

# Let's defend alert n.86

## SOC141 – Phishing URL Detected

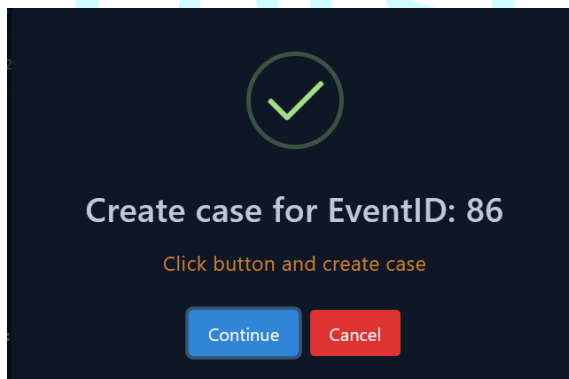
Hello, my name is Francesco, and this is my first write up. I hope the document is well written and clear for everyone. Please, if anything is wrong or not well clear to someone contact me.

## Introduction and case creation

Today we are going to complete this task from the Let's Defend platform.

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Mar, 22, 2021, 09:23 PM	SOC141 - Phishing URL Detected	86	Proxy	>> ✓
<b>Event Details</b>					
EventID :		86			
Event Time :		Mar, 22, 2021, 09:23 PM			
Rule :		SOC141 - Phishing URL Detected			
Level :		Security Analyst			
Source Address :		172.16.17.49			
Source Hostname :		EmilyComp			
Destination Address :		91.189.114.8			
Destination Hostname :		mogagrocol.ru			
Username :		ellie			
Request URL :		http://mogagrocol.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io			
User Agent :		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36			
Device Action :		Allowed			

First, we must create the case, so we can start investigating.



# Gathering information

---

From the investigation channel, we can gather all the information we need to complete this case.

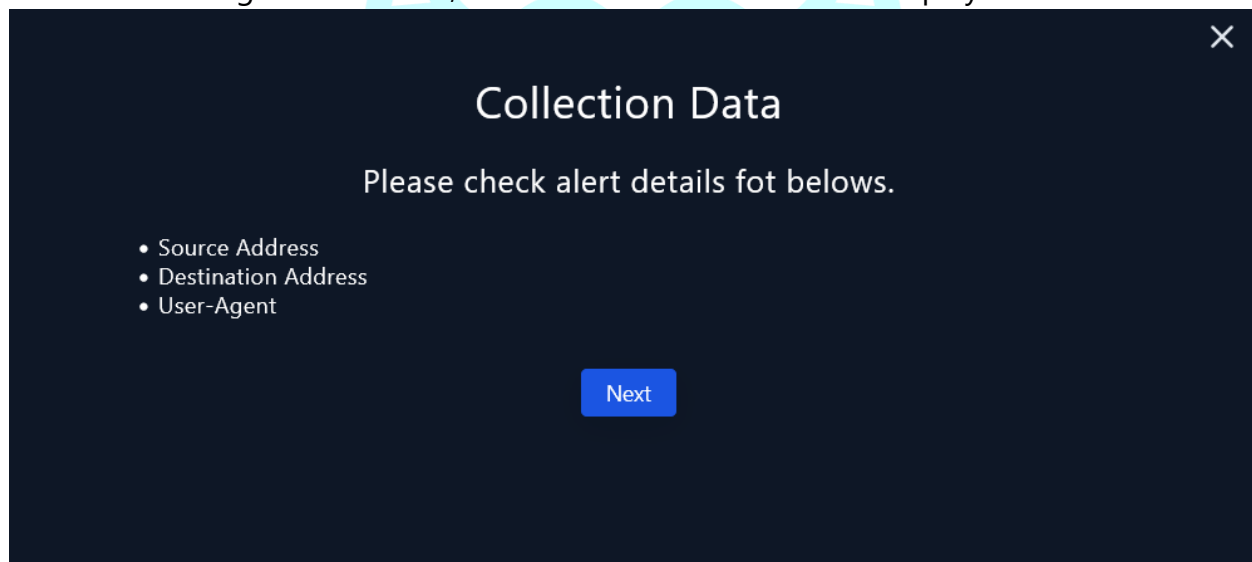
- Date: Mar 22, 2021, 09:23
- Source Address: 172.16.17.49
- Source Hostname: EmilyComp
- Destination Address: 91.189.114.8
- Destination Hostname: mogagrocol.ru
- Username: ellie
- Request URL: <http://mogagrocolf.ru/wp-content/plugins/akismet/fv/index.php?email=ellie@letsdefend.io>

## Start

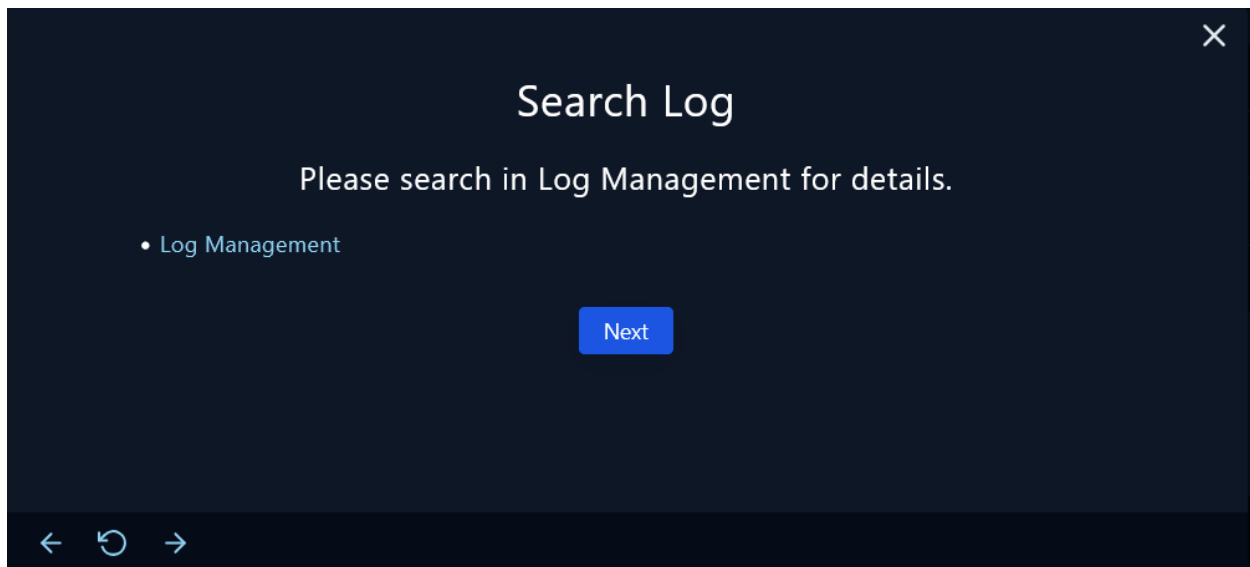
---

(TIP: Open a new tab for easier development of the activity.)

From the Investigation Channel, we create the case and start the playbook.

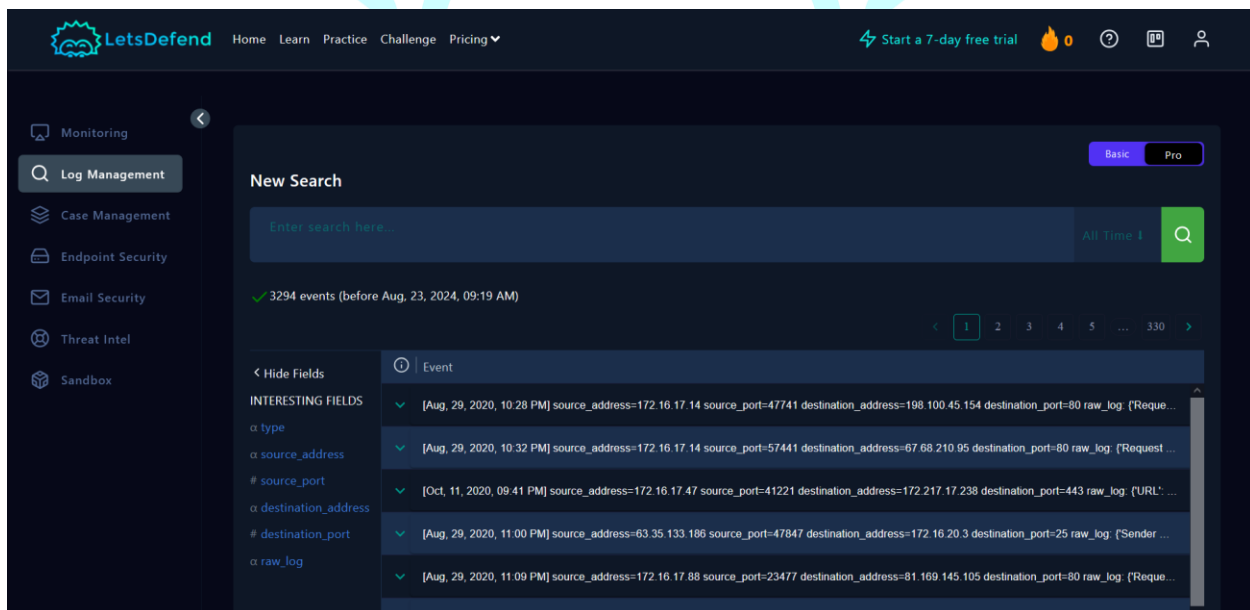


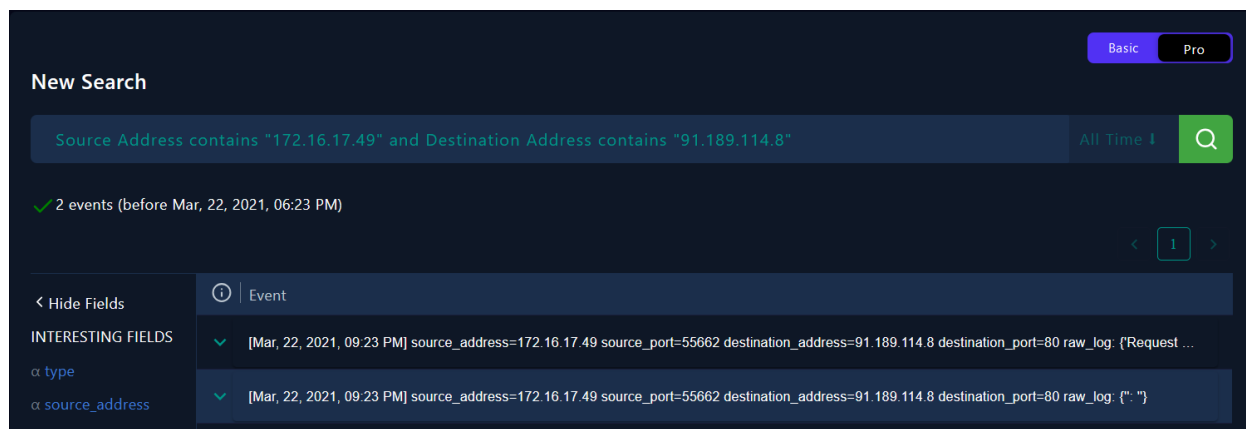
We have already collected all the information we needed earlier, so we can go ahead and head to the log management tab.



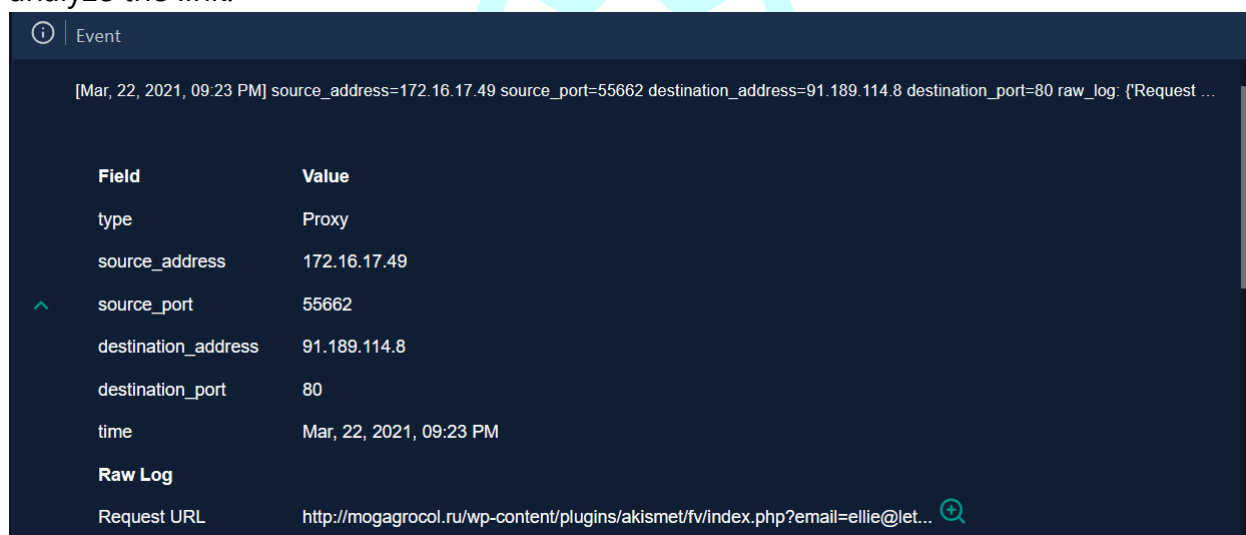
## Checking the Suspicious Link

Once in the log management tab, we start filtering through all the present logs by source IP address and destination IP address.





We take the suspicious link from one of the two logs that showed up (or from the information we gathered in the first step) and use some different third-party tools to analyze the link.



I used Virus Total, but you can use any of the other's platform the page ask you to check (for more security you should try to use all of them, but I'm not going to do it in this write up).

4/96 security vendors flagged this URL as malicious

Community Score: 4 / 96

Status: 403

Content type: text/html; charset=utf-8

Last An...: 2 days ago

text/html external-resources

DETECTION DETAILS COMMUNITY 1

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

Security vendors' analysis

Security vendors' analysis		Do you want to automate checks?	
BitDefender	Phishing	G-Data	Phishing
Kaspersky	Phishing	VIPRE	Phishing
ArcSight Threat Intelligence	Suspicious	Trustwave	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean

As we can see, this link is flagged as a phishing link. In this case, we will click the "Malicious" button.

## Analyze URL Address

Analyze URL in 3rd party tools. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

You can use the free products/services below.

- AnyRun
- VirusTotal
- URLHouse
- URLScan
- HybridAnalysis

Malicious Non-malicious

Next, we must determine if the link has been opened by someone. By looking at the event logs, we understand that the user ellie opened the URL because we found a connection from the internal network to the suspicious link, as we have seen previously. The request is then blocked by the firewall, as we can see in the second log.

[Mar, 22, 2021, 09:23 PM] source\_address=172.16.17.49 source\_port=55662 destination\_address=91.189.114.8 destination\_port=80 raw\_log: {"": ""}

Field	Value
type	Firewall
source_address	172.16.17.49
source_port	55662
destination_address	91.189.114.8
destination_port	80
time	Mar, 22, 2021, 09:23 PM

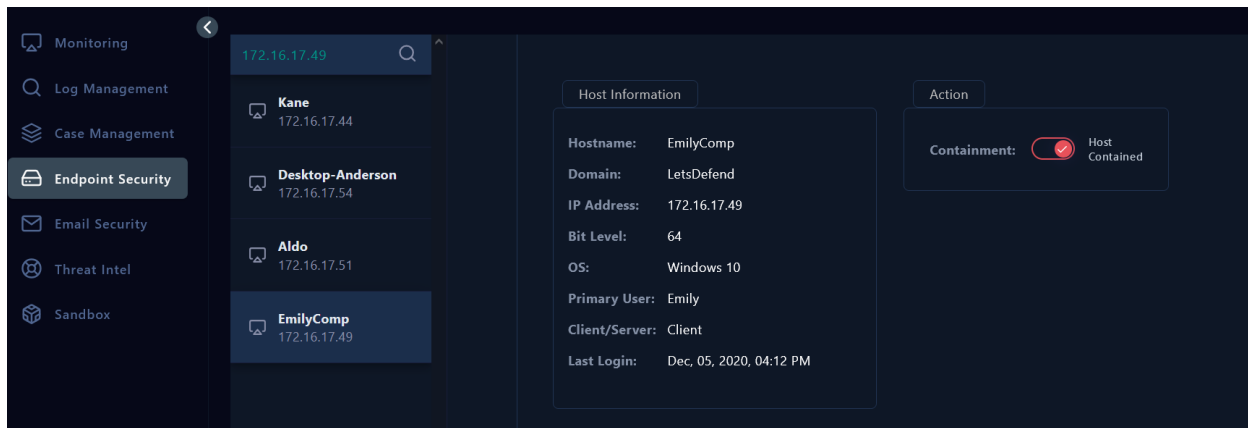
Raw Log

## Containing the machine

Once we understand that the link has been opened by the worker, we must contain the machine. The first step to do this is to go to the Endpoint Security (EDR) and search for the IP of the victim (172.16.17.49).

The screenshot shows the Endpoint Security (EDR) interface. On the left, a sidebar lists navigation options: Monitoring, Log Management, Case Management, Endpoint Security (selected), Email Security, Threat Intel, and Sandbox. The main area displays a list of endpoints with columns for name and IP address. The endpoints listed are Kane (172.16.17.44), Desktop-Anderson (172.16.17.54), Aldo (172.16.17.51), and EmilyComp (172.16.17.49). The 'EmilyComp' endpoint is selected, and its details are shown in the 'Endpoint Information' panel. This panel has two tabs: 'Host Information' and 'Action'. The 'Host Information' tab is active, showing details such as Hostname (EmilyComp), Domain (LetsDefend), IP Address (172.16.17.49), Bit Level (64), OS (Windows 10), Primary User (Emily), Client/Server (Client), and Last Login (Dec, 05, 2020, 04:12 PM). The 'Action' tab is also visible, showing a 'Containment' button with a toggle switch.




Once we find the victim machine, just click on the containment button, and the machine will be blocked.



## Conclusion

In the end, we understand that this case has been a truly positive one. We complete the case by adding some information like the URL, the source IP and the destination IP, we write a little explanation about the case, and we can close the investigation.

That was the last step. With that, we successfully completed the exercise and earned the maximum points. Congratulations!!

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
High	Aug, 27, 2024, 06:50 PM	SOC141 - Phishing URL Detected	86	Proxy	✓	↺
<p>EventID : 86</p> <p>Event Time : Mar, 22, 2021, 09:23 PM</p> <p>Rule : SOC141 - Phishing URL Detected</p> <p>Answer : True Positive (+5 Point)</p> <p>Playbook Answers : Has Anyone Accessed IP/URL/Domain? (+5 Point) Analyze URL Address (+5 Point)</p> <p>Analyst Note : Empty! You should explain why you closed alarm this way.</p> <p>Community Walkthrough : Show</p> <p>Rate this case : ☆</p> <p>Writeups : ✍</p> <p>Discussion : 💬</p> <p>Share :   </p>						