Official incident report

Event ID: 115

Rule Name: SOC165 - Possible SQL Injection Payload Detected

Made By

LinkedIn: Engineer. Ahmed Mansour

Link: https://www.linkedin.com/in/ahmed-mansour-5631b5323/

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.

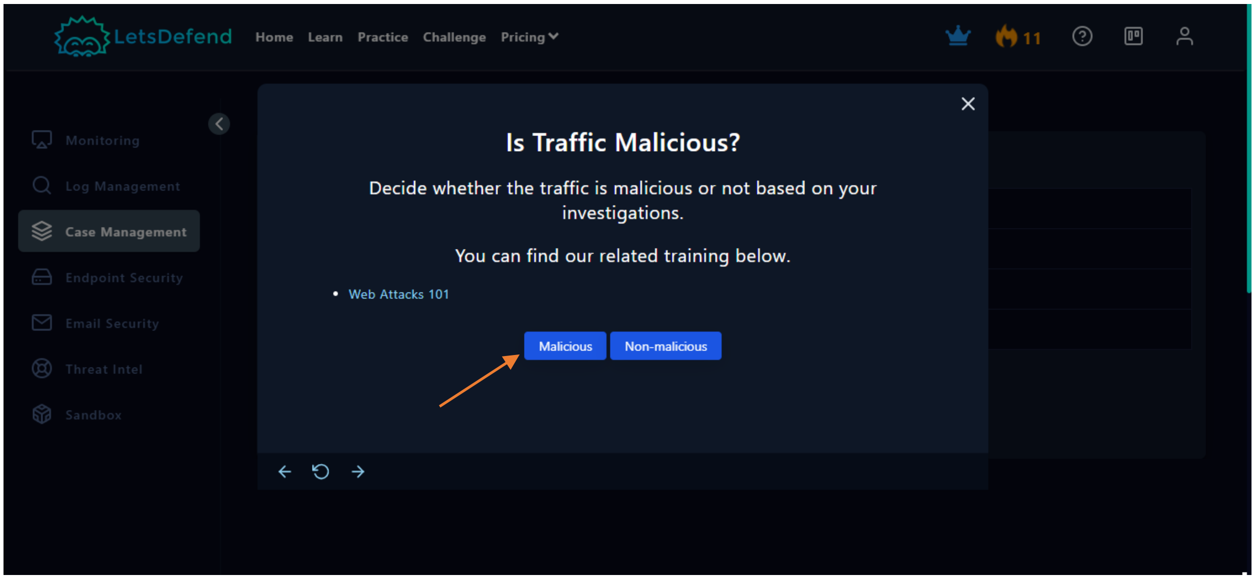
• Destination **Address (172.16.17.18)**: This IP address is within a private IP range (typically used for internal networks). Based on this information, it appears to be an **internal to external attack** since the source address originates from an internal network, and the destination address is external.

This is an external attack.

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.

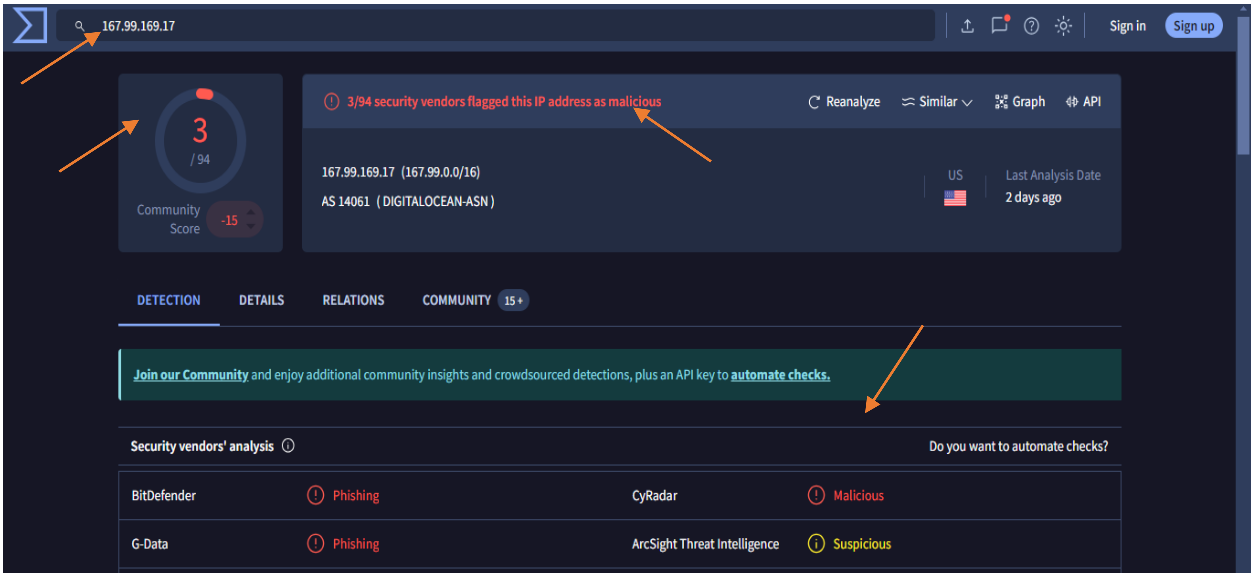
You can find our related training below.

- Web Attacks 101

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

Investigation Details:

1. **Threat Intelligence Analysis**
   - **VirusTotal**
     - We conducted a search for the source IP `167.99.169.17` on VirusTotal. The analysis revealed:
       - **BitDefender**: Flagged as Phishing and Malicious
       - **G-Data**: Flagged as Phishing and Suspicious
     - Link to VirusTotal results
     - See attached screenshot for detailed results



3/94 security vendors flagged this IP address as malicious

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

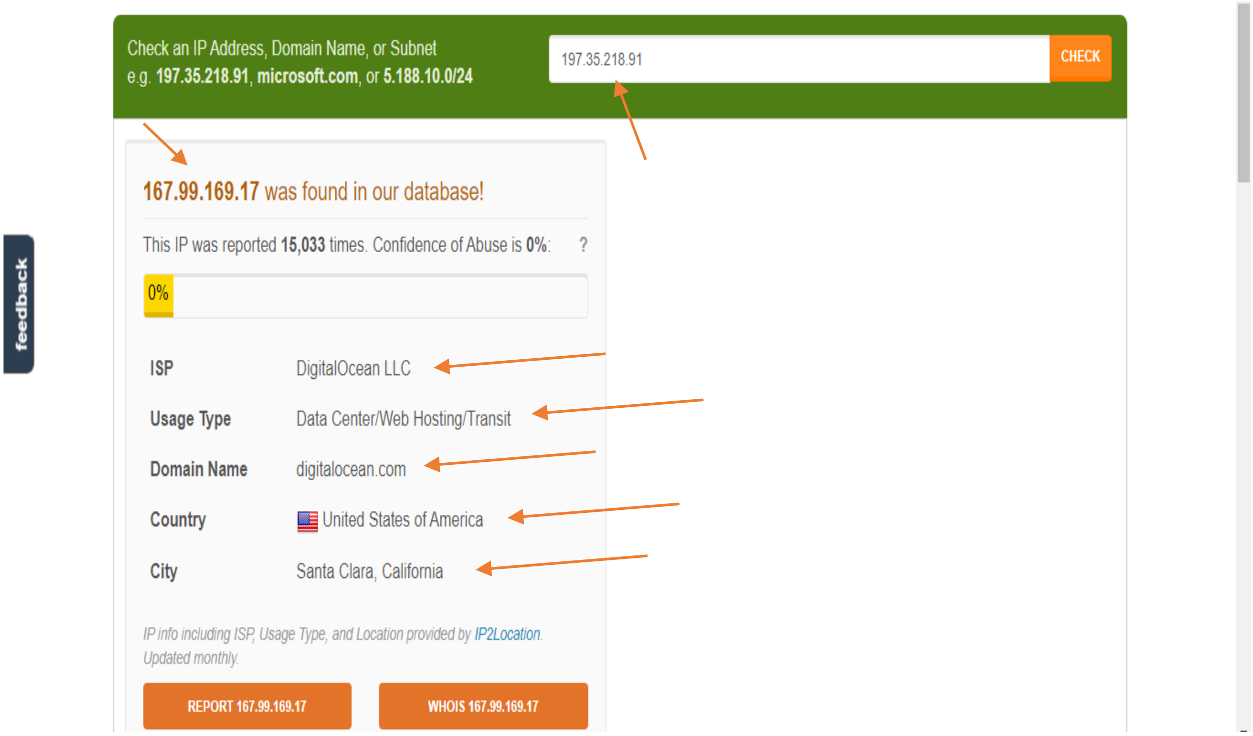
Last Analysis Date
2 days ago

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

Security vendors' analysis

BitDefender	Phishing	CyRadar	Malicious
G-Data	Phishing	ArcSight Threat Intelligence	Suspicious

- **AbuseIPDB**
  - The IP `167.99.169.17` was checked on AbuseIPDB. The findings include:
    - The IP has been reported 15,033 times.
    - ISP: DigitalOcean LLC
    - Usage Type: Data Center/Web Hosting/Transit
    - Domain Name: digitalocean.com
    - Location: Santa Clara, California, USA
  - Link to AbuseIPDB results
  - See attached screenshot for detailed results



Check an IP Address, Domain Name, or Subnet
e.g. **197.35.218.91**, **microsoft.com**, or **5.188.10.0/24**

197.35.218.91

167.99.169.17 was found in our database!

This IP was reported **15,033** times. Confidence of Abuse is **0%**: ?

0%

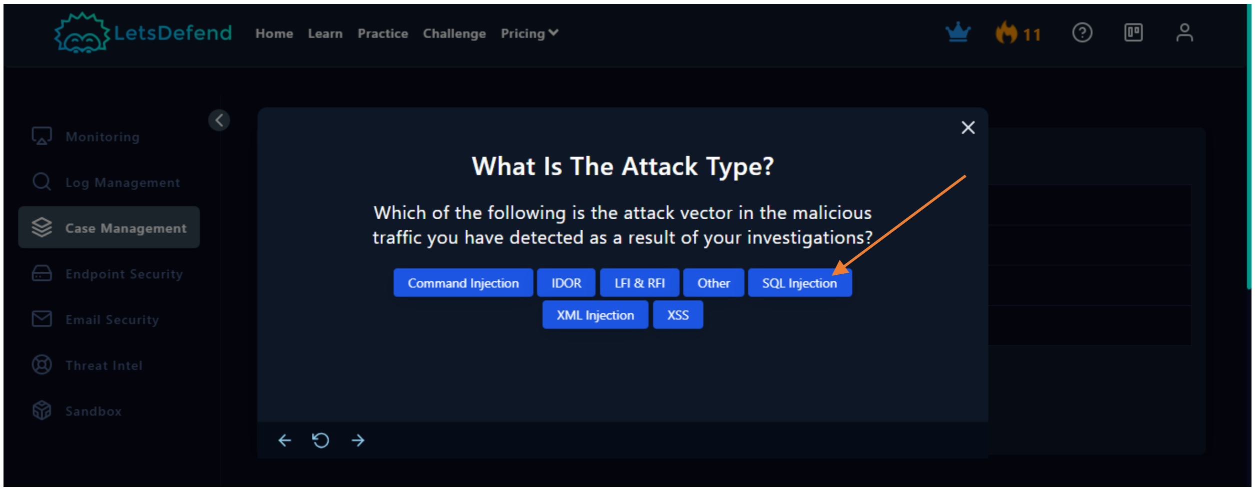
ISP	DigitalOcean LLC
Usage Type	Data Center/Web Hosting/Transit
Domain Name	digitalocean.com
Country	United States of America
City	Santa Clara, California

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

Based on our investigation, the source IP `167.99.169.17` has been identified as malicious. The VirusTotal analysis shows detections by BitDefender and G-Data, indicating phishing and suspicious activity. Additionally, AbuseIPDB records extensive reports of this IP, confirming its association with potentially harmful activity. Therefore, we conclude that the traffic from this IP is malicious and warrants further action.

Analysis:

Playbook Inquiry: What Is the Attack Type?



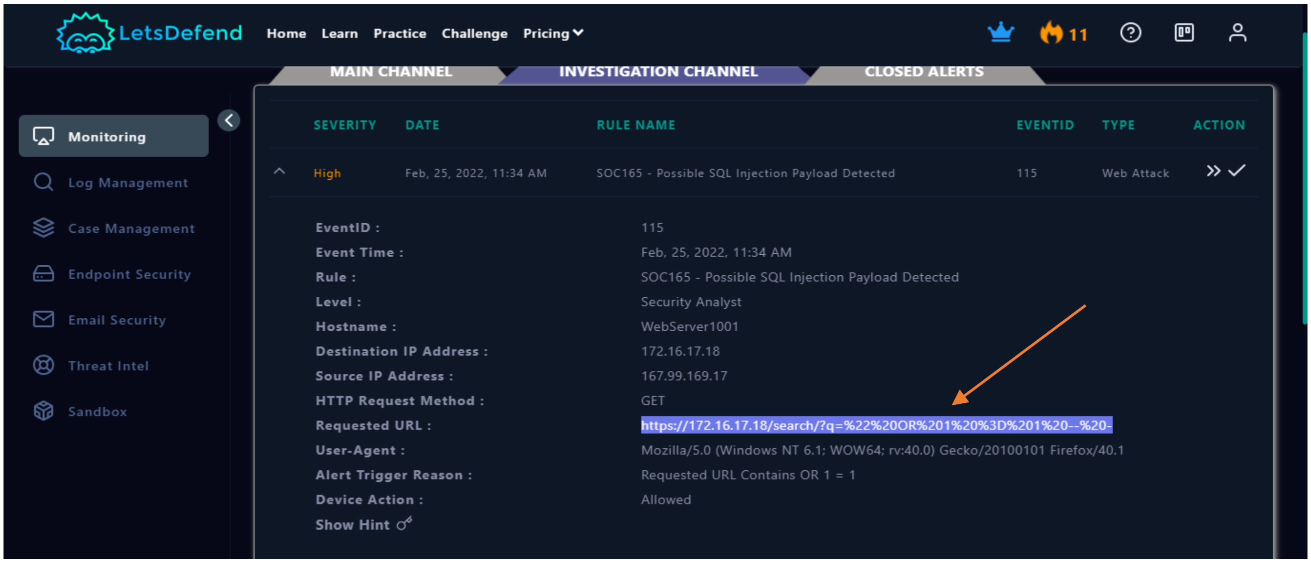
What Is The Attack Type?

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.

Rationale: To confirm this, we will decode the URL step by step to elucidate the nature and purpose of the SQL Injection.

URL Decoding



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

1. **Original Encoded URL**: `https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-`
2. **Decode `%22`**: This is the URL-encoded form of `"` (double quote).
3. **Decode `%20`**: This represents a space character.
4. **Decode `%3D`**: This is the URL-encoded form of `=` (equals sign).
5. **Decode `%2D`**: This represents `-` (hyphen).

   After decoding, the URL is:

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

Decoded URL Breakdown

- **Base URL**: `https://172.16.17.18/search/`
- **Query Parameter**: `q=" OR 1 = 1 -- -`

Explanation of the Payload

- `"`: This starts a string in SQL.
- `OR 1 = 1`: This is a classic SQL Injection payload that always evaluates to true, potentially allowing bypass of authentication or manipulation of query logic.
- `--`: This denotes a comment in SQL, which means the rest of the query is ignored.

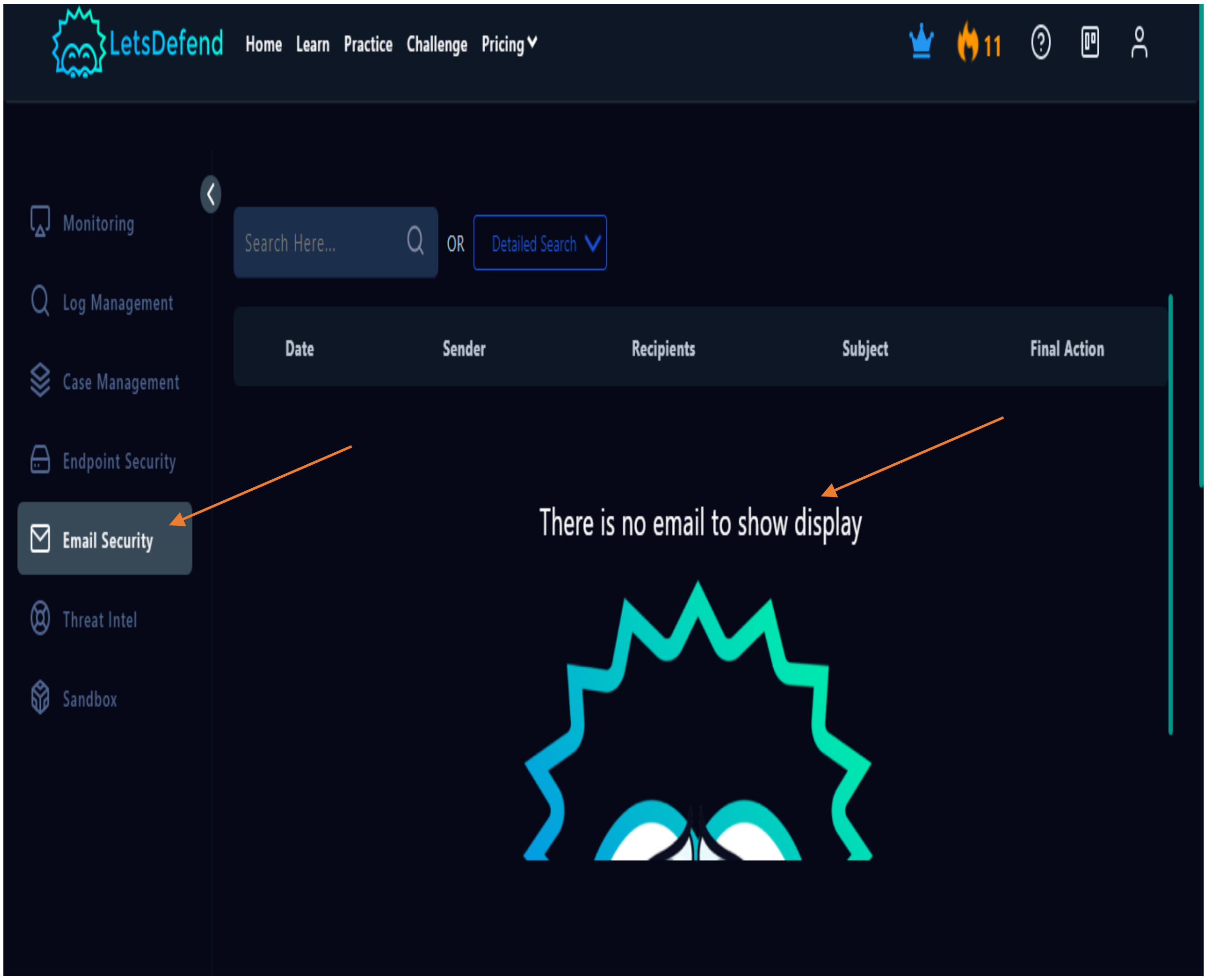
Playbook Inquiry: Is the Malicious Traffic Resulting from a Planned Test?

Conclusion: We have determined that the malicious traffic is not the result of a planned test.

Evidence:

- We reviewed all emails from the Email Security section.
- We investigated the details, including Hostname, Destination IP Address, and Source IP Address, and found no evidence of a planned test.

Supporting Documentation: Please refer to the attached photo for verification.

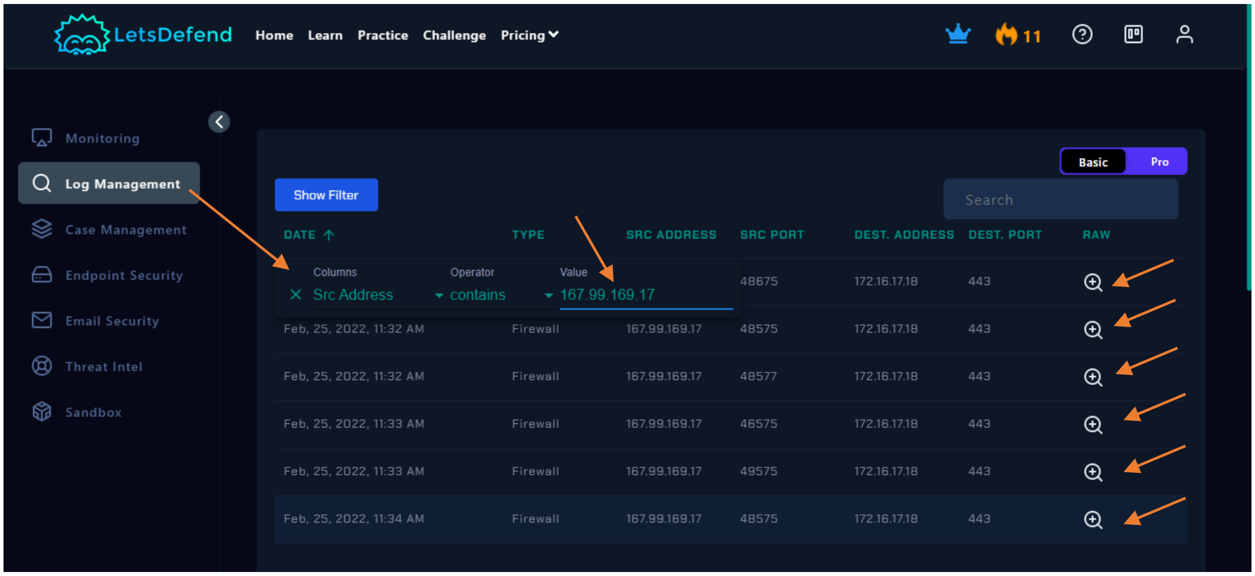


Date	Sender	Recipients	Subject	Final Action

There is no email to show display

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.



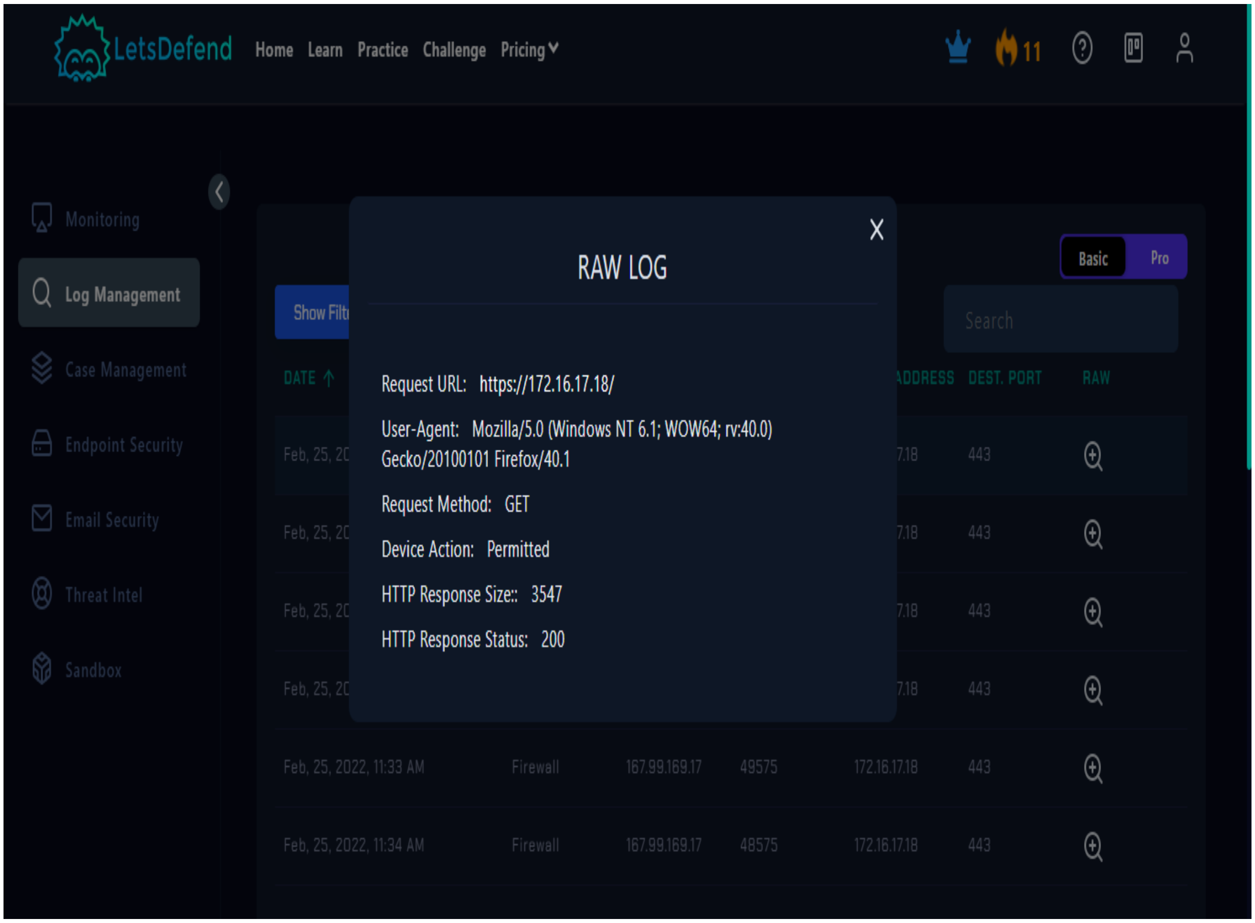
Columns: Src Address, Operator: contains, Value: 167.99.169.17

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
			48675	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, 11:32 AM	Firewall	167.99.169.17	48577	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	
Feb, 25, 2022, 11:34 AM	Firewall	167.99.169.17	48575	172.16.17.18	443	

Log Details:

Date	Type	Source Address	Source Port	Destination Address	Destination Port
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	48575	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, 11:33 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
Feb 25, 2022, 11:34 AM	Firewall	167.99.169.17	48575	172.16.17.18	443

Log 1:



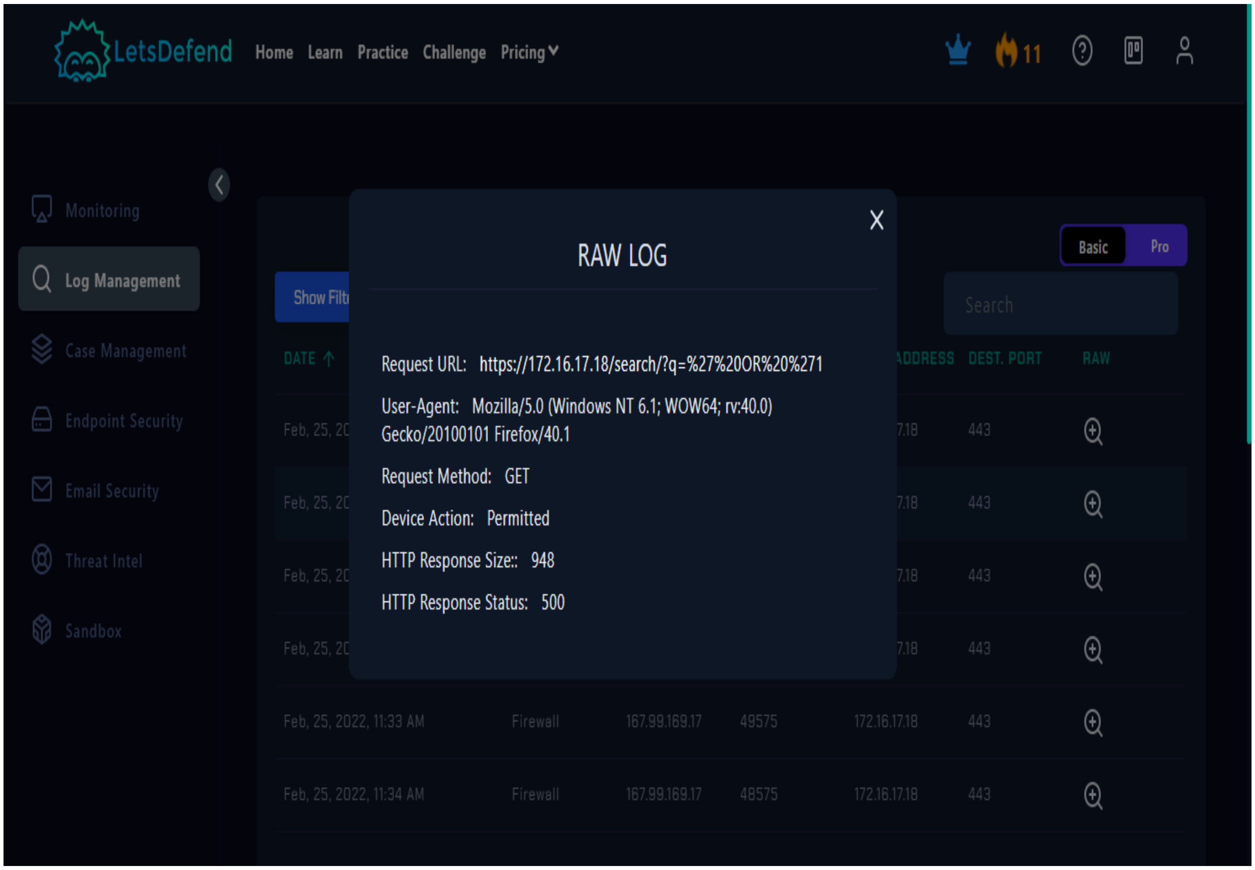
```
Request URL:   https://172.16.17.18/
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   3547
HTTP Response Status:   200
```

```
DATE ↑                                                  ADDRESS      DEST. PORT   RAW
Feb, 25, 2022, 11:33 AM   Firewall   167.99.169.17   49575   172.16.17.18   443
Feb, 25, 2022, 11:34 AM   Firewall   167.99.169.17   48575   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 2:



RAW LOG

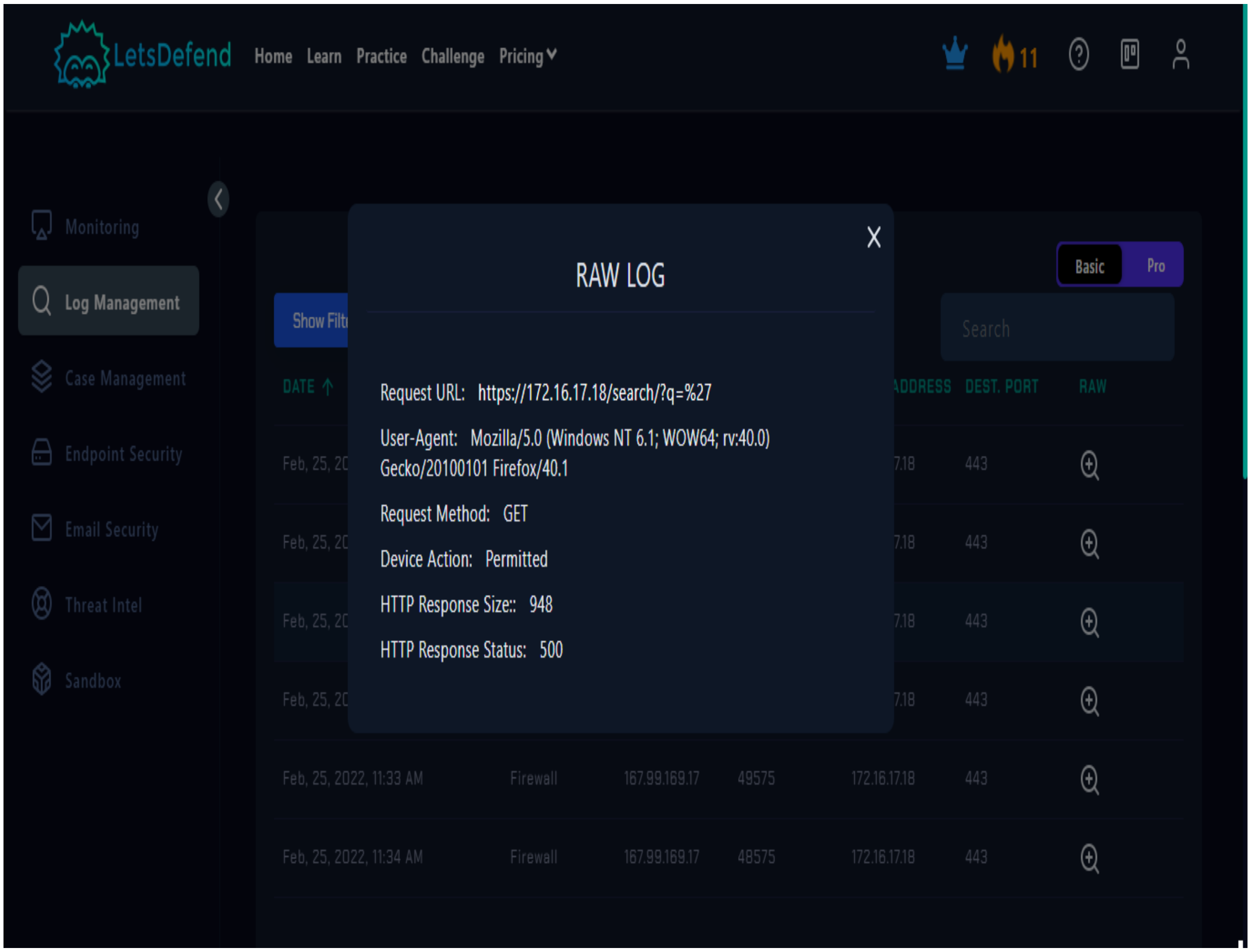
```
Request URL:   https://172.16.17.18/search/?q=%27%20OR%20%271
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   948
HTTP Response Status:   500
```

```
Feb, 25, 2022, 11:33 AM   Firewall   167.99.169.17   49575   172.16.17.18   443
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=%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 3:



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

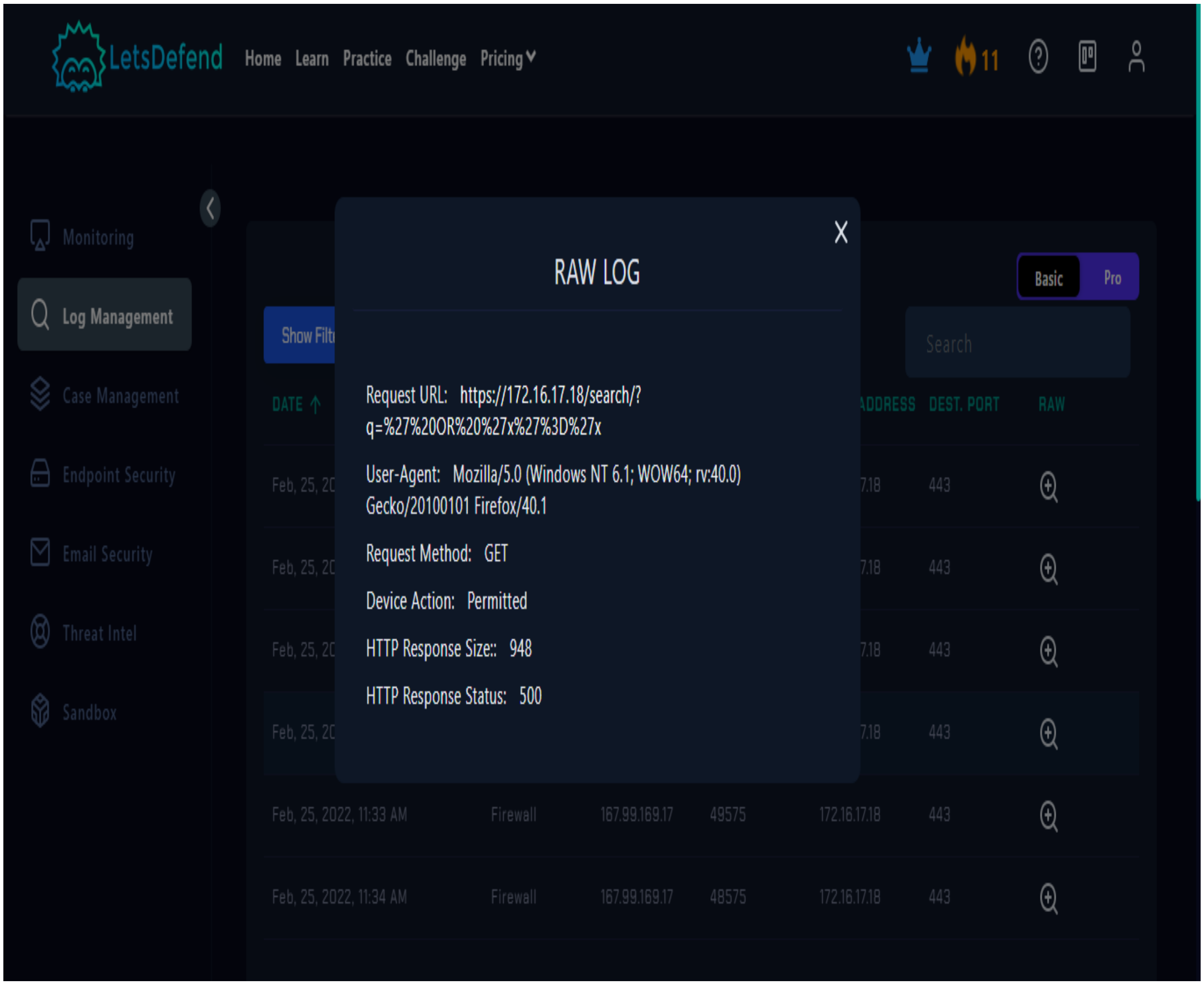
Feb, 25, 2022, 11:33 AM Firewall 167.99.169.17 49575 172.16.17.18 443

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=%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:



RAW LOG

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

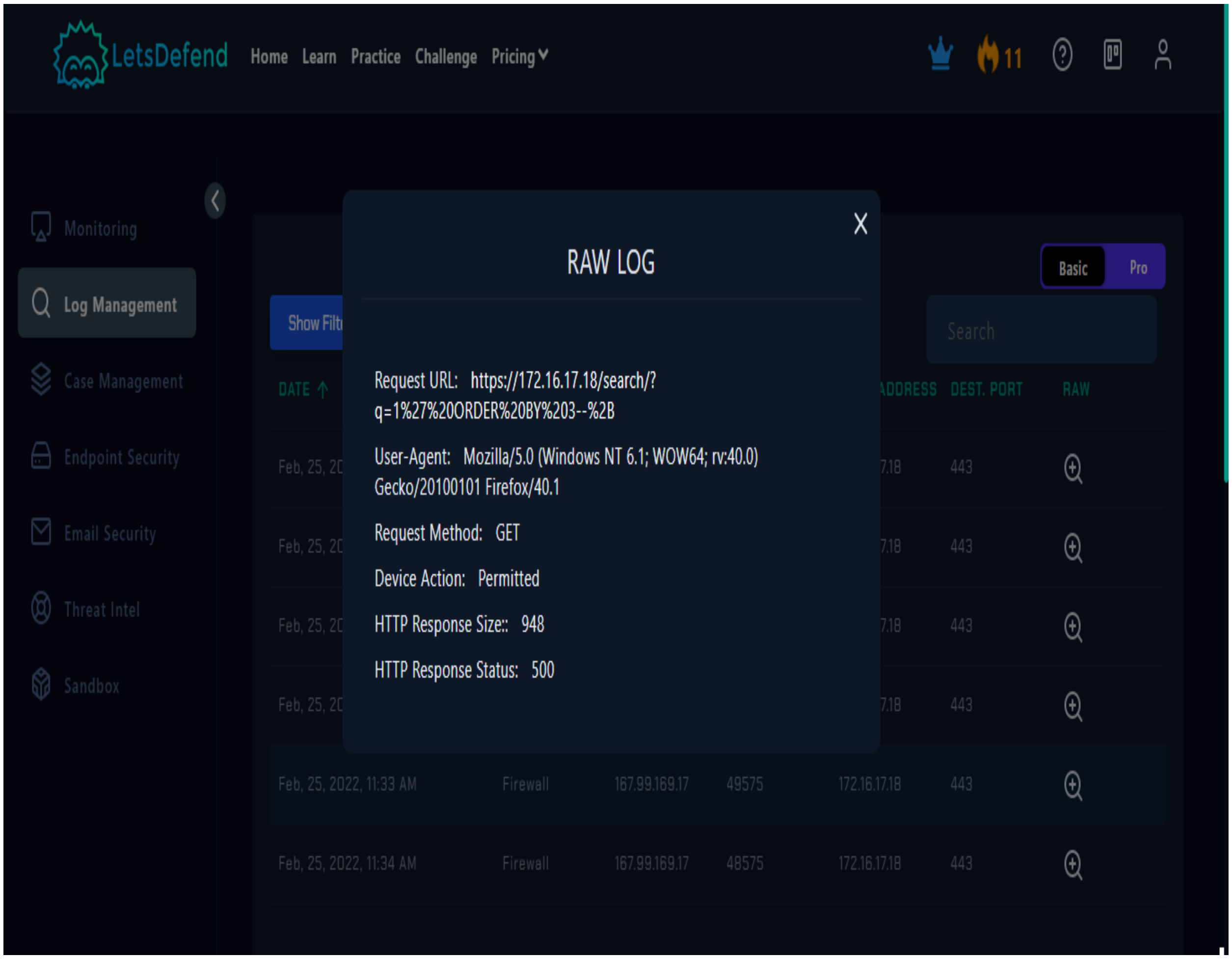
HTTP Response Status: 500

```
Feb, 25, 2022, 11:33 AM   Firewall   167.99.169.17   49575   172.16.17.18   443
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=%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:



RAW LOG

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

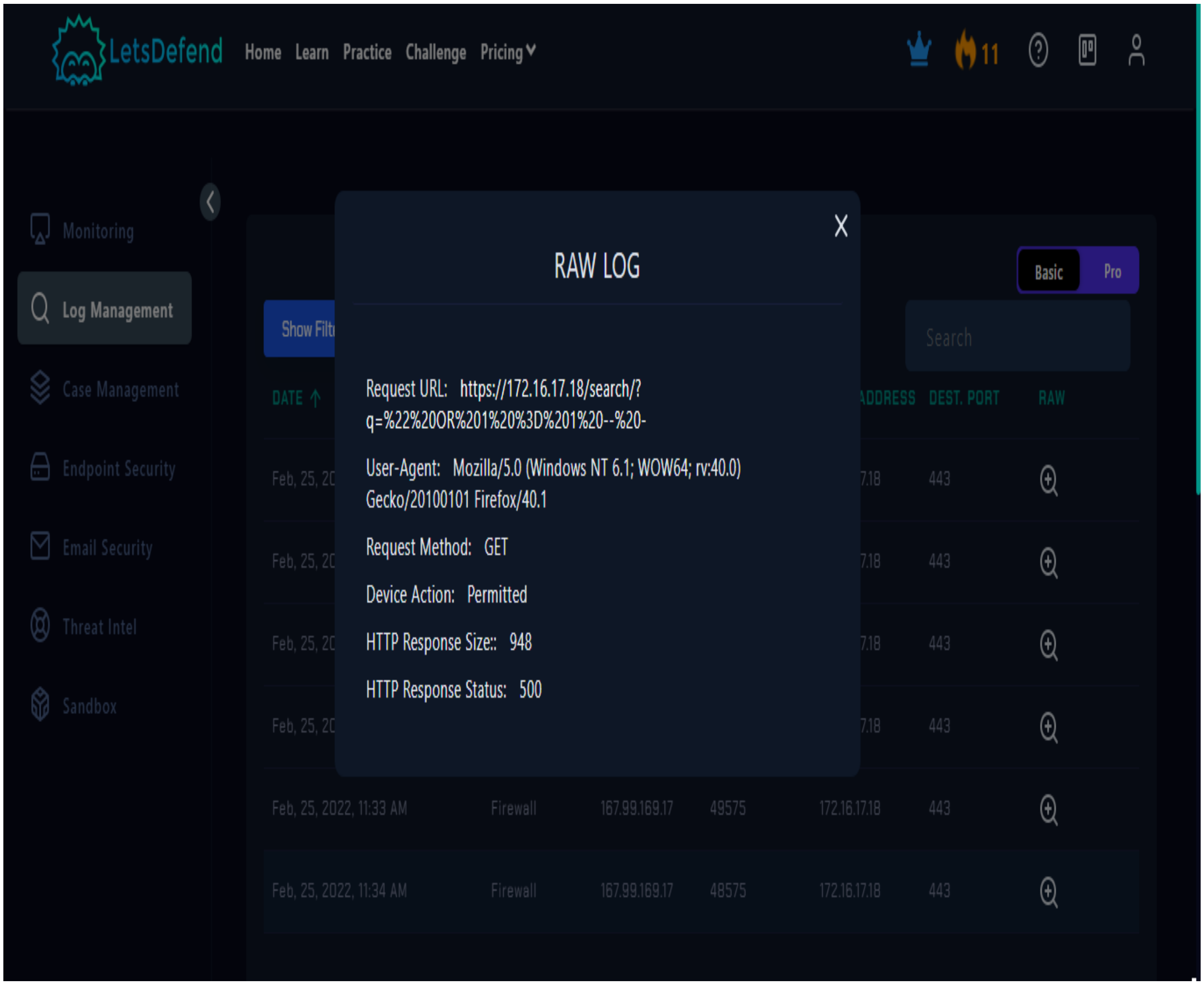
HTTP Response Status: 500

```
DATE ↑                                                  ADDRESS  DEST. PORT  RAW
Feb, 25, 20                                             7.18     443
Feb, 25, 20                                             7.18     443
Feb, 25, 20                                             7.18     443
Feb, 25, 20                                             7.18     443
Feb, 25, 2022, 11:33 AM  Firewall  167.99.169.17  49575  172.16.17.18  443
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 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.

Log 6:



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

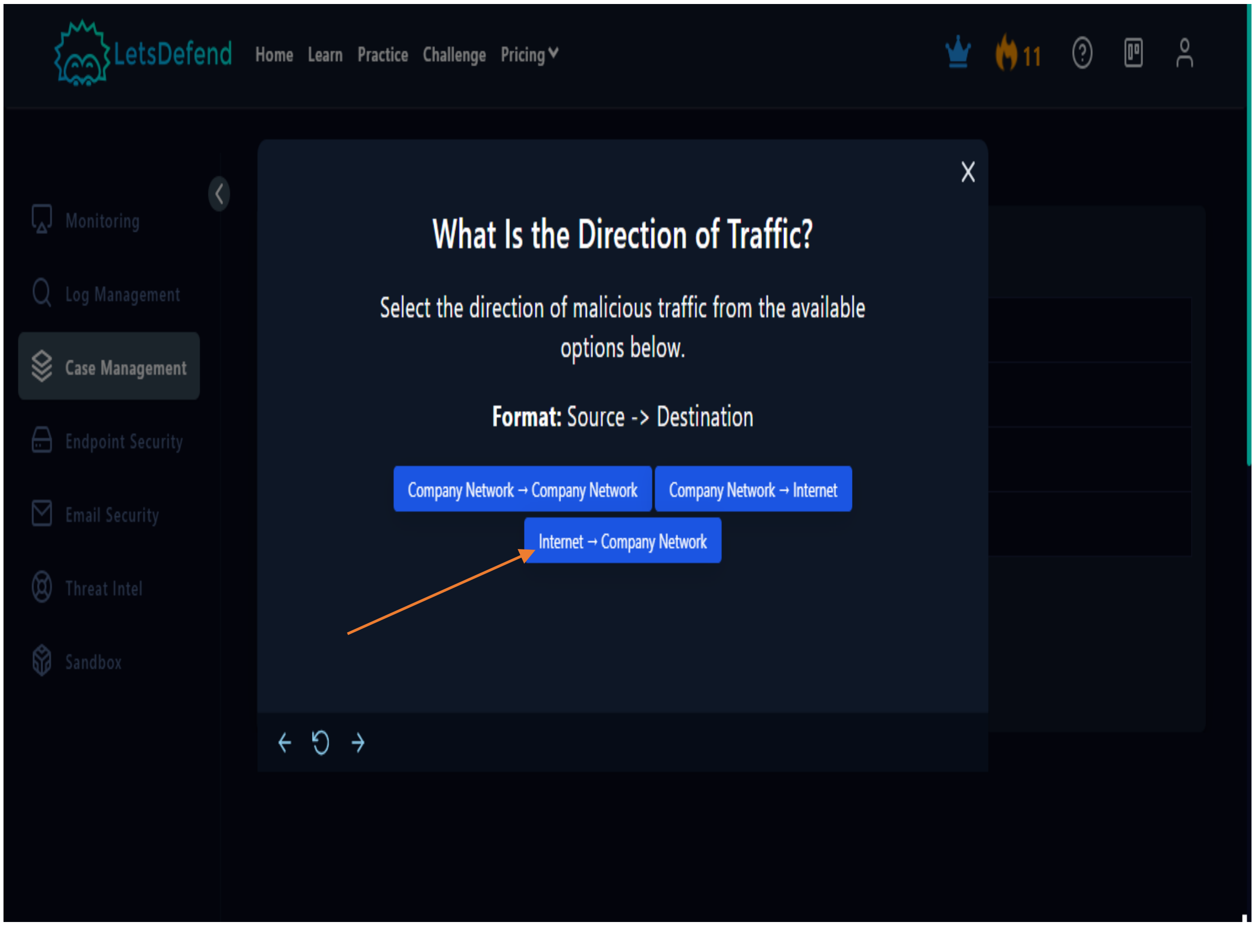
HTTP Response Status: 500

```
Feb, 25, 20                                              7.18         443
Feb, 25, 20                                              7.18         443
Feb, 25, 20                                              7.18         443
Feb, 25, 20                                              7.18         443
Feb, 25, 2022, 11:33 AM   Firewall   167.99.169.17   49575   172.16.17.18   443
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=%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.

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:

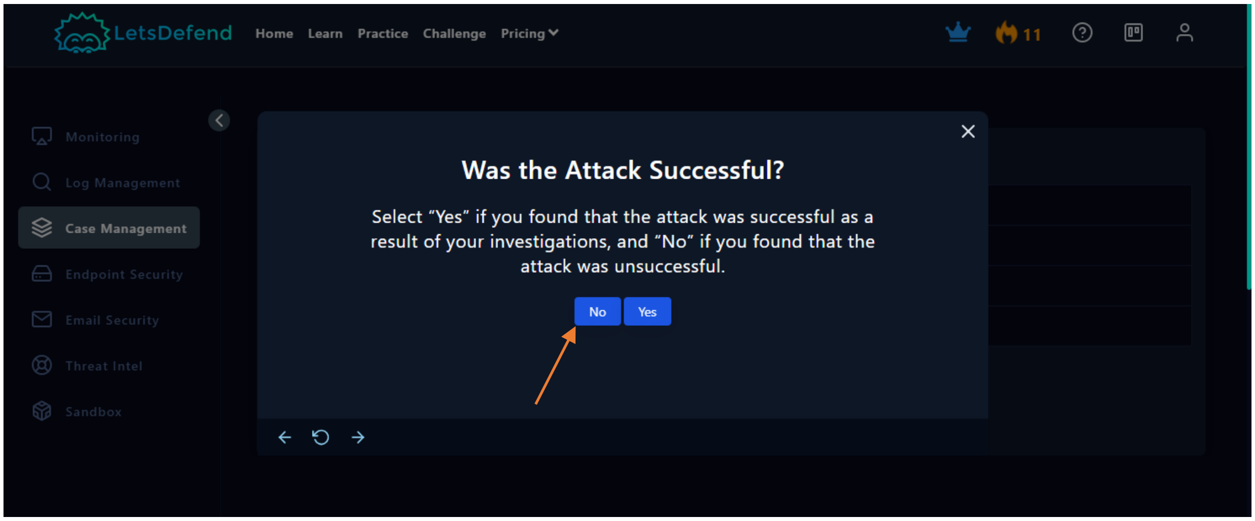
- **Destination Address:** 172.16.17.18
- **Source Address:** 167.99.169.17

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. Here is the detailed breakdown:

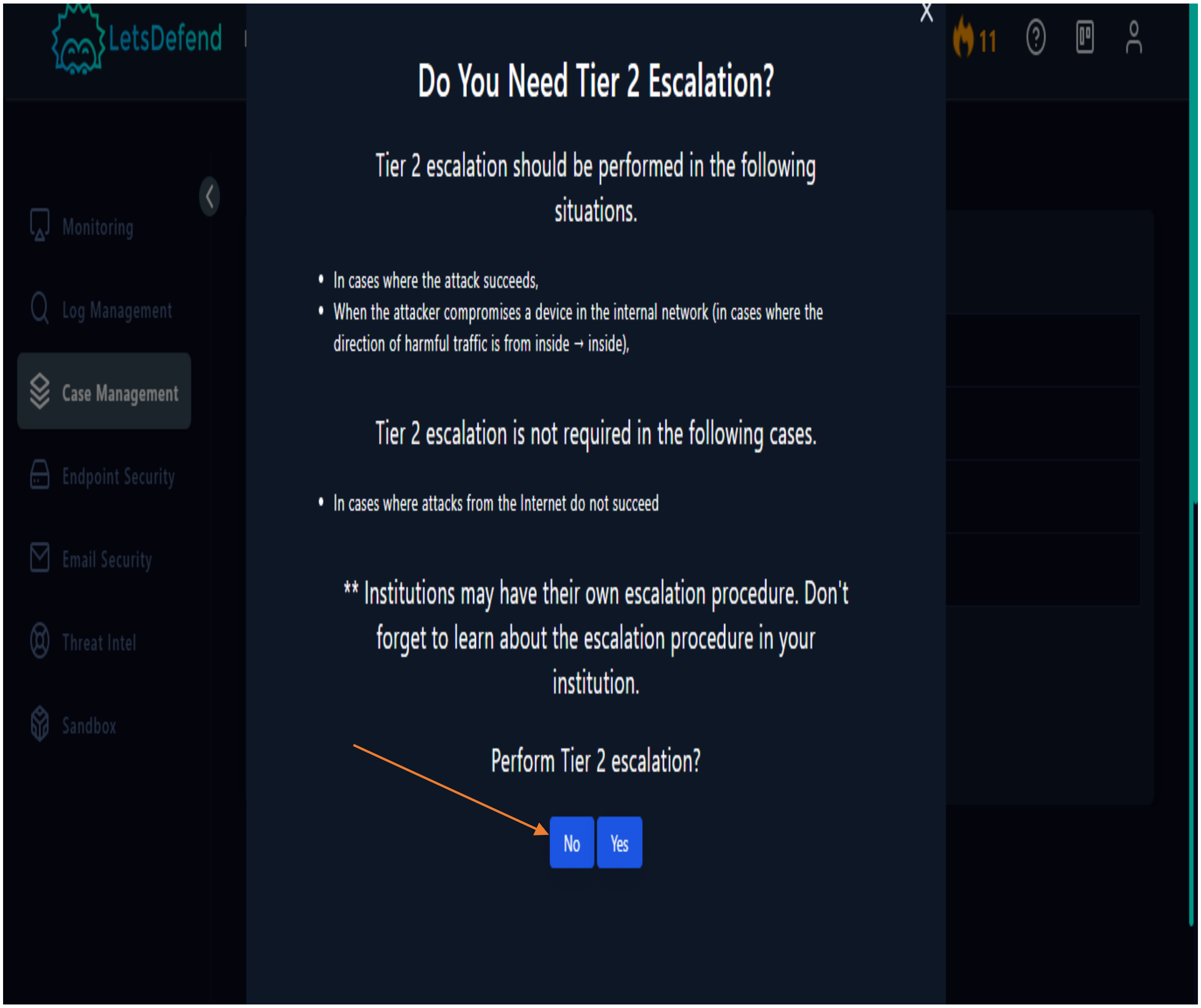
Log Analysis:

- **Log 1:**
  - **Request URL:** `https://172.16.17.18/`
  - **Response Status:** `200 OK`
  - **Explanation:** This entry shows a standard request to the root URL. The `200 OK` status indicates successful processing with no evidence of malicious activity.
- **Log 2:**
  - **Request URL:** `https://172.16.17.18/search/?q=%27%20OR%20%271`
  - **Response Status:** `500 Internal Server Error`
  - **Explanation:** The SQL Injection attempt with payload `%27%20OR%20%271` caused the server to return a `500 Internal Server Error`, indicating improper handling of the payload.
- **Log 3:**
  - **Request URL:** `https://172.16.17.18/search/?q=%27`
  - **Response Status:** `500 Internal Server Error`
  - **Explanation:** The single quote payload (`%27`), a common SQL Injection vector, also triggered a `500 Internal Server Error`, reflecting the server's inability to process this injection.
- **Log 4:**
  - **Request URL:** `https://172.16.17.18/search/?q=%27%20OR%20%27x%27%3D%27x`

    - **Response Status:** `500 Internal Server Error`
    - **Explanation:** This more complex payload attempted to manipulate query logic. The `500 Internal Server Error` suggests failure in processing due to improper handling.
- **Log 5:**
    - **Request URL:** `https://172.16.17.18/search/?q=1%27%20ORDER%20BY%203--%2B`
    - **Response Status:** `500 Internal Server Error`
    - **Explanation:** The payload included `ORDER BY`, used to extract database information. The `500 Internal Server Error` indicates that this attempt did not succeed.
- **Log 6:**
    - **Request URL:** `https://172.16.17.18/search/?q=%22%20OR%201%20%3D%201%20--%20-`
    - **Response Status:** `500 Internal Server Error`
    - **Explanation:** The payload designed to create a tautology (`1=1`) for bypassing authentication resulted in a `500 Internal Server Error`, showing the server encountered an issue processing the request.

The consistent occurrence of `500 Internal Server Error` responses across all SQL Injection attempts indicates that the attacks were not successful. The server’s failure to process these payloads effectively suggests robust input handling and query execution mechanisms in place to mitigate such attacks.

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?

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 involving Event ID 115, triggered by Rule SOC165 - "Possible SQL Injection Payload Detected," represents a notable attempt to compromise our network's security. The attacker, originating from the external IP address 167.99.169.17, executed multiple SQL Injection attempts against the web server at 172.16.17.18. These SQL Injection attacks aimed to exploit potential vulnerabilities in the web application's database by inserting malicious SQL code, which could have resulted in unauthorized access or data retrieval.

Threat Intelligence and Attack Analysis:

A thorough investigation revealed that the source IP address (167.99.169.17) has a known malicious history. Verified through VirusTotal and AbuseIPDB, this IP was flagged for phishing and suspicious activities. VirusTotal 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 known hosting provider.

Despite the sophistication of the attack, it was ultimately unsuccessful. The attacker deployed various SQL Injection payloads designed to manipulate SQL queries and potentially gain unauthorized access to the database. The logs captured multiple SQL Injection attempts, including payloads like "OR 1=1" and "ORDER BY 3--", which are typically used to bypass authentication mechanisms and retrieve database information.

However, all these attempts failed to achieve their objectives. The server responded to each SQL Injection attempt with a 500 Internal Server Error, indicating that the injected payloads were not processed correctly. This consistent response across all logs suggests that the web application’s input validation and query handling mechanisms effectively mitigated the attack.

Attack Impact and Mitigation:

Given the repeated failure of the SQL Injection attempts, it is clear that the attack did not result in any unauthorized access or data breach. The server's consistent handling of the malicious requests prevented the attacker from exploiting any vulnerabilities. This demonstrates the strength of our security measures, particularly in terms of input validation and error handling, which played a critical role in neutralizing the threat.

The attack serves as a validation of our monitoring and response capabilities. The timely detection of the suspicious traffic, combined with a thorough investigation, ensured that the threat was identified and contained without any impact on the network or its data. This incident highlights the importance of maintaining strong security protocols and regularly updating them to defend against evolving threats.

Escalation Decision:

Based on the analysis, there is no need for escalation to Tier 2 support. The attack was unsuccessful, and the 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 underscores the effectiveness of our layered security approach and the robustness of our web application's defenses. The successful prevention of this SQL Injection attack reinforces our network's resilience against external threats. Moving forward, continuous monitoring, regular security updates, and adherence to best practices will remain essential in maintaining this high level of protection.