The Solution

Challenge 1: We need more Cyber Defenders who are proficient

- 70% of organizations say they do not have enough security staff to handle their current demands
- 50% of respondents (security pros and executives) said the shortage of skilled staff is contributing to the incidence of breaches in their organization
- 47% said they believe their customers are being affected

Data from The 2013 (ISC)2 Global Information Security Workforce Study-Frost & Sullivan / ISC2 / Booz Allen

- The threats are dynamic and proliferating,
- New recruits are hired based upon Certifications, not pro/ficiency
- Cyber Defense is trained as an individual “sport”
- Classroom training does not establish proficiency in their people and processes can absorb and leverage
- Organizations are adopting technology faster than Cyber Defense is adequate for quicker, effective response
- Roles based Cyber Defender proficiency

Challenge 2: In our view, the current approach to mobilizing a Cyber Defense is inadequate for quicker, effective response

- Organizations are adopting technology faster than Cyber Defense is adequate for quicker, effective response
- Classroom training does not establish proficiency in their people and processes can absorb and leverage
- Cyber Defense is trained as an individual “sport” when the real environment is role-based, and requires team behaviors and culture
- New recruits are hired based upon Certifications, not proficiency

Challenge 3: The threats are dynamic and proliferating, making it difficult to keep up

- Many solutions are reactive and have a short effective life
- Investments become obsolete quickly

Our Cyber Range is a unique learning system and modeling & simulation capability delivered on an open platform based upon commercial-off-the-shelf (COTS) technology. It has three major components:

Virtual Training Platform (VTP)
- Knowledge Base
- Self-Paced Cyber Security Challenges
- Dynamic Cyber Defense Exercises
- Cyber Analytics and Simulation Platform
- Customisable Virtual Environments
- Virtual Security Operations Center
- Sypris Cyber Range
- Conduct Capture the Flag Exercises
- Industrial Control System Modeling & Simulations
- Network Attack & Malicious Traffic Generation

What Problems Can Be Solved with a Sypris Cyber Range™?

- Executive and Technical Training (and Certification) for Role Profile
- Proficiency Evaluation by Role and Assignment
- Individuals
- Teams
- Cyber Technology Evaluation
- Cyber Defense Protection Strategy Development
- Cyber Incident Countermeasure Development and Evaluation
- Capture the Flag Exercises
- Red vs. Blue Team Cyber Exercises
- Modeling & Simulation of Security Operations with our Virtual Security Operation Center
- Security Protocol Monitoring

Why NEC Cyber Security?

Mature Low Risk Solution, Ready for On-Time Delivery

- 50 Years of Demonstrated Success
- Contributed to the US DOD 8570 Training Program
- Experienced, Qualified and Ready to Succeed
- Leaders in Cyber Readiness and Cyber Training
- Experienced, Qualified and Ready to Succeed
- Basic, Intermediate, Advanced and Individual and Team Proficiency
- Dynamic Defence
- Grow Skilled Workforce to Achieve Promotes Complete Cyber Self-Sufficiency
- Cyber Maturity Model
- Cyber Technology Evaluation
- Teams
- New Recruits
- Individuals
- Expertise and skills with Sypris’ Security
- Real-time cyber security defence strategies
- Cyber Incident Countermeasure Development and Evaluation
- Cyber Technology Evaluation
- Cyber Defense Protection Strategy Development
- Cyber Incident Countermeasure Development and Evaluation
- Capture the Flag Exercises
- Red vs. Blue Team Cyber Exercises
- Modeling & Simulation of Security Operations with our Virtual Security Operation Center
- Security Protocol Monitoring

What is a Sypris Cyber Range™?

Cyber Range

Dynamic Hands-On Training for Cyber Defenders

Cyber Security is a Team Sport. Defend as a Team Against Cyber Threats Today!

Benefits

Companies that are looking for better training to their IT security staff can look into Sypris’ expertise and skills with Sypris’ Security Training and Simulation Platform. Our simulations allow practicing, testing and validating large-scale IT security solutions in a realistic environment including simulating SCADA (Supervisory Control And Data Acquisition) Systems. Through our platform, companies can:

- Early detection of cyber attacks
- Cyber incident response and investigation protocols
- Real-time cyber security defence strategies

Applicable to Mobilize for Cyber Defense

- Urban Services & Immigration Control
- Law Enforcement
- Critical Infrastructure Management & Public Administration Services
- Information Management & Emergency & Disaster Management

Lightweight Design

- Low Total Cost of Ownership

Cyber Range

Dynamic Hands-On Training for Cyber Defenders

Cyber Security

is a Team Sport.

Defend as a Team Against Cyber Threats Today!
The Sypris Cyber Range™ platform provides an unparalleled learning approach to build skills and assess aptitude of both individuals and cyber defense teams by operational role and assignment.

Within this framework, each trainee is assigned a Learning Plan that forms the backbone for a unique scoring approach that measures their proficiency and overall progress.

Four training delivery methods are utilized within the Range to drive your Cyber Defenders’ proficiency:

- **Classroom-Based Modules** with Integrated Simulation Labs
- **Self-Paced Security Challenges**
- **Custom Course Module Assessments and Delivery**

**Core Modules**

- SCADA Devices
- An Architecture that is Flexible, Adaptable and Extensible

**Advanced Course**

- Module 3
- ICS Course
- Module 4.5 Capstone Cross-Sector Cyber Defence Exercise
- Module 4.2 Incident Response Tier 3
- Module 3.2 Industrial Control System Security I
- Module 3.1 Critical Infrastructure Overview
- Module 2.3 Defence in Depth
- Module 2.2 Traffic Analysis
- Module 2.1 International Cyber Incident Response Engagement
- Module 1.2 Cyber Fundamentals II

**Team-Based Dynamic Exercises**

Team-based working on different scenarios:

- Attack & Defend: More machines added into system as objectives and Exercise
- Blue Team: Simulated or can be done as red
- Threat Most
- High
- Normal
- Low
- Threat Level

- Blue Team
- Red Team

- World Challenges
- Real-World Challenges
- Threats
- Opportunities
- Challenges

- Network & Third Party Hardware
- Infrastructure

**Team Custom to Your Environment**

- Team-Based Training
- Network & Third Party Hardware
- Infrastructure

**Training Framework**

- Full Immersive Training Solution
- Self-Paced Training: Security Challenges
- Team-Based Training: Cybersecurity Exercises

**Graduate from our Dynamic Training**

- Reach Security Maturity in Real Security Crisis

**Advance Your Cyber Maturity**

- Agility/Speed of Action
- Mature
- Moderate
- Advanced
- Triage

- Threat Level
- Nation State

- Standard
- Customized

- Standard
- Advanced
- Expert

- Real World
- Mastery
- Expertise

- Self-Paced Training: Knowledge Base