

26 October, 2010



Utilities



Chemical



Oil & Gas



Water



Transportation



How Stuxnet Changed the World

Walt Sikora – VP, Security Solutions

In this Presentation we cover

- **How Stuxnet changed the world**
 - Top ten -Stuxnet
 - How the media focus missed a great opportunity
- **The importance of sharing factual information**
 - Collaboration
 - Private & Public Sector roles
- **The solutions and suggestions to be considered now**
 - Change management
 - Continuous assessment
 - Compliance automation

STUXNET



<http://bit.ly/aThirH>

Top 10 ways Stuxnet changed the world

10. Your friends and neighbors now understand what you do for a living
9. Industrial Control Security conference attendees are no longer just balding, grey haired men
8. You no longer have to justify your annual budget for ICS cybersecurity
7. Industrial control system vendors no longer tell their clients its their problem to secure the system
6. Industrial control system vendors no longer tell their clients their warranty is voided if they try to secure their systems

Top 10 ways Stuxnet changed the world

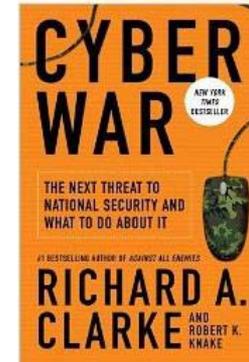
5. There is only one global ICS cybersecurity standard that everyone follows and certifies themselves to
4. IT and OT learn that their respective goals, objectives, and motivations are not mutually exclusive
3. DHS, DOE, INL, Sandia, FBI, US-CERT, ICS-CERT, NCCIC, ES-ISAC... all wish they found it first – and could talk about it
2. Cybersecurity information and disclosure is openly shared and discussed between public, private, owners, operators and vendors
1. Joe Weiss doesn't have to use Maroochy as a cyber example any more



Stuxnet: Malware more complex, targeted and dangerous than ever

Computer Worm May Be Targeting Iranian Nuclear Sites

Bloomberg



The next threat to national security and what to do about it.

STUXNET in the News

The New York Times

A Silent Attack, but Not a Subtle One



FINANCIAL TIMES

Stuxnet worm causes worldwide alarm

Stuxnet worm rampaging through Iran: IT official



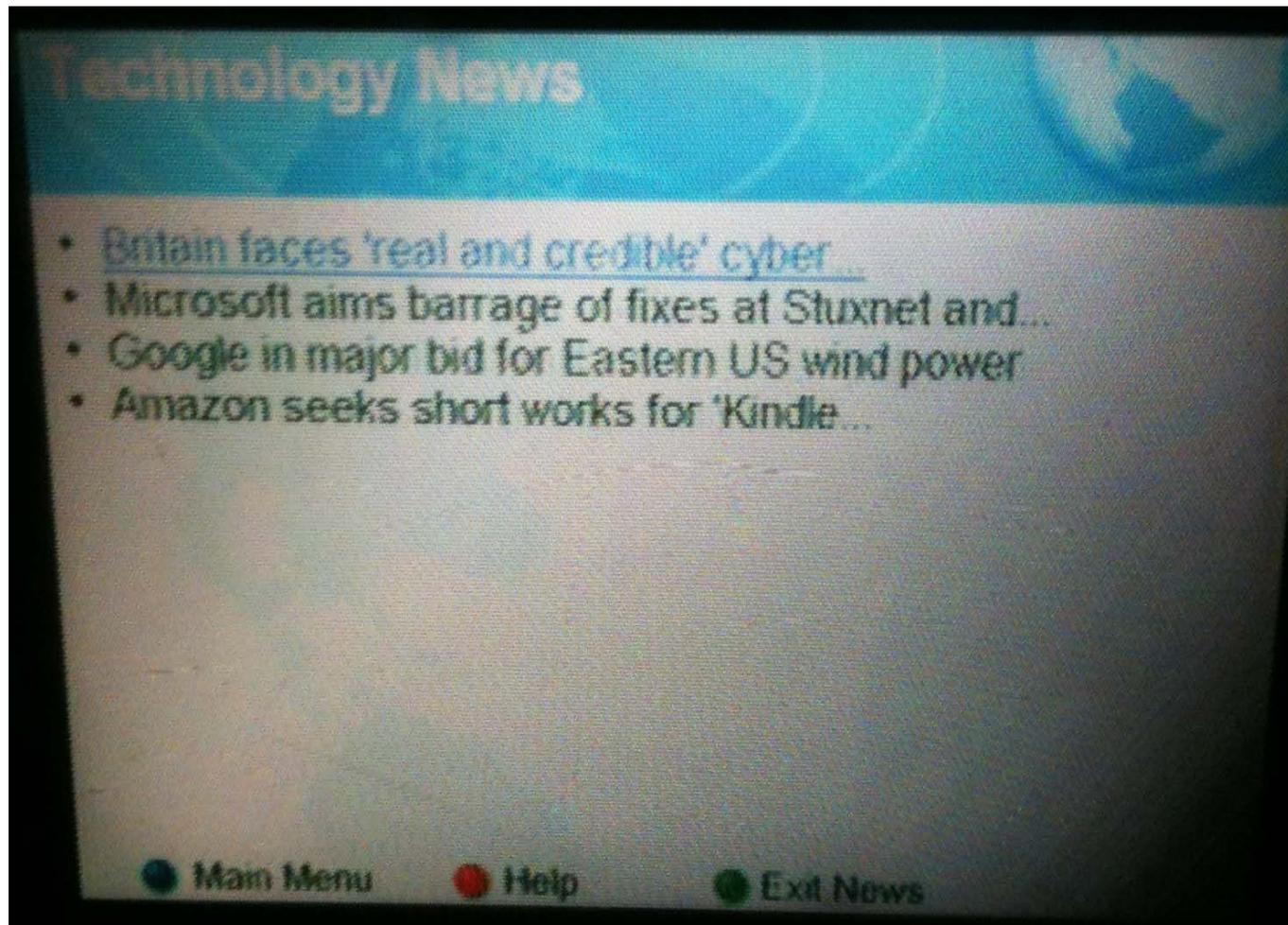
CBS NEWS

Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?

theguardian

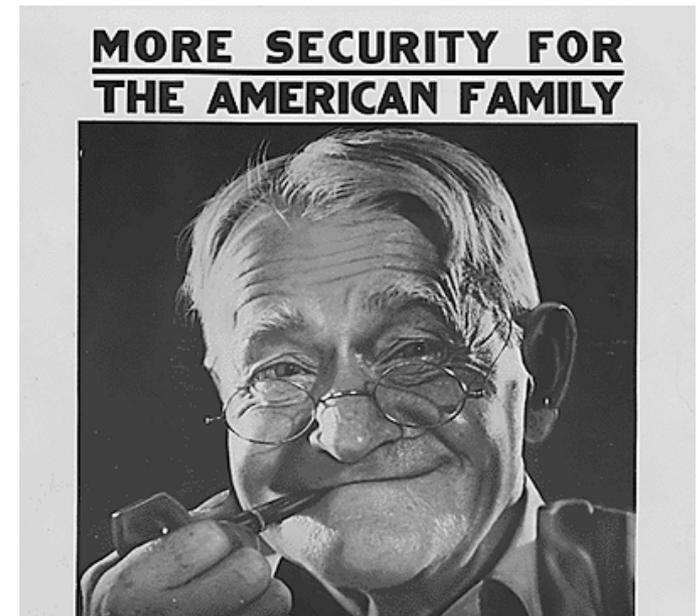
Stuxnet worm is the 'work of a national government agency'

It's even on my in flight entertainment system...



Reality is that Stuxnet did not change the world

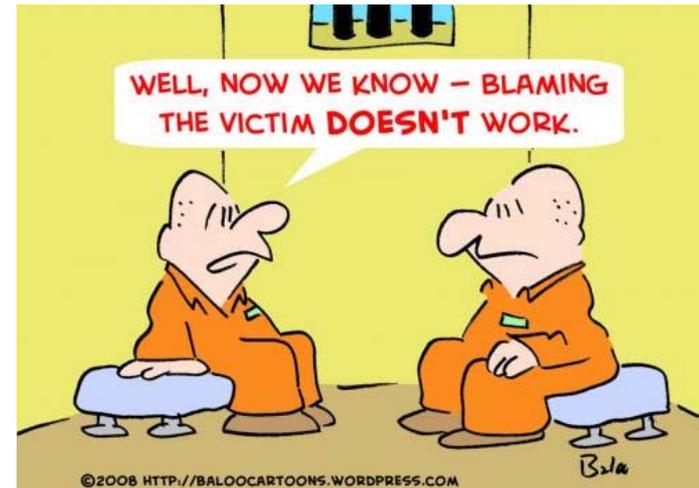
- Despite all the media attention and hype 80% of the people involved in ICS still haven't heard of Stuxnet
- Of those who have, all are still more intrigued and focused as to who and why, then what they should be doing
- Seriousness and proof that our Industrial controls systems can be compromised has not hit home
- Majority of asset owners haven't done anything different since the news broke on Stuxnet



<http://bit.ly/bCVILH>

The blame and excuse game...

- Too much focus on vendor, platform and industry
- Microsoft Windows, zero day vulnerabilities
- ICS owners not patching, firewalling
- Vendors have hard coded passwords
- It only affects Siemens systems...
- The ICS community hasn't taken security seriously or tried to do anything about it



©2008 [HTTP://BALOOCARTOONS.WORDPRESS.COM](http://BALOOCARTOONS.WORDPRESS.COM)

<http://bit.ly/cJgX0d>

Media, Blogs and Speculations...

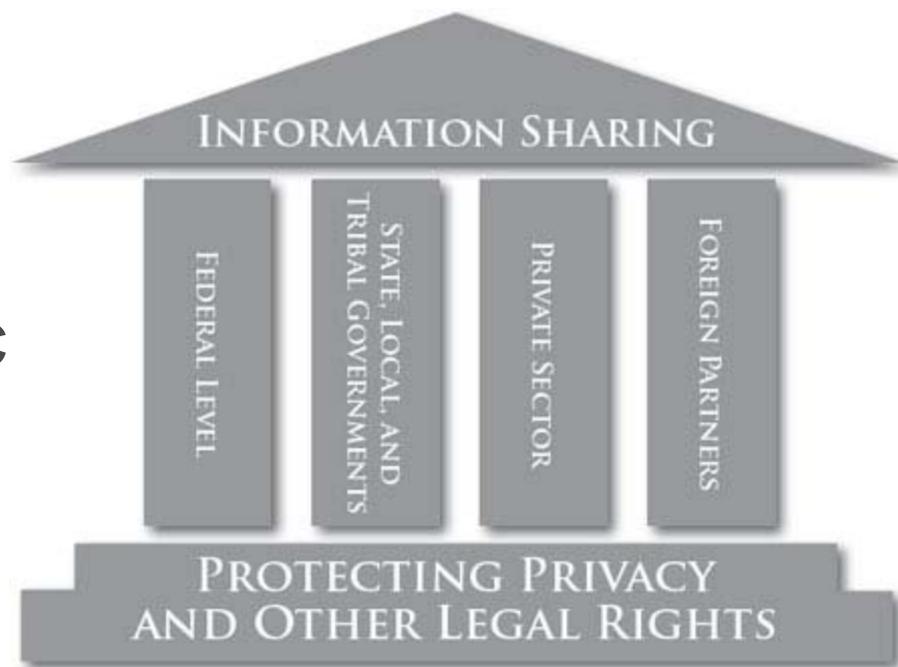
- Too much focus on who created Stuxnet
- “Military grade”, “cyber missal”, “cyberwarfare”
- “Nation State”, “targeting Iran’s nuclear program”
- “Large group with money and intent”
- “Biblical references”, “terrorism”
- “Retribution”, “sophistication”, “aggressive”
“so dangerous”, “designed to blow something up” ...



<http://bit.ly/dnin1j>

Not enough shared on the facts...

- No immediate information about CC, peer to peer, shares or the seven other ways it could move about
- No information about the 4 MS- zero day vulnerabilities
- No Information about the fact it looks for and disable AV
- No information about the PLC wrapper capabilities
- No information about the encrypted payloads



<http://bit.ly/9eW8H1>

Foundations of the National Strategy for Information Sharing

Asset owners still hiding their heads in the sand

- There are thousands of threats that could compromise a control system, and asset owners and vendors need to take that fact seriously
- With known drones, APT capable worms and Botnets, its likely that your system is already compromised and owned by an adversary
- Regardless of who or why Stuxnet is proof that it can happen and you are probably not even aware of it



<http://bit.ly/a9kUMp>

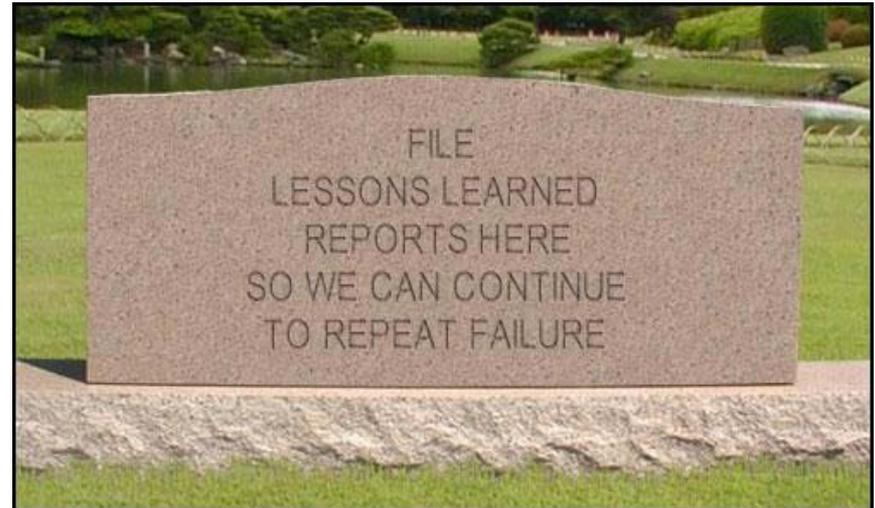
What we're seeing...

- Inter-connectivity (Networking)
- System Openness (COTS)
- Rapidly growing # of devices
- Lack of accountability
- Organizational churn
- Weak or none existing policies
- New systems and complex technologies
- Lack of discipline and change control
- Vendors still not providing security details



What we've learned...

- Being compliant with NERC CIP, WIB, NIST 800, ISO would not have prevented Stuxnet
- Perimeter and data diodes would not have prevented Stuxnet
- Anti-virus would not have prevented Stuxnet
- Air gapping would not have prevented Stuxnet



<http://bit.ly/cBgTc1>

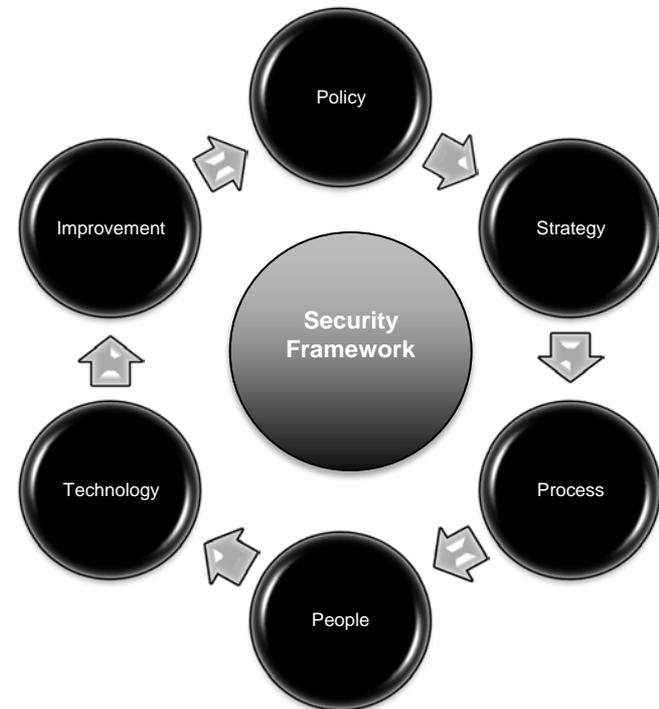
What we're recommending...

- A complete uncompromised understanding of your automation system
- Establishing a secure configuration and system baseline
- Locking down and Denying all access to everything by default
- Deploying multiple security zones to protect every device and service
- “Whitelisting” only known good applications, services and traffic
- Disciplined vigilance on configuration changes and documentation:
 - System configuration and documentation
 - User accounts and access
 - Ports and services
 - Security logging and event reviewing
 - Vulnerability testing
 - Software patching
 - Updating baselines

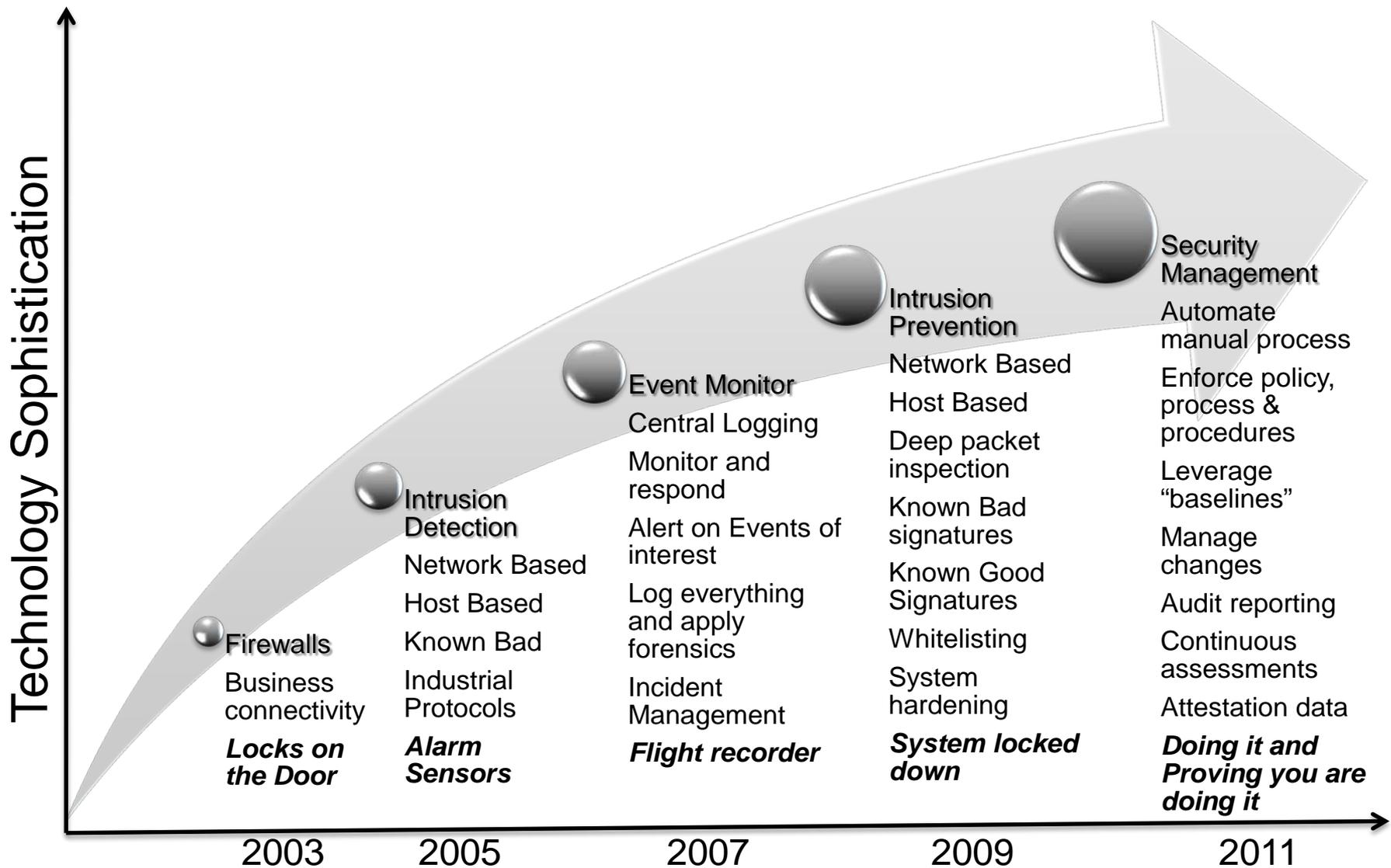


Go back to Security Basics...

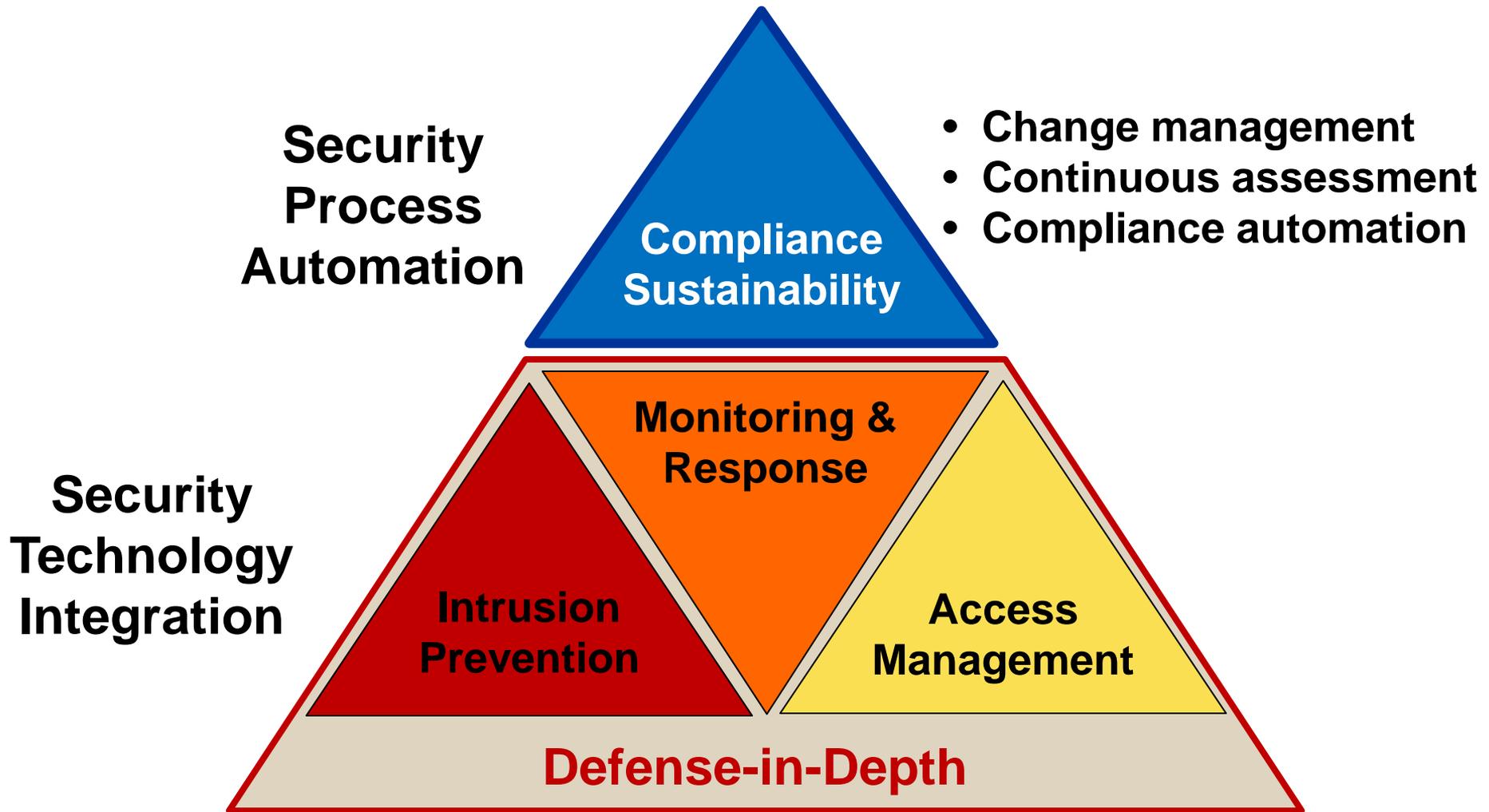
- Catalog of Control System Security <http://bit.ly/91Pinb> 250 controls 44 unique to ICS not in NIST 800-53
- National Strategy for CIP German guide for ICS - <http://bit.ly/biqixQ> broad set of controls inclusive of procurement language
- WIB vendor Security Rev 2 <http://bit.ly/bxilCx> 35 – “Process Areas” grouped into 4 groups
- ISA-99, NERC CIP, ISO 27000, NIST 800-82 ChemITC, IEC 62443-3...
- They are all good and helpful – albeit a lot of work and not cheap...



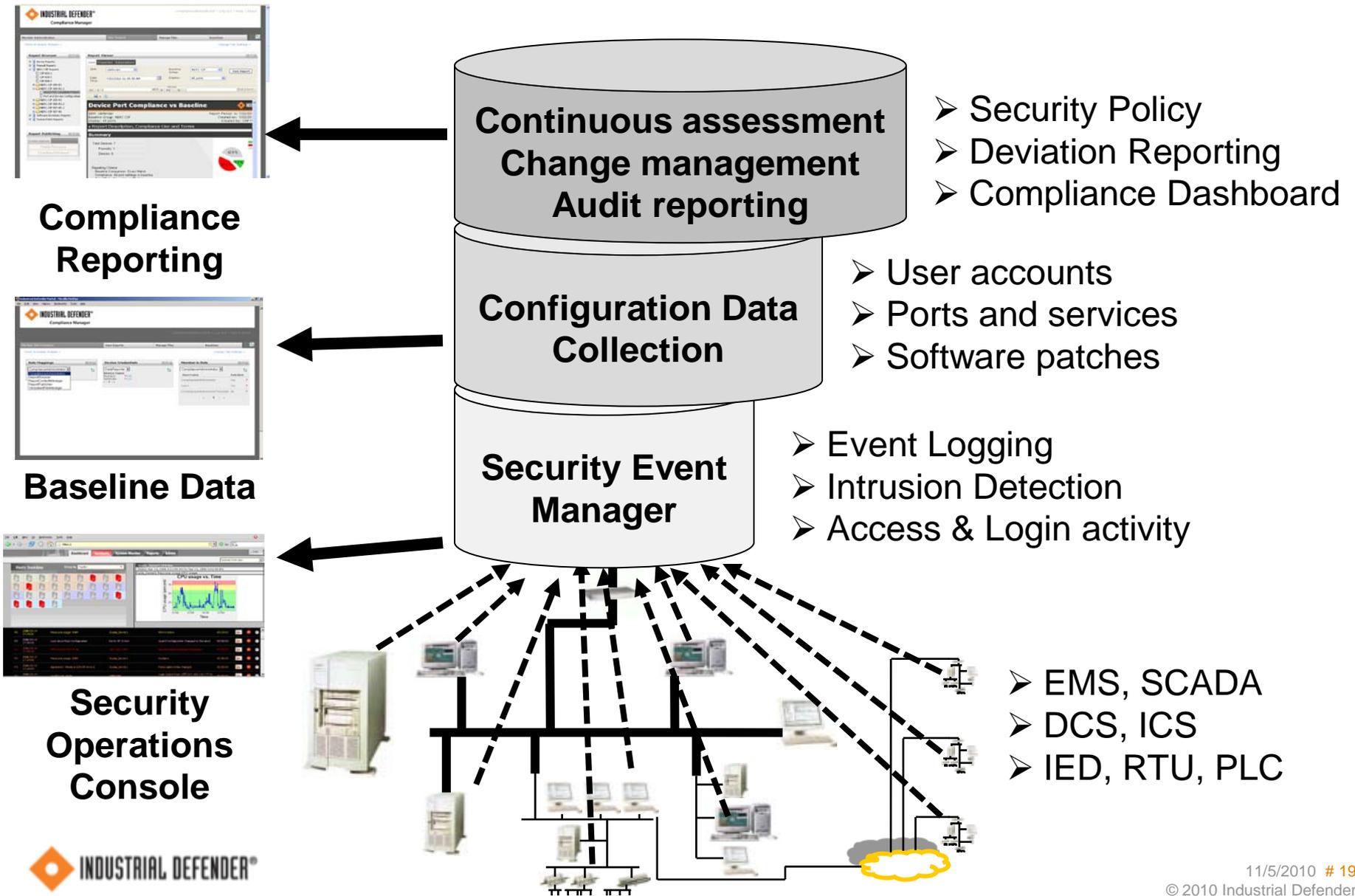
Security Maturity Evolution in ICS



Integrated Automation System Security Management

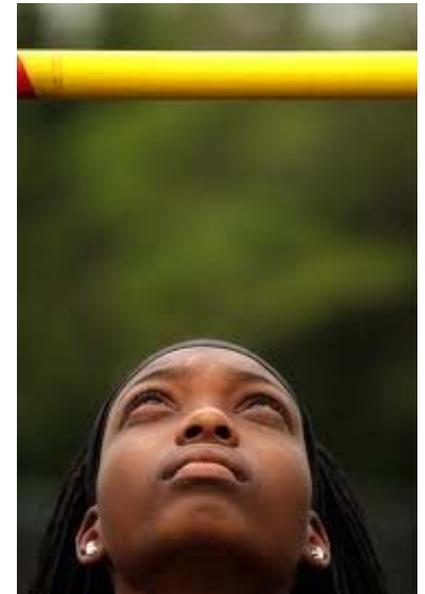


Security Automation



Stuxnet should be an eye opening opportunity...

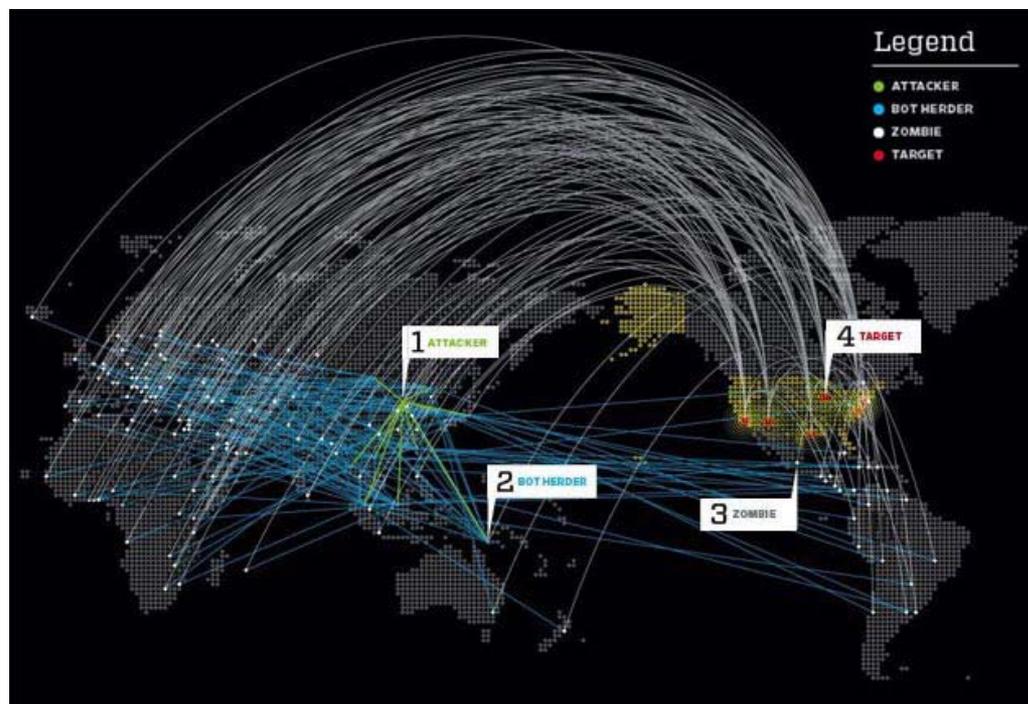
- **Asset owners:** Understanding security's discipline, effort and cost – continue evolving security posture
- **Vendors:** Acknowledging security is not an option for their systems, continue to improve
- **GOV/CERT:** Sharing information and being the “go to” trusted source for the ICS community – more than less
- **Third party Security Vendors:** Innovating and developing more industrial control system specific security solutions and expertise



<http://bit.ly/bL5lrF>

Wrap up...

- Industrial Control Systems are “vulnerable” and are being targeted
- Adversaries are thinking and are working on how to attack your system
- Its very difficult to defend against an attacker, but you can do things to increase your chances...



<http://bit.ly/95JfaG>

Final thoughts you should consider...

- **Re-evaluate security posture in light of changed threat environment**
- **Consider immediately:**
 - Disable USB flash keys or execution of code from flash keys
 - Implement strict egress (outbound connection) filtering on ICS firewalls
- **Consider for short term:**
 - Whitelisting / Host Intrusion Prevention System
 - Tighten up overall security program – look at IT standards for guidance
 - Consider Compliance Management system to help keep security posture strong
- **Consider for long term:**
 - Strong protections for control systems – host hardening, patch programs, regular audits, stronger personnel and physical security measures.
 - Outsource most complex security functions to experts focused on industrial security
- **Develop and maintain a strong defence-in-depth posture**

Layered Security Approach for Vulnerability Risk Assessments



Q & A

Thank you for attending

Walter Sikora

wsikora@industrialdefender.com

(mobile) +1.508.369.5649

Twitter: @nerccip

www.industrialdefender.com

Twitter: @i_defender

Blog/ongoing discussion:

www.findingsfromthefield.com