

Incident Analysis Report

1. Alarm Information

- **Alarm ID / Case No:** 006
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** Phishing from outdoor-project[.]eu
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

2. IOC Information

- **IOC Type:** outdoor-project[.]eu
- **IOC Value:**
- **IOC Location:** [unknown]

3. OSINT Investigation

VirusTotal

- Result: Detected by 1 AV engine (High confidence).
- <https://www.virustotal.com/gui/domain/outdoor-project.eu>

The screenshot shows the VirusTotal interface for the domain `outdoor-project.eu`. At the top, it displays a summary: "11/94 security vendors flagged this domain as malicious". Below this is a card for `outdoor-project.eu`, showing a `tmp-1M` file. To the right, there are buttons for "Reanalyze", "Similar", and "More". A timestamp indicates the "Last Analysis Date" was 16 hours ago. On the left, there's a "Community Score" of 11/94. Below the summary are tabs for "DETECTION", "DETAILS", "RELATIONS", and "COMMUNITY". The "DETECTION" tab is selected, showing a table of "Security vendors' analysis". The table lists various vendors and their findings:

| Vendor | Result | Vendor | Result |
|------------------|-----------|---------------------|-----------|
| alphaMountain.ai | Phishing | CyRadar | Malicious |
| ESET | Phishing | Fortinet | Phishing |
| G-Data | Phishing | Google Safebrowsing | Phishing |
| Seclookup | Malicious | SOCRadar | Malicious |
| Sophos | Phishing | Trustwave | Phishing |
| Webroot | Malicious | Abusix | Clean |
| AegisLab | Clean | ADMINISTRATOR | Clean |

URLscan.io

- Result: **Malicious**

- <https://urlscan.io/result/0198db60-82fa-7127-9f26-0c284c661310/>

4. Analysis & Assessment

- Result: Detected by 1 AV engine (High confidence).
- URLscan.io Result: Detected by 1 AV engine (High confidence).

5. Conclusion / Decision

- **Decision:**  True Positive
 - **Category:** Phishing
 - **Risk Level:** High risk (based on organization's classification)
-

6. Recommended Actions

1. Block the IP address on firewall / IPS.
2. Review SIEM logs for additional login attempts from the same source.
3. Correlate failed logins with user accounts for potential compromise attempts.
4. Consider implementing automated blocking rules for IPs with high abuse scores.