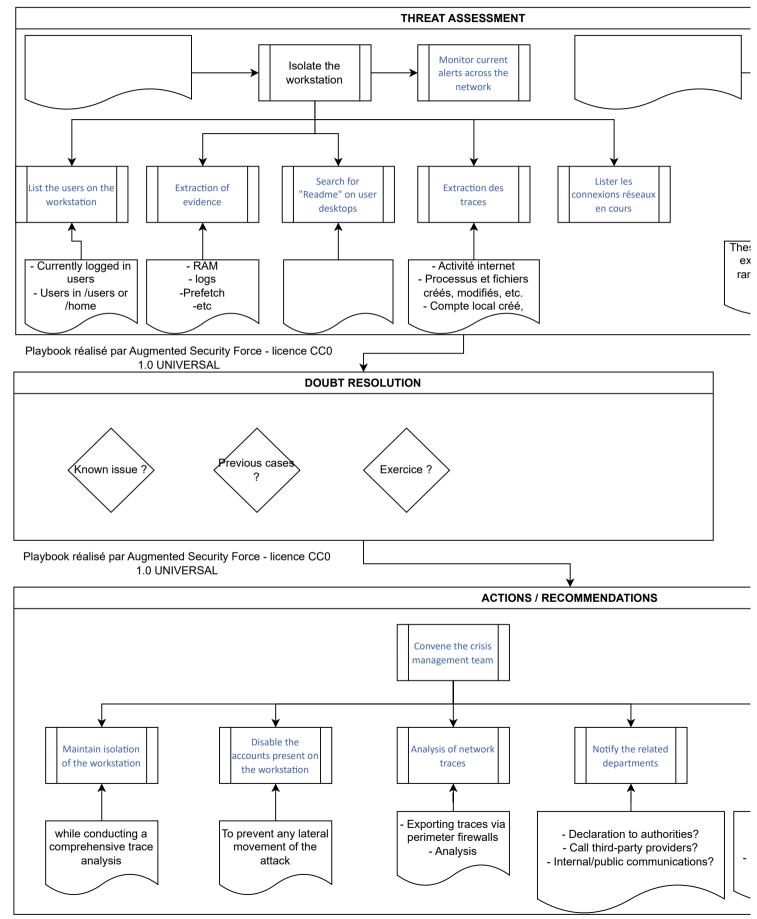# Ransomware

This type of malware prevents users from accessing their files or systems until a payment is made to the cybercriminals. Detection relies on identifying typical ransomware behaviors such as rapid encryption of multiple files, modification of file extensions, and displaying ransom messages.

THREAT ASSESSMENT

Isolate the workstation → Monitor current alerts across the network

- List the users on the workstation
  - Currently logged in users
  - Users in /users or /home
- Extraction of evidence
  - RAM
  - logs
  - Prefetch
  - etc
- Search for "Readme" on user desktops
- Extraction des traces
  - Activité internet
  - Processus et fichiers créés, modifiés, etc.
  - Compte local créé,
- Lister les connexions réseaux en cours

Thes
ex
ran

DOUBT RESOLUTION

- Known issue ?
- Previous cases ?
- Exercice ?

ACTIONS / RECOMMENDATIONS

Convene the crisis management team

- Maintain isolation of the workstation
  - while conducting a comprehensive trace analysis
- Disable the accounts present on the workstation
  - To prevent any lateral movement of the attack
- Analysis of network traces
  - Exporting traces via perimeter firewalls
  - Analysis
- Notify the related departments
  - Declaration to authorities?
  - Call third-party providers?
  - Internal/public communications?

Identify the role of
the workstation

Identify
vulnerabilities
present on the
workstation

se vulnerabilities could be
xploited in the context of
nsomware and guide the
investigation.

Analyze frist IoC
founds

Prepare the backups

Check decryption
tool

- Identify their locations
- Verify availability
- Check timestamps
Prepare for restoration in a private
network

nomoreransom.org