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
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

Effective Training is Key to Providing Needed Protection

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 **

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 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?”
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

(to name a few)
Customer feedback and training available indicated three levels were needed

- **Associate** – skills to allow someone to start in the role under guidance
- **Practitioner** – skills needed to allow independent work in the role (a specialist)
- **Leader** – skills to assume a leadership position (an expert or manager)

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](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 Align to Paths
• Accurate training recommendations

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: IFC-002 Cyber Defense Forensics Analyst - Analyses digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Associate / Foundational
Penetration Testing, Tools and Techniques Learning Tree (LTree: 0571)

Professional / Specialist
Digital Forensics Tools and Techniques Learning Tree (LTree: 0581)

Expert / Leader
Computer Hacking Forensic Investigator EC-Council (LTree: 2023)

Experience Required: A minimum of 24 months practical experience is required for certification at this level.

Skills Assessments
- 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, attack/compromise your network using hacking tools, protect against privilege escalation, execute advanced port scanning, hack web sessions with XSS, modify data flows with man-in-the-middle attacks, deploy stealthy firewalls/IDS/anti-virus software (15 questions)
- Endpoint Security Specialist: 50 minutes
- Incident Responder: 20 minutes
- Information Security Auditor: 20 minutes
- Information Systems Security Officer: 20 minutes
- Junior Security Analyst: 10 minutes
- Network Infrastructure Defender: 30 minutes
- Network Security Specialist: 30 minutes
- Security Administrator: 75 minutes
- Security and Vulnerability Accessor: 30 minutes
- Senior Security Analyst: 55 minutes
- Software Security Engineer: 30 minutes
- Systems Security Analyst: 30 minutes

Accurate to Paths

Depth of Knowledge: 2 Assessments
- Cyber Security • 18 Assessments
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!