RSAC Studio

Connect to Protect

Guiding Principles to Defending Organizations

Rick Howard
CSO – Palo Alto Networks
@raceBannon99

#RSAC

Elon Musk

Elon Musk

paloalto NETWORKS

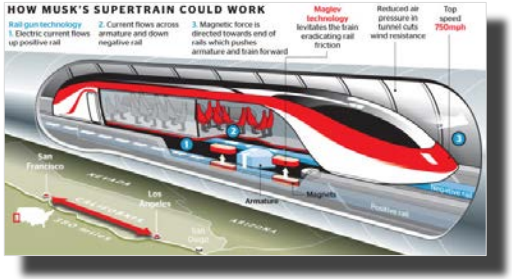
SPACEX

Elon Musk

paloalto NETWORKS

SPACEX

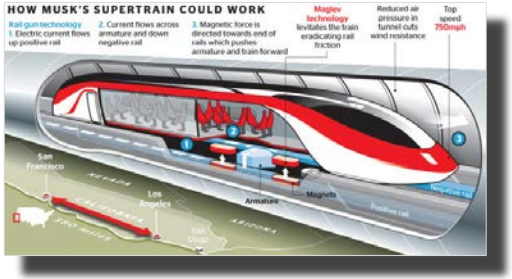
Elon Musk



paloalto NETWORKS

SPACEX

Elon Musk

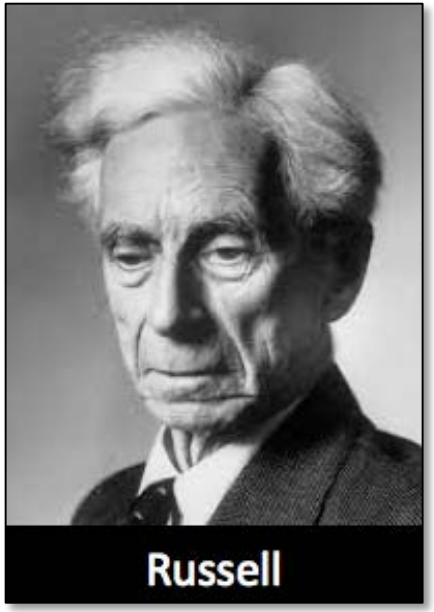


paloalto NETWORKS

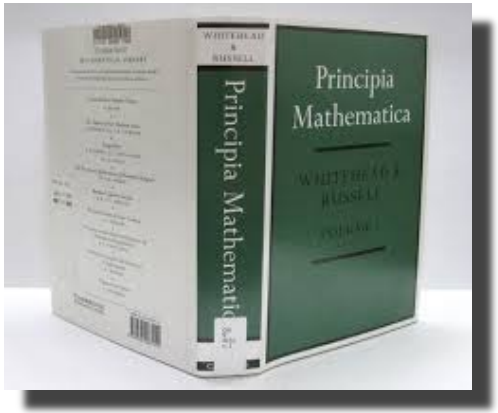

TESLA
Elon Musk's Secret Weapon
A Beginner's Guide to First Principles in Business

Elon Musk

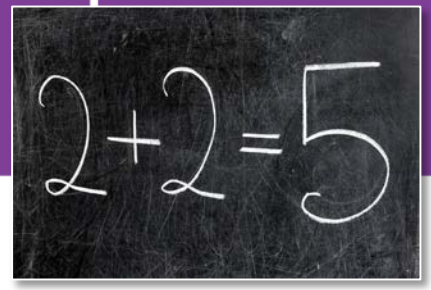
What is a First Principle?

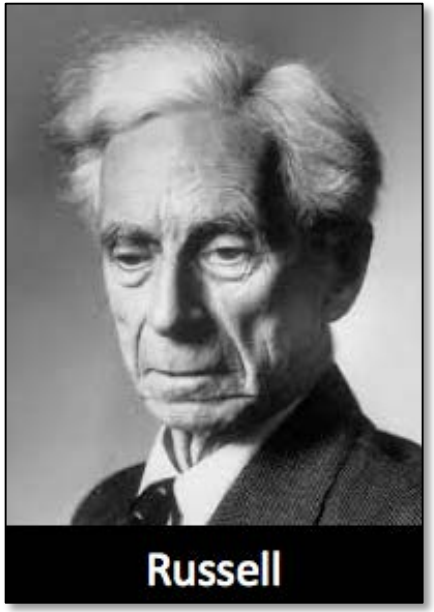


Principia Mathematica
published in 1913

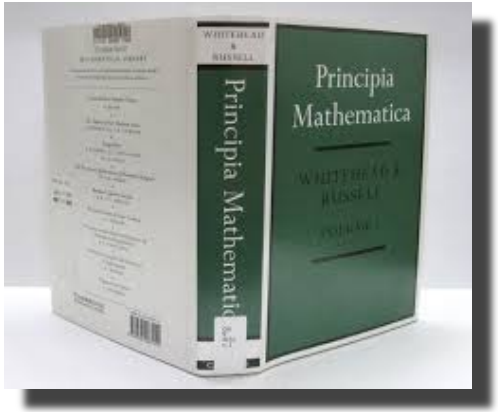


What is a First Principle?





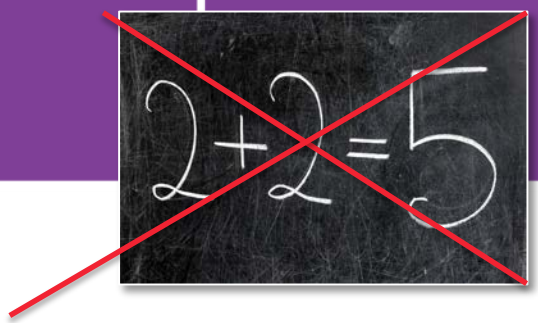
Principia Mathematica
published in 1913

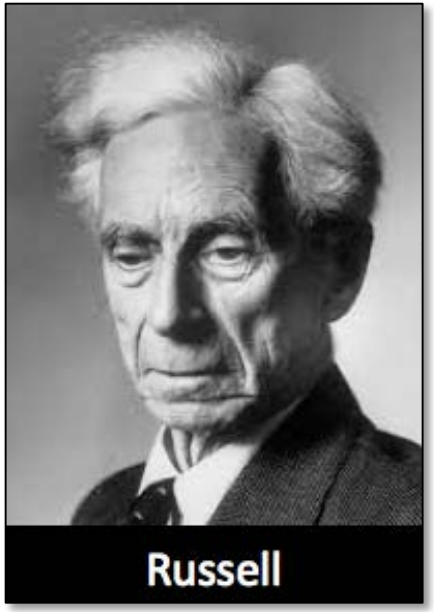


paloalto NETWORKS

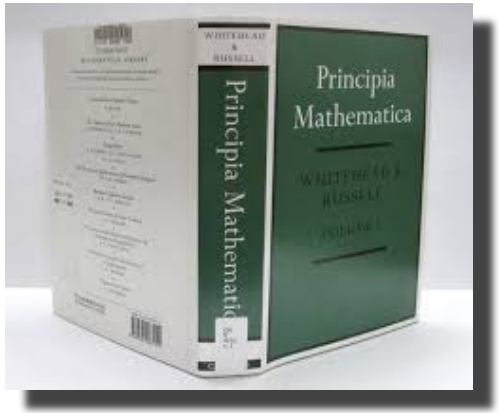
RSAConference2016

What is a First Principle?





Principia Mathematica
published in 1913



paloalto NETWORKS

RSAConference2016

Analogy vs First Principle

Analogy vs First Principle

SIMILAR

paloalto NETWORKS

Analogy vs First Principle

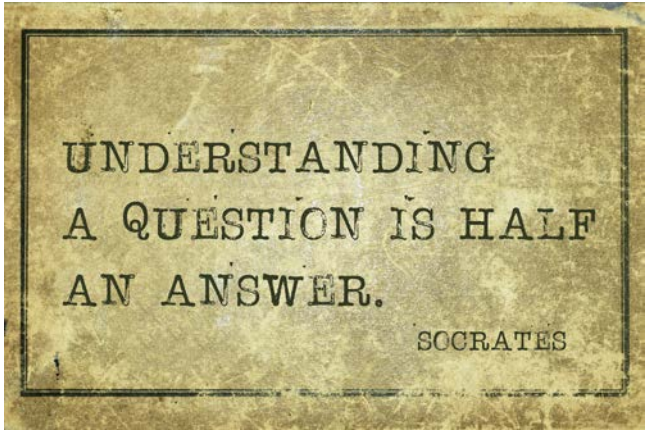
SIMILAR

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

Network Defender First Principles

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

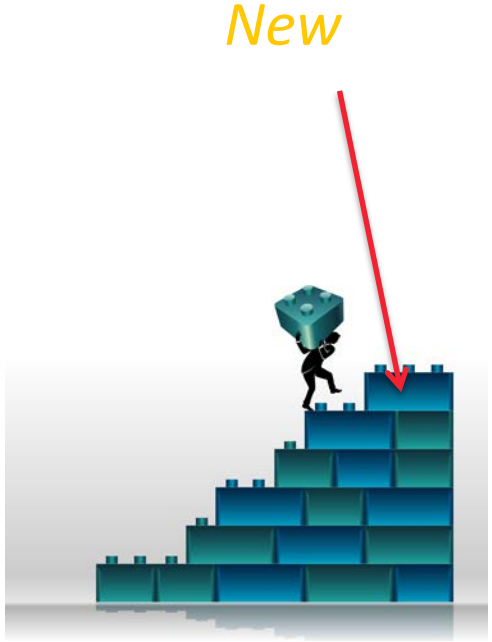
What is a First Principle?

Fundamental

Self Evident

Experts Agree

Atomic



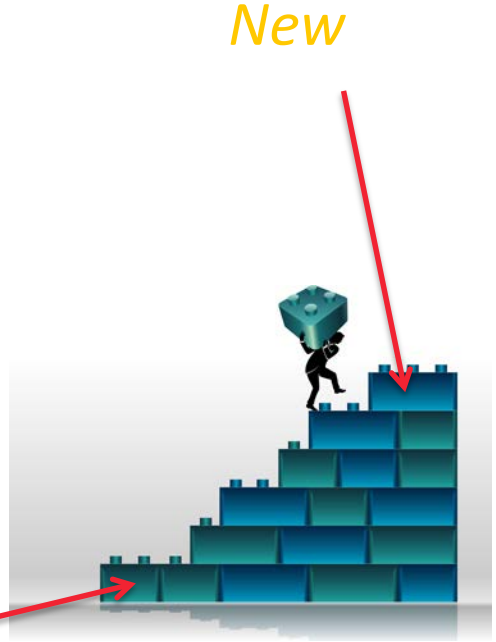
What is a First Principle?

Fundamental

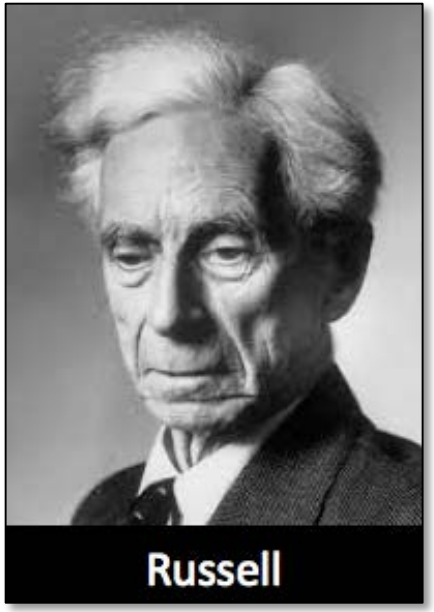
Self Evident

Experts Agree

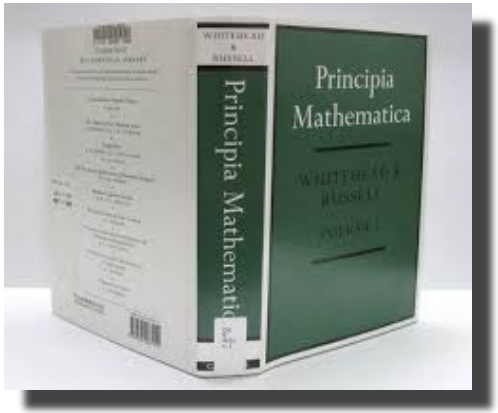
Atomic



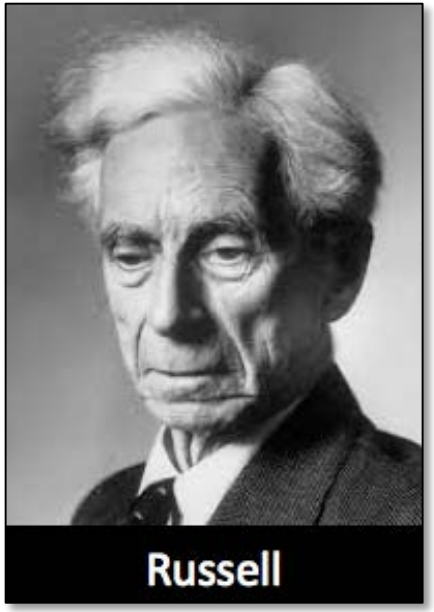
What is a First Principle?



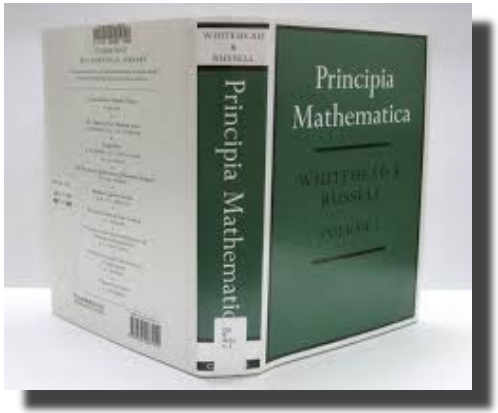
$$1 + 1 = 2$$



What is a First Principle?

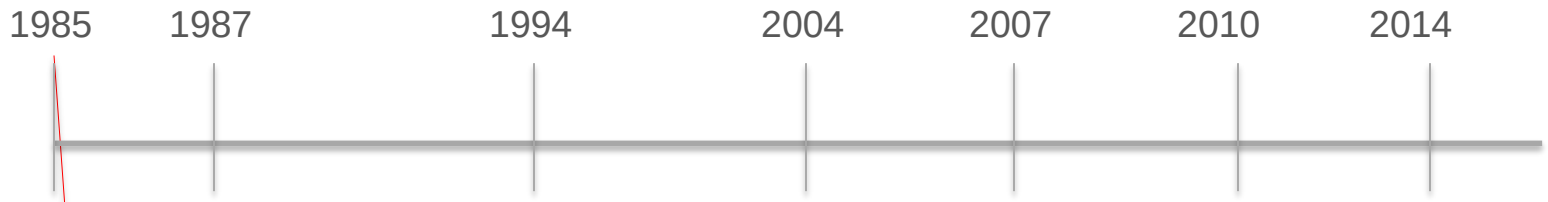


$1 + 1 = 2$



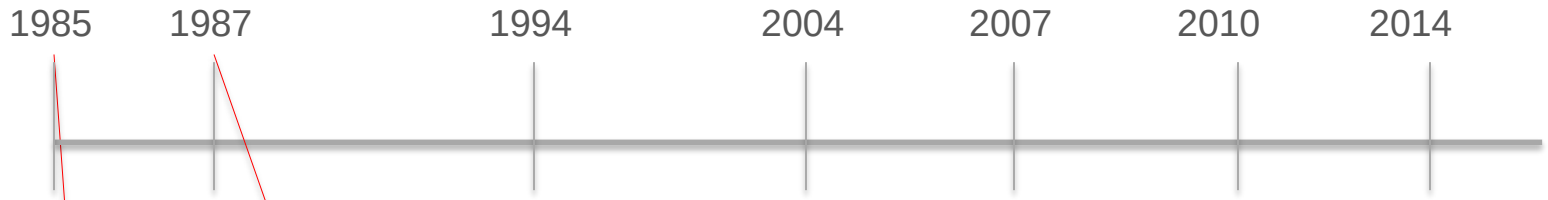
*Note: Might be useful to know

Network Defender Problem Space



First Intrusion Detection System

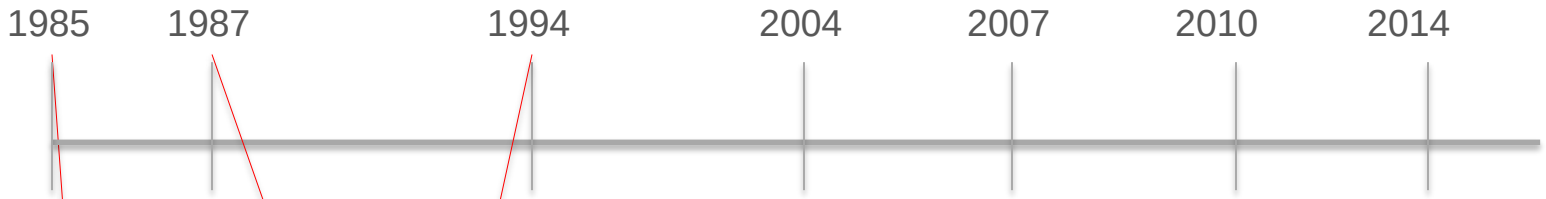
Network Defender Problem Space



First Intrusion Detection System

First Anti-Virus System

Network Defender Problem Space

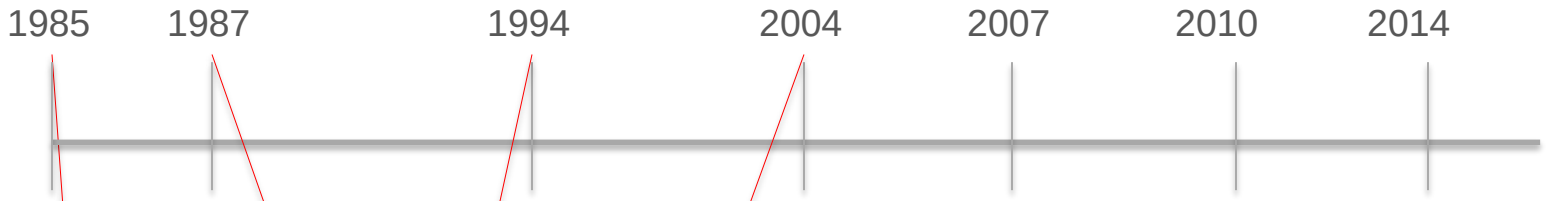


First Intrusion Detection System

First Anti-Virus System

First Firewall

Network Defender Problem Space

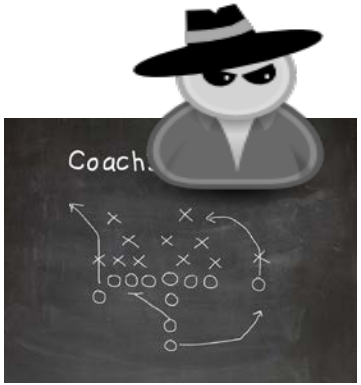


First Intrusion Detection System

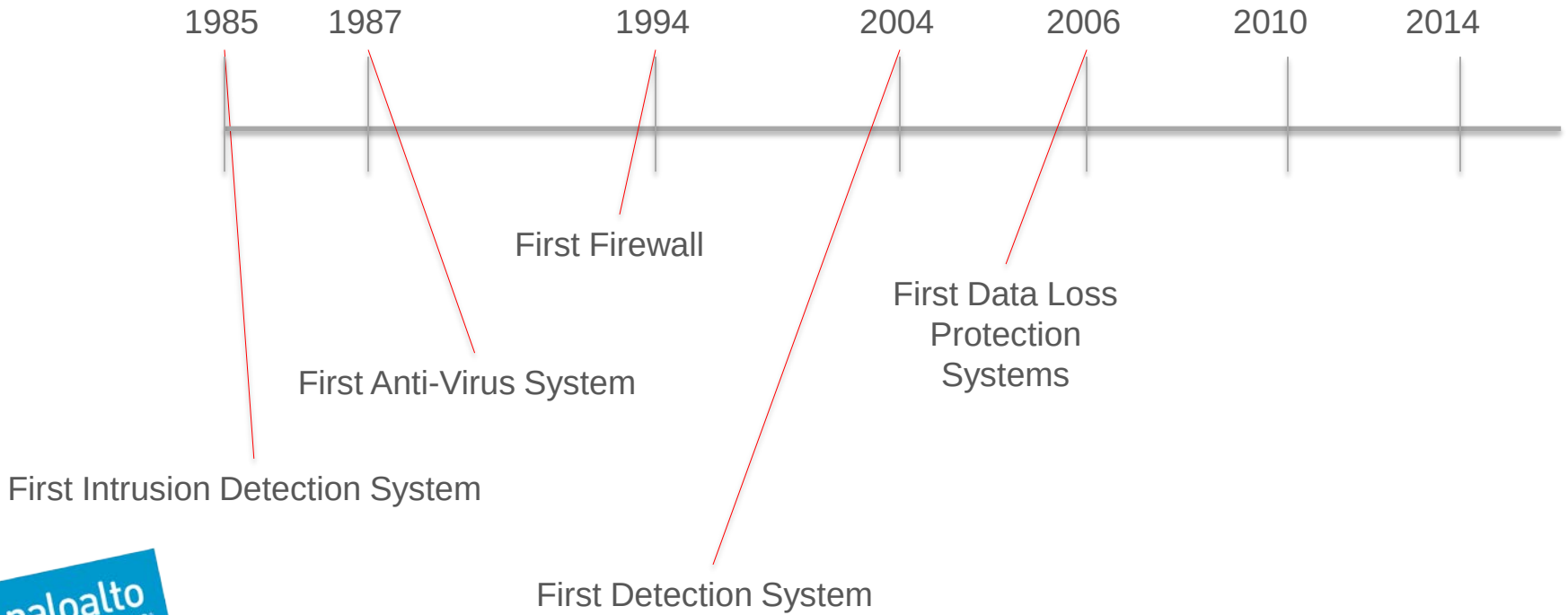
First Anti-Virus System

First Firewall

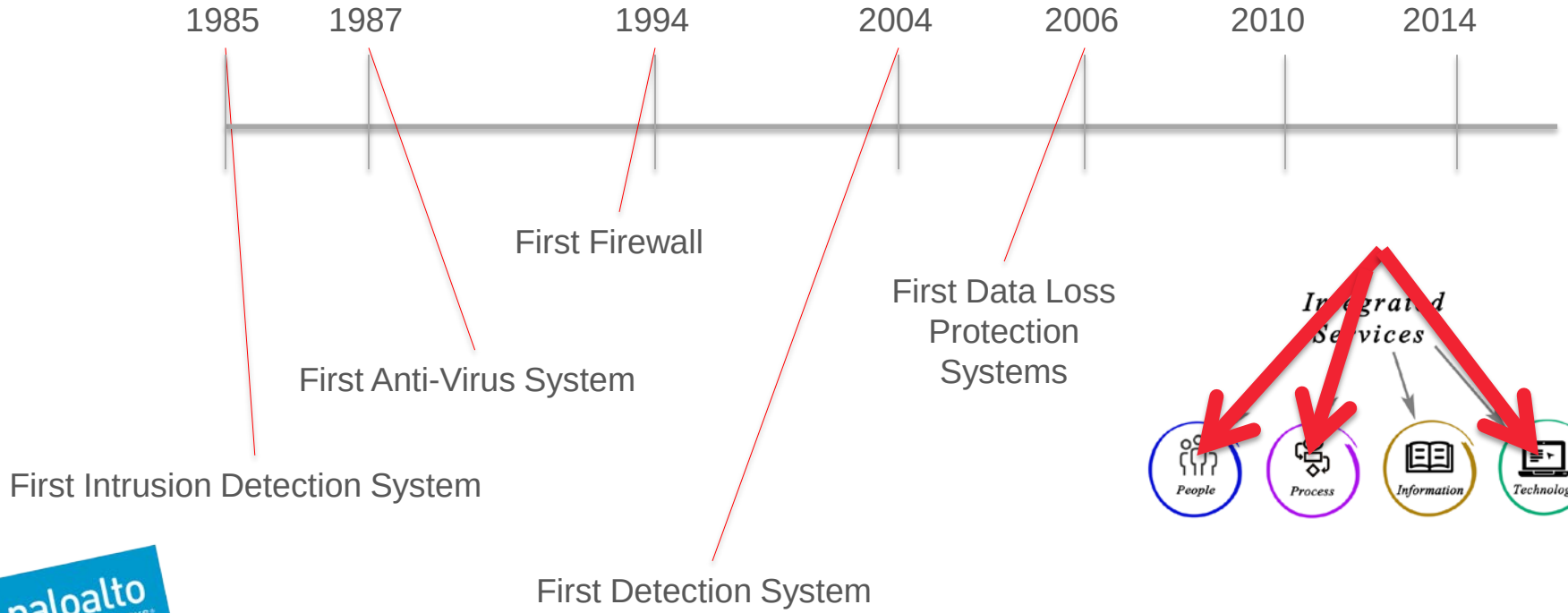
First Detection System



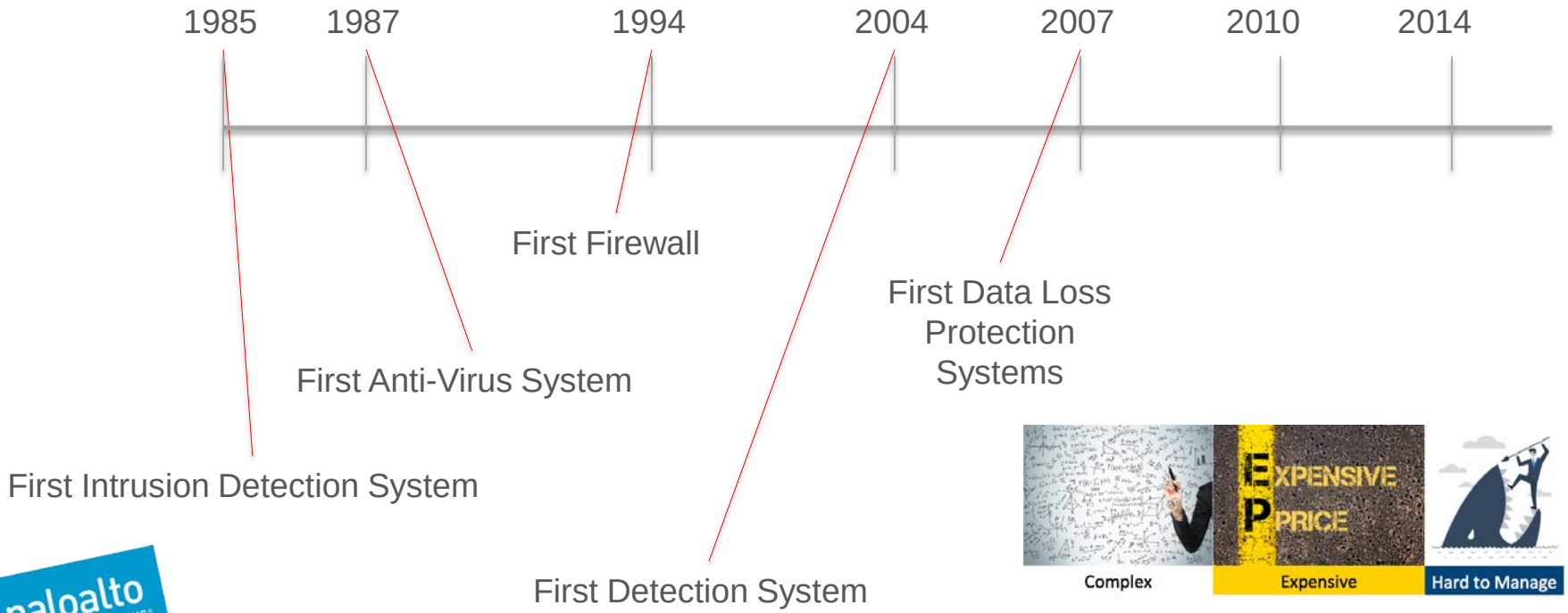
Network Defender Problem Space



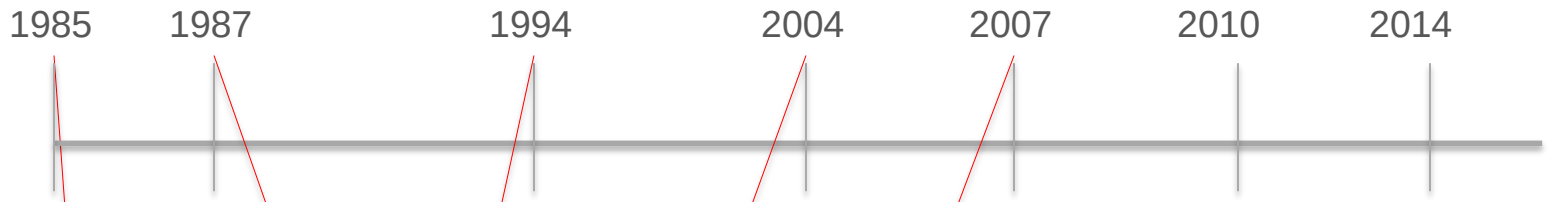
Network Defender Problem Space



Network Defender Problem Space



Network Defender Problem Space



First Intrusion Detection System

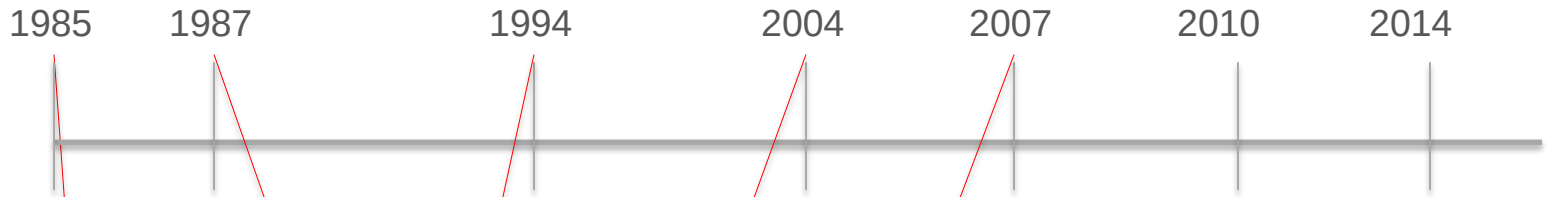
First Anti-Virus System

First Firewall

First Detection System

First Data Loss Protection Systems

Network Defender Problem Space



First Intrusion Detection System

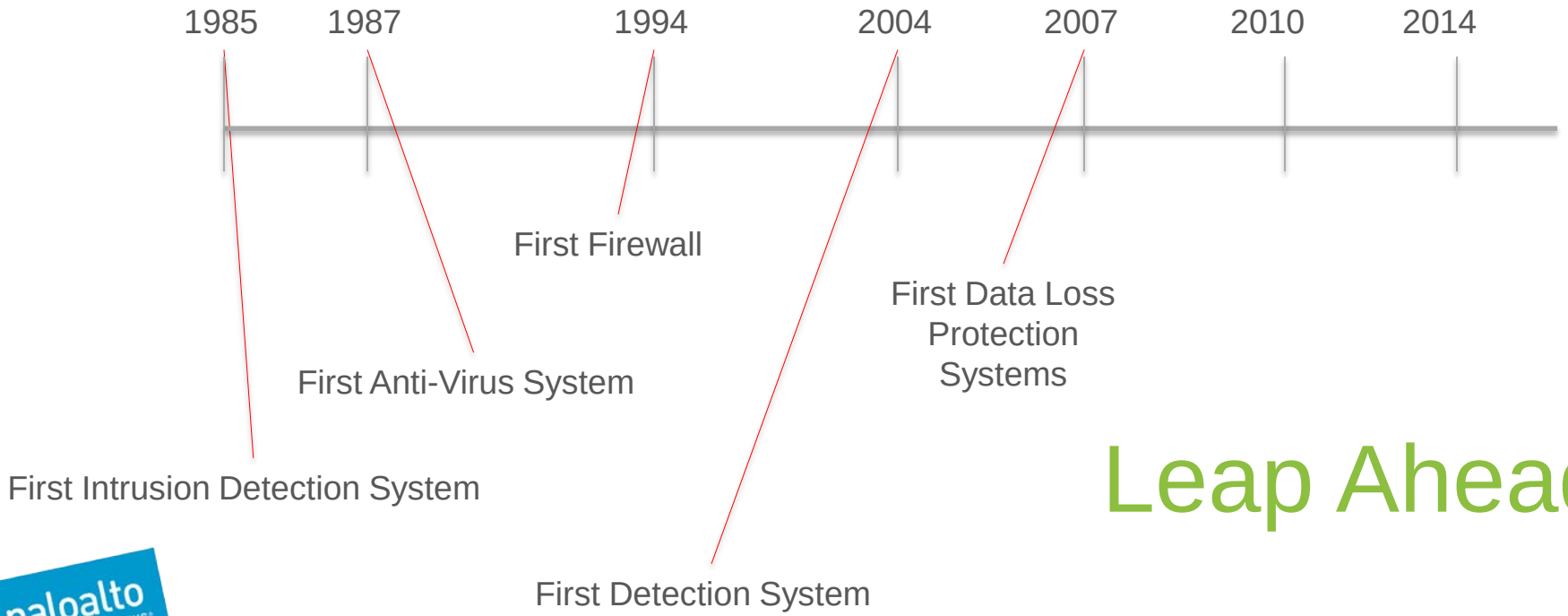
First Anti-Virus System

First Firewall

First Detection System

First Data Loss Protection Systems

Network Defender Problem Space



Leap Ahead

Network Defender Problem Space

1985 1987 1994 2004 2007 2010 2014

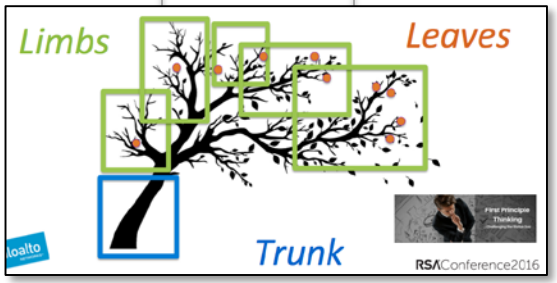
First Intrusion Detection System

First Anti-Virus System

First Firewall

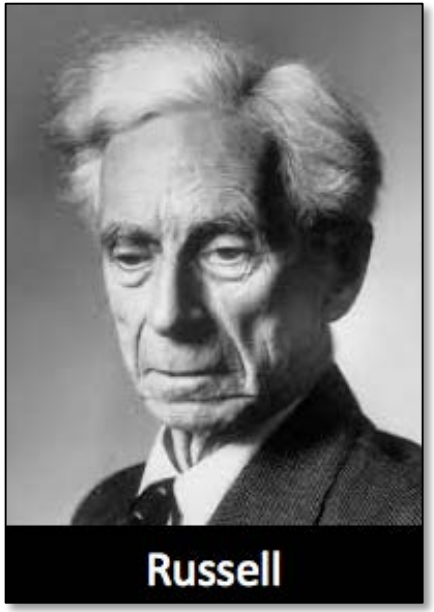
First Detection System

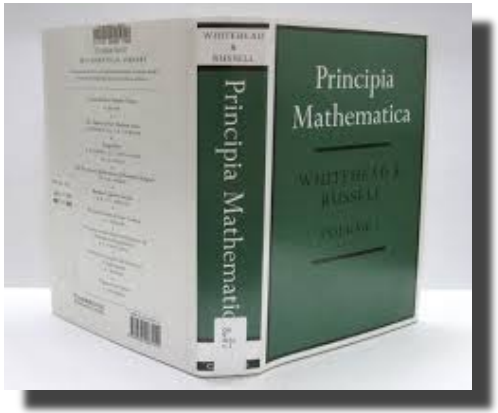
First Data Loss Protection Systems



paloalto NETWORKS

Prefatory First Principle Statements





Prefatory First Principle Statements

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

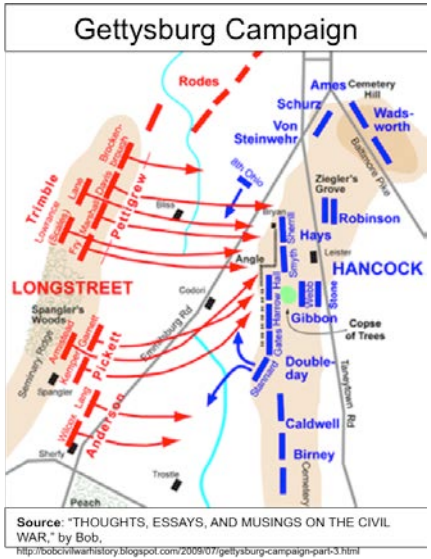
Prefatory First Principle Statements

Prefatory First Principle Statements

Prefatory First Principle Statements

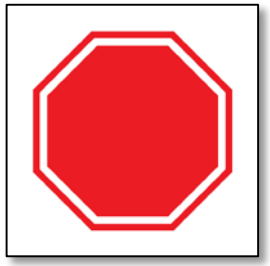
Victim

Prefatory First Principle Statements

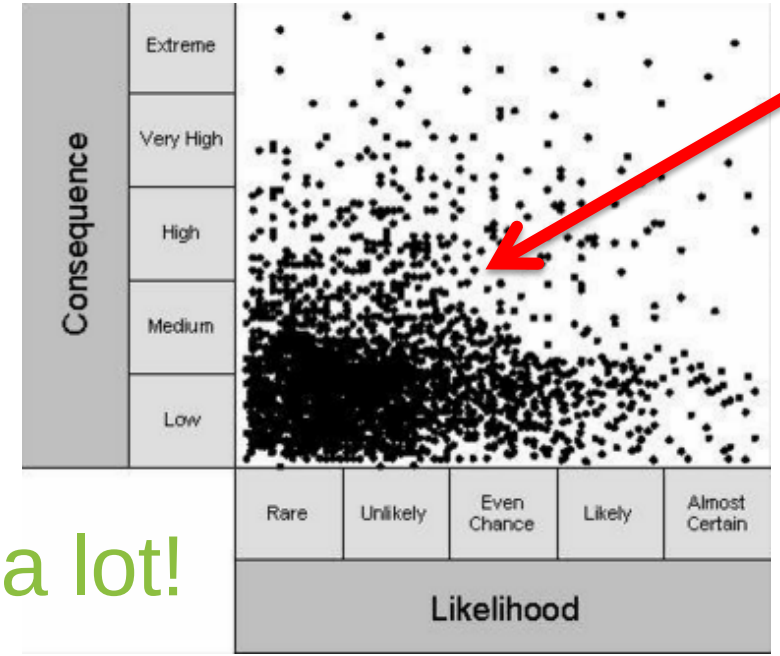


Victim

Prefatory First Principle Statements

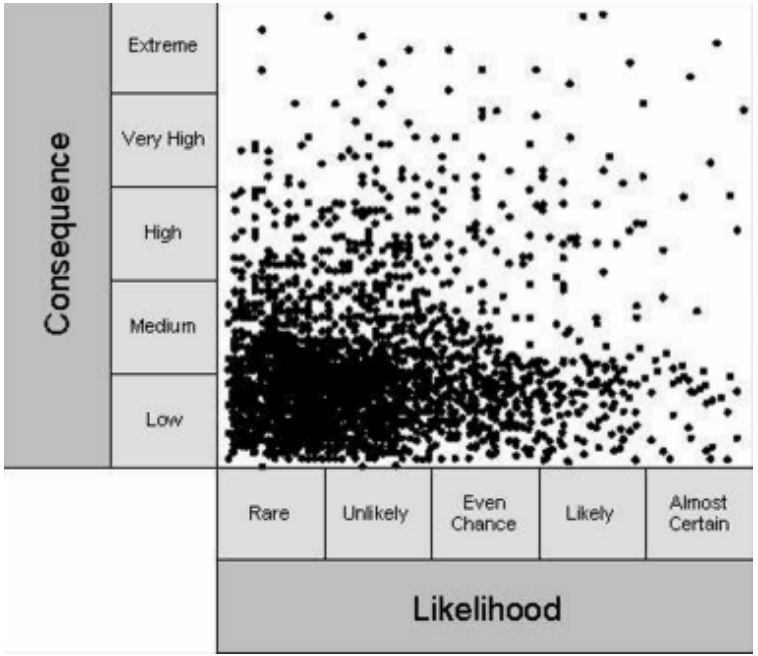


?



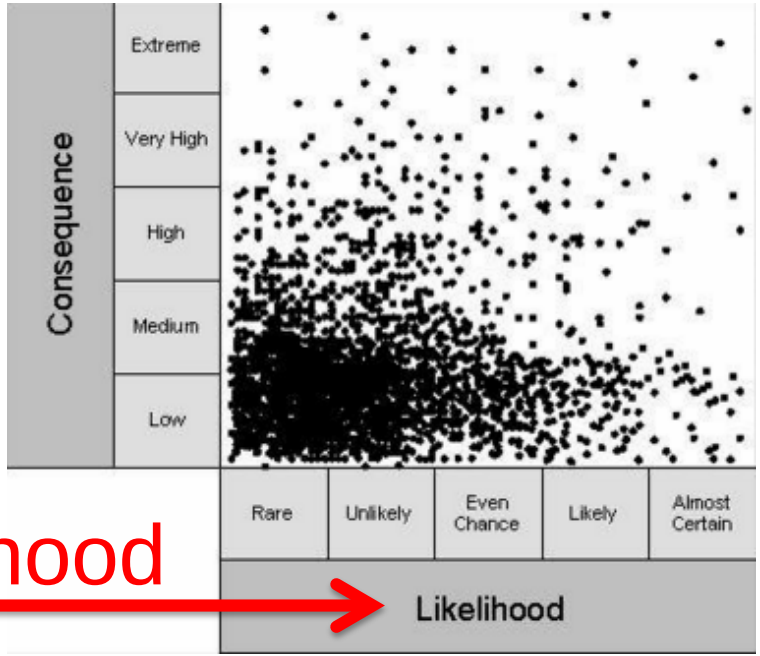
Wow! That's a lot!

Prefatory First Principle Statements



Risk Matrix

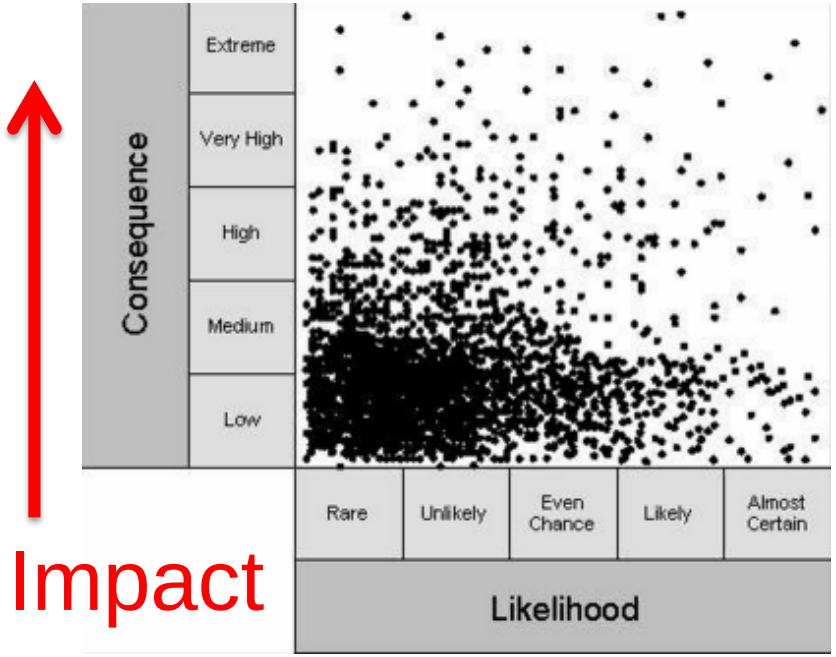
Prefatory First Principle Statements



X-Axis: Likelihood

Risk Matrix

Prefatory First Principle Statements



Y-Axis: Impact

Risk Matrix

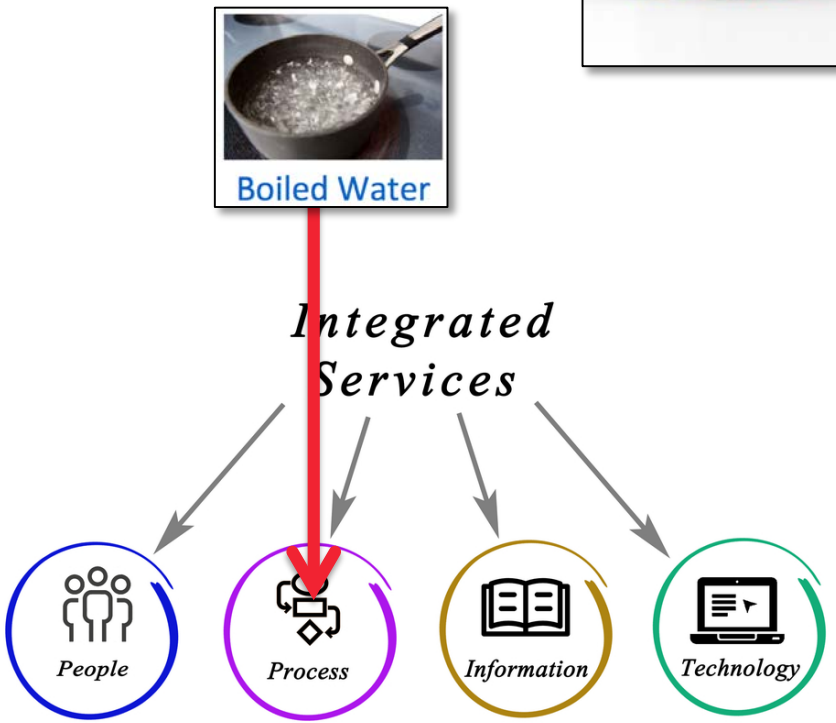
What is a Network Defender First Principle?

What is a Network Defender First Principle?

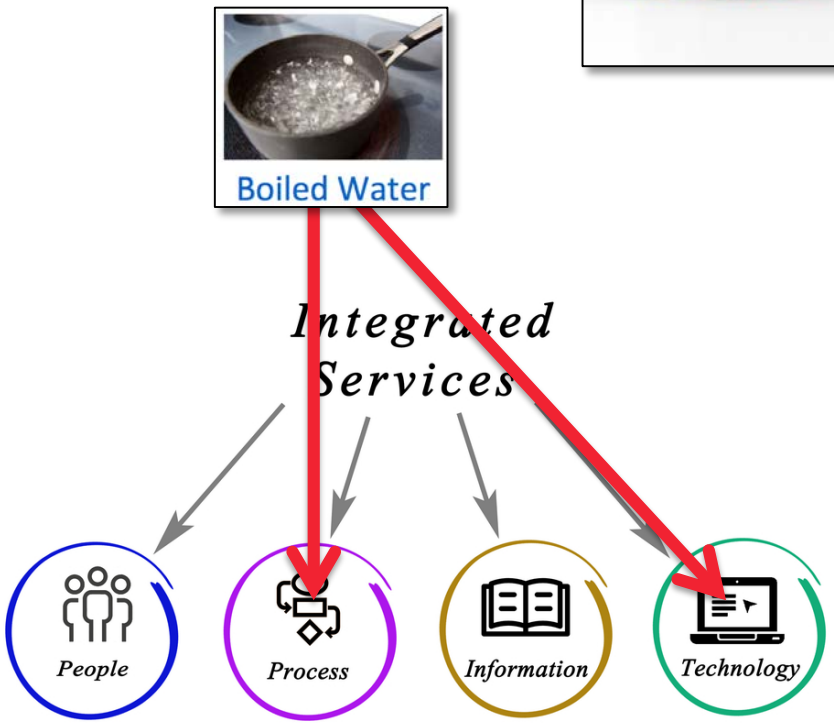
paloalto NETWORKS

RSAConference2016

What is a Network Defender First Principle?



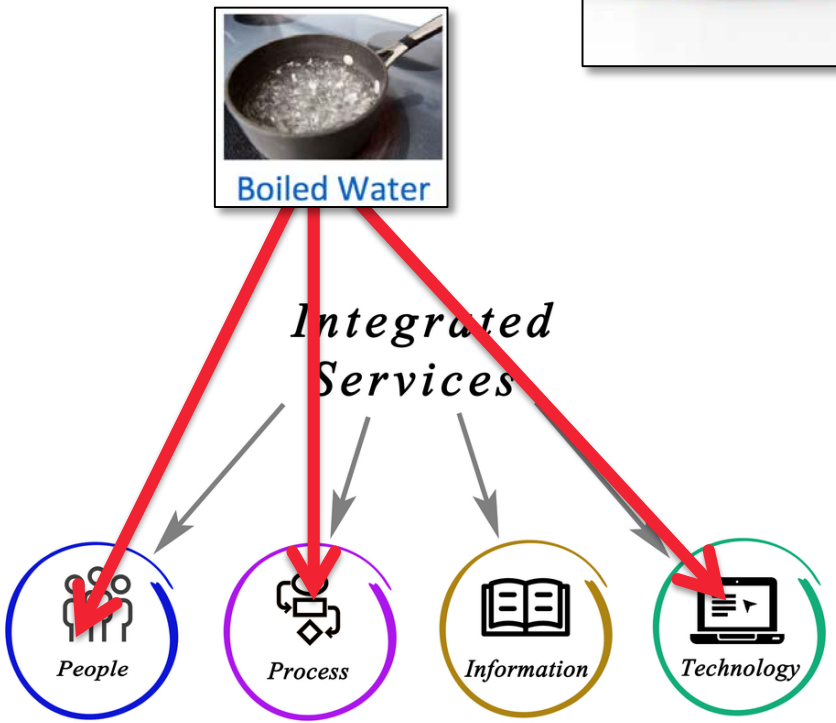
What is a Network Defender First Principle?



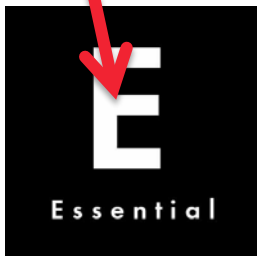
paloalto NETWORKS

RSAConference2016

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

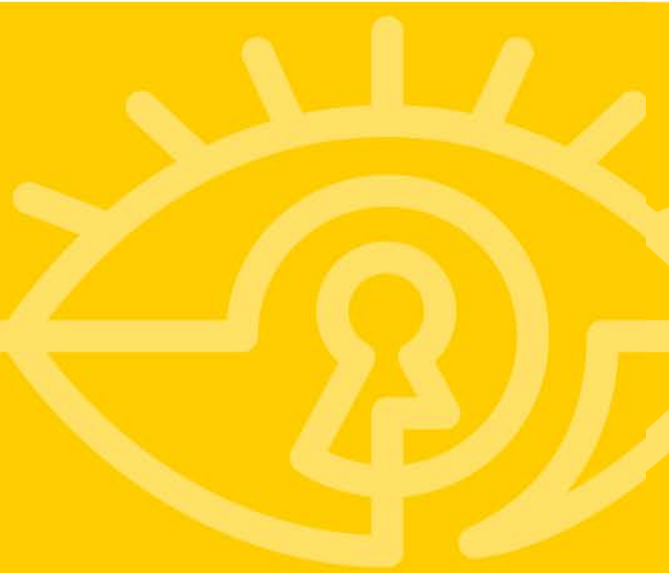
Network Defender Semantic Tree

1 Trunk

Network Defender Semantic Tree

5 Limbs

1 Trunk



The Trunk

Network Defender Semantic Tree: The Trunk

E

Essential

paloalto NETWORKS

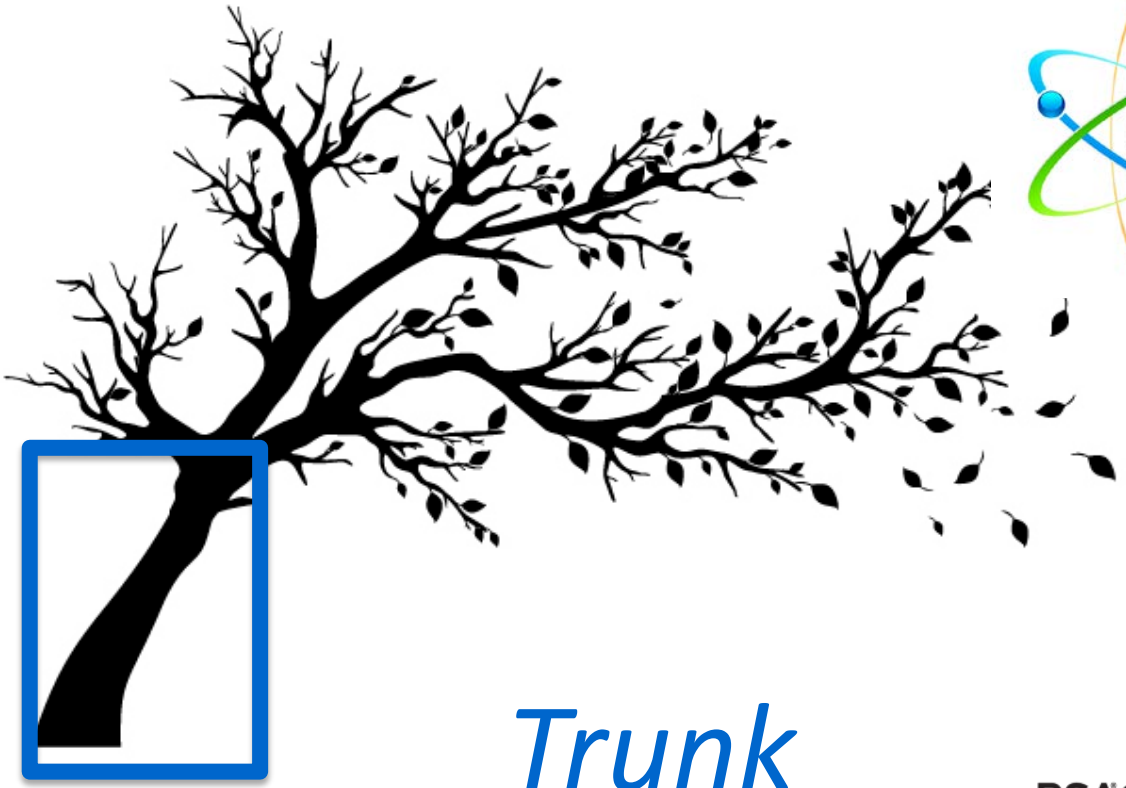
Network Defender Semantic Tree: The Trunk

E

Essential

paloalto NETWORKS

Network Defender Semantic Tree: The Trunk



Trunk

Network Defender Semantic Tree: The Trunk

E

Essential

Prevent High Risk Material Impact

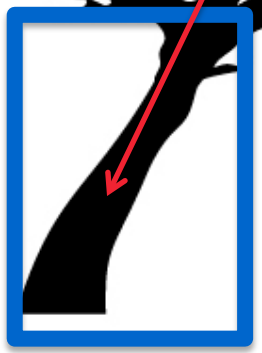
Trunk

paloalto NETWORKS

Network Defender Semantic Tree: The Trunk

Trunk

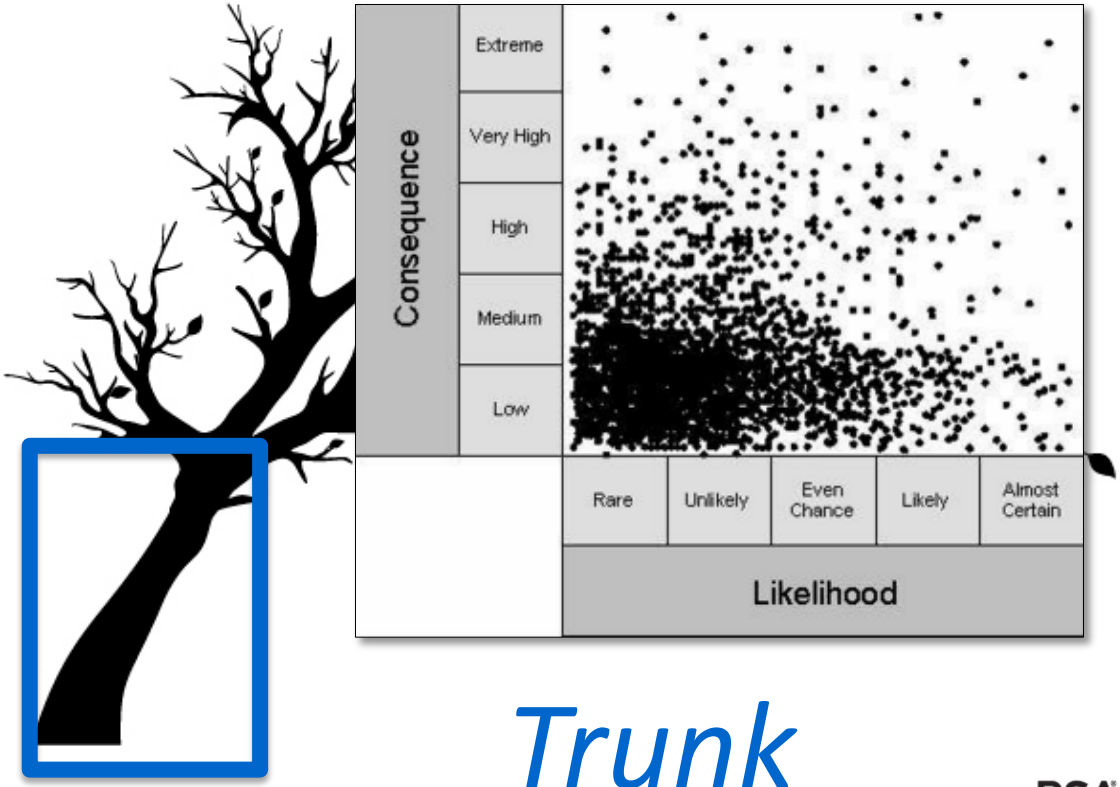
Network Defender Semantic Tree: The Trunk



Trunk

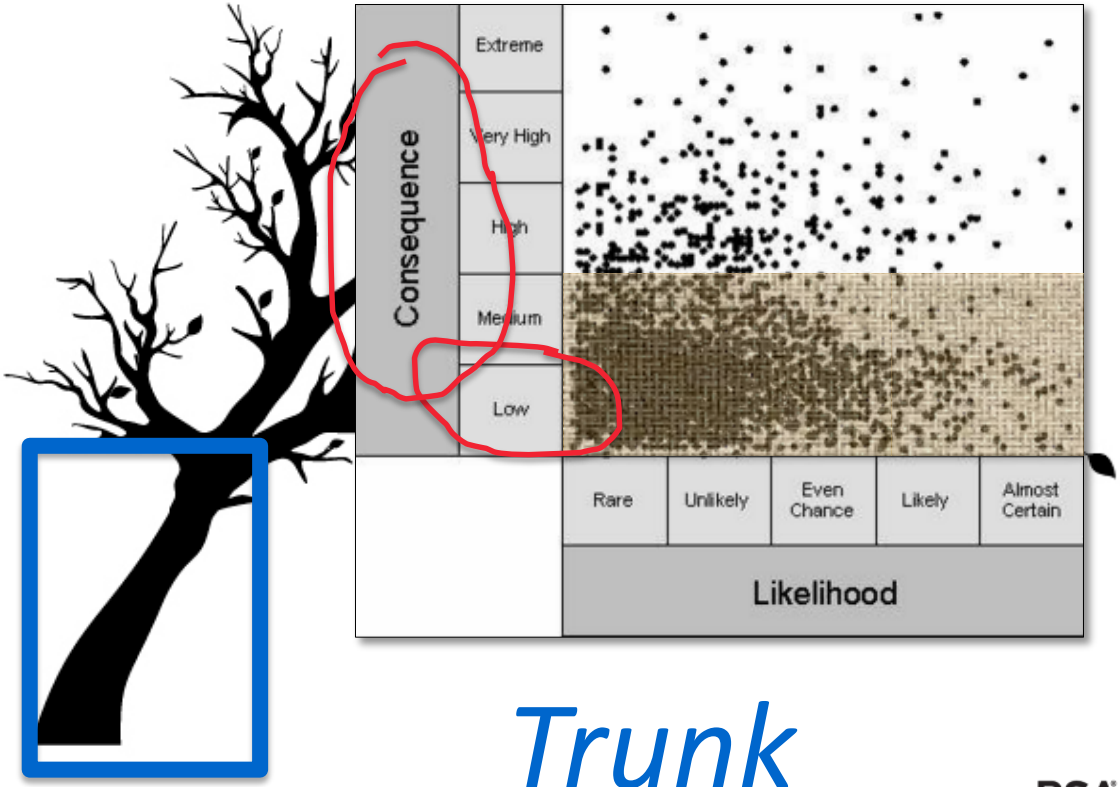
paloalto NETWORKS

Network Defender Semantic Tree: The Trunk



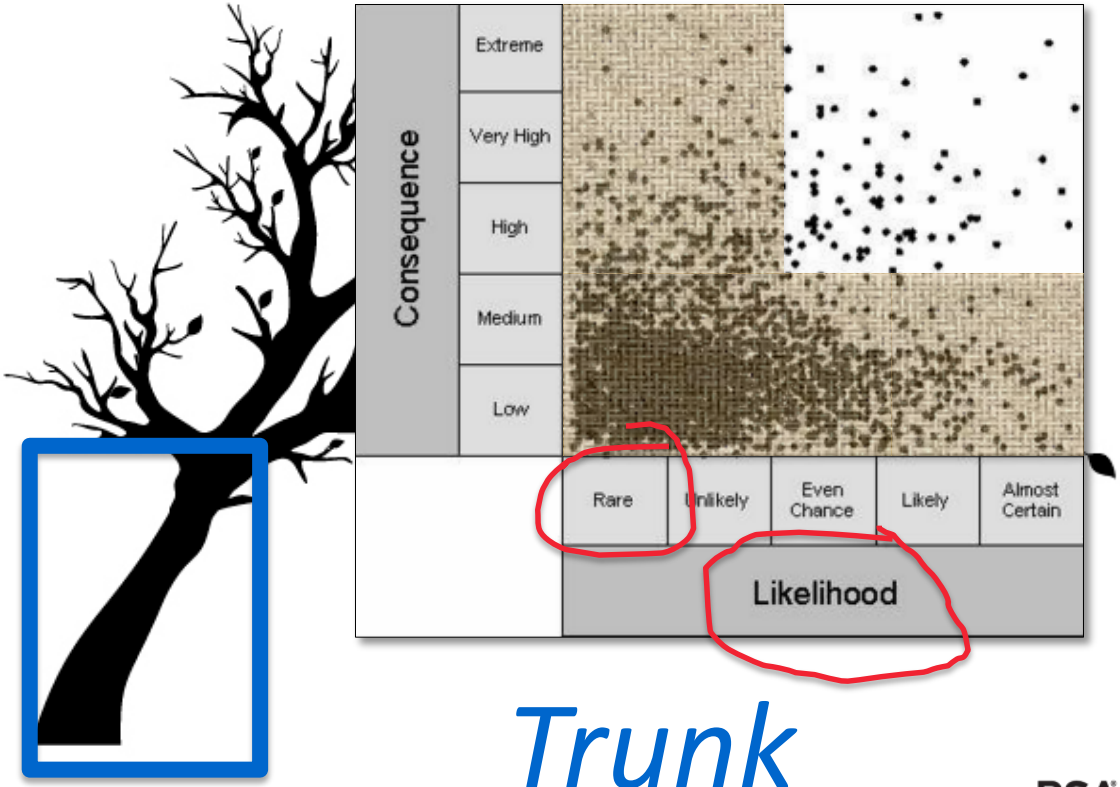
Trunk

Network Defender Semantic Tree: The Trunk



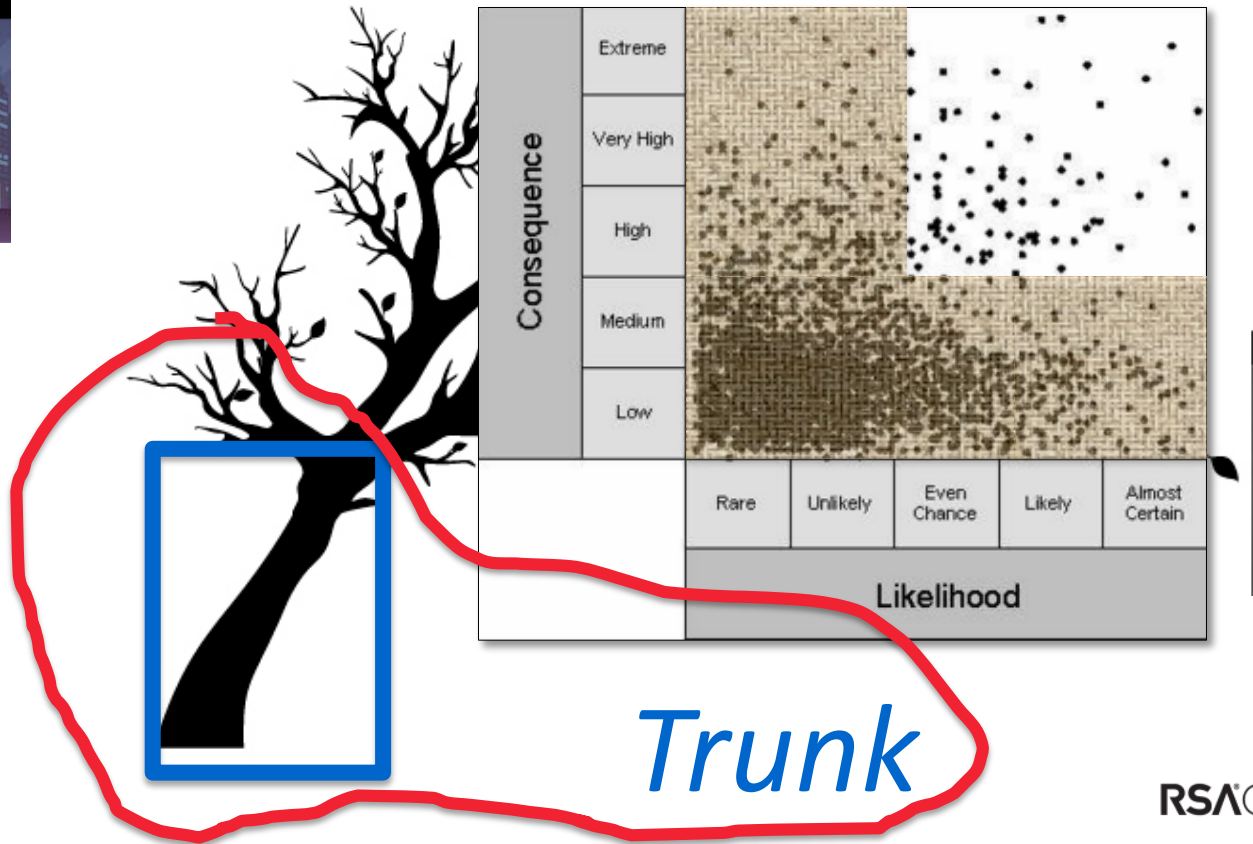
Trunk

Network Defender Semantic Tree: The Trunk

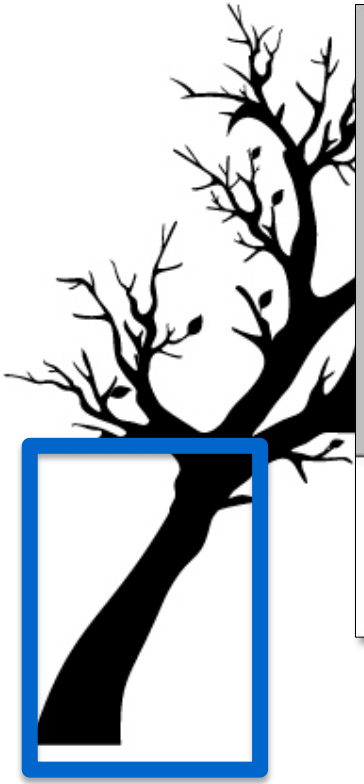


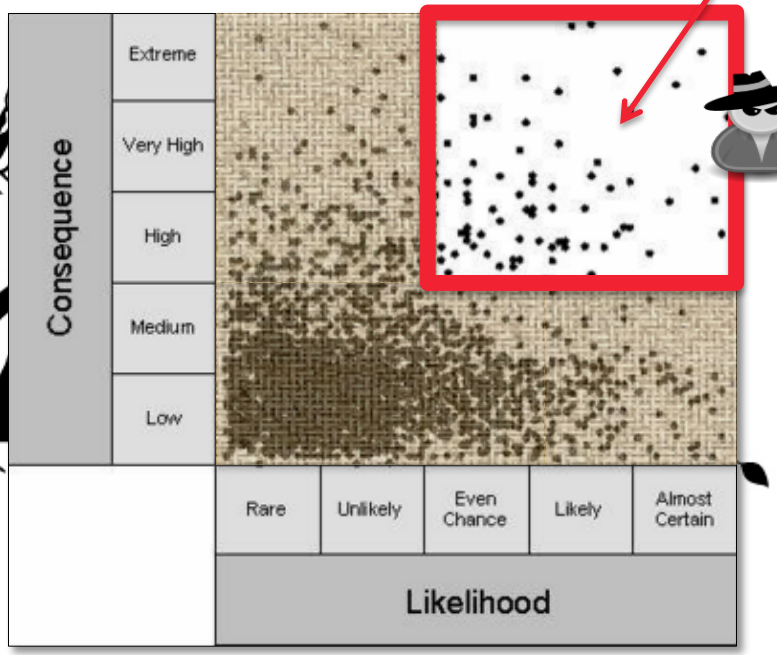
Trunk

Network Defender Semantic Tree: The Trunk



Network Defender Semantic Tree: The Trunk



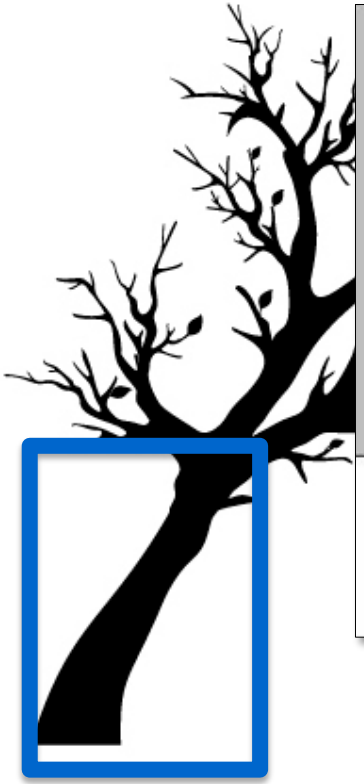


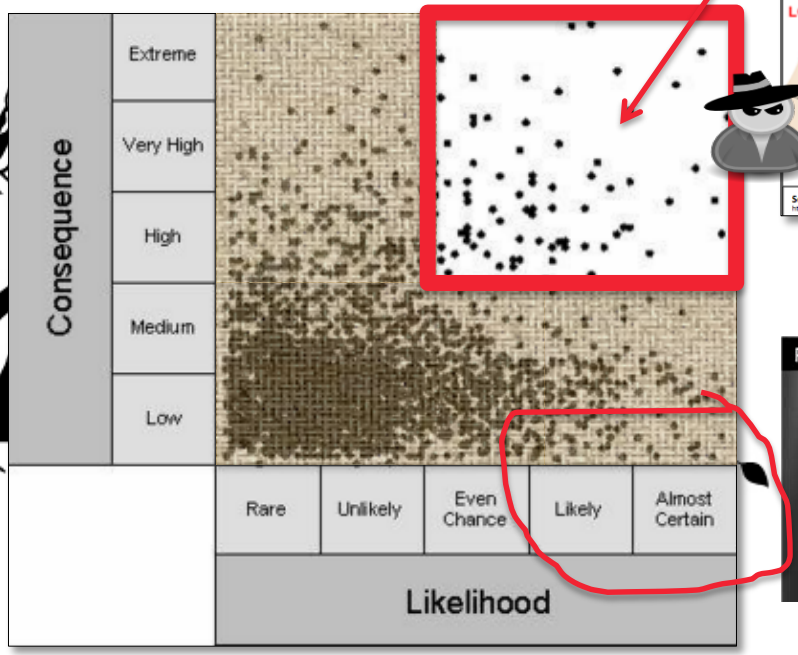
Trunk

paloalto NETWORKS

RSAConference2016

Network Defender Semantic Tree: The Trunk





Trunk

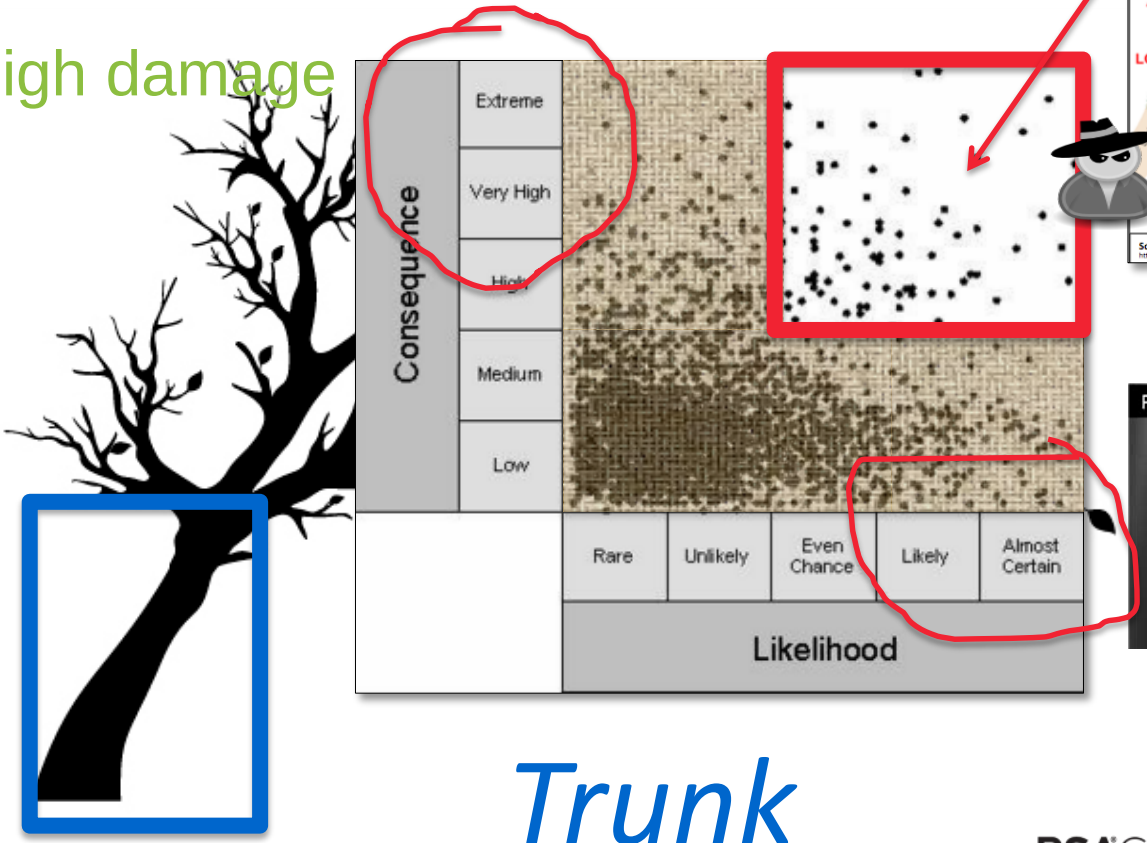
High Probability

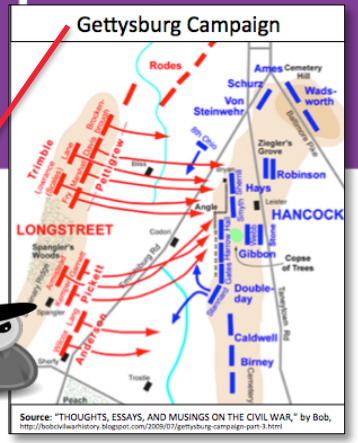
paloalto NETWORKS

RSAConference2016

Network Defender Semantic Tree: The Trunk

High damage





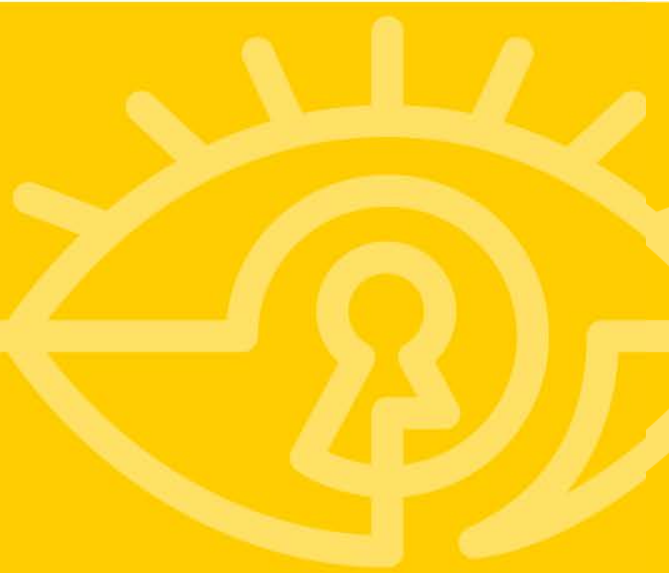
Trunk

paloalto NETWORKS

RSAConference2016

Network Defender Semantic Tree: The Trunk

Prevent High Risk Material Impact



First Limb

Network Defender Semantic Tree: First Limb

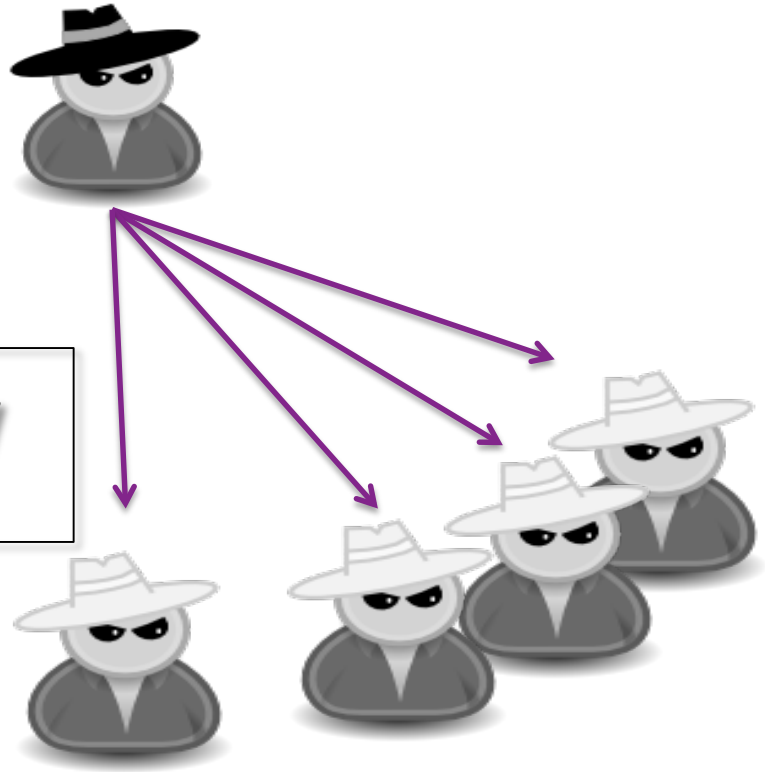
Establish a Robust Threat Prevention program

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

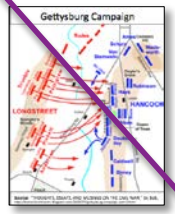
NEW

paloalto NETWORKS

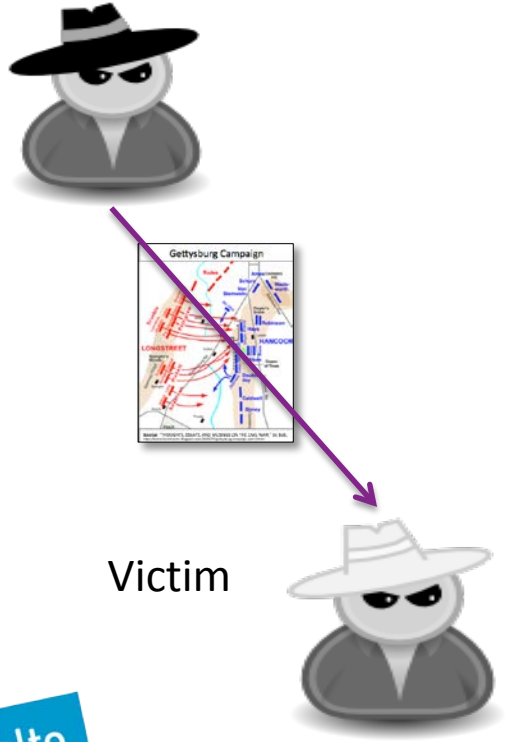
RSAConference2016

Network Defender Semantic Tree: First Limb

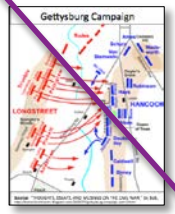
Network Defender Semantic Tree: First Limb



Network Defender Semantic Tree: First Limb



Network Defender Semantic Tree: First Limb



Victim

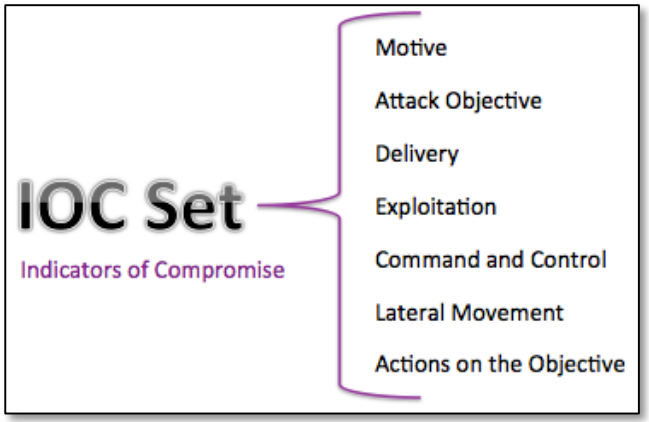
IOC Set

Indicators of Compromise

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

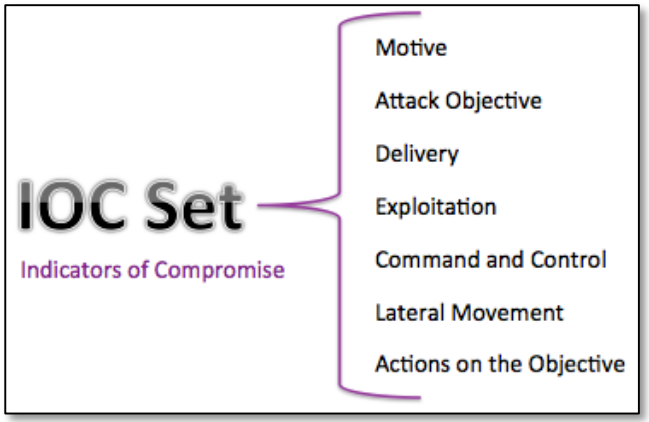
Network Defender Semantic Tree: First Limb

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**.



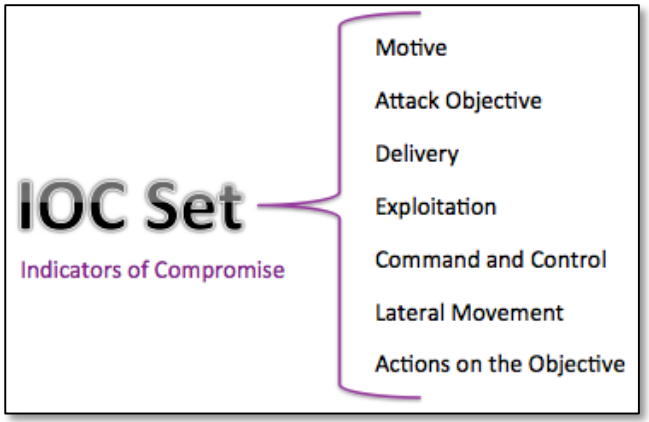
Network Defender Semantic Tree: First Limb

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**.

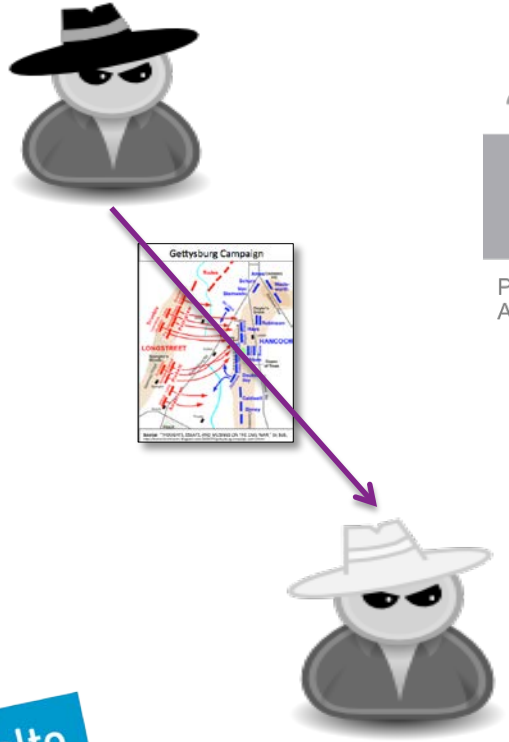


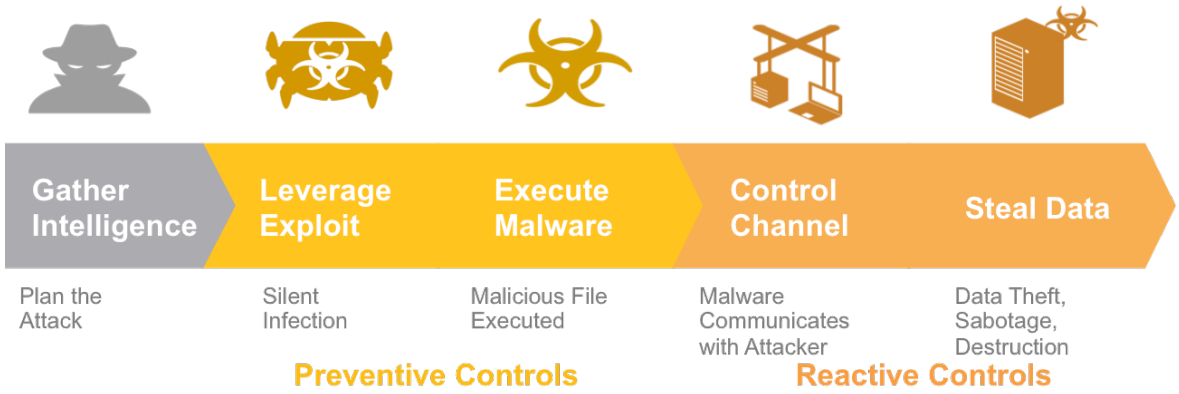
Network Defender Semantic Tree: First Limb

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**.



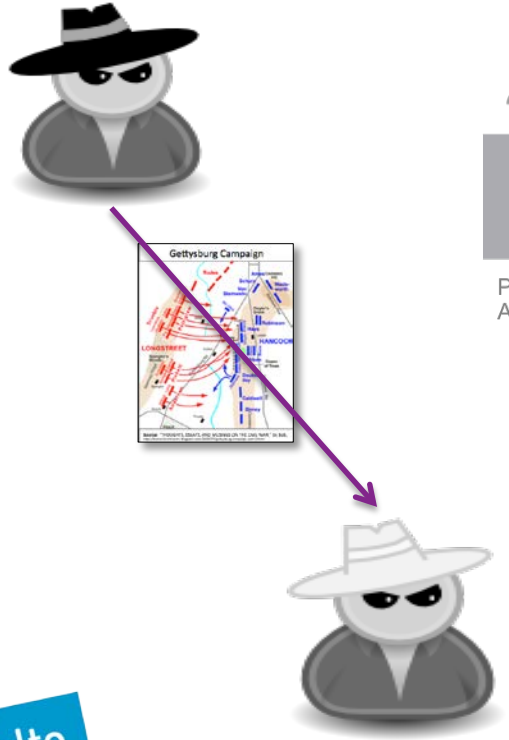
Network Defender Semantic Tree: First Limb

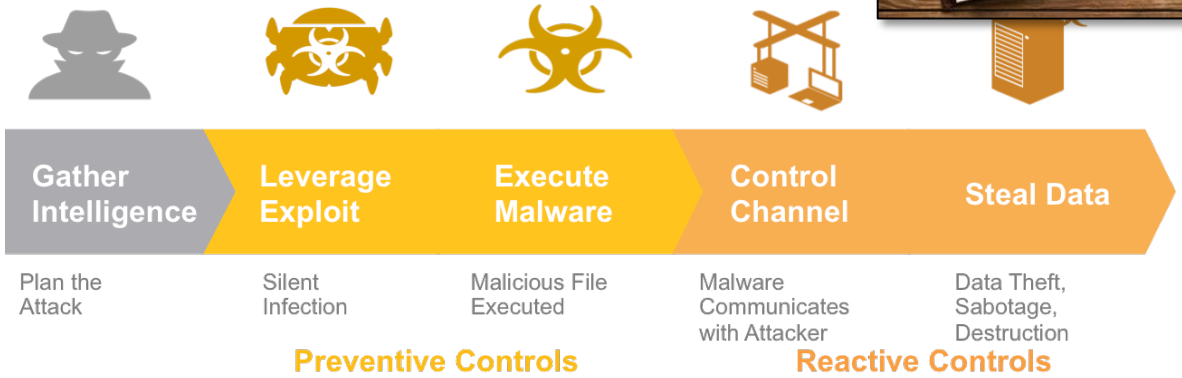




The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

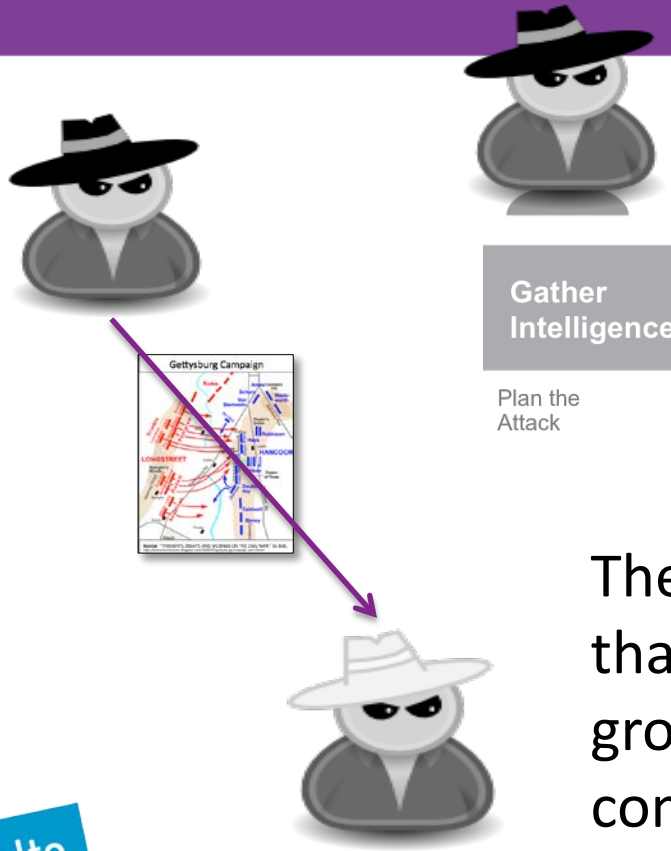
Network Defender Semantic Tree: First Limb





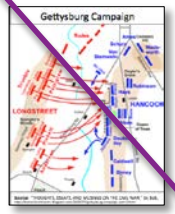
The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: First Limb



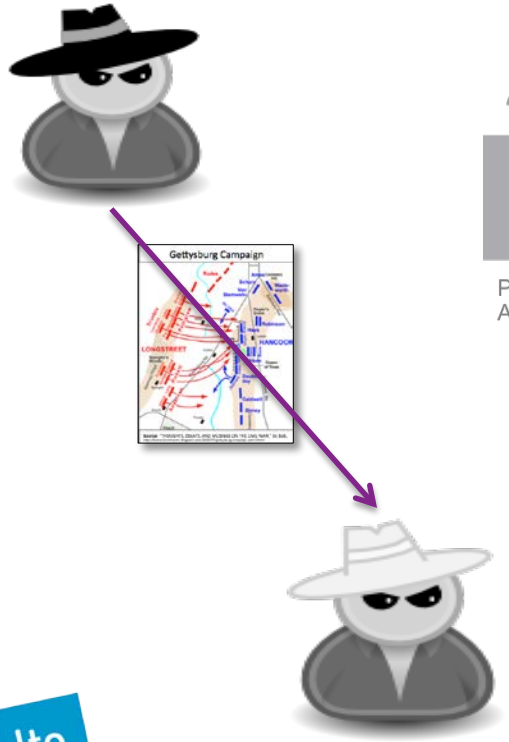
The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: First Limb



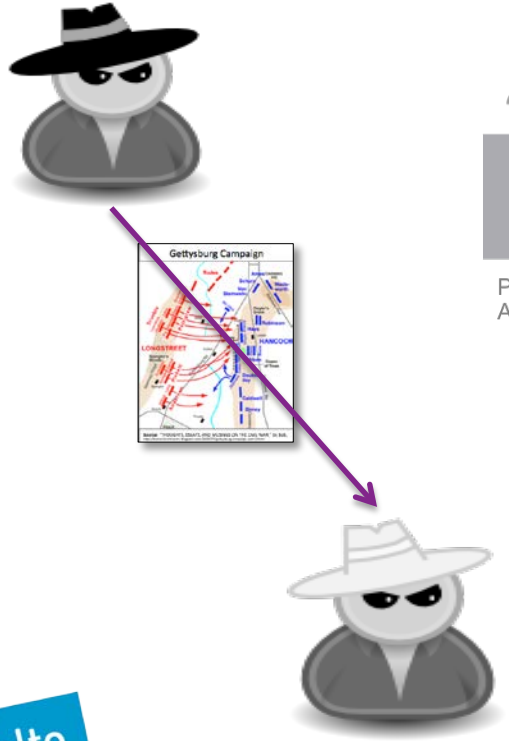
The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission

Network Defender Semantic Tree: First Limb



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

Network Defender Semantic Tree: First Limb

paloalto NETWORKS

paloalto NETWORKS

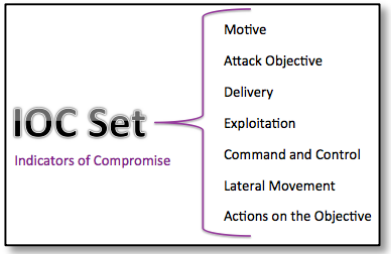
Network Defender Semantic Tree: First Limb

paloalto NETWORKS

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

paloalto NETWORKS

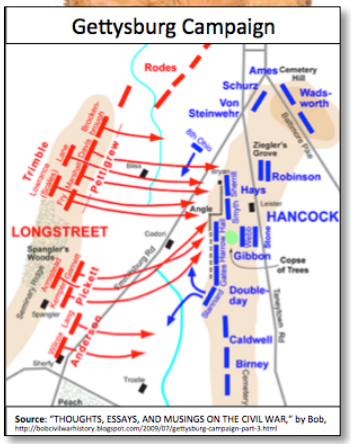
Network Defender Semantic Tree: First Limb

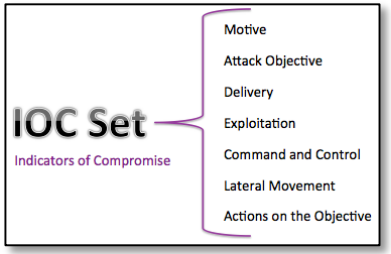


paloalto NETWORKS

paloalto NETWORKS

Network Defender Semantic Tree: First Limb

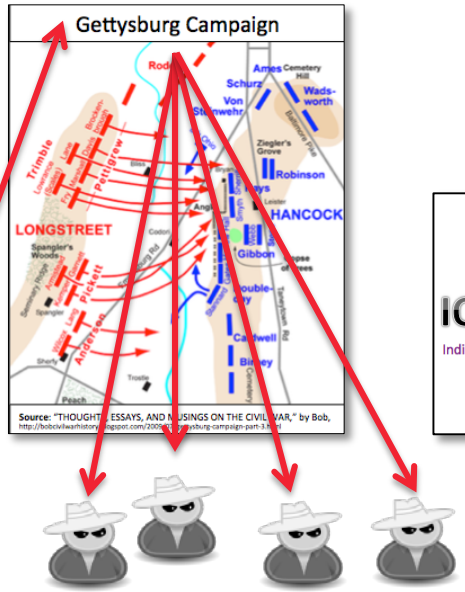


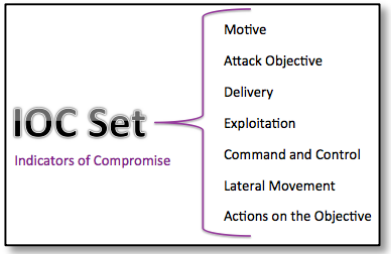


paloalto NETWORKS

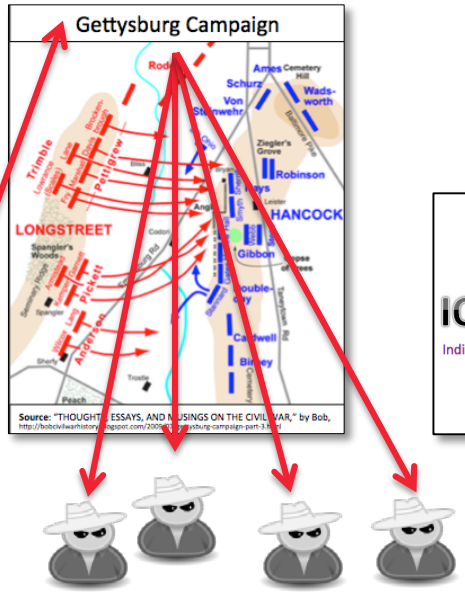
paloalto NETWORKS

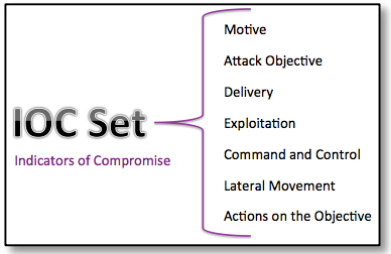
Network Defender Semantic Tree: First Limb



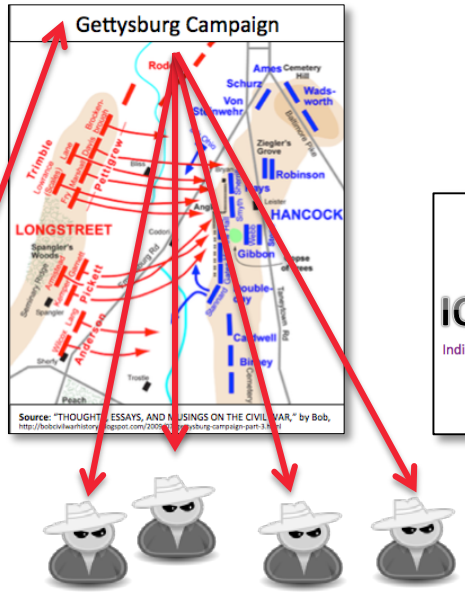


Network Defender Semantic Tree: First Limb

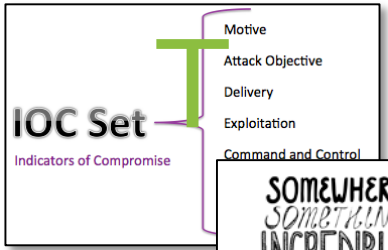


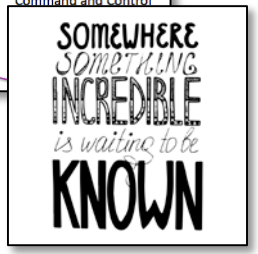


Network Defender Semantic Tree: First Limb

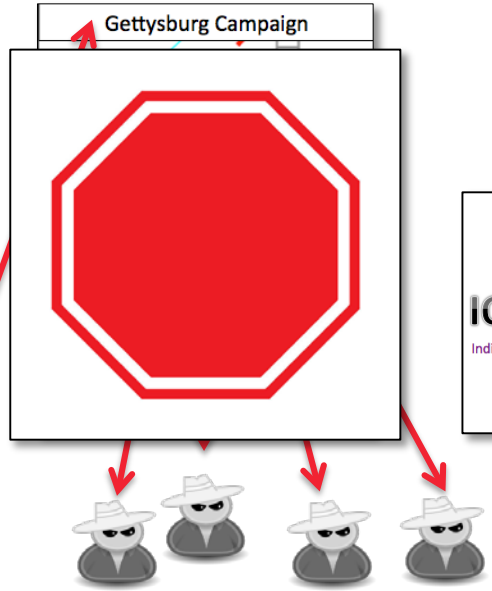


MOS

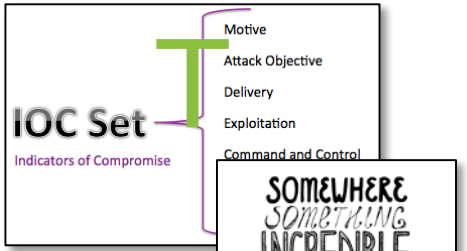


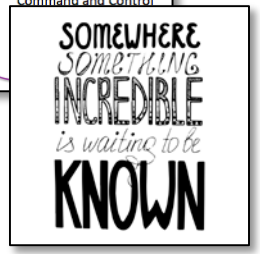


Network Defender Semantic Tree: First Limb



MOS



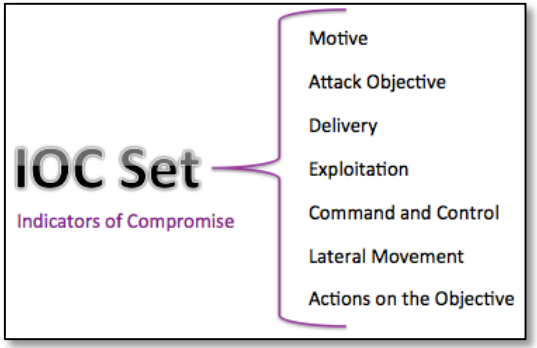


Network Defender Semantic Tree: First Limb

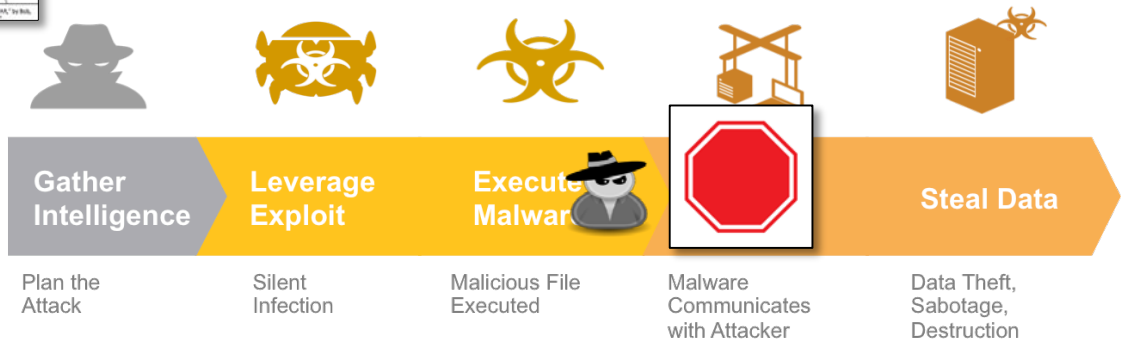
Threat Prevention is the act of turning known indicators of compromise into one or more deployed **prevention controls**.

Network Defender Semantic Tree: First Limb

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

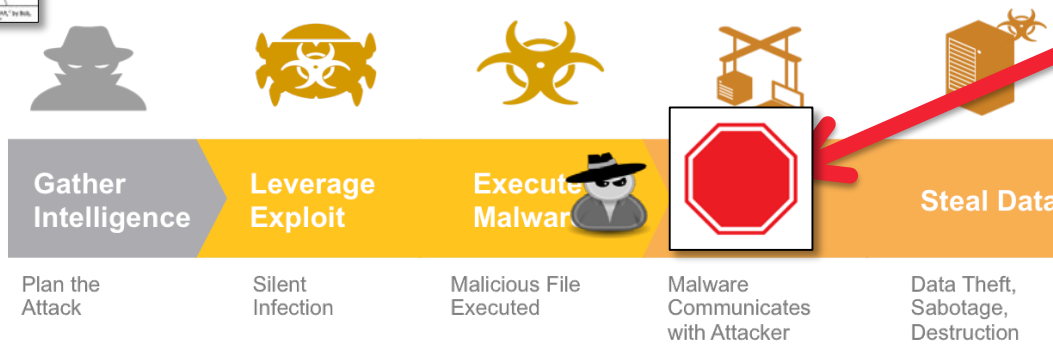


Network Defender Semantic Tree: First Limb



Network Defender Semantic Tree: First Limb

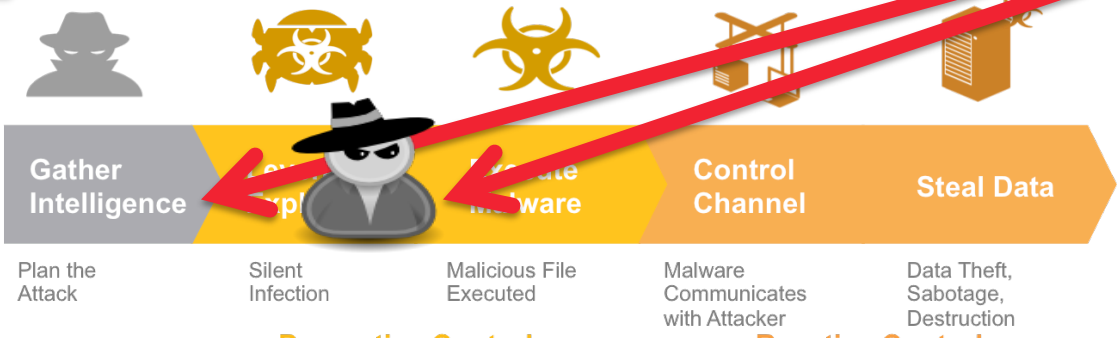
Network Defender Semantic Tree: First Limb



Precision

Network Defender Semantic Tree: First Limb

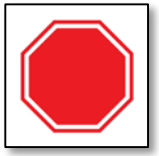
Network Defender Semantic Tree: First Limb



Network Defender Semantic Tree: First Limb

99% Guarantee

Network Defender Semantic Tree: First Limb



99% Guarantee

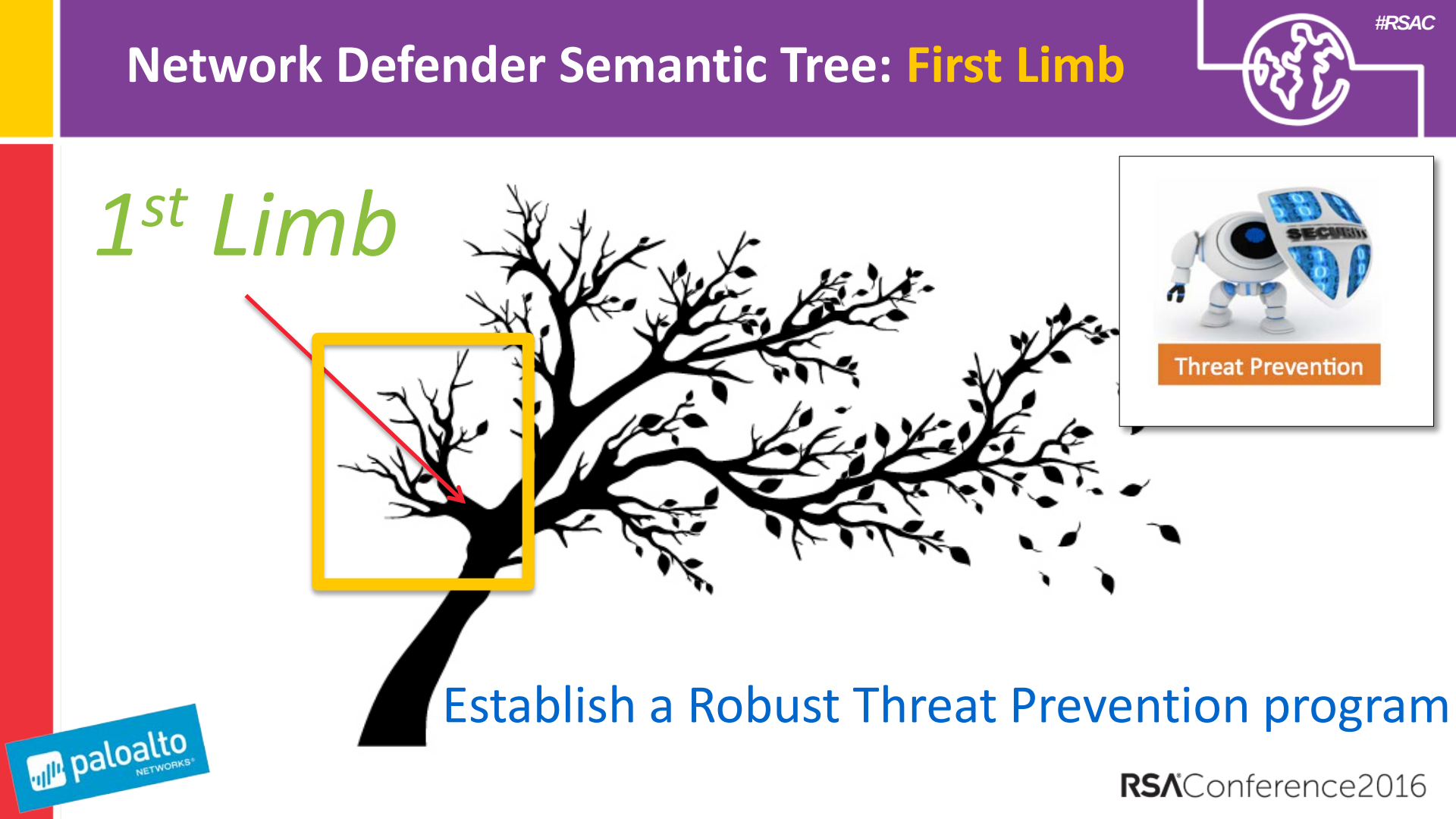
Network Defender Semantic Tree: First Limb

Gather Intelligence | [illegible] Exploit | [illegible] Malware | [illegible]trol Channel | [illegible]al D

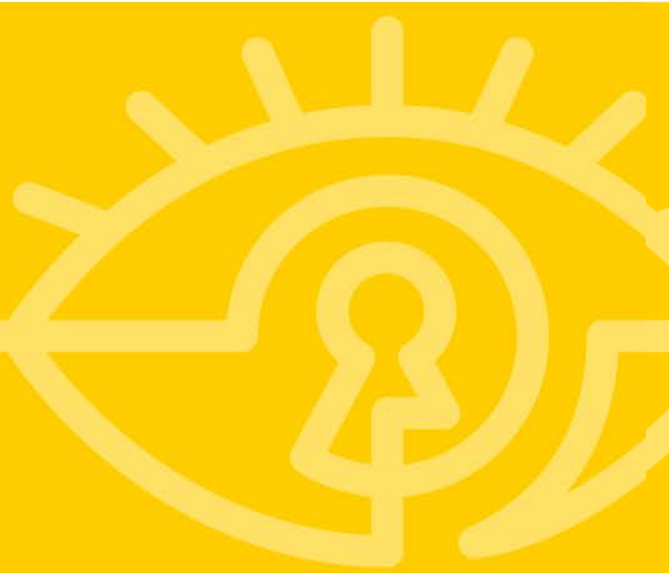
Plan the Attack | Silent Infection | Malicious File Executed | Malware Communicates with Attacker | Data Theft, Sabotage, Destruction

Preventive Controls | Reactive Controls

Network Defender Semantic Tree: First Limb



Establish a Robust Threat Prevention program

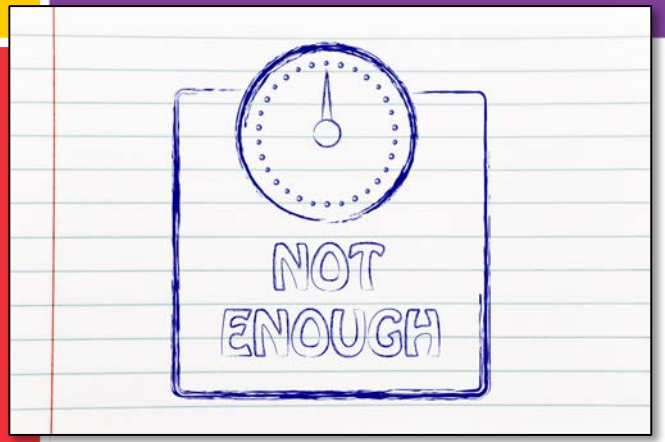


Second Limb

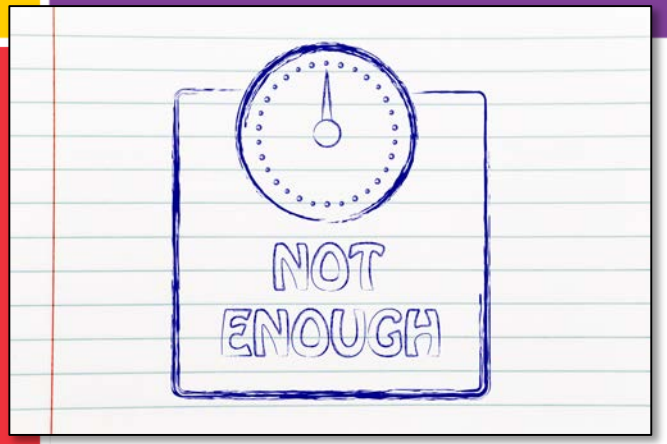
Network Defender Semantic Tree: 2d Limb

Establish a Robust Threat Detection Program

Network Defender Semantic Tree: 2d Limb

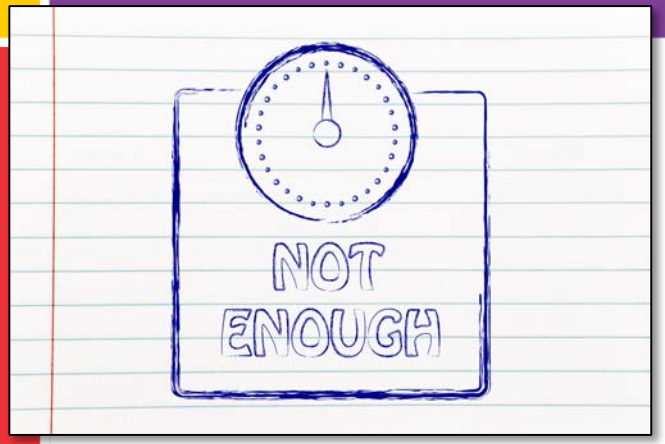


Network Defender Semantic Tree: 2d Limb

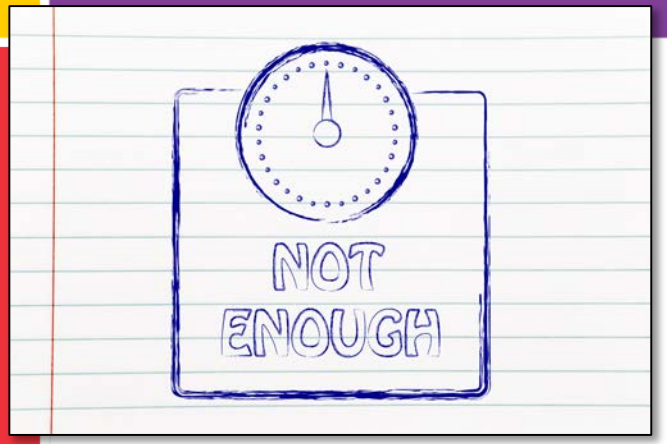


paloalto NETWORKS

Network Defender Semantic Tree: 2d Limb



Network Defender Semantic Tree: 2d Limb



paloalto NETWORKS

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

paloalto NETWORKS

Network Defender Semantic Tree: 2d Limb

paloalto NETWORKS

Network Defender Semantic Tree: 2d Limb

#1

Network Defender Semantic Tree: 2d Limb

#2

paloalto NETWORKS

Network Defender Semantic Tree: 2d Limb

#2

paloalto NETWORKS

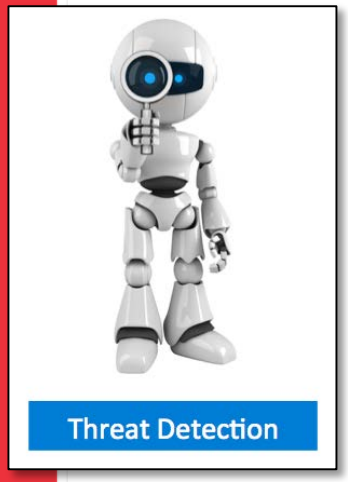
Network Defender Semantic Tree: 2d Limb

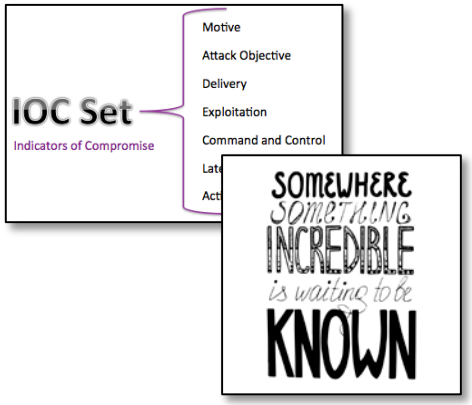
Threat Detection

Network Defender Semantic Tree: 2d Limb

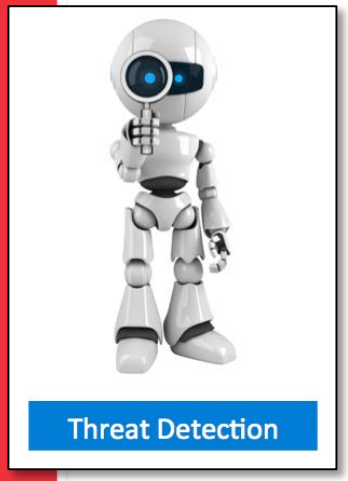
Threat Detection

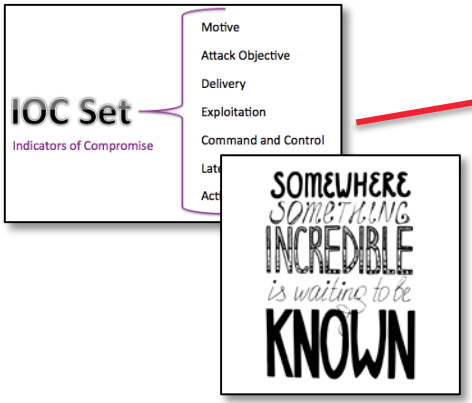
Network Defender Semantic Tree: 2d Limb

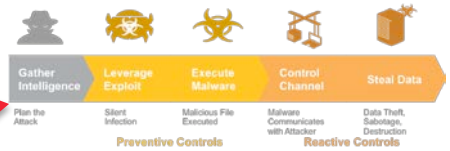




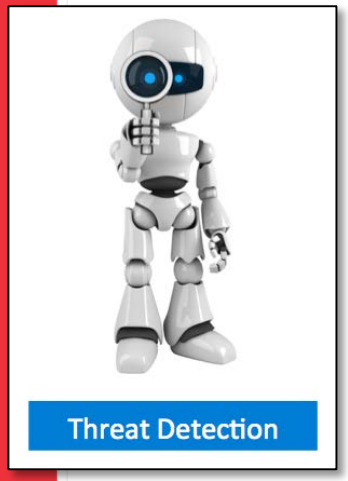
Network Defender Semantic Tree: 2d Limb

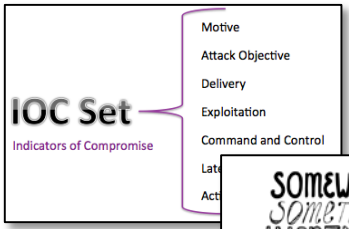


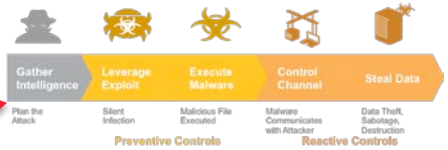




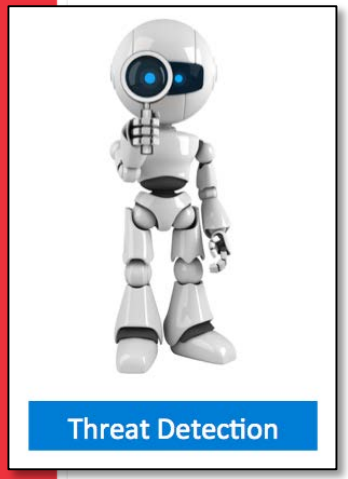
Network Defender Semantic Tree: 2d Limb

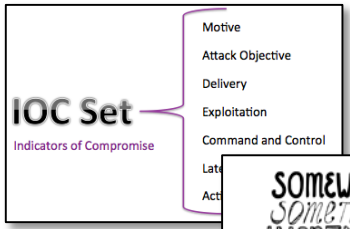


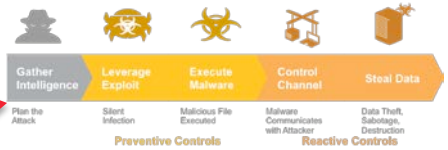




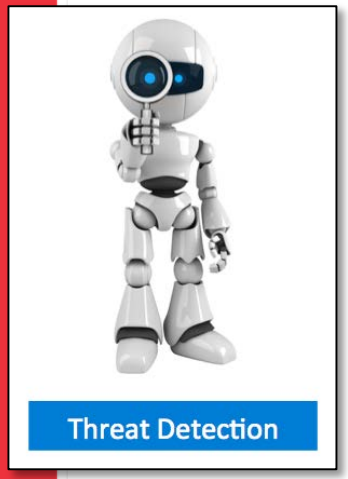
Network Defender Semantic Tree: 2d Limb

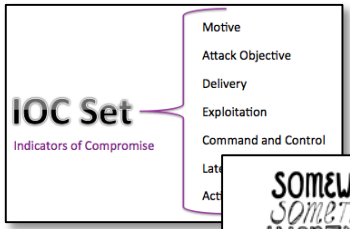


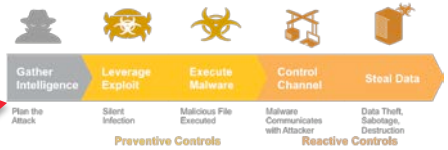


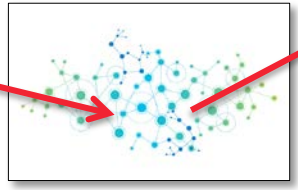


Network Defender Semantic Tree: 2d Limb

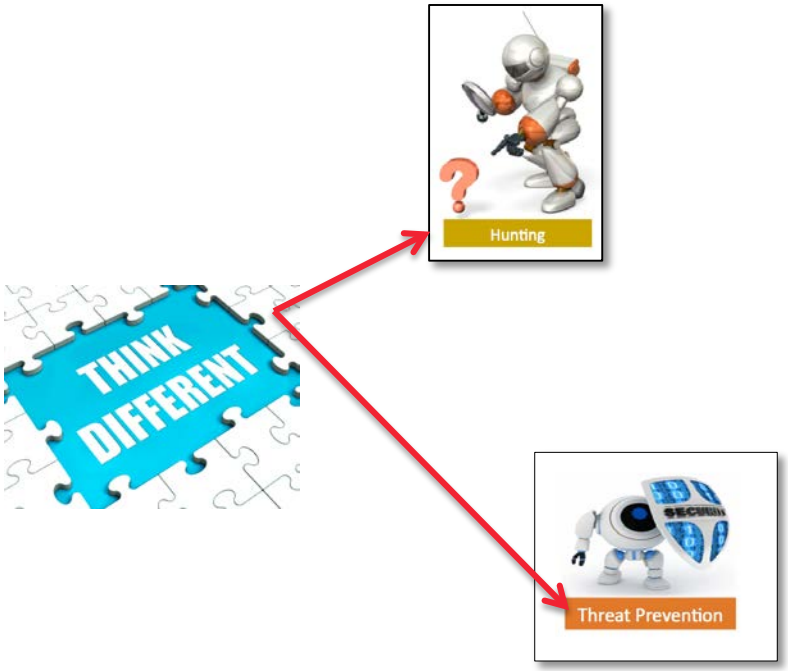




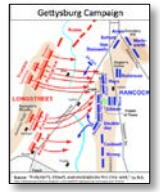


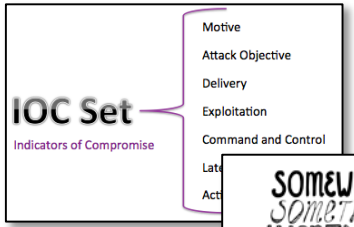


Network Defender Semantic Tree: 2d Limb



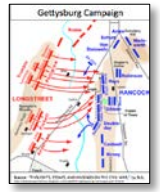
Network Defender Semantic Tree: 2d Limb

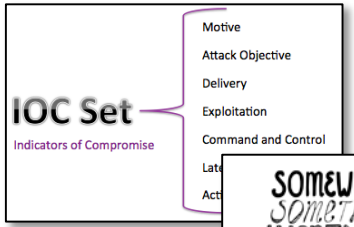




paloalto NETWORKS

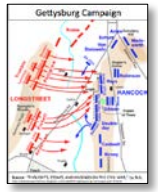
Network Defender Semantic Tree: 2d Limb

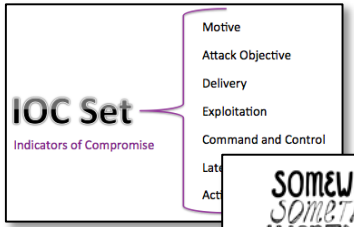




paloalto NETWORKS

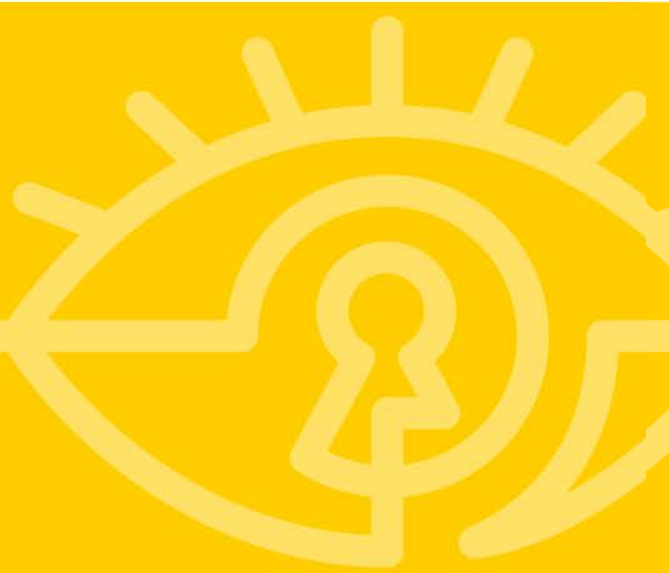
Network Defender Semantic Tree: 2d Limb





Network Defender Semantic Tree: 2d Limb

Establish a Robust Threat Detection Program



Third Limb

Network Defender Semantic Tree: 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

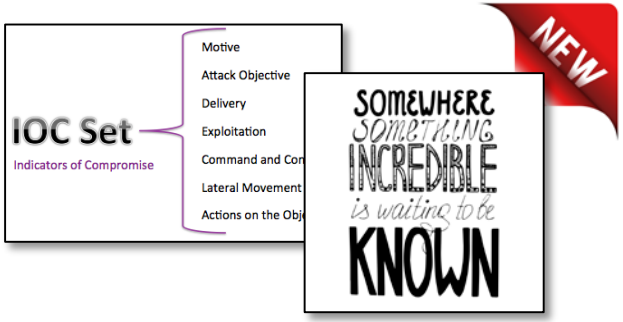
Network Defender Semantic Tree: 3rd Limb

#RSAC

#1

Network Defender Semantic Tree: 3rd Limb

#1



Network Defender Semantic Tree: 3rd Limb

#2

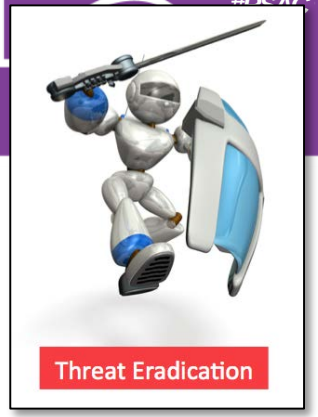
Network Defender Semantic Tree: 3rd Limb

#RSAC

#2

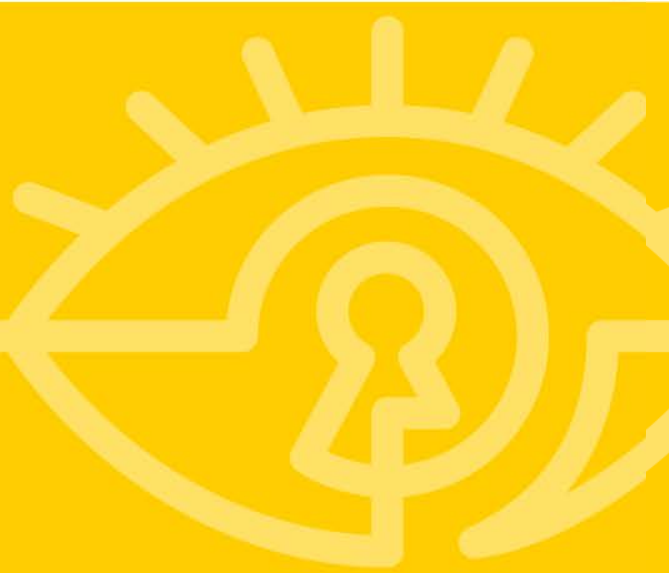
paloalto NETWORKS

Network Defender Semantic Tree: 3rd Limb



3rd Limb

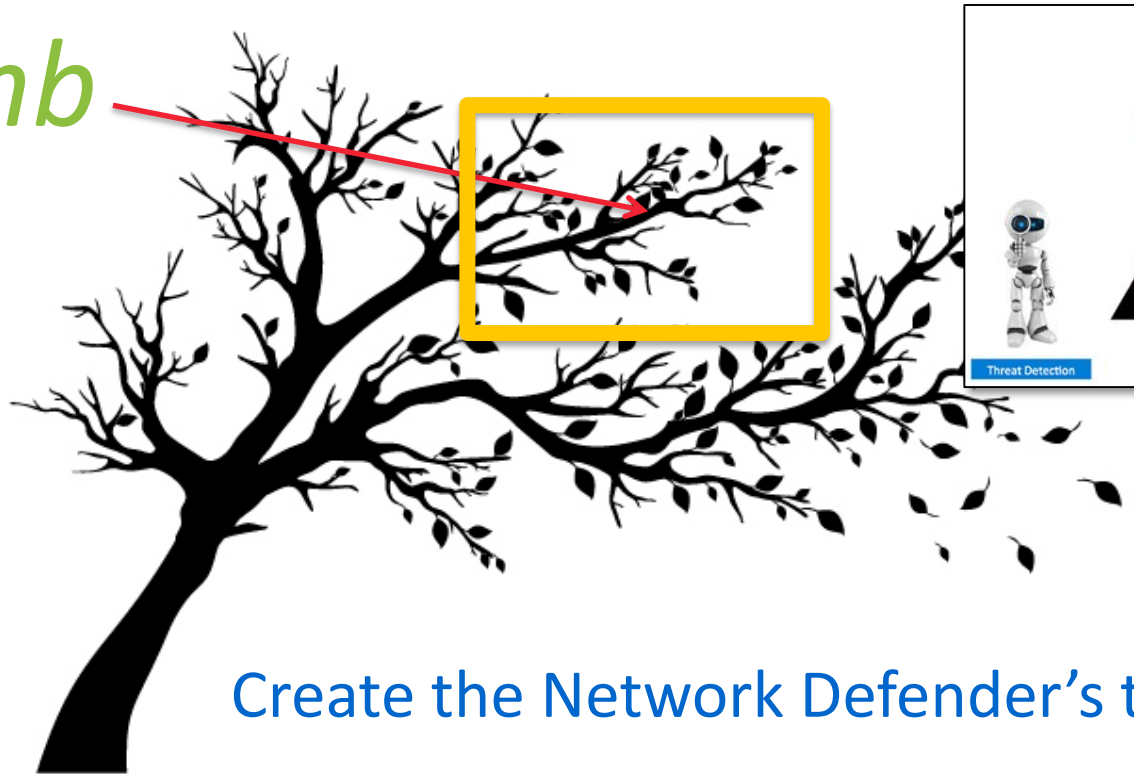
Establish a Robust Threat Eradication Program



Fourth Limb

Network Defender Semantic Tree: 4th Limb

4th Limb



Create the Network Defender's trinity.

Network Defender Semantic Tree: 4th Limb

Essential

Essential

Essential

Network Defender Semantic Tree: 4th Limb

E
Essential

E
Essential

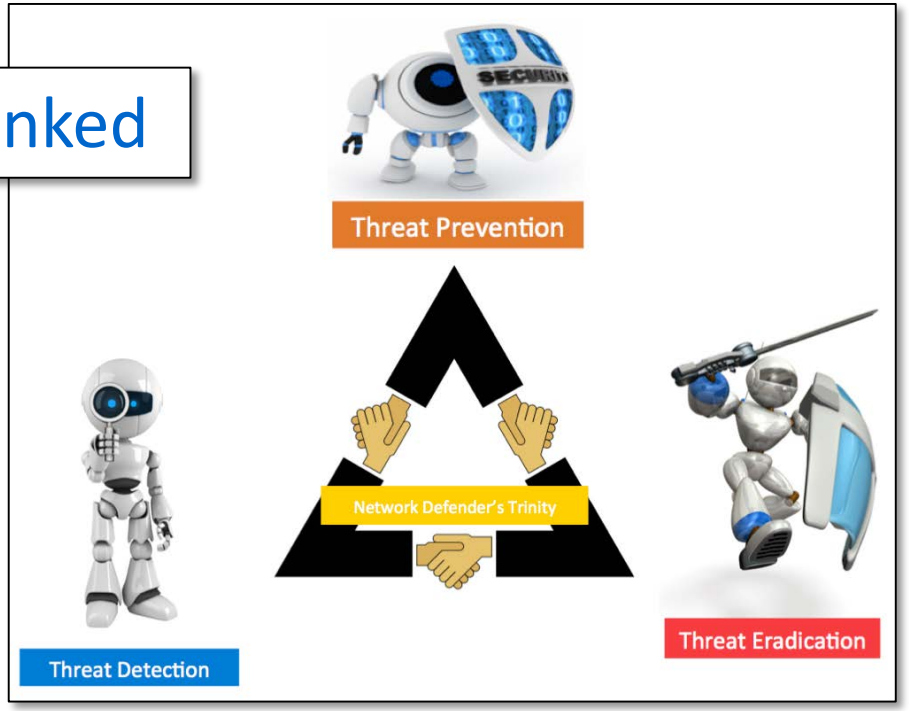
E
Essential

paloalto NETWORKS

RSAConference2016

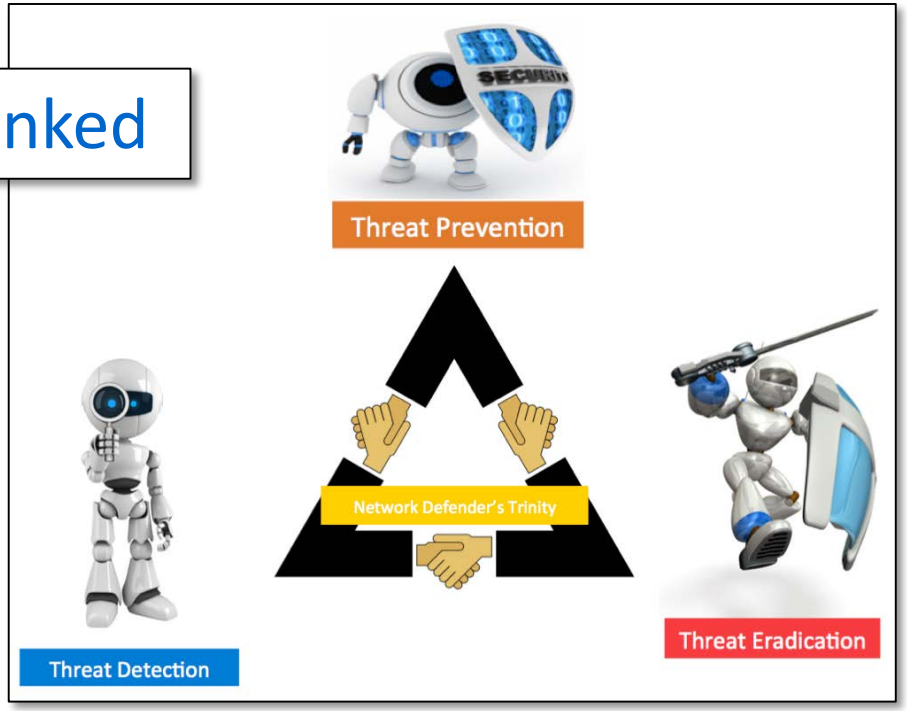
Network Defender Semantic Tree: 4th Limb

Inextricably linked



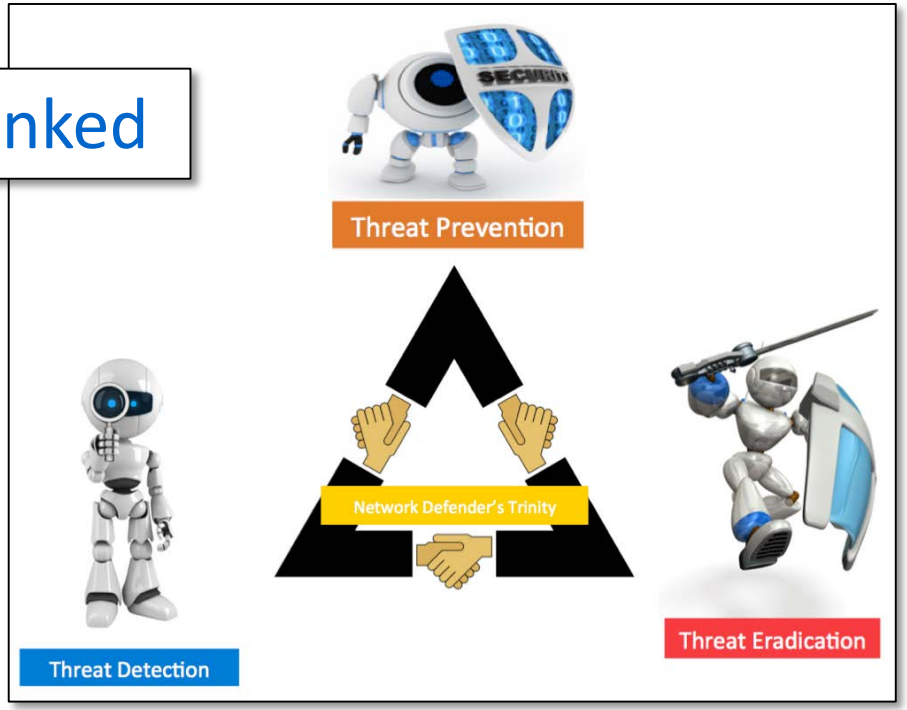
Network Defender Semantic Tree: 4th Limb

Inextricably linked



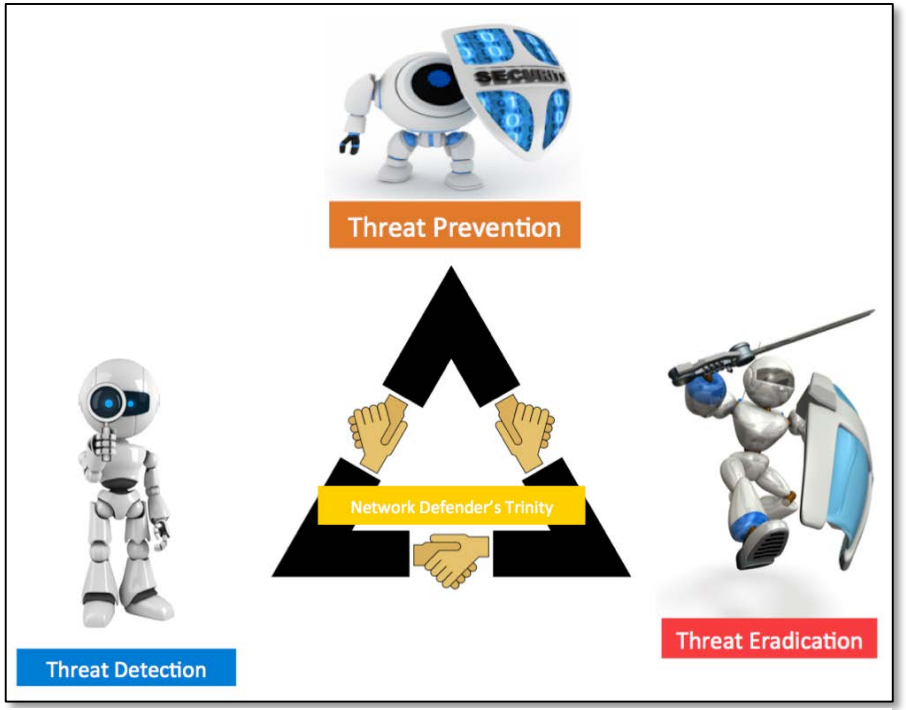
Network Defender Semantic Tree: 4th Limb

Inextricably linked



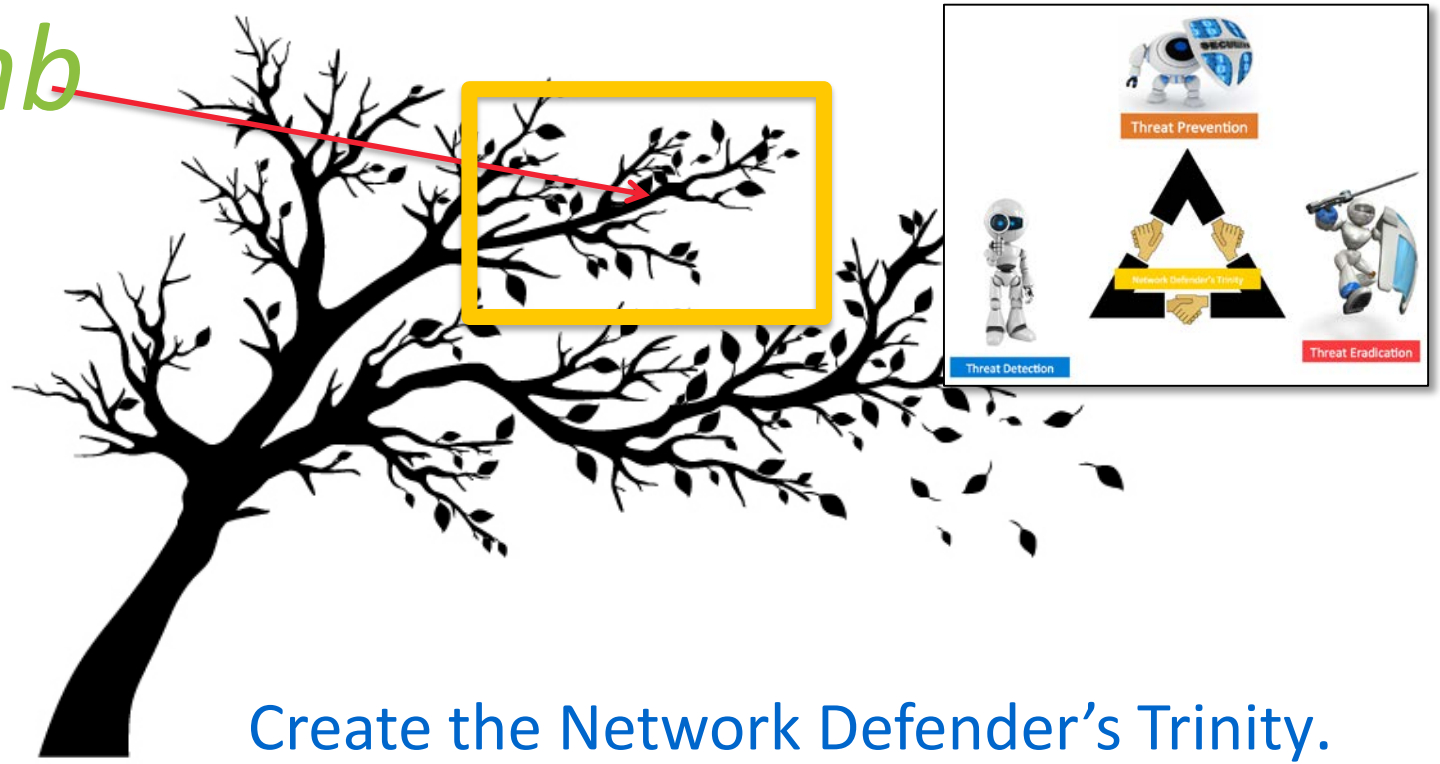
irreducible complexity

Network Defender Semantic Tree: 4th Limb

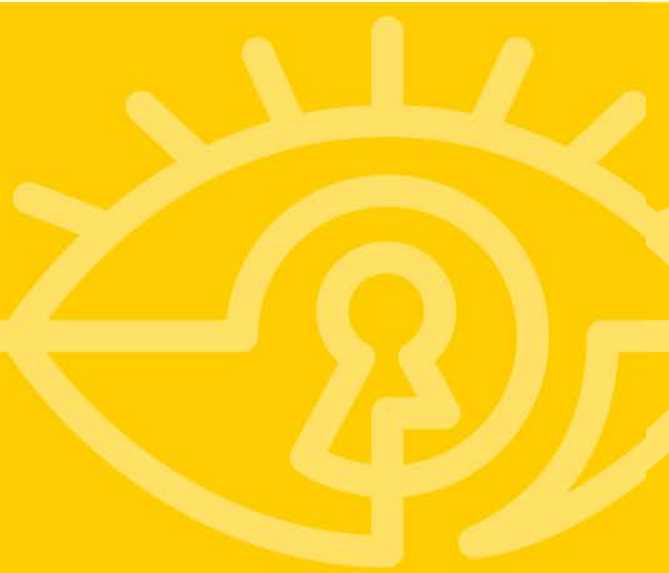


Trinity

Network Defender Semantic Tree: 4th Limb

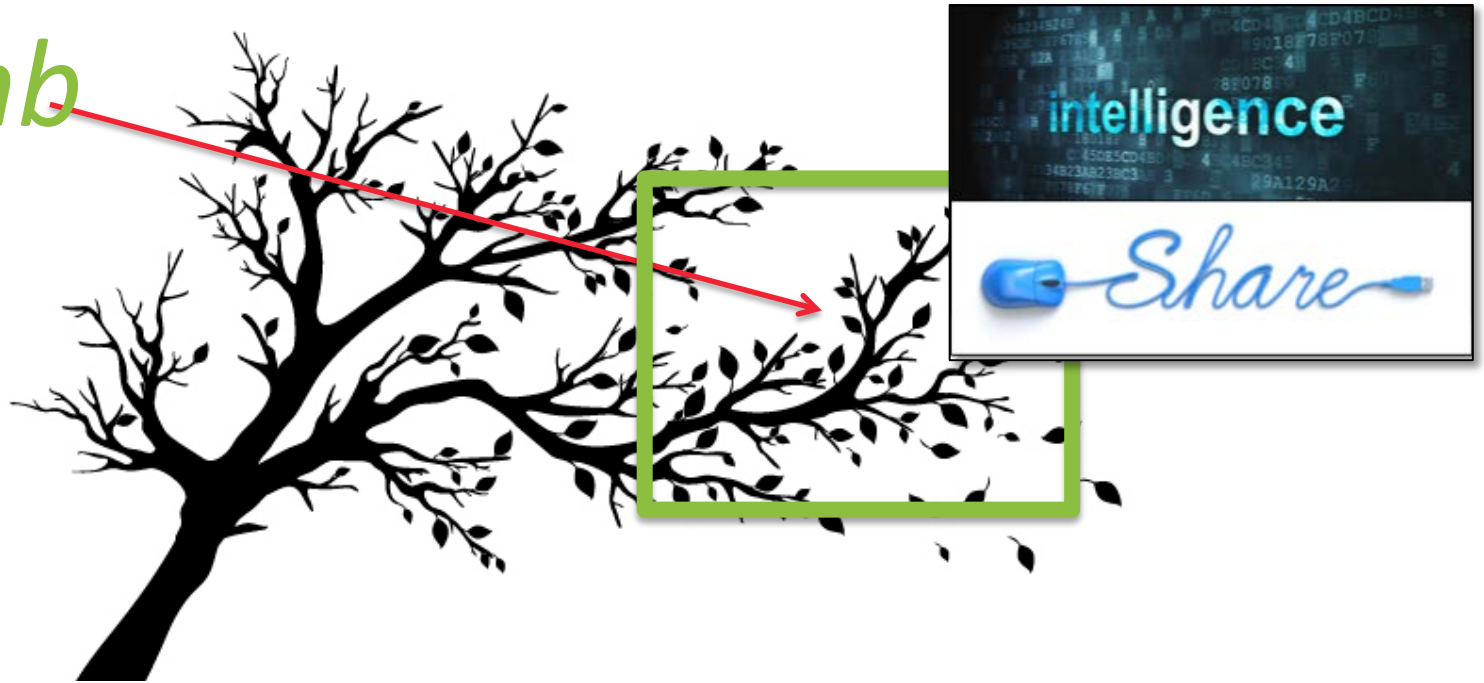


Create the Network Defender's Trinity.



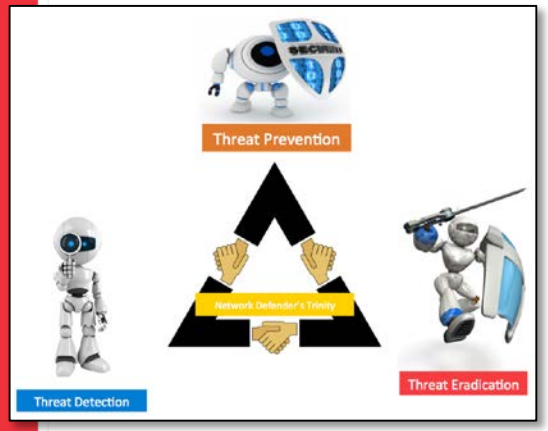
Last Limb

Network Defender Semantic Tree: 5th Limb

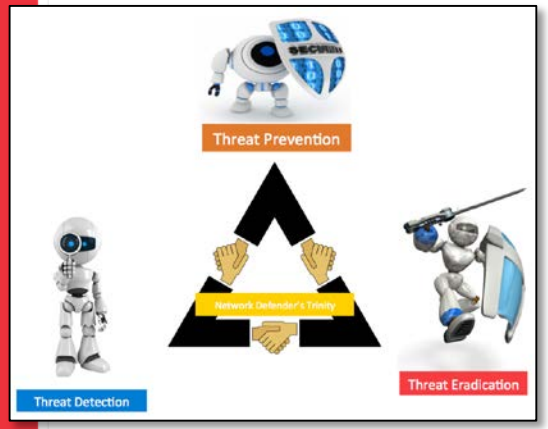


Embrace cybersecurity intelligence collection and ubiquitous sharing

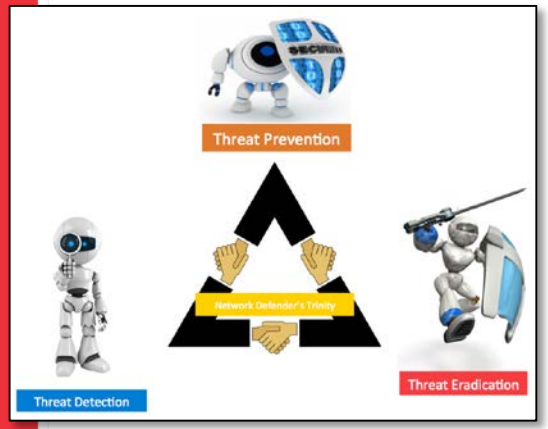
Network Defender Semantic Tree: 5th Limb

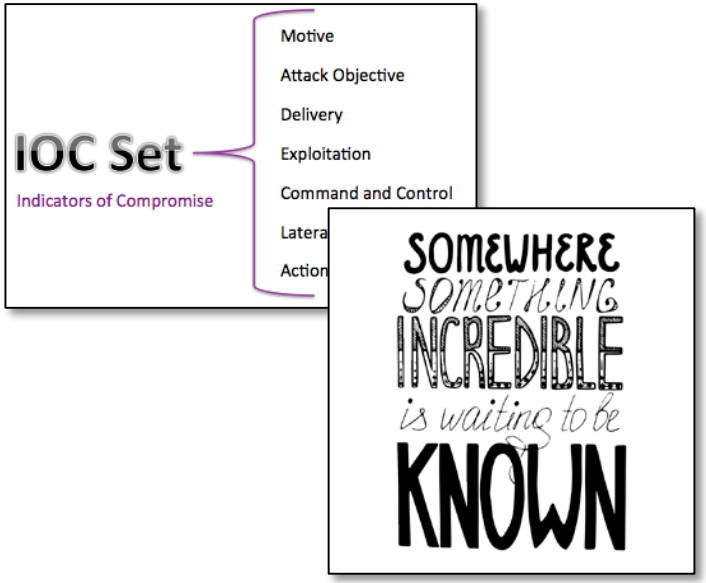


Network Defender Semantic Tree: 5th Limb



Network Defender Semantic Tree: 5th Limb





Collected

Sorted

Evaluated

Prioritized

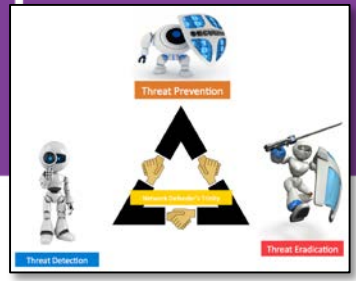
Network Defender Semantic Tree: 5th Limb

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.

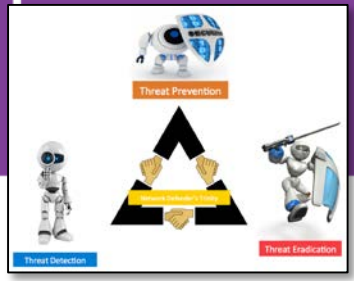
Network Defender Semantic Tree: 5th Limb

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.

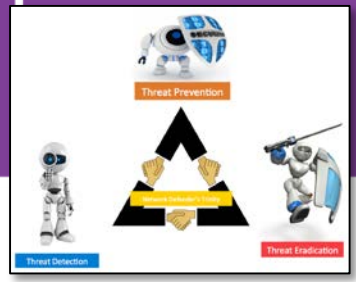
Network Defender Semantic Tree: 5th Limb

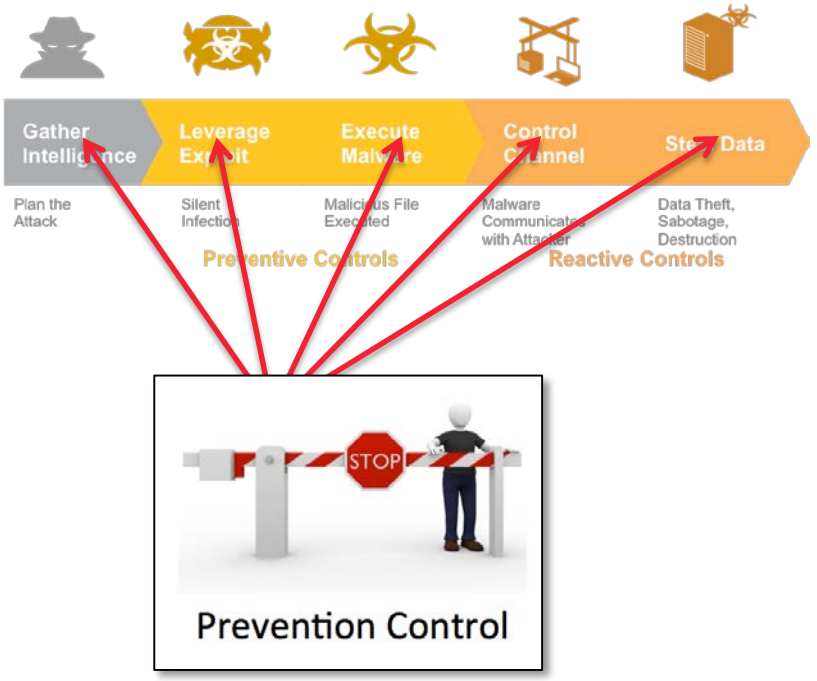


Network Defender Semantic Tree: 5th Limb

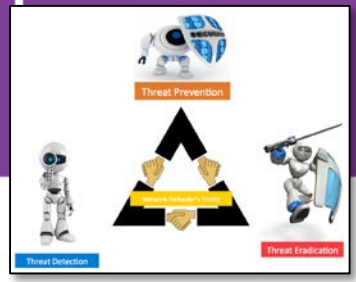


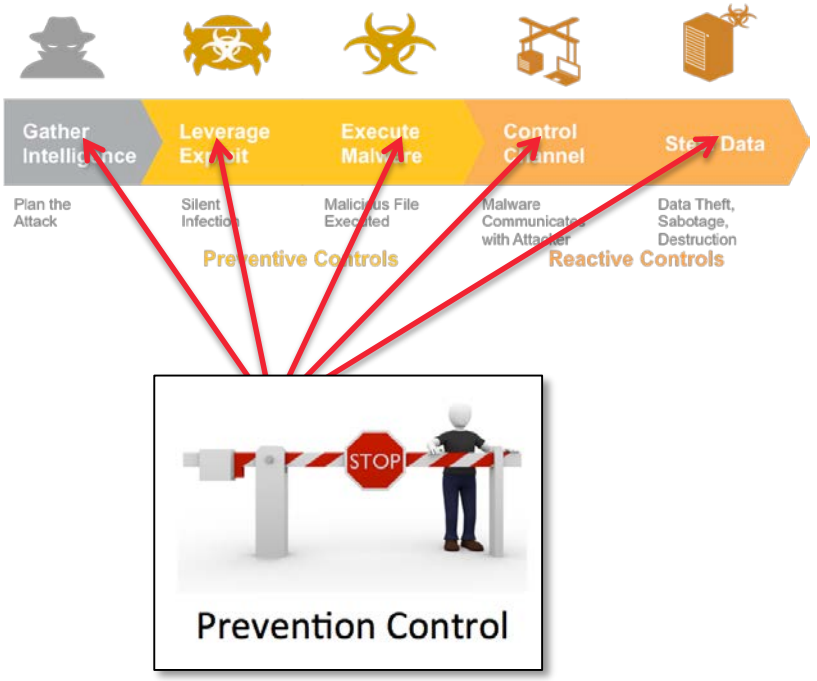
Network Defender Semantic Tree: 5th Limb





Network Defender Semantic Tree: 5th Limb



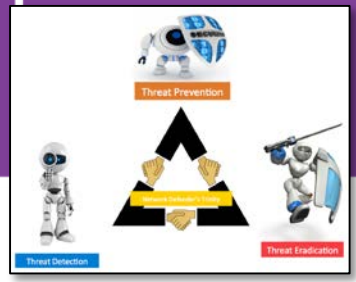


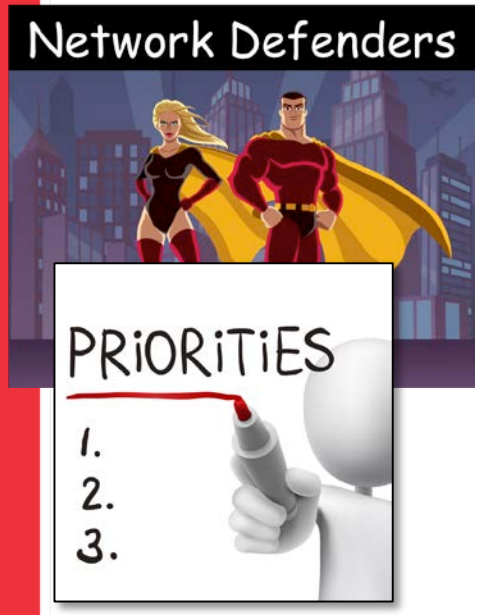
Maximize

paloalto NETWORKS

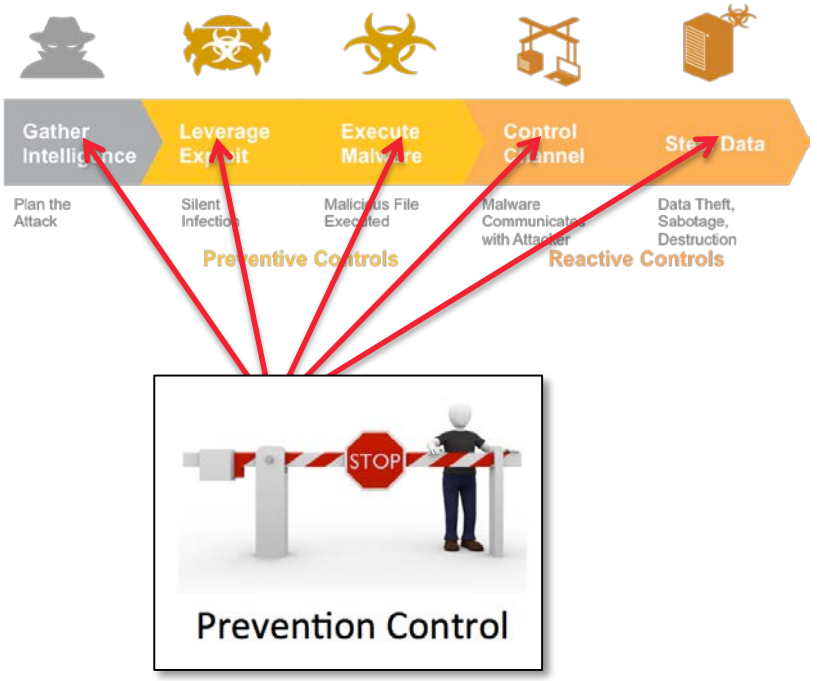
RSAConference2016

Network Defender Semantic Tree: 5th Limb





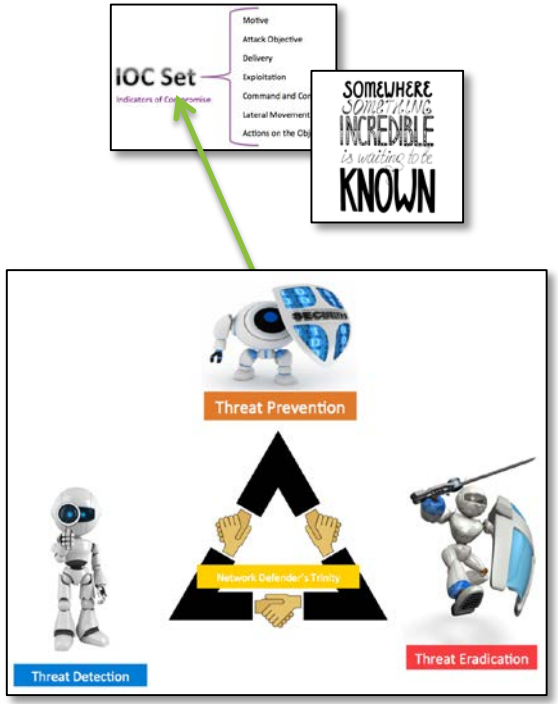
Maximize



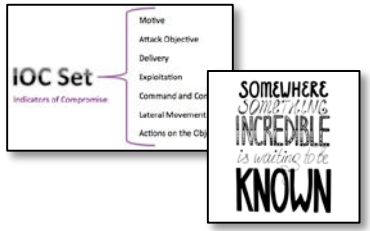
paloalto NETWORKS

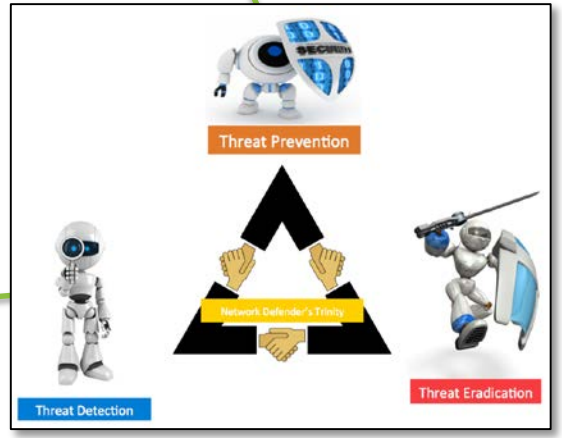
RSAConference2016

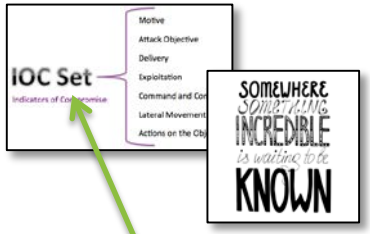
Network Defender Semantic Tree: 5th Limb



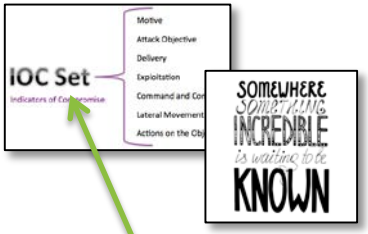
Network Defender Semantic Tree: 5th Limb

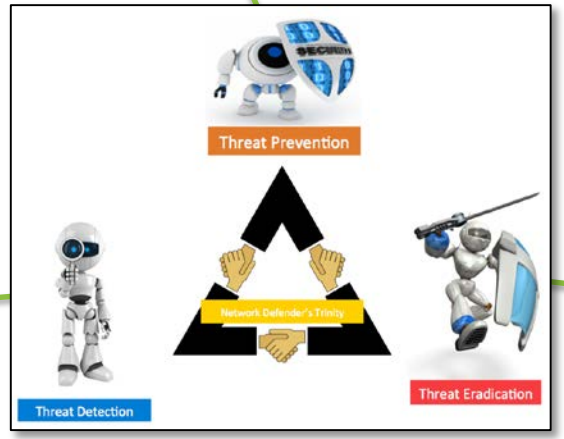


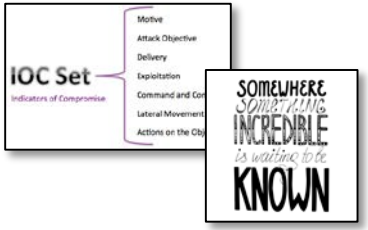




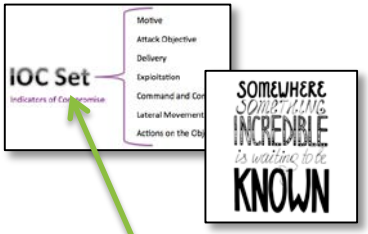
Network Defender Semantic Tree: 5th Limb

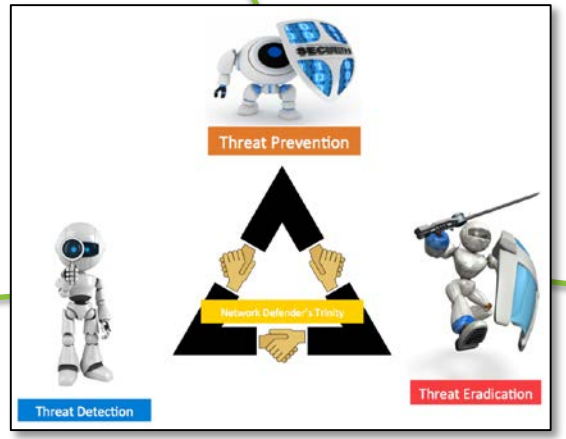


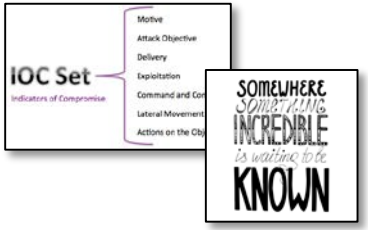




Network Defender Semantic Tree: 5th Limb





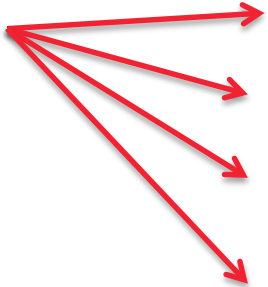


Network Defender Semantic Tree: 5th Limb

paloalto NETWORKS

Network Defender Semantic Tree: 5th Limb

Network Defender Semantic Tree: 5th Limb



Network Defender Semantic Tree: 5th Limb

Benefits

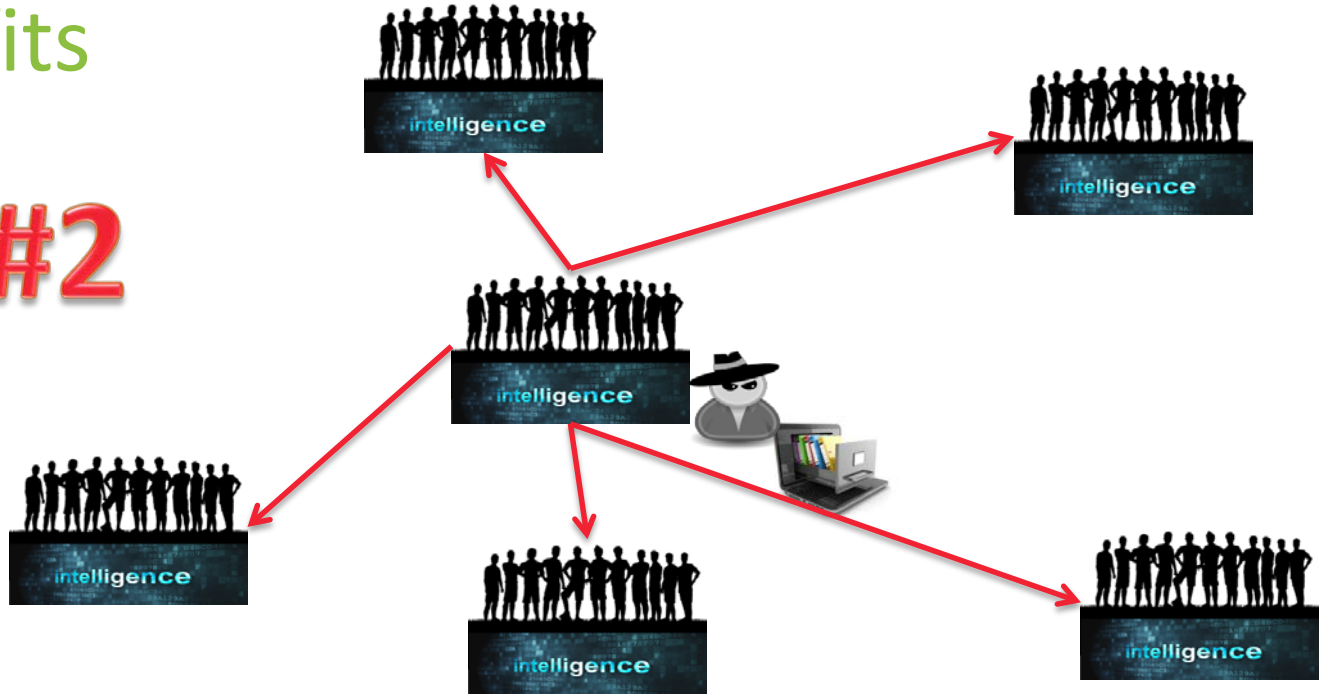
#1

All

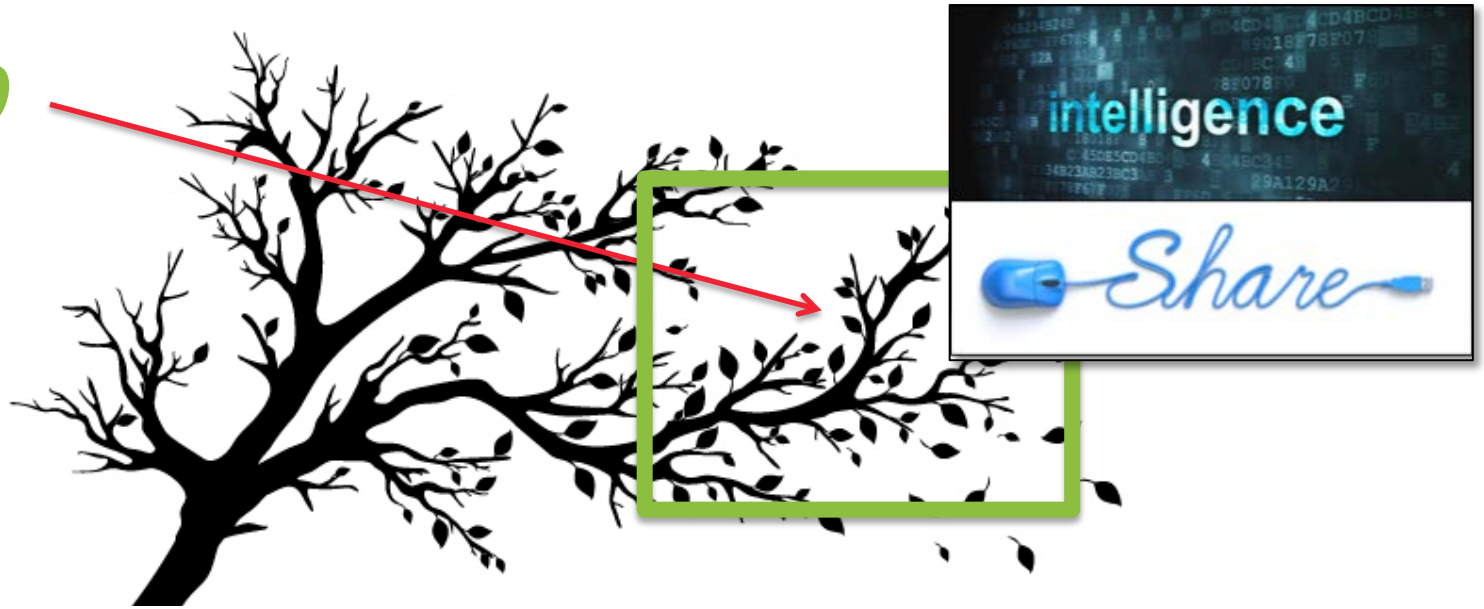
Network Defender Semantic Tree: 5th Limb

Benefits

#2



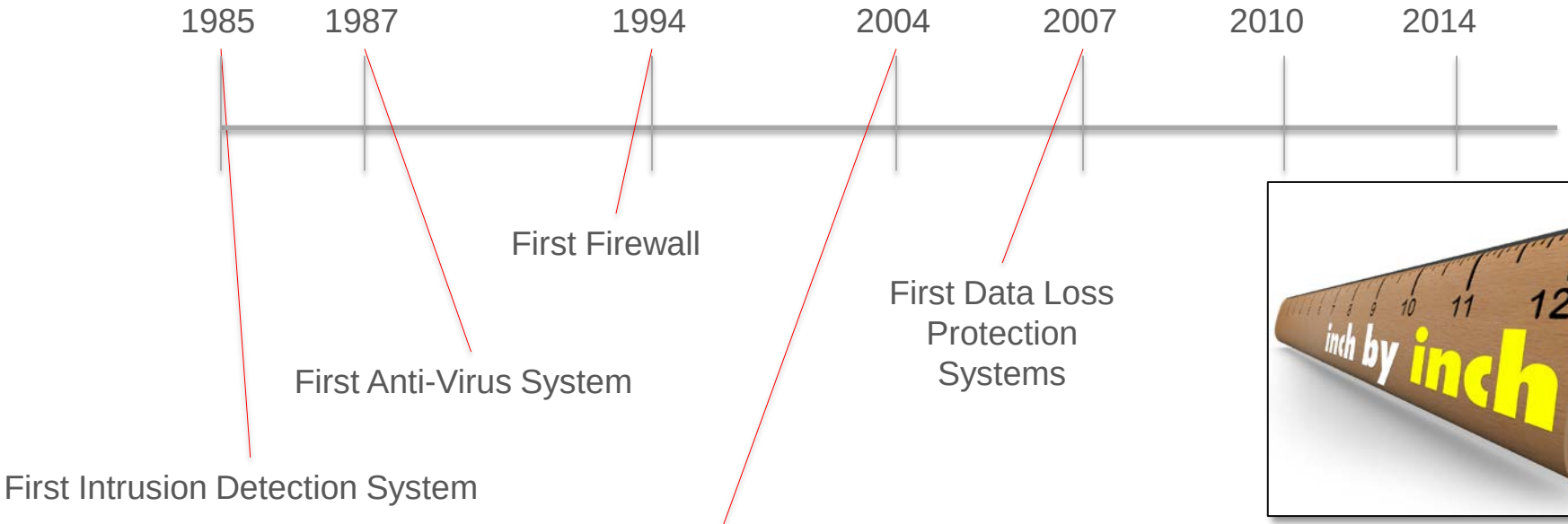
Network Defender Semantic Tree: 5th Limb



Embrace cybersecurity intelligence collection and ubiquitous sharing

Conclusion

25 Years of Incremental Improvement

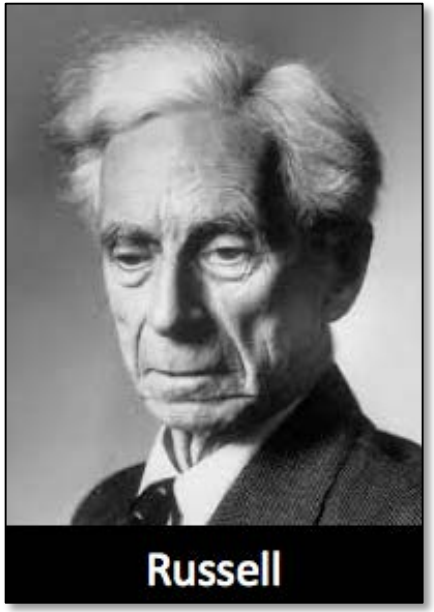


Rethink the Network Defender Problem Space

Leap Ahead

Boiled Water

Rethink the Network Defender Problem Space



Elon Musk

Fundamental

Self Evident

Experts Agree

Atomic

First Principles

Semantic Tree

Limbs

Trunk

Network Defender First Principles

Prevent High Risk Material Impact

paloalto NETWORKS

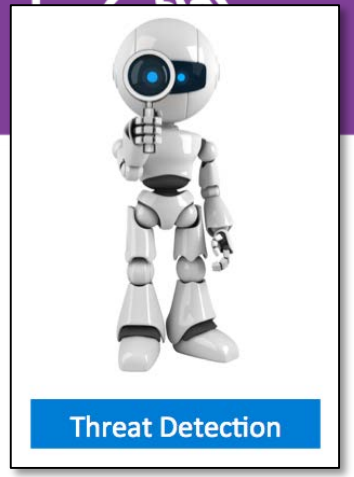
RSAConference2016

Network Defender First Principles

1st Limb

Establish a Robust Threat Prevention program

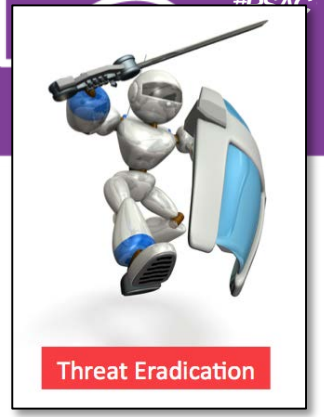
Network Defender First Principles



2nd Limb

Establish a Robust Threat Detection Program

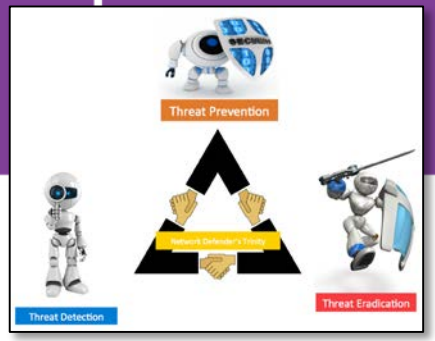
Network Defender First Principles



3rd Limb

Establish a Robust Threat Eradication Program

Network Defender First Principles



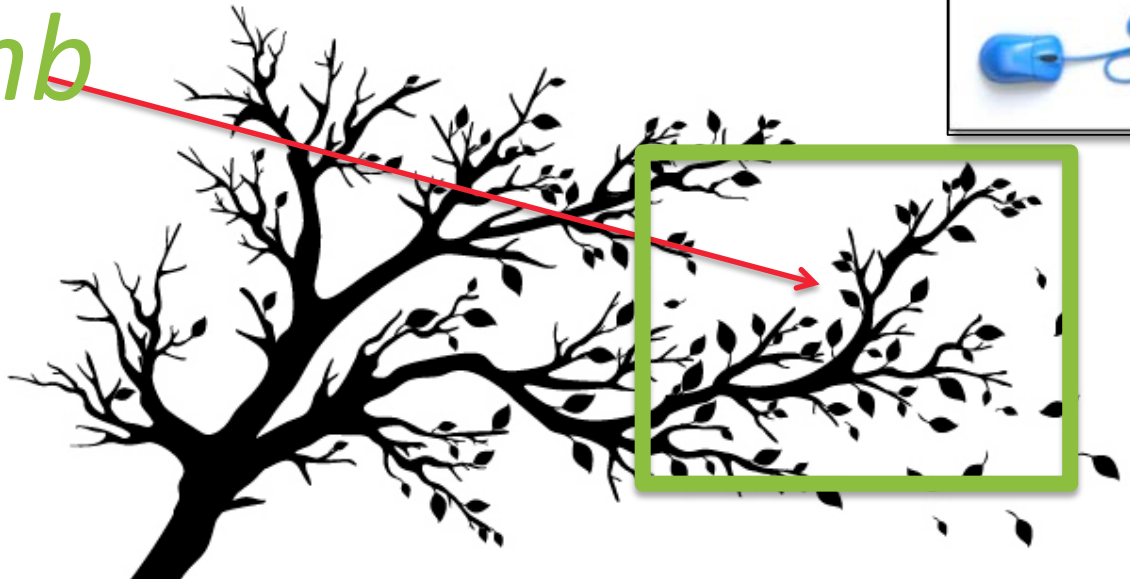
4th Limb

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

paloalto NETWORKS

Network Defender First Principles

5th Limb



Embrace cybersecurity intelligence collection and ubiquitous sharing

paloalto NETWORKS

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

CYBER THREAT ALLIANCE

http://cyberthreatalliance.org/

unit42

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

THE CYBERSECURITY CANON BOOKS EVERY CYBERSECURITY PROFESSIONAL SHOULD READ

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

paloalto NETWORKS

RSAC Studio

Connect to Protect

Guiding Principles to Defending Organizations

Rick Howard
CSO – Palo Alto Networks
@raceBannon99

#RSAC

RSAC Studio

Connect to Protect

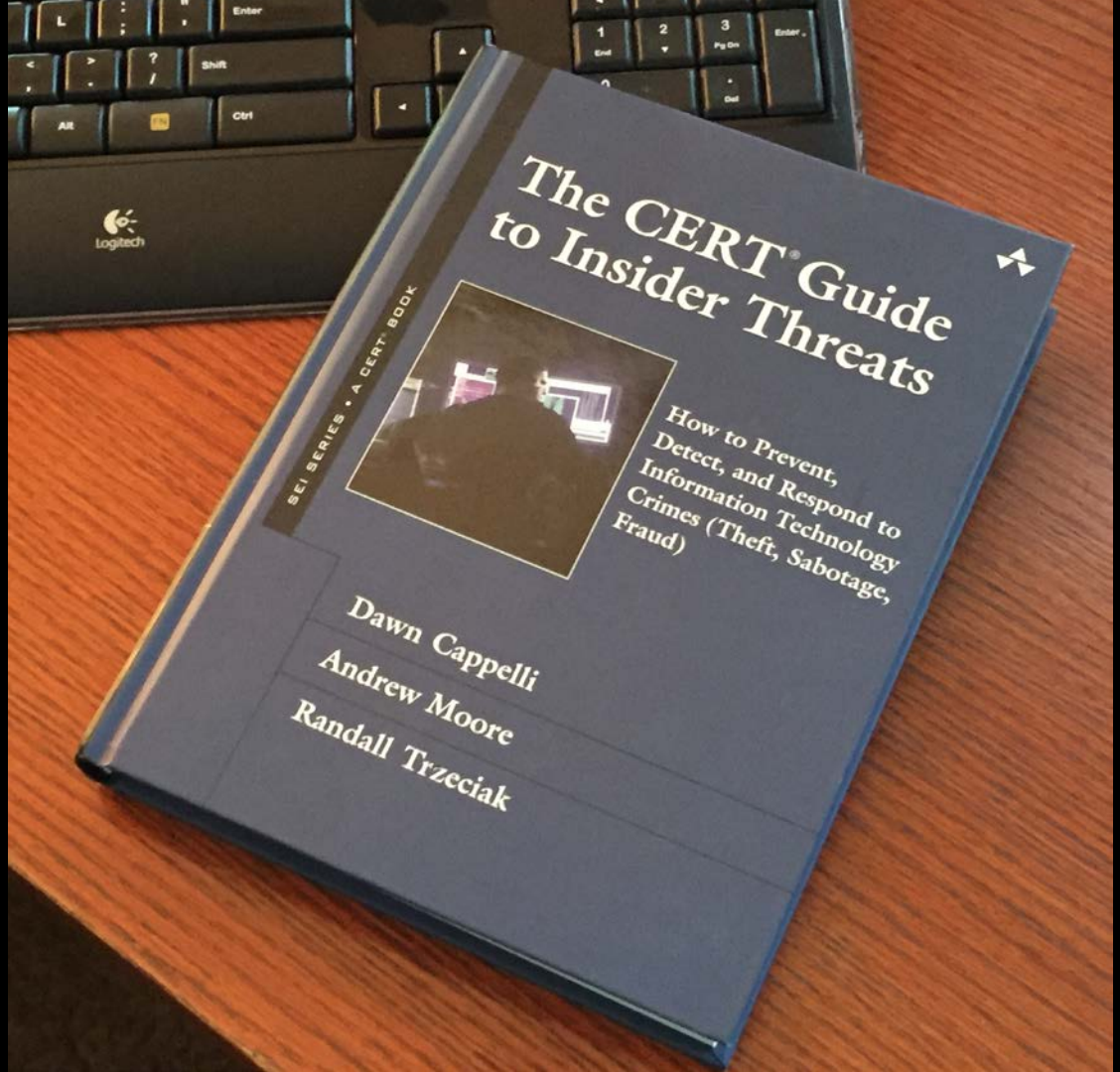
Predictive Techniques to Catch Insider Threats Before they Become Criminals

Dawn M. Cappelli
Vice President, Information Risk Management
Rockwell Automation
@DawnCappelli

#RSAC

Why I'm Here

Why I'm Here


The CERT® Guide to Insider Threats
How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)
SEI SERIES • A CERT BOOK
Dawn Cappelli
Andrew Moore
Randall Trzeciak
Logitech

Actual Insider Cyber Attacks

SCADA

MEDICAL

TELECOMMUNICATIONS

Rockwell Automation Industries


Automotive


Beverage


Entertainment


Fibers & Textiles


Food


Household & Personal Care

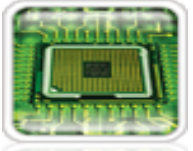

Infrastructure


Life Sciences


Marine


Metals


Oil & Gas


Semiconductor & Electronics


Power Generation


Print & Publishing


Pulp & Paper


Mining, Minerals & Cement


Tire & Rubber


Water Wastewater

Insider Cyber Sabotage Risk Management

No Longer Uncharted Territory!

JANUARY 2016

City on alert amid terror arrests

IS THREAT Dozen suspects held for planning R-Day attacks across country

HT Correspondents
letters@hindustantimes.com

NEW DELHI: Authorities issued an alert in Delhi on Friday after the driver of a taxi allegedly hijacked near the scene of a recent terror attack on Punjab's Pathankot airbase was found murdered, sparking security concerns amid a nationwide crackdown by the NIA on alleged Islamic State militants.

Delhi Police released photos of suspects and vehicle details through their Twitter handle saying the Maruti Alto was hired by three unidentified men on January 20. The driver, Vijay Kumar, was later found dead in Himachal Pradesh's Kangra district, officials said.

The alert came amid heightened security across the nation ahead of Republic Day celebrations to be attended in Delhi by French President Francois Hollande as chief guest, months after his country was hit by a series of coordinated terror attacks claimed by the IS.

The National Investigation Agency arrested or detained over a dozen people, including the self-appointed India head of IS, during raids in Karnataka, UP, Andhra Pradesh and Maharashtra that sources said blew the lid off a sweeping network of the terror group with plans to carry out blasts here.

CONTINUED ON PAGE 6

HT SPECIAL P13

ARE WE READY FOR ANOTHER PATHANKOT?

The men and machines at the heart of the anti-terror mechanism clearly need urgent training and upgrade if security forces have to gain an upper hand over terrorists who strike at will

Army troops stand guard outside Rashtrapati Bhavan after Republic Day rehearsals on Friday. » P4,5 VIRENDRA SINGH GOSAIN / HT

more stories

Salwinder Singh comes out clean in lie-detector test

The Punjab police officer, who was allegedly abducted by the Pathankot attackers, aced the polygraph test, home ministry sources said. Raids on his residences also did not turn up anything suspicious » P11

Shahnawaz gets 'threat' letter

A letter, claiming to be from Islamic State, questioned BJP leader's association with the party and labelled him infidel » P11

KVs shut, security beefed up in univs

HT Correspondents
letters@hindustantimes.com

NEW DELHI: Kendriya Vidyalayas in air force stations in and around the Capital will remain closed till January 27 due to security concerns that also saw DU and JNU up their guard.

The schools remained closed on Friday after a notice said the step was being taken due to threat perception. The decision, said sources, came after Border Security Force and Indian Air Force officials met the schools principals.

Delhi University and Jawaharlal Nehru University too, have tightened security, with advisories asking for guards to be posted at all entry gates and not allow in unauthorised persons. Vehicles entering the sprawling campuses are also being checked. »

The alleged chief, or Ameer, 34-year-old Munabeer Mushtaq from Mumbai, is a software engineer

Sheikh, a trained web designer from Thane Polytechnic, was radicalised over the internet in the past two years

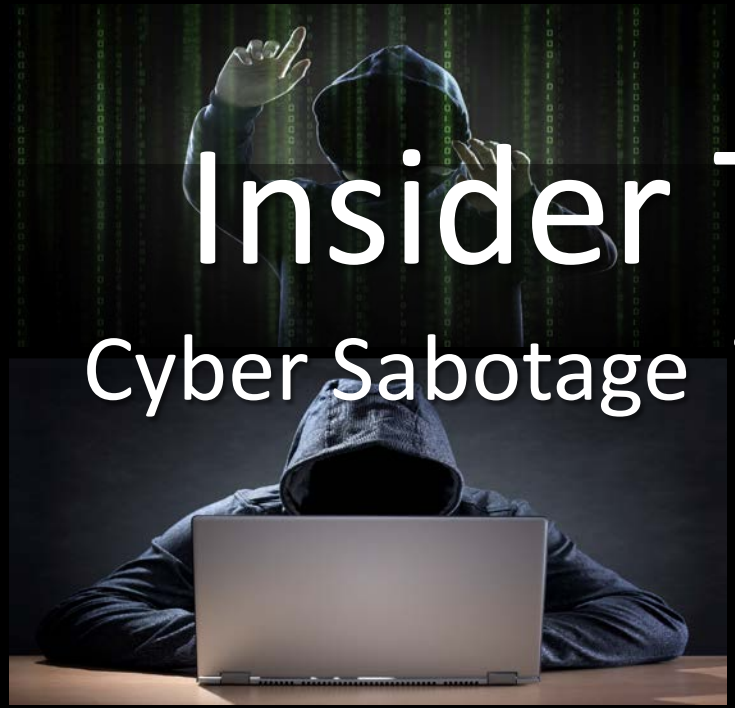
Prediction is Critical!

What is Prediction?

to foretell with precision of calculation, knowledge, or shrewd inference from facts or experience

-- dictionary.com

Two Methods of Prediction

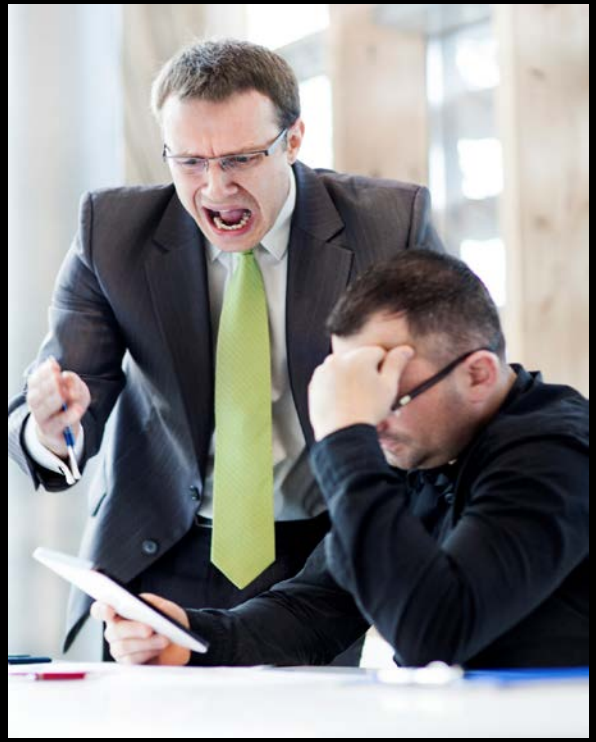


Insider Threats

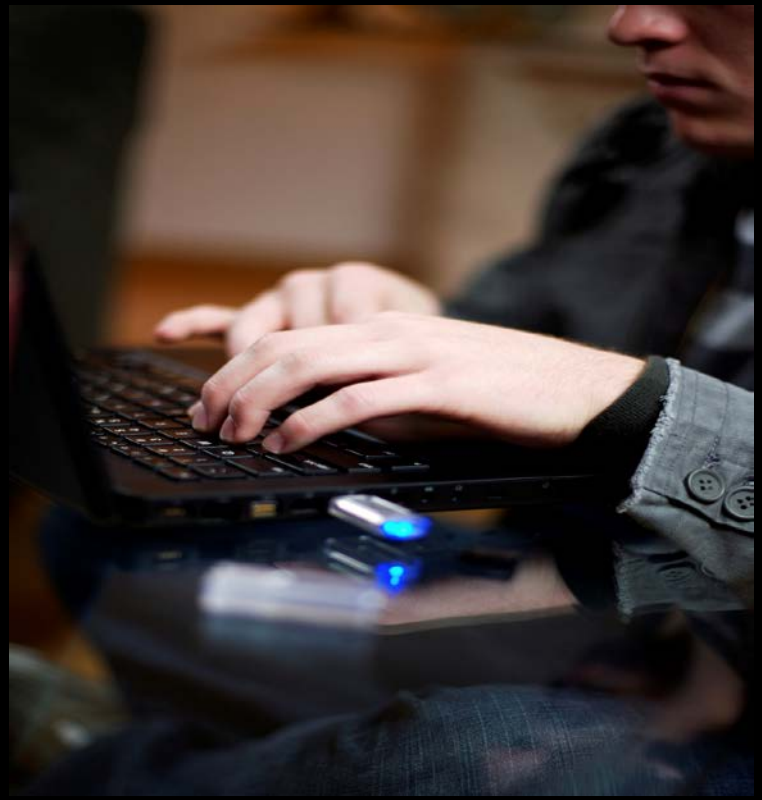
Cyber Sabotage Theft of Information

Prediction: Insider Cyber Sabotage

Key to Prediction



Prediction: Insider Theft of Information



Key to Prediction

Key to Scalability: Automation

Success is Critical!

Please direct comments and questions to:

Dawn Cappelli
Vice President, Information Risk Management
Rockwell Automation

+1 414-323-0404
dmcappelli@ra.rockwell.com

Rockwell Automation

RSAC Studio

Connect to Protect

Predictive Techniques to Catch Insider Threats Before they Become Criminals

Dawn M. Cappelli
Vice President, Information Risk Management
Rockwell Automation
@DawnCappelli

#RSAC