SeConical
SECURITY ANALYTICS

KÜRT Zrt.

Logelemzés heti riport

Felhasználói fiók, illetve felhasználói csoportkezelési műveletek

1. A DOKUMENTUM ADATLAPJA

Ez a dokumentum a SeConical rendszer Logdrill moduljában került generálásra, szerkeszthető formátumban.

A dokumentum bizalmas információkat tartalmaz! Jelen dokumentum a KÜRT Zrt. részére készült. A dokumentumot részben vagy egészben másolni, vagy bármi más módon mások számára elérhetővé tenni kizárólag a KÜRT Zrt. hozzájárulásával megengedett.

Azonosítás	Dokumentum adatai
Vállalat neve	KÜRT Zrt.
Projekt neve	**Kürt ISO 2016**
Dokumentum típusa	Logelemzés heti riport
Állomány neve	SeConical_04_riport
Dokumentum generálás dátuma	**2017-07-28 13:47**

2. FELHASZNÁLÓI FIÓK, ILLETVE FELHASZNÁLÓI CSOPORTKEZELÉSI MŰVELETEK

Az alábbi diagramokon a vizsgált időszakban naplózott felhasználói fiók, illetve felhasználói csoportkezelési műveletek (úgymint: felvétel, létrehozás, engedélyezés, letiltás, módosítás, törlés, felfüggesztés, csoporttagságok változása - pl. admin által) számának alakulása látható napi bontásban.

aaa2.

A vizsgált időszak:

- 2017.07.21 - 2017.07.27

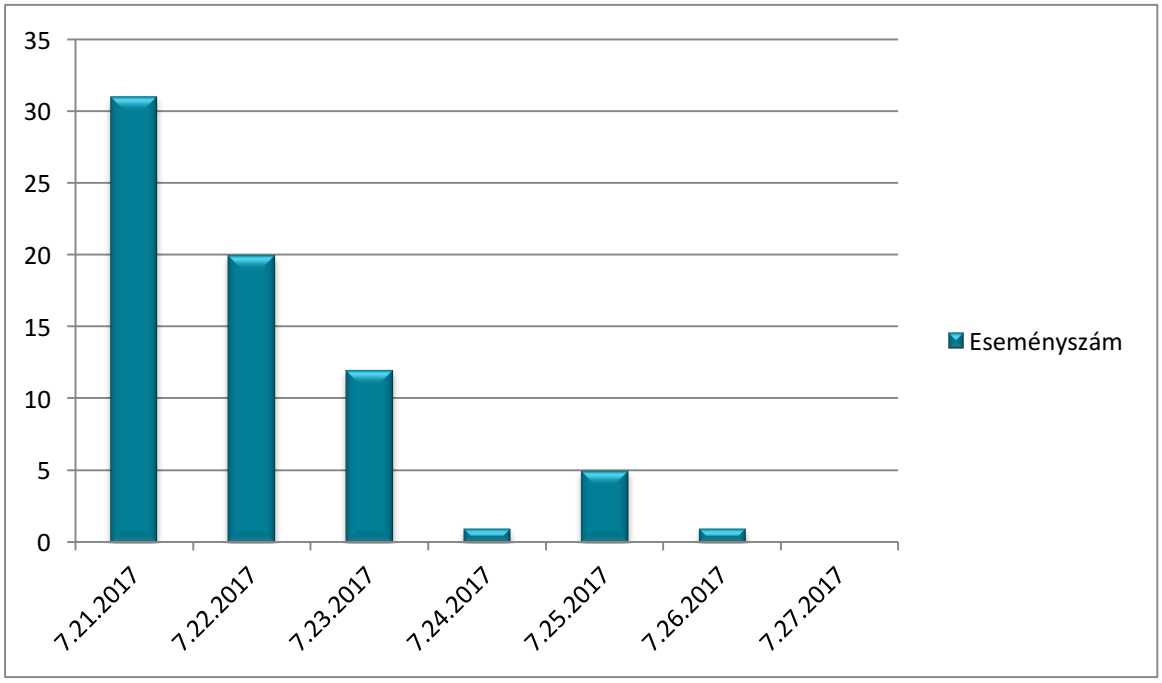
A vizsgált rendszerek:

- Windows alapú rendszerek
- Cisco ASA tűzfalak

2.1 WINDOWS ALAPÚ RENDSZEREK

Az alábbi diagramon a vizsgált időszakban naplózott felhasználói fiók, illetve felhasználói csoportkezelési műveletek (úgymint: felvétel, létrehozás, engedélyezés, letiltás, módosítás, törlés, felfüggesztés, csoporttagságok változása - pl. admin által) számának alakulása látható napi bontásban.

Az események vizsgálatával ellenőrizhetők a jóváhagyás nélkül végrehajtott felhasználói fiók változások és a kiemelt jogosultsággal történő visszaélések.



- Az események számának hirtelen növekedése, vagy adminisztrátor fiókon végzett bármilyen nem tervezett módosítás utalhat illetéktelen hozzáférésre, rosszindulatú tevékenységre. Ilyen esetekben javasolt a további vizsgálat.

2.1.1 NAPLÓ RÉSZLETEK

Részlet az eseményekhez kapcsolódó naplóbejegyzésekből:

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-A5BA-3E3B0328C30D}'/><EventID>4720</EventID><Version>0</Version><Level>0</Level><Task>13824</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2016-07-25T13:55:39.381479300Z'/><EventRecordID>1705</EventRecordID><Correlation/><Execution ProcessID='544' ThreadID='596'/><Channel>Security</Channel><Computer>jenkinsnode04</Computer><Security/></System><EventData><Data Name='TargetUserName'>bviktor</Data><Data Name='TargetDomainName'>JENKINSNODE04</Data><Data Name='TargetSid'>S-1-5-21-2637996-1648435033-1708909359-1000</Data><Data Name='SubjectUserSid'>S-1-5-21-2637996-1648435033-1708909359-500</Data><Data Name='SubjectUserName'>Administrator</Data><Data Name='SubjectDomainName'>JENKINSNODE04</Data><Data Name='SubjectLogonId'>0x314fa</Data><Data Name='PrivilegeList'>-</Data><Data Name='SamAccountName'>bviktor</Data><Data Name='DisplayName'>%%1793</Data><Data Name='UserPrincipalName'>-</Data><Data Name='HomeDirectory'>%%1793</Data><Data Name='HomePath'>%%1793</Data><Data Name='ScriptPath'>%%1793</Data><Data Name='ProfilePath'>%%1793</Data><Data Name='UserWorkstations'>%%1793</Data><Data Name='PasswordLastSet'>%%1794</Data><Data Name='AccountExpires'>%%1794</Data><Data Name='PrimaryGroupId'>513</Data><Data Name='AllowedToDelegateTo'>-</Data><Data Name='OldUacValue'>0x0</Data><Data Name='NewUacValue'>0x15</Data><Data Name='UserAccountControl'> %%2080 %%2082 %%2084</Data><Data Name='UserParameters'>%%1793</Data><Data Name='SidHistory'>-</Data><Data Name='LogonHours'>%%1797</Data></EventData><RenderingInfo Culture='en-US'><Message>A user account was created.Subject: Security ID: S-1-5-21-2637996-1648435033-1708909359-500 Account Name: Administrator Account Domain: JENKINSNODE04 Logon ID: 0x314faNew Account: Security ID: S-1-5-21-2637996-1648435033-1708909359-1000 Account Name: bviktor Account Domain: JENKINSNODE04Attributes: SAM Account Name: bviktor Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: <never> Account Expires: <never> Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User Account Control: Account Disabled 'Password Not Required' - Enabled 'Normal Account' - Enabled User Parameters: <value not set> SID History: - Logon Hours: AllAdditional Information: Privileges -</Message><Level>Information</Level><Task>User Account Management</Task><Opcode>Info</Opcode><Channel>Security</Channel><Provider>Microsoft Windows security auditing.</Provider><Keywords><Keyword>Audit Success</Keyword></Keywords></RenderingInfo></Event>

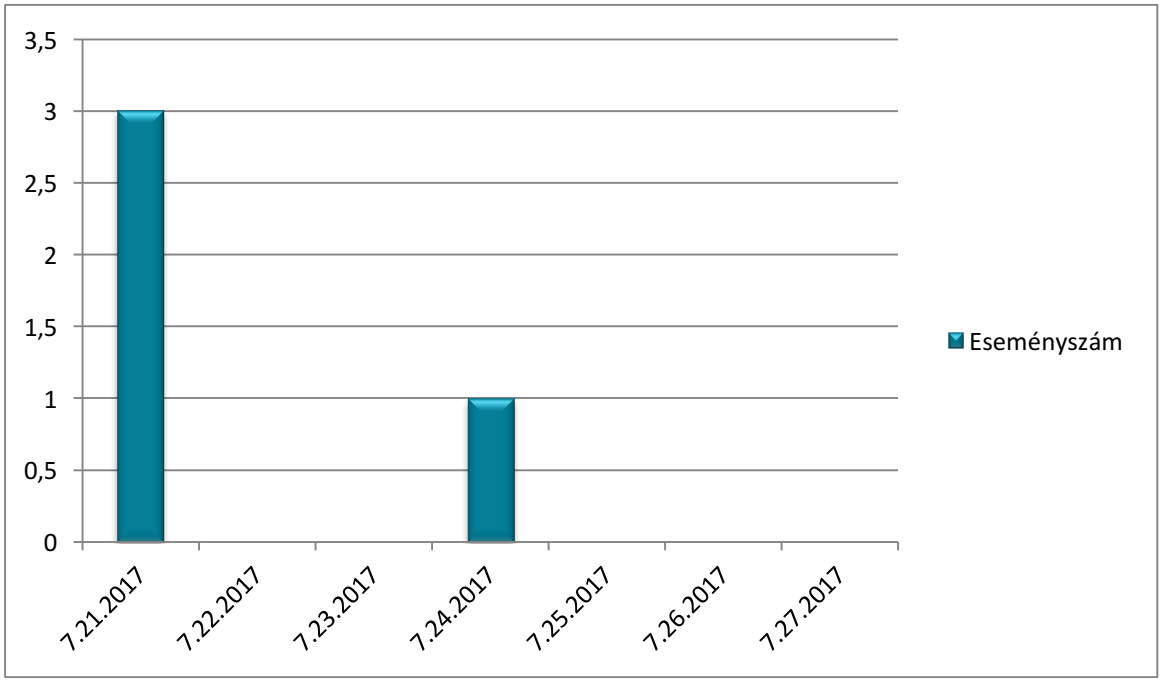
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-A5BA-3E3B0328C30D}'/><EventID>4720</EventID><Version>0</Version><Level>0</Level><Task>13824</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords><TimeCreated SystemTime='2016-07-25T13:55:39.381479300Z'/><EventRecordID>1705</EventRecordID><Correlation/><Execution

ProcessID='544'
ThreadID='596'/><Channel>Security</Channel><Computer>jenkinsnode04</Computer><Security/></System><EventData><Data Name='TargetUserName'>bviktor</Data><Data Name='TargetDomainName'>JENKINSNODE04</Data><Data Name='TargetSid'>S-1-5-21-2637996-1648435033-1708909359-1000</Data><Data Name='SubjectUserSid'>S-1-5-21-2637996-1648435033-1708909359-500</Data><Data Name='SubjectUserName'>Administrator</Data><Data Name='SubjectDomainName'>JENKINSNODE04</Data><Data Name='SubjectLogonId'>0x314fa</Data><Data Name='PrivilegeList'>-</Data><Data Name='SamAccountName'>bviktor</Data><Data Name='DisplayName'>%%1793</Data><Data Name='UserPrincipalName'>-</Data><Data Name='HomeDirectory'>%%1793</Data><Data Name='HomePath'>%%1793</Data><Data Name='ScriptPath'>%%1793</Data><Data Name='ProfilePath'>%%1793</Data><Data Name='UserWorkstations'>%%1793</Data><Data Name='PasswordLastSet'>%%1794</Data><Data Name='AccountExpires'>%%1794</Data><Data Name='PrimaryGroupId'>513</Data><Data Name='AllowedToDelegateTo'>-</Data><Data Name='OldUacValue'>0x0</Data><Data Name='NewUacValue'>0x15</Data><Data Name='UserAccountControl'> %%2080 %%2082 %%2084</Data><Data Name='UserParameters'>%%1793</Data><Data Name='SidHistory'>-</Data><Data Name='LogonHours'>%%1797</Data></EventData><RenderingInfo Culture='en-US'><Message>A user account was created.Subject: Security ID: S-1-5-21-2637996-1648435033-1708909359-500 Account Name: Administrator Account Domain: JENKINSNODE04 Logon ID: 0x314faNew Account: Security ID: S-1-5-21-2637996-1648435033-1708909359-1000 Account Name: bviktor Account Domain: JENKINSNODE04Attributes: SAM Account Name: bviktor Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: <never> Account Expires: <never> Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User Account Control: Account Disabled 'Password Not Required' - Enabled 'Normal Account' - Enabled User Parameters: <value not set> SID History: - Logon Hours: AllAdditional Information: Privileges -</Message><Level>Information</Level><Task>User Account Management</Task><Opcode>Info</Opcode><Channel>Security</Channel><Provider>Microsoft Windows security auditing.</Provider><Keywords><Keyword>Audit Success</Keyword></Keywords></RenderingInfo></Event>

2.2 CISCO ASA TŰZFALAK

Az alábbi diagramon a vizsgált időszakban naplózott felhasználói fiók, illetve felhasználói csoportkezelési műveletek (úgymint: felvétel, létrehozás, engedélyezés, letiltás, módosítás, törlés, felfüggesztés, csoporttagságok változása - pl. admin által) számának alakulása látható napi bontásban.

Az események vizsgálatával ellenőrizhetők a jóváhagyás nélkül végrehajtott felhasználói fiók változások és a kiemelt jogosultsággal történő visszaélések.



- Az események számának hirtelen növekedése, vagy felhasználói fiókon végzett bármilyen nem tervezett módosítás utalhat illetéktelen hozzáférésre, rosszindulatú tevékenységre. Ilyen esetekben javasolt a további vizsgálat.

2.2.1 NAPLÓ RÉSZLETEK

Részlet az eseményekhez kapcsolódó naplóbejegyzésekből:

Error Message %ASA-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string

Error Message %ASA-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string

Error Message %ASA-5-502111: New group policy added: name: policy_name Type: policy_type

Error Message %ASA-5-502112: Group policy deleted: name: policy_name Type: policy_type