

June 27 -29,  
2019

# fisseea

FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

*Role-Based Learning Paths  
for More Effective Training Results*

# DESIGN & TECH TEAM

## PRESENTED BY:

**Richard A. Spires,**  
*Chief Executive Officer*  
*Learning Tree International*

- Cyber Security and Program Management Course Author and Instructor
- Former CIO of Internal Revenue Service
- Former CIO of U.S. Department of Homeland Security

**Gregory L. Adams, P. Eng.**

- Cybersecurity Mapping
- Member of NICE Training and Certification Sub-committee

**Various Cybersecurity Subject Matter Experts,  
Authors & Instructors**



 @raspires | @learningtree



# OVERVIEW

Today we will discuss:

- **The nature of role-based training:**  
*Why it is so important for cybersecurity*
- **The development of role-based learning paths:**  
*How this can improve the efficiency of cybersecurity*
- **How you can participate and collaborate to provide ongoing improvement of the role-based learning paths**

# BACKGROUND

**For Many Organizations,  
a Cyber Security Breach  
is One of its Largest Risks**

- Private sector,  
government and military
- Can cause financial,  
reputational or even physical  
harm

**83% of CIOs Agree  
that Workforce  
Competence is Key \***

- More than technology used or  
the processes followed

**It is Anticipated there  
will be a Shortage of  
Over 3,000,000  
Cyber Professionals  
Over the Next 5 Years \*\***

**Effective Training is Key to Providing Needed Protection**

\* <http://onlinelibrary.wiley.com/doi/10.1111/irel.12066/full>

# EVOLUTION OF ROLES

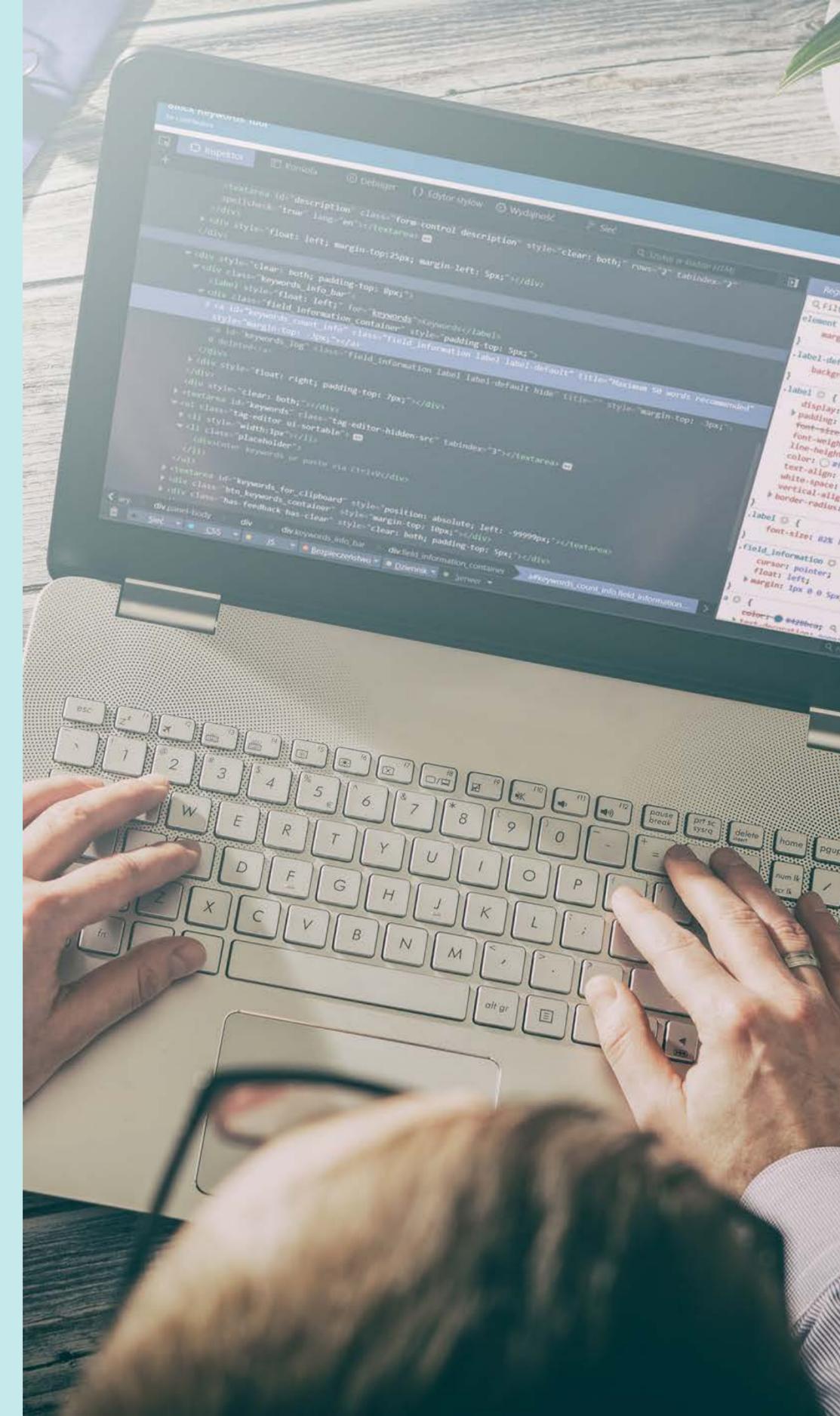
**Selecting Training for a Technology has always been straightforward**

- Progressively more courses from intro to advance, Java for example:  
**Introduction to Java (Course 471)**  
**Advanced Java, Design Patterns & Best Practices (Course 516)**

**Usually Technology is adopted for a purpose**

- Java, for example, is most often used for enterprise web development
- Training would add the following related Java areas:  
**Java Web Development (Course 570)**  
**Java Enterprise Apps (Course 974)**  
**Integrating EJB, JSF, JPA (Course 978)**

**Introduces the concept of a role - in this case, 'Java Enterprise Web Developer'**



# ROLES DEFINITION

## Roles are not jobs or positions

- Often more than one role needed to fill a position

Example: Functional Job = Java Enterprise Web Developer + Agile/Scrum Developer + Soft Skills

## Roles and positions are typically derived from the organization's competency model (skills needed)

- Often self-developed KSAs and tasks at multiple progressive levels
- Creating can be challenging, time consuming and necessary

## In modern times, competency modeling is expedited

- Various Industry Standard Frameworks have appeared
- These have the advantage of saving organizations to create more accurate competency models in significantly less time

## The NIST/NICE National Cybersecurity Workforce Framework is invaluable

- Adoption is widespread and increasing
- Nicely helps answer the question

**“What skills do we need?”**

# NICE FRAMEWORK

**The NICE Framework organizes roles under categories and specialties**

- 50 roles specified as ‘professional’ competencies – meaning technology agnostic
- Full KSAs and tasks are defined for each role

**In a practical sense, for these roles to be deployed within an organization, they need to be expanded to include ‘technical’ competencies**

- Example: how to secure databases is different for SQL Server vs. Oracle
- Depends on the organizations infrastructure

**As organizations adopt the NICE Framework, two additional questions appear:**

**“What skills do we have?”**

**“How do we fill the gaps?”**



# LEARNING PATH EVOLUTION

**As a workforce development company, Learning Tree has strived to provide answers to these questions**

- As early adopters of the NICE Framework, it was recognized that we could not do it all ourselves

**For full coverage, the broader industry offered many useful cyber courses and certifications**

- Some unique, some with overlap, and many at different competency levels and coverage

Gold Learning  
**Microsoft Partner**  
Gold Data Platform  


**ISACA**<sup>®</sup>



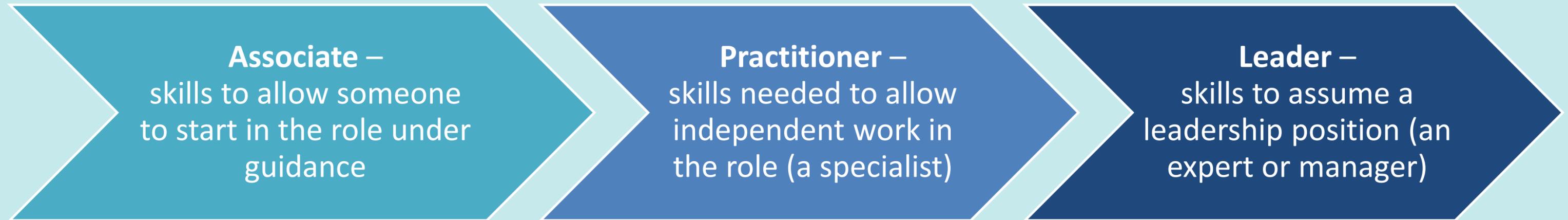
**(ISC)**<sup>2</sup>  
PREFERRED  
OFFICIAL  
TRAINING PROVIDER

**CYBRScore**

(to name a few)

# LEARNING PATH LEVELS

**Customer feedback and training available indicated three levels were needed**



**A collaboration website was created to establish defined paths**

- Initially using ‘concise topic definitions’ and automated tools to compare to NICE Framework skill definitions
- Ultimately validated by subject matter experts
- Development of the paths is ongoing – we encourage you to participate in the evolution

<http://LPaths.org>

# LEARNING PATH BENEFITS

**Primary benefit: provide guidance on how to achieve competency in a role**

- Both individually and as an organization

**Brings an additional question... “Where am I in the learning path?”**

**A significant additional benefit is skills assessment**

- Objective Knowledge Validation to ensure correct placement into a training program
- Courses, certifications, onboarding, coaching and other implementation services

**Learning Tree is committed to providing accurate placement**

- Regardless of the training vendor used
- For more information: <http://learningtree.com/Skills>



# ROLE BASED PATHS & ASSESSMENTS

## Path at Three Levels

- **Foundational** – what is needed to get started
- **Specialist** – needed to be independent practitioner
- **Expert** – what is needed for leadership

## Skills Assessments Aligned to Paths

- Accurate training recommendations

**Cyber Security • 18 Assessments**

- + Depth of Knowledge • 2 Assessments
- Role Based • 16 Assessments
  - + Cyber Help Desk Administrator • 20 minutes
  - + Cyber Security Risk Management Professional • 55 minutes
  - + Cyber Security Strategy Specialist • 30 minutes
  - Digital Forensics Investigator • 20 minutes
    - ▶ Digital Forensics – examiner duties, investigation planning and execution, information acquisition, extraction and analysis methodologies, investigative artifacts, importance prioritization • 15 questions
    - ▶ IT Penetration Testing - tools and techniques to deploy ethical hacking to expose weaknesses in your organization, utilize reconnaissance/published data/scanning tools to gather intelligence, probe/compromise your network using hacking tools, protect against privilege escalation, execute advanced port scanning, hijack web sessions with XSS, modify data flows with man-in-the-middle attacks, defeat stateless firewalls/IDS/anti-virus software. • 15 questions
  - + Endpoint Security Specialist • 30 minutes
  - + Incident Responder • 20 minutes
  - + Information Security Auditor • 20 minutes
  - + Information Systems Security Officer • 20 minutes
  - + Junior Security Analyst • 40 minutes
  - + Network Infrastructure Defender • 30 minutes
  - + Perimeter Security Specialist • 30 minutes
  - + Security Administrator • 75 minutes
  - + Security and Vulnerability Assessor • 30 minutes
  - + Senior Security Analyst • 55 minutes
  - + Software Security Engineer • 30 minutes
  - + Systems Security Analyst • 30 minutes

### Learning Path: Cyber Defense Forensics Analyst



**Category:** Investigate - Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

**Specialty Area:** Digital Forensics - Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

**Role:** IN-FOR-002 Cyber Defense Forensics Analyst - Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Show Course Details To return to the role selection page click [here>>>](#)

Associate / Foundational	Professional / Specialist	Expert / Leader
<p><b>Penetration Testing: Tools and Techniques Learning Tree (LTREE:537)</b> <a href="#">Click for more information &gt;&gt;&gt;</a></p> <p><b>Penetration Testing &amp; Network Exploitation Labs Cyber Score (LTREE:E006)</b> <a href="#">Click for more information &gt;&gt;&gt;</a></p> <p><b>Practical Exam Required</b> Participant must demonstrate their abilities by performing a minimum of two simulations from lab E006 as specified by an expert examiner.</p>	<p><b>Digital Forensics Tools and Techniques Learning Tree (LTREE:2055)</b> <a href="#">Click for more information &gt;&gt;&gt;</a></p> <p><b>Course Exam Required</b> Participant must pass the multiple choice exam from course 2055 with a score of 70% or higher. Exam may be retaken up to three times.</p> <p><b>Digital Media Forensics Lab Cyber Score (LTREE:E004)</b> <a href="#">Click for more information &gt;&gt;&gt;</a></p> <p><b>Practical Exam Required</b> Participant must demonstrate their abilities by performing a minimum of two simulations from lab E004 as specified by an expert examiner.</p>	<p><b>Experience Required:</b> A minimum of 24 months practical experience is required for certification at this level.</p> <p><b>Computer Hacking Forensic Investigator EC-Council (LTREE:2023) CHFI Certification</b> <a href="#">Click for more information &gt;&gt;&gt;</a></p> <p><b>Certification Exam Required</b> Participant must pass the separate certification exam conducted by the EC-Council organization.</p> <p><b>Experience Required:</b> A minimum of 12 months practical experience is required for certification at this level.</p>

Advanced	Daniel demonstrated expert level understanding of Penetration Testing Tools and Techniques (537)
Intermediate	Daniel possesses a good understanding of Digital Forensics Tools and Techniques. It is recommended that Daniel raise his skills through day-to-day on-the-job practice and experience
Primary	
Not-Qualified	Daniel has only modest knowledge of Computer Hacking Forensic Investigator skills. It is recommended that Daniel attend Learning Tree course 2033 and gain the experience to complete the EC-Council CHFI Certification

# SUMMARY – HOW WE CAN HELP

**Learning Tree is a full service provider for workforce development**

- From courses to certifications to coaching
- Enterprise services from LMS integration to skills assessment to implementation workshops

**Proven track record of helping organizations with digital transformation**

- All the training you need at the right time
- Accurate placement for the exact correct path



# QUESTIONS? COMMENTS?

## LET US KNOW!

---



<https://www.learningtree.com/business-solutions/cyber-security-initiative/>