SOC170 - Passwd Found in Requested URL - Possible LFI Attack [Let's Defend – write-up]

SOC170 — Passwd Found in Requested URL — Possible LFI Attack [Let's Defend — write-up] | by Fahad Alotaibi | Jan, 2026 | Medium

Introduction to Local File Inclusion (LFI)

Definition:

- Local File Inclusion (LFI) is a critical security vulnerability that occurs when a web application includes files without properly sanitizing user-provided data. Unlike Remote File Inclusion (RFI), LFI exploits involve files located on the same server where the application is hosted.

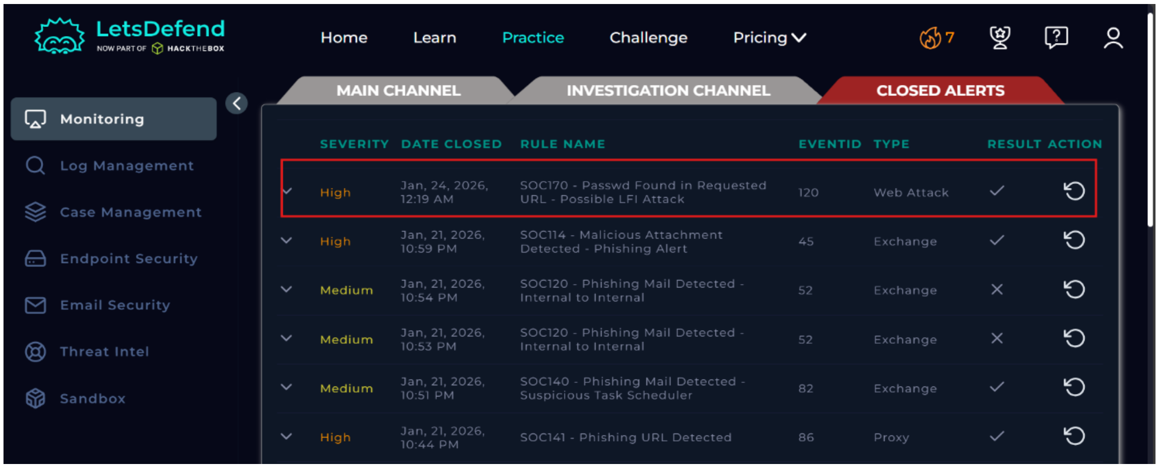
Mechanism:

- Attackers exploit parameters (like ?file= or ?lang=) by injecting Path Traversal sequences (../). This allows them to escape the web directory and navigate to the root system, enabling them to read sensitive files like /etc/passwd.

Detection Method:

- To detect LFI, we monitor web requests for special characters such as /, ., and \. Specifically, we look for common patterns used by attackers to access critical system files or indicators of directory traversal in the URL.

Initial Analysis



SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
High	Jan, 24, 2026, 12:19 AM	SOC170 - Passwd Found in Requested URL - Possible LFI Attack	120	Web Attack	✓	↺
High	Jan, 21, 2026, 10:59 PM	SOC114 - Malicious Attachment Detected - Phishing Alert	45	Exchange	✓	↺
Medium	Jan, 21, 2026, 10:54 PM	SOC120 - Phishing Mail Detected - Internal to Internal	52	Exchange	✗	↺
Medium	Jan, 21, 2026, 10:53 PM	SOC120 - Phishing Mail Detected - Internal to Internal	52	Exchange	✗	↺
Medium	Jan, 21, 2026, 10:51 PM	SOC140 - Phishing Mail Detected - Suspicious Task Scheduler	82	Exchange	✓	↺
High	Jan, 21, 2026, 10:44 PM	SOC141 - Phishing URL Detected	86	Proxy	✓	↺

Figure 1: Alert SOC170 - Passwd Found in Requested URL - Possible LFI Attack.

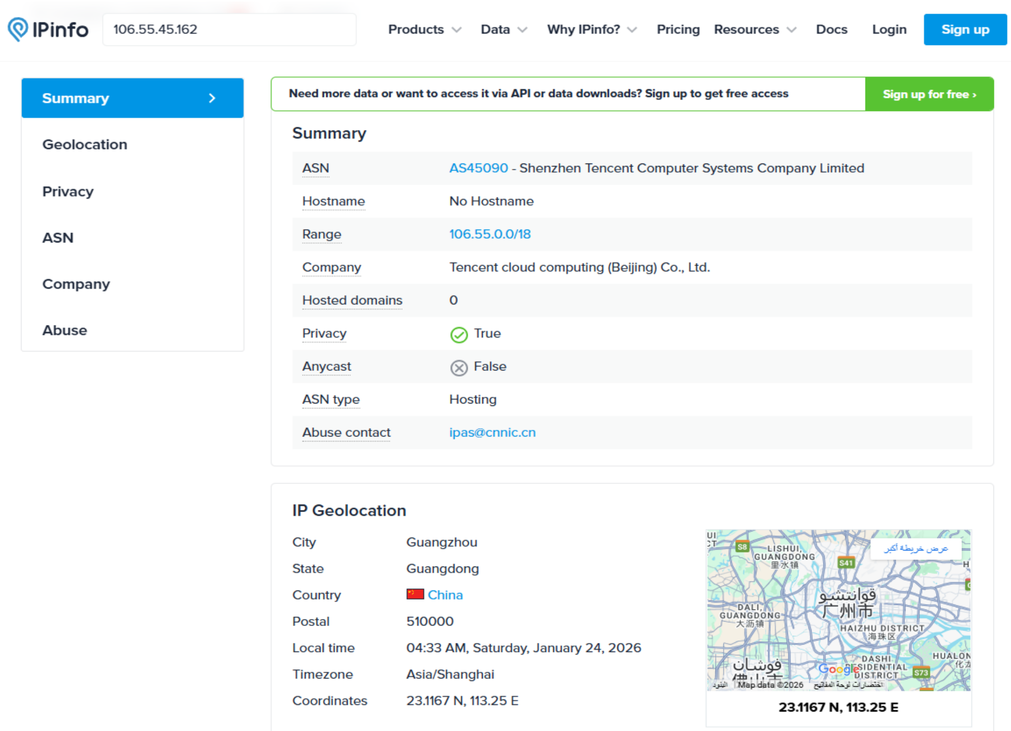
1. Understand Why the Alert Was Triggered

- **Rule:** SOC170 - Possible LFI Attack.

- **Trigger:** The system detected the string **/etc/passwd** with traversal characters **../../../../** in the URL.
- **Direction:** Inbound from External IP (**106.55.45.162**) to Internal WebServer (**172.16.17.13**).

2. Data Collection & Evidence

- **Source Ownership:** The source IP address (106.55.45.162) is an **External IP** located in China. Based on the lookup, it belongs to **Tencent Cloud Computing**, which is a hosting/cloud provider.



IPinfo 106.55.45.162 Products Data Why IPinfo? Pricing Resources Docs Login Sign up

Summary › | Geolocation | Privacy | ASN | Company | Abuse

Need more data or want to access it via API or data downloads? Sign up to get free access — Sign up for free ›

Summary

ASN	AS45090 - Shenzhen Tencent Computer Systems Company Limited
Hostname	No Hostname
Range	106.55.0.0/18
Company	Tencent cloud computing (Beijing) Co., Ltd.
Hosted domains	0
Privacy	✓ True
Anycast	☒ False
ASN type	Hosting
Abuse contact	ipas@cnnic.cn

IP Geolocation

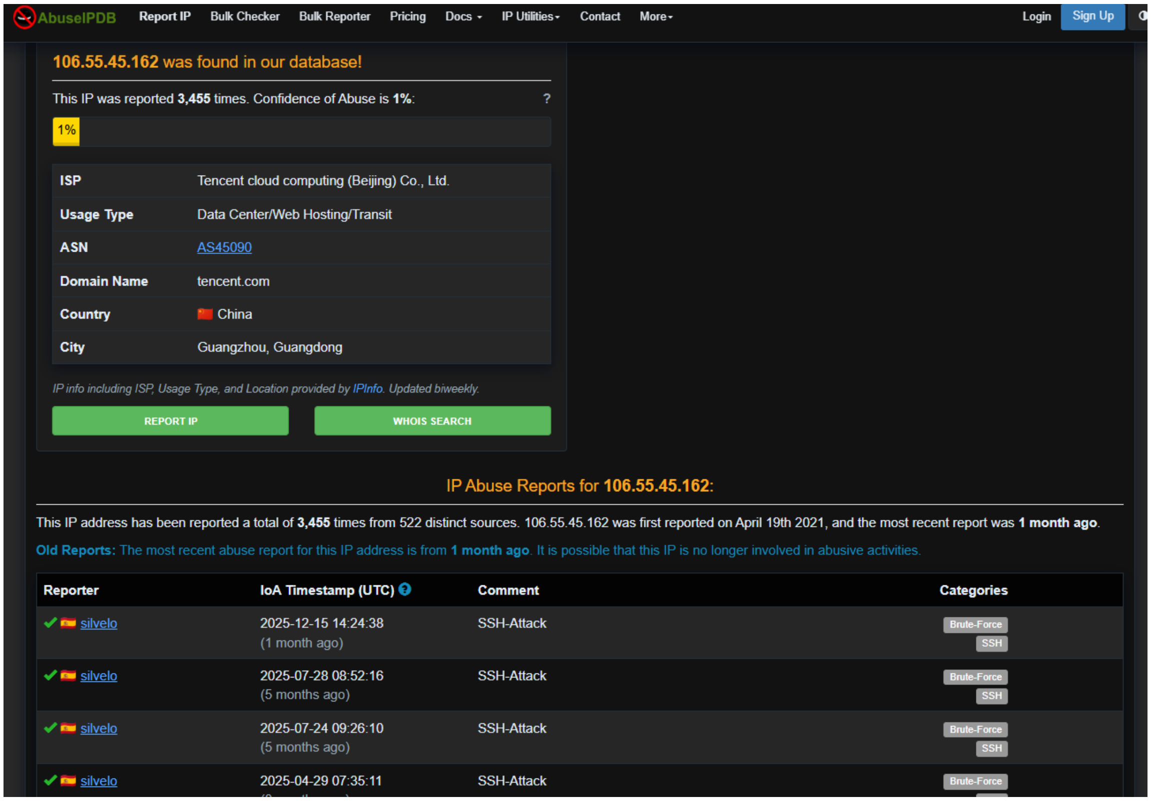
City	Guangzhou
State	Guangdong
Country	China
Postal	510000
Local time	04:33 AM, Saturday, January 24, 2026
Timezone	Asia/Shanghai
Coordinates	23.1167 N, 113.25 E

23.1167 N, 113.25 E

Figure 2: IPinfo ownership details for 106.55.45.162.

- **Destination Ownership**: The destination IP address (**172.16.17.13**) is an Internal Asset identified as **WebServer1006**. This confirms the target is an internal company web server.
- **Reputation Check:** A comprehensive reputation check was performed across multiple platforms:
- **VirusTotal & Cisco Talos:** Returned a "Neutral/Clean" score (0/92), indicating no recent blacklisting by security vendors.
- **AbuseIPDB:** Revealed that this IP is highly suspicious, with over 3,455 reports from 522 distinct sources. The reports explicitly mention SSH Brute-force and Web Application Attacks.

Conclusion: Despite the clean score on some platforms, the extensive history in AbuseIPDB confirms this is a Known Malicious Actor.



106.55.45.162 was found in our database!

This IP was reported **3,455** times. Confidence of Abuse is **1%**:

1%

ISP	Tencent cloud computing (Beijing) Co., Ltd.
Usage Type	Data Center/Web Hosting/Transit
ASN	AS45090
Domain Name	tencent.com
Country	🇨🇳 China
City	Guangzhou, Guangdong

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

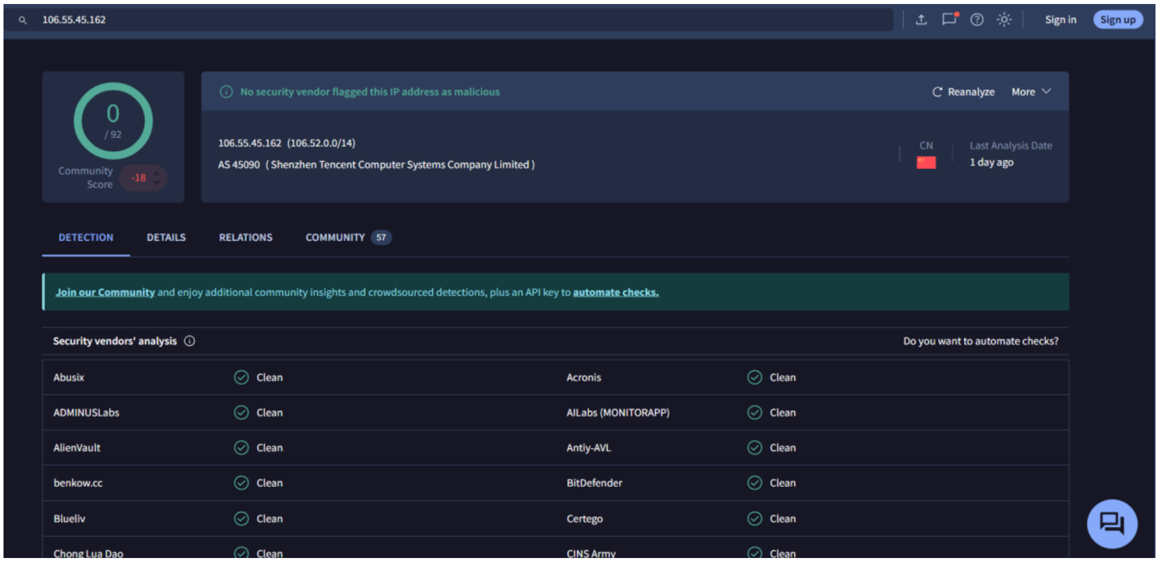
IP Abuse Reports for **106.55.45.162**:

This IP address has been reported a total of **3,455** times from 522 distinct sources. 106.55.45.162 was first reported on April 19th 2021, and the most recent report was **1 month ago**.

Old Reports: The most recent abuse report for this IP address is from **1 month ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC)	Comment	Categories
✓ 🇪🇸 silvelo	2025-12-15 14:24:38 (1 month ago)	SSH-Attack	Brute-Force SSH
✓ 🇪🇸 silvelo	2025-07-28 08:52:16 (5 months ago)	SSH-Attack	Brute-Force SSH
✓ 🇪🇸 silvelo	2025-07-24 09:26:10 (5 months ago)	SSH-Attack	Brute-Force SSH
✓ 🇪🇸 silvelo	2025-04-29 07:35:11	SSH-Attack	Brute-Force

Figure 3: AbuseIPDB reputation score.



0
/ 92
Community Score -18

No security vendor flagged this IP address as malicious

106.55.45.162 (106.52.0.0/14)
AS 45090 (Shenzhen Tencent Computer Systems Company Limited)

CN 🇨🇳

Last Analysis Date
1 day ago

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

Security vendors' analysis

Do you want to automate checks?

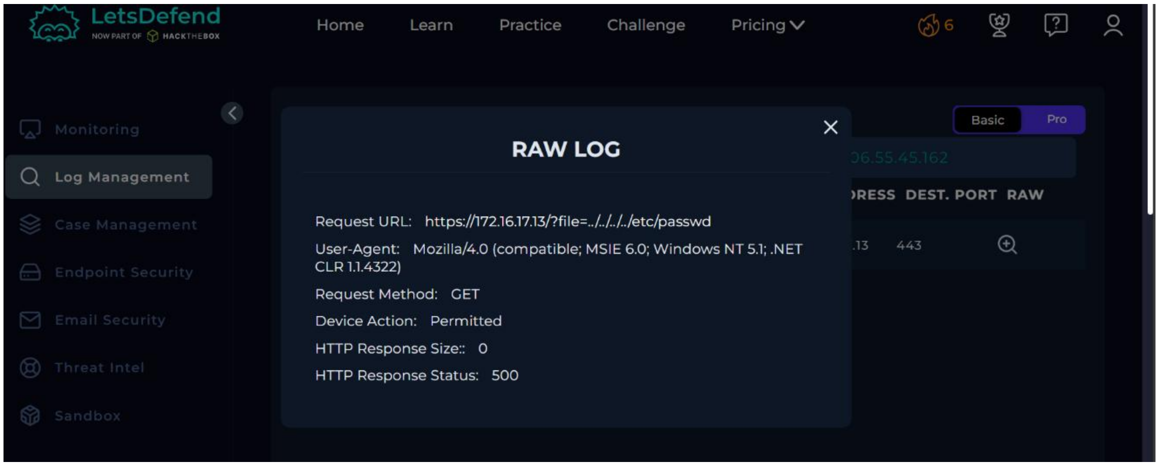
Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean
Chong Lua Dao	✓ Clean	CINS Army	✓ Clean

Figure 4: VirusTotal reputation score.

3. Log Management Investigation

Analysis of Server Logs:

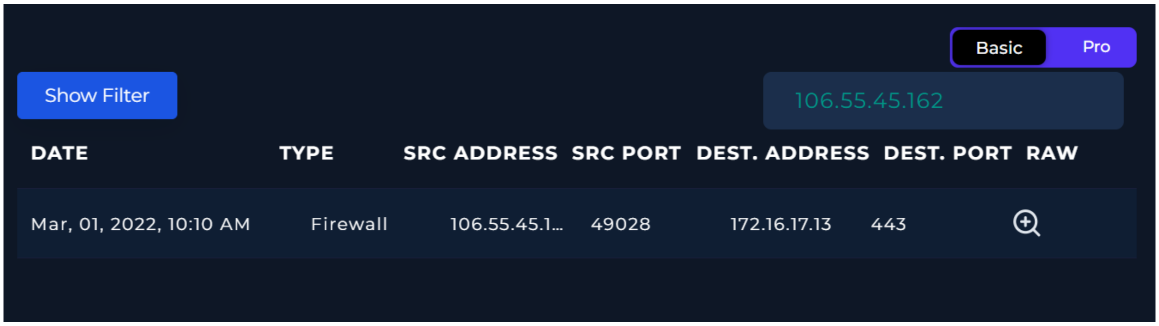
- I conducted a search in the Log Management system for all activities associated with the source IP **106.55.45.162**. I examined the server's response to the specific request: **/?file=../../../../etc/passwd.**



RAW LOG

```
Request URL:   https://172.16.17.13/?file=../../../../etc/passwd
User-Agent:   Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET
CLR 1.1.4322)
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   0
HTTP Response Status:   500
```

Figure 5: Log Management Alert.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 01, 2022, 10:10 AM	Firewall	106.55.45.1...	49028	172.16.17.13	443	⊕

Figure 6: Log Management Alert count.

Key Findings:

- HTTP Response Status: 500 (Internal Server Error).
- HTTP Response Size: 0 Bytes.
- Device Action: Permitted (by Firewall) but effectively failed at the application level.

Investigation Conclusion:

- The Status Code 500 indicates that the web server encountered an error and did not execute the malicious command. Furthermore, the Response Size of 0 confirms that no sensitive data (such as the contents of /etc/passwd) was returned to the attacker.

4. Is Traffic Malicious?

Decision: Yes.

Reasoning:

- Payload: Contains a clear LFI attack **(../../../../etc/passwd).**
- Reputation: The source IP has over 3,400 malicious reports on AbuseIPDB.
- Intent: Clear attempt to access sensitive system files from an unauthorized external source.

5. Planned Test Verification

- **Check for Simulation:**
  - A review of the internal communication and mailbox was performed. No scheduled penetration tests or vulnerability scans were found for **WebServer1006** during this timeframe.
- **Hostname/IP Check:**
  - The source IP and hostname do not belong to any known attack simulation products (e.g., Verodin, Picus).

Conclusion: This is **not** a planned test; it is an unauthorized external attack.

6. Attack Success & Direction

- **Traffic Direction:**
  - The traffic direction is **Internet -> Company Network** (Inbound).
- **Was the Attack Successful?**
  - **Answer: No.**
  - **Reasoning:** As documented in the Log Investigation, the server responded with an **HTTP 500 error** and **0 bytes** were transferred. The system successfully prevented the file inclusion.

7. Containment & Remediation

- **Device Isolation:**
  - **Decision:** No isolation is required for **WebServer1006** as the attack **failed** and there is no evidence of compromise.
- **Actions Taken:**
  - **IP Blacklisting:** Block **106.55.45.162** at the network perimeter.
  - **No Escalation/Containment:** Since the attack failed and the device is not compromised, Tier 2 escalation and device isolation are not required.

   - **Vulnerability Fix:** Patch the vulnerable file parameter on the web application.

8. Final Verdict

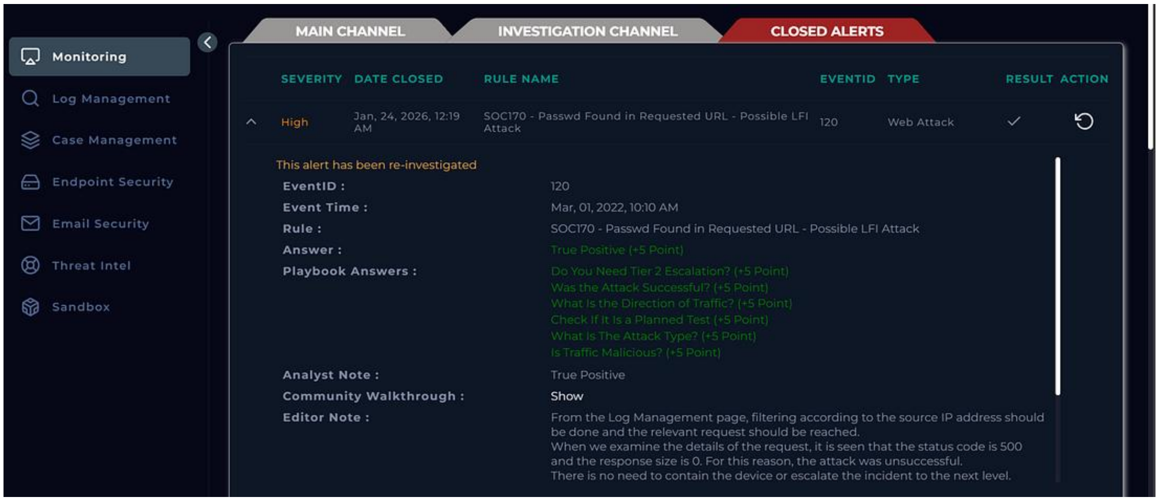
- **Status: True Positive.**
- **Note:** The alert is a True Positive because it detected a real malicious intent (LFI attempt), even though the attack was unsuccessful.

Conclusion & Playbook Verdict

Summary: The investigation confirms this is a **True Positive** case of a malicious **LFI (Local File Inclusion)** attempt. Although the attacker targeted sensitive system files, the attack **failed** at the application level (Status 500), and no data was compromised.

Final Decisions:

- **Is Traffic Malicious?** Yes.
- **Attack Type:** LFI (Local File Inclusion).
- **Planned Test:** No.
- **Traffic Direction:** Internet -> Company Network.
- **Was the Attack Successful?** No.
- **Tier 2 Escalation:** No.



SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
High	Jan, 24, 2026, 12:19 AM	SOC170 - Passwd Found in Requested URL - Possible LFI Attack	120	Web Attack	✓	⟲

This alert has been re-investigated

EventID :	120
Event Time :	Mar, 01, 2022, 10:10 AM
Rule :	SOC170 - Passwd Found in Requested URL - Possible LFI Attack
Answer :	True Positive (+5 Point)
Playbook Answers :	Do You Need Tier 2 Escalation? (+5 Point) Was the Attack Successful? (+5 Point) What Is the Direction of Traffic? (+5 Point) Check If It Is a Planned Test (+5 Point) What Is The Attack Type? (+5 Point) Is Traffic Malicious? (+5 Point)
Analyst Note :	True Positive
Community Walkthrough :	Show
Editor Note :	From the Log Management page, filtering according to the source IP address should be done and the relevant request should be reached. When we examine the details of the request, it is seen that the status code is 500 and the response size is 0. For this reason, the attack was unsuccessful. There is no need to contain the device or escalate the incident to the next level.

Figure 7: Final closure of Alert SOC170.