CYBERINFINITI LTD

Security Operations Center (SOC) Threat Intelligence Report using Open CTI

Report Title: OpenCTI Threat Intelligence Sprint Assessment

Report ID: TIR-CTI-2026-INT-001

Report Date: January 2026

Classification: Confidential / Internal Use

Analysts: John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun.

Report Version: 1.0

Distribution: CyBlack Team, Team 8 SOC Team, Executive Management

---

TABLE OF CONTENTS

1.0 Executive Summary

This Threat Intelligence Report presents the results of a structured Cyber Threat Intelligence (CTI) sprint conducted using the OpenCTI platform in a Docker Container, enriched with intelligence from the AlienVault Open Threat Exchange (OTX) Connector. The primary objective of the task was to identify and assess sector-specific cyber threats, nation-state and criminal activity, targeted victim trends, and also politically motivated threat actors relevant to the organization's operating environment.

The assessment delivers actionable intelligence by correlating real-world indicators, adversary behaviors, and observed attack patterns with established analytical frameworks, including the Diamond Model of Intrusion Analysis, the Cyber(Global) Kill Chain, and the MITRE ATT&CK framework. The findings are designed to support executive decision-making, enhance detection and response capabilities, and strengthen the organization's overall cyber resilience in an evolving, increasingly complex threat landscape.

2.0 Scenario Overview & Objectives

Cyberinfiniti Ltd, Team 8 operated as a dedicated threat Intelligence function within a simulated organizational environment. The team leveraged OpenCTI as the central intelligence management platform, enriching internal datasets with live, community-driven intelligence through the AlienVault OTX connector. This approach enabled the continuous ingestion, correlation, and analysis of threat data across multiple dimensions.

The CTI task focused on transforming raw technical intelligence into operational and strategic insights aligned with organizational risk and leadership priorities.

2.1 Key Objectives

- Profile the cyber threat landscape affecting the organization's industry sector.
- Assess country-level cyber threats impacting headquarters and regional operations.
- Identify recently targeted victims and analyze associated threat actors and campaigns.
- Investigate a politically motivated threat actor involved in recent high-impact activity.
- Translate technical findings into clear, executive-level intelligence to inform risk-based decisions.

3.0 Methodology & Intelligence Sources

The threat intelligence effort followed a structured intelligence lifecycle to ensure analytical rigor, consistency, and relevance to business objectives:

1. **Direction** - Defined intelligence requirements aligned with organizational risk, sector exposure, and geopolitical considerations.
2. **Collection** - Aggregated threat data from OpenCTI and AlienVault OTX intelligence feeds.
3. **Processing** - Normalized and enriched indicators, entities, and relationships within the OpenCTI platform.
4. **Analysis** - Applied analytical frameworks, including the Diamond Model, Cyber Kill Chain, and timeline analysis to identify adversary behavior patterns and campaign activity.
5. **Dissemination**: Produced analyst-ready and executive-level reporting focused on impact, risk, and defensive posture.

3.1 Primary Intelligence Sources

- OpenCTI Platform
- AlienVault Open Threat Exchange (OTX)
- Community-shared indicators, reports, and threat actor profiles
- MITRE ATT&CK Framework
- Open-source intelligence (OSINT)

4.0 OpenCTI Custom Deployment Steps & Architecture (AWS EC2)

Overview

To support the Cyber Threat Intelligence (CTI) sprint, OpenCTI was deployed in a secure, cloud-based environment using Amazon Web Services (AWS). The platform was hosted on a dedicated Ubuntu Linux EC2 instance, accessed remotely via SSH, and containerized using Docker and Docker Compose. This architecture enabled scalable ingestion, correlation, and analysis of threat intelligence from multiple sources, including AlienVault Open Threat Exchange (OTX).

The deployment was designed to simulate a real-world enterprise CTI environment, aligning with industry best practices for cloud security, modular architecture, and connector-based ingestion of intelligence.

4.1 AWS EC2 Environment Configuration

Computer & Operating System

- Instance Type: t3.xlarge
- vCPU: 4
- Memory: 16 GB RAM
- Operating System: Ubuntu Server (64-bit)
- Deployment Model: Single-node OpenCTI deployment using Docker containers

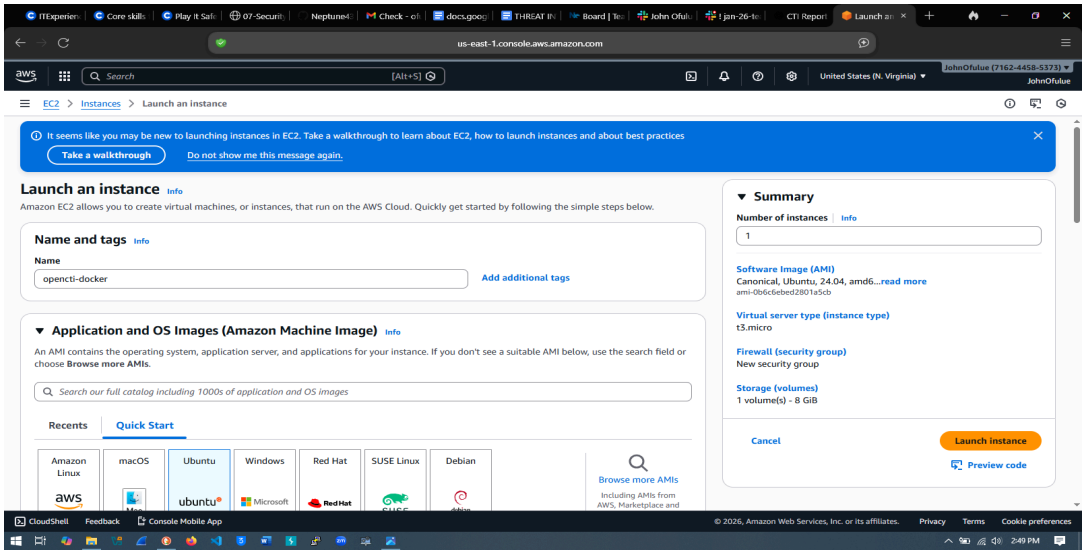

Fig. 1 .0: Creating an Ubuntu Instance

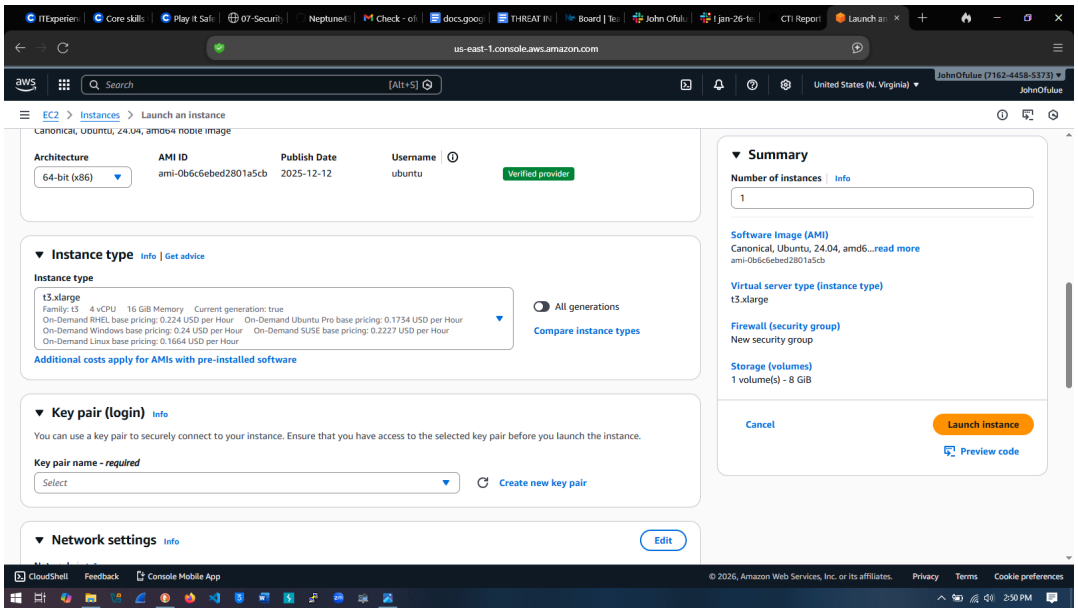

Fig. 1.1: Choosing instance type

The chosen instance size ensured sufficient resources for:

- OpenCTI core services
- Graph database operations

- Docker Containerization & Compose
- Message queuing (RabbitMQ)
- Multiple external intelligence connectors

4.2 Network & Security Group Configuration

The EC2 instance was placed within an AWS Virtual Private Cloud (VPC) and protected using Security Groups acting as a virtual firewall.

Inbound Rules (Restricted to Analyst IP):

S/N	Protocol	Port	Purpose
1.	SSH	22	Secure remote administration
2.	HTTP	80	Optional web access/redirection
3.	HTTPS	443	Secure web access
4.	Custom TCP	8080	OpenCTI Web Interface

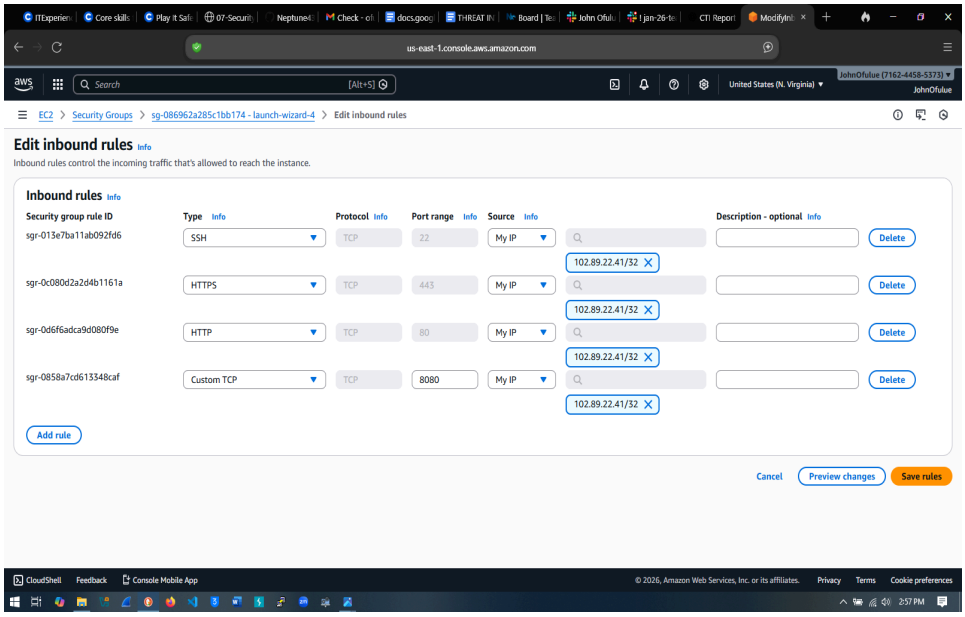

Fig 2.0: Configuring Inbound rules

Key security considerations:

- All inbound access was restricted to the analyst's public IP address
- No public database or message queue ports were exposed
- The OpenCTI platform was accessed via the browser on port 8080

This configuration reflects a least-privilege network exposure model, consistent with SOC and cloud security best practices.

4.3 Secure Access & Administration

SSH Access

The Ubuntu instance was accessed securely using SSH:

- Key-based authentication
- No password-based SSH login

- Root access restricted; administrative actions performed via sudo

This ensured:

- Encrypted communication
- Strong identity assurance
- Reduced risk of brute-force attacks

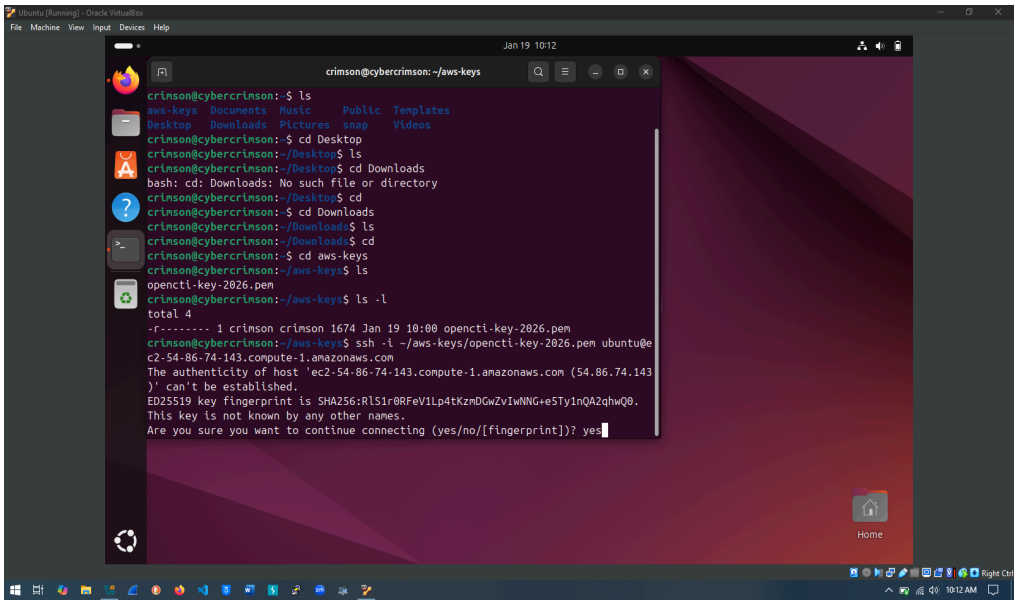

Fig 3.0: Secure SSH access

4.4 Docker & Containerization Setup

OpenCTI was deployed using Docker to ensure modularity, portability, and ease of management.

4.4.1. Step 1: Set up Docker's APT Repository

Docker's official repository was configured to ensure trusted and up-to-date packages.

 # Update package index

sudo apt-get update

sudo apt-get install ca-certificates curl

 # Create directory for Docker keyring

sudo install -m 0755 -d /etc/apt/keyrings

 # Add Docker's official GPG key

sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc

sudo chmod a+r /etc/apt/keyrings/docker.asc

 # Add Docker repository

echo \

"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc]

https://download.docker.com/linux/ubuntu \

$(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}") stable" | \

sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

 # Update package index

sudo apt-get update

4.4.2. Step 2: Install Docker Engine & Docker Compose Plugin

sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin

Important note:

- The modern Docker CLI syntax was used:

sudo docker compose up -d

instead of the deprecated docker-compose binary.

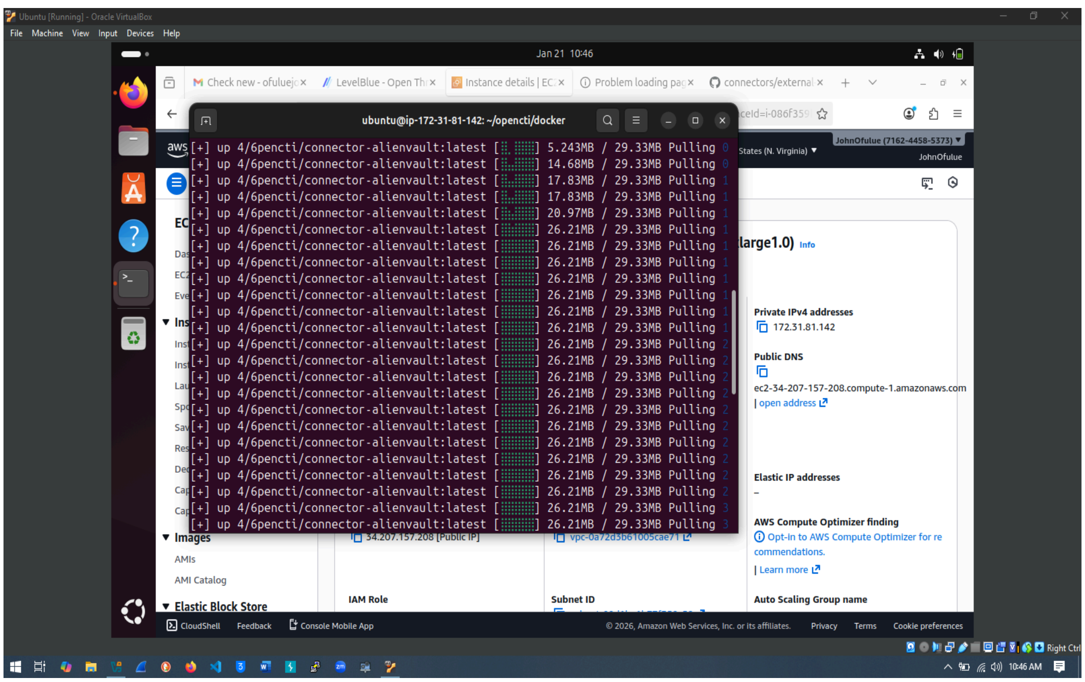

Fig 4.0 Docker Engine & Docker Compose Plugin Installation

4.4.3. Step 3: Install Supporting Tools

Git

sudo apt install git

Used to clone OpenCTI deployment repositories and manage configuration files.

Sublime Text

- Installed for editing .env, docker-compose.yml, and connector configuration files
- Enabled structured editing with syntax highlighting and validation

4.5 OpenCTI Installation & Configuration

Environment Configuration (.env)

During OpenCTI setup, the .env file was edited to define:

- Platform credentials
- Database configuration
- Message queue parameters
- Connector authentication tokens & API key

Credential Requirements (Validation Enforced):

- Username: Minimum 4 characters
- Password: Minimum 8 characters

This validation ensures:

- Secure authentication
- Successful container startup
- Prevention of runtime errors during initialization

4.6 OpenCTI Architecture & Data Flow

Logical Architecture Overview

The OpenCTI deployment followed a microservices-based architecture, with each core function running in its own container.

4.6.1. Architecture Flow (Textual Diagram)

Host Ubuntu Machine

|

| SSH

v

AWS EC2 (Ubuntu 22.04 LTS)

|

| Docker (Network)

v

OpenCTI Platform

├─ OpenCTI API & Frontend

├─ Elasticsearch

├─ Redis

├─ MinIO

├─ RabbitMQ

├─ Graph Database (OpenCTI Storage)

└─ AlienVault OTX Connector

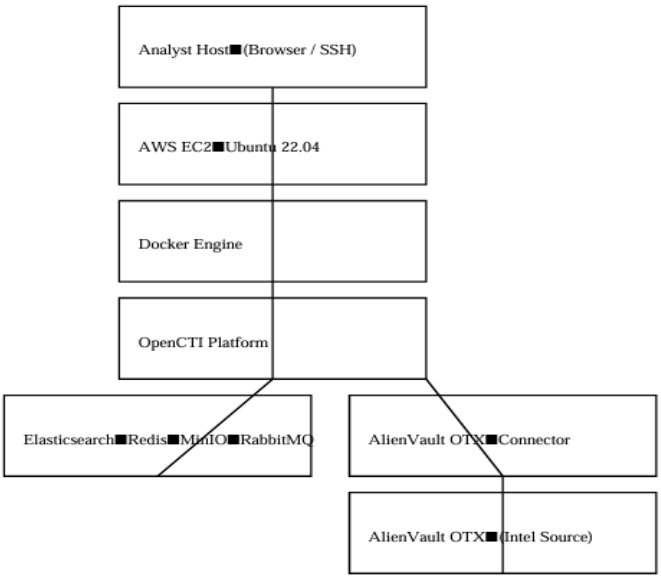

Fig. 5.0 Architecture Flow

4.6.2 Component Roles

OpenCTI Web Interface

- Provides analyst-facing UI
- Used for entity exploration, relationship mapping, and investigation

OpenCTI API

- Central intelligence processing engine
- Exposes REST APIs for connectors and automation
- Enforces authentication and authorization

RabbitMQ

- Acts as the message broker
- Enables asynchronous task handling
- Decouples ingestion from processing to improve scalability and reliability

Graph Database

- Stores entities (threat actors, malware, indicators)
- Maintains relationships using the STIX 2.1 data model

- Enables complex pivoting and correlation

Connectors

- Run as independent containers
- Subscribe to RabbitMQ queues
- Ingest, enrich, or export intelligence data

4.7 AlienVault OTX Connector Integration

Connector Deployment

The AlienVault Open Threat Exchange (OTX) connector was deployed as a Docker container and configured via environment variables.

Key configuration elements included in the “Docker-compose.yml” & .env File:

- OpenCTI API URL
- OpenCTI API authentication token
- AlienVault OTX API key
- Connector scope and polling interval

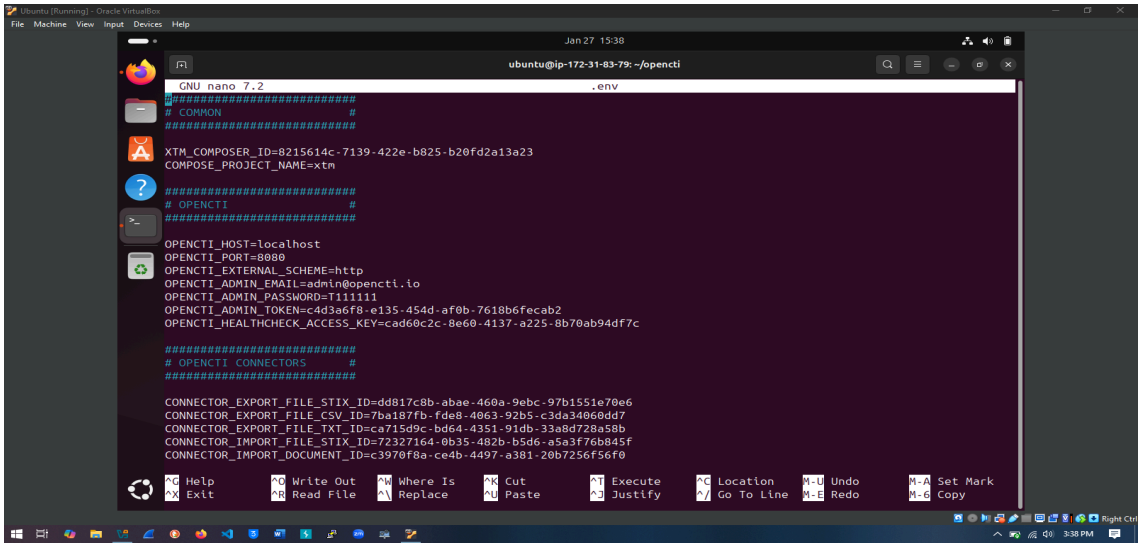

Fig. 6.0 OpenCTI .env Configuration

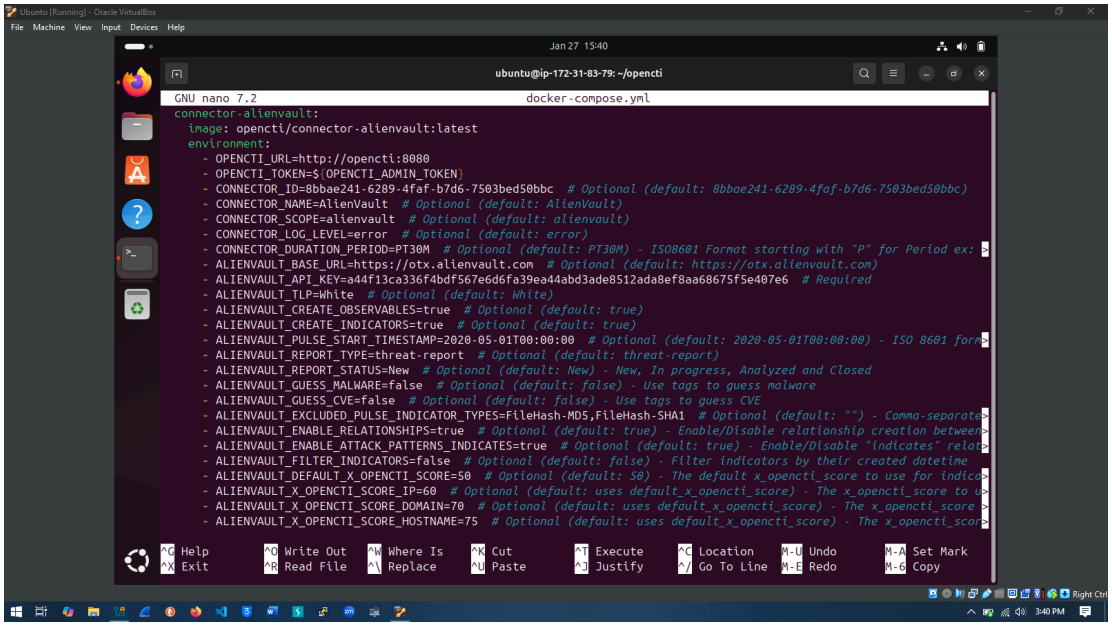

Fig. 6.1 Alienvault Connector Configuration I

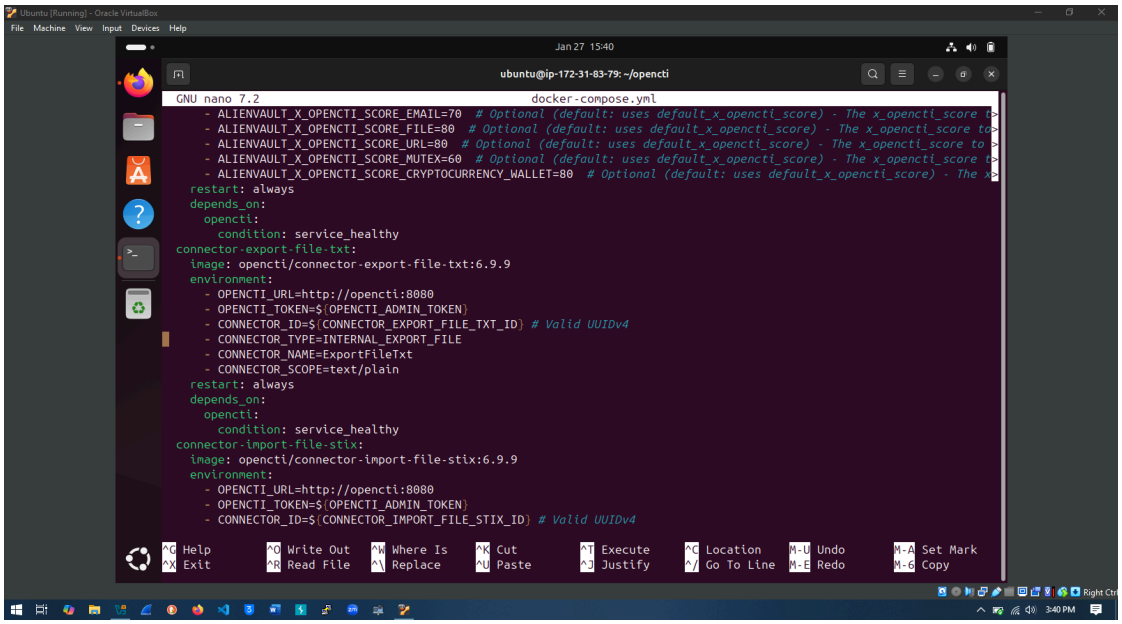

Fig. 6.2 Alienvault Connector Configuration II

Data Ingestion Workflow

1. The AlienVault OTX connector authenticates to OpenCTI using an API token
2. The connector periodically queries the OTX API for:

    - Indicators of Compromise (IOCs)
    - Pulses
    - Malware and threat actor associations
3. Retrieved intelligence is normalized into STIX objects
4. Data is sent to RabbitMQ for processing
5. OpenCTI ingests, correlates, and links the data to existing entities
6. Analysts visualize and analyze enriched intelligence via the OpenCTI UI

Security Considerations

- API keys stored only in environment variables
- No hard-coded credentials in configuration files
- Connector traffic confined to Docker's internal network
- External API communication is encrypted via HTTPS

4.8 Operational Benefits of This Architecture

- Scalable: Additional connectors can be deployed without impacting core services
- Resilient: Message queuing prevents data loss during transient failures
- Secure: Minimal exposed attack surface
- Realistic: Mirrors production-grade CTI environments used in SOCs and MSSPs

4.9 Executive & Technical Takeaways

- The AWS-based OpenCTI deployment successfully simulated an enterprise-grade CTI platform
- Docker-based architecture enabled modular intelligence ingestion and processing
- Secure network controls minimized cloud exposure risk
- AlienVault OTX integration enriched analysis with real-world, community-driven intelligence
- The architecture supports continuous expansion and future automation

5.0 Task 1: Industry Sector Focus & Threat Landscape

5.1 Sector Identification

Cyberinfiniti Ltd is aligned with the Information Technology (IT) sector, encompassing cybersecurity services, managed IT solutions, and managed security service provision (MSSP). Organizations operating in this sector are uniquely exposed because they possess privileged access to customer environments, sensitive intellectual property, authentication systems, and security tooling. As a result, IT firms are often targeted not only for direct financial gain but also as stepping stones for broader supply-chain compromise.

Threat actors targeting this sector typically pursue one or more of the following objectives:

- Monetization through ransomware and extortion
- Long-term espionage and data theft
- Credential harvesting for access to downstream victims
- Disruption of trusted service providers to erode confidence

5.2 Sector Threat Landscape Overview

5.2.1 Ransomware Operations

Ransomware remains the most significant and immediate threat to the IT sector. Modern ransomware campaigns no longer focus solely on encryption but instead adopt double extortion and, in some cases, triple extortion models. These campaigns combine data theft, system encryption, and reputational pressure.

Commonly observed techniques include:

- **T1078 - Valid Accounts:** Use of stolen VPN or administrative credentials for initial access
- **T1486 - Data Encrypted for Impact:** Encryption of production systems
- **T1567 - Exfiltration Over Web Services:** Theft of sensitive data before encryption
- **T1041 - Exfiltration Over C2 Channel:** Data exfiltration using attacker-controlled infrastructure

Akira and Conti-linked ransomware operations demonstrate how attackers exploit single-factor authentication, flat networks, and poor credential hygiene to rapidly escalate impact.

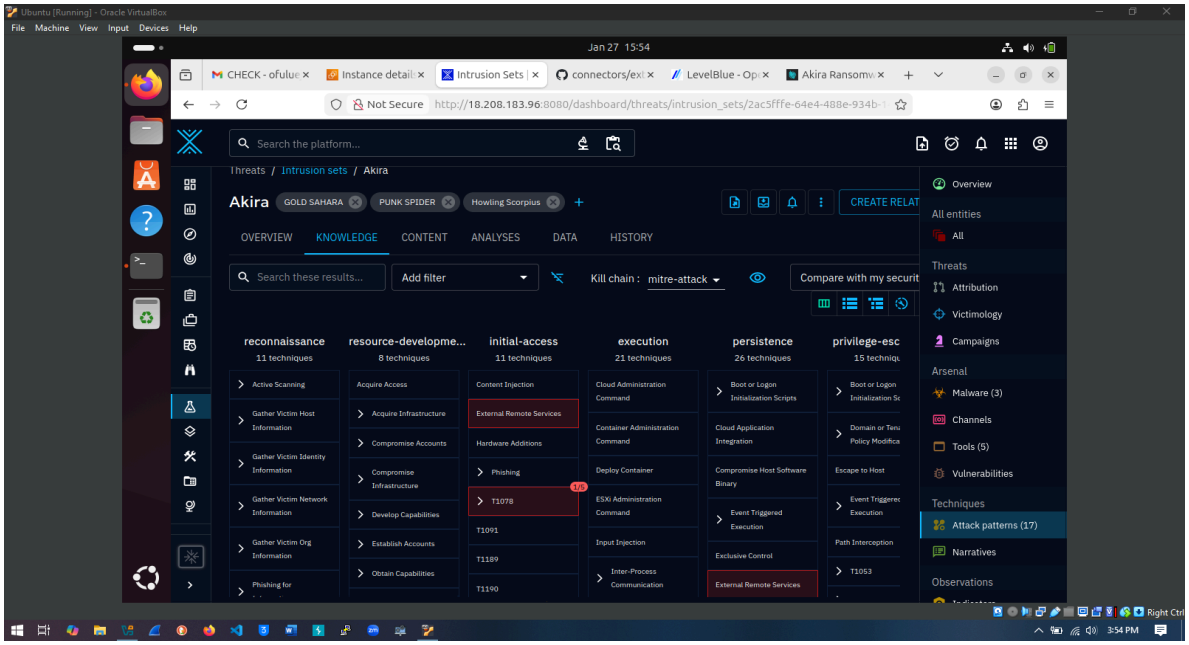

Fig. 7.0 Brief Knowledge of Akira Intrusion Set

5.2.2 State-Sponsored Intrusions (Advanced Persistent Threats)

APT groups targeting IT organizations are typically motivated by strategic intelligence collection rather than immediate financial gain. These actors prioritize stealth, persistence, and long-term access.

Key techniques include:

- **T1095 - Non-Application Layer Protocol:** Use of custom or non-standard protocols for command and control
- **T1055 - Process Injection:** Hiding malicious code within legitimate processes
- **T1547 - Boot or Logon Autostart Execution:** Maintaining persistence across reboots
- **T1027 - Obfuscated Files or Information:** Evading detection through encryption or packing

Such intrusions may remain undetected for months, allowing attackers to harvest credentials, monitor communications, and map organizational infrastructure.

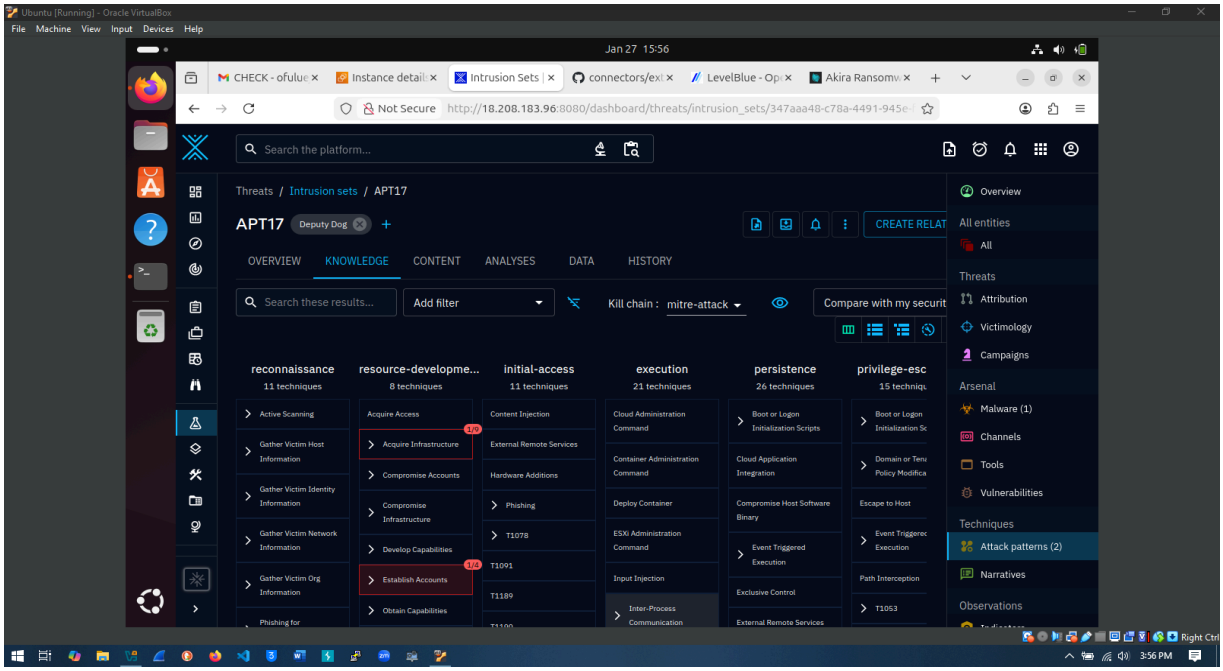

Fig. 7.1 Overview of APT17 Intrusion set

5.2.3 Data Exfiltration Campaigns

Increasingly, threat actors prioritize silent data theft over overt disruption. These campaigns focus on intellectual property, customer data, and internal communications.

Observed techniques include:

- **T1213 - Data from Information Repositories:** Accessing shared drives and document management systems
- **T1114 - Email Collection:** Harvesting email data for intelligence and leverage
- **T1039 - Data from Network Shared Drive:** Collection of sensitive files across enterprise shares

5.2.4 Credential Compromise & Lateral Movement

Credential theft underpins nearly all successful intrusions in the IT sector.

Key techniques:

- **T1003 - OS Credential Dumping:** Extracting credentials from memory or registry
- **T1555 - Credentials from Password Stores:** Harvesting browser or application-stored credentials
- **T1021 - Remote Services:** Lateral movement via SMB, RDP, or WinRM
- **T1046 - Network Service Scanning:** Identifying additional targets within the network

5.3 Key Threat Actors & Campaigns

5.3.1 Akira Ransomware Group

Akira is a Ransomware-as-a-Service (RaaS) operation active since at least March 2023. The group is known for highly targeted intrusions against enterprises, particularly those operating Windows and VMware ESXi environments.

Campaign Characteristics:

Akira operators typically gain initial access through compromised credentials, particularly targeting VPNs and remote access services lacking multi-factor authentication (T1078 - Valid Accounts). Once inside, they conduct extensive internal reconnaissance using tools such as AdFind (T1087 - Account Discovery, T1018 - Remote System Discovery).

Lateral movement is achieved using legitimate administrative tools such as PSExec (T1021.002 - SMB/Windows Admin Shares) and remote service execution (T1569 - System Services). Before ransomware deployment, Akira actors exfiltrate sensitive data using tools such as RClone (T1567 - Exfiltration Over Web Services) to cloud storage controlled by the attacker.

Encryption is executed only after data theft is complete (T1486 - Data Encrypted for Impact), followed by extortion threats leveraging public leak sites.

Technical analysis shows Akira ransomware variants capable of targeting both Windows and VMware ESXi hypervisors, with tooling and infrastructure overlaps linked to historical Conti ransomware operations.

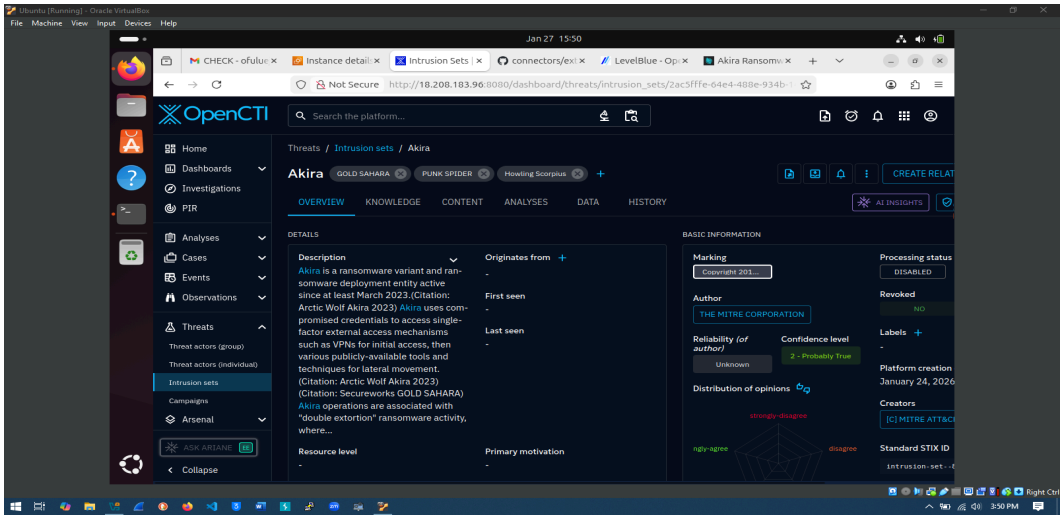

Fig. 7.2 Overview of Akira Ransomware

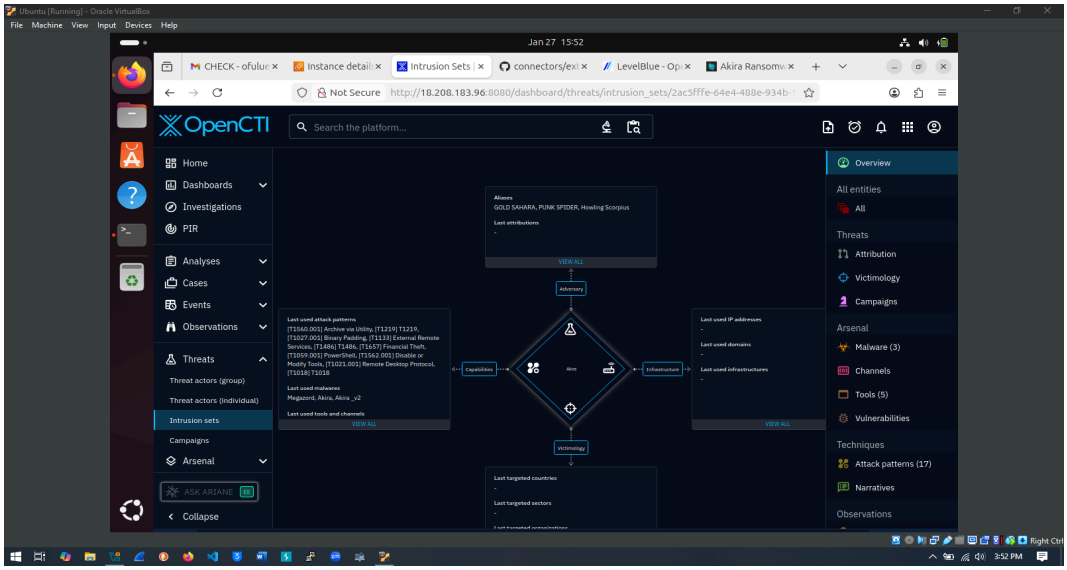

Fig. 7.3 Akira Ransomware Diamond chain

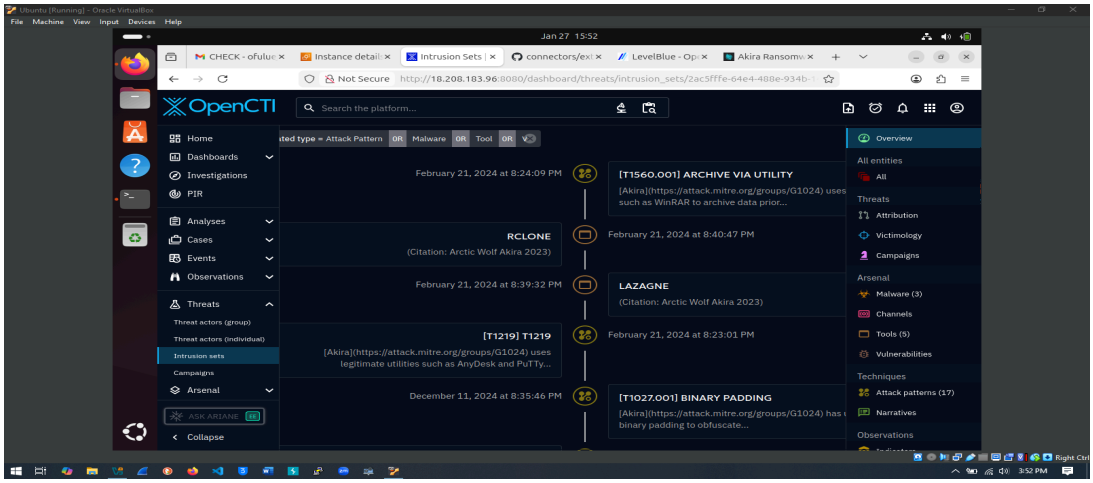

Fig. 7.4 Akira Ransomware attack pattern

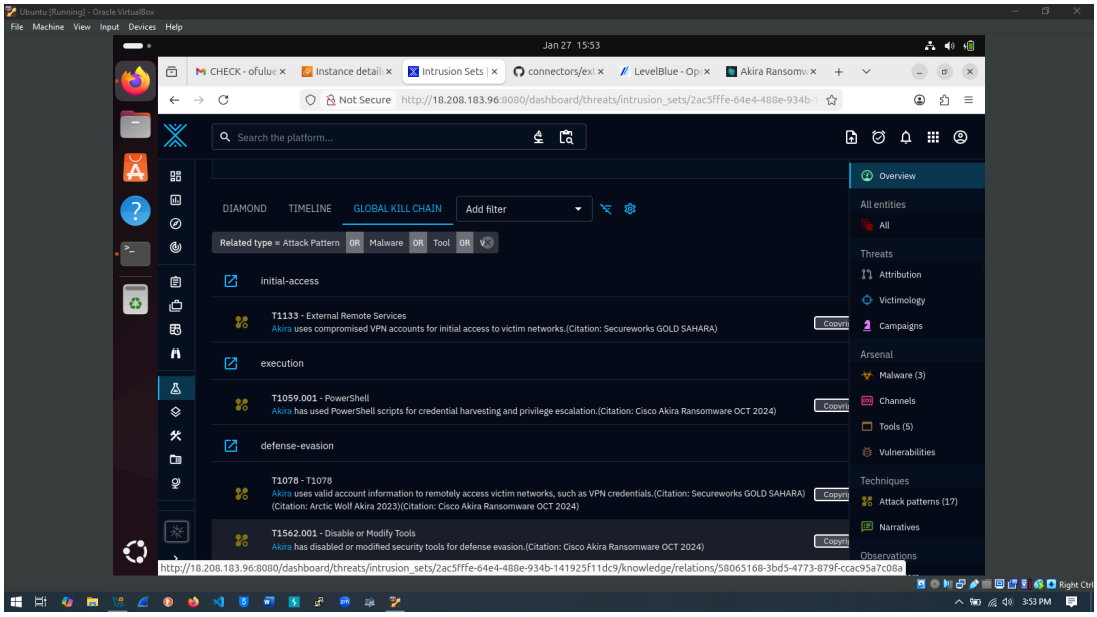

Fig. 7.5 Akira Global kill chain

5.3.2 APT17

APT17 is a **China-based state-sponsored threat group** engaged in long-term cyber espionage operations. The group has historically targeted government agencies, defense contractors, law firms, IT companies, and mining organizations.

Campaign Characteristics:

APT17 operations emphasize stealth and persistence. Initial access is commonly achieved via spear-phishing campaigns (T1566 - Phishing) or exploitation of exposed services (T1190 - Exploit Public-Facing Application).

Once inside a network, APT17 deploys custom backdoors and web shells (T1505.003 - Web Shell) to maintain access. Command-and-control traffic often leverages non-standard protocols (T1095 - Non-Application Layer Protocol) to evade detection.

The group focuses on long-term data collection (T1213 - Data from Information Repositories, T1114 - Email Collection) rather than immediate disruption, aligning with intelligence-gathering objectives.

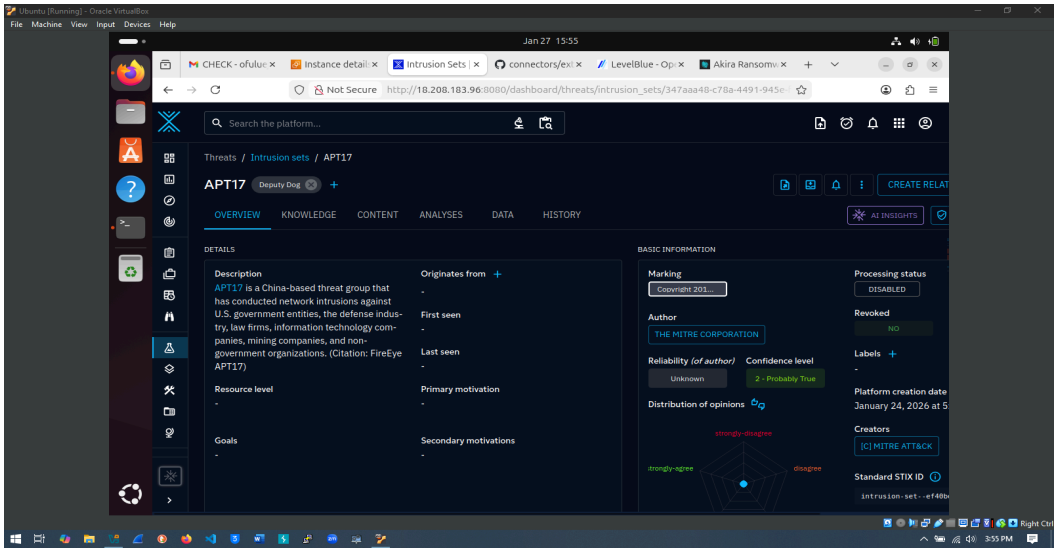

Fig. 8.0 Overview of APT17

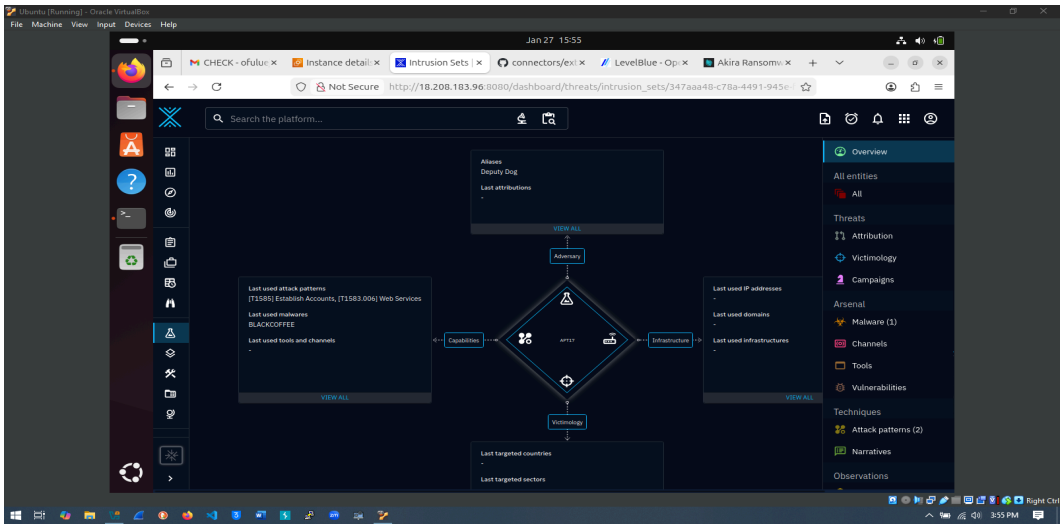

Fig. 8.1 APT17 Diamond chain

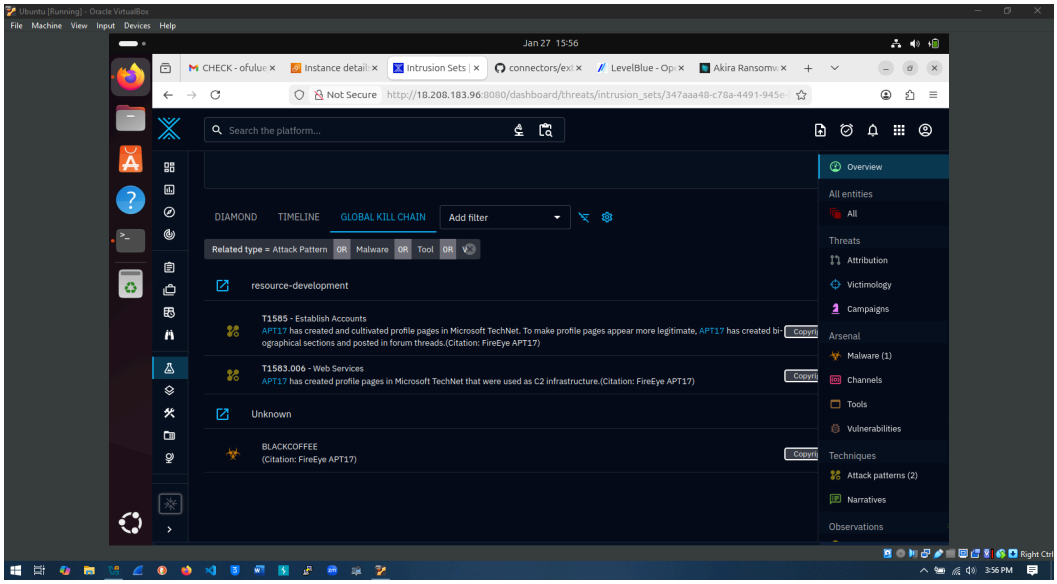

Fig. 8.2 APT17 Global kill chain

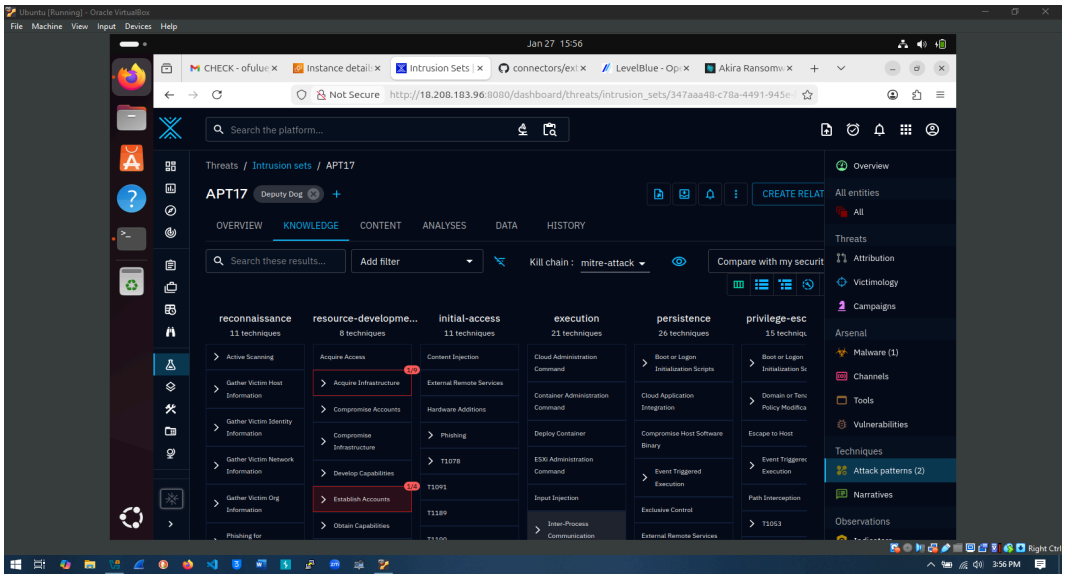

Fig. 8.3 Brief knowledge on the APT17 intrusion set

5.3.3 POLONIUM

POLONIUM is a Lebanon-based threat actor assessed to operate in coordination with Iran's Ministry of Intelligence and Security (MOIS). Active since at least 2022, the group

has targeted Israeli organizations across the IT, defense, and critical manufacturing sectors.

Campaign Characteristics:

POLONIUM campaigns typically begin with credential compromise or phishing (T1078 - Valid Accounts, T1566 - Phishing). The group is known for deploying custom malware and leveraging cloud services for command-and-control (T1102 - Web Service C2).

Persistence mechanisms include scheduled tasks and registry modifications (T1547 - Autostart Execution). Data exfiltration is performed covertly to minimize detection (T1041 - Exfiltration Over C2 Channel), supporting long-term intelligence collection.

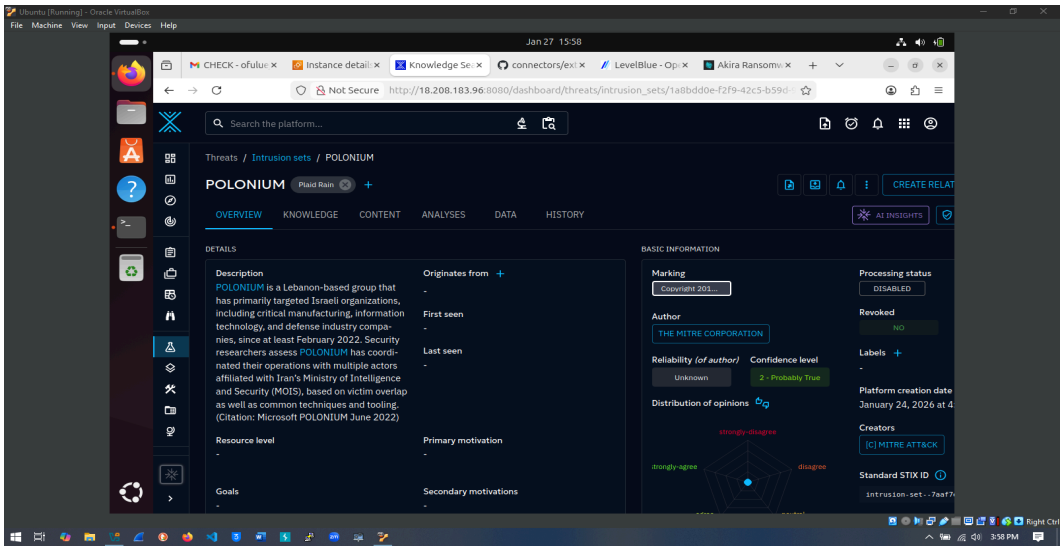

Fig. 9.0 Overview of Polonium

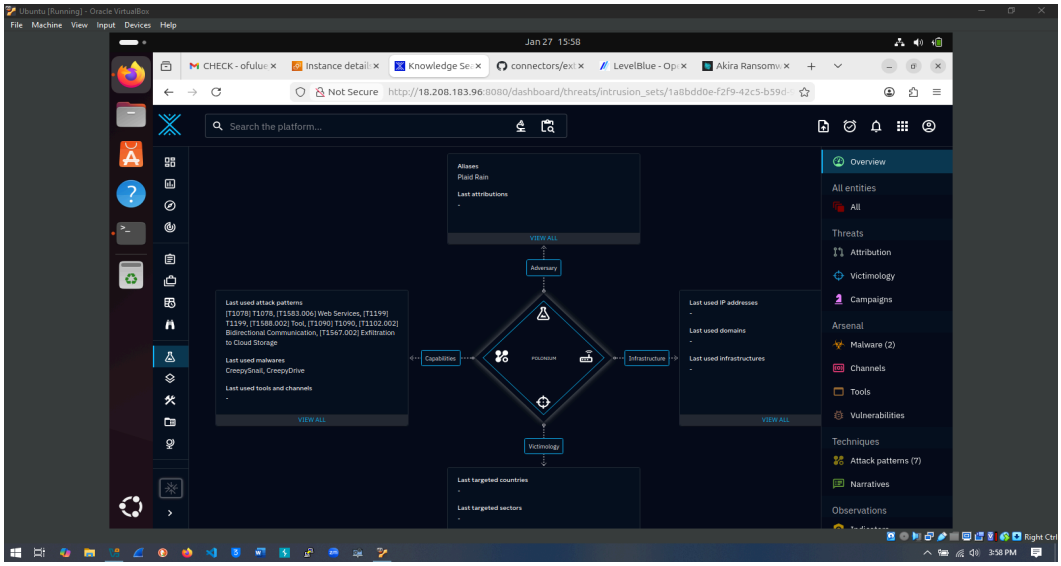

Fig. 9.1 Polonium Diamond chain

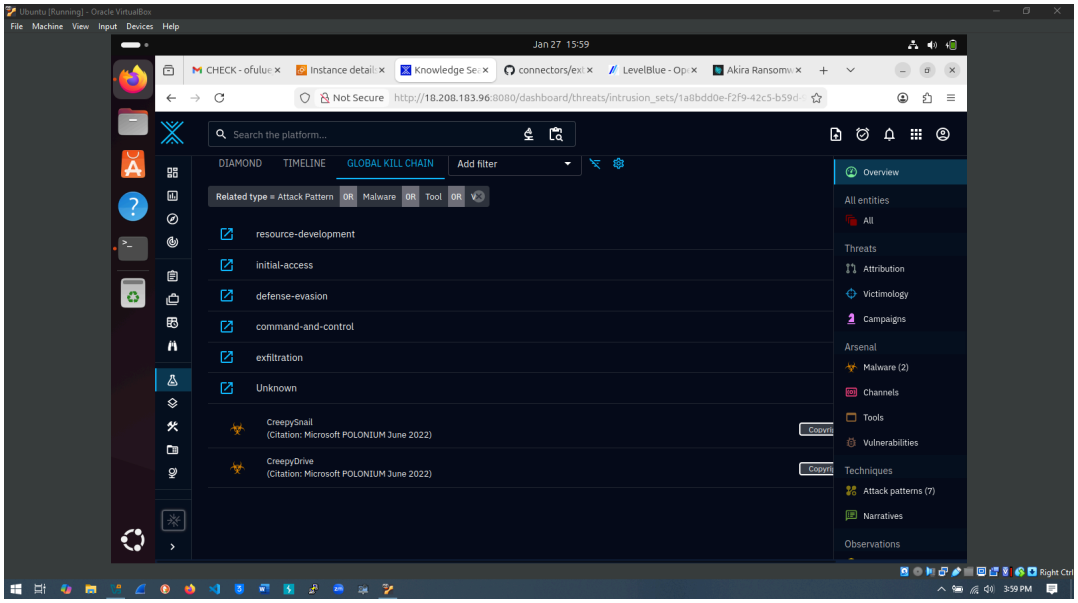

Fig. 9.2 Polonium Global kill chain

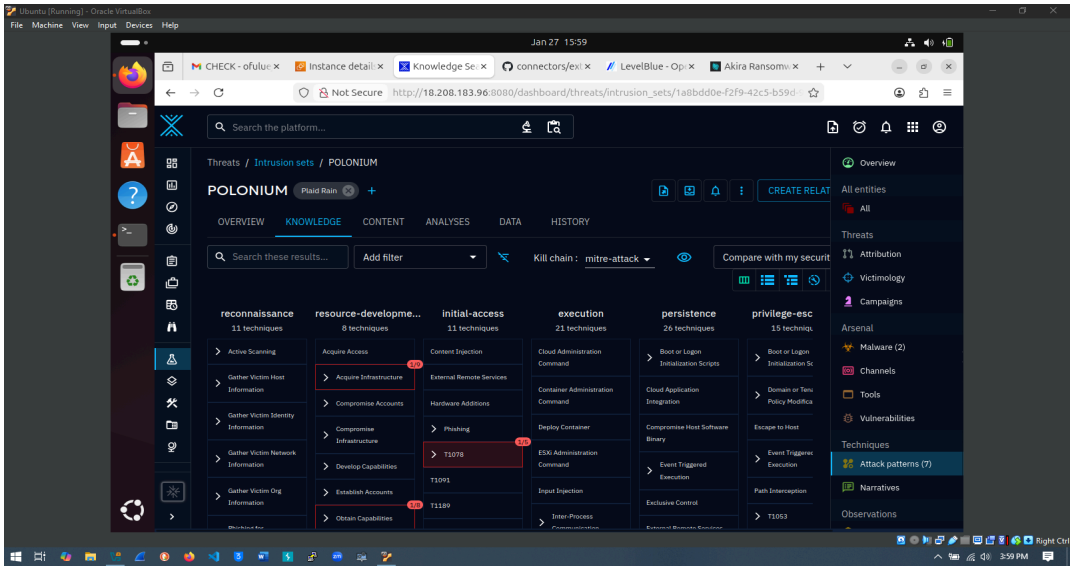

Fig. 9.3 Brief knowledge of the Polonium intrusion set

5.4 Common Tools, Malware & TTPs

Malware & Tools

Akira Ransomware

- T1486 - Data Encrypted for Impact
- T1567 - Exfiltration Over Web Services

  Targets Windows and VMware ESXi systems, encrypting critical infrastructure after data theft.

MiniKatz

- T1003 - OS Credential Dumping

  Extracts plaintext credentials and password hashes from memory.

LaZagne

- T1555 - Credentials from Password Stores

  Harvests stored credentials from browsers and applications.

PSExec

- T1021.002 - SMB/Windows Admin Shares
  Used for lateral movement and remote command execution.

RClone & AdFind

- T1087 - Account Discovery
- T1567 - Exfiltration Over Web Services
  Used for reconnaissance and large-scale data theft.

Fig. 9.4 Common tools used

Techniques & Procedures Summary

- Initial access commonly occurs via phishing (T1566) or stolen credentials (T1078).
- Lateral movement leverages legitimate administrative tools (T1021).
- Data is exfiltrated before encryption (T1041, T1567).
- Ransomware is deployed as the final impact stage (T1486).

5.5 Historical Incidents & Industry Alerts

Historical Events

Akira Ransomware Campaigns (2023-2024)

- Impacted organizations running Windows and VMware ESXi
- Employed double extortion tactics
- Linked to Conti-derived tooling and infrastructure

APT17 Intrusions

- Long-term infiltration of government and IT organizations
- Focused on espionage and data collection rather than disruption

POLONIUM Campaigns (2022-2024)

- Targeted Israeli IT and defense firms
- Demonstrated coordination with Iranian intelligence-aligned actors

Industry Alerts

- **CISA & Arctic Wolf:** Published Akira IOCs, detection guidance, and mitigation strategies

- **Microsoft & FireEye:** Detailed POLONIUM and APT17 TTPs, emphasizing credential theft and stealthy persistence

6.0. Task 2: National Threat Landscape Assessment

Headquarters Country- Nigeria

6.1 Hilalrat / UNC788

Hilalrat (UNC788) is a **financially motivated cybercriminal group** actively targeting corporate networks and financial institutions across West Africa.

Behavior & Tactics:

- Initial access via phishing (T1566) and credential compromise (T1078)
- Deployment of malware for data theft (T1041) and ransomware (T1486)
- Lateral movement using administrative tools (T1021)
- Occasional use of double extortion tactics (T1567)

Indicators of Compromise:

- Suspicious PowerShell or PSExec activity
- Unusual outbound traffic to unknown IPs
- Presence of ransomware-related file extensions

Notable Campaigns:
Active since 2023, with operations timed around financial reporting cycles and holidays to maximize impact.

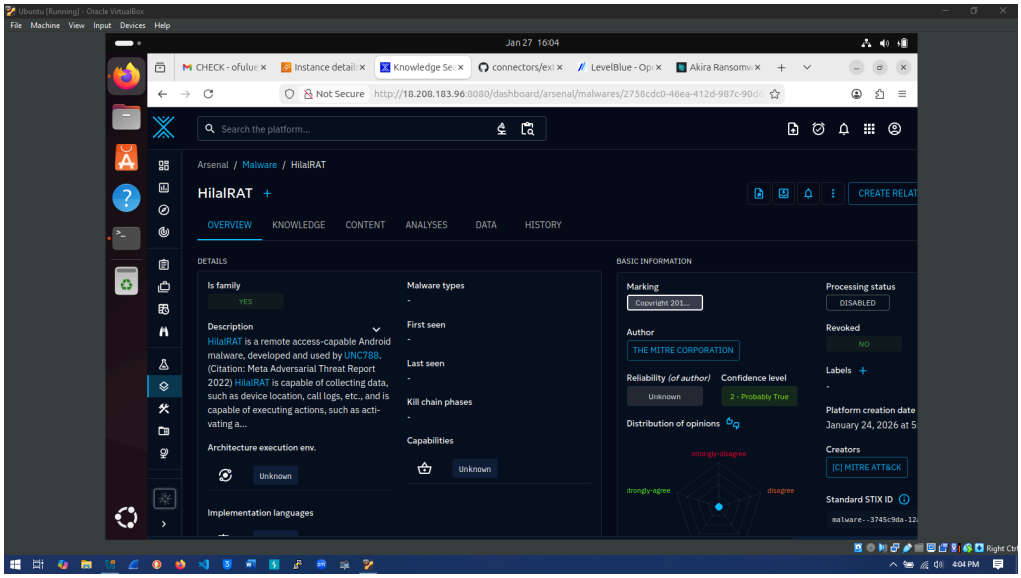

Fig. 10.0 Overview of HilalRAT Group

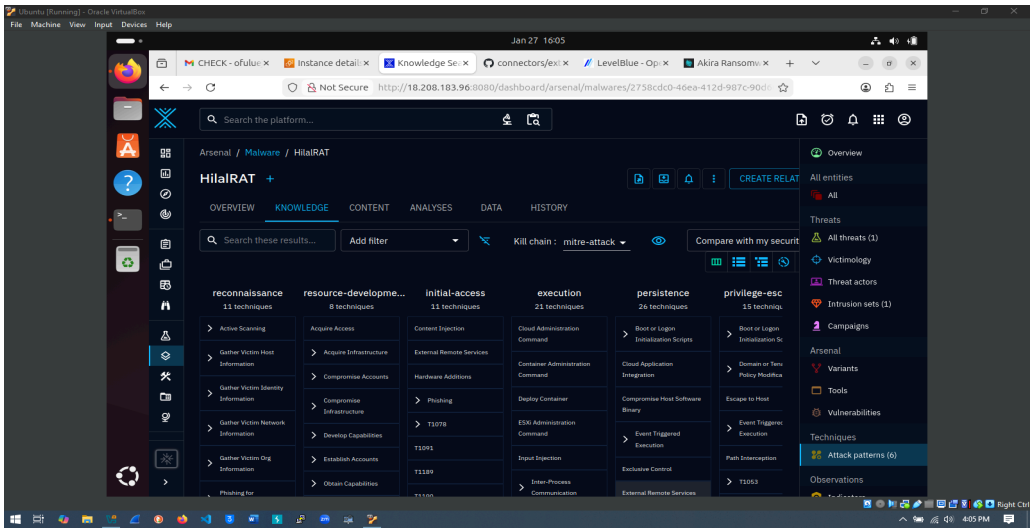

Fig. 10.1 Brief knowledge of the HilalRAT group

6.2 Hoplight / APT38 (Lazarus Group)

Hoplight/APT38 is a **North Korea-linked state-sponsored actor** specializing in financial cyber operations.

Behavior & Tactics:

- Spear-phishing targeting executives (T1566.001)
- Deployment of custom malware (T1055 - Process Injection)
- Exploitation of financial infrastructure (T1190, T1046)
- Encrypted C2 communications (T1095)

Indicators of Compromise:

- Lazarus malware families
- Unauthorized banking transactions
- Known Lazarus C2 infrastructure

Notable Campaigns:

Global financial theft operations have been increasing in reconnaissance targeting African banking networks since 2022.

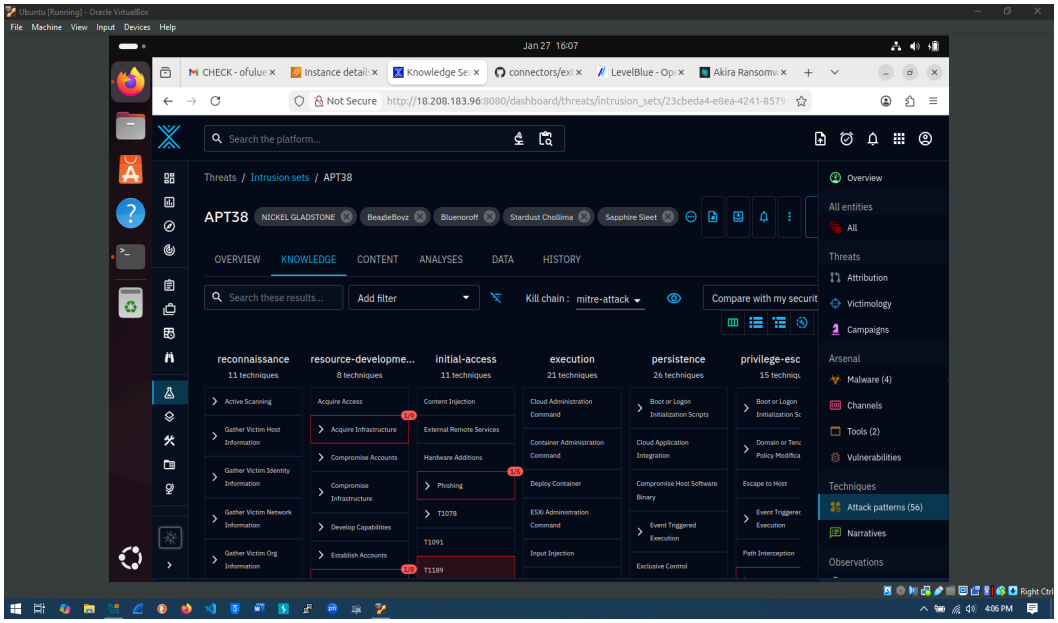

Fig. 11.0 Brief knowledge of Hoplight

7.0 Task 3: Victim Profile & Threat Mapping

Overview

This task focuses on analyzing realistic victim profiles observed within OpenCTI intelligence, mapping each victim to the threat actors, tools, techniques, and objectives most relevant to their sector. The analysis applies the Diamond Model of Intrusion Analysis, MITRE ATT&CK, and Kill Chain mapping to contextualize attacker behavior and intent.

The objective is not only to identify *who* is being targeted, but *how* and *why* these organizations are selected, and what defenders should expect during each phase of an intrusion.

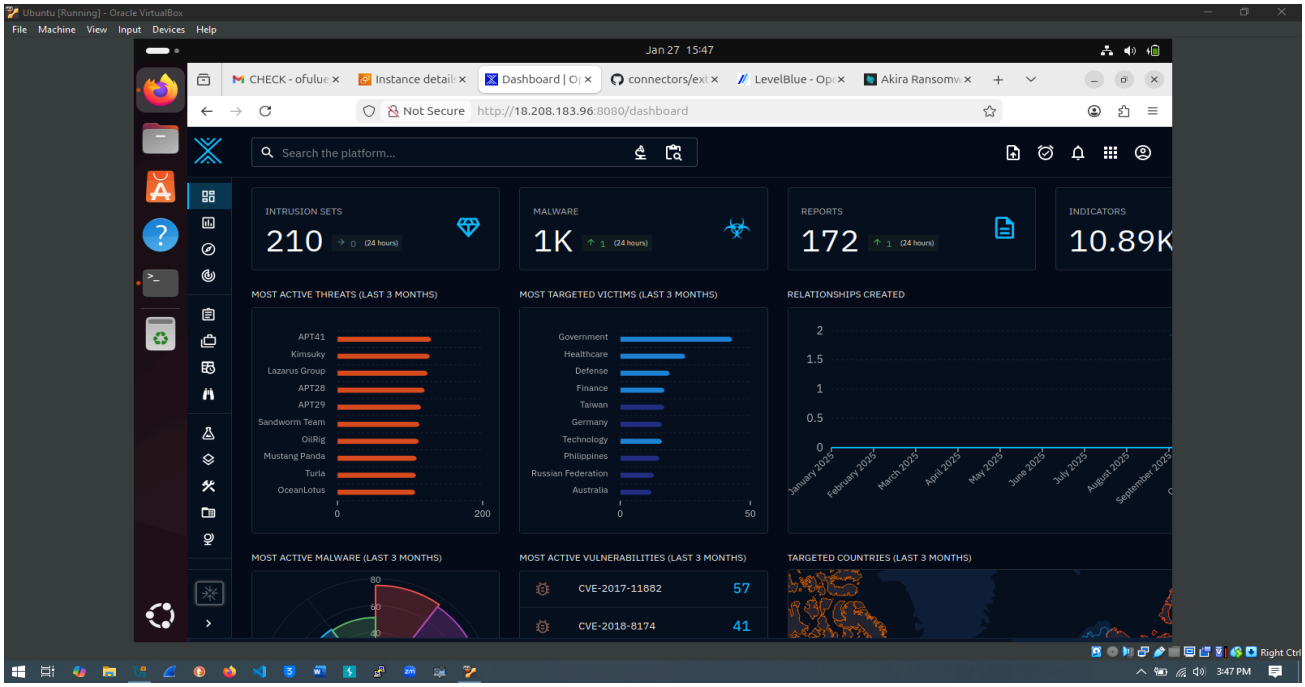

Fig 12.0 OpenCTI Dashboard showing most Active threats & targeted victims

7.1 Victim Profile 1: Government Institutions

Sector Overview

Government institutions represent high-value targets due to their access to sensitive national data, transportation systems, citizen records, and strategic infrastructure. Attacks against this sector are typically motivated by espionage, political influence, or strategic disruption, rather than immediate financial gain.

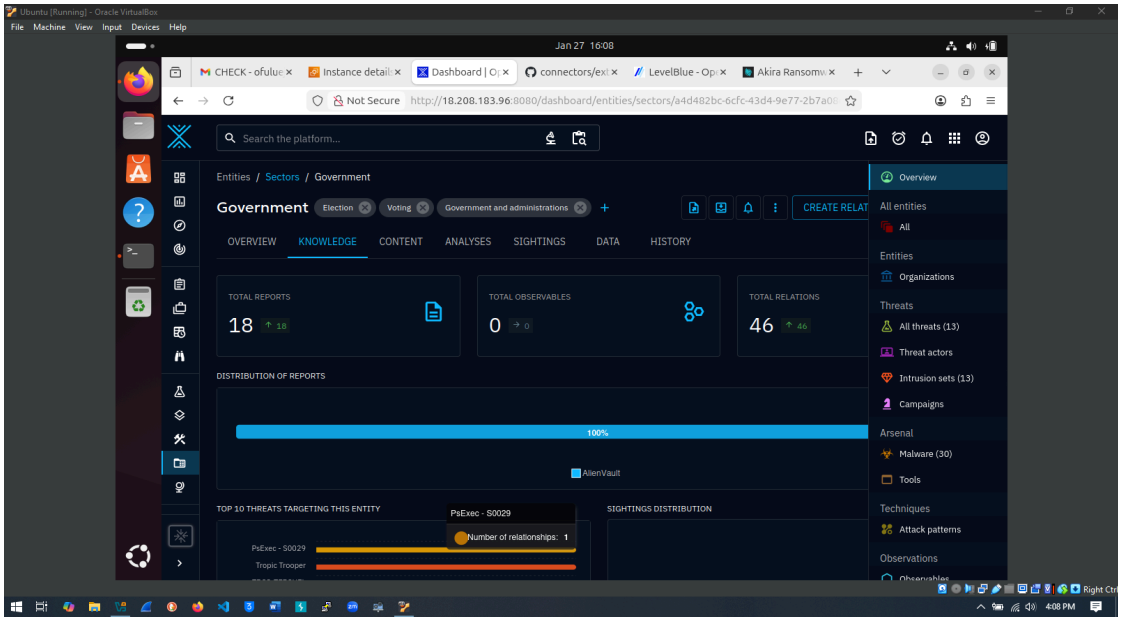

Fig 12.1 Victim profile for the Government Sector

Identified Threat

Primary Tool: PSExec (S0029)
Associated Threat Actor: Chafer

Chafer is a threat group known for targeting government and transportation sectors in the Middle East, with operations focused on credential theft, internal reconnaissance, and long-term access.

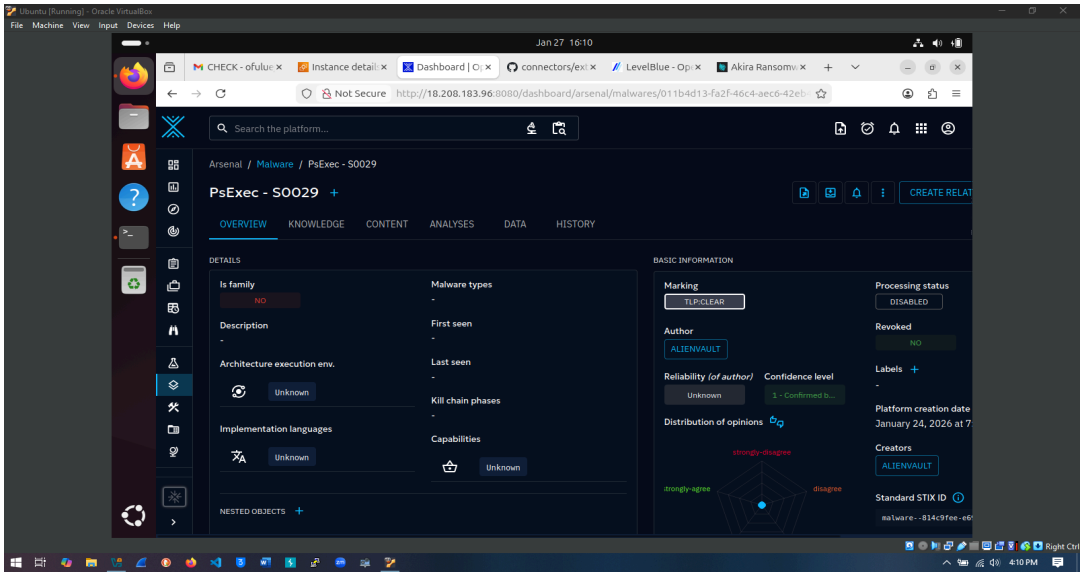

Fig 12.2 Overview of the PsExec tool

7.1.1 Diamond Model Analysis

Adversary

Chafer is assessed as a persistent threat actor specializing in espionage-oriented intrusions. The group favors low-noise techniques and legitimate administrative tooling to blend into normal system activity.

Capability

Chafer's operational capabilities include:

- Credential harvesting (T1003 - OS Credential Dumping)
- Abuse of valid administrative credentials (T1078 Valid Accounts)
- Lateral movement using built-in Windows tools (T1021.002 - SMB/Windows Admin Shares)
- Defense evasion via legitimate binaries (T1218 - Signed Binary Proxy Execution)

Infrastructure

The group leverages:

- Compromised internal servers
- Proxy infrastructure to mask command-and-control traffic (T1090 - Proxy)
- Legitimate remote administration tools to reduce malware footprint

Victimology

Primary targets include:

- Government agencies
- Transportation authorities

Geographic focus historically includes Kuwait and Saudi Arabia, though techniques are globally applicable.

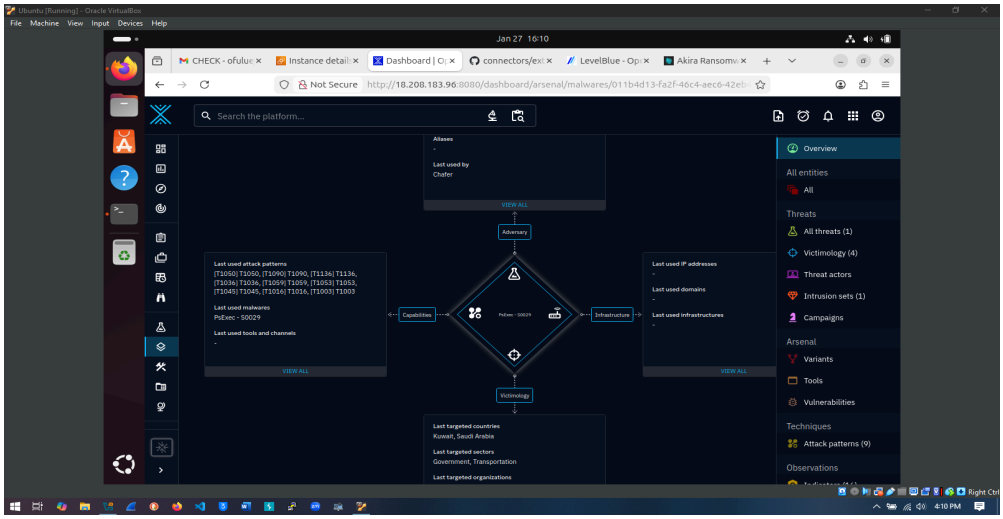

Fig 12.3 PsExec tool Diamond Chain

7.1.2 Kill Chain Mapping

- **Initial Access:**

Credential compromise via phishing or exposed services (T1566 - Phishing,

T1078 - Valid Accounts)

- **Execution:**
  Remote command execution via PSExec (T1569 - System Services)

- **Persistence:**
  Scheduled tasks and service creation (T1053 - Scheduled Task, T1543 - Create or Modify System Process)

- **Defense Evasion:**
  Living-off-the-land binaries (T1218)

- **Credential Access:**
  Memory dumping and registry access (T1003)

- **Discovery:**
  Network and account discovery (T1018 - Remote System Discovery, T1087 - Account Discovery)

- **Command & Control:**
  Proxy-based C2 channels (T1090)

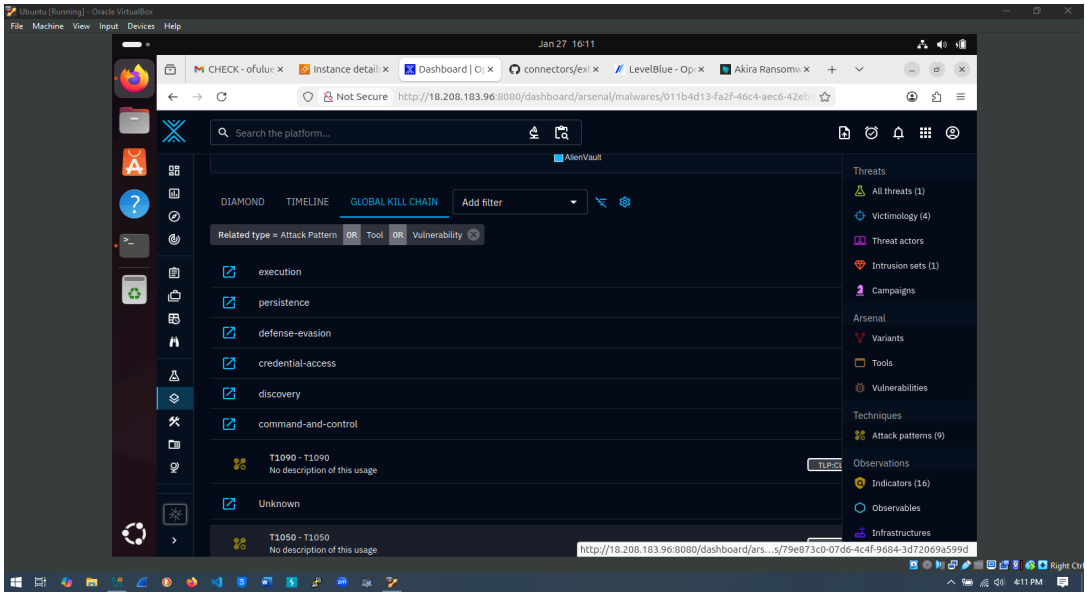

Fig 12.4 PsExec Global kill chain

Timeline

Observed Activity: January 24, 2026 - 6:46 PM

This timestamp aligns with off-hours activity, suggesting deliberate timing to reduce detection by SOC teams.

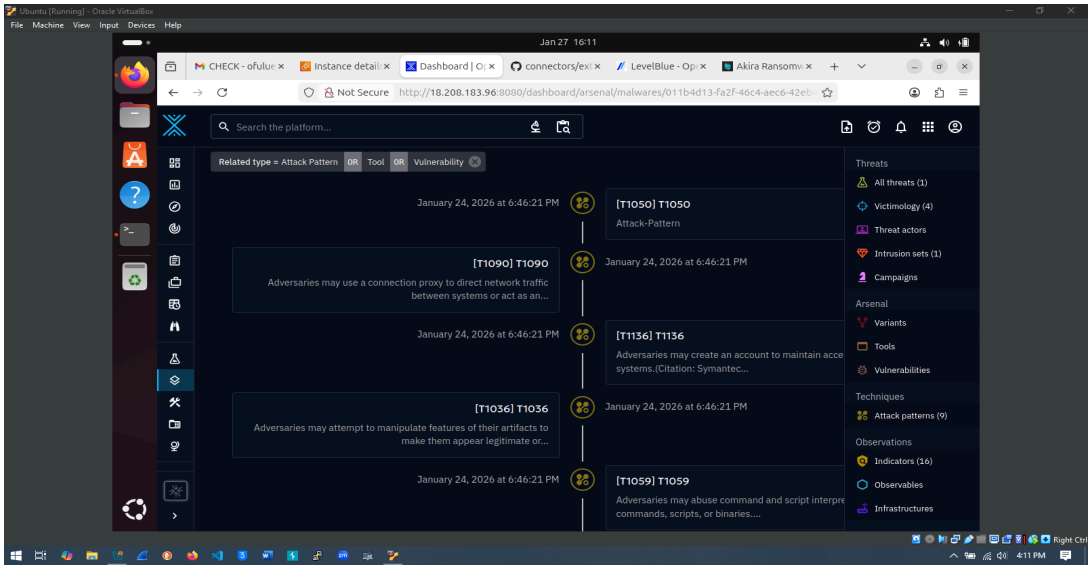

Fig 12.5 Attack timeline I

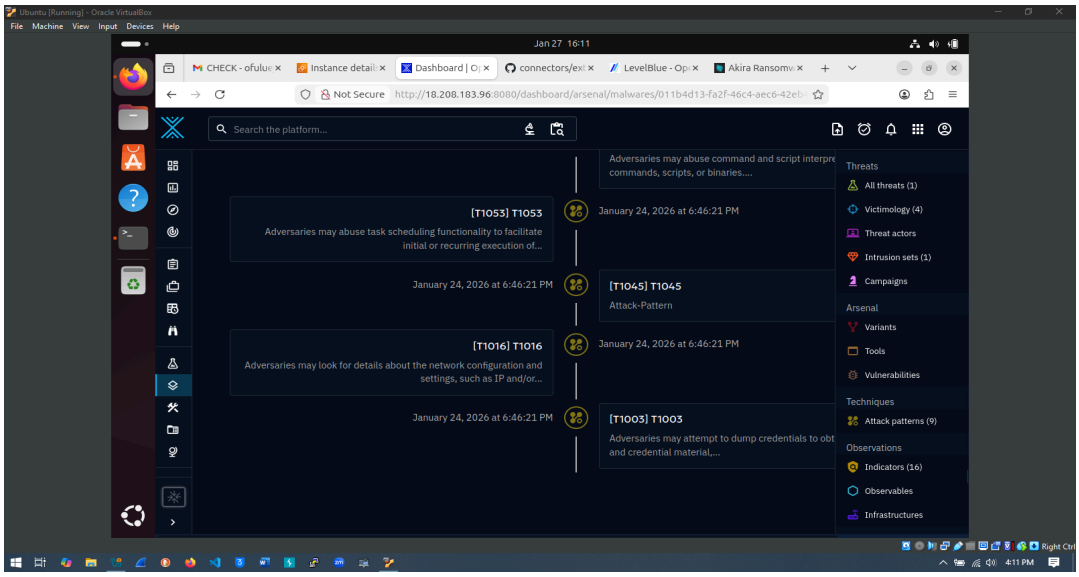

Fig 12.6 Attack timeline II

Strategic Assessment

Chafer's reliance on legitimate administrative tooling highlights the difficulty of detecting such intrusions using signature-based defenses. Government institutions without strong credential hygiene, privileged access monitoring, and behavioral analytics remain particularly vulnerable.

7.2 Victim Profile 2: Healthcare Sector

Sector Overview

Healthcare organizations are increasingly targeted due to:

- High-value personal and medical data
- Operational sensitivity (downtime risks patient safety)
- Historically weaker security postures

Attacks against healthcare often combine espionage, data theft, and operational disruption.

Identified Threat

Threat Group: Tropic Trooper
Associated Actor: Pirate Panda

Tropic Trooper is a long-standing advanced persistent threat active since at least 2011, known for targeting healthcare, government, defense, and high-tech sectors across the Asia-Pacific region.

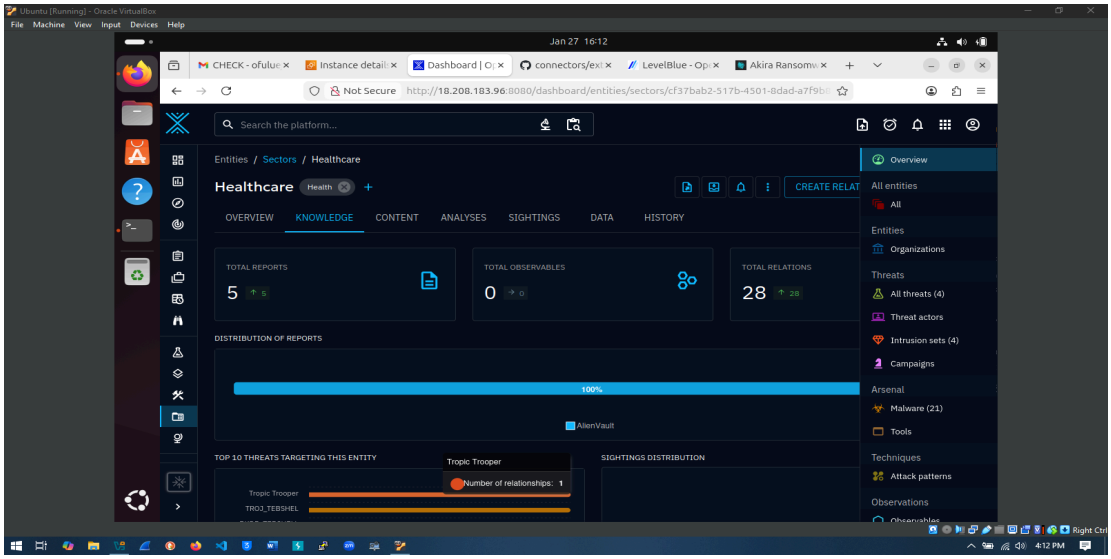

Fig 13.0 Victim profile for the Healthcare Sector

7.2.1 Diamond Model Analysis

Adversary

Pirate Panda operates as a strategic intelligence collection group, prioritizing long-term access and covert exfiltration.

Capability

Key capabilities include:

- Custom backdoors (T1059 - Command and Scripting Interpreter)
- Spear-phishing campaigns (T1566.001 - Spearphishing Attachment)
- Encrypted command-and-control channels (T1095 - Non-Application Layer Protocol)
- Lateral movement via credential reuse (T1021 - Remote Services)

Infrastructure

- Compromised web servers for C2 (T1505.003 - Web Shell)
- DNS-based C2 infrastructure (T1071.004 - DNS)
- Use of removable media in some campaigns (T1092 - Communication Through Removable Media)

Victimology

- Healthcare providers
- Defense organizations
- Government agencies

Primary geographic focus includes the Philippines and Taiwan.

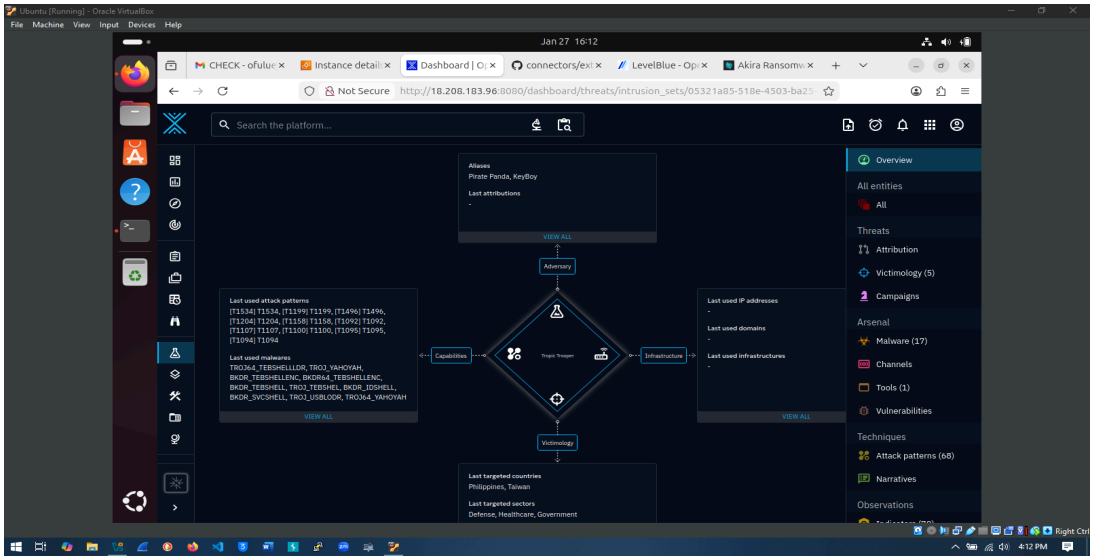

Fig 13.1 Tropic Trooper Diamond Chain

7.2.2 Kill Chain Mapping

- **Initial Access:**
  Spear-phishing emails and malicious attachments (T1566.001)
- **Execution:**
  Script-based payload execution (T1059)
- **Persistence:**
  Registry run keys and scheduled tasks (T1547 - Autostart Execution)
- **Defense Evasion:**
  Obfuscation and encryption (T1027 - Obfuscated Files or Information)
- **Discovery:**
  System and network enumeration (T1082 - System Information Discovery, T1016 - Network Discovery)
- **Lateral Movement:**
  Credential-based access (T1021)
- **Collection:**
  Harvesting medical and research data (T1213 - Data from Information Repositories)

- **Command & Control:**
  DNS and encrypted channels (T1071.004, T1095)

- **Exfiltration:**
  Covert data transfer (T1041 - Exfiltration Over C2 Channel)

- **Impact:**
  Intelligence collection and operational leverage rather than destruction

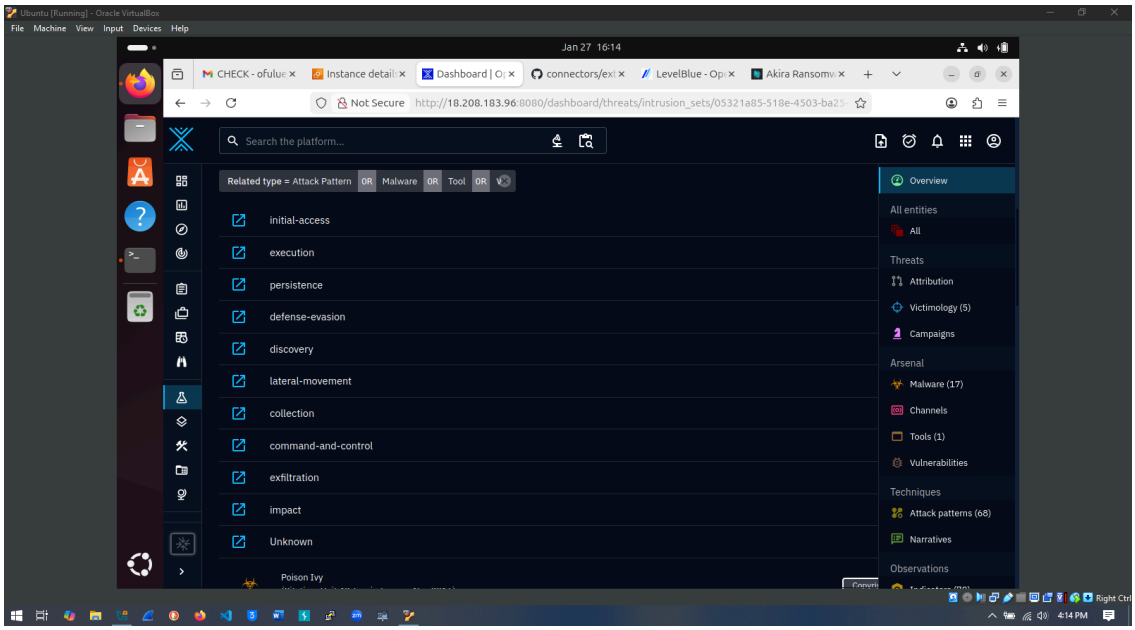

Fig 13.2 Kill chain

Timeline

Observed Activity: January 24, 2026 - 6:46 PM

This consistency across victim profiles suggests coordinated intelligence collection or shared reporting windows rather than isolated incidents.

Strategic Assessment

Healthcare organizations face sustained APT interest due to the sensitivity of their data and their reliance on uptime. Detection requires visibility into email security, DNS traffic, and abnormal credential usage.

7.3 Victim Profile 3: Defense Sector

Sector Overview

Defense organizations represent strategic intelligence targets, with adversaries seeking military capabilities, procurement data, and geopolitical insight.

Identified Threat

Threat Group: Tropic Trooper
Associated Actor: Pirate Panda

The defense sector exhibits identical tooling, techniques, and infrastructure to those observed in healthcare intrusions, indicating a deliberate multi-sector intelligence collection campaign.

7.3.1 Threat Pattern Analysis

The reuse of:

- Phishing infrastructure (T1566)
- Encrypted C2 (T1095)
- Data exfiltration methods (T1041)

Demonstrates a standardized operational playbook optimized for stealth and persistence.

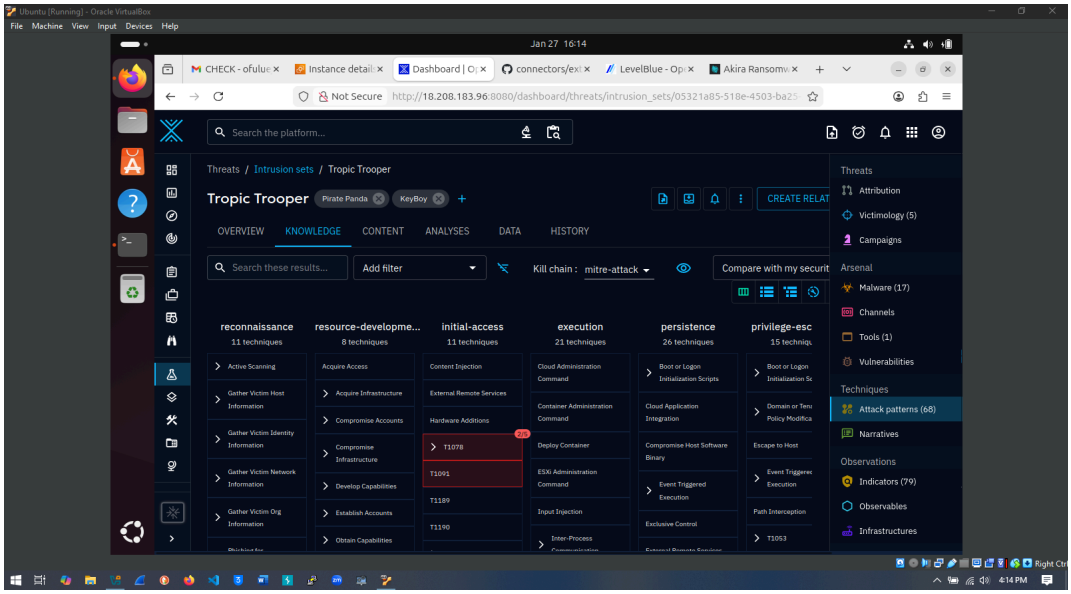

Fig 14.0 Threat pattern analysis I

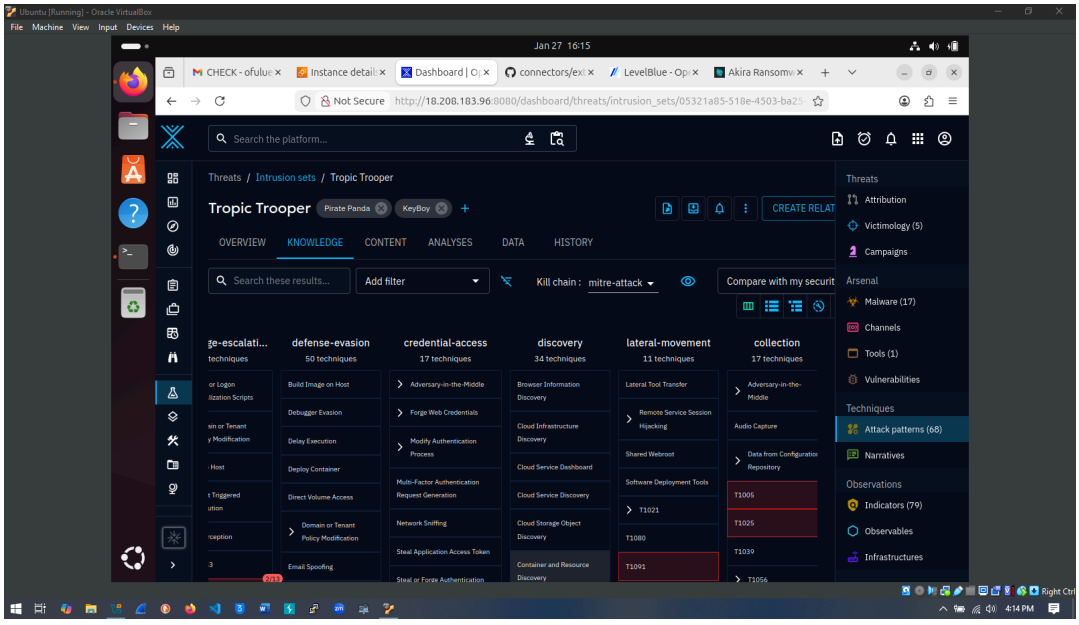

Fig 14.1 Threat pattern analysis II

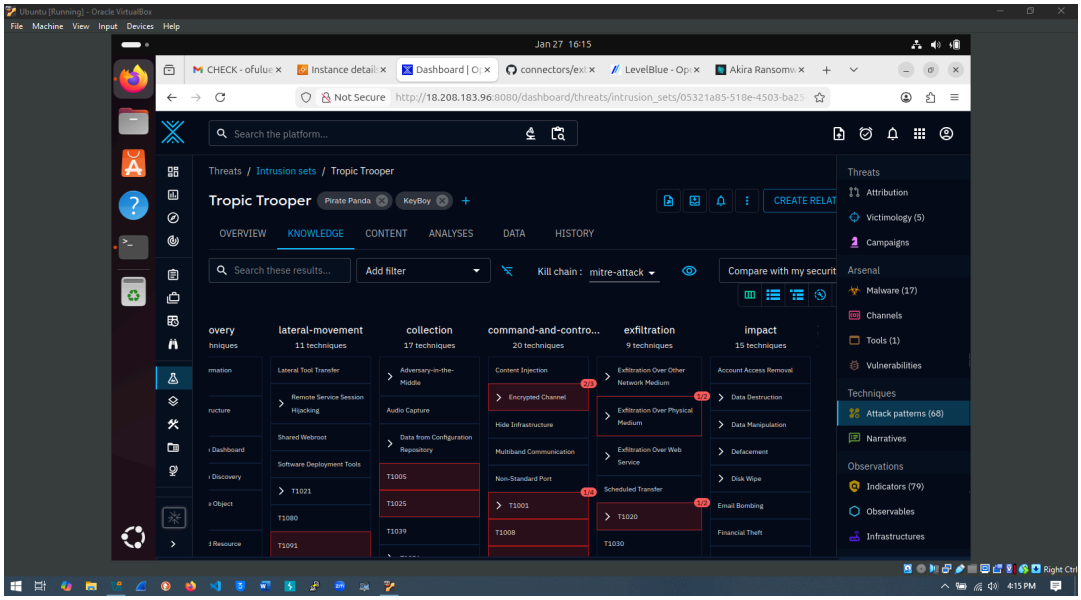

Fig 14.2 Threat pattern analysis III

Strategic Assessment

The overlap between healthcare and defense targeting indicates that Pirate Panda prioritizes data value over sector boundaries. Organizations with shared vendors, contractors, or personnel represent elevated risk due to potential cross-sector exposure.

8.0. Detection & Mitigation Recommendations per Victim

8.1 Government Institutions - Detection & Mitigation

Detection Recommendations

Given Chafer's reliance on legitimate administrative tools and stolen credentials, detection must focus on behavioral anomalies rather than malware signatures.

Credential Abuse & Access Monitoring

- Monitor for abnormal use of privileged accounts (T1078 - Valid Accounts), especially:
    - Logins outside normal business hours
    - Administrative access from non-standard source IPs

- Enable alerts for LSASS access or memory dumping activity (T1003 - OS Credential Dumping)

Lateral Movement Detection

- Log and alert on PSExec usage across the environment (T1021.002 - SMB/Windows Admin Shares)
- Detect creation of new services or scheduled tasks (T1543 - Create or Modify System Process, T1053 - Scheduled Task)

Command-and-Control Visibility

- Monitor outbound traffic to proxy services or unusual routing paths (T1090 - Proxy)
- Correlate internal host behavior with external beaconing patterns

Mitigation Recommendations

- Enforce Multi-Factor Authentication (MFA) on all privileged and remote access accounts
- Apply least privilege principles to administrative users
- Disable or tightly restrict PSExec usage where not operationally required
- Implement Privileged Access Management (PAM) solutions
- Conduct regular credential hygiene audits and password rotations
- Centralize Windows event logs and correlate via SIEM

8.2 Healthcare Sector - Detection & Mitigation

Detection Recommendations

Tropic Trooper operations emphasize phishing, stealthy persistence, and encrypted command-and-control.

Email & Initial Access Monitoring

- Detect spear-phishing attachments and malicious links (T1566.001 - Spearphishing Attachment)
- Monitor macro execution and suspicious scripting activity (T1059 - Command and Scripting Interpreter)

Persistence & Defense Evasion

- Alert on registry run key creation and scheduled task persistence (T1547 - Autostart Execution)
- Detect obfuscated or encrypted binaries on endpoints (T1027 - Obfuscated Files or Information)

C2 & Data Exfiltration

- Monitor DNS traffic for tunneling or abnormal query patterns (T1071.004 - DNS)
- Detect sustained encrypted outbound connections to unknown destinations (T1095 - Non-Application Layer Protocol, T1041 - Exfiltration Over C2 Channel)

Mitigation Recommendations

- Deploy advanced email security gateways with sandboxing
- Implement DNS logging and analysis across the enterprise
- Enforce application allowlisting on endpoints
- Segment clinical systems from corporate IT networks
- Conduct regular phishing awareness training
- Ensure EDR solutions are tuned for script-based attacks

8.3 Defense Sector - Detection & Mitigation

Detection Recommendations

Given the overlap with healthcare targeting, detection strategies should emphasize cross-sector threat reuse.

Threat Hunting

- Hunt for known Tropic Trooper indicators reused across sectors
- Detect credential reuse across unrelated systems (T1078, T1021)

Data Collection Monitoring

- Monitor access to sensitive defense documentation repositories (T1213 - Data from Information Repositories)

- Detect bulk file access or compression before exfiltration (T1560 - Archive Collected Data)

Mitigation Recommendations

- Enforce network segmentation between classified, operational, and administrative systems
- Apply Zero Trust access principles
- Monitor third-party and contractor access closely
- Conduct routine red-team and tabletop exercises simulating APT intrusions
- Align detection coverage explicitly to MITRE ATT&CK techniques observed

Executive Takeaways

- Victim targeting reflects intentional, intelligence-driven selection
- Credential compromise is central across all observed intrusions
- Legitimate tools and stealthy C2 channels complicate detection
- Cross-sector overlaps increase supply-chain and partner risk
- Continuous monitoring mapped to MITRE ATT&CK is essential for early detection

9.0 Task 4: Politically Motivated Threat Group

Overview

Politically motivated threat actors, particularly state-sponsored and state-aligned advanced persistent threat (APT) groups, conduct cyber operations to advance national strategic objectives rather than direct financial gain. These operations are commonly observed during periods of geopolitical tension, armed conflict, or diplomatic pressure and are designed to disrupt critical services, undermine public trust, and exert psychological influence.

Sandworm represents a highly capable, politically motivated cyber threat group whose operations emphasize destructive impact, strategic signaling, and disruption of national infrastructure. Unlike opportunistic cybercrime groups, Sandworm prioritizes operational effect and geopolitical leverage over stealth or monetization.

9.1 Identified Threat Group: Sandworm (APT44 / Seashell Blizzard)

This assessment focuses on Sandworm, a Russia-aligned, state-sponsored threat group attributed with high confidence to the Russian Main Intelligence Directorate (GRU). The group has a long operational history targeting NATO-aligned countries and Ukraine, with recent activity in 2025 extending into Poland's critical energy sector.

Sandworm's campaigns demonstrate a clear pattern of politically motivated cyber sabotage aligned with Russian strategic and military objectives.

9.1.1 Diamond Model Analysis

Adversary

Sandworm is an advanced persistent threat group operating in alignment with Russian state interests. The group is known for conducting destructive cyber operations intended to:

- Support geopolitical and military objectives
- Disrupt critical national infrastructure
- Undermine public confidence in government and essential services
- Apply pressure during periods of geopolitical escalation

Its operations are frequently timed to coincide with symbolic dates or major geopolitical events to maximize psychological and political impact.

Capability

Sandworm possesses advanced offensive cyber capabilities with a strong emphasis on destructive tooling. Observed capabilities include:

- Data-wiping malware (T1485 - Data Destruction)
    - DynoWiper (2025)
    - ZEROLOT and Sting wiper variants
    - Historical tools such as BlackEnergy and KillDisk
- Living-off-the-land (LotL) techniques to evade detection
- Web shell deployment for persistent access (T1505.003 - Web Shell)
- Credential abuse and exploitation of public-facing systems for initial access

These capabilities enable Sandworm to disrupt operational environments and render systems unrecoverable rapidly.

Infrastructure

Sandworm leverages a combination of compromised and legitimate infrastructure to conduct operations, including:

- Compromised Windows enterprise environments
- Web shells deployed on exposed servers
- Stolen or abused credentials for lateral movement
- Targeted industrial and energy management networks (e.g., CHP systems)

The group minimizes reliance on noisy external infrastructure, favoring trusted internal environments to sustain access and execute destructive payloads.

Victimology

Sandworm consistently targets high-value, politically sensitive sectors, including:

- Energy and power grid operators
- Government and military institutions
- Critical national infrastructure
- Logistics and industrial control environments

In 2025, victim targeting expanded beyond Ukraine to include Poland's energy sector, reinforcing Sandworm's focus on NATO-aligned states. Targets are selected for strategic and symbolic value rather than economic gain.

9.1.2 Kill Chain Mapping

Reconnaissance

- Identification of public-facing systems and exposed services
- Targeted selection of critical infrastructure operators
  (T1595 - Active Scanning)

Initial Access

- Exploitation of vulnerable public-facing applications (T1190)
- Abuse of stolen or valid credentials (T1078 - Valid Accounts)

Execution & Persistence

- Deployment of web shells for sustained access
- Use of native system tools (LotL techniques) to avoid detection (T1059 - Command and Scripting Interpreter)

Impact

- Activation of destructive wiper malware
- Irreversible data destruction and system disruption (T1485 - Data Destruction)

9.2 Campaign Analysis

9.2.1 Campaign 1: Poland Energy Sector (December 2025)

Overview:
In late December 2025, Sandworm conducted a destructive cyber operation targeting Poland's energy infrastructure using a newly identified wiper malware, DynoWiper.

Impact:
While the attack did not result in sustained power outages, it represented a significant escalation and demonstrated Sandworm's intent to expand operations into NATO-aligned energy sectors.

Diamond Model Summary:

- **Adversary:** Sandworm (APT44, GRU-aligned)
- **Capability:** DynoWiper data-wiping malware

- **Infrastructure:** CHP plants and renewable energy management networks
- **Victim:** Polish energy infrastructure operators

- **Timeline:** December 29 - 30, 2025

9.2.2 Campaign 2: Ukrainian Government & Energy Sectors (Mid-Late 2025)

Overview:

Between June and September 2025, Sandworm conducted widespread destructive campaigns against the Ukrainian government, energy, logistics, and agricultural sectors.

Malware:

- ZEROLOT
- Variants of Sting wiper malware

Diamond Model Summary:

- **Adversary:** Sandworm (APT44)
- **Capability:** ZEROLOT and Sting destructive payloads
- **Infrastructure:** Compromised enterprise environments and web shells
- **Victim:** Ukrainian government and critical infrastructure entities
- **Timeline:** June-September 2025

These operations resulted in extensive data destruction and operational disruption across multiple sectors.

Detection Recommendations

- Monitor for unauthorized deployment of wiper-like processes and abnormal file deletion activity
- Detect web shell activity and anomalous administrative access

- Correlate threat intelligence reporting with geopolitical events
- Monitor credential usage patterns for signs of abuse

Mitigation Recommendations

- Harden and patch all public-facing systems
- Enforce strong credential hygiene and multi-factor authentication
- Maintain segmented, offline backups of critical systems
- Conduct regular incident response simulations focused on destructive attacks
- Integrate CTI feeds (e.g., OpenCTI, AlienVault OTX) into SOC workflows

9.3 Executive Assessment

Sandworm represents a high-impact, politically motivated cyber threat capable of executing destructive operations against critical national infrastructure. While not always aimed at immediate service disruption, its campaigns are designed to signal capability, undermine confidence, and exert geopolitical pressure.

Organizations operating within energy, government, or critical infrastructure sectors, particularly in NATO-aligned regions, must assume Sandworm as a credible threat actor. Proactive intelligence integration, strong defensive controls, and preparedness for destructive attack scenarios are essential to mitigating risk from this adversary.

10.0 Detection, Monitoring & Defensive Considerations

Detection Strategies

- Monitor OpenCTI for emerging indicators and campaigns
- Correlate OTX pulses with SIEM and EDR telemetry
- Apply behavioral detection aligned with MITRE ATT&CK

Preventive Controls

- Network segmentation and least-privilege access
- MFA enforcement and credential monitoring
- Regular threat intelligence updates and simulations

11.0 Key Findings & Strategic Recommendations

Key Findings

- **Persistent Ransomware Threat:**
  Ransomware activity remains a significant risk, capable of causing operational downtime and data compromise.

- **Active State-Sponsored Espionage:**
  Nation-state actors continue to conduct intelligence collection and pre-positioning within targeted networks.

- **Rise in Politically Motivated Destructive Attacks:**
  Wiper malware and sabotage-focused campaigns are increasingly used to disrupt critical services during geopolitical tensions.

- **Widespread Credential Compromise:**
  Abuse of valid accounts is a common initial access technique across observed

threat campaigns.

- **Increased Targeting of Critical Sectors:**
  Critical infrastructure, government, healthcare, and defense sectors remain high-value targets due to strategic and symbolic importance.

Aligned Strategic Recommendations

- **Enhance Ransomware Readiness:**
  Implement regular offline backups, ransomware-focused incident response playbooks, and recovery testing to reduce operational impact.

- **Strengthen Monitoring for Advanced Threats:**
  Improve detection of lateral movement, persistence, and living-off-the-land techniques associated with state-sponsored actors.

- **Prepare for Destructive Attack Scenarios:**
  Integrate wiper and sabotage attack simulations into business continuity and disaster recovery planning.

- **Harden Identity and Access Management:**
  Enforce MFA, monitor privileged account usage, and deploy continuous authentication monitoring to reduce credential abuse.

- **Adopt Sector-Specific Threat Intelligence:**
  Leverage intelligence platforms such as OpenCTI to track adversaries targeting critical sectors and inform proactive defense measures.

Executive Outlook:

Organizations that treat cyber threat intelligence as a strategic capability, embedded into governance, decision-making, and resilience planning will be better positioned to anticipate, absorb, and recover from high-impact cyber events in an increasingly volatile threat landscape.

12.0 Lessons Learned

- Threat intelligence is most effective when aligned with business context
- Automation and enrichment significantly improve analyst efficiency
- Executive-ready reporting is critical for informed decision-making

References

OpenCTI Documentation

- OpenCTI Documentation. (n.d.). OpenCTI Documentation - Deployment, user guides & references. OpenCTI. Retrieved December 2025, from https://docs.opencti.io/latest/

AlienVault Open Threat Exchange (OTX)

- Open Threat Exchange (OTX). (n.d.). AlienVault Open Threat Exchange - threat intelligence sharing platform. AT&T Cybersecurity. Retrieved January 2026, from https://otx.alienvault.com/

MITRE ATT&CK Framework

- MITRE ATT&CK®. (n.d.). MITRE ATT&CK® - Adversarial Tactics, Techniques, and Common Knowledge framework. The MITRE Corporation. Retrieved January 2026, from https://attack.mitre.org/

Docker Documentation

- Docker. (n.d.). Docker documentation. Docker, Inc. Retrieved January 2026, from https://docs.docker.com/

Ubuntu Documentation

- Canonical. (n.d.). Ubuntu documentation. Canonical Ltd. Retrieved January 2026, from https://ubuntu.com/documentation

AWS Documentation

- Amazon Web Services. (n.d.). AWS documentation. Amazon. Retrieved January 2026, from https://docs.aws.amazon.com/

Appendix A: Sprint Timeline & Meetings

Dates	Times	Attendees
19th-Jan -2026	8:10 pm	John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Odunayo Balogun
21st-Jan-2026	8:10 pm	John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun
24th-Jan-2026	8:10 pm	John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun
27th-Jan-2026	8:10 pm	John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Divine Ezewele, Andrew Moses, Odunayo Balogun
29th-Jan-2026	8:10pm	John Ofulue, Halimat Omorinsola Adepegba, Favour Obisike, Ikenna Emerole, Blessing Ibe, Ayodimeji Omole, Divine Ezewele, Andrew Moses, Odunayo Balogun

Appendix B: Team Contributions

Names	Roles and Responsibilities
John Ofulue	Team lead, assigned tasks, managed meetings, helped with presentation, and assisted with the report.
Halimat Omorinsola Adepegba	Assistant Team Lead. Helped with the Report writing and research.
Favour Obisike	Gave a walk-through of how to install OpenCTI and conducted more detailed research on the threat intel
Ikenna Emerole	Modified the team's report.
Blessing Ibe	Compiled and modified the report and created Appendix A and B
Ayodimeji Omole	Created the slides for the group presentation of the Threat Intel project.
Divine Ezewele	Created the slides for the group presentation of the Threat Intel project.
Andrew Moses	Responsible for this sprints team presentation.
Odunayo Balogun	Supported the setup and configuration of OpenCTI on AWS and locally, created and profiled an organization entity, ingested threat intelligence feeds, analyzed and linked relevant threats using the latest OpenCTI interface, and contributed to the team presentation