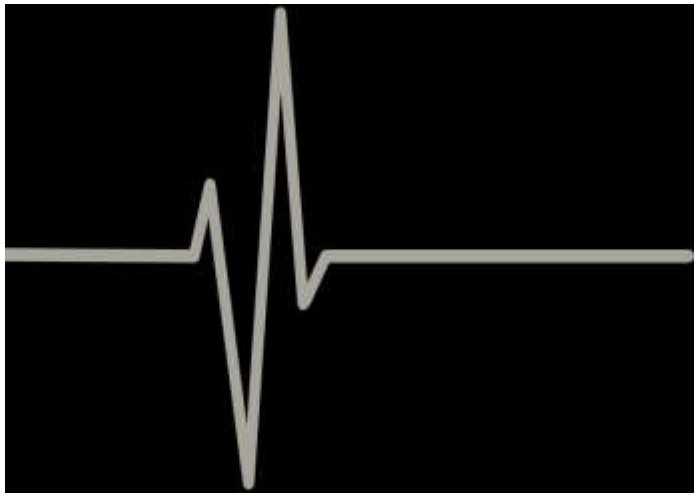
CODE BLUE CLEAR

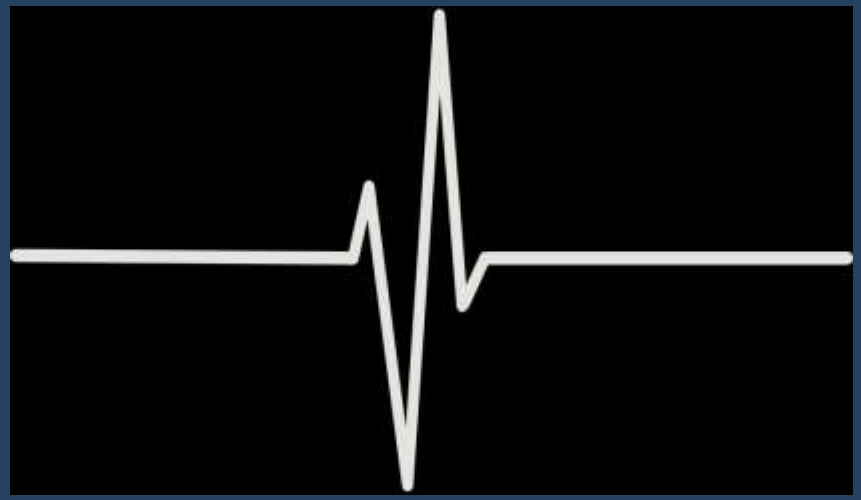


HOW ONE HOSPITAL SURVIVED THE BIGGEST RANSOMWARE ATTACK IN U.S. HISTORY

@REGHARNISH

GreyCastle security

CODE BLUE CLEAR



HOW ONE HOSPITAL SURVIVED THE BIGGEST RANSOMWARE ATTACK IN U.S. HISTORY

@REGHARNISH

GreyCastle security


CBSN ON ASSIGNMENT
E C M C
ERIE COUNTY MEDICAL CENTER
Great Lakes Health System of WNY
Welcome


ERIE COUNTY
MEDICAL CENTER
3
EMERGENCY
Main Entrance
Parking
David Miller Bldg.
E C M C

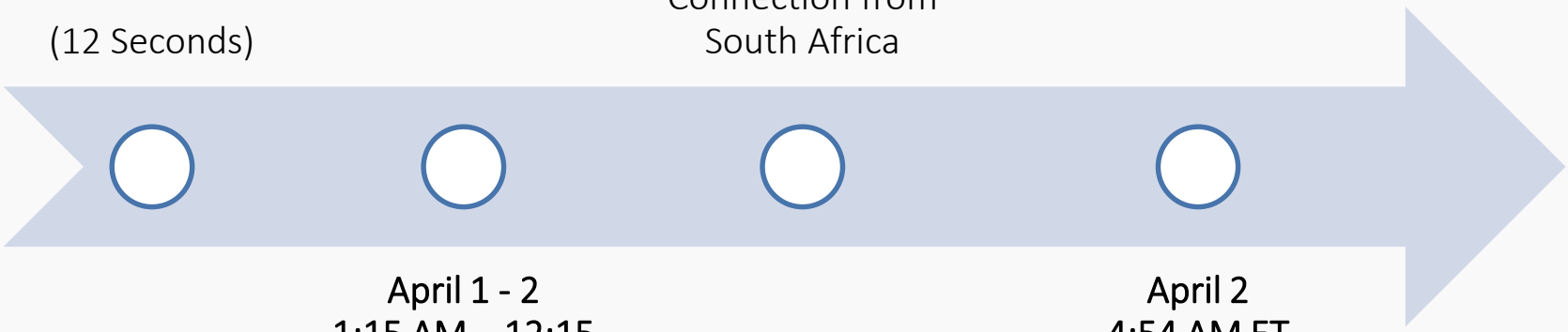
ABOUT ECMC

- 1000 beds
- Level-1 trauma center
- 30 outpatient services
- Member of Great Lakes Health consortium
- 300,000+ outpatient visits
- 12,000+ surgeries
- $600M revenue

GreyCastle security

	[redacted]	[redacted]
ATTACK SOPHISTICATION	LOW	HIGH
COMPROMISED ASSETS	700	6,000
DAYS OFFLINE	7	13
DAYS TO RECOVERY	10	45
RANSOM PAID	$17,000	$0

INSTANT REPLAY



April 1
12:10 AM ET

Remote Desktop Connection from Brazil

(12 Seconds)

April 1 - 2
1:15 AM – 12:15 AM

Multiple Additional Remote Desktop Connections

(11 Hours)

April 2
4:47 AM ET

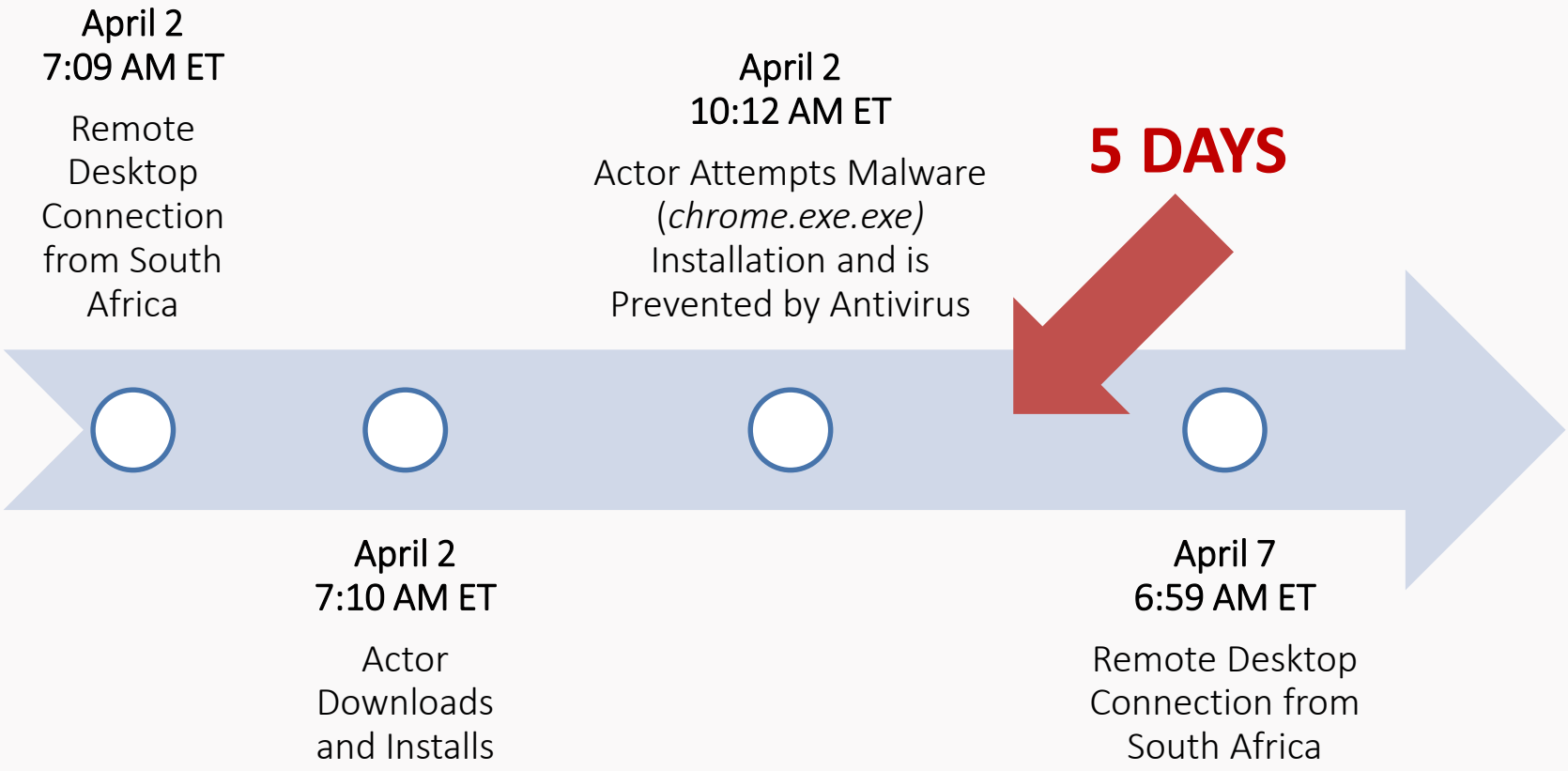
Remote Desktop Connection from South Africa

April 2
4:54 AM ET

Actor Queries *whoer.net* to Gather Public IP Address

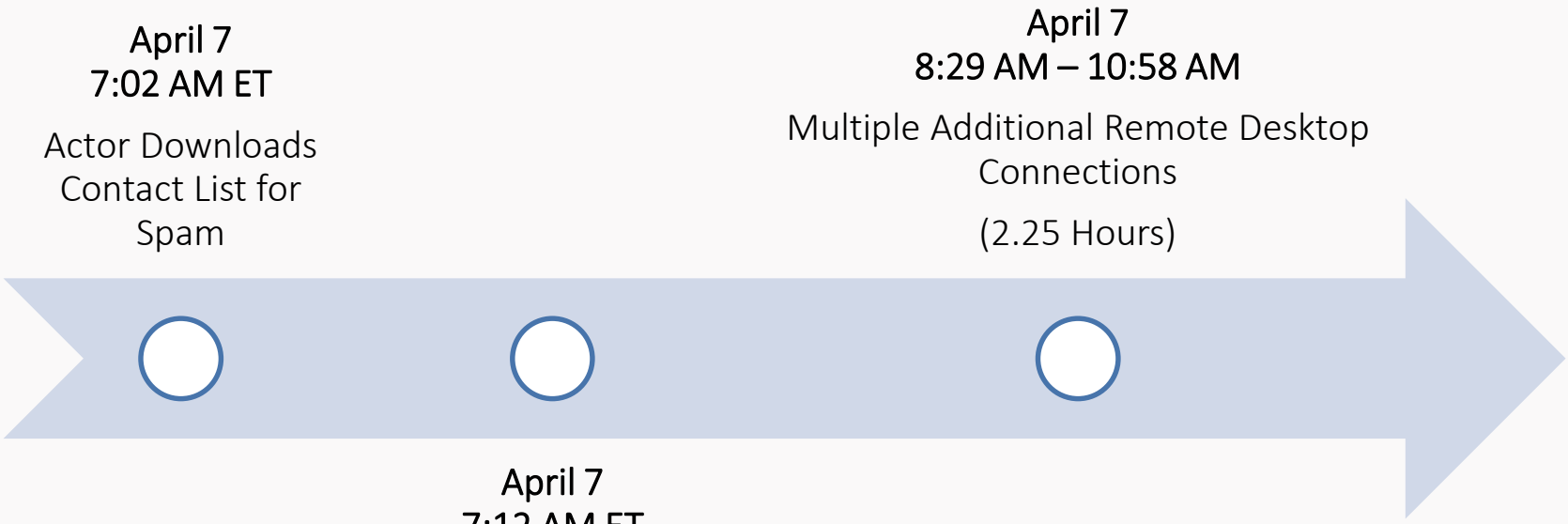
GreyCastle security

INSTANT REPLAY



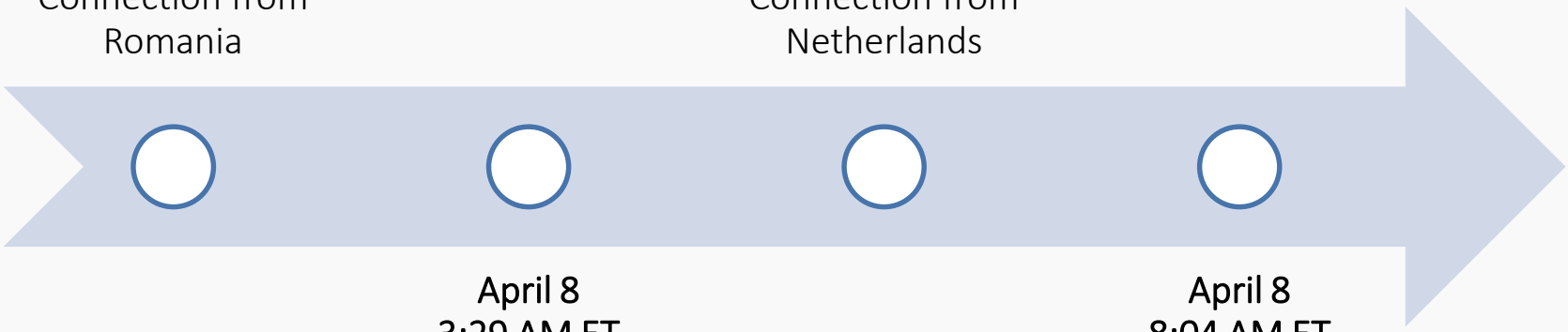
GreyCastle security

INSTANT REPLAY



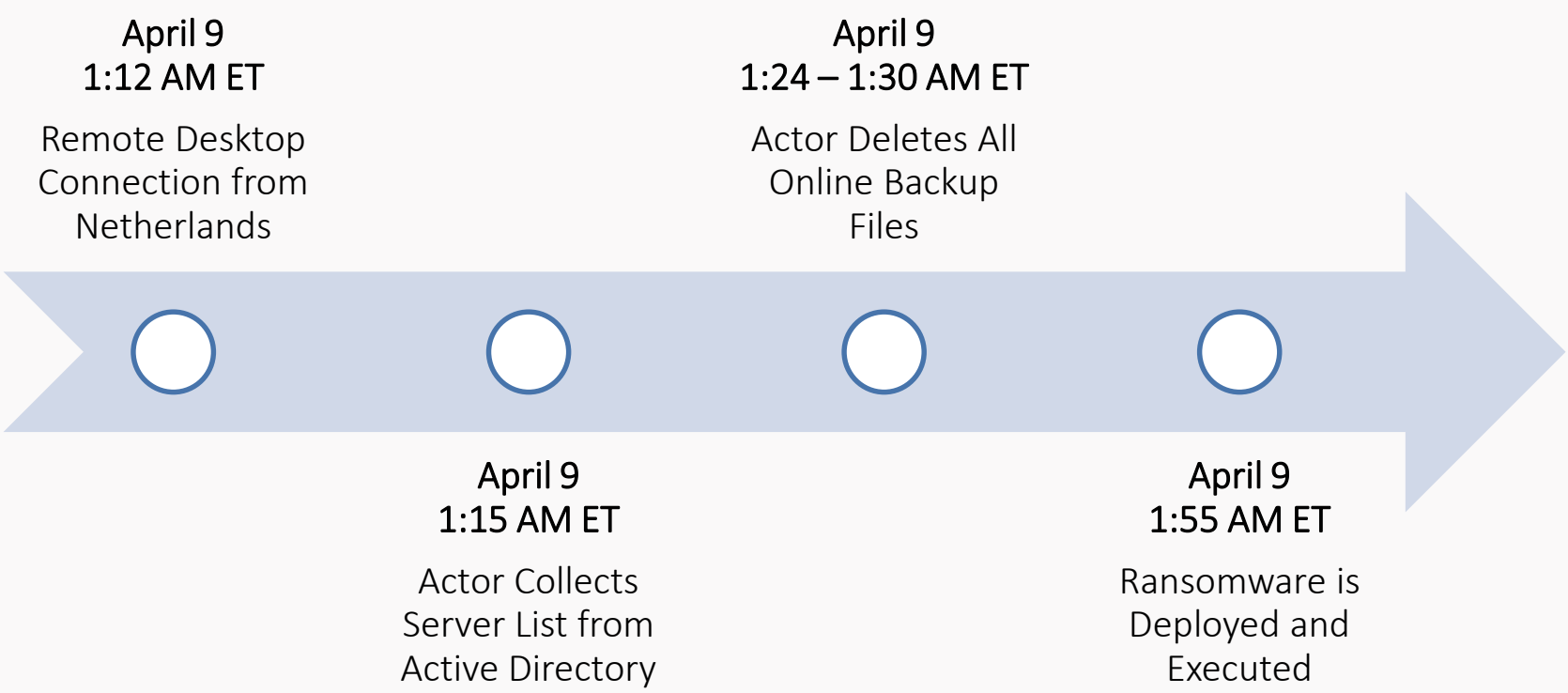
GreyCastle security

INSTANT REPLAY



GreyCastle security

INSTANT REPLAY



GreyCastle security

ATTRIBUTION

https://malwr.com/analysis/YmJlMDY5M2FjZTIhNDc5N2IzY2QxNGFmNmI0MzIxODc/

ATTRIBUTION

- SamSam ransomware variant
- 6,000+ compromised assets
- Default password was Patient0
- Attack did not start with a social engineering

GreyCastle security

SILVER LININGS

- Immediate incident detection and response
- Emergency Management Plan fluency due to recent drill
- Offline backup availability
- Negligible impact to patient care and safety
- Community and peer support
- Legal non-breach determination

INCIDENT RESPONSE FOR HEALTHCARE

CRASH COURSE

INCIDENT RESPONSE FOR HEALTHCARE

1. GO TO DEFCON 1 ASAP

- Formally activate your Incident Response Plan
- Let your ePHI inventory drive response
- Decide on your communications strategy
- Assume that response activities will be scrutinized after the incident

2. ASSEMBLE THE RIGHT TEAM

- Get leadership involved immediately
- Get communications, legal and clinical leaders in the room – IT is secondary
- Escalate to cybersecurity and investigation experts

INCIDENT RESPONSE FOR HEALTHCARE

3. INITIATE "LOCKDOWN"

- Change passwords on critical assets
- Power down or disconnect non-critical assets
- Disable outbound network traffic
- Disable off-hours access
- Disable Internet access
- Freeze bank accounts

4. UNDERSTAND IOCs

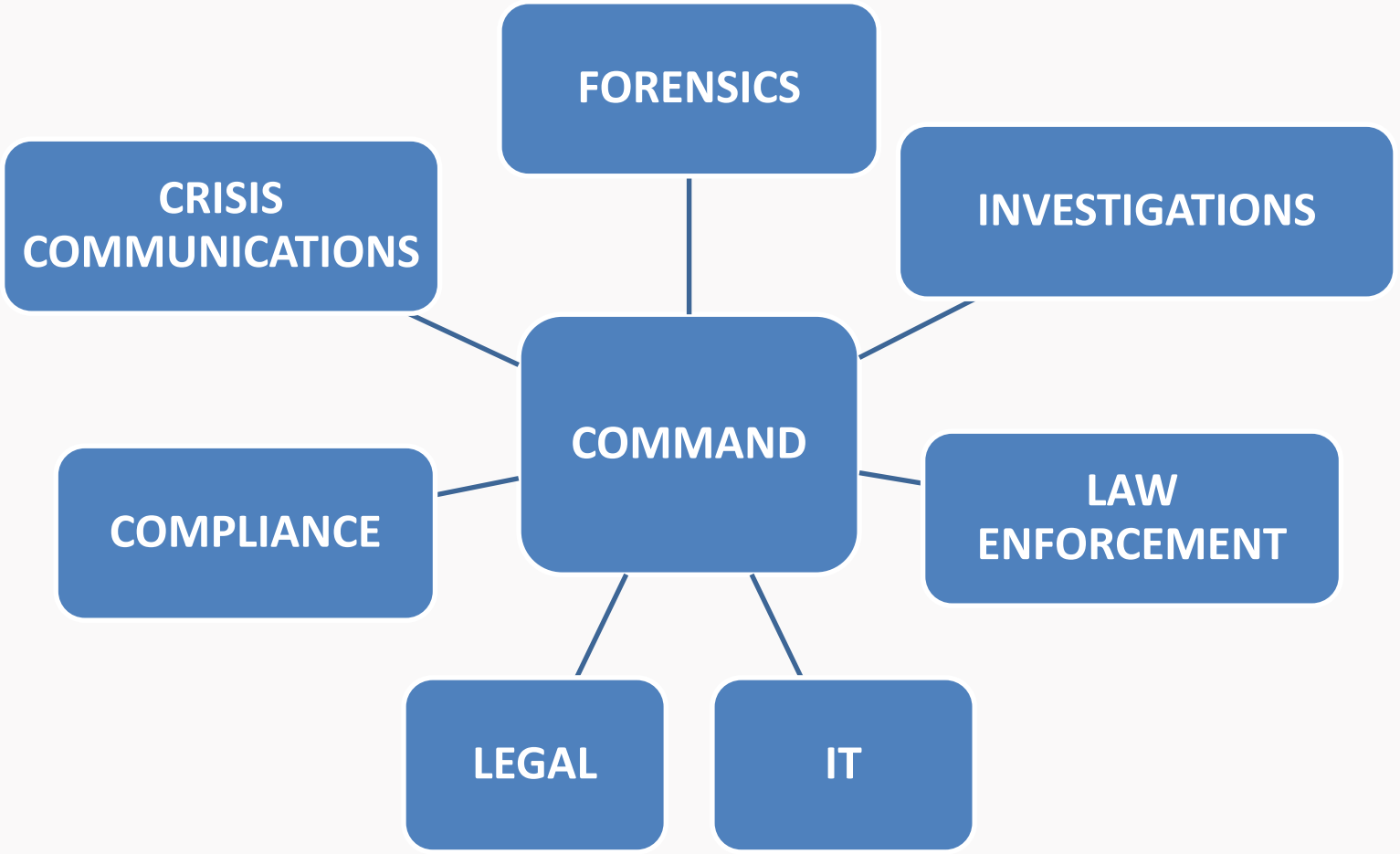
- Know what Indicators of Compromise (IOCs) are and where to look for them
- Focus on IOCs when ePHI assets show signs of compromise

INCIDENT RESPONSE FOR HEALTHCARE

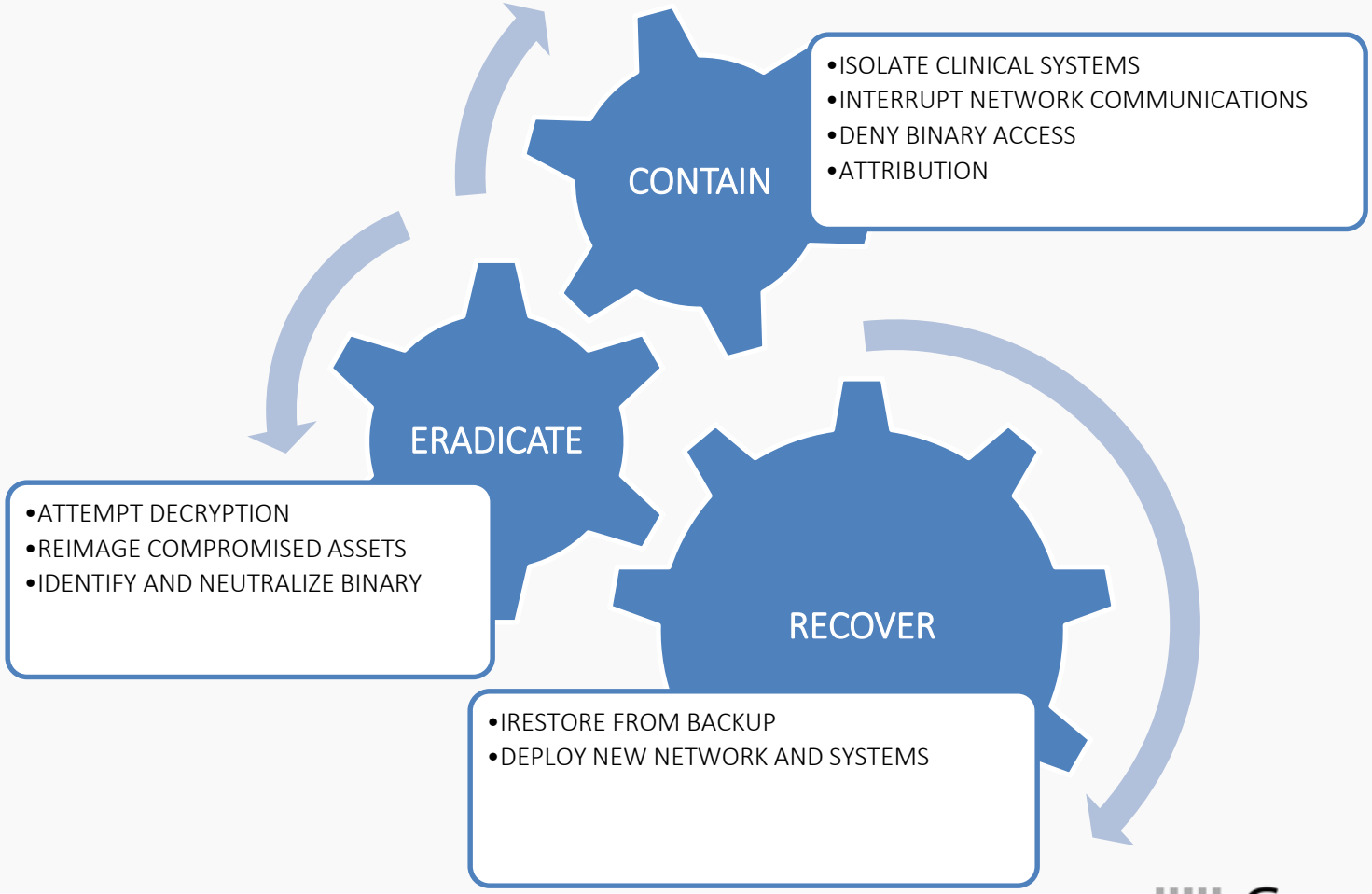
5. MINIMIZE EXPOSURE

- Engage a HIPAA-fluent attorney
- Collect and document all evidence that proves – or even merely suggests – integrity of ePHI

RESPONSE TEAM



RESPONSE PROCESS

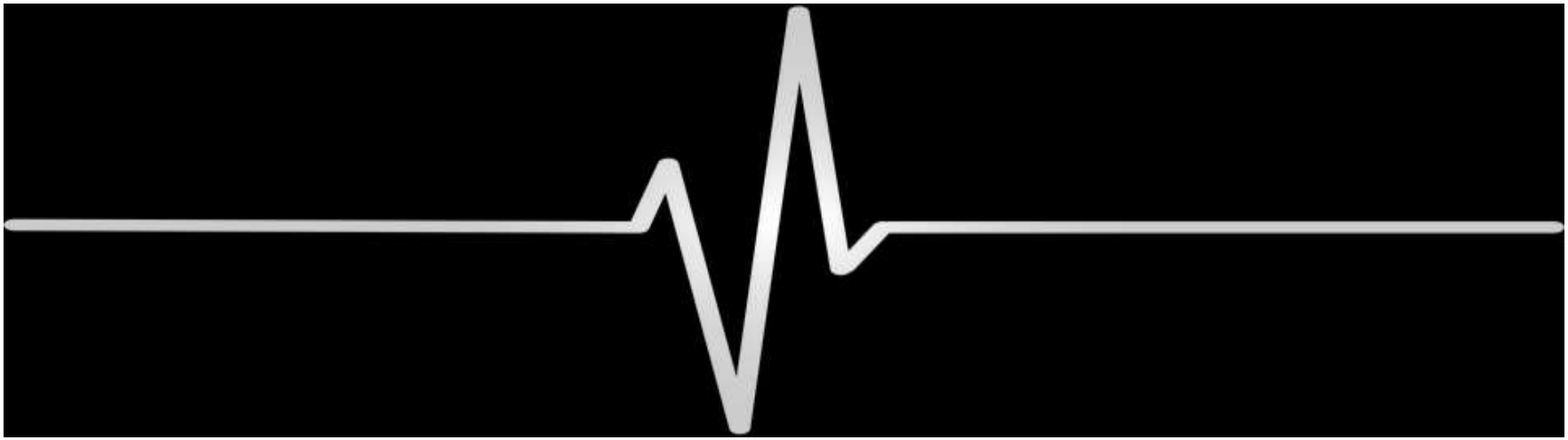


INCIDENT RESPONSE FOR HEALTHCARE

FINAL THOUGHTS

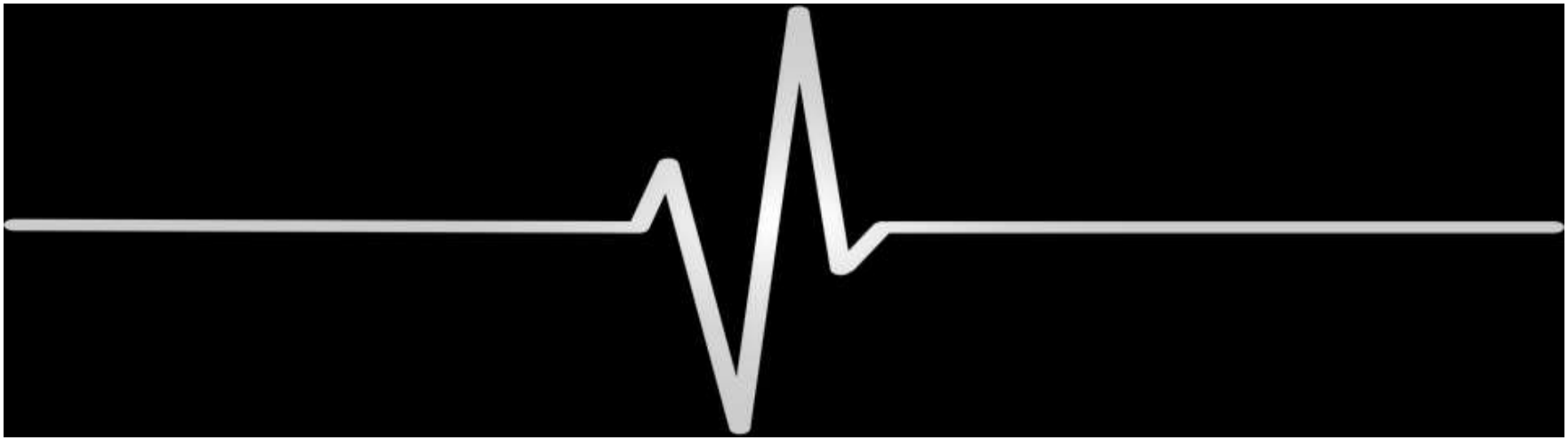
CREATE A

CULTURE OF SECURITY



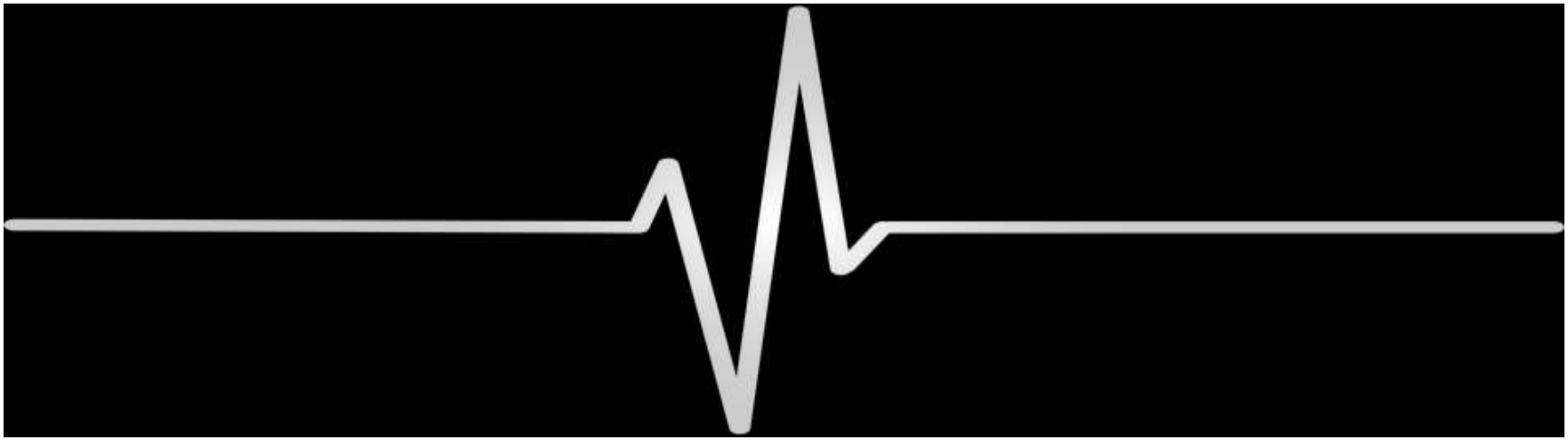
CONSIDER

PAYING THE RANSOM?



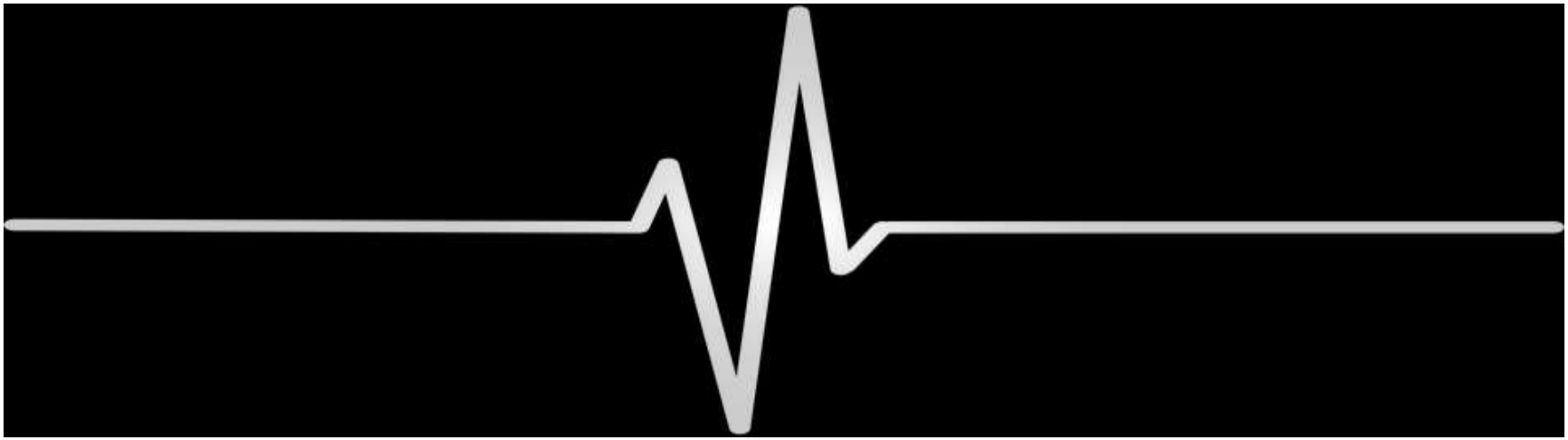
KNOW THE DIFFERENCE BETWEEN

EXPOSURE AND BREACH



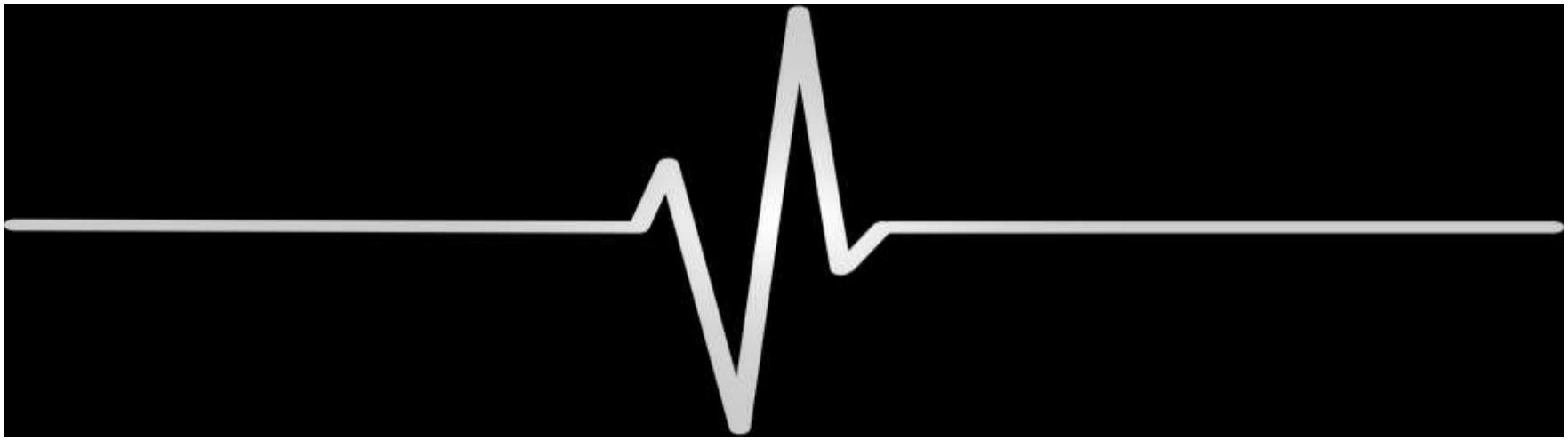
FOCUS RECOVERY EFFORTS ON

PATIENT CARE AND SAFETY



FOR THE LOVE OF ALL THINGS GOOD DO

"THE BIG THREE"




ANY
QUESTIONS
?

@REGHARNISH