Official incident report

Event ID:115

Rule Name: SOC165 - Possible SQL Injection Payload Detected

Made By: Asmaa Abdelrahman

LinkedIn: https://www.linkedin.com/in/asmaa-abdelrahman-93ab46230/

Github link: https://github.com/Asma-Abdelrahman

Table of contents

Event Details

Event ID: 115

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

Rule: SOC165 - Possible SQL Injection Payload Detected

Level: Security Analyst

Network Information Details

Hostname: WebServer1001

Destination Address: 172.16.17.18

Source Address: 167.99.169.17

External / Internal Attack:

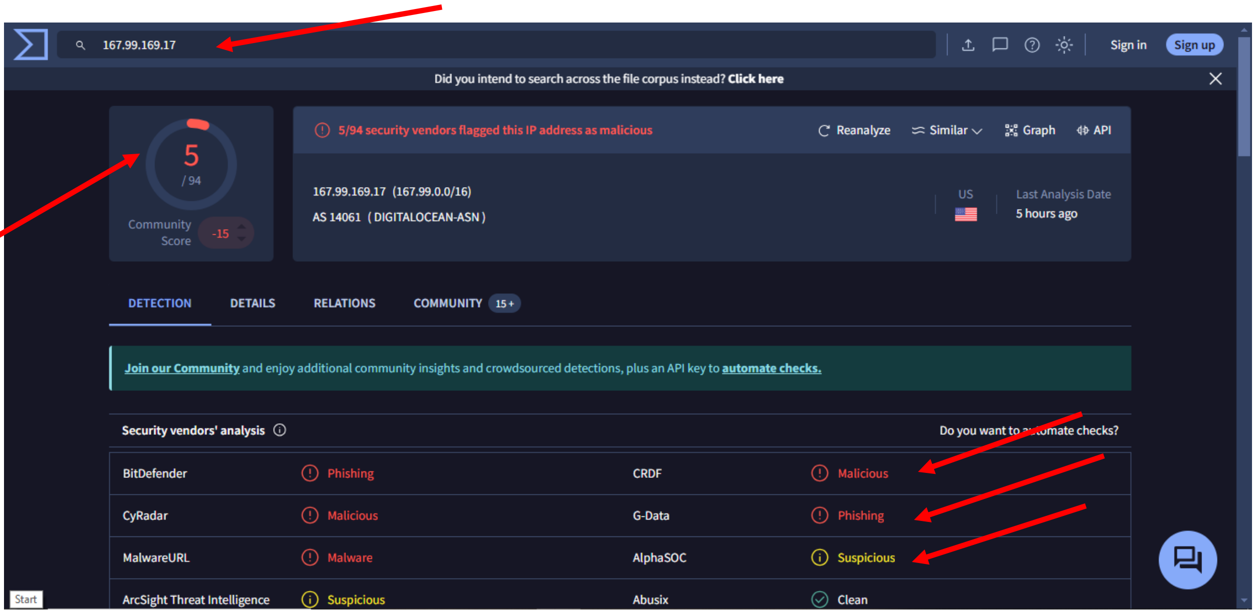
- Source Address (167.99.169.17): This IP address is external, meaning it originates from outside the internal network.
- Destination Address (172.16.17.18): This IP address is within a private IP range (typically used for internal networks). Based on this information, it appears to be an internal to external attack since the source address originates from an internal network, and the destination address is external.

  This is an external attack.

Analysis:
I will check if this IP is malicious or not.

Virus Total Analysis:

The results from Virus Total for this IP address indicate significant threats. For more details, please refer to the link provided.


167.99.169.17

Sign in Sign up

Did you intend to search across the file corpus instead? Click here

5 / 94 Community Score -15

5/94 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

167.99.169.17 (167.99.0.0/16)
AS 14061 (DIGITALOCEAN-ASN)

US

Last Analysis Date
5 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 15+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

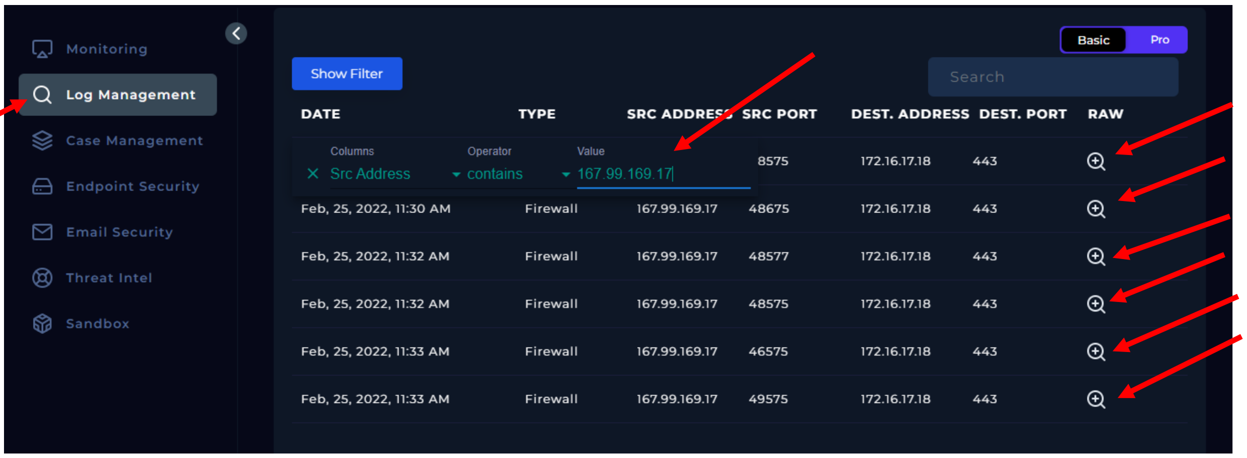
Security vendors' analysis — Do you want to automate checks?

BitDefender	Phishing	CRDF	Malicious
CyRadar	Malicious	G-Data	Phishing
MalwareURL	Malware	AlphaSOC	Suspicious
ArcSight Threat Intelligence	Suspicious	Abusix	Clean

Log Management

We queried the source IP and retrieved six log entries. For a detailed view of these logs, please refer to

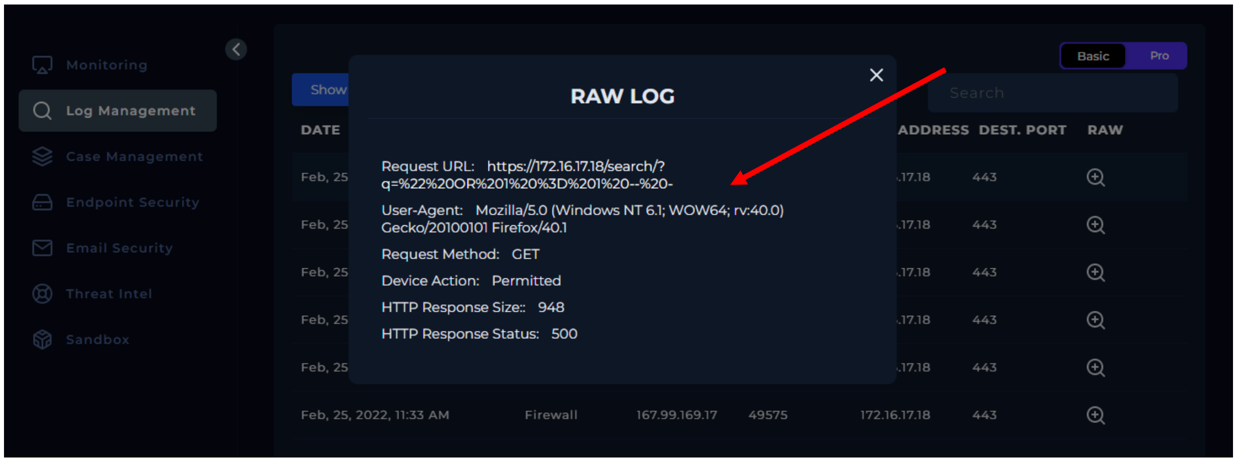
the attached photo.



Columns: Src Address — Operator: contains — Value: 167.99.169.17

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
			8575	172.16.17.18	443	
Feb, 25, 2022, 11:30 AM	Firewall	167.99.169.17	48675	172.16.17.18	443	
Feb, 25, 2022, 11:32 AM	Firewall	167.99.169.17	48577	172.16.17.18	443	
Feb, 25, 2022, 11:32 AM	Firewall	167.99.169.17	48575	172.16.17.18	443	
Feb, 25, 2022, 11:33 AM	Firewall	167.99.169.17	46575	172.16.17.18	443	
Feb, 25, 2022, 11:33 AM	Firewall	167.99.169.17	49575	172.16.17.18	443	

Log 1:



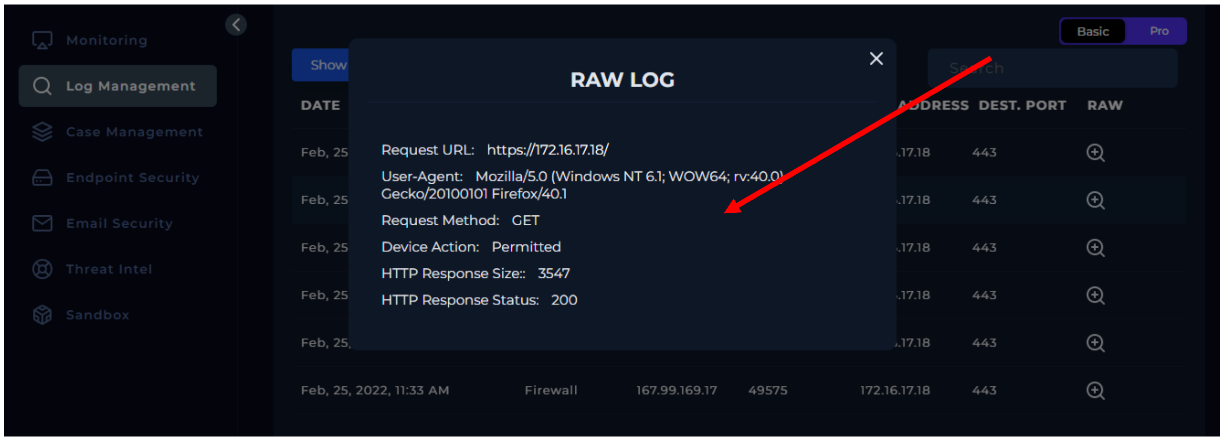
```
RAW LOG

Request 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
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   948
HTTP Response Status:   500
```

```
DATE                                                          ADDRESS   DEST. PORT   RAW
Feb, 25                                                       .17.18    443
Feb, 25                                                       .17.18    443
Feb, 25                                                       .17.18    443
Feb, 25                                                       .17.18    443
Feb, 25                                                       .17.18    443
Feb, 25, 2022, 11:33 AM   Firewall   167.99.169.17   49575    172.16.17.18   443
```

- Request URL: https://172.16.17.18/search/?q=%27%20OR%20%271
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
- Request Method: GET
- Device Action: Permitted
- HTTP Response Size: 948 bytes
- HTTP Response Status: 500 Internal Server Error

Explanation: This log entry shows a GET request with a URL-encoded payload that includes SQL Injection elements ('%20OR%20%271). The HTTP 500 response status indicates that the server encountered an error while processing this request. This suggests that the SQL Injection attempt may have triggered an error, possibly due to improper handling of the injected payload.

Log 1:



```
RAW LOG

Request URL:   https://172.16.17.18/
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   3547
HTTP Response Status:   200
```

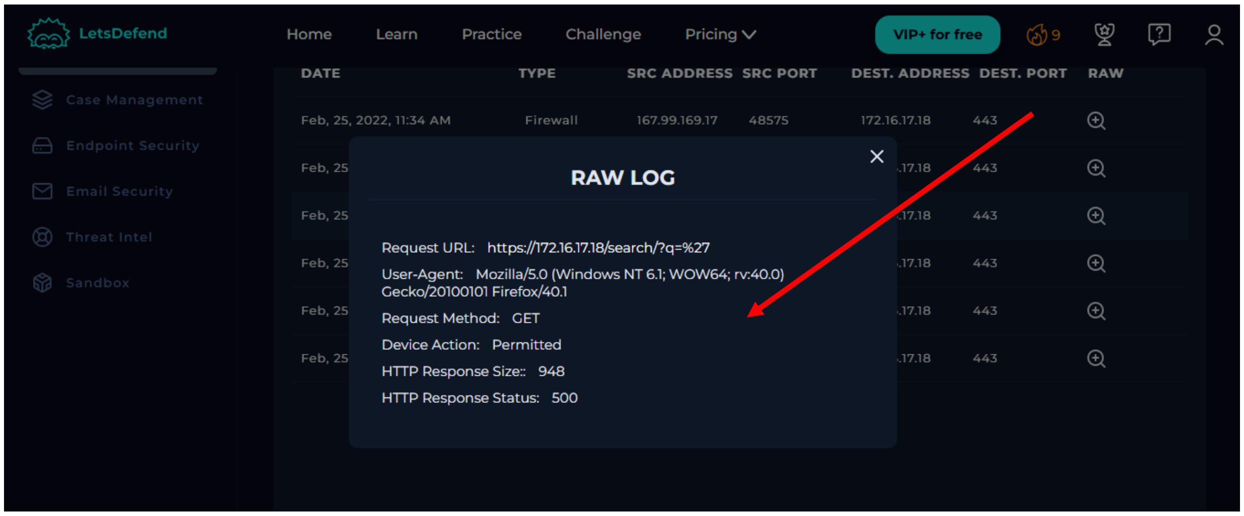
```
DATE                                                          ADDRESS   DEST. PORT   RAW
Feb, 25                                                       .17.18    443
Feb, 25                                                       .17.18    443
Feb, 25                                                       .17.18    443
Feb, 25                                                       .17.18    443
Feb, 25,                                                      .17.18    443
Feb, 25, 2022, 11:33 AM   Firewall   167.99.169.17   49575    172.16.17.18   443
```

Request URL: https://172.16.17.18/

- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
- Request Method: GET
- Device Action: Permitted
- HTTP Response Size: 3547 bytes
- HTTP Response Status: 200 OK

Explanation: This log entry shows a standard GET request to the root URL of the server. The HTTP response status of 200 indicates that the request was successfully processed and the server responded with the requested content. This entry appears to be a normal request with no signs of malicious activity.

Log 3:



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 25, 2022, 11:34 AM	Firewall	167.99.169.17	48575	172.16.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	

RAW LOG

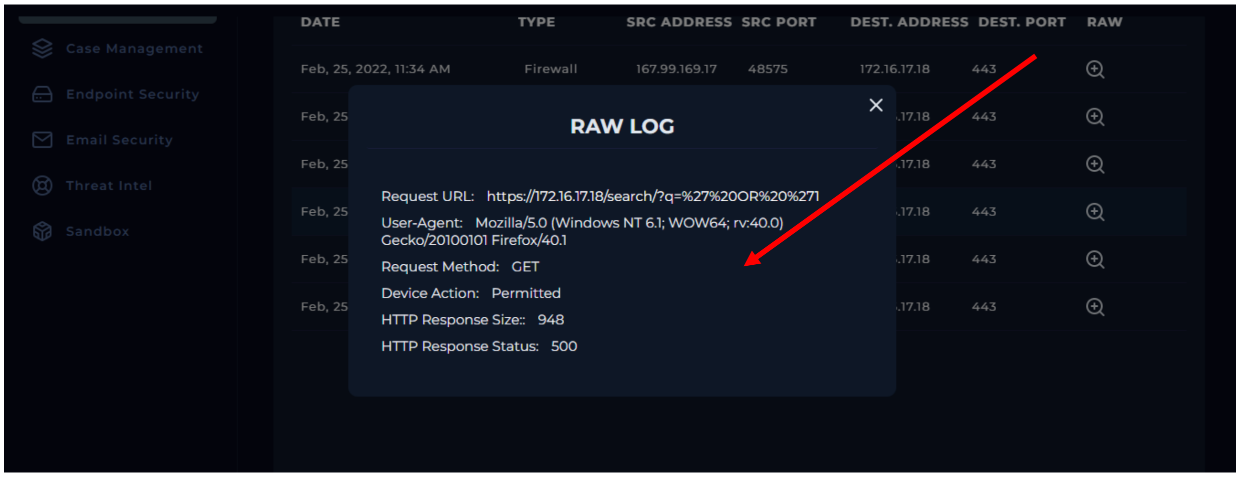
```
Request URL:   https://172.16.17.18/search/?q=%27
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   948
HTTP Response Status:   500
```

Request URL: https://172.16.17.18/search/?q=%27

- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
- Request Method: GET
- Device Action: Permitted
- HTTP Response Size: 948 bytes
- HTTP Response Status: 500 Internal Server Error

Explanation: This entry shows a GET request with a URL-encoded single quote ('%27). This is another SQL Injection attempt where the single quote is often used to break out of a query string. The HTTP 500 response indicates that the server encountered an error, which could be due to the improper handling of this SQL Injection payload.

Log 4:



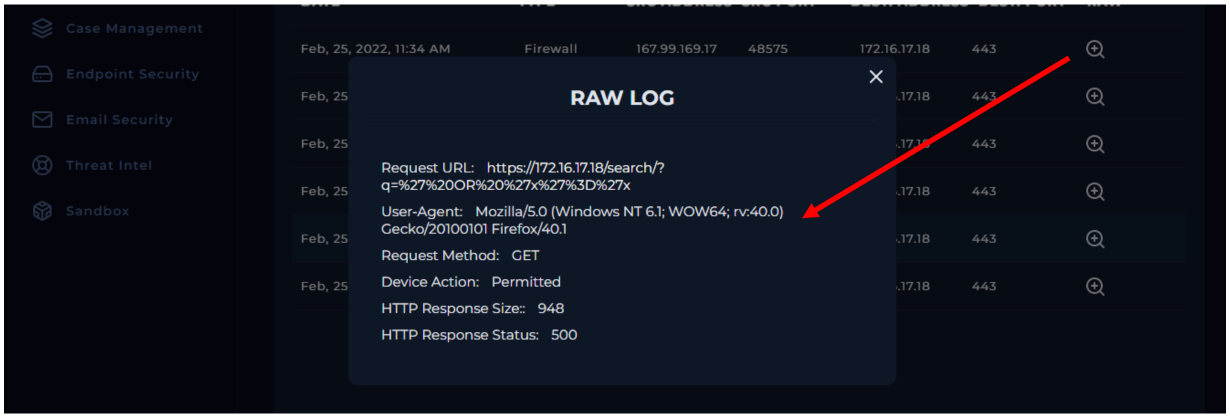
DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 25, 2022, 11:34 AM	Firewall	167.99.169.17	48575	172.16.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	

```
Request URL:   https://172.16.17.18/search/?q=%27%20OR%20%271
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   948
HTTP Response Status:   500
```

- Request URL: https://172.16.17.18/search/?q=%27%20OR%20%27x%27%3D%27x
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
- Request Method: GET
- Device Action: Permitted
- HTTP Response Size: 948 bytes
- HTTP Response Status: 500 Internal Server Error

Explanation: This log entry shows a GET request with a more complex SQL Injection payload ('%20OR%20%27x%27%3D%27x). The payload is designed to bypass authentication or manipulate the query logic by using a tautology. The HTTP 500 response indicates that the server could not process this request, likely due to errors in handling the injection.

Log 5:



Feb, 25, 2022, 11:34 AM	Firewall	167.99.169.17	48575	172.16.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	
Feb, 25				.17.18	443	

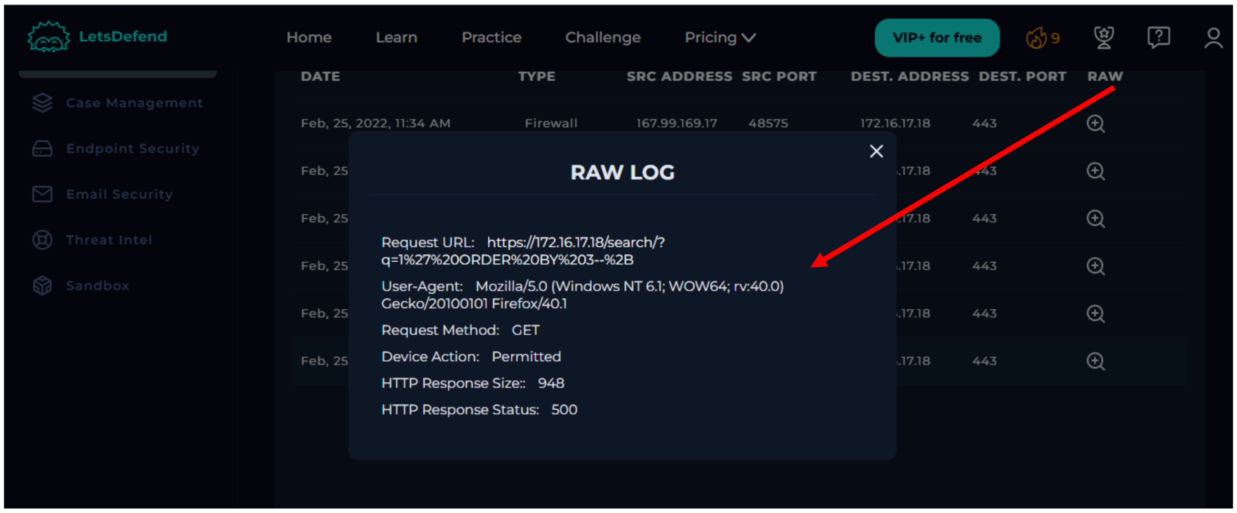
```
Request URL:   https://172.16.17.18/search/?
q=%27%20OR%20%27x%27%3D%27x
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   948
HTTP Response Status:   500
```

Request 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
- Request Method: GET
- Device Action: Permitted
- HTTP Response Size: 948 bytes
- HTTP Response Status: 500 Internal Server Error

Explanation: This log shows a GET request with a URL-encoded SQL Injection payload ("%20OR%201%20%3D%201%20--%20-). This payload is designed to create a tautology (1=1), which can be used to bypass authentication or extract data. The HTTP 500 status suggests that the server encountered an error while processing this request.

Log 6:



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 25, 2022, 11:34 AM	Firewall	167.99.169.17	48575	172.16.17.18	443	

```
Request URL:   https://172.16.17.18/search/?q=1%27%20ORDER%20BY%203--%2B
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   948
HTTP Response Status:   500
```

Request URL: https://172.16.17.18/search/?q=1%27%20ORDER%20BY%203--%2B

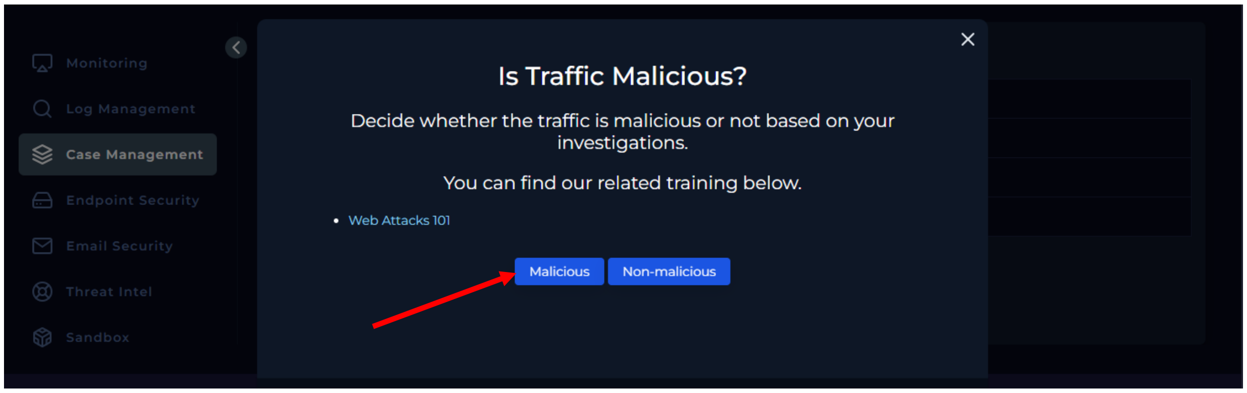
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
- Request Method: GET
- Device Action: Permitted
- HTTP Response Size: 948 bytes
- HTTP Response Status: 500 Internal Server Error

Explanation: This entry shows a GET request with an SQL Injection payload (' ORDER BY 3--). The ORDER BY clause is often used in SQL Injection attacks to gather information about the database structure. The HTTP 500 response indicates an error in processing, which may be related to the server's handling of the SQL Injection.

Detection:

Threat Intelligence Results

Playbook Inquiry: Is the Traffic Malicious?



Is Traffic Malicious?

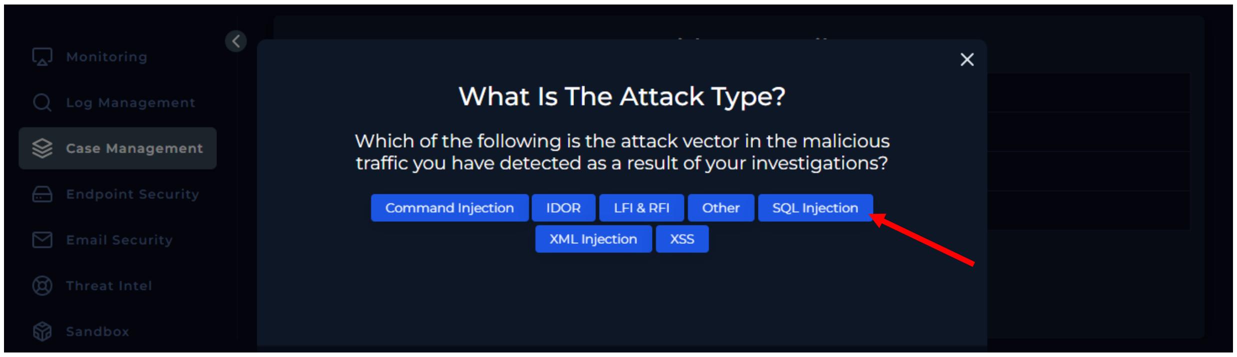
Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

- Web Attacks 101

Conclusion: Based on our thorough investigation, we have classified the traffic as malicious. (IP)

What kind of attack is this?

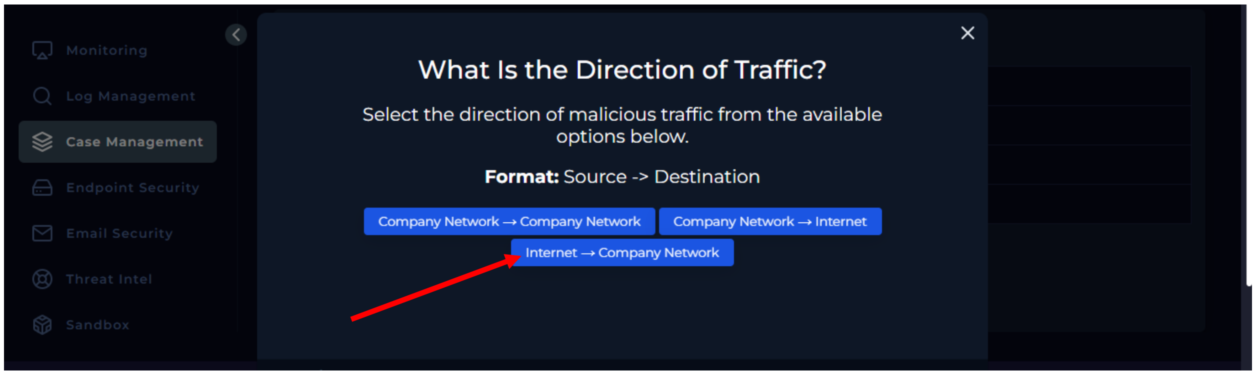


What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

Determination: Based on our analysis, the attack vector identified in the detected malicious traffic is SQL Injection.

Playbook Question: What Is the Direction of Traffic?



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

Response: The direction of the malicious traffic is identified as Internet to Company Network.

Rationale:

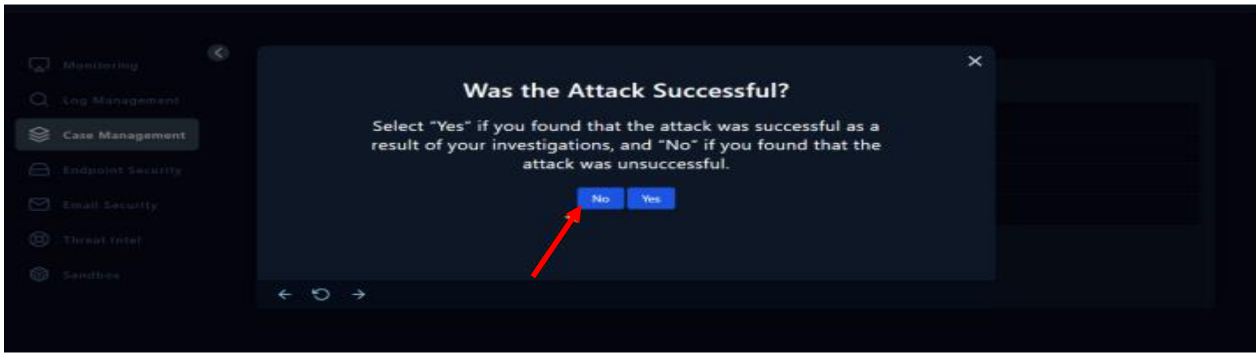
- Destination Address: 172.16.17.18
- Source Address: 167.99.169.17

Analysis:

- Source Address (167.99.169.17): This IP is external, originating from outside the internal network.
- Destination Address (172.16.17.18): This IP is within a private IP range, typically used for internal networks.

Based on the above information, the traffic direction is from an external source to an internal destination, indicating an external attack targeting the company network.

Playbook Question: Was the Attack Successful?



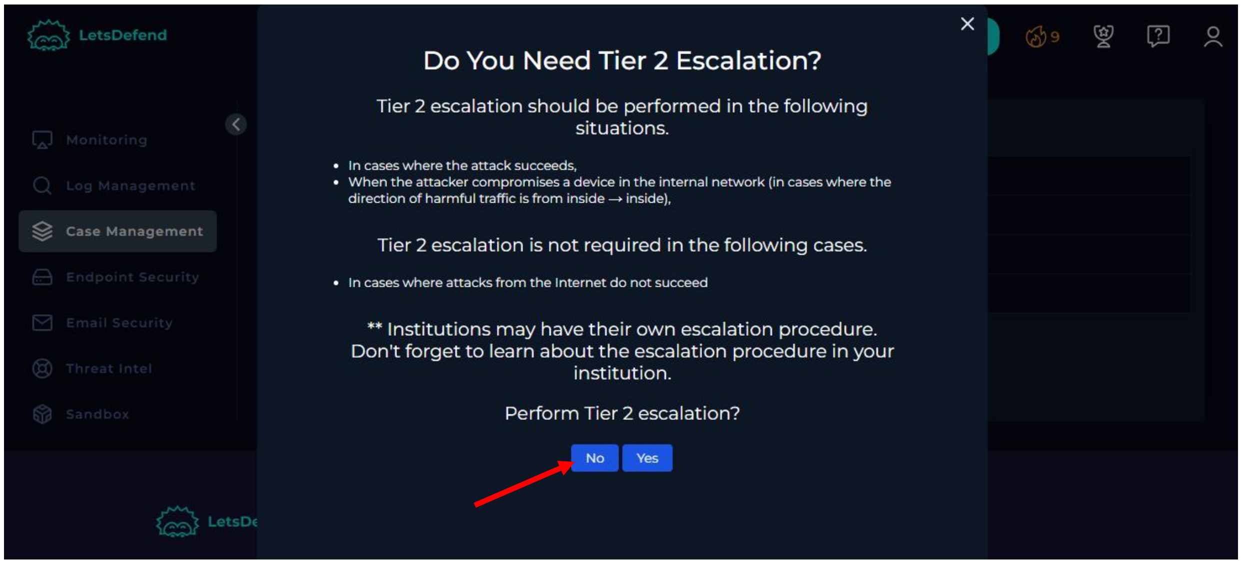
Was the Attack Successful?

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.

Response: No

Rationale: Based on a thorough analysis of the logs, we conclude that the attack was unsuccessful.

Playbook Question: Do You Need Tier 2 Escalation?



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

Response: No

Rationale: Based on our prior analysis, the attacks were unsuccessful. The server's consistent failure to process the SQL Injection attempts, as evidenced by multiple 500 Internal Server Error responses, indicates that the threat was effectively mitigated at this level. Therefore, escalation to Tier 2 is not necessary at this time

Conclusion

The incident related to Event ID 115, triggered by Rule SOC165— "Possible SQL Injection Payload Detected"—highlights a significant attempt to compromise our network security. An attacker from the external IP address 167.99.169.17 executed multiple SQL injection attempts against our web server at 172.16.17.18. These attempts aimed to exploit potential vulnerabilities in the web application's database by injecting malicious SQL code, which could have led to unauthorized access or data retrieval.

Threat Intelligence and Attack Analysis

Through a comprehensive investigation, we found that the source IP address (167.99.169.17) has a known history of malicious activity. This was verified via Virus Total and AbuseIPDB, which flagged the IP for phishing and other suspicious behaviors. Virus Total confirmed detections from BitDefender and G-Data, while AbuseIPDB reported over 15,000 incidents linked to this IP, indicating a pattern of malicious behavior associated with DigitalOcean LLC, a recognized hosting provider.

Despite the sophistication of the SQL injection attacks, they ultimately proved unsuccessful. The attacker employed various payloads, such as "OR 1=1" and "ORDER BY 3--," typically used to bypass authentication and retrieve database information. However, the server consistently responded with a 500 Internal Server Error to all injection attempts, indicating that the malicious payloads were not processed correctly. This consistent response underscores the effectiveness of our web application's input validation and query handling mechanisms in thwarting the attack.

Attack Impact and Mitigation

The repeated failures of these SQL injection attempts confirm that no unauthorized access or data breach occurred. The robust handling of malicious requests by the server prevented the exploitation of any vulnerabilities, demonstrating the strength of our security measures. Effective input validation and error handling played a critical role in neutralizing the threat.

This incident serves as a validation of our monitoring and response capabilities. The swift detection of suspicious traffic, combined with a thorough investigation, ensured that the threat was promptly identified and contained without impacting our network or data. It emphasizes the importance of maintaining strong security protocols and regularly updating them to counter evolving threats.

Escalation Decision

Based on our analysis, there is no need for escalation to Tier 2 support. The attack was unsuccessful, and our server's defense mechanisms effectively neutralized the threat at the current level. The consistent 500 Internal Server Error responses indicate that the threat has been fully mitigated, and no further investigation or remediation is required at this time.

Final Thoughts

This incident reinforces the effectiveness of our layered security approach and the resilience of our web application's defenses. The successful prevention of this SQL injection attack highlights the robustness of our network against external threats. Moving forward, continuous monitoring, regular security updates, and adherence to best practices will remain essential to maintaining this high level of protection.