Official incident report

Event ID: 201

Rule Name: SOC239 - Remote Code Execution Detected in Splunk Enterprise

Table of contents

Event Details

Event ID:
201

Event Date and Time:
Nov, 21, 2023, 12:24 PM

Rule:
SOC239 - Remote Code Execution Detected in Splunk Enterprise

Level:
Security Analyst

Description:
Detected a malicious XSLT upload in Splunk Enterprise with the potential to trigger remote code execution.

Network Information Details

Destination Address:
172.16.20.13

Source Address:
180.101.88.240

External / Internal Attack:
External

Detection:

Threat Intelligence Results

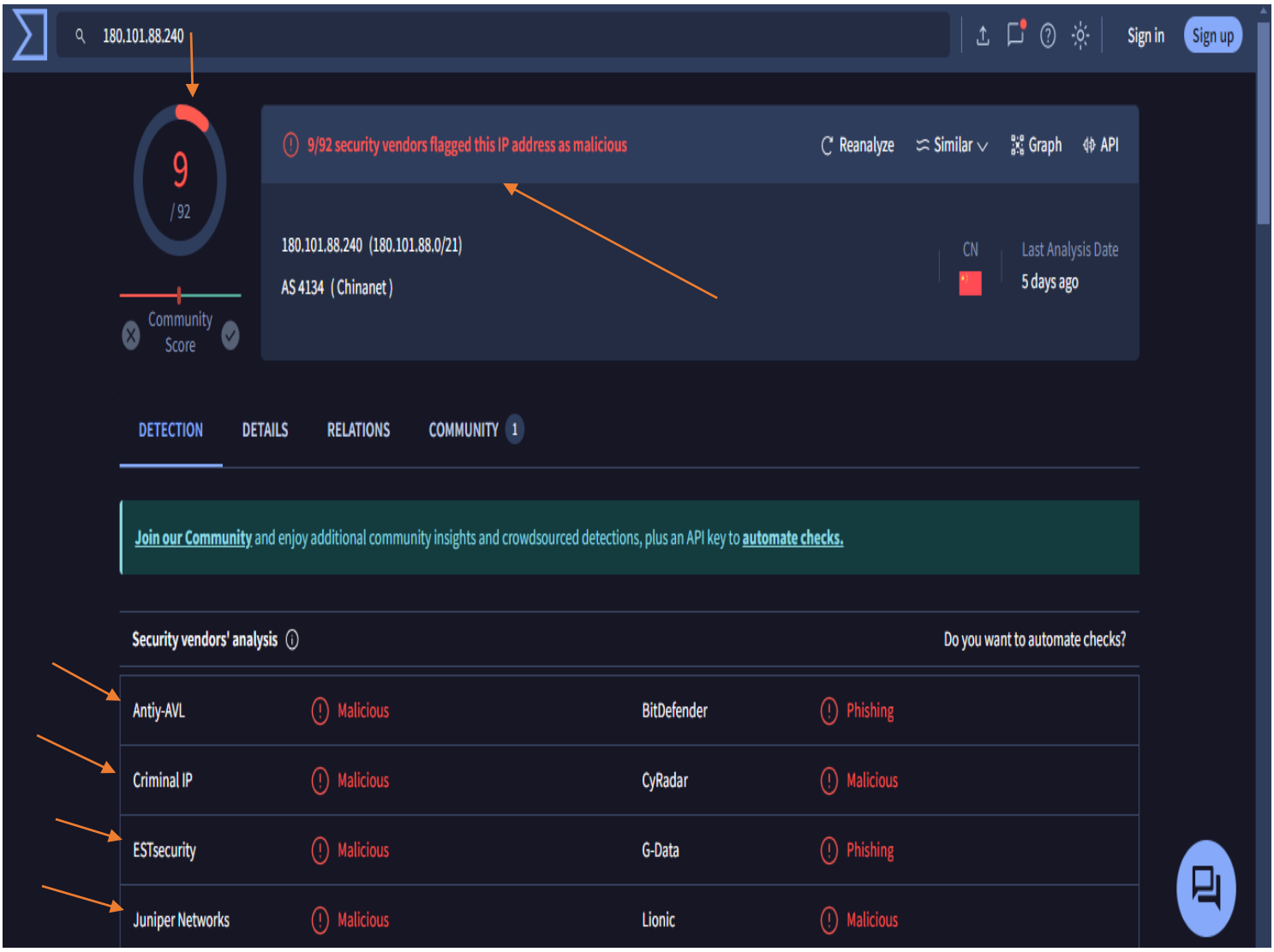
www.virustotal.com

IP Address Scan Results:

- **Malicious Classification:** 10 out of 93 security vendors have flagged this IP address as malicious. Notable security vendors that have classified the IP as malicious include Antiy-AVL, Criminal IP, CyRadar, ESTsecurity, Juniper Networks, and Lionic.
- **Phishing Involvement:** BitDefender and G-Data have identified the IP address as associated with phishing activities.
- **Suspicious Activity:** AlphaSOC has labeled the IP address as suspicious.

  Reference link: https://www.virustotal.com/gui/ip-address/180.101.88.240/detection

  For further reference, please see the attached photo



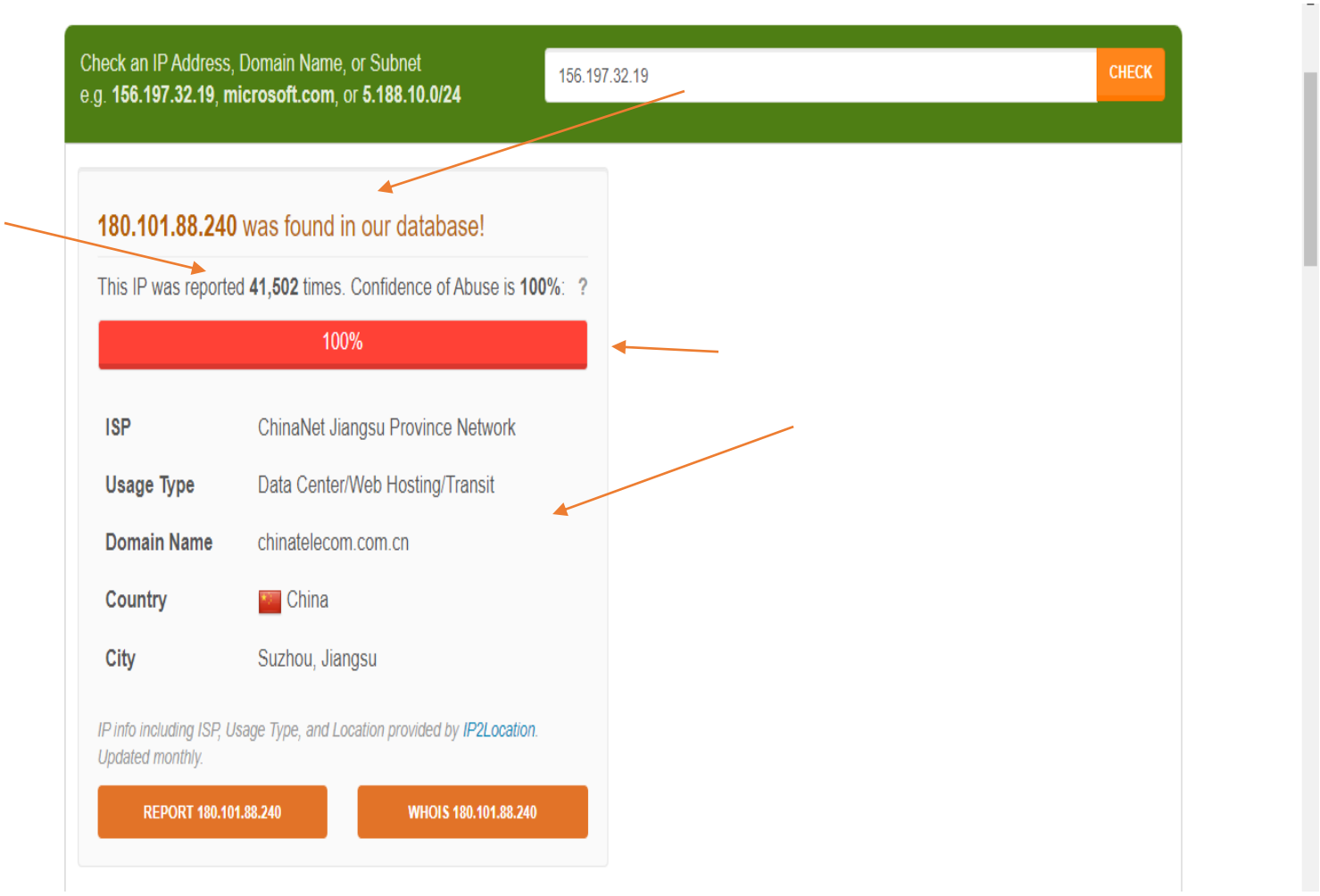
www.abuseipdb.com

- **IP Address:** 180.101.88.240
- **Abuse Reports:** The IP address has been reported 41,502 times with a confidence level of 100% for abuse.
- **ISP:** ChinaNet Jiangsu Province Network
- **Usage Type:** Data Center/Web Hosting/Transit
- **Domain Name:** chinatelecom.com.cn

- **Location:** Suzhou, Jiangsu, China

Reference link: https://www.abuseipdb.com/check/180.101.88.240

For further reference, please see the attached photo

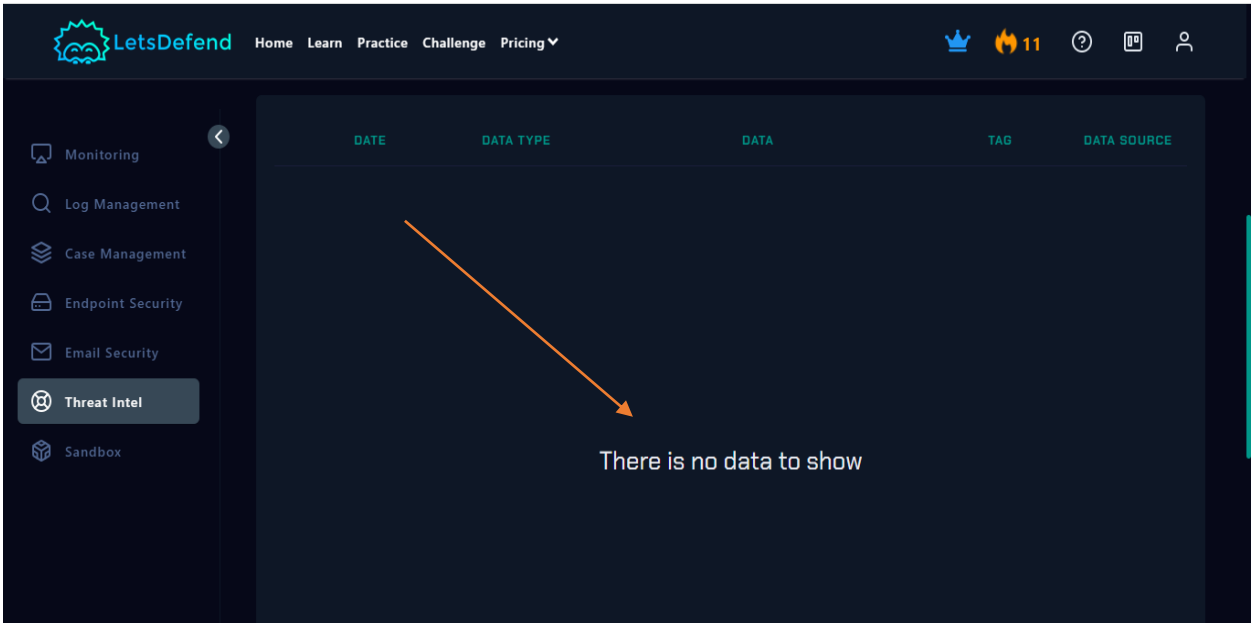


https://app.letsdefend.io/

No results or further details were found for this IP address.

Reference link: https://app.letsdefend.io/threath-intelligence-feed

For further reference, please see the attached photo



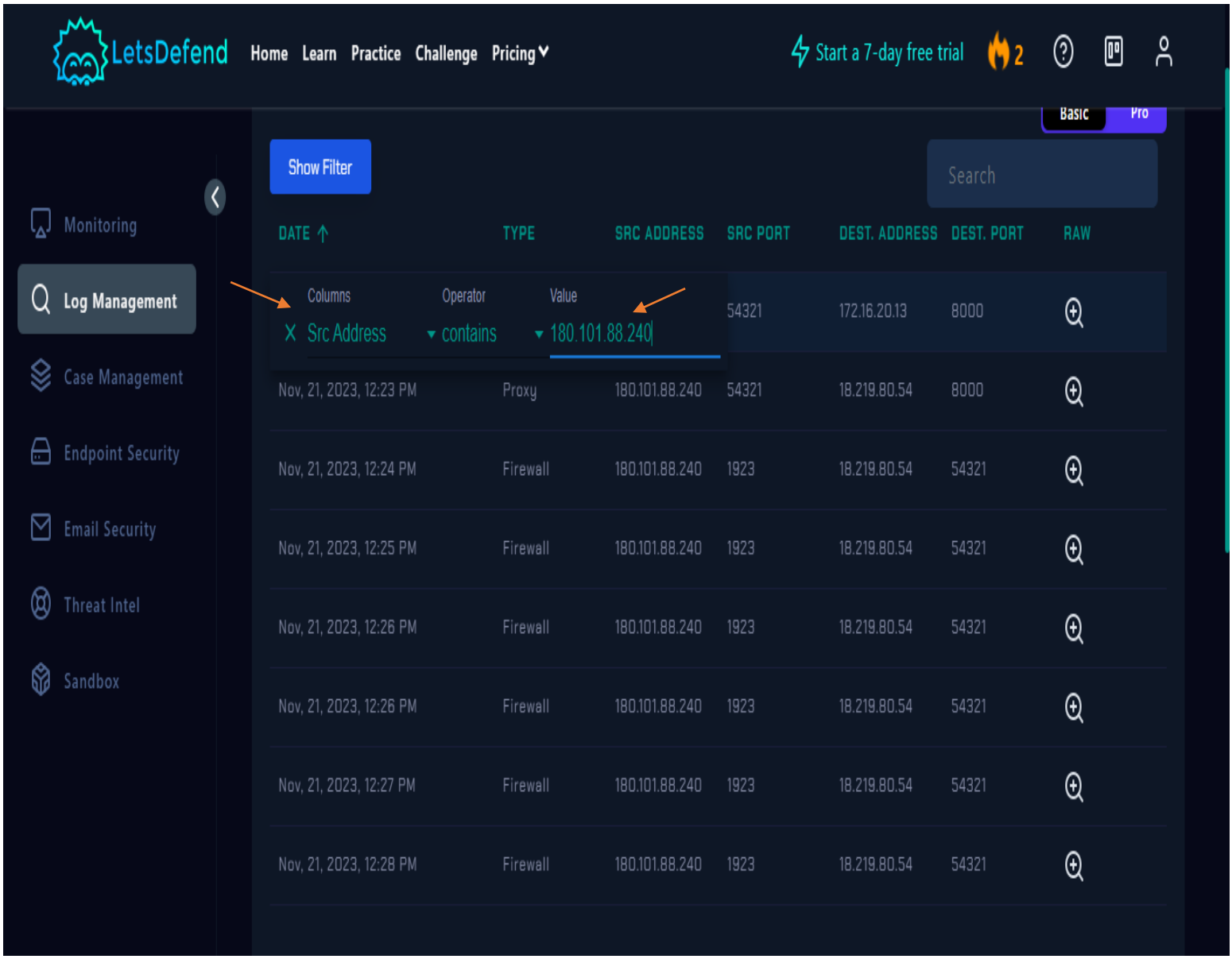
The IP address 180.101.88.240 is widely flagged as malicious by several security vendors and has a substantial number of abuse reports. Given the high confidence level of abuse and multiple vendor reports indicating malicious activity, this IP address should be treated as a significant security concern. It is advisable to block this IP and monitor any associated activity to safeguard your network.

Analysis:

Log Management

In the log management section, I applied a filter by selecting the source address field and entering the specific source IP.

For further reference, please see the attached photo

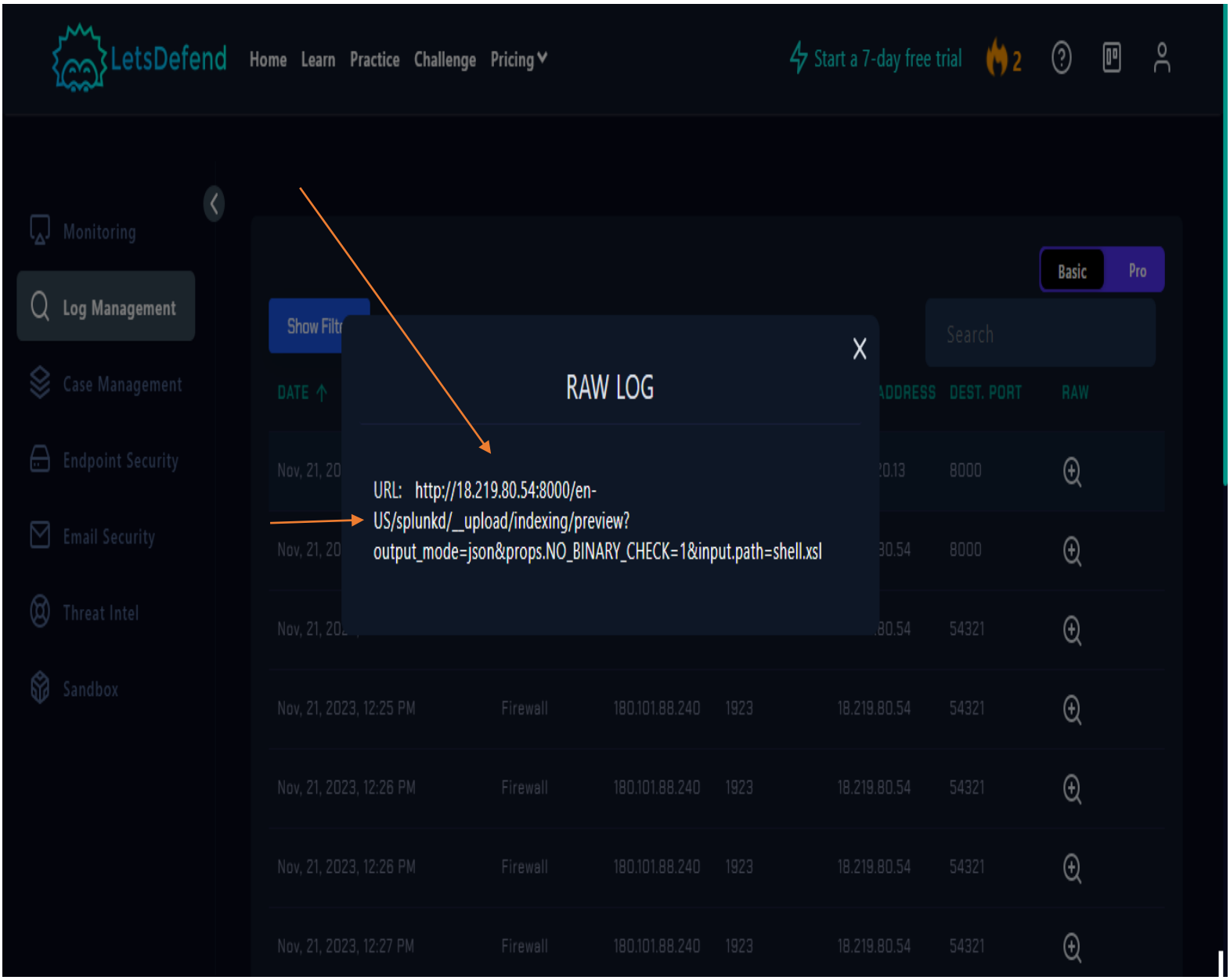


In the logs section, specifically under the proxy log type, the following URL was identified as the first result:

```
http://18.219.80.54:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xsl
```

This URL appears to be associated with a Splunk instance, potentially indicating an attempt to upload a file (`shell.xsl`) for indexing and preview purposes. The parameters suggest that the output is in JSON format, with a specific instruction to bypass binary checks. The presence of such a URL in proxy logs could indicate suspicious activity or a possible security concern, warranting further investigation.

For further reference, please see the attached photo



Detailed Analysis:

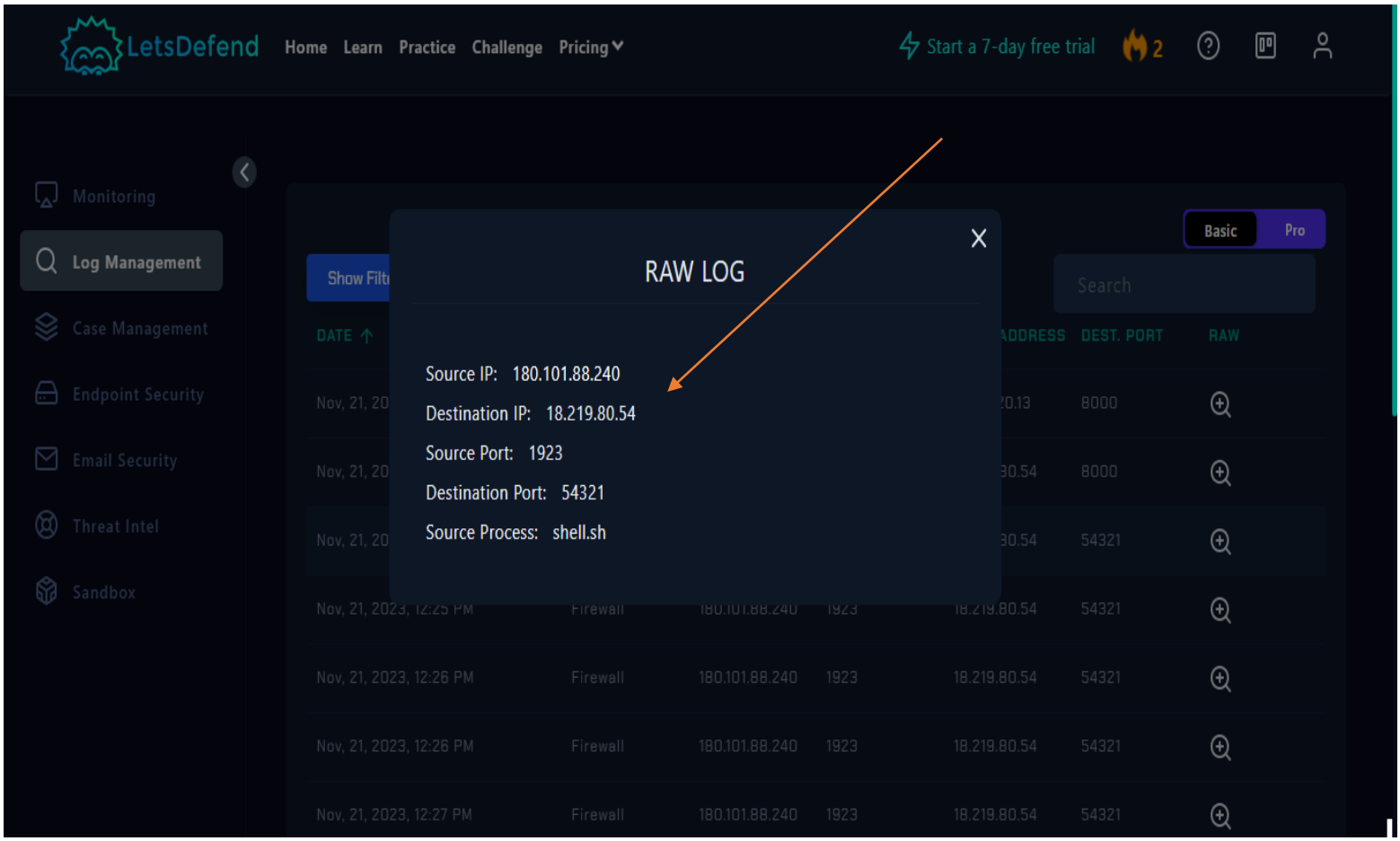
- **Source IP:** 180.101.88.240
- **Destination IP:** 18.219.80.54
- **Source Port:** 1923
- **Destination Port:** 54321
- **Source Process:** shell.sh

Explanation:

A network communication was observed originating from the IP address 180.101.88.240, targeting the IP address 18.219.80.54. The communication initiated from source port 1923 and was directed to destination port 54321. The process responsible for initiating this connection was identified as `shell.sh`. This process name suggests the use of a shell script, which could potentially indicate a scripted action or automation.

The presence of this specific communication and the involvement of a shell script (`shell.sh`) may warrant closer inspection, as it could indicate automated processes, potentially including malicious activity or system management tasks. Further investigation into the nature of this communication and the associated processes is recommended to ensure system security and integrity.

For further reference, please see the attached photo



In the log management section, a filter was applied to the source address field to pinpoint logs associated with a specific source IP address. During this analysis, a notable entry was identified in the proxy log type. The first result included the following URL: http://18.219.80.54:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xsl.

This URL seems to be linked to a Splunk instance, with parameters indicating an attempt to upload a file named "shell.xsl" for indexing and preview purposes. The output is specified to be in JSON format, and the `props.NO_BINARY_CHECK=1` parameter suggests bypassing binary checks. The occurrence of this URL in the proxy logs could point to suspicious activity or a potential security risk, necessitating a deeper investigation.

Detailed Analysis:

- **Source IP:** 180.101.88.240
- **Destination IP:** 18.219.80.54
- **Source Port:** 1923
- **Destination Port:** 54321
- **Source Process:** shell.sh

Explanation:

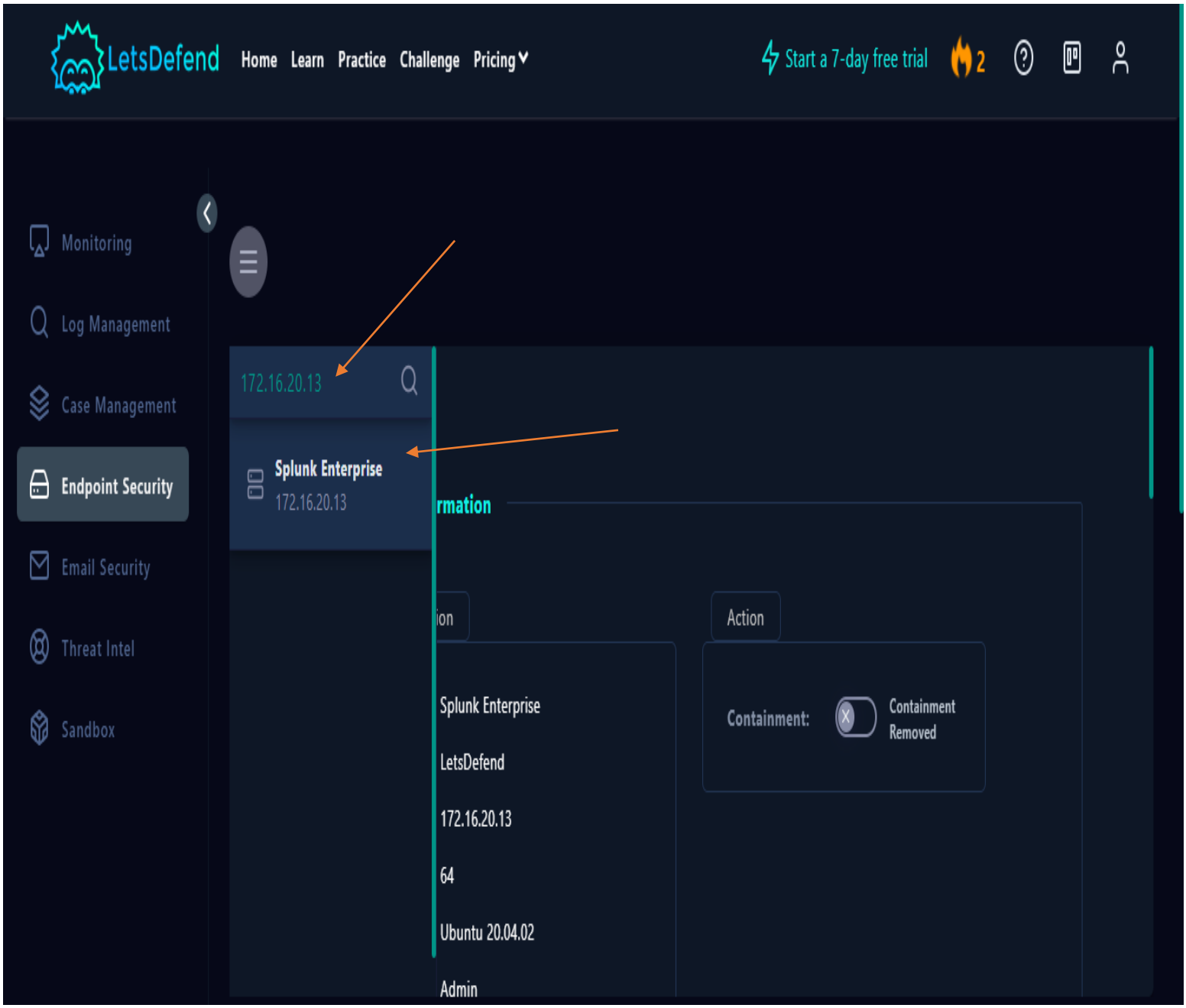
A network communication was detected, originating from IP address 180.101.88.240 and targeting IP address 18.219.80.54. This communication began from source port 1923 and was directed to destination port 54321. The initiating process was identified as "shell.sh," indicating the execution of a shell script. The use of a shell script suggests a scripted or automated action, which could be benign or indicative of malicious intent.

Given the context, the presence of this communication, particularly involving a shell script, raises potential security concerns. It is advisable to conduct a thorough investigation to determine the intent and nature of this activity, ensuring the security and integrity of the system.

Endpoint Security

I entered the attacker's IP address to review details including processes, network activity, terminal history, and browser history.

For further reference, please see the attached photo



Based on the terminal commands observed, the following actions were taken:

System Enumeration:

- `cat /etc/os-release`: Retrieved operating system details.
- `vim --version`: Checked the version of Vim, potentially to verify its availability for editing files.
- `sudo --version`: Checked the version of sudo to understand the system's sudo configuration.
- `ls --color=auto`: Listed files in the directory with color coding.

Navigating to Splunk Scripts:

- `cd /opt/splunk/bin/scripts/`: Navigated to the directory containing Splunk scripts.
- `cat shell.sh`: Displayed the contents of the script "shell.sh," possibly to review or modify it.

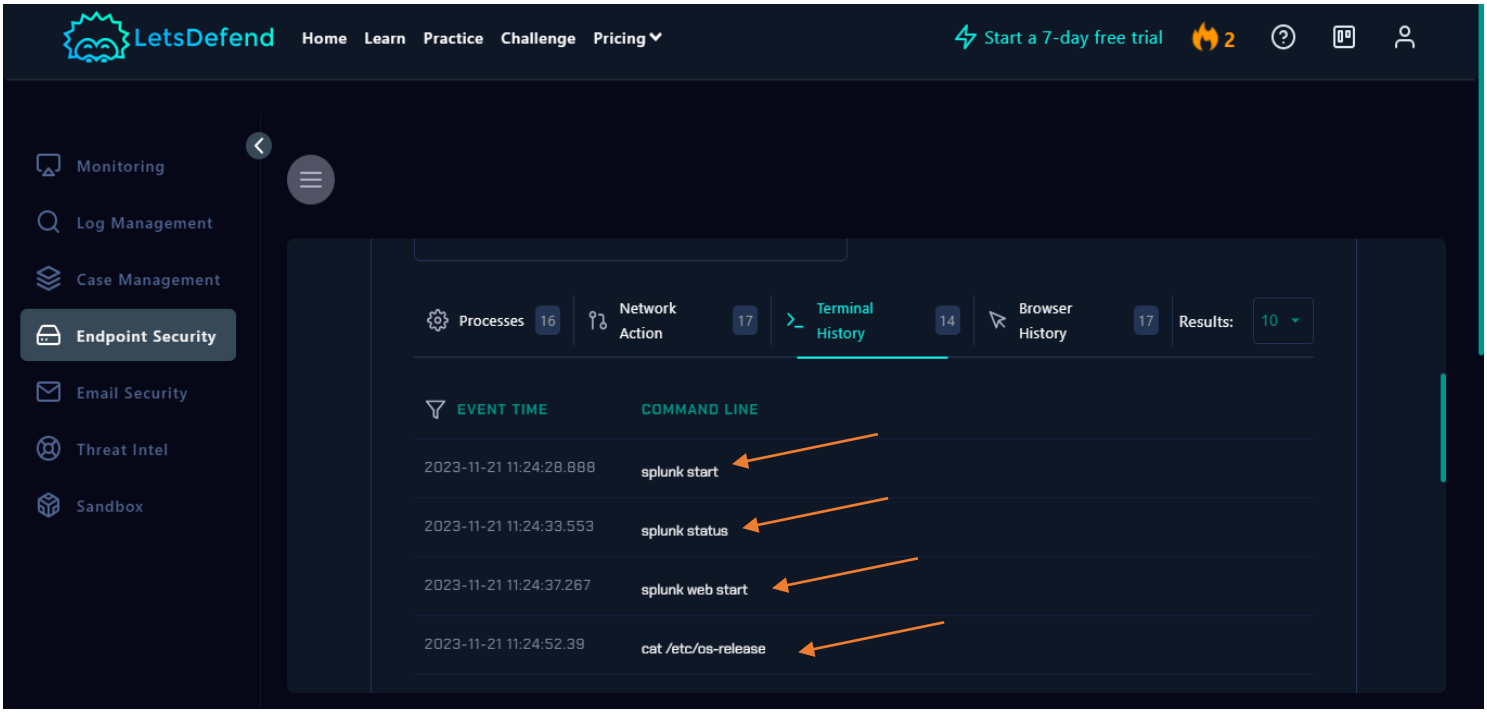
Gathering User Information:

- `id`: Retrieved the user ID and group ID of the current user.
- `whoami`: Retrieved the username of the current logged-in user.
- `groups`: Retrieved the groups associated with the current user.

Creating a New User:

- `useradd -m analsyt`: Attempted to create a new user named "analsyt" with a home directory.
- `passwd analsyt`: Attempted to set a password for the newly created user "analsyt."

For further reference, please see the attached photo



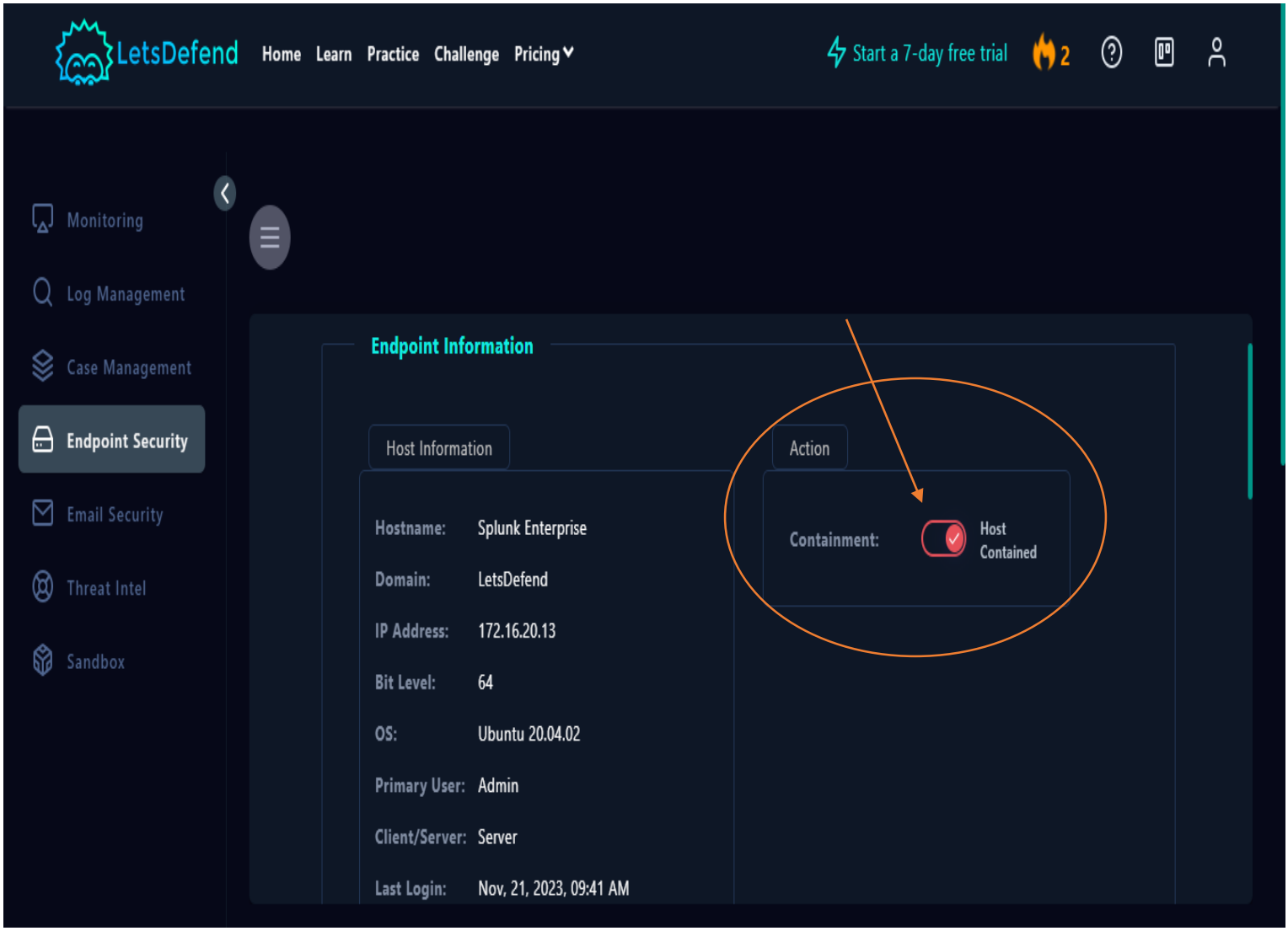
Based on the terminal commands observed, several actions were taken that prompted containment of the server. Initially, system enumeration was performed using commands like `cat /etc/os-release` to retrieve operating system details, `vim --version` to check the version of Vim, and `sudo --version` to understand the sudo configuration. The files in the directory were listed using `ls --color=auto`.

The user then navigated to the Splunk scripts directory with `cd /opt/splunk/bin/scripts/` and viewed the contents of the script "shell.sh" using `cat shell.sh`, possibly to review or modify it. User information was gathered through commands such as `id` to obtain user and group IDs, `whoami` to determine the logged-in username, and `groups` to list the groups the user belongs to.

Furthermore, there was an attempt to create a new user named "analsyt" using `useradd -m analsyt`, followed by setting a password for this user with `passwd analsyt`.

Based on our detection and analysis of these activities, we contained the server to prevent any potential unauthorized access or further malicious actions.

For further reference, please see the attached photo



Conclusion

On November 21, 2023, at 12:24 PM, our security monitoring systems detected a critical event identified as Event ID 201, triggering Rule SOC239 due to suspected remote code execution within Splunk Enterprise. An external attacker, originating from IP address 180.101.88.240, was observed attempting to exploit the system by uploading a potentially malicious XSLT file. This IP address is well-documented in threat intelligence databases, with 10 out of 93 security vendors marking it as malicious, and significant evidence linking it to phishing activities and other abusive behaviors.

Our analysis revealed the presence of a suspicious URL in the proxy logs, which indicated an attempt to upload the file `shell.xsl` to a Splunk instance. The communication details indicated a potentially automated script execution, with network traffic flowing from source port 1923 to destination port 54321, involving the process `shell.sh`.

Further examination of the attacker's terminal commands highlighted a series of system enumeration steps, including the retrieval of OS details and configurations, and an attempted creation of a new user account, "analsyt". These activities, along with the observed network behavior, suggested a sophisticated attempt to establish persistent access to the system.

Given the high-risk nature of the detected activities and the malicious reputation of the originating IP address, we promptly contained the affected server. This preemptive measure was crucial to prevent any unauthorized access or execution of malicious actions. Our team recommends a thorough review of all potentially impacted systems and a reevaluation of security protocols to prevent similar incidents in the future.

This incident underscores the importance of continuous monitoring and swift response in mitigating cybersecurity threats. The detailed analysis and subsequent containment actions reflect our commitment to maintaining the integrity and security of our infrastructure. We will continue to enhance our defenses and remain vigilant against evolving threats.