Left of Boom
-Hold on to your butts

Robert Garbee, CISSP, CEH
Founder: *Roanoke Information Security Exchange*
Network Security Engineer: *Carilion Clinic*

Disclaimer

The views and opinions expressed in this presentation are those of the individual and do not represent official policy, position or views of Carilion Clinic or it's affiliates.

This presentation is largely based off of the following article from Tim MalcomVetter. Please take a look at his original article for more info.

https://malcomvetter.medium.com/left-and-right-of-boom-ef230ed3eae3

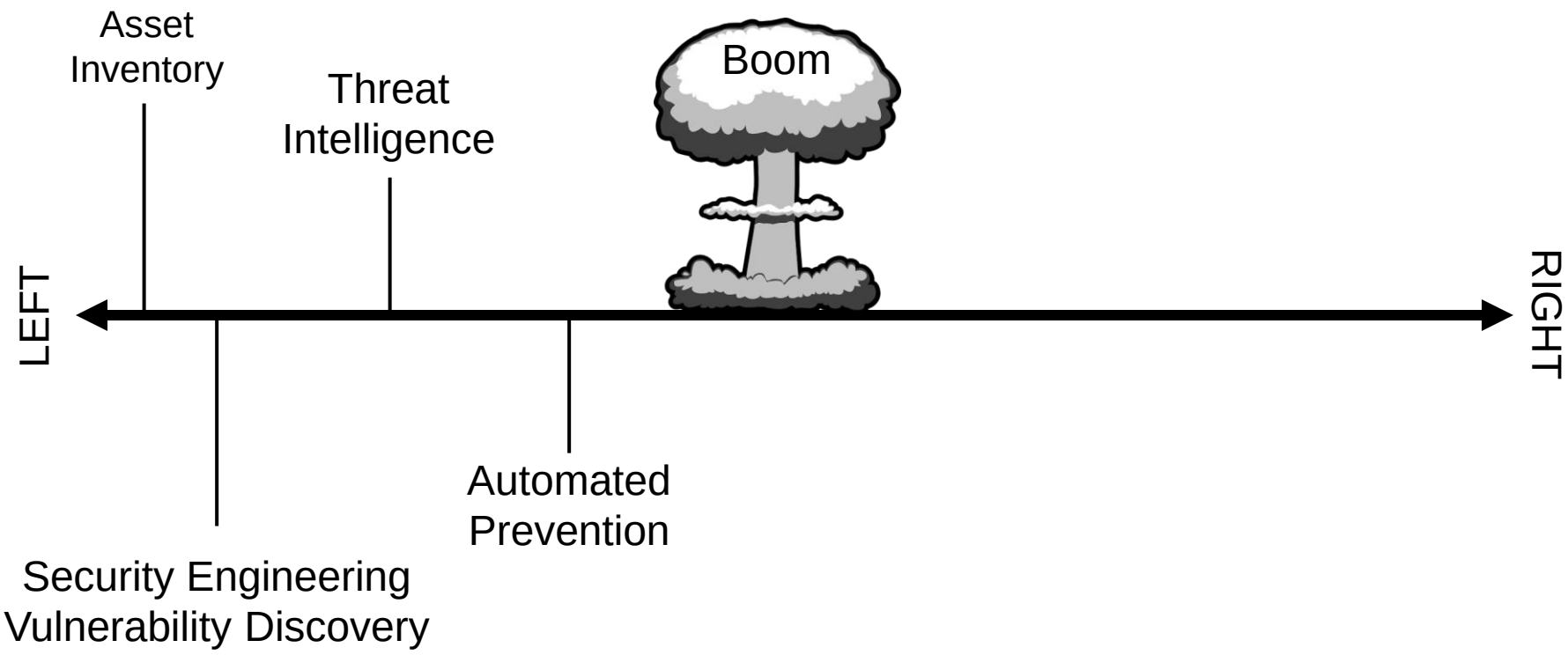
The Story

We need you here right now! Something has happened and we can’t get to anything!

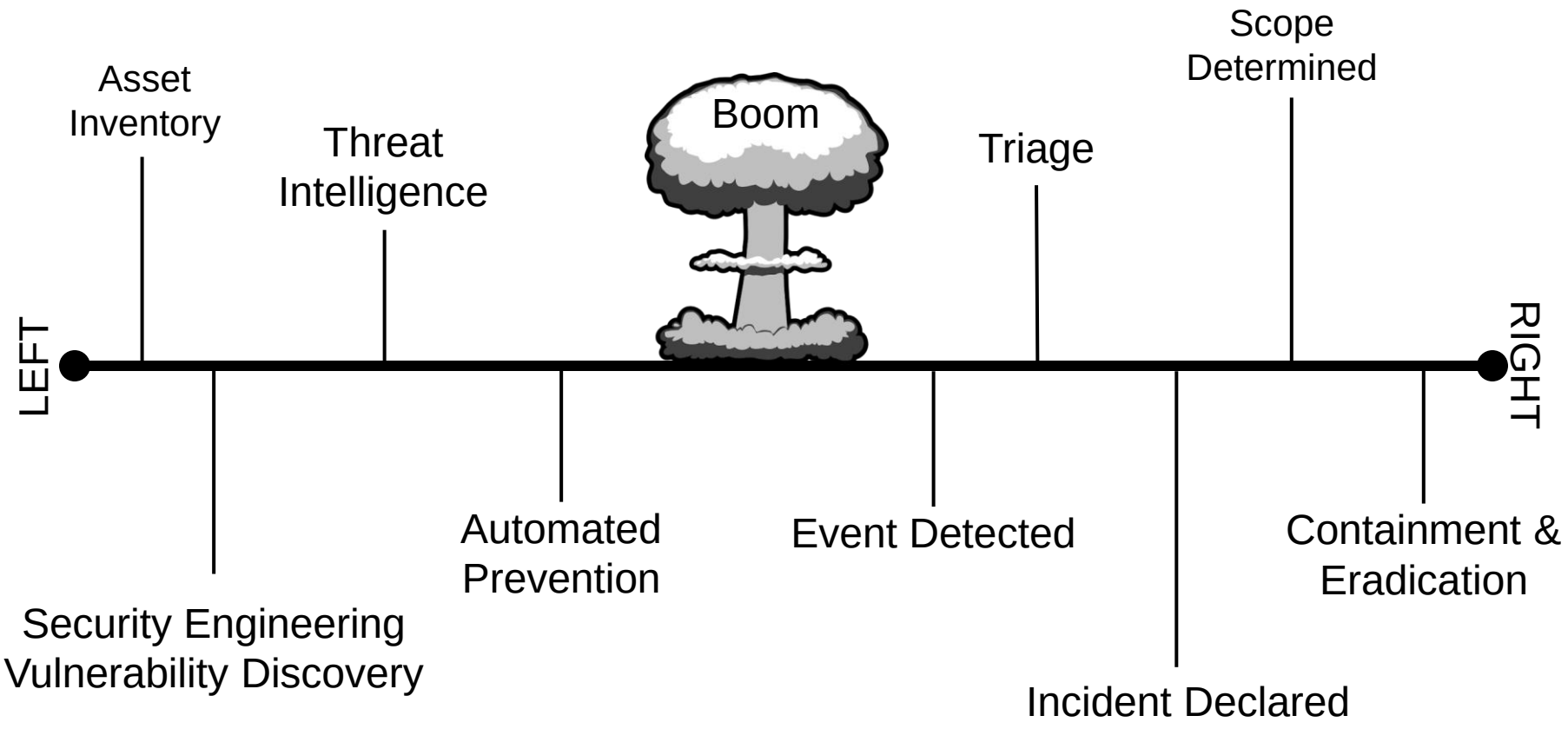
Welcome to the Boom

At its core, “boom” is an unwanted, bad event for the defender — the initial contact from the offender.

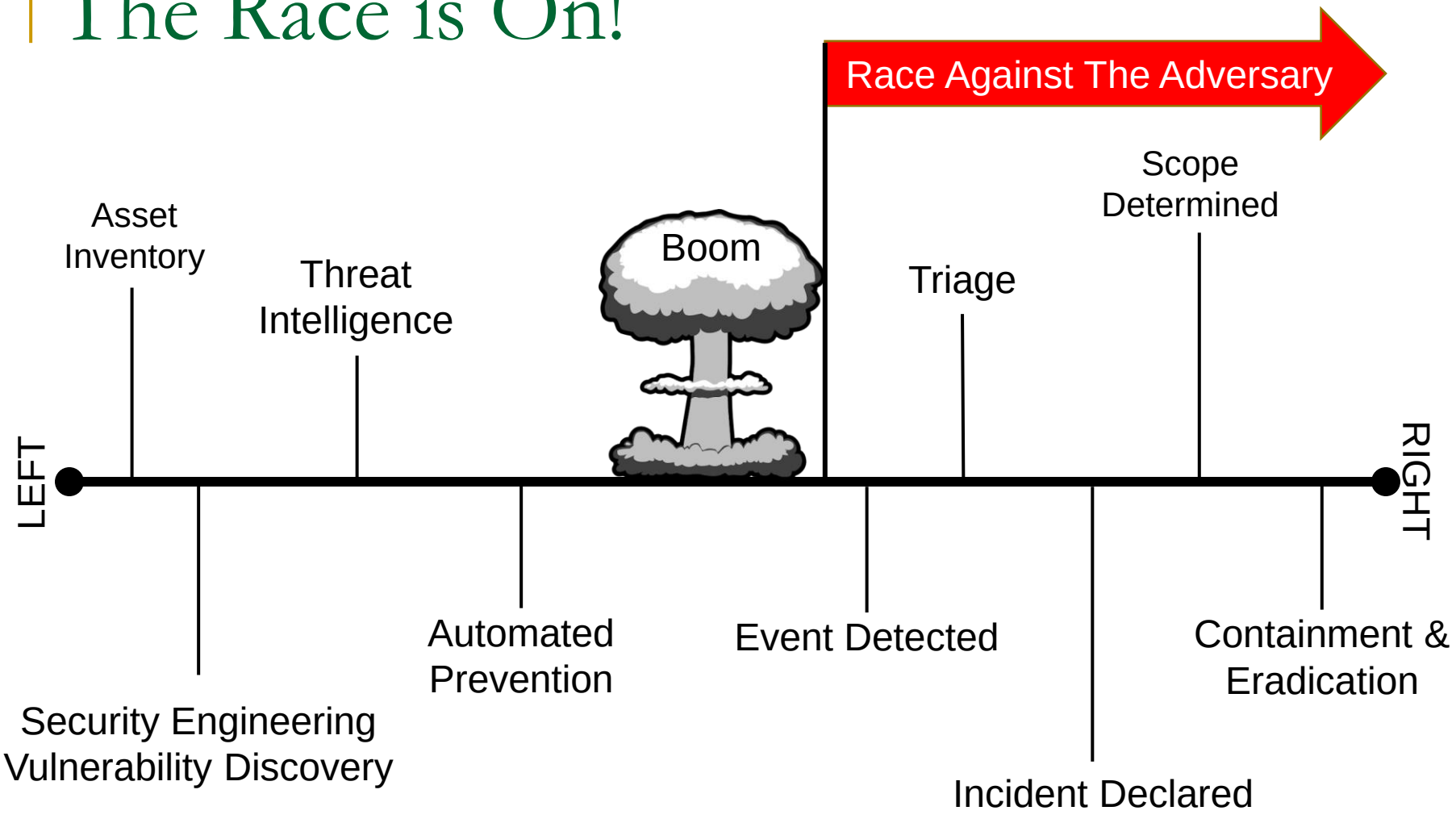
Left of Boom


Asset
Inventory
Threat
Intelligence
Boom
LEFT
RIGHT
Automated
Prevention
Security Engineering
Vulnerability Discovery

Right of Boom



The Race is On!



The Race is On!

- Adversary lives Right of Bang
- Once discovered the race is on
- Decisions based on recon
  - Attack based on your ability to respond
  - Example
    - Ransomware vs AD manipulation
    - Exfil vs Destruction

So what's the "So What"?

Embrace	Embrace the Suck
Prepare	Prepare for Right of Boom
Live	Live Right of Boom for awhile

Questions

- regarbee@Carilionclinic.org
- Info@roanokeinfosec.com