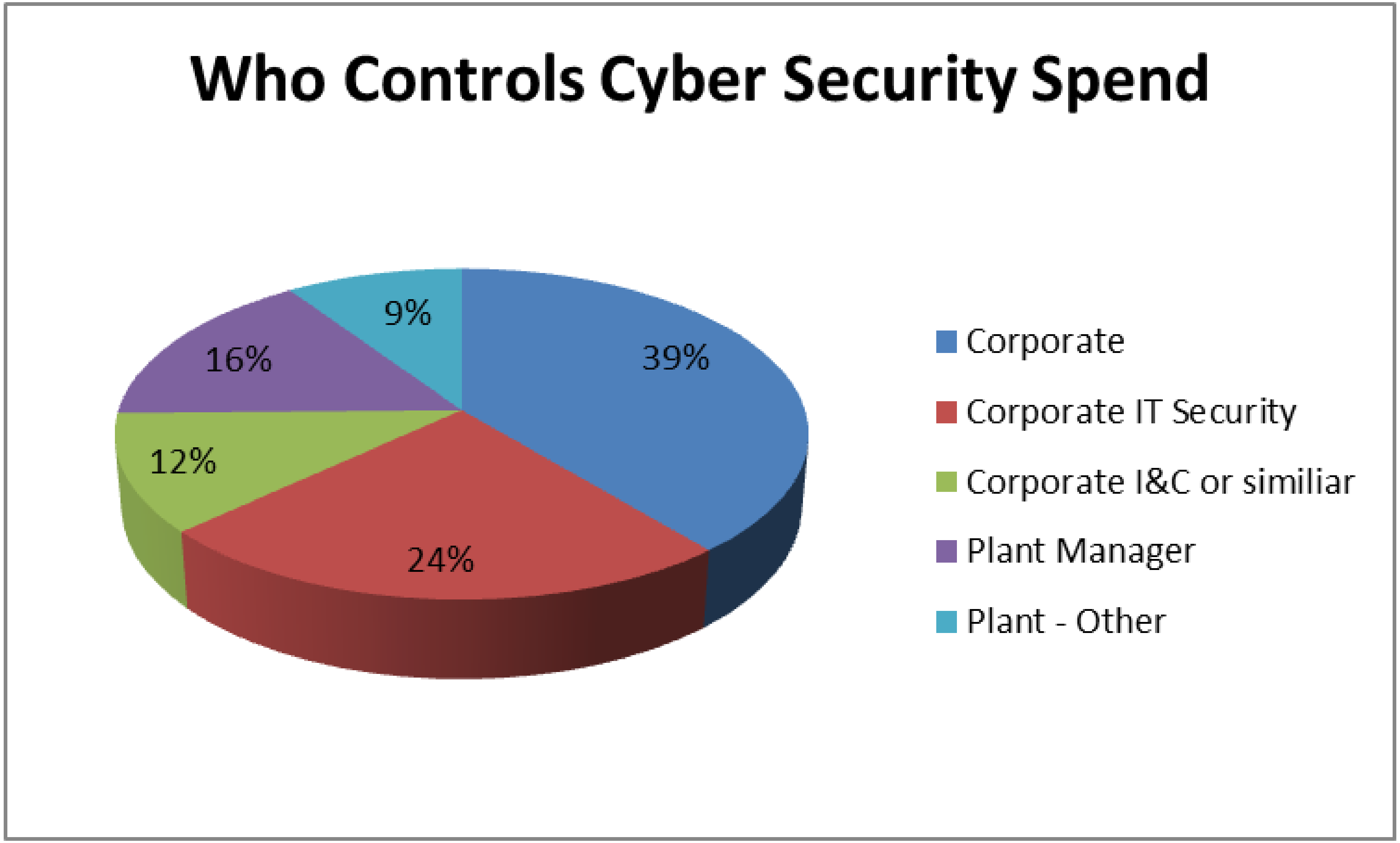
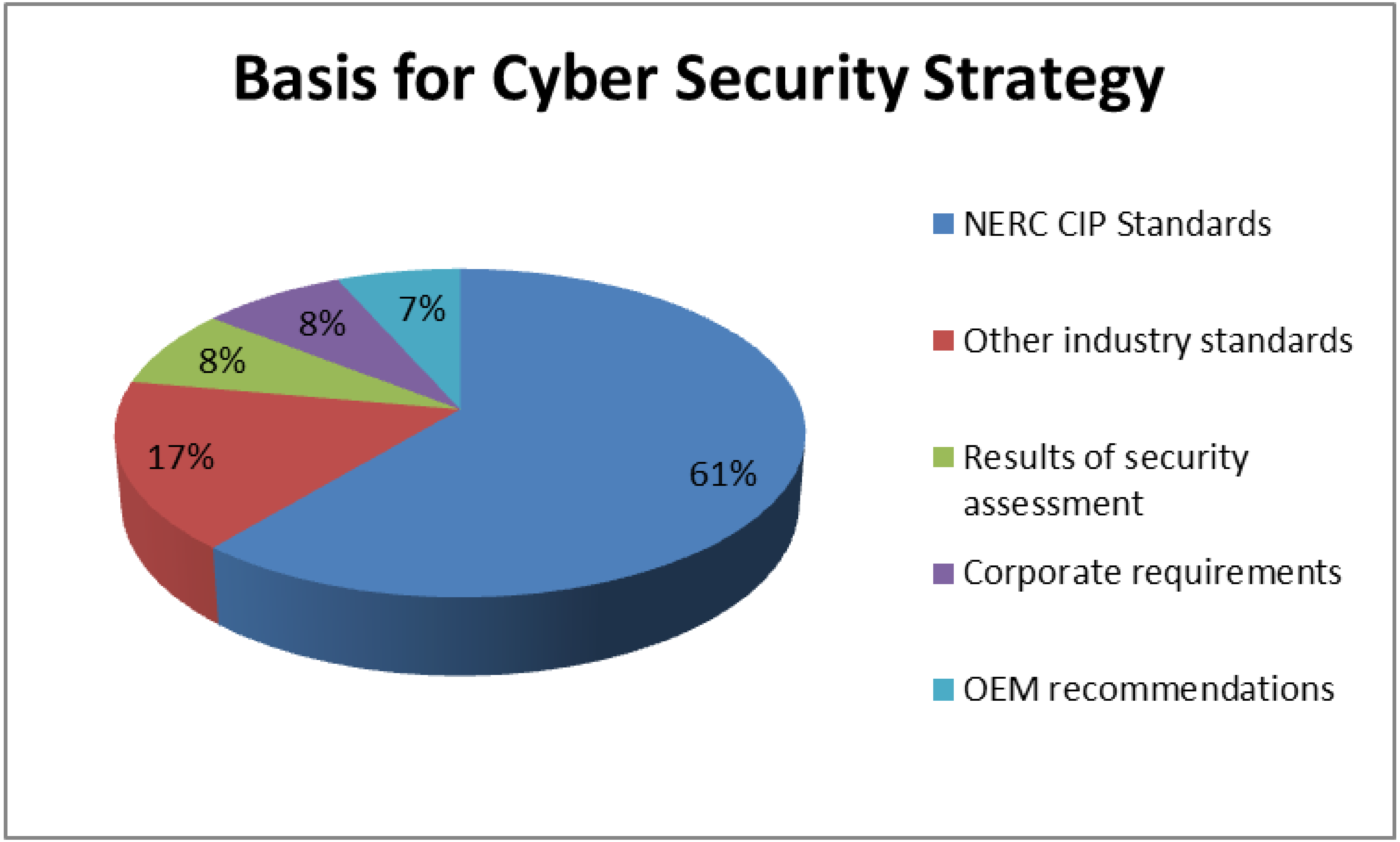
September 25, 2014

ABB Power Generation DCS Users Group
Cyber Security Special Interest Group

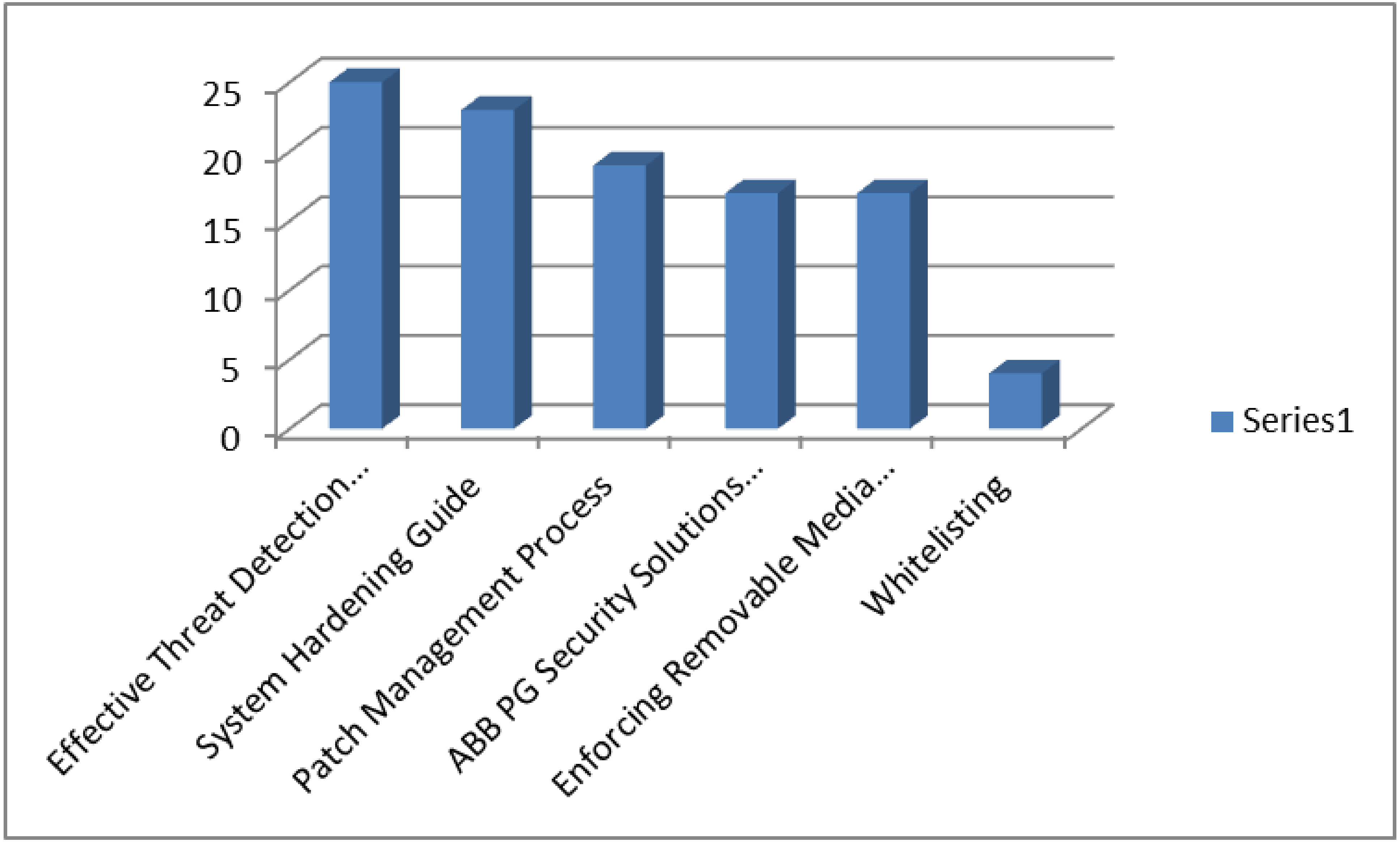
Registration Peer Group Survey



Registration Peer Group Survey



Registration Peer Group Survey – Future Topic



September 25, 2014

ABB Power Generation DCS Users Group
Cyber Security Special Interest Group

Join the ABB DCS Users Group
Share, exchange, and connect with your peers!

- **Website: www.adcsug.com**
- Users of ABB control system products and services industries.
  - Forum to: share experiences, learn and collaborate influence and improve ABB control products and services
- Top 5 reasons to join the group:
  - Networking: true peer-to-peer forums
  - Improvement suggestions: day-to-day challenges discussed and ideas exchanged
  - News: related articles and information from the industry
  - Events calendar: stay connected with users and ABB Power Generation
  - Polls / surveys: express your opinion and make your voice heard
- "The value of a users group, and that in particular of ABB DCS Users Group, is that as a group we have more access and leverage to change and improve the product than as individuals acting alone. It also allows us to participate in discussions that bring the best ideas forward and facilitates sharing information that helps everyone." - Bill Ossman, ABB DCS Users Group STECO member

ABB Power Generation Cyber Security Special Interest Group

Agenda

- Welcome & Introductions
- Power & Utility Industry Intelligence Briefing – Brent Huston
- XP Survival Guide – James Klun
- Thwarting the BadUSB – Joe Catanese
- Audience Q&A - Any security topic of interest
- Response Polling
- Conclude
- Pop-Up Response Survey (5-minutes of your time)

Today’s Panel

- Mike Radigan, Senior Advisor, Cyber Risk Management, ABB PSPG
  - Mike.Radigan@us.abb.com (614) 398-6241
- Brent Huston, Security Evangelist & CEO, MicroSolved, Inc.
  - @lbhuston
- James “Jim” Klun, Security Engineer, MicroSolved, Inc.
  - jklun@microsolved.com
- Joe Catanese, Application Engineer, ABB Power Generation
  - joseph.p.catanese@us.abb.com

ABB Power Generation Cyber Security Special Interest Group

Agenda

- Welcome & Introductions
- **Power & Utility Industry Intelligence Briefing – Brent Huston**
- XP Survival Guide – James Klun
- Thwarting the BadUSB – Joe Catanese
- Audience Q&A - Any security topic of interest
- Response Polling
- Conclude
- Pop-Up Response Survey (5-minutes of your time)

XP Survival Guide

Staying alive with a target on your back

XP: You have it – and it can’t be maintained.

- Microsoft’s Windows XP operating system is pervasive in ICS/SCADA.
- It’s often the “man behind the curtain” – unseen but integral
- Born – April 2001. Died – April 2014. NO MICROSOFT SUPPORT!
- No maintenance of any type – not just “security” maintenance.
- It amounts to a poorly understood component of your environment that – when it breaks (and it will) – cannot be maintained.
- Not only “cyber threats” – any change in your environment that is incompatible with XP poses the risk of an outage.

What to do?   Ideally…

- Upgrade to a supported environment.
- Contact your vendor!
- The new environment should be one that learns from the XP lesson
- That lesson?   Commercial software has a “short” – by industrial standards - lifespan.
- Make sure there is ALWAYS a non-disruptive upgrade path. Ask!
- Plan for ‘end-of-life’.

And if you’re stuck in the XP muck?

Survive!

- Find your XP systems – some will be hidden behind HMI’s etc.
- Scanning:
  - There are “active” tools that can scan networks and identify systems and associated operating systems.
  - **There is risk** – some ICS have components that will lock up on such scans
  - **Passive scans** can tap network traffic without interference – no risk to running systems.
  - They simply watch the traffic - like standing on a river bank and watching the water go by. NO interference.
  - XP systems will reveal themselves by the pattern of traffic they produce.

Passive scanning

- Nessus Passive Vulnerability Scanner – commercial
  - http://www.tenable.com/products/passive-vulnerability-scanner/features
- P0F – open source tool (i.e. free beer!)
  - http://en.wikipedia.org/wiki/P0f

- Both only observe from the side – low risk.
- If an XP device is on the network and produces any traffic, it will be found.
- IT staff can do this… but you must control.

You found them – now what?

- Keep the inventory current – no changes without documentation!
- Are all your XP systems needed? Get rid of any that are not.
- Can they be moved out of the ICS environment?
  - <u>Keep stuff NOT ICS related **OFF** ICS networks</u>.
- Can they be taken down for a while?
  - Get to most current vendor supported maintenance levels.
  - Remove any unneeded software
  - Remove any unneeded network exposures – often same as previous
  - See the paper for details
- Use your IT folks for all this – communicate with them.

Segmentation

- As discussed in the paper, uniquely susceptible systems (read: XP) should be isolated in a way that minimizes the chance for bad stuff to get in.
- If at all possible, ICS network areas with XP present should be isolated from the rest of the ICS and business worlds.
- Software and hardware firewalls are potential ways to do this
- The paper has details on possible solutions

Detection - Technical

- All modern operating systems have some level of logging capability.
- That includes XP
- Those logs can be automatically sent to a central repository for analysis
- It does involve changes to the XP configuration and the addition of new network traffic – so there is some risk. Talk to IT.
- The paper has a discussion

Detection – Human

- **THIS IS THE BIG ONE!**
- Lack of communication within organizations is the biggest reasons what should be minor problems turn in to major ones.
- All staff (yours, vendor's, etc) must be trained to report anomalies in behavior of ICS systems 7X24 to a central group.
- That group should understand ICS and IT environments and have the necessary skills to collect and analyze data and the authority take action.

Summary

The “XP Survival Guide” paper elaborates on all this.

If you get anything out if it, get this:

- Communicate with your vendors
- **Ensure a trust relationship exists between your OT and IT groups.** Without that you have a problem a lot bigger than XP.

ABB Power Generation Cyber Security Special Interest Group

Agenda

- Welcome & Introductions
- Power & Utility Industry Intelligence Briefing – Brent Huston
- XP Survival Guide – James Klun
- **Thwarting the BadUSB – Joe Catanese**
- Audience Q&A - Any security topic of interest
- Response Polling
- Conclude
- Pop-Up Response Survey (5-minutes of your time)

Security Workplace
Removable Media Protection

RISK ASSESSMENT / SECURITY & HACKTIVISM

This thumbdrive hacks computers. “BadUSB” exploit makes devices turn “evil”

Researchers devise stealthy attack that reprograms USB device firmware.

- by **Dan Goodin** - Jul 31, 2014 9:21am EDT

White-hat hackers have devised a feat even more seminal—an exploit that transforms keyboards, Web cams, and other types of USB-connected devices into highly programmable attack platforms that can't be detected by today's defenses.

Dubbed BadUSB, the hack reprograms embedded firmware to give USB devices new, covert capabilities.

Odix Engine Principle

- Odix core technology contains a proprietary algorithm which eliminates and destroys both known and **unknown** malware attacks.
- The patented algorithm is suited for each type of file and removes any malware that resides within the file. No detection is required!
- The innovative algorithms exhibit a totally new approach to cyber defense which proactively protect against current and **future attacks**.

Security Workplace
Removable Media Protection

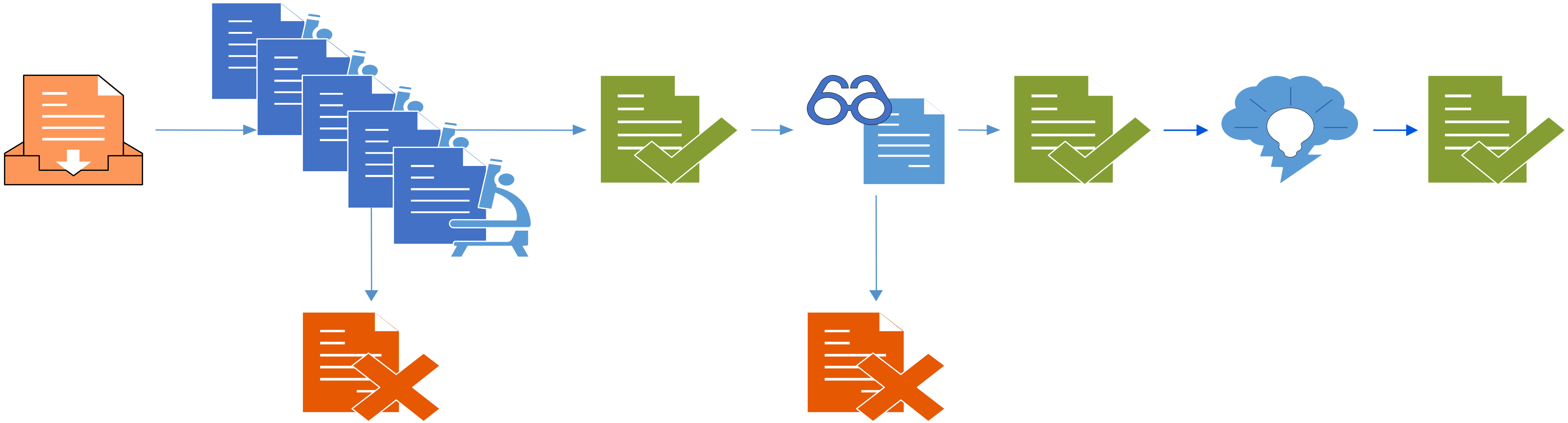
FILE SANITIZER Process

File Begins
SANITATION
Process

Five AntiVirus Solutions are applied to the incoming file
.

File True Type Tests are run to make sure the File is what it is supposed to be. Selected files are run in Sandbox.

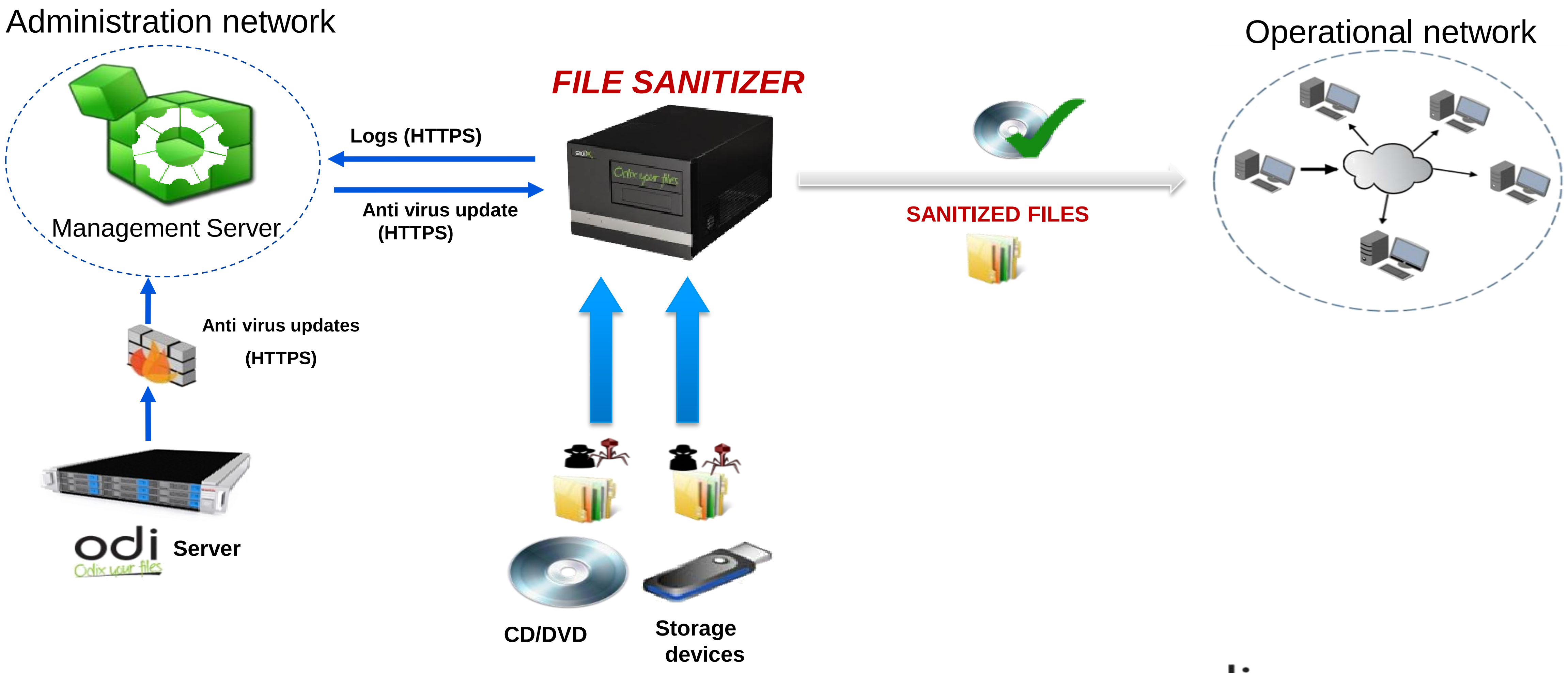
File is SANITIZED through the odi algorithms.



Powered by odi

Security Workplace
Removable Media Protection

Process for Trusted File Transfer



Administration network

Operational network

FILE SANITIZER

Logs (HTTPS)

Anti virus update (HTTPS)

Management Server

SANITIZED FILES

Anti virus updates

(HTTPS)

odi Odix your files Server

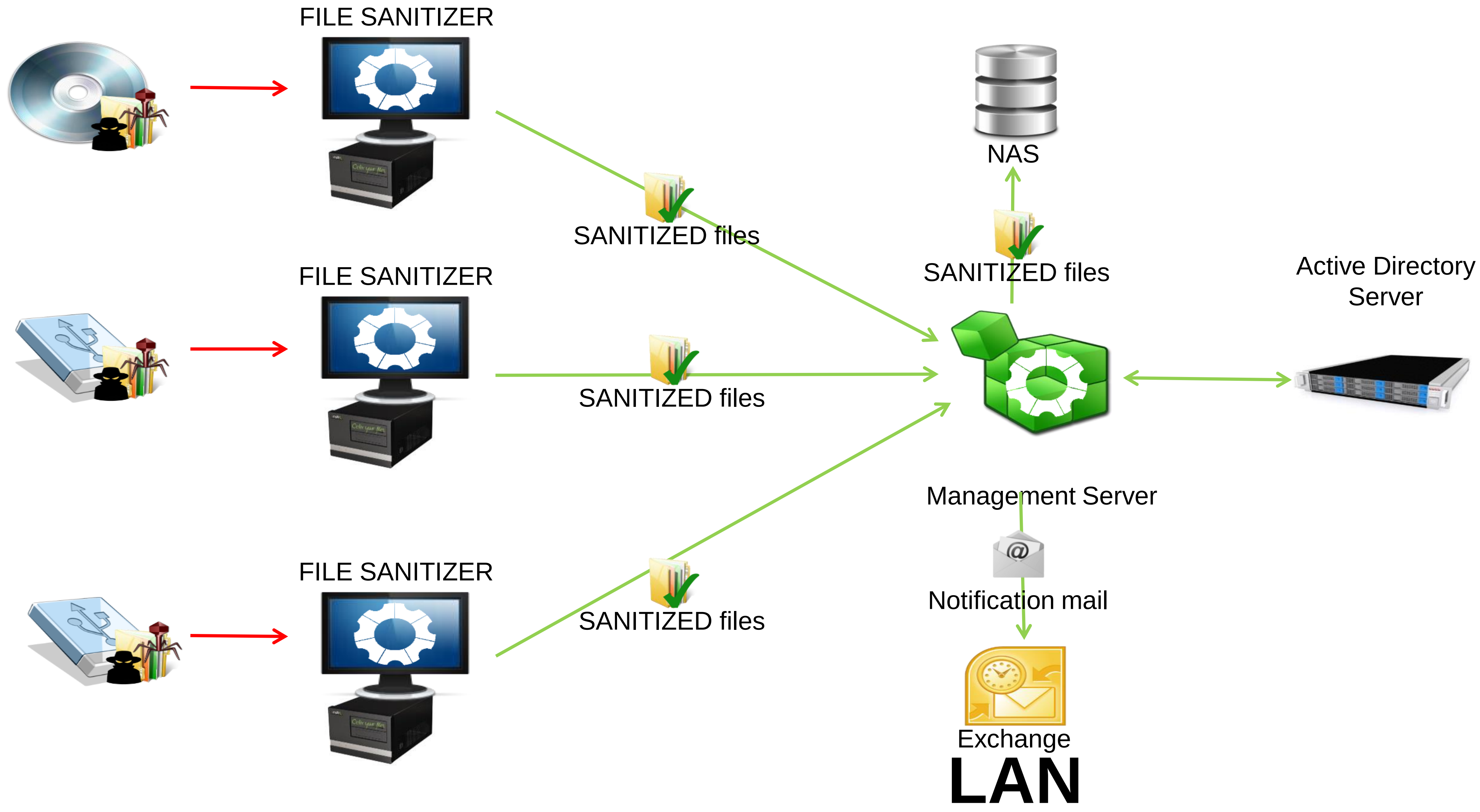
CD/DVD

Storage devices

Powered by odi Odix your files

ABB

File Flow of FILE SANITIZER



ABB

Security Workplace
Reliability – Security – Compliance

Security Workplace

MAINTAIN

- System Hardening
- User Access Control
- MS Patches, Anti Virus, Patch Disk
- **Centralized Microsoft Patching***
- Centralized Anti-Virus Management
- Automated Backup and Recovery
- **Removable Media Protection (ODI-X)***

DEFEND

- **Detect-in-Depth (HPSS + SOPHIA)***
- NIDS (Network Intrusion Detection)
- Security Event Monitoring
- **Application Whitelisting ***
- Configuration Change Management
- IT Asset Management

COMPLY

- Automated Data Collection
- Automated Compliance Reporting
- Workflow Automation Suite

* Indicates product is in managed release

Security Workplace
Removable Media Protection

NERC CIP v5 CIP-010-2 R4

Responsible Entity shall:

- 3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets
- 3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

Security Workplace
Reliability – Security – Compliance

Security Baseline Requirements	MAINTAIN	DEFEND	COMPLY
ServiceGrid support contract	✓	✓	✓
Automated backup & recovery	✓	✓	✓
ServiceGrid Cyber Security Patch delivery	✓	✓	✓
System hardening	✓	✓	✓
Managed anti-virus deployment	✓	✓	✓
Managed Microsoft patching deployment	✓	✓	✓
Proactive Security Measures			
Electronic perimeter protection*		✓	✓
Security event management*		✓	✓
ICS asset management*		0	✓
Configuration change management*		0	✓
NERC CIP Compliance			
Automated data collection*			✓
Automated compliance reporting*			✓
Policy management*			✓

*Available for Fleet-Wide and Multi-Vendor Control Systems

**Active ServiceGrid contract required

✓= Included 0= Available as an option

Power and productivity
for a better world™