Threat Hunting on the Enterprise with Winlogbeat, Sysmon, ELK + ATT&CK

David Bernal Michelena | Eduardo Sánchez
SCILabs

#Whoami

SCI LABS
SCITUM CYBER INTELLIGENCE LABORATORIES

- Lead Security Researcher of SCILabs
- 10 years of experience in DFIR
- 9 GIAC Certifications, SANS Mentor for Latin America
- I like playing the piano and exercising in my free time
- @d4v3c0d3r

#Whoami

about.me/epsanchez
@darkslaker

- Head of SCILabs
- Background on Threat Intelligence, DFIR and Penetration Testing
- Professor CyberSec Master LaSalle University
- Founder Member of BSIDES CDMX
- Gamer and wannabe photographer

What this talk is about

Threat hunting on the enterprise using open source/free tools:

- Sysmon
- Winlogbeat
- Elasticsearch

Detection based on attacker tactics and techniques

What is the problem?

Glabal View of
CYBERSECURITY

TOP AMERICAS

*SOURCE: ITU

México

Year	GCI Score	Regional Place	Global Place
2018	0.629	4	63
2017	0.66	3	28
2015	0.324	10	18

2017

País	GCI Score	Legal	Técnico	Org	Capacidad	Cooperación
USA	0.91	1	0.96	0.92	1	0.73
Canada	0.81	0.94	0.93	0.71	0.82	0.70
México	0.66	0.91	0.89	0.48	0.68	0.34

2018

País	GCI Score	Legal	Técnico	Org	Capacidad	Cooperación
USA	0.926	1	0.92	1	0.955	0.755
Canada	0.892	0.975	0.945	1	0.86	0.685
Uruguay	0.681	0.6	0.62	0.93	0.655	0.6

What is the problem?

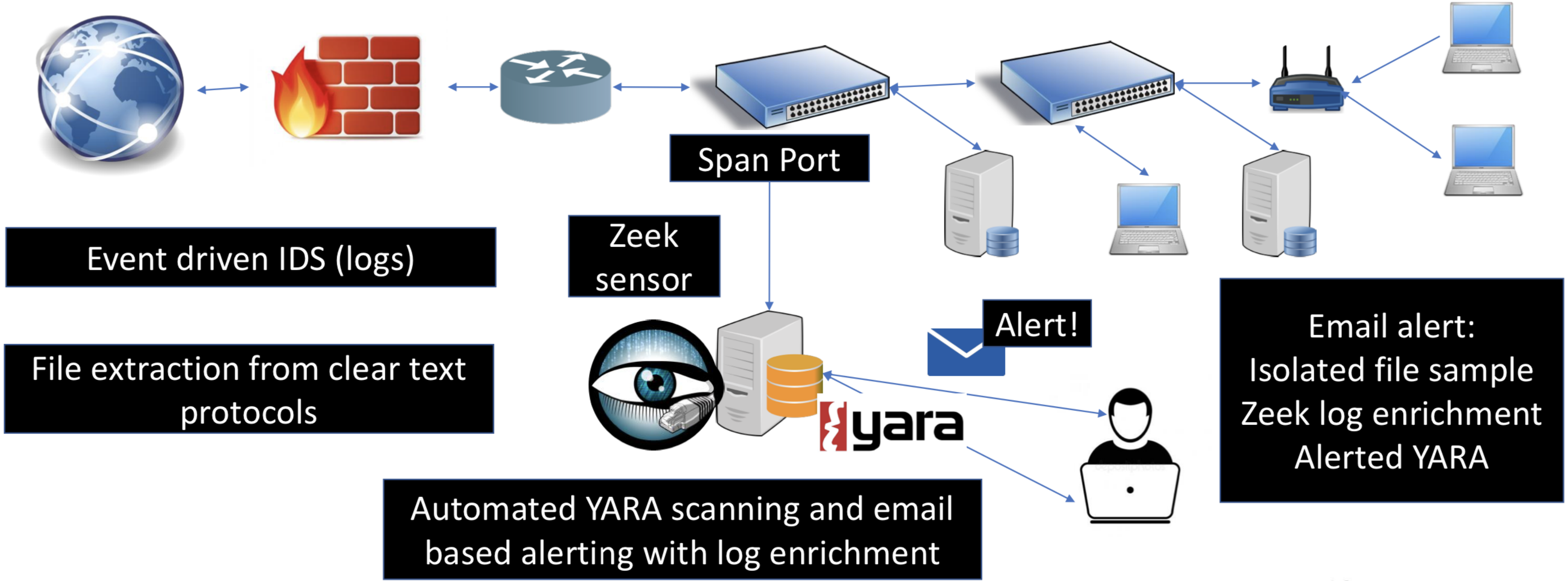
- Lack of Cyber Culture
- Lack of visibility in the organization
- Poor adoption of technologies such as
  - EDR
  - NTA
  - FPC
- High volume of attack, and targeted

.cat.asia

COSMICBANKER

How we face the challenge?

- Visibility on the network
- Visibility on the EndPoint



Span Port

Event driven IDS (logs)

Zeek sensor

File extraction from clear text protocols

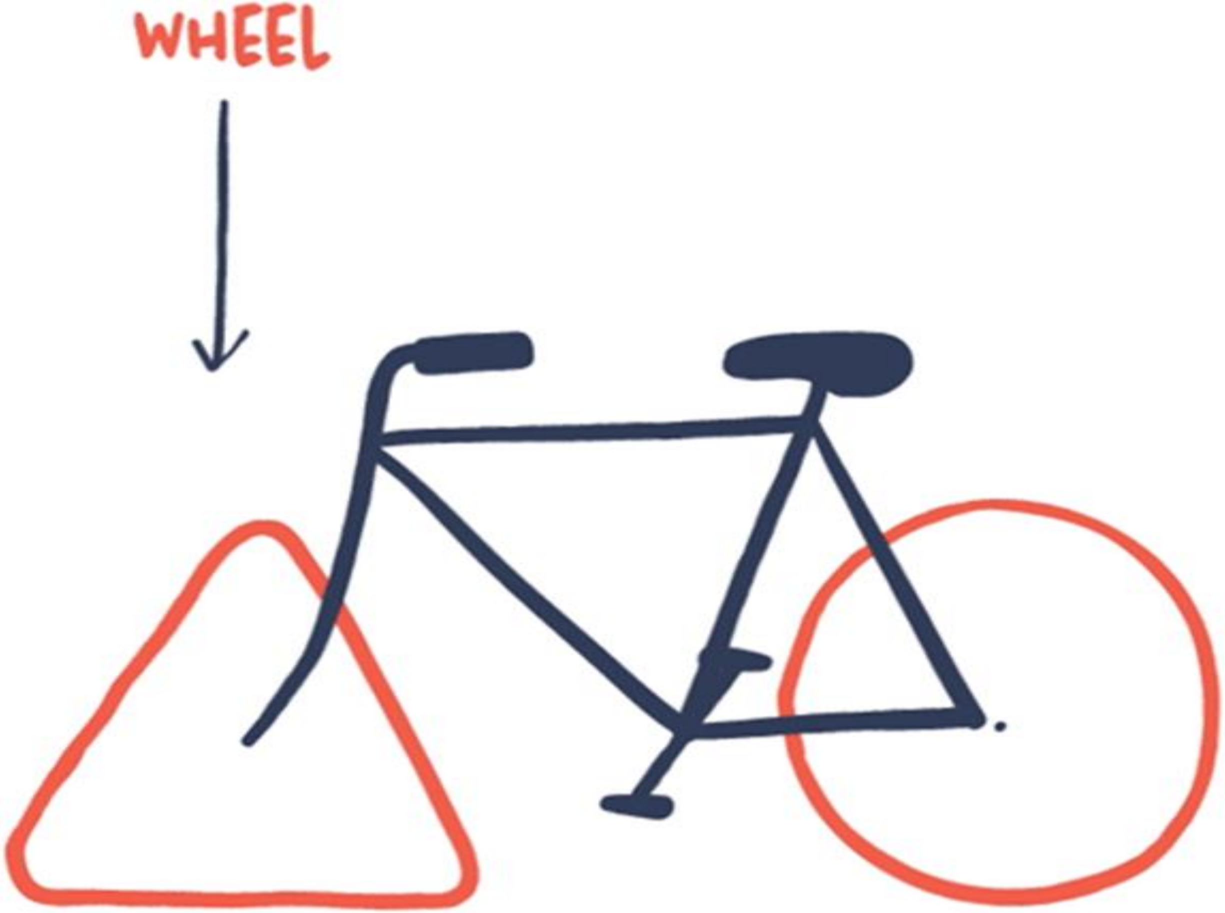
Alert!

Email alert:
Isolated file sample
Zeek log enrichment
Alerted YARA

Automated YARA scanning and email based alerting with log enrichment

https://github.com/SCILabsMX/yaraZeekAlert

The EndPoint

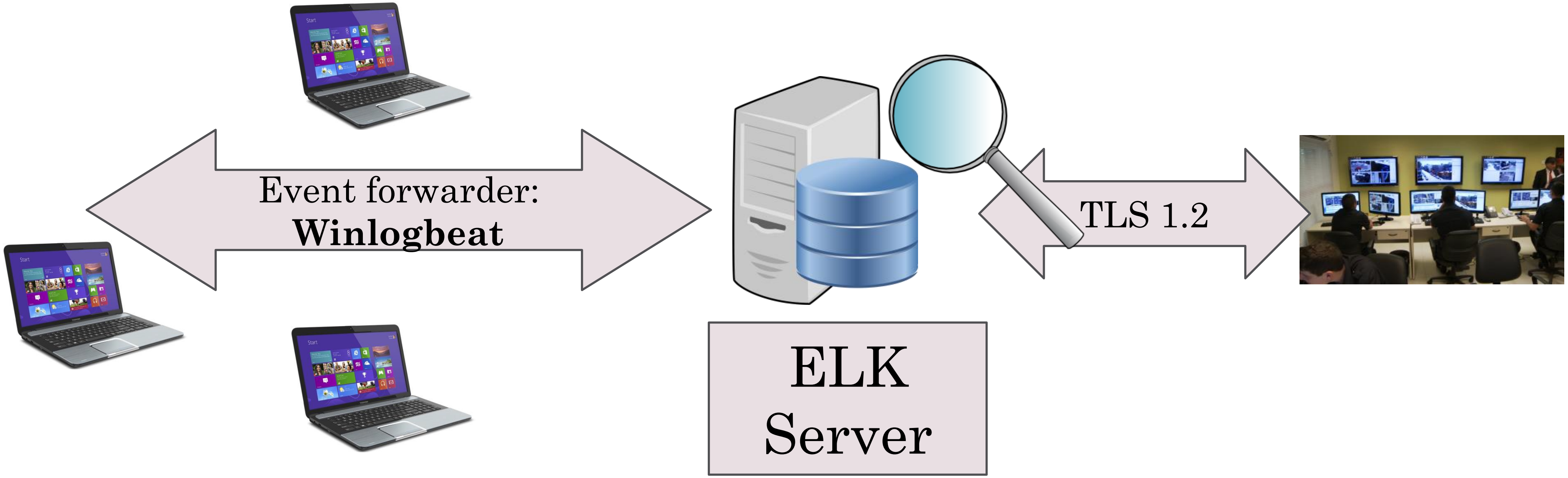


The Journey

ELK + Winlogbeat + Sysmon + ATT&CK™

Credits: Roberto Rodriguez (@Cyb3rWard0g) and Elasticsearch

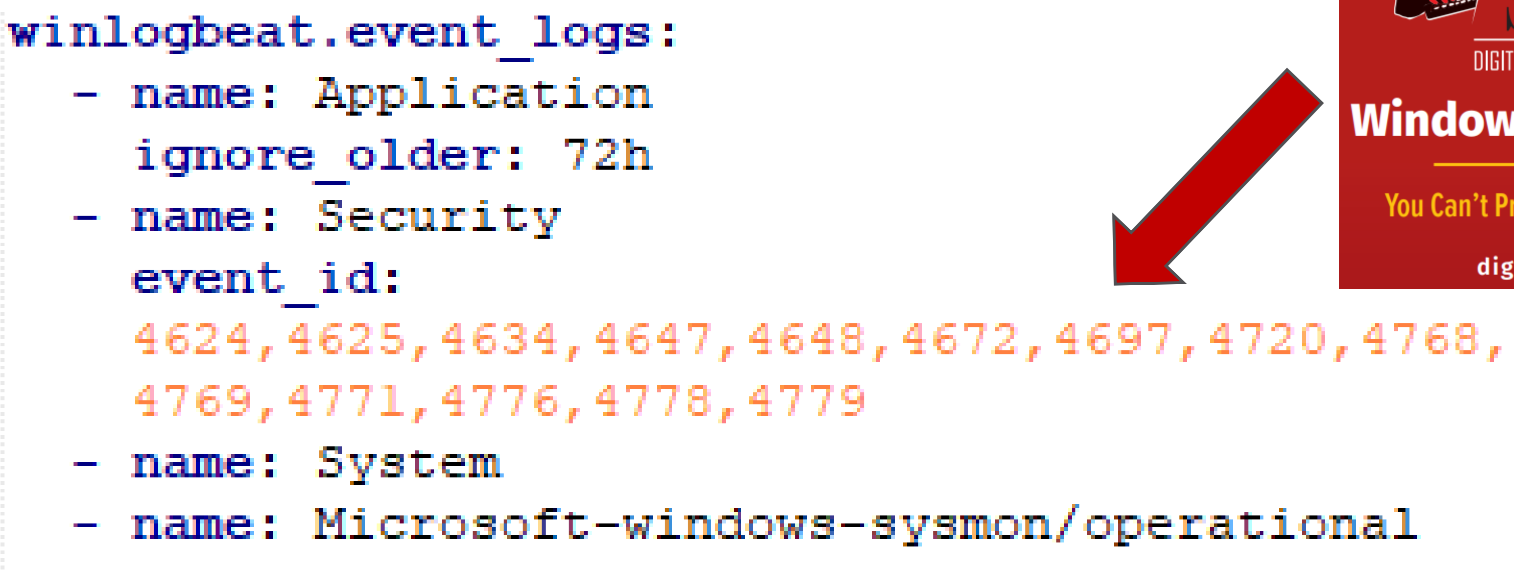
HELK Project https://cyberwardog.blogspot.com/2017/03/building-sysmon-dashboard-with-elk-stack.html



More event logs

Security, System and Application

Security event IDs taken from SANS Evidence Of Poster, “Account Usage” section



```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: Security
    event_id:
    4624,4625,4634,4647,4648,4672,4697,4720,4768,
    4769,4771,4776,4778,4779
  - name: System
  - name: Microsoft-windows-sysmon/operational
```

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
Windows Forensic Analysis
POSTER
You Can’t Protect What You Don’t Know About
digital-forensics.sans.org

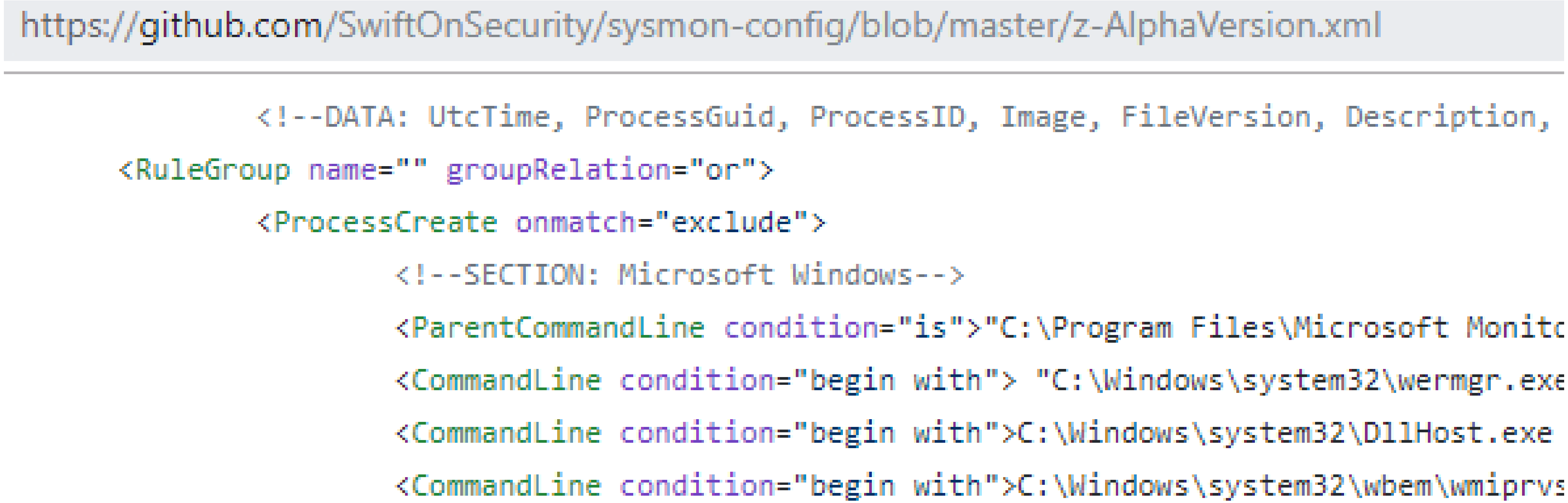
Sysmon fine tuning

- Remove noise, collect useful events through a custom Sysmon configuration file.

- Suggestion: use **SwiftOnSecurity** configuration file as a starting point and enhance it based on your specific environment.

Credits: **@SwiftOnSecurity**

Sysmon **SwiftOnSecurity** configuration file sample



https://github.com/SwiftOnSecurity/sysmon-config/blob/master/z-AlphaVersion.xml

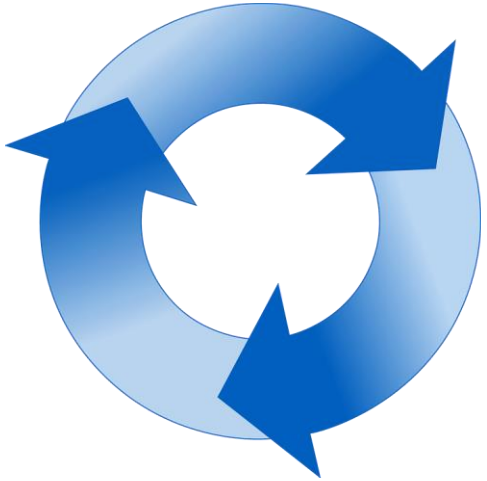
```
                <!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description,
        <RuleGroup name="" groupRelation="or">
                <ProcessCreate onmatch="exclude">
                        <!--SECTION: Microsoft Windows-->
                        <ParentCommandLine condition="is">"C:\Program Files\Microsoft Monitc
                        <CommandLine condition="begin with"> "C:\Windows\system32\wermgr.exe
                        <CommandLine condition="begin with">C:\Windows\system32\DllHost.exe
                        <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvs
```

Credits: **@SwiftOnSecurity**

https://github.com/SwiftOnSecurity/sysmon-config

The Deployment

Sysmon fine tuning before global deployment



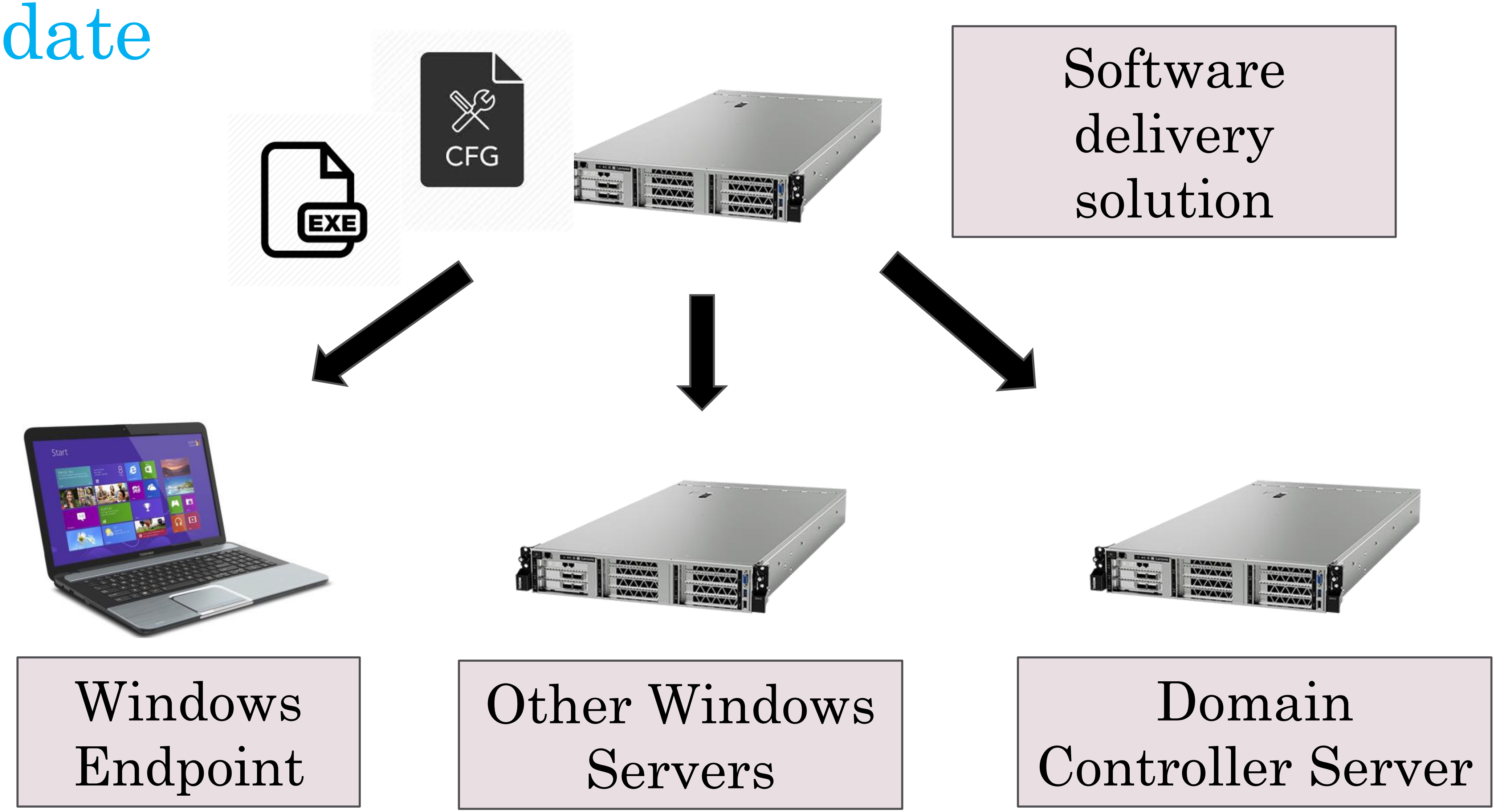
At least one iteration for enhancements
Exclude: antivirus, monitoring agents, etc.

Windows Endpoint

Other Windows Server

Domain Controller Server

Agent and configuration install and update



Software delivery solution

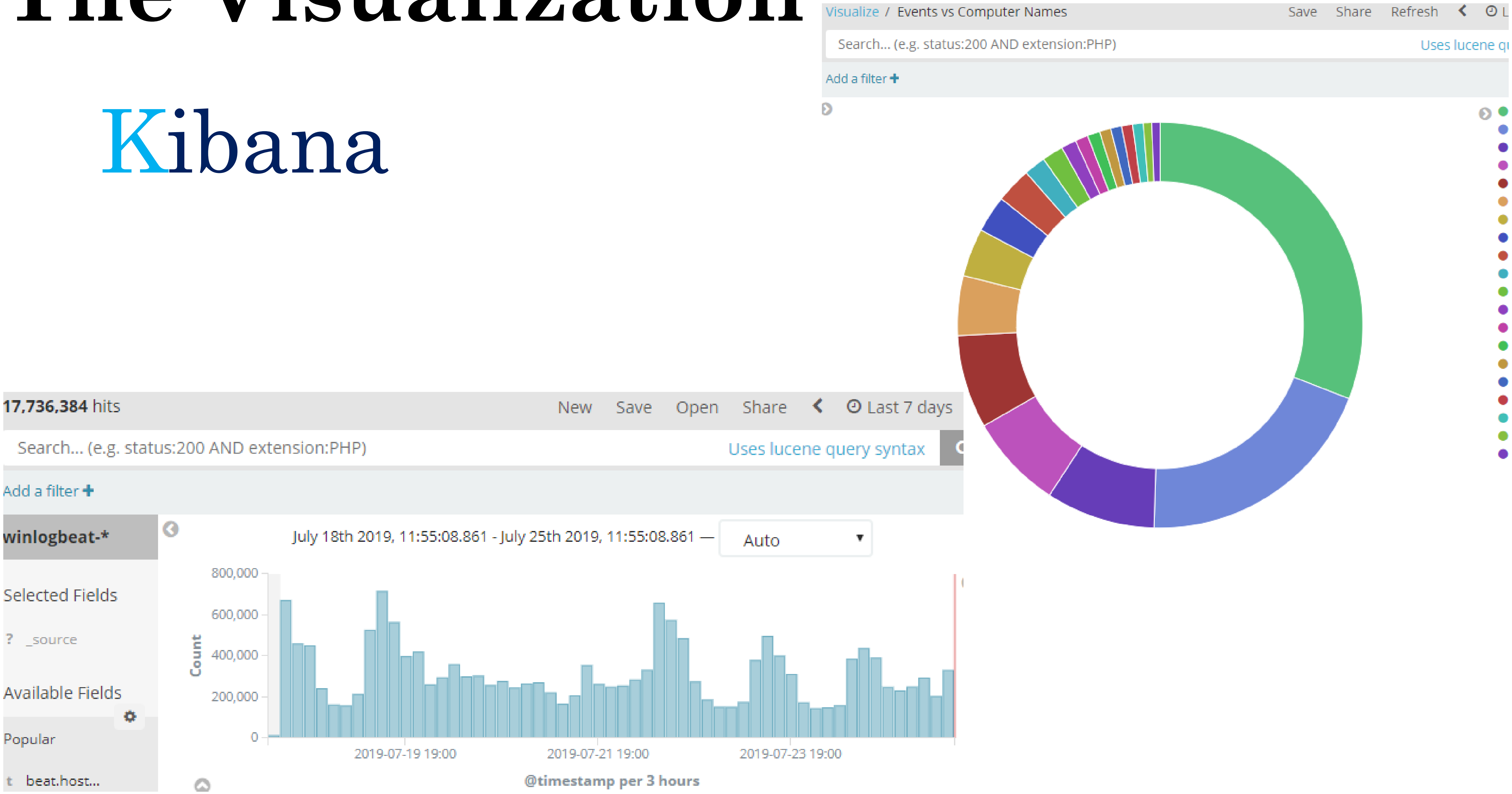
Windows Endpoint

Other Windows Servers

Domain Controller Server

The Visualization

Kibana



Visualize / Events vs Computer Names

Save Share Refresh

Search... (e.g. status:200 AND extension:PHP)

Uses lucene qu

Add a filter +

17,736,384 hits

New Save Open Share Last 7 days

Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax

Add a filter +

winlogbeat-*

Selected Fields

? _source

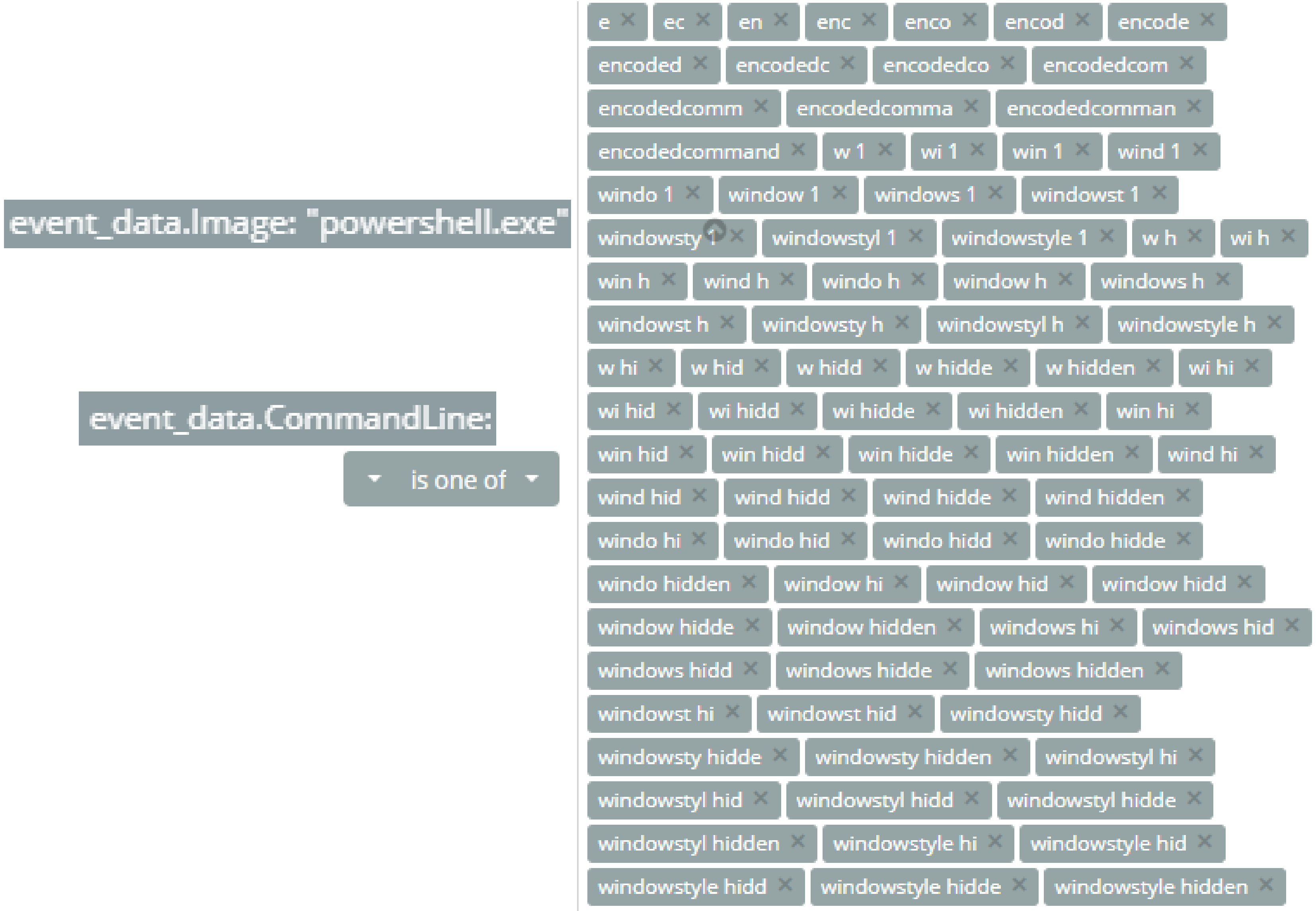
Available Fields

Popular

t beat.host...

July 18th 2019, 11:55:08.861 - July 25th 2019, 11:55:08.861 — Auto

Powershell/fileless attacks T1086



event_data.Image: "powershell.exe"

event_data.CommandLine:

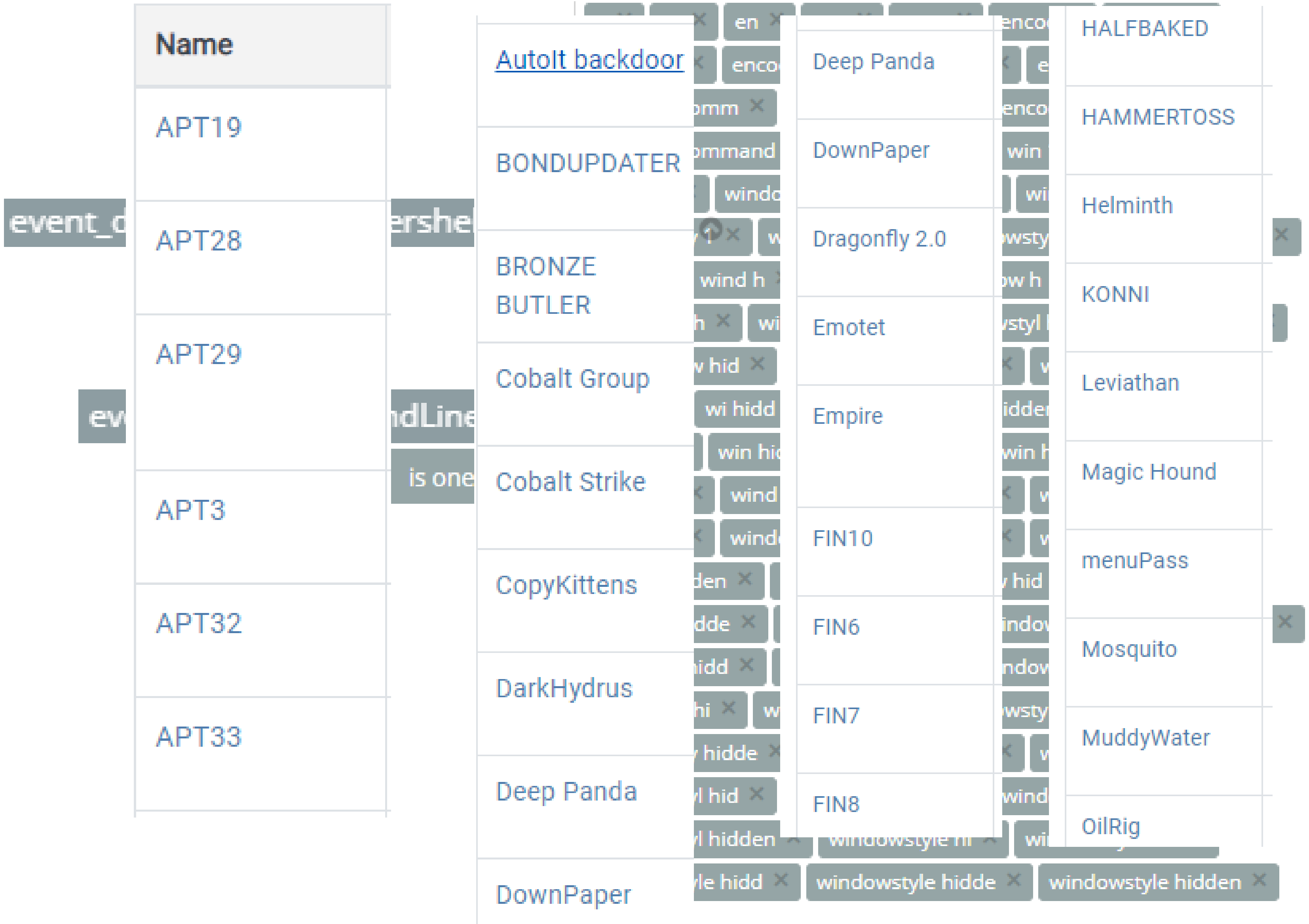
is one of

e × ec × en × enc × enco × encod × encode ×
encoded × encodedc × encodedco × encodedcom ×
encodedcomm × encodedcomma × encodedcomman ×
encodedcommand × w 1 × wi 1 × win 1 × wind 1 ×
windo 1 × window 1 × windows 1 × windowst 1 ×
windowsty 1 × windowstyl 1 × windowstyle 1 × w h × wi h ×
win h × wind h × windo h × window h × windows h ×
windowst h × windowsty h × windowstyl h × windowstyle h ×
w hi × w hid × w hidd × w hidde × w hidden × wi hi ×
wi hid × wi hidd × wi hidde × wi hidden × win hi ×
win hid × win hidd × win hidde × win hidden × wind hi ×
wind hid × wind hidd × wind hidde × wind hidden ×
windo hi × windo hid × windo hidd × windo hidde ×
windo hidden × window hi × window hid × window hidd ×
window hidde × window hidden × windows hi × windows hid ×
windows hidd × windows hidde × windows hidden ×
windowst hi × windowst hid × windowsty hidd ×
windowsty hidde × windowsty hidden × windowstyl hi ×
windowstyl hid × windowstyl hidd × windowstyl hidde ×
windowstyl hidden × windowstyle hi × windowstyle hid ×
windowstyle hidd × windowstyle hidde × windowstyle hidden ×

PowerShell parameter expansion

This targets encoded or hidden PowerShell commands

Powershell/fileless attacks T1086



Name
APT19
APT28
APT29
APT3
APT32
APT33

- AutoIt backdoor
- BONDUPDATER
- BRONZE BUTLER
- Cobalt Group
- Cobalt Strike
- CopyKittens
- DarkHydrus
- Deep Panda
- DownPaper

- Deep Panda
- DownPaper
- Dragonfly 2.0
- Emotet
- Empire
- FIN10
- FIN6
- FIN7
- FIN8

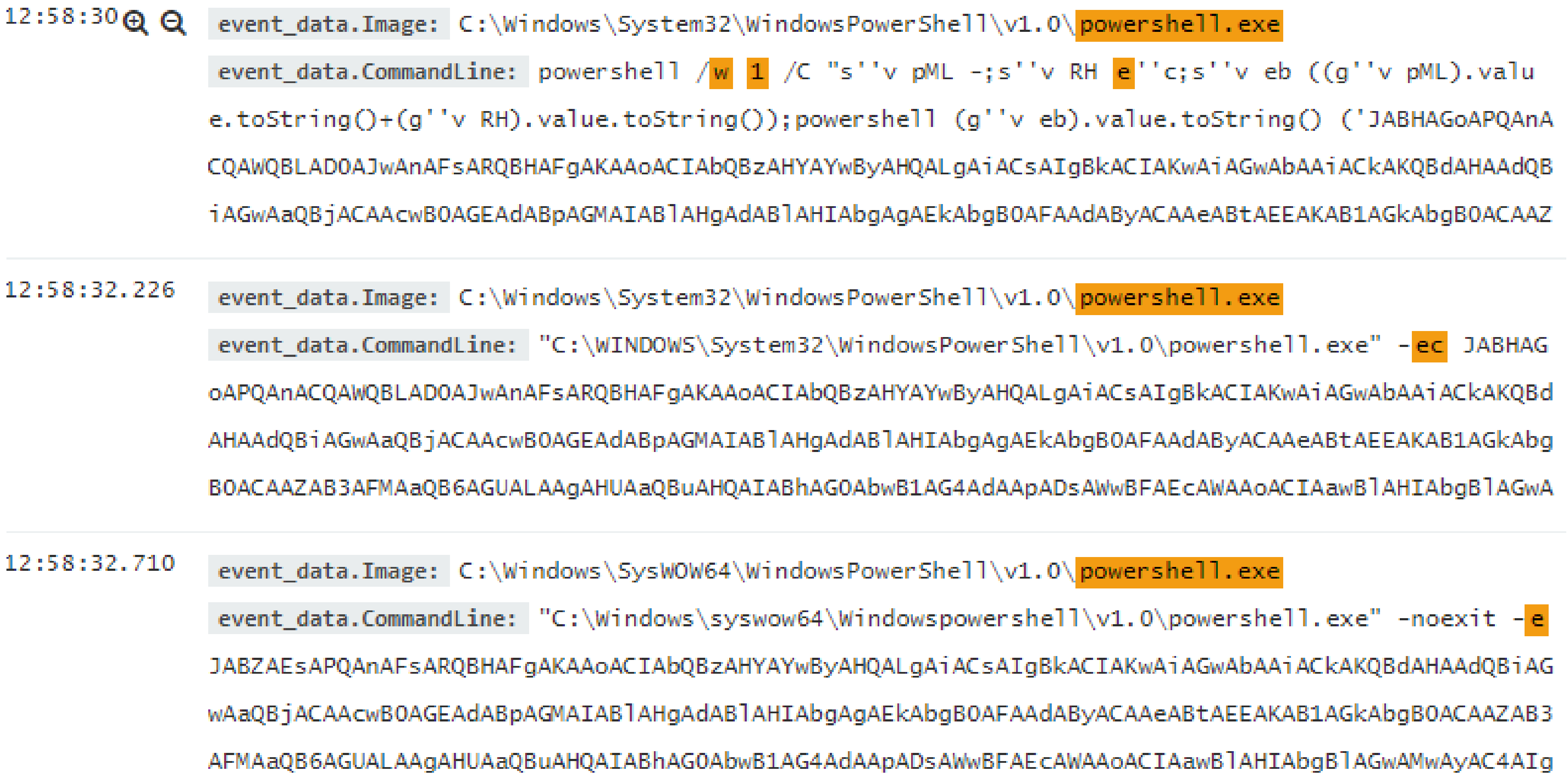
- HALFBAKED
- HAMMERTOSS
- Helminth
- KONNI
- Leviathan
- Magic Hound
- menuPass
- Mosquito
- MuddyWater
- OilRig

Who is using this technique?

The question is who is not using it..

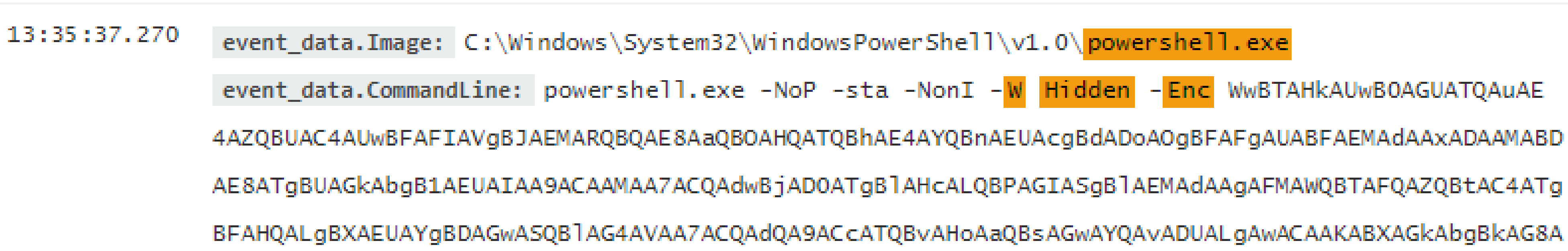
Some Detections

Detecting PowerShell Unicorn



```
12:58:30   event_data.Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
           event_data.CommandLine: powershell /w 1 /C "s''v pML -;s''v RH e''c;s''v eb ((g''v pML).valu
           e.toString()+(g''v RH).value.toString());powershell (g''v eb).value.toString() ('JABHAGoAPQAnA
           CQAWQBLADOAJwAnAFsARQBHAFgAKAAoACIAbQBzAHYAYwByAHQALgAiACsAIgBkACIAKwAiAGwAbAAiACkAKQBdAHAAdQB
           iAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAeABtAEEAKAB1AGkAbgB0ACAAZ

12:58:32.226   event_data.Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
               event_data.CommandLine: "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -ec JABHAG
               oAPQAnACQAWQBLADOAJwAnAFsARQBHAFgAKAAoACIAbQBzAHYAYwByAHQALgAiACsAIgBkACIAKwAiAGwAbAAiACkAKQBd
               AHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAeABtAEEAKAB1AGkAbg
               B0ACAAZAB3AFMAaQB6AGUALAAgAHUAaQBuAHQAIABhAG0AbwB1AG4AdAApADsAWwBFAEcAWAAoACIAawBlAHIAbgBlAGwA

12:58:32.710   event_data.Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
               event_data.CommandLine: "C:\Windows\syswow64\Windowspowershell\v1.0\powershell.exe" -noexit -e
               JABZAEsAPQAnAFsARQBHAFgAKAAoACIAbQBzAHYAYwByAHQALgAiACsAIgBkACIAKwAiAGwAbAAiACkAKQBdAHAAdQBiAG
               wAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAeABtAEEAKAB1AGkAbgB0ACAAZAB3
               AFMAaQB6AGUALAAgAHUAaQBuAHQAIABhAG0AbwB1AG4AdAApADsAWwBFAEcAWAAoACIAawBlAHIAbgBlAGwAMwAyAC4AIg
```

Detecting PowerShell Empire

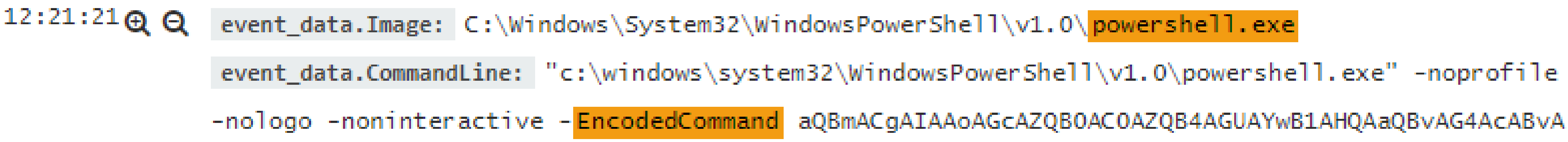


```
13:35:37.270   event_data.Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
               event_data.CommandLine: powershell.exe -NoP -sta -NonI -W Hidden -Enc WwBTAHkAUwB0AGUATQAuAE
               4AZQBUAC4AUwBFAFIAVgBJAEMARQBQAE8AaQBOAHQATQBhAE4AYQBnAEUAcgBdADoAOgBFAFgAUABFAEMAdAAxADAAMABD
               AE8ATgBUAGkAbgB1AEUAIAA9ACAAMAA7ACQAdwBjAD0ATgBlAHcALQBPAGIASgBlAEMAdAAgAFMAWQBTAFQAZQBtAC4ATg
               BFAHQALgBXAEUAYgBDAGwASQBlAG4AVAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAGkAbgBkAG8A
```

Hidden

Encoded

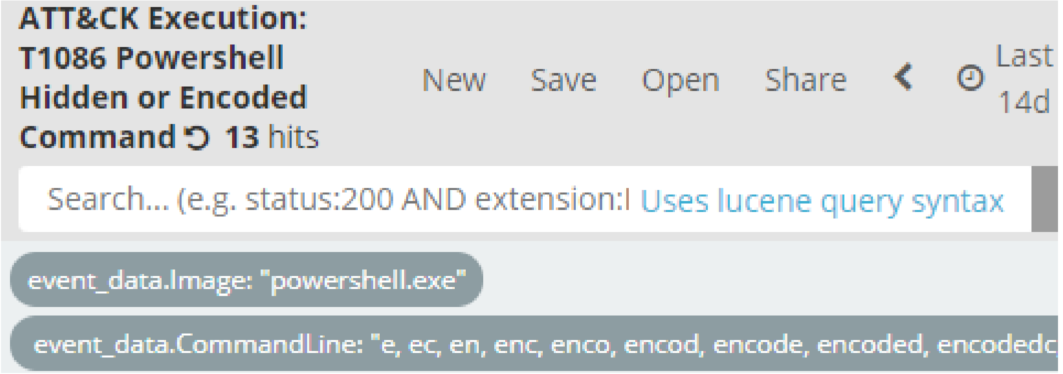
What about false positives?



```
12:21:21  event_data.Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
          event_data.CommandLine: "c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe" -noprofile
          -nologo -noninteractive -EncodedCommand aQBmACgAIAAoAGcAZQB0AC0AZQB4AGUAYwB1AHQAaQBvAG4AcABvA
```

There could be few false positives

Last 14 days, only 9 false positives out of 12,878 PowerShell executions, 3 PowerShell Unicorn, 1 PowerShell Empire

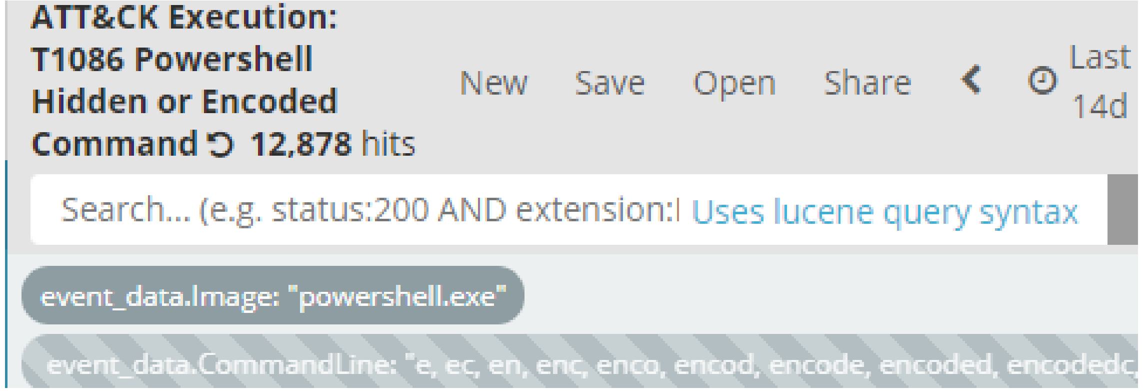


ATT&CK Execution: T1086 Powershell Hidden or Encoded Command ⟲ 13 hits

Search... (e.g. status:200 AND extension:I Uses lucene query syntax

event_data.Image: "powershell.exe"

event_data.CommandLine: "e, ec, en, enc, enco, encod, encode, encoded, encodedc



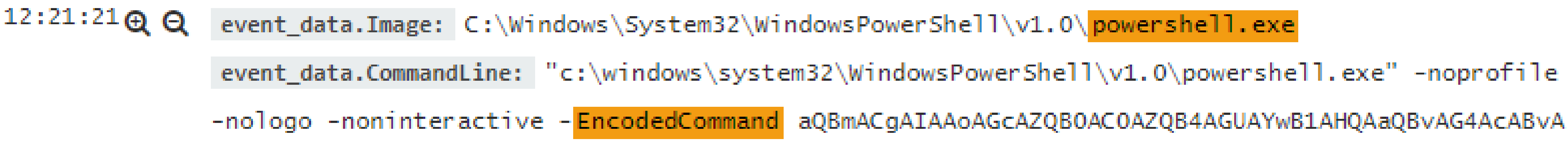
ATT&CK Execution: T1086 Powershell Hidden or Encoded Command ⟲ 12,878 hits

Search... (e.g. status:200 AND extension:I Uses lucene query syntax

event_data.Image: "powershell.exe"

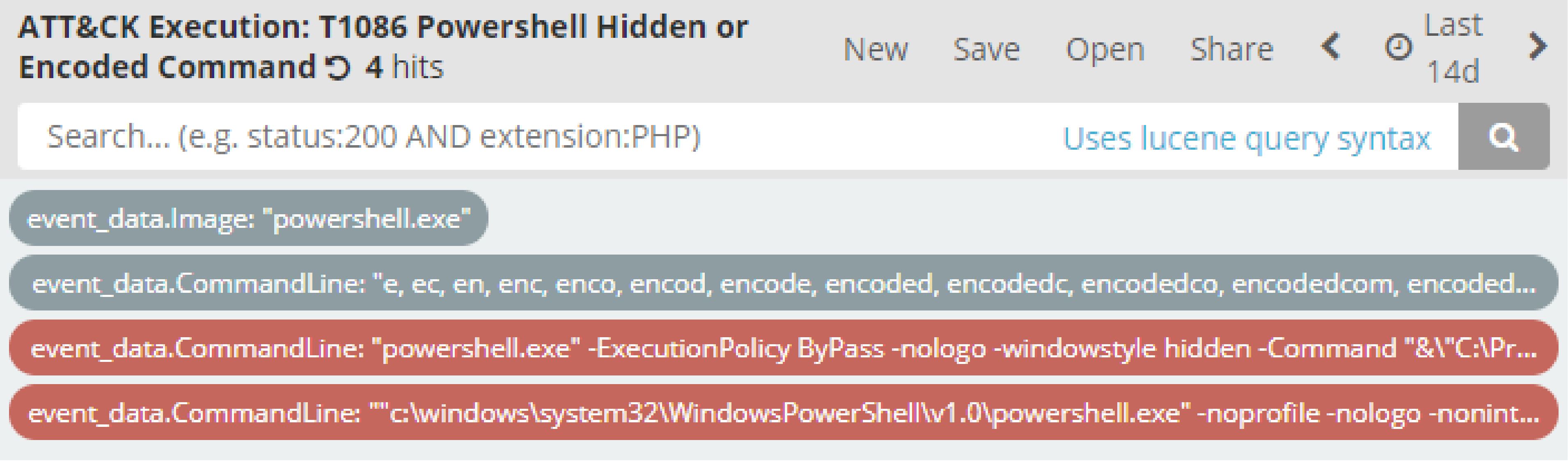
event_data.CommandLine: "e, ec, en, enc, enco, encod, encode, encoded, encodedc

What about false positives?



```
12:21:21  event_data.Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
          event_data.CommandLine: "c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe" -noprofile
          -nologo -noninteractive -EncodedCommand aQBmACgAIAAoAGcAZQB0AC0AZQB4AGUAYwB1AHQAaQBvAG4AcABvA
```

Creating exclusions for known false positives, only true positives now!



ATT&CK Execution: T1086 Powershell Hidden or Encoded Command 4 hits

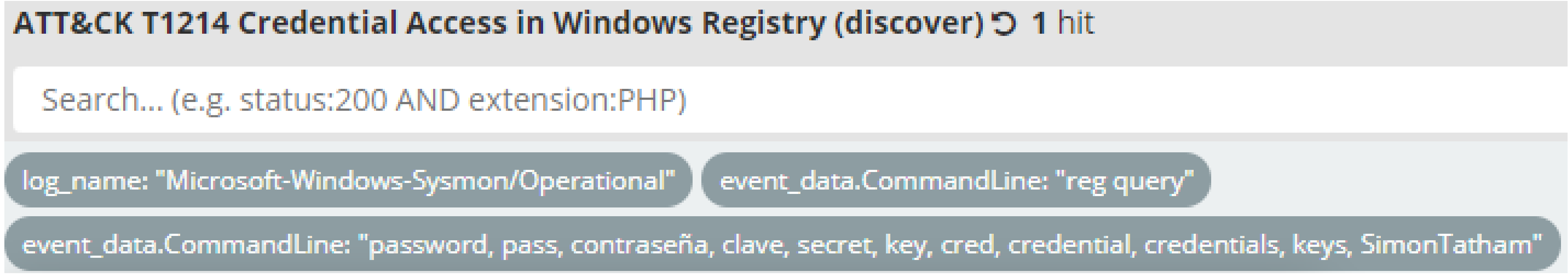
event_data.Image: "powershell.exe"

event_data.CommandLine: "e, ec, en, enc, enco, encod, encode, encoded, encodedc, encodedco, encodedcom, encoded...

event_data.CommandLine: "powershell.exe" -ExecutionPolicy ByPass -nologo -windowstyle hidden -Command "&\"C:\Pr...

event_data.CommandLine: ""c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe" -noprofile -nologo -nonint...

Credential Access in Windows Registry T1214



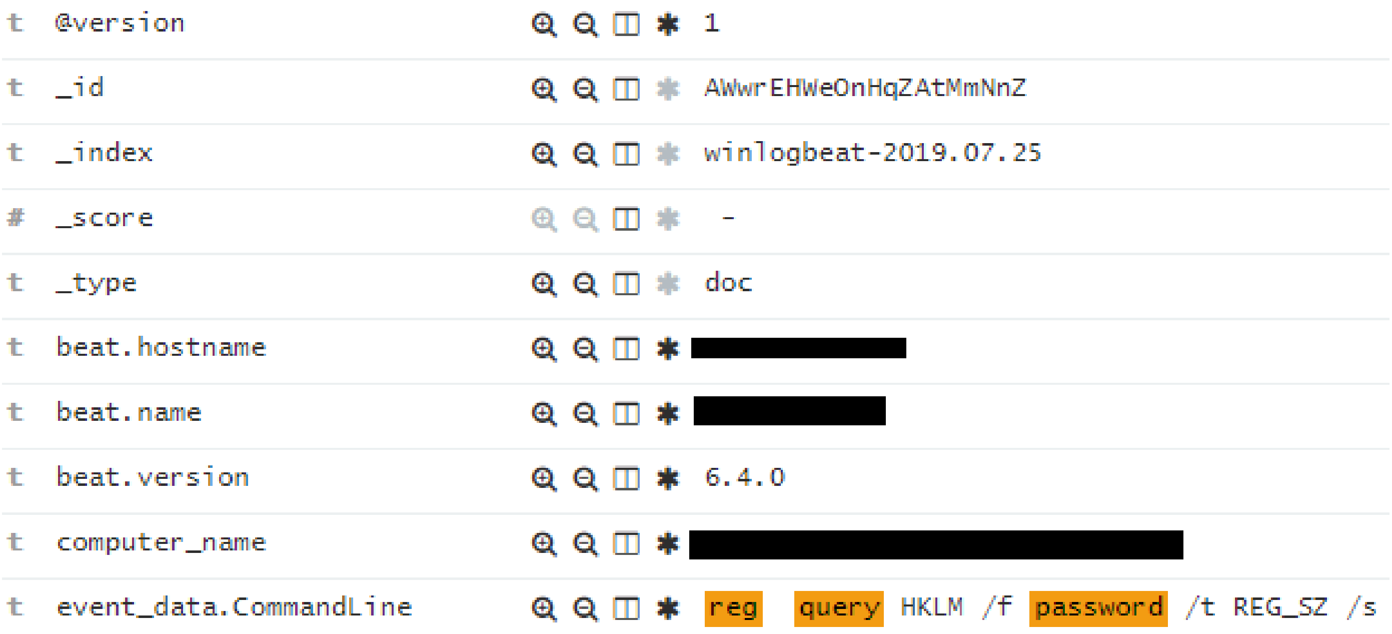
ATT&CK T1214 Credential Access in Windows Registry (discover) ↻ **1** hit

Search... (e.g. status:200 AND extension:PHP)

log_name: "Microsoft-Windows-Sysmon/Operational"

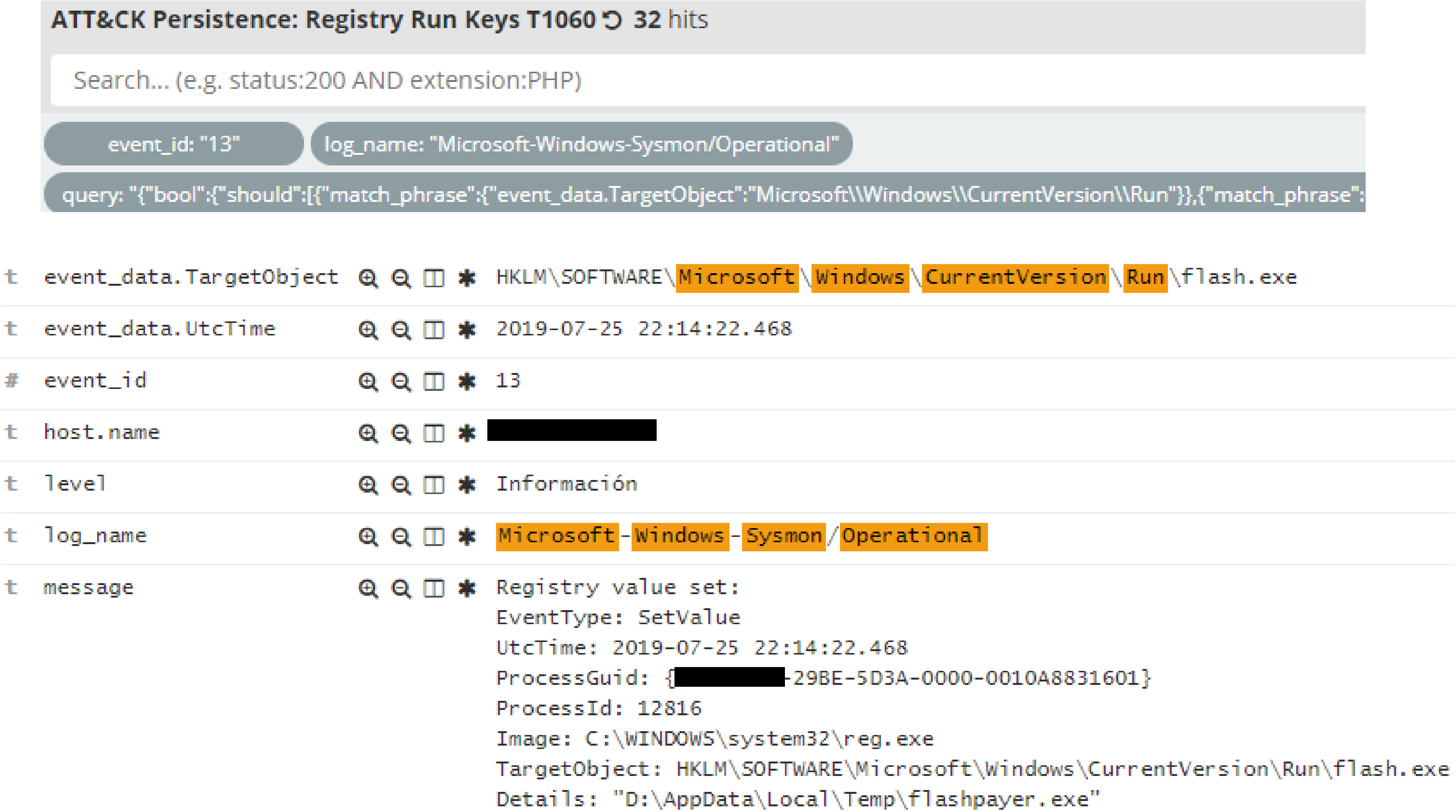
event_data.CommandLine: "reg query"

event_data.CommandLine: "password, pass, contraseña, clave, secret, key, cred, credential, credentials, keys, SimonTatham"



t	@version	1
t	_id	AWwrEHWeOnHqZAtMmNnZ
t	_index	winlogbeat-2019.07.25
#	_score	-
t	_type	doc
t	beat.hostname	[redacted]
t	beat.name	[redacted]
t	beat.version	6.4.0
t	computer_name	[redacted]
t	event_data.CommandLine	reg query HKLM /f password /t REG_SZ /s

Persistence Registry Run Keys T1060



ATT&CK Persistence: Registry Run Keys T1060 ↺ 32 hits

event_id: "13"

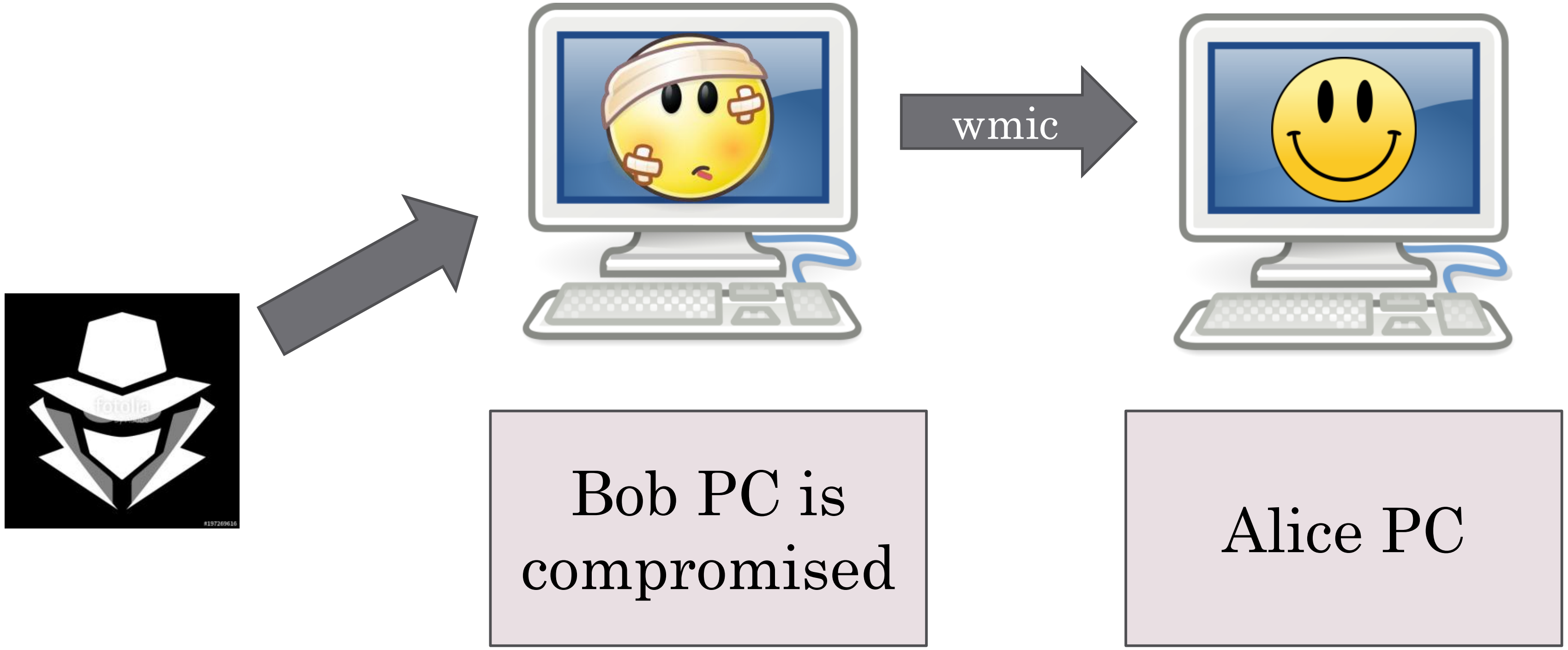
log_name: "Microsoft-Windows-Sysmon/Operational"

query: "{"bool":{"should":[{"match_phrase":{"event_data.TargetObject":"Microsoft\\Windows\\CurrentVersion\\Run"}},{"match_phrase":

t	event_data.TargetObject	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\flash.exe
t	event_data.UtcTime	2019-07-25 22:14:22.468
#	event_id	13
t	host.name	[redacted]
t	level	Información
t	log_name	Microsoft-Windows-Sysmon/Operational
t	message	Registry value set: EventType: SetValue UtcTime: 2019-07-25 22:14:22.468 ProcessGuid: {[redacted]-29BE-5D3A-0000-0010A8831601} ProcessId: 12816 Image: C:\WINDOWS\system32\reg.exe TargetObject: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\flash.exe Details: "D:\AppData\Local\Temp\flashpayer.exe"

Lateral movement and execution

using wmic T1047

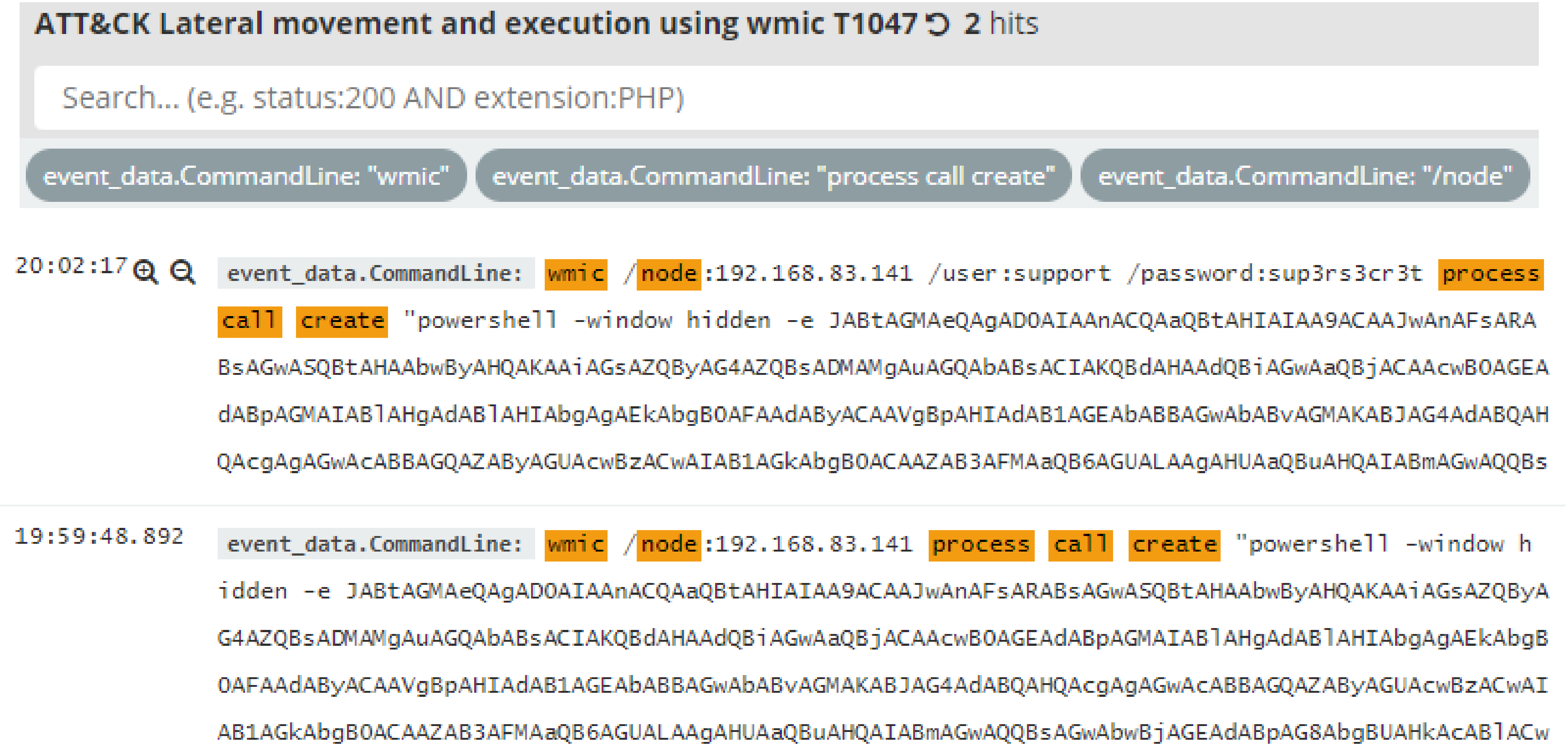


wmic

Bob PC is compromised

Alice PC

Lateral movement and execution using wmic T1047

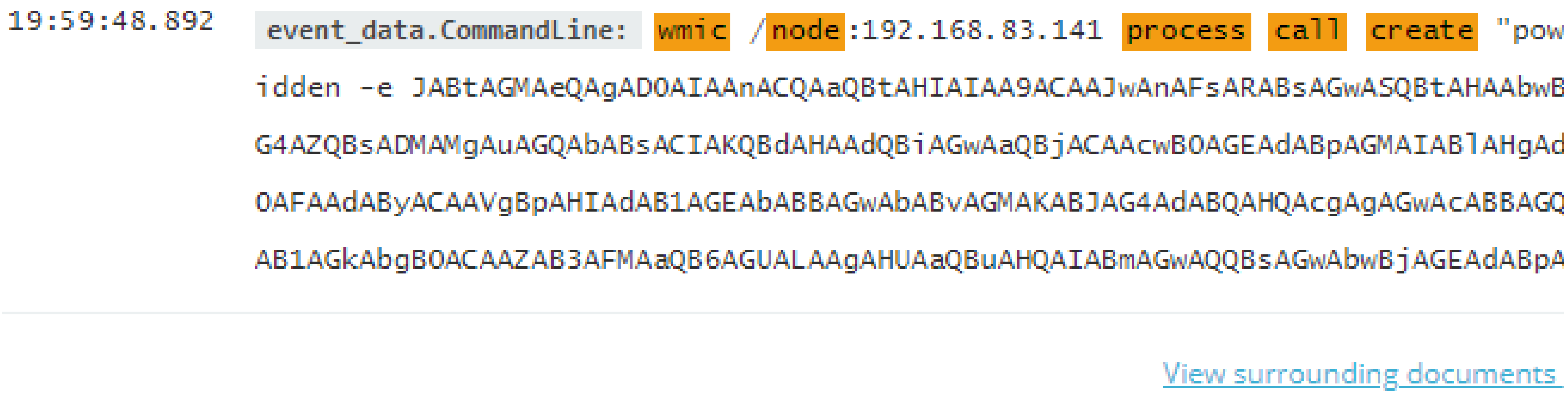


ATT&CK Lateral movement and execution using wmic T1047 ↻ **2** hits

Search... (e.g. status:200 AND extension:PHP)
event_data.CommandLine: "wmic"
event_data.CommandLine: "process call create"
event_data.CommandLine: "/node"

```
20:02:17  event_data.CommandLine: wmic /node:192.168.83.141 /user:support /password:sup3rs3cr3t process
          call create "powershell -window hidden -e JABtAGMAeQAgAD0AIAAnACQAaQBtAHIAIAA9ACAAJwAnAFsARA
          BsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEA
          dABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBpAHIAdAB1AGEAbABBAGwAbABvAGMAKABJAG4AdABQAH
          QAcgAgAGwAcABBAGQAZAByAGUAcwBzACwAIAB1AGkAbgB0ACAAZAB3AFMAaQB6AGUALAAgAHUAaQBuAHQAIABmAGwAQQBs

19:59:48.892  event_data.CommandLine: wmic /node:192.168.83.141 process call create "powershell -window h
          idden -e JABtAGMAeQAgAD0AIAAnACQAaQBtAHIAIAA9ACAAJwAnAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByA
          G4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB
          0AFAAdAByACAAVgBpAHIAdAB1AGEAbABBAGwAbABvAGMAKABJAG4AdABQAHQAcgAgAGwAcABBAGQAZAByAGUAcwBzACwAI
          AB1AGkAbgB0ACAAZAB3AFMAaQB6AGUALAAgAHUAaQBuAHQAIABmAGwAQQBsAGwAbwBjAGEAdABpAG8AbgBUAHkAcABlACw
```

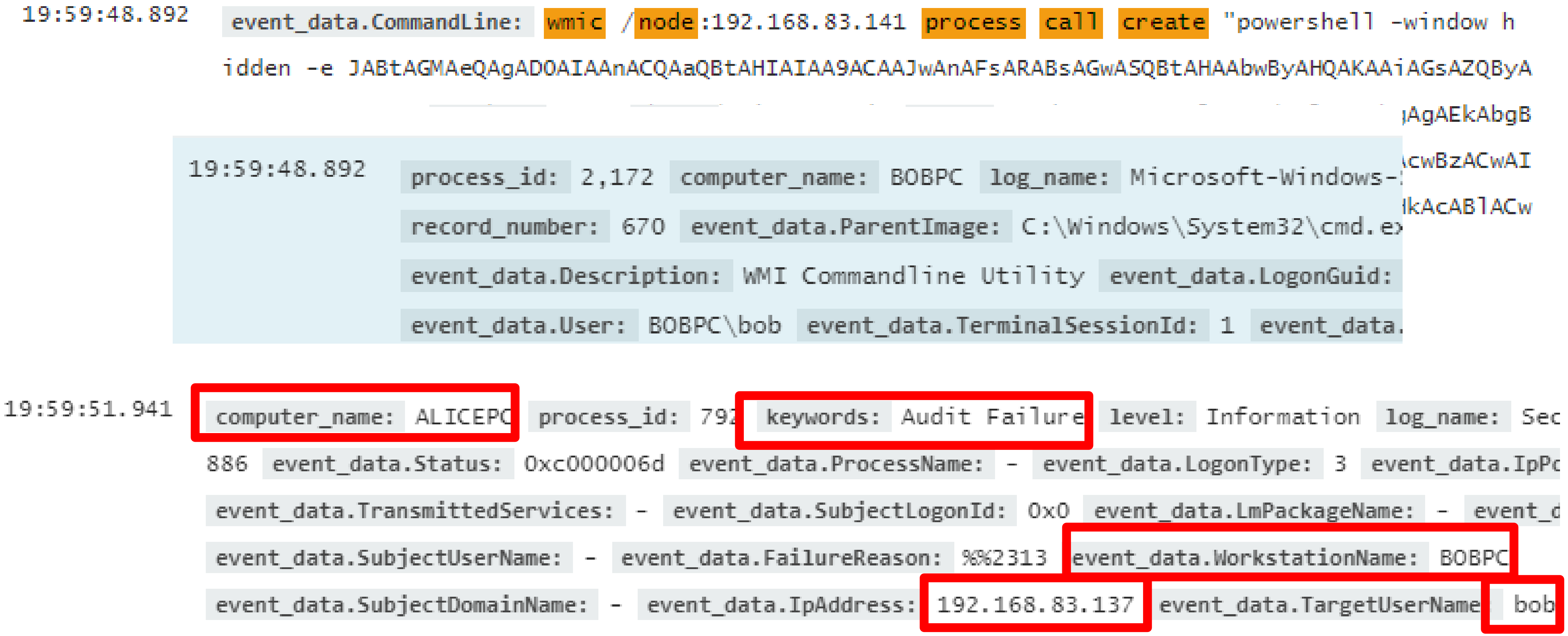
Lateral movement and execution using wmic T1047



```
19:59:48.892    event_data.CommandLine: wmic /node:192.168.83.141 process call create "pow
                idden -e JABtAGMAeQAgAD0AIAAnACQAaQBtAHIAIAA9ACAAJwAnAFsARABsAGwASQBtAHAAbwB
                G4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAd
                0AFAAdAByACAAVgBpAHIAdAB1AGEAbABBAGwAbABvAGMAKABJAG4AdABQAHQAcgAgAGwAcABBAGQ
                AB1AGkAbgB0ACAAZAB3AFMAaQB6AGUALAAgAHUAaQBuAHQAIABmAGwAQQBsAGwAbwBjAGEAdABpA
```

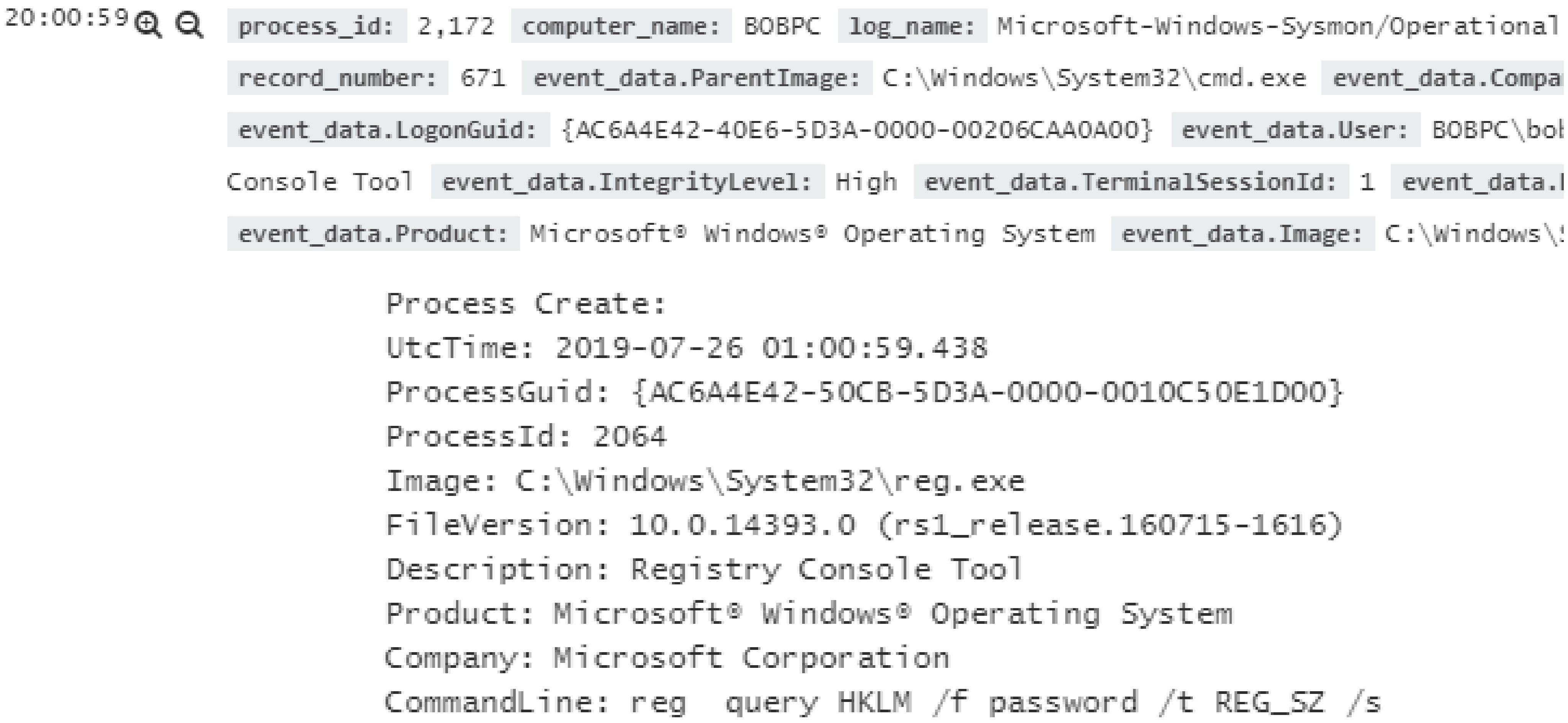
Super useful!

Lateral movement and execution using wmic T1047



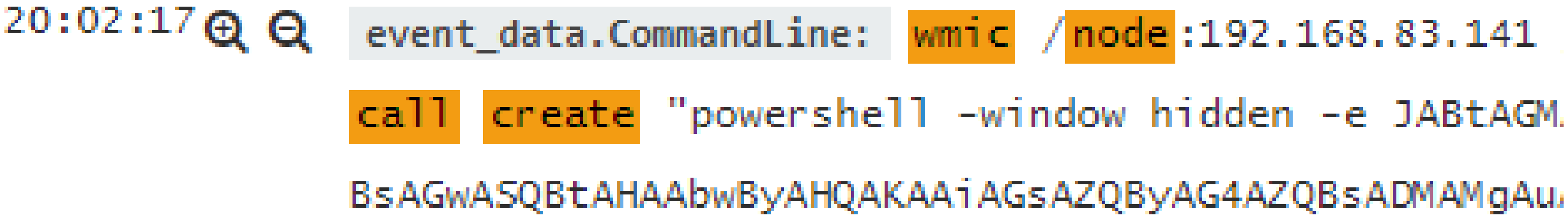
```
19:59:48.892  event_data.CommandLine: wmic /node:192.168.83.141 process call create "powershell -window h
              idden -e JABtAGMAeQAgADOAIAAnACQAaQBtAHIAIAA9ACAAJwAnAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByA
                                                                                                jAgAEkAbgB
     19:59:48.892  process_id: 2,172 computer_name: BOBPC log_name: Microsoft-Windows-    AcwBzACwAI
                   record_number: 670 event_data.ParentImage: C:\Windows\System32\cmd.ex  dkAcABlACw
                   event_data.Description: WMI Commandline Utility event_data.LogonGuid:
                   event_data.User: BOBPC\bob event_data.TerminalSessionId: 1 event_data.

19:59:51.941  computer_name: ALICEPC process_id: 792 keywords: Audit Failure level: Information log_name: Sec
              886 event_data.Status: 0xc000006d event_data.ProcessName: - event_data.LogonType: 3 event_data.IpPo
              event_data.TransmittedServices: - event_data.SubjectLogonId: 0x0 event_data.LmPackageName: - event_d
              event_data.SubjectUserName: - event_data.FailureReason: %%2313 event_data.WorkstationName: BOBPC
              event_data.SubjectDomainName: - event_data.IpAddress: 192.168.83.137 event_data.TargetUserName: bob
```

Lateral movement and execution using wmic T1047

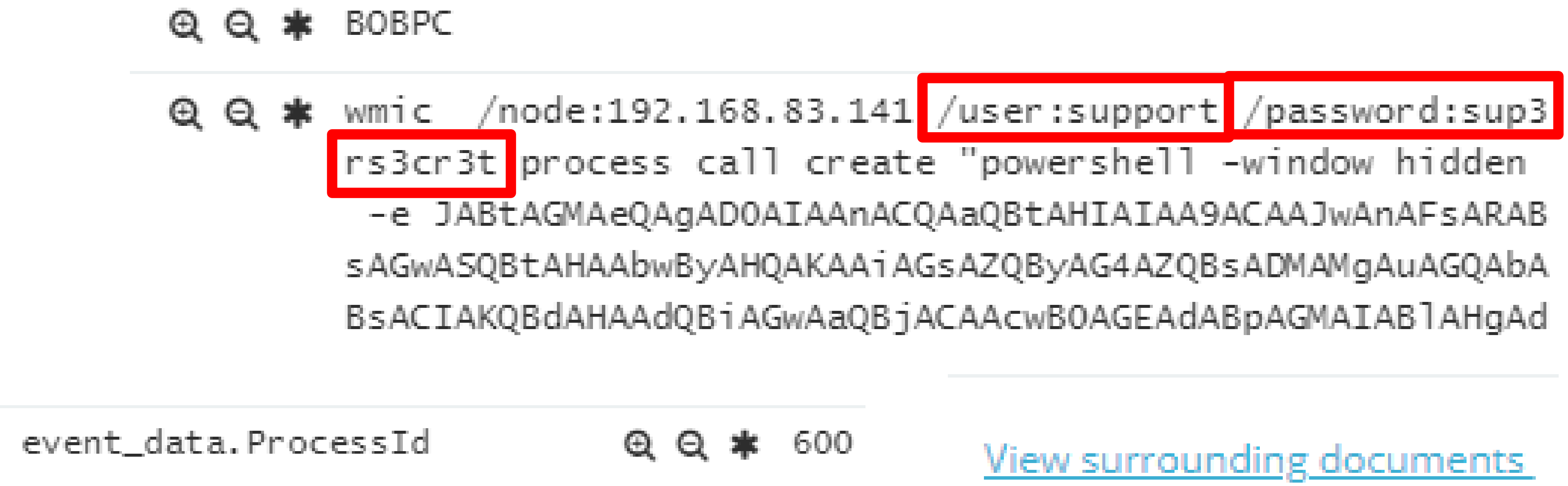


```
20:00:59  process_id: 2,172  computer_name: BOBPC  log_name: Microsoft-Windows-Sysmon/Operational
record_number: 671  event_data.ParentImage: C:\Windows\System32\cmd.exe  event_data.Compa
event_data.LogonGuid: {AC6A4E42-40E6-5D3A-0000-00206CAA0A00}  event_data.User: BOBPC\bo
Console Tool  event_data.IntegrityLevel: High  event_data.TerminalSessionId: 1  event_data.
event_data.Product: Microsoft® Windows® Operating System  event_data.Image: C:\Windows\

        Process Create:
        UtcTime: 2019-07-26 01:00:59.438
        ProcessGuid: {AC6A4E42-50CB-5D3A-0000-0010C50E1D00}
        ProcessId: 2064
        Image: C:\Windows\System32\reg.exe
        FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
        Description: Registry Console Tool
        Product: Microsoft® Windows® Operating System
        Company: Microsoft Corporation
        CommandLine: reg  query HKLM /f password /t REG_SZ /s
```

Lateral movement and execution using wmic T1047

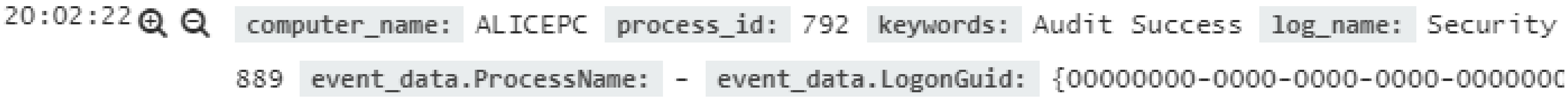


```
20:02:17  event_data.CommandLine: wmic /node:192.168.83.141
          call create "powershell -window hidden -e JABtAGM
          BsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQBsADMAMgAu
```

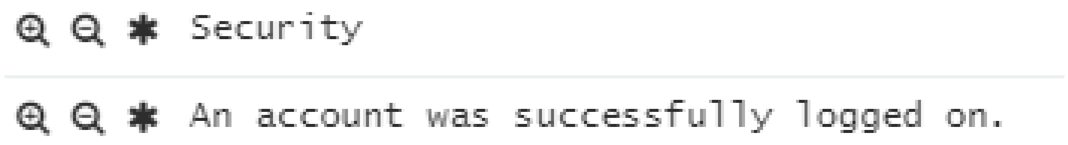


```
BOBPC

wmic /node:192.168.83.141 /user:support /password:sup3
rs3cr3t process call create "powershell -window hidden
 -e JABtAGMAeQAgAD0AIAAnACQAaQBtAHIAIAA9ACAAJwAnAFsARAB
sAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQBsADMAMgAuAGQAbA
BsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAd

event_data.ProcessId          600
```

Lateral movement and execution using wmic T1047

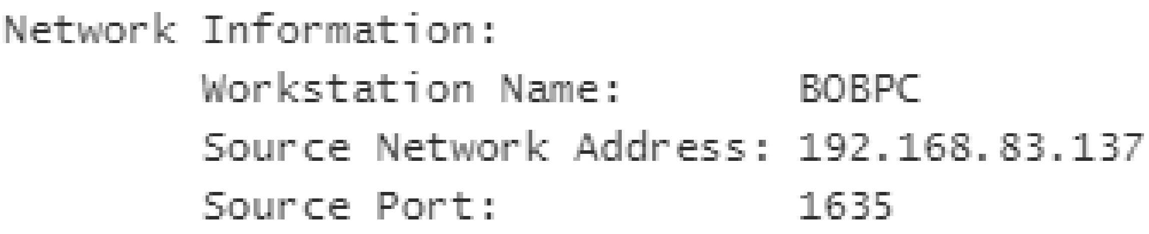


```
20:02:22  computer_name: ALICEPC  process_id: 792  keywords: Audit Success  log_name: Security
          889  event_data.ProcessName: -  event_data.LogonGuid: {00000000-0000-0000-0000-000000C
```

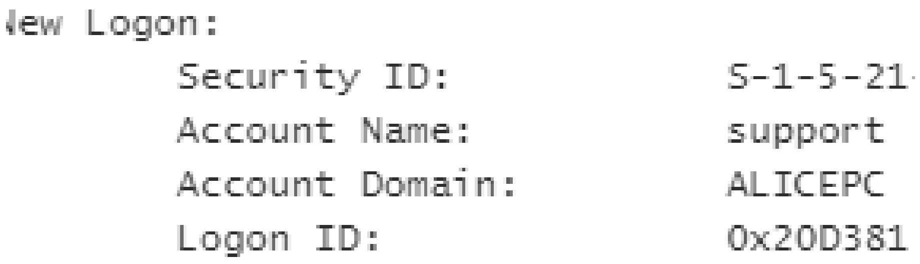


```
Security
An account was successfully logged on.
```

Event ID 4624 confirms successful login

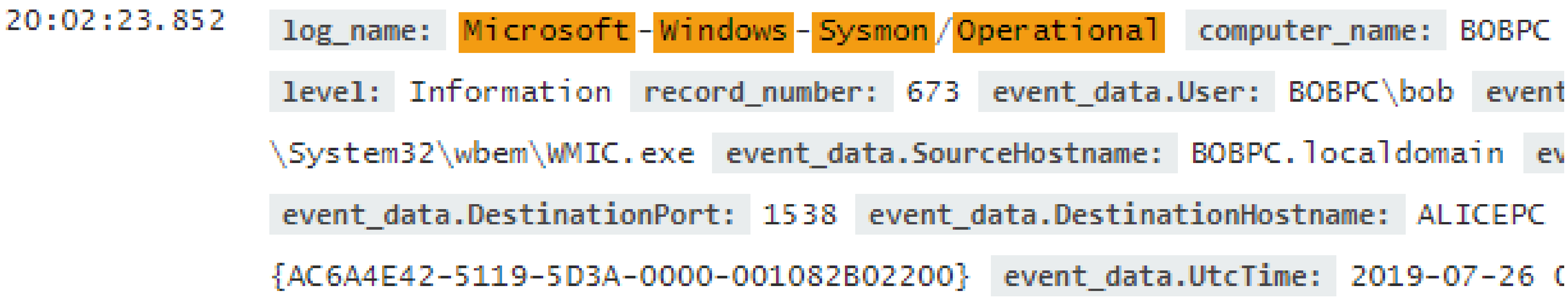


```
Network Information:
        Workstation Name:        BOBPC
        Source Network Address: 192.168.83.137
        Source Port:             1635
```

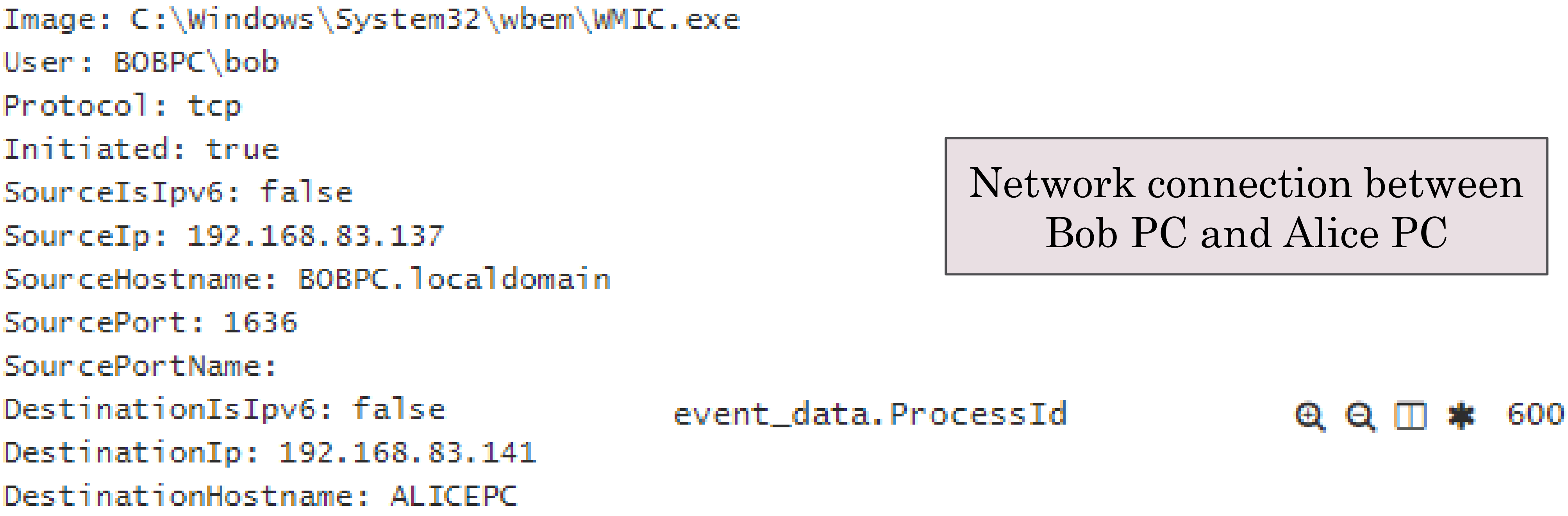


```
lew Logon:
        Security ID:            S-1-5-21
        Account Name:           support
        Account Domain:         ALICEPC
        Logon ID:               0x20D381
```

Lateral movement and execution using wmic T1047



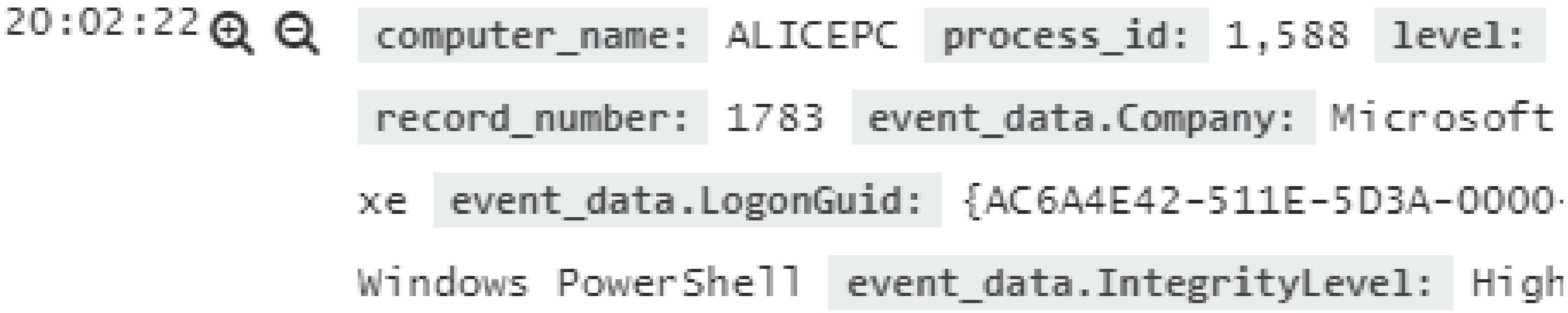
```
20:02:23.852   log_name: Microsoft-Windows-Sysmon/Operational  computer_name: BOBPC
               level: Information  record_number: 673  event_data.User: BOBPC\bob  event
               \System32\wbem\WMIC.exe  event_data.SourceHostname: BOBPC.localdomain  ev
               event_data.DestinationPort: 1538  event_data.DestinationHostname: ALICEPC
               {AC6A4E42-5119-5D3A-0000-001082B02200}  event_data.UtcTime: 2019-07-26 (
```



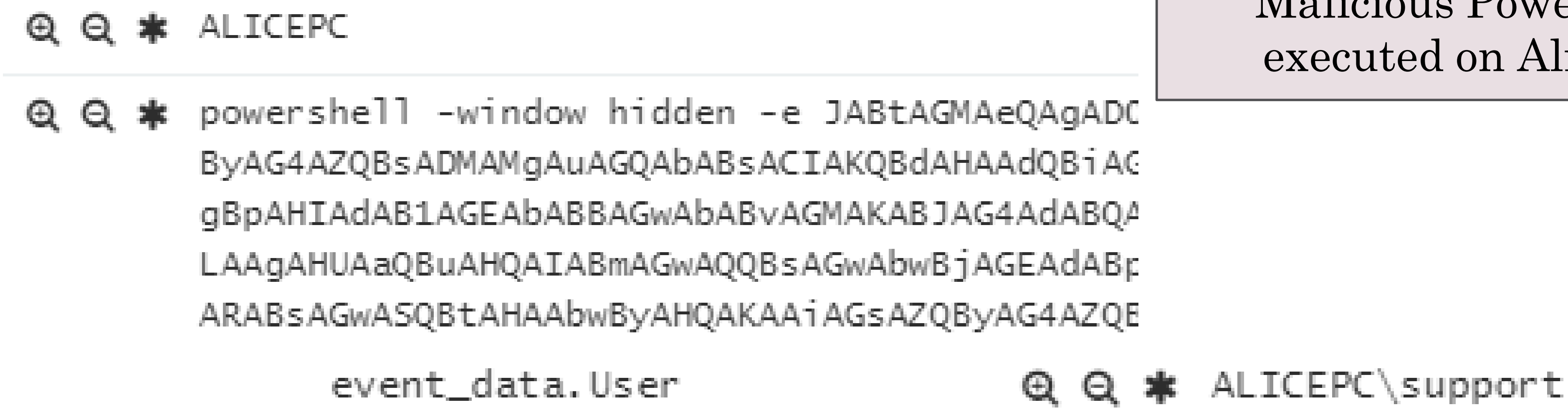
```
Image: C:\Windows\System32\wbem\WMIC.exe
User: BOBPC\bob
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.83.137
SourceHostname: BOBPC.localdomain
SourcePort: 1636
SourcePortName:
DestinationIsIpv6: false                    event_data.ProcessId          600
DestinationIp: 192.168.83.141
DestinationHostname: ALICEPC
```

Network connection between Bob PC and Alice PC

Lateral movement and execution using wmic T1047



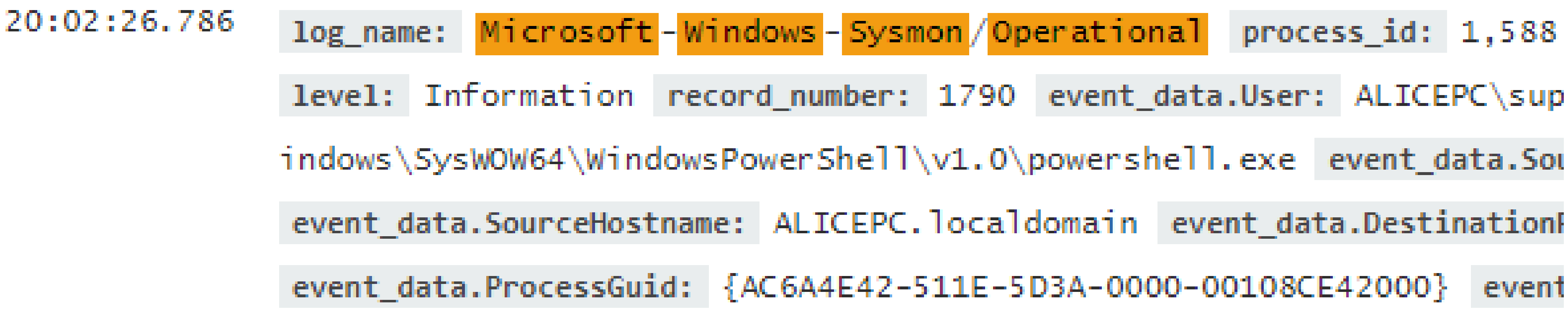
```
20:02:22  computer_name: ALICEPC  process_id: 1,588  level:
          record_number: 1783  event_data.Company: Microsoft
          xe  event_data.LogonGuid: {AC6A4E42-511E-5D3A-0000-
          Windows PowerShell  event_data.IntegrityLevel: High
```



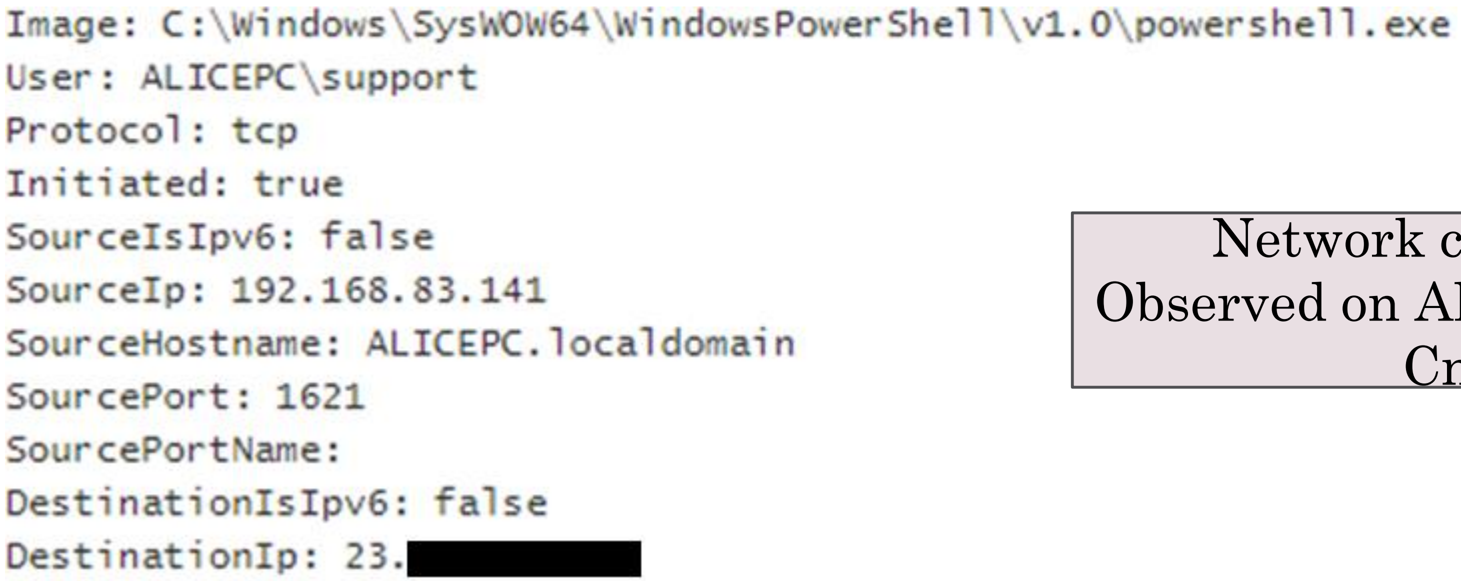
```
ALICEPC

powershell -window hidden -e JABtAGMAeQAgADC
ByAG4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAG
gBpAHIAdAB1AGEAbABBAGwAbABvAGMAKABJAG4AdABQA
LAAgAHUAaQBuAHQAIABmAGwAQQBsAGwAbwBjAGEAdABp
ARABsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQE

event_data.User                ALICEPC\support
```

Malicious PowerShell
executed on Alice PC

Lateral movement and execution using wmic T1047



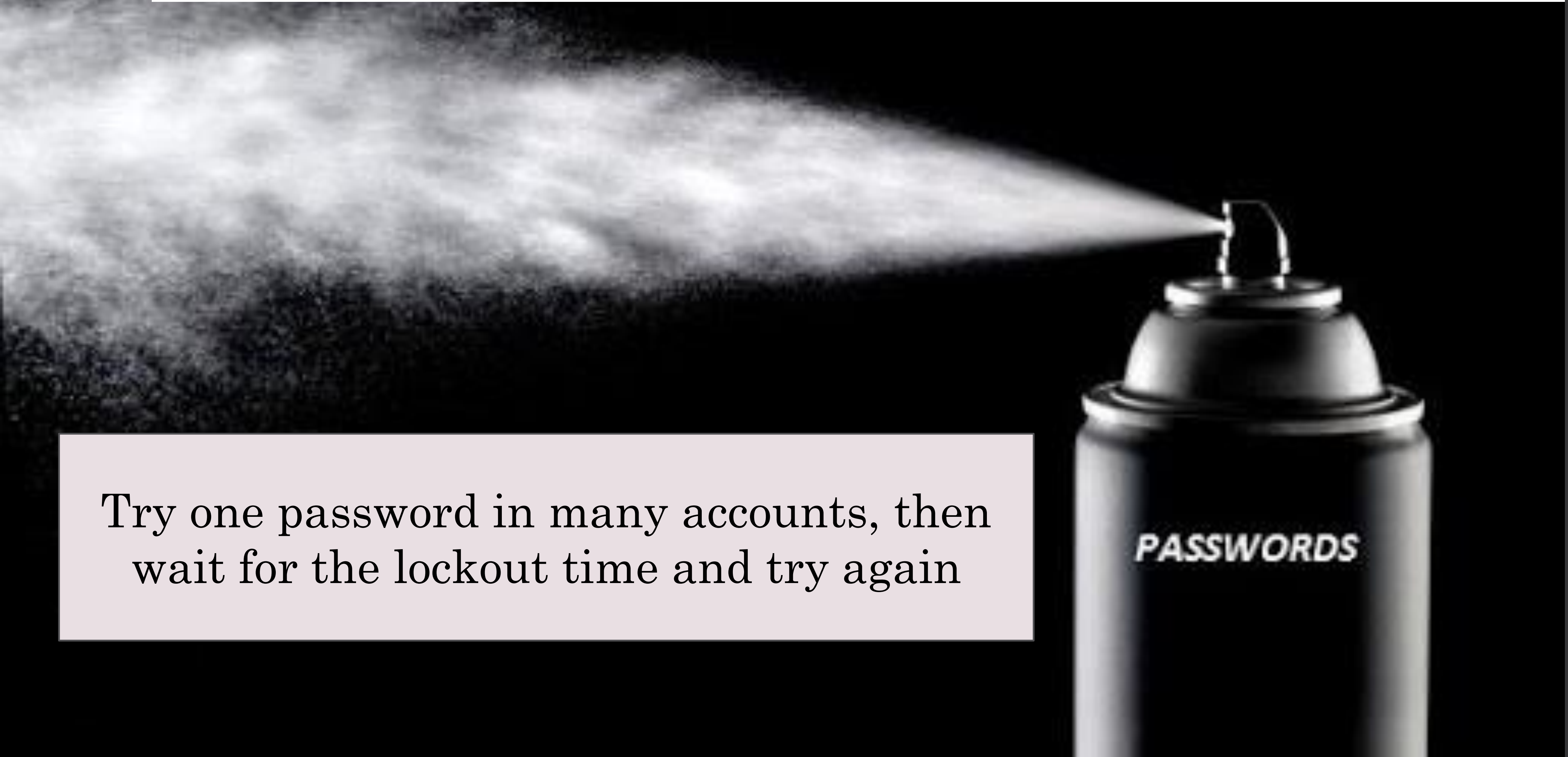
```
20:02:26.786   log_name: Microsoft-Windows-Sysmon/Operational  process_id: 1,588
               level: Information  record_number: 1790  event_data.User: ALICEPC\sup
               indows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe  event_data.Sou
               event_data.SourceHostname: ALICEPC.localdomain  event_data.DestinationH
               event_data.ProcessGuid: {AC6A4E42-511E-5D3A-0000-00108CE42000}  event
```



```
Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
User: ALICEPC\support
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.83.141
SourceHostname: ALICEPC.localdomain
SourcePort: 1621
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 23.[redacted]
```

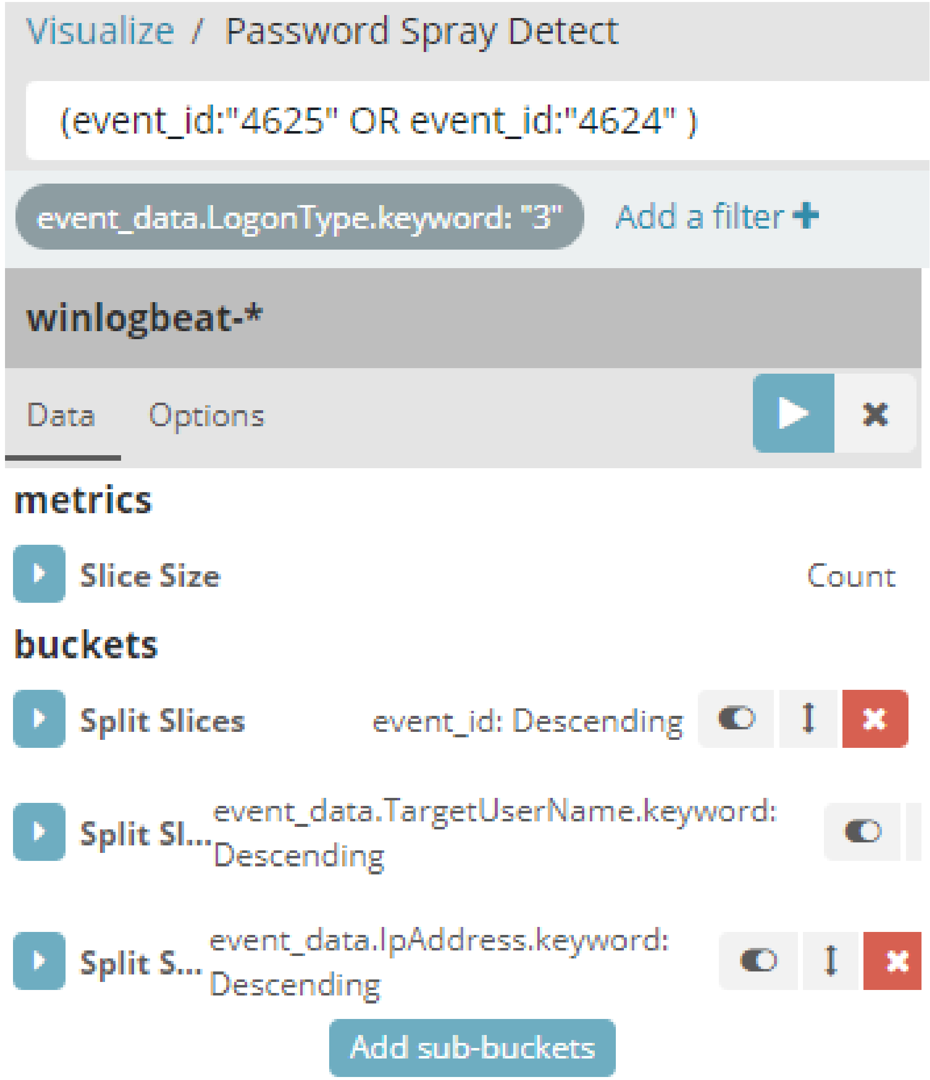
Network connection Observed on Alice to external CnC

T1110 Brute Force -> Password Spraying



Try one password in many accounts, then wait for the lockout time and try again

Password Spraying



Visualize / Password Spray Detect

(event_id:"4625" OR event_id:"4624")

event_data.LogonType.keyword: "3"

winlogbeat-*

metrics

Slice Size: Count

buckets

Split Slices: event_id: Descending

Split Sl...: event_data.TargetUserName.keyword: Descending

Split S...: event_data.IpAddress.keyword: Descending

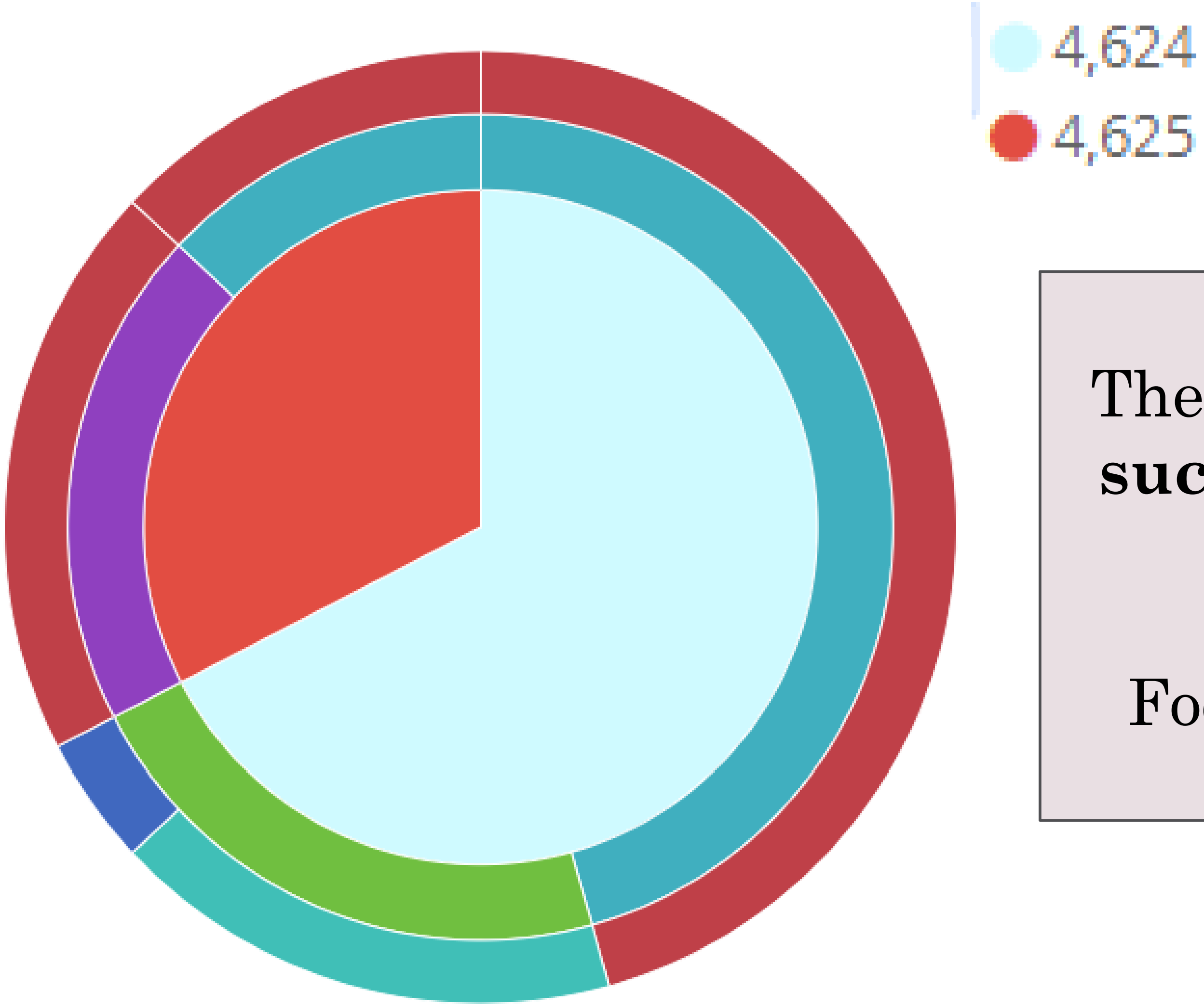
● 4,624

● 4,625

Focus on Network Logon types: 3
Create a Pie visualization with three layers:

- Event ID
- TargetUserName
- Source Network Address

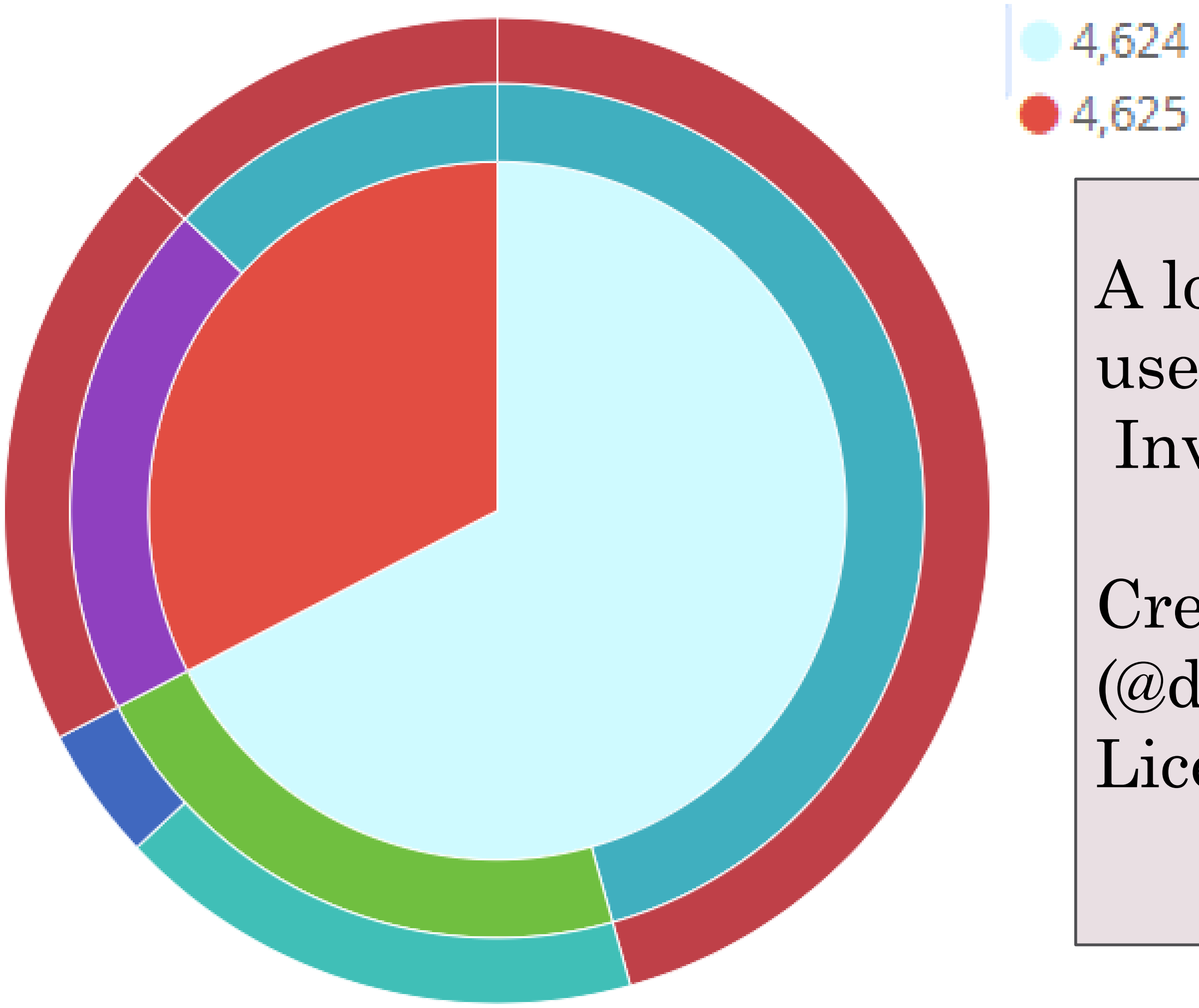
Password Spraying, normal behavior



There should **normally** be more **successful logons (4624)** than **failed logons (4625).**

Focus on the center of the pie.

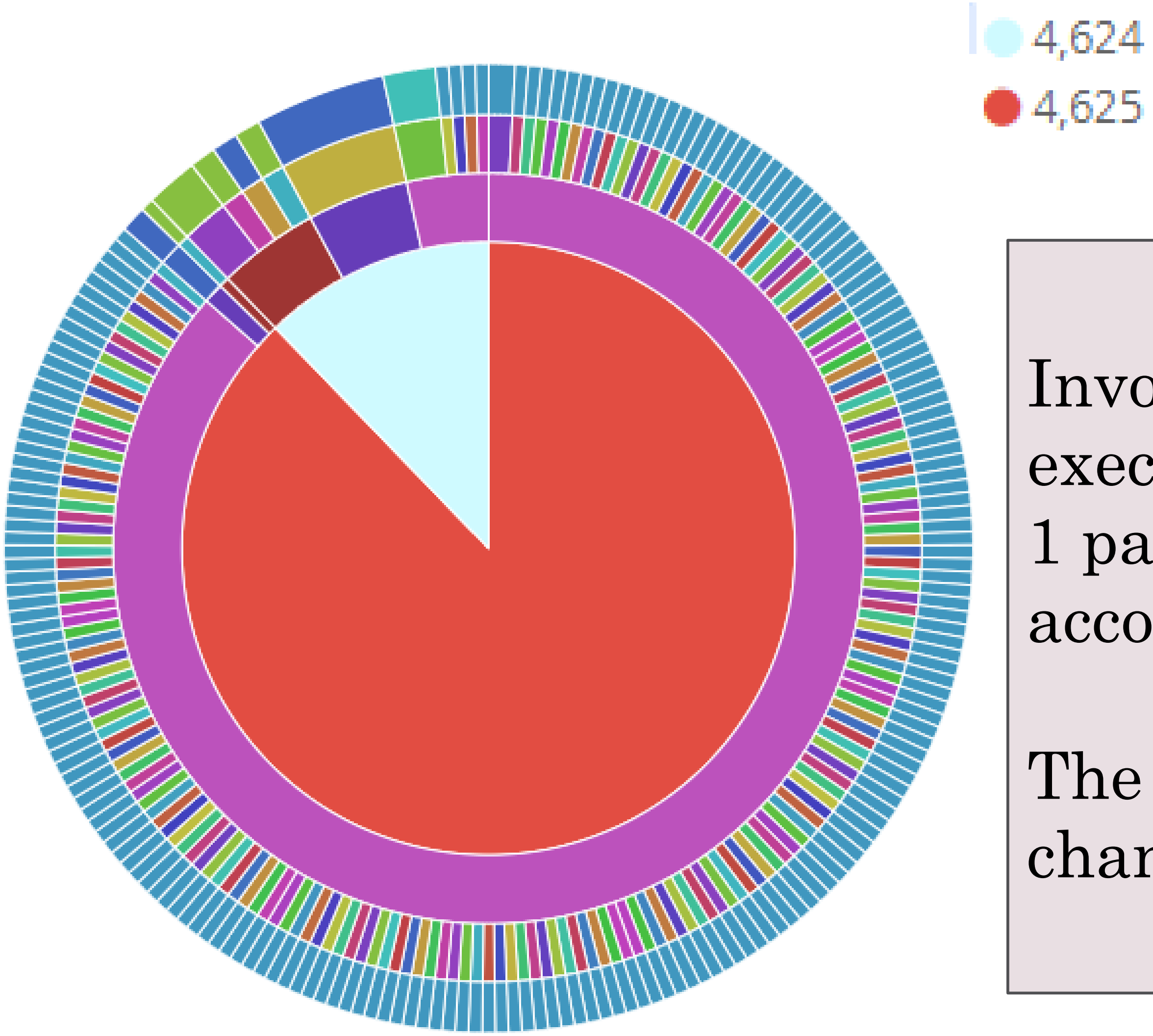
Before Password Spraying



A local password spray attack is used:
 Invoke-LocalPasswordSpray

Credits to author **Beau Bullock** (@dafthack)
License: BSD 3-Clause

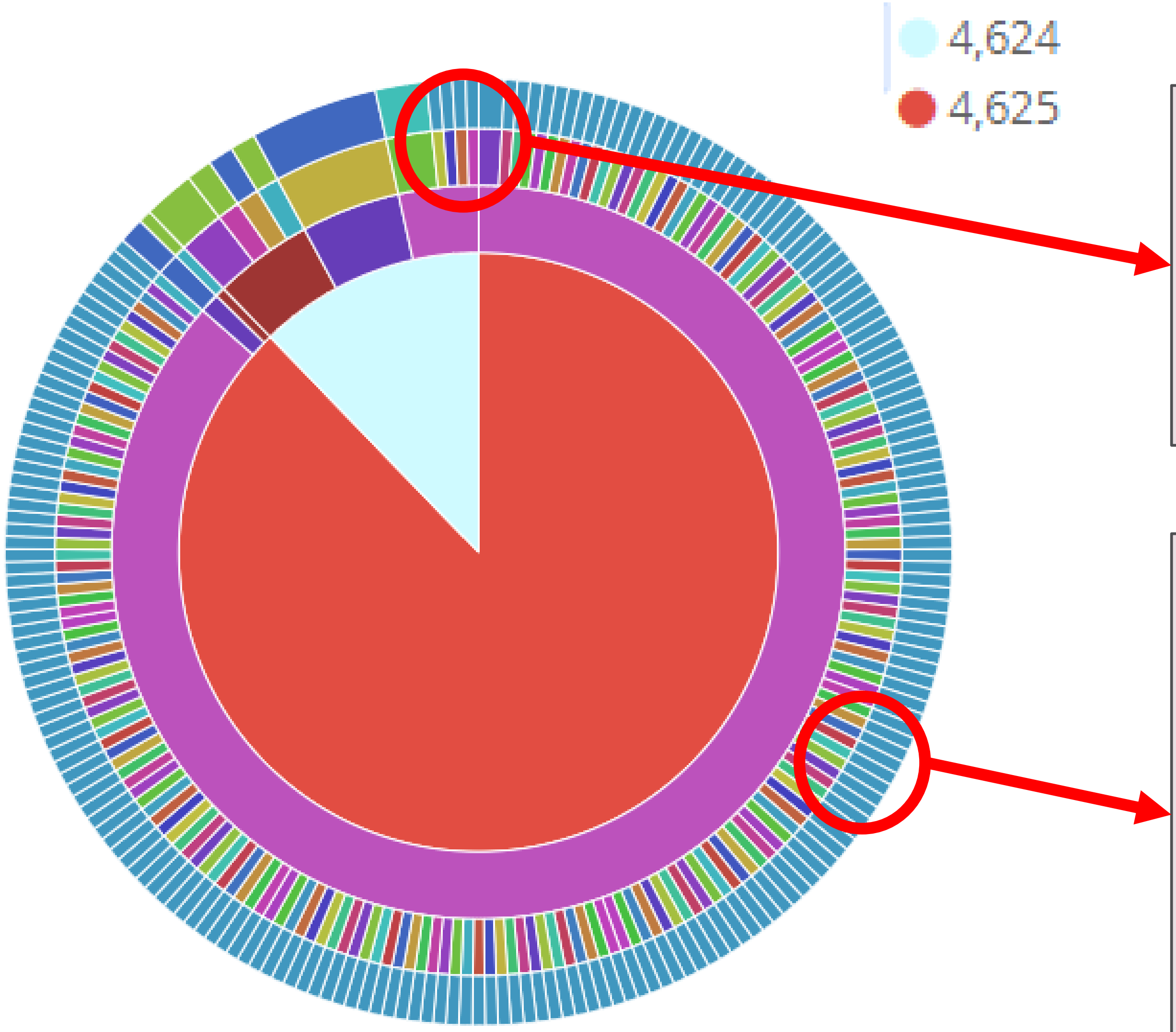
After Password Spraying



Invoke-LocalPasswordSpray is executed,
1 password is tested against 200 accounts, 4 are guessed.

The proportion of 4624/4625 changes notoriously.

After Password Spraying



Accounts correctly guessed, center is green! Source host is the same. 4 accounts guessed!

The outer blue layer represents the source IP, while the layer next to it represents the each targeted user account tested

Challenges

- Apply least privilege principle. Otherwise attackers could mess with your agents:
  - Disable services
  - Delete Sysmon configuration
  - Unload Sysmon driver filter

- Capacity planning can be hard, cloud setups can provide scalability

- Tuning, apply data retention period on Elasticsearch based on available resources and amount of events

Key Takeaways

- Sysmon + Security + System + Application event logs can provide great **visibility** to detect adversary tactics and techniques using ATT&CK as a framework
- Winlogbeat + ELK stack provide a **centralized solution** to search events
- Visualizations are a good way to detect attacks such as **Password Spray**

Next Steps

- MISP - Sysmon integration for automated detection of known IoC (pattern matching):
  - Hashes -> event 1 (Process creation)
  - Domain name -> event 22 (DNSEvent)
  - IP address -> event 3 (Network Connection)
- YaraScan integration.
  - Alerts are sent to ELK, will allow pivoting to endpoint actions based on network YARA alert
- OsQuery

  Integration with other OS (Mac, Linux)

SC LABS

SCITUM CYBER INTELLIGENCE LABORATORIES

David Bernal
@d4v3c0d3r

Eduardo Sánchez
@darkslaker