SOC165 - Possible SQL Injection Payload Detected

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Feb, 25, 2022, 11:34 AM	SOC165 - Possible SQL Injection Payload Detected	115	Web Attack	» ✓

EventID :	115
Event Time :	Feb, 25, 2022, 11:34 AM
Rule :	SOC165 - Possible SQL Injection Payload Detected
Level :	Security Analyst
Hostname :	WebServer1001
Destination IP Address :	172.16.17.18
Source IP Address :	167.99.169.17
HTTP Request Method :	GET
Requested URL :	https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-
User-Agent :	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Alert Trigger Reason :	Requested URL Contains OR 1 = 1
Device Action :	Allowed
Show Hint	

Click on >> and create case and click Continue.

Incident Details

Incident Name:	**EventID: 115 - [SOC165 - Possible SQL Injection Payload Detected]**
Description:	**EventID: 115**
Incident Type:	**Web Attack**
Created Date:	**Jan, 06, 2024, 03:05 PM**

Start Playbook!

Understand Why the Alert Was Triggered

In order to perform a better analysis and to determine whether the triggered alert is false positive, it is first necessary to understand why the rule was triggered. Instead of starting the analysis directly, first understand why this rule was triggered.

- Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.
- Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

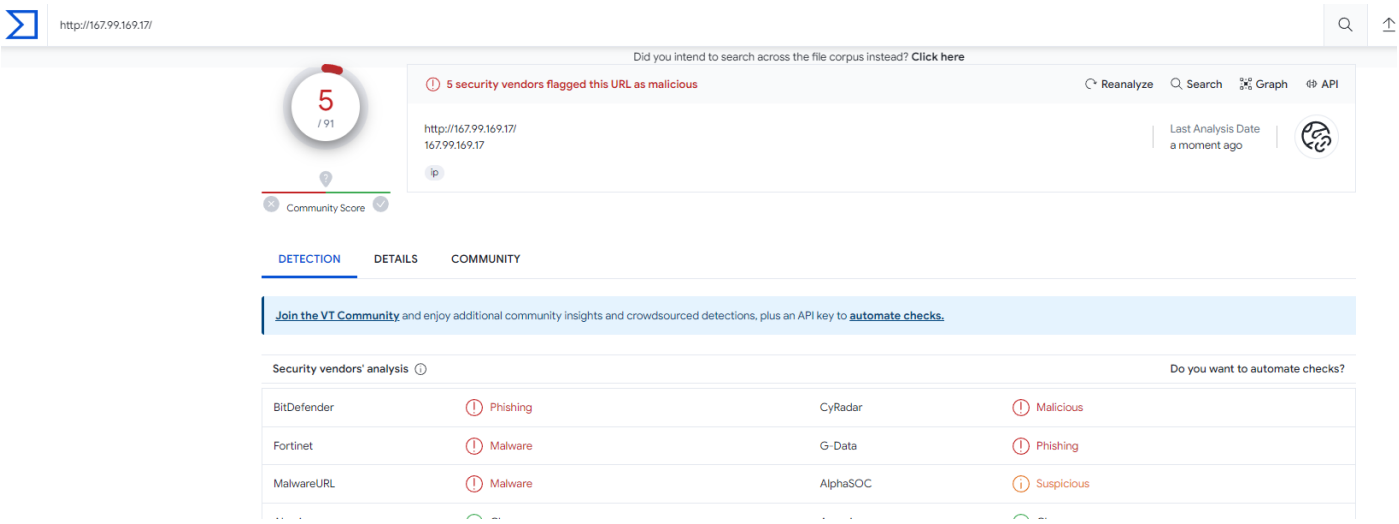
Next

So, the SOC Rule talks about, “Possible SQL Injection Payload” which gives a direction towards the kind of attack we are about to investigate.

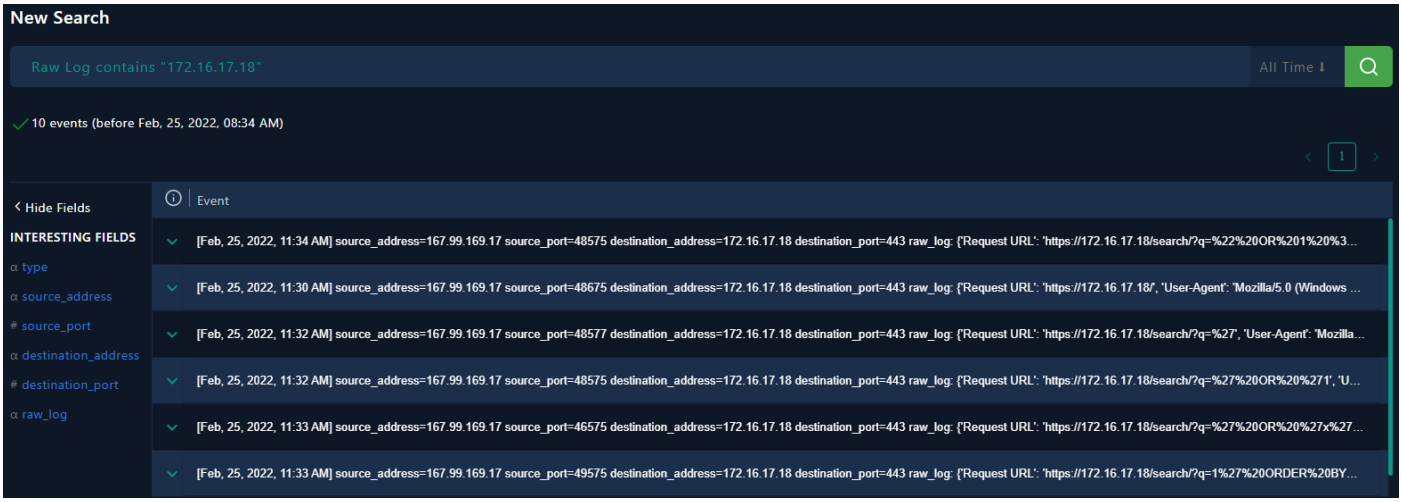
We can see that the requested URL is https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20- which when we pass through URL Decoder comes up as https://172.16.17.18/search/?q=" OR 1 = 1 -- -

With a query such as “ OR 1 = 1”, it is a possible attempt to claim userIDs & passwords from WebServer1001 (mentioned as hostname) with IP address 172.16.17.18

Upon checking the reputation of the source IP address in VirusTotal



By taking a look at the Log management, it can be determined that the WebServer1001 has been receiving hits from source_address=167.99.169.17 since Feb, 25, 2022, 11:30 AM



After decoding the URLs, the results are:

https://172.16.17.18/search/?q=1' ORDER BY 3--+

https://172.16.17.18/search/?q=' OR 'x'='x

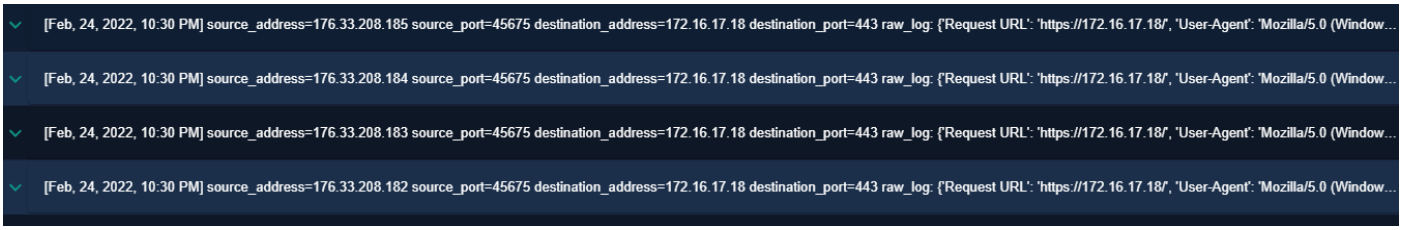
https://172.16.17.18/search/?q=' OR '1

https://172.16.17.18/search/?q='

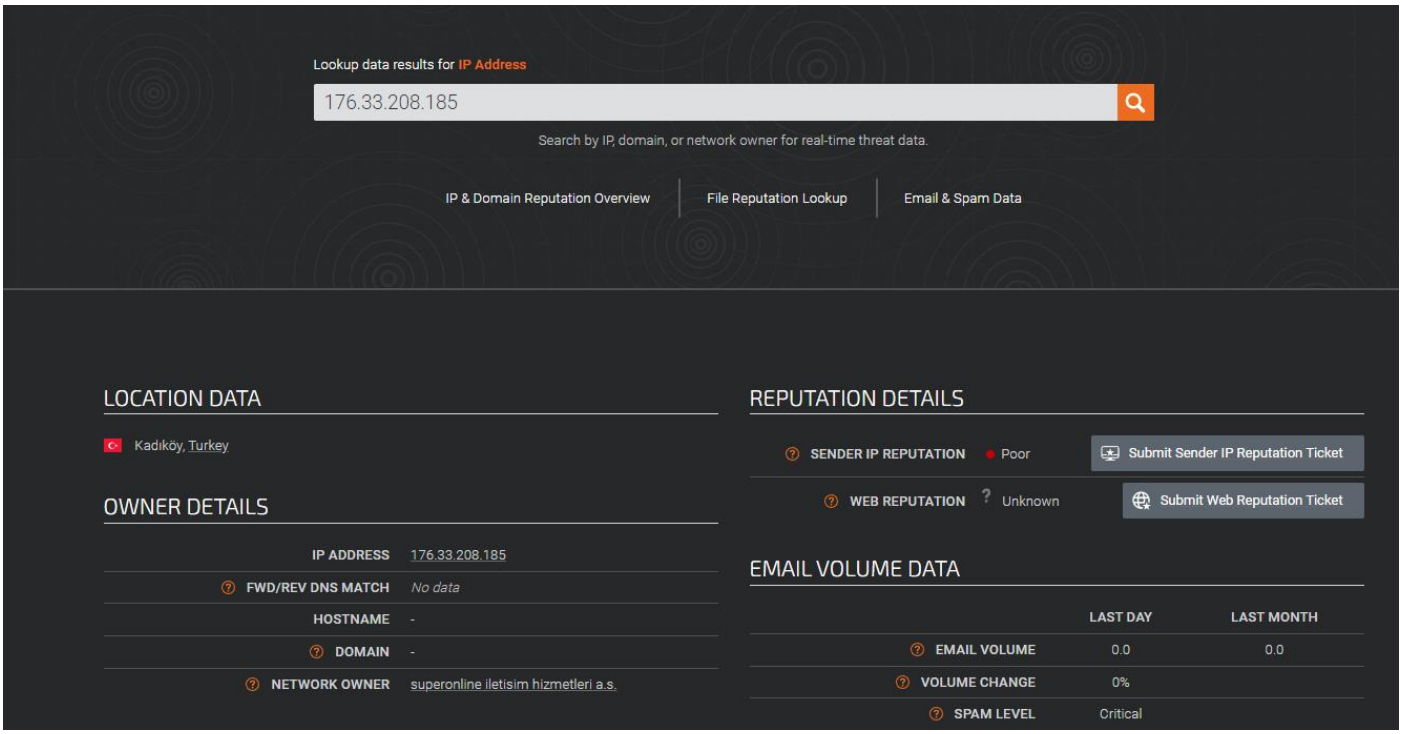
https://172.16.17.18/

https://172.16.17.18/search/?q=" OR 1 = 1 -- -

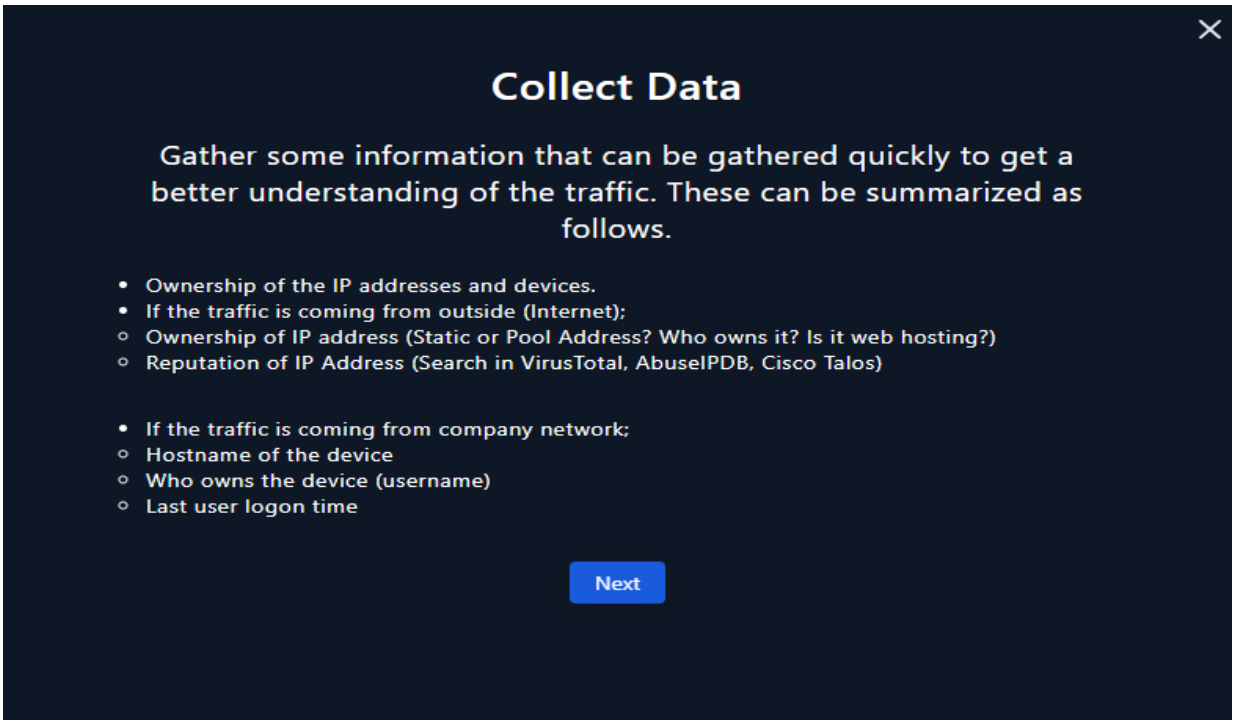
All of the above URLs point to a possible SQL Injection attack on the Webserver. This could be a specific attack on the server. Interestingly, the previous day Feb, 24, 2022, 10:30 AM... there are have been hits on the server at the same time from 4 different IP addresses.



Upon checking one of the addresses on Talos, it has a poor reputation with critical spam level



But since there were no follow-ups, this could well be a fire-and-forget scan. Proceeding with the Playbook,



Ownership of the IP addresses and devices.: Digital Ocean

If the traffic is coming from outside (Internet); Yes

Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?): Digital Ocean

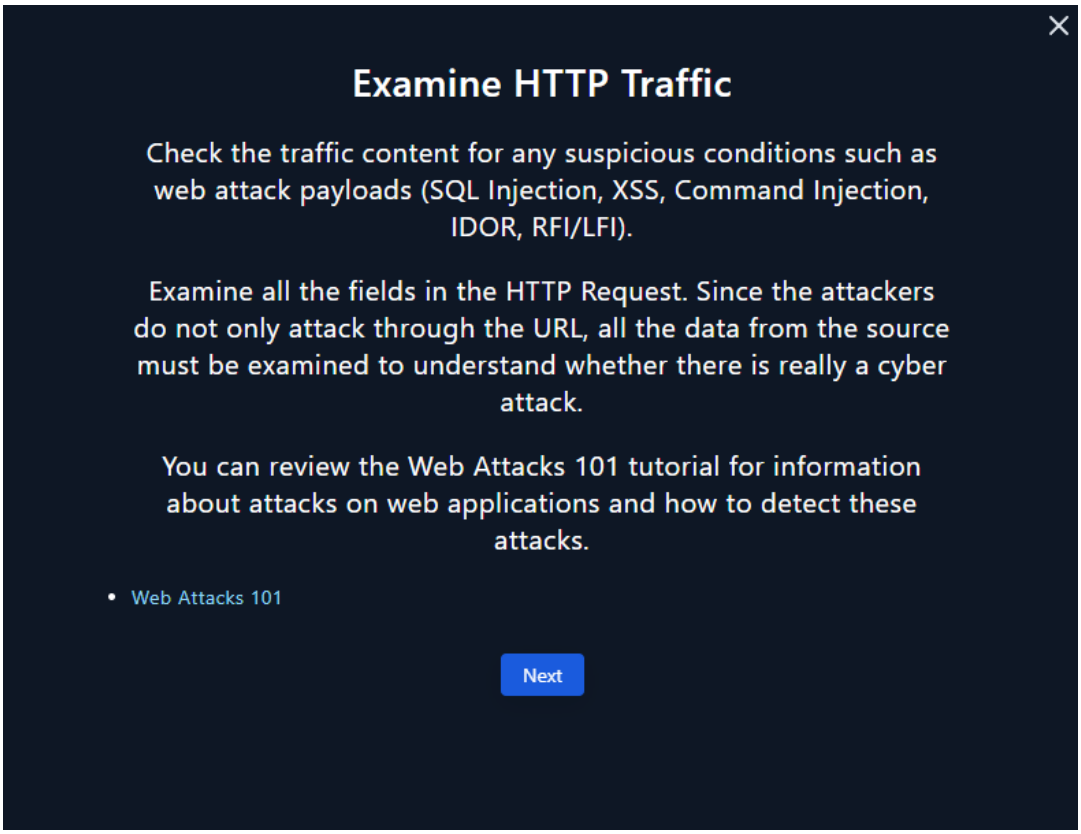
Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos): Malicious

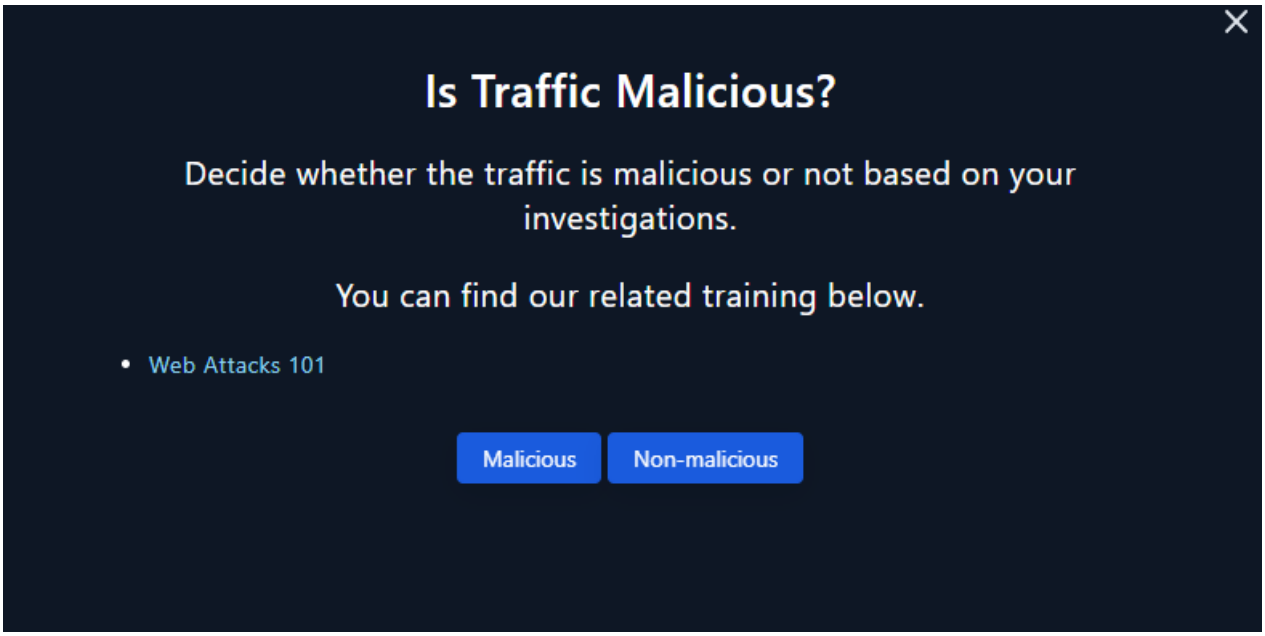
If the traffic is coming from company network; No

Hostname of the device: WebServer1001

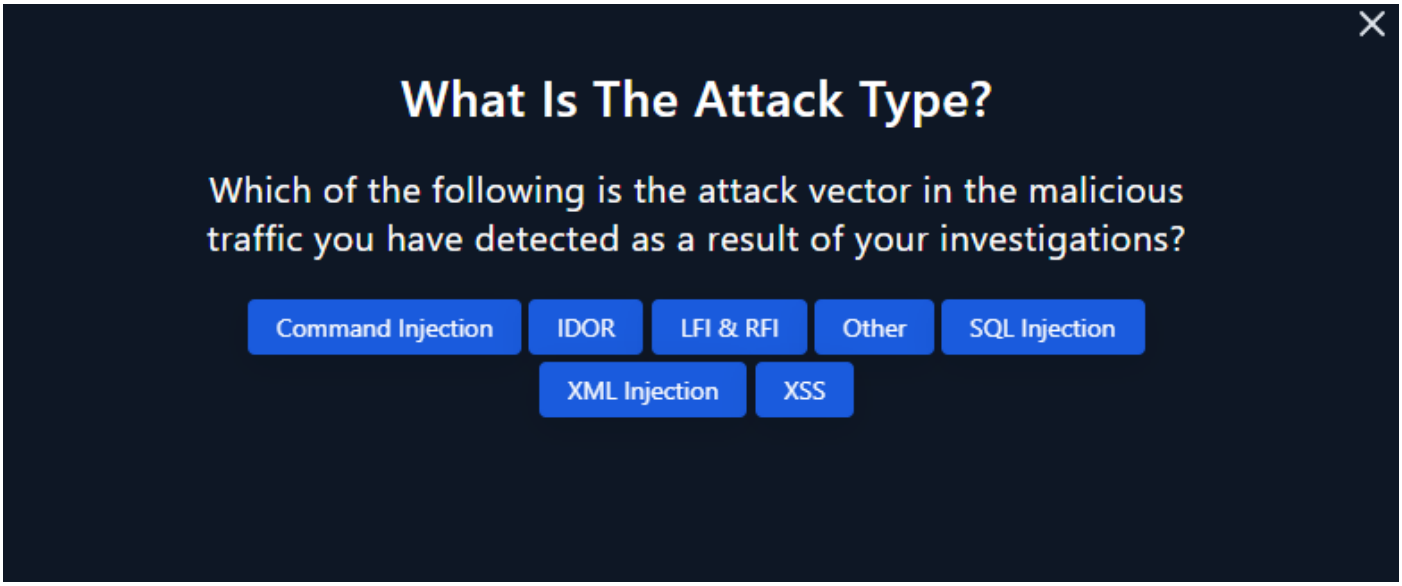
Who owns the device (username): webadmin

Last user logon time: Feb, 10, 2022, 11:12 PM

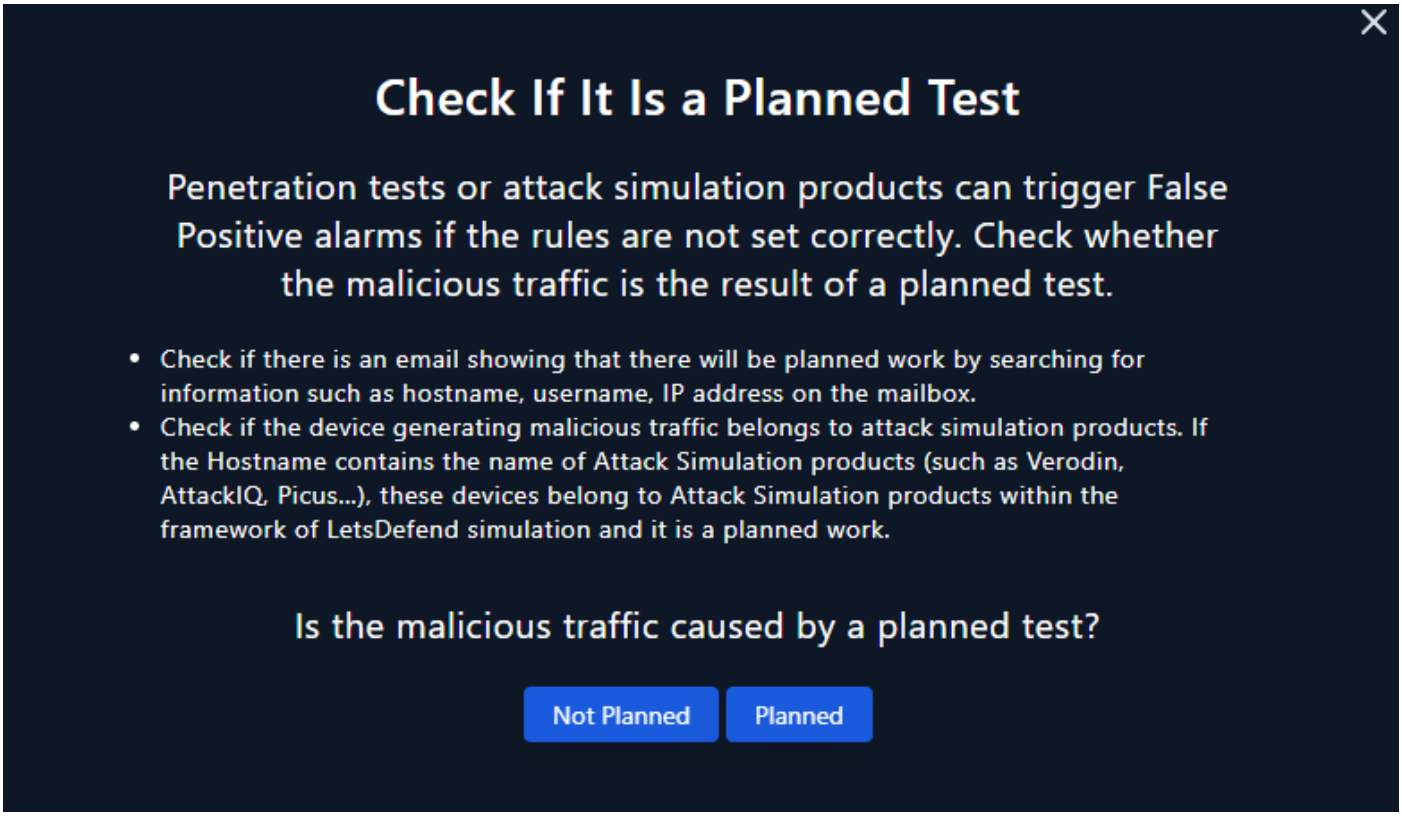




As per our analysis, the traffic has been determined as Malicious with an intention to gain user info.



Selecting SQL Injection based on our finding.



Post searching the mail Security tab for any relevant mails, nothing was found. Hence, selecting Not Planned.

What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

Company Network → Company Network | Company Network → Internet | Internet → Company Network

The source address was 167.99.169.17 and was attempting an SQL injection on the Webserver's address... so it's an INTERNET → Company Network.

Check Whether the Attack Was Successful

Investigate whether the attack was successful. Detection mechanisms vary according to the attack type. Some tips that can help with your investigation;

- In Command Injection attacks, you can understand whether the attack was successful by looking at the "Command History" of the relevant device via Endpoint Security. In SQL Injection attacks, attackers can run commands on the device with the help of functions such as "xp_cmdshell". For this reason, you may need to look at the "Command History" in SQL Injection attacks.
- You can guess by looking at the HTTP Response size in SQL Injection and IDOR attacks.

You can access the Web Attacks 101 training below, in which we explain how you can understand whether the attack is successful or not according to the attack type.

- Web Attacks 101

Next

The attack was not successful because at every attempt, as found in the logs, there was a Response Code of 500 which means it threw a server error. So, the attacker was unable to obtain the required info.

Was the Attack Successful?

Select "Yes" if you found that the attack was successful as a result of your investigations, and "No" if you found that the attack was unsuccessful.

No Yes

Basis above explanation, selecting NO here.

Add Artifacts

+

Value	Comment	Type	Remove
167.99.169.17	Malicious URL	IP Address	

Next

Added the recorded artifact which is the attacker's IP address. You may/may not want to add the other IP address who was trying to get a hit on Feb 24, 2022.

Do You Need Tier 2 Escalation?

Tier 2 escalation should be performed in the following situations.

- In cases where the attack succeeds,
- When the attacker compromises a device in the internal network (in cases where the direction of harmful traffic is from inside → inside),

Tier 2 escalation is not required in the following cases.

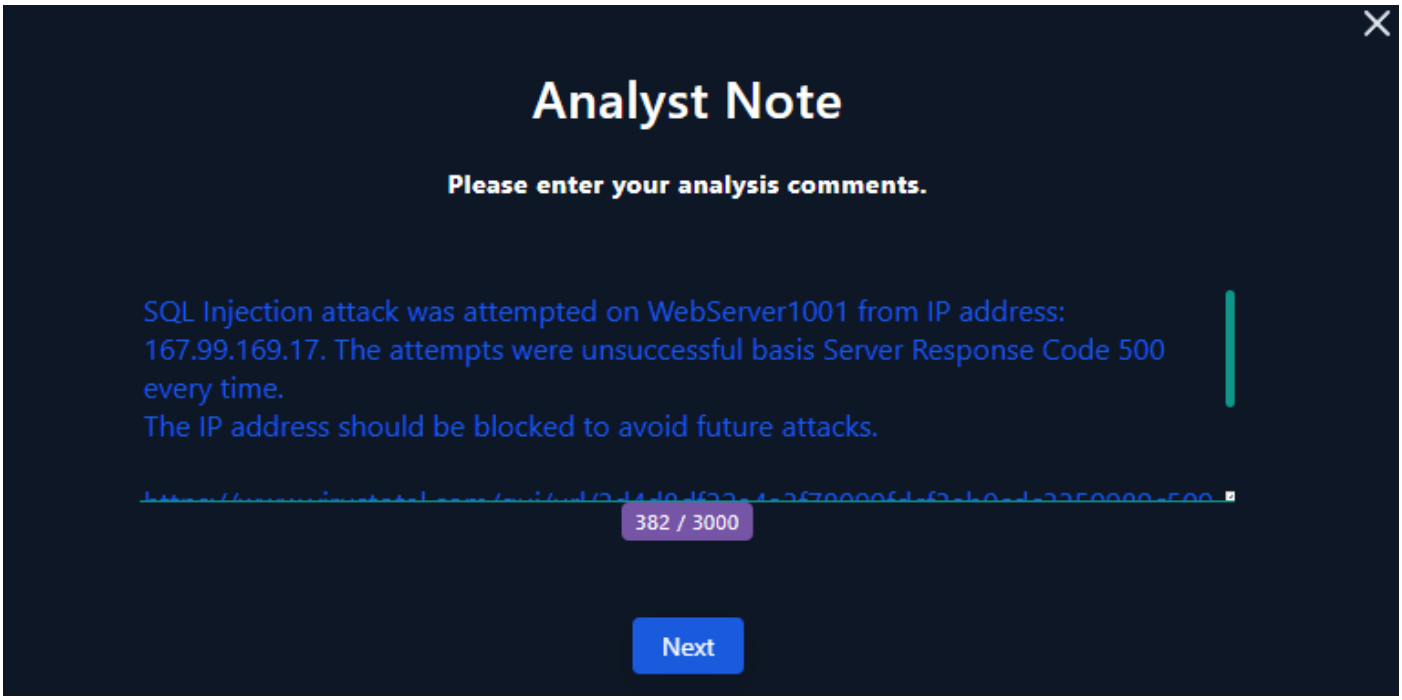
- In cases where attacks from the Internet do not succeed

** Institutions may have their own escalation procedure. Don't forget to learn about the escalation procedure in your institution.

Perform Tier 2 escalation?

No Yes

Since the attack was not successful, it does not require further Tier 2 escalation. Selecting NO here.



Add your finding as comments

"**SQL Injection attack was attempted on WebServer1001 from IP address:**

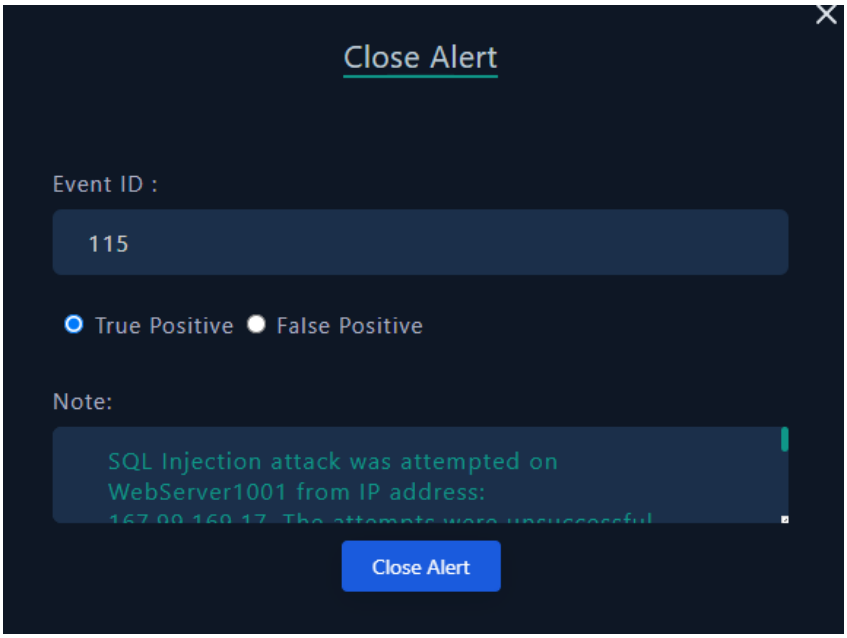
167.99.169.17. The attempts were unsuccessful basis Server Response Code 500 every time.

The IP address should be blocked to avoid future attacks.

https://www.virustotal.com/gui/url/3d4d8df22a4a3f78099fdcf3ab0cdc3359989c50928b3ab1f6718940bf54d56f/detection

https://otx.alienvault.com/indicator/ip/167.99.169.17"

.. And click and confirm on FINISH PLAYBOOK and close the Alert.



This would be a True Positive as a "**Possible SQL Injection Payload**" was detected.

Let’s check the scores now.

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
High	Jan, 07, 2024, 12:54 AM	SOC165 - Possible SQL Injection Payload Detected	115	Web Attack	✓	

EventID : 115

Event Time : Feb, 25, 2022, 11:34 AM

Rule : SOC165 - Possible SQL Injection Payload Detected

Answer : True Positive (+5 Point)

Playbook Answers :
Do You Need Tier 2 Escalation? (+5 Point)
Was the Attack Successful? (+5 Point)
What Is the Direction of Traffic? (+5 Point)
Check If It Is a Planned Test (+5 Point)
What Is The Attack Type? (+5 Point)
Is Traffic Malicious? (+5 Point)

Analyst Note : SQL Injection attack was attempted on WebServer1001 from IP address:
167.99.169.17. The attempts were unsuccessful basis Server Response Code 500 every time.
The IP address should be blocked to avoid future attacks.

https://www.virustotal.com/gui/url/3d4d8df22a4a3f78099fdcf3ab0cdc3359989c50928b3ab1f6718940bf54d56f/detection
https://otx.alienvault.com/indicator/ip/167.99.169.17

Community Walkthrough : Show

Hopefully this helped.