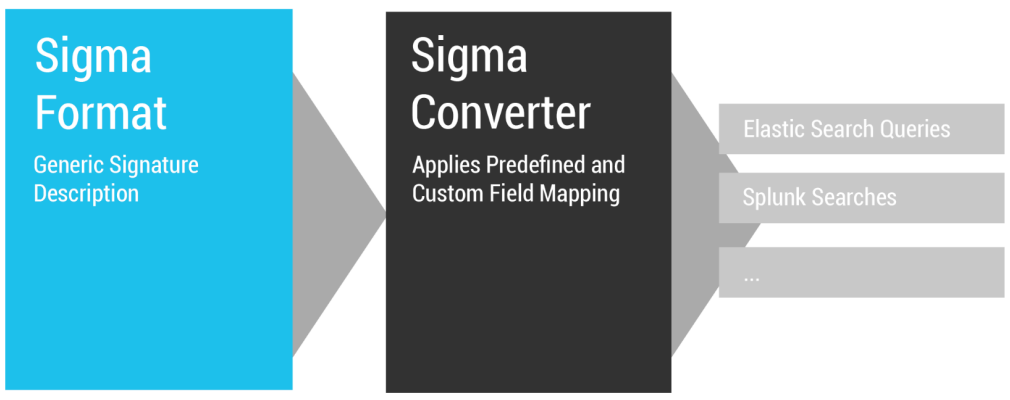


Detecting Local User Creation in AD with Sigma

APRIL 18, 2019 ADMIN SIGMA, SPLUNK, USE CASE

tecting local user creation in
w user creates a Windows
AD environment, only
s.

r, we are able to detect local

```
rvers, which shouldn't happ
en in an Active Directory environment. Apply this Sigma Use Case on your windows
server logs and not on your DC logs.
```


Search ...

RECENT POSTS

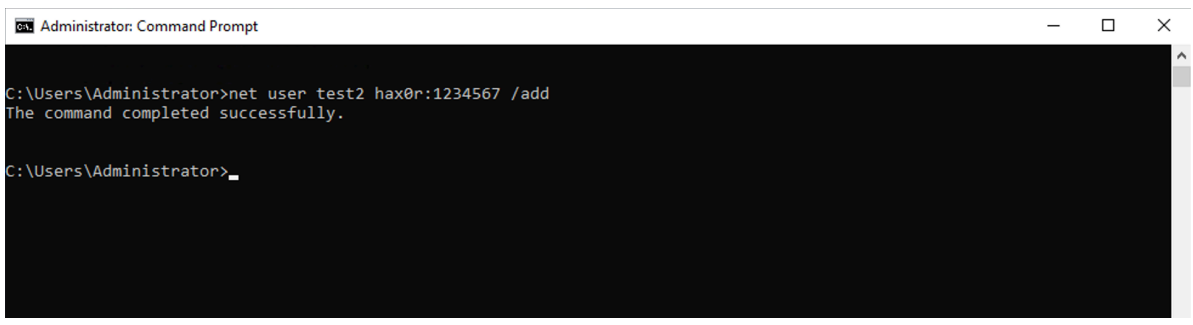
Sigma vs. WannaCry
Sigma vs. TeslaCyrpt
CI/CD in Detection Rule Development
Sigma2SplunkAlert Tutorial
Detecting Local User Creation in AD with Sigma

CATEGORIES

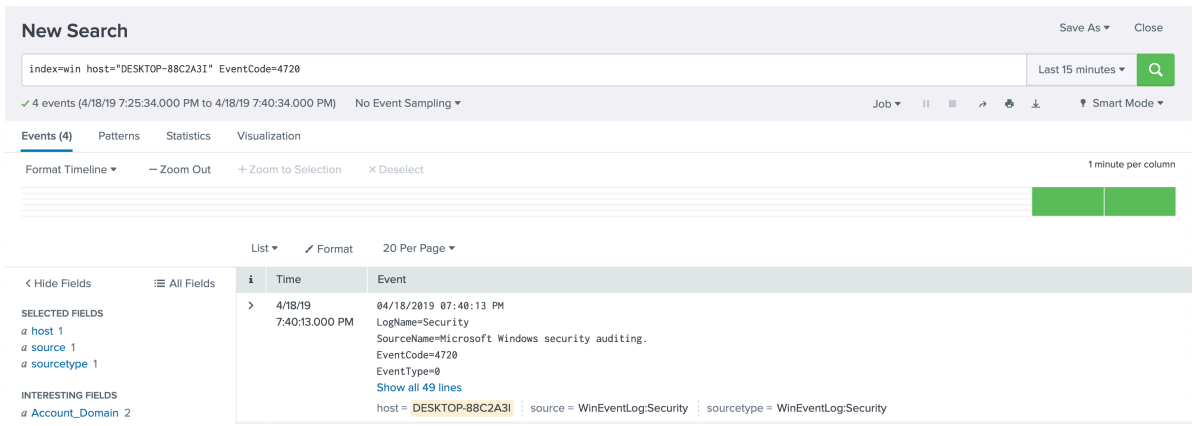
Sigma
Splunk
Threat Intelligence

```
tags:
    - attack.privilege_escalation
    - attack.t1078
references:
    - http://www.patrick-bareiss.com/detecting-local-user-creation-in-ad-with-sig
ma/
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:



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



Thank you for reading.

SIGMA, SPLUNK, USE CASE

DETECT C2 TRAFFIC OVER DNS USING SIGMA

SIGMA2SPLUNKALERT TUTORIAL

Uncategorized

Use Case

Vulnerability Scanning

FOLLOW ME ON TWITTER

Posts from @bareiss_patrick

Nothing to see here - yet

When they post,