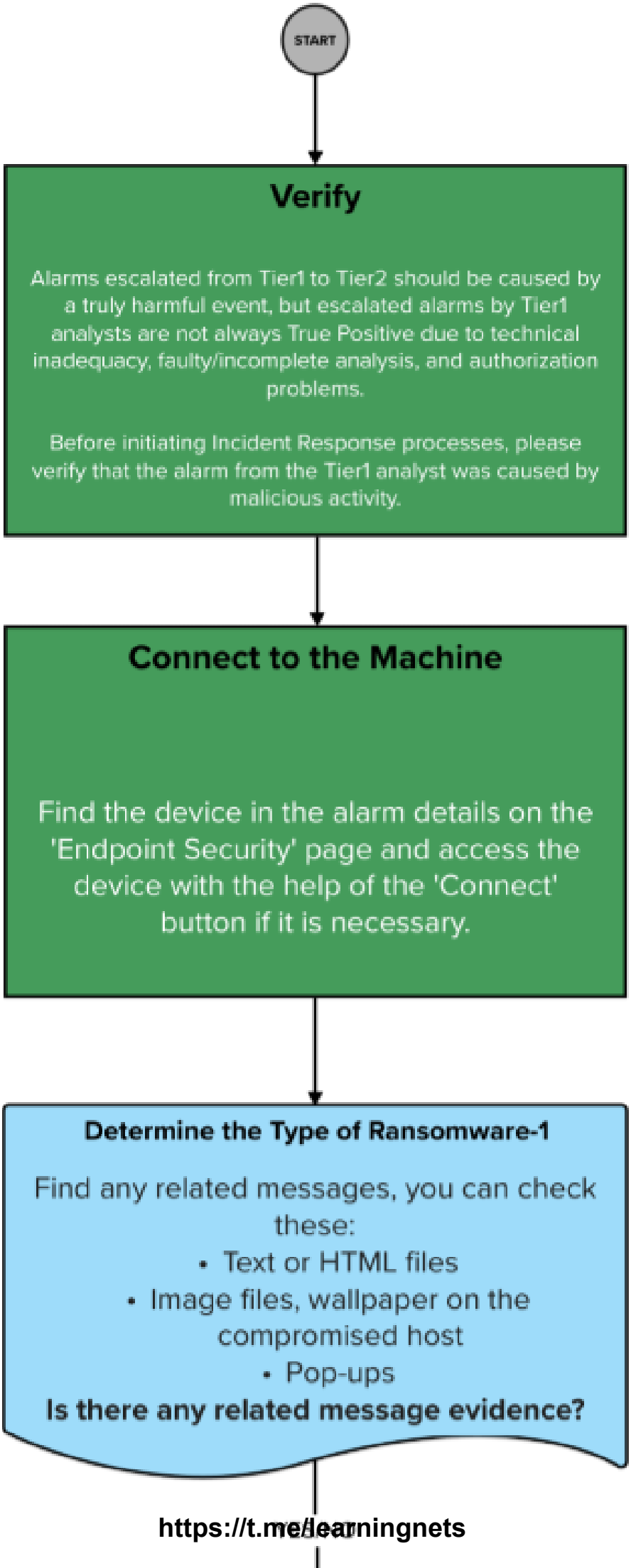
RANSOMWARE PLAYBOOK

FREE

letsdefend.io

LetsDefend

letsdefend.io



YES/NO

Determine the Type of Ransomware-2

Examine Texts to Identify Ransomware Type
- Ransomware name
- Contact email
- Language
- Payment method
- Payment address
- Support chat/support page

Is there any text evidence to identify the ransomware type?

YES/NO

Determine the Type of Ransomware-3

Analyze files, these are will be helpful:
- File extension (e.g., .crypt, .cry, .locked)
- File types and locations
- Icon for encrypted files

Is there file-type evidence to help identify the ransomware type?

YES/NO

Automated Categorization Services

Upload the encrypted file to the following services. Thus, you can obtain data that can be used to detect the variant. Even private keys associated with the respective ransomware variant can be obtained.
- Crypto Sheriff
- ID Ransomware
- ProvenData

Is there any useful data?

YES/NO

YES/NO

Identify The Root Cause

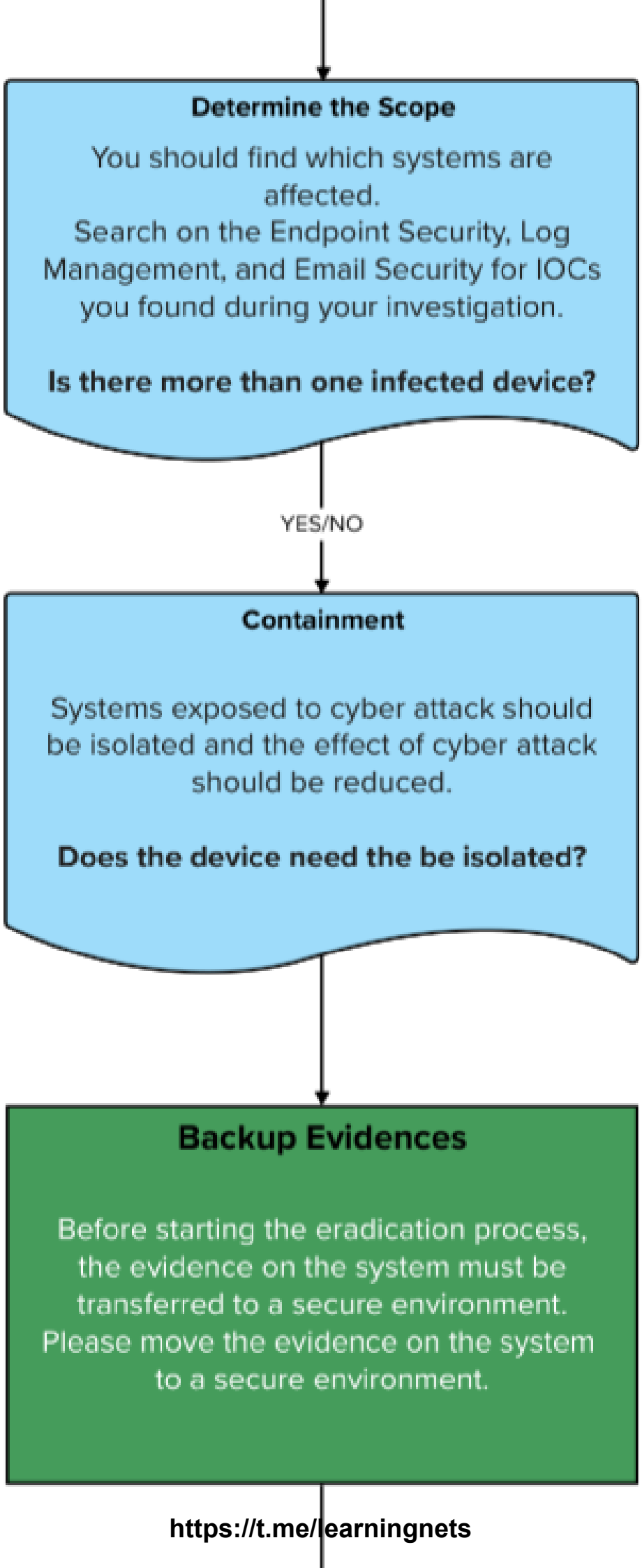
Detecting the root cause is the most important stage of Incident Response processes. The "open door" must be closed quickly by identifying the root cause of the attacker's access to the system. The attacker may have accessed the system by deceiving the user through a service open to the Internet or with a phishing attack.
Please identify the root cause of the incident.

Initial Access

It is very important to determine the technique used by the attacker in the "initial access" tactic in order to determine the root cause, make the systems more secure and not repeat the same incident again. Please choose the correct initial access method that was used in the attack.
If there is no initial access method used, please choose 'None' option.

What is the initial access method used in the attack?

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Addition
- Phishing
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- None



Eradication

Go to Endpoint Security and connect to the machine. Then, destroy any malicious file, user or other suspicious artifact that needs to be destroyed.

Recovery

Recovery phase is restoring all affected systems and devices to allow for normal operations to continue. Playbook's 'Recovery' task has been created to teach the stages of incident response. Recovery will not be performed.

Lesson Learned

- How did the cyber attack happen?
- How well did staff and management perform in dealing with the incident?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?