



Demystifying Performance-based Training and Testing: Notes Concerning Best Practices

James Stanger, PhD
Senior Director, Products

CompTIA

4 November, 2015

Agenda

We're going to talk about:

**A mature look
at assessment –
the candidate's
journey**

**Using
performance-
based teaching
tools**

**Performance-
based vs. linear
items**

**Statistics and
“efficacy” – and
a bit about
licensure**



jstanger@comptia.org

+1 (360) 970-5357

www.comptia.org

**let's take a look inside the
candidate's journey**

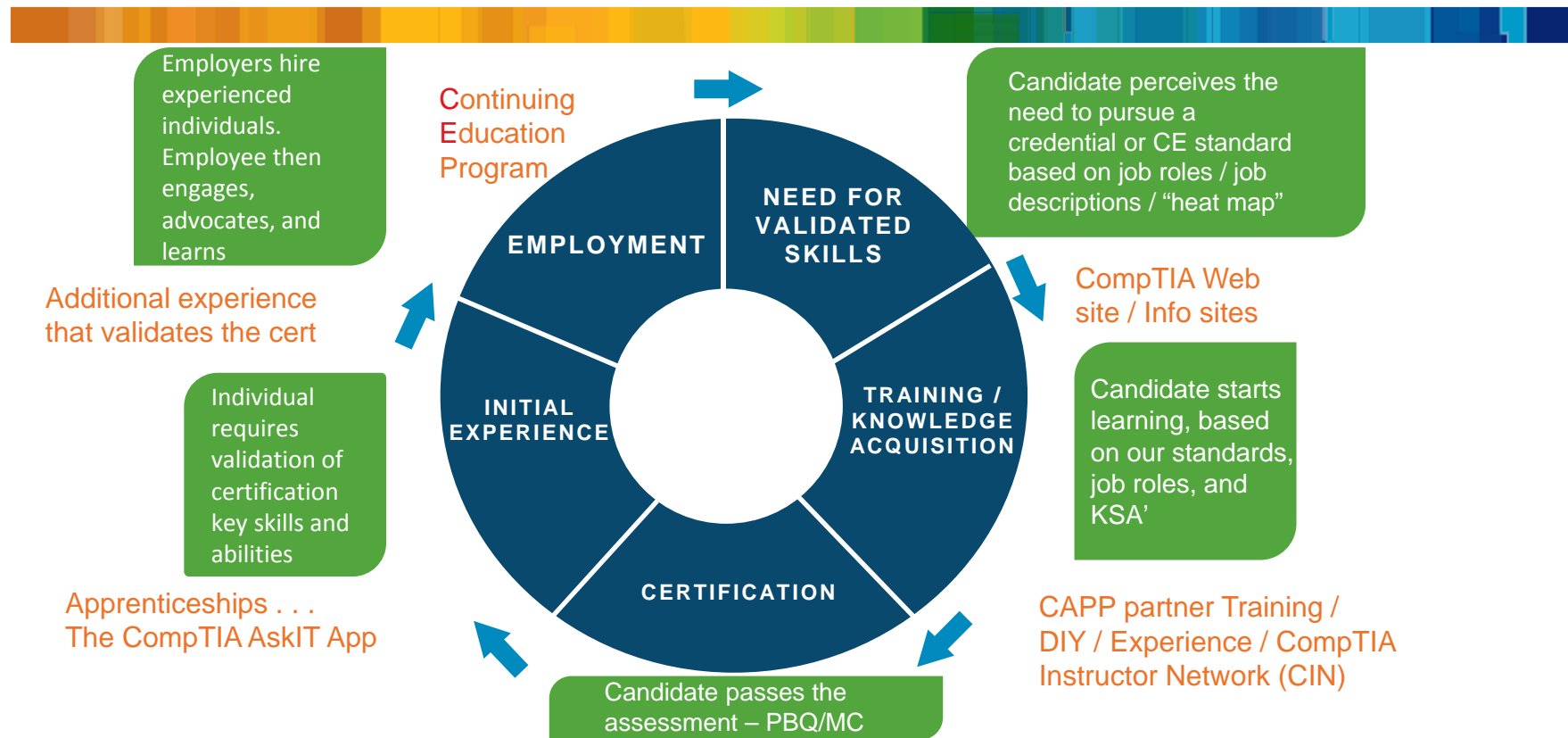
Getting started on the journey

A little story . . .

- Where is the learning path?
- Ups and downs – and sometimes, no real path at all
- Sometimes, just getting going down the right path can be difficult
- How do we help the cyber student find the right path?



The candidate's journey . . .



CompTIA Certifications – a quick overview

Certs in red: *Performance-based*, and also ANSI/ISO certified / US Government 8570

Best Practices

IT Fundamentals
CyberSecure

Professional

A+
Network+
Security+

Project+
Linux+
Server+
Cloud+
Mobility+
CTT+
CDIA+

Mastery

**CompTIA Advanced
Security Practitioner (CASP)**

Specialty

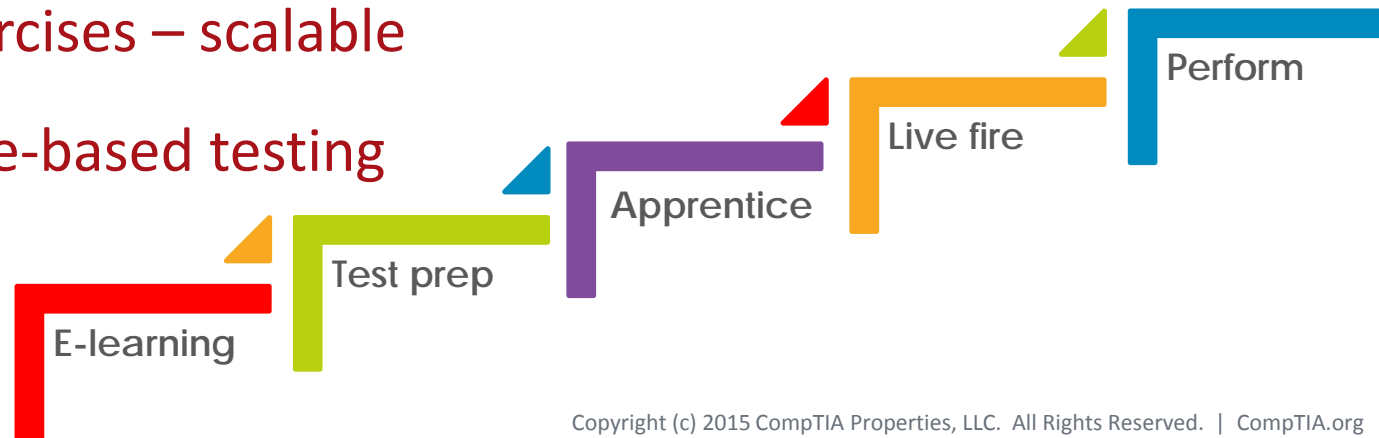
Cloud Essentials
Healthcare IT

trends in assessment – tools of the trade

What does certification mean, really?

It's a question of *“lenses”* and/or *hierarchy*

- E-learning / virtual learning
- Test preparation material
- Apprenticeships
- Live fire exercises – scalable
- Performance-based testing



**job roles – demystifying
the need for “hybrid skills” and
performance-based *everything***

Security+ and job roles

Related job role (JTA)	Descriptions from Dice.com
Security Specialist	Requires an understanding of active directory structure and groups, role based security, and knowledge of various OS system environments (Windows, Linux)
Security Administrator	Responsible for the installation, configuration, maintenance and support of the client's security, network, server and hosting environment
Security Consultant	Requires knowledge of security risk assessment/analysis, encryption, vulnerability scanning/penetration testing, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
Network Administrator	Knowledge of computer LAN systems, network protocols (TCP/IP, EIGRP, BGP, MPLS, etc.), network and device security, bridging, networking monitoring systems, load balancers, routers, and network troubleshooting
Information Assurance (IA) Technician or Manager	Experience with Microsoft Windows OS, active directory, remote desktop, hardware/software troubleshooting, basic network troubleshooting (TCP IP), maintaining and supporting client's security.

Server+ and job roles

Related job role (JTA)	Descriptions from Dice.com
Server Support Technician	Install and maintain servers, network infrastructure and client solutions in a data center. Work with a team of system and network administrators supporting a large and growing hosting network.
Server Administrator	Support the operation of servers on a network. Analyze, diagnose, troubleshoot, and resolve server hardware and software problems. Troubleshoot server configuration errors and hardware performance issues.
IT / Server Technician	Standard rack-n-stack server work. Install new servers. Help maintain server and storage devices.
Storage Administrator	Design, implementation, administration, maintenance, and performance of SAN and NAS storage environments. Troubleshooting, change management coordination, site performance analysis and capacity planning & monitoring.
Storage Server / Systems Administrator	Management and operations of a storage environments.

Linux+ and job roles

Job role	Descriptions from Indeed.com
Systems administrator	Configure Linux systems to support file sharing, databases, and e-commerce solutions. Includes configuring services, DNS, IPv6, DHCP, and enabling storage solutions.
Web systems administrator	Manage DevOps infrastructure, including Apache, Linux and Web services. Work with programmers to quickly establish infrastructure mapped to business needs.
Virtualization/ Linux and Windows administrator	Create and maintain virtual servers, as well as secure systems against intrusion. Create virtualized environments to ensure business continuity. Includes virtualizing Windows and Linux systems.
Intrusion detection technician / analyst / consultant	Enable intrusion detection and honeypot systems, including the Snort IDS. Use logging systems and signature databases to enable scanning of network systems.
Penetration tester	Support Information Technology Services programs which include risk management, compliance management, audits and assessments, client inquiries, and security awareness. Assist in analysis of technology and operational risks to the enterprise.
Linux developer / Mobile app developer / Application engineer	In addition to developing software solutions, the ideal candidate will have a thorough understanding of Linux platforms, including how to navigate the command line.
Storage engineer	Implement SAN and NAS-based solutions on open source and Linux platforms.
© Hadoop administrator	Implement technology to create heat maps, and use MapReduce using Hadoop on Linux.

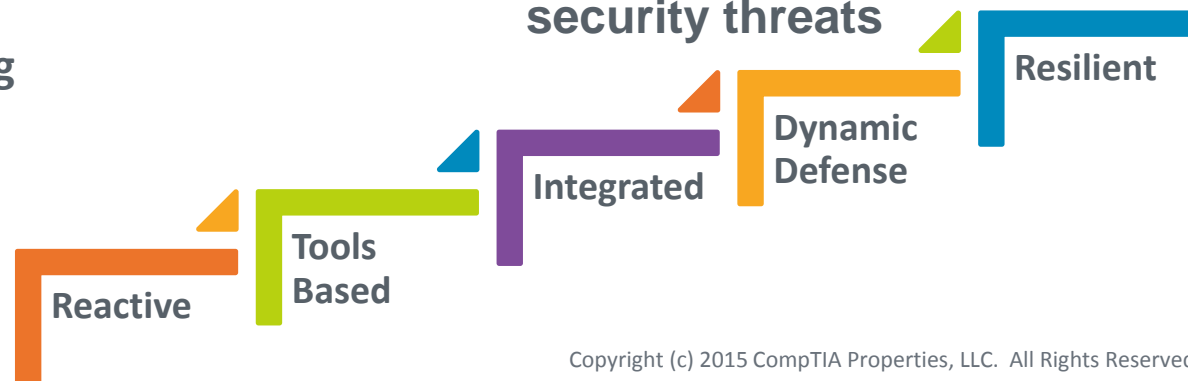
Creating a dynamic defense

- **Focus on being proactive, not reactive**
 - Custom detection tied to actors
- **Detection across attacker lifecycles**
- **Analysis driven**
- **Self-notifying**

Resilience

- Intel-driven
- Anticipatory
- Responsive & Agile
- Externally sharing

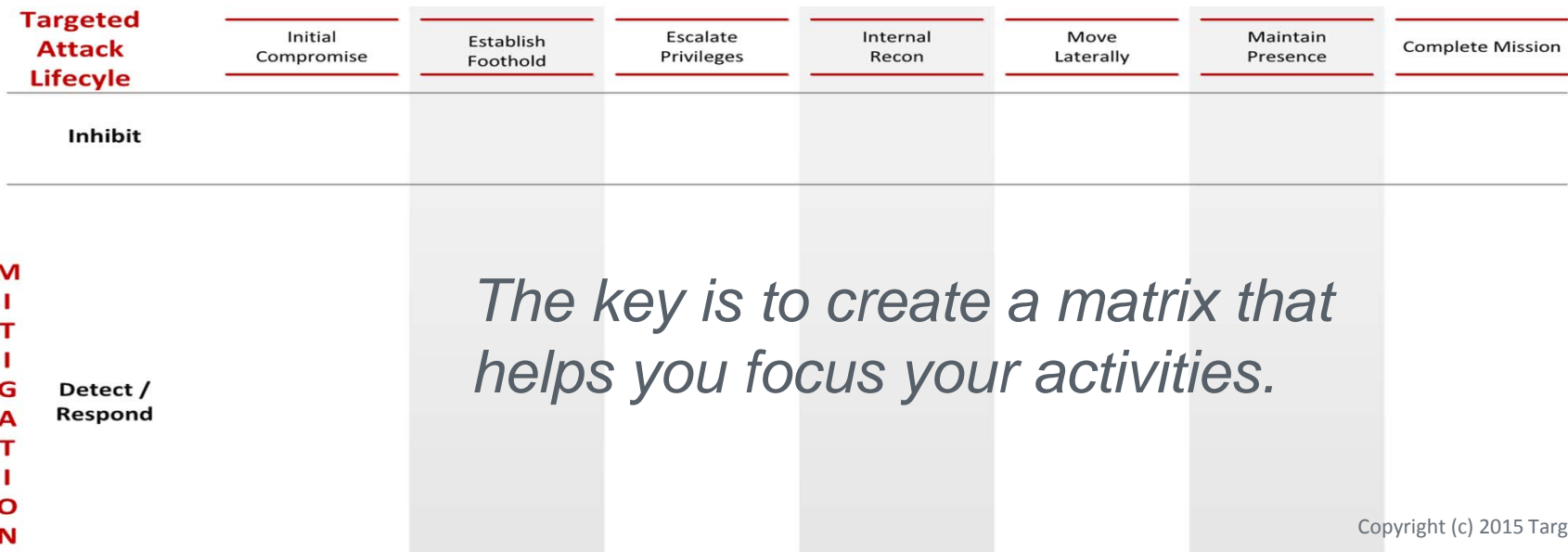
It's all about creating an environment that allows professionals to respond to security threats



Maturing overall operations

It's vital to focus on identifying the hacker cycle

Mitigation involves inhibiting the hacker as well as detection and response



Copyright (c) 2015 Target

Questions to ask when creating a framework

1. How do we detect that initial footprint?
2. How do we detect lateral movement?
3. How do we detect that initial prevention failure?
4. How do you cut down on “dwell time?”
 - Taking dwell time from 14 days to 3 days.
 - What framework and technology can you put in place?

“Dwell time:” The amount of elapsed time between an initial breach to containment



The 80/20 rule: In many cases, organizations are already at the 80% threshold; getting to 90% and above requires hard work and smart allocation of resources.

Who is going to implement this framework?

The wizard/hot shot/
ranger

How can we emerge
from this model?

The collective
approach – *the team*

- The “scruffy expert”
- Appealing to us as a society
 - The “wizard” likes the job security
 - The boss likes the wizard, because he or she receives a sense of certainty and indemnification



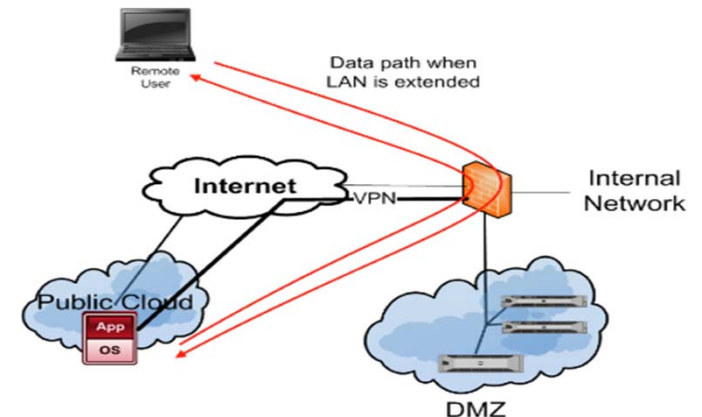
- The expert as “captain” over the “lieutenants,” or as the “quarterback”
- The person who can cut through all of the “white noise” and “fog/TMI”

Red/blue teaming and pen testing

- It's a question of approaches and metaphors
 - Process versus “hot shot” approach.
 - Metrics: Funny how the security industry can't agree on set metrics.
 - Vulnerabilities solved versus information protected. Don't focus on X number of vulnerabilities. It's all about protecting the data where it is, and using that framework.



- Approaches
 - Traditional
 - Cloud – how has this changed auditing procedures?



types of learners – and learning trends

Types of learners

- **A working list**

- Hands-on / physical /task-based (kinesthetic)
- Audio/aural
- Verbal / linguistic
- Visual / spatial
- Solitary vs. social/team
- Logical

- **Some questions**

- What does industry want?
- What is new and hip?
- What does the student need?



Types of learners, cont'd – but is that really the issue?

- **We're really looking for people who can:**
 - Work and play well together
 - Mix with various team members and create custom security solutions
- **Because we believe in the channel,**
 - Instructors can gain intelligence from:
 - What industry wants
 - Teaching tips – from other instructors
 - We influence publishers to create the best tools
 - This includes simulations

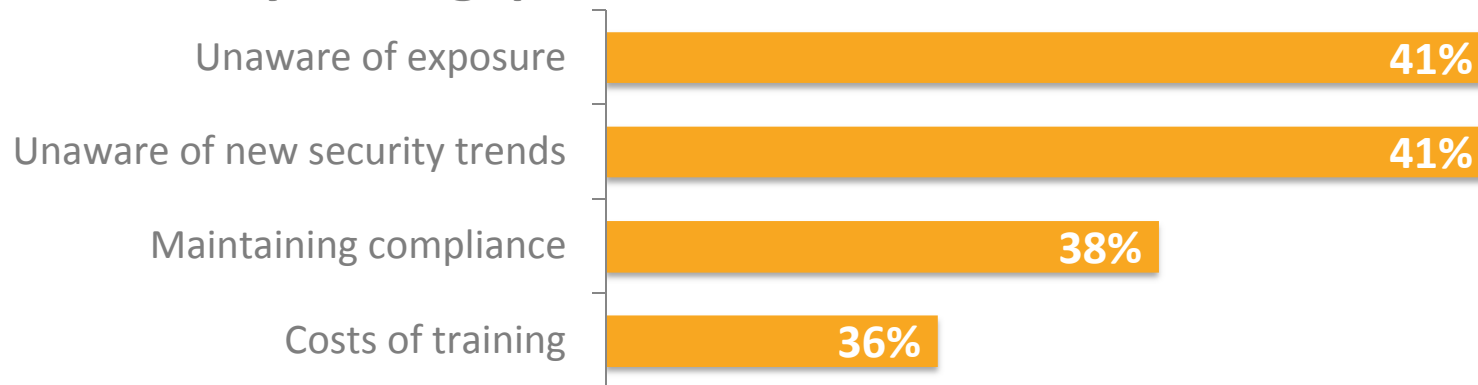


training trends

Let's focus on security in and of itself . . .



Effect of security skills gaps



Current skills

- Firewall
- VPN


New skills

- Data Loss Prevention (DLP)
- Identity and Access Management (IAM)

Repetitive learning

Rejection of traditional learning

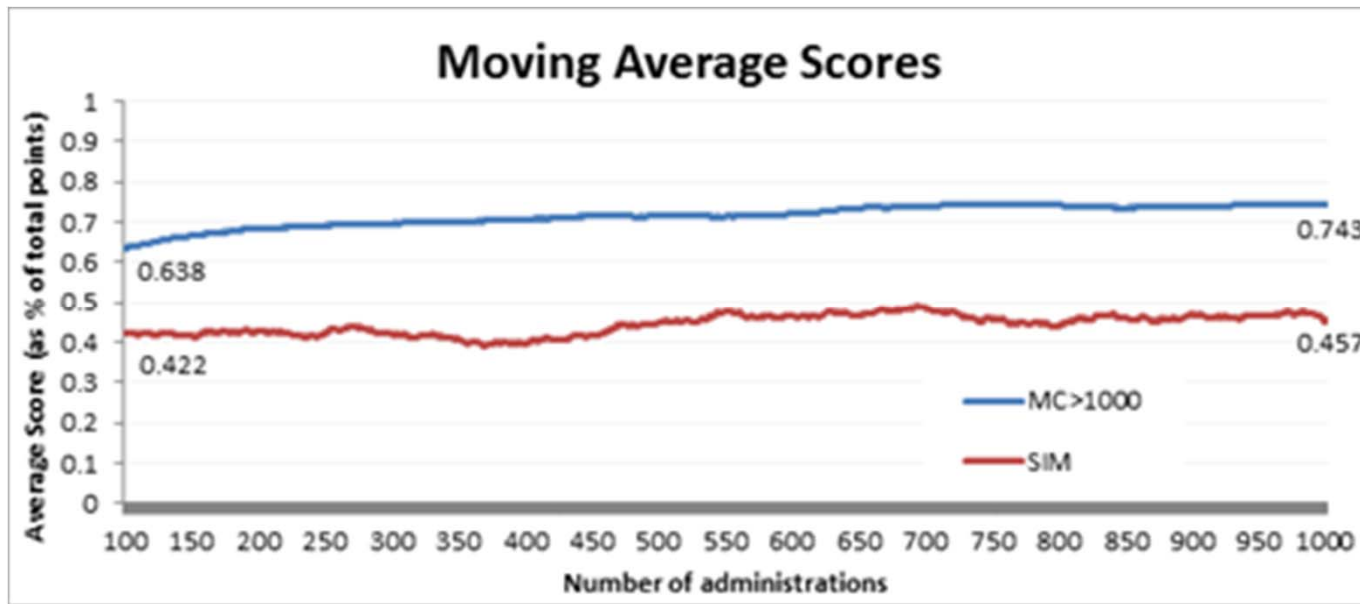
- How do performance-based items help this person from being “bored?”
- How do performance-based items help the industry get the best person for the job?
- How does the right foundation for education help instructors teach better?



“I don’t want to be bored. Show me the important stuff, and don’t dilly dally around.”

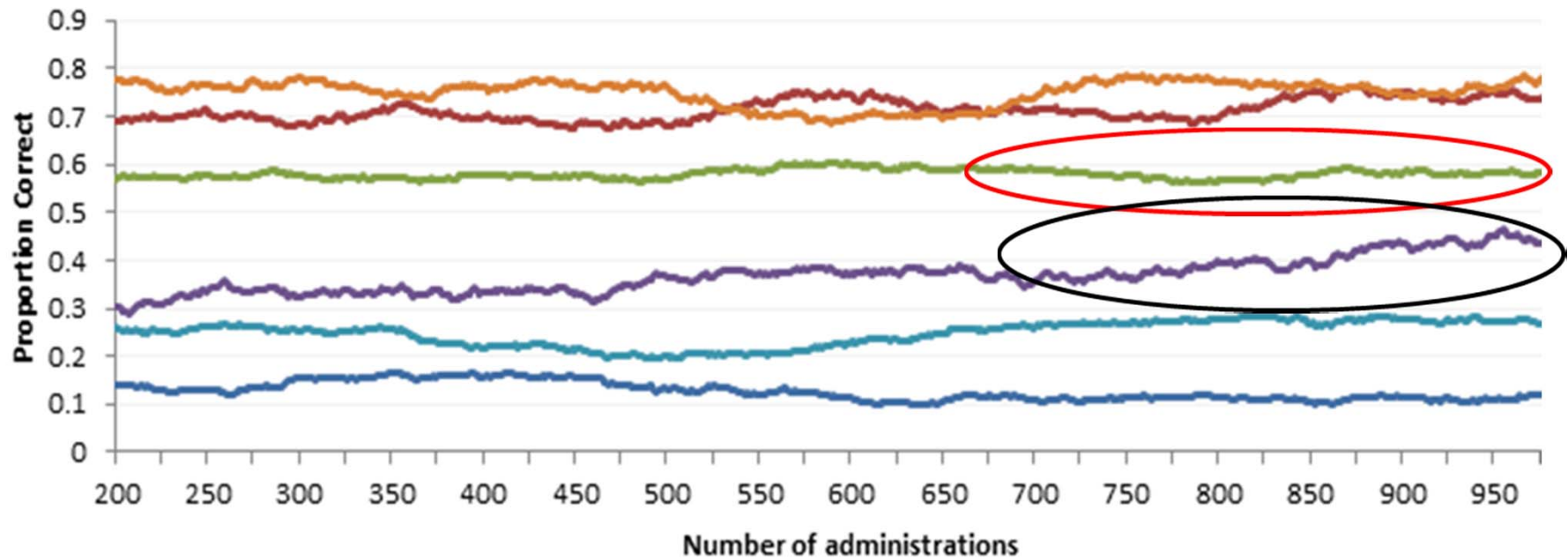
exam statistics and best practices

Performance – PBQ/SIM vs. Linear/MC



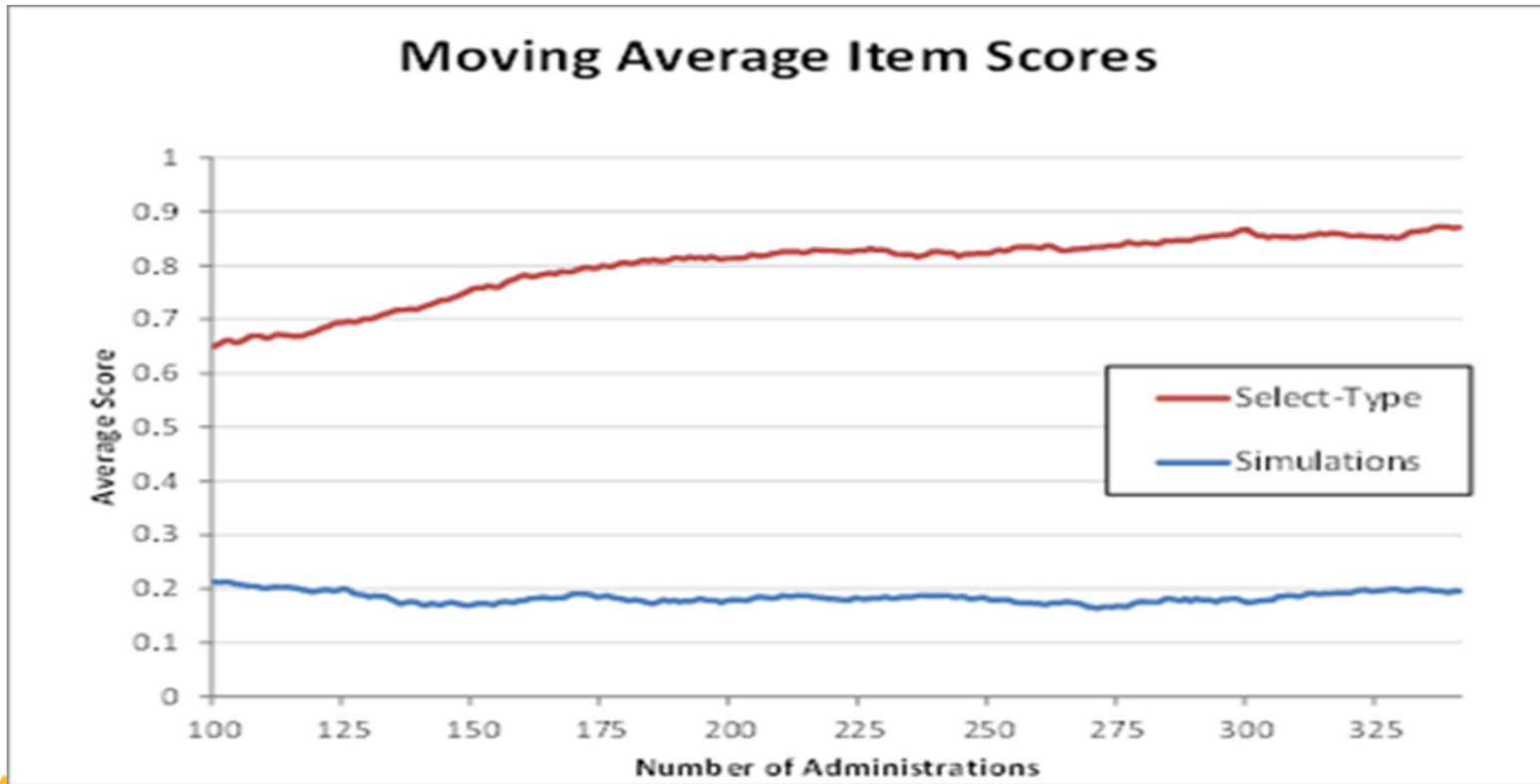
Performance-based items have proven to be less susceptible to exposure even after 500-1000 administrations. Not all performance-based items are created equal, though . . .

Performance – both PBQ

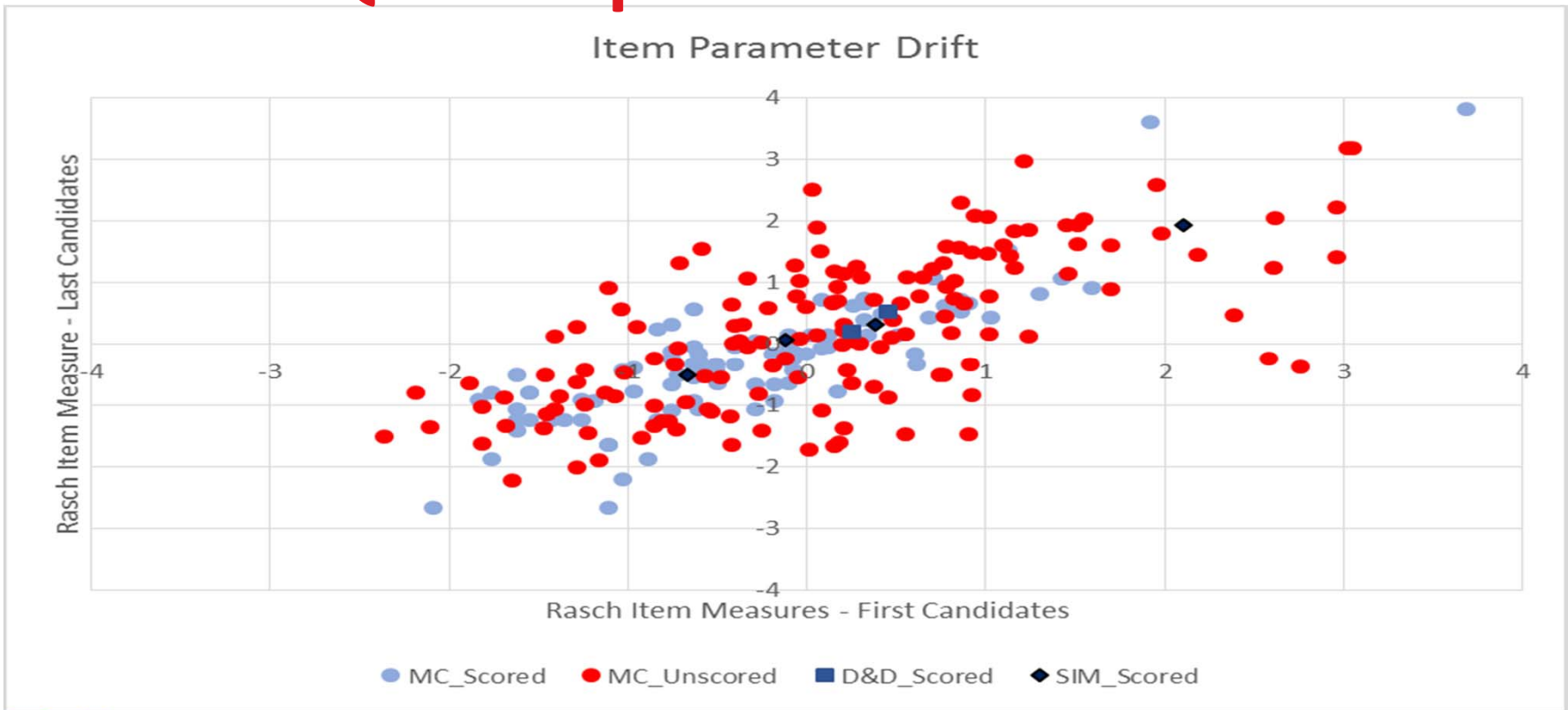


Still, the items that test well perform much better than select type items that seem more susceptible to exposure.

PBQs and performance over time



How PBQ items perform



Less drift – but linear items have their uses, too

Item Type	First 100 Candidates		Last 100 Candidates	
	Avg. Rasch Item Measure	Avg. PTME	Avg. Rasch Item Measure	Avg. PTME
Scored - Simulation	0.42	0.36	0.45	0.44
Scored - Drag & Drop	0.35	0.38	0.37	0.42
Unscored - Multiple Choice	0.18	0.28	0.14	0.28
Scored - Multiple Choice	-0.34	0.33	-0.27	0.28



Takeaways

- Performance based items have their place.
 - Longer shelf life
 - Face validity
 - Increased satisfaction
- Text Based items have their place.
 - Quicker to develop
 - Appropriate for certain objectives
 - Cost effective

Mature programs are able to prove these conclusions. We've been using performance-based items now for five years.

But, this is a bit “wonky,” in that it focuses on exam stats. What does the certification actually do for individuals in the field and for organizations that need to improve security?

applying the concepts – some “war stories”

Team building and testing

- Why has hands-on learning become such a focus?
- Is it to help convert the certification “naysayers?”
- No, it is here to help build a team ethos



Types of learners – is that really the issue?

- **Joint Base Lewis-McChord and Hill Airforce Base**
 - Airforce – they wanted to know the industry
 - The “retiree” in Washington state who became a consultant
- **High schools in the greater DC area - 2012**
 - Virtual classroom for a “train the trainer” session
 - Taught instructors industry standards (Security+)
- **New Horizons – “flipping the classroom”**

What great teaching programs have in common...

- Celebrate student success (T-shirts, Tweets, framed certificates, and more)
- Practice exams
- Use great materials
- Track pass/fail rates
- Instructors are certified
- Focus on get a job
- Create community
- Lead with a problem rather than lead with content
- Provide problem-oriented real life experiences

Terrific tips from Jean Andrews, an instructor and author in our channel



Lead with the problem



Assignment
or goal

Project or Problem

- A security incident
- Upgrading a service pack level
- Using virtualization to enable redundancy

Inquiry
Learning

Use as
needed

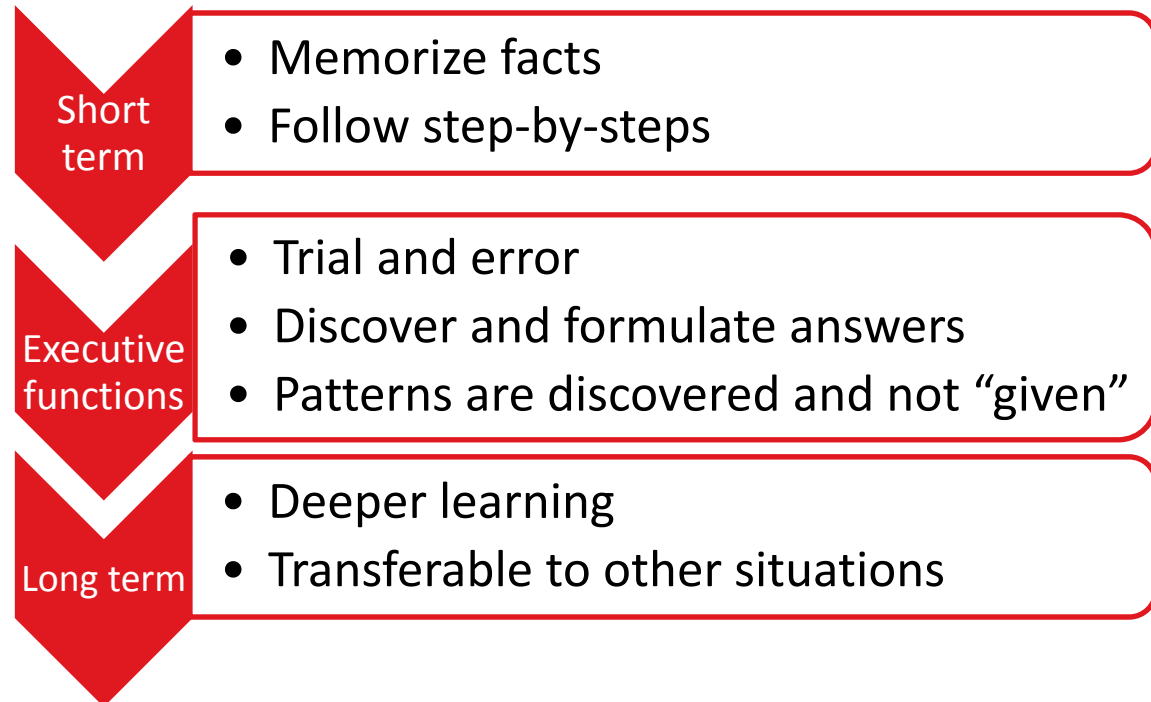
Resources/Knowledge Base

- Videos/lectures/tutorials
- Example solutions
- Step-by-steps
- Explanations
- Google it
- eBook



Flipping the classroom

Why flip?



SO THAT MORE LEARNING GOES FROM SHORT-TERM TO LONG-TERM MEMORY



Who or what is driving?

The key to hands-on, experiential learning is allowing the student to take the wheel



- Organize your course by projects and activities rather than by the textbook
- Make resources available to students and turn them loose to work
- Allow students to self pace and help each other
- Coach from the sidelines
- Lecture only when students are stuck and then only to a few

Scenario: S0620 User says computer needs more memory

Step: 2: Open and Review Ticket

Quiz

Show Me

eBook

?

Score: 12

Scenario Description

Company Background

Who's Who

Case Study

Instructions for Step 2

Open Ticket S0620 and read the description of the problem or request, noting the name of the user who initiated the ticket. Close the application when you're finished.

Project or Problem

Click here and drag to reposition window

The screenshot shows a web browser window with the URL localhost:8080/ehelpdesk/home.gml. The page features a navigation menu with options like 'My Tickets', 'New Ticket', 'Search', 'Filters', 'Reports', 'Knowledgebase', 'Dashboards', and 'Templates'. A search bar is present with the text 'Ticket Search'. Below the navigation, there's a welcome message for 'Paul Robertson' and a 'Sign out' button. A notification banner reads 'Welcome to the Bonanza Mining Corporation Call Tracking System'. The main content area is titled 'My Tickets' and displays a table of tickets. The table has columns for Priority, Ticket Number, Subject, Category, Contact, Location, Assigned To, and Actions. The ticket S0620 is highlighted in blue.

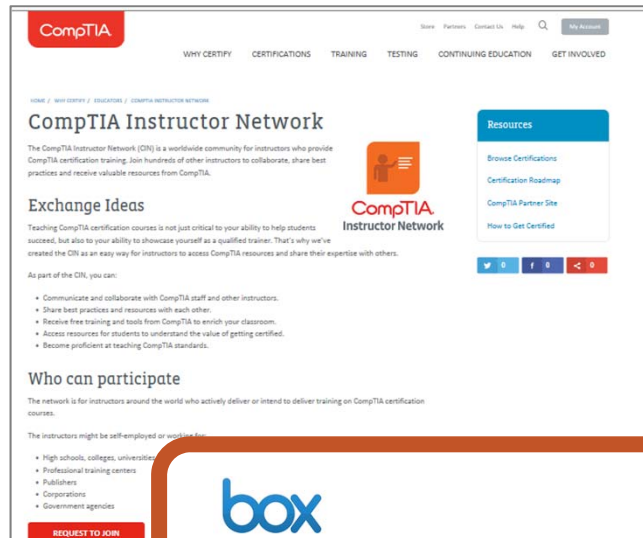
Priority	Ticket Number	Subject	Category	Contact	Location	Assigned To	Actions
	S0590	Install network printer on training computer in Sales	End User Support	Helen Cartwright	San Francisco	Paul Robertson	
	S0600	Training Center Module on Good Customer Relations	Maintenance	Victor Sanchez	Philadelphia	Paul Robertson	
	S0610	Inventory motherboards in server closet	Maintenance	Victor Sanchez	Philadelphia	Paul Robertson	
	S0620	Computer needs more memory	End User Support	Ken Blocker	San Francisco	Paul Robertson	
	S0630	User says his Aero interface doesn't work	End User Support	Michael Green	Philadelphia	Paul Robertson	
	S0630	Users says his Aero interface doesn't work	End User Support	Michael Green	Philadelphia	Paul Robertson	
	S0680	Inventory expansion cards in server closet	Maintenance	Victor Sanchez	Philadelphia	Paul Robertson	
	S0050	User's video is not working	End User Support	Annette Cruz	Philadelphia	Paul Robertson	
	S0700	System doesn't recognize DVD drive	End User Support	John Withers	San Francisco	Paul Robertson	

Social engineering – help desk

empowering instructors

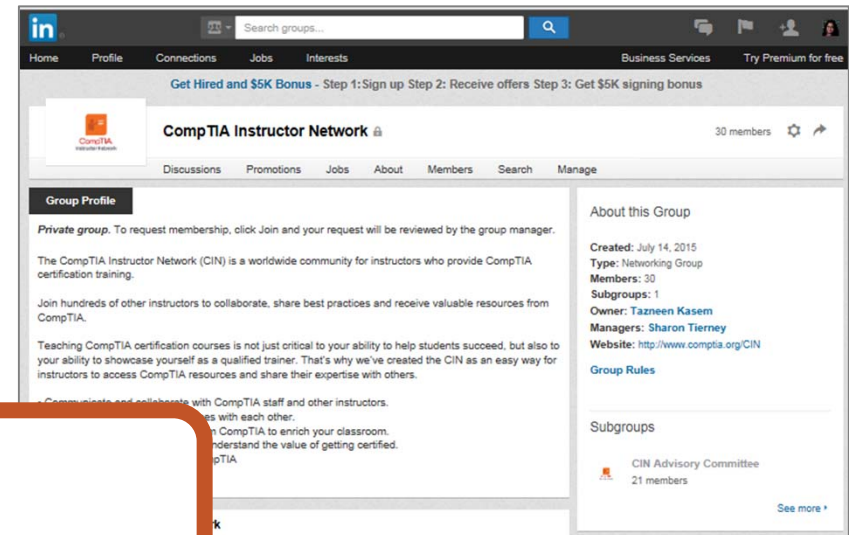
How do you join?

www.comptia.org/CIN



The screenshot shows the CompTIA Instructor Network website. The header includes the CompTIA logo and navigation links: WHY CERTIFY, CERTIFICATIONS, TRAINING, TESTING, CONTINUING EDUCATION, and GET INVOLVED. The main content area features the title "CompTIA Instructor Network" and a description: "The CompTIA Instructor Network (CIN) is a worldwide community for instructors who provide CompTIA certification training. Join hundreds of other instructors to collaborate, share best practices and receive valuable resources from CompTIA." Below this is a "Resources" sidebar with links for "Browse Certifications", "Certification Roadmap", "CompTIA Partner Site", and "How to Get Certified". A "Who can participate" section lists various roles like high schools, colleges, universities, professional training centers, publishers, corporations, and government agencies. A red "REQUEST TO JOIN" button is visible at the bottom.

<https://www.linkedin.com/grps/CompTIA-Instructor-Network-8350296/about?>



The screenshot shows the LinkedIn group page for "CompTIA Instructor Network". The page header includes the LinkedIn logo, search bar, and navigation links: Home, Profile, Connections, Jobs, Interests, Business Services, and Try Premium for free. The group name "CompTIA Instructor Network" is displayed with 30 members. Below the name are tabs for Discussions, Promotions, Jobs, About, Members, Search, and Manage. The "Group Profile" section is active, showing a "Private group" status and a description: "The CompTIA Instructor Network (CIN) is a worldwide community for instructors who provide CompTIA certification training." It also lists the group's owner, Tazneen Kasem, and the website URL: http://www.comptia.org/CIN. A "Subgroups" section lists the "CIN Advisory Committee" with 21 members.



<https://app.box.com/Instructor-Resources>

licensure

Licensure

- **Definition**

- State-issued, time-based credential
- For professionals – not student



Certification
and Licensure

- **Some caveats**

- The security industry has not matured
- Change is constant
- Can you apply licensure to something changing so quickly?
- Who will apply licensure?

Conclusions

Some things to consider

- **Call for participants**
 - Performance-based, “live labs”
 - We will apply metrics
 - We have instructors lined up
 - Contact me to participate
- **Performance based learning and testing is useful when:**
 - Building teams
 - Ensuring students actually learn the concepts
- **Is performance-based testing an all-encompassing panacea?**
 - No – use the right tool for the right job
 - Metrics are essential



QUESTIONS?



James Stanger
jstanger@comptia.org
Skype: stangernet

To learn more about CompTIA, please go to the following URL:
www.comptia.org

Thank you!