Adventium LABS

SCADA System and Technology Issues "Your SCADA and business is under attack! What are you doing about it?"

Brian Isle
Senior Fellow
Adventium Labs
&
University of Minnesota
Brian.isle@adventiumlabs.com

Agenda

- Setting the stage
- What did Stuxnet, Duqu, & Shamoo tell us?
- The security path forward

© 2014 Adventium

Setting the Stage – Cyber War

- **Criminal and Nation-State exploitation for financial gain, collection of intellectual property, and exploitation of U.S. infrastructure is where the "game" will be played over the next 5 years.**
- **Cyber space is a level playing field.**
- **The adversary is good at the "game", adapts quickly, and is in it for financial gain and positioning for the future.**

"The Nation-States will attack the C-level, and they will succeed! Put plans in place to mitigate the damage." FBI Section Chief Peter Trahon, Section Chief of the Cyber National Security Section

© 2014 Adventium

What is“SCADA?”

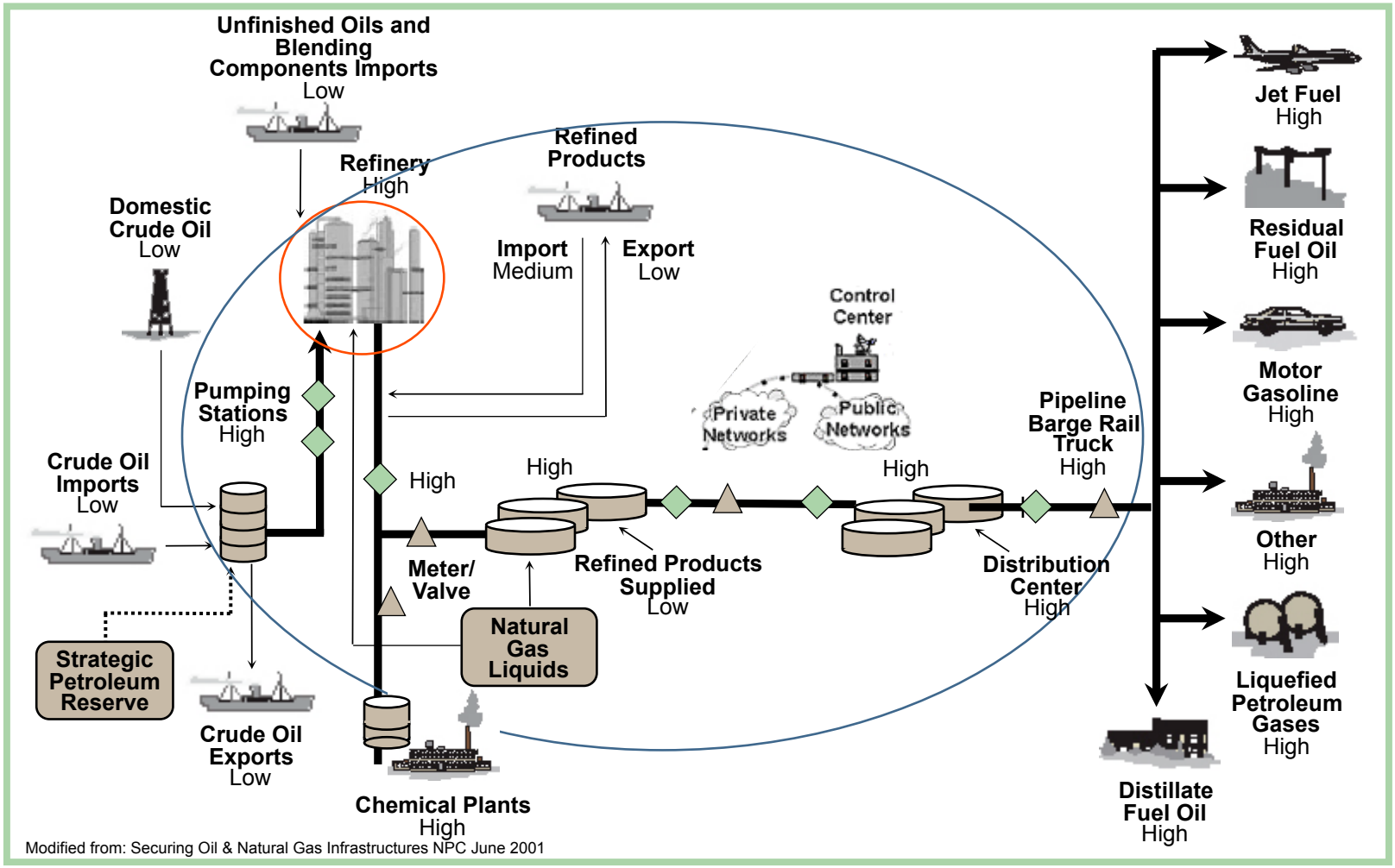
- SCADA is “Supervisory Control and Data Acquisition” – realtime industrial process control systems used to centrally monitor and control remote or local industrial equipment such as motors, valves, pumps, relays, etc.
- SCADA is used to control chemical plant processes, oil and gas pipelines, electrical generation and transmission equipment, manufacturing facilities, water purification and distribution infrastructure, etc.
- Industrial plant-scale SCADA is also referred to as
  - “Distributed Control System” or DCS
  - “Industrial Control System” or ICS
  - “Industrial Automation & Control System” or IACS

Joe S”t Sauver, Ph.D, NLANR/Internet2 Joint Techs Me”eting, Columbus OH, July 21, 2004

The vulnerabilities are the same across SCADA, DCS, and ICS.

© 2014 Adventium

Oil Infrastructure



SCADA is literally what makes the critical infrastructure function.

© 2014 Adventium

Chocolate Bayou Chemicals Complex

The 2,400-acre Chocolate Bayou Chemicals Complex—home to the second largest hydrocarbons cracker in the U.S.—is located 45 miles south of Houston near the Gulf of Mexico. The plant manufacturers two main product lines—olefins and polypropylene—and ships product by rail, roadway, pipeline and barge.

http://www.ineos-op.com/26-Chocolate_Bayou_Works.htm

SCADA is everywhere, from metro transit to refineries.

© 2014 Adventium

How Wide Spread is SCADA?

"On Christmas Eve not long ago, a call was made from a prison warden: all of the cells on death row popped open. Not sure how or if it could happen again, the prison warden requested security experts to investigate. Many prisons and jails use SCADA systems with PLCs to open and close doors. As a result of Stuxnet academic research, we have discovered significant vulnerabilities in PLCs used in correctional facilities by being able to remotely flip the switches to "open" or "locked closed" on cell doors and gates. ……."

SCADA & PLC VULNERABILITIES IN CORRECTIONAL FACILITIES
White Paper, Newman, Rad, LLC, Strauchs, LLC, 7/30/2011

SCADA is everywhere, including your local jail.

© 2014 Adventium

SCADA & Data Security - CIA

Common security framework for data security:

- **Availability:** "Ensuring timely and reliable access to and use of information..." A loss of *availability* is the disruption of access to or use of information or an information system.
- **Integrity:** "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity..." A loss of *integrity* is the unauthorized modification or destruction of information.
- **Confidentiality:** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..." A loss of *confidentiality* is the unauthorized disclosure of information.

FISMA Definition [44 U.S.C., Sec. 3542] FIPS 199 Definition

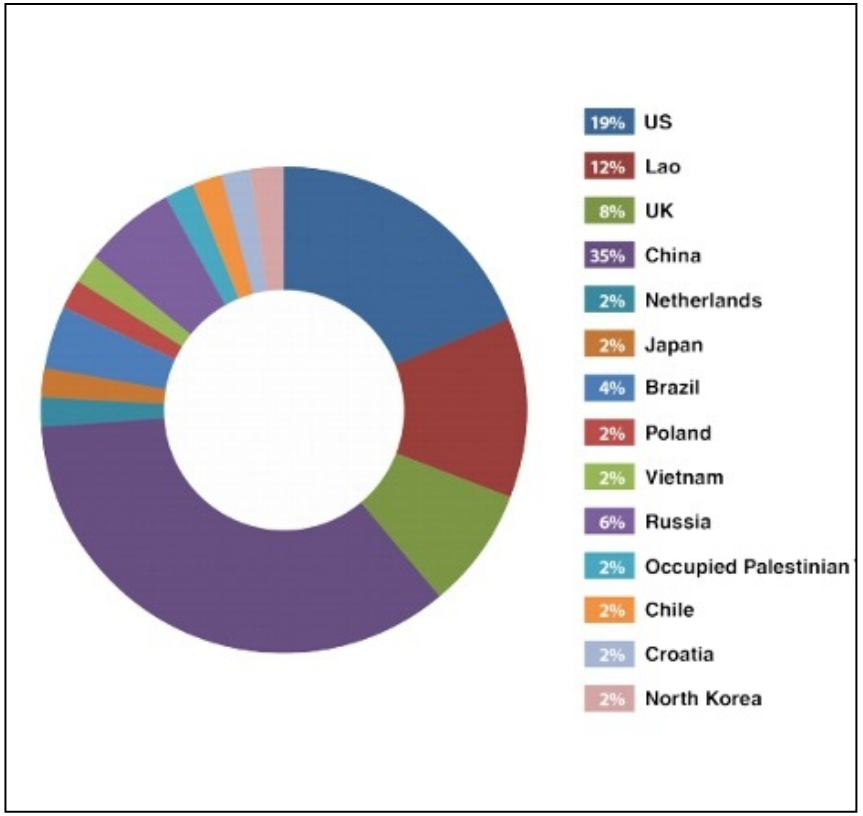
Broadly accepted in the process industry is that plant safety, efficiency, and effectiveness dictate that data integrity and availability are paramount.

© 2014 Adventium

ICS are of Interest to Nation States & Criminals

ICS Honeypot experiment: Two dummy industrial control systems (ICS) and one real one to the Internet

- First attack in 18 hours.
- 12 unique attacks that could be classified as "targeted,"
- 13 attacks repeated by same actors.
- Attackers used automated tools that search out industrial.
- Hackers probed the site and manipulate devices if possible.
- Attacks included modifying settings to change water pressure and stop the flow on a water pump.
- Attacks used techniques specific to industrial control systems.
- Attacks involved sending emails to the administrator address.



www.waterworld.com/articles/iww/print/volume-13/issue-3/columns/industrial-control-systems-targeted-by-hackers.html?goback=.gde_1222087_member_251346148

© 2014 Adventium

SCADA Vulnerabilities

"In general, ICS vulnerabilities continue to make news. On Thanksgiving Day in the US, Aaron Portnoy, the vice president of research at Exodus Intelligence, was able to uncover no fewer than 23 vulnerabilities in SCADA systems in just a few hours. The first exploitable zero-day took a mere seven minutes to discover. "I had a morning's worth of time to wait for a turkey to cook, so I decided to take a shot at finding as many SCADA 0day vulnerabilities as possible," he explained. "For someone who has spent a lot of time auditing software used in the enterprise and consumer space, SCADA was absurdly simple in comparison."

http://www.infosecurity-magazine.com/view/31203/another-honeywell-ics-vulnerability-rears-its-head-in-building-control/?goback=.gde_1222087_member_222594055

The above story sums up my observations over 25 years.

© 2014 Adventium

Stuxnet

"Stuxnet is a new class and dimension of malware. Not only for its complexity and sophistication (eg by the combination of exploiting four different vulnerabilities in Windows, and by using two stolen certificates) and from there attacking complex Siemens SCADA systems. The attackers have invested a substantial amount of time and money to build such a complex attack tool."

Dr Udo Helmbrecht, executive director of ENISA

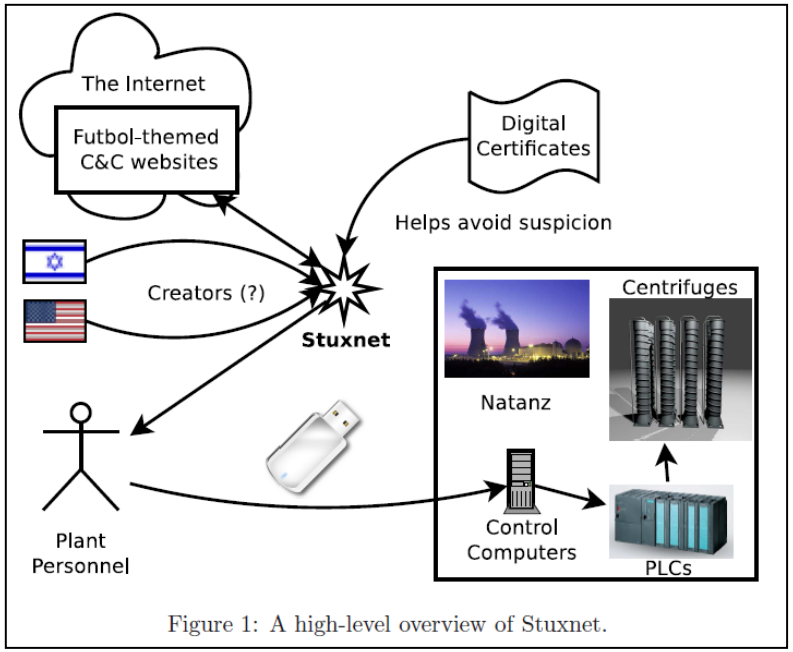


Figure 1: A high-level overview of Stuxnet.

The Stuxnet Worm, Paul Mueller and Babaki Yadegar
www.cs.arizona.edu/~collberg/.../report.pdf

Stuxnet removed all remaining doubt about ability of cyber attack to cause physical damage

Then there was Shamoon

"The Shamoon attack was a wake up call for the oil and gas industry on several fronts; not only did it manage to destroy data from over 30,000 computers at the worlds largest oil producer, Saudi Aramco, but according to experts the virus could have been designed by a second year computer science student."

"The low sophistication of the Shamoon virus software is not only worrying because it would be very easy to copy, but it also highlighted huge vulnerabilities and gaps in not just the energy sector, but the entire critical infrastructure space." Oil & Gas Industry News 6/2013

Brian's hint about SCADA: Shamoon attacks computers running MS NT operating systems.

© 2014 Adventium

But Wait – What About Confidentiality?

"…U.S. companies lose some $250 billion to intellectual property theft every year…. Internationally, $114 billion was lost to cybercrimes, but that number could be as high as $388 billion if the value of time and business opportunities lost is included. McAfee, the computer software and security company, gives an even higher number, saying $1 trillion is spent globally in remediation efforts." – Gen. Keith Alexander, National Security Agency Director

Intellectual Property is contained in the plant design, operation, and product recipes.

© 2014 Adventium

Case Study – Valspar

Secret formula stolen on USB device

"Between 2008 and 2009, a chemist with Valspar Corporation named David Yen Lee used his access to an internal computer network to download 160 secret documents related to paints and coatings. Lee intended to bring this information to his new company with Nippon Paint in Shanghai, China." (http://www.justice.gov/usao/iln/pr/chicago/2009/pr0626_01a.pdf)

© 2014 Adventium

Case Study – Night Dragon

Hackers Breach Tech Systems of Oil Companies

NY Times, 10 Feb 2011: At least **five multinational oil and gas companies suffered computer network intrusions from a persistent group of computer hackers based in China**, …. Computer security researchers at McAfee Inc. said the attacks, …, appeared to be aimed at corporate espionage.

Operating from what was a base apparently in Beijing, the intruders established control servers in the United States and Nether-lands to break into computers in Kazakhstan, Taiwan, Greece and the United States, according to a report, "**Global Energy Cyber attacks: 'Night Dragon.**' " The focus of the intrusions was on oil and gas field production systems as well as **financial documents related to field exploration and bidding** for new oil and gas leases, according to the report.

Source: http://www.nytimes.com/2011/02/10/business/global/10hack.html

© 2014 Adventium

Adventium LABS

Malware Focused on Exfiltration

- Duqu
  - Identified September 2011
  - Designed to capture key strokes and system information
- Flame
  - Identified May 2012
  - Believed the original malware dates to 2006
  - “Scout” for Stuxnet
  - Largest malware program ever seen (20 MB)
- Red October
  - Discovered October 2012
  - Advanced cyber espionage targeted diplomatic, governmental and scientific research organizations worldwide
  - Operated 6+ years
  - Auto shut-down after discovery

© 2014 Adventium

Another Reason to be Concerned

BAI – " Howard, please comment on the repurposing of Duqu, Flame, and Stuxnet by criminal organizations"

HS – "Yes, you are correct. We are seeing a massive reuse of the components of these sophisticated attacks. Once the malware was discovered and dissected, the reuse started in a matter of weeks."

Howard Schmidt, former Special Assistant to the President and Cyber Security Coordinator, Cyber Security Summit, Oct. 9th 2012

© 2014 Adventium

Why Is Securing SCADA so Hard?

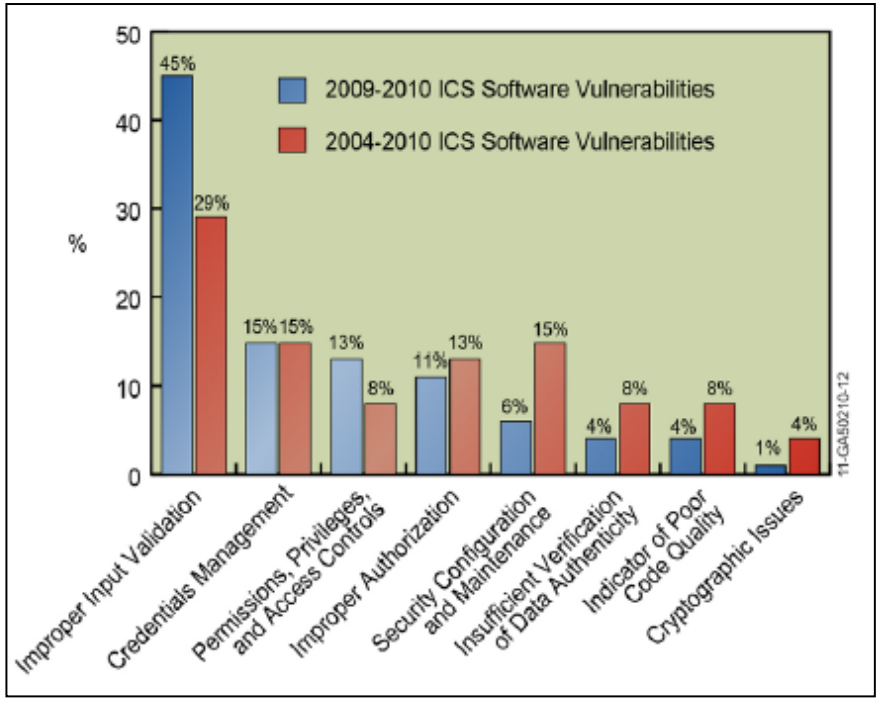
Control Systems are Unique and different from IT

- Control systems are often viable for 20 or 30 years.
- Controls are integrated into a larger system by a third party.
- Security is not a core competency of control engineers nor integrators – the folks who specify, design, assemble, and operate the systems.
- The overall system will change continuously for the life of the plant.
- There is no tolerance for a blue-screen due to a software patch.
- The often cited security approach of “air gap” is a myth.

© 2014 Adventium

DHS Current ICS Vulnerabilities 2009 - 2010

"Current vulnerabilities in ICS product assessments continue to be improper input validation by ICS code. Through bad coding practices and improper input validation, access can be granted to an attacker allowing them to have unintended functionality or privilege escalation on the systems"



DHS, *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, May 2011, Figure 3.

© 2014 Adventium

The Problem is Not Technology

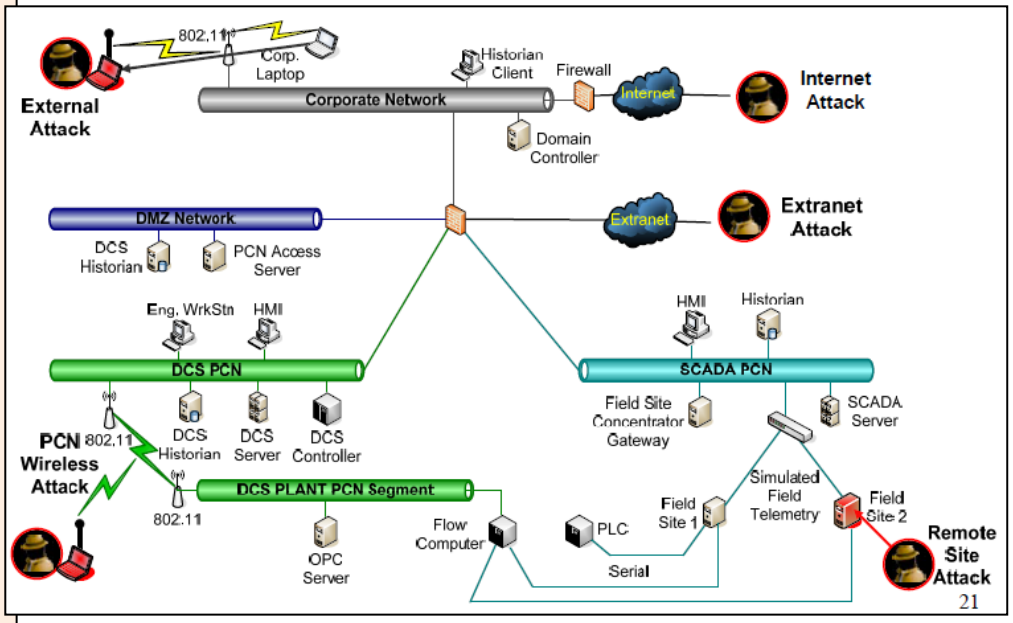
LOGIIC 2007

Standard IT Defenses

- Network Segment Firewalls
- Host Firewalls
- Network Intrusion Detection Systems (IDS)
- Network Devices (switches, routers, wireless devices)

Control System Event Sources

- Standard IT network IDS using signatures for a control system protocol (Modbus)
- Alarms from SCADA and DCS systems
- Alarms from a flow computer



http://www.logiic.org

LOGIIC and other programs showed that SOA IT technology can detect and deter attacks in ICS/SCADA systems.

The Security Path Forward

是故勝兵先勝而後求戰，敗兵先戰而後求勝。
Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.

http://en.wikiquote.org/wiki/Sun_Tzu

Brian's opinion: We have been in "in war, seeking to win" for way too long.

© 2014 Adventium

The Secure Path Forward

The ICS/SCADA world is moving in the right direction

- Documenting and analyzing SCADA vulnerabilities.
- National level standards and best practices.
- Cybersecurity testing and certification for systems and embedded devices.
- Vendors are adopting a “system life cycle” security perspective.

© 2014 Adventium

Conversation With Process Control Industry Leader

- Never depend on the system integrator – or – end user to be able to correctly configure for security.
- Design all products to be secure by design.
  - Shipped with least privileges
  - Minimum Role-based-access define
    - Separation of roles and duties
    - Each component has at least two roles:
      - Commissioning role
      - User role
- Make security simple for everyone who touches the product.
    - Easy to commission, Easy to update, Easy to maintain.

"Security must be in the DNA of all aspects of the company from R&D to procurement."

© 2014 Adventium

SDLC: Security Considerations

System Development Life Cycle
- Initiation
- Acquisition / Development
- Implementation / Commissioning
- Operation / Maintenance
- Decommissioning / Disposal

	Initiation	Acquisition/ Development	Implementation	Operations/ Maintenance	Disposal
SDLC	Needs Determination: • Perception of a need • Linkage of need to mission and performance objective • Assessment of alternatives to capital assets • Preparing for investment review and budgeting	• Functional statement of need • Market research • Feasibility study • Requirements analysis • Alternatives analysis • Cost-benefit analysis • Software conversion study • Cost analysis • Risk management plan • Acquisition planning	• Installation • Inspection • Acceptance testing • Initial user training • Documentation	• Performance measurement • Contract modifications • Operations • Maintenance	• Appropriateness of disposal • Exchange and sale • Internal organization screening • Transfer and donation • Contract closeout
Security Considerations	• Security categorization • Preliminary risk assessment	• Risk assessment • Security functional requirements analysis • Security assurance requirements analysis • Cost considerations and reporting • Security planning • Security control development • Developmental security test and evaluation • Other planning components	• Inspection and acceptance • System integration • Security certification • Security accreditation	• Configuration management and control • Continuous monitoring	• Information preservation • Media sanitization • Hardware and software disposal

Table 10-1 NIST's Breakdown of a SDLC Model

CISSP: All-in-One Exam Guide (6th Edition) by Shon Harris pg 1094

© 2014 Adventium

System/Software Lifecycle Development Process

Software Lifecycle Standards, Tools & Resources (examples)

- ISA Secure
  - Software development lifecycle
  - System Security Assurance (SSA)
    - http://www.isasecure.org/ISASecure-Program/SSA-Certification.aspx
- Building Security In Maturity Model http://bsimm.com/
- Microsoft Security Development Lifecycle (SDL) – Process Guidance
  - http://msdn.microsoft.com/en-us/library/windows/desktop/84aed186-1d75-4366-8e61-8d258746bopq.aspx
- Building Security In Maturity Model http://bsimm.com/
- SAFECode organization - software security practices (www.safecode.org)
- Software Engineering Institute (ISO 12207, ISO 15288, DHS-CBK) http://www.sei.cmu.edu/solutions/softwaredev/

© 2014 Adventium

System/Software Cyber Testing/Certification

Test and certify cyber readiness (examples)

- Wurldtech Achilles certification
  http://www.wurldtech.com/product_services/
- ISA Secure – certification program for components and system.
- Veracode - security verification of mobile, web, developed, purchased or outsourced software applications and third-party components.
  http://www.veracode.com/solutions
- Fortify On Demand
  https://trial.hpfod.com/services-and-solutions

© 2014 Adventium

SCADA Security Bottom Line

- The problem is bigger then we thought.
- The problem is manageable, if not solvable:
  - Security: A priority for entire system life cycle.
    - From requirements to integration to decommissioning.
    - Policy and procedures that reinforce security.
    - Systems that are certified secure.
    - Personnel through-out the life cycle with security education.

The answer is having security in the DNA of all aspects of the ICS / SCADA system life cycle.

© 2014 Adventium

Questions?

Useful References

- “Targeted Nation State Attacks” www.acsac.org/2007/casestudies/Ritchey.pdf
- 2012 & 2011 Data Breach Investigations Report – Verizon Risk team, US Secret Service, Dutch High Tech Crime Unit
- The Nitro Attacks: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf
- NIST SP800-30 Risk Assessment: http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf
- NIST SP800-39 Risk Management: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
- MANDIANT: APT1 Exposing One of China’s Cyber Espionage Units
- http://csis.org/publication/raising-bar-cybersecurity
- IT Governance and Oversight: COBIT 5 (http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx)
- IT Security Management Standards: ISO/IEC 27000 series http://en.wikipedia.org/wiki/ISO/IEC_27000-series
- DHS Cyber Security Framework: NICE Framework http://csrc.nist.gov/nice/framework/
- http://scadahacker.com/library/

© 2014 Adventium