EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

Správa a dohled nad počítačovou sítí

SOC – Přihlášení Doménového Administrátora

Metodický list

Autor: Ing. Josef Bezchleba, Metodik: Bc. Jaroslav Tihlařík

Recenzent: Ing. Peter Jankovský

Rok vydání: 2023

Obsah

Cíle 2

Dovednosti 2

Pracovní prostředí 2

1 Průběh výuky 3

2 Zadání 4

2.1 ČÁST Logger 4

2.2 ČÁST ESM 5

Návod: 5

2.2.1 Filter - UC2_[Prijmeni]_Domain_Administrator_Logon 5

2.2.2 Rule – UC2_[Prijmeni]_Domain_Administrator_Logon 5

2.2.3 Active Channel – SC1_[Prijmeni]_Alerts 7

2.2.4 Úklid ESM 7

Seznam použitých zdrojů 9

Cíle

- Žák vysvětlí možné problémy spojené s přihlášením doménového administrátora na běžnou pracovní stanici.
- Žák vlastními slovy popíše možné zranitelnosti spojené s přihlašováním doménového administrátora k běžné pracovní stanici.

Dovednosti

- Žák navrhne a aplikuje filtr pro vyhledání záznamů v ArcSight Loggeru související s přihlášením doménového administrátora k běžné pracovní stanici.
- Žák interpretuje výsledky vyhledávání.
- Žák identifikuje účet doménového administrátora, který se přihlašuje na běžné pracovní stanice.
- Žák navrhne a aplikuje filtr a pravidla pro automatické vyhodnocování událostí v nástroji ArcSight ESM.

Pracovní prostředí

Úlohu lze realizovat v prostředí Cylab JCEKB

Pro práci budeme potřebovat následující:

- SCx[1] Replay Connector
- ArcSight Logger
- ArcSight ESM
- Dokument ArcSight Categorization.xlsx
- Dokument ArcSight CommonEventFormatV25.pdf
- Web: https://www.logbinder.com/

[1] Za x dosaťte číslo SC, které vám bylo přiřazeno administrátorem Cylabu.

1 Průběh výuky

Přihlaste se v prostředí Cylab do *Replay Connectoru*.

1. Opakování z předchozí hodiny
2. Spusťte program *ArcSight Replay Connector* (zástupce na ploše)
3. Přejděte na kartu *Replay*
4. Před spuštěním provozu nastavte následující parametry
    a. Část Logger a ESM: 60 událostí za **sekundu**
5. Spusťte následující provoz a nechte jej běžet:
    a. dhcp_3h.events
    b. dns_3h.events
    c. winc_3h.events
    d. UC2_Domain-Admin.events

2 Zadání

2.1 ČÁST Logger

1. Pod jakým uživatelským účtem se přihlašuje doménový administrátor?

```
categoryBehavior=/Authentication/Verify AND categoryOutcome=/Success  AND NOT
destinationUserName ENDSWITH $ | top destinationUserName
```

Odpověď: sysadmin

2. Ověř, že se skutečně jedná o privilegovaný účet s vyšším oprávněním.

```
destinationUserName=sysadmin AND externalId=4672
```

Odpověď: Ano, jedná se o privilegovaný účet s oprávněním:

SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeImpersonatePrivilege
SeDelegateSessionUserImpersonatePrivilege
SeEnableDelegationPrivilege

3. Na jaké pracovní stanice se přihlašoval administrátor za poslední 2 hodiny?

```
categoryBehavior = /Authentication/Verify AND destinationUserName="sysadmin" | top
destinationHostName
```

Odpověď: win-01.cylab.lan

4. Jaké podezřelé aktivity prováděl administrátor na stanici?

```
(destinationUserName="sysadmin" OR sourceUserName="sysadmin") AND deviceHostName = "win-
01.cylab.lan" | top name
```

Podezřelé aktivity (name, externalId):

- A user account was created, 4720
  - Vytvoření uživatele “attacker”.
- A member was added to a security-enabled local group, 4732
  - Přidání uživatele “attacker” do skupiny “Administrators”.
- A user account was deleted, 4726
  - Smazání uživatele “attacker”.
- The audit log was cleared, 1102
  - Smazání Security audit logu, zametení stop.

2.2 ČÁST ESM

Vyučující nechá žáky pracovat samostatně, ale průběžně kontroluje jejich práci. Nejdříve žáci vytvoří filtr a po společné kontrole (prezentace) pokračují žáci tvorbou pravidla. Vyučující postupně kontroluje jednotlivé části pravidla (Conditions, Aggregations, Actions) dle prezentace na obrazovce.

Žáci mají za úkol:

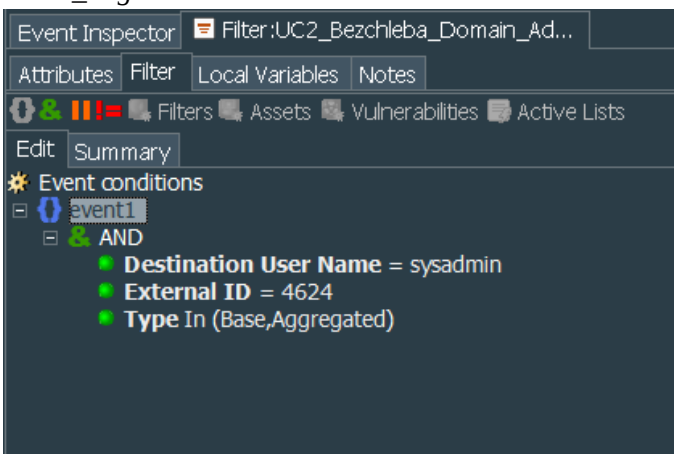
1. Vytvořte pravidlo, které bude detekovat každé úspěšné přihlášení doménováho administrátora.
    a. 1x Filtr
        i. *UC2_[Prijmeni]_Domain_Administrator_Logon*
        ii. Událost: 4624
    b. 1x Standard Rule
        i. *UC2_[Prijmeni]_Domain_Administrator_Logon*
2. Pro každou stanici nebo server kam se doménový administrátor přihlásí vznikne samostatný alert.

Práci je nutné ukončit "Úklidem ESM".

Návod:

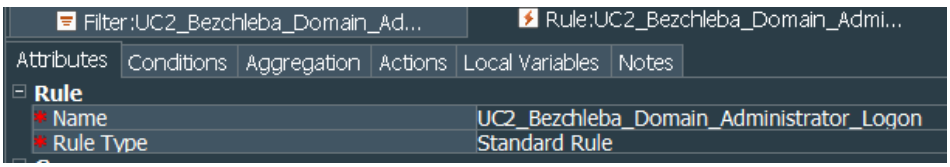
2.2.1 Filter - UC2_[Prijmeni]_Domain_Administrator_Logon

1. Vytvoříme nový filtr *Filters -> SC[x]'s Filters -> KB[x] [Prijmeni] -> UC2_[Prijmeni]_Domain_Administrator_Logon*

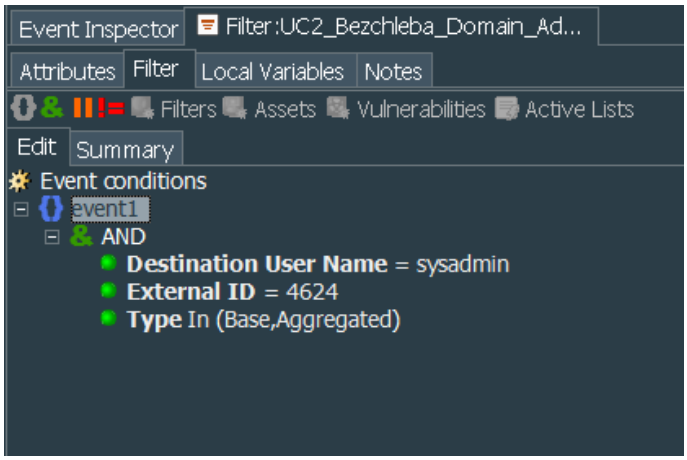


2.2.2 Rule – UC2_[Prijmeni]_Domain_Administrator_Logon

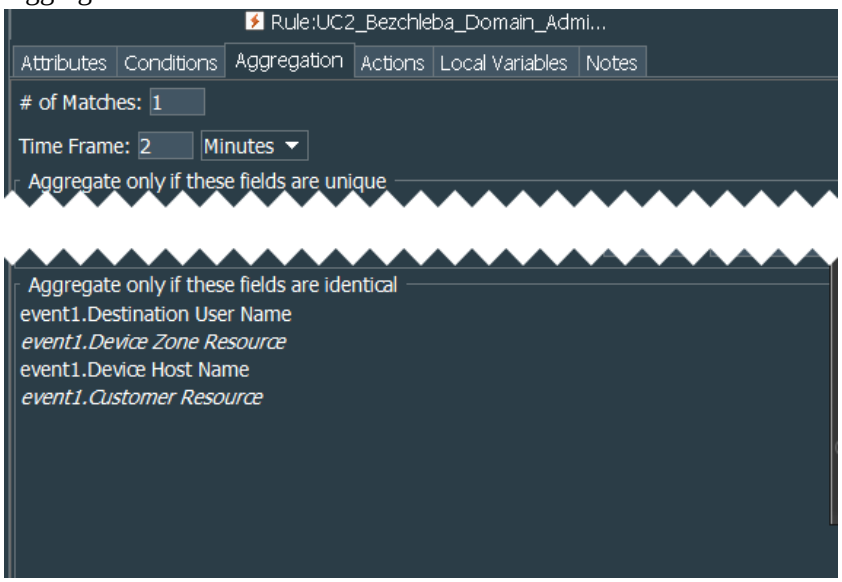
1. Vytvoříme pravidlo *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC2_[Prijmeni]_Domain_Administrator_Logon*
    a. Attributes



b. Conditions



c. Aggregation



d. Actions

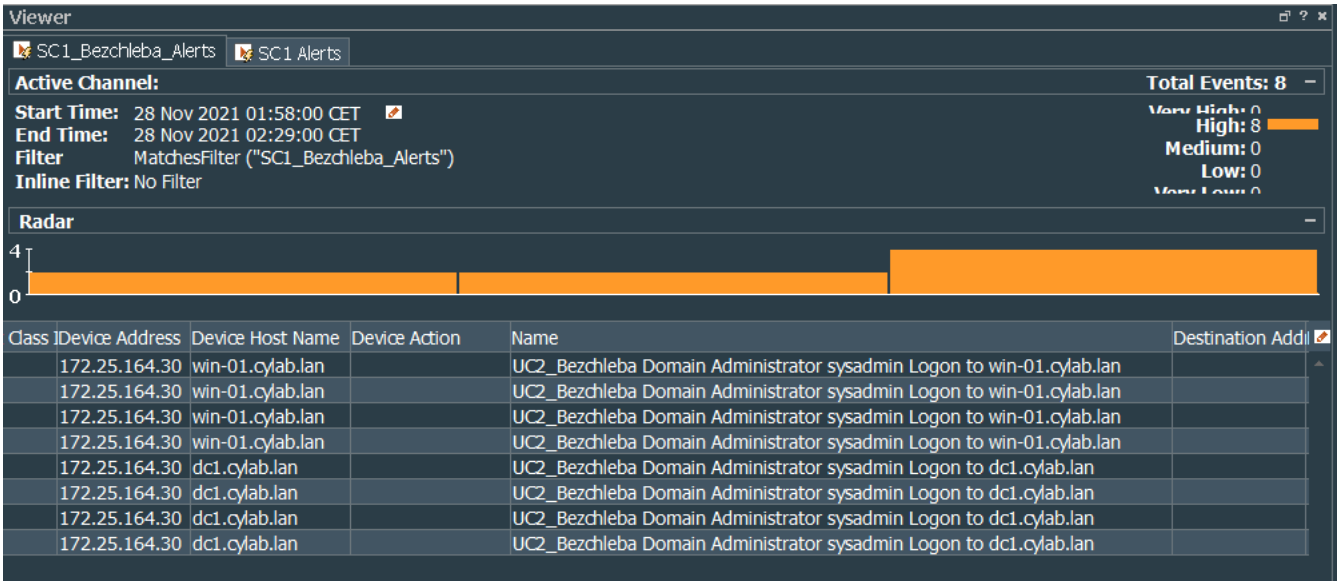
2. Pravidlo přesuneme metodou „Drag & Drop“ do složky *Rules -> Shared -> SC[x] Real-Time Rules*
   a. **Ve vyskakovacím okně „Drag & Drop zvolím Link.**

3. Pravidlo je aktivní a začíná korelovat.

2.2.3 Active Channel – SC1_[Prijmeni]_Alerts

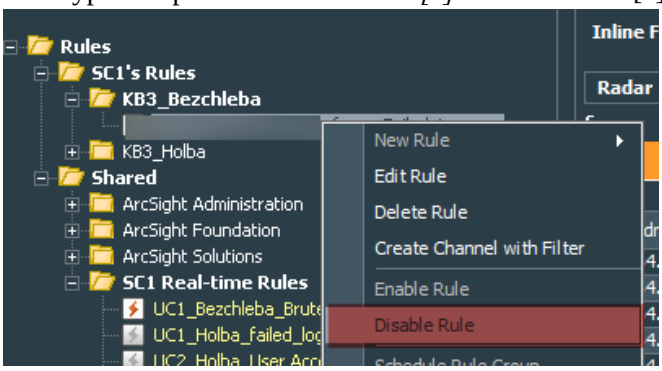
V tomto aktivním kanále zobrazíme alerty.

Pokud jsme postupovali správně, začnou se v aktivním kanále postupně zobrazovat alerty.

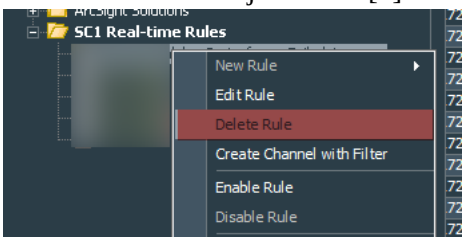


2.2.4 Úklid ESM

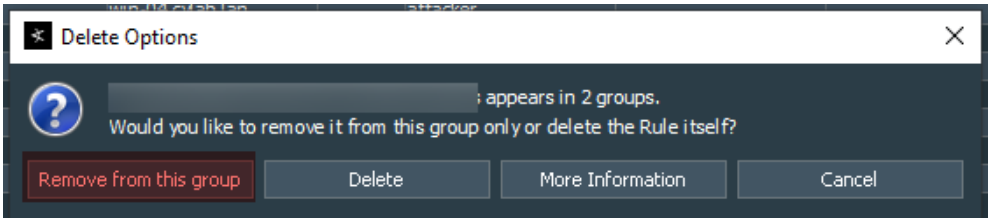
1. Vypneme pravidlo *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC2_[Prijmeni]_Administrator_Logon*



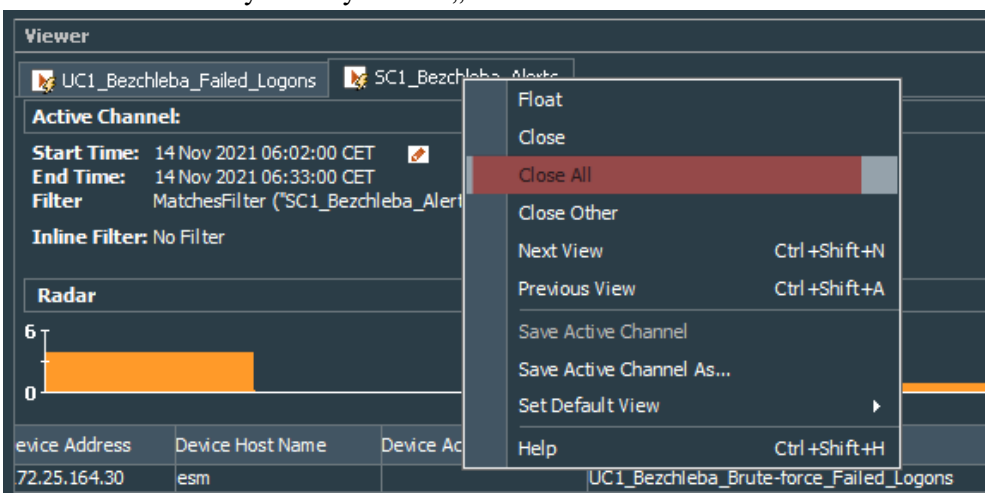
2. Pravidlo odlinkujeme z SC[x] Real-time Rules.



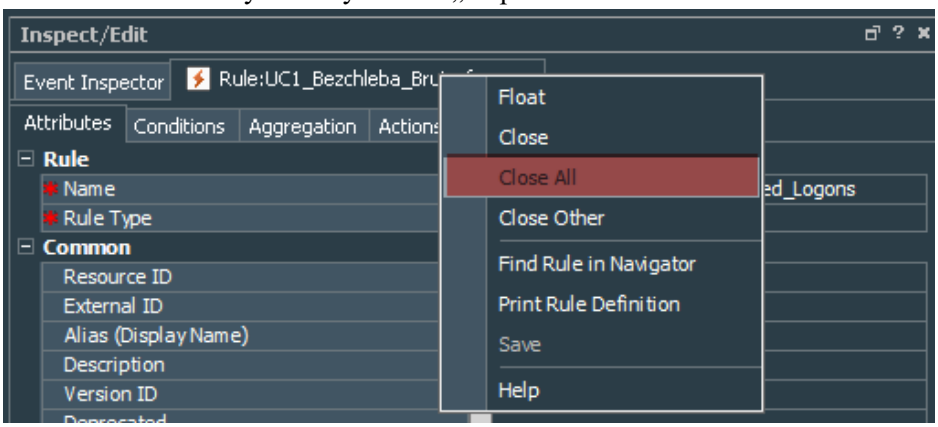
Pozor!!! Zvolíme – „Remove from this group“. Pokud bychom zvolil možnost „Delete“, tak pravidlo se celé smaže.



3. Zavřeme všechny záložky v okně „Viewer“.



4. Zavřeme všechny záložky v okně „Inspect/Edit“



Seznam použitých zdrojů

Windows Security Log Event ID 4625. *Ultimate IT Security* [online]. [cit. 2021-12-16]. Dostupné z: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

Brute Force. *MITRE ATT&CK* [online]. [cit. 2021-12-16]. Dostupné z: https://attack.mitre.org/techniques/T1110/