SOC CAPSTONE REPORT

Threat Detection & Incident Response using:

Wireshark, pfSense and Wazuh

SoCra Tech

Lum Rina Ngwan
Role: Security Operations Center (SOC) Analyst

Date: 25th April 2025

Table of Content

Executive Summary

With the use of networking industry tools such as Wireshark, pfSense, and Wazuh, an elaborated three-phase Soc analysis was conducted for a growing technology solution provider SoCra Tech. The main objectives were to detect and respond to network anomalies, prevent malicious traffic, and investigate potential security threats. During the analysis, multiple critical Indicators of Compromise (IoCs) were detected and effectively mitigated. With regards to the outcome, final recommendations were provided to enhance the organization's overall cybersecurity posture.

Project Scenario

SoCra Tech recently observed a surge in network anomalies, prompting concerns related to potential malware infections, unauthorized access, and insider threats. In response, I was assigned as part of the SOC team to deploy security monitoring tools, capture and analyze network traffic, and respond to emerging threats using industry-standard methodologies. This report details the strategic approach, implementation process, and key findings of the investigation.

Methodology

A structured, multi-phase approach was used to assess and secure the network environment. This included;

- **Wireshark:** deployed to perform network sniffing and packet-level analysis, aiding in the identification of unusual traffic patterns and potential threats.
- **pfSense:** configured to serve as a perimeter firewall, enforce geo-restrictions on internet access, and manage IDS/IPS rules to detect and block suspicious activities in real time.
- **Wazuh:** implemented as a centralized SIEM platform, enabling comprehensive

log ingestion, real-time event correlation, threat hunting, and coordinated incident response.

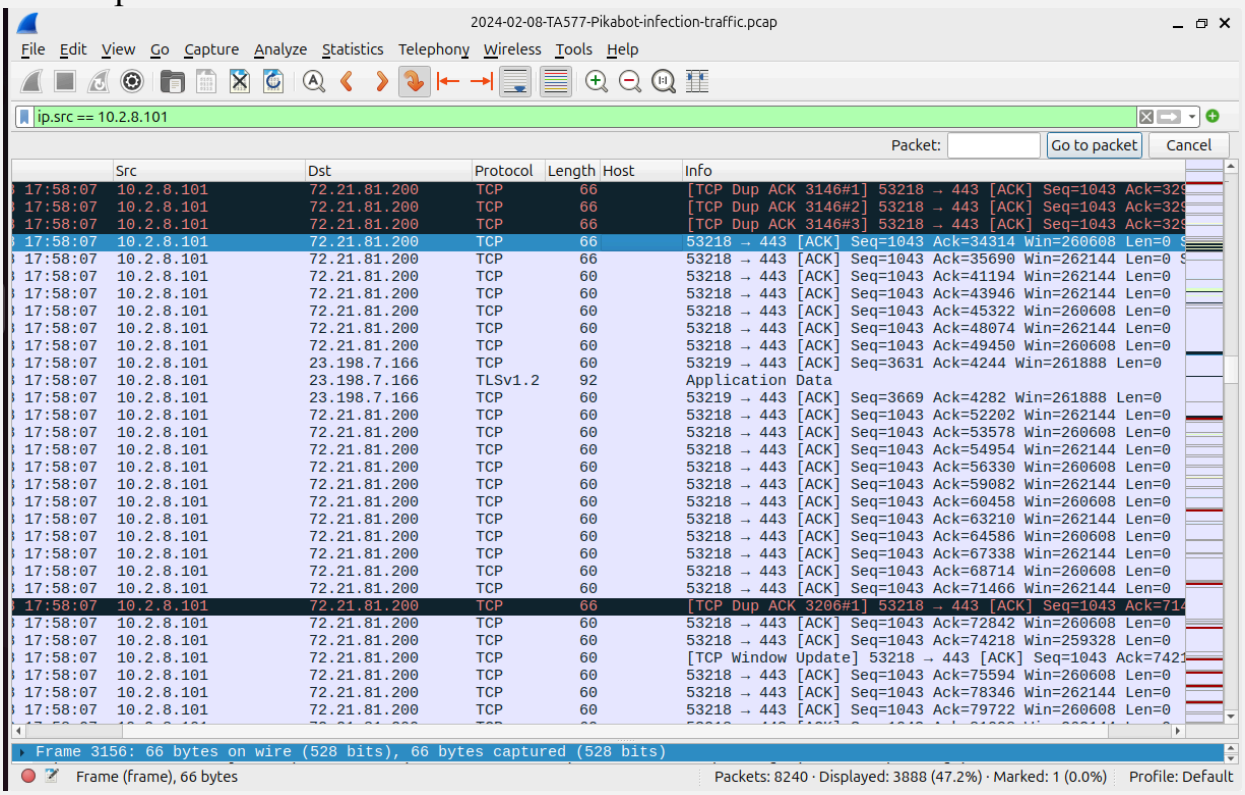
Phase 1: Wireshark – Network Sniffing & Packet Analysis

Objective: Capture and analyze suspicious network behavior such as malware behavior and unauthorized connections.

Key Action: Focus on HTTP, DNS, SSH traffic

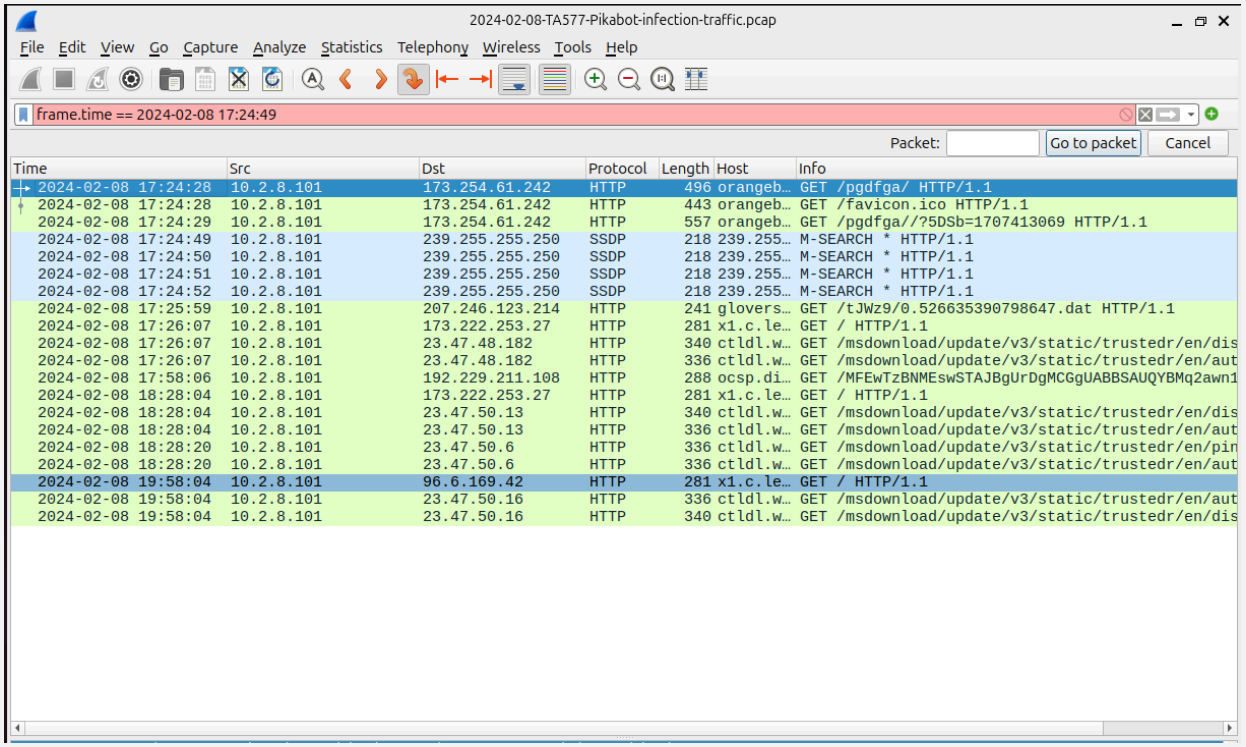
Findings

1. **Malware beaconing**: Endpoint ([redacted]) within the corporate network was found to periodically attempt to report back to a suspected C2 server.



Source: screenshot from wireshark packet traffic.

2. **Data Exfiltration:** Endpoint ([redacted]) attempted to exfiltrate data via HTTP to a remote location ([redacted]) which was resolved to a cloud storage service.



Source: screenshot from wireshark packet traffic.

Phase 2: pfSense – Firewall & Policy Enforcement

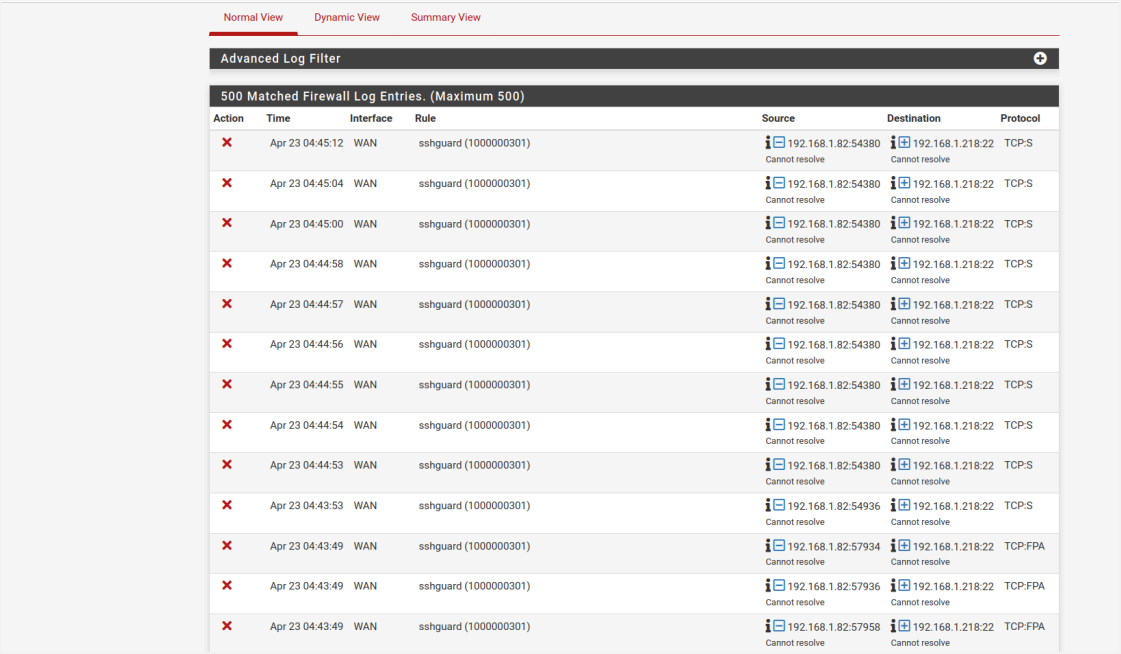
Objective: Configure firewall rules to regulate traffic flow in accordance with the company's security policies and access requirements.

Key Actions:

1. Configure GeoIP filtering to restrict access to and from high risk Countries
2. Block all SSH traffic from public addresses to mitigate unauthorized access attempt
3. Setup IDS alerting and IPS blocking rules
4. Analyze firewall logs for malicious traffic and threat actors
5. Setup centralized log aggregation with Wazuh

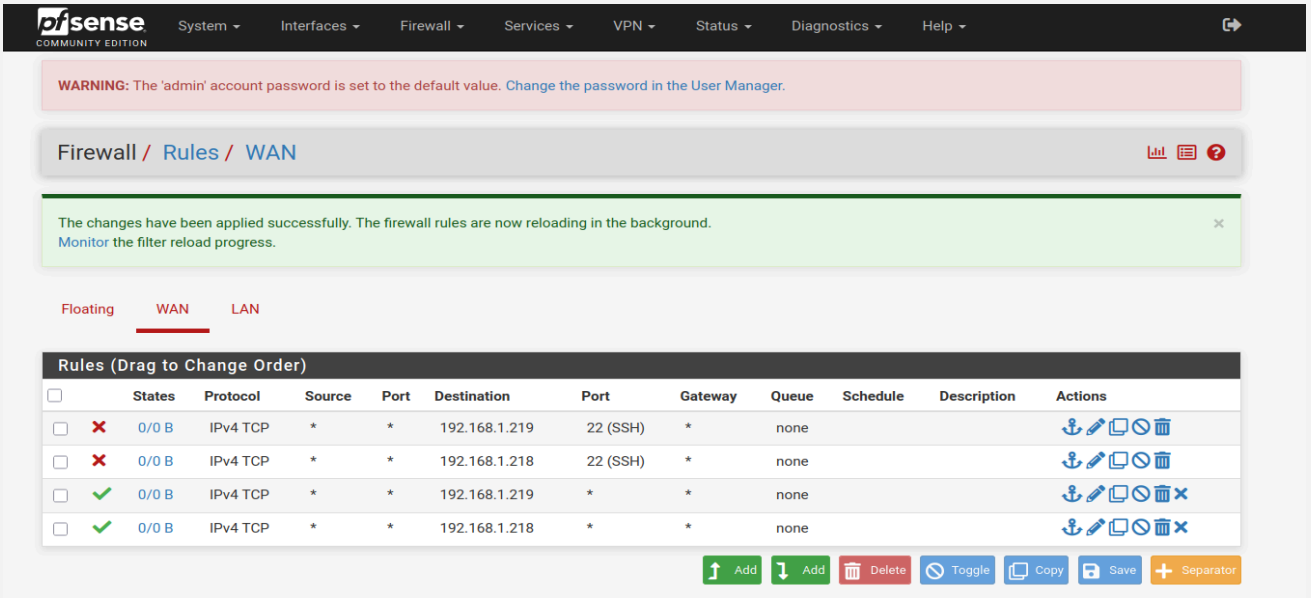
Findings:

1. Lateral Movement: Multiple unauthorized SSH login attempts to access Admin account for the firewall.



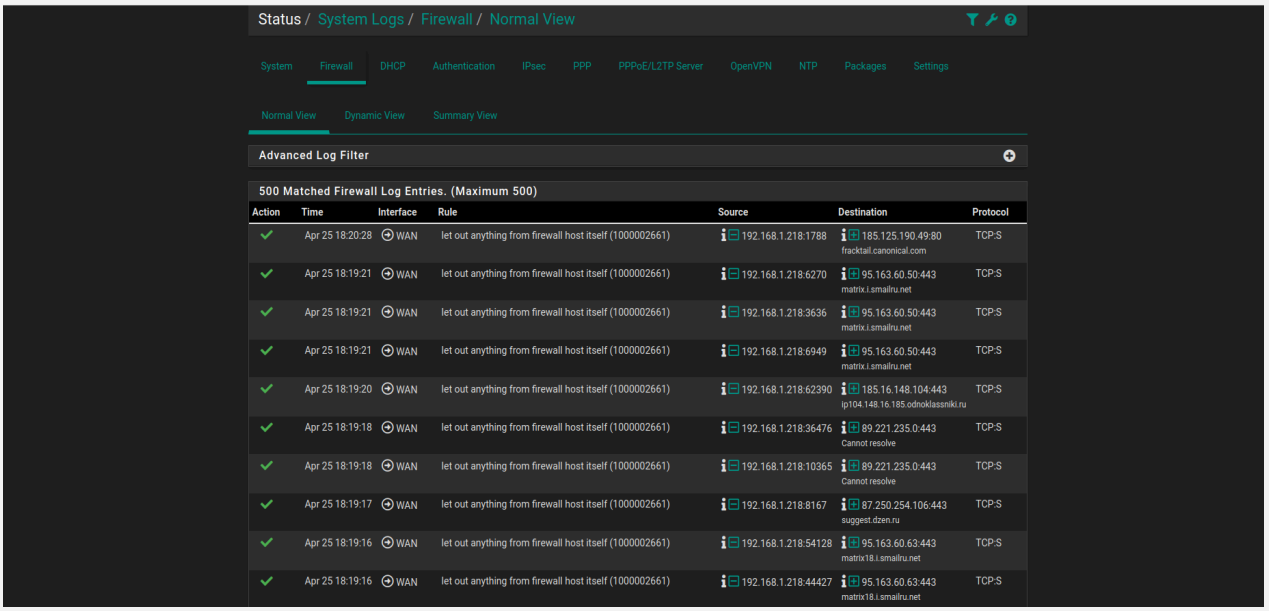
Source: pfsense dashboard/pfblockerNG net devel/GeoIP

Mitigated finding above by updating firewall rules to block all SSH traffic from external addresses as shown below.



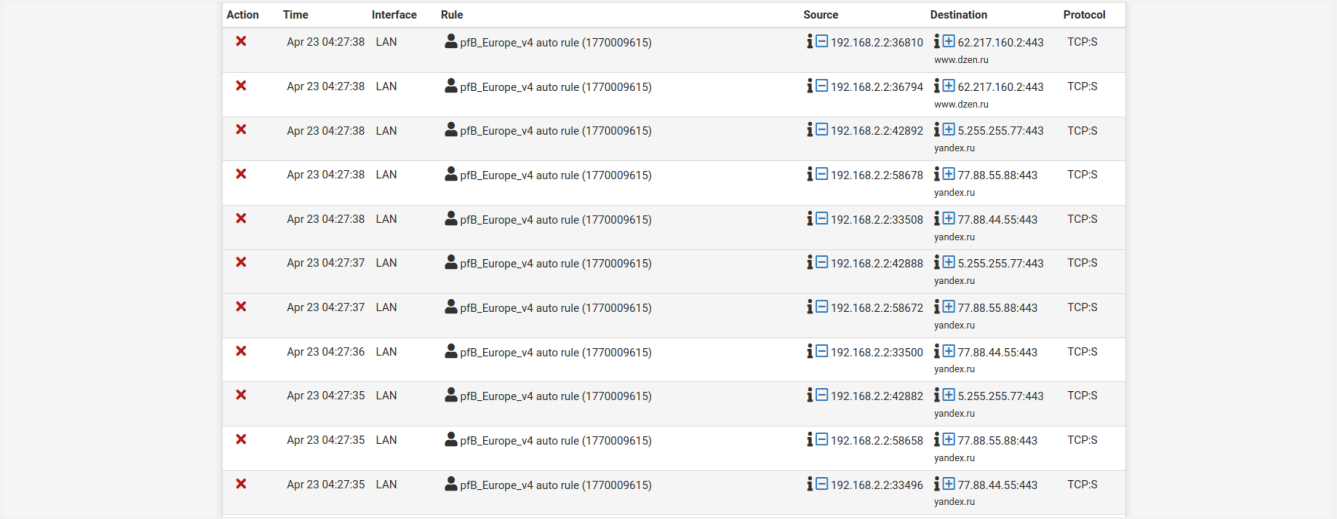
Source: pfsense firewall dashboard

2. Multiple outbound connections were made to high risk countries as seen in the firewall log below.



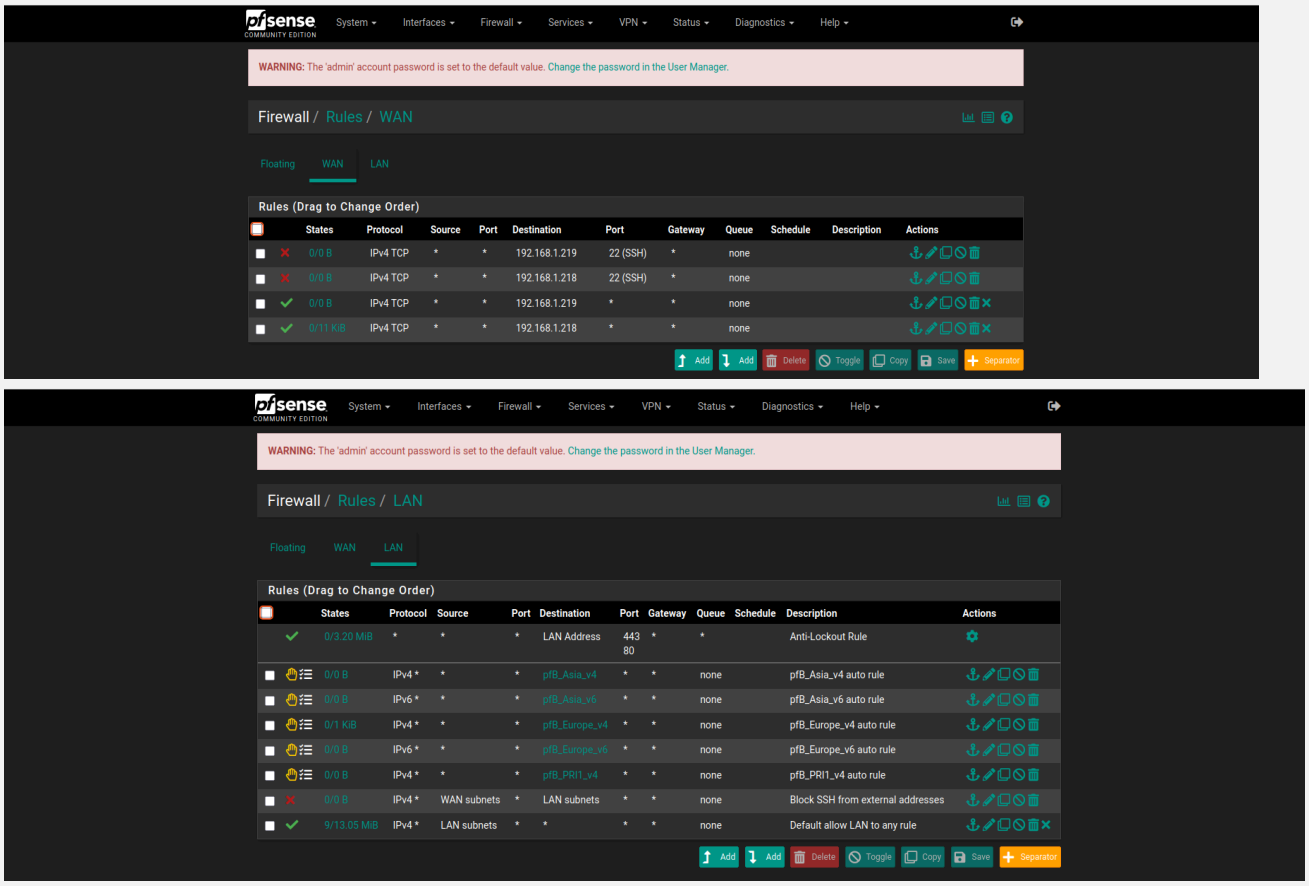
Source: screenshot pfsense/system/logs

Mitigated finding above by enabling GeoIP filtering to prevent access to high risk countries and potentially malicious websites as seen below



Source: screenshot pfsense/system/logs

3. Firewall rules were created to enforce company policy for internet access and security as shown below



Source: screenshot pfsense/rules/WAN

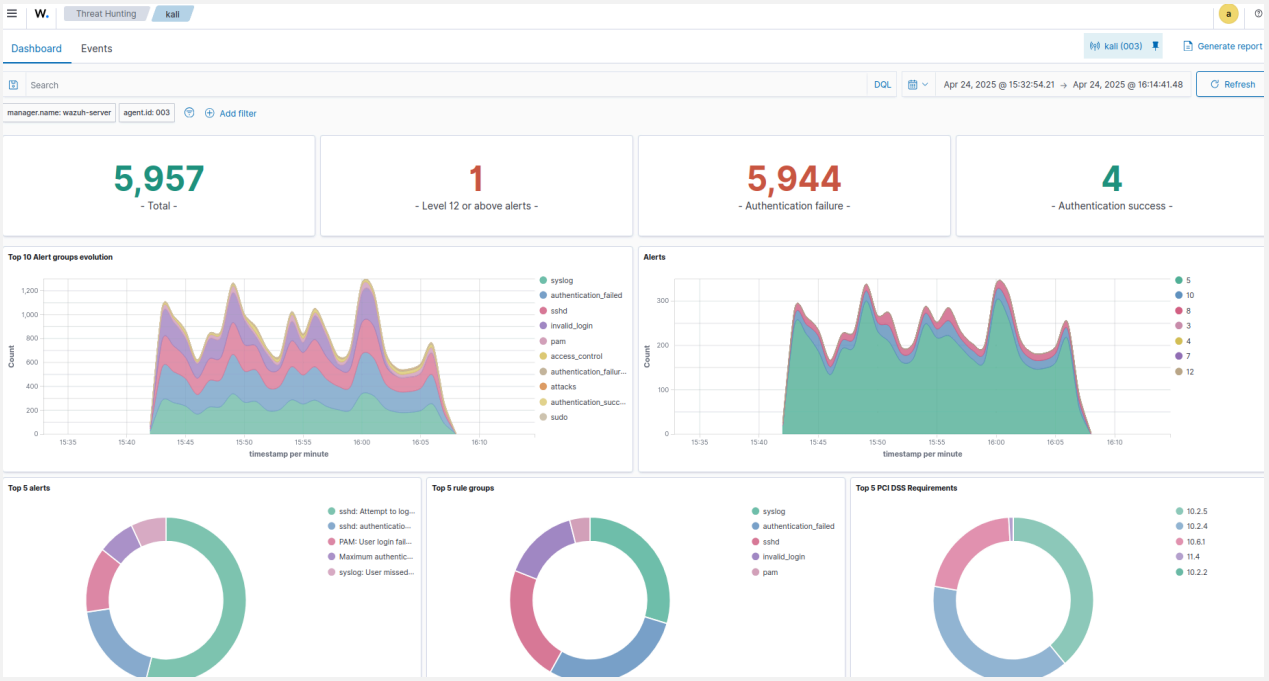
Phase 3: Wazuh – Security Event Monitoring & Response

- **Aim:** Aggregate logs and respond to security incidents
- **Key Actions:**
    - Configure log forwarding from pfSense and endpoints
    - Perform threat hunting to identify indicators of compromise
    - Set up alert rules for brute force attack and privilege escalation.

Findings:

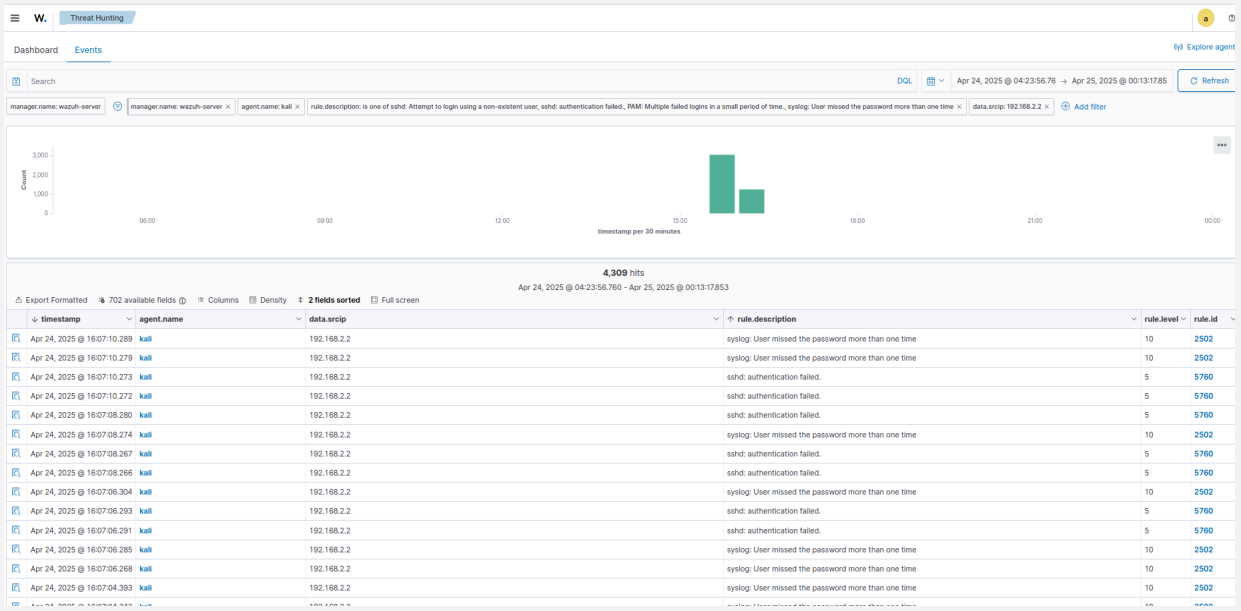
Multiple alerts correlated with anomalies identified in Wireshark and pfSense.

1. Brute Force Attack: SIEM alert dashboard showing over five thousand failed authentication attempts, which correlates with Wireshark findings (Image 3, phase 1) above. A clear indicator of a brute force attack.



Source: wireshark threat hunting dashboard

Image below shows a more detailed view of the brute force attack referenced in phase 1(image3) above.



Source: wireshark threat hunting dashboard

Final Findings and Impacts

The engagement confirmed that SoCra Tech was susceptible to

1. Brute force attacks due to improperly configured endpoints and firewall rules.
2. In the event of a breach, improperly set up network segmentation and data loss prevention makes lateral movement and data exfiltration effortless.
3. Improperly setup firewall rules and filters permitted access to potentially malicious internet resources.
4. Lack of staff training allowed for a successful phishing campaign that created initial access for malicious actors.

Recommendations

1. Based on findings, the following are recommended:
2. Staff training and sensitization to reduce the risk of successful phishing attacks.
3. Setup more restrictive firewall rules and filtering.
4. Adopt principle of least privilege for all user accounts.
5. Deploy a DLP on the network to prevent data exfiltration.
6. Disable all unused protocols on the network.
7. Perform regular vulnerability assessment and management.

Conclusion

In a nutshell, with regards to the SOC analysis project carried out for SoCra Tech, a realistic approach to network defense, allowing us to apply detection, monitoring, and incident response using professional tools such as Wireshark, Pfsense and Wazuh. The threats uncovered and mitigated serve as a wake-up call for proactive security posture improvement at SoCra Tech.