Evolution of the Network Defenders Strategy

First Principle Thinking in Cybersecurity

CISSE 25 Colloquium: Challenges in Teaching Cybersecurity

Rick Howard
CSO, Chief Analyst, Senior Fellow
The CyberWire

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

Professional Career

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

Tactical Networks, Garrison Networks, Professor, ACERT

Professional Career

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

Tactical Networks, Garrison Networks, Professor, ACERT

16 Years: Commercial

Professional Career

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

Tactical Networks, Garrison Networks, Professor, ACERT

16 Years: Commercial

Security Vendor: Counterpane, iDefense/Verisign, Palo Alto Networks

Professional Career

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

- Tactical Networks, Garrison Networks, Professor, ACERT

16 Years: Commercial

- **Security Vendor**: Counterpane, iDefense/Verisign, Palo Alto Networks
- **Enterprise**: TASC, The Cyberwire

Professional Career

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

Tactical Networks, Garrison Networks, Professor, ACERT

16 Years: Commercial

Security Vendor: Counterpane, iDefense/Verisign, Palo Alto Networks

Enterprise: TASC, The Cyberwire

Advisory Board: Cybersecurity Canon Project, Cyber Threat Alliance, Verticap, Spotlight, Splunk

Professional Career

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

Tactical Networks, Garrison Networks, Professor, ACERT

16 Years: Commercial

Security Vendor: Counterpane, iDefense/Verisign, Palo Alto Networks

Enterprise: TASC, The Cyberwire

Advisory Board: Cybersecurity Canon Project, Cyber Threat Alliance, Verticap, Spotlight, Splunk

Education

Professional Career

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

Tactical Networks, Garrison Networks, Professor, ACERT

16 Years: Commercial

Security Vendor: Counterpane, iDefense/Verisign, Palo Alto Networks

Enterprise: TASC, The Cyberwire

Advisory Board: Cybersecurity Canon Project, Cyber Threat Alliance, Verticap, Spotlight, Splunk

Education

BS in Engineering from the United States Military Academy

Professional Career

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com, rahhoward@gmail.com

26 Years: US Army

Tactical Networks, Garrison Networks, Professor, ACERT

16 Years: Commercial

Security Vendor: Counterpane, iDefense/Verisign, Palo Alto Networks

Enterprise: TASC, The Cyberwire

Advisory Board: Cybersecurity Canon Project, Cyber Threat Alliance, Verticap, Spotlight, Splunk

Education

BS in Engineering from the United States Military Academy

MS in Computer Science from the Naval Postgraduate School

Professional Career

The Cybersecurity Canon Project

https://icdt.osu.edu/cybercanon

The Ohio State University
Institute for CYBERSECURITY & DIGITAL TRUST
HOME
MISSION
CYBERSECURITY CANON
Cybersecurity Canon
CYBERSECURITY
CANON

Advisory Board: Cybersecurity Canon Project, Cyber Threat Alliance, Verticap, Spotlight, Splunk

Free Educational Resource

A Curated Catalog of Must-Read Security Books

What is the Cybersecurity Canon Project ?

*"**Must-read** books for all cybersecurity practitioners—be they from industry, government or academia—where the content is **timeless**, genuinely represents an aspect of the community that is **true and precise**, reflects the highest **quality** and, if not read, will leave a hole in the cybersecurity professional's education that will make the practitioner incomplete.”*

https://icdt.osu.edu/cybercanon

CYBERSECURITY
CANON

How Are Books Chosen?

- Crowdsourced Recommendations
- Committee reads, reviews, recommends
  - Hall of Fame
  - Niche Audience
  - Do Not Read
- Committee votes on Hall of Fame recommendations
  - Remains a candidate for 5 years
- Hall of Fame Winners are awarded each May

https://icdt.osu.edu/cybercanon

CYBERSECURITY
CANON

How Are Books Chosen?

- Crowdsourced Recommendations
- Committee reads, reviews, recommends
  - Hall of Fame
  - Niche Audience
  - Do Not Read
- Committee votes on Hall of Fame recommendations
  - Remains a candidate for 5 years
- Hall of Fame Winners are awarded each May

https://icdt.osu.edu/cybercanon

CYBERSECURITY CANON

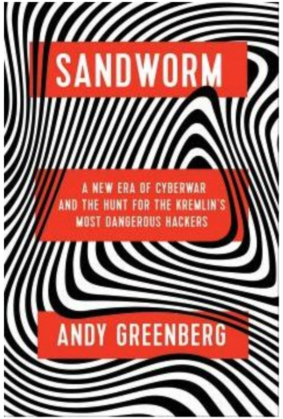
How Can You Get Involved?

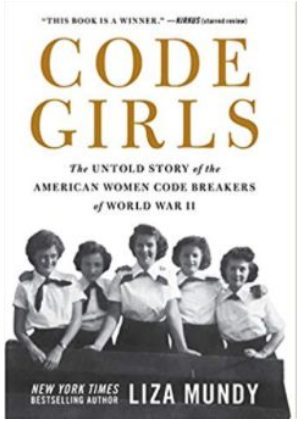
- Read a Security Book
- Write A Review
- Submit the Review, with Recommendation, to the Committee

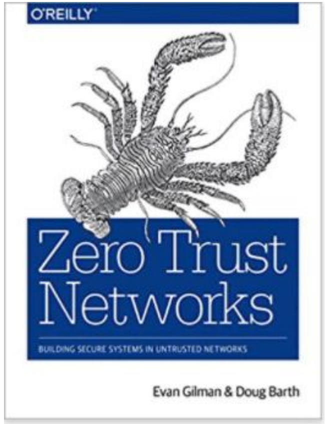
https://icdt.osu.edu/cybercanon

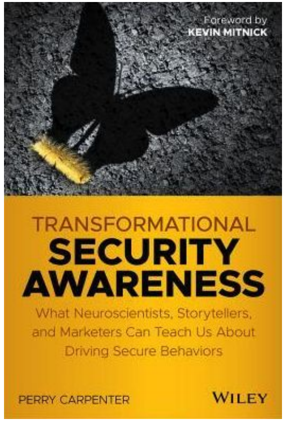
CYBERSECURITY CANON

2020-21 Hall of Fame Winners


SANDWORM
A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS
ANDY GREENBERG


"THIS BOOK IS A WINNER." —KIRKUS (starred review)
CODE GIRLS
The UNTOLD STORY of the AMERICAN WOMEN CODE BREAKERS of WORLD WAR II
NEW YORK TIMES BESTSELLING AUTHOR
LIZA MUNDY




Foreword by KEVIN MITNICK
TRANSFORMATIONAL
SECURITY AWARENESS
What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors
PERRY CARPENTER
WILEY

https://icdt.osu.edu/cybercanon

CYBERSECURITY CANON

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com

Current Job

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com

The ideas, strategies and technologies that senior cybersecurity executives wrestle with on a daily basis.

thecyberwire.com/pro/cso-perspectives

A fun and informative infosec audio glossary from the CyberWire.

thecyberwire.com/podcasts/word-notes

Quarterly discussion of the most impactful cybersecurity news items from the past 90 days.

thecyberwire.com/search?query=Quarterlyt%20Analyst%20Call

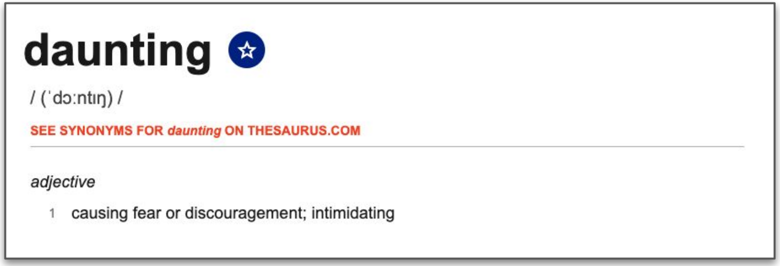
"In a world overloaded by information, we separate the signal from the noise."

Evolution of the Network Defenders Strategy

First Principle Thinking in Cybersecurity

CISSE 25 Colloquium: Challenges in Teaching Cybersecurity

Rick Howard
CSO, Chief Analyst, Senior Fellow
The CyberWire



daunting

/ (ˈdɔːntɪŋ) /

SEE SYNONYMS FOR *daunting* ON THESAURUS.COM

adjective

1 causing fear or discouragement; intimidating

Boy on a High Dive - Norman Rockwell - 1947

daunting

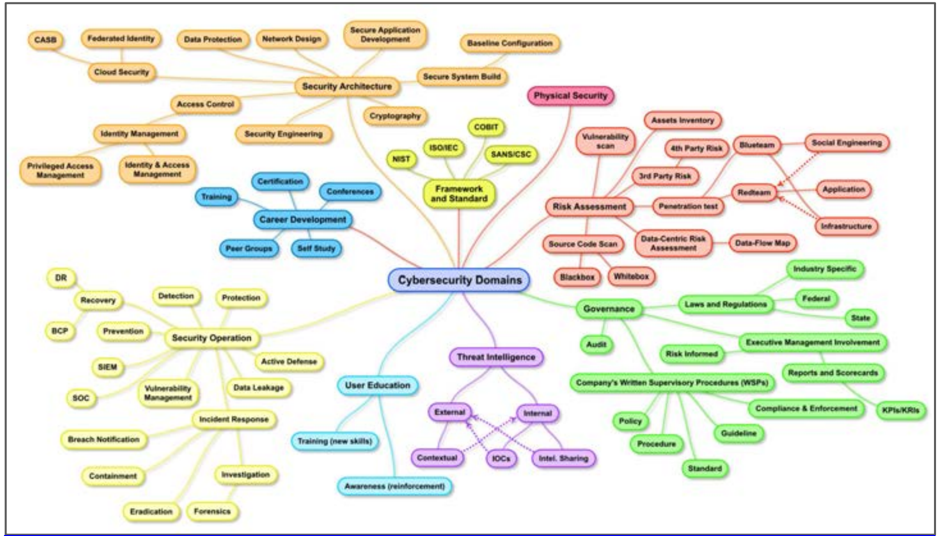
/ (ˈdɔːntɪŋ) /

SEE SYNONYMS FOR *daunting* ON THESAURUS.COM

adjective

1 causing fear or discouragement; intimidating

CISO’s World



Source: Henry Jiang: Chief Information Security Officer at Diligent Corporation

Boy on a High Dive - Norman Rockwell - 1947

CISO’s World

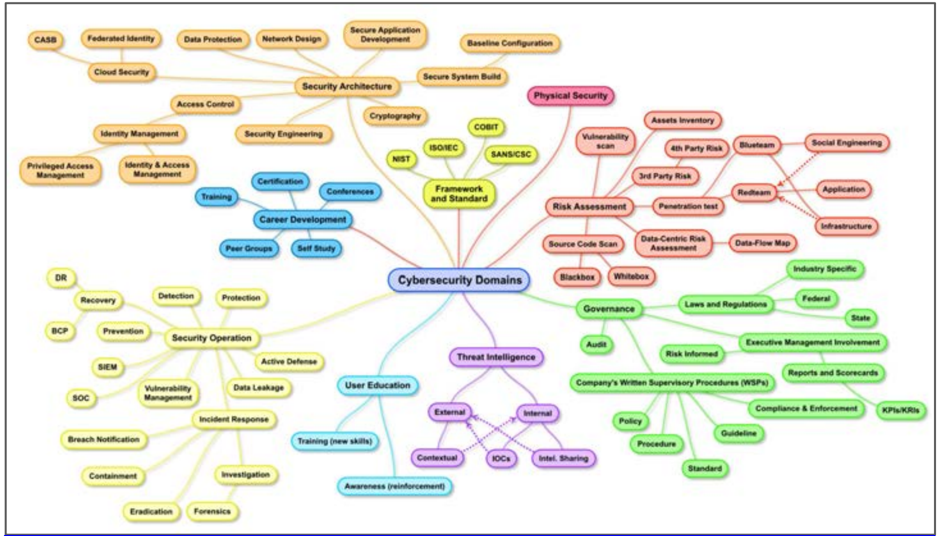
daunting

/ (ˈdɔːntɪŋ) /

SEE SYNONYMS FOR *daunting* ON THESAURUS.COM

adjective

1 causing fear or discouragement; intimidating

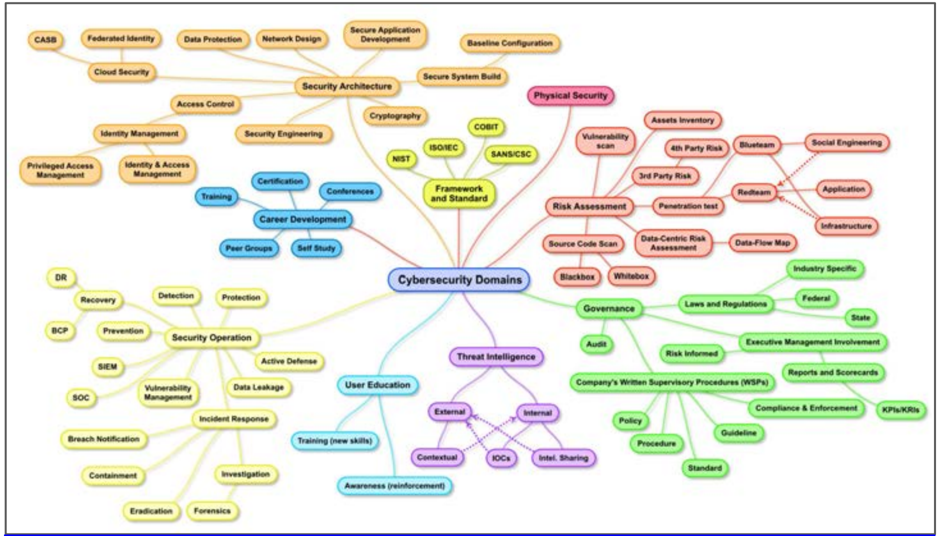


Source: Henry Jiang: Chief Information Security Officer at Diligent Corporation

Projects

Boy on a High Dive - Norman Rockwell - 1947

CISO’s World



Source: Henry Jiang: Chief Information Security Officer at Diligent Corporation

daunting ☆

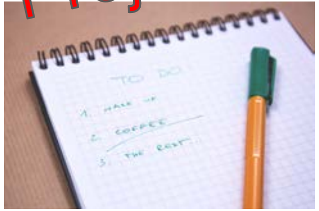
/ (ˈdɔːntɪŋ) /

SEE SYNONYMS FOR *daunting* ON THESAURUS.COM

adjective

1 causing fear or discouragement; intimidating

Projects



Boy on a High Dive - Norman Rockwell - 1947

daunting ☆

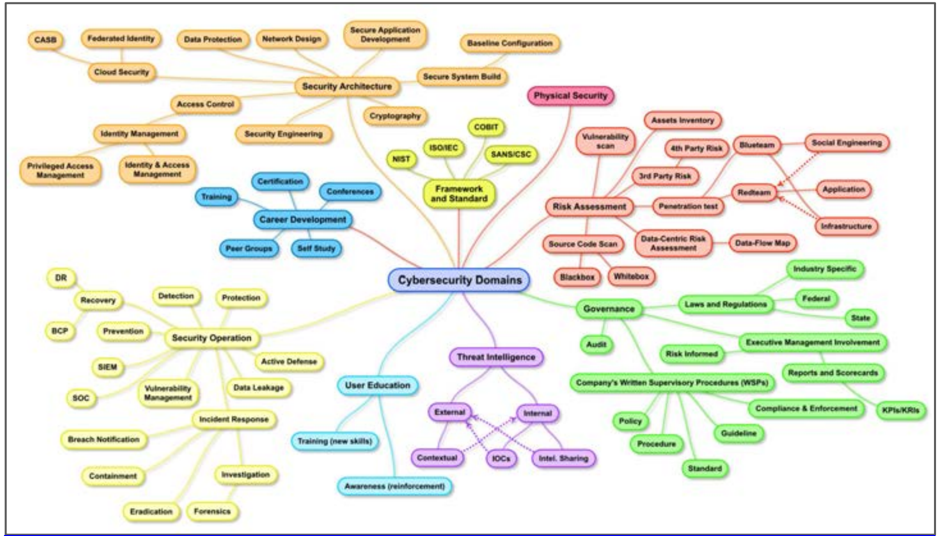
/ (ˈdɔːntɪŋ) /

SEE SYNONYMS FOR *daunting* ON THESAURUS.COM

adjective

1 causing fear or discouragement; intimidating

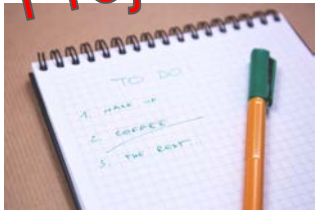
CISO’s World



- Cybersecurity Domains
  - Security Architecture
    - Cloud Security
      - CASB
      - Federated Identity
    - Data Protection
    - Network Design
    - Secure Application Development
    - Secure System Build
      - Baseline Configuration
    - Access Control
      - Identity Management
        - Privileged Access Management
        - Identity & Access Management
    - Security Engineering
    - Cryptography
  - Framework and Standard
    - NIST
    - ISO/IEC
    - COBIT
    - SANS/CSC
  - Physical Security
  - Career Development
    - Training
    - Certification
    - Conferences
    - Peer Groups
    - Self Study
  - Risk Assessment
    - Vulnerability scan
    - Assets Inventory
    - 3rd Party Risk
      - 4th Party Risk
    - Penetration test
      - Blueteam
      - Redteam
        - Social Engineering
        - Application
        - Infrastructure
    - Source Code Scan
      - Blackbox
      - Whitebox
    - Data-Centric Risk Assessment
      - Data-Flow Map
  - Security Operation
    - Recovery
      - DR
      - BCP
    - Detection
    - Protection
    - Prevention
    - SIEM
    - SOC
    - Vulnerability Management
    - Active Defense
    - Data Leakage
    - Incident Response
      - Breach Notification
      - Containment
      - Eradication
      - Forensics
      - Investigation
  - User Education
    - Training (new skills)
    - Awareness (reinforcement)
  - Threat Intelligence
    - External
    - Internal
    - Contextual
    - IOCs
    - Intel. Sharing
  - Governance
    - Laws and Regulations
      - Industry Specific
      - Federal
      - State
    - Executive Management Involvement
      - Risk Informed
      - Reports and Scorecards
        - KPIs/KRIs
    - Audit
    - Company's Written Supervisory Procedures (WSPs)
      - Policy
      - Procedure
      - Standard
      - Guideline
      - Compliance & Enforcement

Source: Henry Jiang: Chief Information Security Officer at Diligent Corporation

Projects



Boy on a High Dive - Norman Rockwell - 1947

Priorities?

CISO’s World

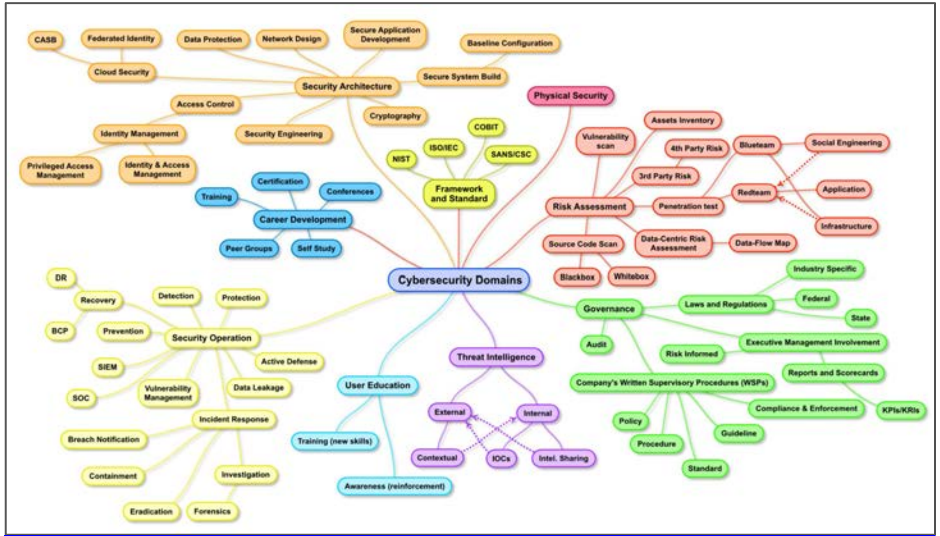
daunting ☆

/ (ˈdɔːntɪŋ) /

SEE SYNONYMS FOR *daunting* ON THESAURUS.COM

adjective

1 causing fear or discouragement; intimidating



Source: Henry Jiang: Chief Information Security Officer at Diligent Corporation

Crisis of the Day

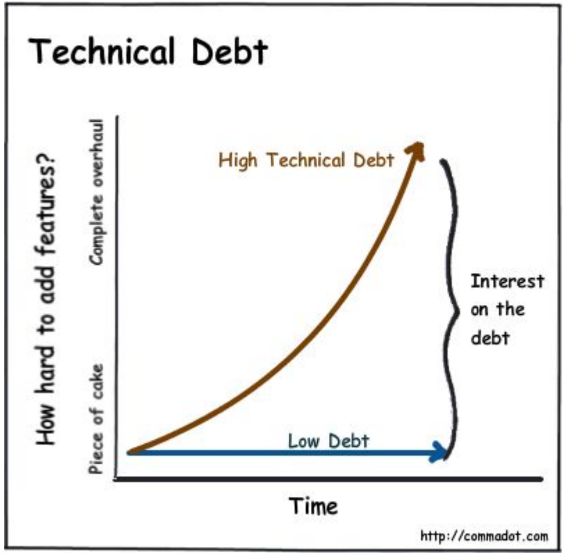
Crisis of the Day

Best Practice

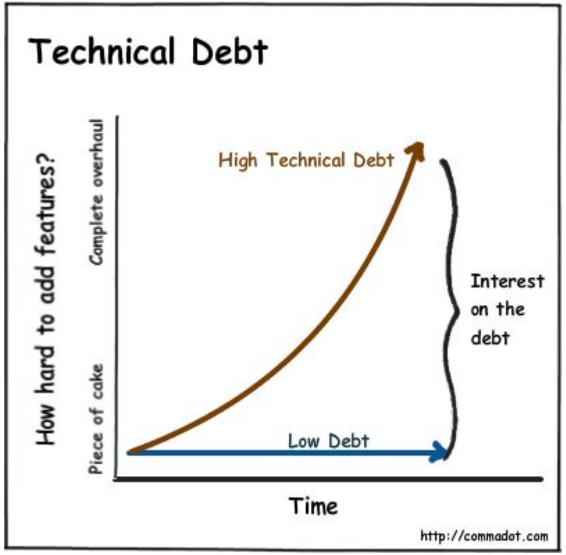
Crisis of the Day

Best Practice

Crisis of the Day

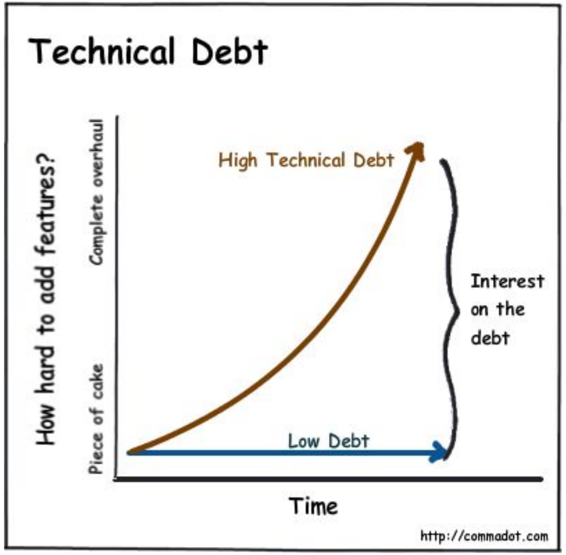


Crisis of the Day



Crisis of the Day

No Inovation



Crisis of the Day

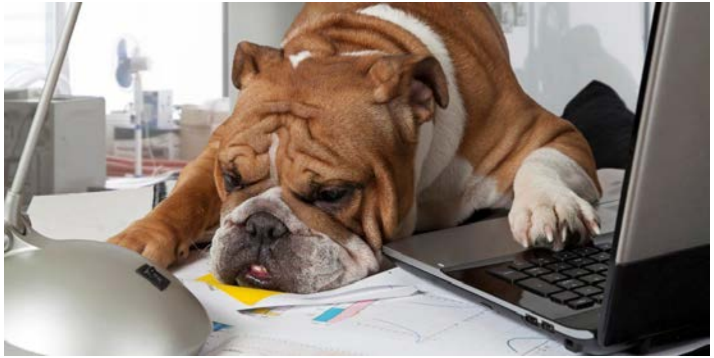
No Inovation

No new features

Old Fashioned

No Inovation

No new features

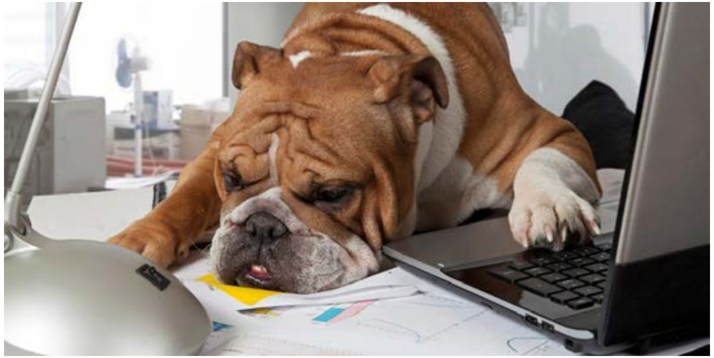


Old Fashioned

Exhausting

No Inovation

No new features

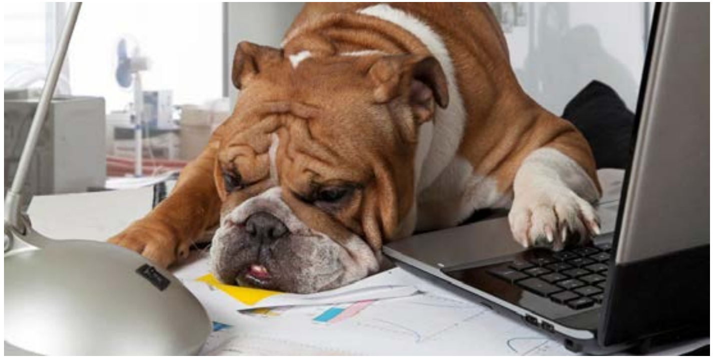


Old Fashioned

Exhausting

No Inovation

No new features

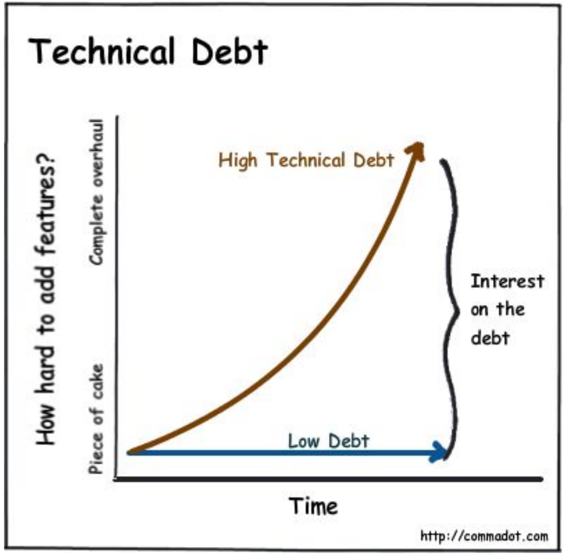


Old Fashioned

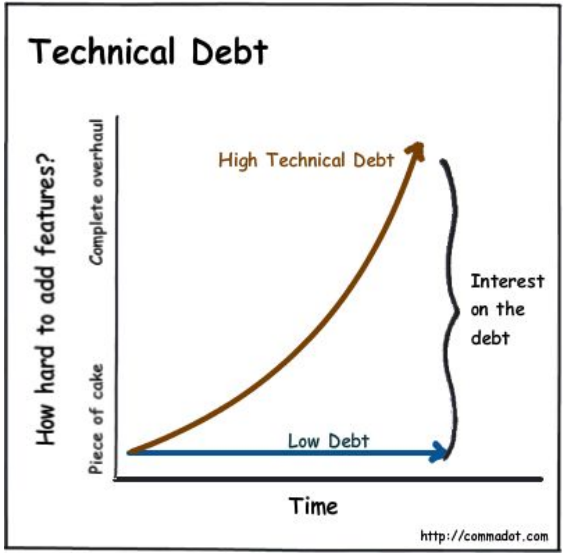
Exhausting

No Inovation

No new features

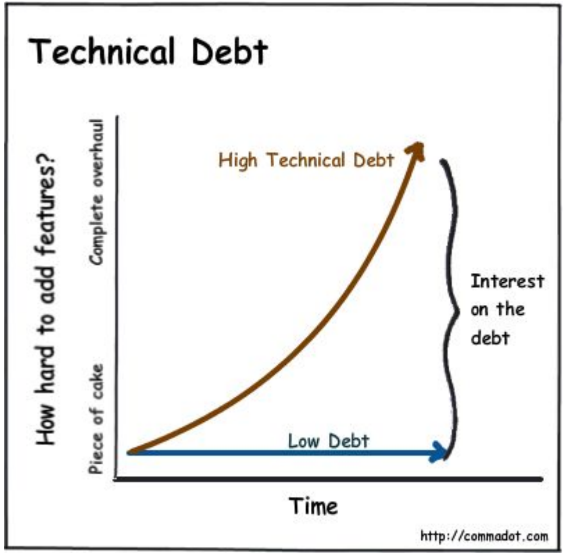

Technical Debt
How hard to add features?
Complete overhaul
Piece of cake
High Technical Debt
Low Debt
Interest on the debt
Time
http://commadot.com

NOT SUCKING
SUCKING
THE PAST
THE FUTURE
Progress


Technical Debt
How hard to add features?
Complete overhaul
Piece of cake
High Technical Debt
Interest on the debt
Low Debt
Time
http://commadot.com

NOT SUCKING
SUCKING
THE PAST
THE FUTURE
Progress

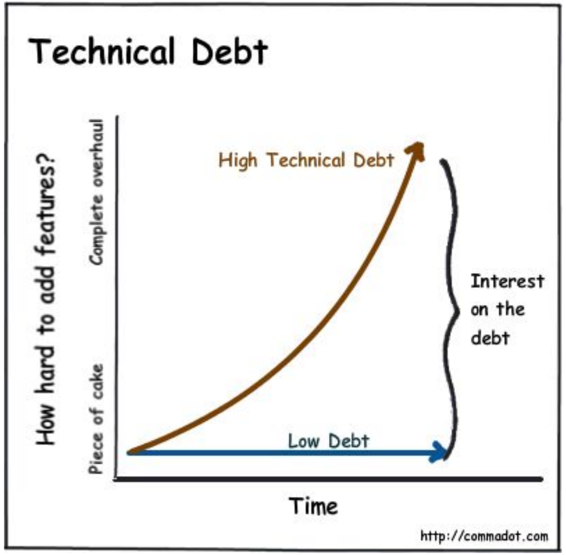
Done

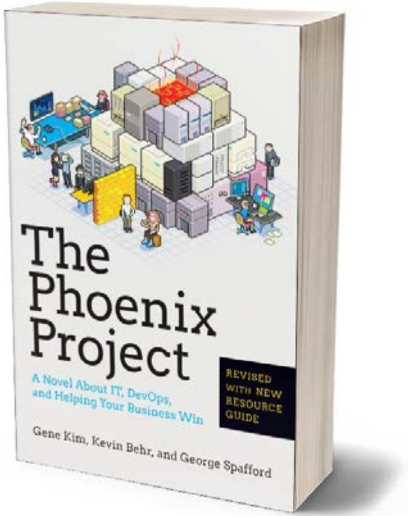

Technical Debt
How hard to add features?
Complete overhaul
Piece of cake
High Technical Debt
Low Debt
Interest on the debt
Time
http://commadot.com

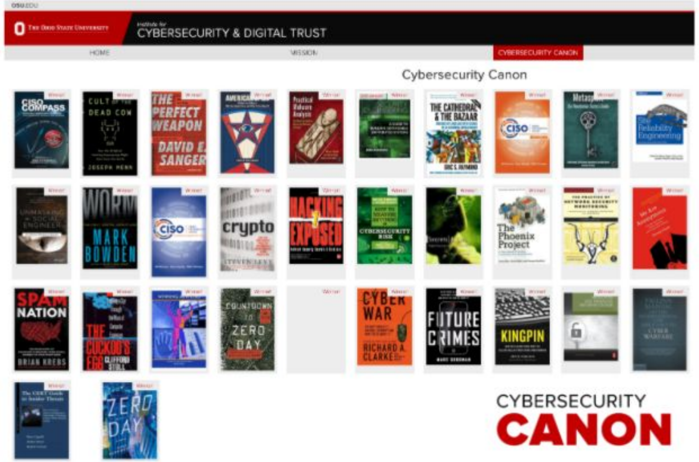
Another Way

NOT SUCKING
SUCKING
THE PAST
THE FUTURE
Progress

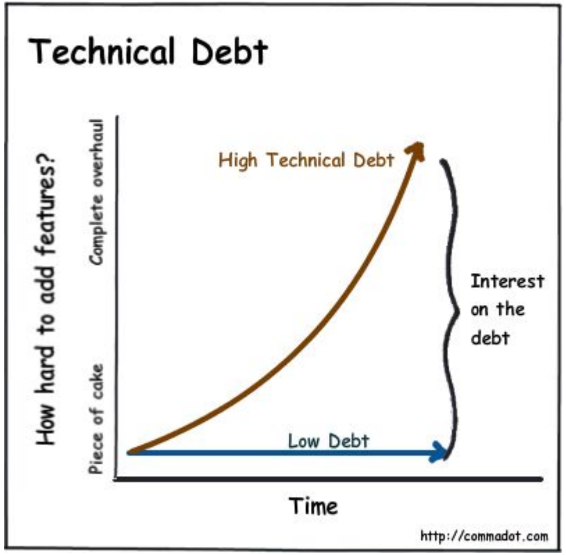
Done



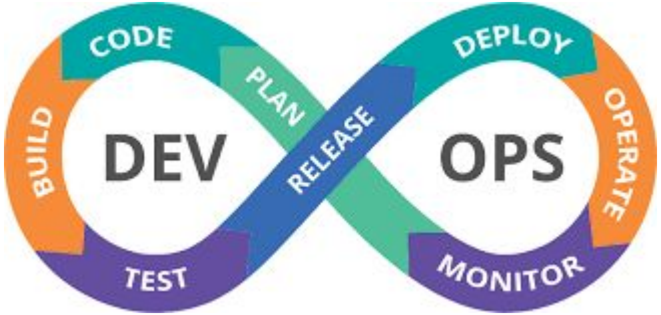

The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win
REVISED WITH NEW RESOURCE GUIDE
Gene Kim, Kevin Behr, and George Spafford

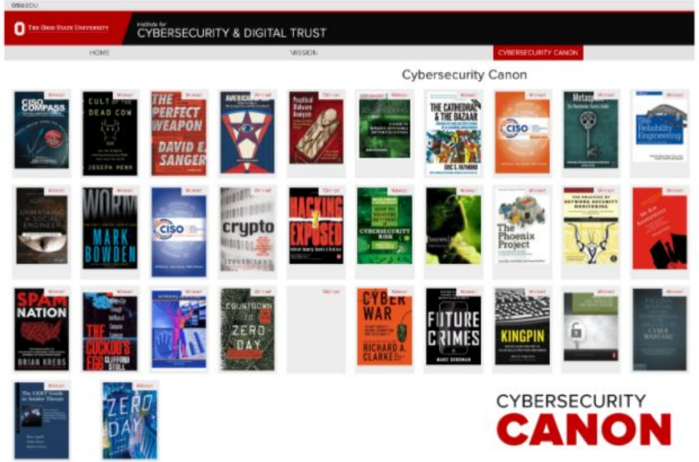


Cybersecurity Canon


Technical Debt
How hard to add features?
Complete overhaul
Piece of cake
High Technical Debt
Low Debt
Interest on the debt
Time
http://commadot.com

The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win
REVISED WITH NEW RESOURCE GUIDE
Gene Kim, Kevin Behr, and George Spafford

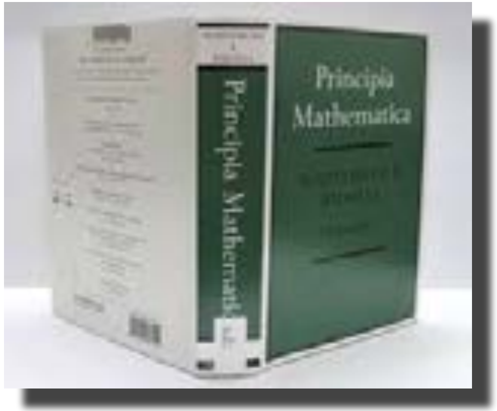

CODE
PLAN
BUILD
DEV
TEST
RELEASE
DEPLOY
OPS
OPERATE
MONITOR


THE OHIO STATE UNIVERSITY
Institute for CYBERSECURITY & DIGITAL TRUST
HOME
MISSION
CYBERSECURITY CANON
Cybersecurity Canon
CYBERSECURITY CANON

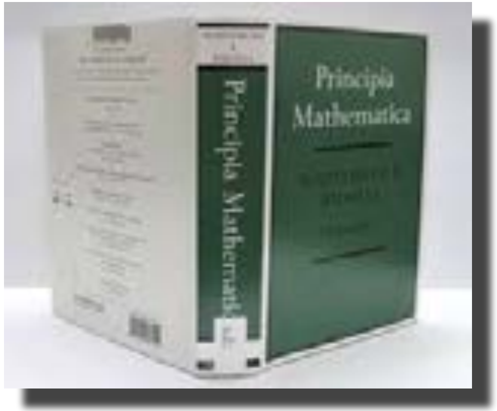
Whitehead

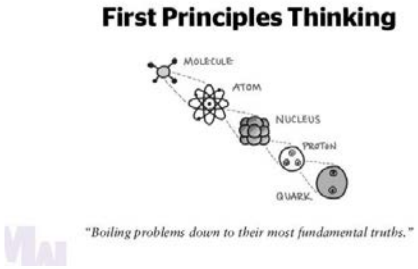
Russell

***Principia Mathematica* published in 1910**



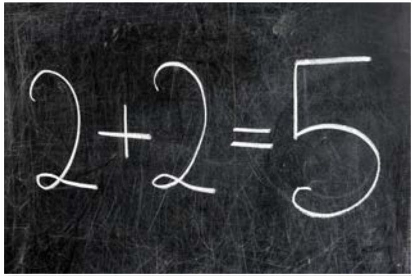
Principia Mathematica published in 1910

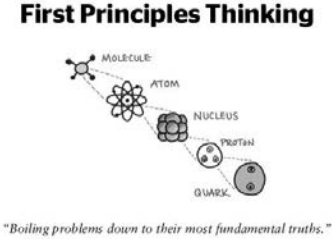




"Boiling problems down to their most fundamental truths."

Principia Mathematica published in 1910

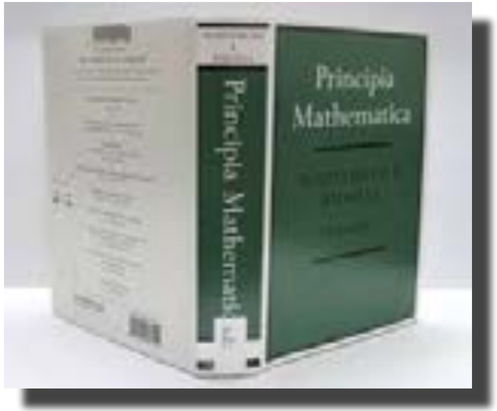


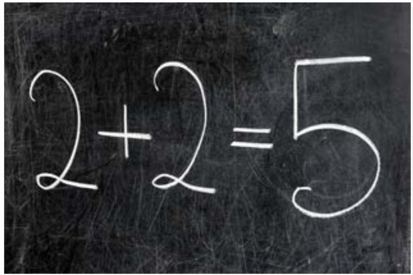


First Principles Thinking

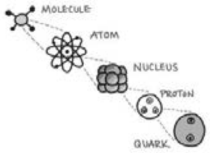
"Boiling problems down to their most fundamental truths."

Principia Mathematica published in 1910

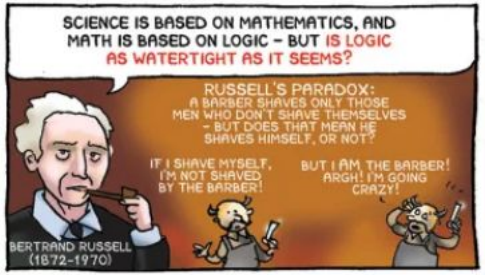




First Principles Thinking



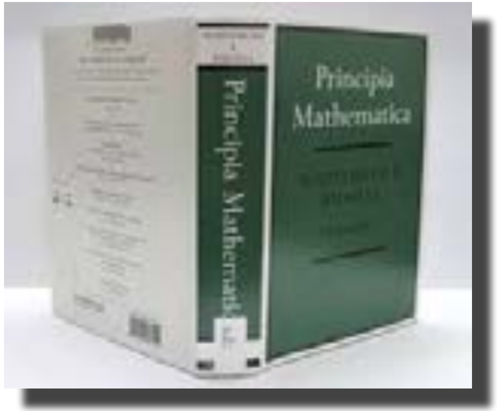
"Boiling problems down to their most fundamental truths."

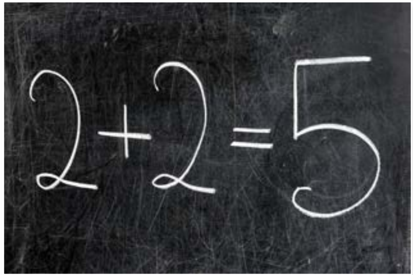

SCIENCE IS BASED ON MATHEMATICS, AND MATH IS BASED ON LOGIC – BUT IS LOGIC AS WATERTIGHT AS IT SEEMS?
RUSSELL'S PARADOX: A BARBER SHAVES ONLY THOSE MEN WHO DON'T SHAVE THEMSELVES – BUT DOES THAT MEAN HE SHAVES HIMSELF, OR NOT?
IF I SHAVE MYSELF, I'M NOT SHAVED BY THE BARBER!
BUT I AM THE BARBER! ARGH! I'M GOING CRAZY!
BERTRAND RUSSELL (1872-1970)

Source: "Science: A Discovery in Comics," by Margreet de Heer

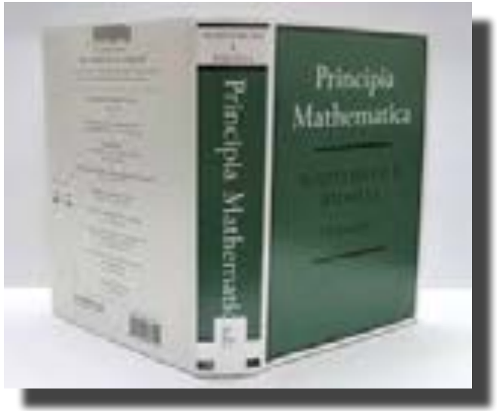
Whitehead

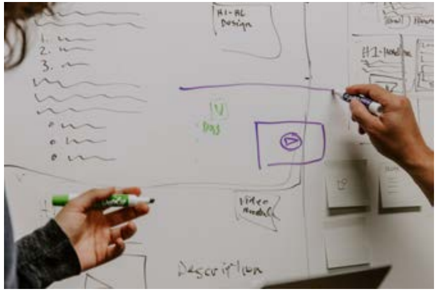
Russell


Principia Mathematica
Principia Mathematica


2+2=5

CITIES SKYLINES
PRECISION ENGINEERING

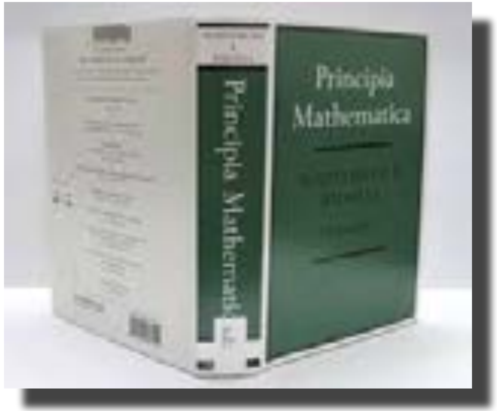


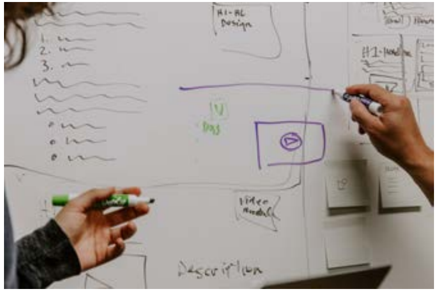


Drawing Board

80 Pages

$$1 + 1 = 2$$

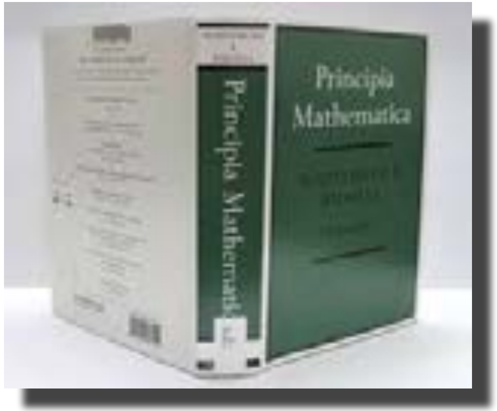




Drawing Board

80 Pages

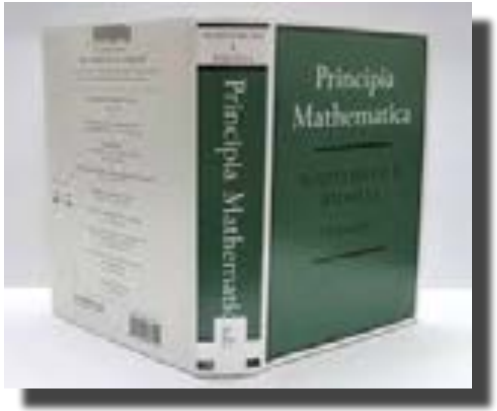
$$1 + 1 = 2$$



*Note: Might be useful to know

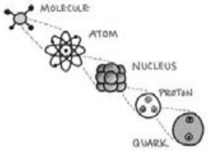
80 Pages

$$1 + 1 = 2$$



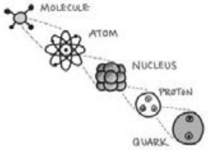
*Note: Might be useful to know

First Principles Thinking

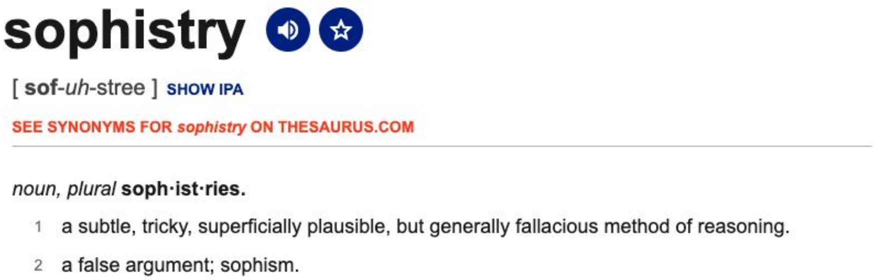


"Boiling problems down to their most fundamental truths."

First Principles Thinking



"Boiling problems down to their most fundamental truths."



sophistry

[**sof**-*uh*-stree] SHOW IPA

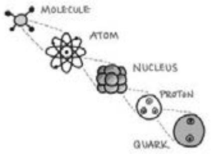
SEE SYNONYMS FOR *sophistry* ON THESAURUS.COM

noun, plural **soph·ist·ries.**

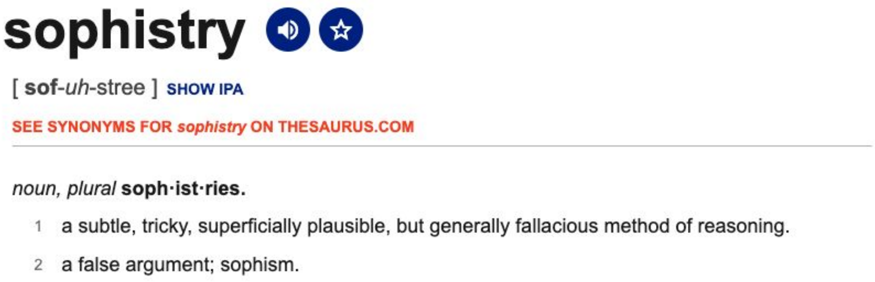
1 a subtle, tricky, superficially plausible, but generally fallacious method of reasoning.

2 a false argument; sophism.

First Principles Thinking



"Boiling problems down to their most fundamental truths."



sophistry

[sof-*uh*-stree] **SHOW IPA**

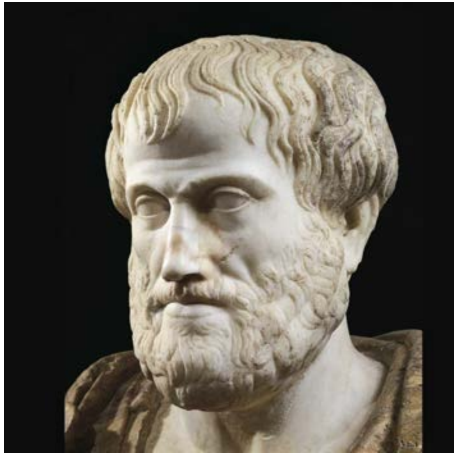
SEE SYNONYMS FOR *sophistry* ON THESAURUS.COM

noun, plural **soph·ist·ries.**

1 a subtle, tricky, superficially plausible, but generally fallacious method of reasoning.

2 a false argument; sophism.

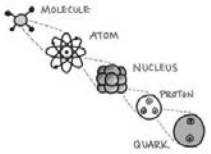
Aristotle



Source: "Aristotle: Biography, History and Contributions," by World History Edu

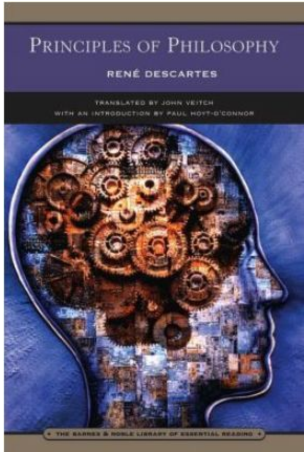
*"In every systematic inquiry where there are **first principles**, or causes, or elements, […] science result[s] from acquiring knowledge of these."*

First Principles Thinking



"Boiling problems down to their most fundamental truths."

1644



PRINCIPLES OF PHILOSOPHY

RENÉ DESCARTES

TRANSLATED BY JOHN VEITCH
WITH AN INTRODUCTION BY PAUL HOYT-O'CONNOR

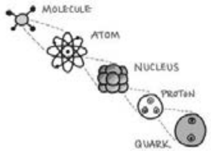
THE BARNES & NOBLE LIBRARY OF ESSENTIAL READING

René Descartes

Source: "René Descartes," by Britanica

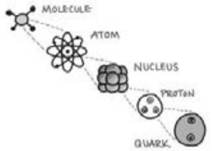
*"… in order to study the acquisition of [knowledge], we must commence with the investigation of those **first causes** which are called **Principles**."*

First Principles Thinking



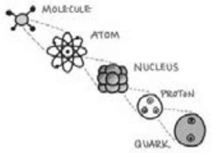
"Boiling problems down to their most fundamental truths."

First Principles Thinking



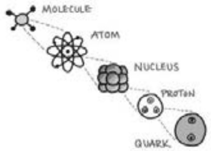
"Boiling problems down to their most fundamental truths."

First Principles Thinking



"Boiling problems down to their most fundamental truths."

First Principles Thinking



"Boiling problems down to their most fundamental truths."

Elon Musk

NASA

Elon Musk

BOEING

NASA

Elon Musk

BOEING

NASA

Apollo

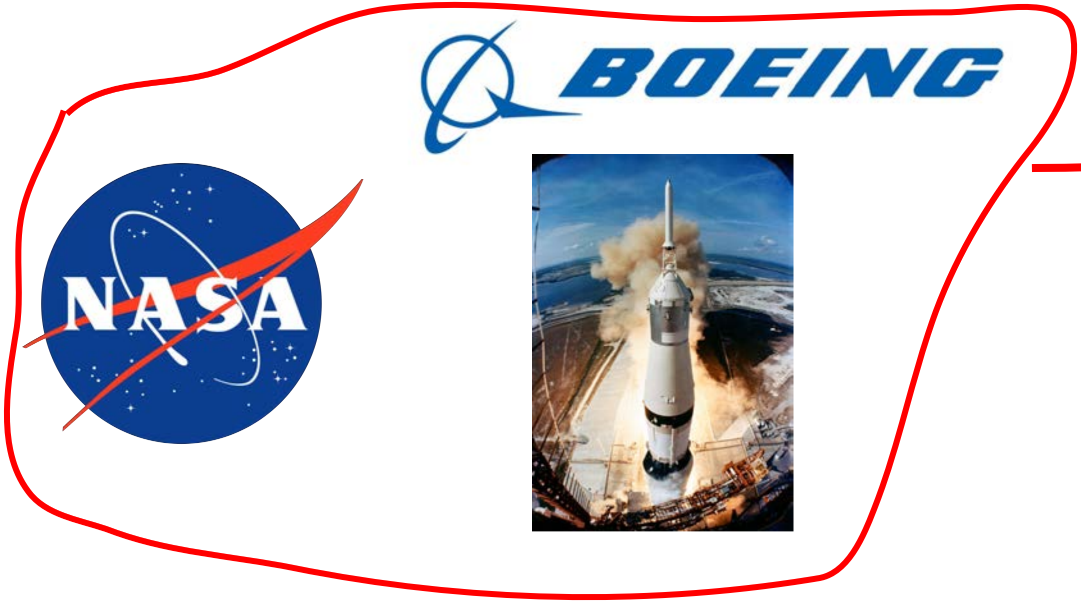
Elon Musk

BOEING

NASA

Apollo

Elon Musk



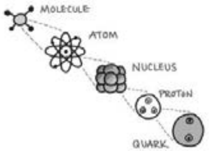
Elon Musk

BOEING

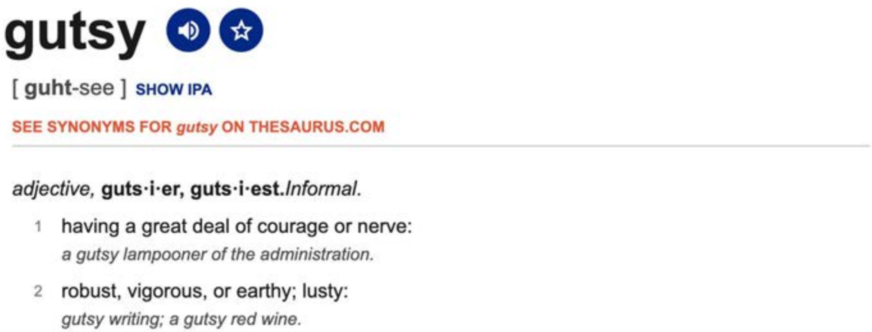
NASA

Elon Musk

First Principles Thinking



"Boiling problems down to their most fundamental truths."



gutsy

[guht-see] SHOW IPA

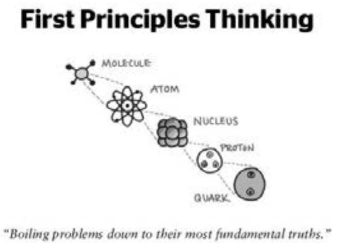
SEE SYNONYMS FOR *gutsy* ON THESAURUS.COM

adjective, **guts·i·er, guts·i·est.***Informal.*

1 having a great deal of courage or nerve:
a gutsy lampooner of the administration.

2 robust, vigorous, or earthy; lusty:
gutsy writing; a gutsy red wine.

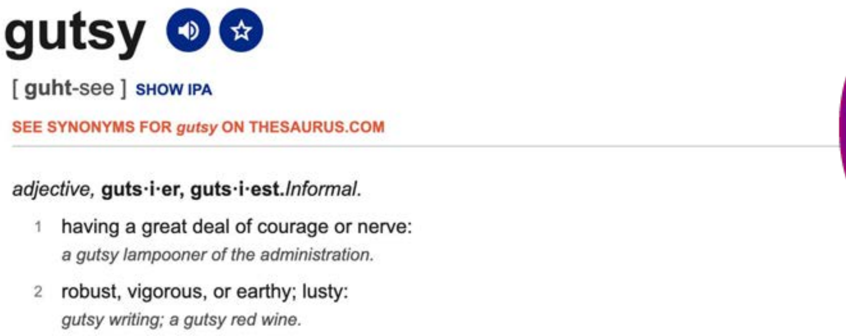
Elon Musk



First Principles Thinking

"Boiling problems down to their most fundamental truths."

Gazillionaire!™



gutsy

[guht-see] SHOW IPA

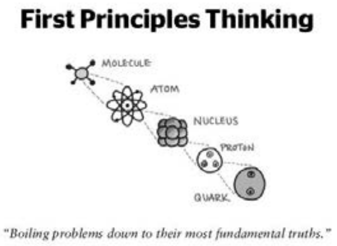
SEE SYNONYMS FOR *gutsy* ON THESAURUS.COM

adjective, **guts·i·er, guts·i·est.***Informal.*

1 having a great deal of courage or nerve:
a gutsy lampooner of the administration.

2 robust, vigorous, or earthy; lusty:
gutsy writing; a gutsy red wine.

Elon Musk



First Principles Thinking

"Boiling problems down to their most fundamental truths."

What are First Principles?

What are First Principles?

Fundamental

What are First Principles?

Fundamental

Self Evident

What are First Principles?

Fundamental

Self Evident

Elementary

What are First Principles?

Fundamental

Self Evident

Elementary

Experts Agree

What are First Principles?

Fundamental

Self Evident

Elementary

Experts Agree

Crucial to understanding

What are First Principles?

Fundamental

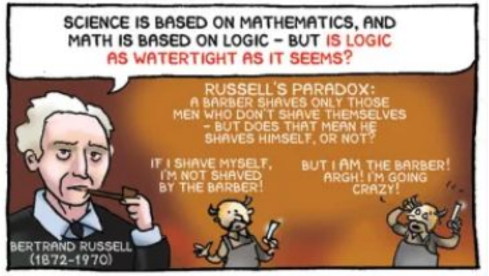
Self Evident

Elementary

Experts Agree

Crucial to understanding

What are First Principles?


SCIENCE IS BASED ON MATHEMATICS, AND MATH IS BASED ON LOGIC – BUT IS LOGIC AS WATERTIGHT AS IT SEEMS?
RUSSELL'S PARADOX: A BARBER SHAVES ONLY THOSE MEN WHO DON'T SHAVE THEMSELVES – BUT DOES THAT MEAN HE SHAVES HIMSELF, OR NOT?
IF I SHAVE MYSELF, I'M NOT SHAVED BY THE BARBER!
BUT I AM THE BARBER! ARGH! I'M GOING CRAZY!
BERTRAND RUSSELL (1872-1970)

Source: "Science: A Discovery in Comics," by Margreet de Heer

Fundamental

Self Evident

Elementary

Experts Agree

Crucial to understanding

What are First Principles?

Atomic

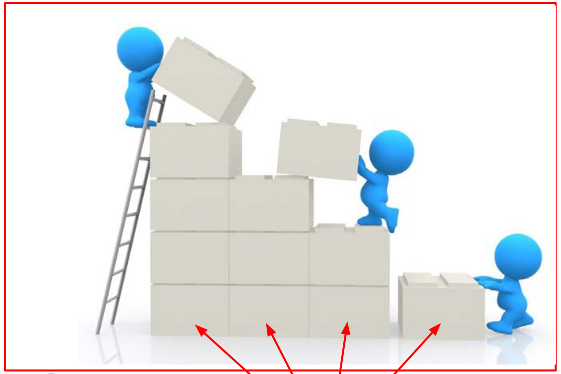
What are First Principles?

Atomic

What are First Principles?

Atomic

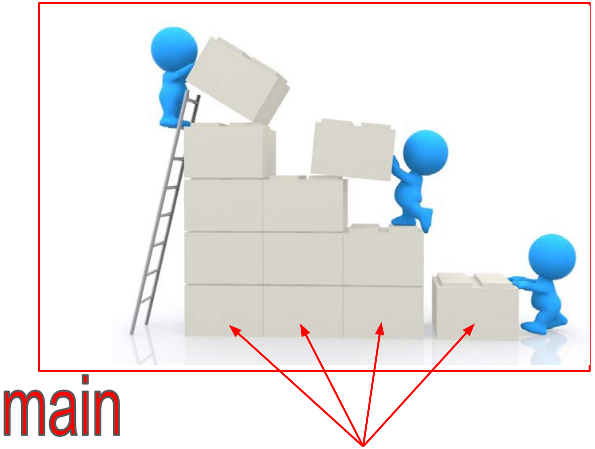
What are First Principles?



Problem Domain

Atomic

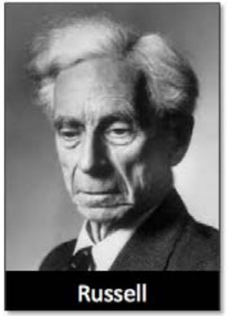
What are First Principles?



Problem Domain

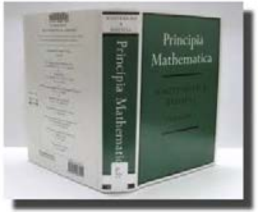
Atomic

Whitehead


Russell

80 Pages

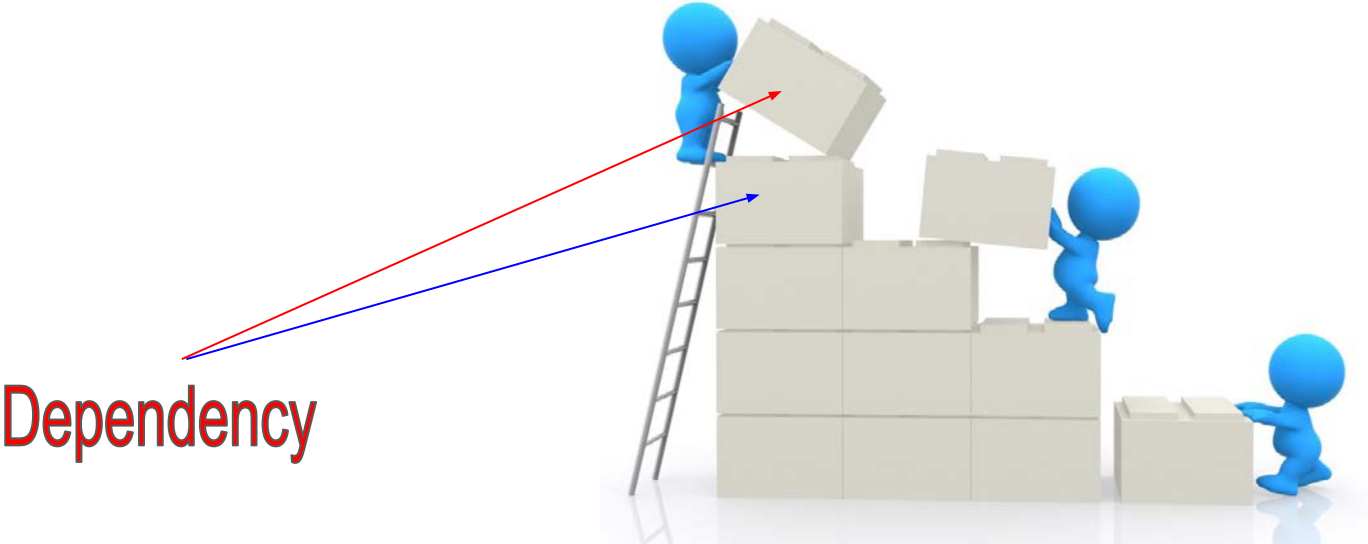
$1 + 1 = 2$



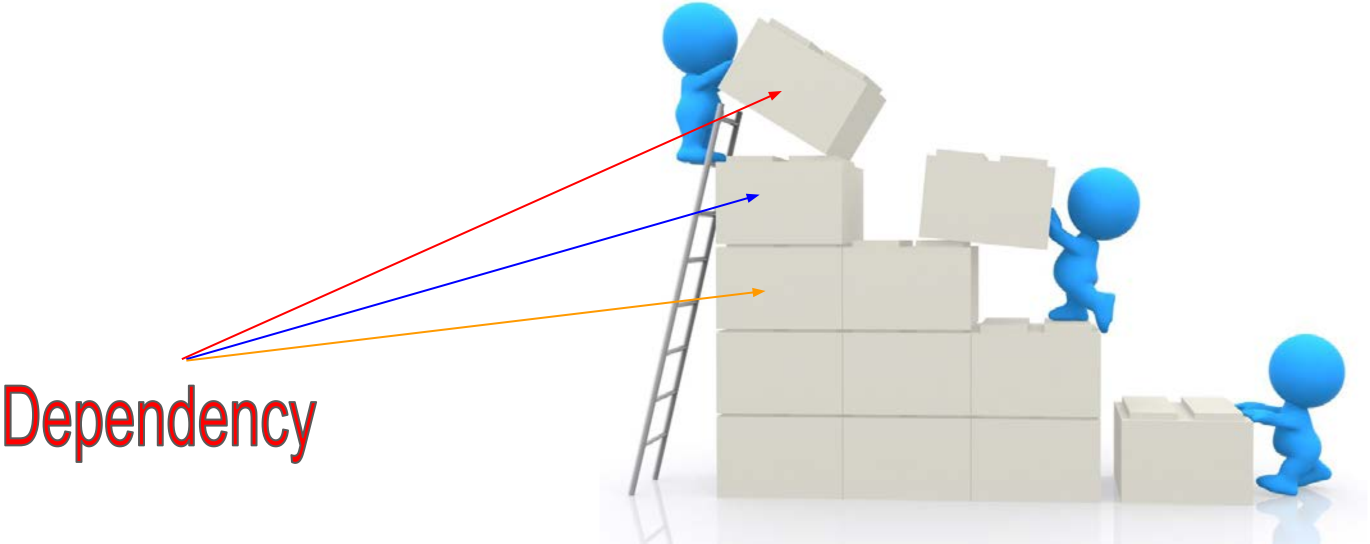
What are First Principles?

What are First Principles?

What are First Principles?

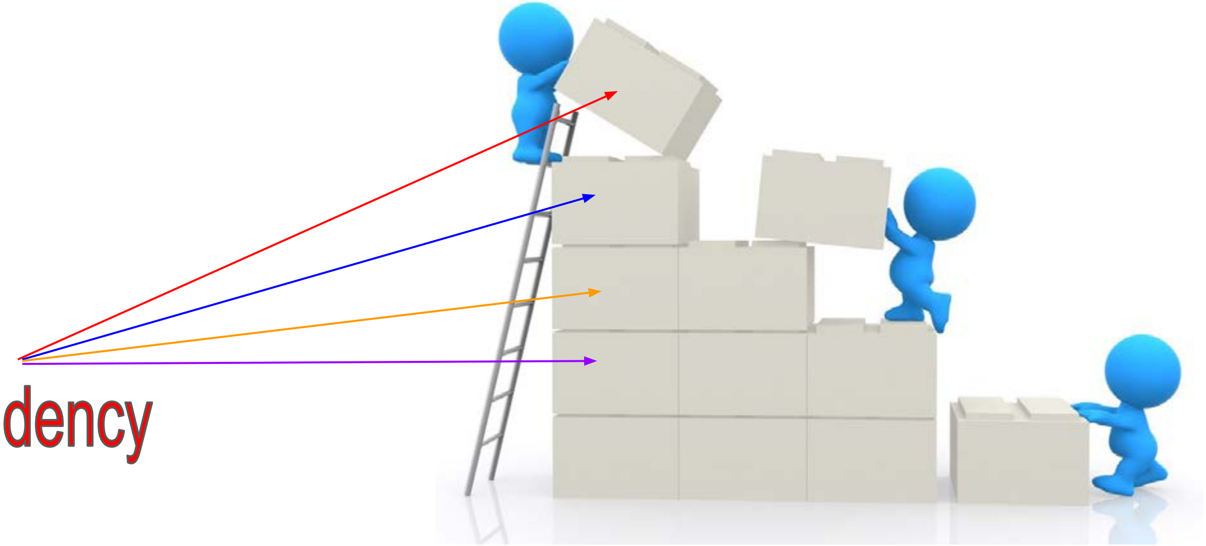


What are First Principles?



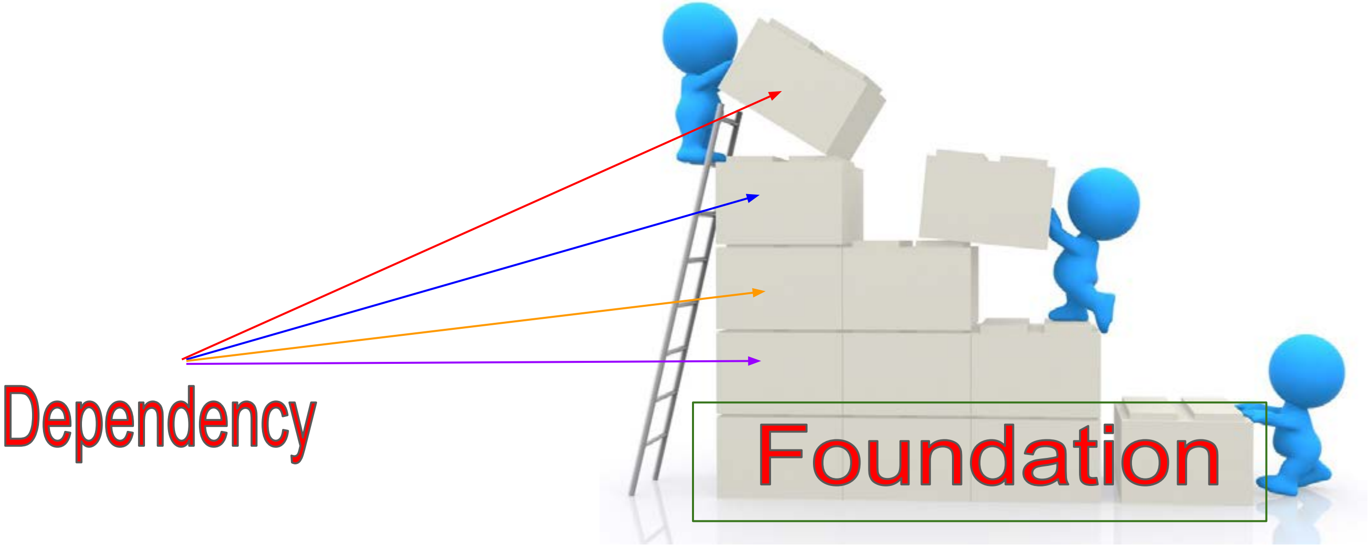
Dependency

What are First Principles?



Dependency

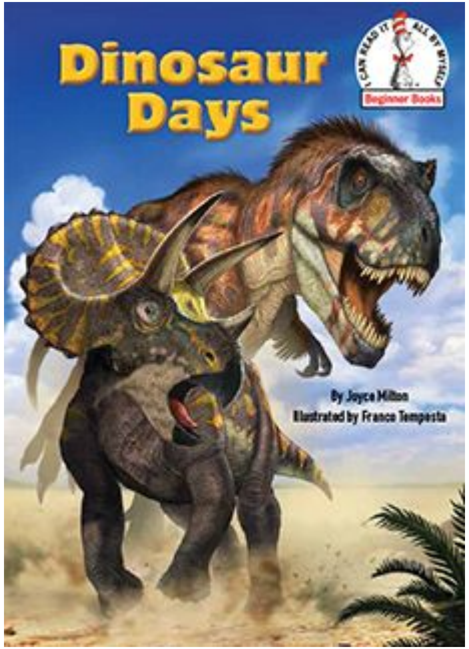
What are First Principles?



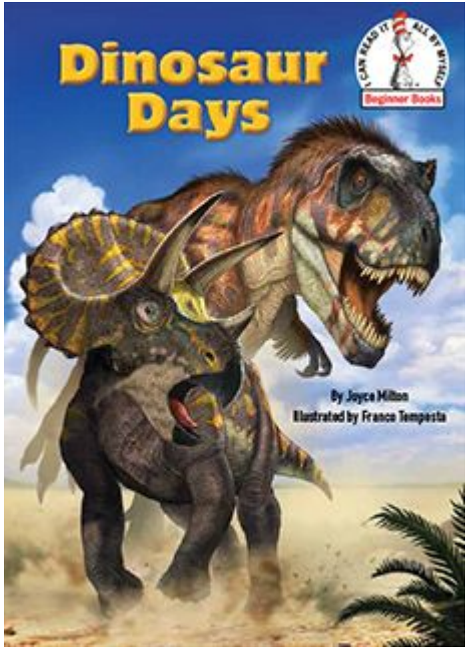
Dependency

Foundation

What is the network defender's ultimate First Principle?


Dinosaur Days
I CAN READ IT ALL BY MYSELF
Beginner Books
By Joyce Milton
Illustrated by Franco Tempesta

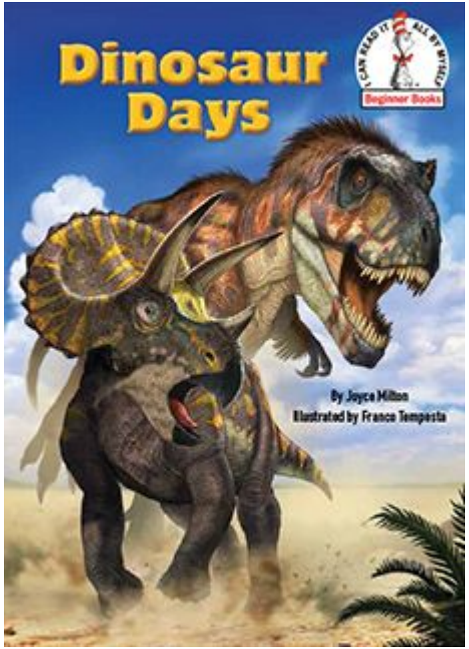
Mid-1990s



The original iPhone

Mid-1990s

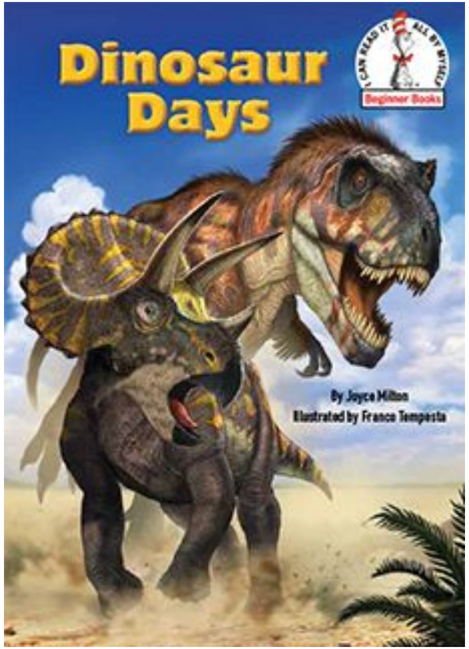
BA - Before Apple



The original iPhone

Mid-1990s

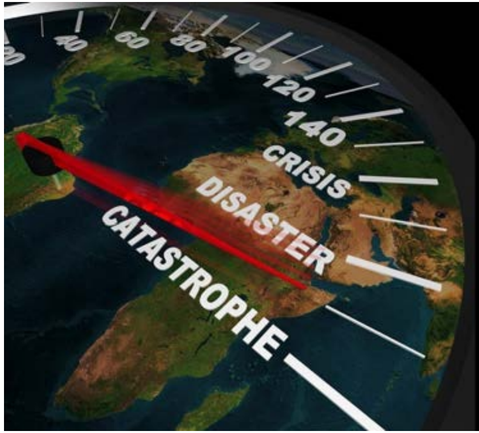
BA - Before Apple



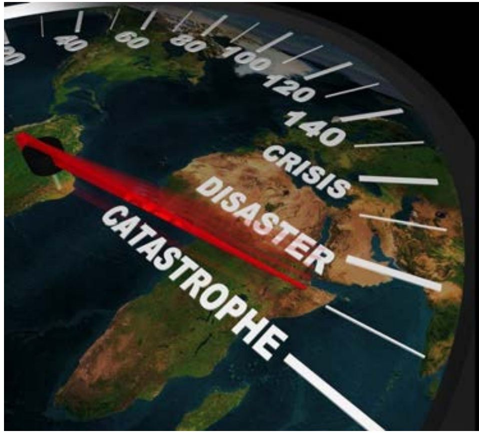
The original iPhone

Mid-1990s

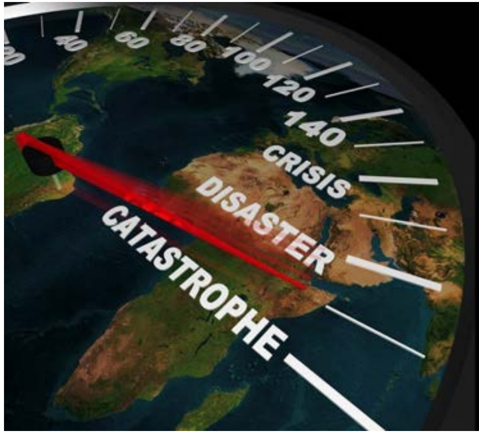
BA - Before Apple



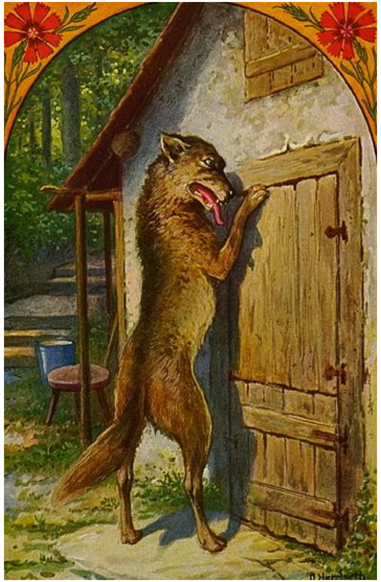
Zero Day Vulnerability in an Obscure and Never Used Printer Driver.

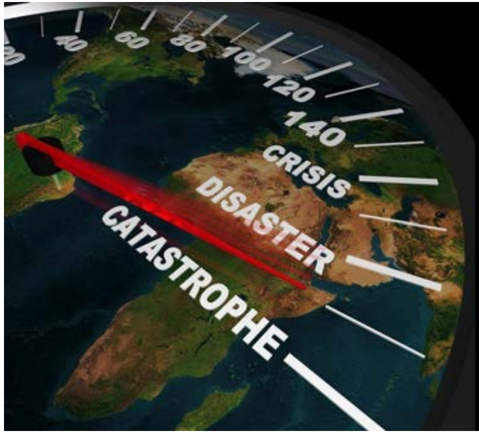


Zero Day Vulnerability in an Obscure and Never Used Printer Driver.

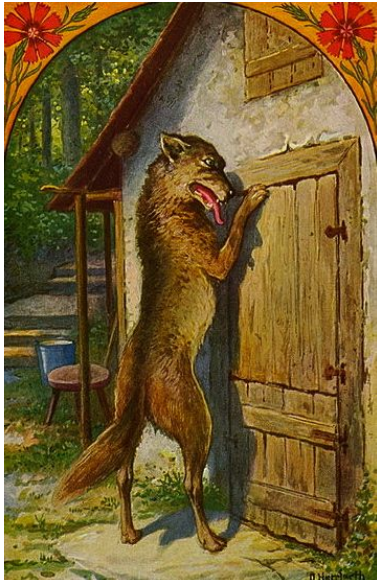


Zero Day Vulnerability in an Obscure and Never Used Printer Driver.





Zero Day Vulnerability in an Obscure and Never Used Printer Driver.



World’s End

Older and Wiser

Older and Wiser

Fatter and Lazier

Older and Wiser

Fatter and Lazier

No energy for that nonsense

What is the network defender's ultimate First Principle?

Foundation

1 What is the network defender's ultimate First Principle?

→ **Prevent All Breaches**

Foundation

What is the network defender’s ultimate First Principle?

→ **Prevent All Breaches**

Foundation

What is the network defender's ultimate First Principle?

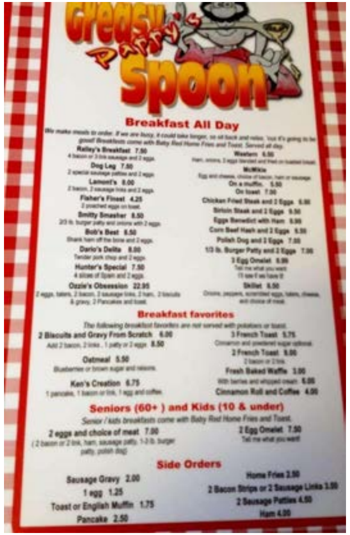
→ **Prevent All Breaches**

Foundation

Crown Jewels

What is the network defender's ultimate First Principle?

Prevent All Breaches



Greasy Pappy's Spoon

Breakfast All Day

We make meals to order. If we are busy, it could take longer, so sit back and relax. but it's going to be good! Breakfasts come with Baby Red Home Fries and Toast. Served all day.

Railey's Breakfast 7.50
4 bacon or 3 link sausage and 2 eggs.

Dog Leg 7.50
2 special sausage patties and 2 eggs.

Lamont's 8.00
2 bacon, 2 sausage links and 2 eggs.

Fisher's Finest 4.25
2 poached eggs on toast.

Smitty Smasher 8.50
2/3 lb. burger patty and onions with 2 eggs.

Bob's Best 8.50
Shank ham off the bone and 2 eggs.

Dario's Delite 8.00
Tender pork chop and 2 eggs.

Hunter's Special 7.50
4 slices of Spam and 2 eggs.

Ozzie's Obsession 22.95
2 eggs, taters, 2 bacon, 2 sausage links, 2 ham, 2 biscuits & gravy, 2 Pancakes and toast.

Western 6.50
Ham, onions, 2 eggs blended and fried on toasted bread.

McMike
Egg and cheese, choice of bacon, ham or sausage
On a muffin. 5.50
On toast 7.00

Chicken Fried Steak and 2 Eggs 8.00

Sirloin Steak and 2 Eggs 9.50

Eggs Benedict with Ham 9.00

Corn Beef Hash and 2 Eggs 9.50

Polish Dog and 2 Eggs 7.00

1/3 lb. Burger Patty and 2 Eggs 7.00

3 Egg Omelet 8.00
Tell me what you want
I'll see if we have it

Skillet 8.50
Onions, peppers, scrambled eggs, taters, cheese, and choice of meat.

Breakfast favorites

The following breakfast favorites are not served with potatoes or toast.

2 Biscuits and Gravy From Scratch 6.00
Add 2 bacon, 2 links, 1 patty or 2 eggs 8.50

Oatmeal 5.50
Blueberries or brown sugar and raisins.

Ken's Creation 6.75
1 pancake, 1 bacon or link, 1 egg and coffee.

3 French Toast 5.75
Cinnamon and powdered sugar optional.

2 French Toast 8.00
2 bacon or 2 link.

Fresh Baked Waffle 3.00
With berries and whipped cream 5.00

Cinnamon Roll and Coffee 4.00

Seniors (60+) and Kids (10 & under)

Senior / kids breakfasts come with Baby Red Home Fries and Toast.

2 eggs and choice of meat 7.00
(2 bacon or 2 link, ham, sausage patty, 1-3 lb. burger patty, polish dog)

2 Egg Omelet 7.50
Tell me what you want

Side Orders

Sausage Gravy 2.00

1 egg 1.25

Toast or English Muffin 1.75

Pancake 2.50

Home Fries 2.50

2 Bacon Strips or 2 Sausage Links 3.00

2 Sausage Patties 4.50

Ham 4.00

Foundation

Crown Jewels

What is the network defender's ultimate First Principle?

Prevent All Breaches

Greasy Pappy's Spoon

Breakfast All Day

We make meals to order. If we are busy, it could take longer, so sit back and relax. [illegible] good! Breakfasts come with Baby Red Home Fries and Toast. Served all day.

Railey's Breakfast 7.50
4 bacon or 3 link sausage and 2 eggs.

Dog Leg 7.50
2 special sausage patties and 2 eggs.

Lamont's 8.00
2 bacon, 2 sausage links and 2 eggs.

Fisher's Finest 4.25
2 poached eggs on toast.

Smitty Smasher 8.50
2/3 lb. burger patty and onions with 2 eggs.

Bob's Best 8.50
Shank ham off the bone and 2 eggs.

Dario's Delite 8.00
Tender pork chop and 2 eggs.

Hunter's Special 7.50
4 slices of Spam and 2 eggs.

Ozzie's Obsession 22.95
2 eggs, taters, 2 bacon, 2 sausage links, 2 ham, 2 biscuits & gravy, 2 Pancakes and toast.

Western 6.50
Ham, onions, 2 eggs blended and fried on toasted bread.

McMikie
Egg and cheese, choice of bacon, ham or sausage.
On a muffin. 5.50
On toast 7.00

Chicken Fried Steak and 2 Eggs 8.00

Sirloin Steak and 2 Eggs 9.50

Eggs Benedict with Ham 9.00

Corn Beef Hash and 2 Eggs 9.50

Polish Dog and 2 Eggs 7.00

1/3 lb. Burger Patty and 2 Eggs 7.00

3 Egg Omelet 8.00
Tell me what you want
I'll see if we have it

Skillet 8.50
Onions, peppers, scrambled eggs, taters, cheese and choice of meat.

Breakfast favorites

The following breakfast favorites are not served with potatoes or toast.

2 Biscuits and Gravy From Scratch 6.00
Add 2 bacon, 2 links, 1 patty or 2 eggs 8.50

Oatmeal 5.50
Blueberries or brown sugar and raisins.

Ken's Creation 6.75
1 pancake, 1 bacon or link, 1 egg and coffee.

3 French Toast 5.75
Cinnamon and powdered sugar optional.

2 French Toast 6.00
2 bacon or 2 link.

Fresh Baked Waffle 3.00
With berries and whipped cream 5.00

Cinnamon Roll and Coffee 4.00

Seniors (60+) and Kids (10 & under)

Senior / kids breakfasts come with Baby Red Home Fries and Toast.

2 eggs and choice of meat 7.00
(2 bacon or 2 link, ham, sausage patty, 1/3 lb. burger patty, polish dog)

2 Egg Omelet 7.50
Tell me what you want

Side Orders

Sausage Gravy 2.00

1 egg 1.25

Toast or English Muffin 1.75

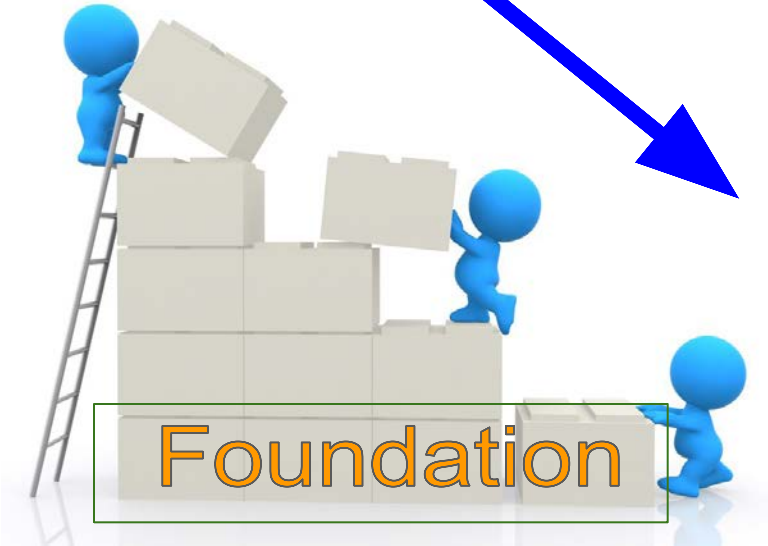
Pancake 2.50

Home Fries 2.50

2 Bacon Strips or 2 Sausage Links 3.00

2 Sausage Patties 4.50

Ham 4.00



Foundation

Crown Jewels

What is the network defender's ultimate First Principle?

Prevent All Breaches

Greasy Parry's Spoon

Breakfast All Day

We make meals to order. If we are busy, it could take longer, so sit back and relax, but it's going to be good! Breakfasts come with Baby Red Home Fries and Toast. Served all day.

Ralley's Breakfast 7.50
4 bacon or 3 link sausage and 2 eggs.

Dog Leg 7.50
2 special sausage patties and 2 eggs.

Lamont's 8.00
2 bacon, 2 sausage links and 2 eggs.

Fisher's Finest 4.25
2 poached eggs on toast.

Smitty Smasher 8.50
2/3 lb. burger patty and onions with 2 eggs.

Bob's Best 8.50
Shank ham off the bone and 2 eggs.

Dario's Delite 8.00
Tender pork chop and 2 eggs.

Hunter's Special 7.50
4 slices of Spam and 2 eggs.

Ozzie's Obsession 22.95
2 eggs, taters, 2 bacon, 2 sausage links, 2 ham, 2 biscuits & gravy, 2 Pancakes and toast.

Western 6.50
Ham, onions, 2 eggs blended and fried on toasted bread.

McMikie
Egg and cheese, choice of bacon, ham or sausage.
On a muffin. 5.50
On toast 7.00

Chicken Fried Steak and 2 Eggs 8.00

Sirloin Steak and 2 Eggs 9.50

Eggs Benedict with Ham 8.00

Corn Beef Hash and 2 Eggs 9.50

Polish Dog and 2 Eggs 7.00

1/3 lb. Burger Patty and 2 Eggs 7.00

3 Egg Omelet 6.99
Tell me what you want
I'll see if we have it

Skillet 8.50
Onions, peppers, scrambled eggs, taters, cheese and choice of meat.

Breakfast favorites

The following breakfast favorites are not served with potatoes or toast.

2 Biscuits and Gravy From Scratch 6.00
Add 2 bacon, 2 links, 1 patty or 2 eggs 8.50

Oatmeal 5.50
Blueberries or brown sugar and raisins.

Ken's Creation 6.75
1 pancake, 1 bacon or link, 1 egg and coffee.

3 French Toast 5.75
Cinnamon and powdered sugar optional.

2 French Toast 8.00
2 bacon or 2 link.

Fresh Baked Waffle 3.00
With berries and whipped cream 5.00

Cinnamon Roll and Coffee 4.00

Seniors (60+) and Kids (10 & under)

Senior / kids breakfasts come with Baby Red Home Fries and Toast.

2 eggs and choice of meat 7.00
(2 bacon or 2 link, ham, sausage patty, 1/3 lb. burger patty, polish dog)

2 Egg Omelet 7.50
Tell me what you want

Side Orders

Sausage Gravy 2.00
1 egg 1.25
Toast or English Muffin 1.75
Pancake 2.50

Home Fries 2.50
2 Bacon Strips or 2 Sausage Links 3.50
2 Sausage Patties 4.50
Ham 4.00

Foundation

Crown Jewels

What is the network defender's ultimate First Principle?

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?

Prevent All Breaches

No Flexibility

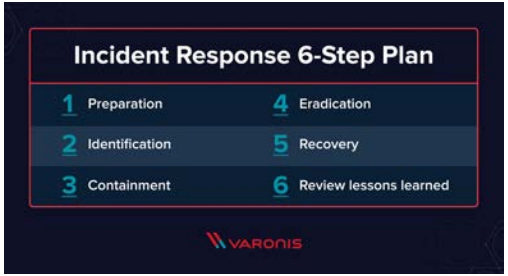
Foundation

What is the network defender's ultimate First Principle?

→ **Prevent All Breaches**

No Flexibility

Foundation



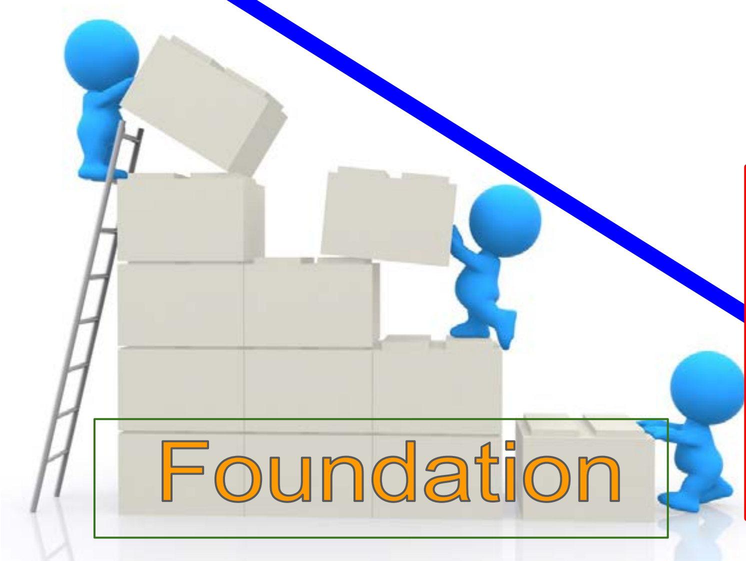
Incident Response 6-Step Plan

1 Preparation	4 Eradication
2 Identification	5 Recovery
3 Containment	6 Review lessons learned

VARONIS

What is the network defender’s ultimate First Principle?

Prevent All Breaches

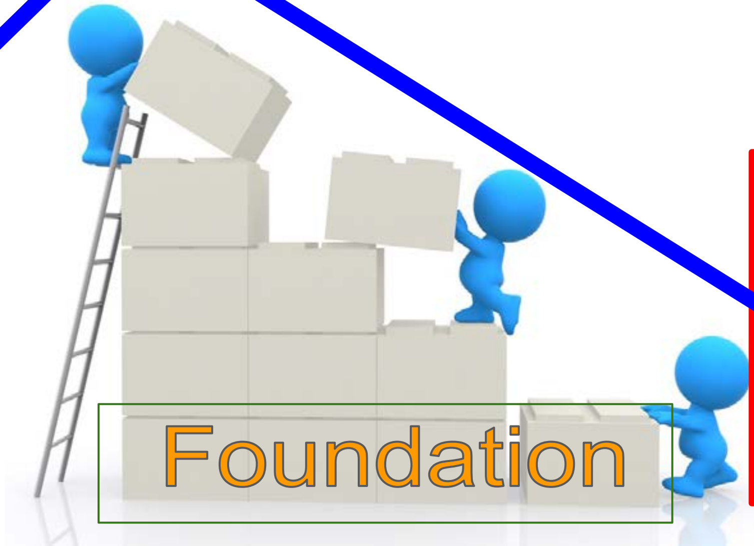


Foundation

What is the network defender’s ultimate First Principle?

Prevent All Breaches

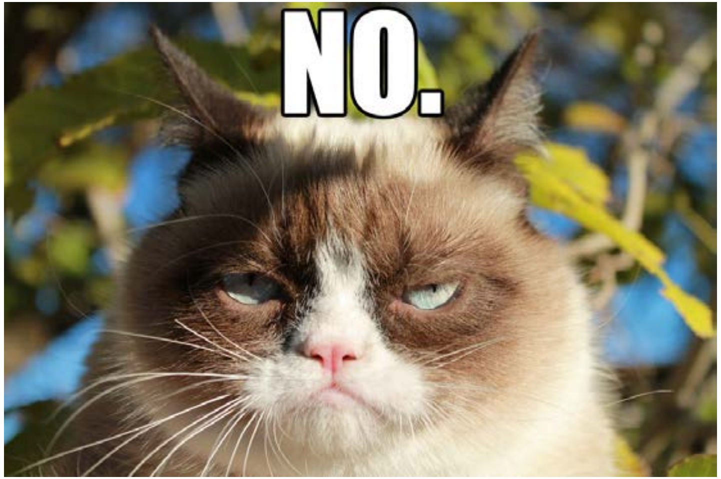
Crown Jewels



Foundation

What is the network defender’s ultimate First Principle?

Prevent Breaches



Foundation

What is the network defender’s ultimate First Principle?

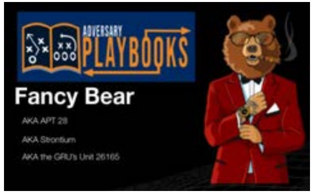
→ **Prevent Adversary Campaigns**

Foundation

What is the network defender’s ultimate First Principle?

→ **Prevent Adversary Campaigns**

Foundation



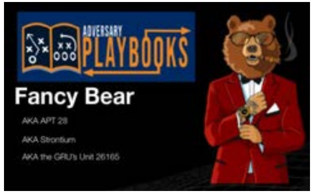
What is the network defender's ultimate First Principle?

→ **Prevent Adversary Campaigns**

MITRE
ATT&CK
Adversarial Tactics, Techniques & Common Knowledge

Foundation

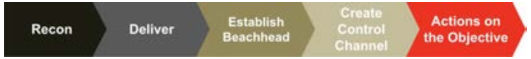
100



What is the network defender's ultimate First Principle?

→ **Prevent Adversary Campaigns**

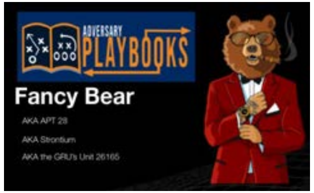
CYBER THREAT ALLIANCE



500

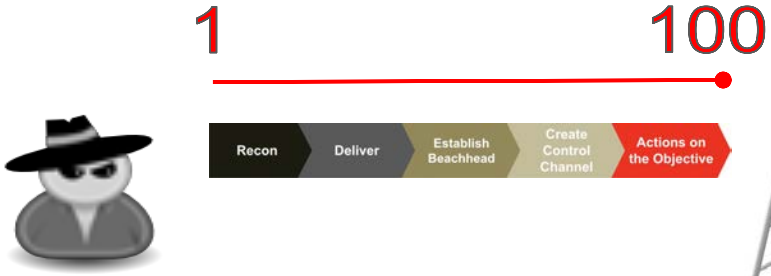
Foundation

100



What is the network defender's ultimate First Principle?

→ Prevent Adversary Campaigns


1

100

Recon

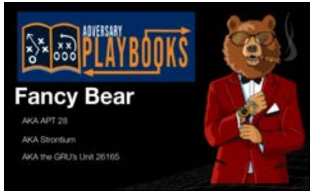
Deliver

Establish Beachhead

Create Control Channel

Actions on the Objective

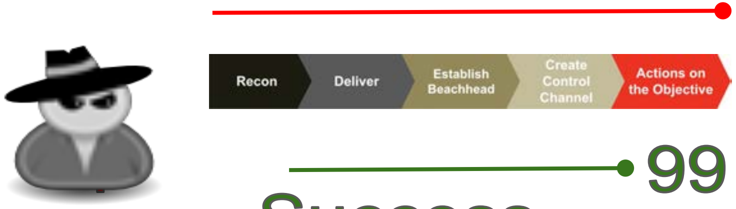
Foundation



What is the network defender's ultimate First Principle?

→ **Prevent Adversary Campaigns**

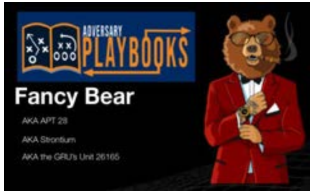
1 100



99

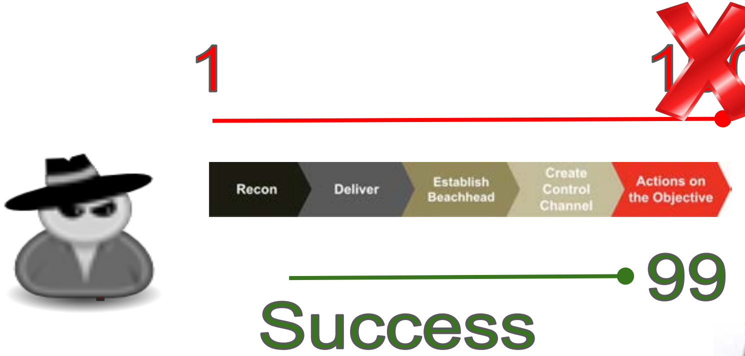
Success

Foundation



What is the network defender's ultimate First Principle?

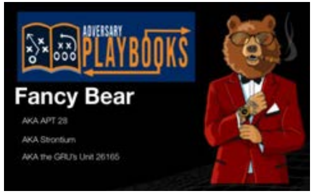
→ Prevent Adversary **Campaigns**



Recon → Deliver → Establish Beachhead → Create Control Channel → Actions on the Objective

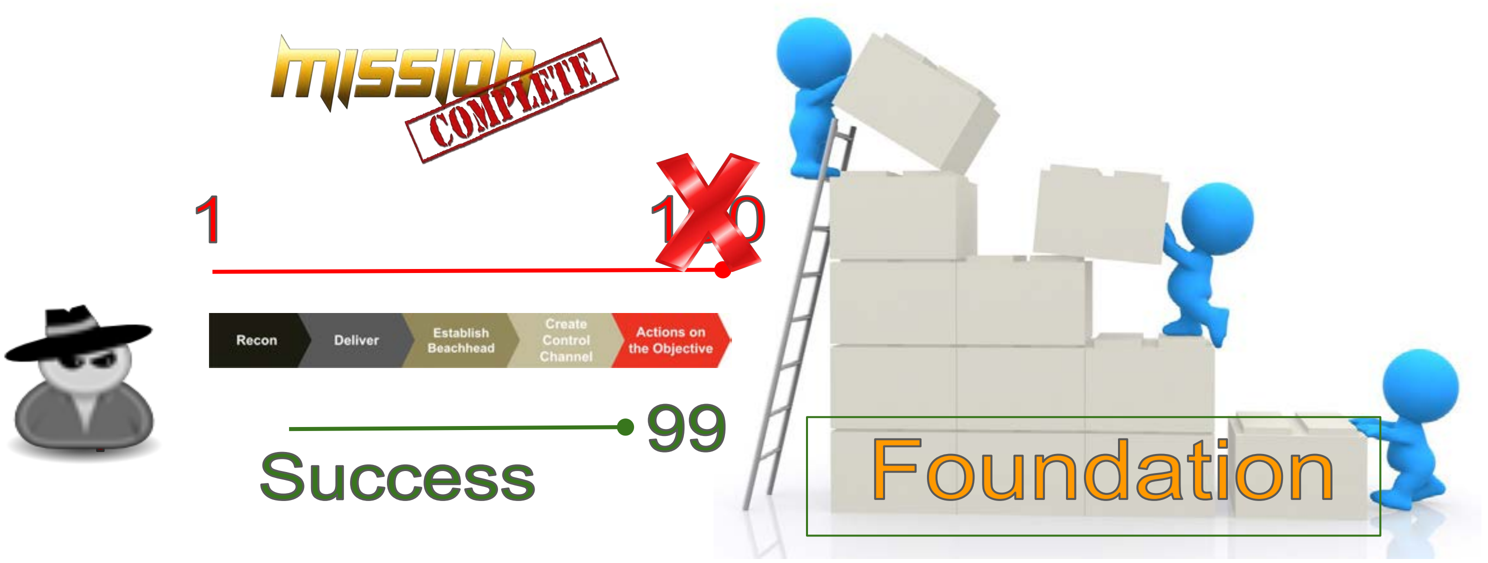
Success

Foundation



What is the network defender's ultimate First Principle?

→ Prevent Adversary **Campaigns**



1

100

Recon

Deliver

Establish Beachhead

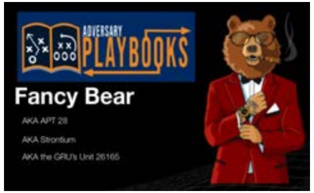
Create Control Channel

Actions on the Objective

99

Success

Foundation



Fancy Bear

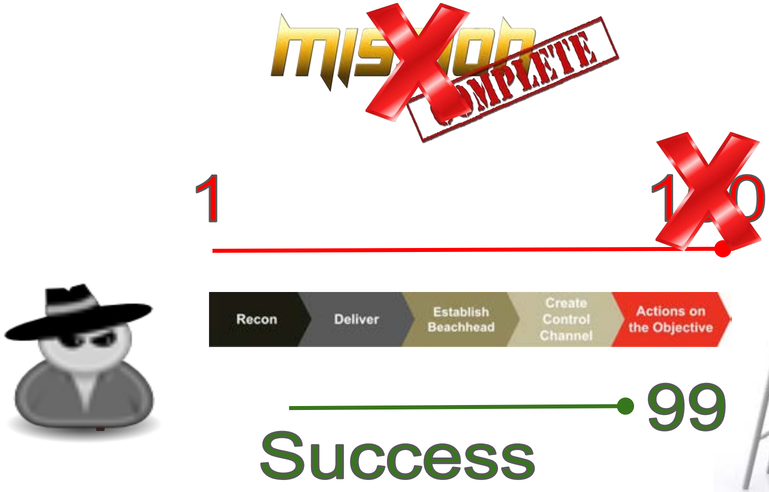
AKA APT 28

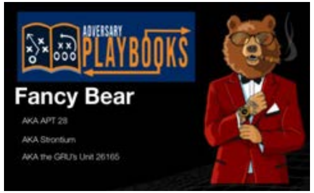
AKA Strontium

AKA the GRU's Unit 26165

What is the network defender's ultimate First Principle?

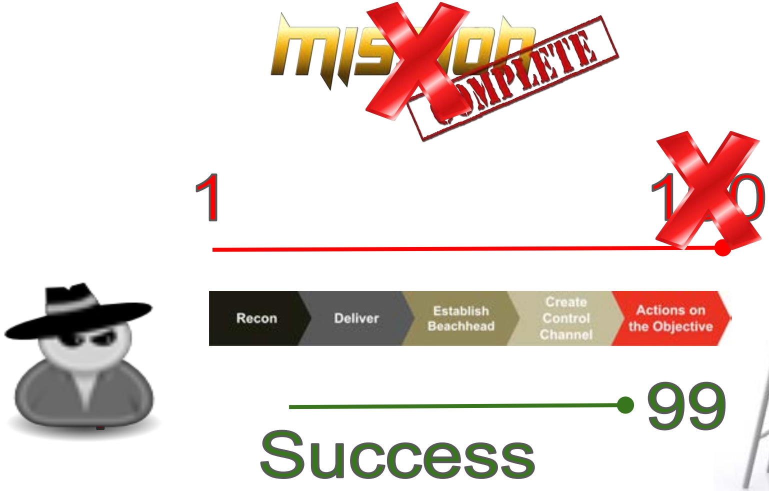
→ Prevent Adversary Campaigns





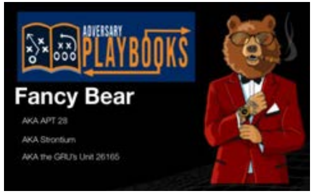
What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns



Recon → Deliver → Establish Beachhead → Create Control Channel → Actions on the Objective

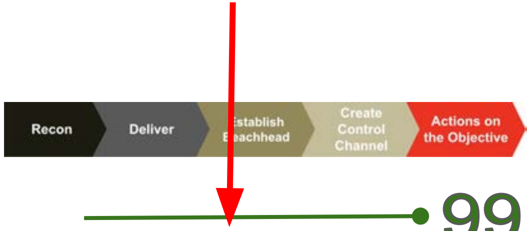
Foundation



What is the network defender's ultimate First Principle?

→ Prevent Adversary Campaigns

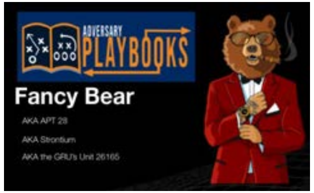
troublesome



99

Success

Foundation



ADVERSARY PLAYBOOKS

Fancy Bear

AKA APT 28

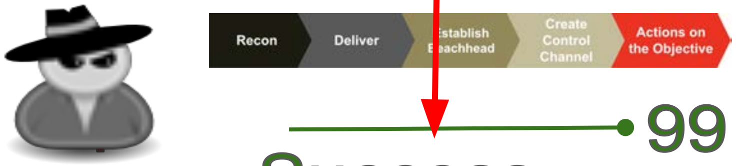
AKA Strontium

AKA the GRU's Unit 26165

What is the network defender's ultimate First Principle?

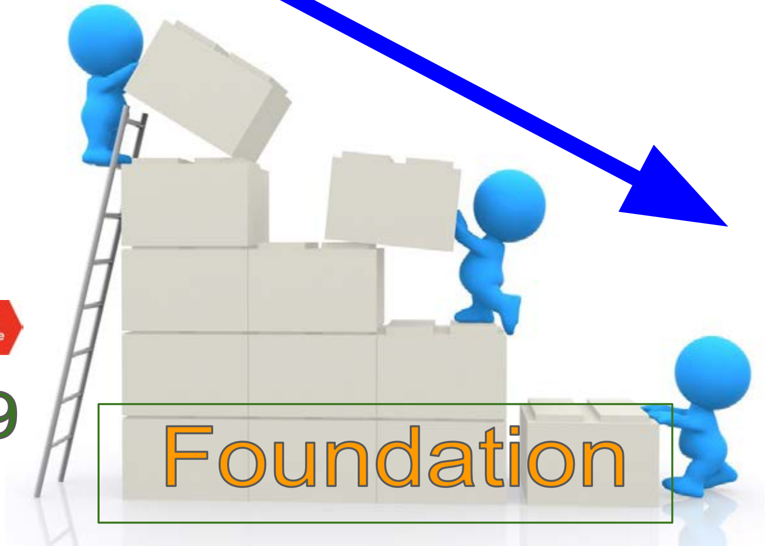
Prevent Adversary Campaigns

troublesome

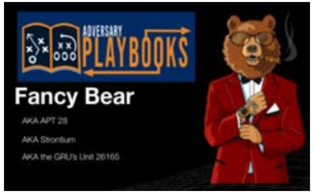


99

Success



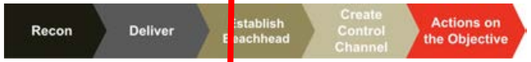
Crown Jewels



What is the network defender’s ultimate First Principle?

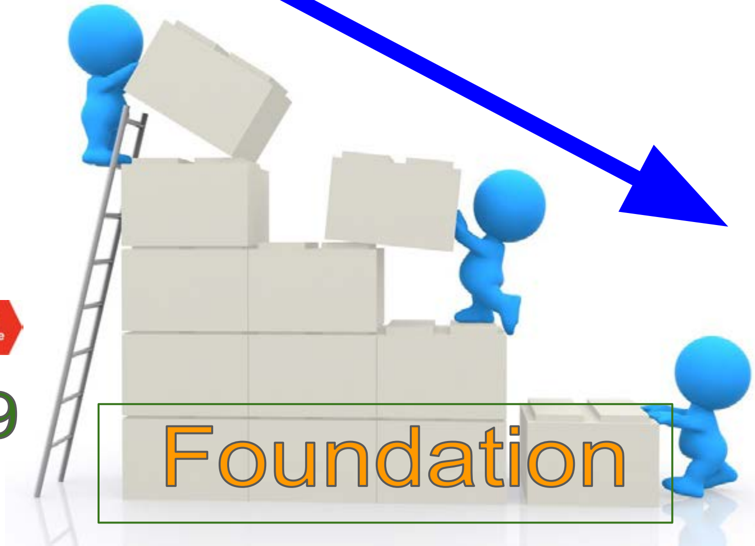
Prevent Adversary Campaigns

troublesome

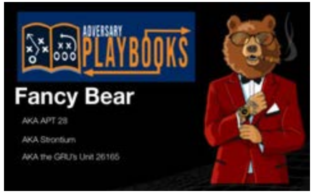


99

Success



Crown Jewels



What is the network defender’s ultimate First Principle?

Prevent All Breaches

Foundation

What is the network defender’s ultimate First Principle?

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

Foundation

What is the network defender’s ultimate First Principle?

Foundation

What is the network defender's ultimate First Principle?

Kevin

Foundation

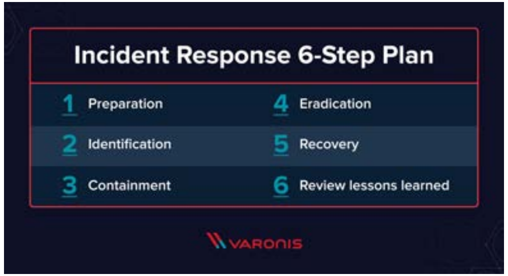
What is the network defender's ultimate First Principle?

Kevin

Foundation

Crown Jewels

What is the network defender’s ultimate First Principle?



Incident Response 6-Step Plan

1 Preparation

2 Identification

3 Containment

4 Eradication

5 Recovery

6 Review lessons learned

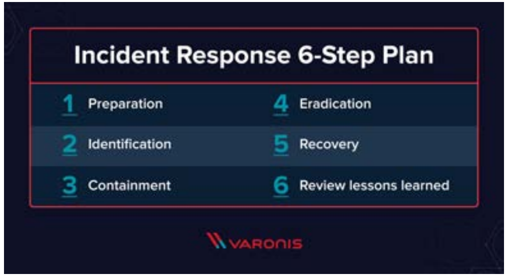
VARONIS

Kevin

Foundation

Crown Jewels

What is the network defender's ultimate First Principle?



Incident Response 6-Step Plan

1 Preparation	4 Eradication
2 Identification	5 Recovery
3 Containment	6 Review lessons learned

VARONIS

Kevin

Foundation

Crown Jewels

What is the network defender's ultimate First Principle?

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

Kevin

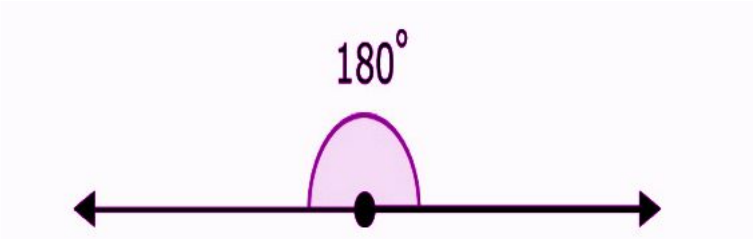
Foundation

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

Kevin



Foundation

What is the network defender's ultimate First Principle?

Prevent All Breaches

What is the network defender’s ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?

Atomic

Prevent Adversary Campaigns

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?

Atomic

Prevent Adversary Campaigns

Prevent All Breaches

Black	White

Foundation

What is the network defender's ultimate First Principle?

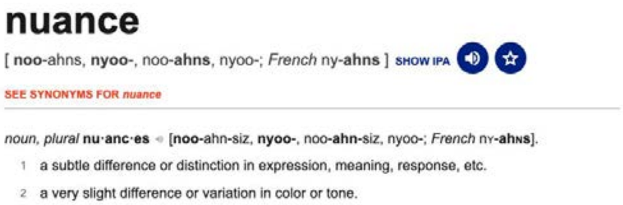
Atomic

Prevent Adversary Campaigns

Prevent All Breaches

Foundation

What is the network defender's ultimate First Principle?



nuance

[noo-ahns, nyoo-, noo-ahns, nyoo-; French ny-ahns] SHOW IPA

SEE SYNONYMS FOR *nuance*

noun, plural **nu·anc·es** [noo-ahn-siz, nyoo-, noo-ahn-siz, nyoo-; *French* ny-ahns].

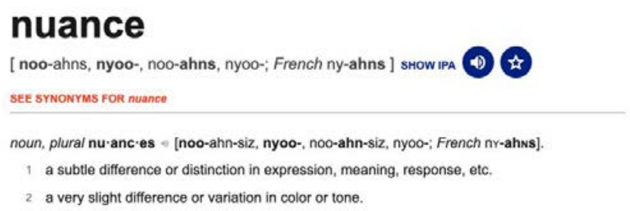
1 a subtle difference or distinction in expression, meaning, response, etc.

2 a very slight difference or variation in color or tone.

Prevent Adversary Campaigns

Prevent All Breaches

What is the network defender’s ultimate First Principle?



nuance

[**noo**-ahns, **nyoo**-, noo-**ahns**, nyoo-; *French* ny-**ahns**] SHOW IPA

SEE SYNONYMS FOR *nuance*

noun, plural **nu·anc·es** [**noo**-ahn-siz, **nyoo**-, noo-**ahn**-siz, nyoo-; *French* ny-**ahns**].

1 a subtle difference or distinction in expression, meaning, response, etc.

2 a very slight difference or variation in color or tone.

What is the network defender’s ultimate First Principle?

What is the network defender’s ultimate First Principle?

What is the network defender’s ultimate First Principle?

What is the network defender’s ultimate First Principle?

What is the network defender’s ultimate First Principle?

What is the network defender’s ultimate First Principle?

What is the network defender’s ultimate First Principle?

DIVERGENT

What is the network defender's ultimate First Principle?

DIVERGENT

Stupid

What is the network defender’s ultimate First Principle?

Stupid

What is the network defender’s ultimate First Principle?

QUESTIONNAIRE

☐

Very often ☑

Often ☐

Sometimes ☐

Rarely ☐

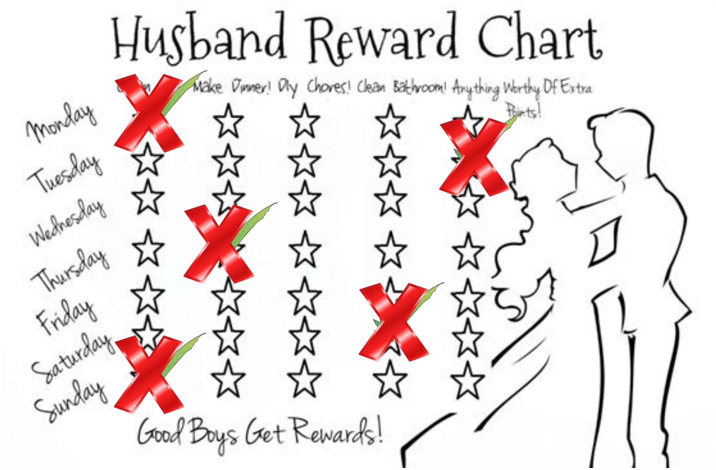
Husband Reward Chart

	Clean up!	Make Dinner!	Diy Chores!	Clean Bathroom!	Anything Worthy Of Extra Points!
Monday	✓	☆	☆	☆	☆
Tuesday	☆	☆	☆	☆	✓
Wednesday	☆	☆	☆	☆	☆
Thursday	☆	✓	☆	☆	☆
Friday	☆	☆	☆	☆	☆
Saturday	☆	☆	☆	✓	☆
Sunday	✓	☆	☆	☆	☆

Good Boys Get Rewards!

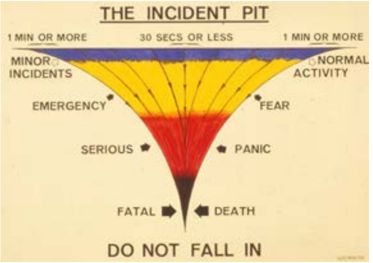
Stupid

What is the network defender's ultimate First Principle?



Stupid

What is the network defender’s ultimate First Principle?



Husband Reward Chart

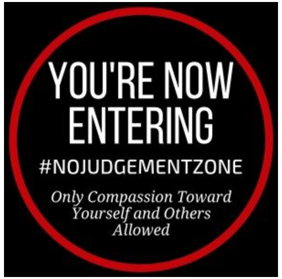
	Clean up!	Make Dinner!	Diy Chores!	Clean Bathroom!	Anything Worthy Of Extra Points!
Monday	✓	☆	☆	☆	☆
Tuesday	☆	☆	☆	☆	✓
Wednesday	☆	☆	☆	☆	☆
Thursday	☆	✓	☆	☆	☆
Friday	☆	☆	☆	☆	☆
Saturday	☆	☆	☆	✓	☆
Sunday	✓	☆	☆	☆	☆

Good Boys Get Rewards!

So Many Likes

Stupid

What is the network defender's ultimate First Principle?

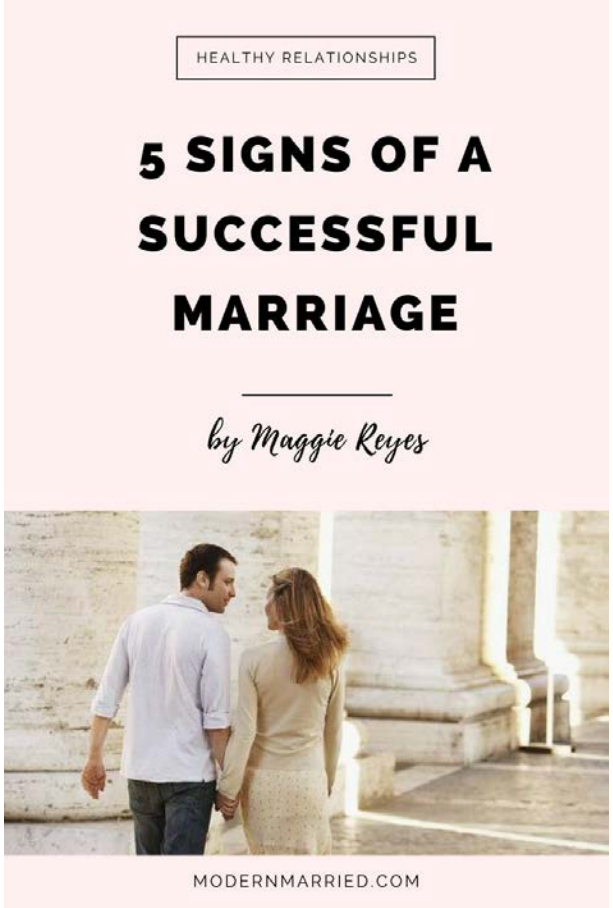


What is the network defender’s ultimate First Principle?

Husband Reward Chart

	Clean up!	Make Dinner!	Diy Chores!	Clean Bathroom!	Anything Worthy Of Extra Points!
Monday	✓	☆	☆	☆	☆
Tuesday	☆	☆	☆	☆	✓
Wednesday	☆	☆	☆	☆	☆
Thursday	☆	✓	☆	☆	☆
Friday	☆	☆	☆	☆	☆
Saturday	☆	☆	☆	✓	☆
Sunday	✓	☆	☆	☆	☆

Good Boys Get Rewards!

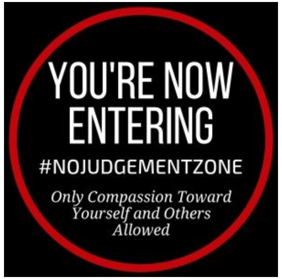


HEALTHY RELATIONSHIPS

5 SIGNS OF A SUCCESSFUL MARRIAGE

by Maggie Reyes

MODERNMARRIED.COM



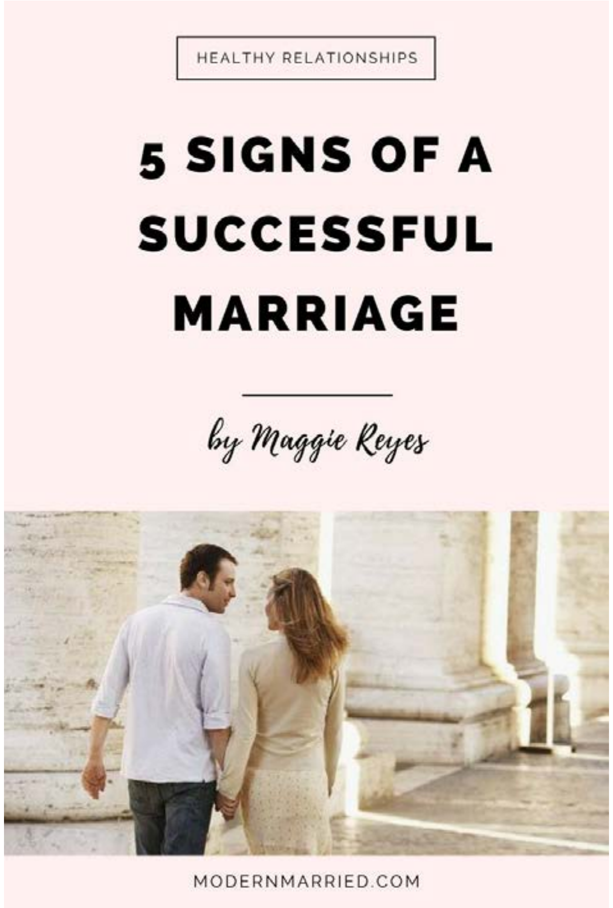
YOU'RE NOW ENTERING

#NOJUDGEMENTZONE

Only Compassion Toward Yourself and Others Allowed

What is the network defender's ultimate First Principle?

Z ZERO TOLERANCE

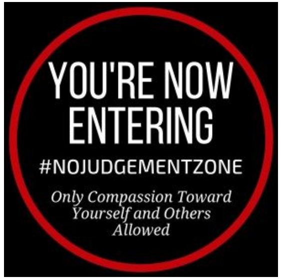


HEALTHY RELATIONSHIPS

5 SIGNS OF A SUCCESSFUL MARRIAGE

by Maggie Reyes

MODERNMARRIED.COM



YOU'RE NOW ENTERING

#NOJUDGEMENTZONE

Only Compassion Toward Yourself and Others Allowed

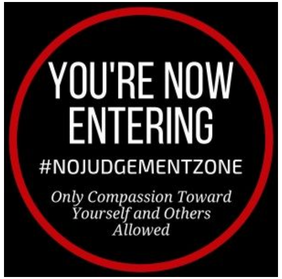
What is the network defender's ultimate First Principle?

HEALTHY RELATIONSHIPS

5 SIGNS OF A SUCCESSFUL MARRIAGE

by Maggie Reyes

MODERNMARRIED.COM



YOU'RE NOW ENTERING

#NOJUDGEMENTZONE

Only Compassion Toward Yourself and Others Allowed

Z ZERO TOLERANCE

What is the network defender's ultimate First Principle?

Z ZERO TOLERANCE

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

What is the network defender’s ultimate First Principle?

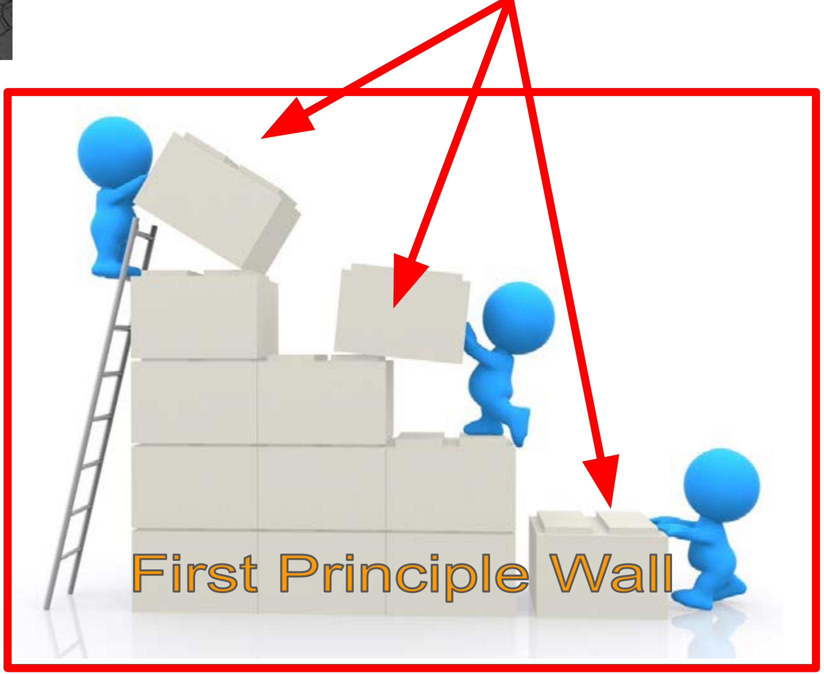
Prevent Adversary Campaigns

Prevent All Breaches

What is the network defender’s ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches



What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

What is the network defender’s ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

FAIL
First Principle Wall

What is the network defender's ultimate First Principle?

Prevent Adversary Campaigns

Prevent All Breaches

FAIL
First Principle Wall

What is the network defender's ultimate First Principle?

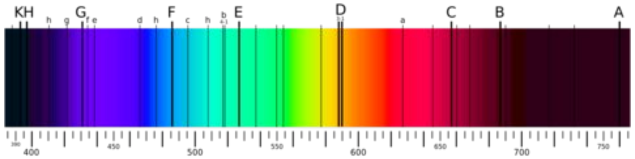
Prevent Adversary Campaigns

Prevent All Breaches

FAIL
First Principle Wall

What is the network defender's ultimate First Principle?

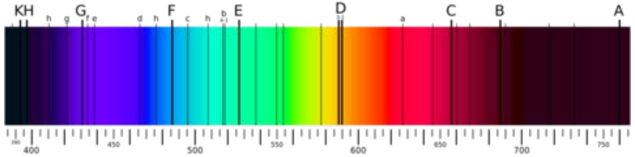
What is the network defender's ultimate First Principle?



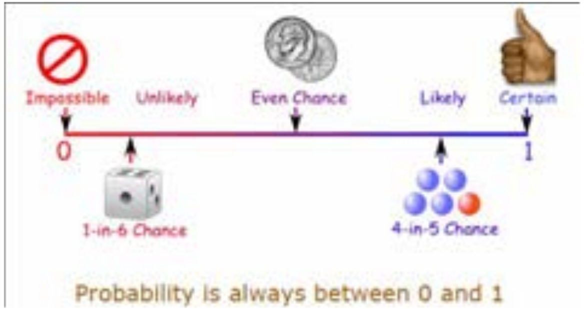
← Scale →

First Principle Wall

What is the network defender's ultimate First Principle?



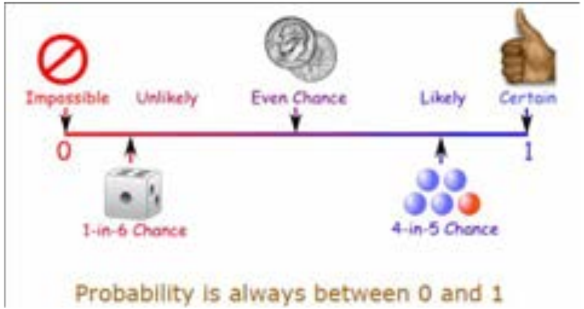
← Scale →



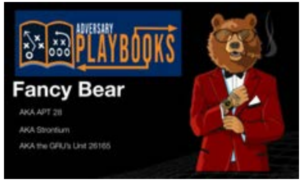
Probability Range

First Principle Wall

What is the network defender's ultimate First Principle?



Probability Range

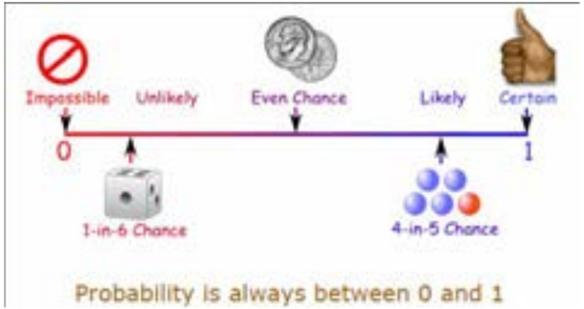


First Principle Wall

What is the network defender's ultimate First Principle?

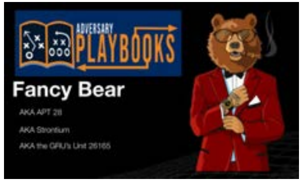
First Principle Thinking

...Challenging the Status Quo



Probability is always between 0 and 1

Probability Range



ADVERSARY PLAYBOOKS

Fancy Bear

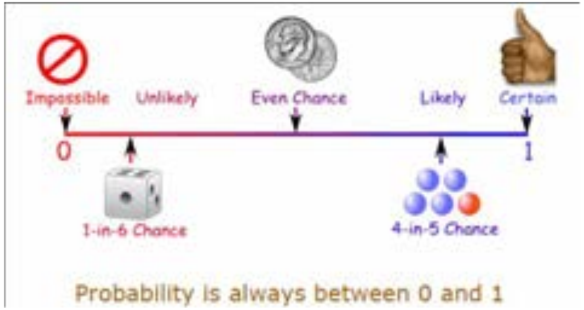
AKA APT 28

AKA Strontium

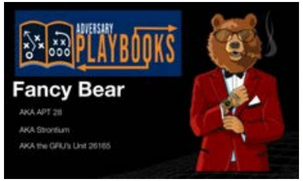
AKA the GRU's Unit 26165

First Principle Wall

What is the network defender's ultimate First Principle?

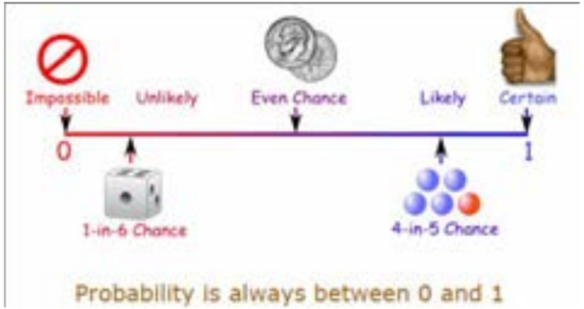


Probability Range

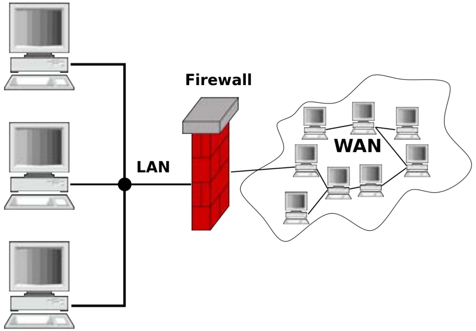


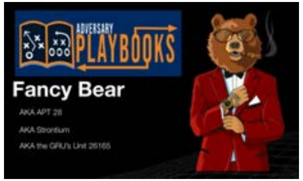
First Principle Wall

What is the network defender’s ultimate First Principle?

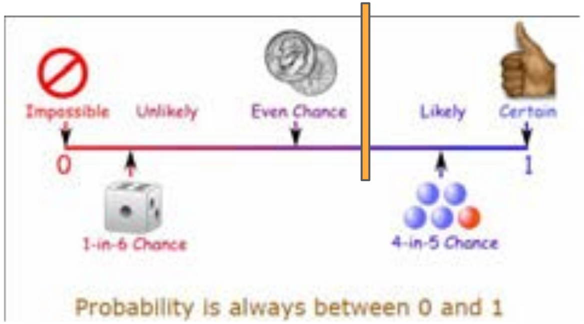


Probability Range

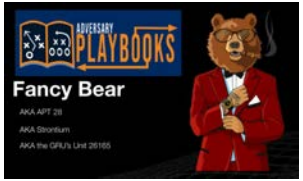




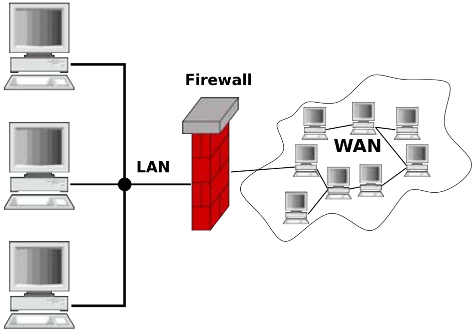
What is the network defender's ultimate First Principle?



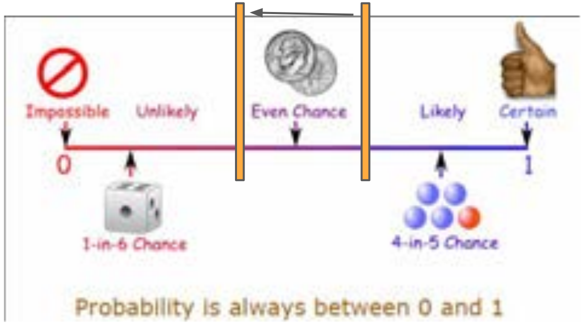
Probability Range



First Principle Wall

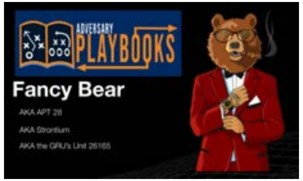


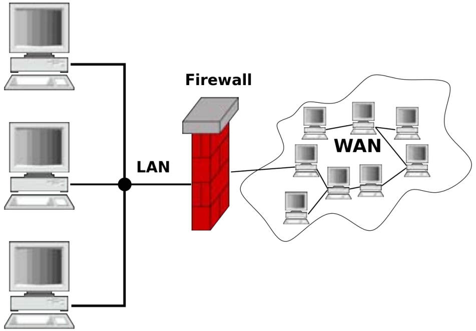
What is the network defender's ultimate First Principle?



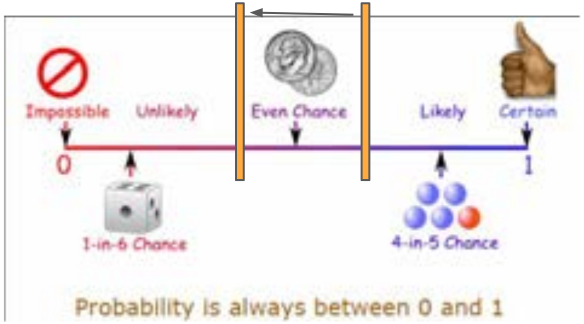
Probability Range

First Principle Wall

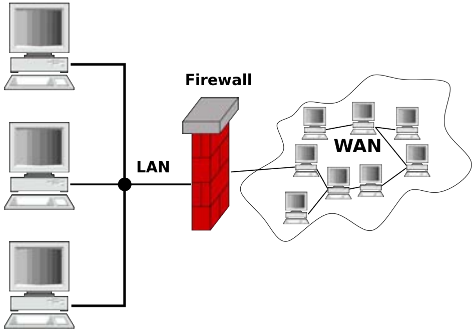




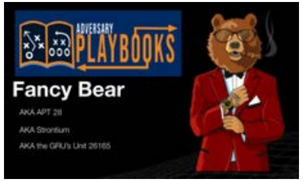
What is the network defender’s ultimate First Principle?



Probability Range



First Principle Wall



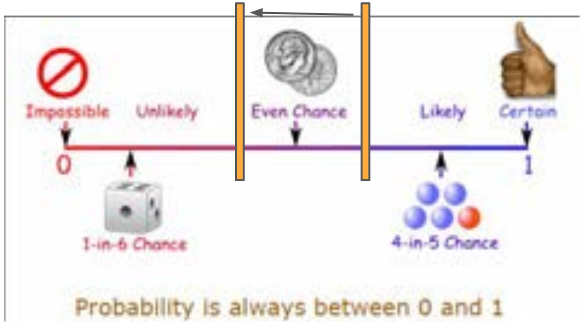
Fancy Bear

AKA APT 28

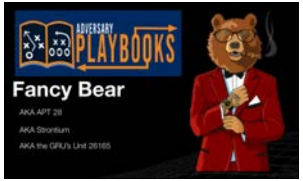
AKA Strontium

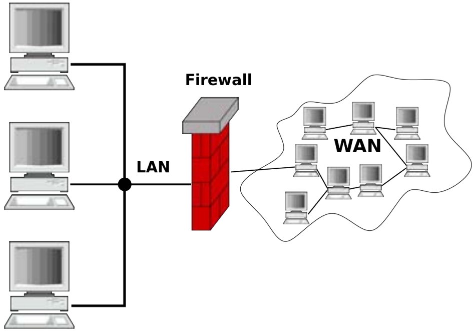
AKA the GRU's Unit 26165

What is the network defender's ultimate First Principle?

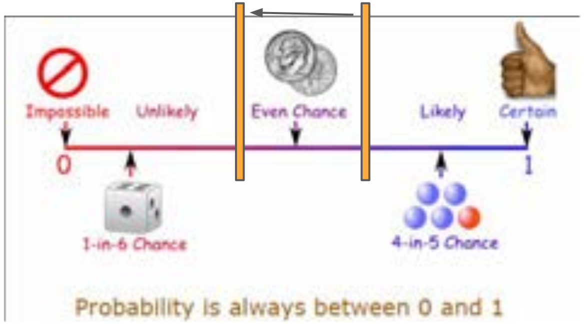


Probability Range





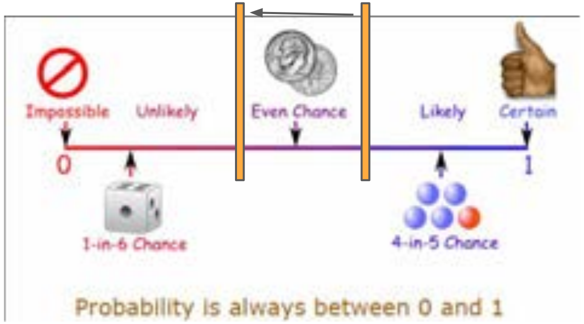
What is the network defender's ultimate First Principle?



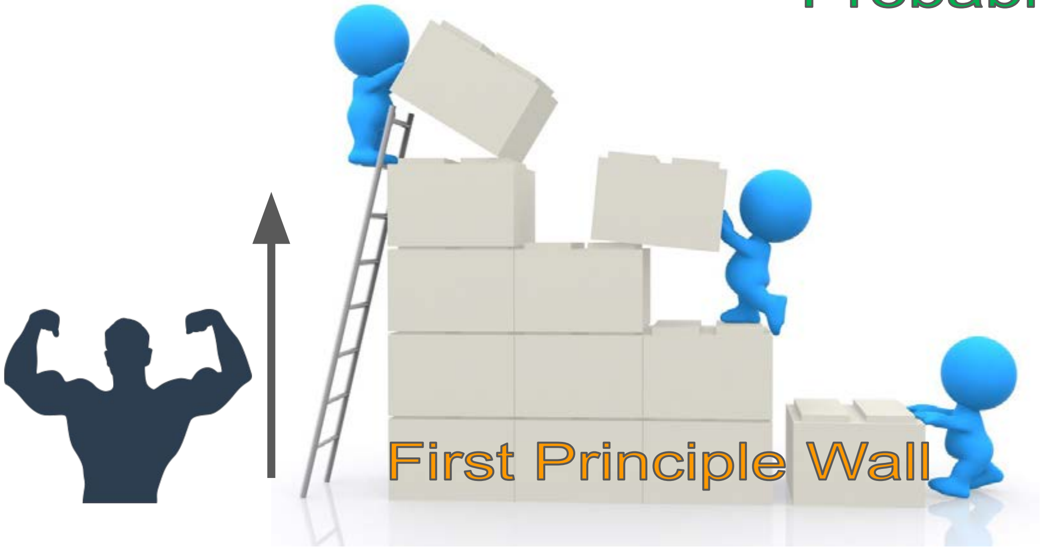
Probability Range

First Principle Wall

What is the network defender's ultimate First Principle?



Probability Range



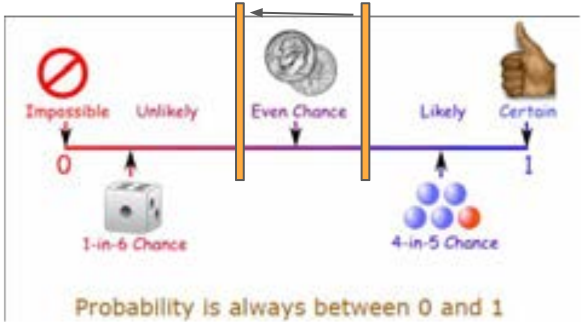
First Principle Wall

What is the network defender's ultimate First Principle?

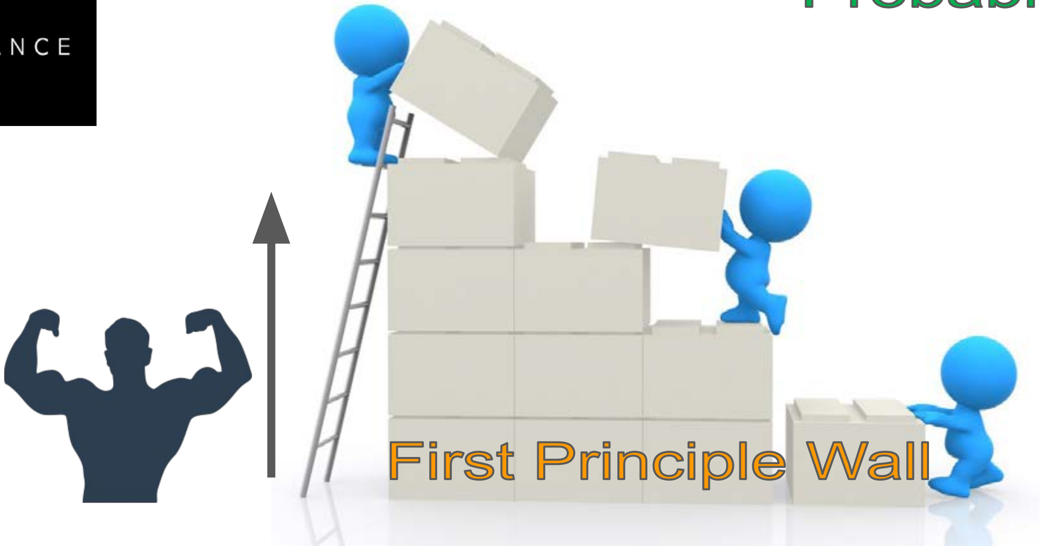
Z ZERO TOLERANCE

Prevent Adversary Campaigns

Prevent All Breaches

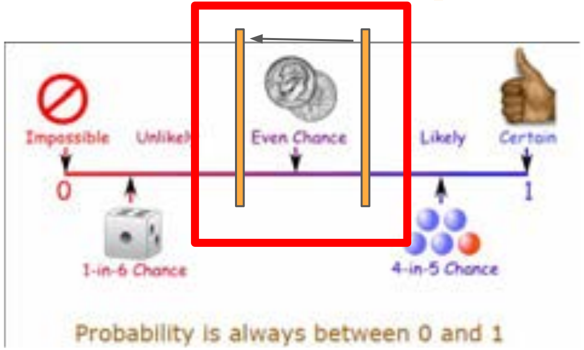


Probability Range



First Principle Wall

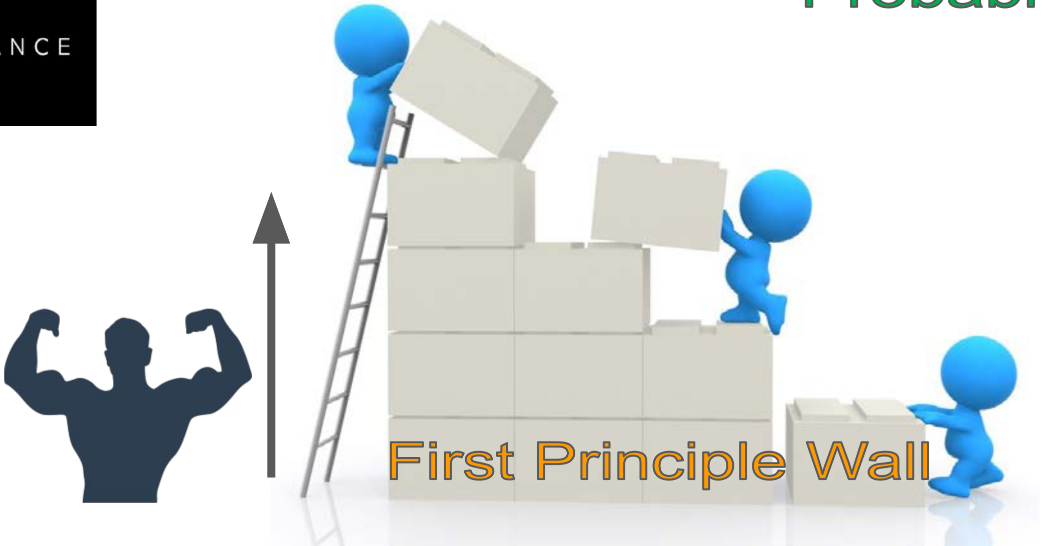
What is the network defender's ultimate First Principle?



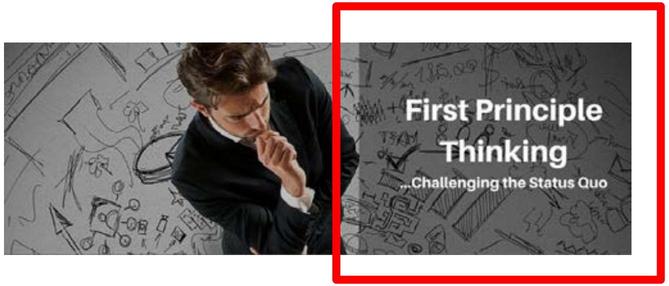
Probability Range

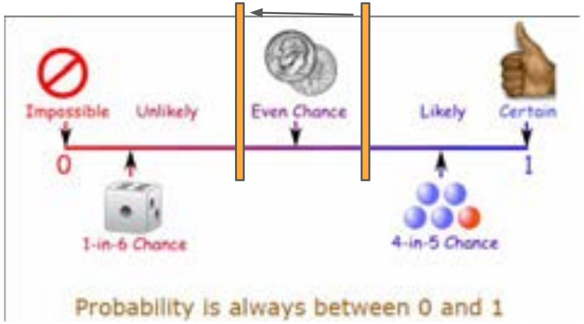
Prevent Adversary Campaigns

Prevent All Breaches



What is the network defender's ultimate First Principle?

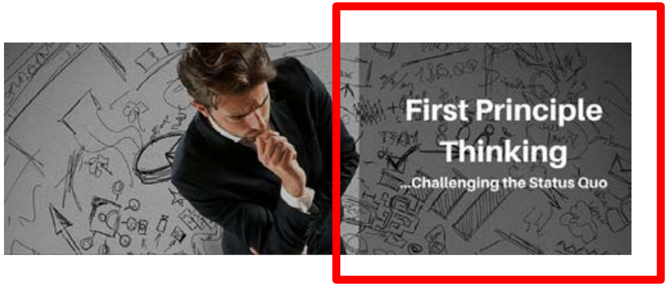


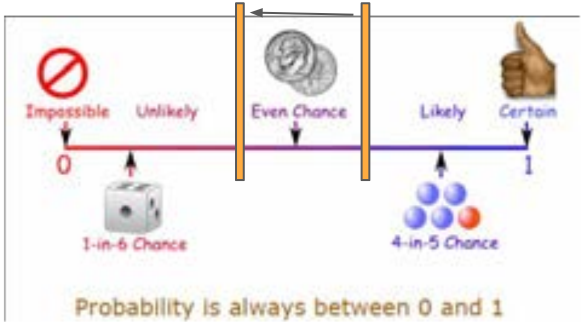


Probability Range

First Principle Wall

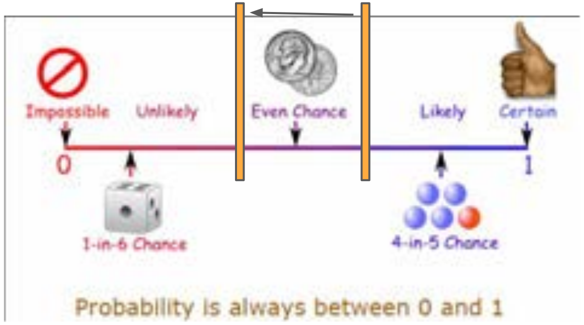
What is the network defender's ultimate First Principle?





Probability Range

What is the network defender's ultimate First Principle?

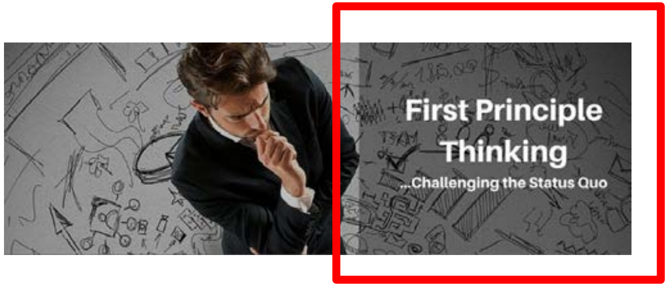


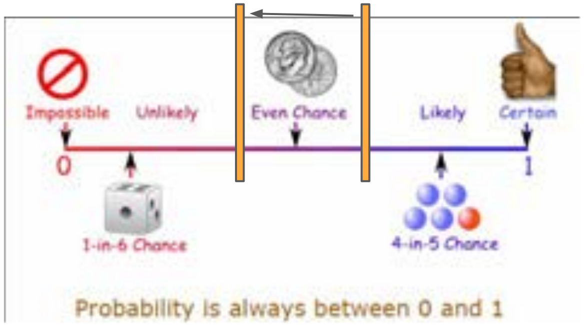
Probability Range

First Principle Wall

BINARY

What is the network defender’s ultimate First Principle?

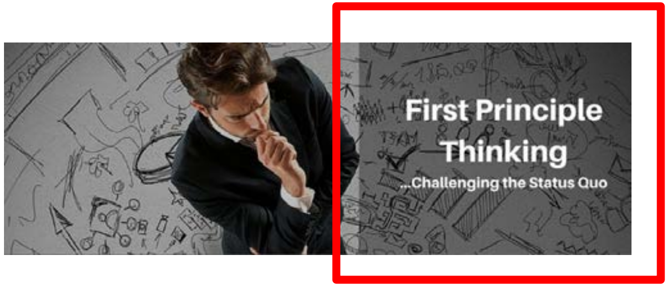


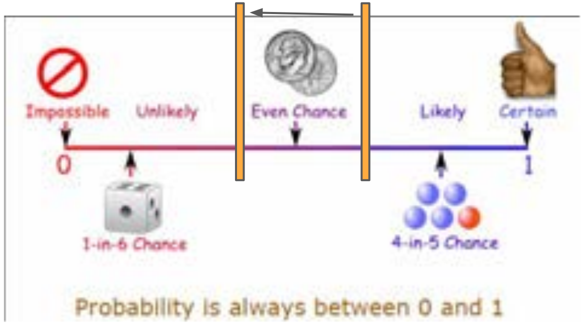


Probability Range

First Principle Wall

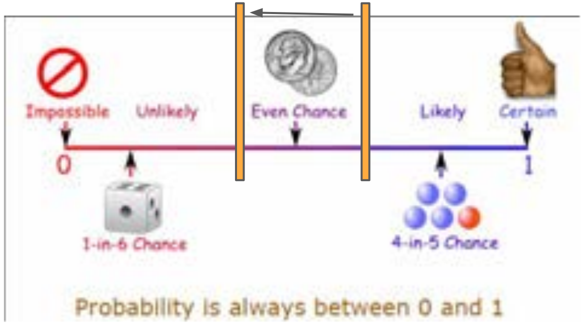
What is the network defender’s ultimate First Principle?



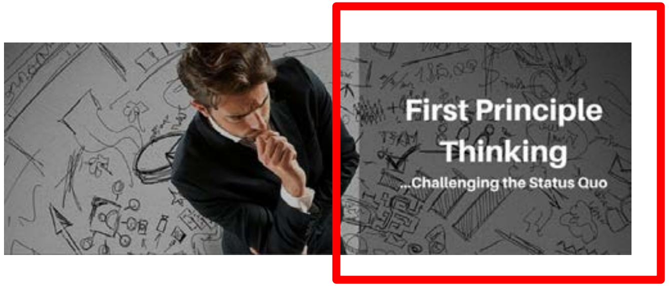


Probability Range

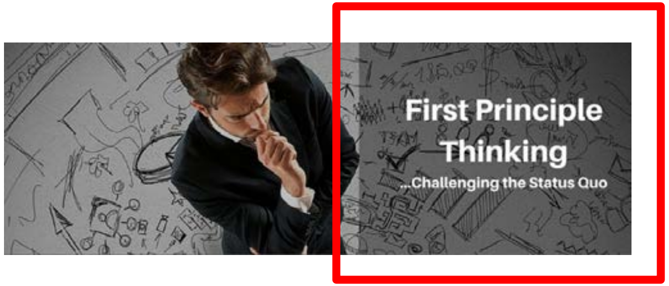
What is the network defender's ultimate First Principle?

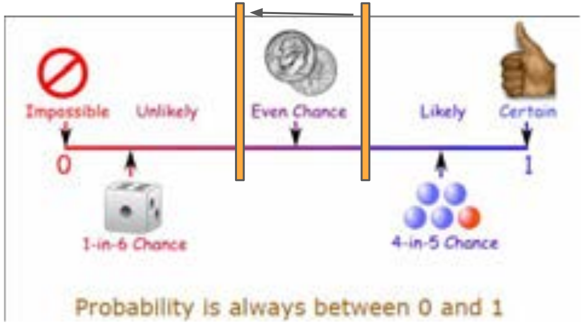


Probability Range



What is the network defender's ultimate First Principle?

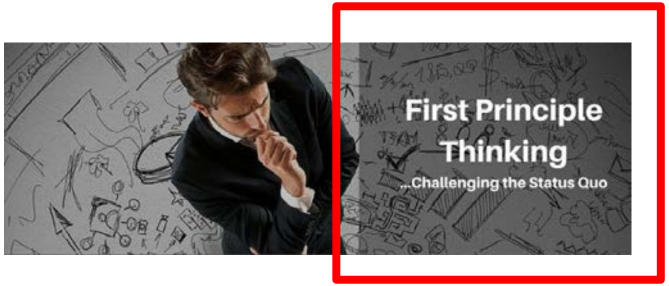


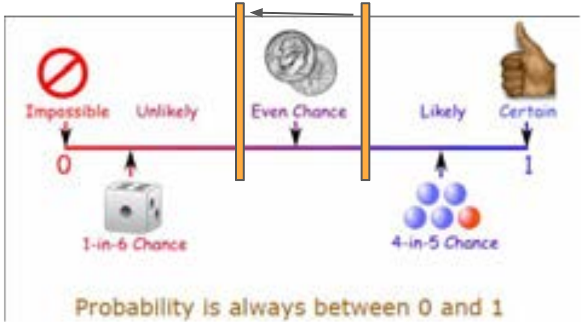


Probability Range

First Principle Wall

What is the network defender’s ultimate First Principle?





Probability Range

First Principle Wall

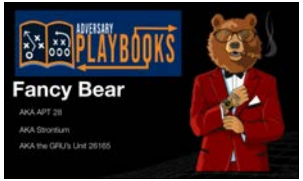
What is the network defender's ultimate First Principle?

●◯ Essential ?

First Principle Wall

What is the network defender's ultimate First Principle?

First Principle Wall



Fancy Bear

AKA APT 28

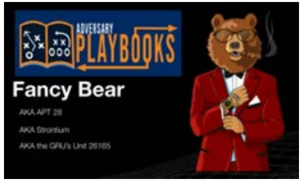
AKA Strontium

AKA the GRU's Unit 26165

●◘ Essential ?

What is the network defender’s ultimate First Principle?

●◘ Essential ?



Fancy Bear

AKA APT 28

AKA Strontium

AKA the GRU's Unit 26165

What is the network defender’s ultimate First Principle?

LUNCH SPECIALS

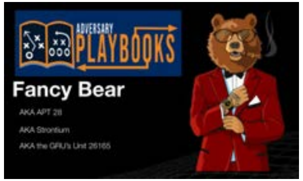
ITEMS 1-12

SALADS

BURRITOS

SPECIALTIES

Essential ?



Fancy Bear

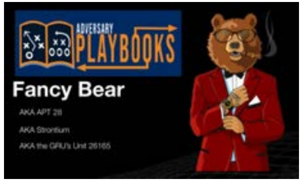
AKA APT 28

AKA Strontium

AKA the GRU's Unit 26165

What is the network defender's ultimate First Principle?

●◻ Essential ?



Fancy Bear

AKA APT 28

AKA Strontium

AKA the GRU's Unit 26165

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

What is the network defender's ultimate First Principle?

LUNCH SPECIALS

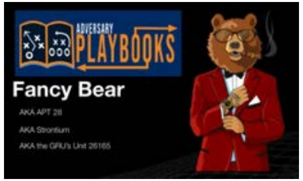
ITEMS 1-12

SALADS

BURRITOS

SPECIALTIES

Essential ?



Fancy Bear

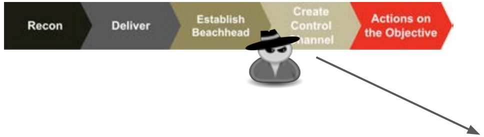
AKA APT 28

AKA Strontium

AKA the GRU's Unit 26165

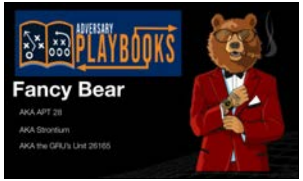
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

What is the network defender's ultimate First Principle?



LUNCH SPECIALS
ITEMS 1-12
SALADS
BURRITOS
SPECIALTIES

Essential ?



Fancy Bear

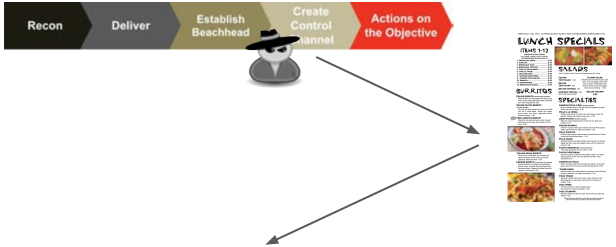
AKA APT 28

AKA Strontium

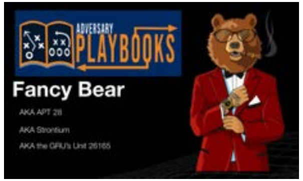
AKA the GRU's Unit 26165

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

What is the network defender's ultimate First Principle?

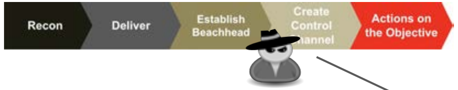


Essential ?



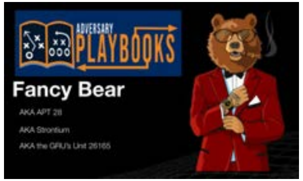
DEPARTMENT OF JUSTICE · FEDERAL BUREAU OF INVESTIGATION

What is the network defender’s ultimate First Principle?



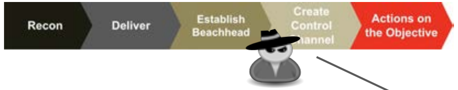
LUNCH SPECIALS
ITEMS 1-12
SALADS
BURRITOS
SPECIALTIES

Essential ?



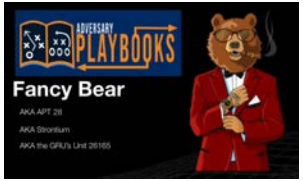
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

What is the network defender's ultimate First Principle?


Recon → Deliver → Establish Beachhead → Create Control Channel → Actions on the Objective

LUNCH SPECIALS
ITEMS 1-12
SALADS
BURRITOS
SPECIALTIES

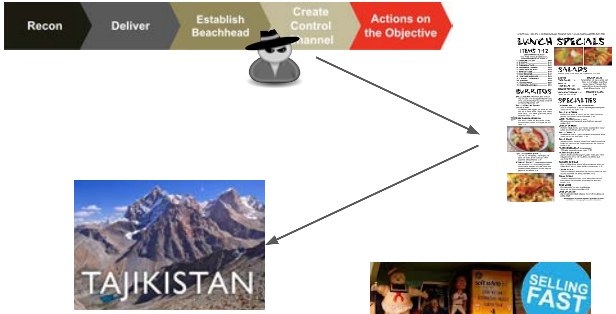
Essential ?

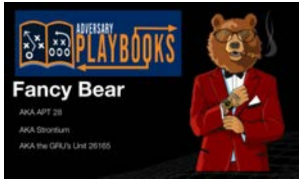


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

What is the network defender's ultimate First Principle?

NO WORRIES!





Fancy Bear

AKA APT 28

AKA Strontium

AKA the GRU's Unit 26165

Essential ?

What is the network defender's ultimate First Principle?

What is the network defender's ultimate First Principle?

finite

First Principle Wall

What is the network defender's ultimate First Principle?

finite

First Principle Wall

What is the network defender's ultimate First Principle?

What is the network defender’s ultimate First Principle?

Projects

First Principle Wall

What is the network defender's ultimate First Principle?

Projects

First Principle Wall

What is the network defender's ultimate First Principle?

Projects

First Principle Wall

What is the network defender’s ultimate First Principle?

Projects

What is the network defender’s ultimate First Principle?

Projects

First Principle Wall

What is the network defender's ultimate First Principle?

Projects

First Principle Wall

What is the network defender’s ultimate First Principle?

Projects

What is the network defender's ultimate First Principle?

First Principle Wall

What is the network defender’s ultimate First Principle?

“A ***material*** *issue can have a* ***major impact*** *on the financial, economic, reputational, and legal aspects of a company, as well as on the system of internal and external stakeholders of that company.” - Datamaran*

What is the network defender's ultimate First Principle?

"A ***material*** *issue can have a* ***major impact*** *on the financial, economic, reputational, and legal aspects of a company, as well as on the system of internal and external stakeholders of that company." - Datamaran*

finite

What is the network defender's ultimate First Principle?

*"A **material** issue can have a **major impact** on the financial, economic, reputational, and legal aspects of a company, as well as on the system of internal and external stakeholders of that company." - Datamaran*

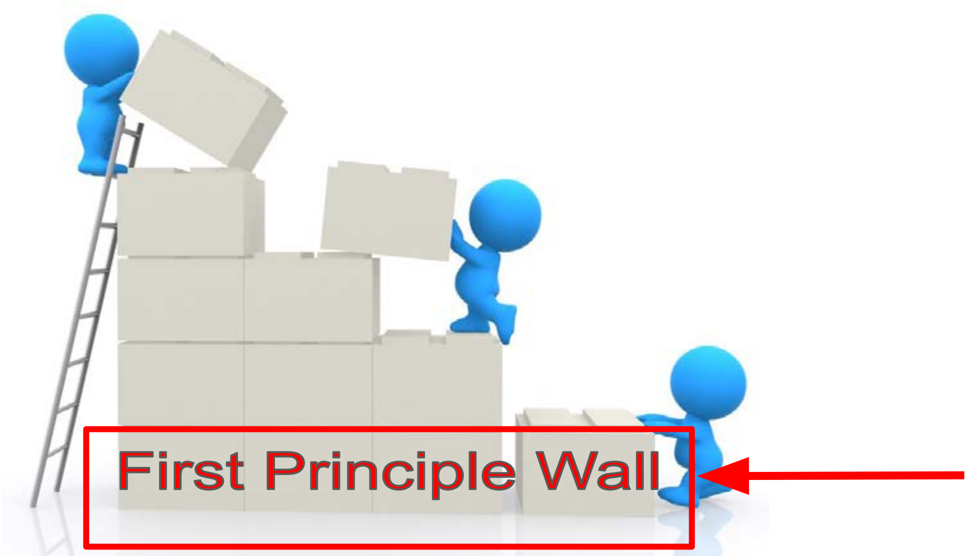
What is the network defender's ultimate First Principle?

*"A **material** issue can have a **major impact** on the financial, economic, reputational, and legal aspects of a company, as well as on the system of internal and external stakeholders of that company." - Datamaran*

What is the network defender's ultimate First Principle?

First Principle Wall

What is the network defender’s ultimate First Principle?


First Principle Wall

What is the network defender’s ultimate First Principle?

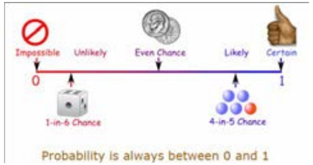
Reduce the probability of material impact due to a cyber event.

Impossible
Unlikely
Even Chance
Likely
Certain
0
1
1-in-6 Chance
4-in-5 Chance
Probability is always between 0 and 1

Probability Range

What is the network defender's ultimate First Principle?

Reduce the probability of material impact due to a cyber event.



Probability Range

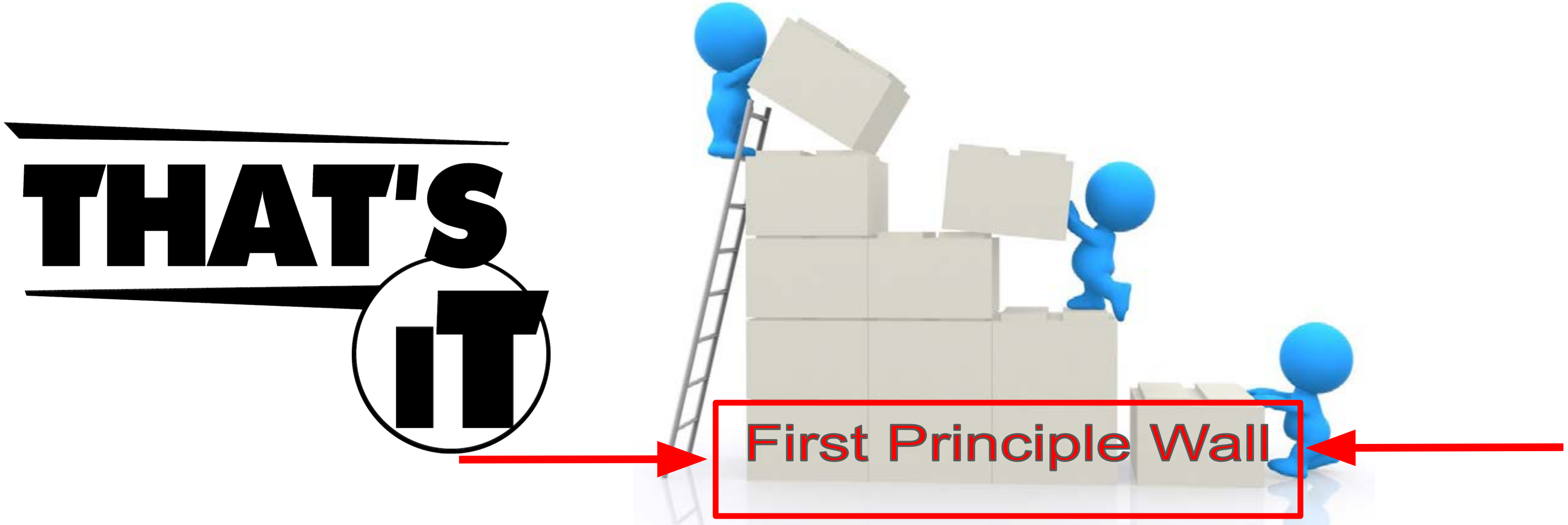
THAT'S IT

What is the network defender's ultimate First Principle?

Reduce the probability of material impact due to a cyber event.

What is the network defender's ultimate First Principle?

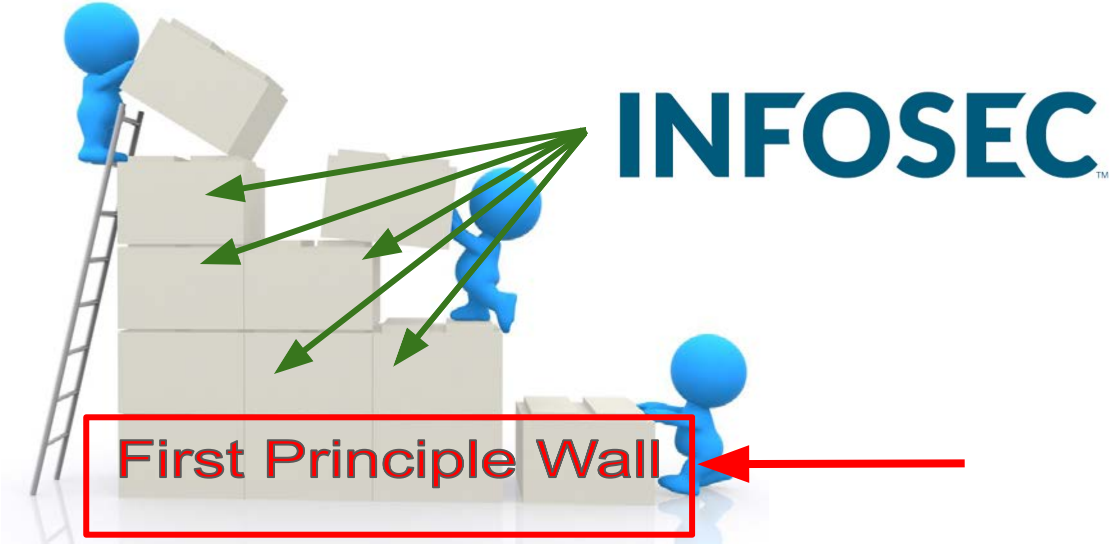
Reduce the probability of material impact due to a cyber event.



What is the network defender's ultimate First Principle?

Reduce the probability of material impact due to a cyber event.

THAT'S IT



What is the network defender's ultimate First Principle?

Reduce the probability of material impact due to a cyber event.

What is the network defender’s ultimate First Principle?

Reduce the probability of material impact due to a cyber event.

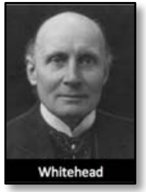
What is the network defender's ultimate First Principle?

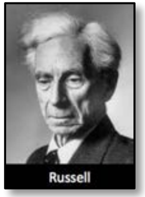
Reduce the probability of material impact due to a cyber event.

What is the network defender's ultimate First Principle?

Reduce the probability of material impact due to a cyber event.

First Principle Wall

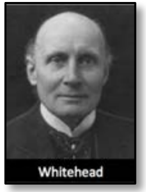


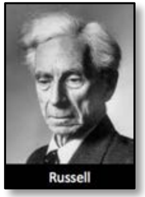


What is the network defender's ultimate First Principle?

Reduce the probability of material impact due to a cyber event.

1 + 1 = 2

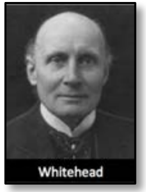


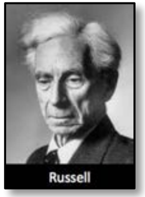


What is the network defender's ultimate First Principle?

Reduce the probability of material impact due to a cyber event.

1 + 1 = 2





The End

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

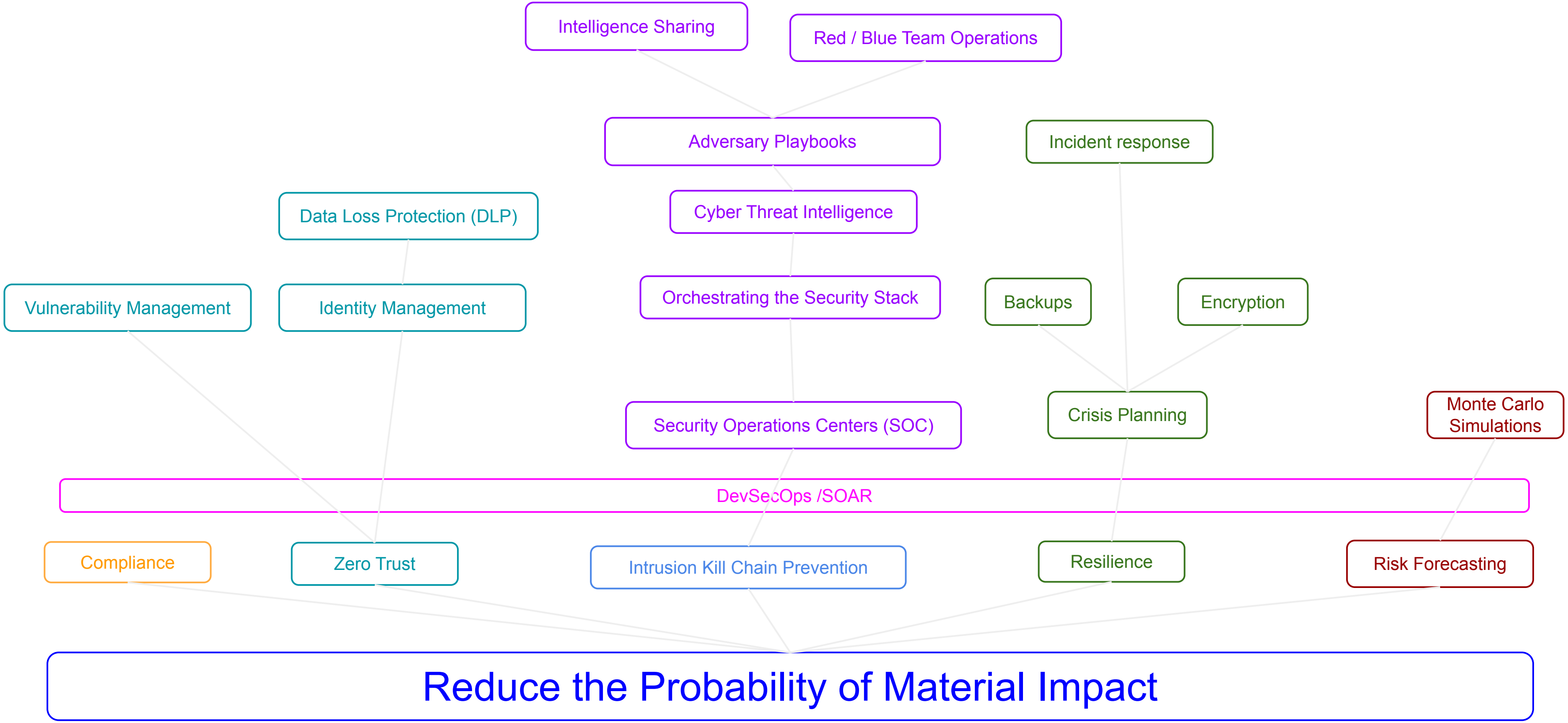
Email: rick.howard@thecyberwire.com

The ideas, strategies and technologies that senior cybersecurity executives wrestle with on a daily basis.

thecyberwire.com/pro/cso-perspectives

"In a world overloaded by information, we separate the signal from the noise."

First Principle Wall



This is what we talked about

This is what we talked about

A CISO’s world is daunting and overwhelmeing.

This is what we talked about

A CISO’s world is daunting and overwhelmeing.

Incremental improvements but more technical debt.

This is what we talked about

A CISO’s world is daunting and overwhelmeing.

Incremental improvements but more technical debt.

A first principles mindset can help.

This is what we talked about

A CISO’s world is daunting and overwhelmeing.

Incremental improvements but more technical debt.

A first principles mindset can help.

The network defender’s atomic first principle:

This is what we talked about

A CISO’s world is daunting and overwhelmeing.

Incremental improvements but more technical debt.

A first principles mindset can help.

The network defender’s atomic first principle:

Reduce the probability of material impact to our organization.

Homework

Homework

Read:

Cybersecurity Canon Hall of Fame Book: “The Phoenix Project.”

Homework

Read:

Cybersecurity Canon Hall of Fame Book: “The Phoenix Project.”

CYBERSECURITY CANON

Book Reviews at the Canon Website

Homework

Read:

Cybersecurity Canon Hall of Fame Book: “The Phoenix Project.” CYBERSECURITY CANON

Book Reviews at the Canon Website

Listen:

Homework

Read:

Cybersecurity Canon Hall of Fame Book: “The Phoenix Project.” CYBERSECURITY CANON

Book Reviews at the Canon Website

Listen:

“'Principia Mathematica' Celebrates 100 Years” on NPR

Homework

Read:

Cybersecurity Canon Hall of Fame Book: “The Phoenix Project.”

Book Reviews at the Canon Website

Listen:

“'Principia Mathematica' Celebrates 100 Years” on NPR

“Cybersecurity First Principles” on Cyberwire Pro.

No – Really This Time

Rick Howard: CSO, Chief Analyst, and Senior Fellow

the cyberwire

Email: rick.howard@thecyberwire.com

The ideas, strategies and technologies that senior cybersecurity executives wrestle with on a daily basis.

thecyberwire.com/pro/cso-perspectives

A fun and informative infosec audio glossary from the CyberWire.

thecyberwire.com/podcasts/word-notes

Quarterly discussion of the most impactful cybersecurity news items from the past 90 days.

thecyberwire.com/search?query=Quarterlyt%20Analyst%20Call

"In a world overloaded by information, we separate the signal from the noise."