12TH ANNUAL LEADERSHIP EVENT

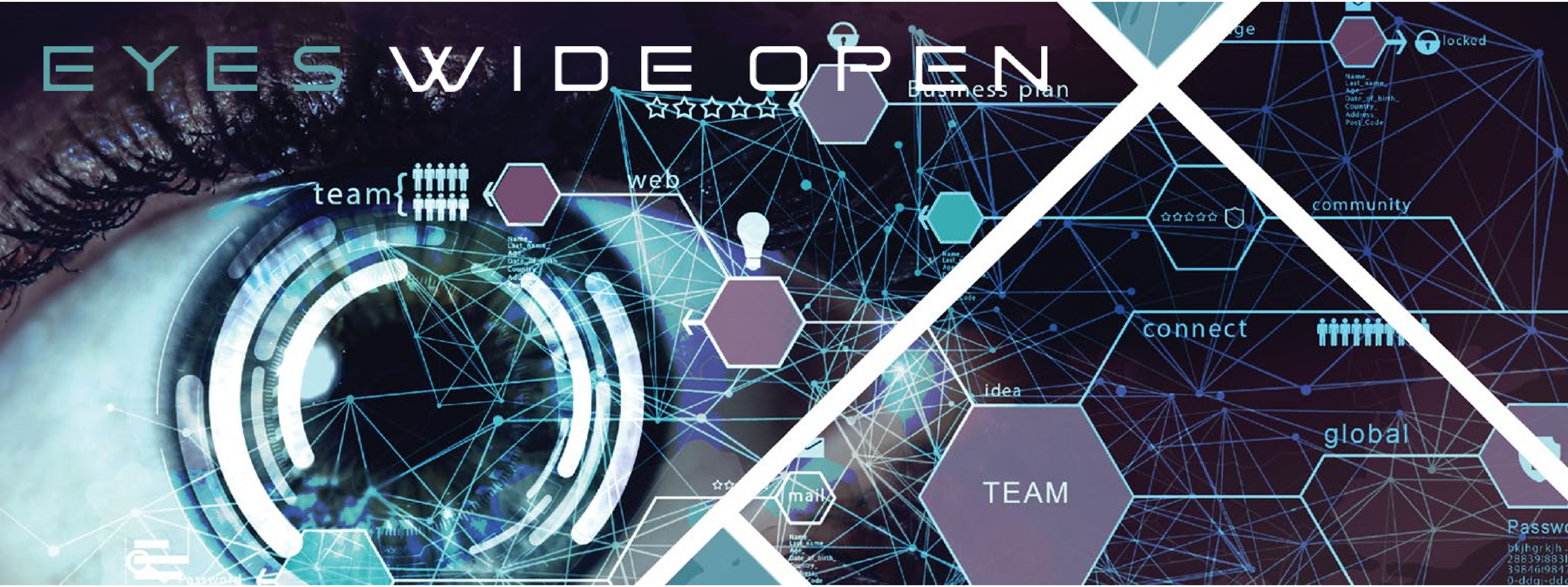
CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island

EYES WIDE OPEN



Idaho National Labs (INL) Overview of Cybersecurity Research, ICS COP w/focus on Cyber-CHAMP©

Shane Stailey

Organizational Cybersecurity Development & Training Strategist, Idaho National Laboratory

Glenn Merrell

Owner & Freelance Consultant, Industrial Control System Security

Idaho National Laboratory (INL) Overview of Cybersecurity Research, ICS COP w/focus on Cyber-CHAMP©

Building the Critical Infrastructure Cybersecurity Workforce of the Future

National Workforce Capability Gaps

Over 3 million

unfilled **cybersecurity jobs** globally in 2021

– *Cybersecurity Ventures*

Innovative R&D and proactive validation for long-term solutions

Actionable threat analysis, situational awareness, and information sharing

High quality and immediate incident response and forensics

Hands-on training and applicable skills from education

Cyber-informed and advanced technology education

Over 90%

national **control systems cybersecurity** workforce needs are NOT being met.

–CyberSeek

N&HS ICS Workforce Development Mission

Address the most critical control systems challenges that require a national collaborative, inter-disciplinary environment

Drive a culture change in engineering

Increase cybersecurity of systems deployed and under development

Enhanced partnerships

Advance control systems cybersecurity gaps

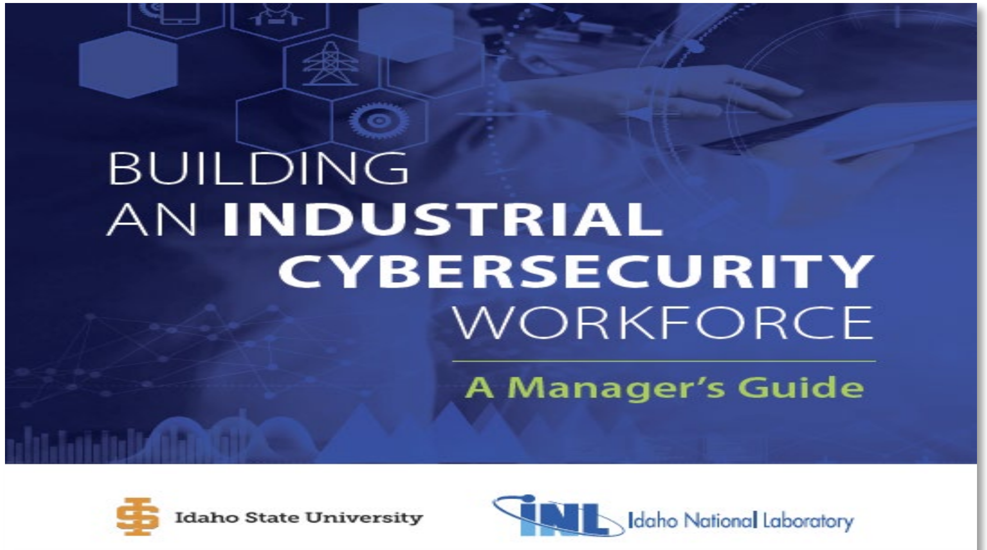
Accelerate workforce development

Support demand for control system cybersecurity talent

Leading Out on ICS Workforce Development

Industrial Cybersecurity Community of Practice (ICS COP)

- Consists of over 300 participants worldwide, 100+ entities, 25 countries
- From industry, academia, and government with bi-annual public workshops
- Sub-group meetings on workforce development, curriculum and education standards, hands on training…
- Impacts / Outcomes
  - Focus of Idaho Cyber Research Project ICS COP driven
  - Partnerships formed for grants and future funding
  - Standards work being moved forward on several fronts:
    - ISA
    - NICE/NIST
- Opportunity to demonstrate capability and expertise at national scale
  - Industry visits to validate and utilize Cyber-CHAMP
  - Model and process gaining national/international attention



BUILDING AN INDUSTRIAL CYBERSECURITY WORKFORCE

A Manager's Guide

Idaho State University

INL Idaho National Laboratory

INDUSTRIAL CYBERSECURITY EDUCATION AND TRAINING WORKSHOP

NOVEMBER 10, 2020 • VIRTUAL

Cyber Workforce Development "Gap"

Companies do not know what they do not know about their cyber workforce development.

How can an organization tackle its cyber workforce needs?

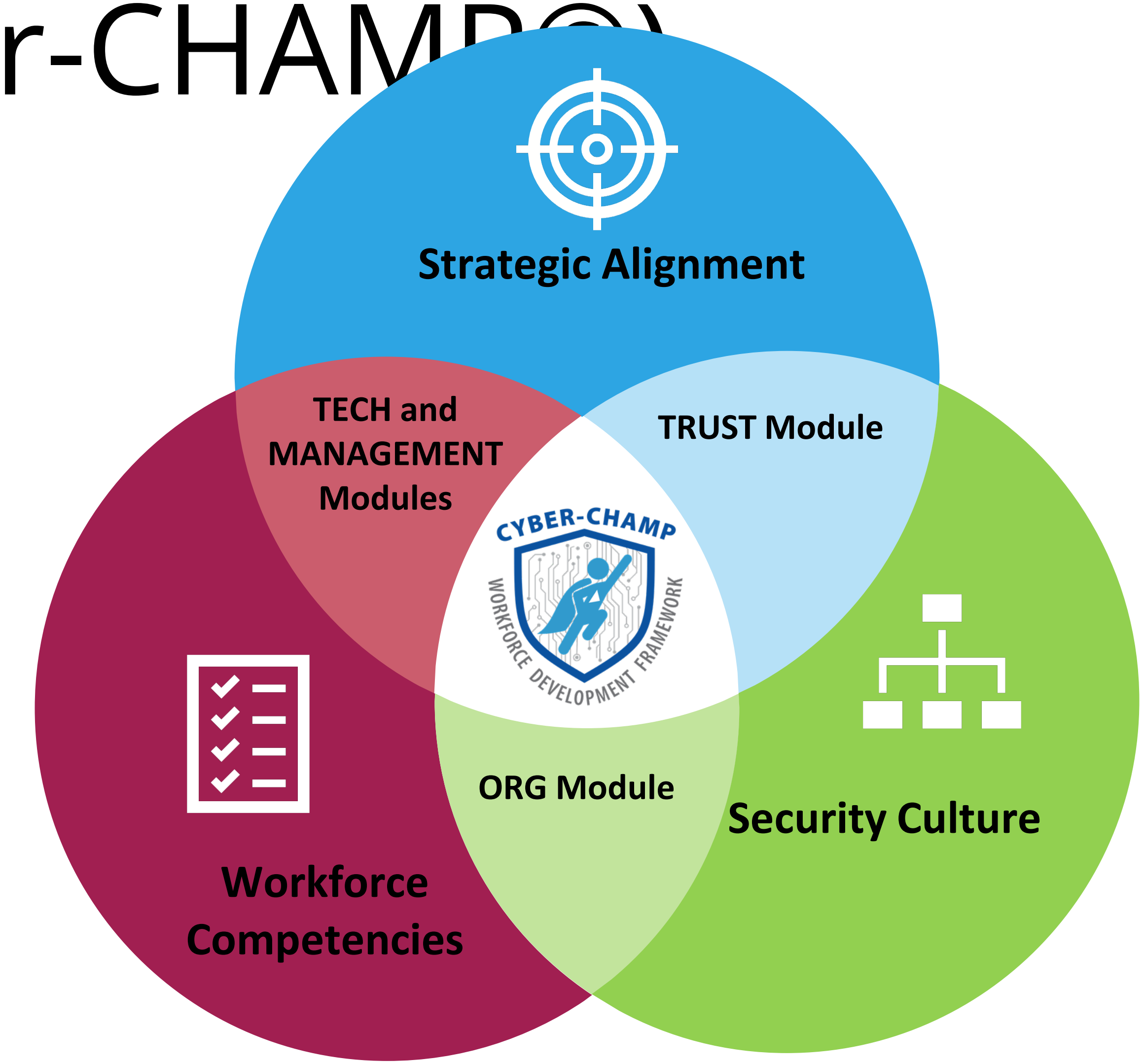
Assess cyber "health" and "maturity"

Identify most effective organizational cyber structure

Determine competency-based training needs and recommendations

How do organizations create an effective cyber workforce development program?

Cyber Competency Health and Maturity Progression Model (Cyber-CHAMP©)



Strategic Alignment

TECH and MANAGEMENT Modules

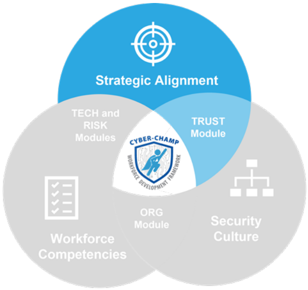
TRUST Module

Workforce Competencies

ORG Module

Security Culture

Strategic Alignment



Challenge: Security mandates

Application: Organizational Cyber Hygiene

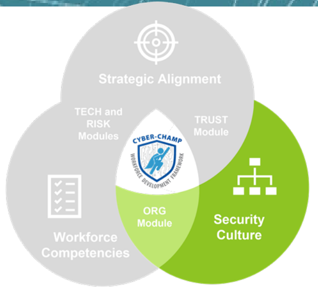
Result: Baselined cyber hygiene with target roadmaps

DIRECTION	TRACKING	EFFICIENCY
STRATEGY	PROCESSES	PRACTICES
GOALS	MATURITY	COMPLIANCE
Security strategy alignment with business goals Known gaps and direction for improvement	Measured policy/ process maturity Established targets	Verified policy/process compliance in practice

Organizational Alignment

Challenge: Analyze security culture within an organization

Result: Align security culture to support strategy



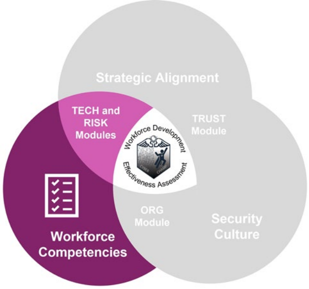
SECURITY PRIORITY	SECURITY INITIATIVES	COMPETENCY ACROSS ORGANIZATION
STRUCTURE	SECURITY EDUCATION, AWARENESS, AND TRAINING	JOB ROLE GROUPINGS AND COMPETENCIES
SECURITY POSITION	SETA PROGRAM	ORGANIZATIONAL COMPETENCIES
Known gaps for security leadership to inform organizational design that empowers and enables security	Roadmap to build a solid security education, training, and awareness program	Organizational competency matrix to understand security roles in relation to security functions

Technical and Management Competencie

Challenge: Individual workforce development and training based on functional roles

Approach: Individual workforce development and training based on functional roles

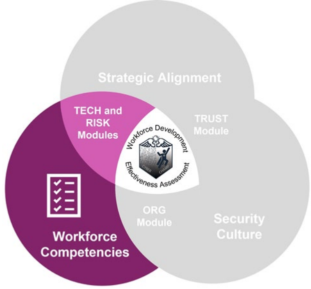
Results: Workforce development and training roadmaps

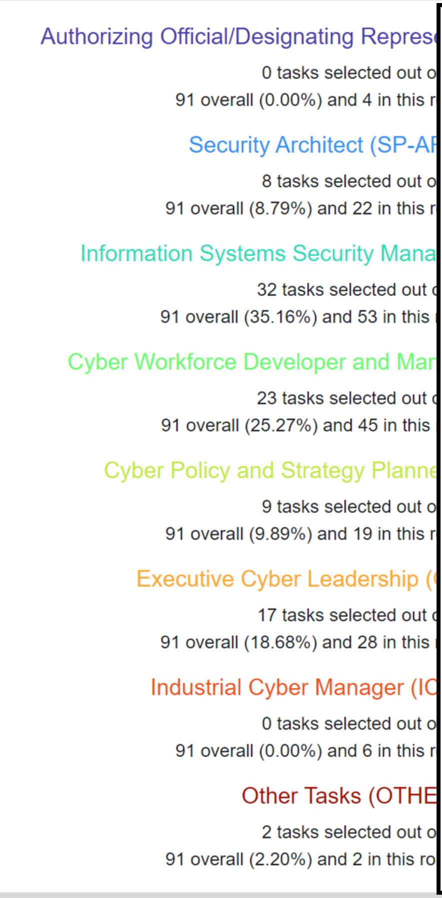


TECHNICAL STAFF	MANAGEMENT	RETURN ON INVESTMENT
TASK ANALYSIS	RESPONSIBILITY ANALYSIS	MAP TRAINING/ CERTIFICATIONS
TECHNICAL JOB DESCRIPTION	MANAGEMENT JOB DESCRIPTION	RECOMMENDATIONS
Task-based competency decomposition for each position	Responsibility/duty-based competency decomposition for each position	Industry education/ training recommendations

Technical and Management Competencies

Result: Workforce development and training roadmaps





Authorizing Official/Designating Represe

0 tasks selected out o
91 overall (0.00%) and 4 in this r

Security Architect (SP-AR

8 tasks selected out o
91 overall (8.79%) and 22 in this r

Information Systems Security Mana

32 tasks selected out o
91 overall (35.16%) and 53 in this

Cyber Workforce Developer and Man

23 tasks selected out o
91 overall (25.27%) and 45 in this

Cyber Policy and Strategy Planne

9 tasks selected out o
91 overall (9.89%) and 19 in this r

Executive Cyber Leadership (

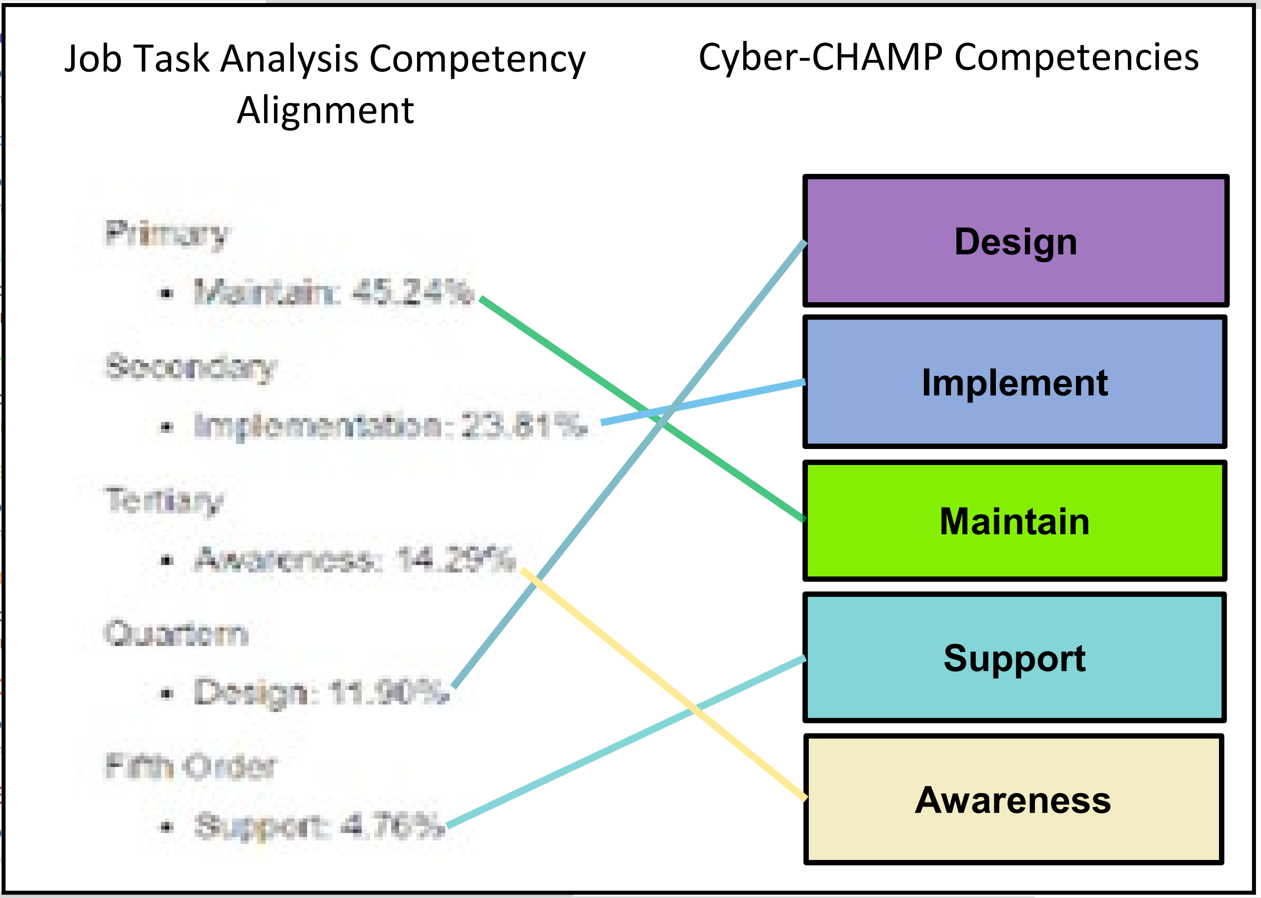
17 tasks selected out o
91 overall (18.68%) and 28 in this

Industrial Cyber Manager (IC

0 tasks selected out o
91 overall (0.00%) and 6 in this r

Other Tasks (OTHE

2 tasks selected out o
91 overall (2.20%) and 2 in this ro



Job Task Analysis Competency Alignment

Cyber-CHAMP Competencies

Primary
- Maintain: 45.24%

Secondary
- Implementation: 23.81%

Tertiary
- Awareness: 14.29%

Quartern
- Design: 11.90%

Fifth Order
- Support: 4.76%

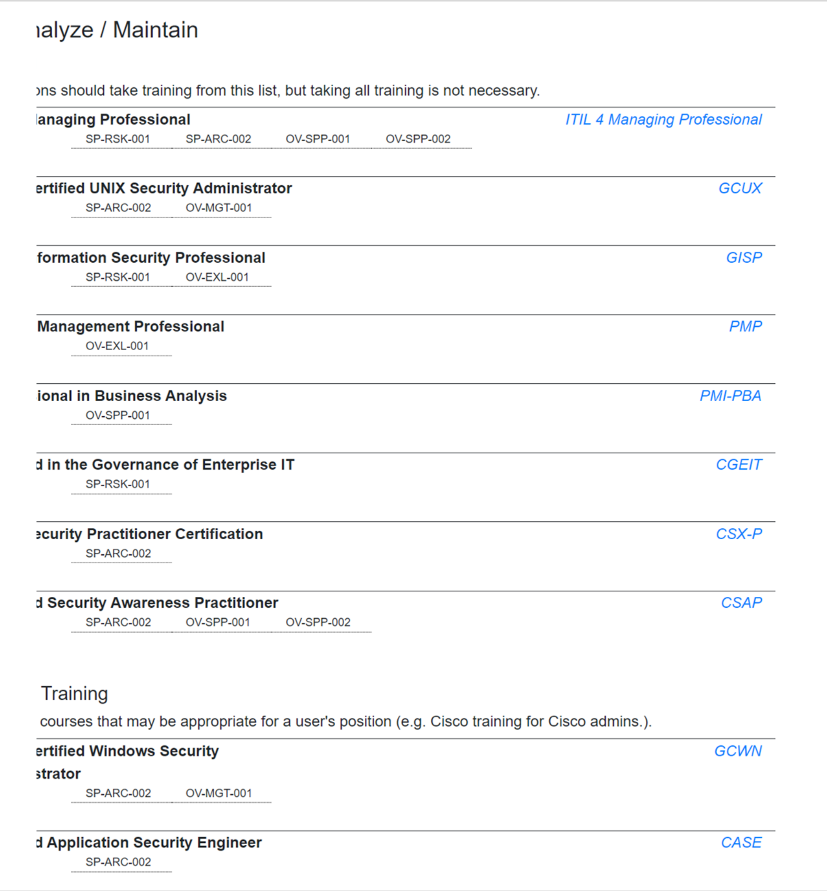
Design

Implement

Maintain

Support

Awareness



ıalyze / Maintain

ɔns should take training from this list, but taking all training is not necessary.

ıanaging Professional SP-RSK-001 SP-ARC-002 OV-SPP-001 OV-SPP-002	*ITIL 4 Managing Professional*
ertified UNIX Security Administrator SP-ARC-002 OV-MGT-001	*GCUX*
formation Security Professional SP-RSK-001 OV-EXL-001	*GISP*
Management Professional OV-EXL-001	*PMP*
ional in Business Analysis OV-SPP-001	*PMI-PBA*
d in the Governance of Enterprise IT SP-RSK-001	*CGEIT*
ecurity Practitioner Certification SP-ARC-002	*CSX-P*
d Security Awareness Practitioner SP-ARC-002 OV-SPP-001 OV-SPP-002	*CSAP*

Training

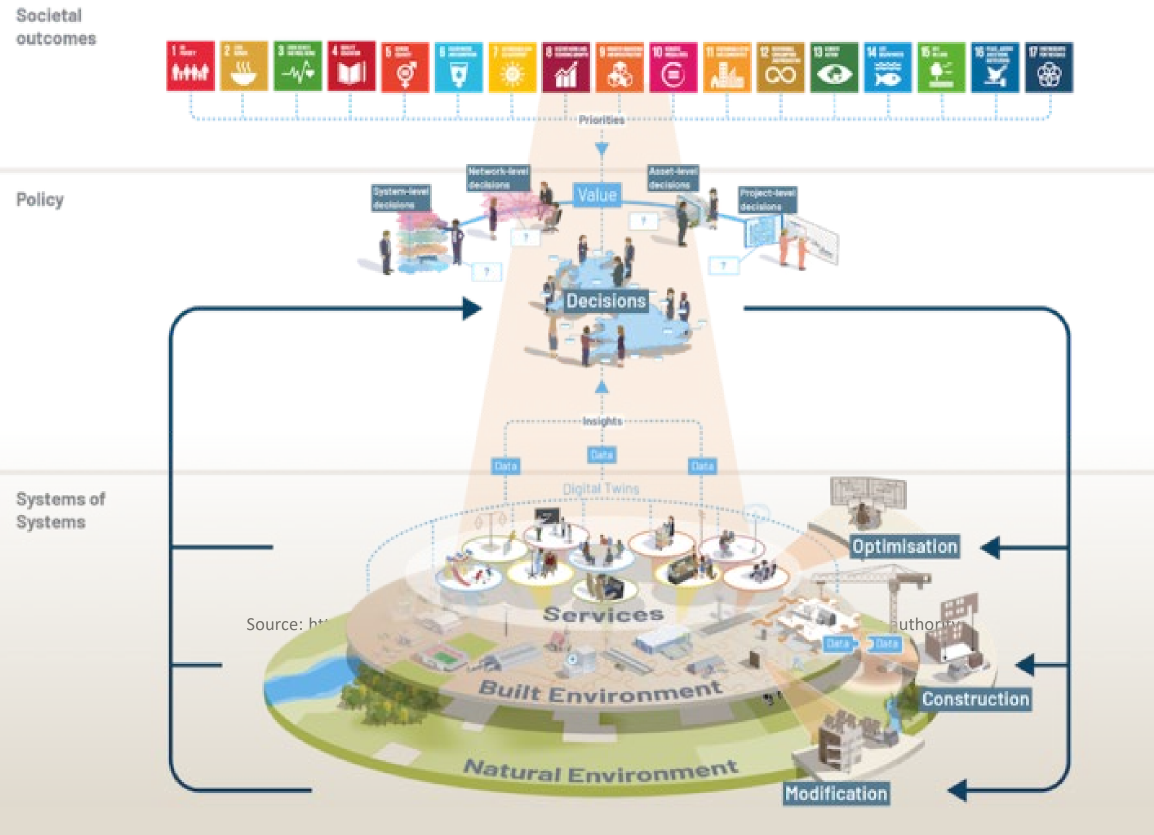
courses that may be appropriate for a user's position (e.g. Cisco training for Cisco admins.).

ertified Windows Security strator SP-ARC-002 OV-MGT-001	*GCWN*
d Application Security Engineer SP-ARC-002	*CASE*

Cyber-CHAMP© - CI Sector Guidebooks

Sector and Sub-Sector Guidebooks

- General Work Roles
- Common Organizational Structures and Issues
- Generic Training Paths for Tech and Managers
- Common Vulnerabilities vs. Training Needs
- Cyber Dependencies and Supply Chain
- Emergency Response and Infrastructure Impacts
- Infrastructure Dependency / Supply Chain Analysis
- Resources
- Etc.



Source: ht

uthority

Source: http://lifewinning.com/projects/networks-of-new-york/

Source: The Public Finance Tax Blog; Feb 7, 2022

Benefits of Building a Critical Infrastructure Workforce Development(WD) Profiles

CYBER-CHAMP
WORKFORCE DEVELOPMENT FRAMEWORK

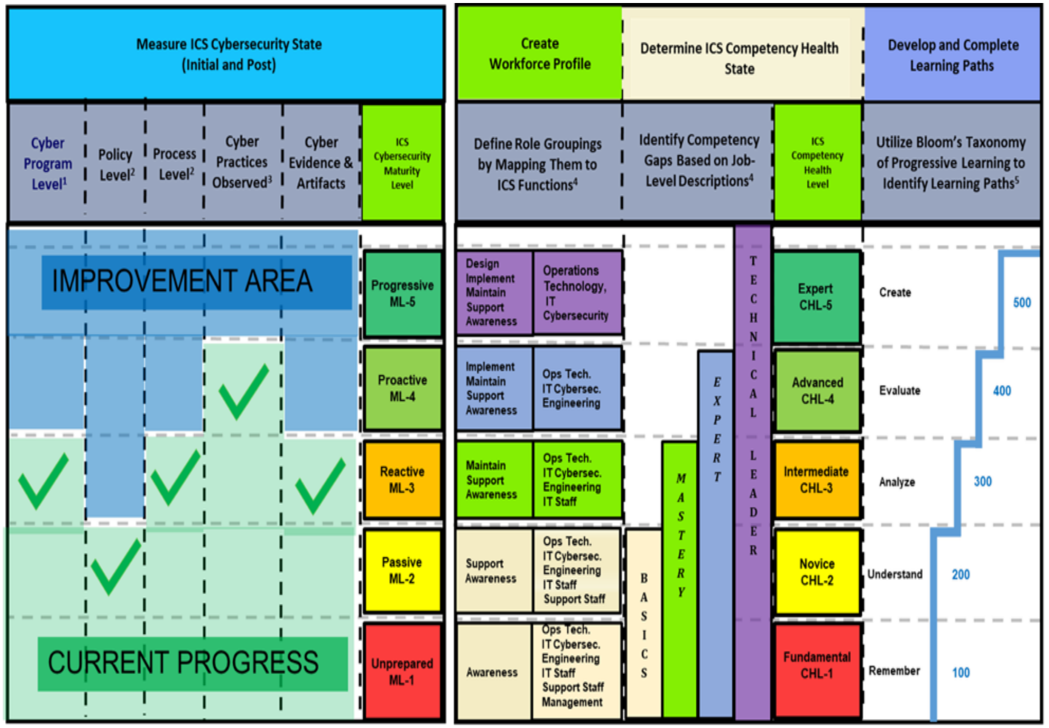
Example: for the Critical Manufacturing (CM) Sector

- CyManII collaborates with 10-15 critical manufacturing organizations
- Perform a Cyber-CHAMP evaluation in each organization
- Combine information to form a Critical manufacturing WD profile

Organizations apply the WD profile for the CM sector

- No prescriptive notion in the profile (just a starting place)
  - Each ‘future’ manufacturing organization has a WD starting point
  - Ideas for WD structure and cyber-ready teams will exist:
    - Regardless of size of organization
    - Regardless of type of organization
  - Identification of needed roles will begin to form
  - Identification of needed education, training, and cert pathways will begin to form

- Industry and sector dashboards can be developed
  - Combining of industry and sector information to provide insight:
    - What does a cyber-ready team really look like
    - What information can be provided in the CR or Board Room



Measure ICS Cybersecurity State (Initial and Post)
Cyber Program Level[1]
Policy Level[2]
Process Level[2]
Cyber Practices Observed[3]
Cyber Evidence & Artifacts
ICS Cybersecurity Maturity Level
IMPROVEMENT AREA
CURRENT PROGRESS
Progressive ML-5
Proactive ML-4
Reactive ML-3
Passive ML-2
Unprepared ML-1
Create Workforce Profile
Determine ICS Competency Health State
Develop and Complete Learning Paths
Define Role Groupings by Mapping Them to ICS Functions[4]
Identify Competency Gaps Based on Job-Level Descriptions[4]
ICS Competency Health Level
Utilize Bloom's Taxonomy of Progressive Learning to Identify Learning Paths[5]
Design Implement Maintain Support Awareness
Operations Technology, IT Cybersecurity
Implement Maintain Support Awareness
Ops Tech. IT Cybersec. Engineering
Maintain Support Awareness
Ops Tech. IT Cybersec. Engineering IT Staff
Support Awareness
Ops Tech. IT Cybersec. Engineering IT Staff Support Staff
Awareness
Ops Tech. IT Cybersec. Engineering IT Staff Support Staff Management
BASICS
MASTERY
EXPERT
TECHNICAL LEADER
Expert CHL-5
Advanced CHL-4
Intermediate CHL-3
Novice CHL-2
Fundamental CHL-1
Create
Evaluate
Analyze
Understand
Remember
500
400
300
200
100

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

WWW.INL.GOV