THREAT HUNTING & THREAT INTELLIGENCE PIPELINE

Made by: **CyberSentinels**

Table of Contents

1 Introduction

This project aims to design and implement a proactive **Threat Hunting and Threat Intelligence (CTI) Pipeline** that integrates open-source intelligence (OSINT) feeds, threat actor profiling, and behavioral analytics to detect and understand advanced persistent threats (APTs). The focus of this project is on **APT41**, a sophisticated cyber-espionage and financially motivated threat group.

The pipeline leverages the **Elastic Stack (Elasticsearch, Logstash, Kibana, Beats)** for data ingestion, visualization, and hunting, integrated with **MISP** for threat intelligence enrichment and IOC (Indicators of Compromise) management.

---

2 Environment Setup

Platform: Ubuntu Server (VM)
SIEM: Elastic Stack (ELK)
Threat Intelligence Platform: MISP (Malware Information Sharing Platform)
Attack Simulation Tools: Nmap / Atomic Red Team
Network & Log Sources: System logs, simulated attack telemetry, and network traffic (pcap/Wireshark).

---

3 Project Phases

3.1 Week 1: Threat Intelligence and IOC Enrichment

Goal: Integrate threat intelligence feeds and classify known adversaries using MITRE ATT&CK.

- **Setup:** Deploy MISP and connect to CTI feeds such as AlienVault OTX.
- **Enrichment:** Collect and normalize IOCs (domains, IPs, hashes, URLs) associated with APT41.
- **Classification:** Use the MITRE ATT&CK framework to map APT41's techniques and tactics.
- **Deliverables:**
  - IOC Enrichment Documentation (source feeds, indicators, correlation results)
  - Threat Actor Profile Report (APT41 overview, TTPs, campaigns, detection relevance)

3.2 Week 2: Threat Hunting Lab

Goal: Conduct controlled attack simulations to generate realistic data for hunting.

- **Setup:** Create a virtualized lab environment using vulnerable hosts and attacker systems.
- **Execution:** Simulate intrusions mimicking APT41's known TTPs (e.g., credential dumping, web shell deployment).
- **Data Capture:** Collect logs and network data using Beats (Winlogbeat) and wireshark and forward them to Elasticsearch.
- **Hunting:** Use Kibana to query, visualize, and identify suspicious behavior in the collected data.
- **Deliverables:**
  - Screenshots and log analysis of hunting activities.
  - Threat Hunting Hypothesis & Findings Report.

3.3 Week 3: Tactics, Techniques, and Procedures (TTPs) Mapping

Goal: Map observed behaviors to MITRE ATT&CK and evaluate detection coverage.

- **Mapping:** Identify which APT41 behaviors appeared in your dataset and align them with corresponding ATT&CK techniques.
- **Visualization:** Use MITRE ATT&CK Navigator to build a heatmap of covered and uncovered techniques.
- **Analysis:** Highlight detection gaps where current telemetry does not provide visibility.
- **Deliverables:**
  - ATT&CK Navigator Heatmap.
  - Detection Gaps Analysis Report.

3.4 Week 4: Reporting & Final Presentation

Goal: Consolidate the project outcomes and present the complete threat hunting and intelligence pipeline.

- **Report:** Summarize findings across all weeks — intelligence collection, attack simulation, detection results, and TTP mapping.

- **Recommendations:** Provide remediation and detection improvement steps based on gap analysis.
- **Deliverables:**
  - Final CTI & Threat Hunting Report.
  - Presentation: End-to-end story of detecting and profiling APT41.

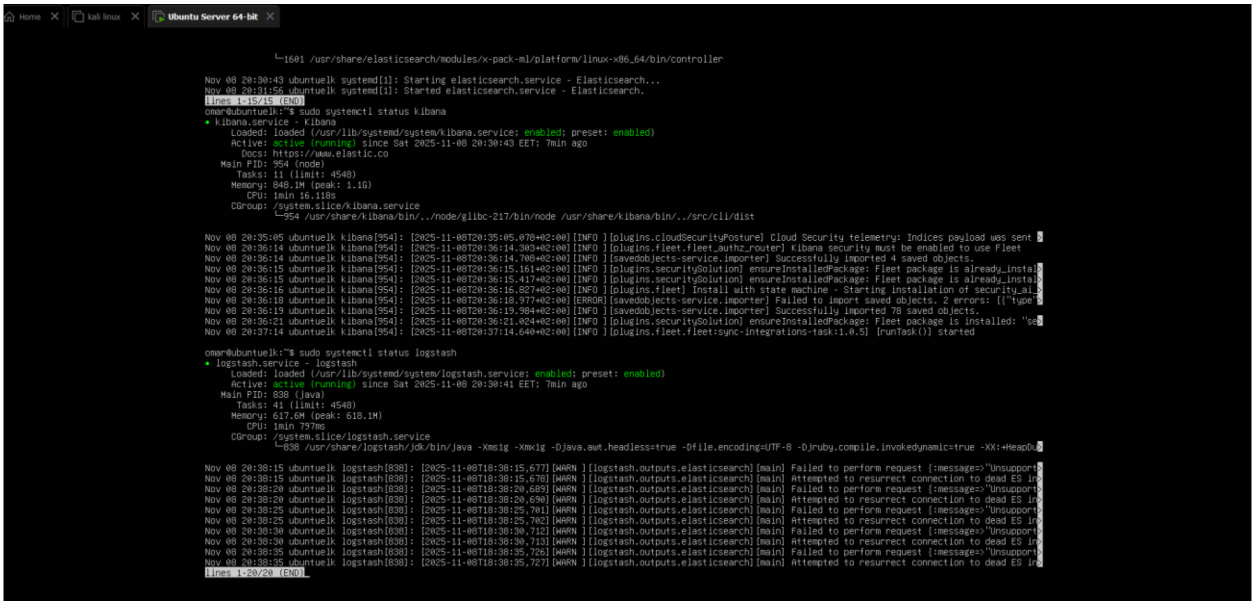
---

4 Expected Outcomes

- Working integration between **MISP** and **Elastic Stack** for real-time IOC correlation.
- A **threat hunting workflow** from intelligence ingestion to detection validation.
- Comprehensive **APT41 profile** including mapped TTPs and detection strategies.
- Actionable insights into detection coverage and potential improvement areas.

---

5 Screenshots



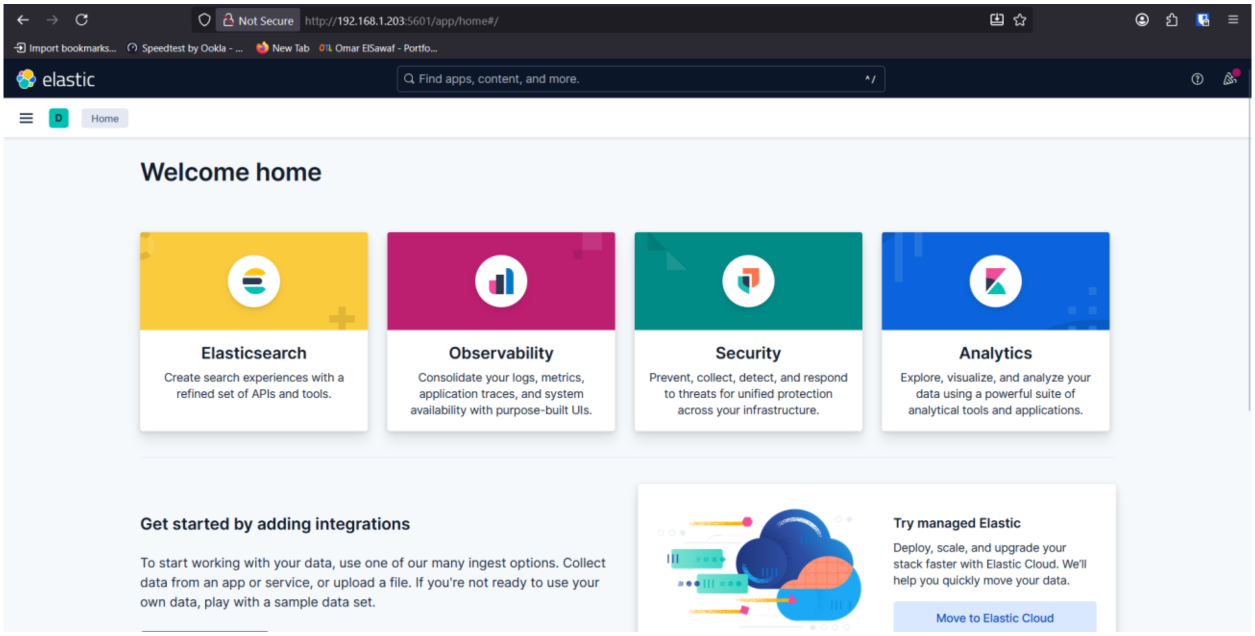
```
             └─1601 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Nov 08 20:30:43 ubuntuelk systemd[1]: Starting elasticsearch.service - Elasticsearch...
Nov 08 20:31:56 ubuntuelk systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-15/15 (END)
omar@ubuntuelk:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-11-08 20:30:43 EET; 7min ago
       Docs: https://www.elastic.co
   Main PID: 954 (node)
      Tasks: 11 (limit: 4548)
     Memory: 848.1M (peak: 1.1G)
        CPU: 1min 16.118s
     CGroup: /system.slice/kibana.service
             └─954 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

Nov 08 20:35:05 ubuntuelk kibana[954]: [2025-11-08T20:35:05.078+02:00][INFO ][plugins.cloudSecurityPosture] Cloud Security telemetry: Indices payload was sent >
Nov 08 20:36:14 ubuntuelk kibana[954]: [2025-11-08T20:36:14.303+02:00][INFO ][plugins.fleet.fleet_authz_router] Kibana security must be enabled to use Fleet
Nov 08 20:36:14 ubuntuelk kibana[954]: [2025-11-08T20:36:14.708+02:00][INFO ][savedobjects-service.importer] Successfully imported 4 saved objects.
Nov 08 20:36:15 ubuntuelk kibana[954]: [2025-11-08T20:36:15.161+02:00][INFO ][plugins.securitySolution] ensureInstalledPackage: Fleet package is already_instal>
Nov 08 20:36:15 ubuntuelk kibana[954]: [2025-11-08T20:36:15.417+02:00][INFO ][plugins.securitySolution] ensureInstalledPackage: Fleet package is already_instal>
Nov 08 20:36:16 ubuntuelk kibana[954]: [2025-11-08T20:36:16.827+02:00][INFO ][plugins.fleet] Install with state machine - Starting installation of security_ai_>
Nov 08 20:36:18 ubuntuelk kibana[954]: [2025-11-08T20:36:18.977+02:00][ERROR][savedobjects-service.importer] Failed to import saved objects. 2 errors: [{"type">
Nov 08 20:36:19 ubuntuelk kibana[954]: [2025-11-08T20:36:19.984+02:00][INFO ][savedobjects-service.importer] Successfully imported 78 saved objects.
Nov 08 20:36:21 ubuntuelk kibana[954]: [2025-11-08T20:36:21.024+02:00][INFO ][plugins.securitySolution] ensureInstalledPackage: Fleet package is installed: "se>
Nov 08 20:37:14 ubuntuelk kibana[954]: [2025-11-08T20:37:14.640+02:00][INFO ][plugins.fleet.fleet:sync-integrations-task:1.0.5] [runTask()] started

omar@ubuntuelk:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/usr/lib/systemd/system/logstash.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-11-08 20:30:41 EET; 7min ago
   Main PID: 838 (java)
      Tasks: 41 (limit: 4548)
     Memory: 617.6M (peak: 618.1M)
        CPU: 1min 797ms
     CGroup: /system.slice/logstash.service
             └─838 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic=true -XX:+HeapDu>

Nov 08 20:38:15 ubuntuelk logstash[838]: [2025-11-08T18:38:15,677][WARN ][logstash.outputs.elasticsearch][main] Failed to perform request {:message=>"Unsupport>
Nov 08 20:38:15 ubuntuelk logstash[838]: [2025-11-08T18:38:15,678][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection to dead ES in>
Nov 08 20:38:20 ubuntuelk logstash[838]: [2025-11-08T18:38:20,689][WARN ][logstash.outputs.elasticsearch][main] Failed to perform request {:message=>"Unsupport>
Nov 08 20:38:20 ubuntuelk logstash[838]: [2025-11-08T18:38:20,690][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection to dead ES in>
Nov 08 20:38:25 ubuntuelk logstash[838]: [2025-11-08T18:38:25,701][WARN ][logstash.outputs.elasticsearch][main] Failed to perform request {:message=>"Unsupport>
Nov 08 20:38:25 ubuntuelk logstash[838]: [2025-11-08T18:38:25,702][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection to dead ES in>
Nov 08 20:38:30 ubuntuelk logstash[838]: [2025-11-08T18:38:30,712][WARN ][logstash.outputs.elasticsearch][main] Failed to perform request {:message=>"Unsupport>
Nov 08 20:38:30 ubuntuelk logstash[838]: [2025-11-08T18:38:30,713][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection to dead ES in>
Nov 08 20:38:35 ubuntuelk logstash[838]: [2025-11-08T18:38:35,726][WARN ][logstash.outputs.elasticsearch][main] Failed to perform request {:message=>"Unsupport>
Nov 08 20:38:35 ubuntuelk logstash[838]: [2025-11-08T18:38:35,727][WARN ][logstash.outputs.elasticsearch][main] Attempted to resurrect connection to dead ES in>
lines 1-20/20 (END)
```



Welcome home

Elasticsearch

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

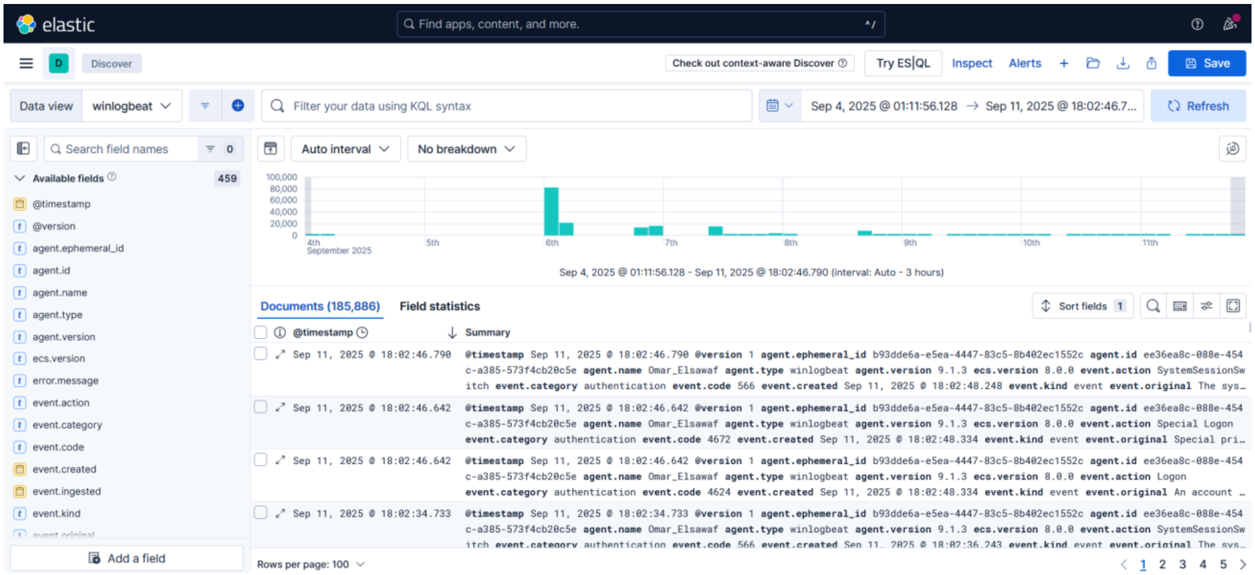
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

Try managed Elastic

Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.



Data view: winlogbeat

Filter your data using KQL syntax

Sep 4, 2025 @ 01:11:56.128 → Sep 11, 2025 @ 18:02:46.7...

Available fields 459

@timestamp
@version
agent.ephemeral_id
agent.id
agent.name
agent.type
agent.version
ecs.version
error.message
event.action
event.category
event.code
event.created
event.ingested
event.kind
event.original

Sep 4, 2025 @ 01:11:56.128 - Sep 11, 2025 @ 18:02:46.790 (interval: Auto - 3 hours)

Documents (185,886)

```
@timestamp                   Summary
Sep 11, 2025 @ 18:02:46.790  @timestamp Sep 11, 2025 @ 18:02:46.790 @version 1 agent.ephemeral_id b93dde6a-e5ea-4447-83c5-8b402ec1552c agent.id ee36ea8c-088e-454
                             c-a385-573f4cb20c5e agent.name Omar_Elsawaf agent.type winlogbeat agent.version 9.1.3 ecs.version 8.0.0 event.action SystemSessionSw
                             itch event.category authentication event.code 566 event.created Sep 11, 2025 @ 18:02:48.248 event.kind event event.original The sys…
Sep 11, 2025 @ 18:02:46.642  @timestamp Sep 11, 2025 @ 18:02:46.642 @version 1 agent.ephemeral_id b93dde6a-e5ea-4447-83c5-8b402ec1552c agent.id ee36ea8c-088e-454
                             c-a385-573f4cb20c5e agent.name Omar_Elsawaf agent.type winlogbeat agent.version 9.1.3 ecs.version 8.0.0 event.action Special Logon
                             event.category authentication event.code 4672 event.created Sep 11, 2025 @ 18:02:48.334 event.kind event event.original Special pri…
Sep 11, 2025 @ 18:02:46.642  @timestamp Sep 11, 2025 @ 18:02:46.642 @version 1 agent.ephemeral_id b93dde6a-e5ea-4447-83c5-8b402ec1552c agent.id ee36ea8c-088e-454
                             c-a385-573f4cb20c5e agent.name Omar_Elsawaf agent.type winlogbeat agent.version 9.1.3 ecs.version 8.0.0 event.action Logon
                             event.category authentication event.code 4624 event.created Sep 11, 2025 @ 18:02:48.334 event.kind event event.original An account …
Sep 11, 2025 @ 18:02:34.733  @timestamp Sep 11, 2025 @ 18:02:34.733 @version 1 agent.ephemeral_id b93dde6a-e5ea-4447-83c5-8b402ec1552c agent.id ee36ea8c-088e-454
                             c-a385-573f4cb20c5e agent.name Omar_Elsawaf agent.type winlogbeat agent.version 9.1.3 ecs.version 8.0.0 event.action SystemSessionSw
                             itch event.category authentication event.code 566 event.created Sep 11, 2025 @ 18:02:36.243 event.kind event event.original The sys…
```

6 References

- MITRE ATT&CK Group G0096 – APT41
- ATT&CK® Navigator
- FortiGuard Threat Actor Encyclopedia
- Apt41 Arisen from Dust
- https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_1j0vun2r7rgb
- https://www.cisa.gov/sites/default/files/2022-12/stix-bp-v1.0.0.pdf

- Johnson, C. , Feldman, L. and Witte, G. (2017), Cyber Threat Intelligence and Information Sharing, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=923332 (Accessed October 20, 2025)
- https://www.iso.org/standard/68427.html
- https://www.iso.org/standard/78973.html
- https://otx.alienvault.com/adversary/APT41
- https://otx.alienvault.com/pulse/68abf0f55f8716f665e33ffd
- https://otx.alienvault.com/pulse/68480e89dbe1f2bc0746a80c
- https://otx.alienvault.com/pulse/68de2cc8e4c38a8cbc7ffc40

7 Team Collaboration

CyberSentinels Team Members:

1. Omar Mohamed Hatem Abdelrahman
2. Ziad Osman Emam
3. Nour Mohamed Elsharnoby
4. Youssef Khaled Tawfiq
5. Mohamed Ahmed Abou ouf