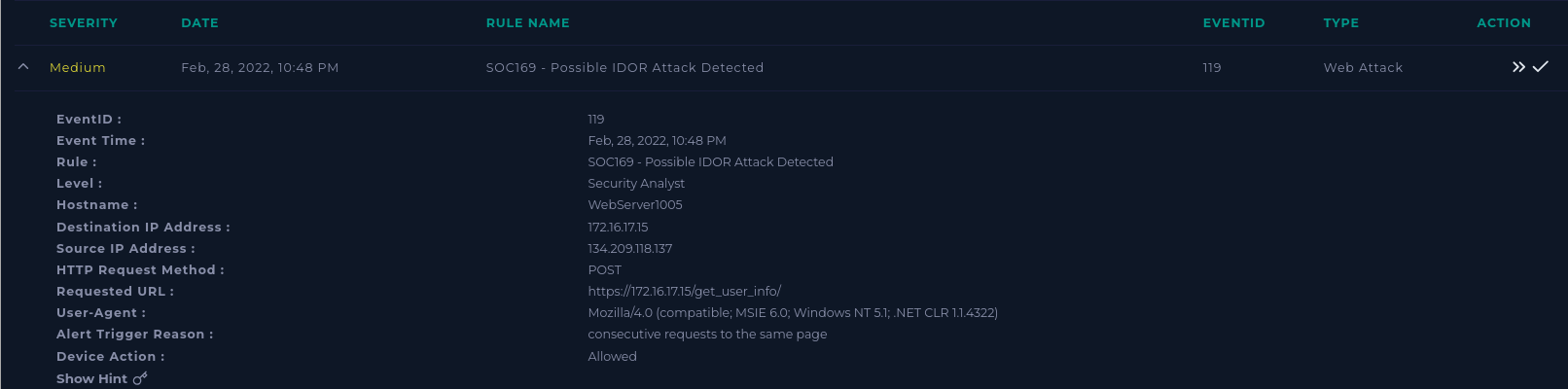
I’m going to create a playbook for the LetsDefend alert “SOC169 - Possible IDOR Attack Detected”.



First it is important to review the alert information.

When did the event occur?

Feb, 28, 2022, 10:48 PM

What is the destination IP?

The destination IP is 172.16.17.15. This IP is within our network and belongs to WebServer1005.

What is the Source IP?

The source IP is 134.209.118.137.

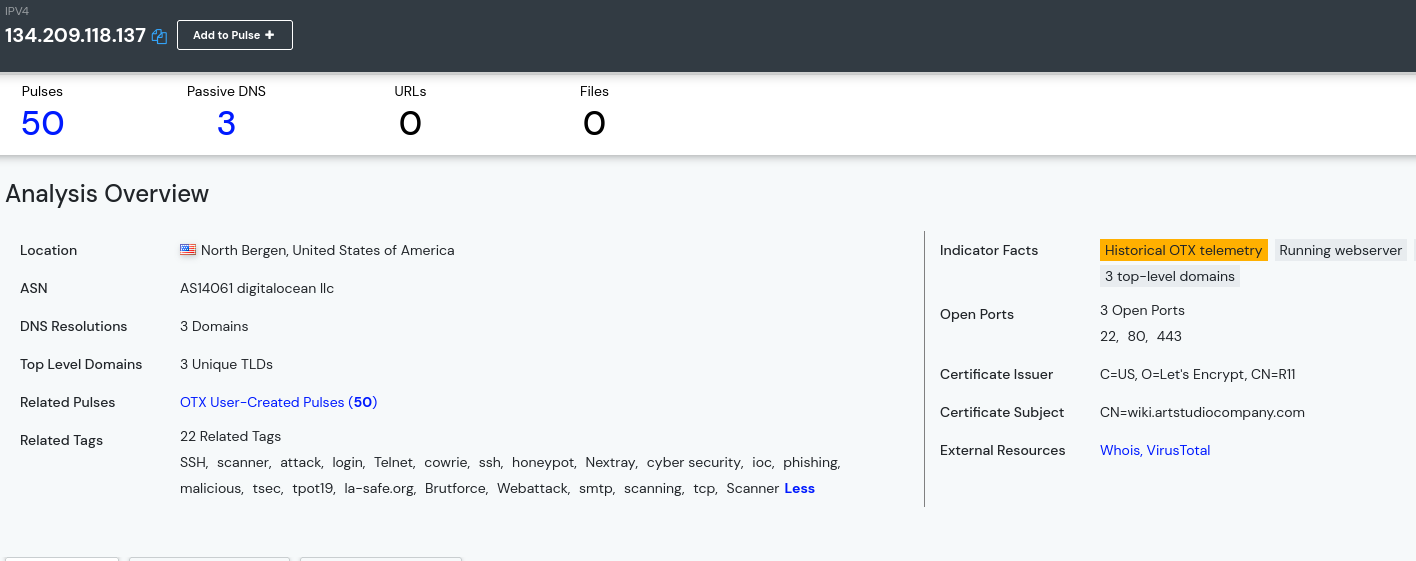
Why was the alert created?

SOC169 - Possible IDOR Attack Detected. IP 134.209.118.137 sent consecutive requests to WebServer1005.

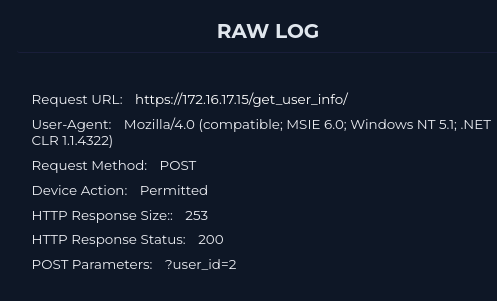
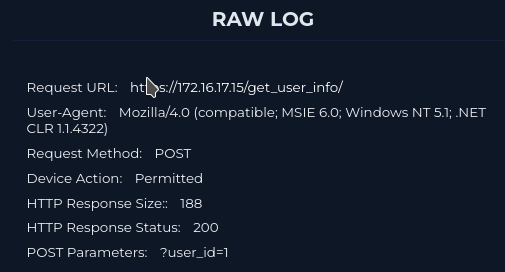
Next, I will gather some data to help understand the flow of the traffic.

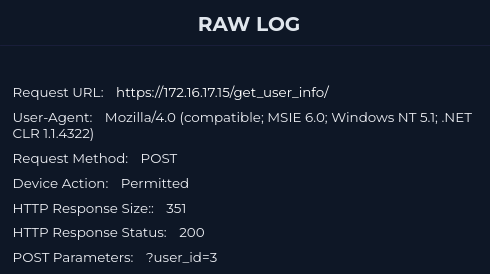
Ip address ownership and reputation:

The source IP is out of network, when looking into this IP using virus total, it is marked malicious by SOCRadar. Using alienvault for more information, we find that the IP has several tags linking to malicious activities.



To find the direction of traffic, I query any logs from the source IP 134.209.118.137 on Feb 28, 2022.

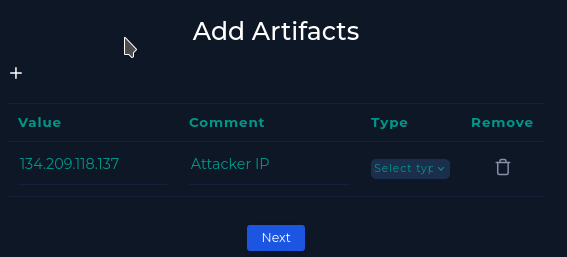




These logs show that the source IP made five requests to the same webpage over a few minutes with different post parameters. The HTTP response status is 200 and so was approved, and the Response Size is different for each log meaning it is likely the attack was successful. As these are five consecutive requests on the same page with incrementing post parameters, this is likely a insecure direct object reference attack.

It is important to know if this attack is a false positive by a planned attack or simulation. Searching the Email Security by the destination IP yields no results meaning that this is likely a real attack. The endpoint WebServer1005 is contained from the network for further investigation.

Artifacts:



Analyst Note:  
This attack occurred because an external IP (134.209.118.137) sent multiple requests to WebServer1005 (172.16.17.15). These requests contained incrementing post values leading to an IDOR attack as follows:

?user\_id=1

?user\_id=2

?user\_id=3

?user\_id=4

?user\_id=5

Each request had a HTTP response status of 200 and varying response sizes (158-351). This leads me to believe that this was a successful IDOR attack which returned five desired webpages.

The affected device WebServer1005 has been contained due to the possible attack. This case has been escalated to tier 2 analysis for further investigation.