

the official

Training Guide for



New Superheroes



by Pete Herzog

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Why We Need Superheros



Some People Are Born to Be Victims

- It starts as children when they get conflicting messages.
 - Don't talk to strangers. Talk to Policeman, Fireman, and Teachers because they are there to help you.
 - Don't take candy from strangers but hey, Happy Halloween - Trick or Treat! Visit strangers at home and take candy!
- We are inundated by false and misleading advertising.
 - 97% fat free yogurt! (Whole milk is 3% fat)
 - Exercise makes you gain weight! (Muscle weighs more than fat)
- Authorities and experts give wishy-washy qualifiers for advice.
 - Well, since there's no such thing as perfect security so there's no guarantee you won't get attacked. (Covers their butts)
 - If an attacker wants in they'll get in. (There are physical limitations)
 - Something is better than nothing. (Not if something causes problems)

It's Up To You to Fix Things

- Realize now that what you have been taught about security may be wrong or at least inaccurate.
- Bad security builds the enemy's army.
- Incompetence and indifference make victims of the innocent and threats to the public.
- Security is NOT about being bigger, stronger, smarter, or faster than the evil-doers.
- Security is about HOW you interact with good and evil and doing THAT right makes you a Superhero.

But You Might Still Be on the Kent Farm



- Because you learn by getting the basic understanding first.
 - And you get the basic products like firewalls and antivirus.
- Because you watch the news for the latest threats.
 - Or read about them in magazines and mailing lists.

Is This Your Typical Farm Work?



- You mimic what others do to get by.
 - Search the web for How-Tos and Best Practices
- You do what you are told you have to do to protect yourself and those who cannot protect themselves.
 - Policy.
 - Training and Configuration.
 - Compliance.

But Will It Work in Metropolis?

No. It won't.



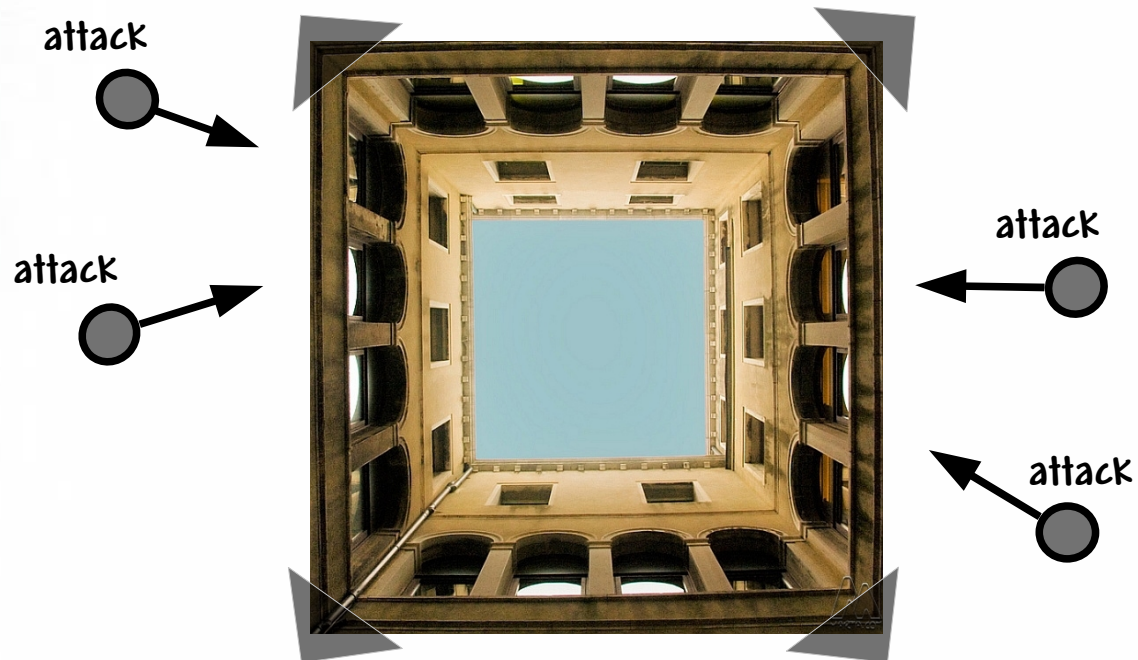
What Doesn't Work in Metropolis?

- Best practices are best for whom? Where did they come from?
- Mostly "best practice" is one person's experience in a unique environment and then copied by the lazy. Much research is then further expanded on this original knowledge as if it were fact. This creates a chain of lies that seem true and authoritative.
- Compliance is just the requirement to help those who can't help themselves and most of the time it's a lowered ceiling and not a raised bar.
- Know that compliance may not get you security but security will certainly get you compliance.
- Can "security" even be attained? If not, why do so many sell what cannot be delivered? Doesn't that sound scammy to you?!

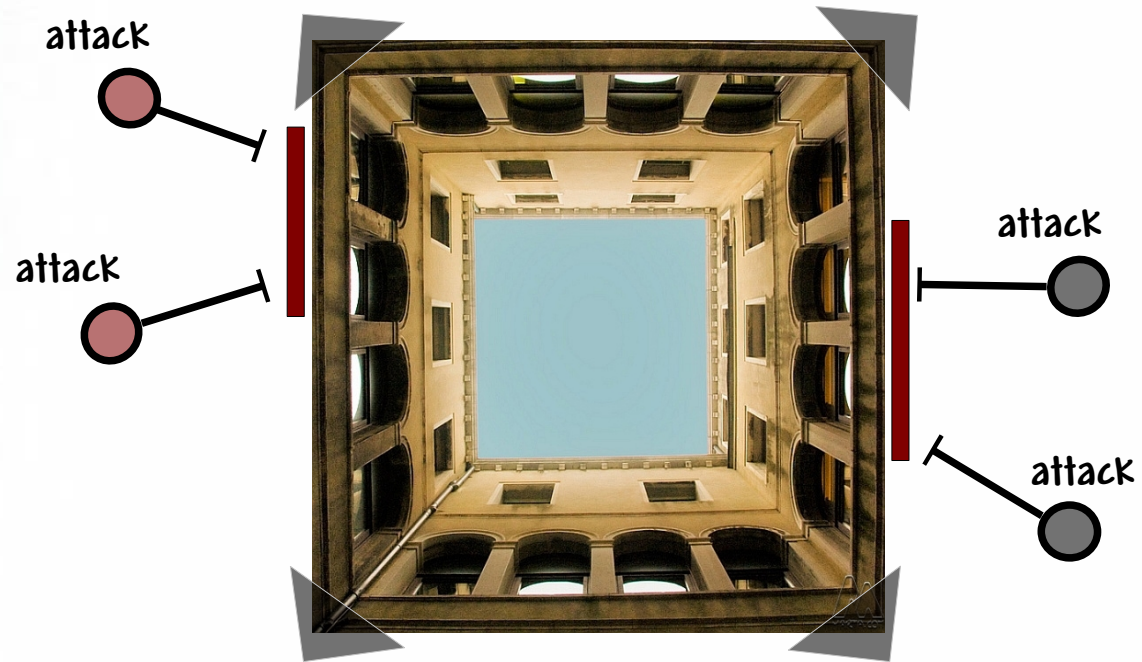
Preparing for Metropolis

- Know your Attack Surface; exactly how much security, controls, and limitations you have by vector and channel.
- Know your Defense in Width; how your defenses interlock spanning Channels and what they are capable of regardless of the threat.
- Know how to trust without your gut; analyzing trust rationally and logically.

What is the Attack Surface?



Changing the Attack Surface



Risk and the Attack Surface 1



Risk and the Attack Surface 2



Risk and the Attack Surface 3



Operational Security is Prevention

- OpSec is defined as the separation of an asset and a threat.
 - (Assets is a cold, inhuman, and self-important term the heroes-for-hire use to refer to people or things and information of value.)
- OpSec is the prevention of interactions between the asset and the threat.
- Interactions are classified as:
 - Visibilities (opportunity)
 - Accesses (interaction from outside the scope)
 - Trusts (interaction between entities within the scope)
- Prevention means setting non-interactive boundaries.

Prevention - How to Make a Valid Boundary



- Move the asset.
- Hide the asset.
- Change the threat to a harmless state.
- Destroy the threat.
- Destroy the asset (rarely recommended).

Classifying Some Boundaries

Class	Channel	Description
PHYSSEC	Human	Comprises the human element of communication where interaction is either physical or psychological.
	Physical	Physical security testing where the channel is both physical and non-electronic in nature. Comprises the tangible element of security where interaction requires physical effort or an energy transmitter to manipulate.
SPECSEC	Wireless Communications	Comprises all electronic communications, signals, and emanations which take place over the known EM spectrum. This includes ELSEC as electronic communications, SIGSEC as signals, and EMSEC which are emanations untethered by cables.
COMSEC	Data Networks	Comprises all electronic systems and data networks where interaction takes place over established cable and wired network lines.
	Telecommunications	Comprises all telecommunication networks, digital or analog, where interaction takes place over established telephone or telephone-like network lines.

Operational Safety



Operational Controls

- The 10 operational controls which make assets safer are divided into two categories:
 - Interactive
 - Process
- Furthermore, there are 2 non-operational controls which make up one of the Interactive Controls, Authentication:
 - Identification
 - Authorization
- These controls cannot be expressed operationally because they cannot be transferred.

Controlling the Threat

- It is the means to mitigate attacks which occur through operations.
- To make an asset safe, you need to identify and then control the threat as it appears.
- Often times controls have limitations which make them less effective.
- More controls also may increase your Attack Surface.



Interactive Controls

- These are controls which can directly affect interaction with Visibility, Access, or Trust.
- These include:
 - Authentication (includes Identification and Authorization)
 - Indemnification
 - Subjugation
 - Continuity
 - Resilience

Process Controls

- These are controls which are used to protect assets once the threat is already present.
- These include:
 - Non-repudiation
 - Confidentiality
 - Privacy
 - Integrity
 - Alarm

Know Your Limitations

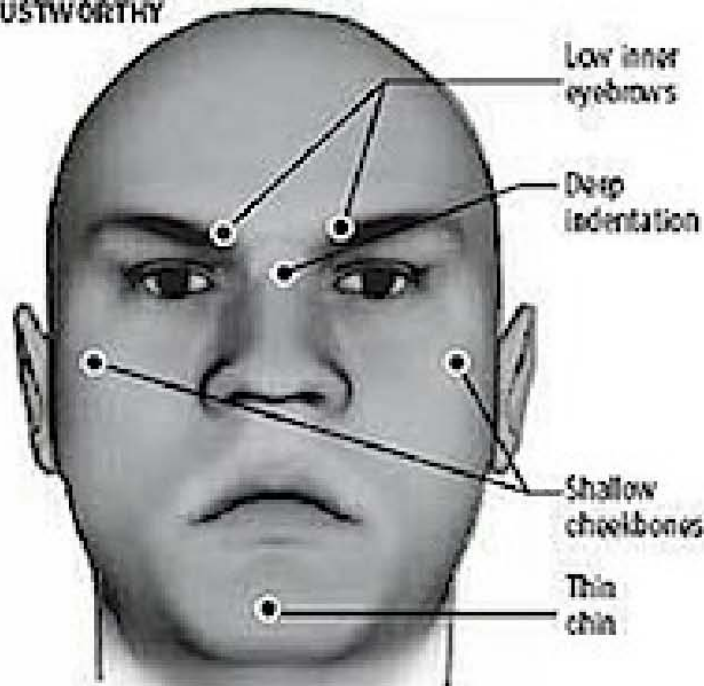
- Vulnerability
- Weakness
- Concern
- Exposure
- Anomaly.



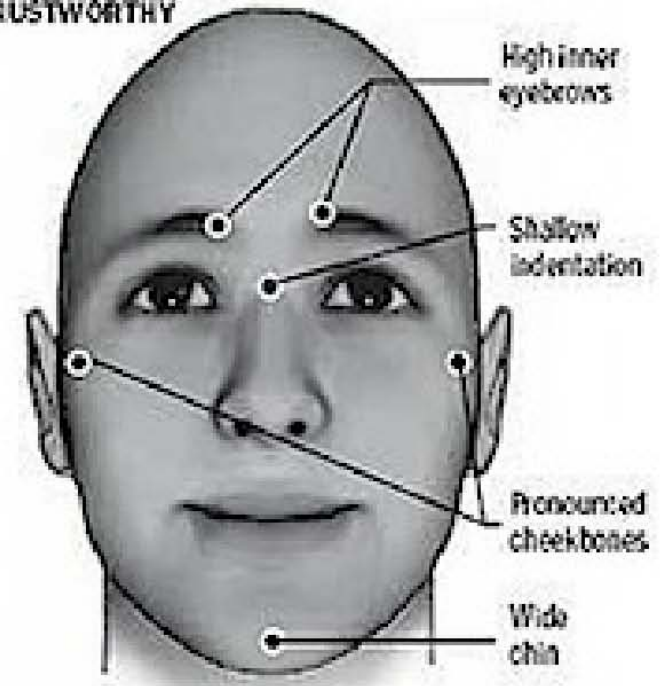
Know Who/What You Can Trust

- If you could take a pill that makes you more trusting of others, would you?

FEATURES THAT APPEAR UNTRUSTWORTHY

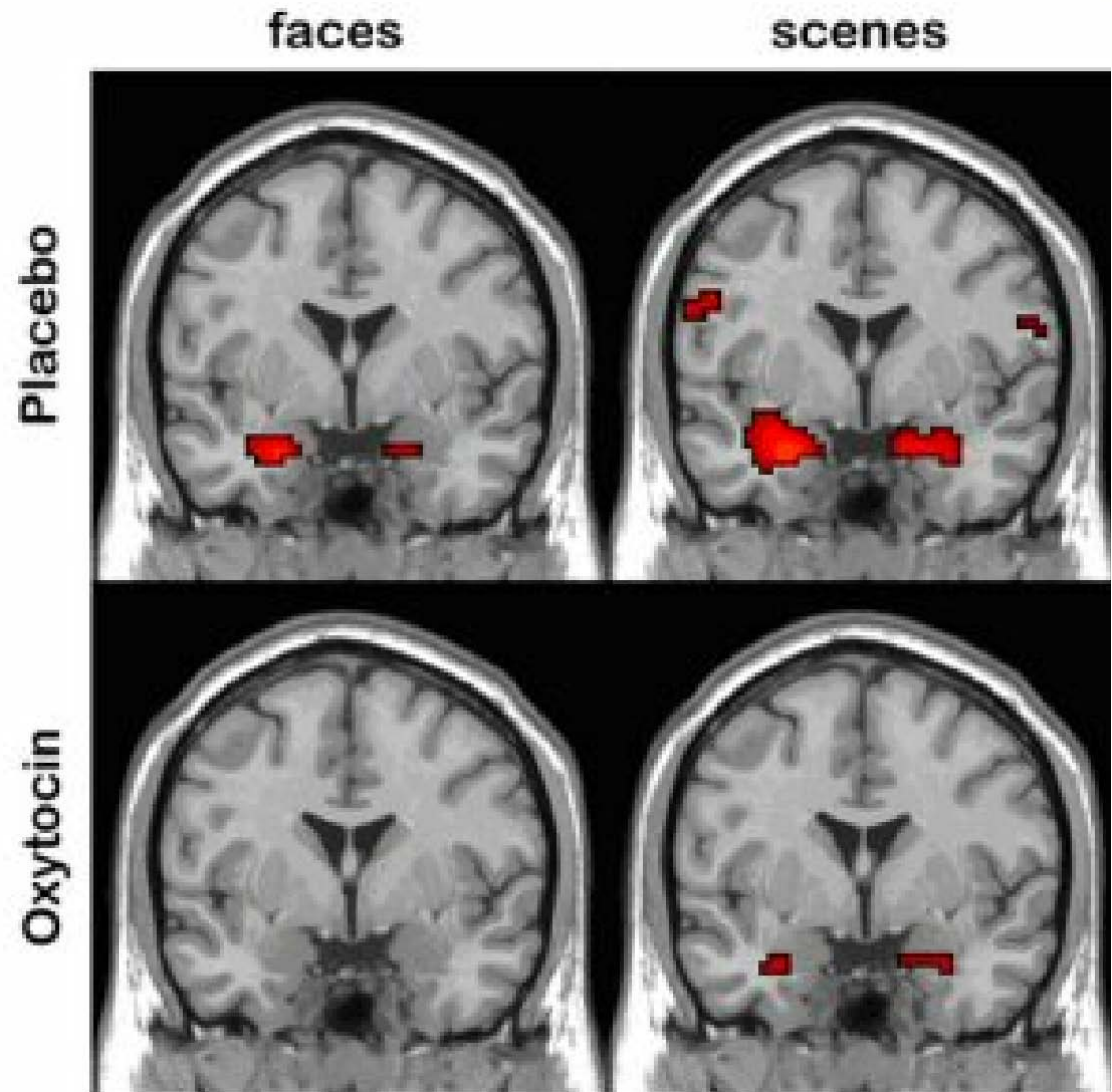


FEATURES THAT APPEAR TRUSTWORTHY



Trust Properties

- Size
- Symmetry
- Transparency
- Control
- Consistency
- Integrity
- Offsets
- Reward
- Components
- Operational Security



Taking a Stand



Attack Surface Sample

- As the guardian of your city, one of your assets to protect is the collection of "real" moon rocks given to you by the American ambassador.
- The rocks are stored in the museum vault and only brought out for special showings like fund raisers and the mayor's birthday party.
- As one of your city's vital assets you must assess what level of protection is provided for the rocks and what is the attack surface.



Entering the Museum



High-grade
Door Lock,
glass door
panes

Closed-circuit
Camera

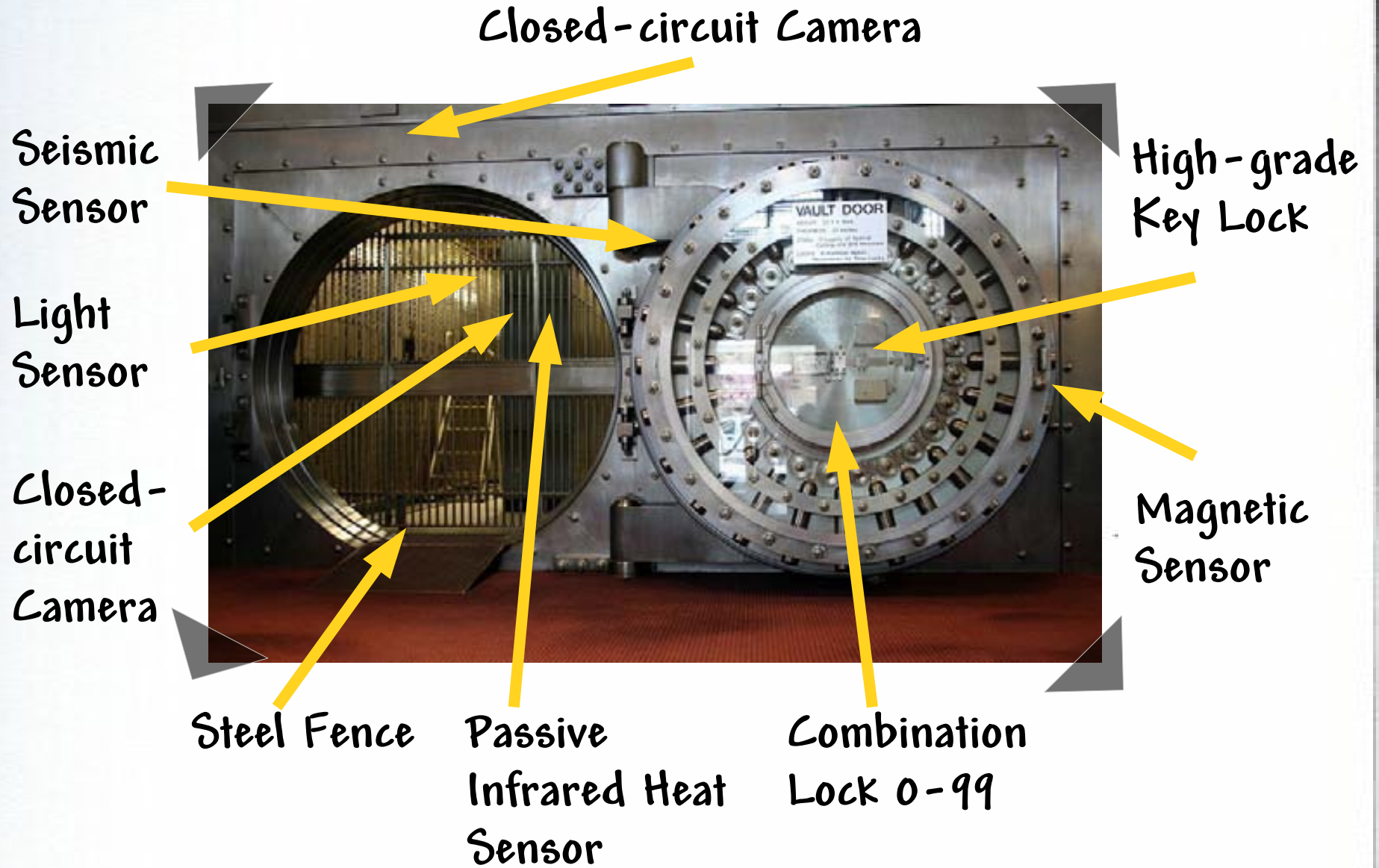
Entranceway to the Vault

Passive
Infrared Heat
Sensor

Motion
Sensor

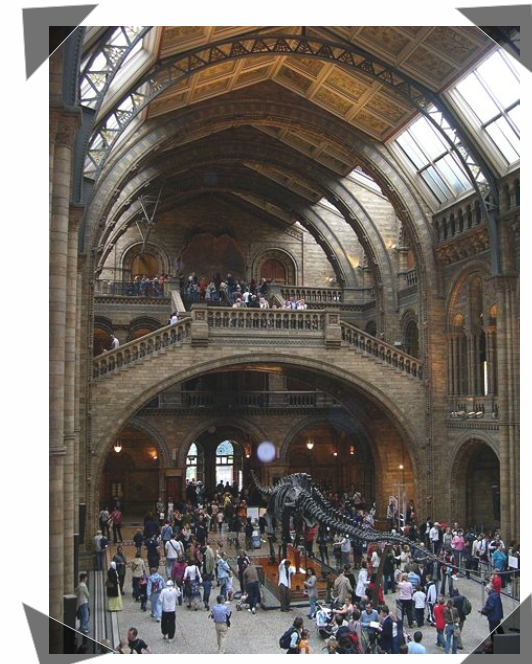


The Vault



Entrance Security Limitations

- Entering the Museum
 - Door lock circumventable through glass panes
 - Authentication - Weakness - Vulnerability
 - Camera monitored only during the day
 - Authentication + Alarm - Concern
- Vault Hallway
 - Heat Sensor
 - Alarm - Concern
 - Motion Sensor
 - Alarm - Concern



Vault Security Limitations

- External Vault

- Key Lock

- Authentication - Weakness - Vulnerability

- Combination Lock unhooded and viewable from afar

- Authentication - Weakness + Privacy - Concern

- Camera monitored only during the day

- Authentication - Weakness + Alarm - Concern

- Magnetic Sensor

- Alarm - Concern

- Seismic Sensor

- Alarm



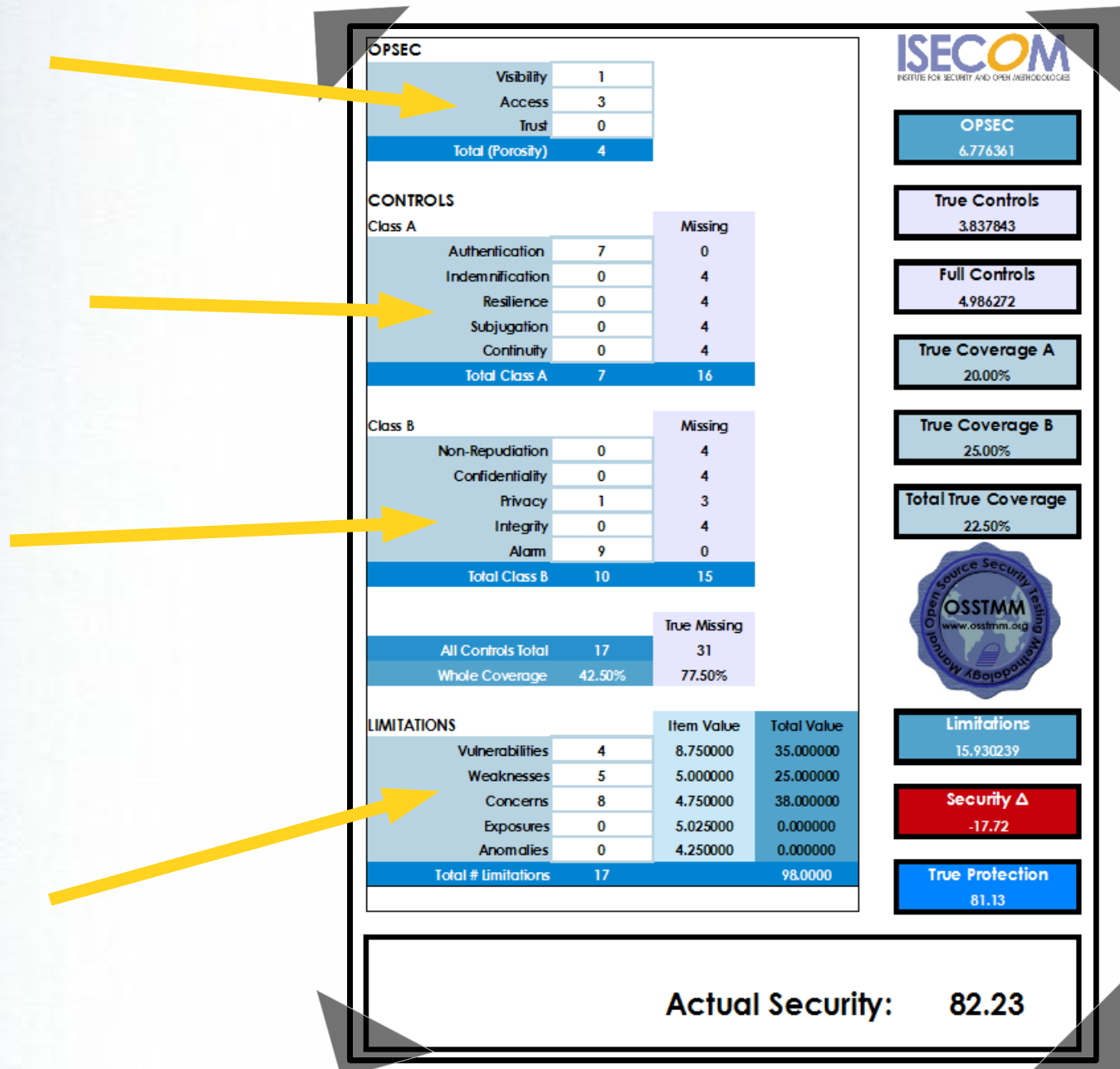
Vault Security Limitations

- Internal Vault

- Heat Sensor
 - Alarm - Concern
- Light Sensor
 - Alarm - Concern
- Camera
 - Authentication - Weakness + Alarm - Concern
- Steel Fence is kept unlocked for convenience
 - Authentication - Weakness - Vulnerability



Calculate the Attack Surface




More Than Just a Number

OPSEC	
Visibility	1
Access	3
Trust	0
Total (Porosity)	4

CONTROLS		
Class A		
		Missing
Authentication	7	0
Indemnification	0	4
Resilience	0	4
Subjugation	0	4
Continuity	0	4
Total Class A	7	16
Class B		
		Missing
Non-Repudiation	0	4
Confidentiality	0	4
Privacy	1	3
Integrity	0	4
Alarm	9	0
Total Class B	10	15
All Controls Total	17	True Missing 31
Whole Coverage	42.50%	77.50%

LIMITATIONS			
		Item Value	Total Value
Vulnerabilities	4	8.750000	35.000000
Weaknesses	5	5.000000	25.000000
Concerns	8	4.750000	38.000000
Exposures	0	5.025000	0.000000
Anomalies	0	4.250000	0.000000
Total # Limitations	17		98.0000



OPSEC
6.776361


True Controls
3.837843

Full Controls
4.986272

True Coverage A
20.00%

True Coverage B
25.00%

Total True Coverage
22.50%



Limitations
15.930239

Security Δ
-17.72

True Protection
81.13

Actual Security: 82.23

Money Translation

OPSEC

Visibility	1
Access	3
Trust	0
Total (Porosity)	4

CONTROLS

Class A

Authentication	7	Missing	0
Indemnification	0		4
Resilience	0		4
Subjugation	0		4
Continuity	0		4
Total Class A	7		16


Class B

Non-Repudiation	0	Missing	4
Confidentiality	0		4
Privacy	1		3
Integrity	0		4
Alarm	9		0
Total Class B	10		15

All Controls Total	17	True Missing	31
Whole Coverage	42.50%		77.50%

LIMITATIONS

		Item Value	Total Value
Vulnerabilities	4	8.750000	35.000000
Weaknesses	5	5.000000	25.000000
Concerns	8	4.750000	38.000000
Exposures	0	5.025000	0.000000
Anomalies	0	4.250000	0.000000
Total # Limitations	17		98.0000



OPSEC
6.776361


True Controls
3.837843

Full Controls
4.986272

True Coverage A
20.00%

True Coverage B
25.00%

Total True Coverage
22.50%



Limitations
15.930239

Security Δ
-17.72

True Protection
81.13

Actual Security: 82.23

Be a Superhero

- Know your assets, what they do, and how they interact with everything across all Channels.
- Measure their interactions.
- Measure how much you can trust those interactions so you can focus attention where trust is low.
- Measure the controls which exist for your assets.
- Prevent by reducing porosity.
- Balance porosity with controls.
- Remove or control those Limitations which affect your controls and increase porosity.
- Patrol, watching for trust changes and adjust controls and porosity accordingly.

Now You're Ready for Metropolis!



OSSTMM 3 Works for Metropolis

- The Open Source Security Testing Methodology Manual established Jan. 2001.
- The OSSTMM provides a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way.
- OSSTMM researches requirements about 8 - 10 years ahead of the mainstream testing.
- Developed by ISECOM, an open, non-profit, security research organization.
- ISECOM provides various certification programs for superheroes, mutants, super soldiers, mad scientists, evil medical schools, and some normal humans.



ISECOM Philosophy

- Make sense of security.



Professional Certifications

- OPST
 - Skills-based Professional Security Tester Exam
- OPSA
 - Skills-based Professional Security Analyst Exam
- OWSE
 - Applied-knowledge-based Wireless Security Expert Exam
 - Full electro-magnetic spectrum analysis
- OPSE
 - Knowledge-based OSSTMM Professional Security Expert Exam
 - Full understanding of the OSSTMM
- CTA
 - Applied-knowledge-based Trust Analyst Exam
 - Full understanding of applying trust metrics

Presentation Creator:

- Pete Herzog
- Co-founder and Managing Director of ISECOM
- OSSTMM Creator and Project Lead



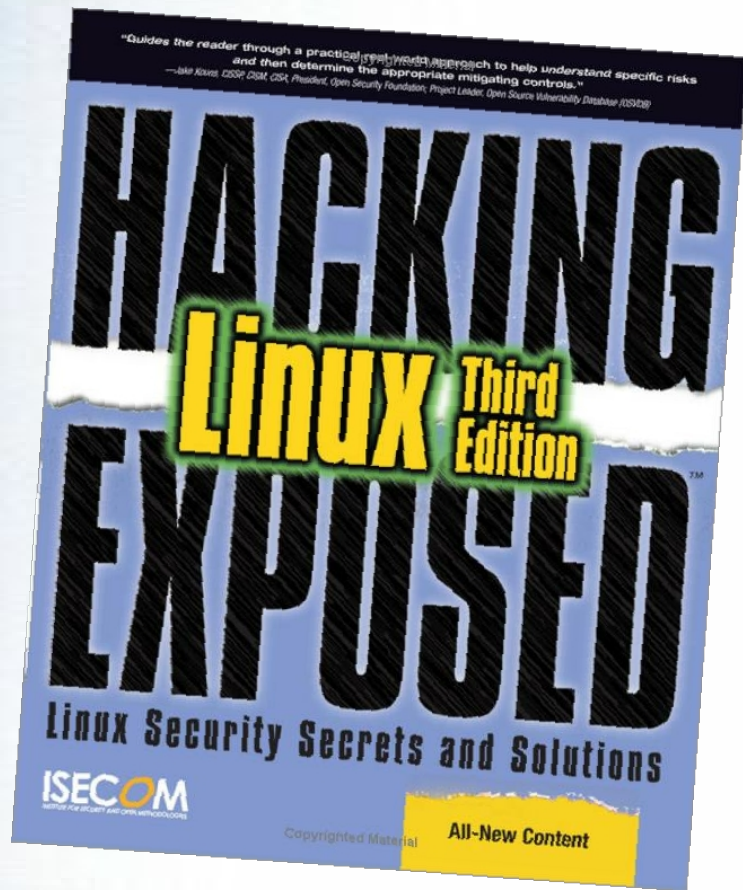
Photographic images provided by:

- Marta Barceló
- Co-founder and Director of Operations of ISECOM
- Photographer, Marta.com



Special thanks to Wikimedia Commons
for the museum and vault photos.





www.isecom.org
www.osstmm.org