Ad integrazione di quanto scritto vi segnalo alcune osservazioni (in rosso i punti relativi alla mail):

- Il conteggio delle righe di codice è **giornaliero**

* Si è verificato che ad oggi:
  + In collaudo per 5 gg di retention il valore delle righe è circa 155.000
  + In parallelo per 10 gg di retention il valore delle righe è circa 85.000

- In merito alla frase: "Nello stesso RH conferma che tutti i punti di requisiti di sicurezza sono rispettati." Red Hat non può certificare che tutti i requisiti di sicurezza sono rispettati, i macro punti di cui abbiamo parlato, sono presenti negli audit logs per quanto inerenti con il prodotto, ma ad esempio eventuali operazioni su antivirus apparati di sicurezza collegati ad openshift non sono visibili negli audit.

Riporto cosa è possibile intercettare:

Tutte le operazioni effettuate alle configurazioni di OpenShift ed alle risorse dello stesso (CRD , Service Account... etc), nel dettaglio

* watch
* list
* get
* delete
* create
* patch
* update
* list
* post

Dalla configurazione attualmente implementata sono esclusi nell'invio al SIEM tutti i logs di tipo infrastructure / application.

**Tutti i punti di sicurezza vanno dettagliati e riportati nel contesto OpenShift, in quanto al momento sono troppo generici e non siamo a conoscenza delle esatte risorse che volete monitorare.**

È opportuno validare e certificare una lista di risorse e operazioni presenti negli audit logs tramite il supporto Red Hat, attraverso un nuovo case, oppure integrando sul case già aperto per il filtering: [https://access.redhat.com/support/cases/#/case/03844939/](https://urldefense.com/v3/__https:/access.redhat.com/support/cases/*/case/03844939/__;Iw!!OrxsNty6D4my!8g87lIJ8I5rsgS3ZoUhM5WJQKgd5gxrKXjtgYRKYw9Kmy5XLQ-LnM50xEQho24TkkhEoLCHgeUwRYPfSfSEj-SOCtlPQ5w$)

- Per quanto concerne la frase: "Durante l’ultima ora del meeting CAGS SEC ha approfondito con RH...." abbiamo intercettato e descritto le operazioni di Login Success / Failed e Logout

In particolare:

Login Failed:

```json

"annotations": {

"[authentication.openshift.io/decision](https://urldefense.com/v3/__http:/authentication.openshift.io/decision__;!!OrxsNty6D4my!8g87lIJ8I5rsgS3ZoUhM5WJQKgd5gxrKXjtgYRKYw9Kmy5XLQ-LnM50xEQho24TkkhEoLCHgeUwRYPfSfSEj-SMd3sVcuw$)": "deny",

"[authentication.openshift.io/username](https://urldefense.com/v3/__http:/authentication.openshift.io/username__;!!OrxsNty6D4my!8g87lIJ8I5rsgS3ZoUhM5WJQKgd5gxrKXjtgYRKYw9Kmy5XLQ-LnM50xEQho24TkkhEoLCHgeUwRYPfSfSEj-SNJ6iKdkw$)": "pippo",

"requestURI": "/login",

"verb": "post"

```

Login Success:

```json

"annotations": {

"[authentication.openshift.io/decision](https://urldefense.com/v3/__http:/authentication.openshift.io/decision__;!!OrxsNty6D4my!8g87lIJ8I5rsgS3ZoUhM5WJQKgd5gxrKXjtgYRKYw9Kmy5XLQ-LnM50xEQho24TkkhEoLCHgeUwRYPfSfSEj-SMd3sVcuw$)": "allow",

"[authentication.openshift.io/username](https://urldefense.com/v3/__http:/authentication.openshift.io/username__;!!OrxsNty6D4my!8g87lIJ8I5rsgS3ZoUhM5WJQKgd5gxrKXjtgYRKYw9Kmy5XLQ-LnM50xEQho24TkkhEoLCHgeUwRYPfSfSEj-SNJ6iKdkw$)": "kubeadmin",

"requestURI": "/login",

"verb": "post"

```

Logout:

```json

"requestURI": "/apis/[oauth.openshift.io/v1/oauthaccesstokens/\*](https://urldefense.com/v3/__http:/oauth.openshift.io/v1/oauthaccesstokens/*__;Kg!!OrxsNty6D4my!8g87lIJ8I5rsgS3ZoUhM5WJQKgd5gxrKXjtgYRKYw9Kmy5XLQ-LnM50xEQho24TkkhEoLCHgeUwRYPfSfSEj-SOuwVBNrQ$)",

"responseObject": {

"userName": "afilice",

"userUID": "5c5eda6c-4ce1-48b6-bb99-a57abf98d2b1"

},

"verb": "delete"

```

Aggiungo inoltre che non è possibile eliminare i logs simili ai seguenti e presenti al path /var/log/audit/audit.log:

|  |
| --- |
|  |
| type=PROCTITLE msg=audit(1719402301.327:11715): proctitle=2F7573722F7362696E2F43524F4E002D50 |
|  |

In quanto è richiesta una funzionalità presente in OpenShift Logging 5.9

```yaml

- drop:

- test:

- field: .message

matches: ^type=

name: drop\_audit\_linux

type: drop

```

Cordialmente

Il giorno mer 26 giu 2024 alle ore 13:20 Ragno, Filomena <[filomena.ragno@accenture.com](mailto:filomena.ragno@accenture.com)> ha scritto:

Ciao

  Di seguito un recap della sessione odierna.

* Si è verificato che ad oggi:
  + In collaudo per 5 gg di retention il valore delle righe è circa 155.000
  + In parallelo per 10 gg di retention il valore delle righe è circa 85.000
* Durante la call sono stati effettuati i seguenti interventi operativi:

***COLLAUDO***

A scopo di test e al fine di definire quali sono i corretti campi di login e logout avvenuti e falliti, è stato proceduto ad applicare ulteriore configurazione.

Il log aggiuntivi che venivano visti lato SIEM facevano riferimento a Jaeger, JWT del service account che viene rinnovato ogni 24 ore. Si è proceduto a raffinare ulteriormente il log di riferimento.

***PARALLELO***

·       Per gli ulteriori punti riportati sotto, RH segnala che per gli stessi, al fine di essere esaustivi, è necessario che vengano inviati tutti gli audit log:

o   Operazioni che permettono di alterare il funzionamento dei sistemi (es. modifiche ai parametri di configurazione, avvio/arresto dei sistemi, ecc.)

o   Operazioni che permettono di alterare la configurazione di sicurezza dei sistemi con conseguente esposizione a vulnerabilità (es. cancellazione o modifica di regole di accesso impostate su apparati di sicurezza, disattivazione del sistema antivirus, ecc.)

o   Operazioni che possono compromettere l’erogazione dei servizi (es. arresto o riavvio di una macchina che eroga un particolare servizio agli utenti, ecc.);

o   Operazioni di modifica della profilazione degli utenti o assegnazione di nuove abilitazioni.

·       Effettuata configurazione per inoltro del file di audit log. Nello stesso RH conferma che tutti i punti di requisiti di sicurezza sono rispettati.

* Di seguito documentazione fornita da RH per dettagli su:
  + *Login e Logout per audit log*

[https://docs.redhat.com/it/documentation/openshift\_container\_platform/4.14/html/security\_and\_compliance/audit-log-view#nodes-pods-audit-log-basic\_audit-log-view](https://urldefense.com/v3/__https:/docs.redhat.com/it/documentation/openshift_container_platform/4.14/html/security_and_compliance/audit-log-view*nodes-pods-audit-log-basic_audit-log-view__;Iw!!OrxsNty6D4my!8g87lIJ8I5rsgS3ZoUhM5WJQKgd5gxrKXjtgYRKYw9Kmy5XLQ-LnM50xEQho24TkkhEoLCHgeUwRYPfSfSEj-SNZ1GIpsA$)

* *Descrizione dei campi per audit log*

[https://docs.redhat.com/it/documentation/openshift\_container\_platform/4.14/html/security\_and\_compliance/audit-log-view#nodes-pods-audit-log-basic\_audit-log-view](https://urldefense.com/v3/__https:/docs.redhat.com/it/documentation/openshift_container_platform/4.14/html/security_and_compliance/audit-log-view*nodes-pods-audit-log-basic_audit-log-view__;Iw!!OrxsNty6D4my!8g87lIJ8I5rsgS3ZoUhM5WJQKgd5gxrKXjtgYRKYw9Kmy5XLQ-LnM50xEQho24TkkhEoLCHgeUwRYPfSfSEj-SNZ1GIpsA$)

[@Federico Salsa](mailto:federico.salsa@nttdata.com), [@ELISA BALLINI](mailto:elisa.ballini@nttdata.com) ci confermate che, da pianificazione complessiva di progetto, sono in corso i test di carico in ambiente di Parallelo per Openshift?

* Al termine dei test di carico, CAGS SEC confermerà che i log di audit di Parallelo arrivano e sono quelli attesi.
* A seguito della conferma dovrà essere schedulata sessione congiunta per implementare la configurazione del file di audit log verso i corretti connettori, che CAGS Security condividerà.
* Durante l’ultima ora del meeting CAGS SEC ha approfondito con RH ulteriori dettagli per parser da condividere con il SOC. [@Alberto Filice](mailto:afilice@redhat.com) per cortesia puoi condividere ultimi dettagli condivisi con Giulio?

***Prossimi passi:***

* Conferma di ricezione dei log di audit di Parallelo e conferma risultato atteso [**CAGS SEC**]
* Condivisione per ogni ambiente del connettore Target [**CAGS SEC**]
* Configurazione dell’intero audit log per tutti gli ambienti secondo i connettori condivisi al punto precedente **[ACN/RH]**