1" pattern-id="EventName-Pattern-1" field="EventName" />
  <event-match-multiple force-qidmap-lookup-on-fixup="false" send-identity="UseDSMResults" pattern-id="EventName-Pattern-1" />
</match-group>
</ns2:device-extension>
```

Save

Cancel

360071326791

Di seguito è riportato un esempio di un bucket gestito da Cisco:

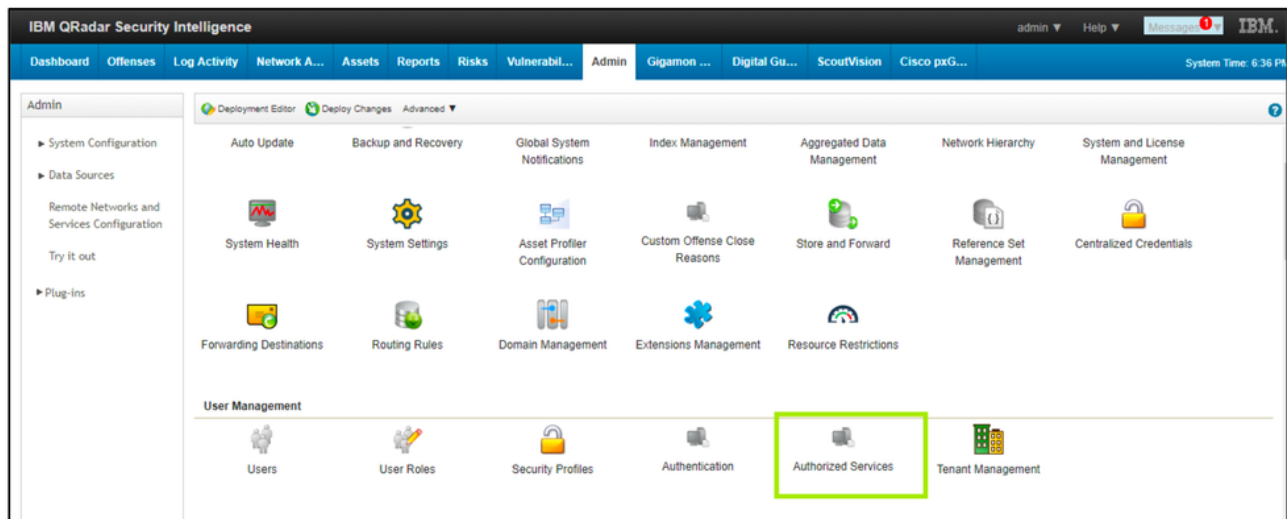
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxx/dnslogs

Tornare a Cisco Cloud Security App Settings e impostare la frequenza di aggiornamento del pannello in ore su un valore minimo di "1" per consentire ai grafici di visualizzare i dati.

Generazione del token di autenticazione

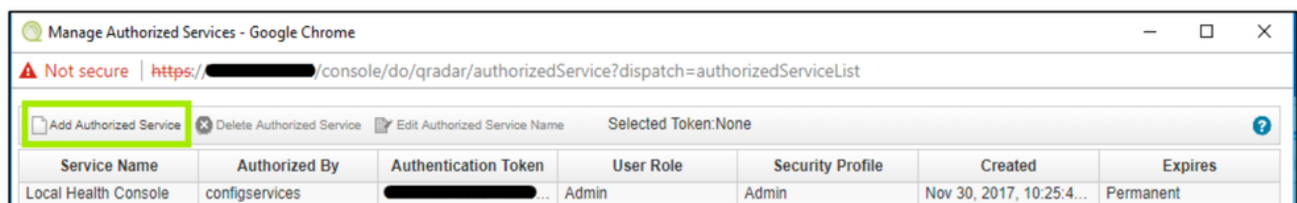
L'amministratore deve generare un token del servizio da aggiungere all'app Cisco Security. È buona norma ricreare il token del servizio autorizzato ogni 90 giorni:

1. Accedere a QRadar > Scheda Amministrazione > Servizi autorizzati.



360071965571

2. Aggiungere servizi autorizzati.



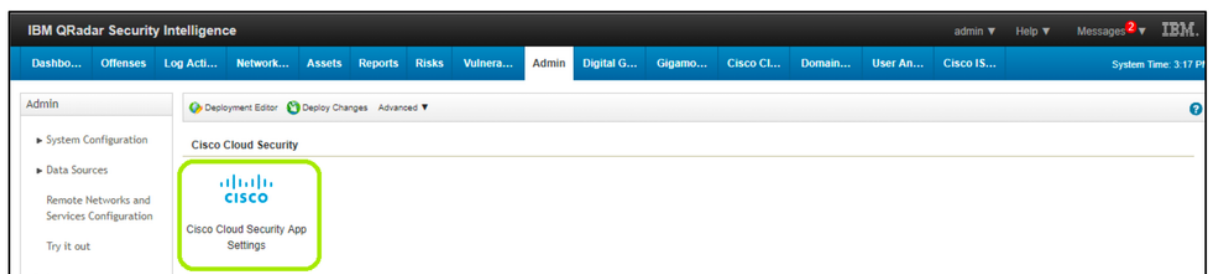
360071965551

3. Immettere i dettagli e generare il token di autenticazione.

4. Dopo aver generato il token, fare clic su "Deploy Changes" (Distribuisce modifiche).

Configurazione dell'app Cisco Cloud Security

1. Dalla scheda Admin sulla barra di navigazione di QRadar, scorrere verso il basso e aprire Cisco Cloud Security App Settings.



360071754732

2. Immettere il token di autenticazione generato nel passaggio precedente.



Qradar Settings

QRadar Server IP	
QRadar Server port	
QRadar service token	

360072462992

3. Modificare le impostazioni dell'Api come segue:

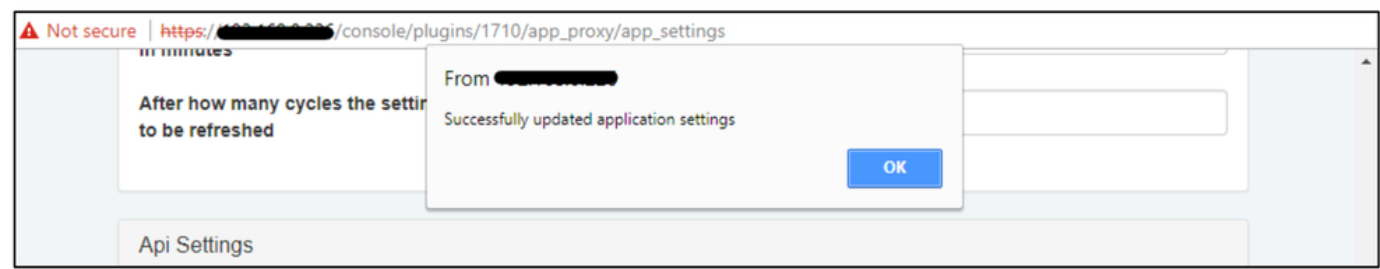
- URL di base investigazione Cisco: <https://investigate.api.umbrella.com/>
- Token API Cisco Investigate: genera mediante il dashboard Umbrella -> Indaga -> Chiavi API -> Crea nuovo token; per ulteriori informazioni, visitare il sito <https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key>
- URL di base Cisco Enforce: <https://s-platform.api.opendns.com/1.0/>
- Cisco Enforce CustomerKey: genera mediante il dashboard Umbrella -> Componenti delle policy -> Integrazioni -> Aggiungi; per ulteriori informazioni, visitare il sito <https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations>
- URL di base Cisco Cloudlock: <https://{YourCloudlockAPIServer}/api/v2> (ad esempio, <https://api-demo.cloudlock.com/api/v2/>). Confermare l'URL di base Cloudlock o l'URL dell'API Cloudlock Enterprise inviando un'e-mail a support@cloudlock.com.)
- Token API Cisco Cloudlock: generate via Cloudlock -> Settings -> Authentication & API -> Generate; per ulteriori informazioni, visitare il sito <https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication>

Api Settings

Show Cisco Cloudlock incident details to end user	☒ Yes ☐ No
Show Cisco Cloudlock UEBA Panels	☒ Yes ☐ No
Cisco Investigate Base URL	
Cisco Investigate API token	
Cisco Enforce Base URL	
Cisco Enforce CustomerKey	
Cisco Cloudlock Base URL	
Cisco Cloudlock API token	

360072703611

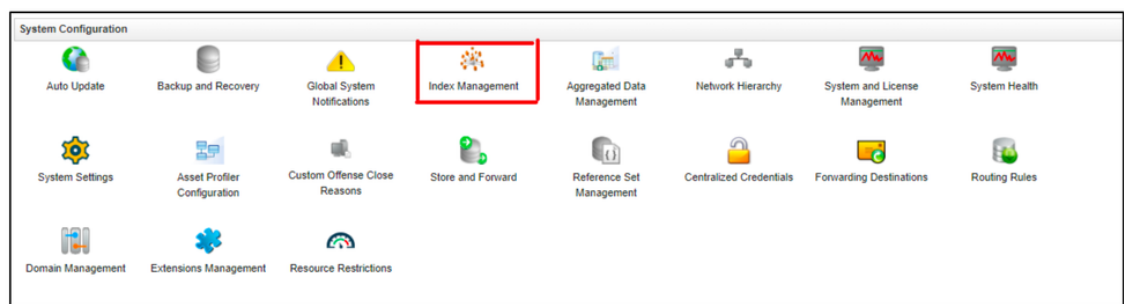
Un popup indica che le impostazioni dell'applicazione sono state aggiornate correttamente.



360071986151

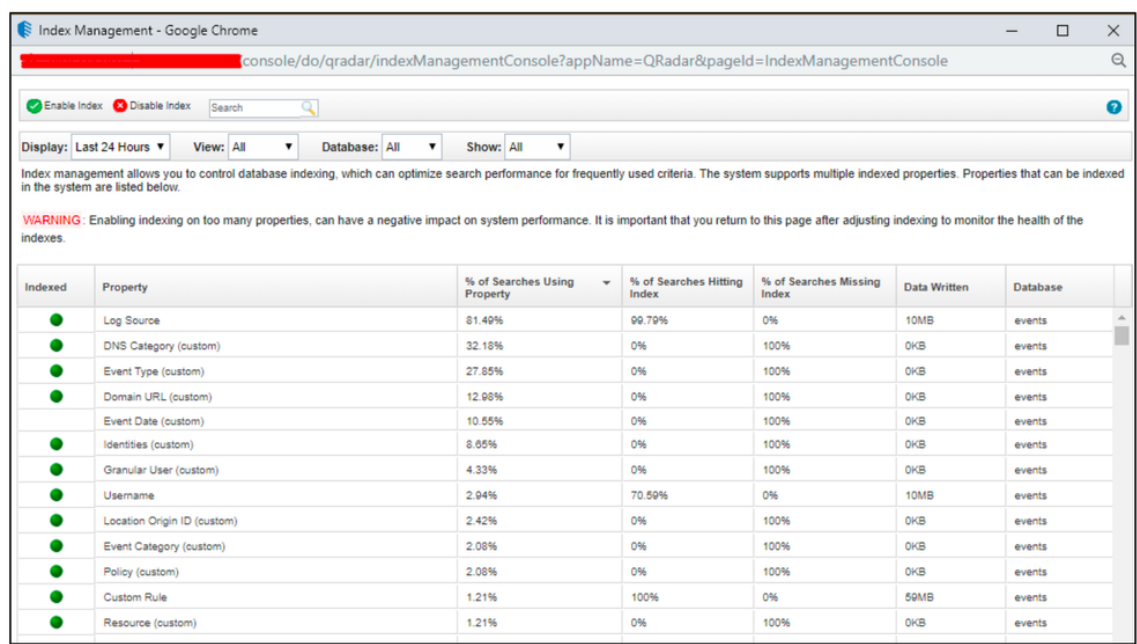
Indicizzazione in QRadar

1. Passare alla scheda Admin, quindi fare clic su Index Management (Gestione indici).



360071780112

2. Indicizza i CEP inseriti nel pacchetto con l'app.



360071988811

Di seguito sono riportati i CEP consigliati da indicizzare:

1. Origine registro
2. Categoria DNS
3. Tipo di evento
4. URL dominio
5. Identità
6. Utente granulare
7. Username
8. ID origine ubicazione
9. Categoria evento
10. Policy
11. Risorsa

A questo punto è possibile utilizzare QRadar per iniziare le attività di monitoraggio per i dettagli Cisco Umbrella, Investigate e CloudLock. Ulteriori istruzioni su come navigare in QRadar sono disponibili qui: [Navigazione in Cisco Cloud Security App](#).

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).