Bringing the Sexy Back to...

Defense In Depth
“Defense is hard.”

“Defense always loses.”

“Defense doesn’t get any of the sexy tools like those Red Team folks get. All we get is a bunch of expensive boxes with blinky lights that get owned or bypassed.”

So….how do we few, we brave few, get better at defense? How do we change the Defense Culture? How do we Stop Losing And Do Things Right?
Who Is This Chucklehead?

20 years in IT.....7 years in infosec...been in the commercial aviation, financial, and healthcare sectors...

Former Armor officer in the US Army...

Host of The Southern Fried Security Podcast for the last three years...

Presented at ShmooCon, SOURCE Boston, Security Zone 2012 in Cali, Colombia, various Security BSides events, and lots of other events

I have a lot of opinions and am more than willing to share them in exchange for you sharing your opinions and ideas.
What is “Defense In Depth”?

1: a tactical system of mutually supporting positions that are each capable of all-round defense and that have sufficient depth to prevent the enemy from achieving freedom of maneuver before his attack is broken up and absorbed.

2: a strategic succession of defended areas which will permit continuation of a war after forward areas have been lost.

**Defense in Depth** is an IT security strategy that focuses on protecting your company's critical IT data and resources through multiple layered solutions. A typical Defense in Depth Strategy will often contain, but is not limited to, the following IT components:

- Firewall
- Antivirus
- Encryption
- Intrusion Detection and Prevention Systems
- Automated Patch Management
- Formal End-User security training
Defense in Depth is a mindset... a way of thinking about the battle...

Defense in Depth is not a checklist of point solutions you half-ass implemented over the last 5 years.
How We Got Where We Are

BLINKY LIGHTS!

Thought that technology by itself would solve the problem

MORE BLINKY LIGHTS!

Bought into the Sales/Marketing/Consulting pitch about Defense In Depth means “Just install our appliance and you’re creating depth”.

DID WE MENTION BLINKY LIGHTS YET?

Totally drank the “100% or Nothing” Kool-Aid

Non-carbonated fruit flavored drink when it came to defining Success....
Can We All Just Agree It Didn’t Work The Way We Wanted?
So What Do We Do Now?
Start Thinking About Your Zones

Zone of Observation
Zone of Influence
Zone of Control
Zones??!!
What About “Asymmetric Warfare”?
Let’s Examine That...
Zone of Observation

**Meat Space**
- Uses aerial (drone, satellite, manned aircraft) assets
- Signals Intelligence (SIGINT)
- Electronic Intelligence (ELINT)
- Human Intelligence (HUMINT)
- Eyeball, Calibrated, Mk 1

**Cyber Space**
- Threat Intel Subscriptions
- Intrusion Detection/Prevention
- Full Packet Capture/Analysis
- Honeypots / Canaries
Zone of Observation

You can look.... but you can’t touch.

So Much Data.... Can’t Analyze It All!

Is (hopefully) the “other side” of your perimeter demarcation...

For most organizations there is a very limited range.
Zone Of Influence

**Meat Space**
- Patrols – Day & Night
- Random Checkpoints
- Cultivate Positive Relationships w/Population
- Rapid & Effective Response to Incidents

**Cyber Space**
- Log Review/SIEM
- Internal IDS/Honeypots
- User Education
- Rapid & Effective Response to Incidents

![Image of soldiers and civilians]

![Image of book: Computer Security For Dummies]
Zone of Influence

Monitoring.... with a kick

IT Operations 101...
Configure, Monitor, Patch

This will probably make up over 85% of your total network

Be aware – assets can move from “Influence” to “Observation” zones quickly
Zone of Control

**Meat Space**
- Multiple fixed checkpoints requiring multiple IDs with barriers to all other entry paths
- Searches of people entering and leaving
- Only certified vehicles permitted entry AFTER comprehensive search

**Cyber Space**
- Multi-factor auth for all privileged transactions
- Deep packet inspection of all traffic
- Intense config management and detection of drift
Zone of Control

Very expensive.

Look for reasons to throw the asset out of zone.

Only a mature org can do this for more than the Crown Jewels.

Only let assets that you are 100% sure enter this zone.
And then check them again.
And again.
And again.
Rules Of The Zones

- The natural progression of assets is Control > Influence > Observation.
- Takes hard work to keep an asset in the Influence or Control zones.
- Unsure? Put the asset in the lower classification and remediate.
- Each level up requires an order of magnitude more effort to reach and maintain for each asset.
Wait, What?

AntiVirus is Dead.

IPS is Dead.

Firewalls are Dead.

SIEM is Dead.
Ready For Some Truth?

Defense *is* hard....

If you subscribe to the "Red only has to be lucky once, Blue has to be lucky all the time" you’re probably a very frustrated defender...

If you think that to win as a defender it means you *never* get breached you’re either very new to the game or very depressed.
#Winning
How To Win As A Defender...

Know what you’re defending and spend your resources defending what *really* matters.
Resolve that the adversary isn’t going to win. Not today. Not on my watch.
How To Win As A Defender

Realize that you will take losses... Just don’t make those losses meaningless...
How To Win As A Defender...

Don’t be afraid to mix things up. Make changes. Do things differently. Red does...
How To Win As A Defender

Every day you must learn from yesterday, plan for tomorrow, and fight for today.
JOIN THE BLUE TEAM!
We have cookies! And Caboose!
Martin Fisher
armorguy@gmail.com
@armorguy
www.southernfriedsecurity.com