

Network Defender First Principles



Rick Howard - CSO



Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

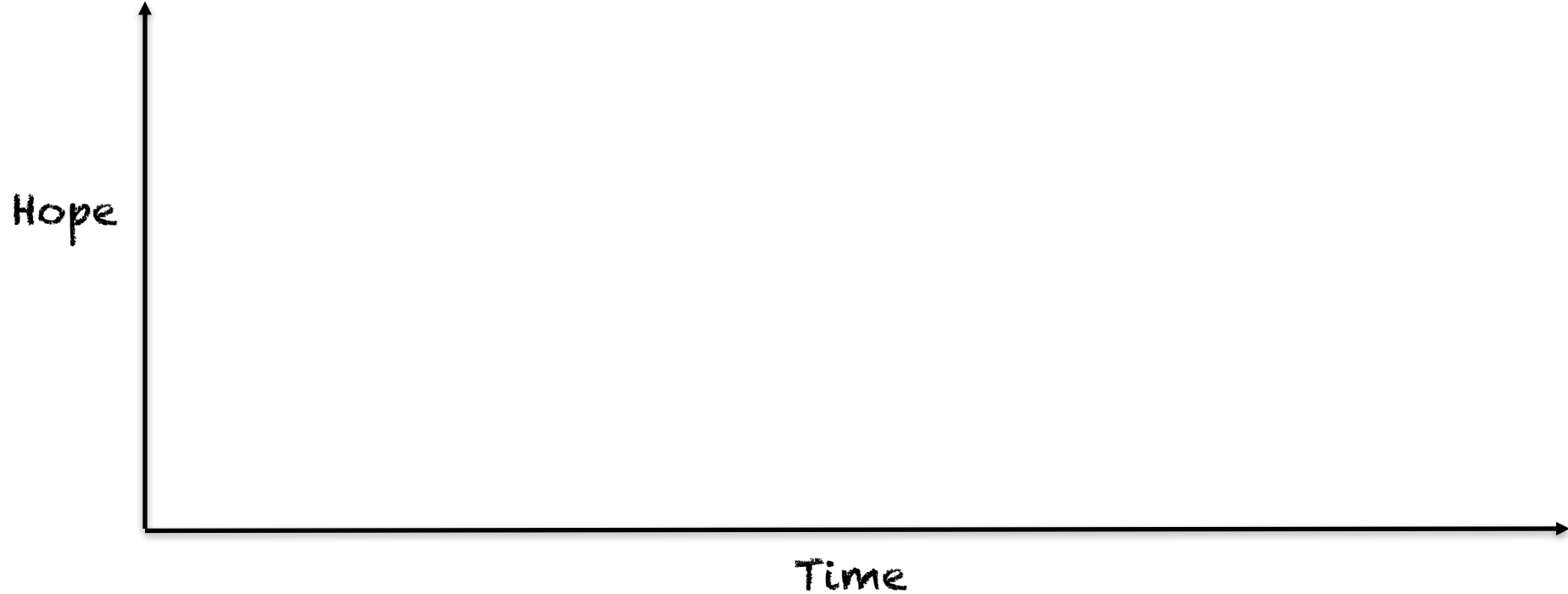
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

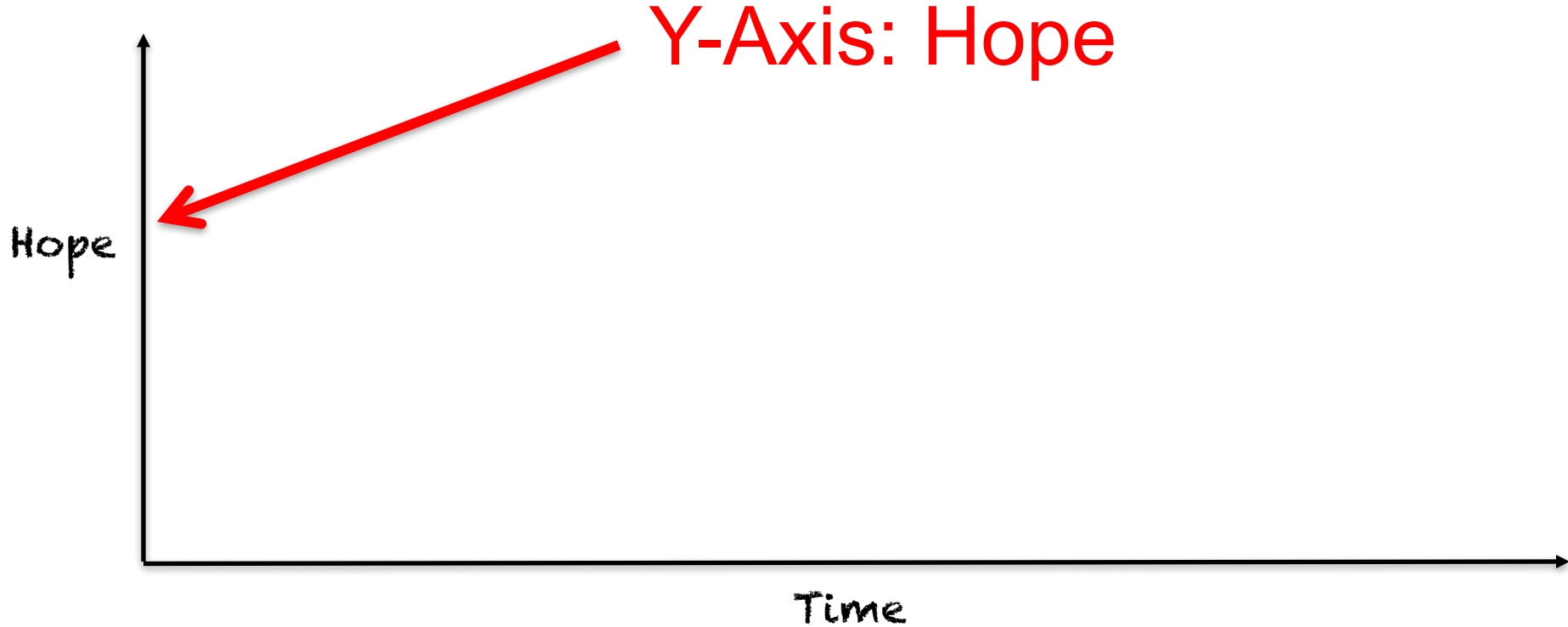
Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



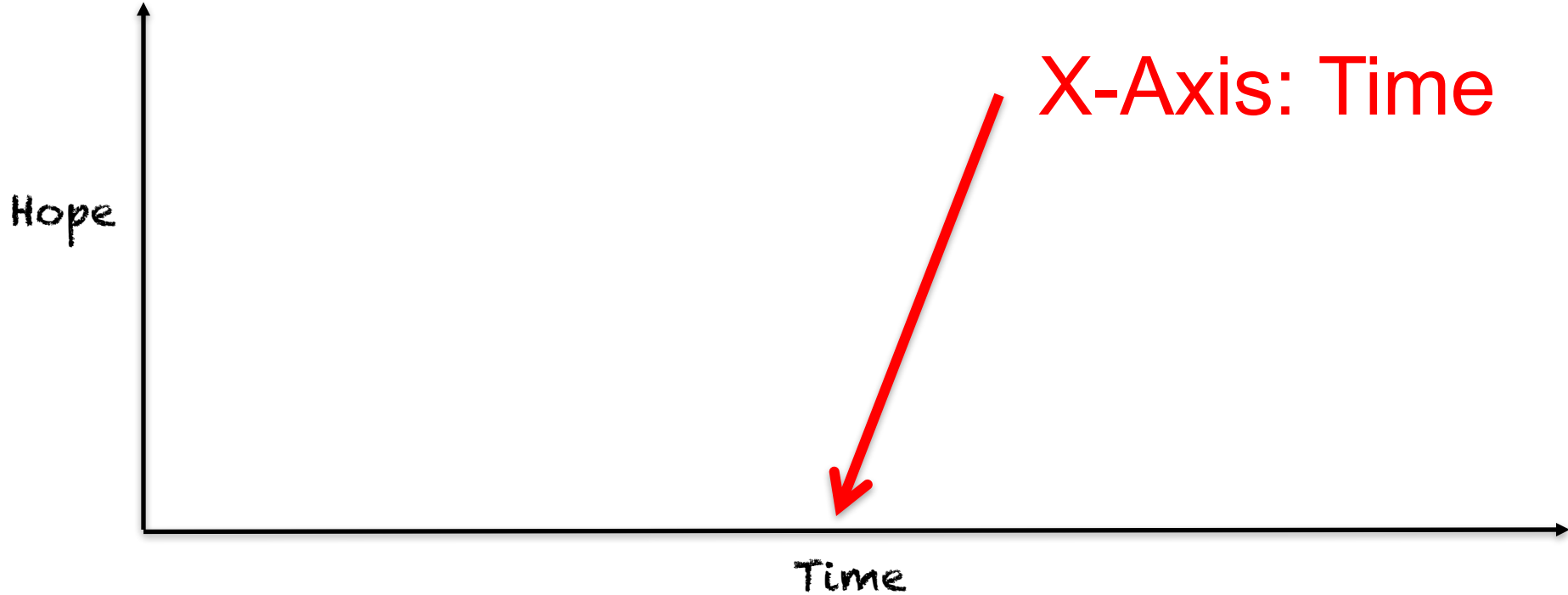
Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



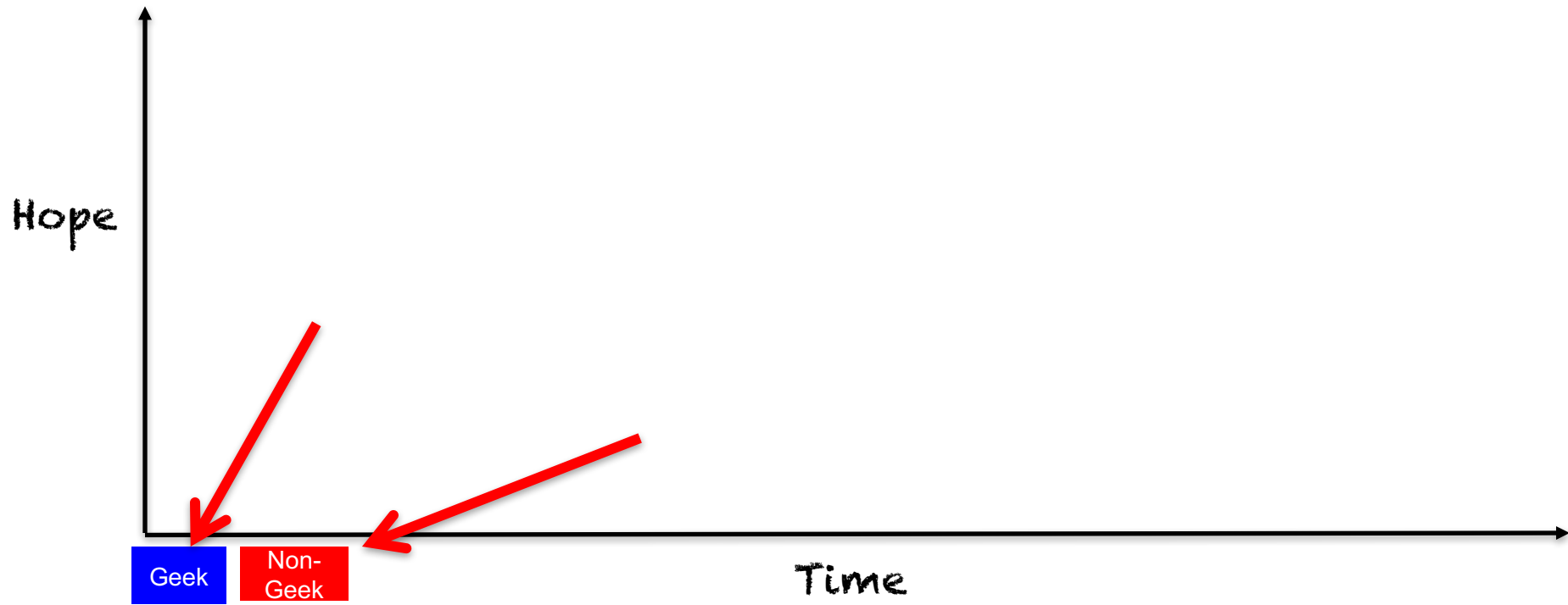
Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

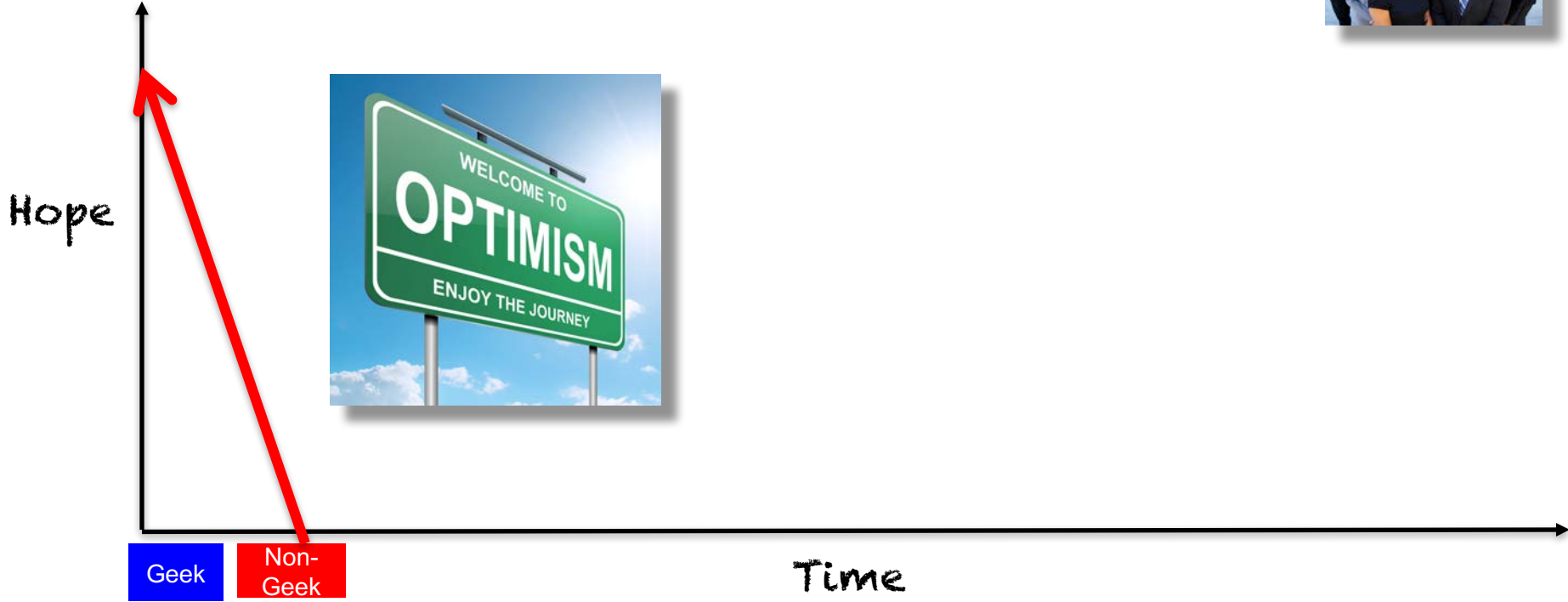


Non-Geeks – The Beautiful People

Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

Non-Geeks – The Beautiful People



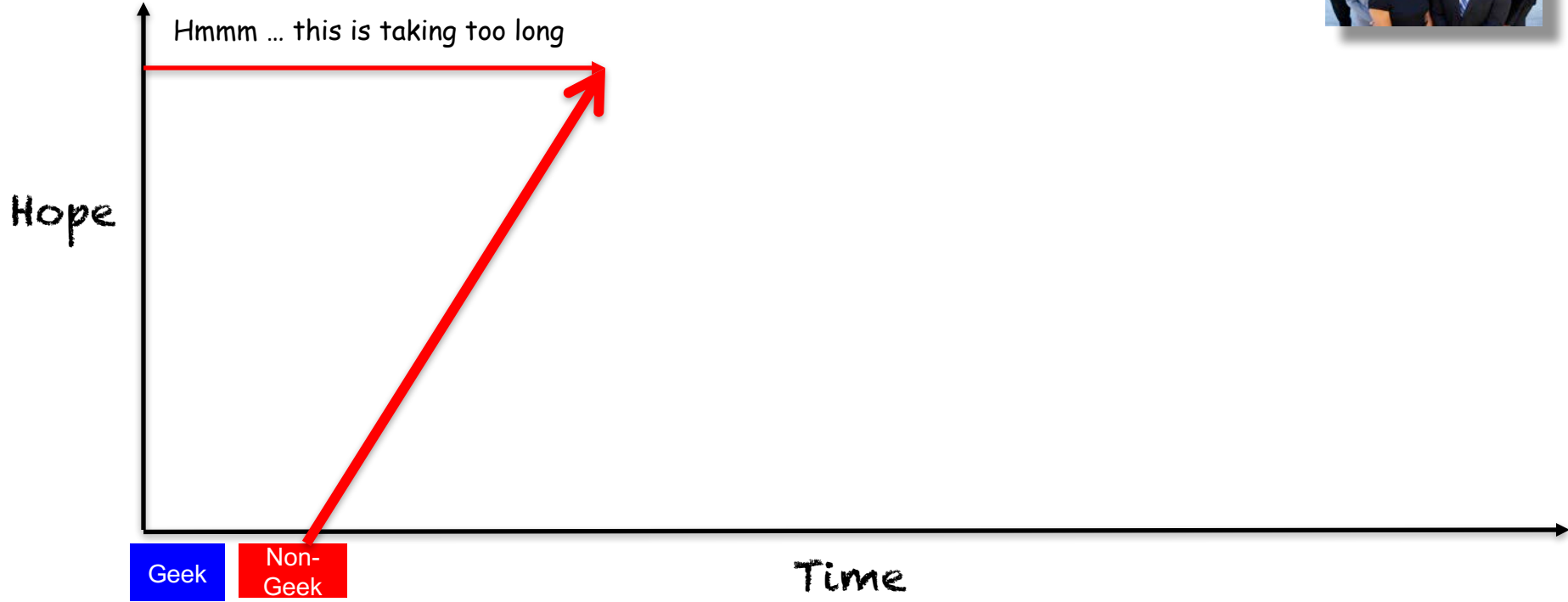
Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

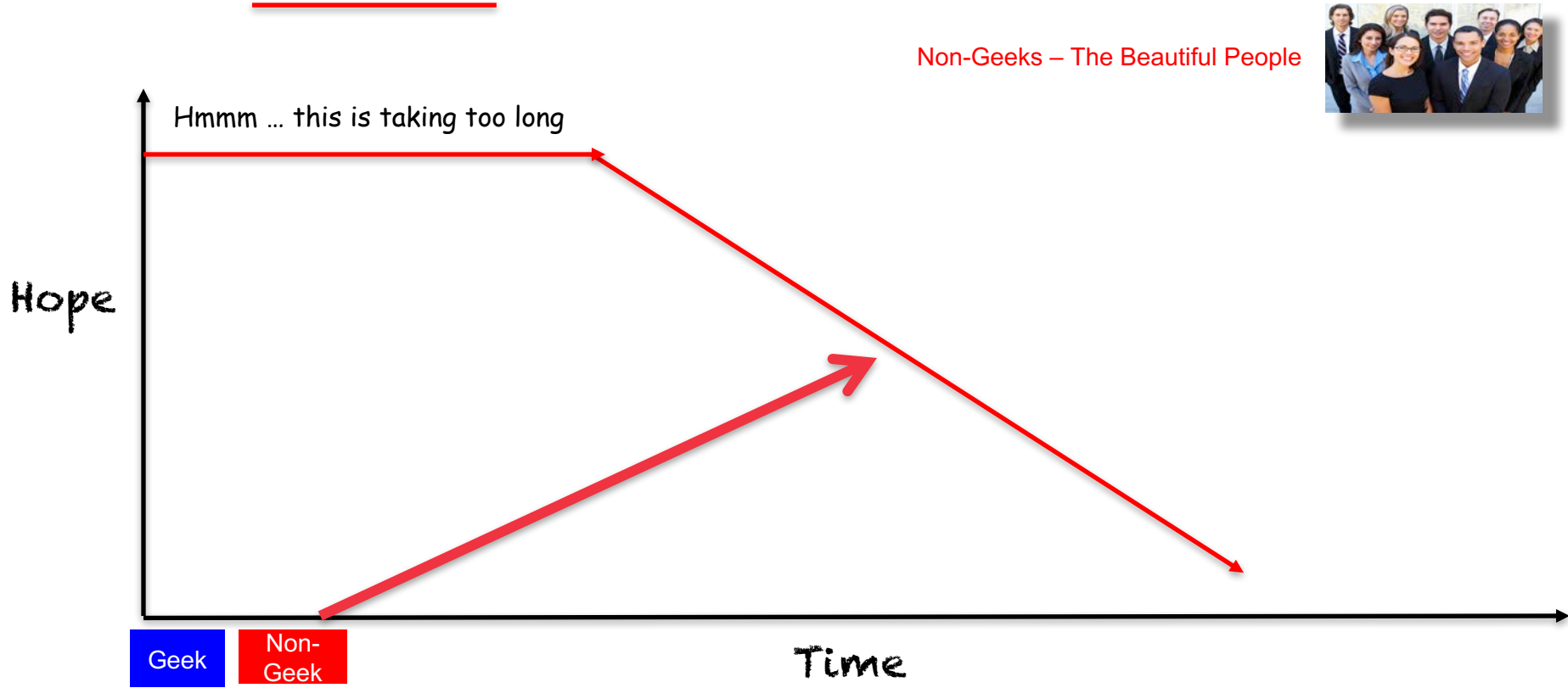


Non-Geeks – The Beautiful People



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

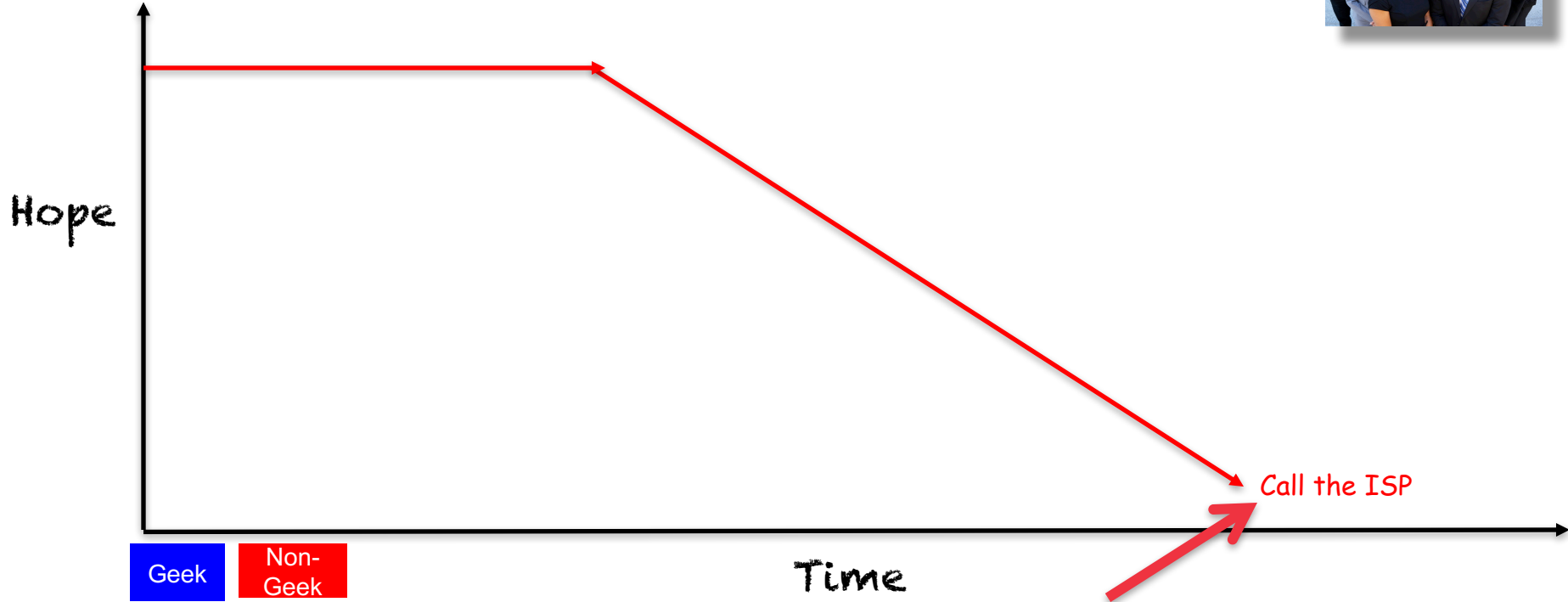


Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Non-Geeks – The Beautiful People

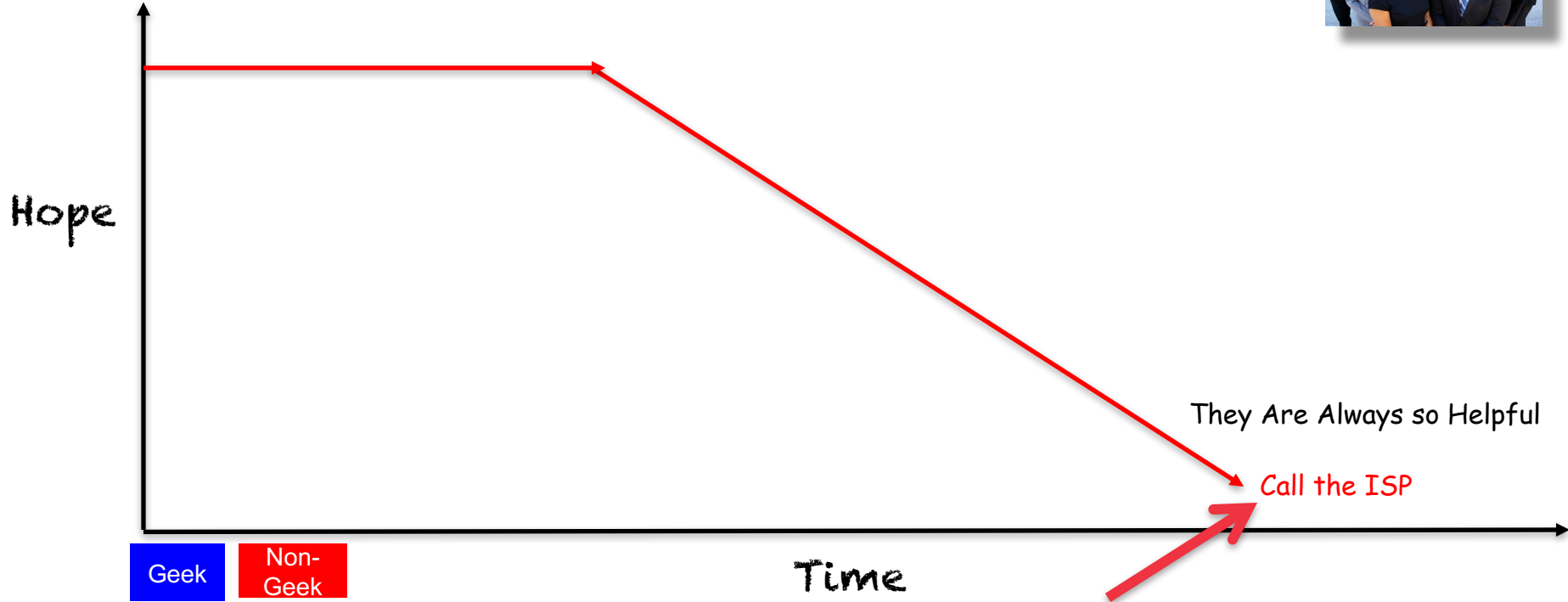


Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

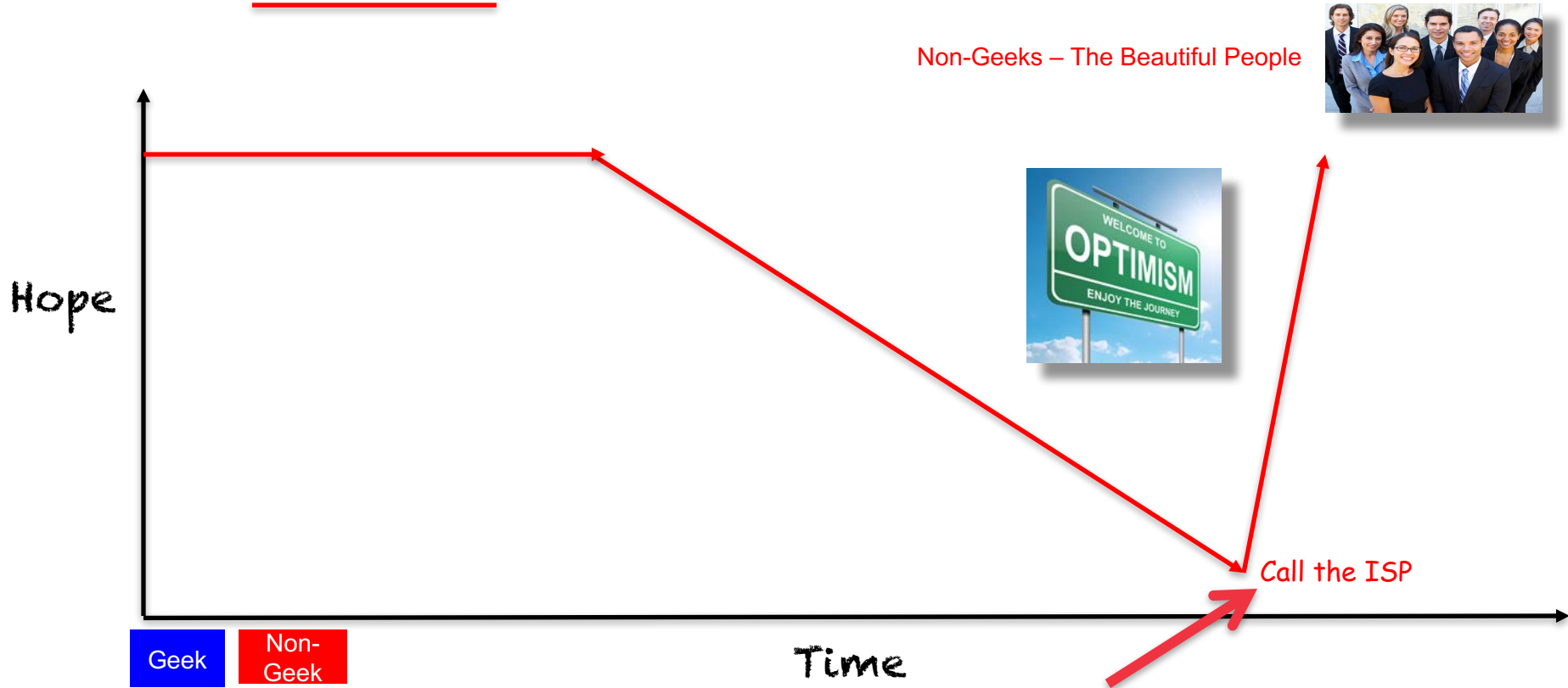


Non-Geeks – The Beautiful People



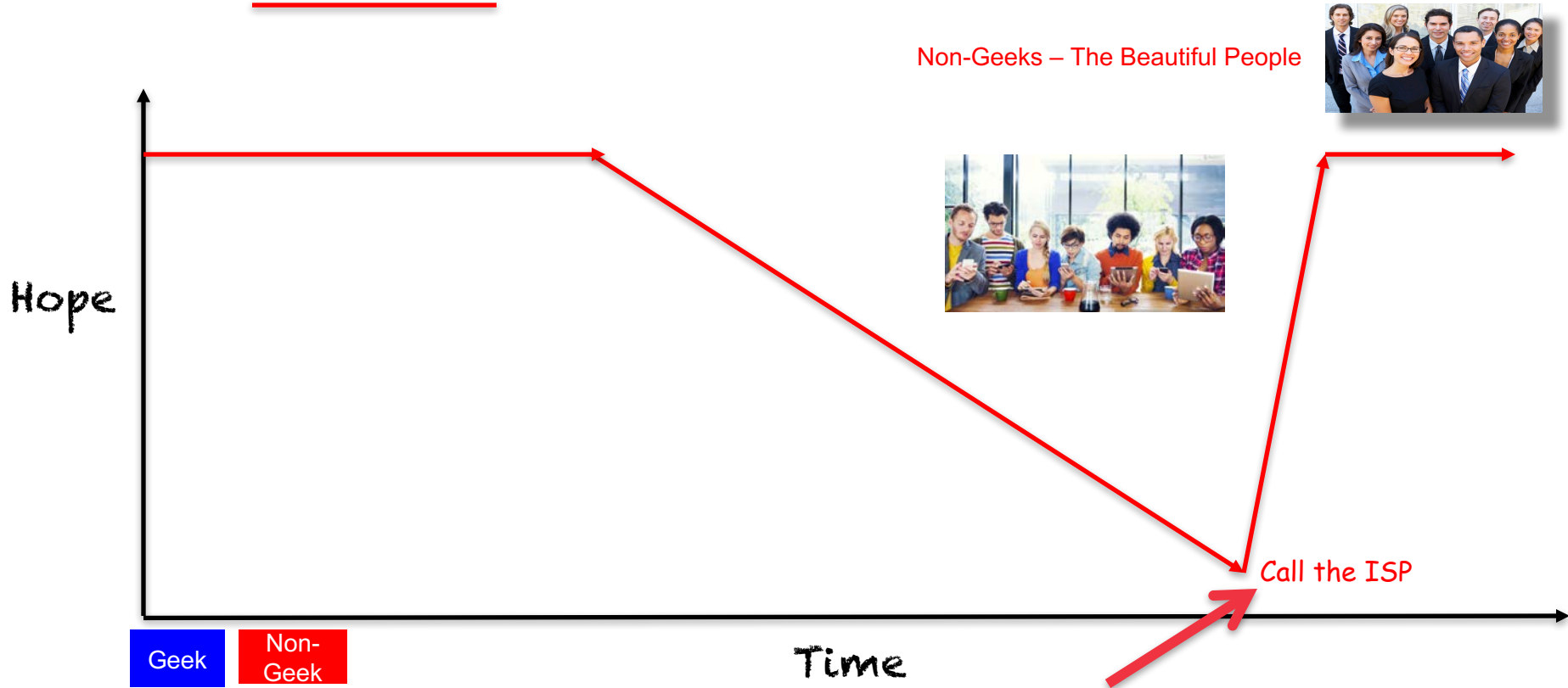
Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

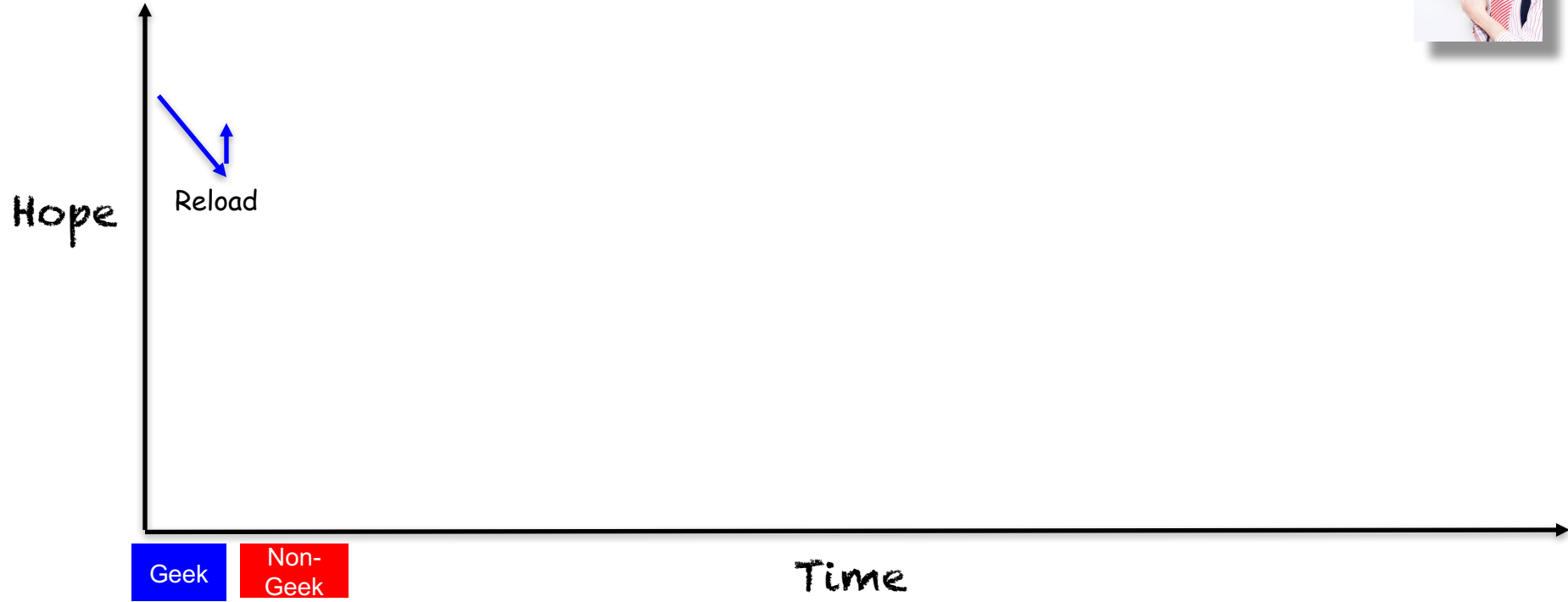


Geeks – My Peeps

Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

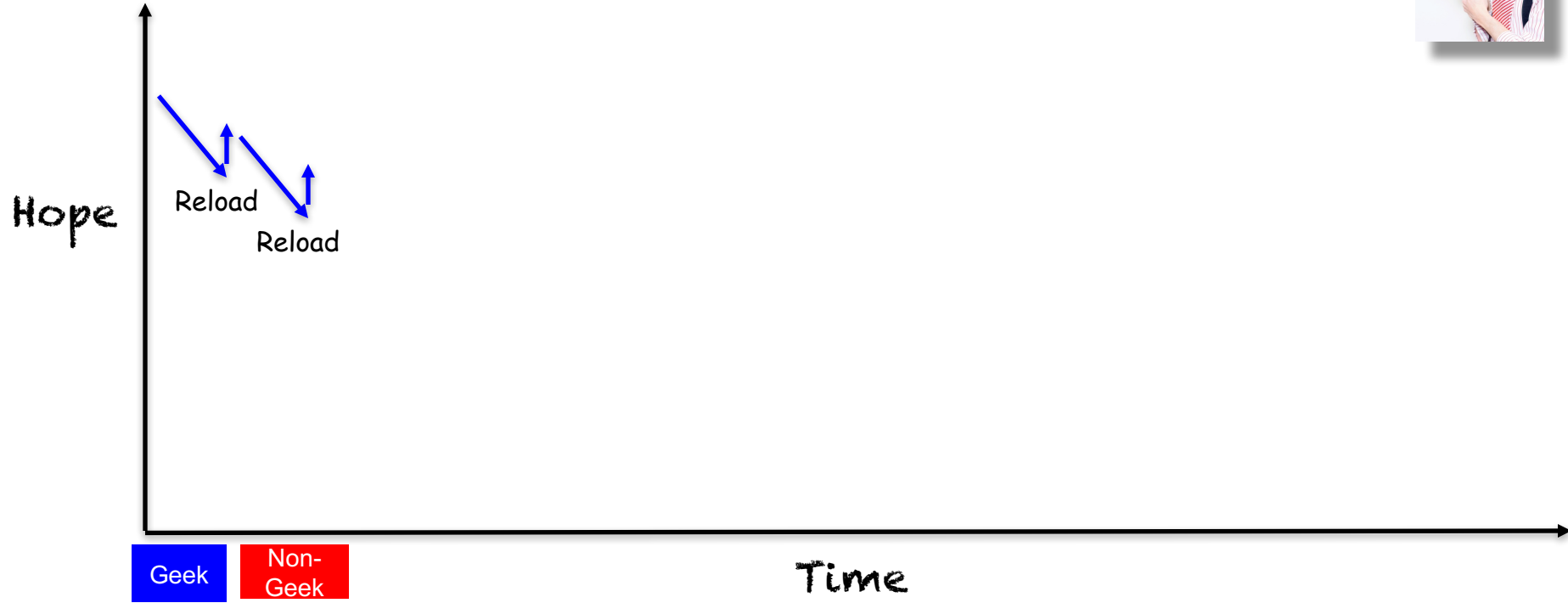
Geeks – My Peeps



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

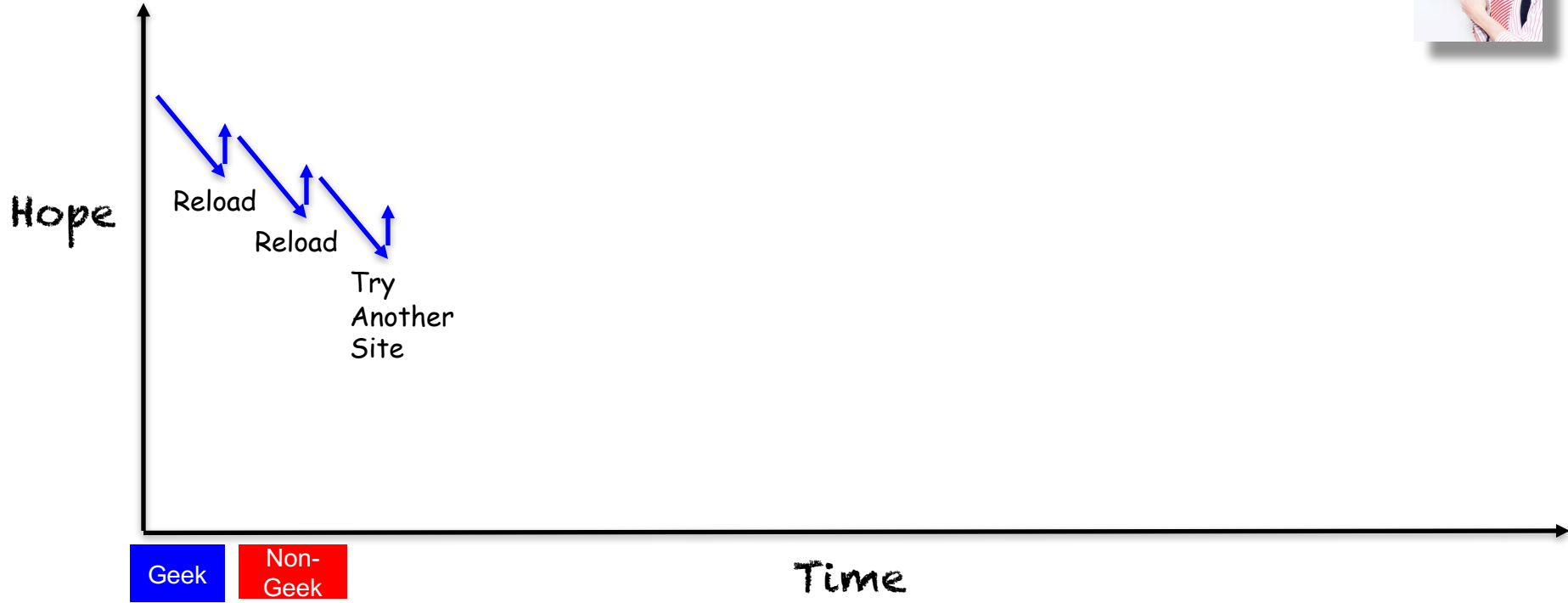
Geeks – My Peeps



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

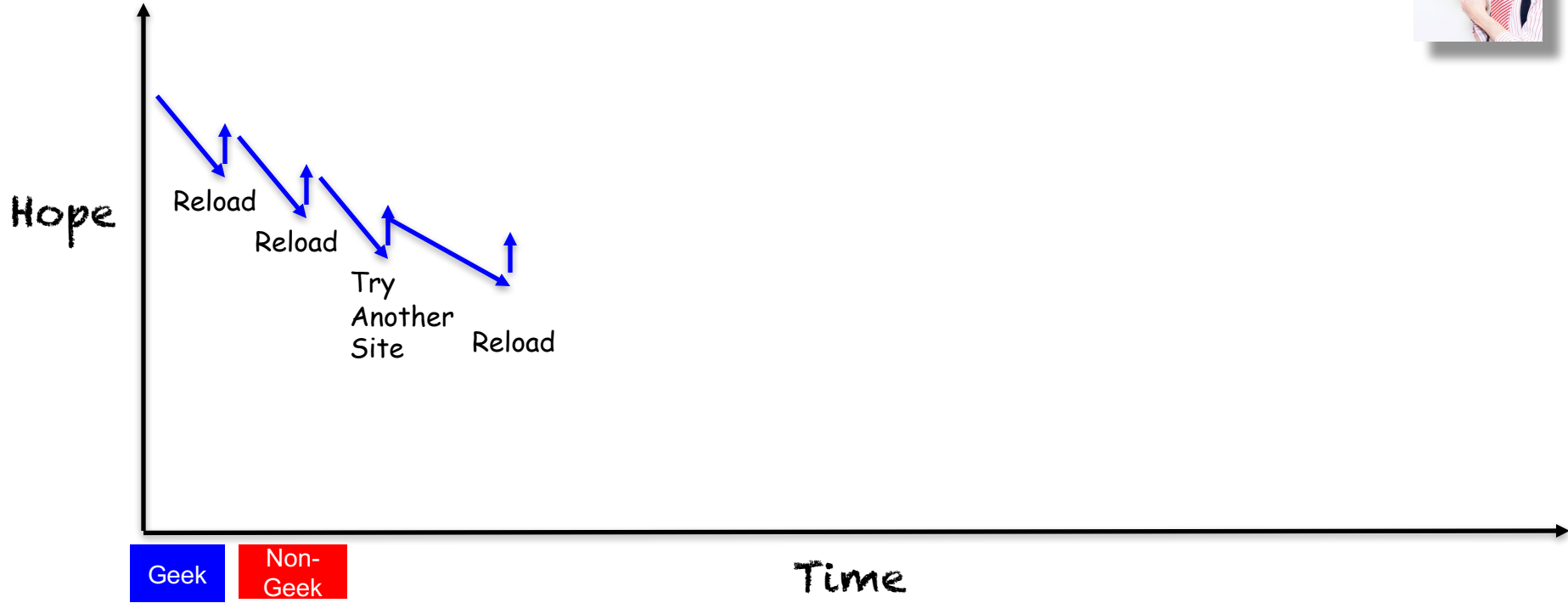
Geeks – My Peeps



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

Geeks – My Peeps



Geek

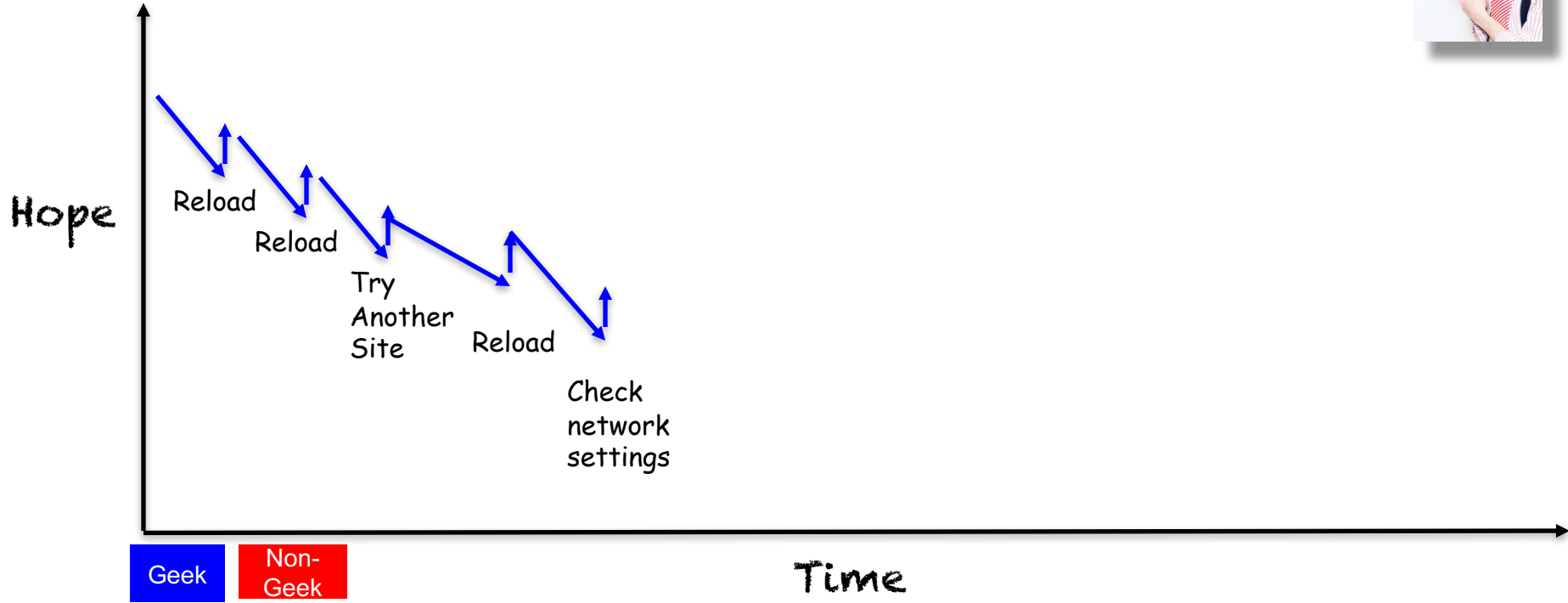
Non-Geek

Time

Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

Geeks – My Peeps



Geek

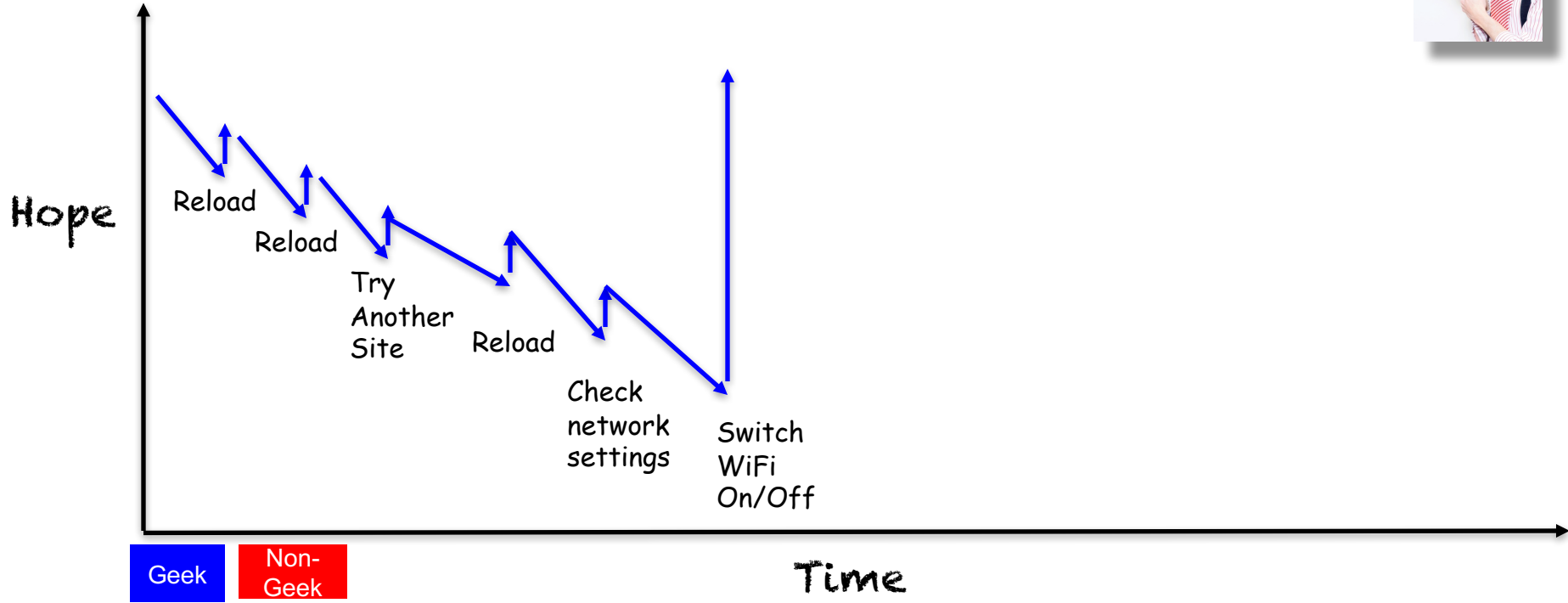
Non-Geek

Time

Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

Geeks – My Peeps



Geek

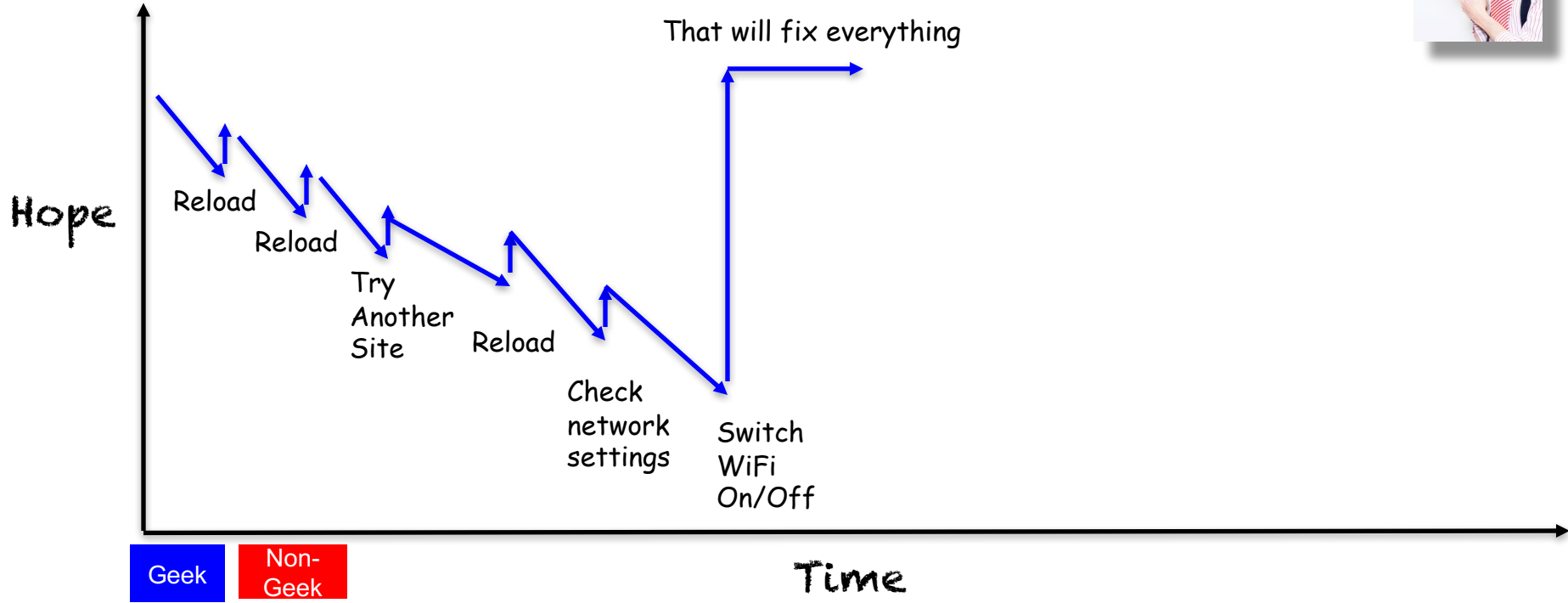
Non-Geek

Time

Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

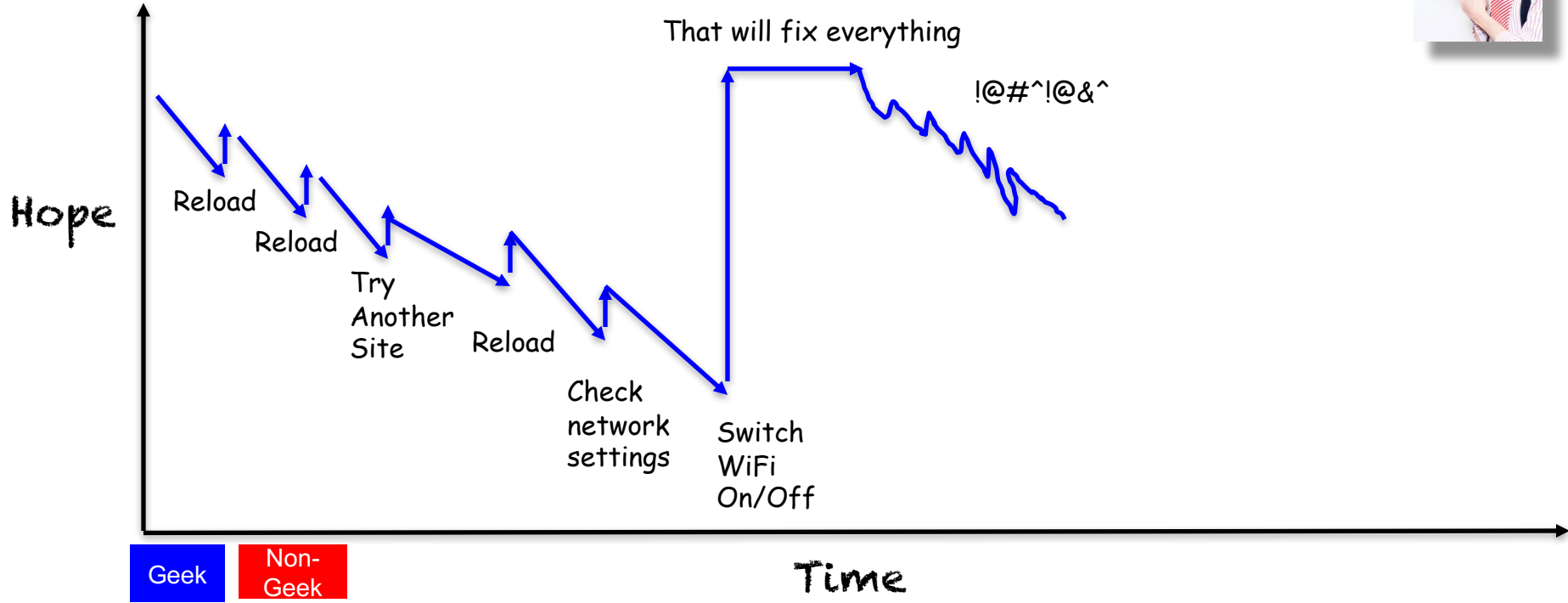
Geeks – My Peeps



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

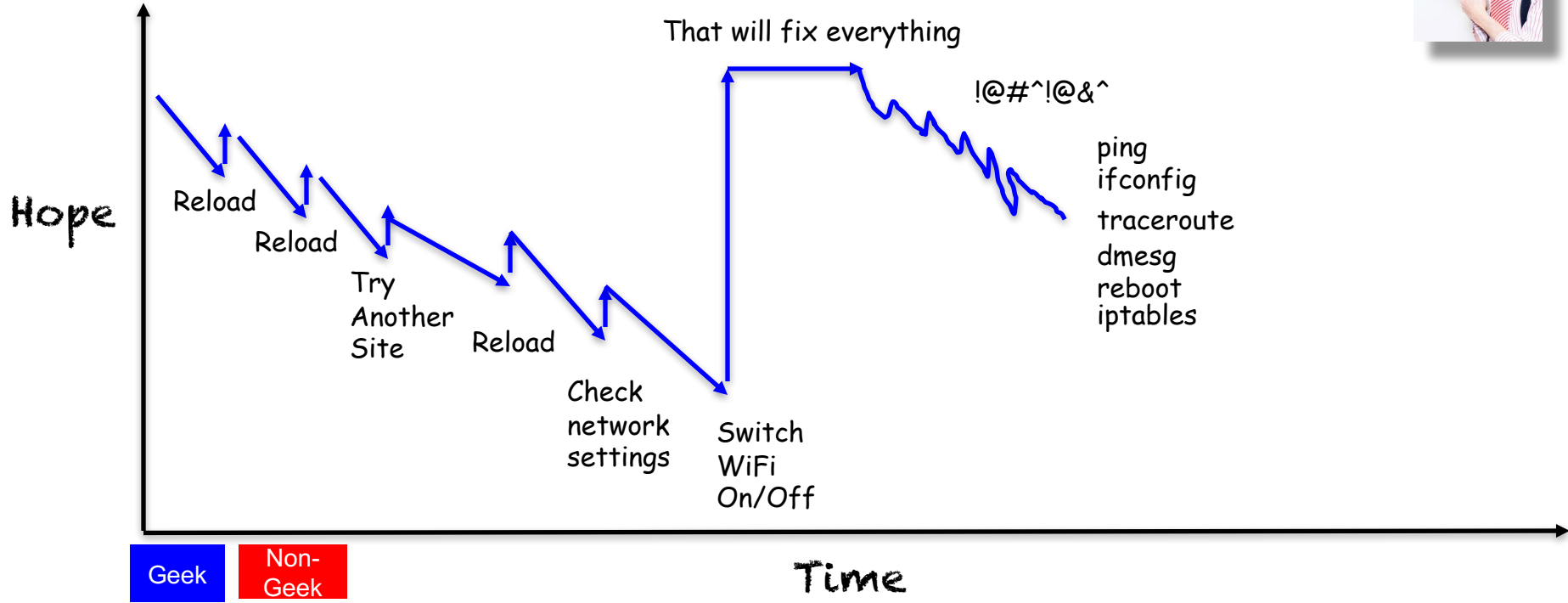
Geeks – My Peeps



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

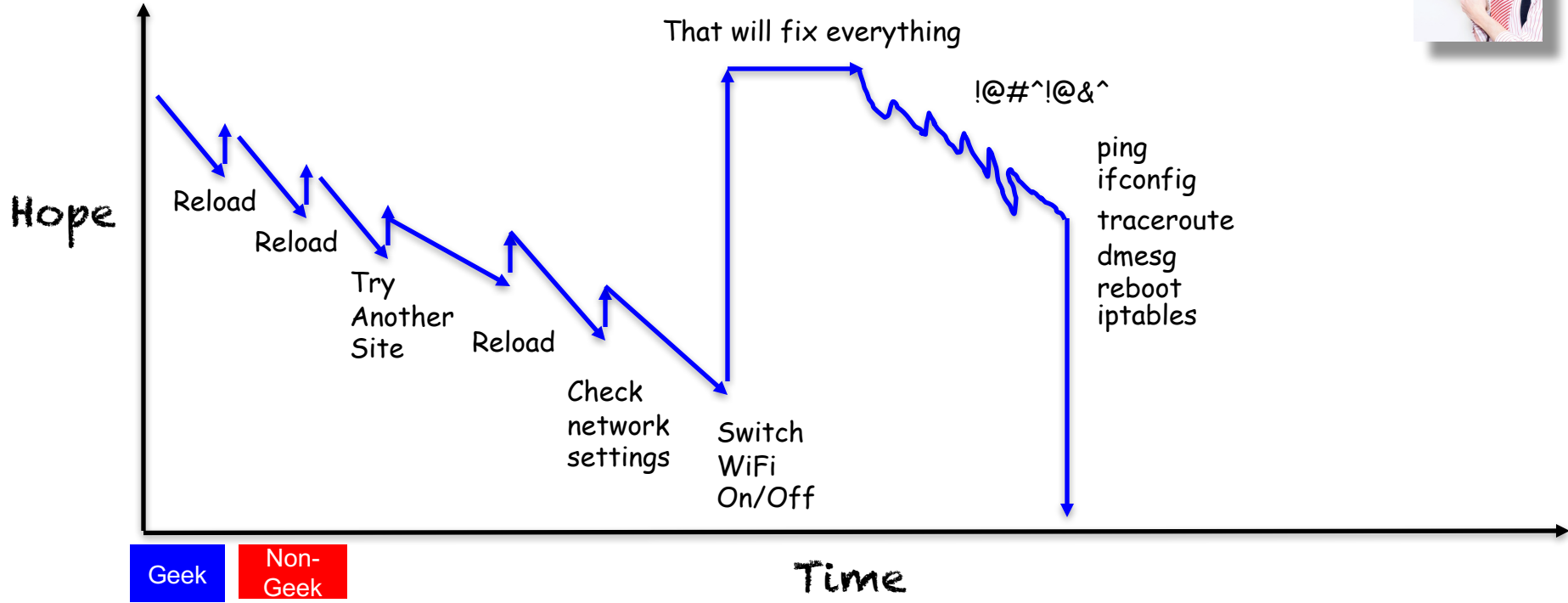
Geeks – My Peeps



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

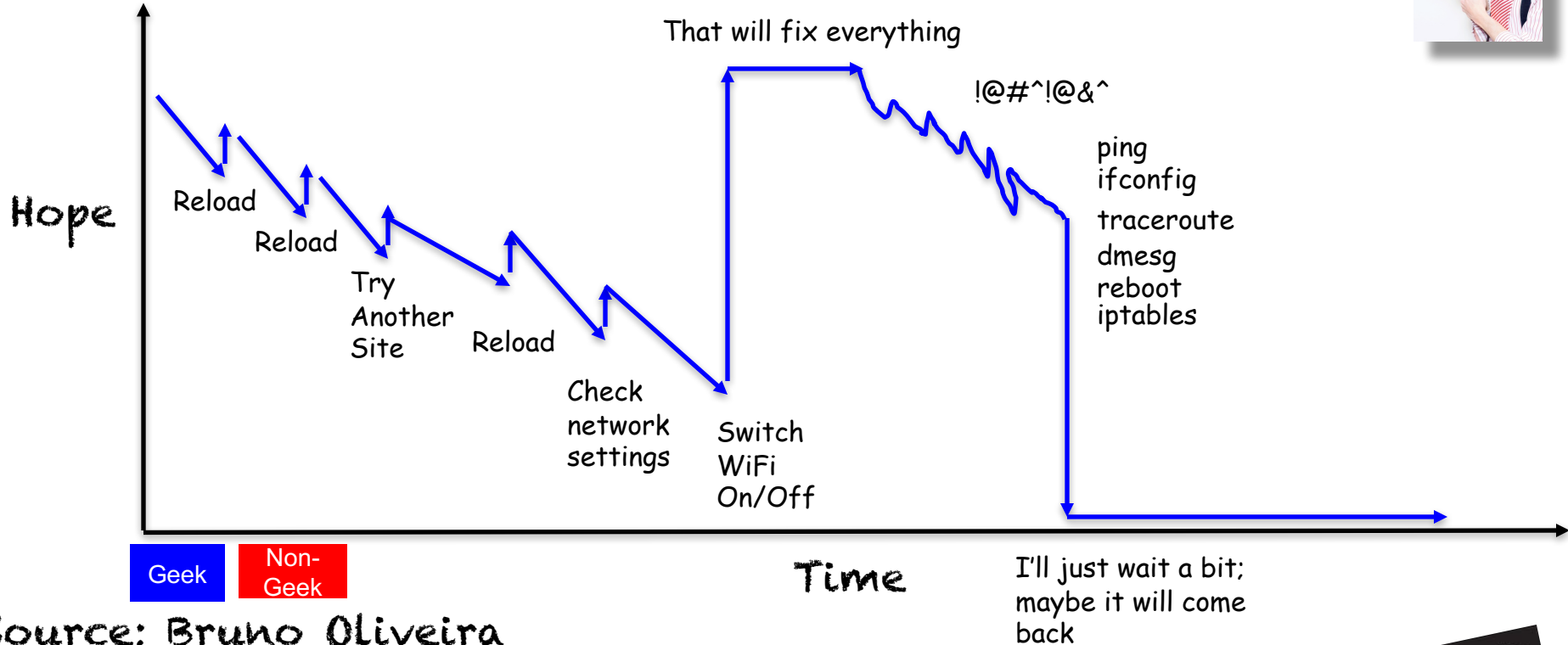
Geeks – My Peeps



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

Geeks – My Peeps



Geek

Non-Geek

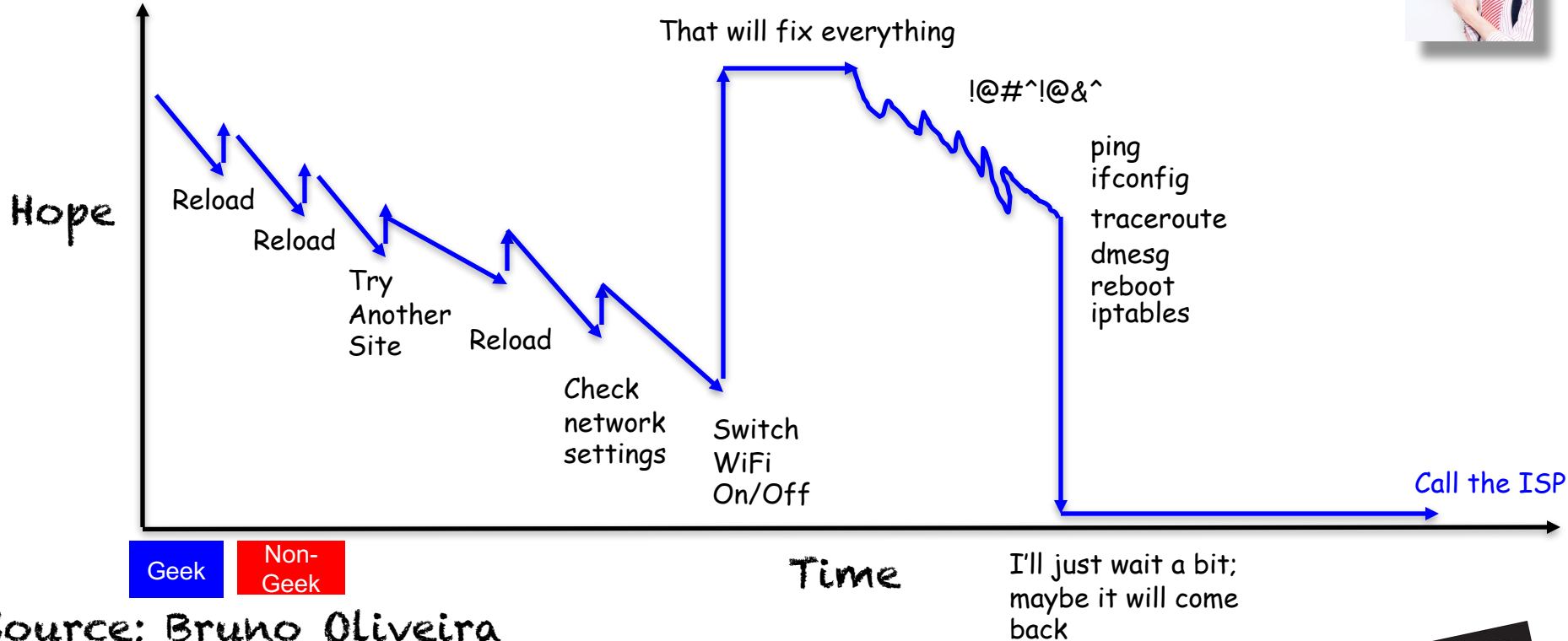
Time

I'll just wait a bit; maybe it will come back

Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

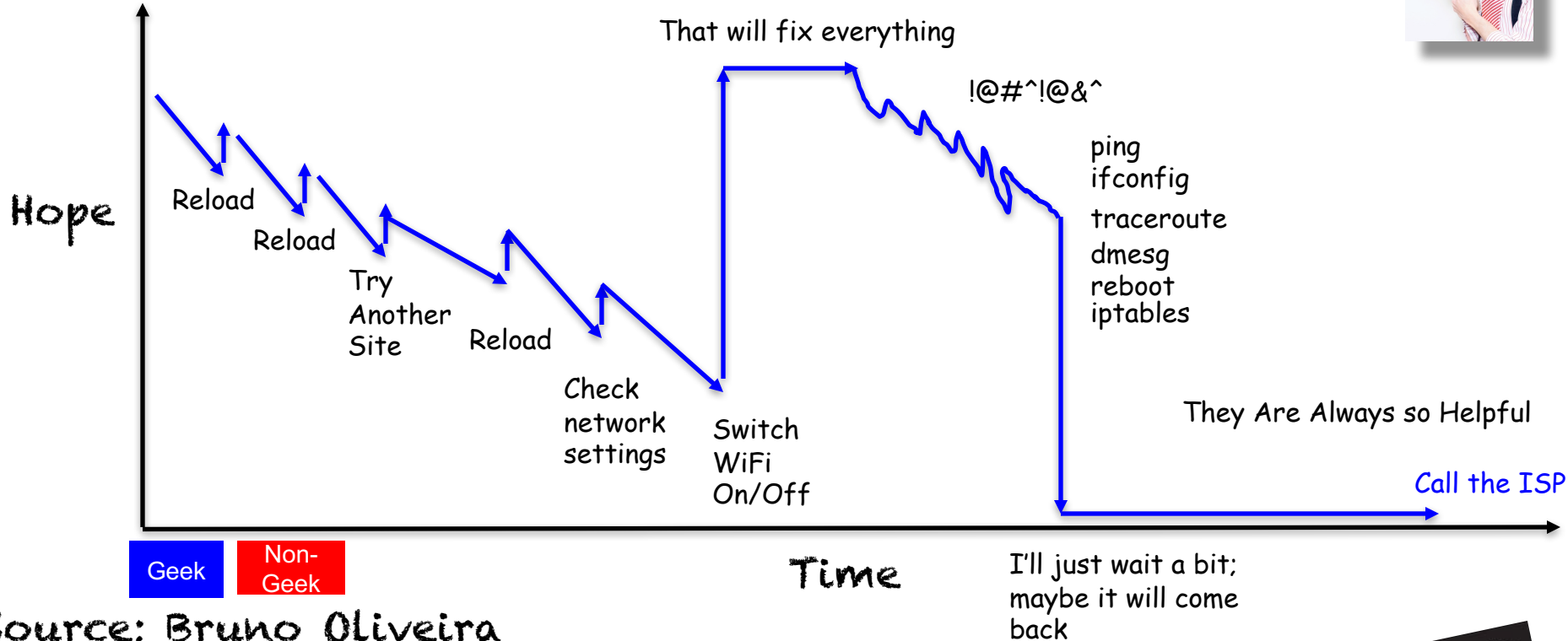
Geeks – My Peeps



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection

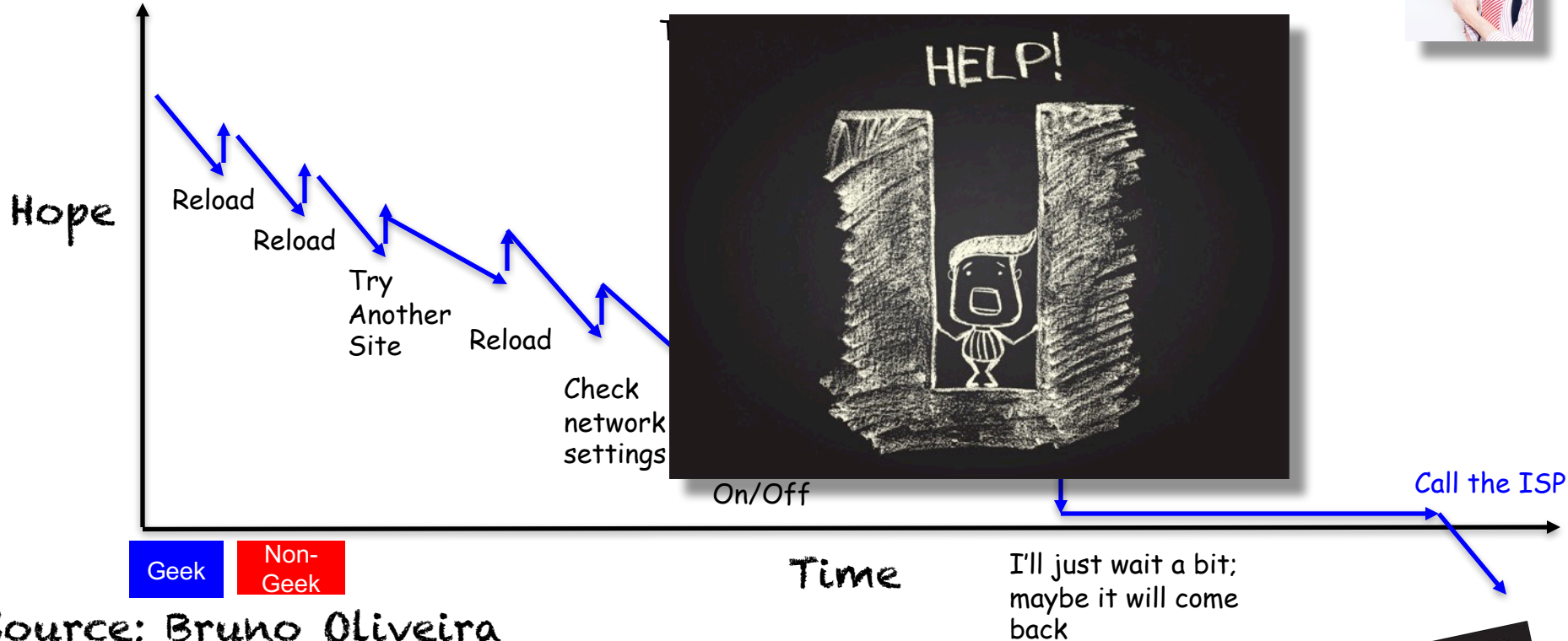
Geeks – My Peeps



Source: Bruno Oliveira

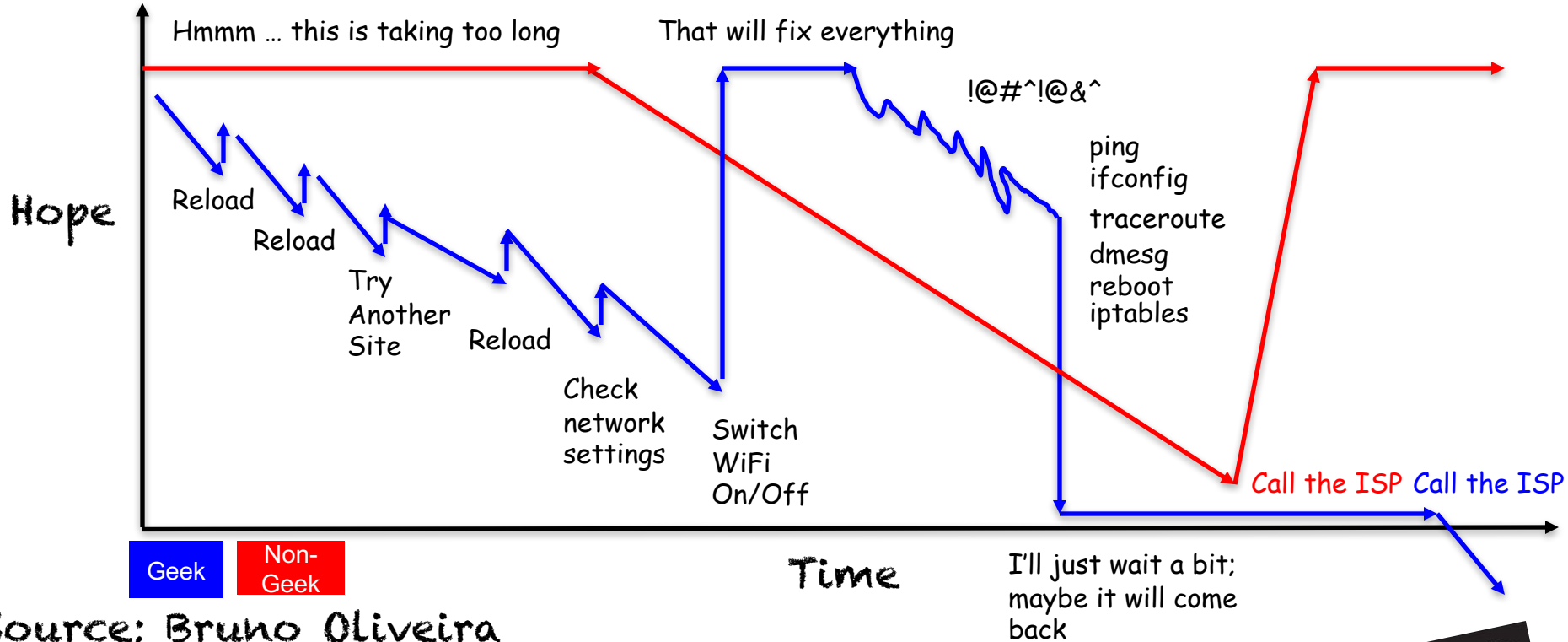
Geeks vs Non-Geeks: Reaction to flaky internet connection

Geeks – My Peeps



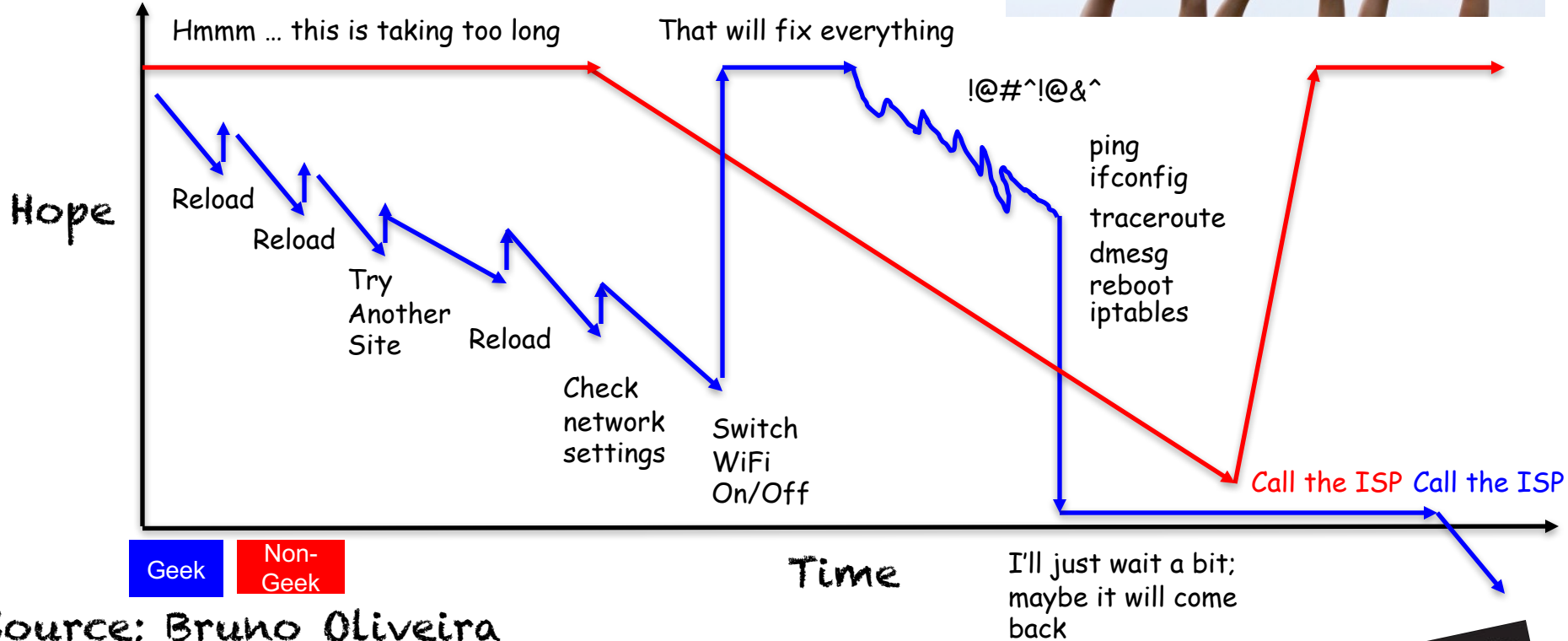
Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



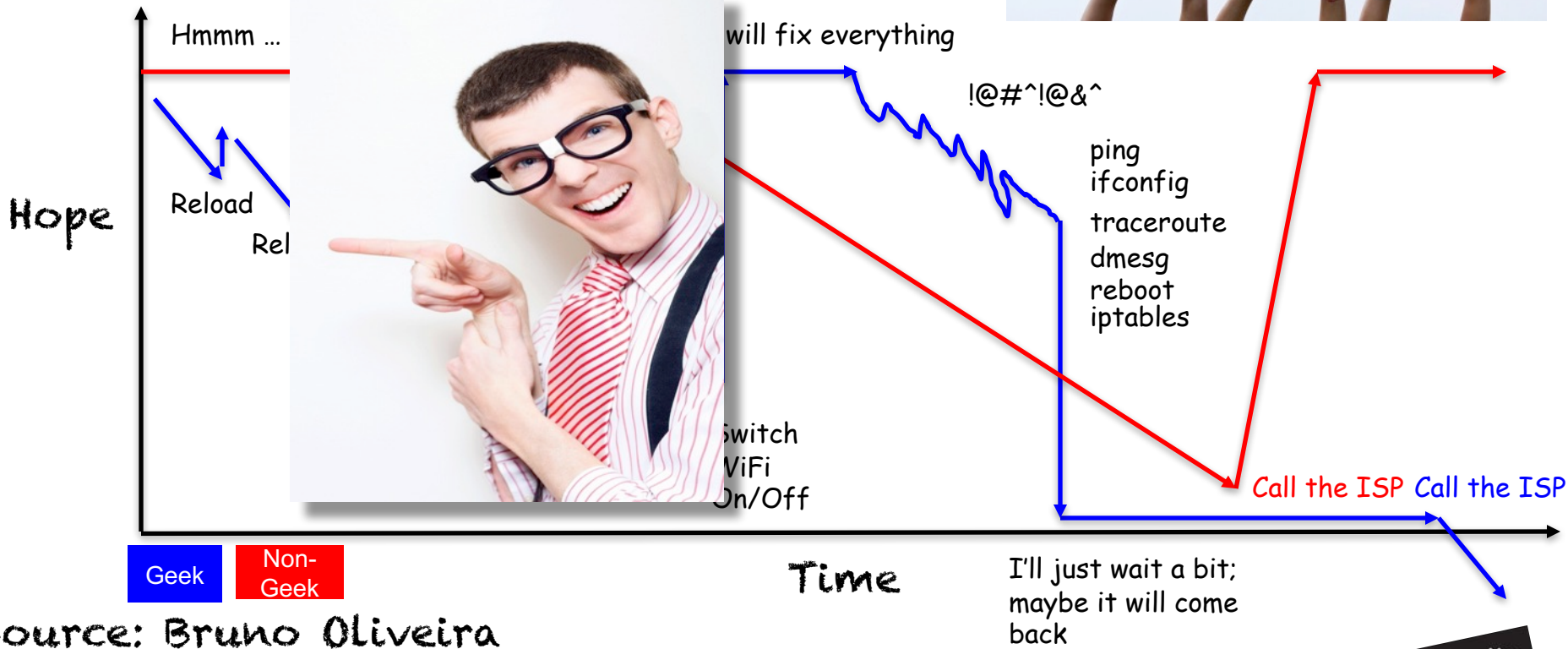
Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Source: Bruno Oliveira

Geeks vs Non-Geeks: Reaction to flaky internet connection



Source: Bruno Oliveira





AUTHORITY: FEAR UNCERTAINTY AND DOUBT COMMITTEE



STATE OF CALIFORNIA

CERTIFIED

AUTHORITY: FEAR UNCERTAINTY AND DOUBT COMMITTEE



STATE OF CALIFORNIA



Network Defender First Principles



Elon Musk



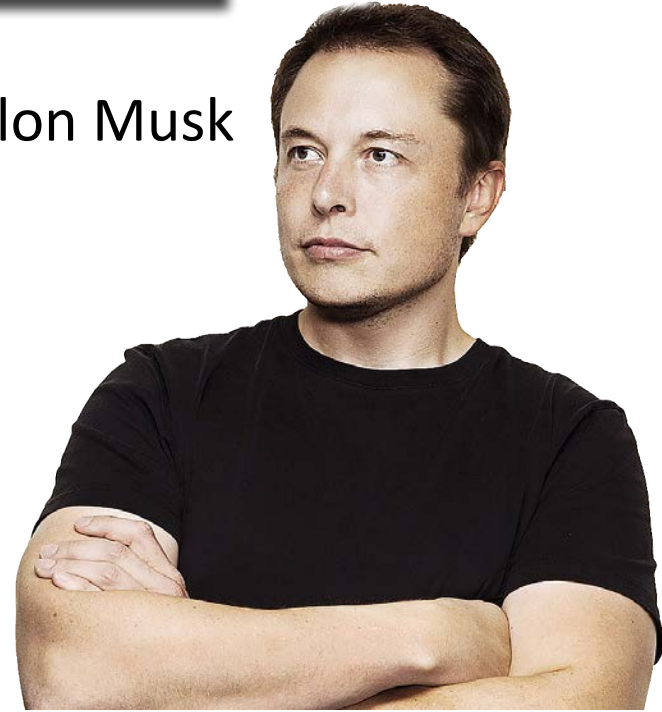


Elon Musk



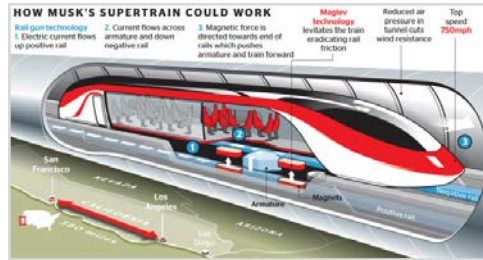


Elon Musk



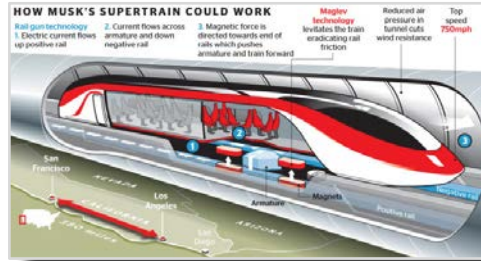


Elon Musk





Elon Musk





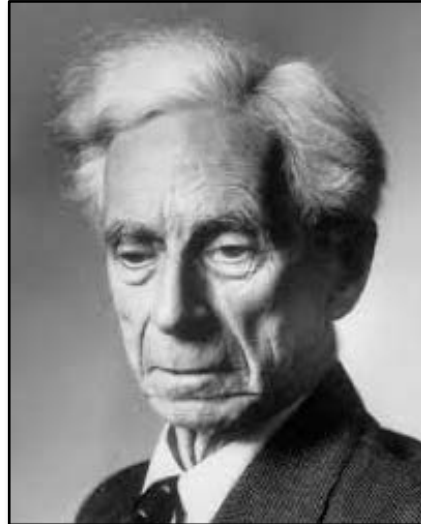
Elon Musk



What is a First Principle?

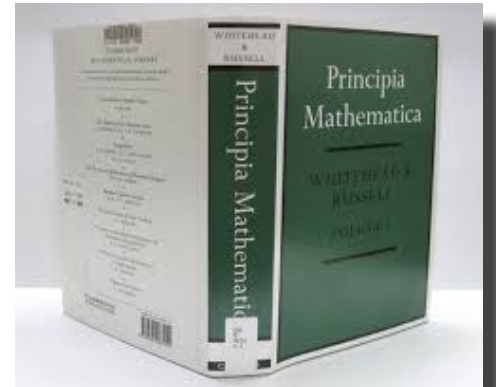


Whitehead

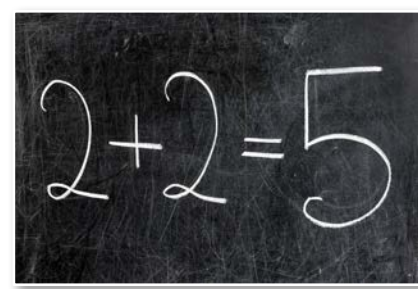


Russell

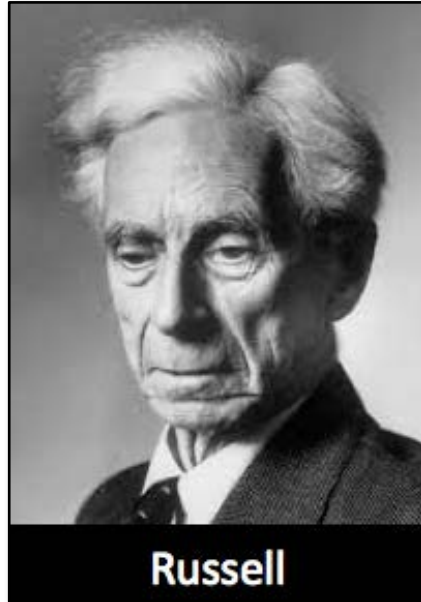
Principia Mathematica
published in 1913



What is a First Principle?

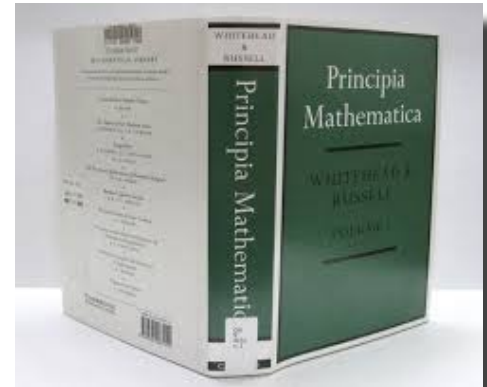


Whitehead

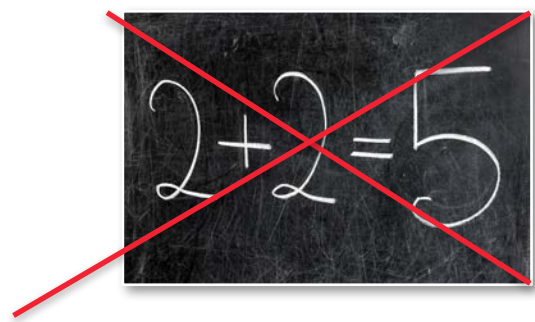
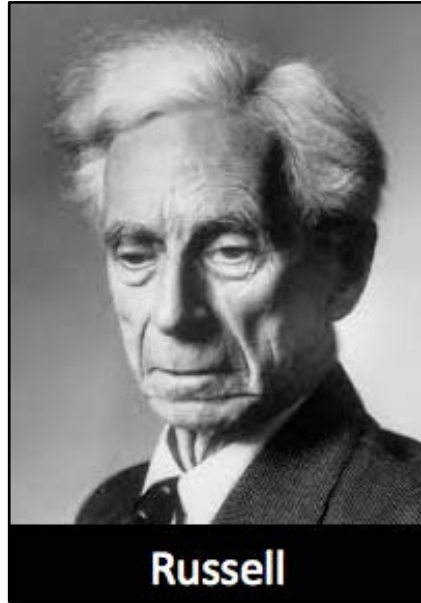


Russell

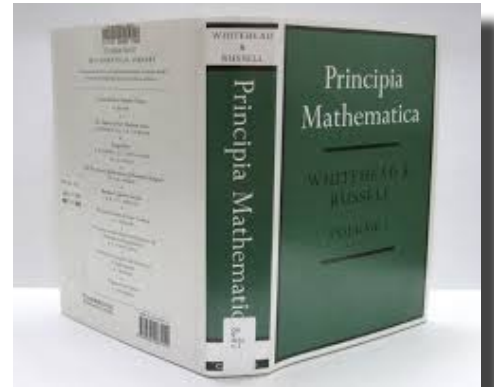
Principia Mathematica
published in 1913



What is a First Principle?



Principia Mathematica
published in 1913



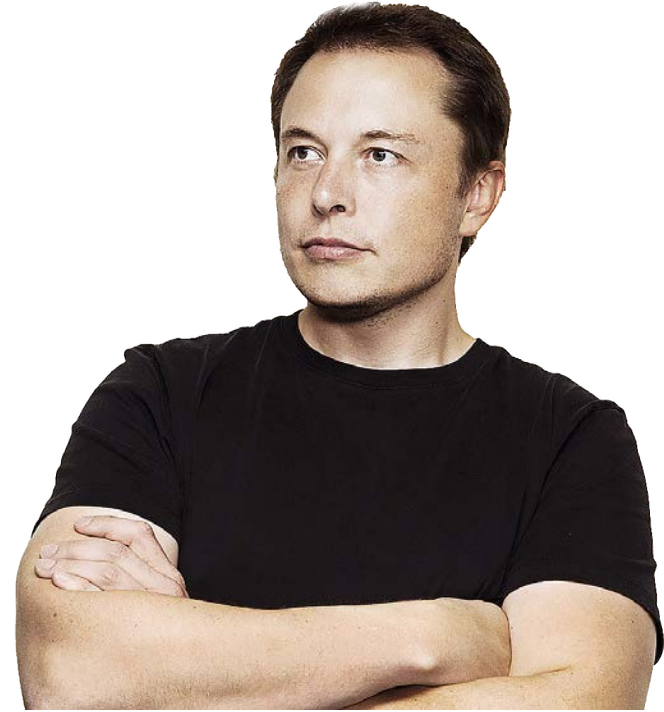
Analogy vs First Principle



Analogy vs First Principle



SIMILAR



Analogy vs First Principle



SIMILAR



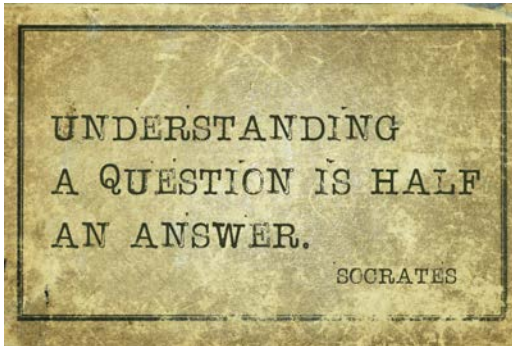
Analogy vs First Principle

LEAP AHEAD



Analogy vs First Principle

LEAP AHEAD



Analogy vs First Principle

LEAP AHEAD



Boiled Water



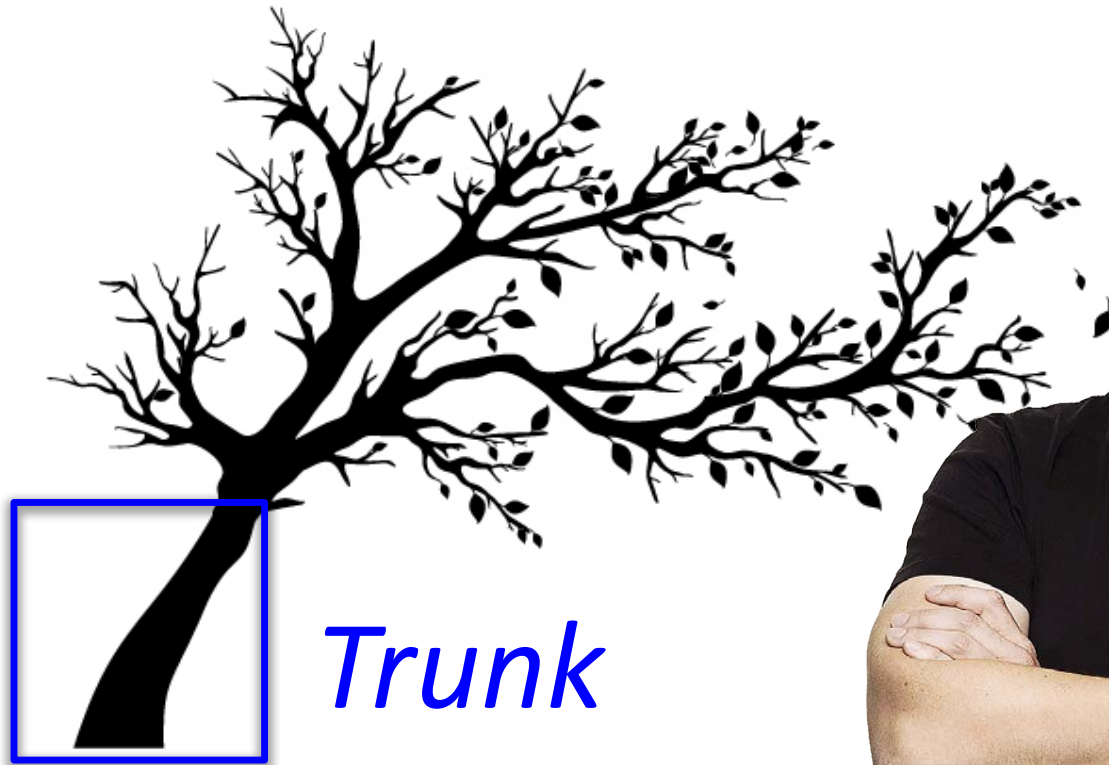
Semantic Tree



Semantic Tree



Semantic Tree



Trunk



Semantic Tree

Limbs



Semantic Tree

Leaves



What is a First Principle?



What is a First Principle?



Fundamental

What is a First Principle?



Fundamental

Self Evident

What is a First Principle?



Fundamental

Self Evident

Experts Agree

What is a First Principle?



Fundamental

Self Evident

Experts Agree

Atomic

What is a First Principle?



Fundamental

Self Evident

Experts Agree

Atomic



What is a First Principle?

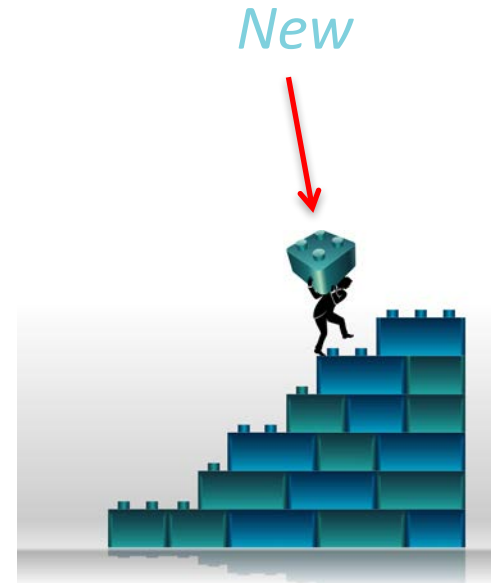


Fundamental

Self Evident

Experts Agree

Atomic



What is a First Principle?



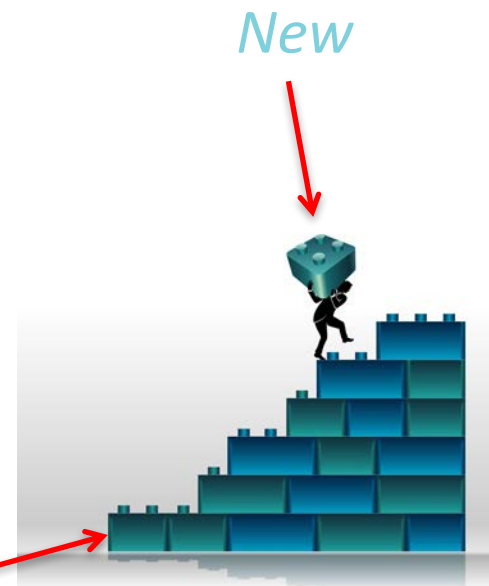
Fundamental

Self Evident

Experts Agree

Atomic

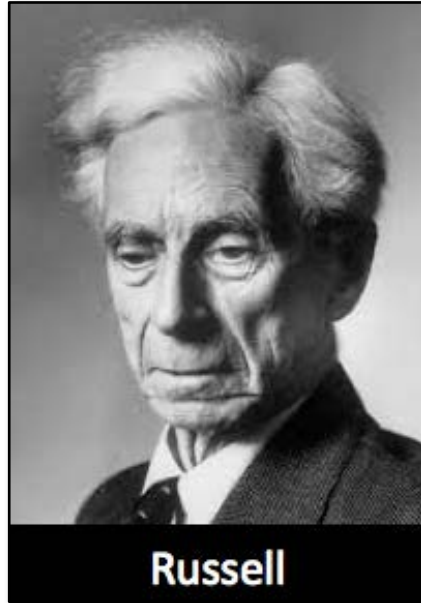
First Principles



What is a First Principle?

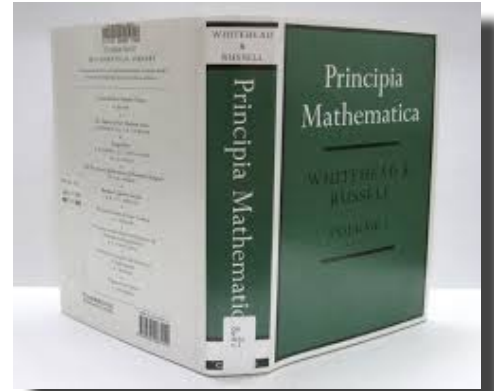


Whitehead

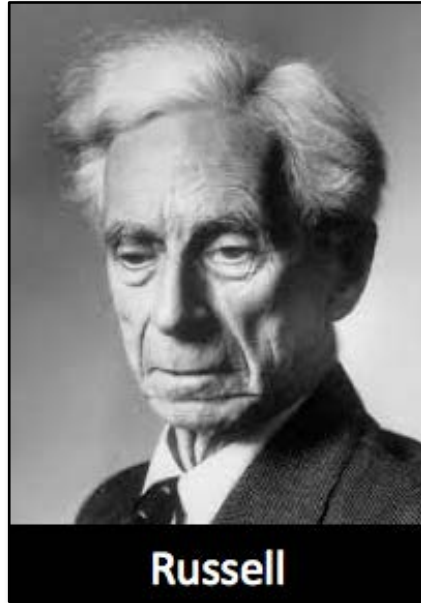


Russell

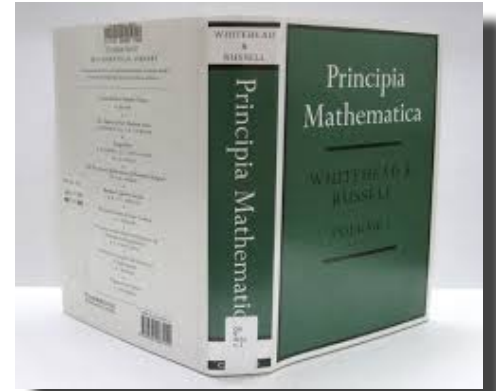
$$1 + 1 = 2$$



What is a First Principle?



$$1 + 1 = 2$$



*Note: Might be useful to know

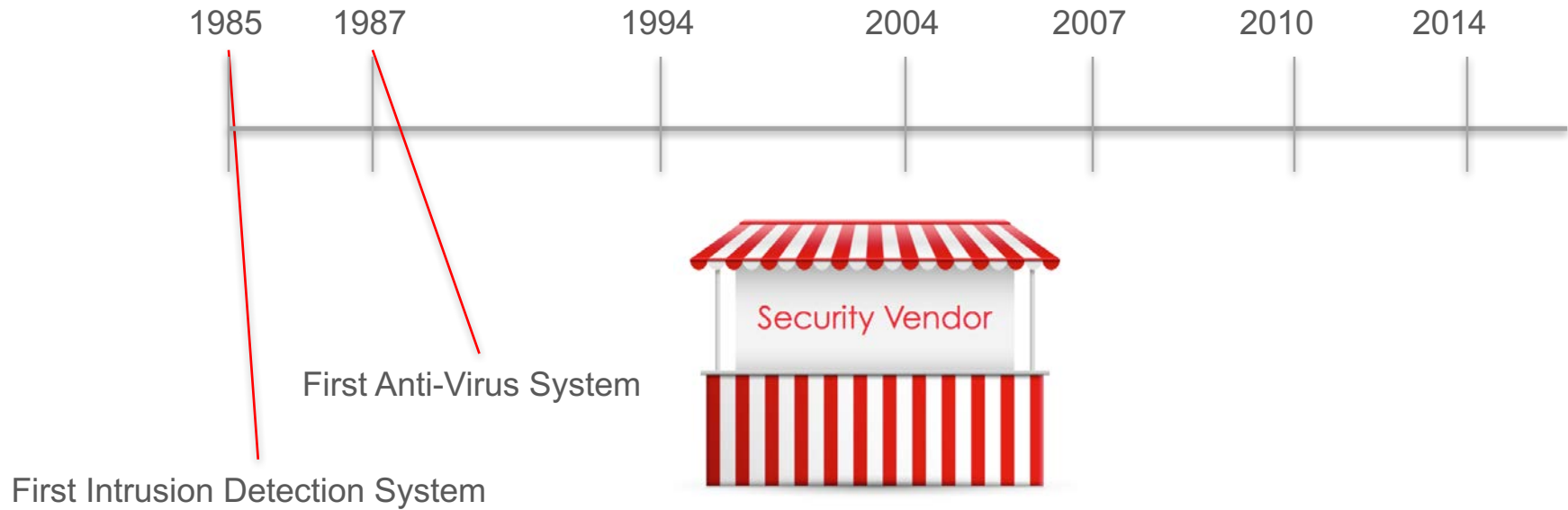
Network Defender Problem Space



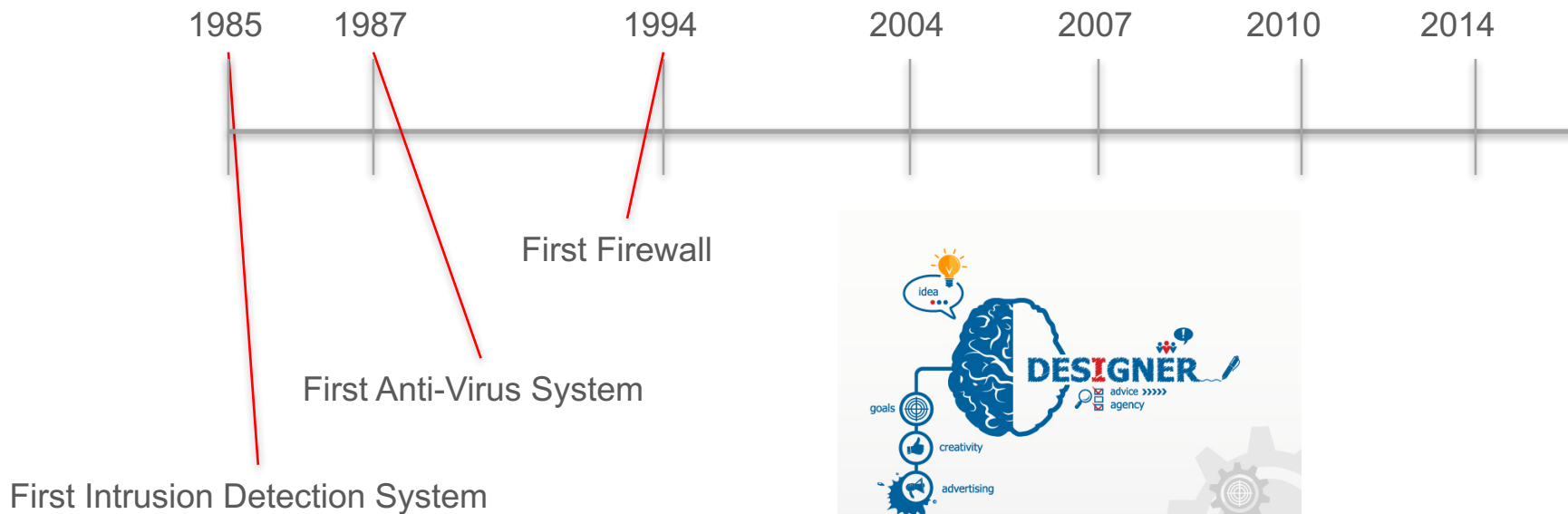
First Intrusion Detection System



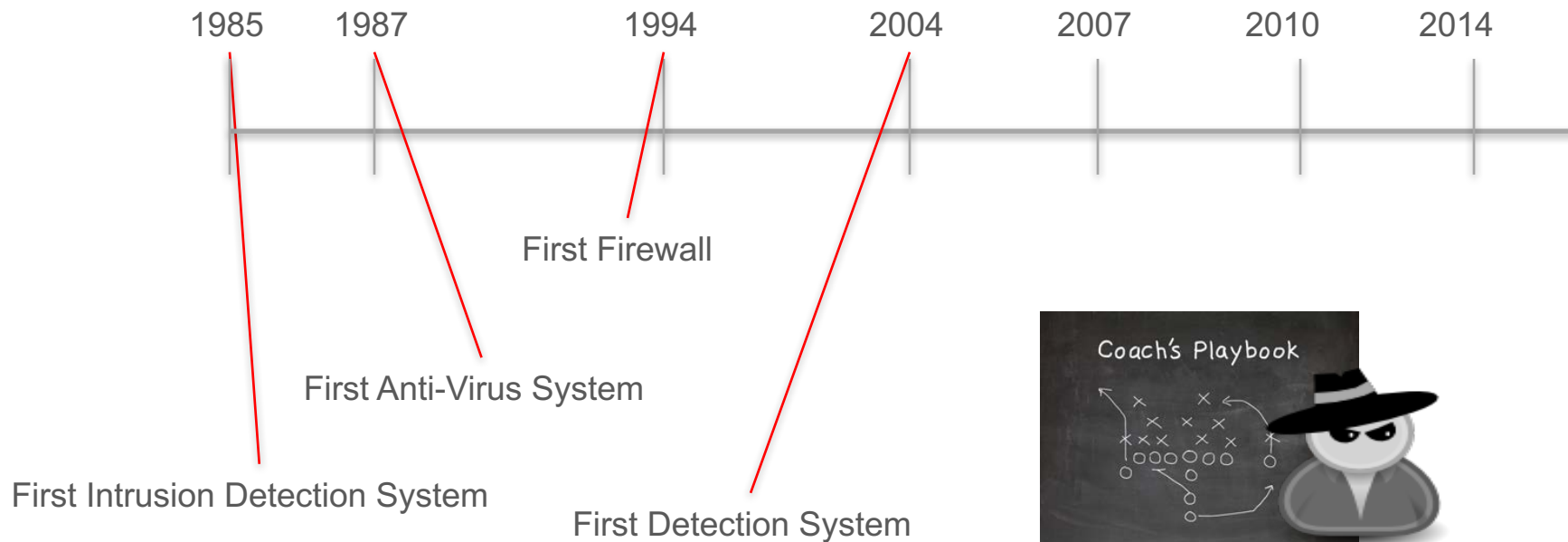
Network Defender Problem Space



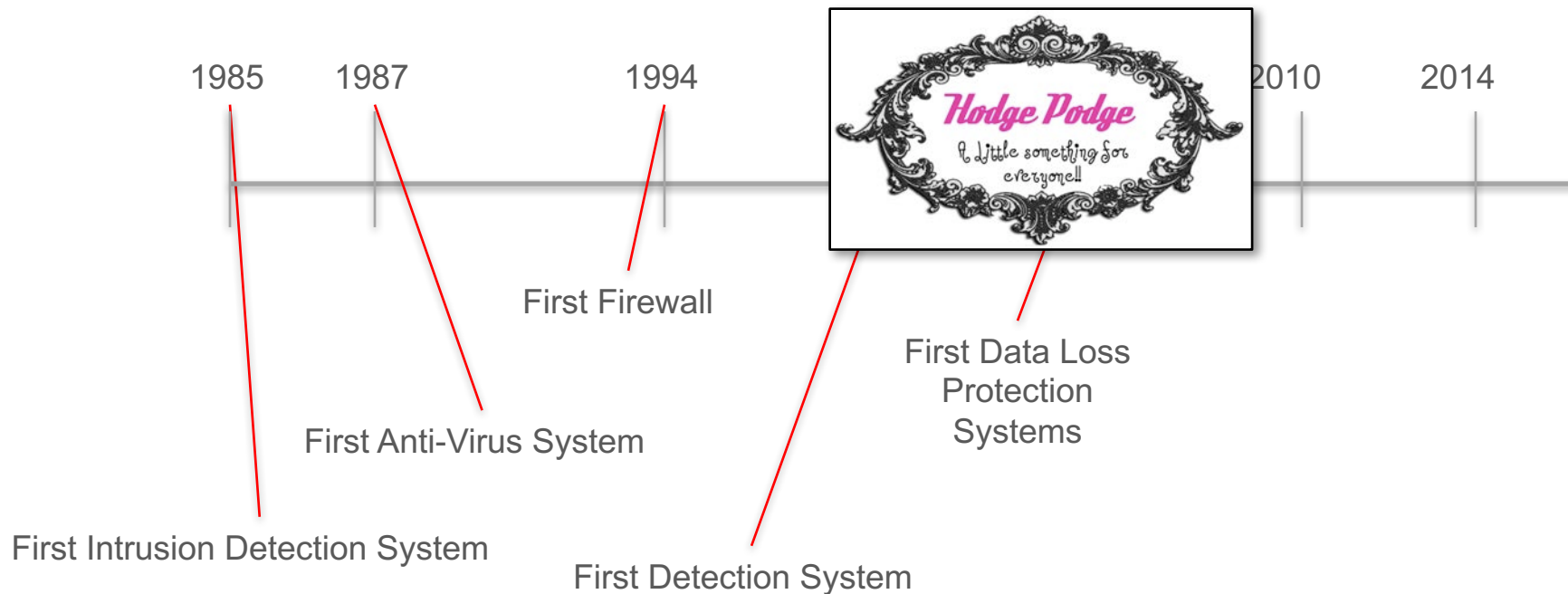
Network Defender Problem Space



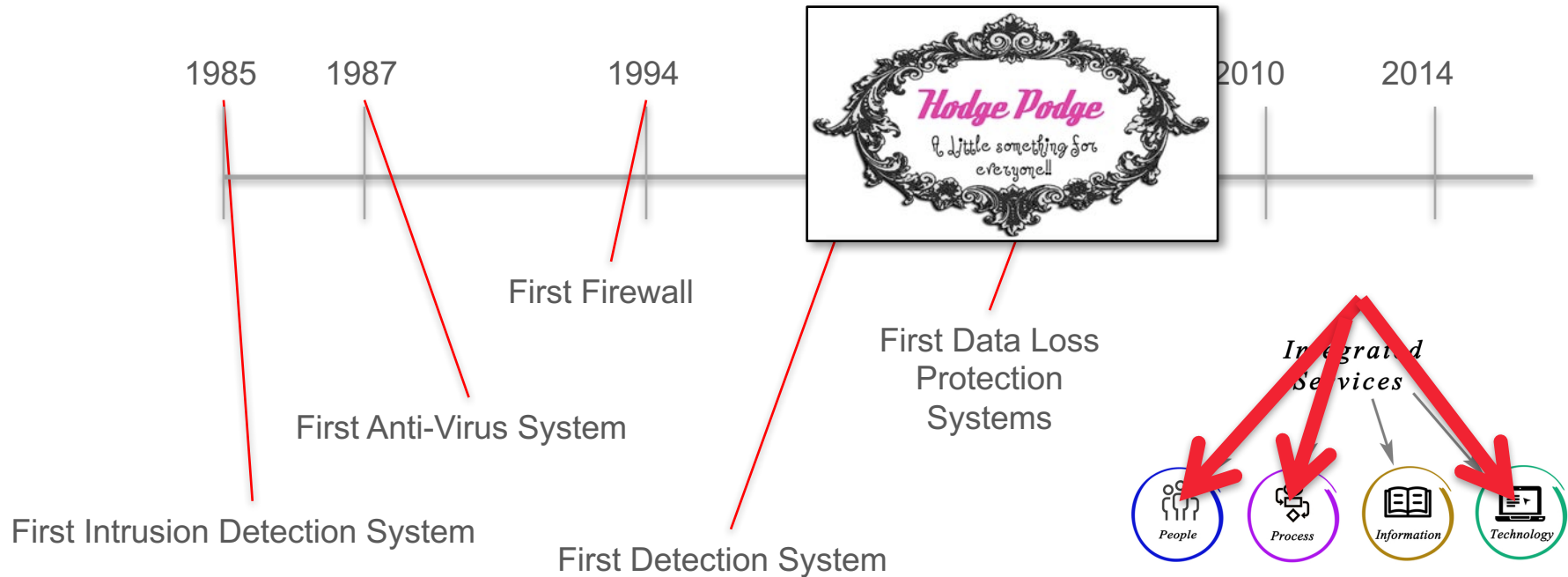
Network Defender Problem Space



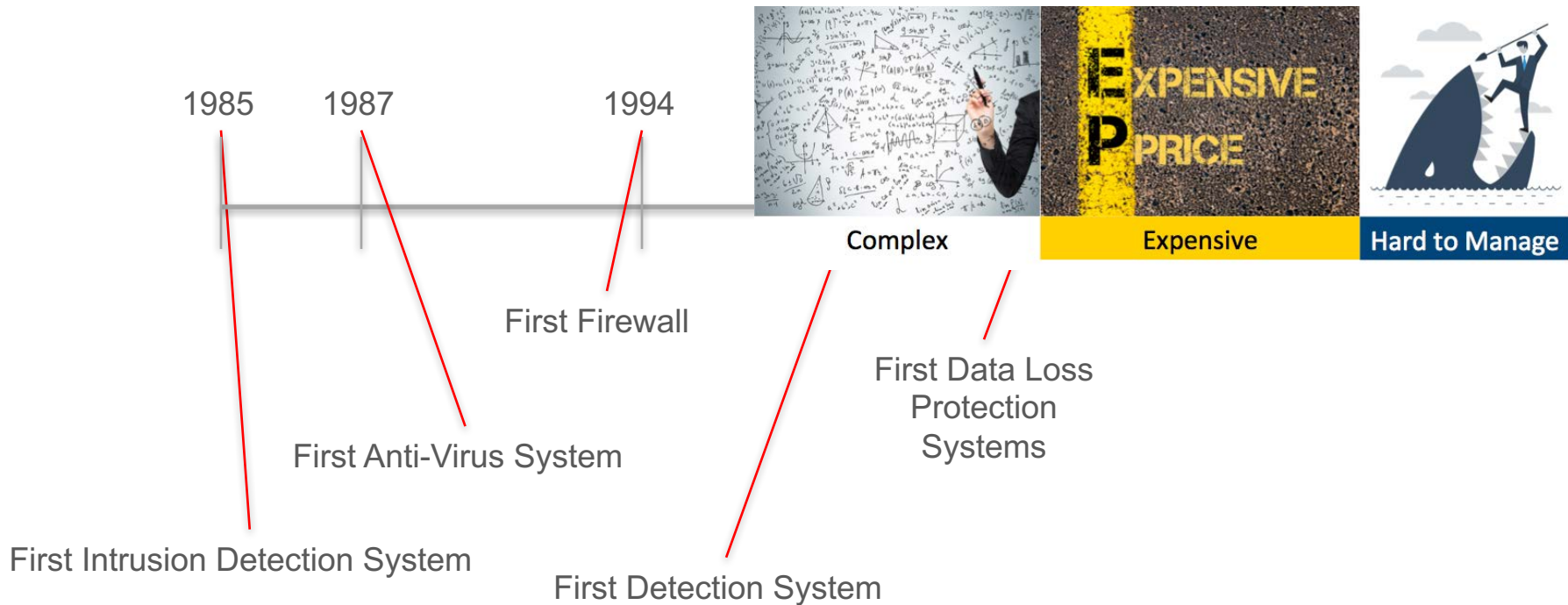
Network Defender Problem Space



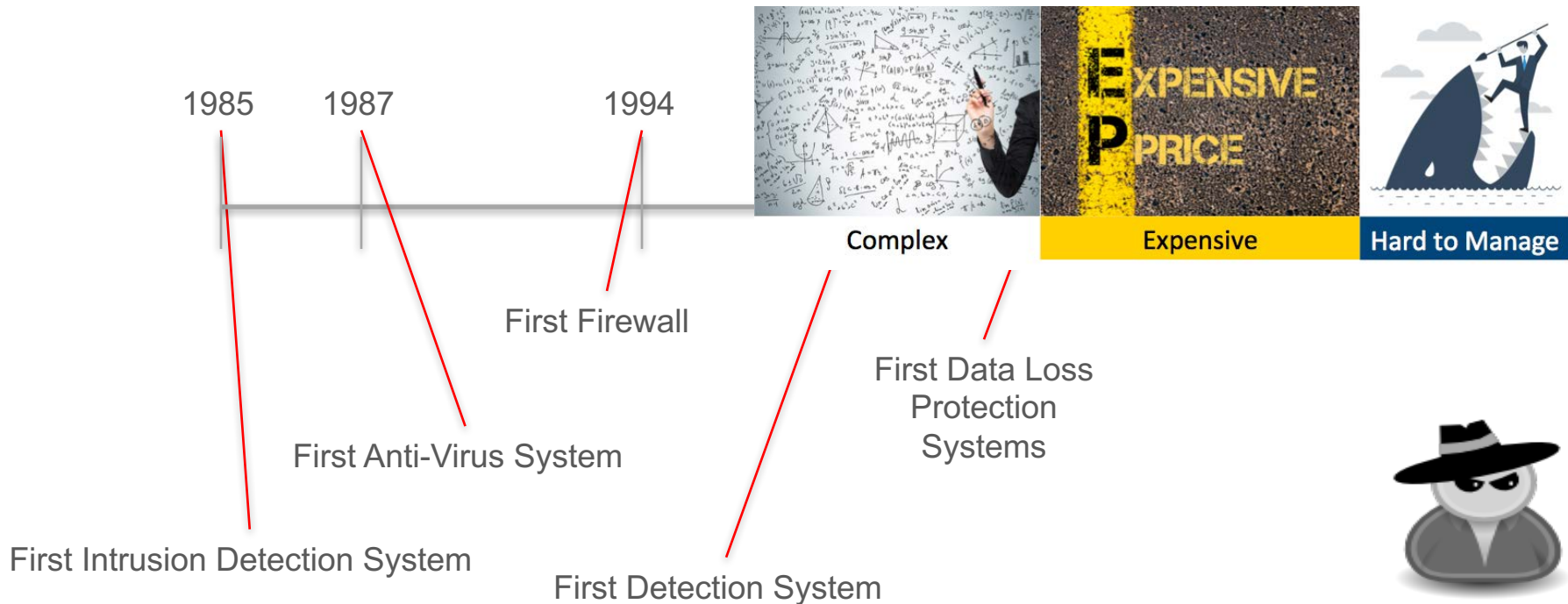
Network Defender Problem Space



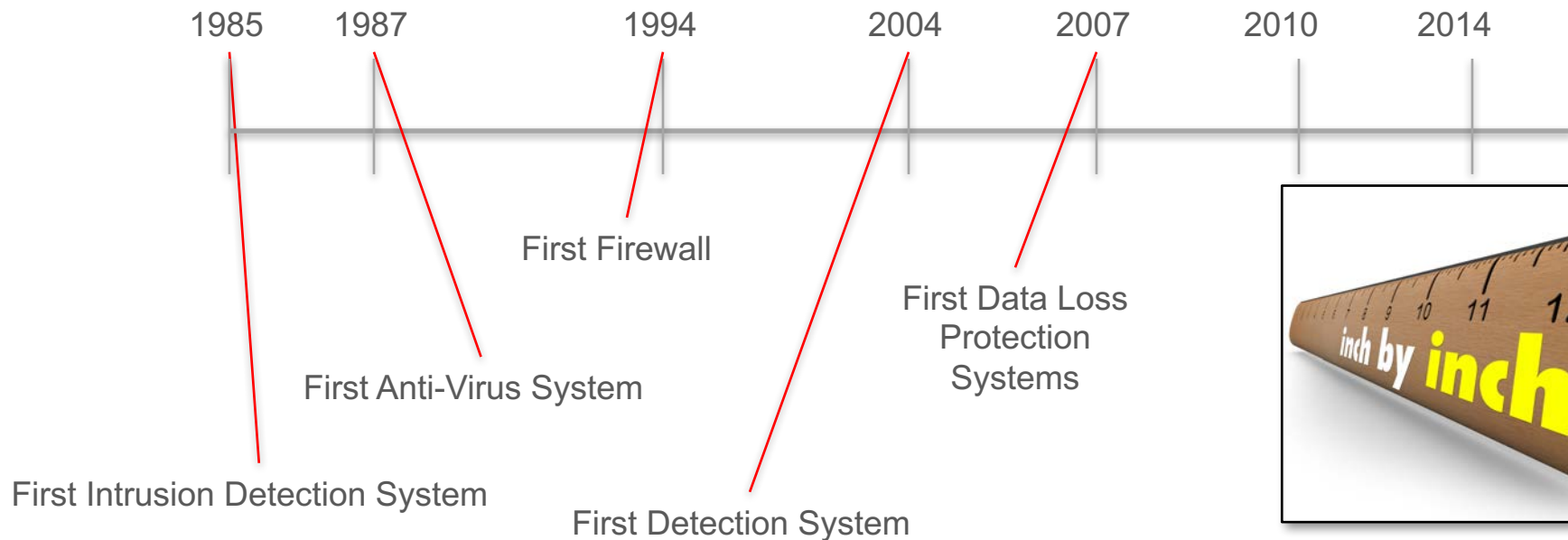
Network Defender Problem Space



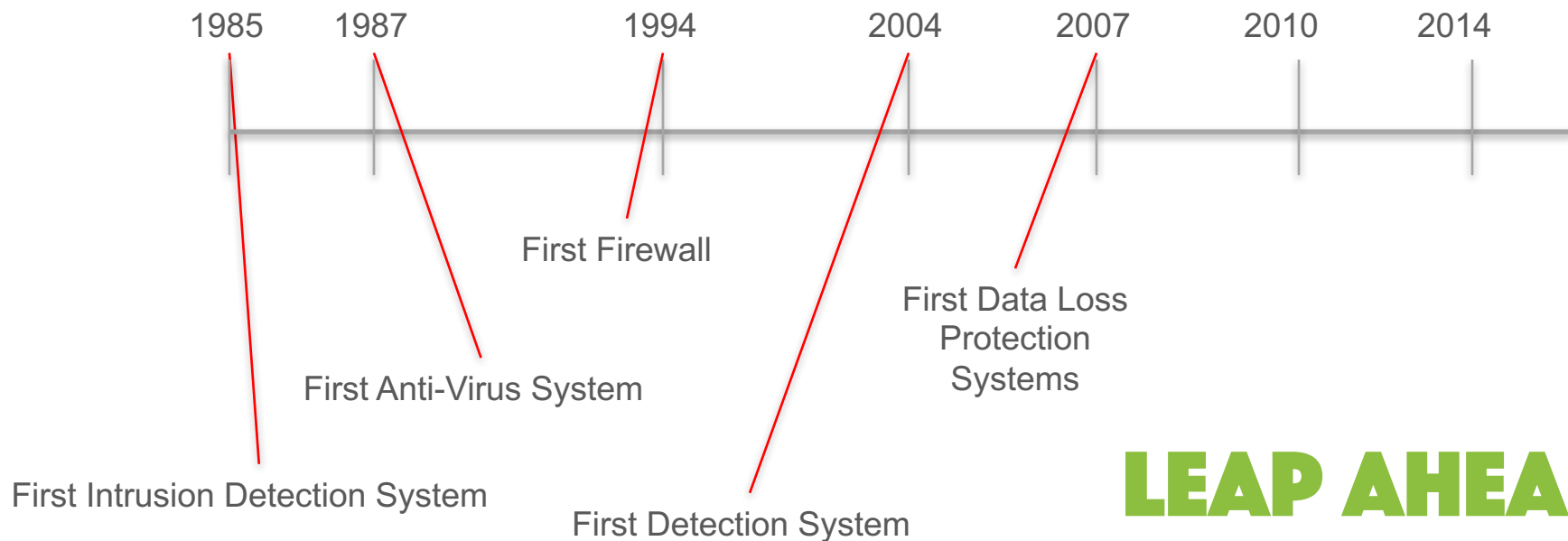
Network Defender Problem Space



Network Defender Problem Space

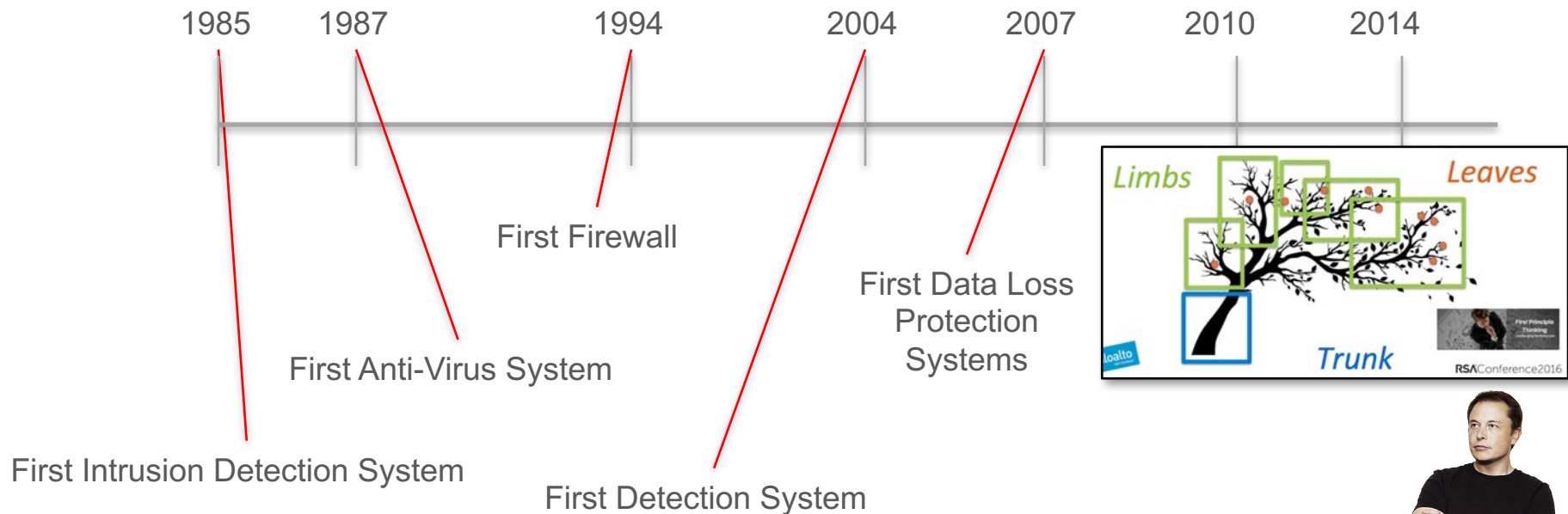


Network Defender Problem Space



LEAP AHEAD

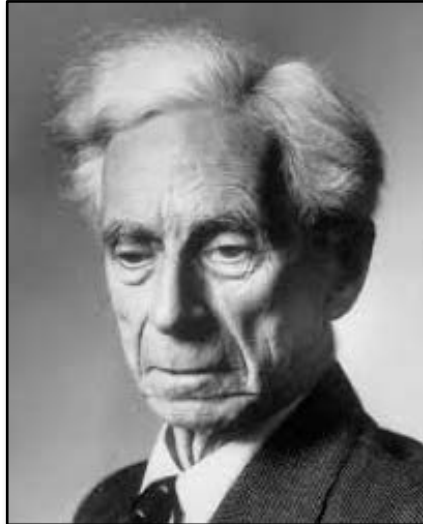
Network Defender Problem Space



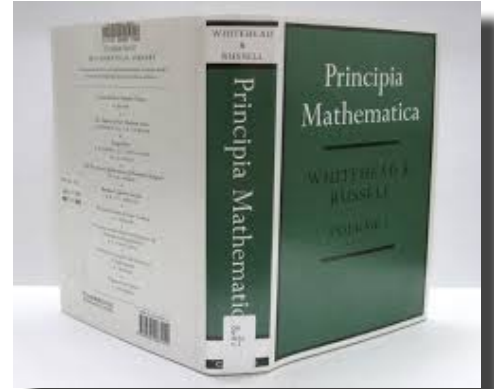
Prefatory First Principle Statements



Whitehead



Russell



Prefatory First Principle Statements



Prefatory First Principle Statements



Prefatory First Principle Statements



CYBER ESPIONAGE	
CYBER CRIME	
CYBER HACKTIVISM	
CYBER WARFARE	
CYBER MISCHIEF	
CYBER TERRORISM	

Prefatory First Principle Statements



CYBER ESPIONAGE	
CYBER CRIME	
CYBER HACKTIVISM	
CYBER WARFARE	
CYBER MISCHIEF	
CYBER TERRORISM	



Prefatory First Principle Statements



CYBER ESPIONAGE	
CYBER CRIME	
CYBER HACKTIVISM	
CYBER WARFARE	
CYBER MISCHIEF	
CYBER TERRORISM	



Prefatory First Principle Statements



Prefatory First Principle Statements



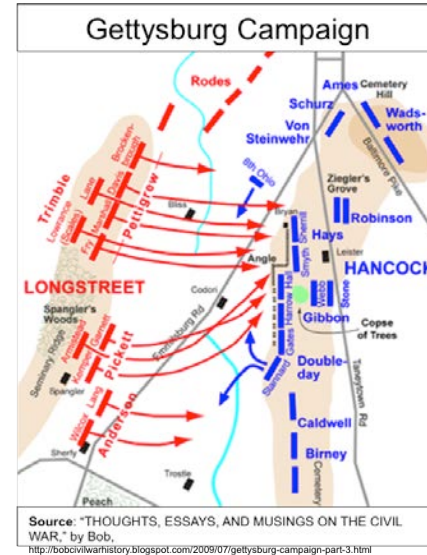
Prefatory First Principle Statements



Victim



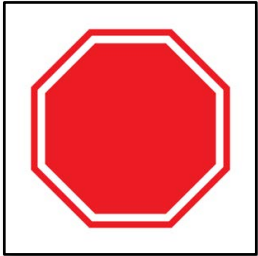
Prefatory First Principle Statements



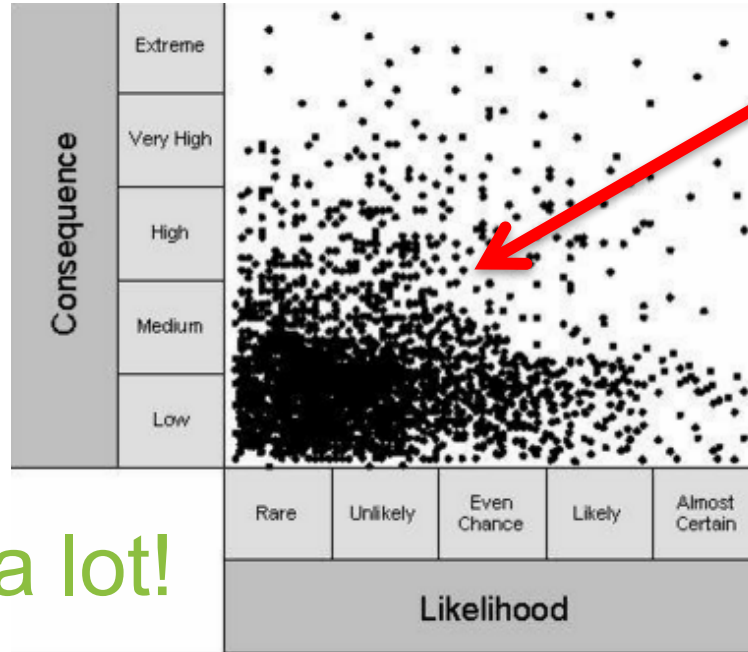
Victim



Prefatory First Principle Statements

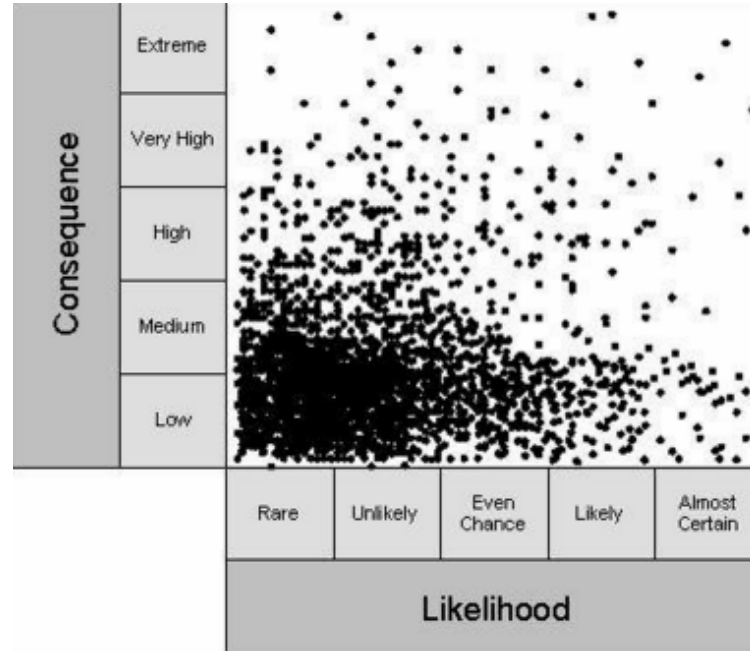


Wow! That's a lot!



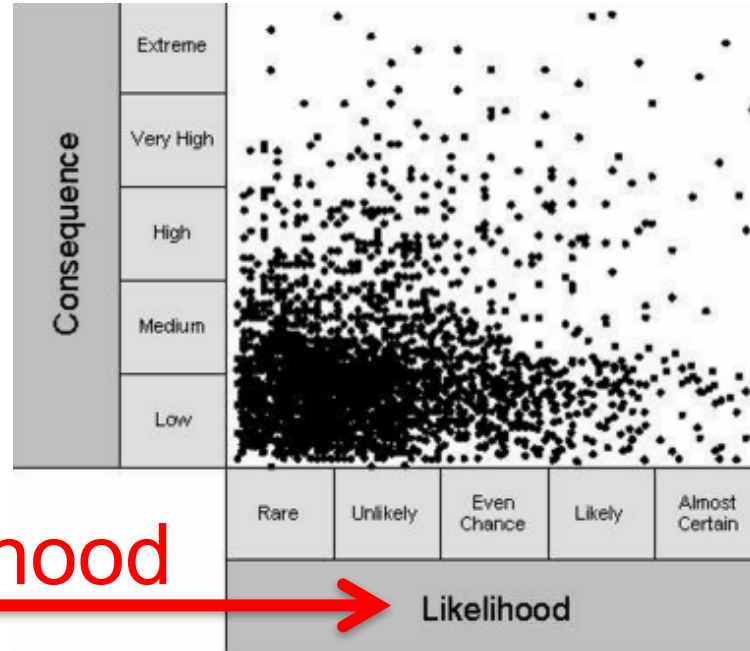
Threats

Prefatory First Principle Statements



Risk Matrix

Prefatory First Principle Statements

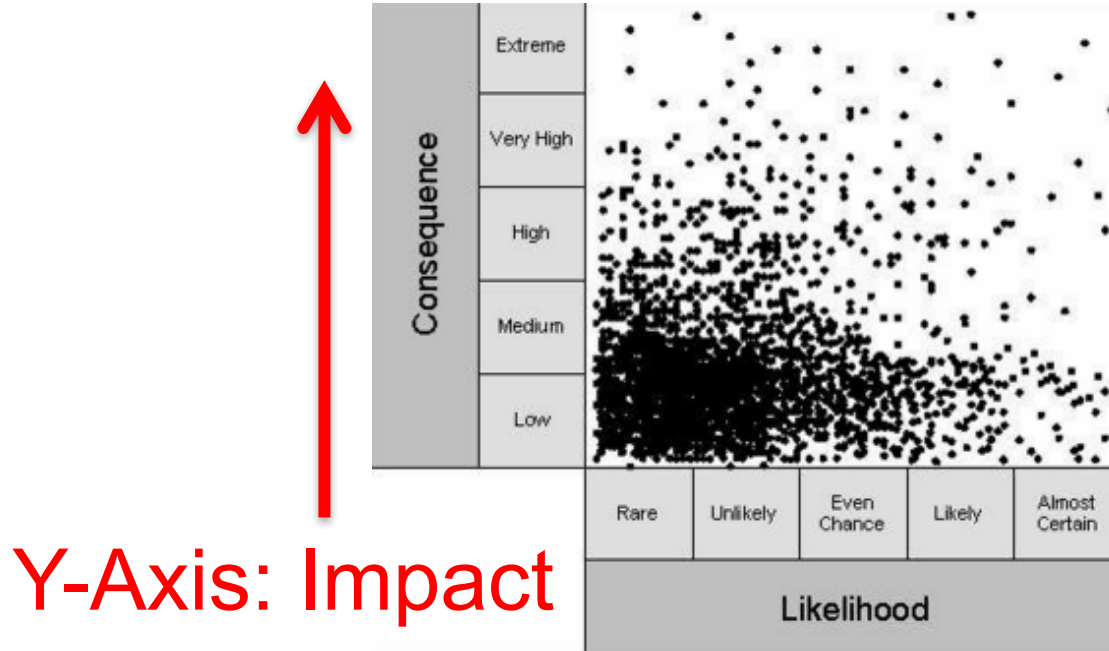


X-Axis: Likelihood



Risk Matrix

Prefatory First Principle Statements



Y-Axis: Impact

Risk Matrix

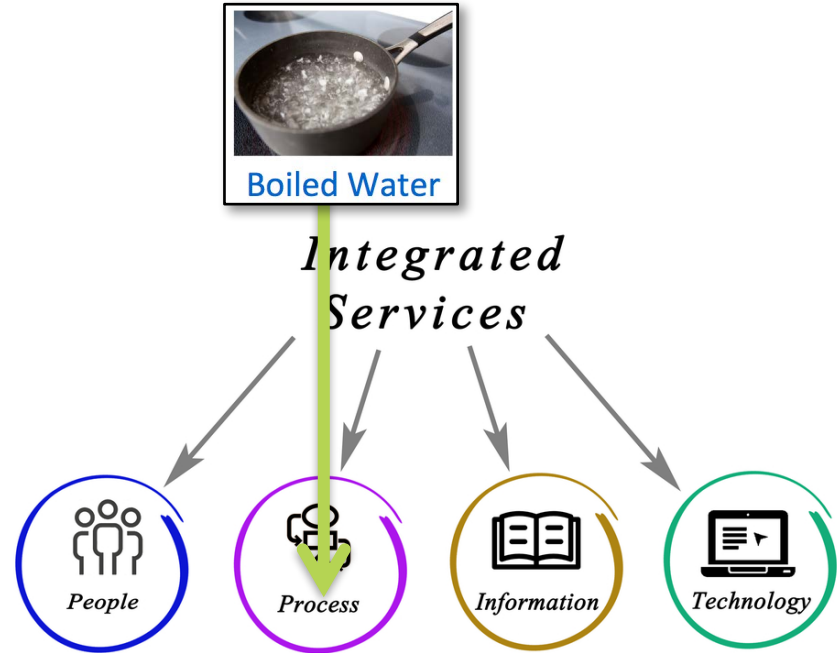
What is a Network Defender First Principle?



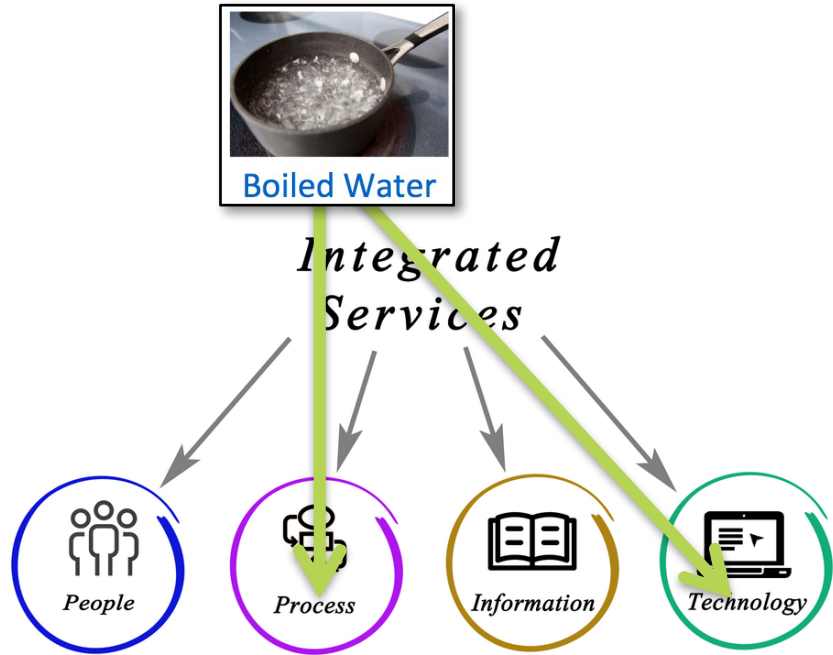
What is a Network Defender First Principle?



What is a Network Defender First Principle?



What is a Network Defender First Principle?



What is a Network Defender First Principle?



What is a Network Defender First Principle?



What is a Network Defender First Principle?



What is a Network Defender First Principle?



What is it?

What is a Network Defender First Principle?



What is it?

What should it be?

What is a Network Defender First Principle?



What is it?

What should it be?

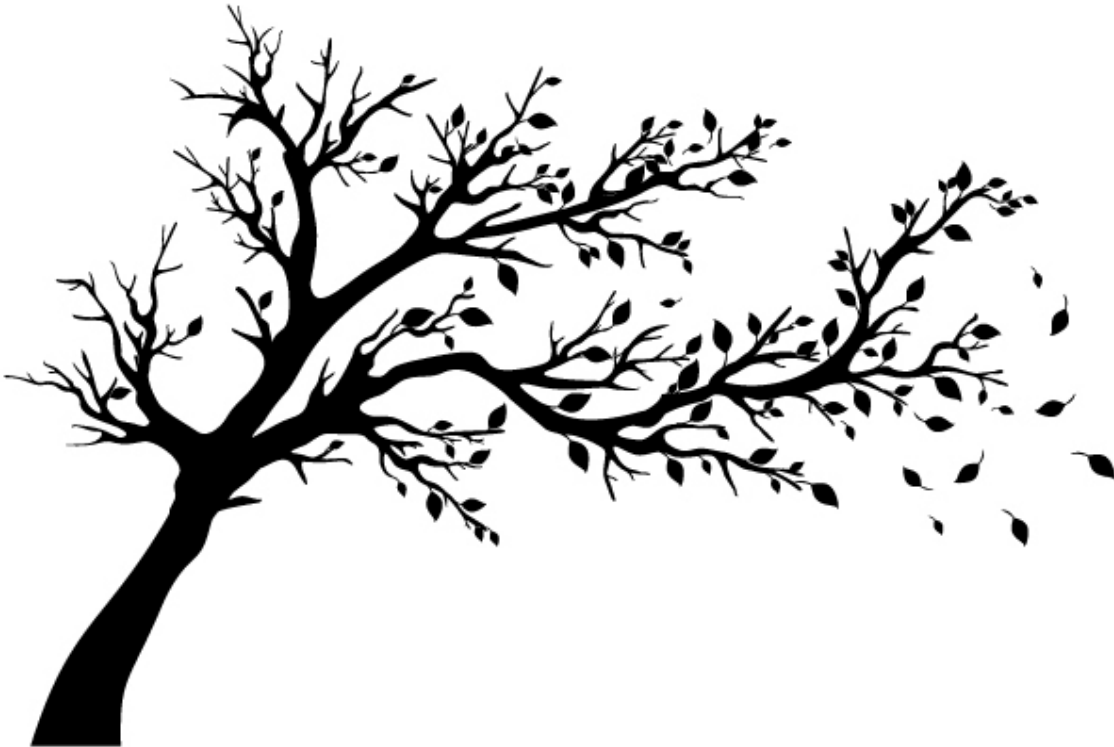
What do we agree that it should it be?

What is a Network Defender First Principle?

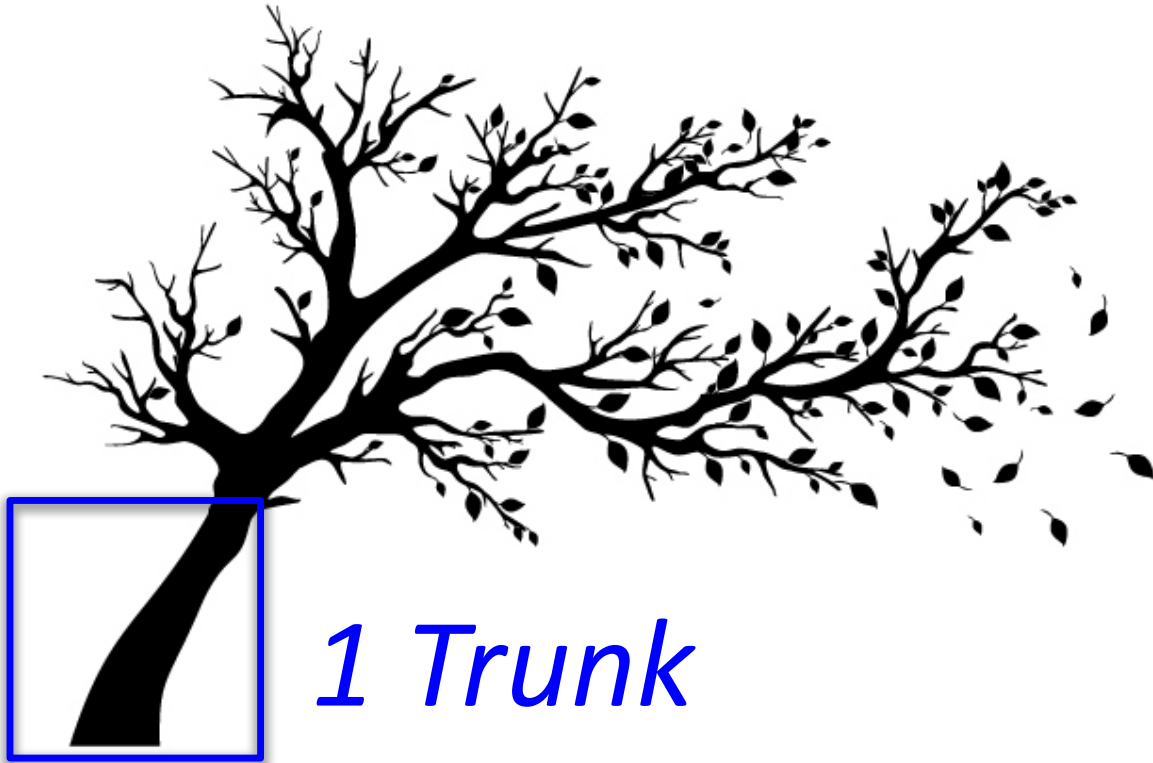


“We must identify the trunk and the big branches first so that when we discover the leaves later, we will have something to hang them on.”

Network Defender Semantic Tree



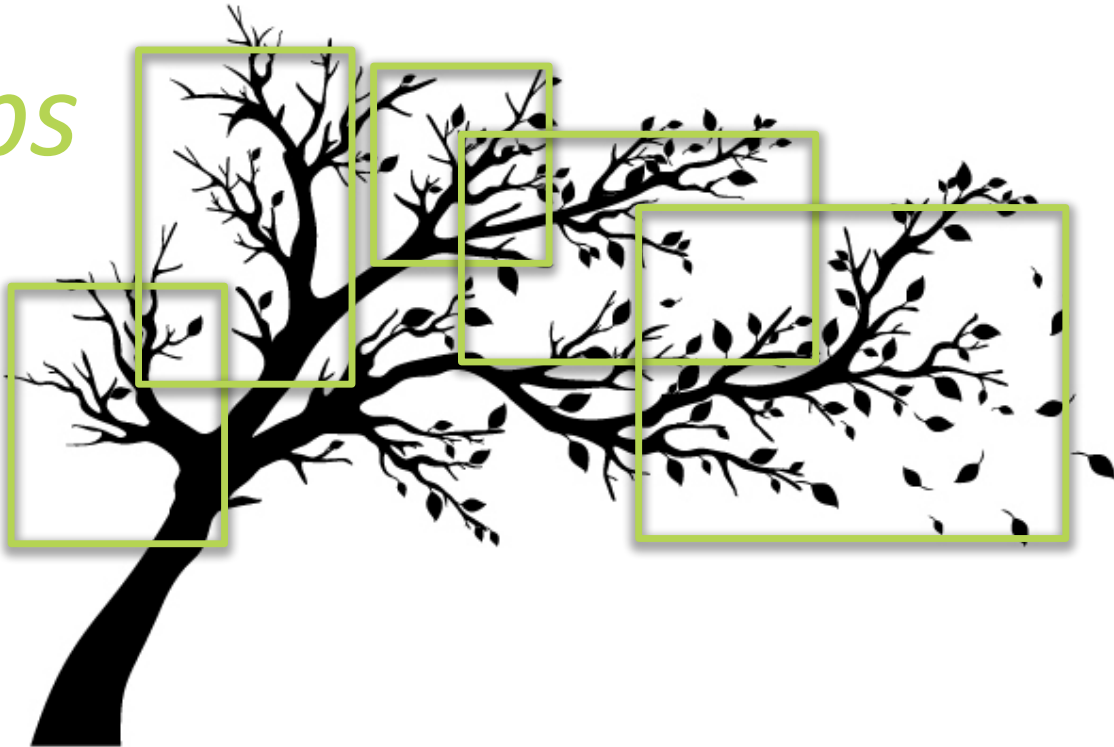
Network Defender Semantic Tree



1 Trunk

Network Defender Semantic Tree

5 Limbs



Network Defender Semantic Tree

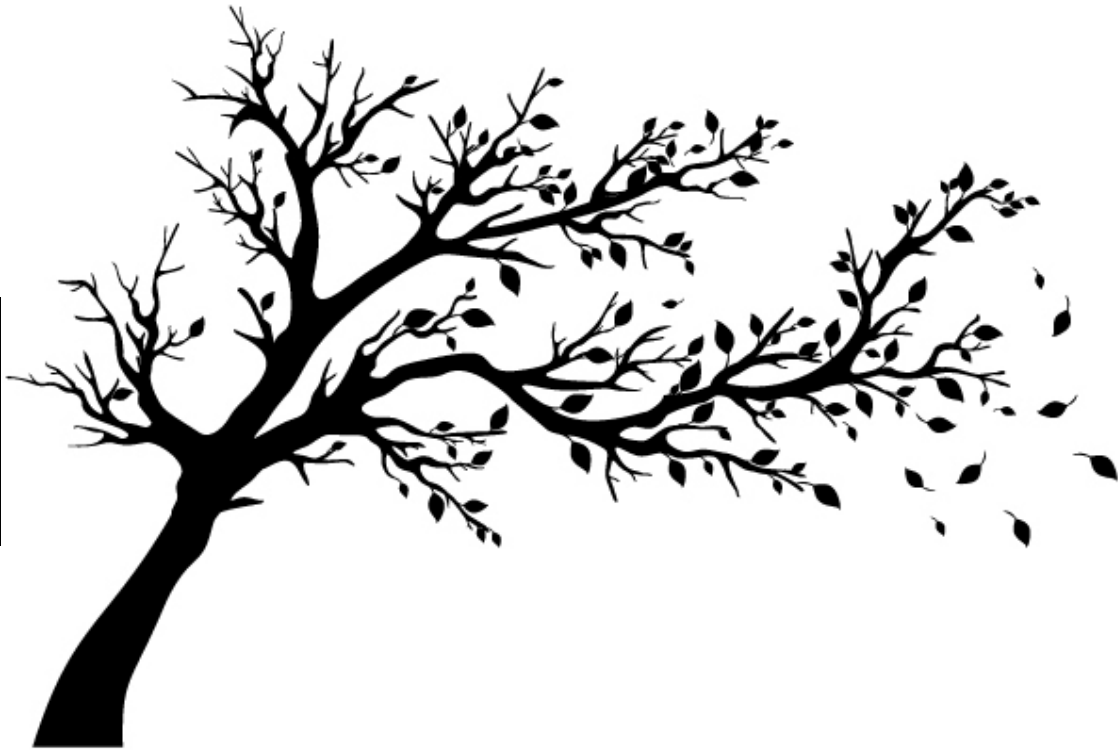
Leaves



The Trunk



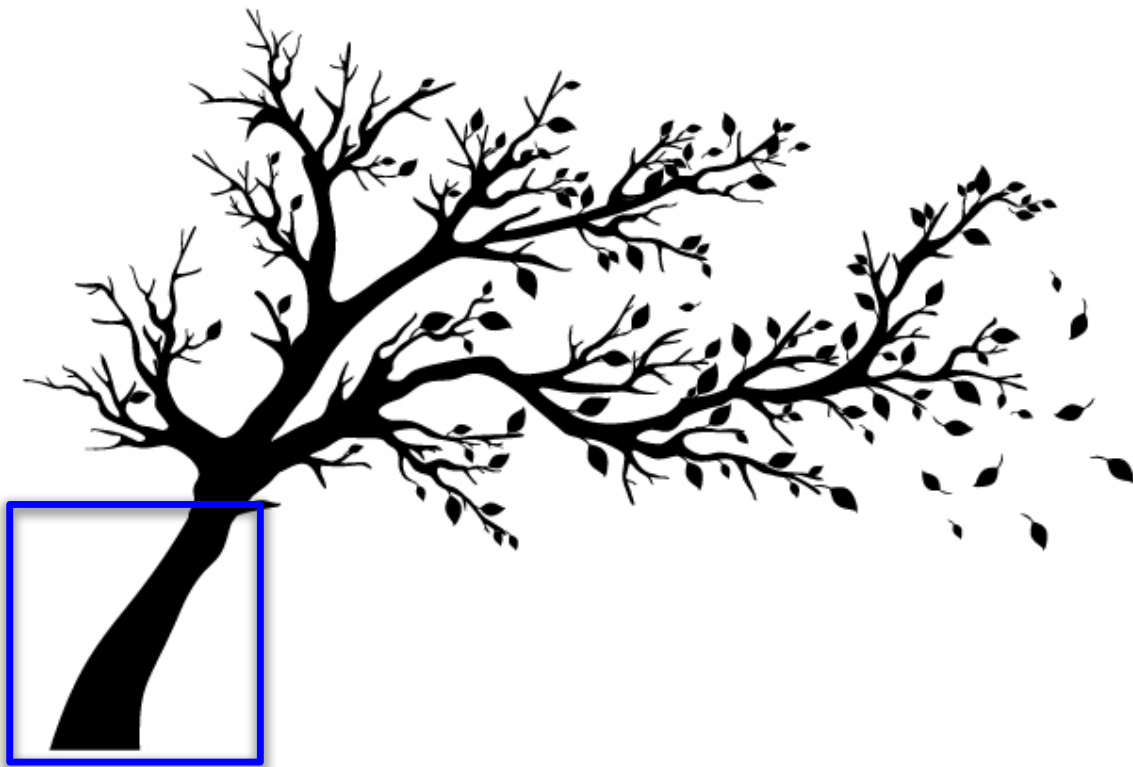
Network Defender Semantic Tree: *The Trunk*



Network Defender Semantic Tree: *The Trunk*



Network Defender Semantic Tree: *The Trunk*



Trunk

Network Defender Semantic Tree: *The Trunk*

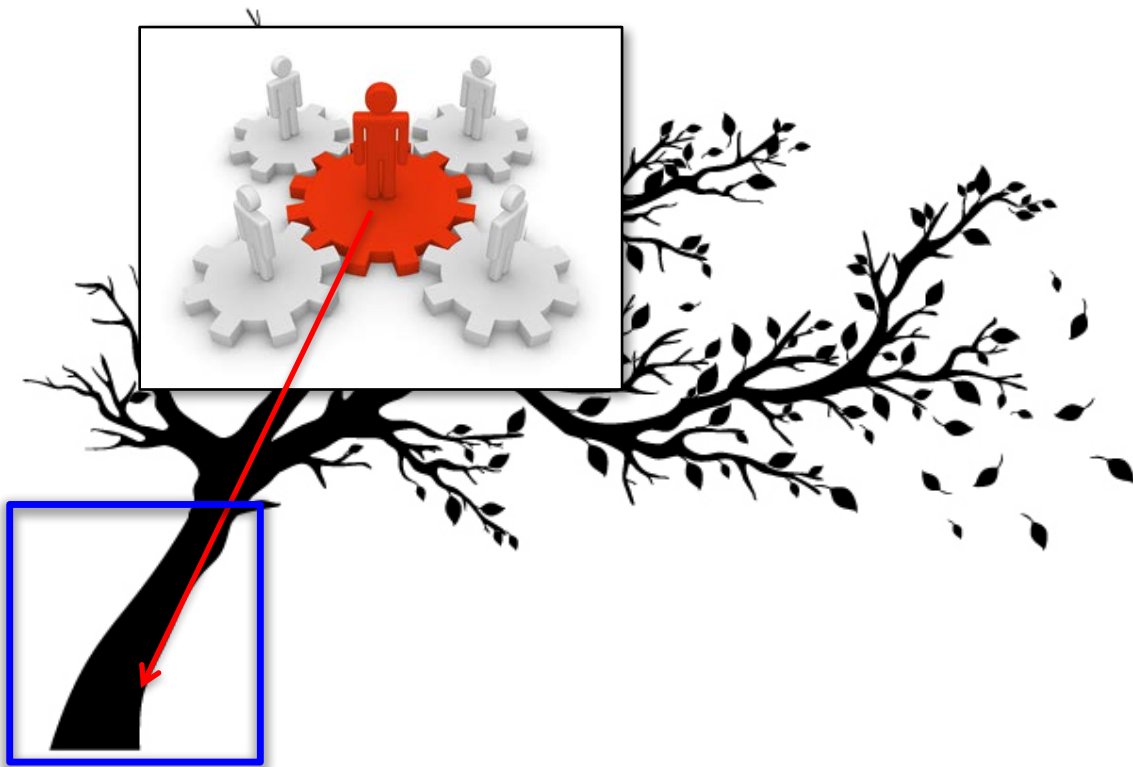


Trunk

Prevent High Risk Material Impact

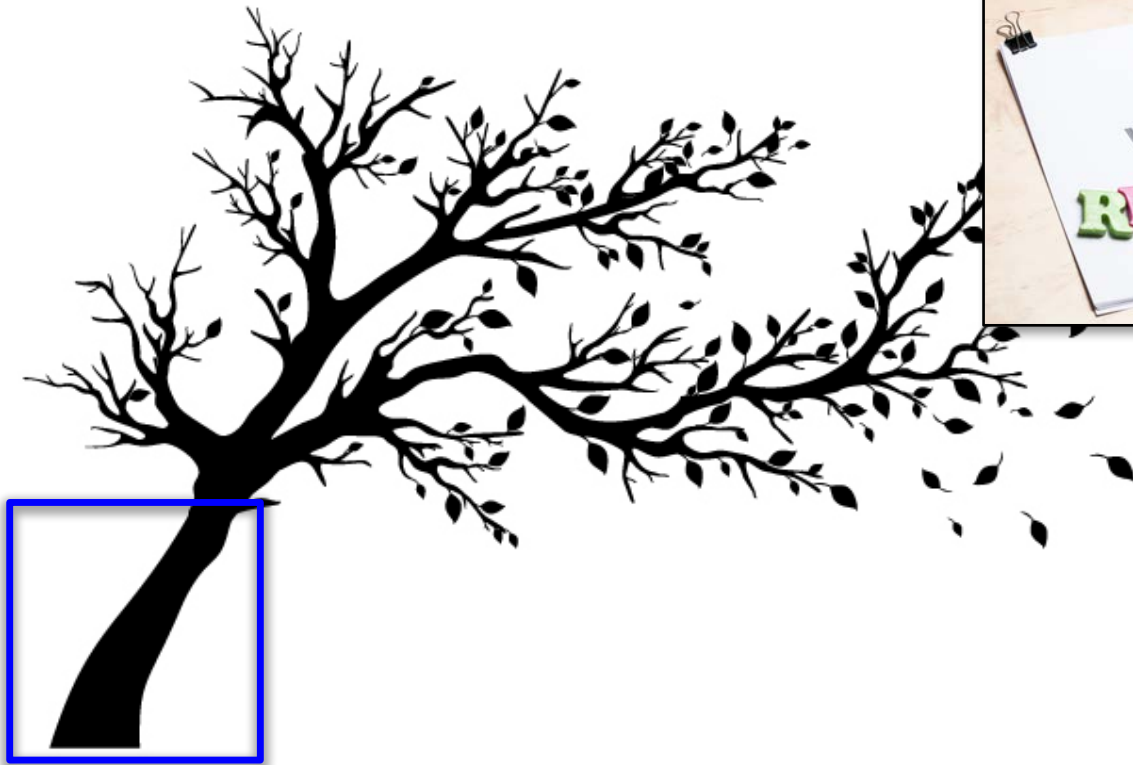


Network Defender Semantic Tree: *The Trunk*



Trunk

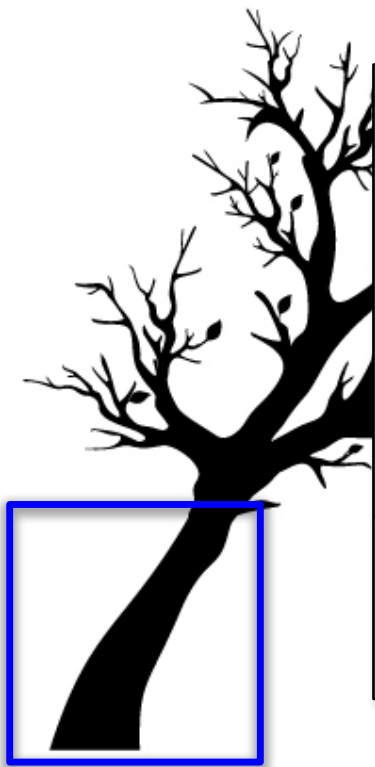
Network Defender Semantic Tree: *The Trunk*



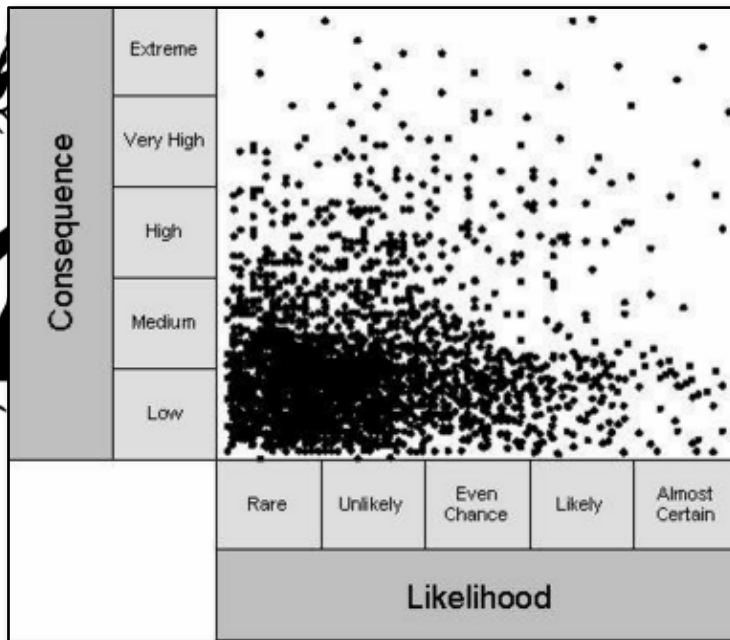
Trunk



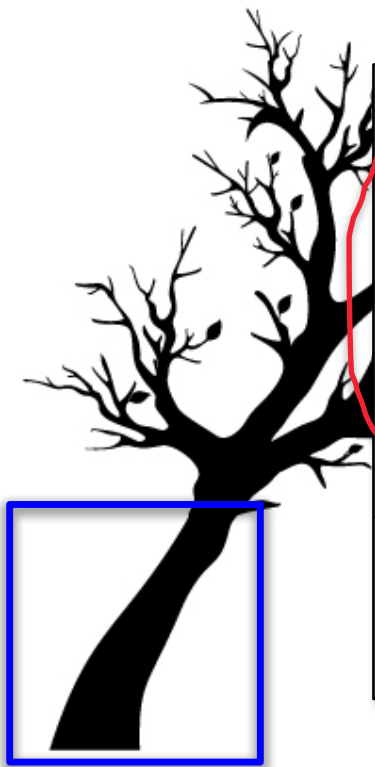
Network Defender Semantic Tree: *The Trunk*



Trunk



Network Defender Semantic Tree: *The Trunk*

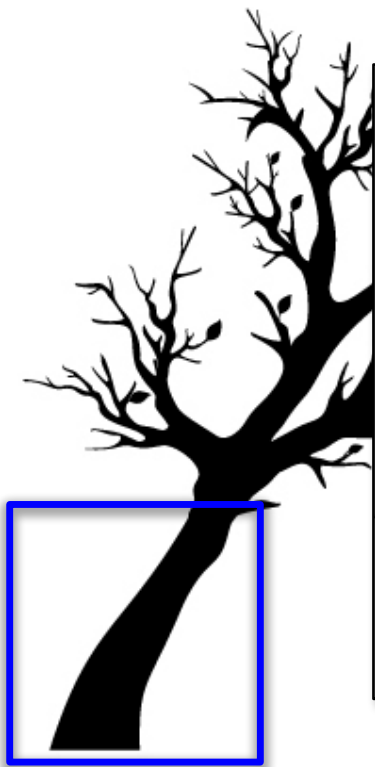


Trunk

Consequence	Extreme	[Scatter plot of black dots]				
	Very High	[Scatter plot of black dots]				
	High	[Scatter plot of black dots]				
	Medium	[Scatter plot of brown dots]				
	Low	[Scatter plot of brown dots]				
		Rare	Unlikely	Even Chance	Likely	Almost Certain
		Likelihood				



Network Defender Semantic Tree: *The Trunk*

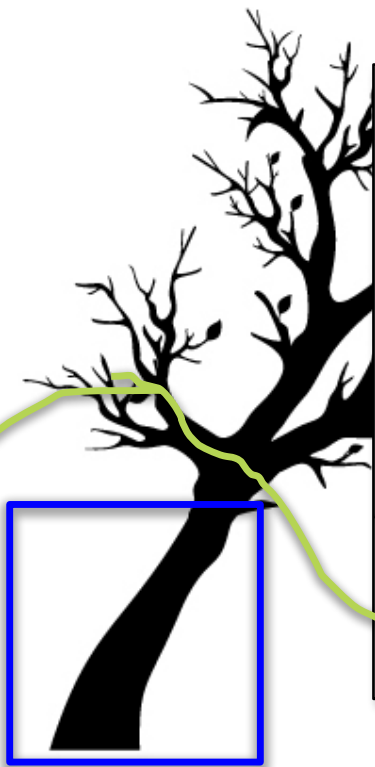


Trunk

Consequence	Extreme	[Visual representation of risk distribution]				
	Very High	[Visual representation of risk distribution]				
	High	[Visual representation of risk distribution]				
	Medium	[Visual representation of risk distribution]				
	Low	[Visual representation of risk distribution]				
		Rare	Unlikely	Even Chance	Likely	Almost Certain
		Likelihood				



Network Defender Semantic Tree: *The Trunk*



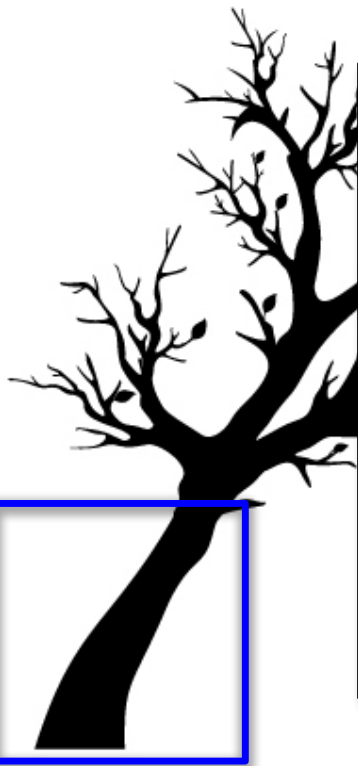
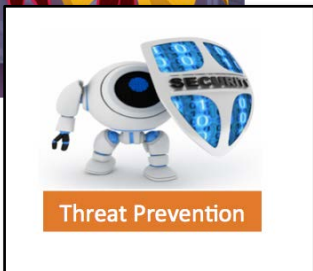
Trunk

Consequence	Extreme	[Visual representation of Extreme consequence]				
	Very High	[Visual representation of Very High consequence]				
	High	[Visual representation of High consequence]				
	Medium	[Visual representation of Medium consequence]				
	Low	[Visual representation of Low consequence]				
		Rare	Unlikely	Even Chance	Likely	Almost Certain
		Likelihood				



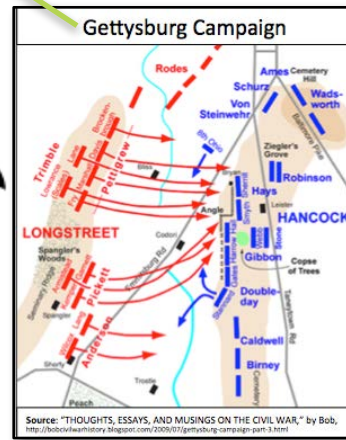
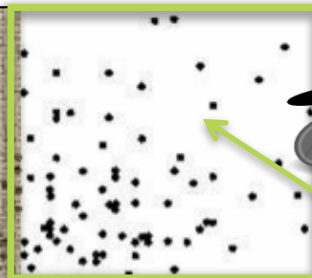
Network Defender Semantic Tree: *The Trunk*

Network Defenders



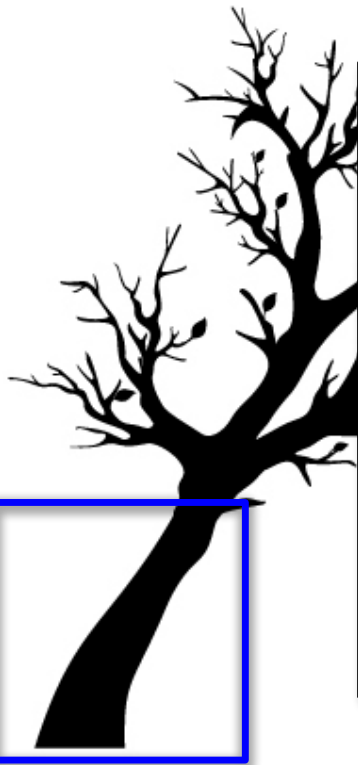
Trunk

Consequence	Extreme					
	Very High					
	High					
	Medium					
	Low					
		Rare	Unlikely	Even Chance	Likely	Almost Certain
		Likelihood				



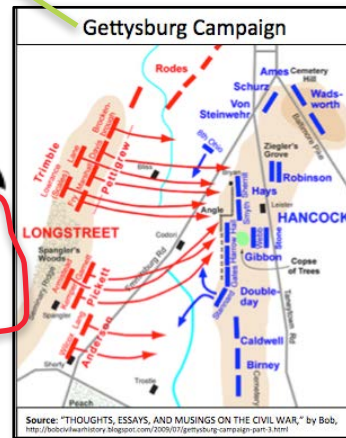
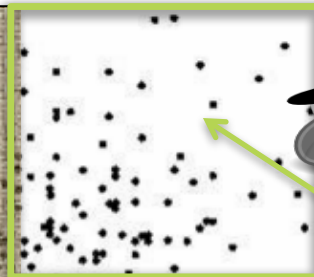
Network Defender Semantic Tree: *The Trunk*

Network Defenders



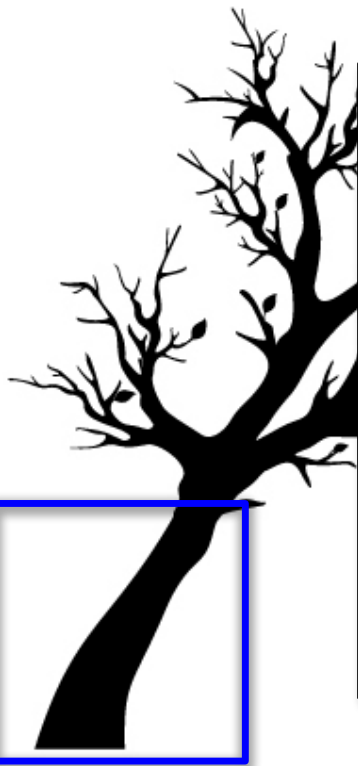
Trunk

Consequence	Extreme					
	Very High					
	High					
	Medium					
	Low					
		Rare	Unlikely	Even Chance	Likely	Almost Certain
		Likelihood				

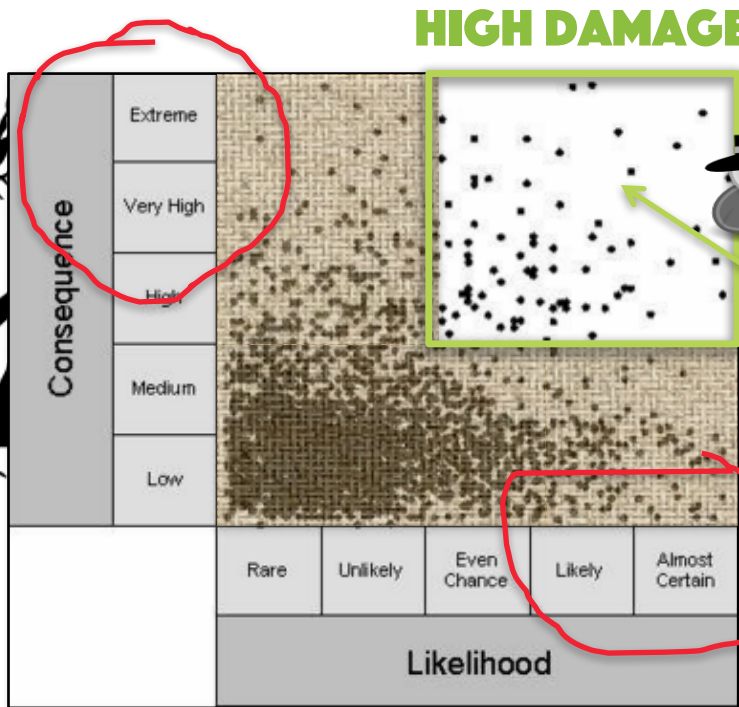


HIGH PROBABILITY

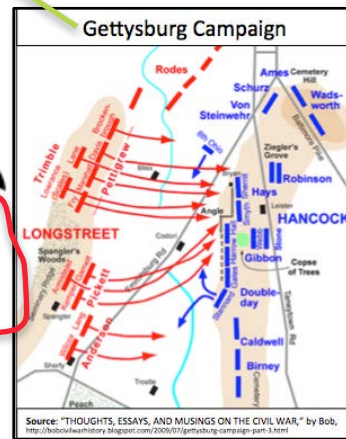
Network Defender Semantic Tree: *The Trunk*



Trunk

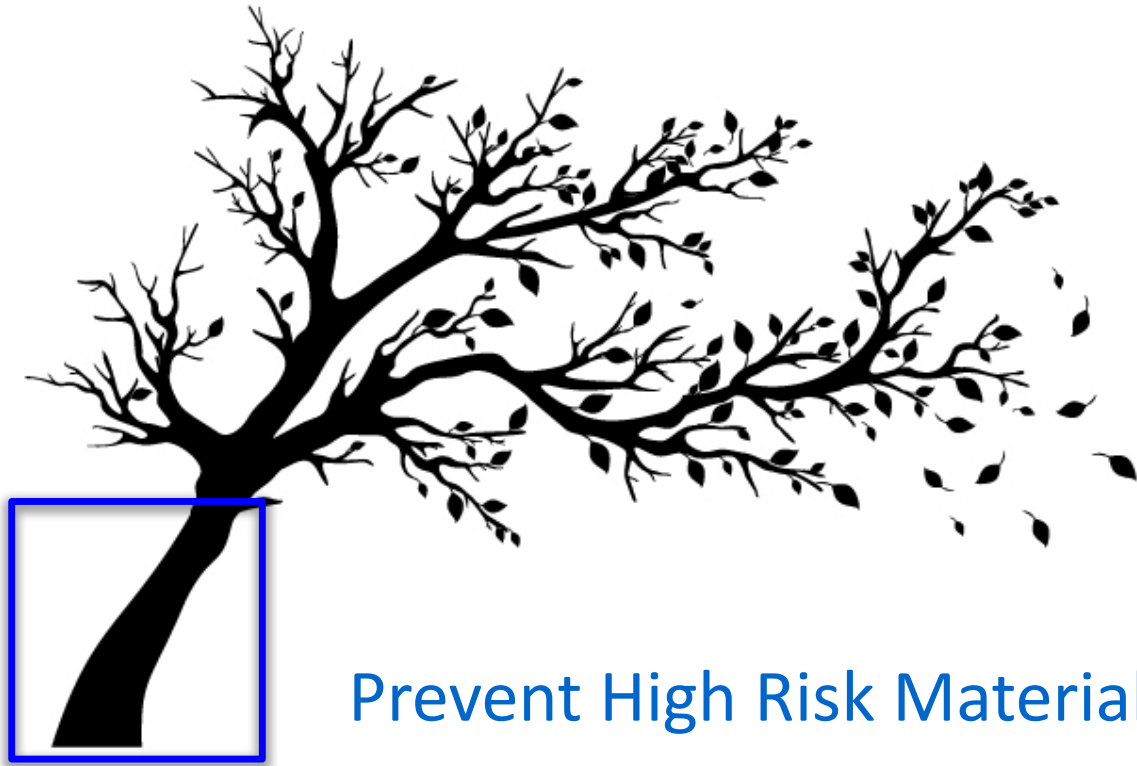


HIGH DAMAGE



HIGH PROBABILITY

Network Defender Semantic Tree: *The Trunk*

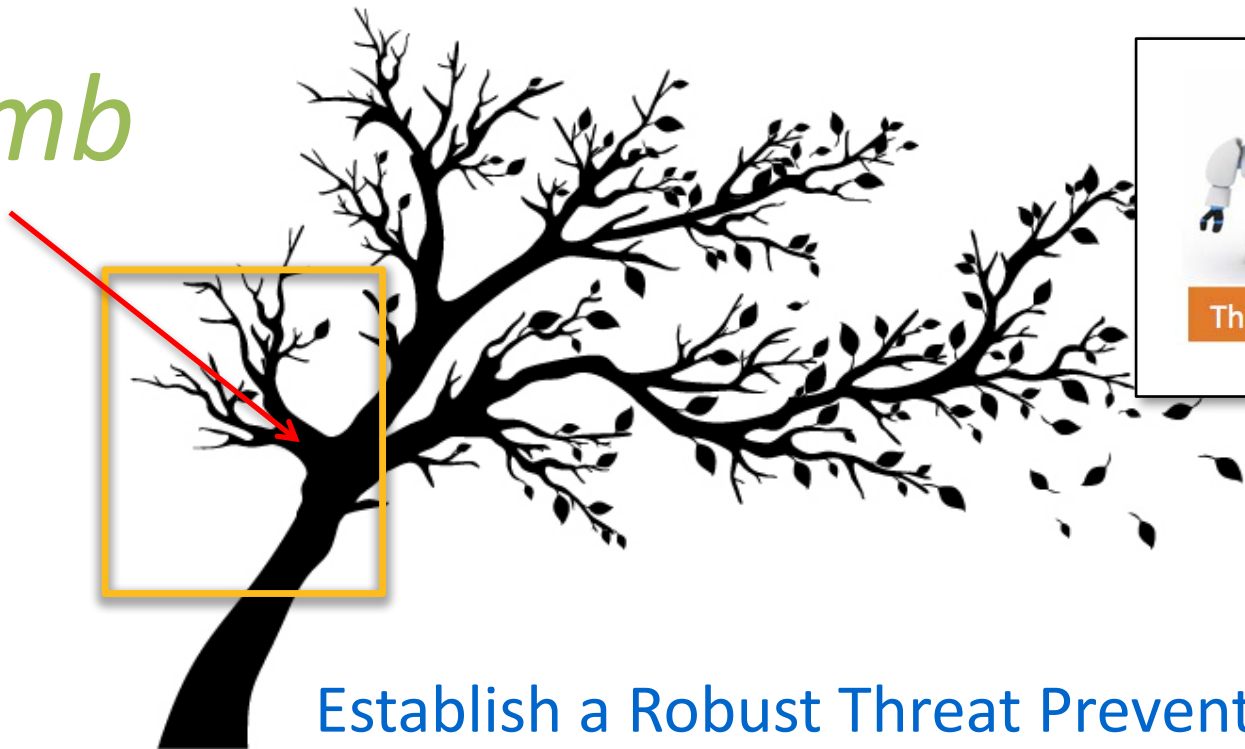


The First Limb



Network Defender Semantic Tree: *First Limb*

Limb



Establish a Robust Threat Prevention program

Network Defender Semantic Tree: *First Limb*



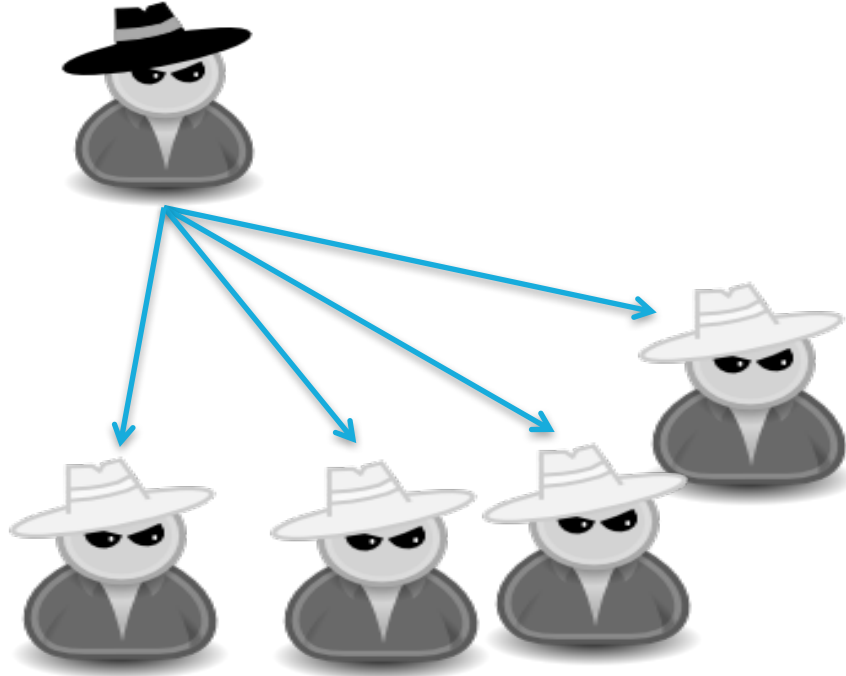
Network Defender Semantic Tree: *First Limb*



Network Defender Semantic Tree: *First Limb*



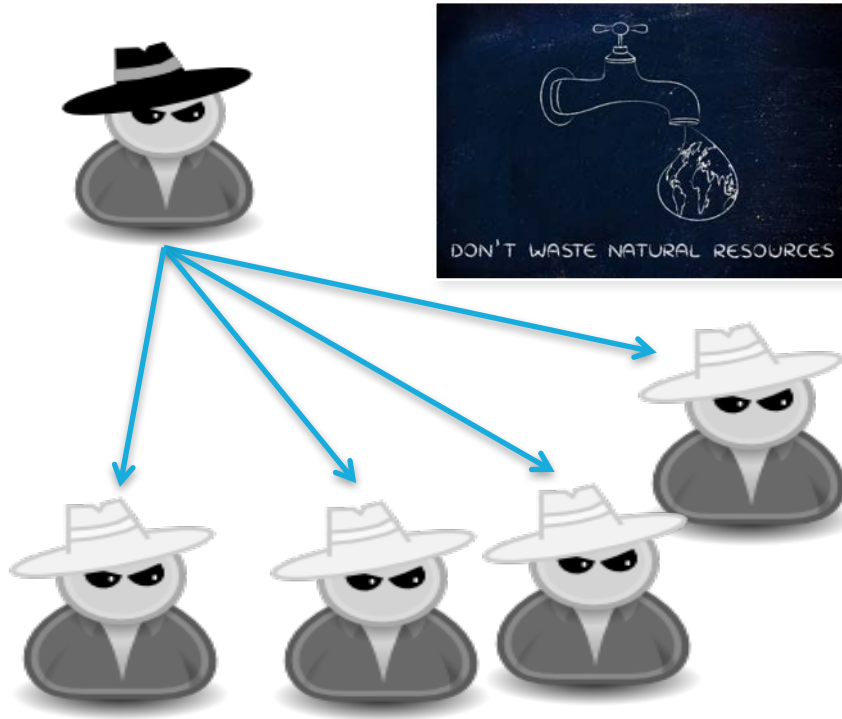
NEW



Network Defender Semantic Tree: *First Limb*



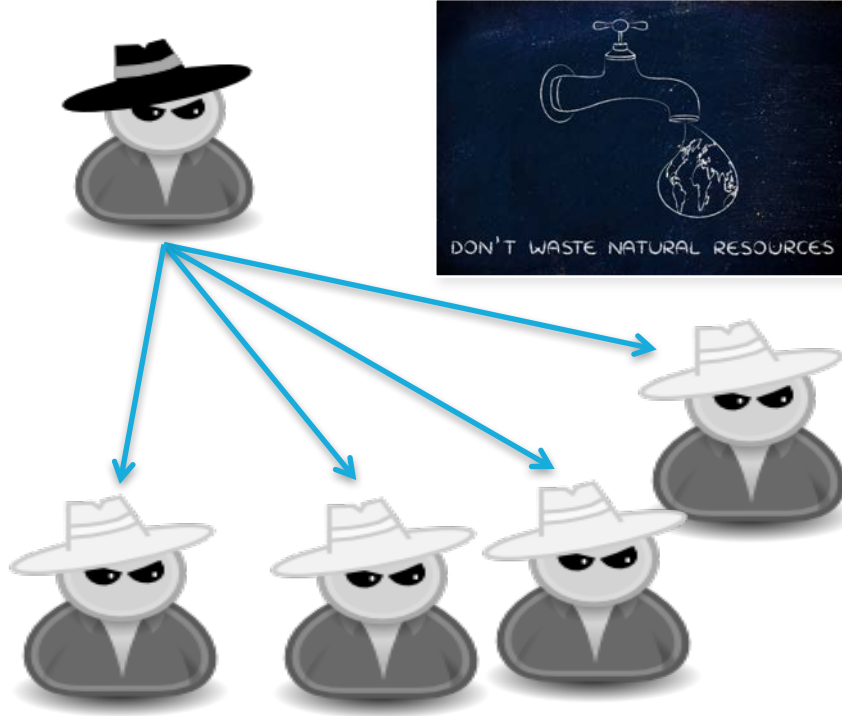
NEW



Network Defender Semantic Tree: *First Limb*



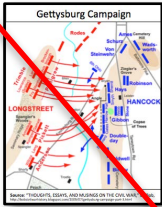
NEW



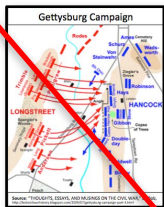
Network Defender Semantic Tree: *First Limb*



Network Defender Semantic Tree: *First Limb*



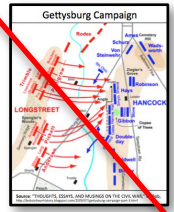
Network Defender Semantic Tree: *First Limb*



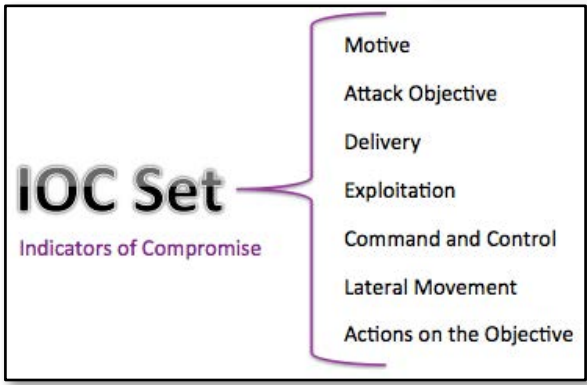
Victim



Network Defender Semantic Tree: *First Limb*



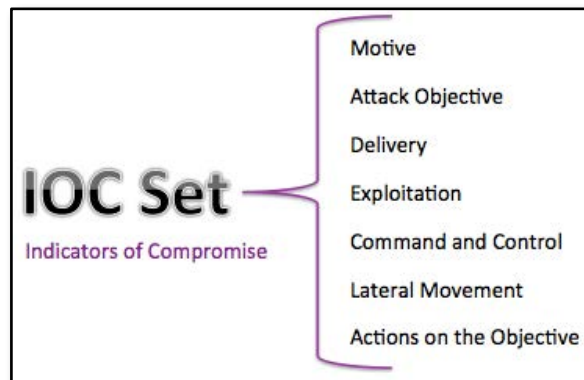
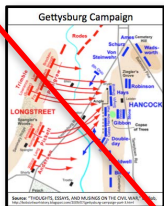
Victim



Network Defender Semantic Tree: *First Limb*



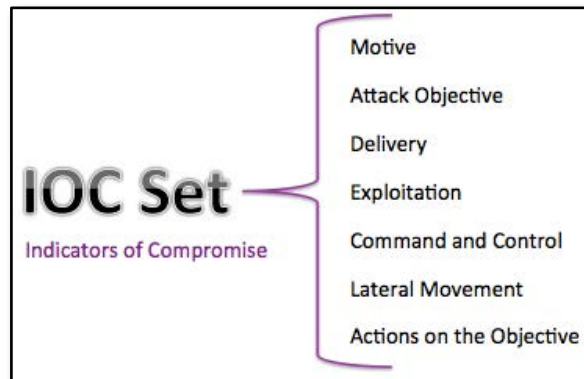
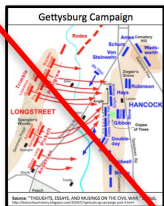
Indicators of Compromise are forensic artifacts that describe an adversary's methodology; digital clues left behind by the adversary group as it works its way through the phases of the **attack lifecycle**.



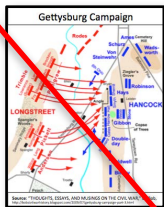
Network Defender Semantic Tree: *First Limb*



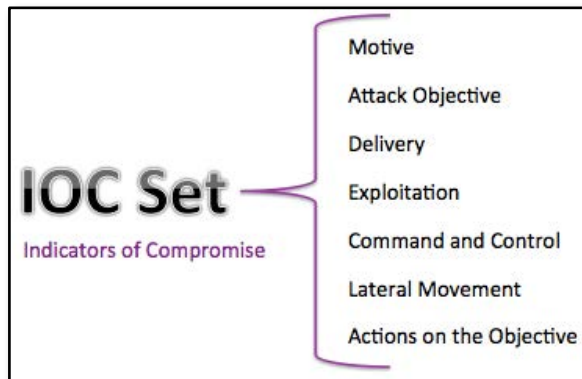
Indicators of Compromise are forensic artifacts that describe an adversary's methodology; digital clues left behind by the adversary group as it works its way through the phases of the **attack lifecycle**.



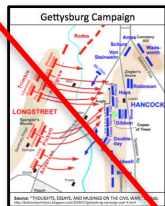
Network Defender Semantic Tree: *First Limb*



Indicators of Compromise are forensic artifacts that describe an adversary's methodology; digital clues left behind by the adversary group as it works its way through the phases of the **attack lifecycle**.



Network Defender Semantic Tree: *First Limb*



Gather Intelligence

Leverage Exploit

Execute Malware

Control Channel

Steal Data

Plan the Attack

Silent Infection

Malicious File Executed

Malware Communicates with Attacker

Data Theft, Sabotage, Destruction

Preventive Controls

Reactive Controls

The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: *First Limb*



Gather Intelligence

Leverage Exploit

Execute Malware

Control Channel

Steal Data

Plan the Attack

Silent Infection

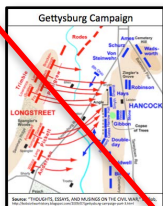
Malicious File Executed

Malware Communicates with Attacker

Data Theft, Sabotage, Destruction

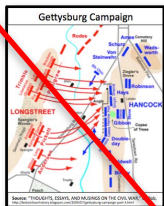
Preventive Controls

Reactive Controls



The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: *First Limb*



Gather Intelligence

Leverage Exploit

Execute Malware

Control Channel

Steal Data

Plan the Attack

Silent Infection

Malicious File Executed

Malware Communicates with Attacker

Data Theft, Sabotage, Destruction

Preventive Controls

Reactive Controls

The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: *First Limb*



Plan the Attack

Silent Infection

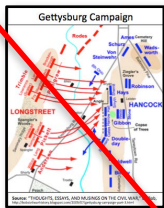
Malicious File Executed

Malware Communicates with Attacker

Data Theft, Sabotage, Destruction

Preventive Controls

Reactive Controls



The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: *First Limb*



Plan the Attack

Silent Infection

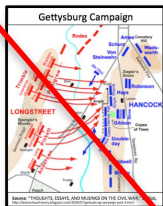
Malicious File Executed

Malware Communicates with Attacker

Data Theft, Sabotage, Destruction

Preventive Controls

Reactive Controls



The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: *First Limb*



Plan the Attack

Silent Infection

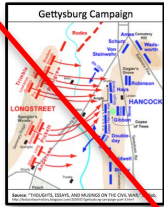
Malicious File Executed

Malware Communicates with Attacker

Data Theft, Sabotage, Destruction

Preventive Controls

Reactive Controls



The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: *First Limb*



Gather Intelligence

Leverage Exploit

Execute Malware

Control Channel

Steal Data

Plan the Attack

Silent Infection

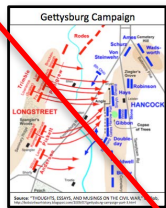
Malicious File Executed

Malware Communicates with Attacker

Data Theft, Sabotage, Destruction

Preventive Controls

Reactive Controls



The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: *First Limb*



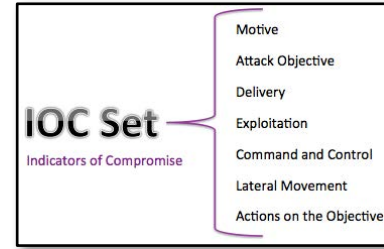
Network Defender Semantic Tree: *First Limb*



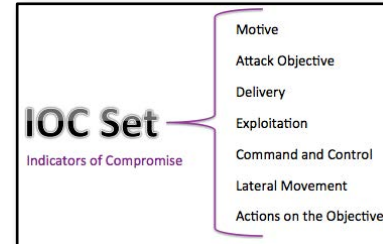
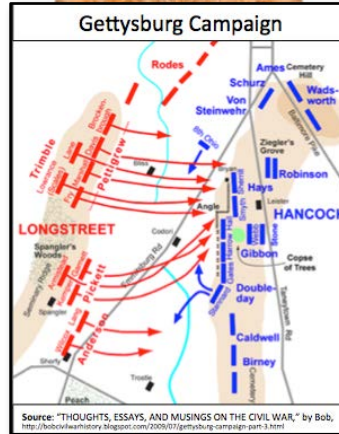
Network Defender Semantic Tree: *First Limb*



Network Defender Semantic Tree: *First Limb*

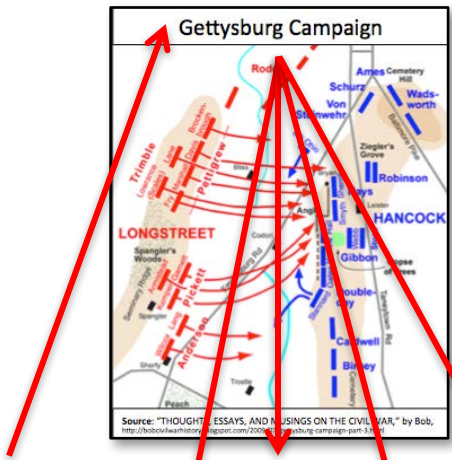


Network Defender Semantic Tree: *First Limb*



Network Defender Semantic Tree: *First Limb*

Coach's Playbook



IOC Set
Indicators of Compromise

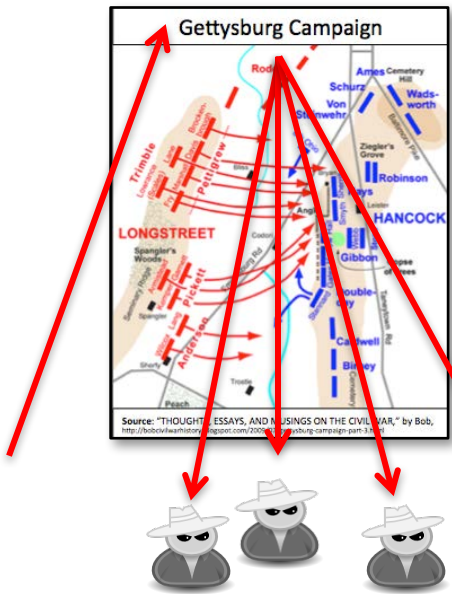
- Motive
- Attack Objective
- Delivery
- Exploitation
- Command and Control
- Lateral Movement
- Actions on the Objective

Network Defender Semantic Tree: *First Limb*

Coach's Playbook



A circular logo with three green arrows forming a cycle, containing the text "REUSE REDUCE RECYCLE".



IOC Set
Indicators of Compromise

- Motive
- Attack Objective
- Delivery
- Exploitation
- Command and Control
- Lateral Movement
- Actions on the Objective



Network Defender Community

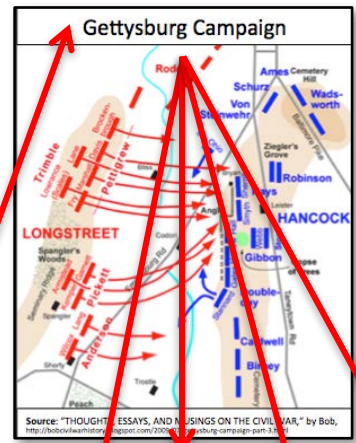
A box containing a hacker icon at the top and a group of colorful human figures below it, representing a community.

Network Defender Semantic Tree: *First Limb*

Coach's Playbook



A circular logo with three green arrows forming a triangle, containing the words REUSE, REDUCE, and RECYCLE.



MOST

IOC Set
Indicators of Compromise

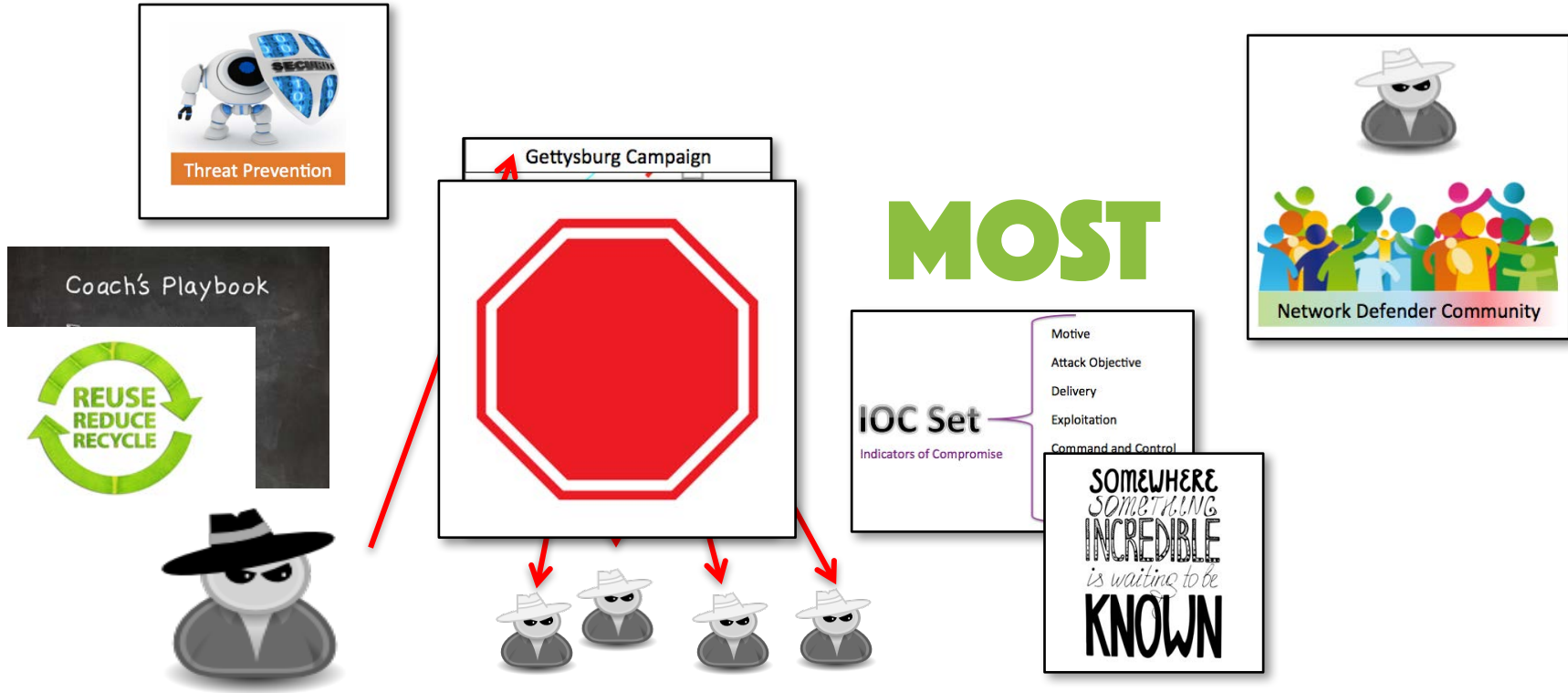
- Motive
- Attack Objective
- Delivery
- Exploitation
- Command and Control

SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN



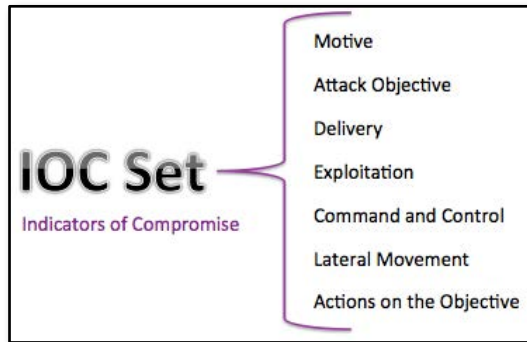
Network Defender Community

Network Defender Semantic Tree: *First Limb*

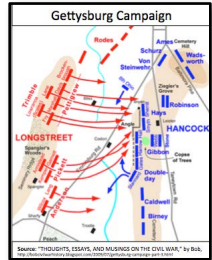


Threat Prevention is the act of turning known indicators of compromise into one or more deployed **prevention controls**.

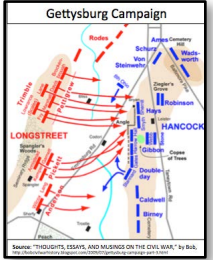
Threat Prevention is the act of turning known indicators of compromise into one or more deployed **prevention controls**.



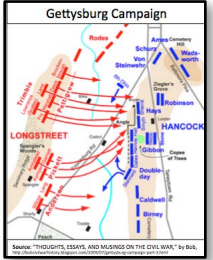
Network Defender Semantic Tree: *First Limb*



Network Defender Semantic Tree: *First Limb*

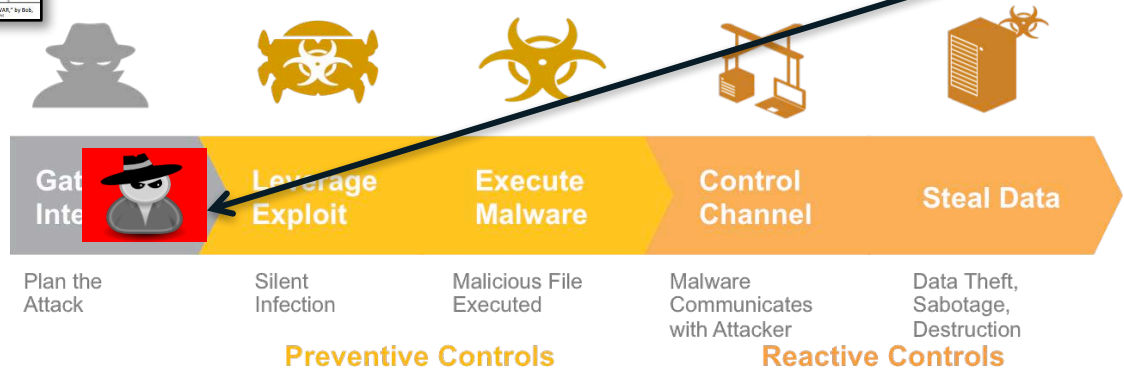
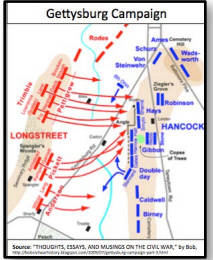


Network Defender Semantic Tree: *First Limb*

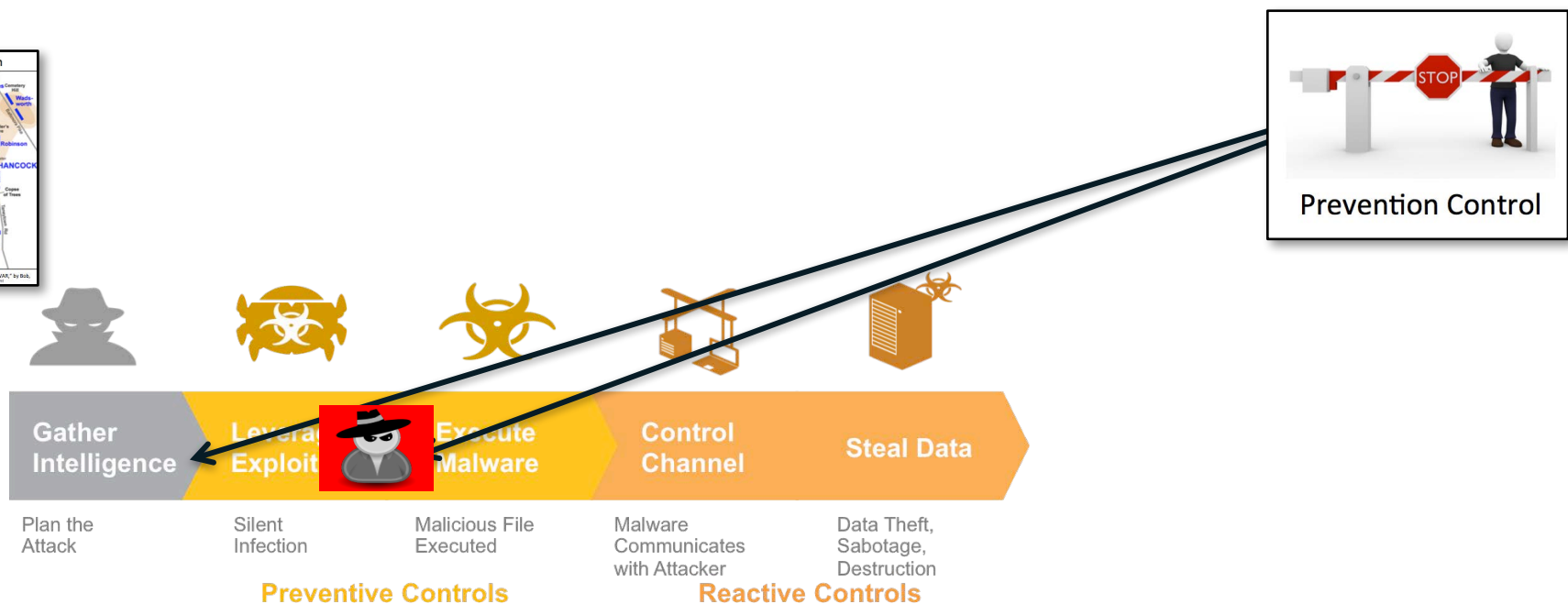
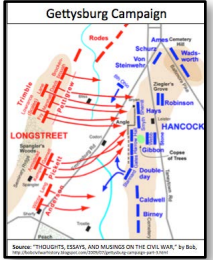


PRECISION

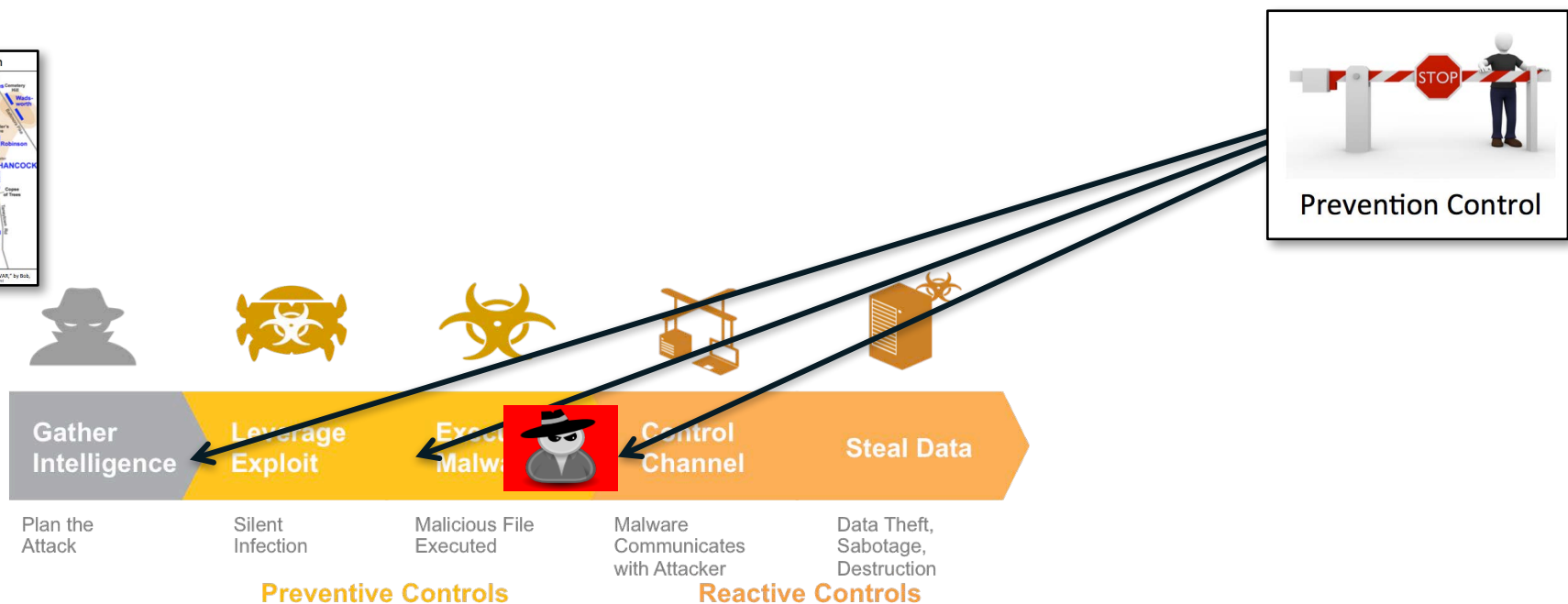
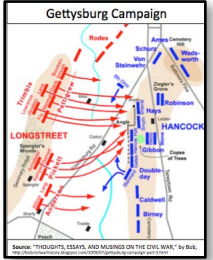
Network Defender Semantic Tree: *First Limb*



Network Defender Semantic Tree: *First Limb*



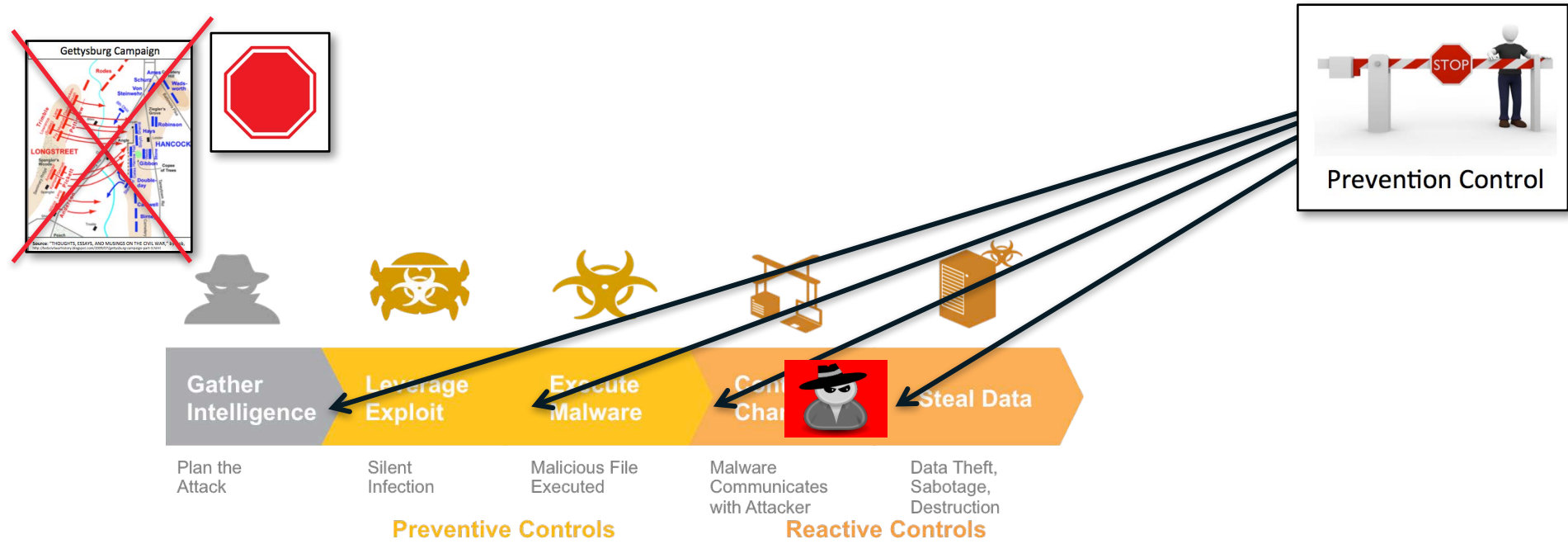
Network Defender Semantic Tree: *First Limb*



99% GUARANTEE

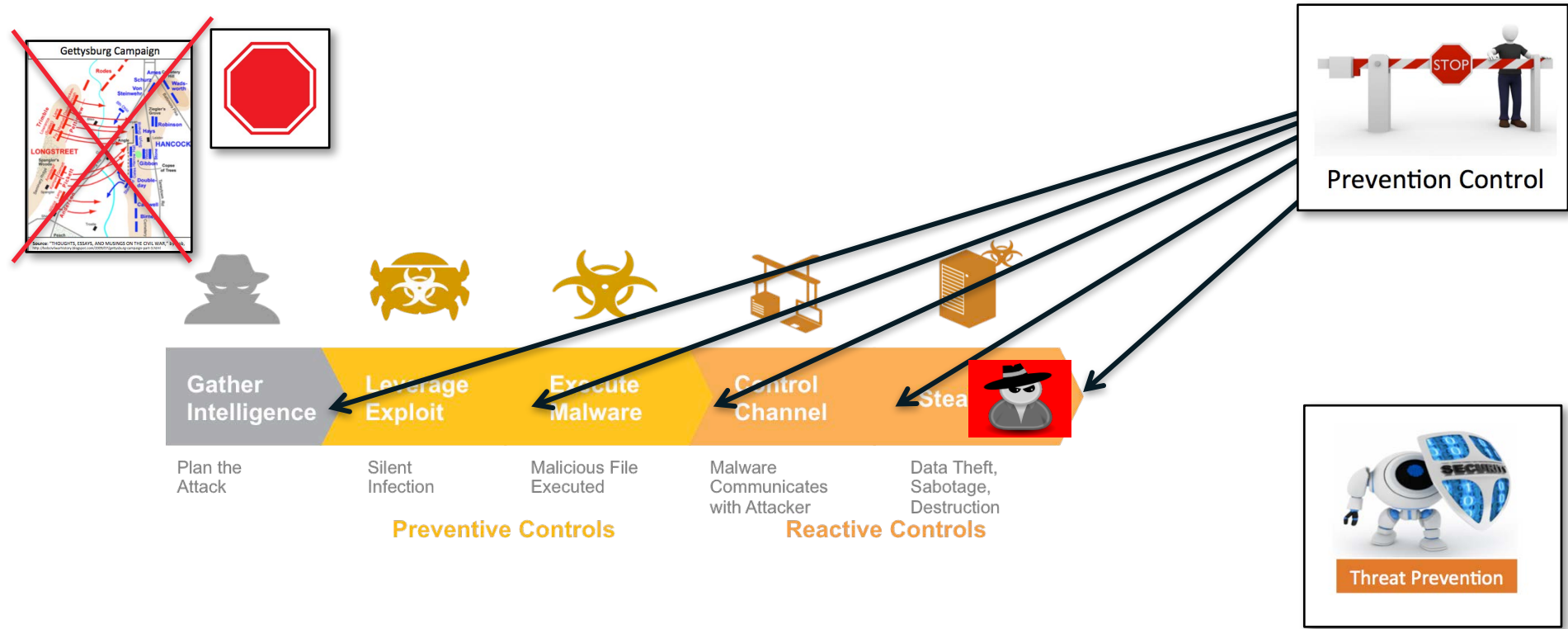


Network Defender Semantic Tree: *First Limb*



99% GUARANTEE

Network Defender Semantic Tree: *First Limb*



Network Defender Semantic Tree: *First Limb*

1st Limb



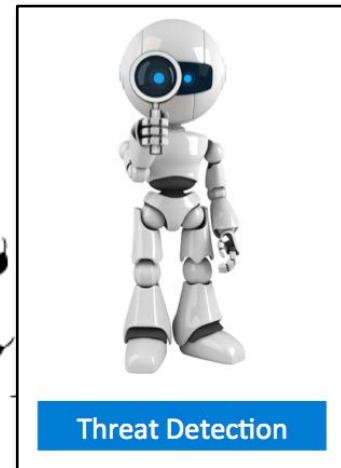
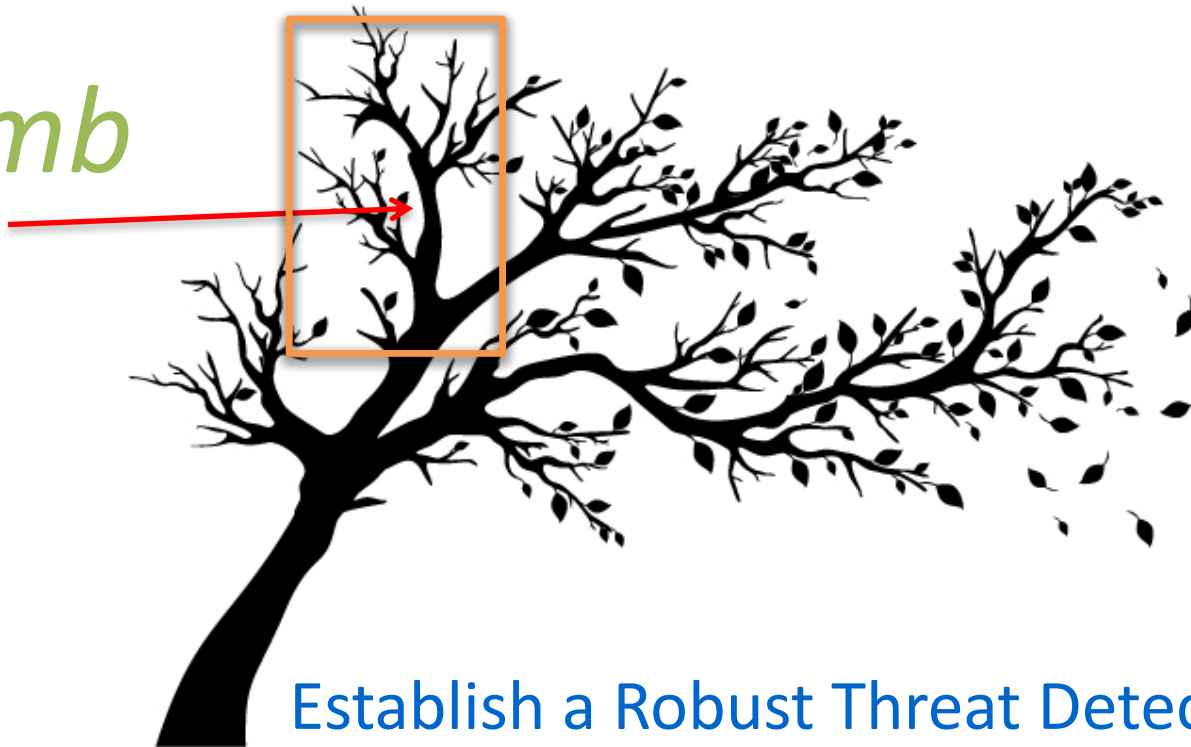
Establish a Robust Threat Prevention program

The Second Limb



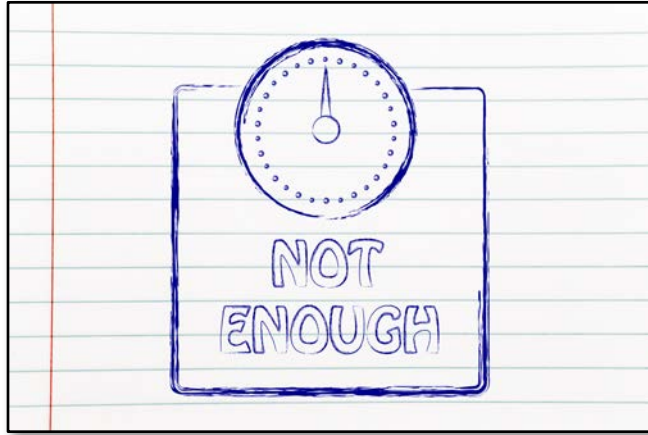
Network Defender Semantic Tree: 2d Limb

Limb

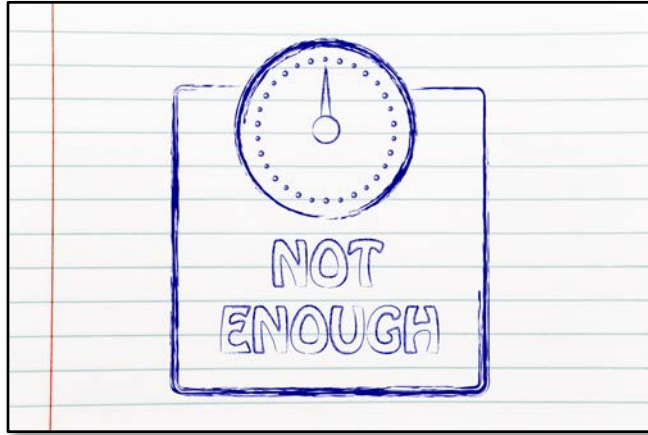


Establish a Robust Threat Detection Program

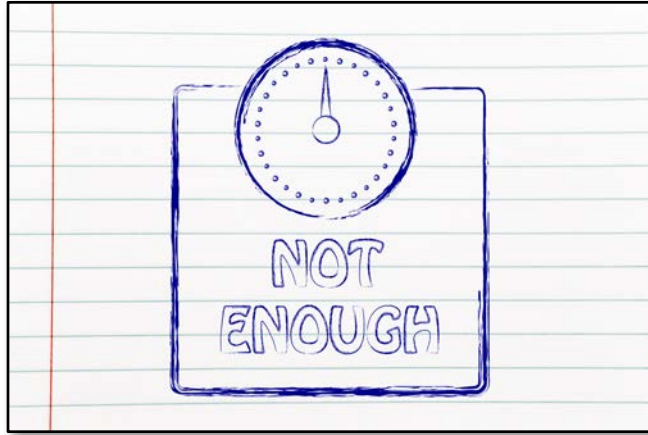
Network Defender Semantic Tree: 2d Limb



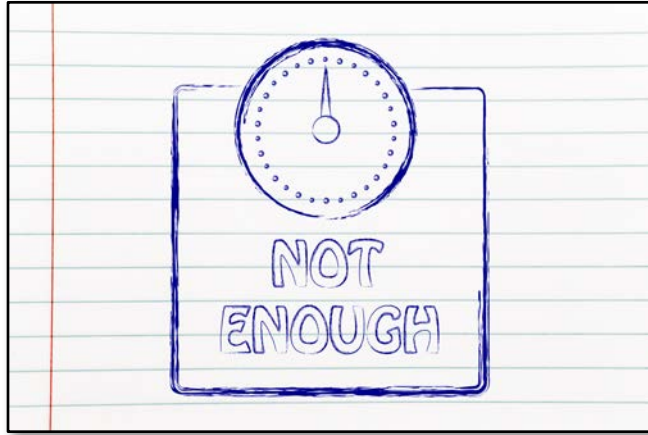
Network Defender Semantic Tree: 2d Limb



Network Defender Semantic Tree: 2d Limb



Network Defender Semantic Tree: 2d Limb



Network Defender Semantic Tree: 2d Limb



Network Defender Semantic Tree: 2d Limb



Network Defender Semantic Tree: 2d Limb



Network Defender Semantic Tree: 2d Limb



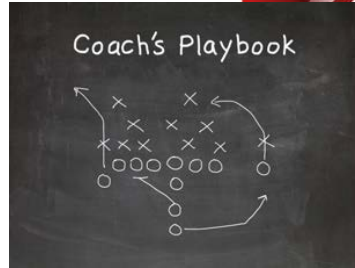
Network Defender Semantic Tree: 2d Limb

#1



Network Defender Semantic Tree: 2d Limb

#1



Network Defender Semantic Tree: 2d Limb

#1



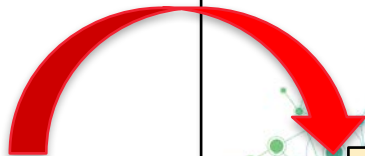
Network Defender Semantic Tree: 2d Limb

#2



Network Defender Semantic Tree: 2d Limb

#2



Network Defender Semantic Tree: 2d Limb



Threat Detection

Network Defender Semantic Tree: 2d Limb



Threat Detection



Hunting

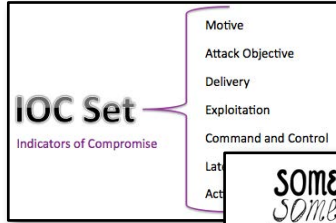
Network Defender Semantic Tree: 2d Limb



Threat Detection

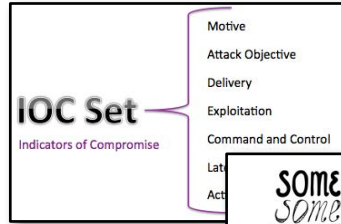


Hunting



SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN

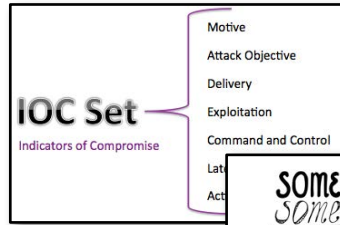
Network Defender Semantic Tree: 2d Limb



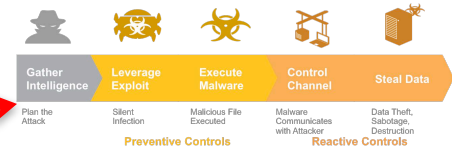
SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN



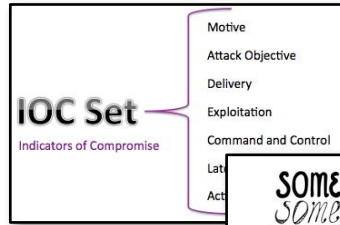
Network Defender Semantic Tree: 2d Limb



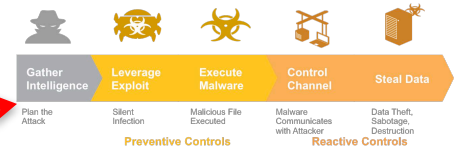
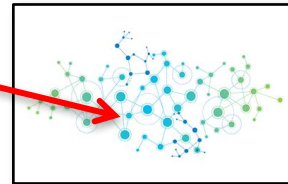
SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN



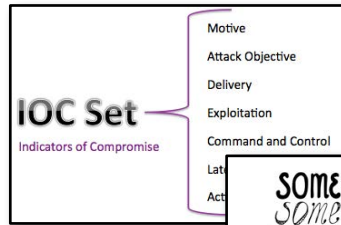
Network Defender Semantic Tree: 2d Limb



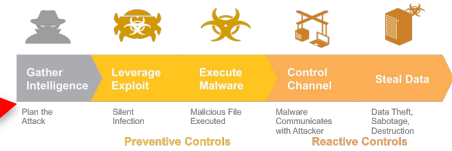
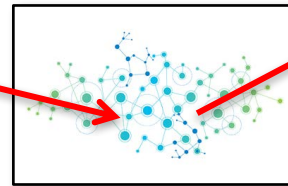
SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN



Network Defender Semantic Tree: 2d Limb

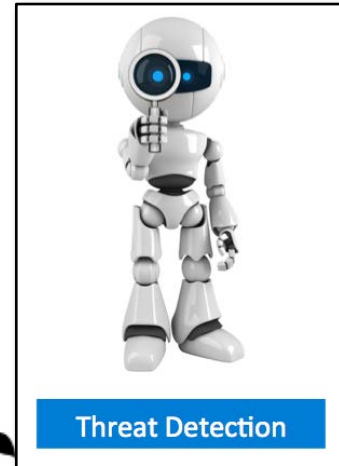
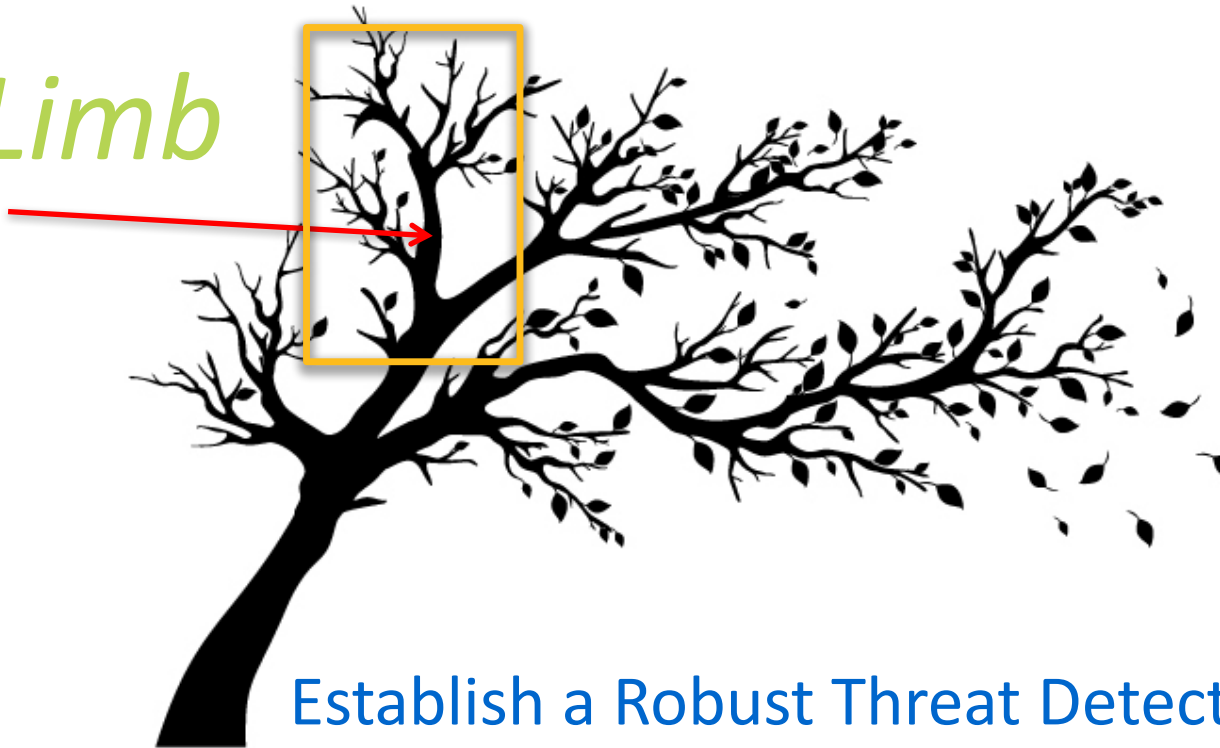


SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN



Network Defender Semantic Tree: 2d Limb

2nd Limb



Establish a Robust Threat Detection Program

The Third Limb



Network Defender Semantic Tree: 3rd Limb

3rd Limb

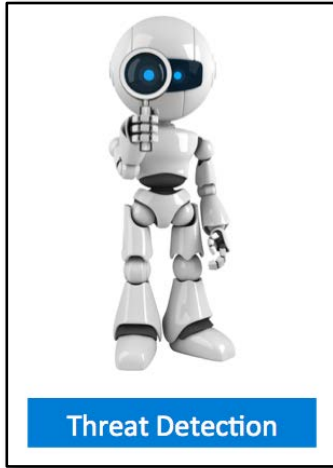


Establish a Robust Threat Eradication Program

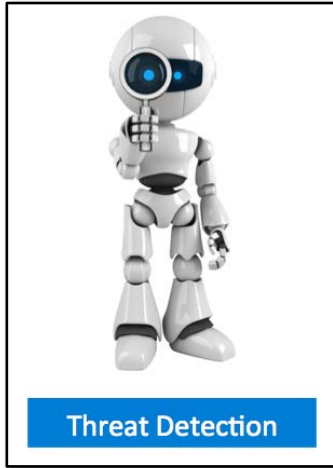
Network Defender Semantic Tree: 3rd Limb



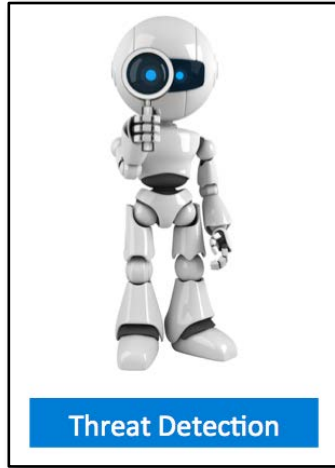
Network Defender Semantic Tree: 3rd Limb



Network Defender Semantic Tree: 3rd Limb



Network Defender Semantic Tree: 3rd Limb



Network Defender Semantic Tree: 3rd Limb

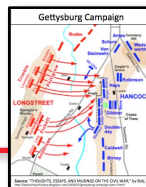
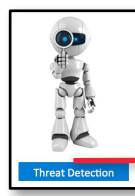


Threat eradication is the act of **minimizing** the effectiveness of newly discovered adversary campaign activity by **blocking** future activity through the **Threat Prevention program**, analyzing the purpose of this new campaign, and installing additional countermeasures that will likely thwart the accomplishment of the campaign objectives.

Network Defender Semantic Tree: 3rd Limb



Threat eradication is the act of minimizing the effectiveness of newly discovered adversary campaign activity by blocking future activity through the Threat Prevention program, analyzing the purpose of this new campaign, and installing additional countermeasures that will likely thwart the accomplishment of the campaign objectives.



IMPACT MITIGATION

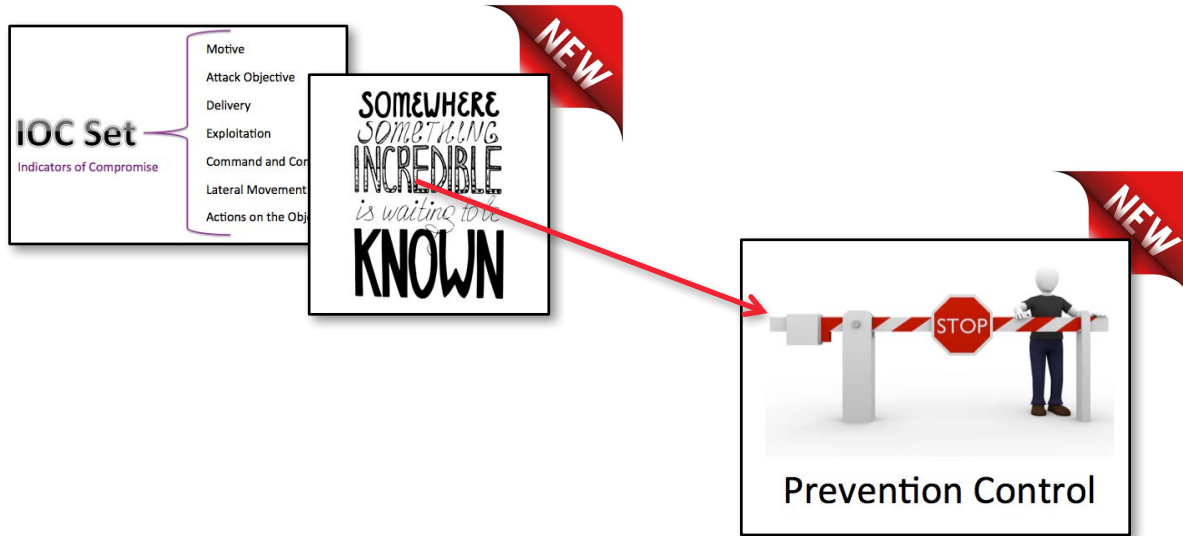
Network Defender Semantic Tree: 3rd Limb

#1



Network Defender Semantic Tree: 3rd Limb

#1



#2



#2

Motivations	
CYBER ESPIONAGE	
CYBER CRIME	
CYBER HACKTIVISM	
CYBER WARFARE	
CYBER MISCHIEF	
CYBER TERRORISM	

Objectives



Network Defender Semantic Tree: 3rd Limb

3rd Limb



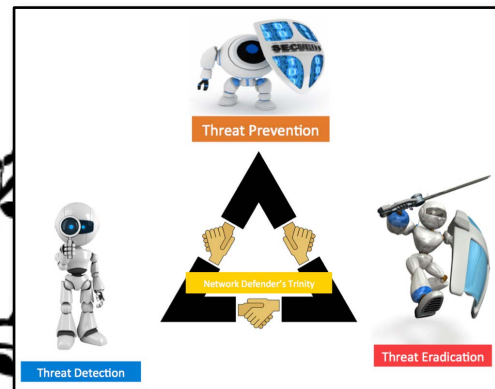
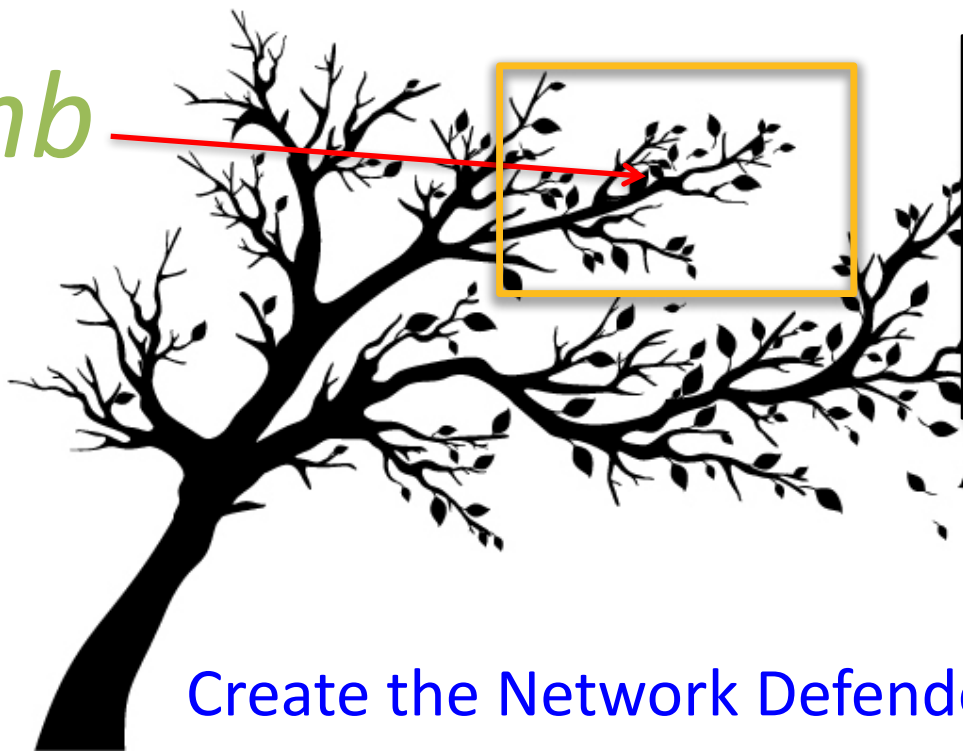
Establish a Robust Threat Eradication Program

The Fourth Limb



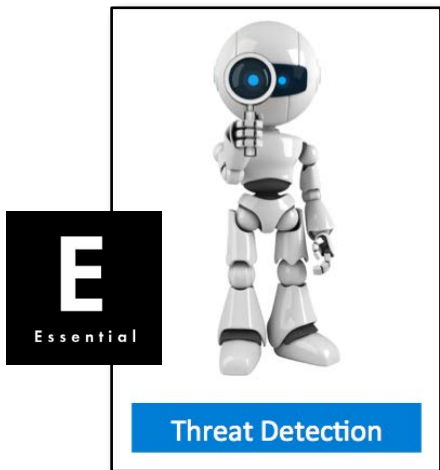
Network Defender Semantic Tree: 4th Limb

4th Limb




Create the Network Defender's Trinity.

Network Defender Semantic Tree: 4th Limb



Network Defender Semantic Tree: 4th Limb



E
Essential

Threat Detection



E
Essential

Threat Prevention



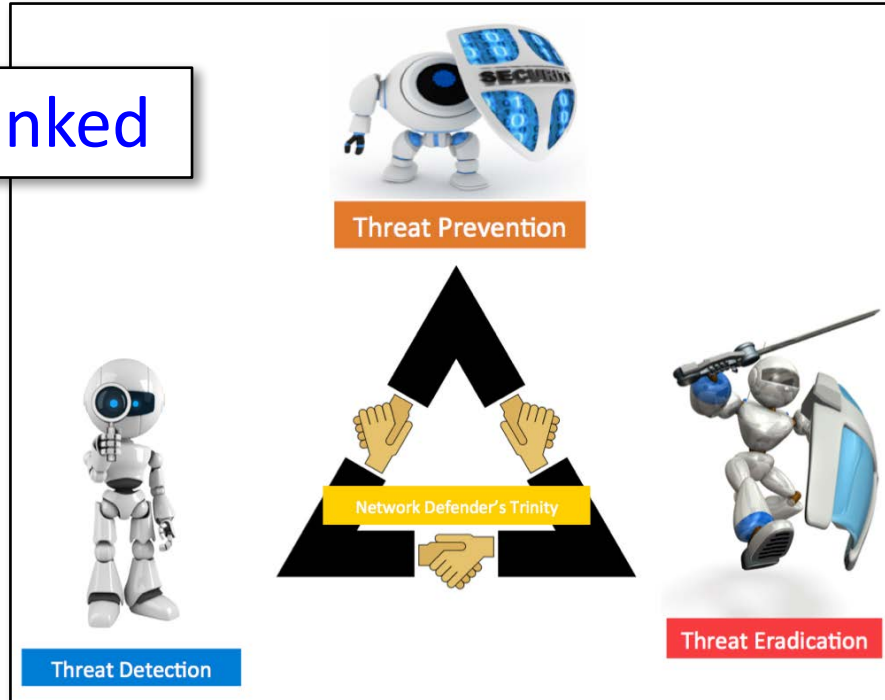
E
Essential

Threat Eradication



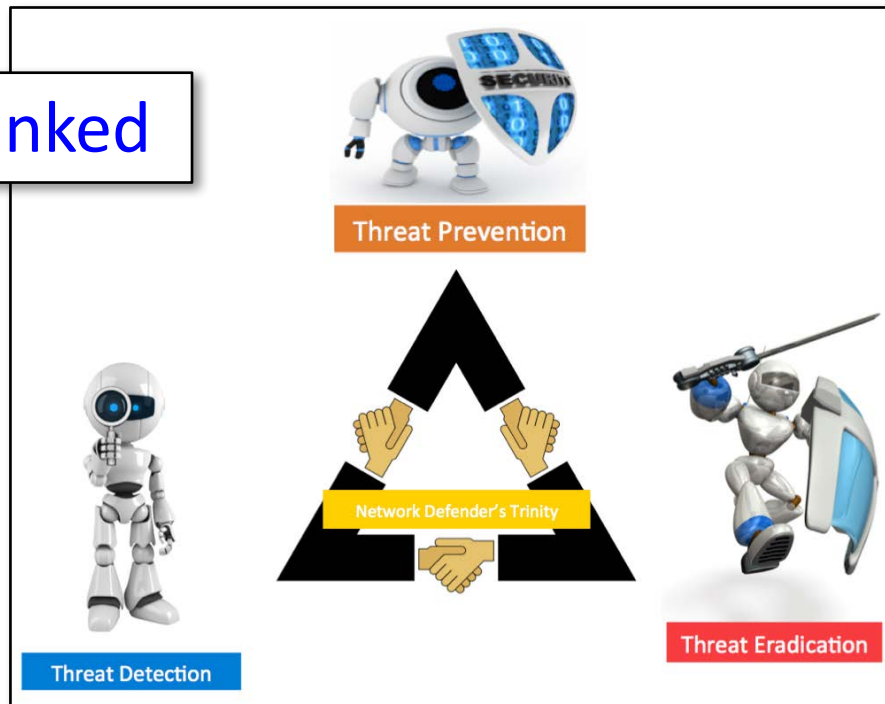
Network Defender Semantic Tree: 4th Limb

Inextricably linked



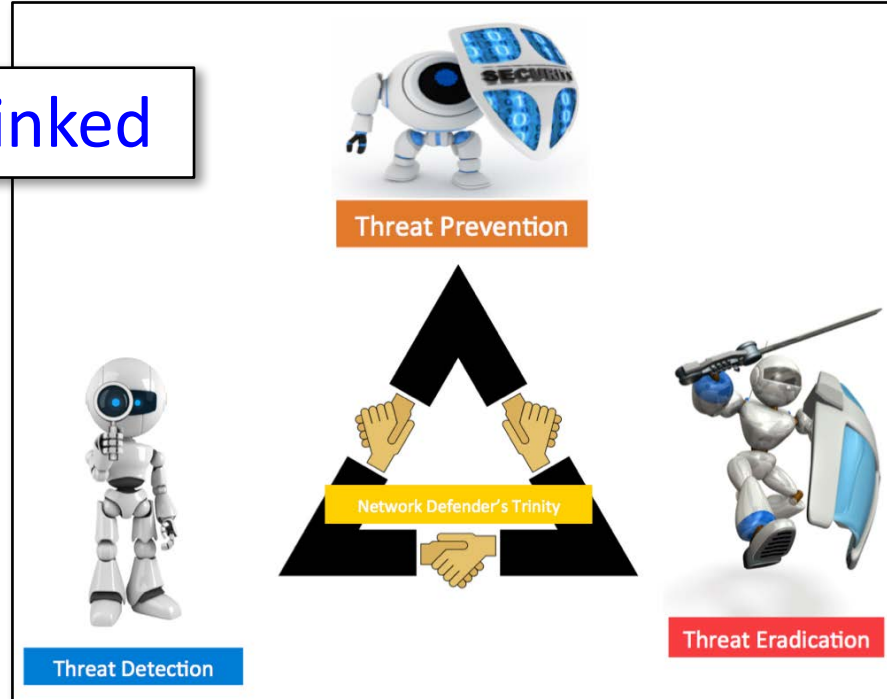
Network Defender Semantic Tree: 4th Limb

Inextricably linked



Network Defender Semantic Tree: 4th Limb

Inextricably linked

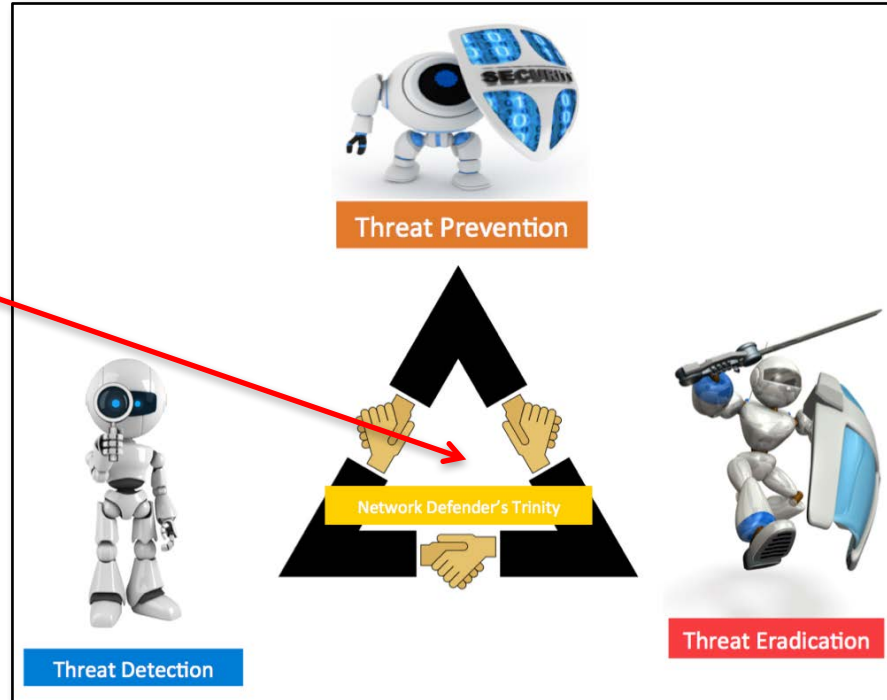


irreducible
complexity

Network Defender Semantic Tree: 4th Limb

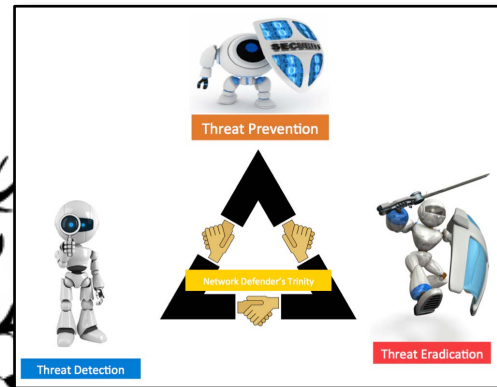
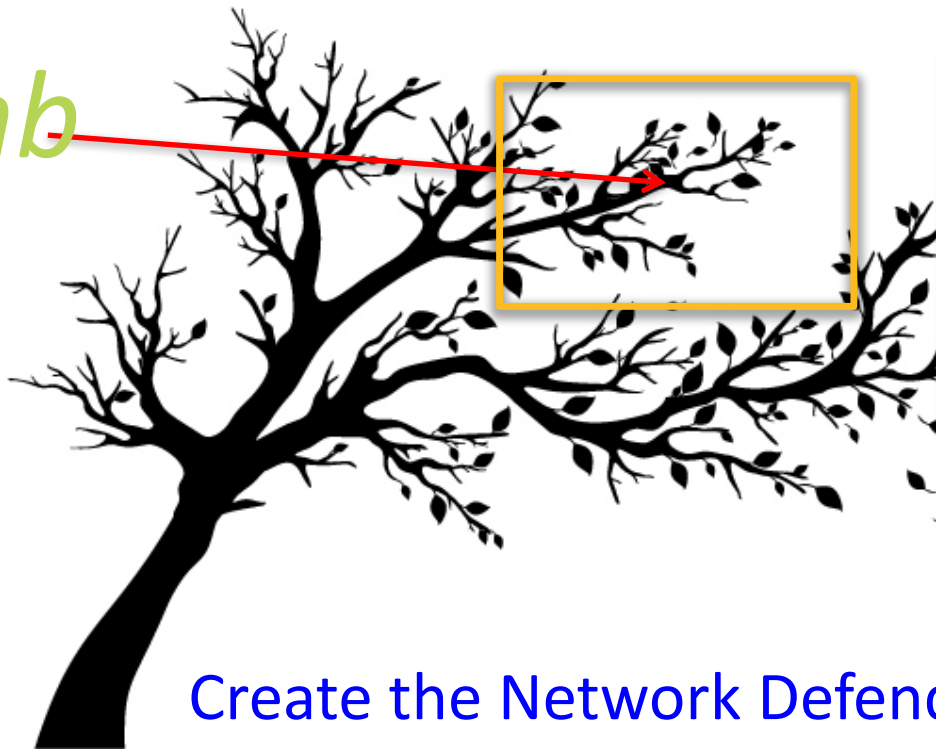


Trinity



Network Defender Semantic Tree: 4th Limb

4th Limb



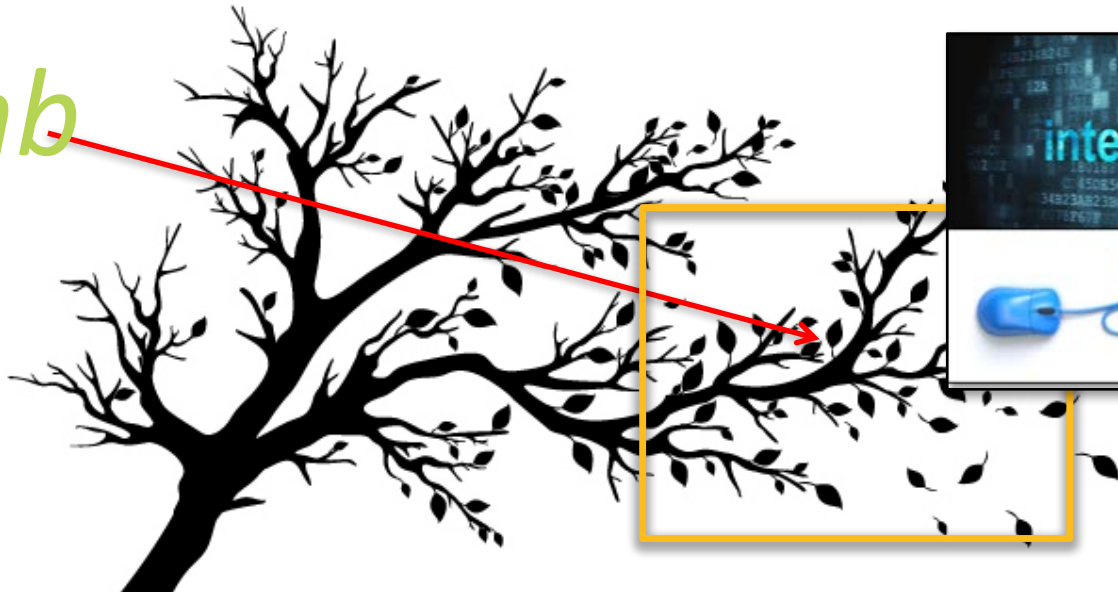
Create the Network Defender's Trinity.

The Last Limb



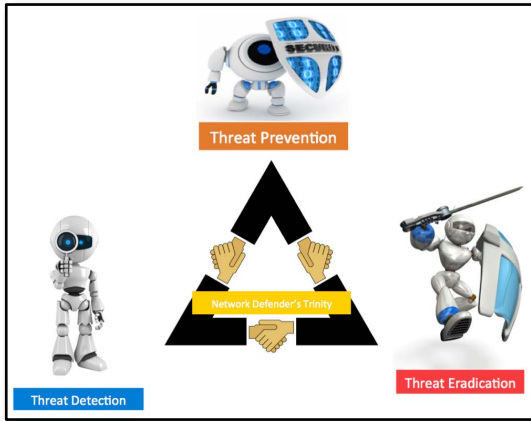
Network Defender Semantic Tree: 5th Limb

5th Limb

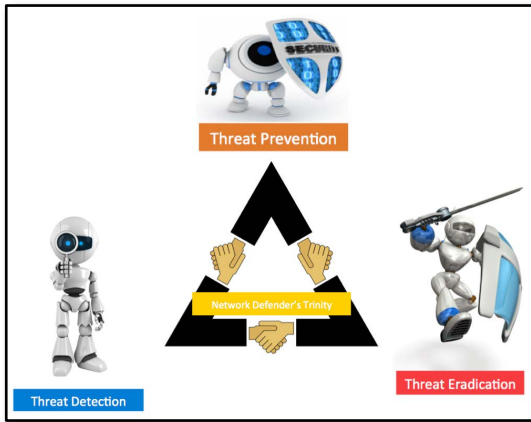


Embrace cybersecurity intelligence collection and ubiquitous sharing

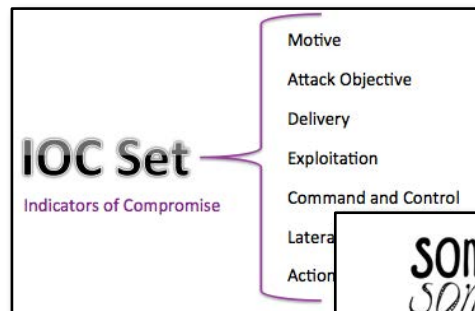
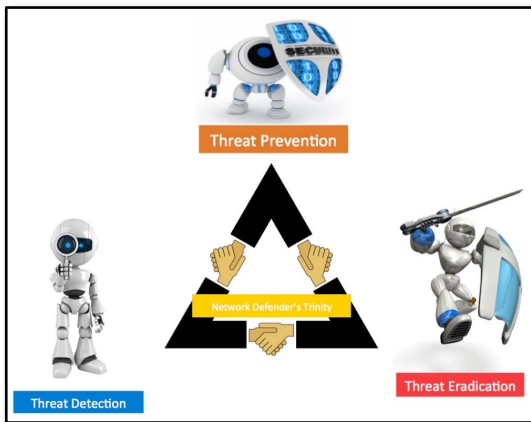
Network Defender Semantic Tree: 5th Limb



Network Defender Semantic Tree: 5th Limb



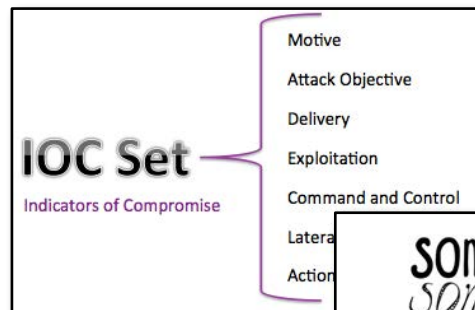
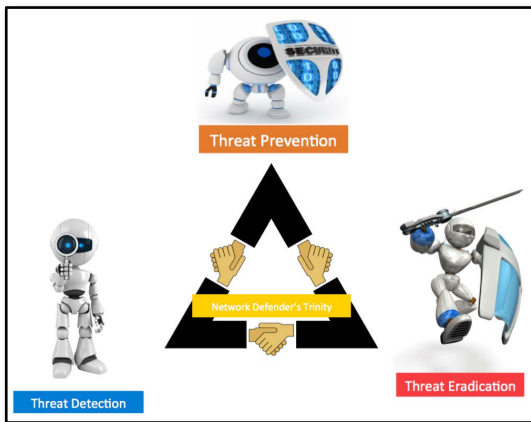
Network Defender Semantic Tree: 5th Limb



SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN

Collected

Network Defender Semantic Tree: 5th Limb

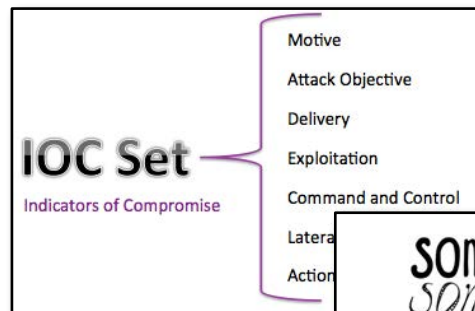
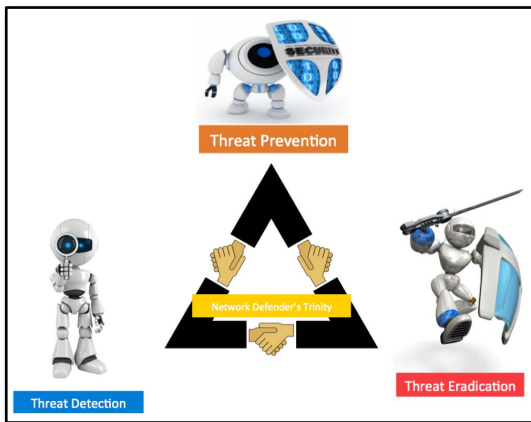


SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN

Collected

Sorted

Network Defender Semantic Tree: 5th Limb



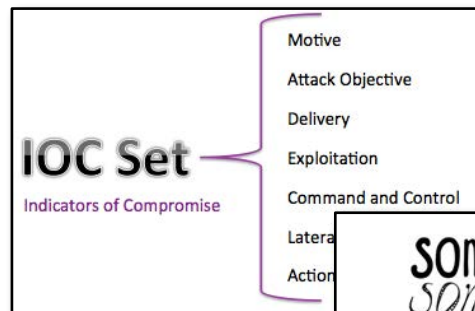
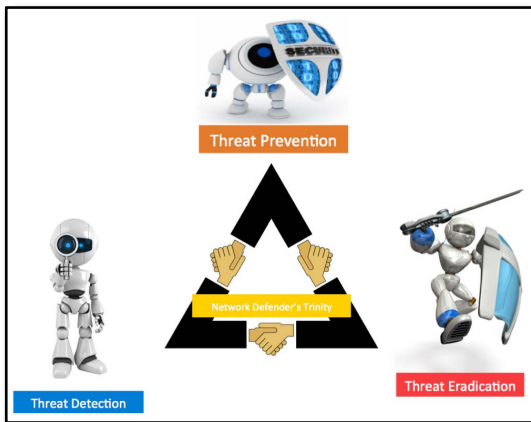
SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN

Collected

Sorted

Evaluated

Network Defender Semantic Tree: 5th Limb



SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN

Collected

Sorted

Evaluated

Prioritized

Network Defender Semantic Tree: 5th Limb

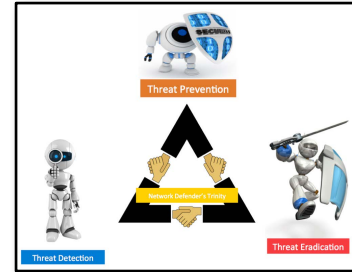
Intelligence collection is the act of gathering **Indicators of Compromise** from **network and endpoint** systems throughout the enterprise and discovering any supplemental information from internal and external sources that can **add context** about what the adversary group is about.



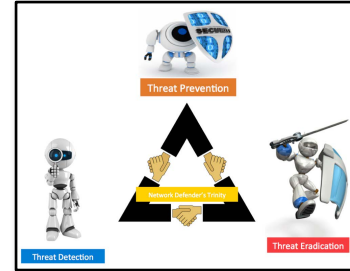
Intelligence collection is the act of gathering **Indicators of Compromise** from **network and endpoint** systems throughout the enterprise and discovering any supplemental information from internal and external sources that can **add context** about what the adversary group is about.



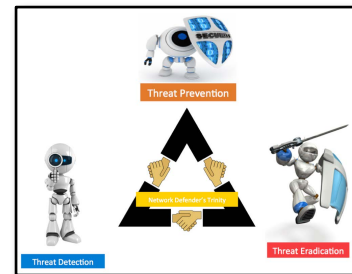
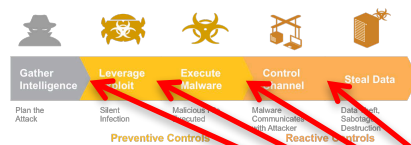
Network Defender Semantic Tree: 5th Limb



Network Defender Semantic Tree: 5th Limb



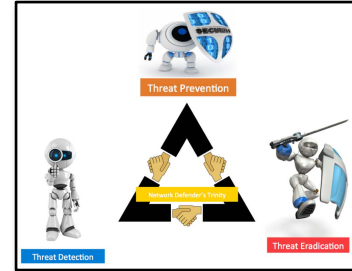
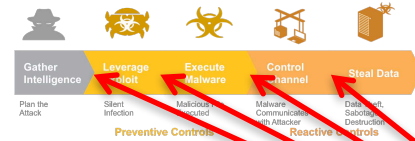
Network Defender Semantic Tree: 5th Limb



Network Defender Semantic Tree: 5th Limb



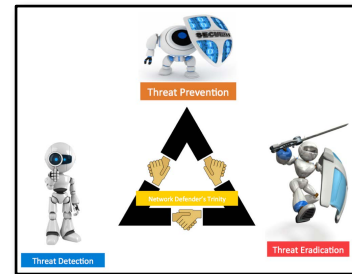
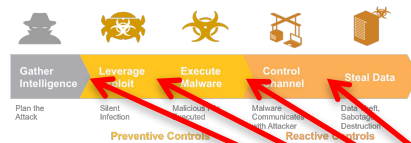
Maximize



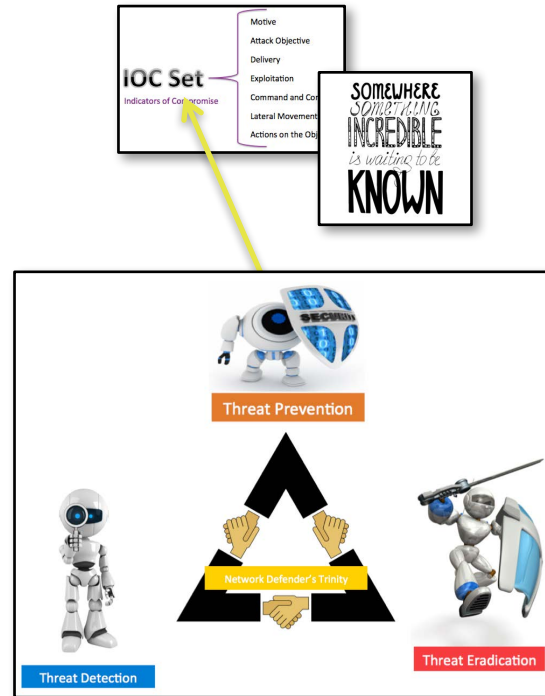
Network Defender Semantic Tree: 5th Limb



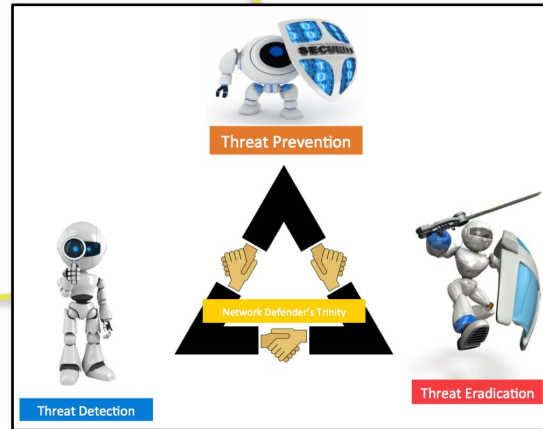
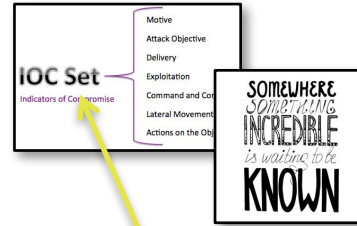
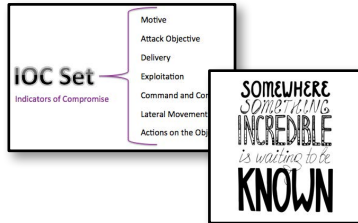
Maximize



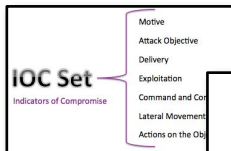
Network Defender Semantic Tree: 5th Limb



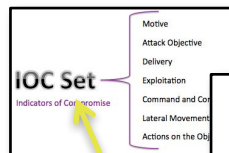
Network Defender Semantic Tree: 5th Limb



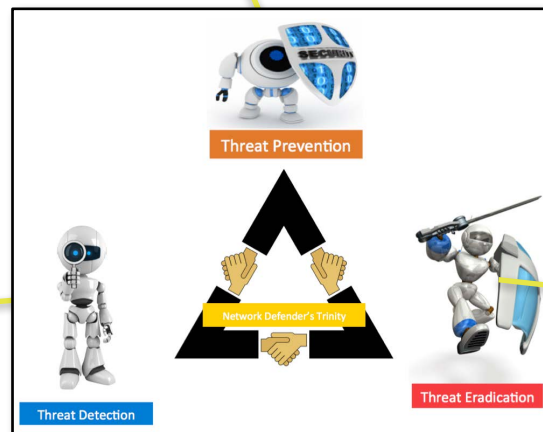
Network Defender Semantic Tree: 5th Limb



SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN

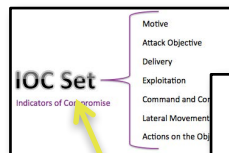


SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN

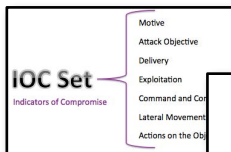


NEW

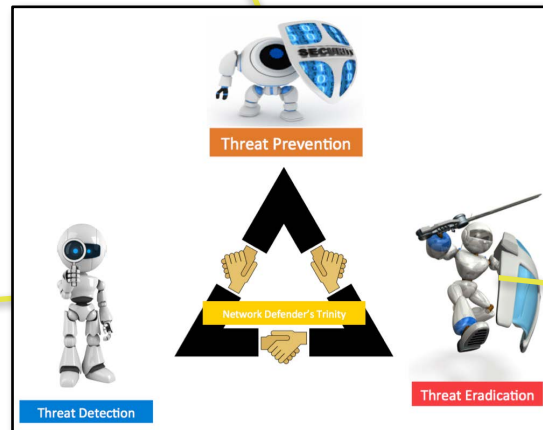
Network Defender Semantic Tree: 5th Limb



SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN



SOMEWHERE
SOMETHING
INCREDIBLE
is waiting to be
KNOWN



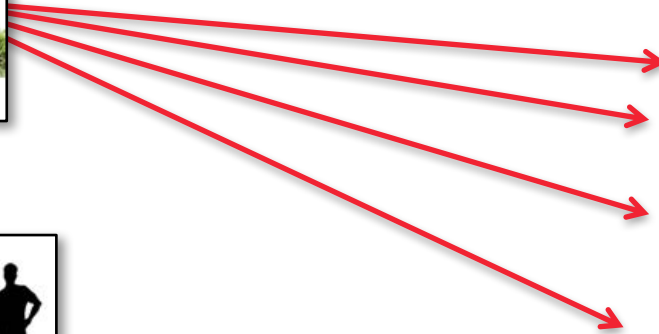
Network Defender Semantic Tree: 5th Limb



Network Defender Semantic Tree: 5th Limb



Network Defender Semantic Tree: 5th Limb



Benefits

#1



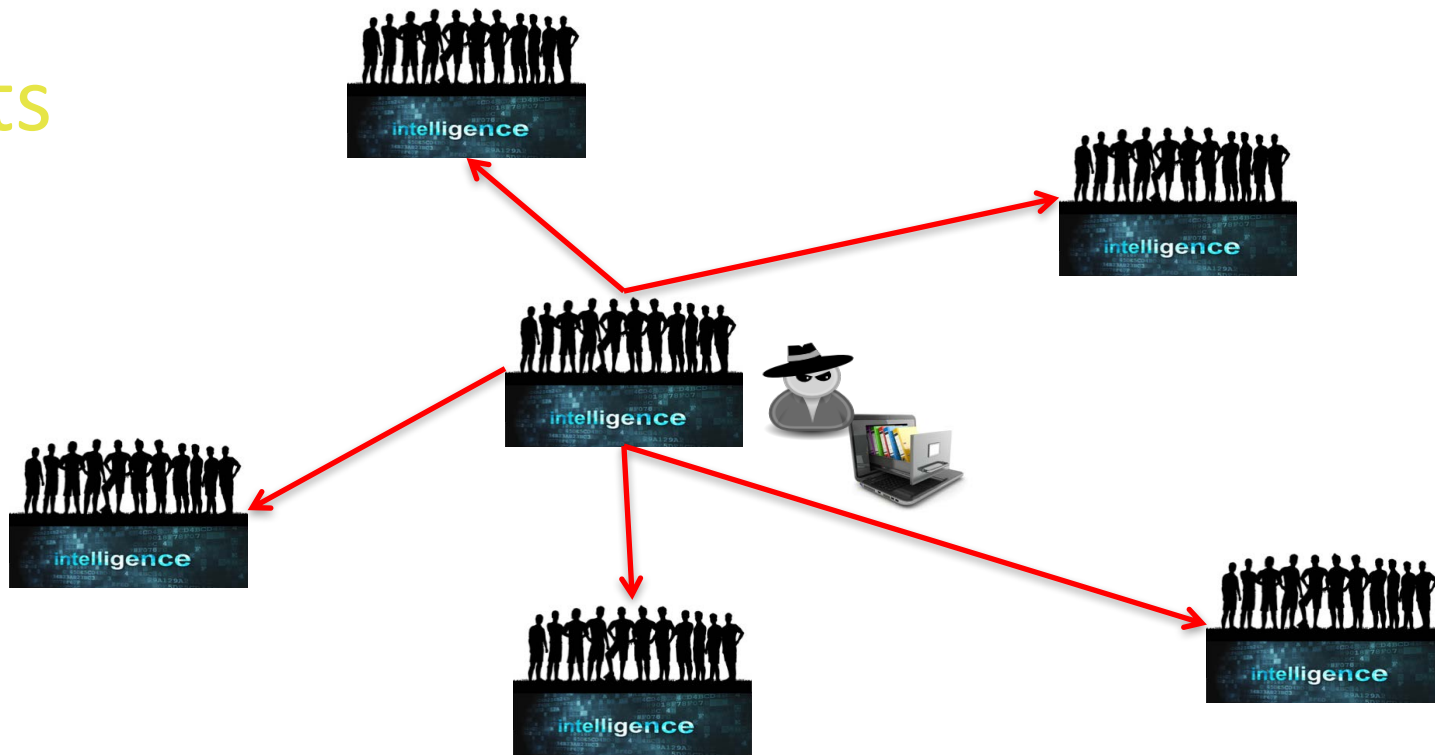
All



Network Defender Semantic Tree: 5th Limb

Benefits

#2



Network Defender Semantic Tree: 5th Limb

Limb



Embrace cybersecurity intelligence collection and ubiquitous sharing

The Cyber Threat Alliance





Founding CEOs



Mark McLaughlin



Michael Brown



Ken Xie



Chris Young





Founding Members:



Purpose: The Cyber Threat Alliance is a group of cyber security practitioners that have chosen to share threat information with each other for the purpose of improving defenses against advanced cyber adversaries across member organizations and their customers.





Working Committee



Rick Howard Vishaal Hariprasad

Joe Chen

Derek Manky

Vincent Weafer Jeannette Jarvis





2 Initial Issues

Build Trust

Build Infrastructure



Rick Howard Vishaal Hariprasad

Joe Chen

Derek Manky

Vincent Weafer Jeannette Jarvis





New Contributing Members:



Membership: Open to any organization that can share a minimum volume of threat intelligence designed by the Alliance.





New Contributing Members:



Membership: Open to any organization that can share a minimum volume of threat intelligence designed by the Alliance.

White House Summit on Cybersecurity and Consumer Protection held at Stanford University





Two Unique Organizing Principles:

- Must Contribute.
- Whatever is shared goes directly into the product line.

Result: Automatic Prevention Controls.



Founding CEOs



Mark McLaughlin



Michael Brown



Ken Xie



Chris Young





Founding CEOs



Mark McLaughlin



Michael Brown



Ken Xie



Chris Young





Mark McLaughlin



Michael Brown



Ken Xie



Chris Young





Mark McLaughlin



Michael Brown

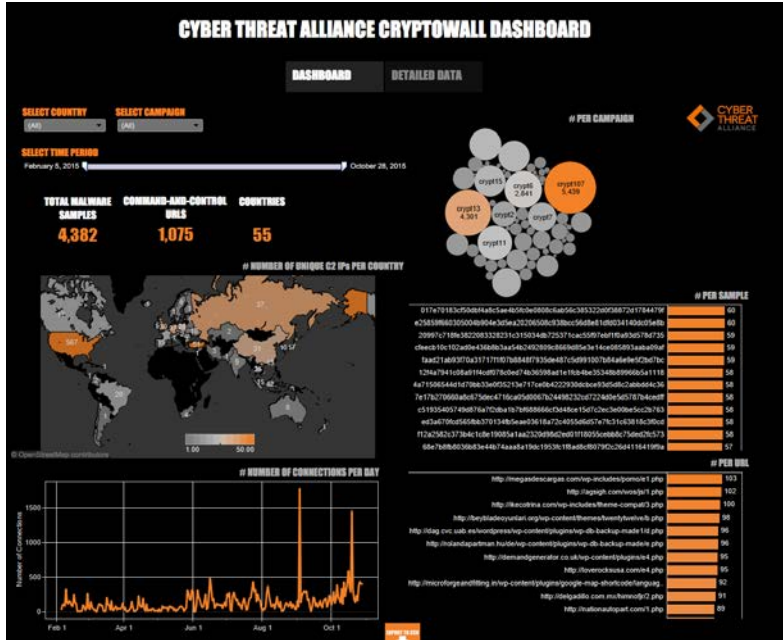


Ken Xie



Chris Young





CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

\$325M in estimated damages across the globe

839 command and control URLs

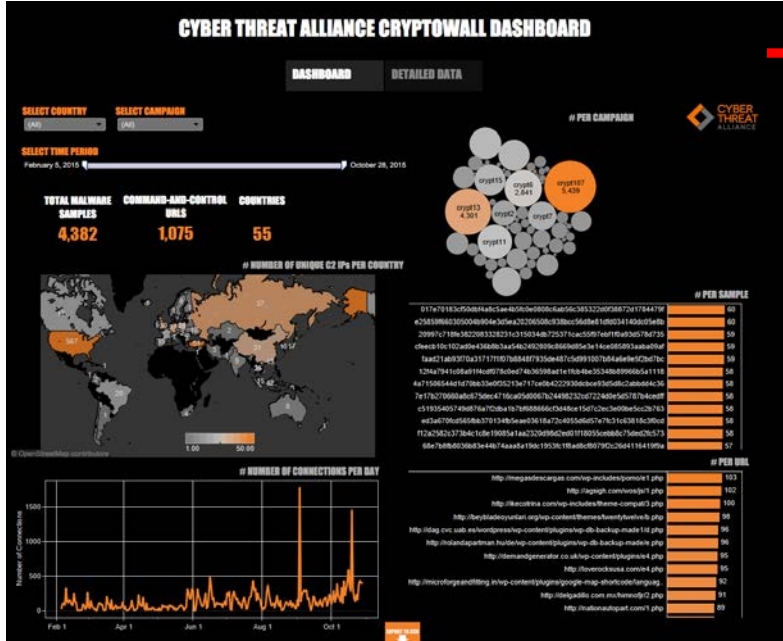
5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples





CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

\$325M in estimated damages across the globe

839 command and control URLs

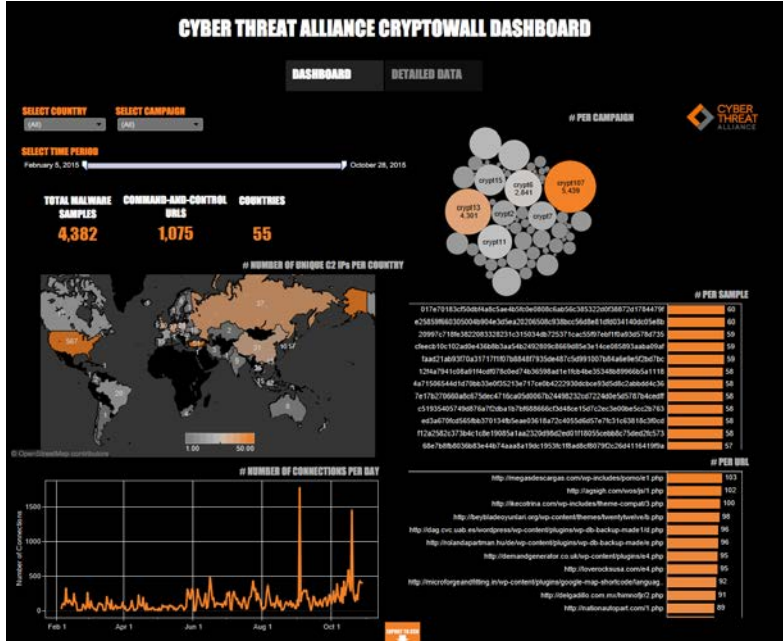
5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples





CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

\$325M in estimated damages across the globe

839 command and control URLs

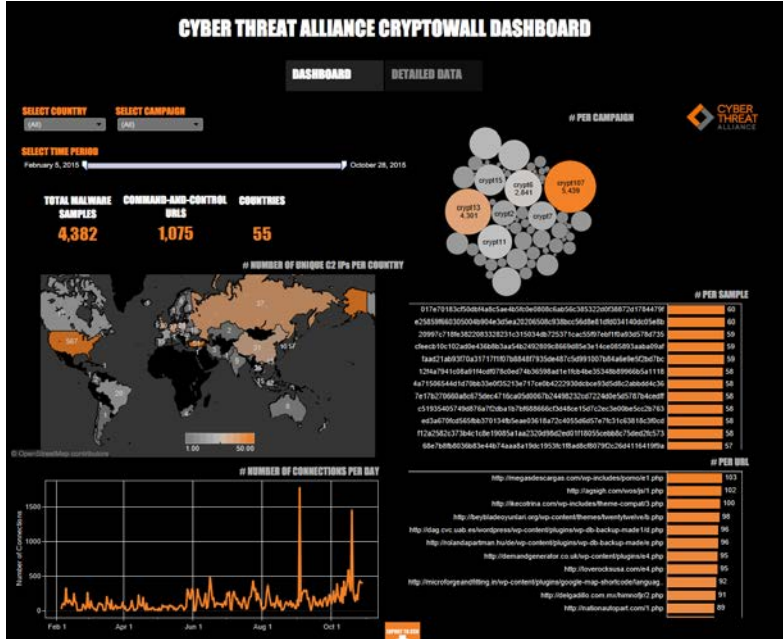
5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples





CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

\$325M in estimated damages across the globe

839 command and control URLs

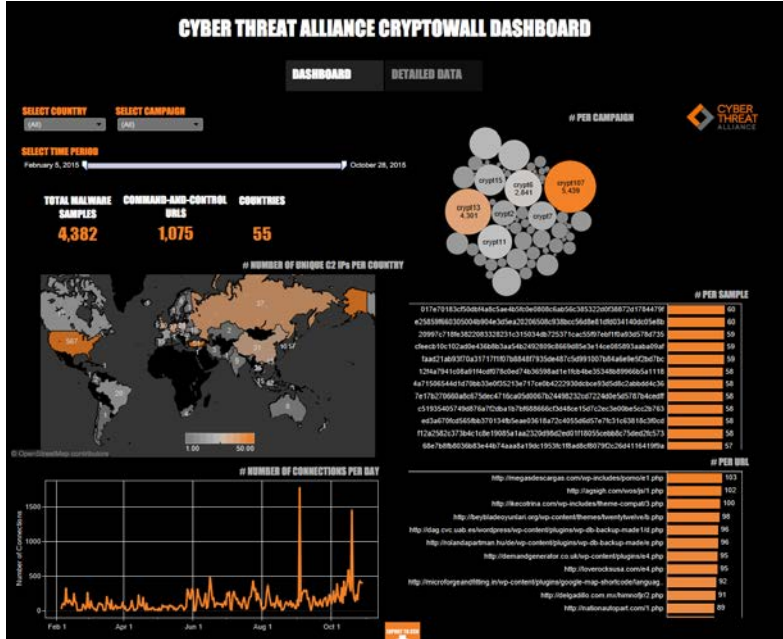
5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples





CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

\$325M in estimated damages across the globe

839 command and control URLs

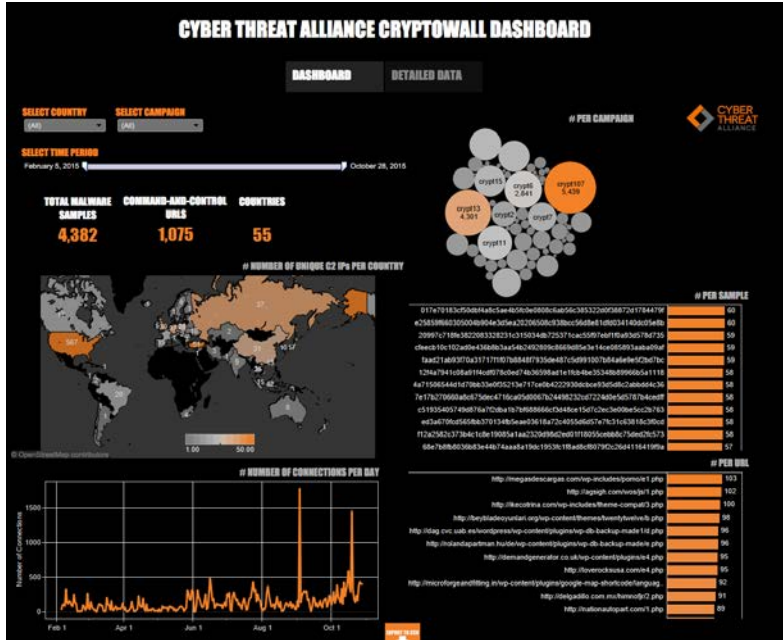
5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples





CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

\$325M in estimated damages across the globe

839 command and control URLs

5 second-tier IP addresses used for command and control

49 campaign code identifiers → **406,887** attempted infections of CryptoWall version 3

4,046 malware samples

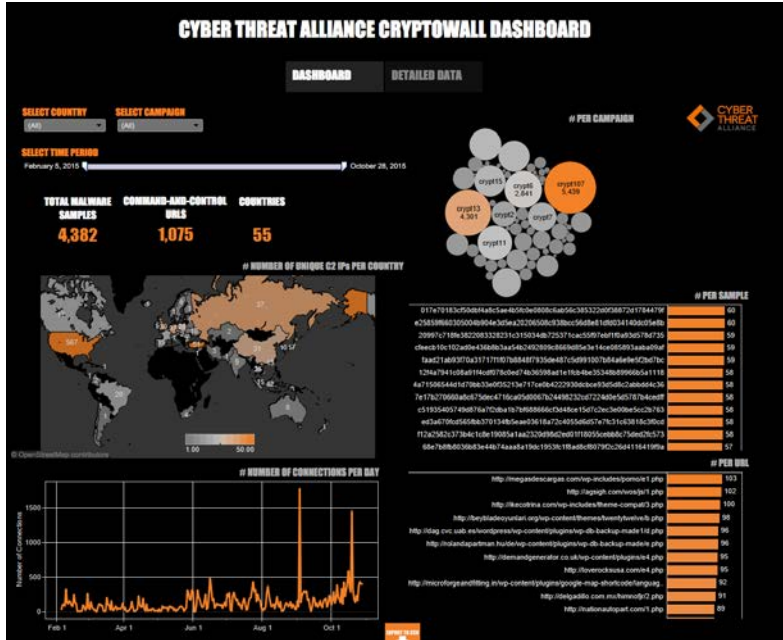




CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:



\$325M in estimated damages across the globe

839 command and control URLs

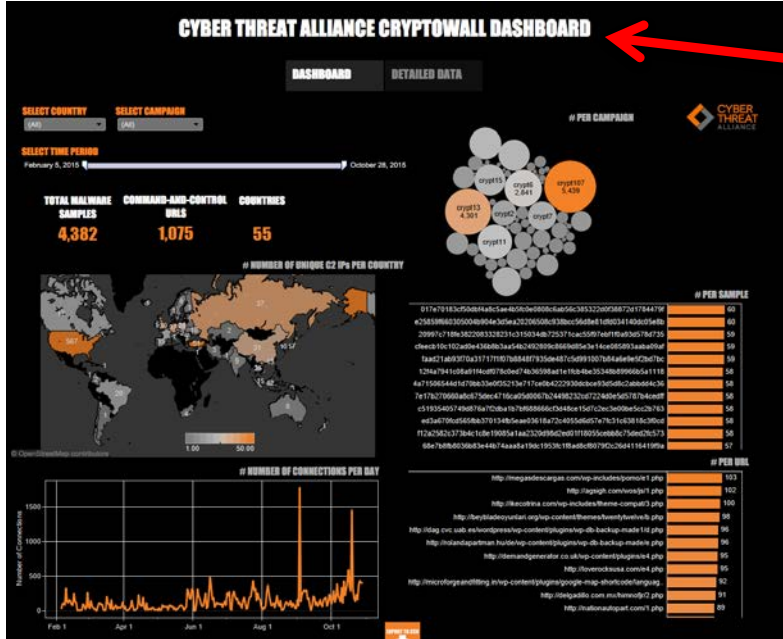
5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples





CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

\$325M in estimated damages across the globe

839 command and control URLs

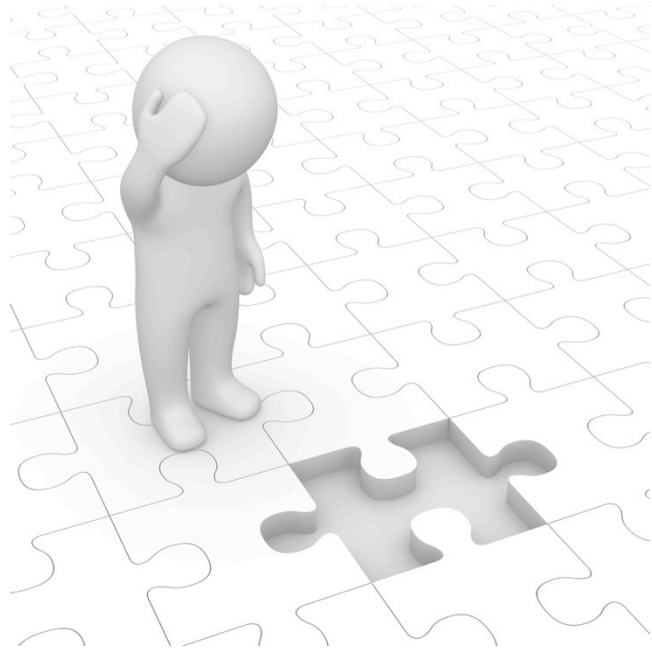
5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples





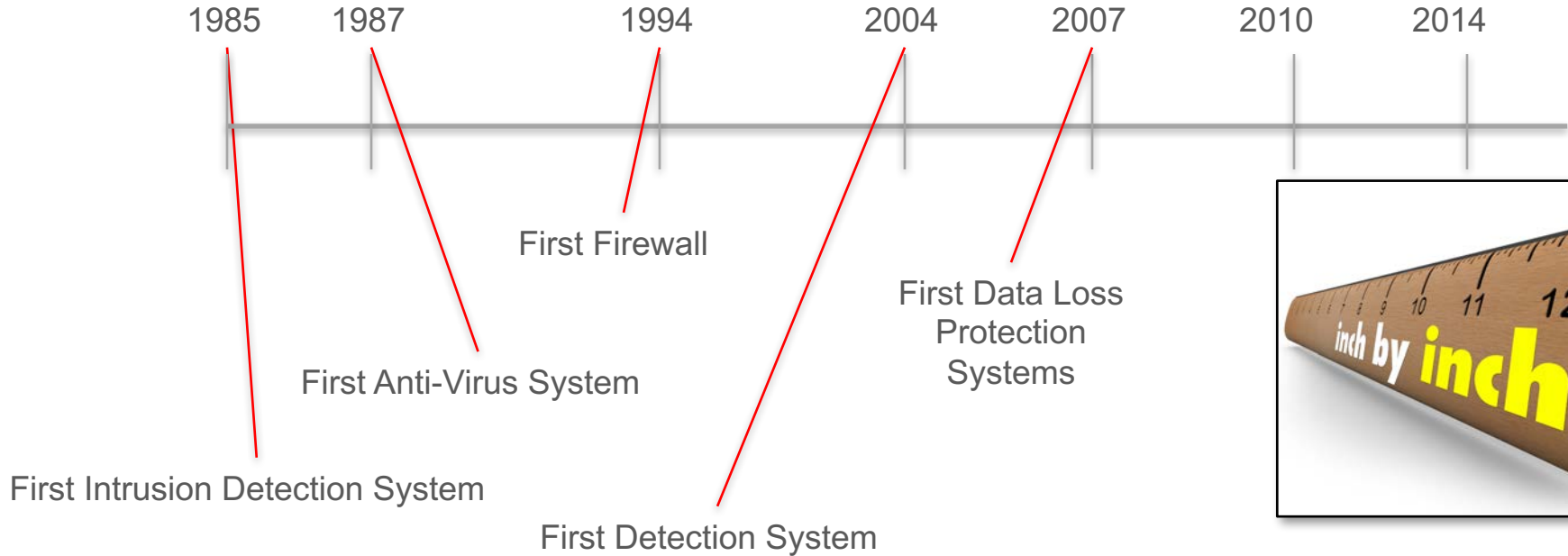
Where We Need to Go

The only smart thing for the network defender to do is to **share everything; crowd source threat intelligence** so that only the advanced adversary can keep up.

Conclusion



25 Years of Incremental Improvement



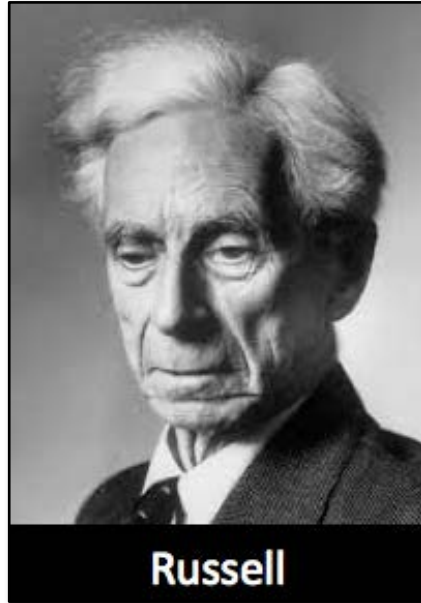
Rethink the Network Defender Problem Space

LEAP AHEAD



Boiled Water

Rethink the Network Defender Problem Space



Rethink the Network Defender Problem Space



Fundamental

Self Evident

Experts Agree

Atomic

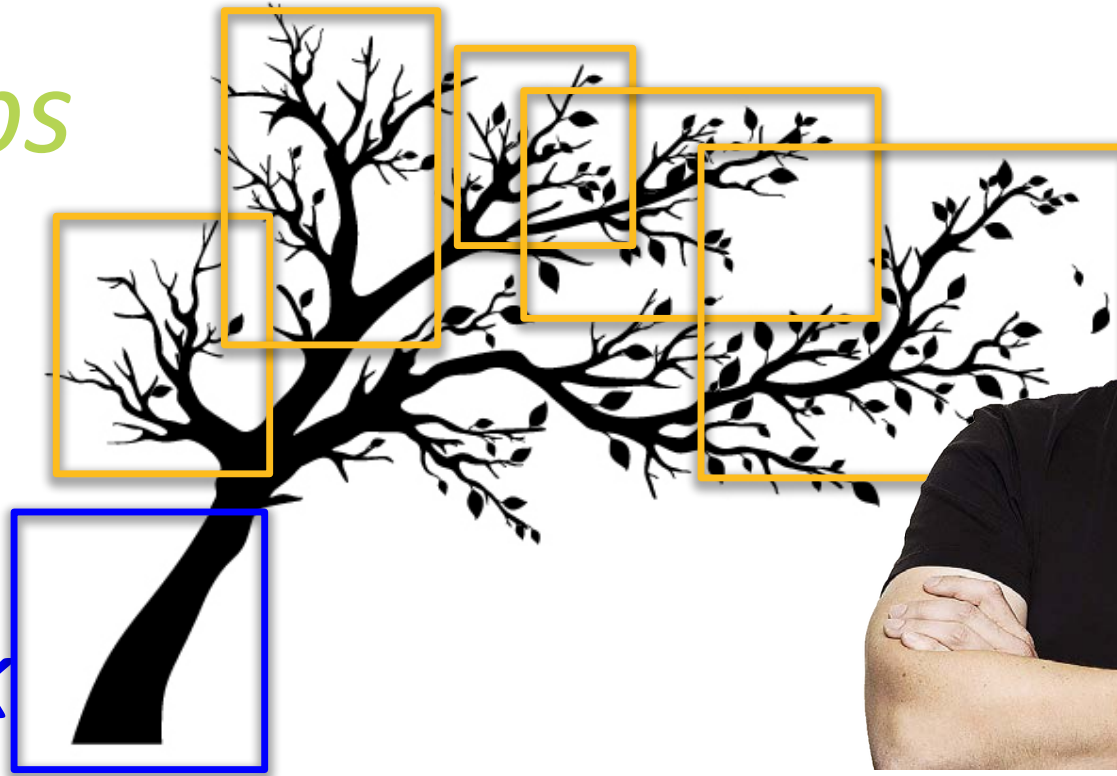


First Principles

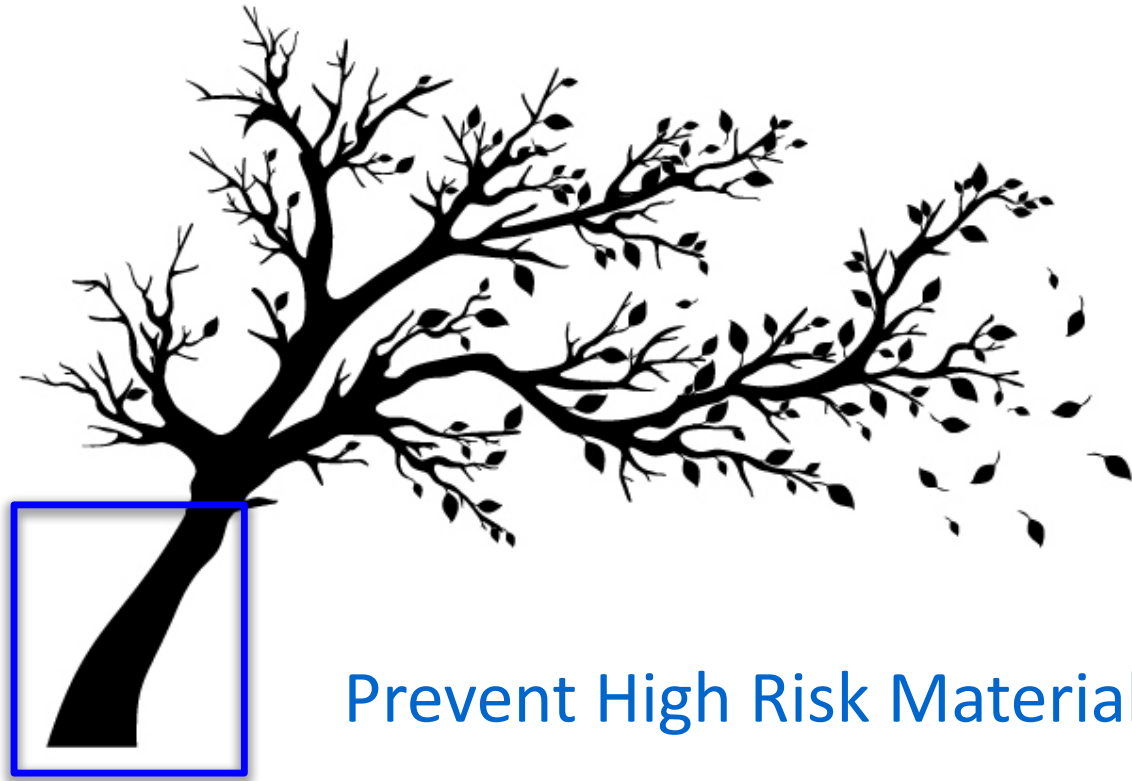
Semantic Tree

Limbs

Trunk



Network Defender First Principles



Network Defender First Principles

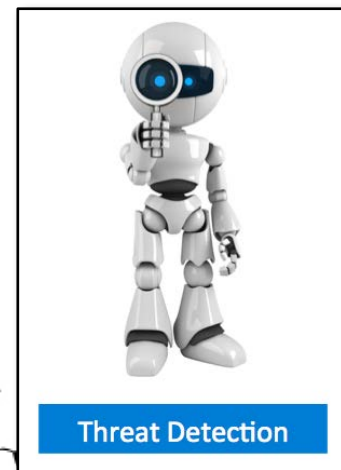
1st Limb



Establish a Robust Threat Prevention program

Network Defender First Principles

2nd Limb



Establish a Robust Threat Detection Program

Network Defender First Principles

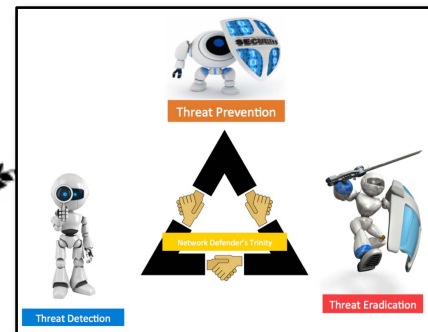
3rd Limb



Establish a Robust Threat Eradication Program

Network Defender First Principles

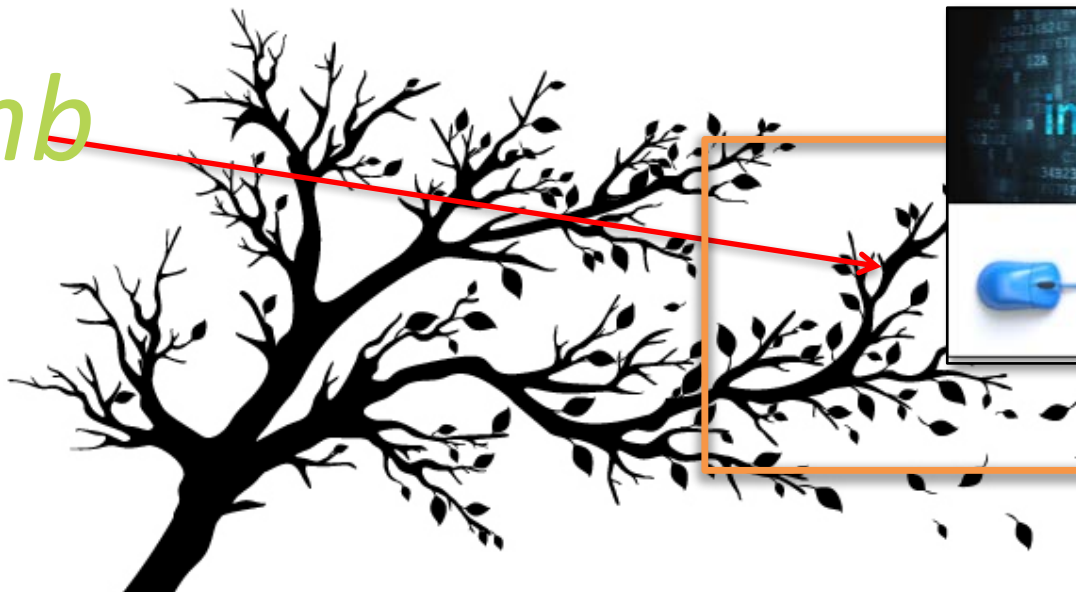
4th Limb



The Network Defender's trinity is inextricably linked, atomic, and irreducible

Network Defender First Principles

5th Limb



Embrace cybersecurity intelligence collection
and ubiquitous sharing

More Information



Call to Action

First Principle White Paper:

<http://researchcenter.paloaltonetworks.com/2016/03/first-principles-for-network-defenders-a-unified-theory-for-security-practitioners/>



Rick Howard: CSO Palo Alto Networks

Email: rhoward@paloaltonetworks.com

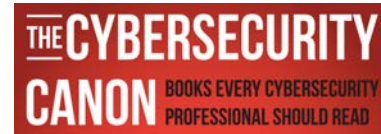
Twitter: [@raceBannon99](https://twitter.com/raceBannon99)



<http://cyberthreatalliance.org/>



<https://paloaltonetworks.com/threat-research.html>



<https://paloaltonetworks.com/threat-research/cybercanon.html>



End

