

# RSA<sup>®</sup>Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: SBX1-W05

## How to Get into ICS Security



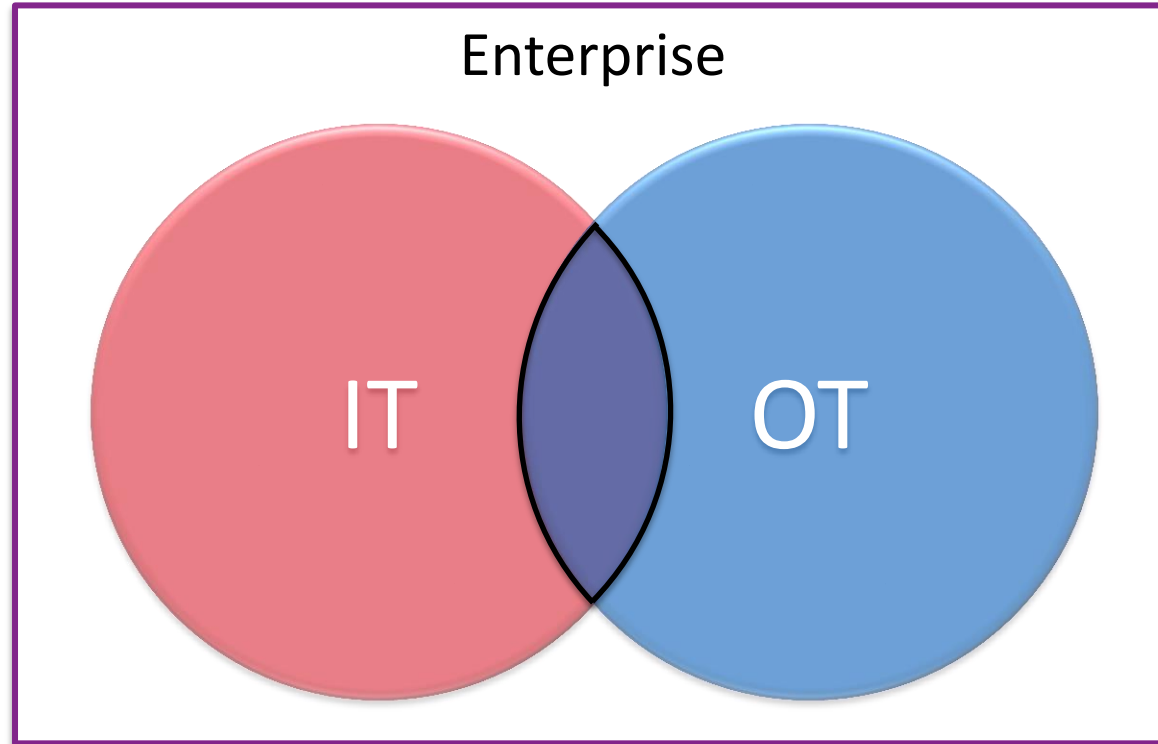
Connect **to**  
Protect

**Chris Sistrunk**

Senior ICS Security Consultant  
Mandiant  
@chrissistrunk



#RSAC



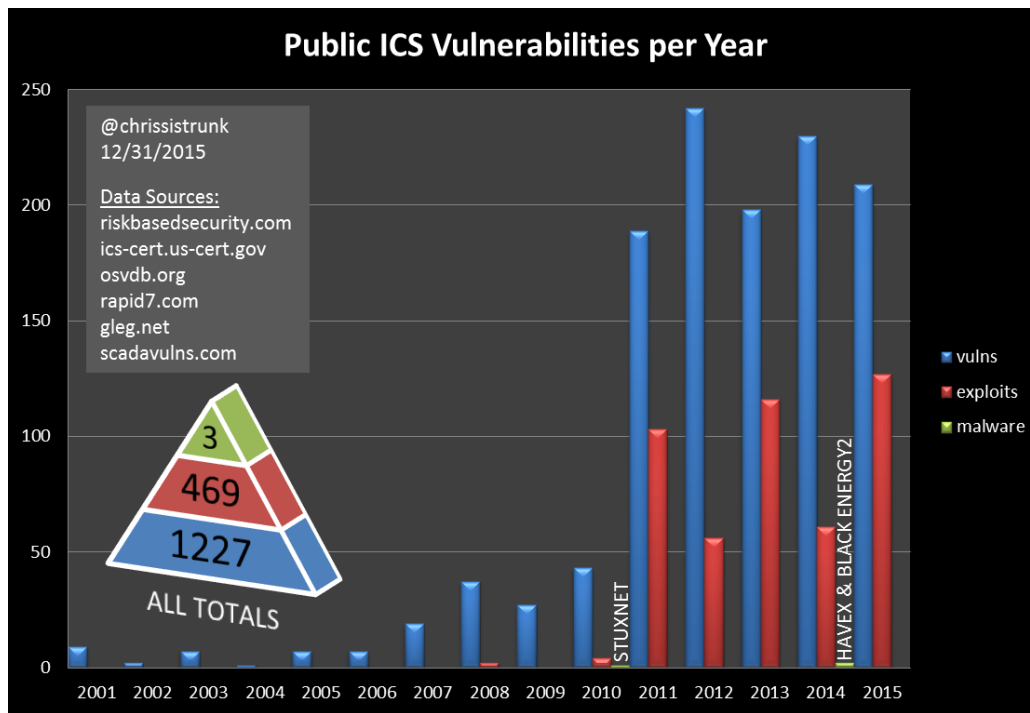


# So...what would you say you do here?



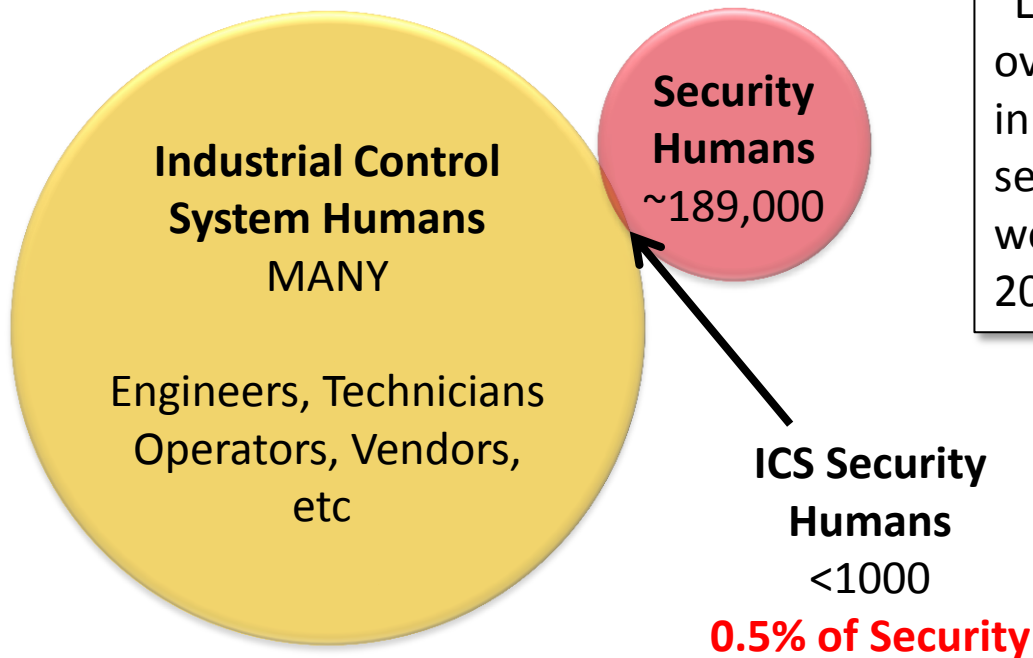
- Why are you here?
- What excites you about ICS security?
- Is ICS or security in your job now?
- Do you want it to be?

# Some numbers





# Some numbers



“LinkedIn data identified over 189,000 professionals in active information security positions worldwide as of June 2015.” - Cory Scott

# Is 0.5% enough to protect Critical Infra?



#RSAC





# I'm recruiting you for ICS Security



# WE WANT YOU



OT Side > ICSsec





# Operational Technology

- You've got the engineering or technical background
- You know how the plant or process works
- You probably already work with:
  - ICS components like PLCs and RTUs
  - ICS protocols like Modbus, Ethernet/IP, DNP3, etc
  - Networking (ethernet, serial, including wireless)
  - NERC/CIP or CFATS requirements



# Get familiar with security

- Learn
  - Security Conferences!
  - Lots and lots of security material online (SecurityTube, etc)
  - Security Training (ICS-CERT, SANS ICS, Red Tiger, SCADAhacker)
  - SamuraiSTFU, Kali, Security Onion Linux Distros
  - shodan.io
- Make friends with the IT Security team



# Make an ICS Security Lab

- Many companies with control systems have labs
- If not, you may have spare equipment laying around...get creative!



# So...Stuxnet happened



#RSAC





# What would be your Stuxnet?

- Think like a bad guy...with a hard hat!
- ...like an attacker has your prints
- Who knows...you might find a vulnerability

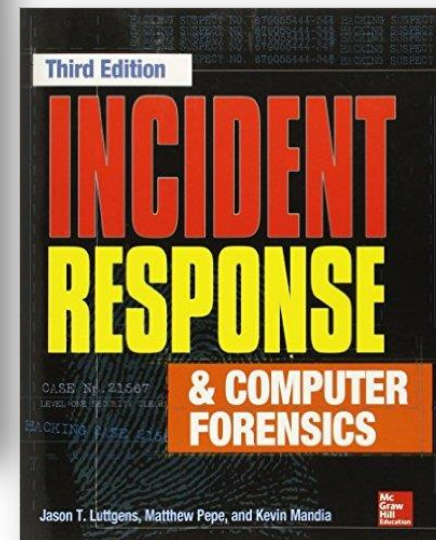
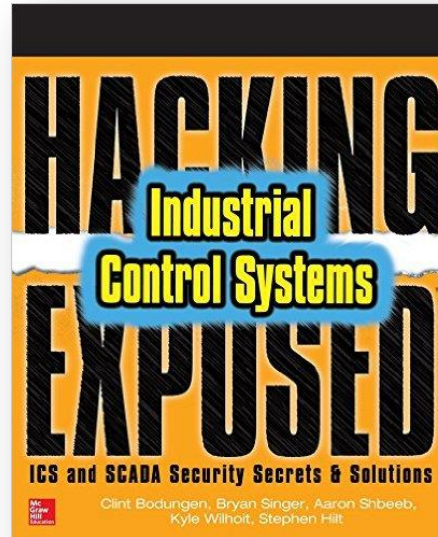
“To make things work well, you must break them”

“Find evil, or ways for evil to do evil”



# Red Team and Blue Team

- Learn how to use Metasploit
- Search shodan.io
- Learn about Modbus Fuzzing
- Write some Snort rules
- Read up on Digital Forensics & Incident Response (DFIR)





# Red Bull



#RSAC





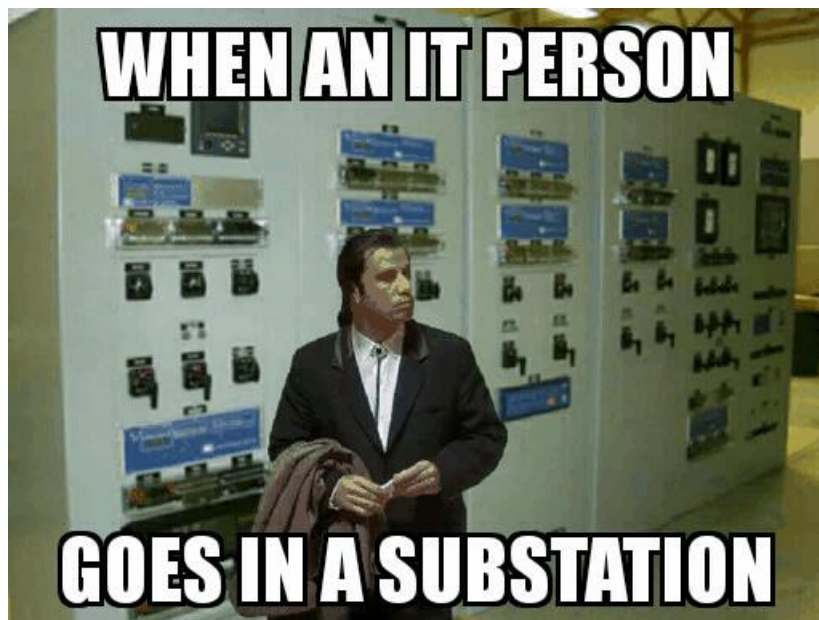
# Get to know your IT Security gurus







#RSAC





IT Side > ICSsec



# Information Technology

- You've got the computer and networking skills
- You know how business technology work
- You probably already know:
  - Routers, switches, firewalls, domain controllers
  - Web, email, and business applications
  - Certifications like CCNA and CISSP
  - HIPAA or PCI DSS requirements



- <https://www.youtube.com/watch?v=RXJKdh1KZ0w>





# Google all the things

- Modbus.org > modbus specification
- Tons of code on github: opendnp3, modbus, etc
- Wireshark
- Pcaps online > Netresec has a library, SANS, S4

# Videos



#RSAC

- YouTube & Vimeo
- “SCADA”
- “Control Systems”
- “PLC”
- Conference Talks
- “How It’s Made” Marathon!





# Make an ICS network at home

- Raspberry Pi
  - opendnp3, modbus, BACnet
- Arduino
  - modbus
- \$15 HMI from eBay (got lucky)
- ~\$700 for a new Phoenix Contact PLC





# You know security, but not ICS...yet

- What I am about to tell you is the single greatest secret to go from IT Security into ICS...



# Donuts



#RSAC



# Get your hardhat dirty



## LITTLE BOBBY



by Robert M. Lee and Jeff Haas





## **ICS Security Resources**









- SCADAsec email list at Infracritical
- ICS Security Conferences
  - DigitalBond's S4
  - SANS ICS Summit
  - 4SICS
  - EnergySec
  - Oil & Gas Security Summit
  - ICS Cyber Security Conference "Weisscon"



# Information Sharing

## National Council of ISACs

-  Downstream Natural Gas [www.dngisac.com](http://www.dngisac.com)
-  Electricity [www.esisac.com](http://www.esisac.com)
-  Oil & Natural Gas [www.ongisac.org](http://www.ongisac.org)
-  Water [www.waterisac.org](http://www.waterisac.org)

ISAOs coming, knowledge sharing, ICS-ISAC, “BEER-ISAC”



# Books

- Robust Control System Networks, Ralph Langner
- Industrial Network Security, 2nd Edition, Knapp & Langill
- Cybersecurity for Industrial Control Systems, Macaulay & Singer
- Countdown to Zero Day, Kim Zetter

## ***Coming soon!***

- Handbook of SCADA/Control Systems, 2nd Ed., Radvanovsky & Brodsky
- Hacking Exposed Industrial Control Systems, Bodungen, et al



# Intelligence Sources

- ICS-CERT portal
- ISAC portals
- FBI Infragard
- iSight Partners
- Twitter #ICS #SCADA
- Google

iSIGHT Partners > Blog > Sandworm Team and the Ukrainian Power Authority Attacks

## Sandworm Team and the Ukrainian Power Authority Attacks

By John Hultquist January 7, 2016 iSIGHT Partners



SANDWORM TEAM

### Update 1.11.16 – SANS ICS Team Connects Dots

Updating the blog entry to bring attention to the recent analysis by Mike Assante from the SANS ICS team.

"After analyzing the information that has been made available by affected power co researchers, and the media it is clear that cyber attacks were directly responsible for Ukraine. The SANS ICS team has been coordinating ongoing discussions and providing multiple international community members and companies. We assess with high confidence that the incident was an intentional attack."

Read the [full SANS post here](#) – and see below for iSIGHT

### iSIGHT Partners Analyst Comment

The SANS ICS blog confirms conclusions previously reached by iSIGHT regarding the Ukrainian attacks (specifically the role of destructive malware and phone disruption) and attribution to

**CSMPasscode** @CSMPasscode · Feb 1  
#blackenergy malware evolved from a 2007 piece of crappy Russian malware. It's no Stuxnet, says @RobertMLee. #CyberUkraine

**Hacker Samurai** @HackerSamurai\_ · Feb 1  
Infection by #malware such as #BlackEnergy on infrastructure system has potential to be #catastrophic | #Cylance [ow.ly/XNxzq](#)

**BlackEnergy and the Ukraine: Signals vs. Noise**  
Fear of hackers causing real-world damage has long been part of Hollywood's history. We've watched these movies for decades and become almost numb to it. But ... [blog.cylance.com](#)

**Cyber Guy** @The\_Cyber\_Guy · Feb 1  
#BlackEnergy and the #Ukraine : Signals vs. Noise [ow.ly/XNBDJ](#)

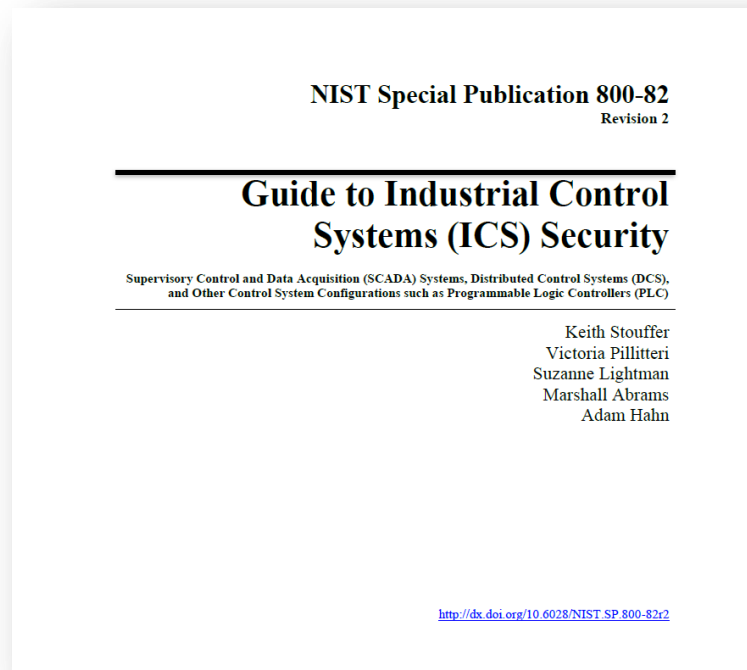
**Cyber Alliance** @A1\_Cyber · Feb 1  
Word up: #BlackEnergy #SCADA #hackers change tactics [ow.ly/XNuwp](#)

**Ridgway Center** @Ridgway\_Ctr · Feb 1  
Group behind the #cyber attacks against #Ukraine is spreading #BlackEnergy malware through #Word documents. [securityaffairs.co/wordpress/4403...](#)

**ATP group uses Word Docs to drop BlackEnergy M...**  
The ATP group behind the recent cyber attacks against critical infrastructure in Ukraine is spreading BlackEnergy malware through specially crafted Word documents. [securityaffairs.co](#)



- NIST SP800-82 Revision 2
- IEC 62443
- NERC/CIP
- CFATS
- ...to name a few





- ICS-CERT
  - Free online training and resources
  - Free 5-day Red vs Blue ICS exercise
- ICS Vendor Training
- SANS ICS410 and ICS515
- Red Tiger Security, Lofty Perch, SCADAhacker



# Certification



#RSAC

- There isn't a Professional Engineering license for Security...  
...but not everyone is an engineer.
- GICSP is a new certification out to teach IT folks the basics of ICS and OT folks the basics of security.





# Links

- <https://ics-cert.us-cert.gov/Standards-and-References>
- <http://dx.doi.org/10.6028/NIST.SP.800-82r2>
- <https://scadahacker.com/library/index.html>
- <http://www.dhs.gov/dhs-daily-open-source-infrastructure-report>
- <http://news.infracritical.com/mailman/listinfo/scadasec>
- <http://scadaperspective.com/>
- <http://pen-testing.sans.org/holiday-challenge/2013>
- <http://www.netresec.com/?page=PcapFiles>
- <http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp>
- <https://www.shodan.io/explore/category/industrial-control-systems>



# You're still here

- What excites **you** about ICS security?
- Do **you** want to join us in ICS security?



WE WANT YOU



# Apply What You Have Learned Today

- Next week you should:
  - Identify critical components within your ICS network
  - Find out if they have any published security vulnerabilities, or if they are connected to the IT network, or even the Internet
- In the next three months:
  - Understand who is accessing the ICS, from where, and why
- Within six months you should:
  - Drive an implementation project to protect the most critical ICS devices
  - Develop a roadmap to enhance ICS security architecture
  - Capture some ICS network traffic and look for “evil”



**Thank you!**  
**Questions?**