Threat Intelligence Report for PrimeSoft Solutions

Executive Summary

This project demonstrates the practical application of threat intelligence processes for detecting and analyzing malicious infrastructure. Using suspicious IP addresses gathered from primesofts firewall, SSH logs and phishing emails, I applied enrichment techniques with VirusTotal to assess their maliciousness. The project highlights how to extract and clean Indicators of Compromise (IOCs), investigate them with open-source threat intelligence tools, and correlate results across multiple sources. Findings were mapped to the MITRE ATT&CK framework to provide contextual understanding of attacker tactics, techniques, and procedures (TTPs). This documentation showcases both technical skills and the ability to produce actionable intelligence reports for stakeholders.

Introduction

With the increase of phishing and brute-force SSH attempts, this project was designed to simulate a real-world threat intelligence workflow. Logs and phishing emails were parsed to extract suspicious IPs, which were then enriched using VirusTotal and other threat intel platforms to validate malicious activity.

Objectives

- The objectives of this project were to:

- Extract IOCs from logs and phishing emails.
- Clean and organize IP addresses for analysis.
- Enrich IP reputation with VirusTotal.
- Correlate malicious indicators across multiple sources.
- Map findings to MITRE ATT&CK techniques.
- Document results in a professional threat intelligence report.

Tools Used

- VirusTotal
- MITRE ATT&CK Framework

Methodology

The workflow for this project involved the following steps:

1. Data Extraction – Collected IP addresses from logs and phishing email headers.

2. Data Cleaning – Removed duplicates and formatted IPs into Excel.

3. IOC Enrichment – Queried VirusTotal for reputation, geolocation, and campaign associations.

4. Correlation – Cross-checked IPs across logs and emails to find overlaps.

5. Threat Mapping – Mapped results to MITRE ATT&CK techniques (e.g., T1566 Phishing, T1110 Brute Force).

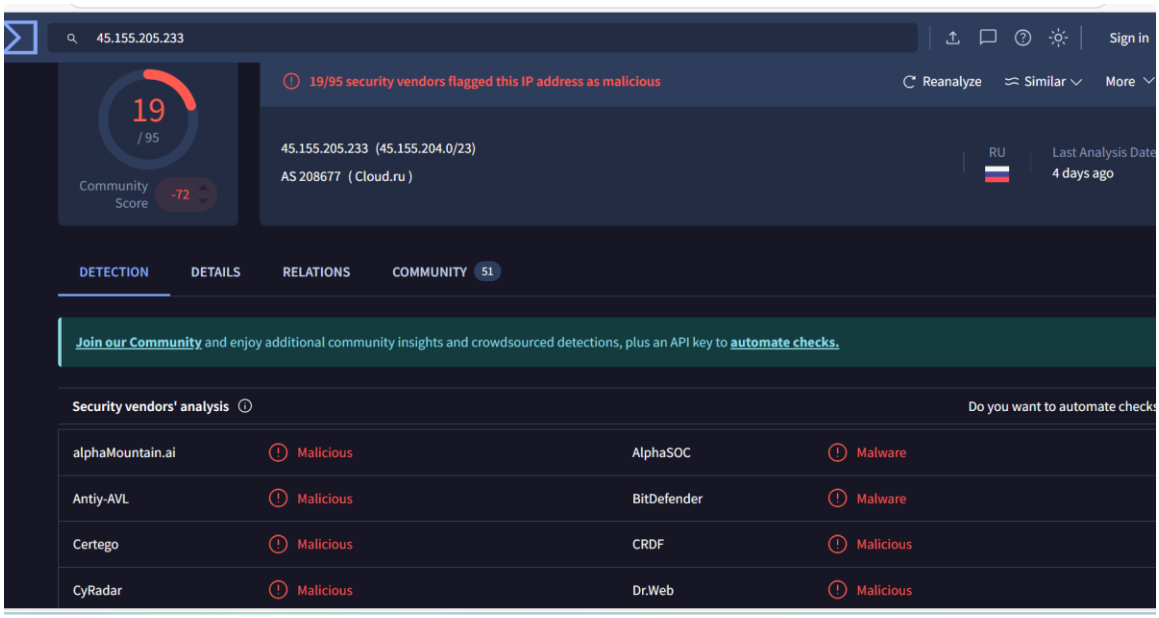
6. Documentation – Results compiled into Excel and summarized in this report.

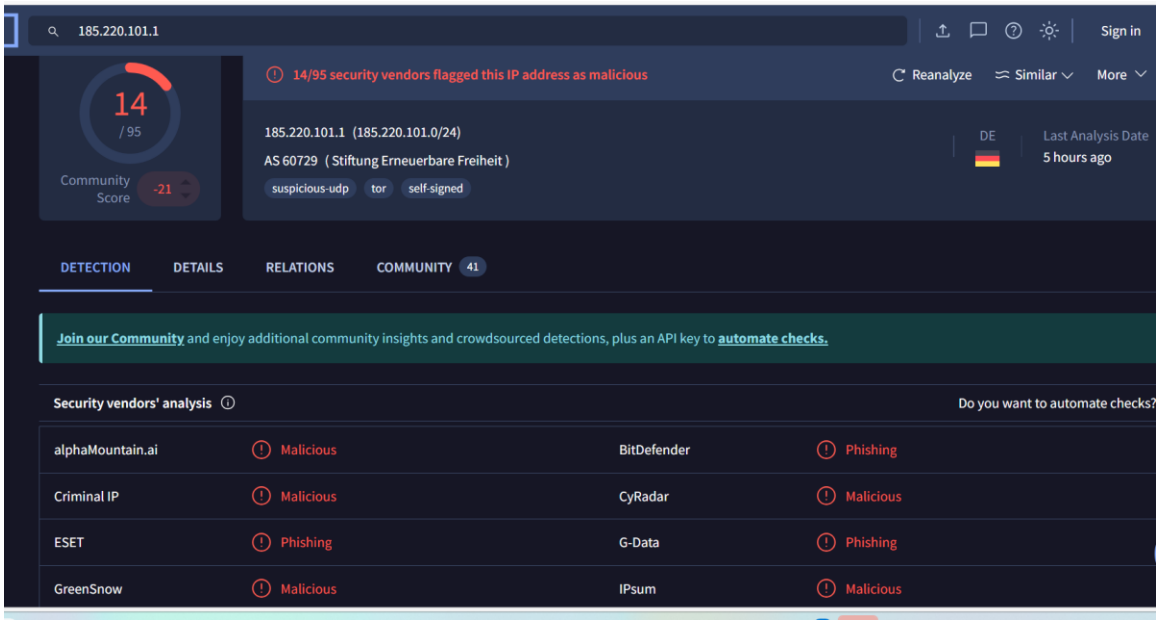
Results

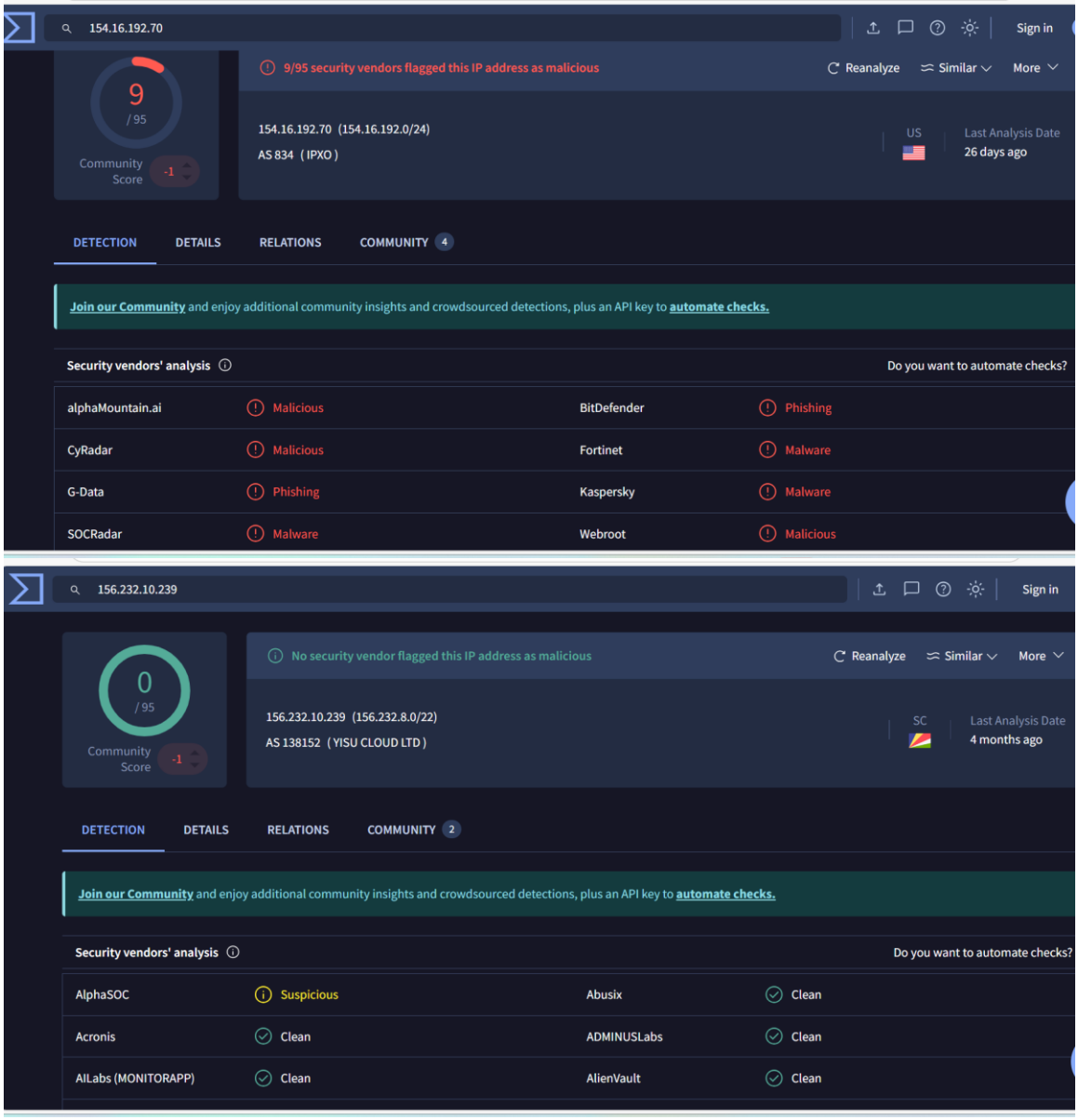
The analysis included several suspicious IPs. The majority were confirmed as malicious by VirusTotal, with associations to phishing and brute-force activities. Key findings include:

- Number of IPs analyzed.
- Percentage flagged as malicious vs clean.
- Geographical hotspots (e.g., concentration from specific regions).
- Malware families or campaigns linked to the IPs.

See below sample screenshots from VirusTotal




185.220.101.1
Sign in
14
/ 95
Community Score
-21
14/95 security vendors flagged this IP address as malicious
Reanalyze
Similar
More
185.220.101.1 (185.220.101.0/24)
AS 60729 (Stiftung Erneuerbare Freiheit)
suspicious-udp
tor
self-signed
DE
Last Analysis Date
5 hours ago
DETECTION
DETAILS
RELATIONS
COMMUNITY 41
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?
alphaMountain.ai
Malicious
BitDefender
Phishing
Criminal IP
Malicious
CyRadar
Malicious
ESET
Phishing
G-Data
Phishing
GreenSnow
Malicious
IPsum
Malicious



Analysis & Correlation

The correlation of IPs across firewall logs and auth.logs and phishing emails revealed overlaps suggesting coordinated attacker infrastructure. The findings were mapped to MITRE ATT&CK techniques, providing insights into adversary tactics such as phishing (T1566), brute-force (T1110), and malicious link execution (T1204.001).

Lessons Learned

• IOC enrichment is critical before making security decisions.
• Cross-correlation of data sources improves visibility of attacker operations.
• Mapping to MITRE ATT&CK standardizes the analysis and helps communicate findings effectively.

Conclusion & Recommendations

This project demonstrated the threat intelligence lifecycle from extraction, enrichment, and correlation to reporting. The findings reinforce the importance of continuous monitoring and proactive threat hunting. Recommendations for enterprises include blocking malicious IPs, automating IOC enrichment workflows, and integrating threat intelligence platforms with SIEM for enhanced detection.

Appendices

• IOC Results Excel file containing enriched IP addresses.
• Screenshots from VirusTotal highlighting sample malicious detections.
• Workflow diagram illustrating the process from extraction to reporting.