LetsDefend

Official incident report

Event ID: 189

Rule Name: SOC227 - Microsoft SharePoint Server Elevation of Privilege - Possible CVE-2023-29357 Exploitation

Made By

LinkedIn: Engineer.Ahmed Mansour

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

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

Table of contents

Event Details

Event ID:
189

Event Date and Time:
Oct, 06, 2023, 08:05 PM

Rule:
SOC227 - Microsoft SharePoint Server Elevation of Privilege - Possible CVE-2023-29357 Exploitation

Level:
Security Analyst

Hostname:
MS-SharePointServer

HTTP Request Method:
GET

Requested URL:
/_api/web/siteusers

User-Agent:
python-requests/2.28.1

User-Agent:
python-requests/2.28.1

Alert Trigger Reason:
This activity may be indicative of an attempt to exploit the CVE-2023-29357 vulnerability, which could potentially lead to unauthorized access and privilege escalation within the SharePoint server.

Device Action:
Allowed

Network Information Details

Destination IP Address:
172.16.17.233 internal

Source IP Address:
39.91.166.222 external

- **IP Address Details:**

Destination IP Address: 172.16.17.233

This is an internal IP address belonging to your company's MS-SharePointServer.

IP addresses in the range 172.16.0.0 to 172.31.255.255 are private, meaning they are used within internal networks and not routable on the public internet.

Source IP Address: 39.91.166.222

This is an external IP address. The 39.91.x.x range is a public IP, meaning it comes from outside your organization's internal network.

It indicates that the source of the request is coming from an external entity, potentially over the internet.

Conclusion:

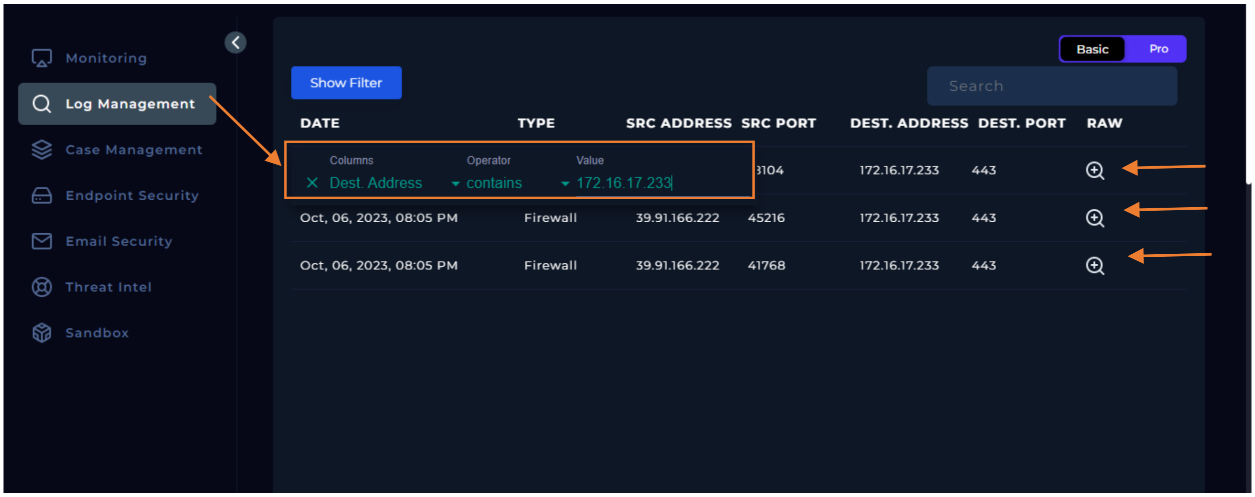
The attack originated from an external source (39.91.166.222) and was targeting an internal server (172.16.17.233). Since the source IP is not part of your internal network and belongs to a public IP range, this confirms that **the attack is external**.

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.



Columns: Dest. Address | Operator: contains | Value: 172.16.17.233

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
			3104	172.16.17.233	443	⊕
Oct, 06, 2023, 08:05 PM	Firewall	39.91.166.222	45216	172.16.17.233	443	⊕
Oct, 06, 2023, 08:05 PM	Firewall	39.91.166.222	41768	172.16.17.233	443	⊕

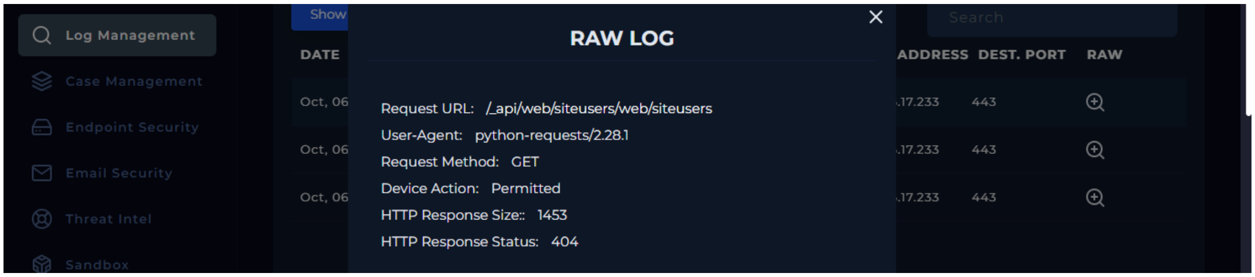
3 Logs records for the destination IP.

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

We will explain all of them step by step

Log Analysis

- **Log1:**



RAW LOG

```
Request URL:   /_api/web/siteusers/web/siteusers
User-Agent:   python-requests/2.28.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   1453
HTTP Response Status:   404
```

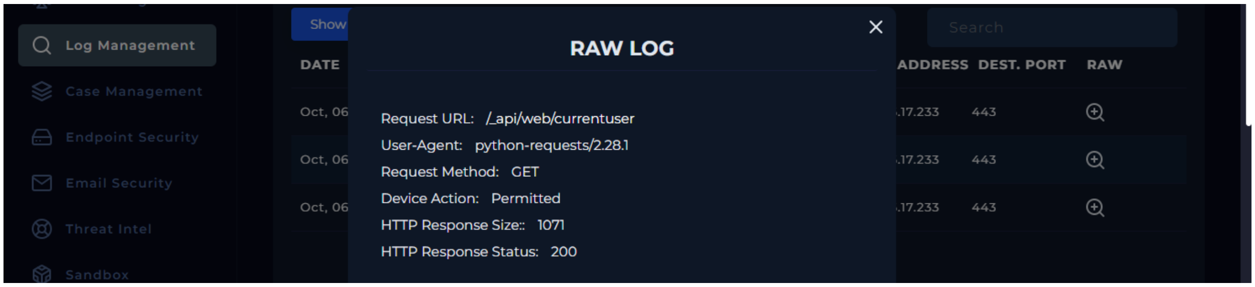
Request URL: `/_api/web/siteusers/web/siteusers`

- **User-Agent**: `python-requests/2.28.1`
  - This indicates that the request was made by a Python script using the `requests` library, version 2.28.1.
- **Request Method**: `GET`
  - A `GET` request is used to retrieve information from the server. In this case, the user is trying to access the `siteusers` endpoint, potentially to list the users of the site.
- **Device Action**: `Permitted`
  - The request was allowed by the device, meaning no security controls or restrictions blocked it at this point.
- **HTTP Response Size**: `1453`
  - The response size is 1453 bytes. This indicates the amount of data the server returned, despite an error response.
- **HTTP Response Status**: `404`
  - A `404` status code means "Not Found." The requested resource (`/web/siteusers/web/siteusers`) doesn't exist or couldn't be found on the server.

What Happened:

In this log, the Python script attempted to access an invalid or non-existent API endpoint (`/web/siteusers/web/siteusers`). The server responded with a `404 Not Found` error, indicating the resource is not available. The request was permitted, meaning no network or security rules blocked it.

- **Log2:**



```
Request URL:   /_api/web/currentuser
User-Agent:   python-requests/2.28.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   1071
HTTP Response Status:   200
```

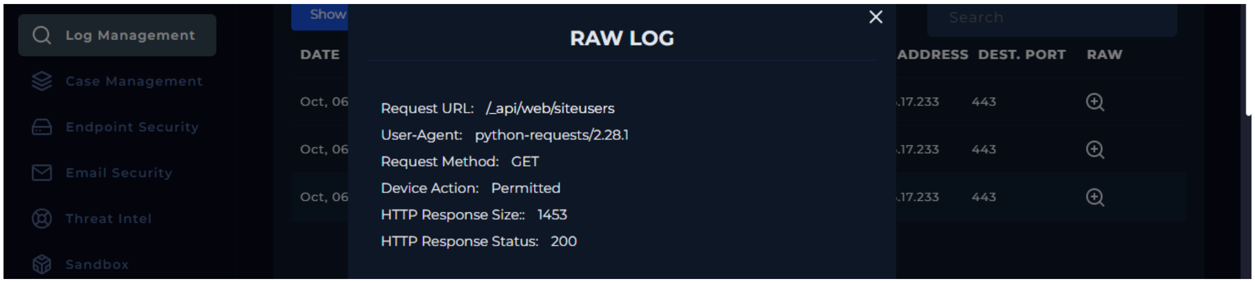
Request URL: `/_api/web/currentuser`

- **User-Agent**: `python-requests/2.28.1`
  - Again, a Python script using `requests` made this request.
- **Request Method**: `GET`
  - The script is attempting to retrieve information about the current authenticated user via the API.
- **Device Action**: `Permitted`
  - The request was allowed by the device.
- **HTTP Response Size**: `1071`
  - The response size is 1071 bytes, indicating a successful data retrieval.
- **HTTP Response Status**: `200`
  - The `200 OK` status means the request was successful, and the server returned the requested data.

What Happened:

In this case, the script successfully retrieved data about the current user using the `/currentuser` API endpoint. This response likely contains details about the authenticated user, such as their username, email, and permissions.

- **Log3:**



RAW LOG

```
Request URL:   /_api/web/siteusers
User-Agent:   python-requests/2.28.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   1453
HTTP Response Status:   200
```

Request URL: `/_api/web/siteusers`

- **User-Agent**: `python-requests/2.28.1`
  - A Python script using `requests` made this request as well.
- **Request Method**: `GET`
  - The script is trying to retrieve a list of all users on the site via the `/siteusers` API.
- **Device Action**: `Permitted`
  - The request was allowed by the device.
- **HTTP Response Size**: `1453`
  - The response size is 1453 bytes, likely containing data about the site users.
- **HTTP Response Status**: `200`
  - The `200 OK` status means the request was successful, and the server returned the requested data.

What Happened:

This log shows that the script successfully accessed the `/siteusers` API endpoint to retrieve a list of all users on the site. The data was returned in a 1453-byte response, which probably contains information such as usernames, user IDs, or other user-related metadata.

Summary of Events:

1. **First Log**: The script tried to access an invalid or non-existent API endpoint (`/web/siteusers/web/siteusers`) and received a `404 Not Found` error.
2. **Second Log**: The script successfully retrieved information about the current user using the `/currentuser` API, receiving a valid response (`200 OK`).
3. **Third Log**: The script successfully retrieved a list of site users using the `/siteusers` API, also receiving a valid response (`200 OK`).

Possible Context:

- These logs suggest a Python script or automated tool is attempting to interact with a web application's API, likely for user enumeration. The failed request (log 1) may indicate a misconfigured or outdated script, while the successful requests (logs 2 and 3) show that the script is able to query user-related information.

Security Considerations:

- **User Enumeration**: The script appears to be trying to gather user information from the site. This could be part of legitimate activity (e.g., an admin tool or user audit), but it could also indicate **reconnaissance** activity by an attacker trying to enumerate users on the system.
- **Automated Scripts**: Since the requests are coming from a Python script, it's important to validate whether this activity is authorized or potentially malicious.

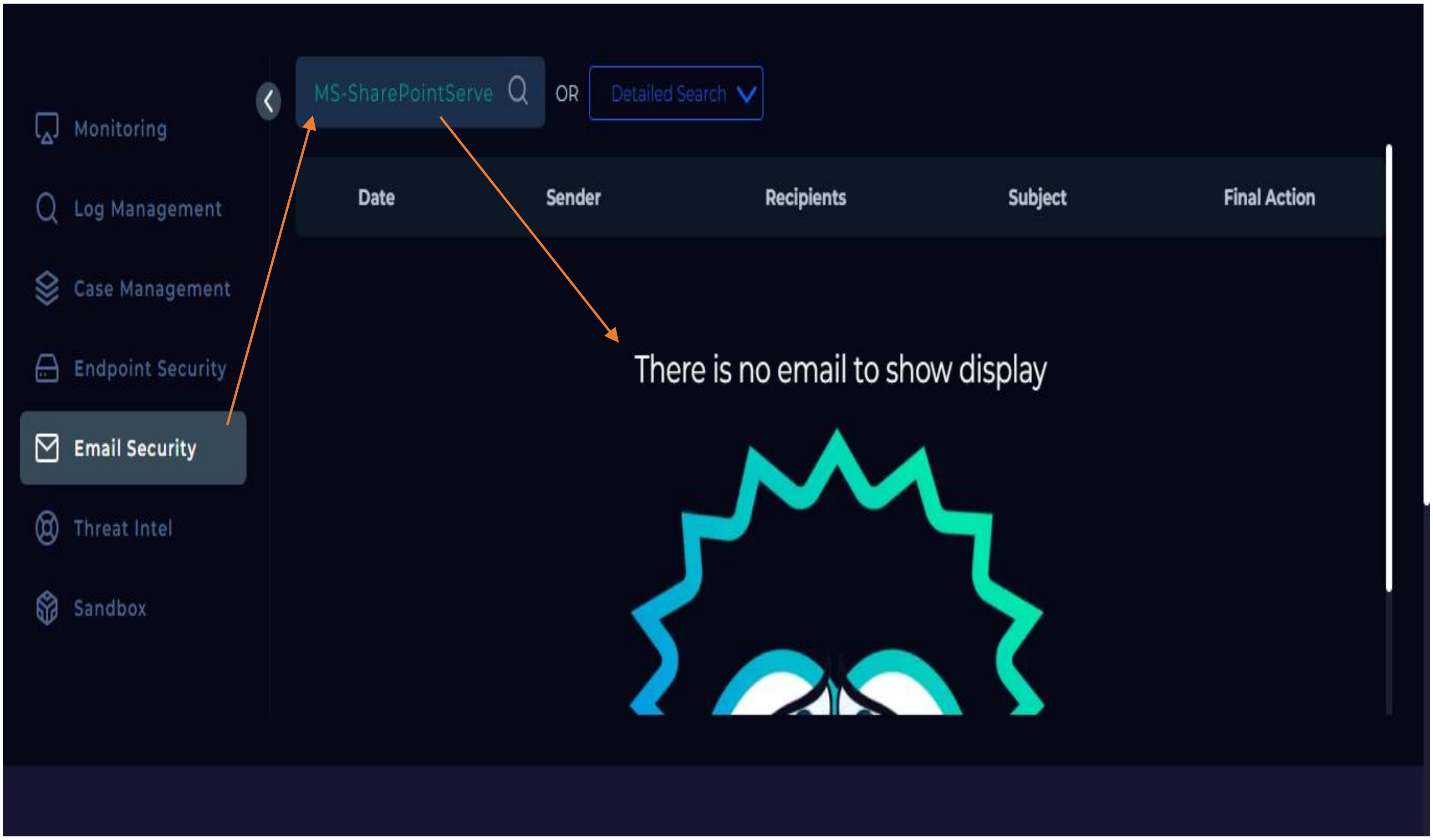
Based on the analysis, it has been determined that the attack was **successful**. The identified attack vector appears to involve **API enumeration or reconnaissance**, rather than the following common attack types:

- **Command Injection**: No evidence of command execution or injection was detected on the server.
- **IDOR (Insecure Direct Object Reference)**: No signs of object reference manipulation are present in the logs.
- **LFI/RFI (Local/Remote File Inclusion)**: No attempts to access local or remote files were observed.
- **SQL Injection**: There is no indication of SQL query manipulation or database exploitation.
- **XML Injection**: No interaction with XML-based inputs or manipulation of XML was identified.
- **Cross-Site Scripting (XSS)**: No scripts or payloads targeting the client-side environment were injected.

Recommendation:

Due to the confirmed nature of the attack and the potential risk to internal systems, **immediate escalation to Tier 2 support** is required for further investigation and response.

Email Security:



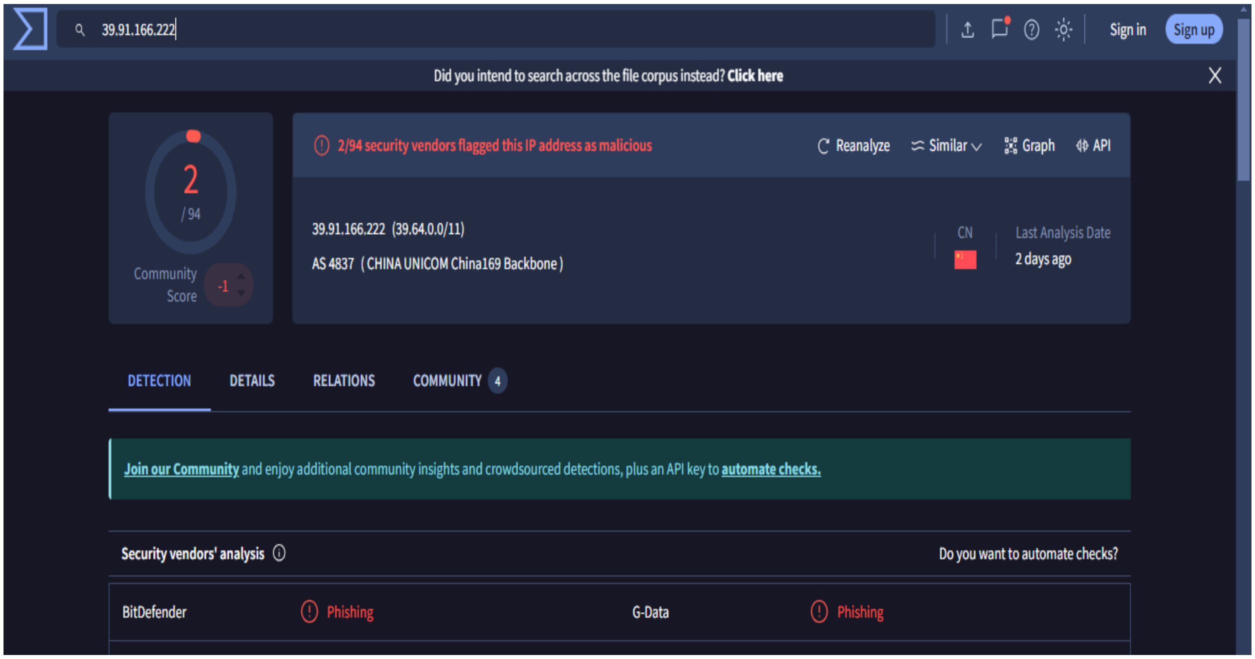
There is no email to show display

- **Despite entering the source host name in the email security section, no emails have been sent, indicating that the attack was not executed.**

Detection:

Threat Intelligence Results

We will conduct a comprehensive scan of the source IP address using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



39.91.166.222

Did you intend to search across the file corpus instead? **Click here**

2
/ 94

Community Score -1

2/94 security vendors flagged this IP address as malicious

39.91.166.222 (39.64.0.0/11)

AS 4837 (CHINA UNICOM China169 Backbone)

CN

Last Analysis Date
2 days 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?

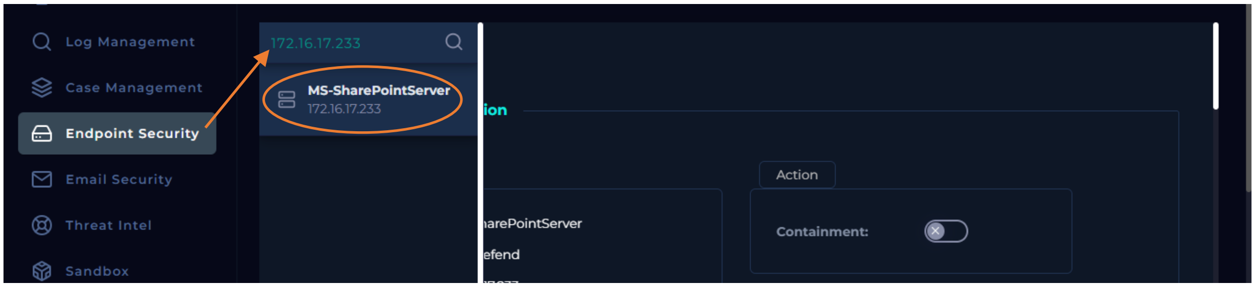
BitDefender	Phishing	G-Data	Phishing

- Reference result.
- **Origin**: China
- **Security Vendor Detection**:
  - **2/94 security vendors** have flagged this IP address as malicious, specifically for **phishing** activities:
    - **BitDefender**: Phishing
    - **G-Data**: Phishing

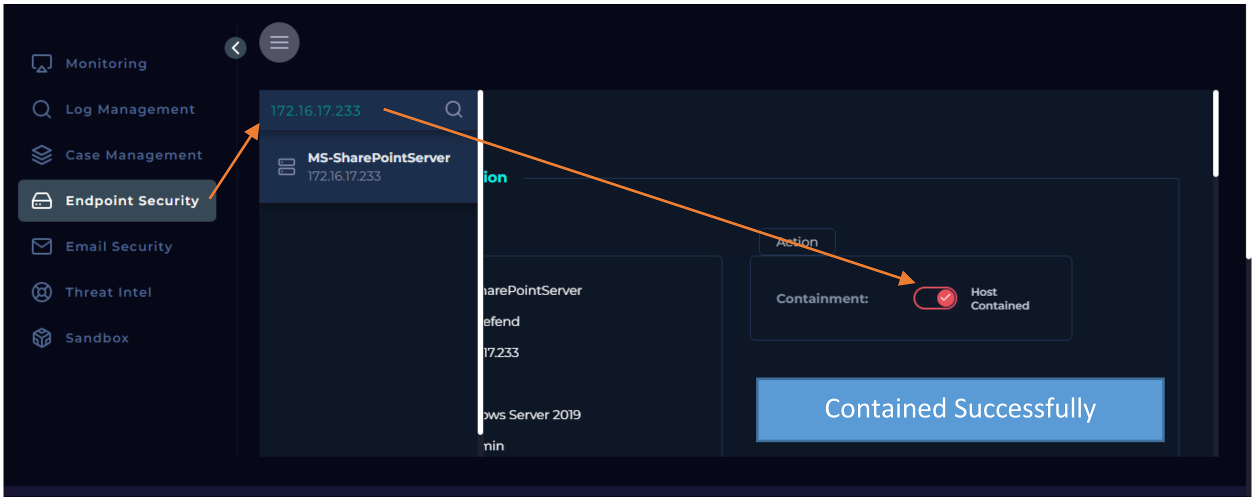
Malware Analysis Report:

- **Source**: Automated report from Levallois-Perret, France.
- **Date**: Sun, 01 Oct 2023, 19:01:16 +0200.
- **Incident**: The IP address **39.91.166.222** was observed performing an **SSH brute-force attack** or using stolen credentials.
- **The Traffic is Malicious**

Endpoint Security:



- **Based on our analysis, the reconnaissance activity identified is focused on gathering victim and company user's identity information's.**
- **The device must be Contain. And we contained Successfully**.



Conclusion:

The incident involving **Event ID 189** reveals a successful reconnaissance attack originating from an external IP address, **39.91.166.222**, targeting the internal **MS-SharePointServer** at IP **172.16.17.233**. The attacker leveraged **API enumeration**, potentially attempting to exploit **CVE-2023-29357**, a vulnerability in Microsoft SharePoint that could result in unauthorized access and privilege escalation.

Three separate `GET` requests were detected in the logs, all utilizing the **Python `requests` library (version 2.28.1)**. The requests targeted sensitive API endpoints, specifically `/siteusers` and `/currentuser`. The first request resulted in a `404 Not Found` error, indicating an attempt to access a non-existent endpoint. However, the subsequent requests were successful, returning HTTP `200 OK` responses with user-related data, potentially including usernames and user IDs, indicative of a **user enumeration attempt**.

The source IP was identified as external, originating from **China**, and flagged by **VirusTotal**. Two security vendors, **BitDefender** and **G-Data**, identified the IP as associated with phishing activities. Furthermore, the IP had been previously reported for malicious SSH brute-force attacks, strengthening the suspicion of malicious intent.

Given the confirmed reconnaissance activity and potential vulnerability exploitation, immediate action was taken to successfully contain the affected device. However, the attack's success in accessing user information suggests a heightened risk for future attempts at privilege escalation or further exploitation.

Due to the severity of this incident, **escalation to Tier 2 support** is strongly recommended for deeper investigation. It is crucial to review the SharePoint server's security posture, ensure patching against **CVE-2023-29357**, and enhance monitoring of external connections to safeguard against further threats.