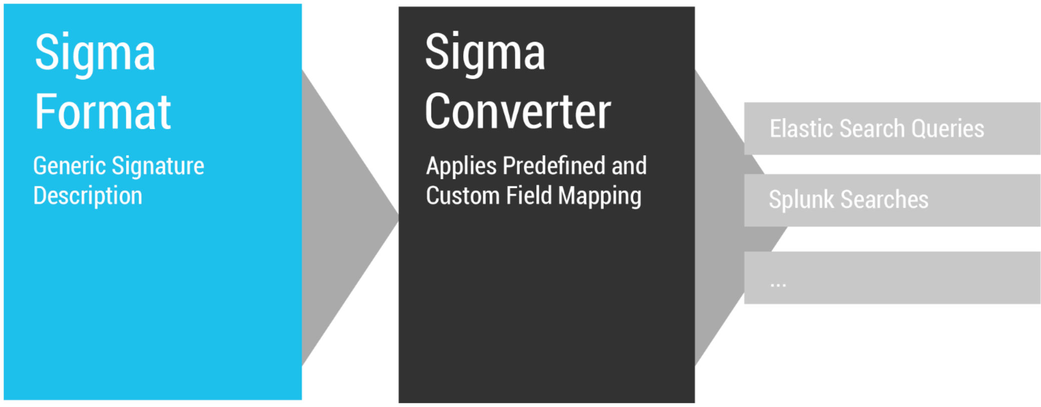
Patrick Bareiss

IT Security Blog

IT Security Blog

Click the button below to start exploring my website

START EXPLORING


Sigma Format
Generic Signature Description
Sigma Converter
Applies Predefined and Custom Field Mapping
Elastic Search Queries
Splunk Searches
...

Detecting Local User Creation in AD with Sigma

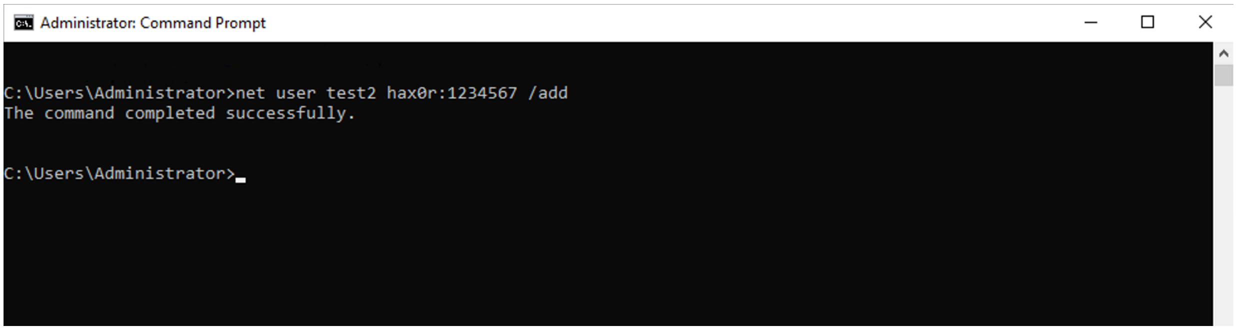
APRIL 18, 2019 ADMIN SIGMA, SPLUNK, USE CASE

In this blog post, I will introduce a new Sigma Use Case detecting local user creation in an Active Directory (AD) environment. The creation of a new user creates a Windows Event Log of Type Security with the Event Code 4720. In an AD environment, only domain controller should create these Windows Event Logs.

By monitoring the Event Log 4720 on non domain controller, we are able to detect local user creation on windows servers:

```
title: Detects local user creation
description: Detects local user creation on windows servers, which shouldn't happen in an Active Directory environment. Apply this Sigma Use Case on your windows server logs and not on your DC logs.
tags:
    - attack.privilege_escalation
    - attack.t1078
references:
    - http://www.patrick-bareiss.com/detecting-local-user-creation-in-ad-with-sigma/
author: Patrick Bareiss
logsource:
    product: windows
    service: security
detection:
    selection:
        EventID: 4720
    condition: selection
fields:
    - EventCode
    - Account_Name
    - Account_Domain
falsepositives:
    - Domain Controller Logs
level: high
```

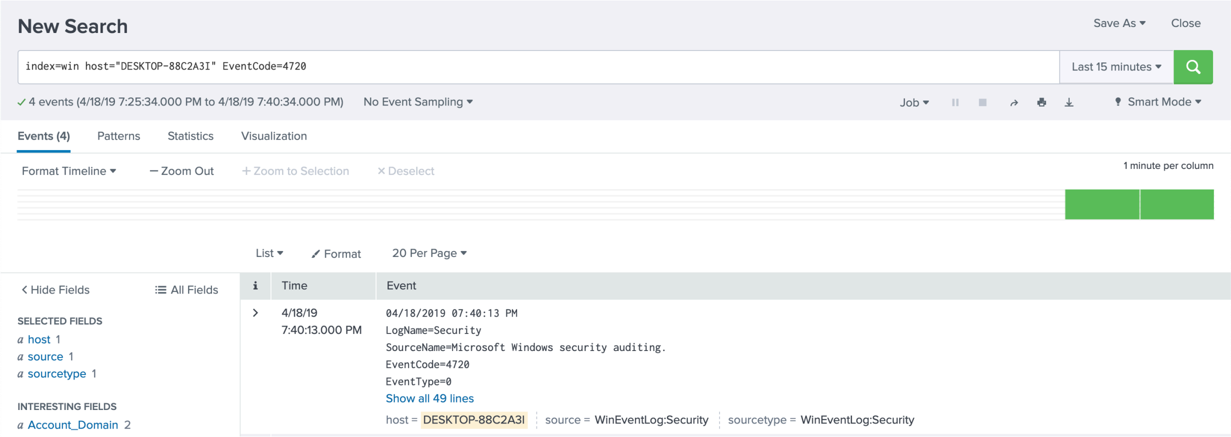
In order to test it, we create a local user on a non domain controller:



```
C:\Users\Administrator>net user test2 hax0r:1234567 /add
The command completed successfully.

C:\Users\Administrator>_
```

Subsequently, we run the Sigma Use Case in Splunk and were able to detect the event:



```
index=win host="DESKTOP-88C2A3I" EventCode=4720
```

✓ 4 events (4/18/19 7:25:34.000 PM to 4/18/19 7:40:34.000 PM)   No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 2

i	Time	Event

>	4/18/19
	7:40:13.000 PM
		04/18/2019 07:40:13 PM
		LogName=Security
		SourceName=Microsoft Windows security auditing.
		EventCode=4720
		EventType=0
		Show all 49 lines
		host = DESKTOP-88C2A3I source = WinEventLog:Security sourcetype = WinEventLog:Security

Thank you for reading.

SIGMA, SPLUNK, USE CASE

DETECT C2 TRAFFIC OVER DNS USING SIGMA

SIGMA2SPLUNKALERT TUTORIAL

Search …

RECENT POSTS

Sigma vs. WannaCry

Sigma vs. TeslaCyrpt

CI/CD in Detection Rule Development

Sigma2SplunkAlert Tutorial

Detecting Local User Creation in AD with Sigma

CATEGORIES

Sigma

Splunk

Threat Intelligence

Uncategorized

Use Case

Vulnerability Scanning

FOLLOW ME ON TWITTER

My Tweets

Follow Me

Impressum

- Cookie Policy
- Impressum
- Privacy Policy