



Official incident report

Event ID: 117

Rule Name: SOC167 - LS Command Detected in Requested URL

Made By

LinkedIn: Engineer.Ahmed Mansour

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

Github link: <https://github.com/AhmedMansour93>

Table of contents

Official incident report	1
Event ID: 117	1
Rule Name: SOC167 - LS Command Detected in Requested URL	1
Table of contents	2
Event Details	3
Network Information Details	3
Analysis	4
Log management	4
Detection	10
Threat intelligence	10
Conclusion	11

Event Details

Event ID:

117

Event Date and Time:

Feb, 27, 2022, 12:36 AM

Rule:

SOC167 - LS Command Detected in Requested URL

Level:

Security Analyst

Hostname:

EliotPRD

HTTP Request Method:

GET

Requested URL:

<https://letsdefend.io/blog/?s=skills>

User-Agent:

Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0

Alert Trigger Reason:

URL Contains LS

Device Action:

Allowed

Network Information Details

Destination Address:

172.16.17.16 internal

Source Address:

61.177.172.87 external

External / Internal Attack:

Based on the event details, the attack appears to be **external**.

Analysis:

Log Management

We'll proceed by entering the destination IP address and reviewing the results.

Please refer to the attached image for further details regarding the attack.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Columns	Operator	Value				
X Dest. Address	contains	188.114.96.15				
Feb, 27, 2022, 12:37 AM	Proxy	172.16.17.46	47473	188.114.96.15	443	
Feb, 27, 2022, 12:35 AM	Proxy	172.16.17.46	48463	188.114.96.15	443	
Feb, 27, 2022, 12:23 AM	Proxy	172.16.17.46	49843	188.114.96.15	443	
Feb, 27, 2022, 12:13 AM	Proxy	172.16.17.46	49273	188.114.96.15	443	
Feb, 27, 2022, 12:05 AM	Proxy	172.16.17.46	49122	188.114.96.15	443	
Feb, 27, 2022, 12:01 AM	Proxy	172.16.17.46	48123	188.114.96.15	443	
Jan, 25, 2024, 01:30 PM	Proxy	212.8.243.136	44123	188.114.96.15	443	

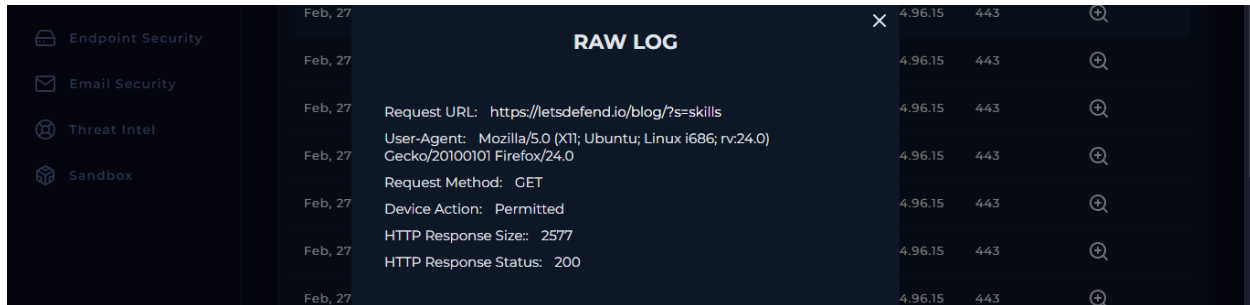
8 Logs records for the destination IP.

Please refer to the attached image for further details regarding the attack.

We will explain all of them step by step

Log Analysis

- **Log1:**

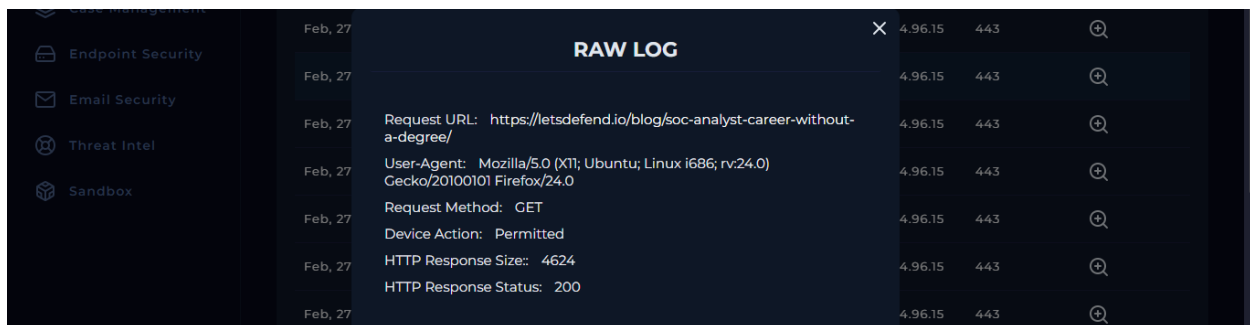


The screenshot shows a security dashboard with a sidebar on the left containing icons for Endpoint Security, Email Security, Threat Intel, and Sandbox. The main area displays a 'RAW LOG' entry for Feb, 27. The log details a GET request to 'https://letsdefend.io/blog/?s=skills' with a User-Agent of 'Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0'. The response size is 2577 bytes and the status is 200. The IP address 4.96.15 and port 443 are listed on the right.

Date	Request URL	User-Agent	Request Method	Device Action	HTTP Response Size	HTTP Response Status	IP	Port
Feb, 27	https://letsdefend.io/blog/?s=skills	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0	GET	Permitted	2577	200	4.96.15	443

Explanation: The user accessed the search page of the LetsDefend blog, searching for articles related to "skills." The response was successful, and the page was served with a size of 2577 bytes.

- **Log2:**




The screenshot shows the same security dashboard as Log1, but with a different log entry for Feb, 27. This entry details a GET request to 'https://letsdefend.io/blog/soc-analyst-career-without-a-degree/'. The User-Agent is the same, but the response size is 4624 bytes and the status is 200. The IP address 4.96.15 and port 443 are listed on the right.

Date	Request URL	User-Agent	Request Method	Device Action	HTTP Response Size	HTTP Response Status	IP	Port
Feb, 27	https://letsdefend.io/blog/soc-analyst-career-without-a-degree/	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0	GET	Permitted	4624	200	4.96.15	443

Explanation: The user accessed a specific blog post titled "SOC Analyst Career Without a Degree." The response was successfully delivered with a size of 4624 bytes.


- **Log3:**



Endpoint Security	Feb, 27	RAW LOG	4.96.15	443	🔍
Email Security	Feb, 27		4.96.15	443	🔍
Threat Intel	Feb, 27	Request URL: https://letsdefend.io/blog/how-to-prepare-soc-analyst-resume/	4.96.15	443	🔍
Sandbox	Feb, 27	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0	4.96.15	443	🔍
	Feb, 27	Request Method: GET	4.96.15	443	🔍
	Feb, 27	Device Action: Permitted	4.96.15	443	🔍
	Feb, 27	HTTP Response Size: 3451	4.96.15	443	🔍
	Feb, 27	HTTP Response Status: 200	4.96.15	443	🔍

Explanation: The user accessed a blog post on how to prepare a SOC analyst resume. The response was served successfully with a size of 3451 bytes.

- **Log4:**



Endpoint Security	Feb, 27	RAW LOG	4.96.15	443	🔍
Email Security	Feb, 27		4.96.15	443	🔍
Threat Intel	Feb, 27	Request URL: https://letsdefend.io/blog/red-team-vs-blue-team-learn-the-difference/	4.96.15	443	🔍
Sandbox	Feb, 27	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0	4.96.15	443	🔍
	Feb, 27	Request Method: GET	4.96.15	443	🔍
	Feb, 27	Device Action: Permitted	4.96.15	443	🔍
	Feb, 27	HTTP Response Size: 6412	4.96.15	443	🔍
	Feb, 27	HTTP Response Status: 200	4.96.15	443	🔍

Explanation: The user accessed a blog post discussing the differences between Red Team and Blue Team roles. The page was delivered successfully with a size of 6412 bytes.

- **Log5:**

Endpoint Security	Feb, 27	RAW LOG	4.96.15	443	⊕
Email Security	Feb, 27		4.96.15	443	⊕
Threat Intel	Feb, 27	Request URL: https://letsdefend.io/blog/how-to-analyze-rtf-template-injection-attacks/	4.96.15	443	⊕
Sandbox	Feb, 27	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0	4.96.15	443	⊕
	Feb, 27	Request Method: GET	4.96.15	443	⊕
	Feb, 27	Device Action: Permitted	4.96.15	443	⊕
	Feb, 27	HTTP Response Size: 6423	4.96.15	443	⊕
	Feb, 27	HTTP Response Status: 200	4.96.15	443	⊕

Explanation: The user accessed a blog post about analyzing RTF template injection attacks. The response was successfully served with a size of 6423 bytes.

- **Log6:**

Endpoint Security	Feb, 27	RAW LOG	4.96.15	443	⊕
Email Security	Feb, 27		4.96.15	443	⊕
Threat Intel	Feb, 27	Request URL: https://letsdefend.io/blog/how-to-become-a-soc-analyst/	4.96.15	443	⊕
Sandbox	Feb, 27	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0	4.96.15	443	⊕
	Feb, 27	Request Method: GET	4.96.15	443	⊕
	Feb, 27	Device Action: Permitted	4.96.15	443	⊕
	Feb, 27	HTTP Response Size: 1935	4.96.15	443	⊕
	Feb, 27	HTTP Response Status: 200	4.96.15	443	⊕

Explanation: The user accessed a blog post about how to become a SOC analyst. The page was successfully served with a size of 1935 bytes.

- **Log7:**

Endpoint Security

Email Security

Threat Intel

Sandbox

Feb, 27

RAW LOG

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27

Feb, 27</

Explanation: The user accessed the main blog page of LetsDefend. The response was successful, with a page size of 3527 bytes.

- **Log8:**

Category	Date	Request Details	IP	Port	Action
Email Security	Feb, 27		4.96.15	443	
	Feb, 27		4.96.15	443	
	Feb, 27	Raw Data: Date=29/Jan/2023:13:30:10 +0000, Client IP=172.16.20.3, Source IP=212.8.243.136, Request=GET, URI=owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fletsdefend.io%2fowa%2f, Protocol=HTTP/1.0, Response Status=200	4.96.15	443	

Explanation: This log entry shows an HTTP request related to an Outlook Web App (OWA) authentication attempt. The request was made to log into OWA, and it included a URL to LetsDefend. The response was successful (status 200), indicating the request was processed correctly.

Summary of Logs

- **Search and Article Access:**

- Several logs show users accessing various pages on the LetsDefend blog, including search results and specific articles related to cybersecurity, such as SOC analyst careers and resume preparation. Each request resulted in a successful response (HTTP status 200) with varying response sizes.

- **Page Details:**

- **Search Query:** The user searched for articles related to "skills" on the blog.
- **Articles Accessed:** The user viewed posts about SOC analyst careers without a degree, preparing SOC analyst resumes, differences between Red Team and Blue Team, analyzing RTF template injection attacks, and becoming a SOC analyst.
- **Main Blog Page:** The user also accessed the main blog page.

- **Authentication Attempt:**

- There is a log entry showing an HTTP request for authentication to Outlook Web App (OWA) with a URL redirecting to LetsDefend, indicating a successful login attempt or authentication process.

2. Is Traffic Malicious?

Based on the logs provided, there is **NO** immediate evidence to suggest that the traffic is malicious.

3. What Is The Attack Type?

Our analysis determines that the attack type is a **Command Injection Attack**.

4. Is the malicious traffic caused by a planned test?

After reviewing the email security section, it has been confirmed that this malicious traffic **was not the result of a planned test**.

5. Was the Attack Successful?

No, Based on the logs provided, there are no indications of a successful attack.

Detection:

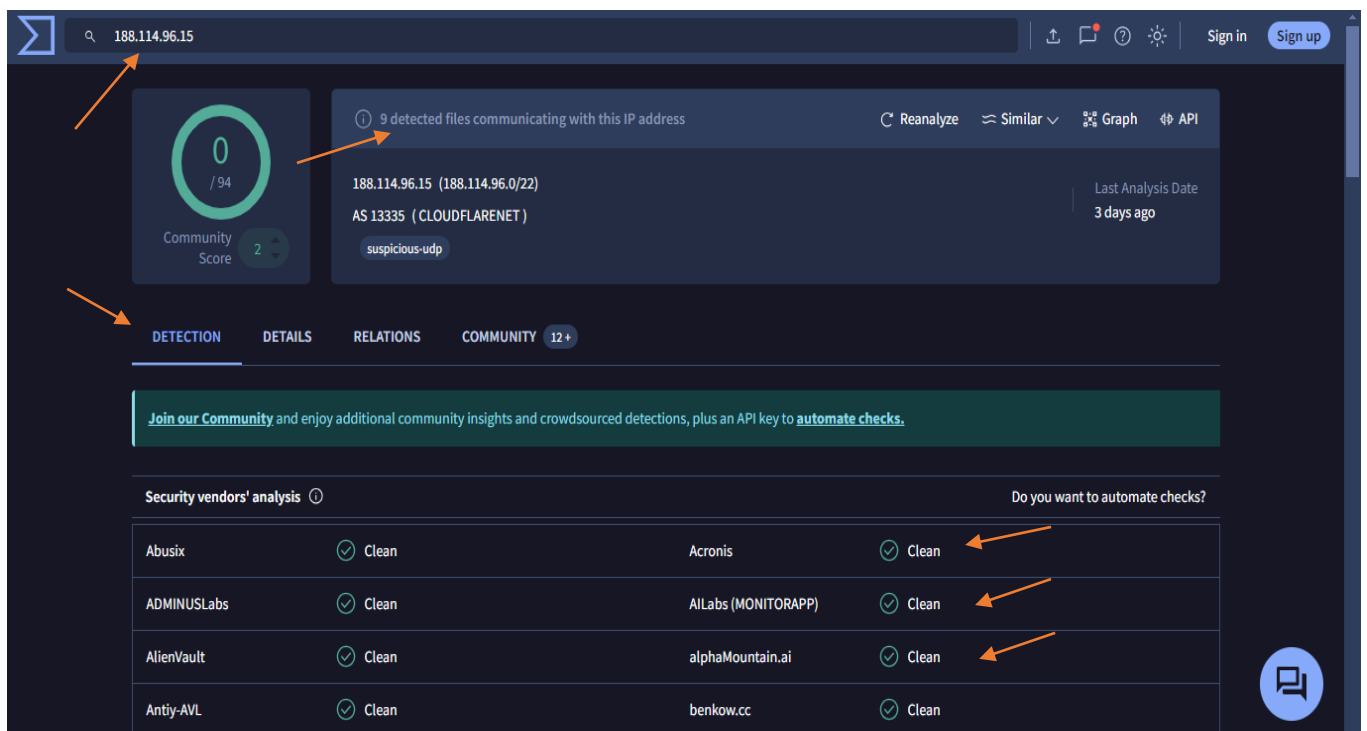
Threat Intelligence Results

Destination IP Analysis on VirusTotal

Objective: Evaluate the source IP address using VirusTotal and review the findings in various sections.

1. Detection Section

- **Status:** The Detection section shows us its **CLEAN**.



The screenshot shows the VirusTotal interface for the IP address 188.114.96.15. The top navigation bar includes a search bar with the IP address, and buttons for 'Sign in' and 'Sign up'. The main content area features a large green circle with the number '0' and the text 'Community Score 2'. To the right, a summary box indicates '9 detected files communicating with this IP address' and lists the IP address, AS 13335 (CLOUDFLARENET), and a 'suspicious-udp' tag. Below this, a tabbed interface shows 'DETECTION', 'DETAILS', 'RELATIONS', and 'COMMUNITY'. The 'DETECTION' tab is active, displaying a table of security vendors' analysis. The table has two columns for vendor names and their analysis results, all showing 'Clean'. A 'Do you want to automate checks?' link is visible in the top right of the table area. Arrows point to the search bar, the community score, the detected files count, and the 'Clean' results in the table.

Security vendors' analysis		Do you want to automate checks?	
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AlIabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean

- **Reference:** [View Detection Section](#)

2. Do You Need Tier 2 Escalation?

NO, based on our analysis, there is no indication of a successful attack. Therefore, escalation to Tier 2 is not necessary at this time.

Conclusion

Upon thorough analysis of the incident with Event ID 117, which occurred on February 27, 2022, at 12:36 AM, we can confidently summarize the findings and actions taken:

Incident Overview: The event was triggered by Rule SOC167, which detected a command pattern in the requested URL: <https://letsdefend.io/blog/?s=skills>. This triggered an alert for potential command injection activity. The traffic was flagged as external, originating from IP address 61.177.172.87 and directed towards an internal address, 172.16.17.16.

Log Analysis: Our review of the related logs reveals that the requests were for standard blog content and an authentication attempt for Outlook Web App (OWA). All responses were successfully processed with HTTP status 200, confirming that the pages were served as intended. There is no evidence of any anomalies or errors in these requests.

Key Findings:

- **Traffic Nature:** The traffic was not identified as malicious. The URL requests and the corresponding blog content retrieval were consistent with normal user behavior.
- **Attack Type:** Although the rule identified potential command injection, detailed analysis confirms that no successful command injection attack occurred. The incident was not the result of a planned test, as verified through email security checks.
- **Success of Attack:** Based on the logs and further investigation, there are no indicators of a successful attack. The destination IP was also scanned on VirusTotal, showing a clean status, which corroborates our findings.

Escalation and Actions: Given that our analysis indicates no successful attack and the traffic does not appear to be malicious, escalation to Tier 2 is deemed unnecessary at this time. The incident should be closed with the understanding that all security protocols were adhered to, and appropriate measures were in place to handle potential threats.

Final Note: Our proactive analysis and response to this incident reflect our commitment to maintaining robust security posture and ensuring prompt resolution of potential threats. The incident has been handled efficiently, and all necessary steps have been taken to confirm that no further action is required.