

the official

Training Guide for



New Superheroes



by Pete Herzog

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Life as a Superhero



- Saw a commercial for Smallville with my kids...
- My daughter asked what it was about.
- So I explained it's about Superman as a boy learning his new powers while at the same time figuring out how to fight all these new villains showing up with new powers.
- She says, "That would be so hard to do!"

Our Own Private Smallville

- **It is hard to do.** And it's what we do in security.
- Problems are caused by interactions in an environment not designed to separate proper use from a mutating threat.
- The same solution that keeps out the bad (especially if it mutates) will also keep out the good.
- The best solutions are usually time intensive, costly, and make the environment unpleasant at best and sometimes unusable.



Everyone's Smallville

- The the threats return. They are ever-present within such a hostile environment.
- Threats are unavoidable because to survive, you need to put yourself out there which inevitably means you expose yourself to them.



- Even "normal" daily events will create unintended interactions and open you up to threats.

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)

Who Can People Turn To?

- Many trusted industries have lied to us (or at least covered up the fact that they were ever wrong) and we are cool with it.
 - We accept that most industries don't put our best interests over their bottom line.
 - We accept if they lie to us as long as they are lying to everyone equally.
 - We accept they make mistakes.
 - We accept that there are ALWAYS risks.
 - And we even accept that sometimes someone gets hurt.
- You thought the security industry was bad? The Pharmaceutical industry makes the Security industry look like matronly angels riding on unicorns with diffused lighting in a pastoral setting covered in butterflies and rainbows. The Financial industry is even worse. And government?!
- So who can the people really trust to help?

The World Needs You

- Many industries like the security industry follow certain patterns where good intentions are skewed from reality for maximum commercial potential.
- Government rules and laws are the whims of lobbyists and the effects of advertising on the ordinary voters.
- More than likely you already doubt the sincerity and security claims of many security providers, enough to have a cynical eye on the industries.
- But what about those who don't? What about those who blindly trust these industries? Do you think they want to learn it's all a lie?

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



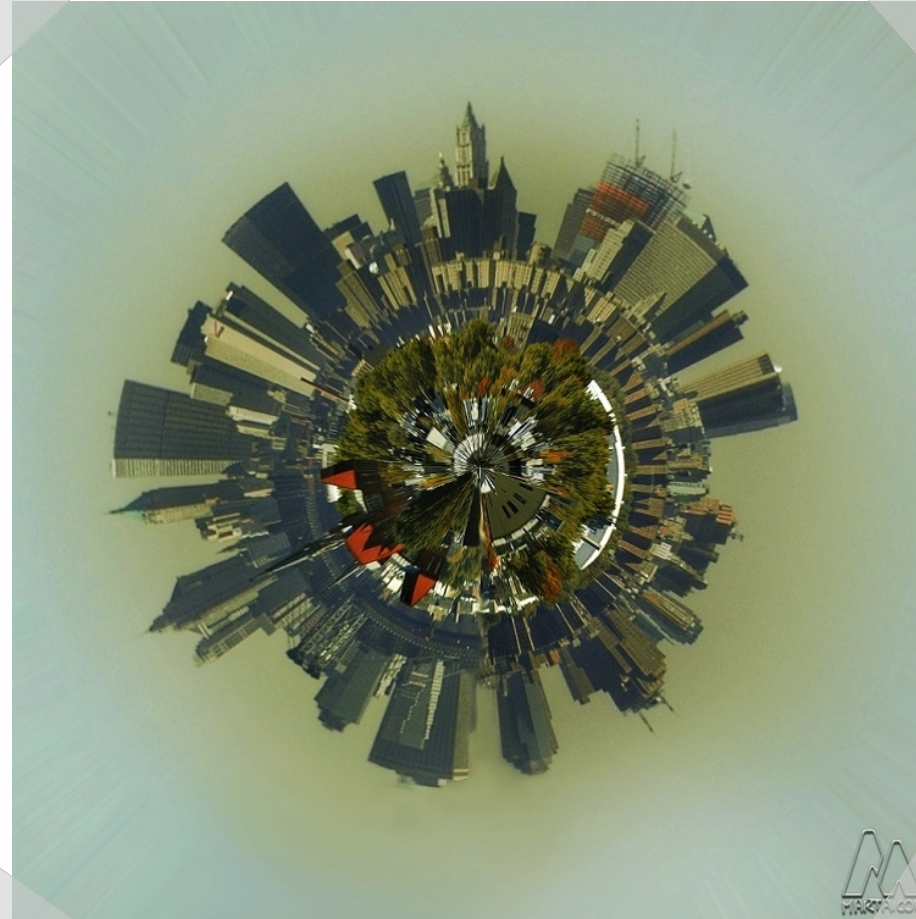
- Because you learn by getting the basic understanding first.
 - And you get the basic products like firewalls and antivirus.
- Because you watch the news for the latest threats.
 - Or read about them in magazines and mailing lists.

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.**
- Metropolis **NEEDS** superheroes.

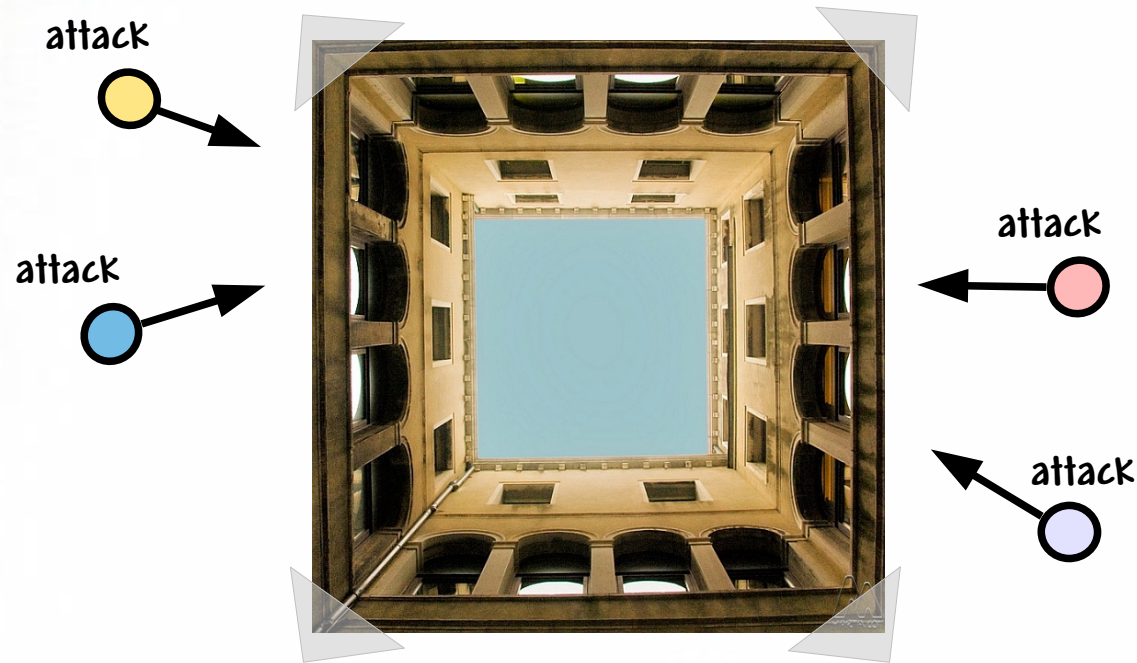
What Doesn't Work in Metropolis?

- 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

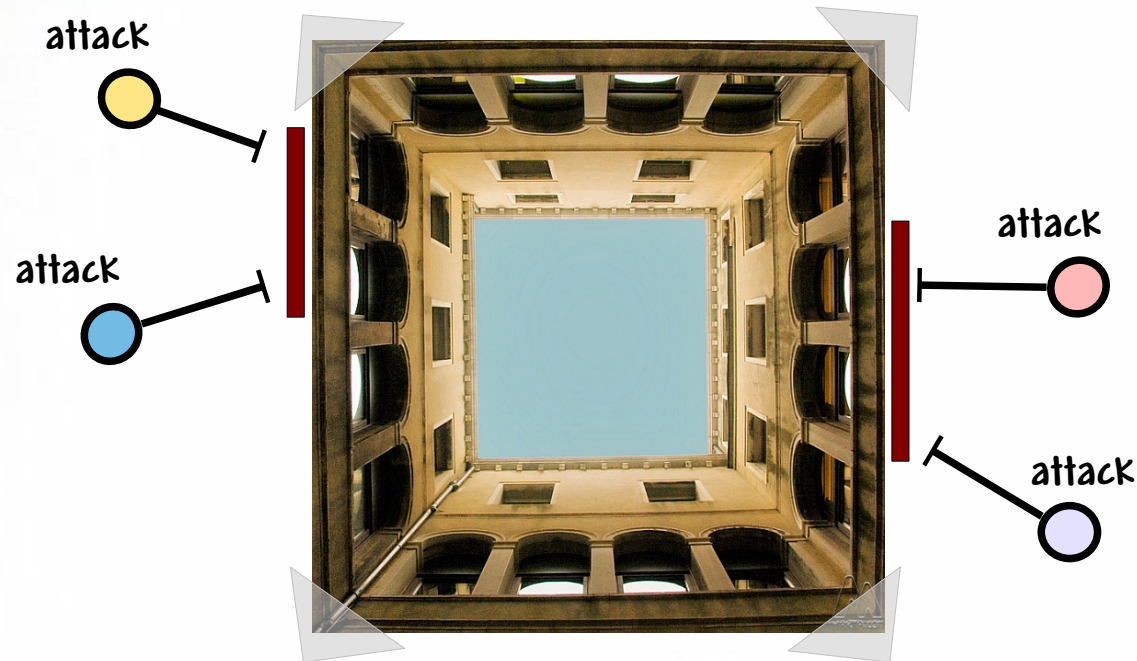
- Know your Attack Surface; exactly how much security, controls, and limitations you have by vector and channel.
- Know your Defense in Width; what your defenses are capable of regardless of the threat.
- Know how to trust without your gut; analyzing trust rationally and logically.

What is the Attack Surface?



- What we can measure in security is its Attack Surface.
- The Attack Surface is how much of something or someone is unprotected. It shows how much can be attacked.
- The Attack Surface is static against the environment (and somewhat against time).

Changing the Attack Surface



- If you know your Attack Surface you know how much is unprotected, uncontrolled, and open to certain classes of threats and you can **CHANGE** that.
- If you want to make a risk assessment, which is a way of making an educated guess if something bad could or will happen, you need to start by knowing the Attack Surface.

Risk and the Attack Surface 1



- Take a normal person who is not wearing armor and you have an almost 100% Attack Surface.
- That person on the road of a pastoral village will have a low risk of harm.

Risk and the Attack Surface 2



- Move that person to a war zone and their risk of harm goes up however the Attack Surface remains the same.
- Risk is variable. Attack Surface is static. You can determine your attack surface without risk. You can't do it the other way around though. But it's usually done so.

Risk and the Attack Surface 3



- Reduce the Attack Surface of a person by either improving the defenses on the person or by controlling the threats around the person.
- Risk is variable. Attack Surface is static. You can determine your attack surface without risk. You can't do it the other way around though. But it's usually tried so anyway.

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

- To understand **which** interactions we must separate we classify interactions into 3 Classes and further subclass them into 5 Channels.

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

- Safety is what happens when you need to be around the threat because it is not possible to identify it or contain it.
- Sometimes, the threat is another asset and only becomes a threat in the wrong situation or by accident.



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

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.
- This is done through any combination of 10 operational controls
 - These are not management type controls like documentation, training, or auditing stuff of which there are many.
 - If your super powers include accounting, auditing, or management stuff, although excellent, maybe you should consider something less dangerously interactive as a career.
- 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

- These limitations affect how well your prevention and controls can work.
- Categorized and measurable by operation and not by some ideas about risk somebody made up.
- Operational limits can be classified to 5 types which delimits what happens when something is broken: Vulnerability, Weakness, Concern, Exposure, and Anomaly.



Now Measure Your Attack Surface

- Count the porosity in the scope.
 - all that which is visible and interactive outside of the scope and allows for free interaction between other targets in the scope
- Account for the controls in place per target.
 - Determine where any of the 10 controls are in place such as Authentication, Subjugation, Non-repudiation, etc.
- Account for the limitations found in the protection and the controls.
- The attack surface is controls minus porosity minus limitations

Why Measure?

- It shows you what should be secured, what should be protected first, and what should just be controlled.
- It helps you locate to areas where you will have the best response time to the most assets (maybe not necessary for those with super speed).
- Shows what additional protection you need and how it should be set it up for maximum effect.
- Shows where you have too much or too much of the same type of controls.
- Lets you measure security efforts and measure improvements.
- Shows where you are reducing your exposure to specific types of threats.

What About the Threats?

- In OPSEC you should don't focus on threats.
 - That's risk! You can't generate facts on what threat exists because until it hits it is not a threat and after it hits you shouldn't speculate it will hit again the same way.
 - Instead, analyze your capabilities in security, controls, and response from each vector and channel.
- This differs greatly from risk analysis. It allows you to know your posture in regards to ANY threat as opposed to only certain threats.
 - Risk analysis will try to determine if a threat can get through a defense.
 - Security analysis will determine the soundness of the defense, the vectors it defends, how it fails, and time needed to respond when it fails.

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

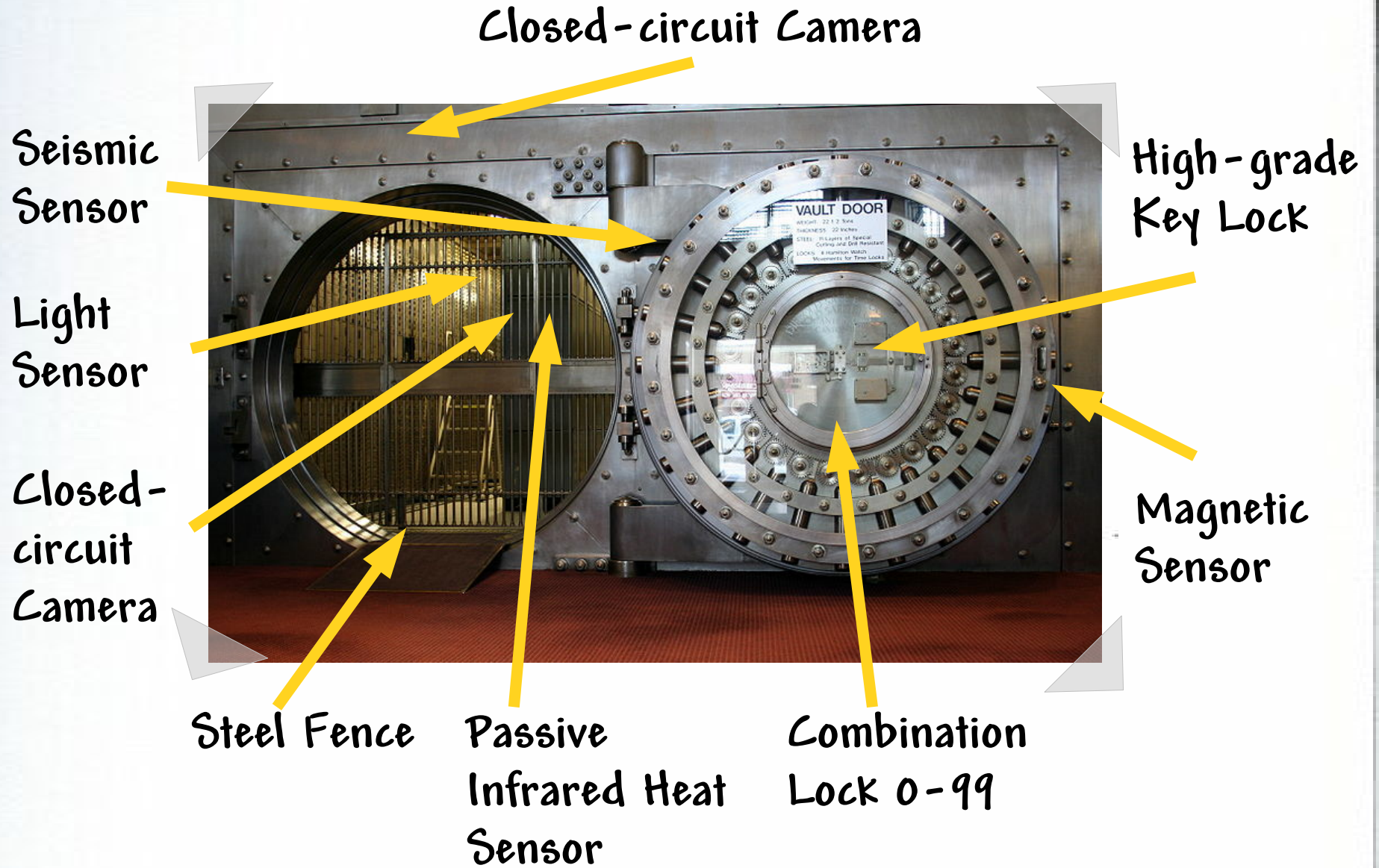
Entranceway to the Vault

Passive
Infrared Heat
Sensor

Motion
Sensor

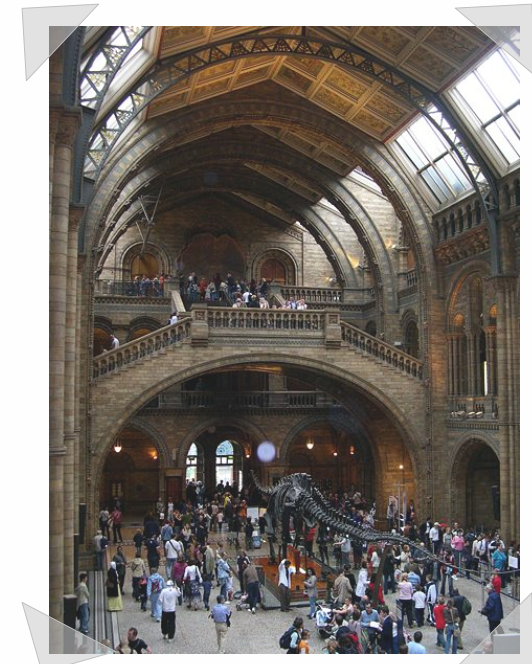


The Vault



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

Count and classify the holes

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

Classify the interactive controls

CONTROLS		
Class A		
Authentication		7
Indemnification		0
Resilience		0
Subjugation		0
Continuity		0
Total Class A		7

Classify the process controls

Class B		
Non-Repudiation		0
Confidentiality		0
Privacy		1
Integrity		0
Alarm		9
Total Class B		10

All Controls Total		17
Whole Coverage		42.50%

Classify the limitations

LIMITATIONS		
Vulnerabilities		4
Weaknesses		5
Concerns		8
Exposures		0
Anomalies		0
Total # Limitations		17

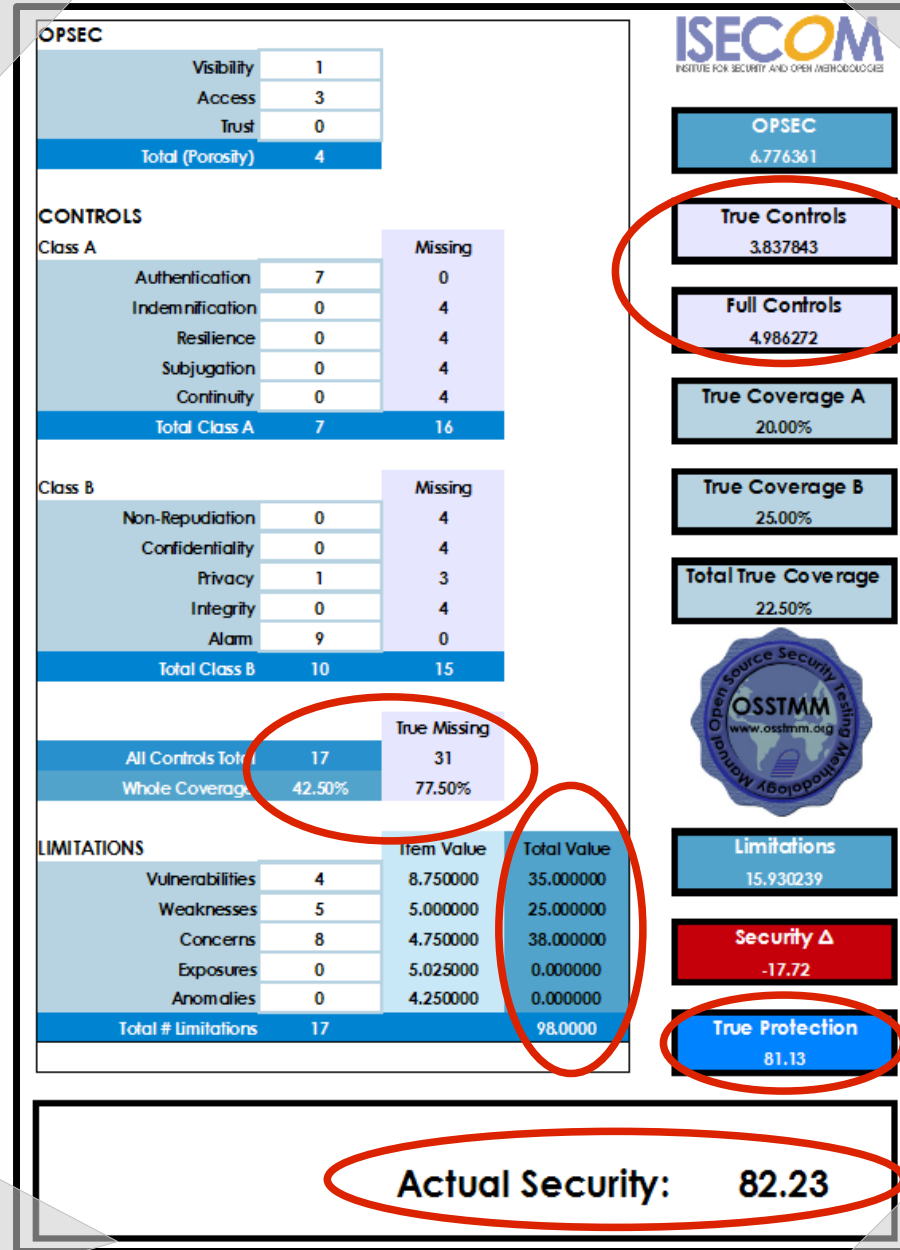


Actual Security:

More Than Just a Number

Controls which are missing, chain-like, or overly-used become quickly apparent.

Limitations not weighted and are calculated from Controls and OPSEC



You can see what's protected either with all controls (Whole) or without the redundant (same chain) controls.

True Protection shows the balance between controls and OpSec while Actual Security shows the attack surface.

Money Translation

What purpose do these openings have?
 Transactions?
 Maintenance?
 Response?
 Administration?


The security budget translates to these controls.
 What is the ratio of cost per solution?

Which Limitations effect which purpose of openings. Which effect which controls?

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			
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

What you spend is related to Whole coverage. However the difference between True and Whole coverage may be what you overspend or spend wrong. You can use this to investigate if that spending serves some other purpose (like it makes customers happy).

Has a change in spending influenced this value from last time?

Is this good enough to protect BILLIONS?!

The Little Details

- Calculating the Attack Surface can be as granular as you want.
- It's your choice as to how many decimal places you need to take the calculation depending on how carefully you want to moderate change.
- Besides the final value (the RAV) there are many facts you can take away from this to help you improve your infrastructure.
- Furthermore, a drill-down approach is possible where the OPSEC and Controls of each item in a scope is calculated independently and even sub categories to highlight problem areas.
 - Campus > Building > Floor/Department > Room
 - Network > Server > Daemon/Service > Application

Being the 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!



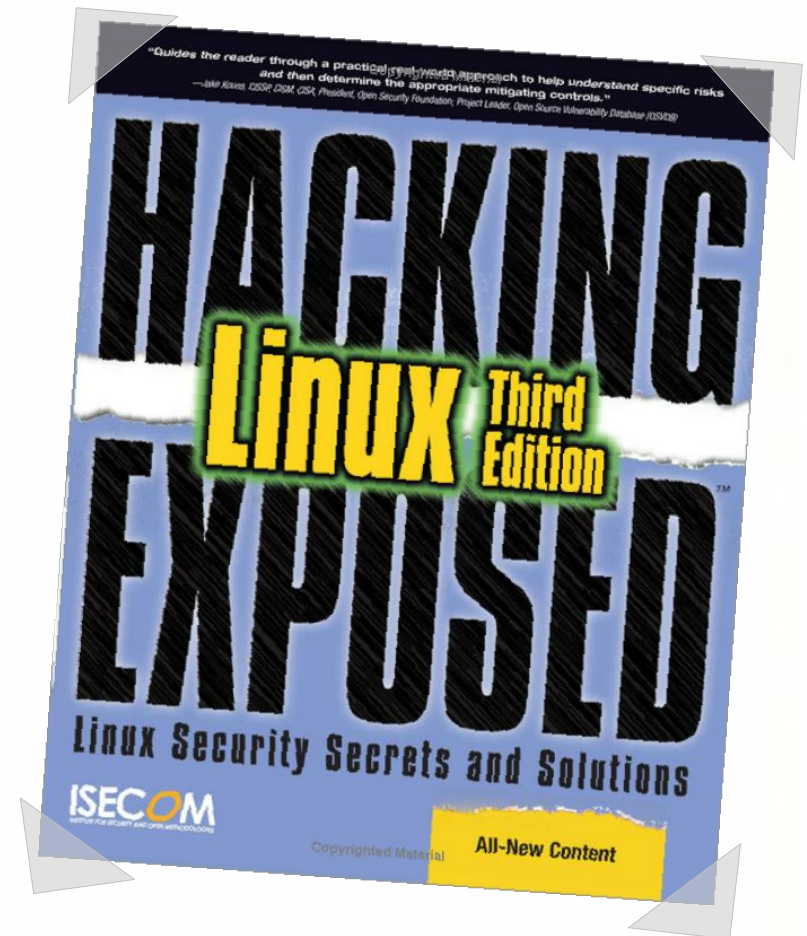
OSSTMM 3 Works for Metropolis

- 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.
 - The humanization of testing into an art form rather than a science introduces all sorts of analysis errors.
 - Understanding who we are as Humans and how we think needs to change how we perceive and define 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

Secret Origins

- This guide is based on research for the Open Source Security Testing Methodology Manual v. 3. (Legionnaires of the 32nd century, please refer to the OSSTMM v. 4 published in 3109.)
- OSSTMM 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 was created by mild-mannered Pete Herzog and Developed by ISECOM, an open, non-profit, security research organization and group of alternate super friends.
- ISECOM provides various certification programs for superheroes, mutants, super soldiers, mad scientists, evil medical schools, and normal humans.

Presentation Creator:

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



Presentation Support:

- Nick Mayencourt
- Director of Business, ISECOM
- Founder and CEO of Dreamlab Technologies Ltd.

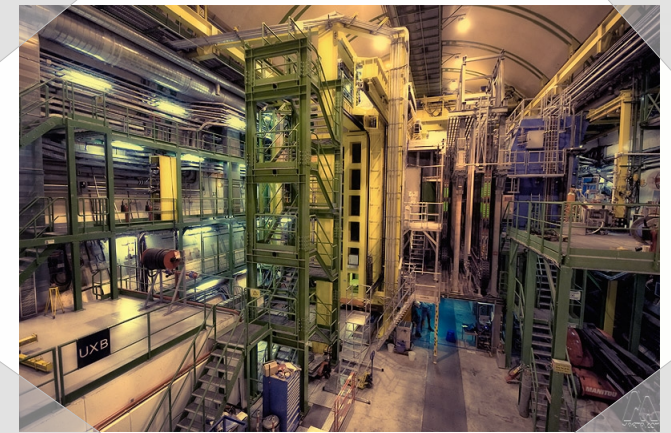


Photographic images provided by:

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



Special thanks to Andreas Unterkircher and the rest of the helpful staff of CERN for the seminar hosting this presentation and the tours of the facilities.



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



www.isecom.org
www.osstmm.org