Cyber Industry Day
Partnering with Industry

Art "Wally" Wachdorf
24 AF/CA

24AF Interface with Industry

- The process
  - Contact 24AF/CA to arrange a meeting with 24AF and its units
  - We will arrange to have the “brain trust” available so you can talk with all relevant players at once
- Then what
  - Way ahead items will be identified at the meeting
  - Follow-up meetings if necessary
  - Frank feedback
- We can’t do all we want to do!
- The Matrix

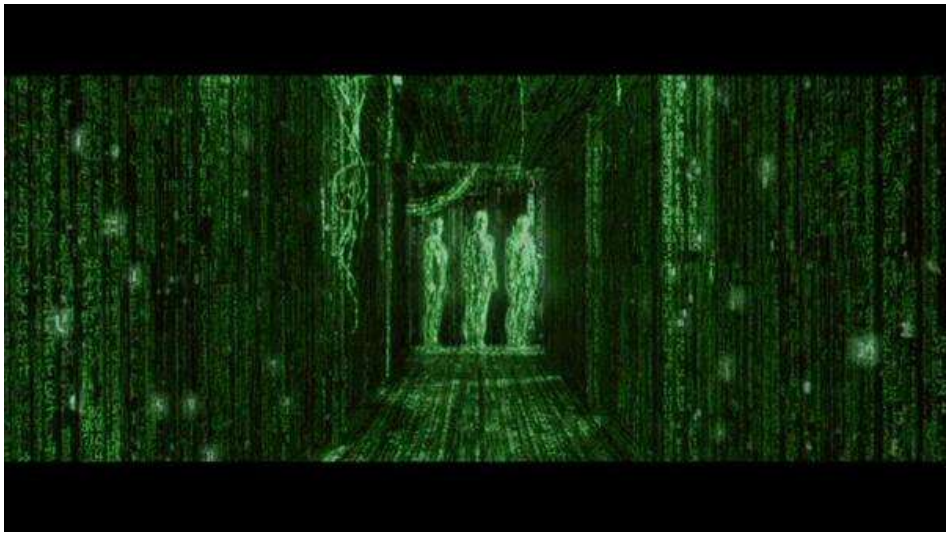
Our Matrix

Clips from the movie The Matrix

The Matrix

Technology Provider	Date of Last visit*	Description of Technology	Mission supported	Does it support CORONA Strategy	1-n Requirements	CSAF Funding Priority	Assessment	Status	Cost
Infokretzer	Jan-12	Technology automatically maps network and highlights misconfigured or non-compliant devices	Network operations	Reduces manpower required to accomplish process	Persistent NetOps	AFNet Sustainment	Very useful capability but hasn't been fielded in any large scale deployments…supporting architecture not consistent with current plans, very expensive…other vendors cheaper	Waiting to hear from CEO, Mr. Mike "the brain" Kretzer about results of deployment on larger network (1000 devices)	Enterprise license is $12.8B per year, not including support
V8 Cyber Technologies	Jun-12	AutoVanquisher: Provides capability to detect malware and vanquishes the sender automatically	Defensive cyber operations	Automates existing processes	Defensive Counter Cyberspace	Passive and Defensive Counter cyberspace	Great capability that works well and has been demonstrated at multiple government sites. Adversary shakes in his boots when they even consider being pitted against V8 technology	Planning to implement at one gateway as risk reduction effort	$24.75 for enterprise fielding, includes support
Wally Cyber Stuff	Aug-11	Detects insider threats and shocks them through the keyboard	Network operations and passive defense	Reduces support or operations costs	Data Confidentiality & Integrity Systems	None	Sounds great, but failed in every test. Shocks the wrong people and fails to detect 95% of insiders. Most claims are exaggerated	Informed vendor that no current interest in shocking our folks but would reach out to them when that became a mission area	Unlimited supply of diet coke for life
White Consulting Services	May-12	Provide network support and consulting service; can assess and quantify risk	Supports 67NWW operations and can assist A5/6 and 688 with network analysis	No specific efficiency gained	Multiple	None	They have promising capabilities for risk management but their contract support for operations is not significantly better than others	Looking to have Welch Laboratories do an assessment of their risk management capability	Awaiting final cost proposal for risk management only

Now you can see it decoded



Clips from the movie The Matrix

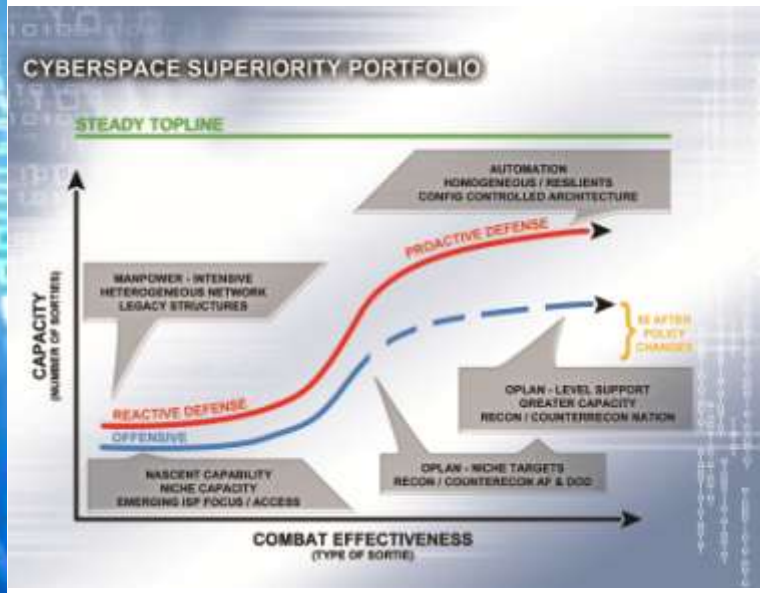
Thoughts on Future Acquisitions

- Simplicity
  - Leverage what we have
  - Reduce complexity
- Good quickly is better than perfection in FY2025
- Start with small spiral implementations
  - Risk reduction
  - Learn as we go
- Leverage leading edge technology while it still is
- We'll date, but not interested in marriage…yet

"A good plan violently executed now is better than a perfect plan executed next week." George S. Patton

What Works

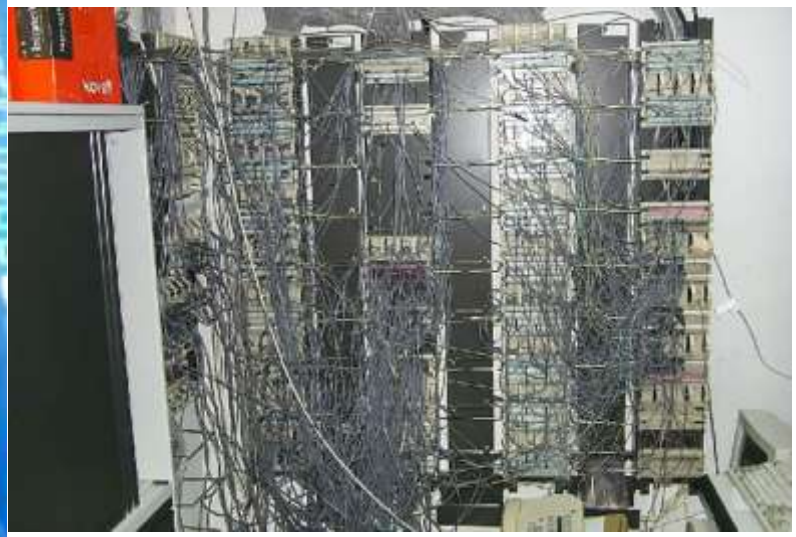
- Capability must integrate
  - Integrate with our existing operational and systems architectures
- It must be easier to use
  - 1980's PC verses a 2012 Laptop



- Capability must support the CORONA Strategy
- Scalability
- Simplicity
- Solve our toughest problems

What Doesn't Work

- Complicated proprietary systems
- Duplicative architectures
  - Leverage existing data
- Systems that don't feed our situational awareness



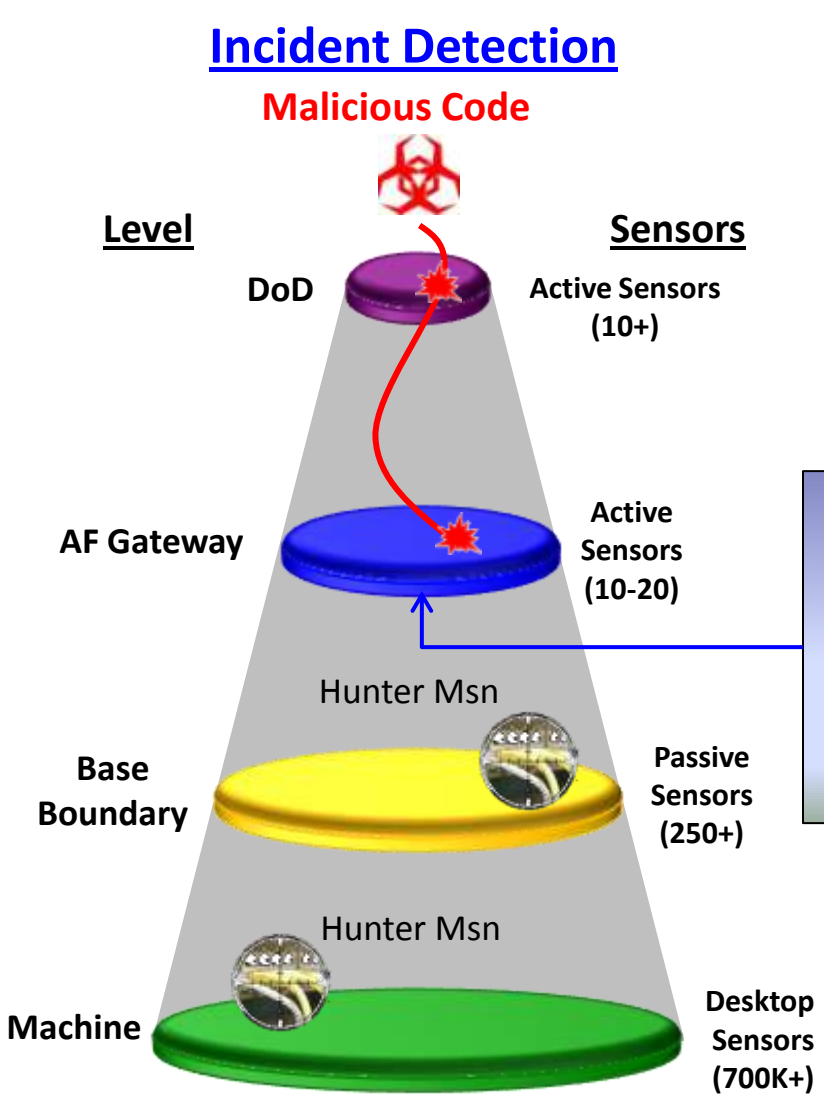
- Manpower intensive systems or processes

Industry, Academia and the Labs

- Partnering with University Labs to assess capability
  - Labs can assess capabilities within the context of our architecture
  - Used as a risk reduction
- Develop operating concepts up front
- Assess how industry capabilities integrate with what we already have
- CRADAs

Questions?

Pro-Active Defense
Layered "Defense in Depth"

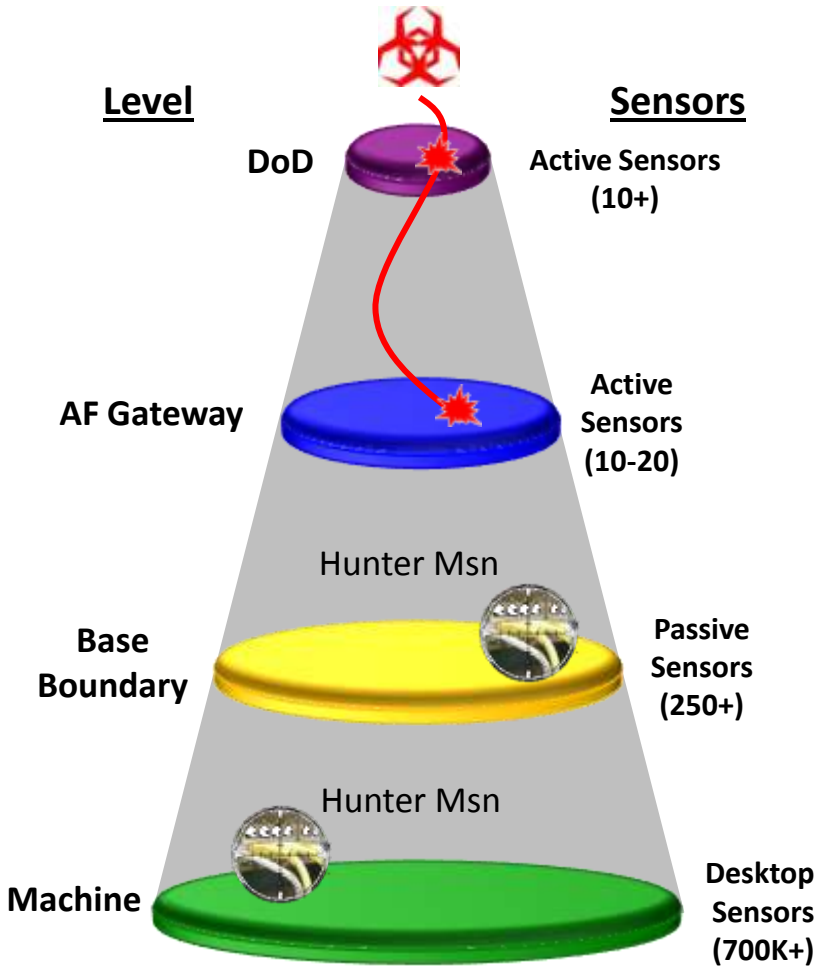


Slammer Worm Block

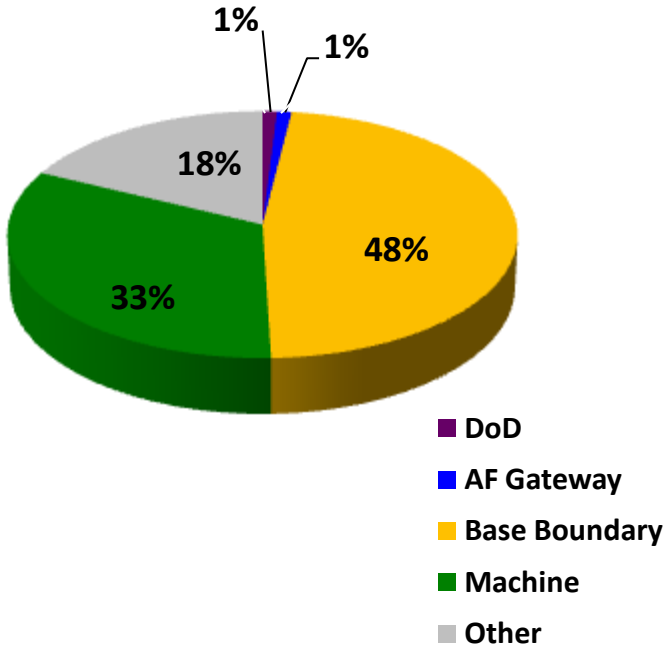
- Enabled real-time correlation as single attack
- Identified 'source' to enable immediate blocking actions
- Saved bandwidth
- Saved 'cleaning' time
- Enabled response actions

Pro-Active Defense
Layered "Defense in Depth"

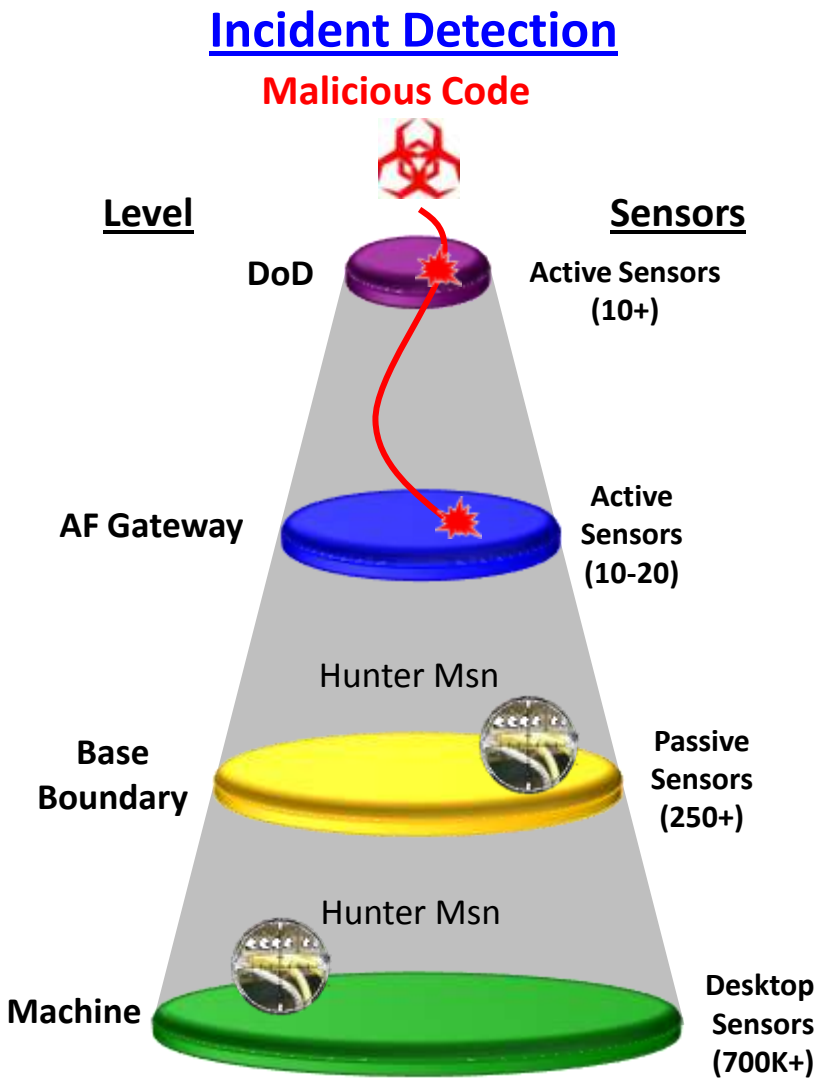
Incident Detection



Detection by Sensor



Pro-Active Defense
Layered "Defense in Depth"



Forensics

Signatures

Heuristics