GLOBAL INFORMATION SECURITY

ZURICH

Leveraging Your Security Operations Center

Nov 28, 2018

Matilda McVann
Global Head of Cyber Incident Response

Cyber Fusion Center and Security Operations

Who I am:

Cyber Fusion Center and Security Operations

Who we are:

Cyber Response

Reactive

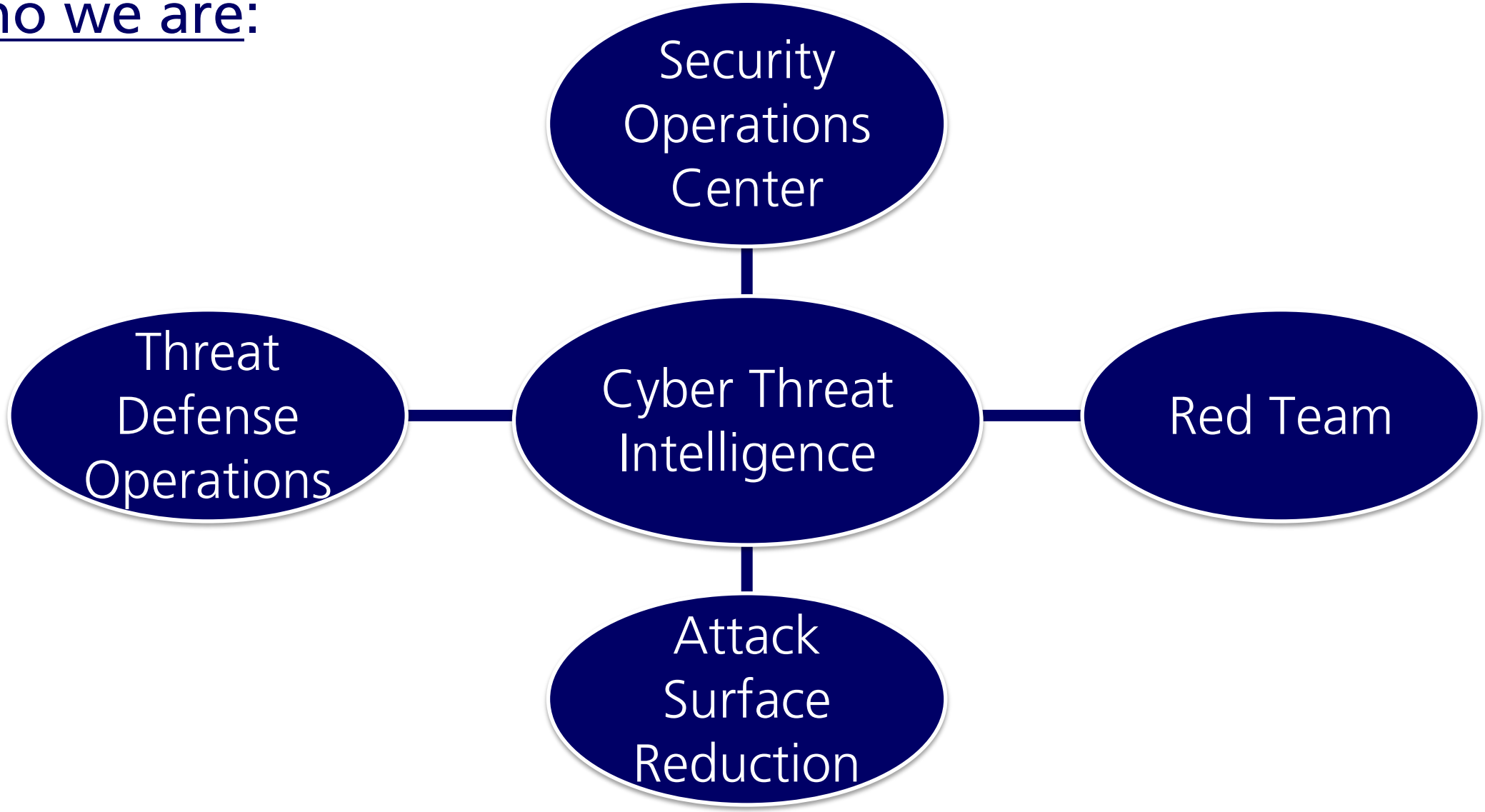
As the front line of the CFC, their skilled Incident Response team specialists are the first responders when any information security incident occurs.

Proactive

Operating under an 'assumed threat' model, the Cyber Response Hunt Team shifts to proactive mode and seeks out threats on the network that may have avoided other defensive measures.

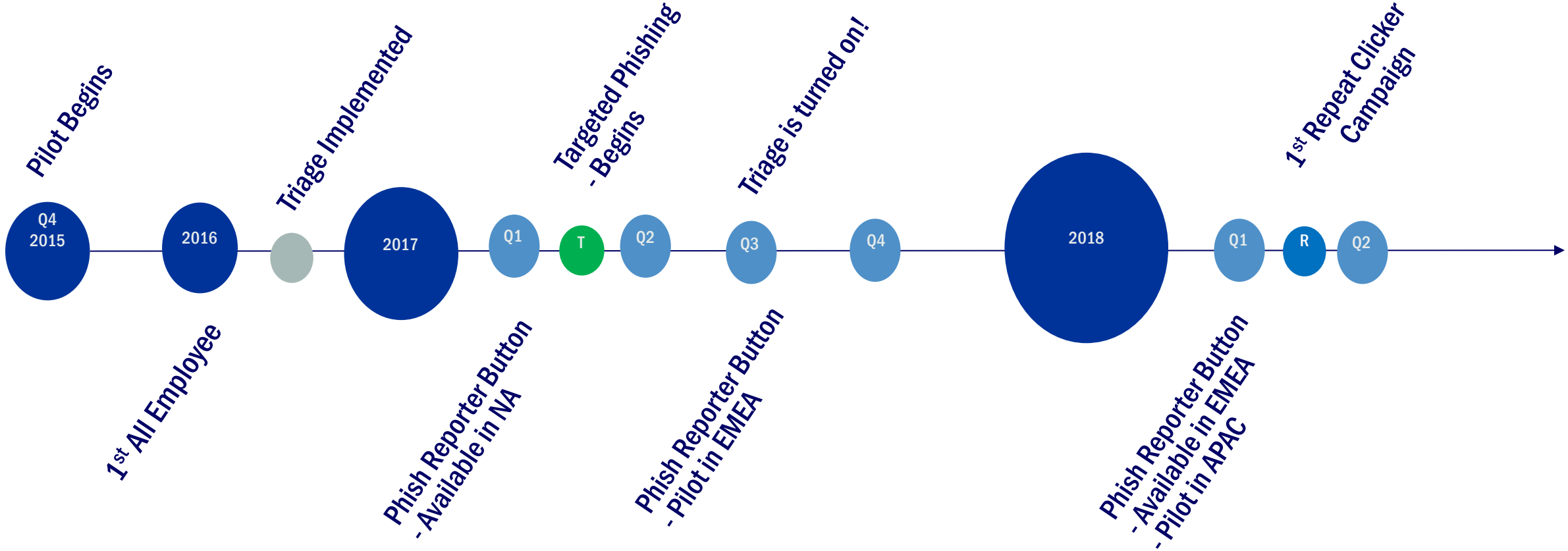
Cyber Fusion Center and Security Operations

Who we are:



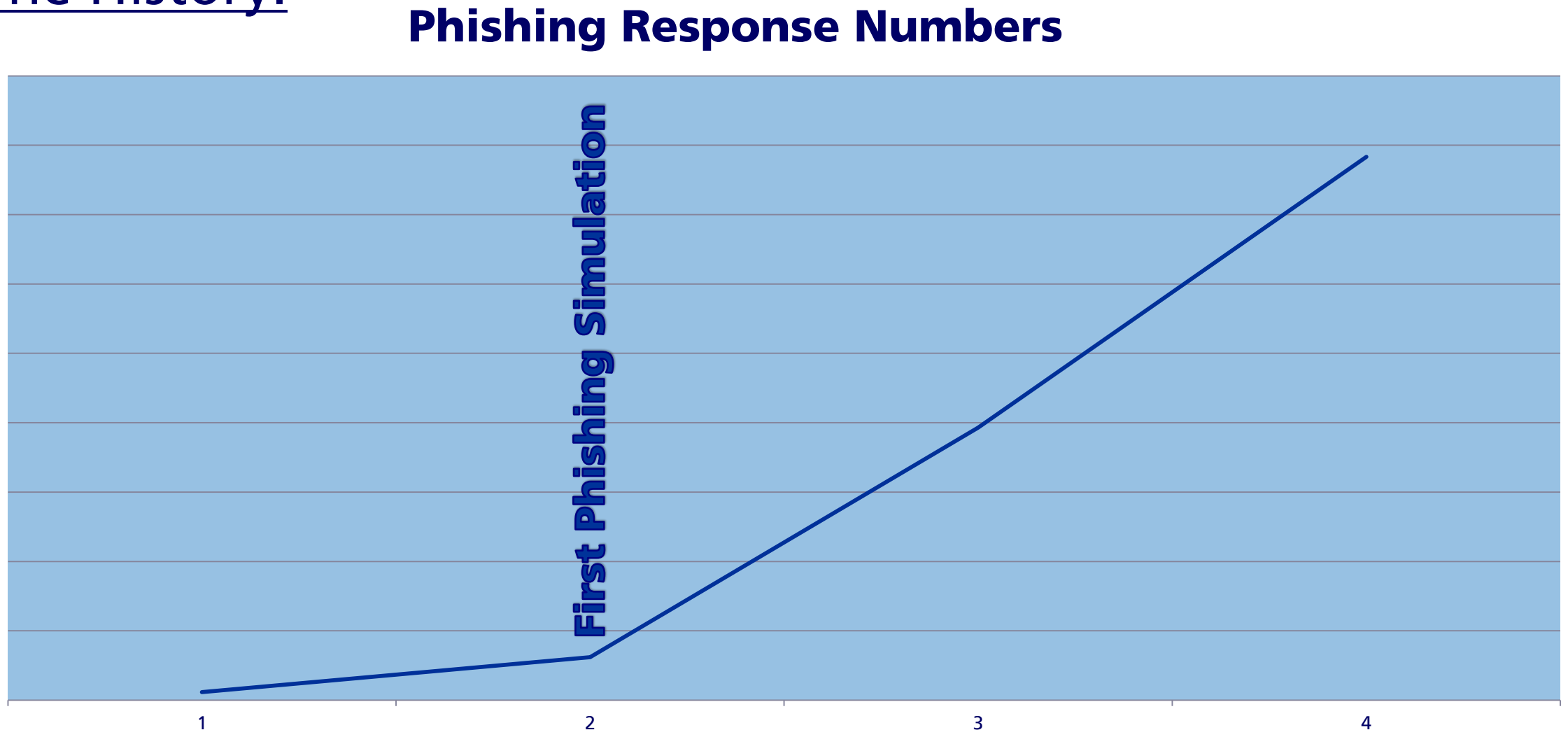
Cyber Fusion Center and Security Awareness

The History:



Cyber Fusion Center and Security Awareness

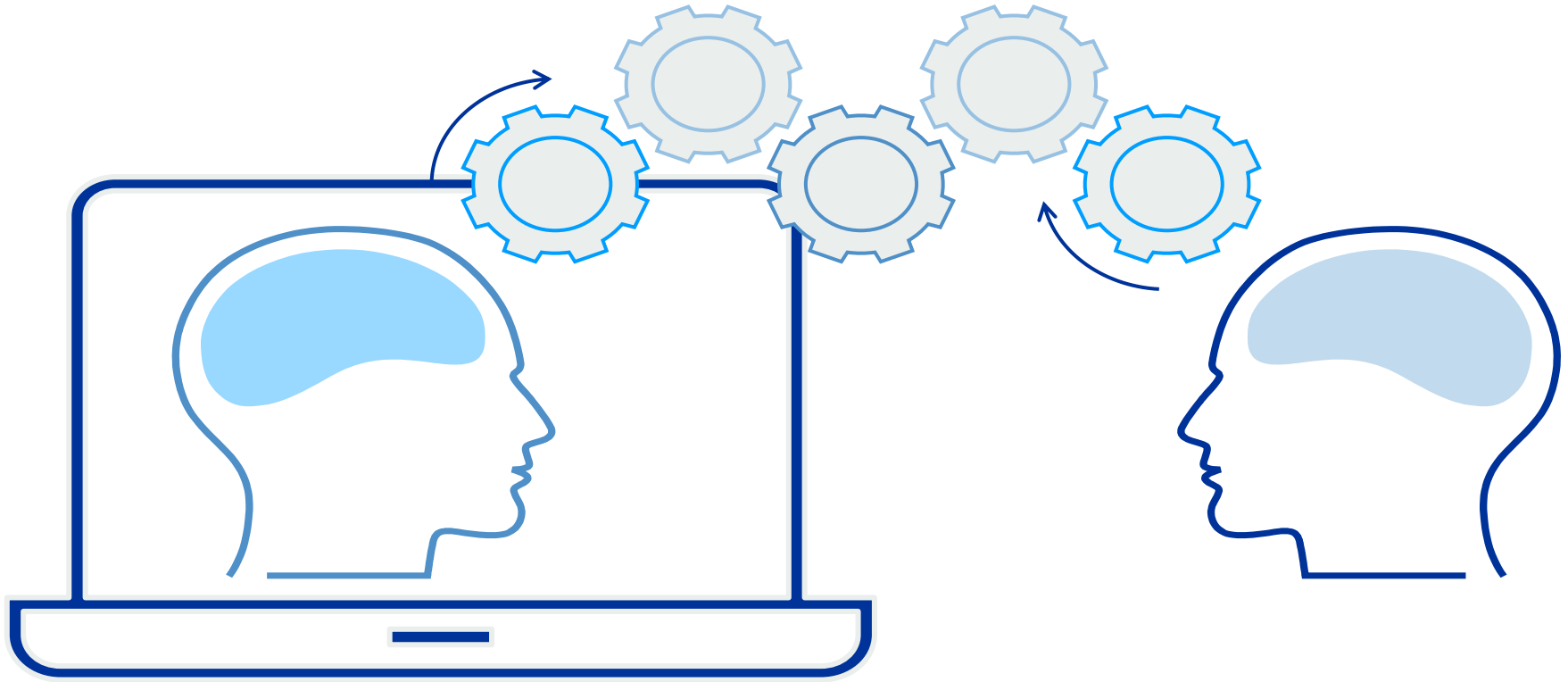
The History:



Cyber Fusion Center and Security Awareness

The Problem:

Convincing leadership that the Cyber/Security Awareness relationship is important to a successful program!



Cyber Fusion Center and Security Awareness

What we learned:

1. Leverage the relationships the SOC has already built.

2. Collaborate on improvements.

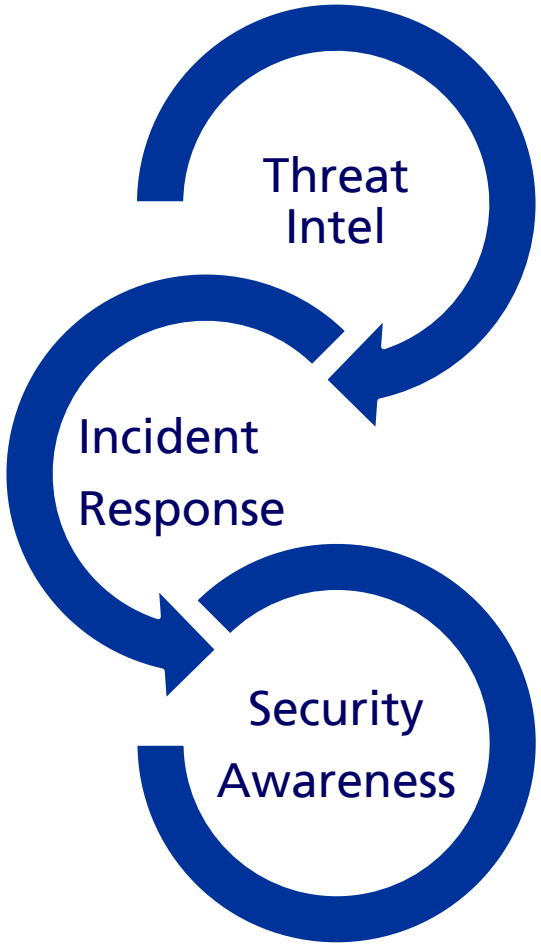
3. Security Awareness is not just employee phishing simulations and tip-sheets.

Cyber Fusion Center and Security Awareness

Leverage SOC relationships:

Cyber Fusion Center and Security Awareness

Collaborate on improvements:



Cyber Fusion Center and Security Awareness

What else:

Cyber Fusion Center and Security Awareness

ZURICH

Action Items:

1. Reach out to your IR or SOC leads, build that relationship.

2. Understand pain points for the SOC/IR. You may be surprised to learn resolving issues could be beneficial for you too.

3. Identify other SMEs who can provide value to your team, leverage the SOC/IR to initiate introduction.

4. Understand what SOC/IR processes, playbooks or KBs align with your training.

Leveraging Your Security Operations Center

ZURICH

Questions?