Dream Team: Building the Perfect SCADA Team

- SANS, Barcelona, 10 December 2012
- Tyler Williams / Auke Huistra
AGENDA

- Setting the scene
- The Perfect SCADA team (?)
- Behavioral Change
- Skill-pool development
Setting the scene
IT IS ALL ABOUT

Protecting our (critical) assets:
1. Ensuring the safe, secure and reliable operation of manufacturing and production facilities

Preventing incidents that cause:
1. Unplanned disruption to project progress and/or;
2. Product deferment or loss for manufacturing and production facilities.
3. Cyber security related HSSE incidents
THE WHOLE PICTURE?

- Procurement: Buy Secure
- Projects: Deploy Secure
- Sites: Run & Maintain Secure

December 2012
PCD IT Security Control Framework

**Organize**
- Training
- Roles and Responsibilities
- Asset Inventory

**Defend**
- PCD Access
- Portable Media
- Portable Computers
- Operating System Security Patches

**Collect**
- Security Log Collection and Management

**Contain**
- Anti-virus
- Network Segmentation

**Respond**
- Backup and Restore
- Incident Response

December 2012
AND NOW: THE WHOLE PICTURE

Boardroom – Leading by doing

Think Secure for PCD

Base Practices PCD IT Security

Buy Secure

Procurement

Projects

Deploy Secure

Sites

Run & Maintain Secure

Informed buyers

Informed, Skilled and trained personnel

Informed, Skilled and trained personnel

December 2012
The perfect SCADA team (?)
<table>
<thead>
<tr>
<th>Situation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cyber security threats continue to increase in both frequency and sophistication</td>
</tr>
<tr>
<td>• Process Control Domain (PCDs) getting more automated, integrated and interconnected, are facing a real challenge</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Complications</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To manage risk effectively in our industrial domains, technology, standards, policies and practices are not enough, <strong>people are crucial!</strong></td>
</tr>
<tr>
<td>• There is a lack of two fundamental underlying pieces to the puzzle:</td>
</tr>
<tr>
<td>• <strong>Awareness</strong> material about cyber security risks and consequences to inform both behavior and business decisions for operational resources</td>
</tr>
<tr>
<td>• Easily accessible, domain specific <strong>skill-pool and competency frameworks</strong>, training programs and materials</td>
</tr>
<tr>
<td>• A standardized foundational set of skills, knowledge and abilities for PCD IT Security across the industry is lacking, but useful</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Main question</th>
</tr>
</thead>
<tbody>
<tr>
<td>How do we ensure that our workforce in the industrial operations have <strong>enough Skills, Knowledge and Ability</strong> to keep the operational environment <strong>safe, secure and resilient</strong> against current and emerging cyber threats?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Behavioral change PCD Stakeholders:</strong> Design, implement and operationalize an enterprise-wide PCD IT Security program to drive behavioral change at PCD stakeholders (boardroom, management, engineers, operators, contractors, vendors, integrators)</td>
</tr>
<tr>
<td>• <strong>Skill-pool Management:</strong> Design, implement and operationalize an enterprise-wide (ECO-system wide) PCD IT Security Skill-pool framework.</td>
</tr>
</tbody>
</table>
1. reducing re-training costs and improving on-boarding from one organization to another.
2. reducing likelihood, consequence and mean-time-to-recovery from an incident.
3. decreasing recruitment time/costs and likelihood of brain drain.
4. reducing HR churn and providing opportunities for career development.
5. reducing recruitment/sourcing costs, time-to-market for solutions and response time to
The perfect SCADA team doesn’t exist

- It is an **joint effort** of the whole organization – like Safety!
- **Combination of:**
  - The boardroom taking leadership
  - Informed Buyers
  - Informed, Skilled and Trained People on-site: e.g. accountable manager, site focal points, trained operators / engineers
  - Central PCD IT Security team that adds value to the business with e.g. Technical Authorities, Technical Experts, PCD IT Assist Desk
  - Contractors, Vendors, Integrators with right skill-set and training
- **Combination of** the boardroom, a management and technical skill-pool, as well as specific roles: e.g. Architects, Software designers, Software developers, Testers
The Perfect SCADA Team (De)Central

- Roles needed on every site or project:
  - PCD IT Security Accountable Manager (e.g. General Manager, Operational Manager, Engineering Manager)
  - PCD IT Security Site/Project Focal Point (e.g. CS-IT - Control Systems IT professional or CSE – Control Systems Engineer)
  - PCD IT Support
  - PCD Incident Owner

- PCD IT Security team needed centrally that does:
  - Company Standards & Practices
  - Technology Demonstration / Innovation / New solutions
  - Vendor engagement
  - Technical Authority (incl. sign off on major changes)
  - Deep technical expertise
  - (Threat) analysis

December 2012
## The Perfect SCADA Team – RACI On-Site

<table>
<thead>
<tr>
<th>Practice</th>
<th>Role</th>
<th>PCD IT Security Accountable Manager</th>
<th>PCD IT Security Site/Project Focal Point</th>
<th>PCD IT Support</th>
<th>PCD Incident Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training</td>
<td>AR</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Roles and Responsibilities</td>
<td>AR</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Asset Inventory</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>PCD Access</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Portable Media</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Portable Computers</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Operating System Security Patches</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Security Log Collection and Management</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Anti-virus</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Network Segmentation</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Backup and Restore</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

December 2012
WORKFORCE DEVELOPMENT FRAMEWORK

Skill-pool development

Management Skill-pool

E.g.
- Senior Management
- PCD IT Security Manager (central team/CoE)
- PCD IT Security Accountable Manager (on-site)

Technical Skill-pool

- PCD IT Security Engineer III
  - Technical Authority

- PCD IT Security Engineer II
  - Technical Expert

- PCD IT Security Engineer I
  - PCD IT Support
  - Site/Project Focal Point
  - CS-IT
  - IRM PCD Analyst
  - Capital project support

Specific roles

E.g.
- R&D
- Architect
- Software designer
- Software developer
- Tester

Level 1: All People that have interaction with systems in the PCD

Level 0: All people that enter the PCD

December 2012
Behavioral Change
THINK SECURE – BASIC BEHAVIOR

Target Audience
Level 1: All People that have interaction with systems in the PCD

Groups
• Company own Engineers / operators
• Contractors
• Vendors
• Integrators

Learning goals
Basic behavior to work secure in the PCD

Means / methods
• E-learning
  • Basic training
  • Webcast on base practices PCD IT Security
• Think Secure for PCD materials:
  • Videos
  • Posters
  • Roll-ups
  • Branded USB-sticks
  • PCD IT Security portal
  • Etc.

December 2012
Basic messages for Think Secure for PCD campaign:

<table>
<thead>
<tr>
<th>Campaign subject</th>
<th>Think Secure for PCD behaviors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inappropriate use of portable media, mainly USB-stick</td>
<td>• Don’t use USB sticks&lt;br&gt;• If you have to use them, only use USB sticks approved by the Site/Project Focal Point&lt;br&gt;• Scan these USB sticks before AND after use with up-to-date AV solutions</td>
</tr>
<tr>
<td>Unapproved, unscanned laptops</td>
<td>• Connect only laptops to PCD Systems that are approved by the Site Focal Point (who does a malicious scan check)</td>
</tr>
<tr>
<td>Intervene and report</td>
<td>• Report PCD IT Security incidents and ‘near misses’ to your Site Focal Point&lt;br&gt;• Intervene in unsecure or non-compliant situations</td>
</tr>
</tbody>
</table>

Work with a valid work permit when required

Wear your seat belt

While driving, do not use your phone and do not exceed speed limits

December 2012
• Control Room Posters
• Branded USB Sticks & How to guide for USB usage
  • Incl. solutions
• Security Roll-ups
• Training / HSSE material for Site Focal Points to use on site
• (Youtube) videos
  • HSSE Induction Video
  • Introduction to the importance of cyber security
  • Think Secure for PCD with the do’s and don’t’s
Skill-pool development
WORKFORCE DEVELOPMENT FRAMEWORK

Level 0: All people that enter the PCD

Level 1: All people that have interaction with systems in the PCD

Basic Behaviour

Management Skill-pool

Technical Skill-pool

Specific roles

E.g.
- R&D
- Architect
- Software designer
- Software developer
- Tester

E.g.
- Senior Management
- PCD IT Security Manager (central team/CoE)
- PCD IT Security Accountable Manager (on-site)

E.g.
- Technical Authority
- PCD IT Security Engineer III
- Technical Expert
- PCD IT Security Engineer II
- PCD IT Support
- Site/Project Focal Point
- CS-IT
- IRM PCD Analyst
- Capital project support

E.g.
- R&D
- Architect
- Software designer
- Software developer
- Tester

First focus area

Skill-pool development

Basic Behaviour
TECHNICAL SKILL-POOL

Job Category

- PCD IT Security Engineer III
  • Technical Authority
- PCD IT Security Engineer II
  • Technical Expert
- PCD IT Security Engineer I
  • PCD IT Support
  • Site Focal Point / CSIT
  • IRM PCD Analyst
  • Capital project support

Experience

- Engineering
  • IT
  • Cyber Security
  • Sectoral / Company

Competencies (Knowledge, Skills, Abilities)

- Leadership
- Engineering
- IT
- Cyber Security
- Sectoral / Company

Qualifications

- Engineering
  • IT
  • Cyber Security
  • Sectoral / Company

December 2012
## Technical Skill-pool Framework

### Technical Skill-pool PCD IT Security

**Overview Expertise / Leadership / Competencies / Qualifications PCD IT Security Engineer (level I - III)**

<table>
<thead>
<tr>
<th>Expertise (years of experience)</th>
<th>PCD IT Security Engineer I</th>
<th>PCD IT Security Engineer II</th>
<th>PCD IT Security Engineer III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering</td>
<td>&lt;2</td>
<td>3-5</td>
<td>6-8</td>
</tr>
<tr>
<td>IT</td>
<td>3-5</td>
<td>3-5</td>
<td>6-8</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>3-5</td>
<td>6-8</td>
<td>&gt;8</td>
</tr>
<tr>
<td>Sector/company</td>
<td>&lt;2</td>
<td>3-5</td>
<td>3-5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Leadership attributes</th>
<th>Individual Performer</th>
<th>Leader of teams</th>
<th>Leader of a community</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering</td>
<td>Knowledge</td>
<td>Skill</td>
<td>Skill</td>
</tr>
<tr>
<td>IT</td>
<td>Skill</td>
<td>Skill</td>
<td>Skill</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>Skill</td>
<td>Skill</td>
<td>Mastery</td>
</tr>
<tr>
<td>Corporate, Industry and Professional Standards</td>
<td>Knowledge</td>
<td>Skill</td>
<td>Mastery</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qualifications</th>
<th>PCD IT Security Engineer I</th>
<th>PCD IT Security Engineer II</th>
<th>PCD IT Security Engineer III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering</td>
<td>• Instrumentation and Basic Process Control</td>
<td>• Instrumentation and Basic Process Control</td>
<td>• Instrumentation and Basic Process Control</td>
</tr>
<tr>
<td>IT</td>
<td>Network (CCA or eq) Windows (MCSE)</td>
<td>Network (CCA or eq) Windows (MCSE)</td>
<td>Network (CCA or eq) Windows (MCSE)</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>CISSP</td>
<td></td>
<td>CISSP CISM Advanced Cyber Security training (e.g. INL, Red Tiger Security, SCADA Hacker)</td>
</tr>
</tbody>
</table>

December 2012
Basis for specific job descriptions
Basis for hiring and assessing new people but also the existing workforce (e.g. for assurance reasons)
Basis for Individual Development Plans (or PDP or POP or ....)
Basis for a skilled and trained workforce

Example PCD IT Security Engineer III from Skill-pool framework:

<table>
<thead>
<tr>
<th>Cyber Security competencies</th>
<th>Knowledge</th>
<th>Skill</th>
<th>Mastery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main topics:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) IT security on conceptual level as well as on a technical and procedural level</td>
<td>Explain in detail IT security standards, practices, methodologies and frameworks.</td>
<td>Being involved in security architecture, risk, network, access management, encryption, testing, physical or logical security, assurance review or advisory on a daily basis.</td>
<td>Manage information security specialists.</td>
</tr>
<tr>
<td>2) IT Security Standards (like IEC/ISA 62443) Practices and Solutions (e.g. for USB usage, laptops, hardening, monitoring and logging)</td>
<td>Have industry security certification and draw on this knowledge in my work.</td>
<td>Provide detailed advise on optimal IT Security architecture.</td>
<td>Recognized as an IT security expert.</td>
</tr>
<tr>
<td>3) Computer Network Defense (skill in detecting host and network-based intrusions via intrusion detection technologies (e.g. IDS))</td>
<td>Being involved in the support of security architecture, risk, network, access management, encryption, testing, physical or logical security, assurance review or advisory on a daily basis.</td>
<td>Select and implement successfully several IT security methods, tools or technologies.</td>
<td>Develop and improve methods, tools and technology for IT security.</td>
</tr>
<tr>
<td>4) Incident response and handling methodologies</td>
<td>Have deep knowledge of and can advise on one or more IT security methods, tools or technologies.</td>
<td>Train or act as a mentor to junior security professionals.</td>
<td>Set the direction for securing information assets.</td>
</tr>
<tr>
<td>5) Root Cause Analysis of security incidents and operational issues relating to PCD IT Security</td>
<td>Give advice on security direction within the business.</td>
<td>Designing and assure implementation of a uniform framework for managing risks.</td>
<td>Play an active role in security governance.</td>
</tr>
</tbody>
</table>
The Individual Development Plan (IDP) should exist of 4 areas

- **Reference materials**: Relevant samples of book titles on subject competence
- **Training courses**: Internal (e.g. Face to Face and eLearning) and External training
- **On-the-job coaching**: Enabling others to strengthen performance by helping them develop skills and competences important to individual and organizational success.
- **Actions to build professional experience**: Examples of job and project assignments where skill in identified competence may be gained
CONCLUSIONS

• People are crucial for a secure PCD
• From boardroom to work floor
• It is a joint effort
• Basic behaviour is key
• The skill-pool needs development

It is an industry effort!
Questions?

Tyler Williams  
Manager, Process Control Domain IT Security at Shell Global Solutions

Auke Huistra  
Project manager Nationale Roadmap Secure PCS - CPNI.NL  
auke.huistra@tno.nl / +31 6 21479272