Official incident report

Event ID: 234

Rule Name: SOC176- RDP Brute Force Detection

Table of contents

Event Details

Event ID:
234

Event Date and Time:
Mar, 07, 2024, 11:44 AM

Rule:
SOC176 - RDP Brute Force Detected

Level:
Security Analyst

Description:
Login failure from a single source with different non existing accounts

Network Information Details

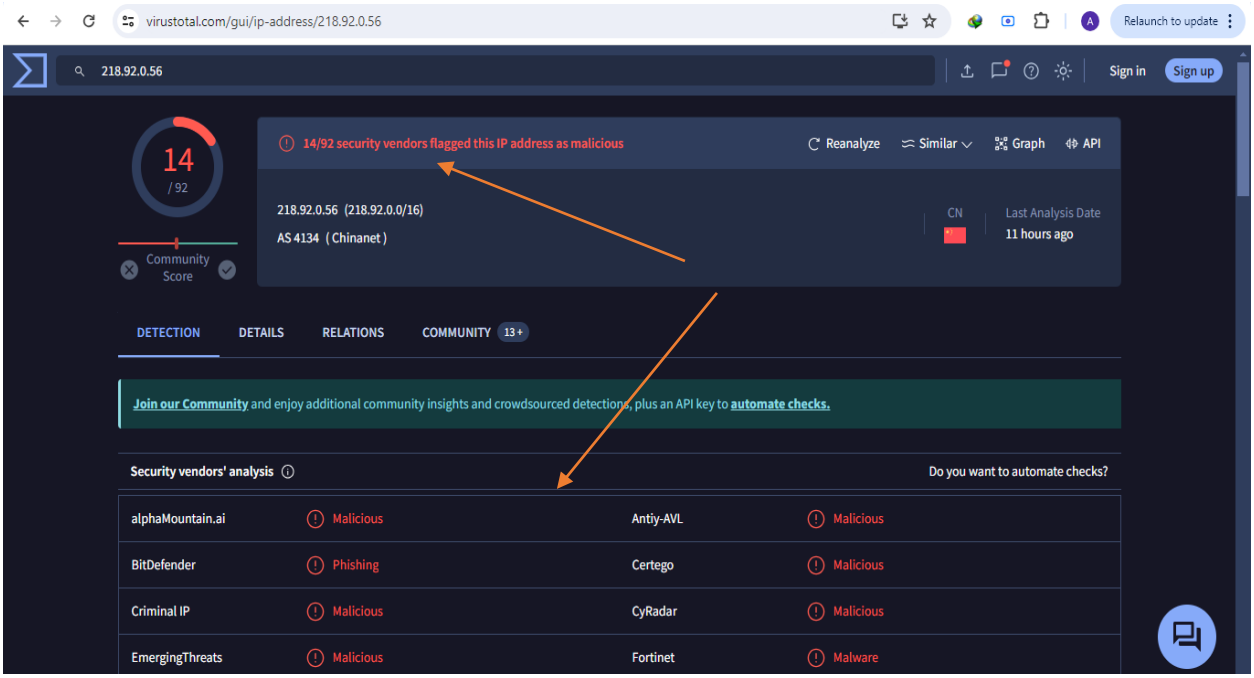
Destination Address:
172.16.17.148

Source Address:
218.92.0.56

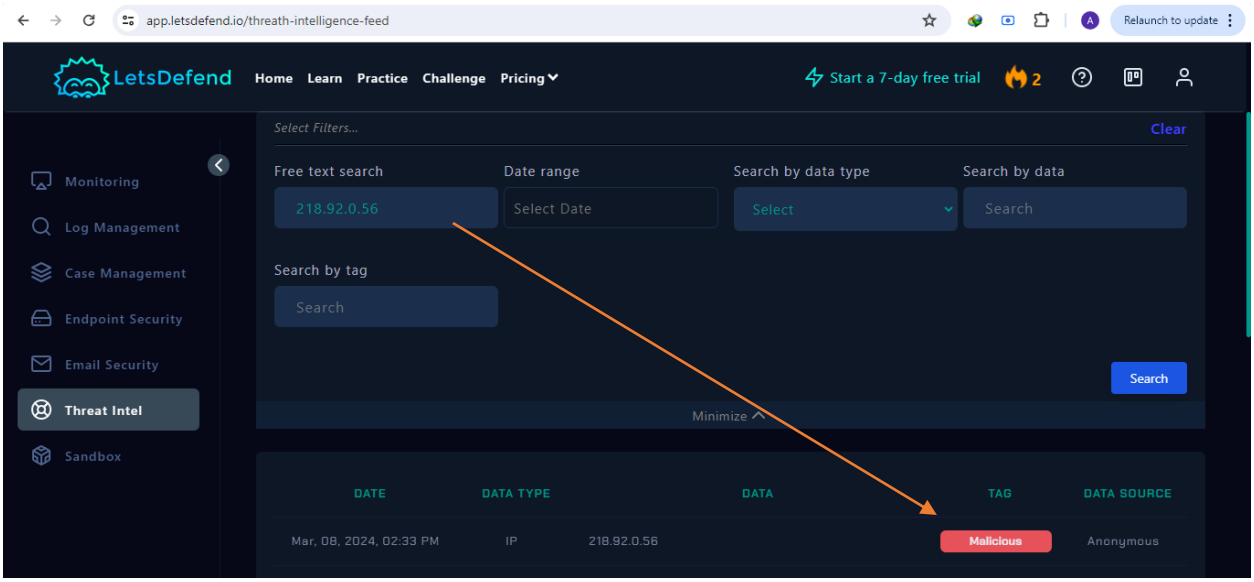
Detection:

Threat Intelligence Results

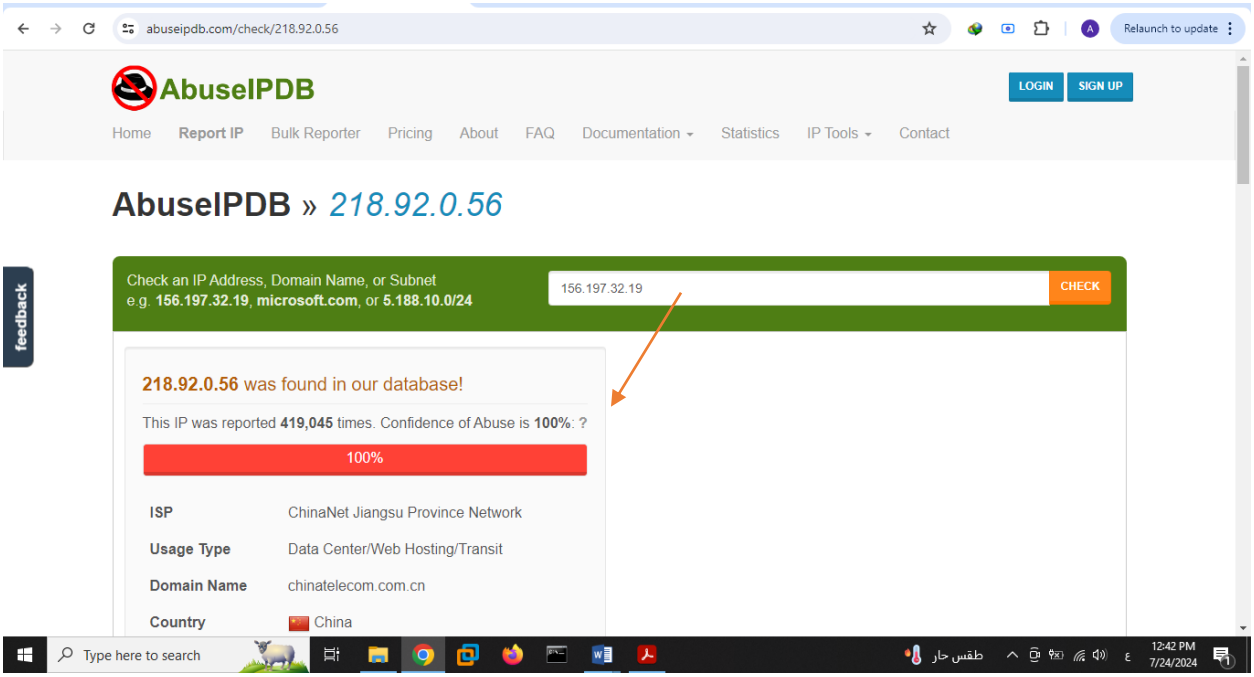
www.virustotal.com



www.letsdefend.io



www.letsdefend.io



Based on the threat intelligence gathered from various reputable sources, the IP address 218.92.0.56 has been determined to be malicious. Below are the detailed findings:

VirusTotal:

14/92 security vendors flagged this IP address as malicious.

Notable detections include:

alphaMountain.ai: Malicious

Antiy-AVL: Malicious

BitDefender: Phishing

Certego: Malicious

Criminal IP: Malicious

CyRadar: Malicious

EmergingThreats: Malicious

Fortinet: Malware

G-Data: Phishing

GreenSnow: Malicious

Juniper Networks: Malicious

Lionic: Malicious

VIPRE: Phishing

Webroot: Malicious

Additional suspicious classifications by:

AlphaSOC: Suspicious

ArcSight Threat Intelligence: Suspicious

AbuseIPDB:

The IP address 218.92.0.56 was found in the AbuseIPDB database.

Reported 419,045 times with a 100% Confidence of Abuse.

Associated details:

ISP: ChinaNet Jiangsu Province Network

Usage Type: Data Center/Web Hosting/Transit

Domain Name: chinatelecom.com.cn

Country: China

City: Lianyungang, Jiangsu

LetsDefend:

The IP address 218.92.0.56 is flagged as malicious.

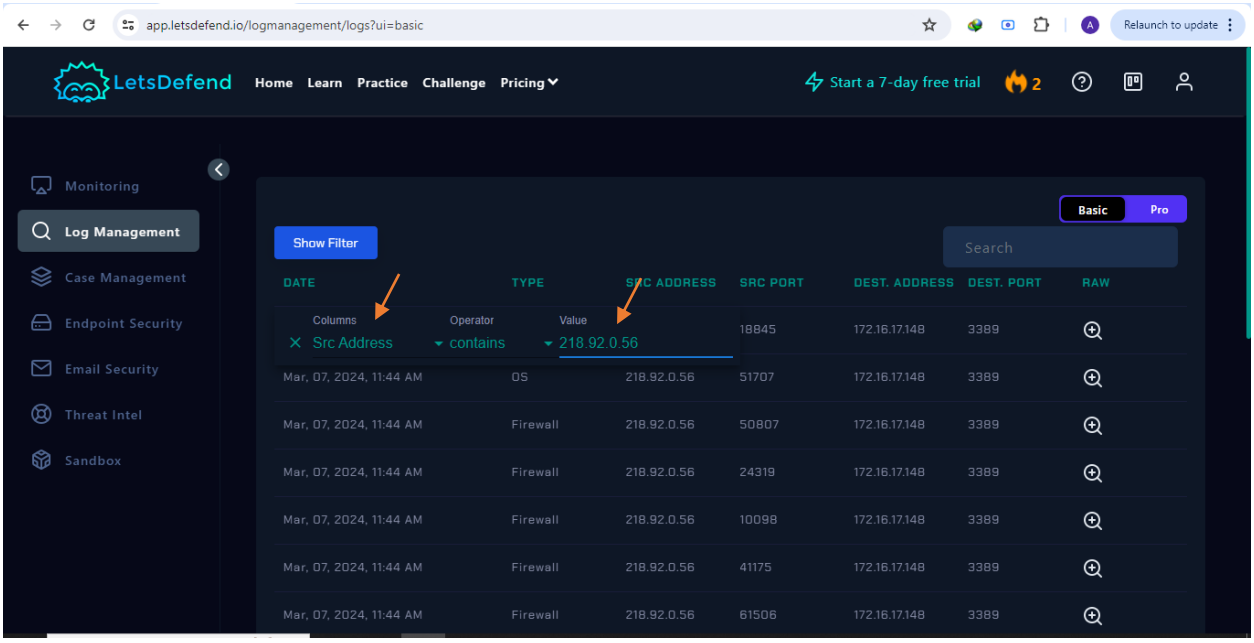
Conclusion:

The IP address 218.92.0.56 has been extensively reported and verified as malicious across multiple threat intelligence platforms. The significant number of reports and high confidence levels, coupled with its classification as a phishing and malware source, indicate that this IP poses a considerable threat. It is strongly recommended to block this IP address and monitor for any related activity within the network.

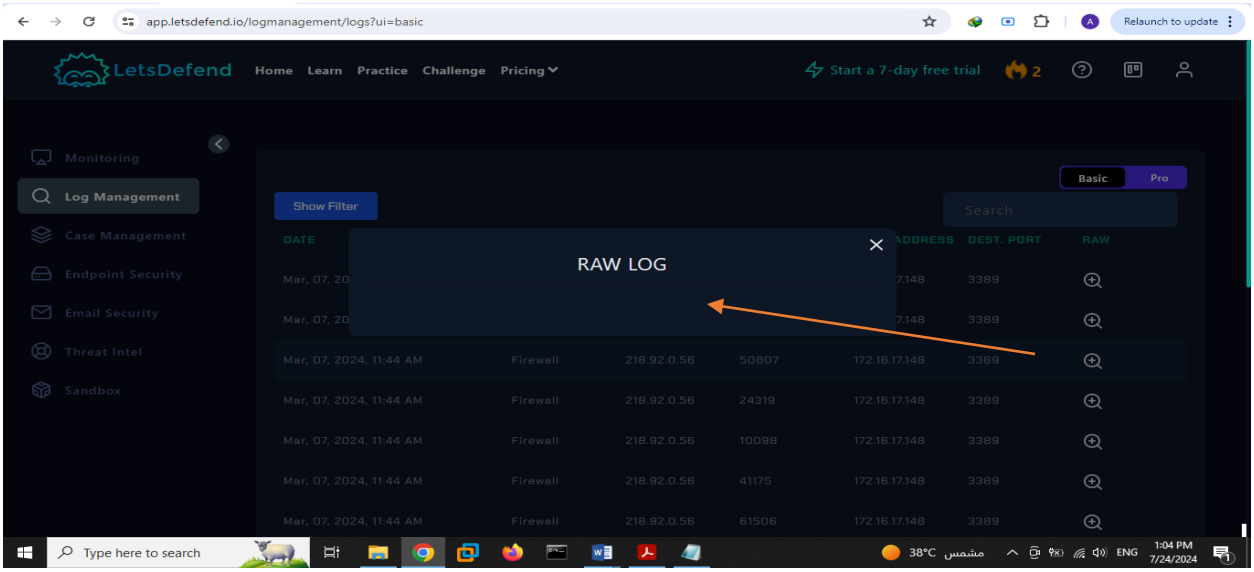
Analysis:

Log Management

***I opened log management section then I filtered the results by choosing the source address and typing the typing the attacker IP.**

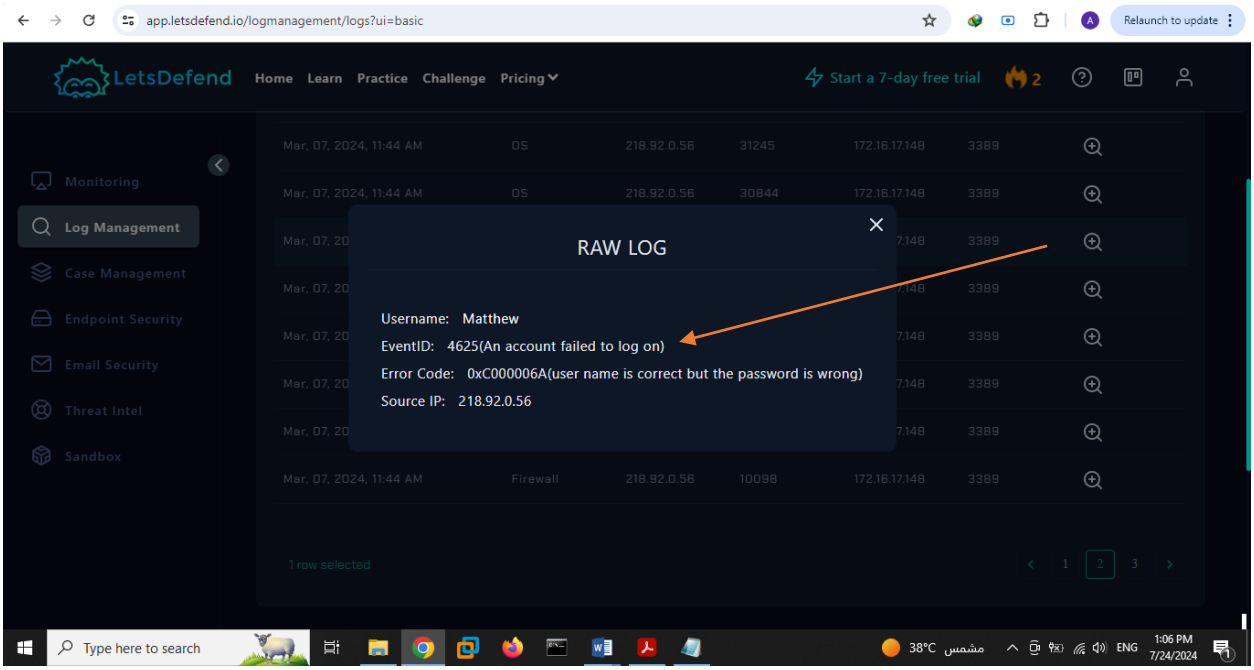


***I Checked all the Firewall results and its all the same**



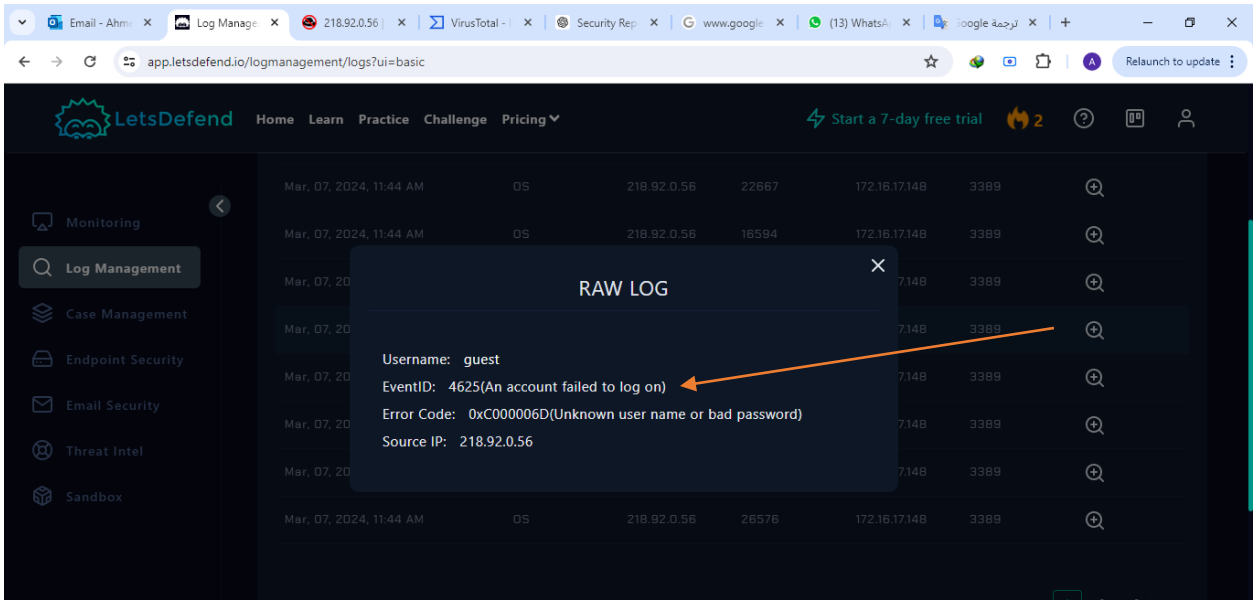
1. Attacker tried to login by correct user name: Matthew, but failed to login because he doesn't know the password and he is trying to make bruit force attack to login.

   Event ID 4625, Error Code: 0xC000006A (user name is correct but the password is wrong) , Target service (Destination port): RDP 3389.



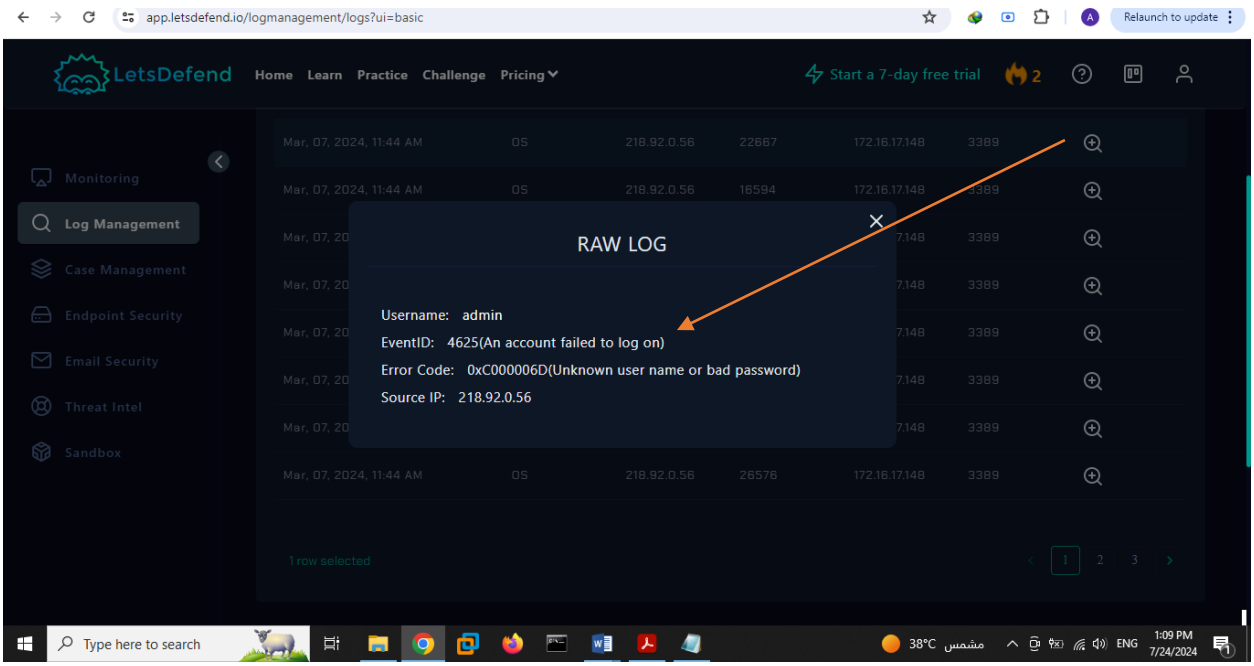
2. Attacker tried to login by wrong user name: guest, but failed to login because he doesn't know the username and password and he is trying to make bruit force attack to login.

   Event ID 4625, Error Code: 0xC000006D (Unknown user name or bad password), Target service (Destination port): RDP 3389.

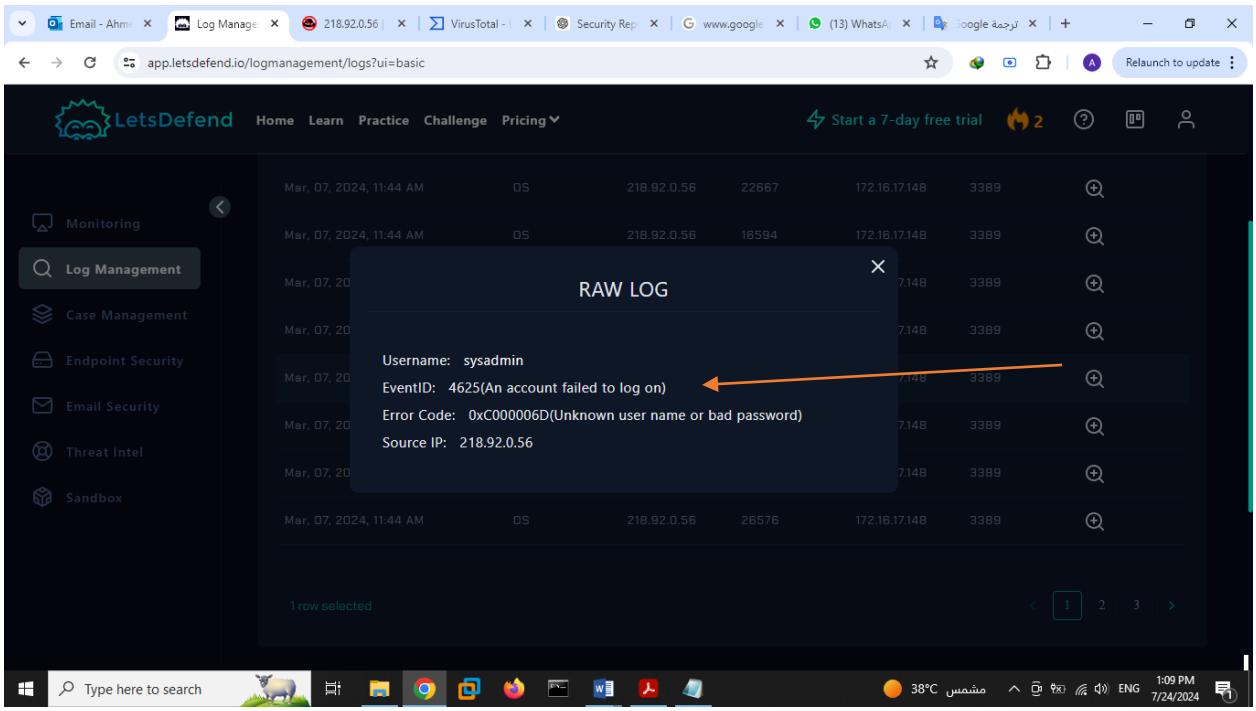


3. Attacker tried to login by wrong user name: admin, but failed to login because he doesn't know the username and password and he is trying to make bruit force attack to login.

   Event ID 4625, Error Code: 0xC000006D (Unknown user name or bad password) , Target service (Destination port): RDP 3389.



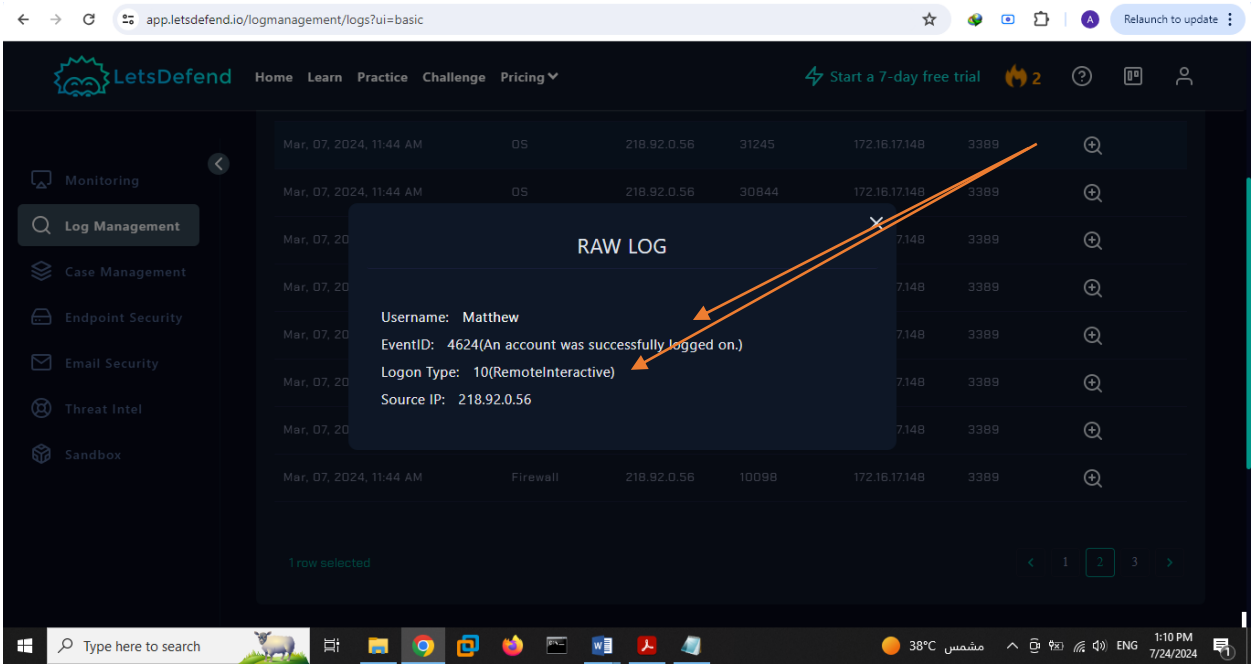
4. Attacker tried to login by wrong user name: sysadmin, but failed to login because he doesn't know the username and password and he is trying to make bruit force attack to login.



5. Attacker logged in by correct username: Matthew, and correct password.

   Event ID: 4624(An account was successfully logged on.)

   Logon Type: 10(Remote Interactive)



The attacker initiated a brute force attack on the system's RDP service (port 3389), attempting multiple logins with both correct and incorrect usernames. Initial attempts with the username "Matthew" failed due to incorrect passwords (Event ID 4625, Error Code: 0xC000006A). Subsequent attempts using "guest," "admin," and "sysadmin" also failed due to incorrect usernames and passwords (Event ID 4625, Error Code: 0xC000006D). Eventually, the attacker succeeded in logging in with the correct credentials for the username "Matthew" (Event ID 4624, Logon Type: 10). This indicates a successful brute force attack, necessitating immediate security measures to prevent further unauthorized access.

Endpoint Security

Based on our detection and analysis we contained the device

Conclusion

On March 07, 2024, at 11:44 AM, a security event (Event ID: 234) was detected under SOC Rule SOC176, indicating a brute force attack on the RDP service (port 3389) targeting our system. The attacker, originating from the malicious IP address 218.92.0.56, attempted multiple login attempts using both correct and incorrect usernames.

The attack sequence included:

1. Multiple failed login attempts with the username "Matthew" due to incorrect passwords (Event ID 4625, Error Code: 0xC000006A).

2. Failed login attempts using non-existing usernames "guest," "admin," and "sysadmin" (Event ID 4625, Error Code: 0xC000006D).

3. A successful login using the correct username "Matthew" and password (Event ID 4624, Logon Type: 10).

Threat intelligence from VirusTotal, AbuseIPDB, and LetsDefend consistently flagged the source IP as malicious, with significant evidence of phishing, malware, and other malicious activities. Given the high confidence levels and extensive reports, it is evident that this IP poses a significant threat.

Our analysis confirmed repeated brute force attempts, ultimately leading to unauthorized access. Immediate actions have been taken to contain the compromised endpoint and prevent further breaches. It is strongly recommended to block the IP address 218.92.0.56 and monitor for any related suspicious activity within the network.