Building Security Into ICS/SCADA Products

George Wrenn, CISSP,ISSEP, CEH
Cyber Security Officer (CSO)

Paul Forney, CSSLP
Cyber Security Evangelist

Product Security Office (PSO)

March 2014

Schneider Electric

About presenters:
George Wrenn, CISSP,ISSEP,CEH

- CSO at Schneider Electric
- Harvard University / MIT Background
- Computer Security Since Apple IIe (brun hacking 1983)
- Been involved for 30 years in computer security
- MIT Trained in Advanced Cryptography
- Graduate Fellow at MIT (Sloan, MediaLab & Eng.)
- NSA Sponsored ISSEP Certification
- IBM, KPMG, EMC, RSA and Unisys
- Serve as 1st Lt. (Officer) USAF/Aux – Hanscom AFB
- Mission Pilot (SAR/DR)
- Live in Boston area with family
- Interests include flying planes and helicopters, surfing
- Six Sigma Black Belt, LSS and Kaizen Facilitator
- Awarded two patents in “SaaS/Cloud Security

Surfing Rye Rocks Reef Break Winter 2014

About presenters:
Paul Forney, CSSLP

Mr. Forney is a voting board member of the ISA Security Compliance Institute (ISCI) which develops the conformance specifications to the ISA 99/IEC 62443 ICS cyber security standard, has held the Co-chair position for the Research and Development Sub-group of the Department of Homeland Security Industrial Control System Joint Working Group and sits on the Board of Advisors for Cylance.

He is also an active participant in the ISA99 WG4 TG6 committee. Paul has been a guest speaker on the subject of SDL and incident response in industrial control systems at national and international conferences for Microsoft, Gartner, SANS, ICSJWG, RCMP and Public Safety Canada. Paul works closely with the ICS-CERT organization on ICS cyber vulnerabilities and also with cyber researchers around the globe.

Mr. Forney has been awarded ten patents in areas such as failure prediction for upstream Oil and Gas and collaboration technologies for Power; and for twenty-four years, has been involved in the design and implementation of SCADA, Event Driven/Service Oriented Architecture (EDA/SOA) and distributed control software and systems for industrial automation.

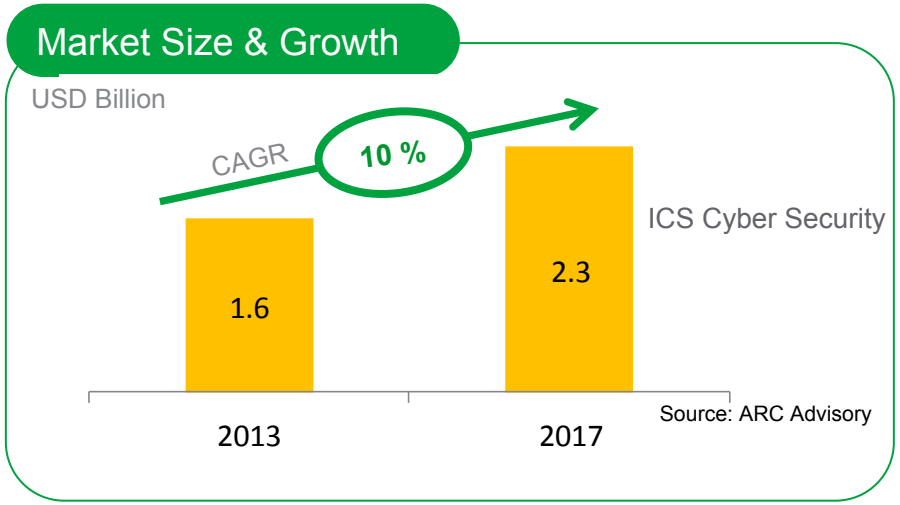
Paul is a Certified Secure Software Lifecycle Professional (CSSLP) and an avid jazz musician.

Trends & Drivers

Cyber security threats are creating increasing demands for trusted, security capability from ICS/SCADA vendors.
We are all facing both an opportunity and risk that must be addressed.

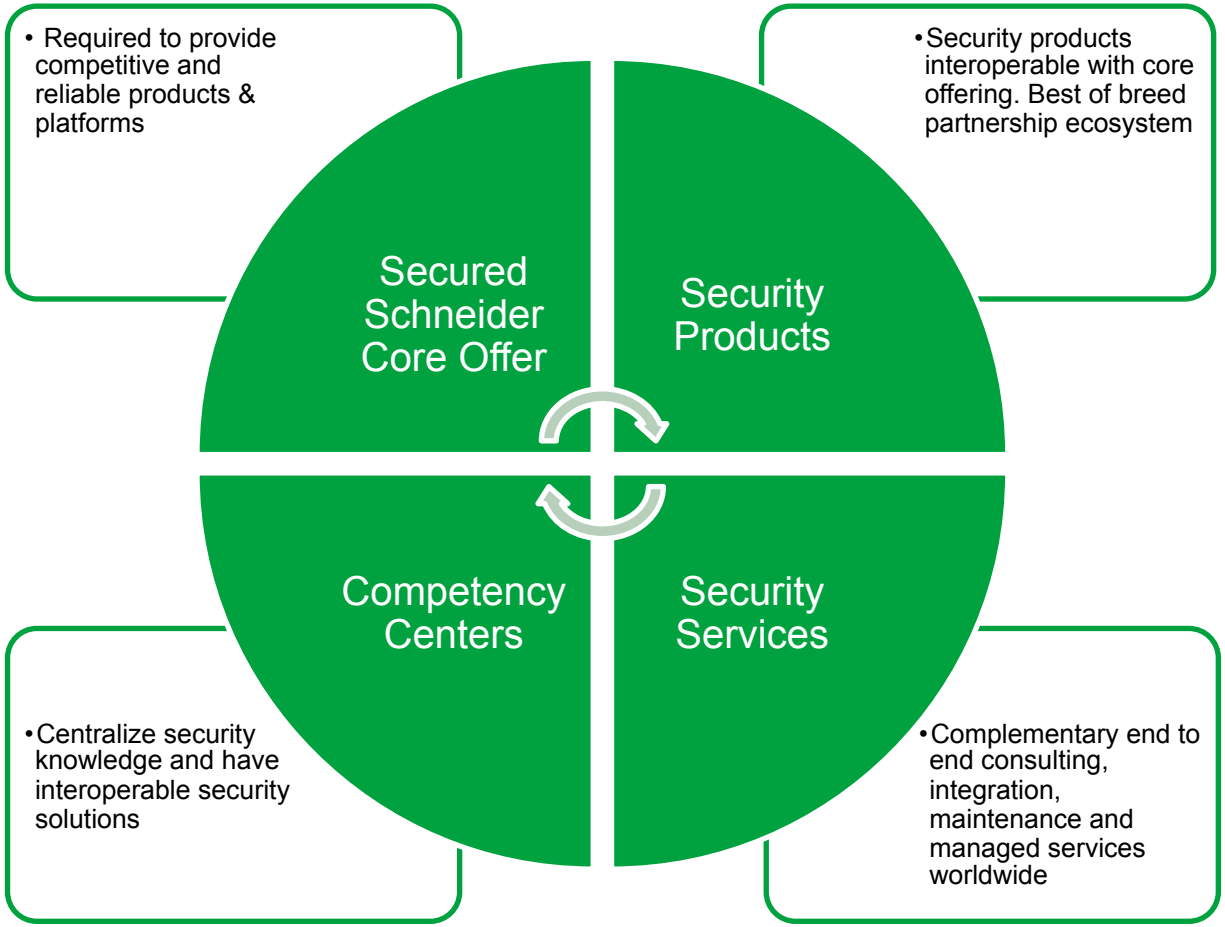
- **Demand**: Exponential growth in cyber security attacks and high regulatory pressure
- **Market Expectation**: ICS vendor to provide secure products and services
- **Strategic Fit**: Cyber security to differentiate offerings, while protecting customers
- **Downside**: ICS vendors not always providing security capability will face share erosion

"… the cyber threat will be the **number one threat to our country** (US)." – Robert Mueller, FBI Director, Feb 1st 2012



Comprehensive Security Offer

Schneider Electric enables a comprehensive portfolio of secure products, solutions & services for our customers to meet this challenge

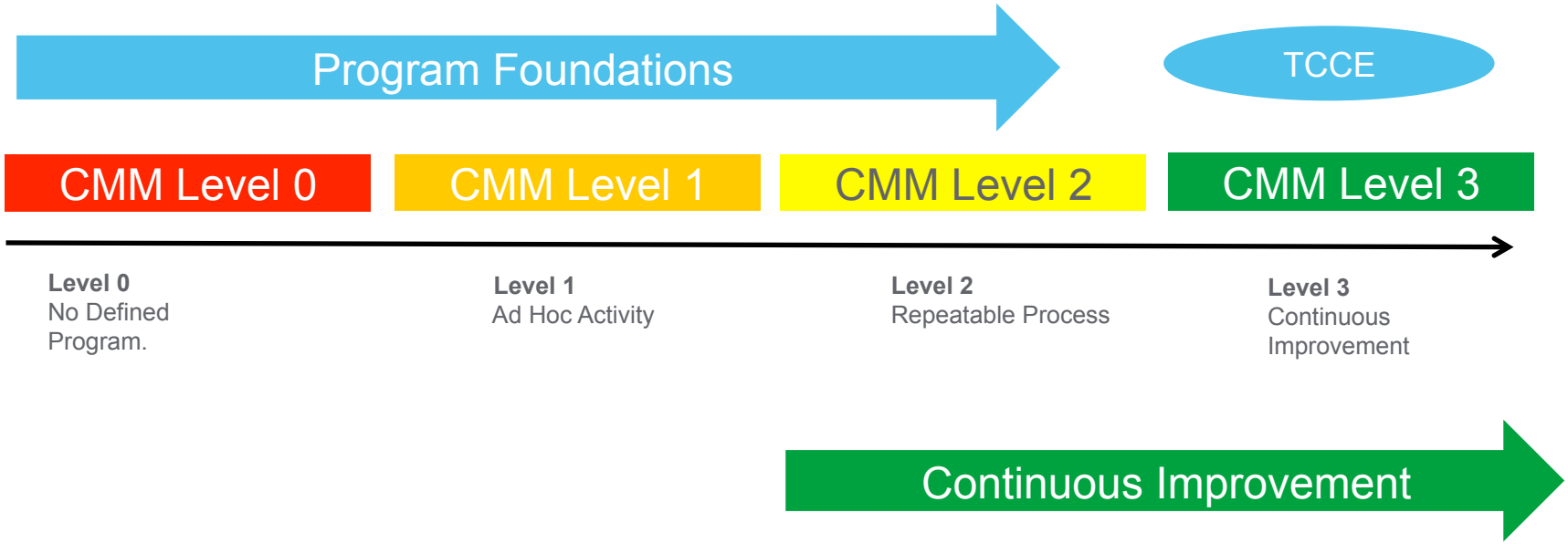


Trustworthy & Compliant Control Environment (TCCE)

What it means to be secure.. Our vision for the future..

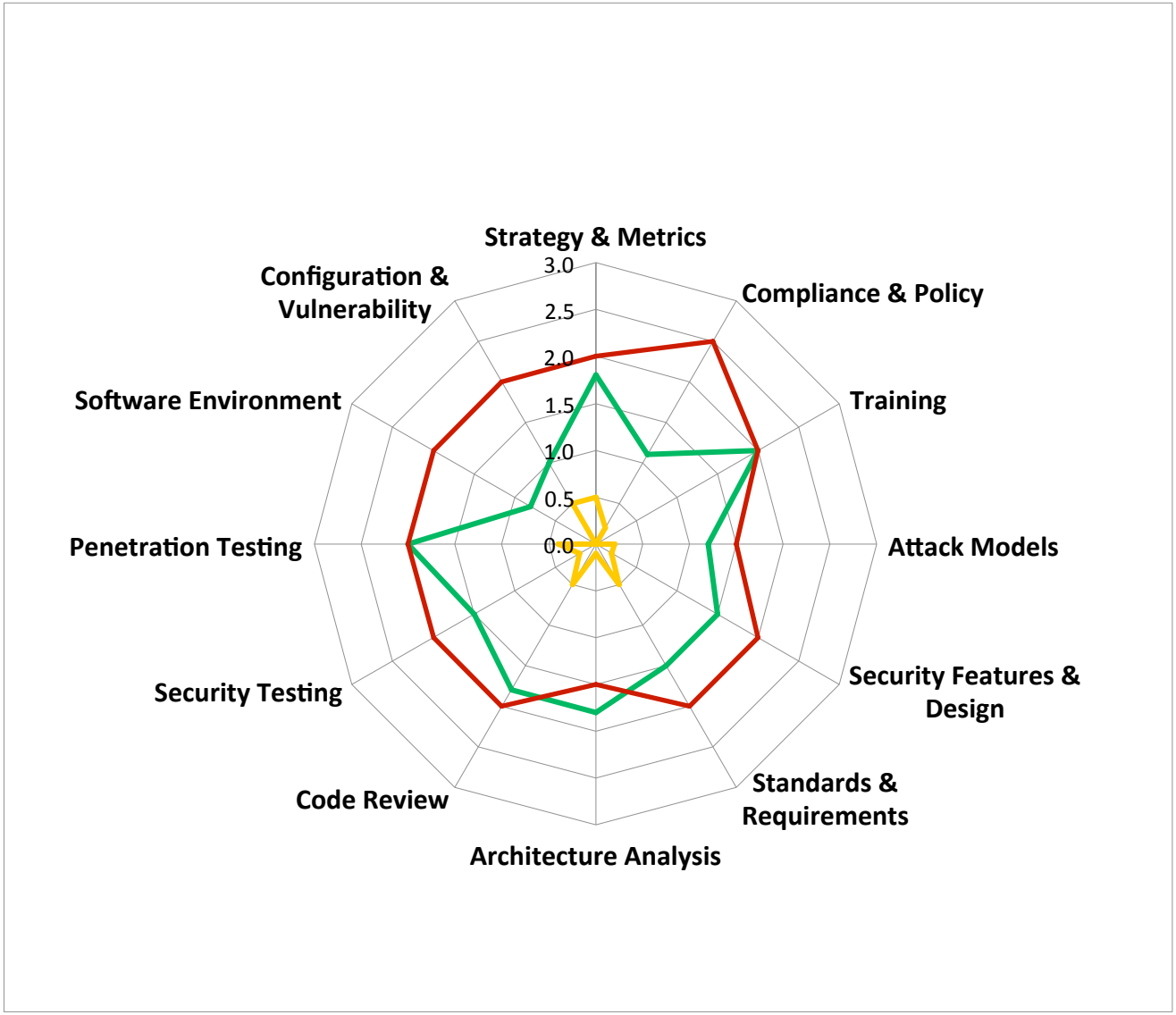
- Schneider customers *trust* Schneider to deliver reliable, safe and secure offerings.
- The foundation of this trust is represented at the smallest unit in our products that are combined to produce an offering or solution to solve one or more customer business challenges.
- Changes to the threat-scape now make delivering on this expectation much more of challenging.
- Digitization is connecting our products to the “internet of everything”.
- The internet of everything is opening up unprecedented opportunity but also a significant potential risk for everyone in the industry
- The trustworthy control environment is comprised of secure products, combined with security services in a tested and validated manner to solve one or more customer cyber security objectives.

Schneider Electric Cyber Security Capability Maturity Model (CS-CMM)



Example of SDL Maturity on B-SIMM Scale

Build Security In Maturity Model (B-SIMM) measures internal software cyber security on 12 dimensions across 4 main topic areas.



Repeatable Standards Based Approach

Create a Trustworthy & Compliant Control Environment (TCCE)

Increase the overall Schneider security capability maturity

Engage deeply with partners to “secure the internet of everything” which includes our devices (Cisco, IBM, HP, et al)

Continue to culturally integrate cyber security processes into the “way we do things”

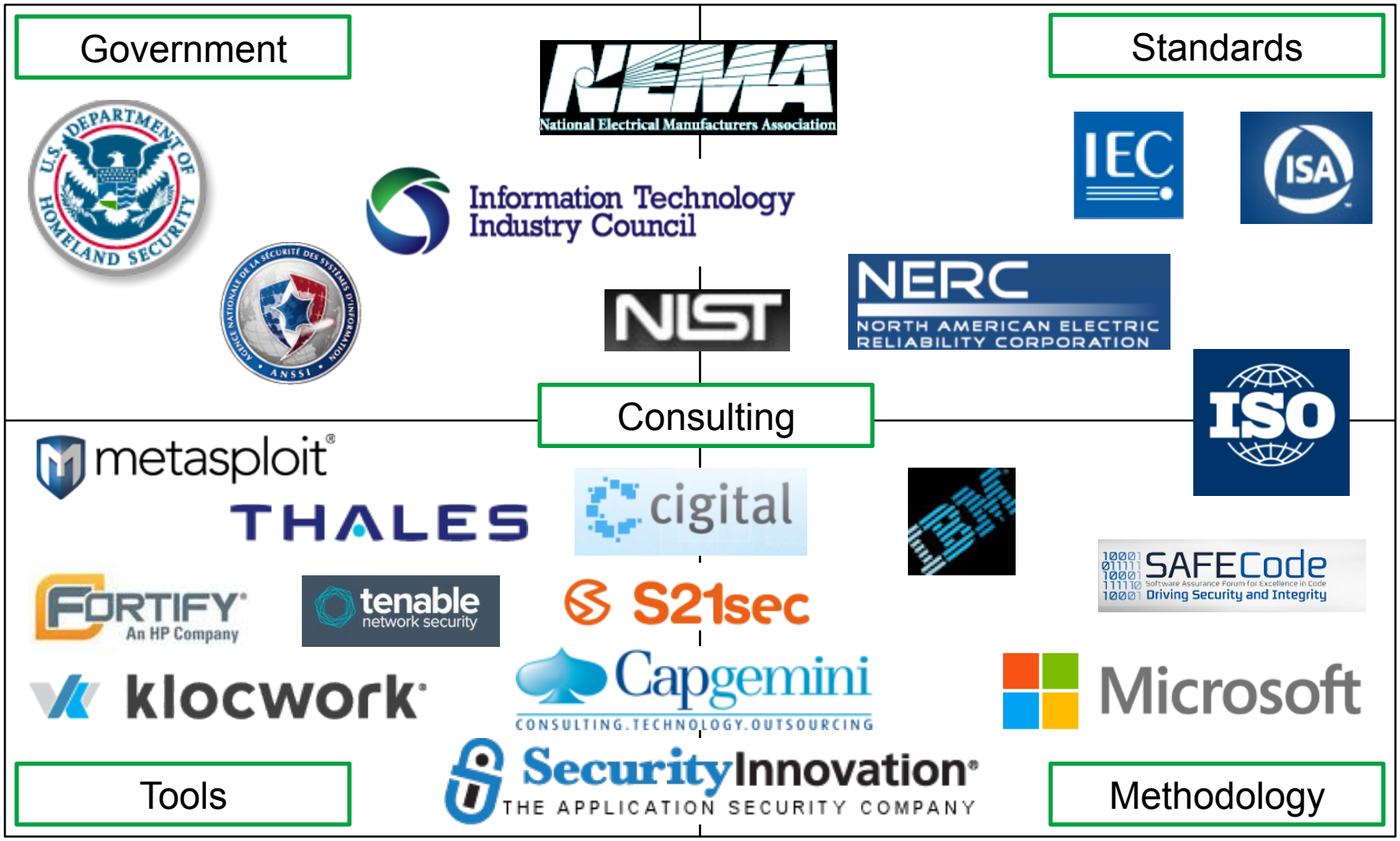
Build a cyber security aware and trained workforce to call upon to build and deliver our offerings securely

Certify products to meet operational requirements such as DIACAP to enable entry into more regulated markets

Common Security Platform (CSP) for use on all products

Embrace standards such as ISO:27034 to demonstrate security capability

Schneider Electric Cyber Security Eco System
To support our global program



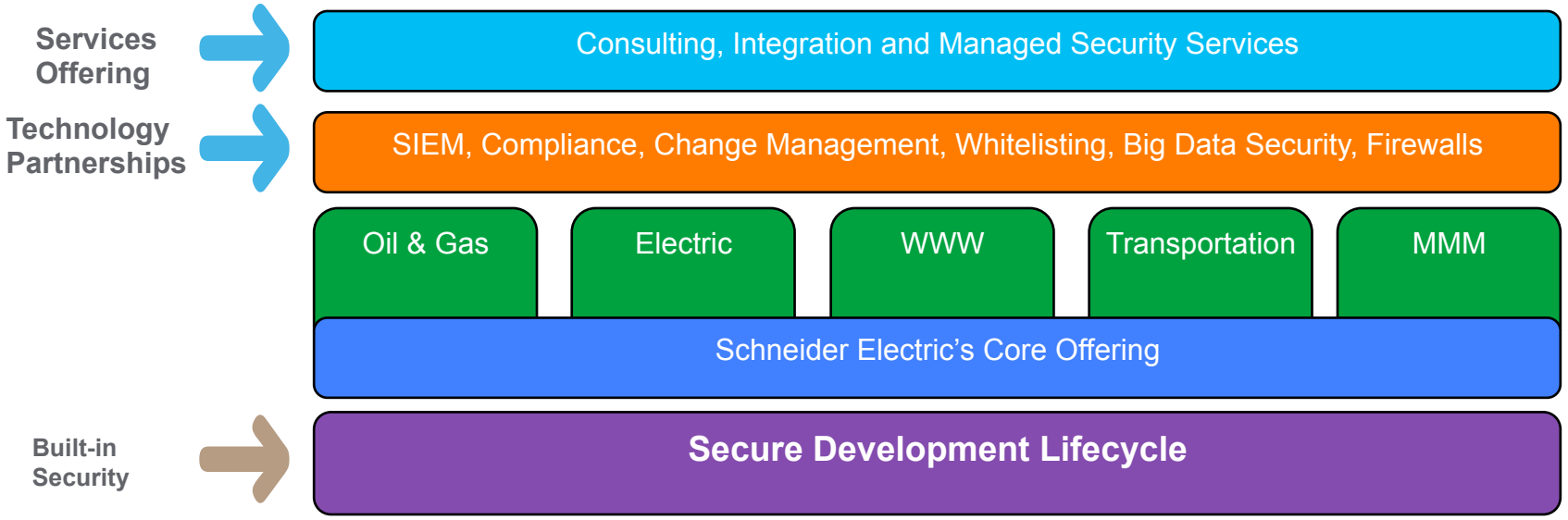
Holistic Approach to Security

Schneider Electric stands by a safe, reliable and secure core offering. SDL is driving security improvements to our products.

Cyber security products & services, increasing prevention, detection & response.

Providing portfolio of services through recognized Schneider Electric's consulting arm & local players

Bringing best third party solutions through partnership ecosystem & 'vendor agnostic' mindset



Global SDLP Required and Process Aligned

VERSION 1.2 Secure Development Lifecycle Policy (SDLP)

Table of Contents

Secure Development Lifecycle for Products and Solutions

Deliver Security Training	Security Requirements	Secure Design Reviews	Secure Code Practices	Security Testing	Secure Release Management	Secure Deployment	Incident Response
On-demand training for each role	Security requirements based on regulations	Conduct Threat Modeling and Architecture Review	Scan all code related to product	Secure white box and black box testing	Documentation and process details to securely deploy the offering	Full security lifecycle services for customers	Respond to incidents and vulnerabilities reported

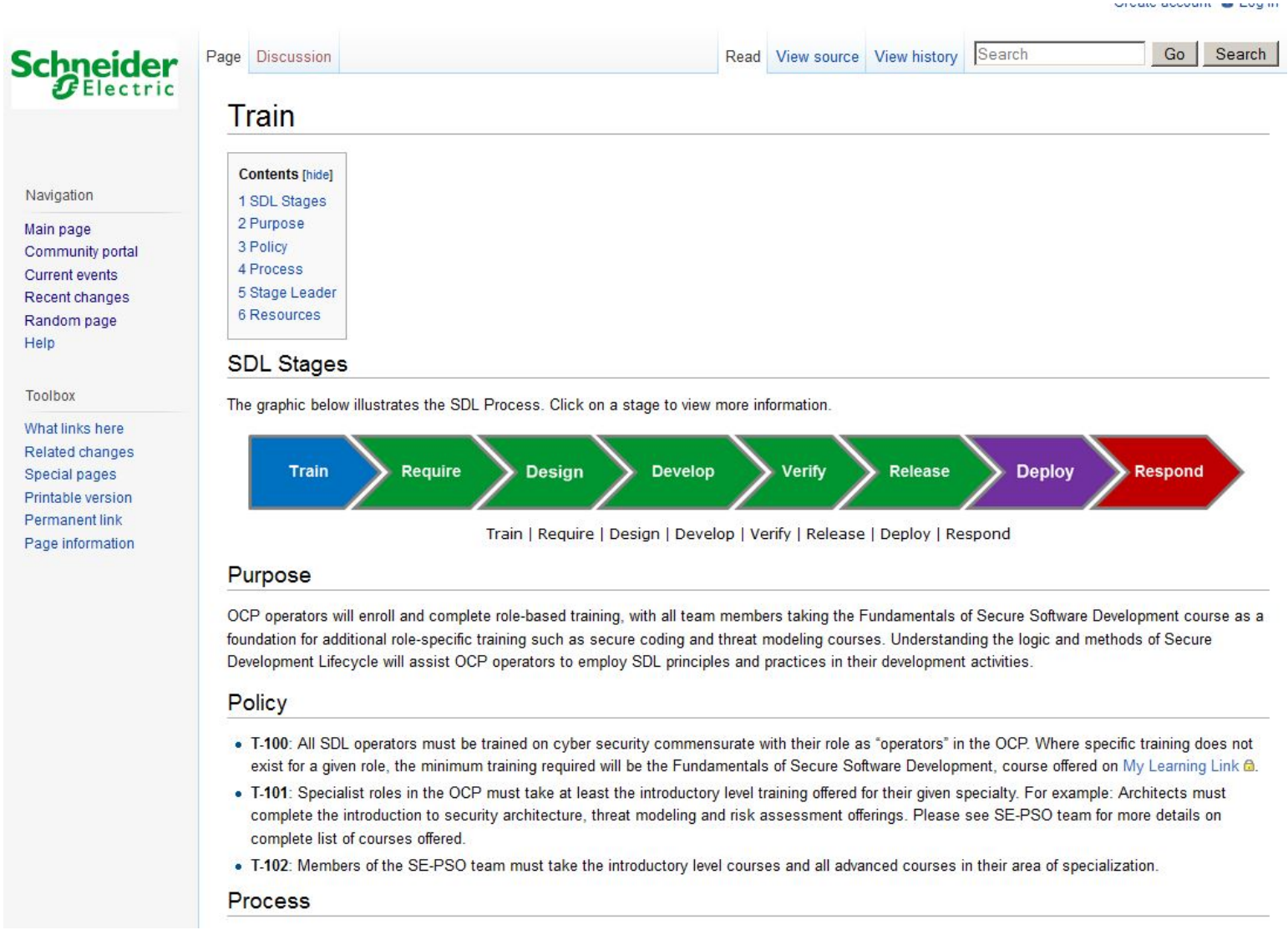
Stage Deliverables

On demand training delivered through our global learning platform	Completed security requirements checklist per project based on regulatory requirements	Threat model workshop and final threat model report with next steps	Security test report from code security quality tool	Security test results report with categorized findings by severity	Security documentation that details security features and deployment best practices	Deliverables will vary by customer engagement and project scope	Disclosure report posted to web and external sites such as ICS-CERT where applicable

PSO Resources and Stage Leads

Training content by partner Security Innovation Leader	Requirements checklist based on industry regulations Leader	STRIDE methodology and internal report template Leader	Klocwork, Fortify onDemand code scan tools and test labs Leader	Consultants, Nessus, Achilles, MetaSploit and test labs Leader	Standard security document template Leader	Deployment guide based on release package & consulting resource Leader	PSO & BU Team Resources, Legal and PR Staff Leader

Global Portal to Support Deployment



Schneider Electric

Page | Discussion | Read | View source | View history | Search | Go | Search

Train

Navigation

- Main page
- Community portal
- Current events
- Recent changes
- Random page
- Help

Toolbox

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

Contents [hide]

SDL Stages

The graphic below illustrates the SDL Process. Click on a stage to view more information.

Train | Require | Design | Develop | Verify | Release | Deploy | Respond

Purpose

OCP operators will enroll and complete role-based training, with all team members taking the Fundamentals of Secure Software Development course as a foundation for additional role-specific training such as secure coding and threat modeling courses. Understanding the logic and methods of Secure Development Lifecycle will assist OCP operators to employ SDL principles and practices in their development activities.

Policy

- **T-100**: All SDL operators must be trained on cyber security commensurate with their role as "operators" in the OCP. Where specific training does not exist for a given role, the minimum training required will be the Fundamentals of Secure Software Development, course offered on My Learning Link.
- **T-101**: Specialist roles in the OCP must take at least the introductory level training offered for their given specialty. For example: Architects must complete the introduction to security architecture, threat modeling and risk assessment offerings. Please see SE-PSO team for more details on complete list of courses offered.
- **T-102**: Members of the SE-PSO team must take the introductory level courses and all advanced courses in their area of specialization.

Process

Questions ?

LinkedIn: Paul Forney & George Wrenn (connect)