

Cybersecurity Incident Response:

From Detection to Recovery

A clear workflow from detection through recovery



DETECT AN INCIDENT

Security alert triggers investigation

Suspicious login

Malware detection

Unusual network activity



**NEXT STEP:
ASSESS THE INCIDENT**

ASSESS AND CLASSIFY

Determine affected systems

Assess potential impact and severity

Confirm if incident is valid

Understand scope and context



NEXT STEP:
CONTAINMENT

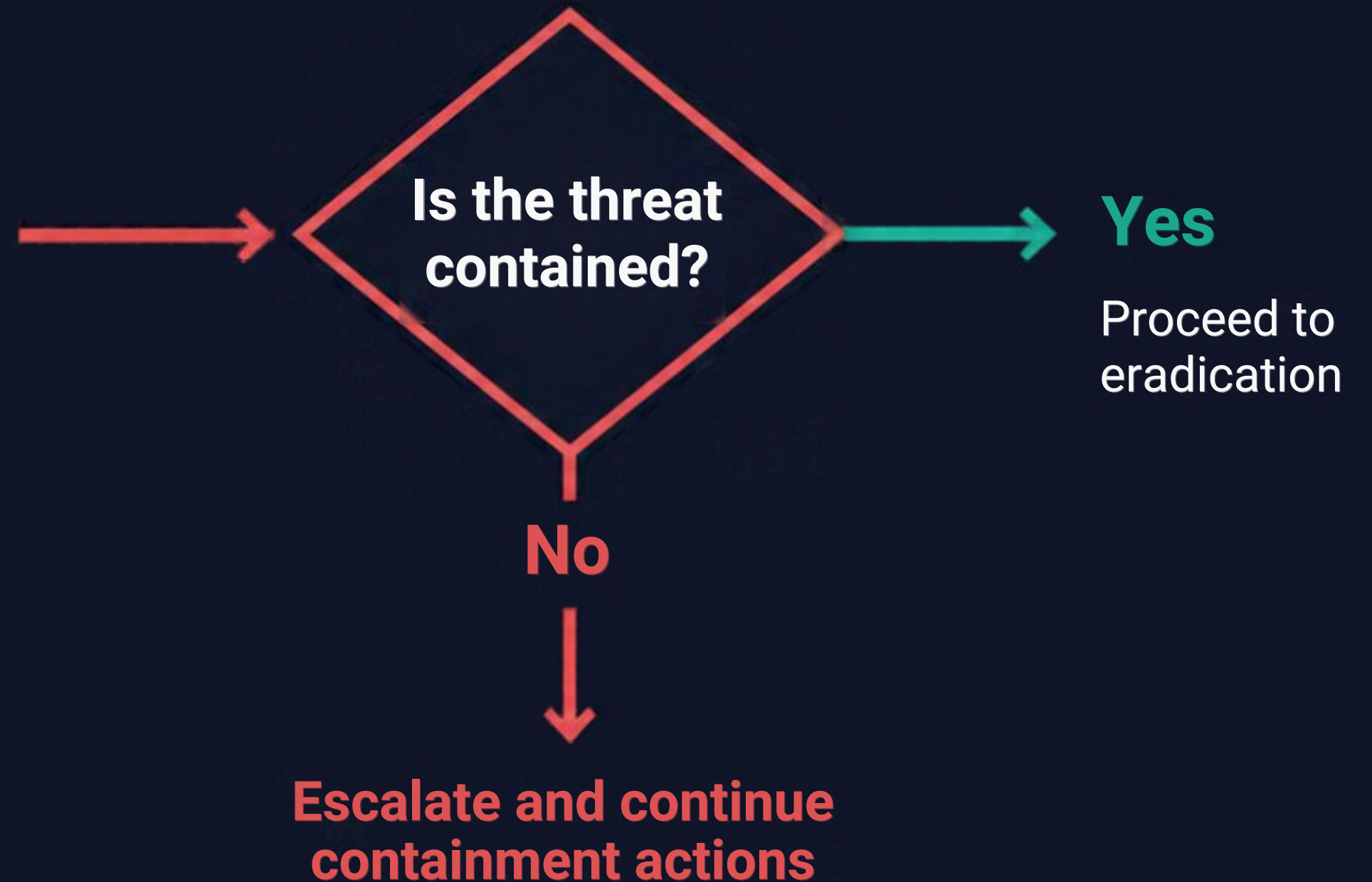
CONTAIN THE THREAT

Act quickly to isolate and limit damage.

Isolate affected devices

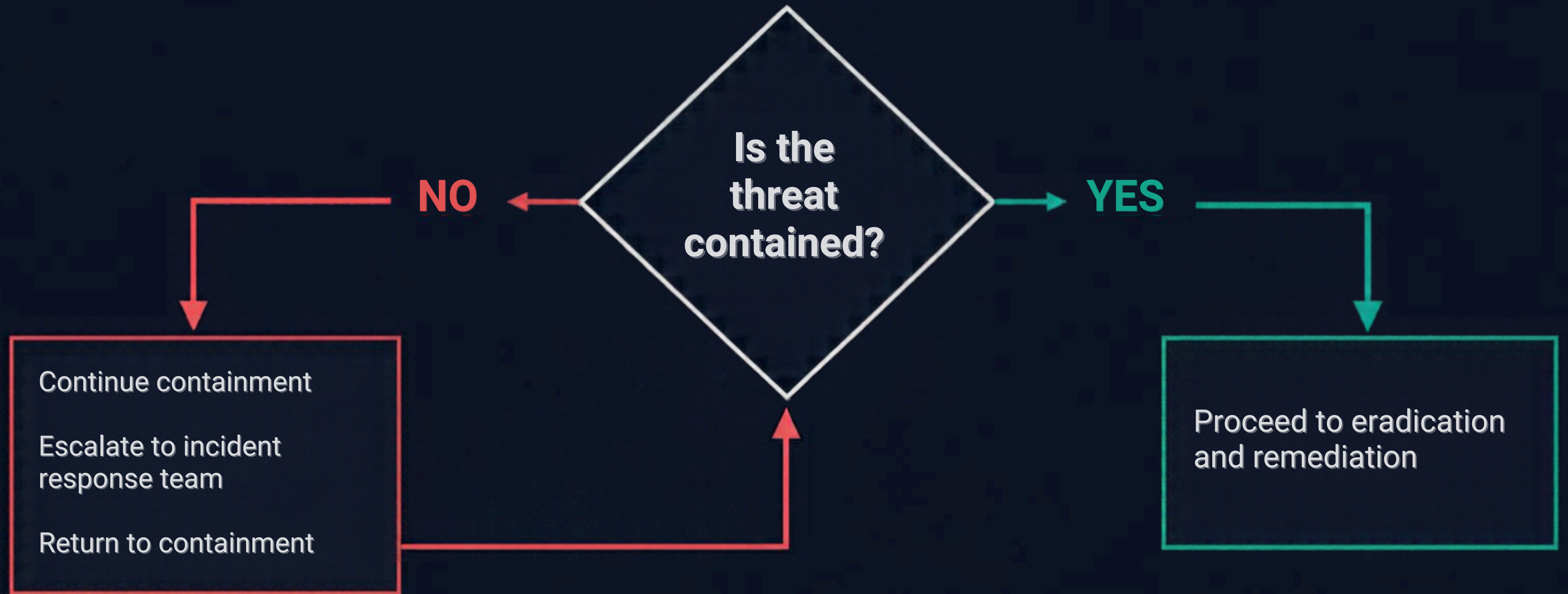
Disable compromised accounts

Restrict malicious network traffic



DECISION

IS THE THREAT CONTAINED?



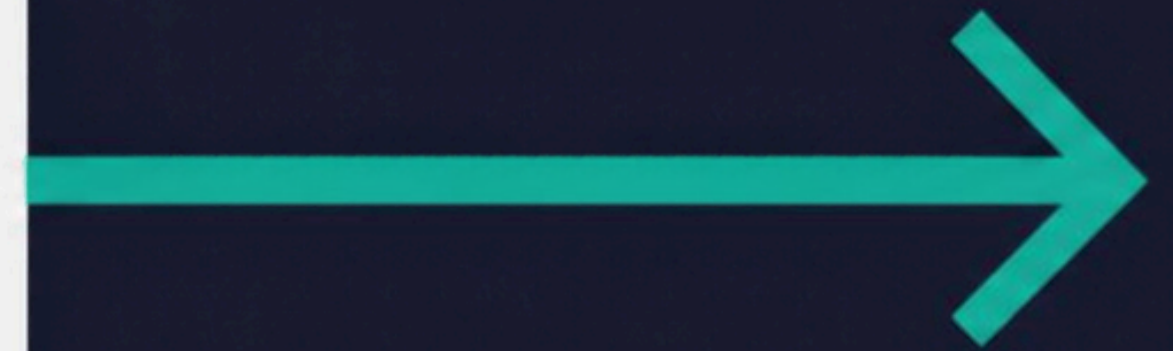
ERADICATE THE CAUSE

Remove malware

Close exploited vulnerabilities

Revoke compromised credentials

Fix root causes



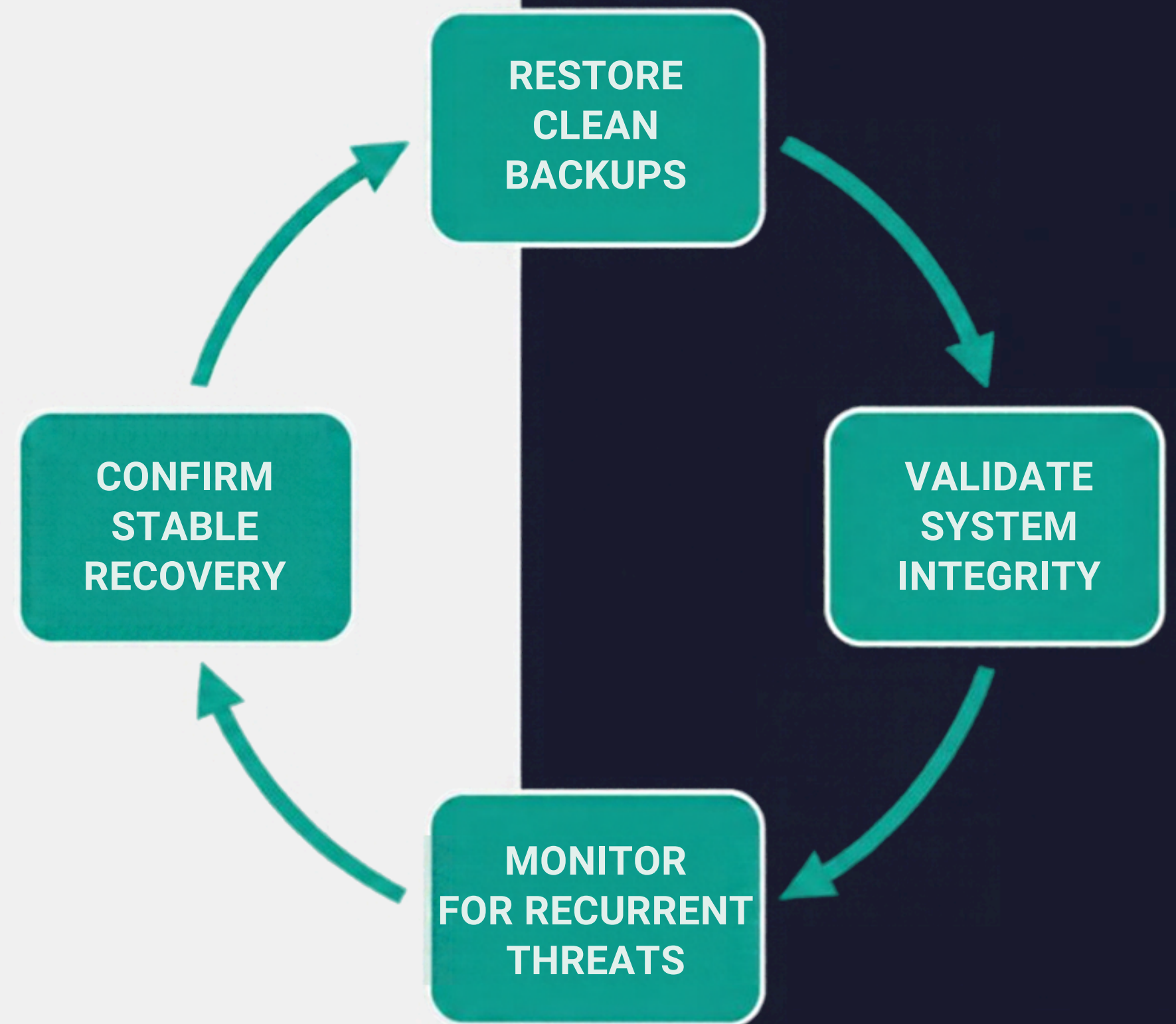
**NEXT STEP:
RECOVERY**

RECOVER SYSTEMS

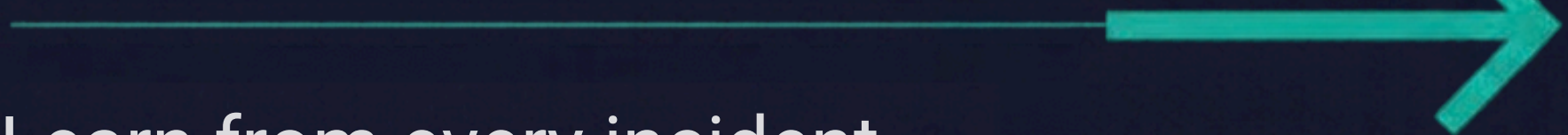
Restore clean backups as needed

Validate system integrity

Monitor for recurring
suspicious activity



REVIEW AND IMPROVE



Learn from every incident to strengthen your security posture.

Document the incident

Evaluate the response effectiveness

Update cybersecurity policies

Revise incident response playbooks

Address gaps found during investigation

SUPPORTING PILLARS

Policies define security requirements

Assessments identify weaknesses

Audits verify whether controls work

Playbooks guide response actions



THANK YOU

for your attention

QUESTIONS?