Training Technical Teams

The rocket science behind the “awareness”

SECURITY INNOVATION

About Ed Adams

- CEO, Security Innovation Inc.
- Host of Ed TALKS: www.edtalks.io
- Director, ICMCP
- Research Fellow, Ponemon Institute
- Privacy by Design Ambassador, Canada
- Mechanical Engineer, Software Engineer
- In younger days, built non-lethal weapons systems for government & law enforcement

International Consortium of Minority CYBERSECURITY PROFESSIONALS

About Security Innovation

- Securing software in challenging places….

- Helping clients get smarter about software security
  - **Assessment:** show me the gaps
  - **Standards:** set goals and make it easy
  - **Training:** enable me to make good decisions

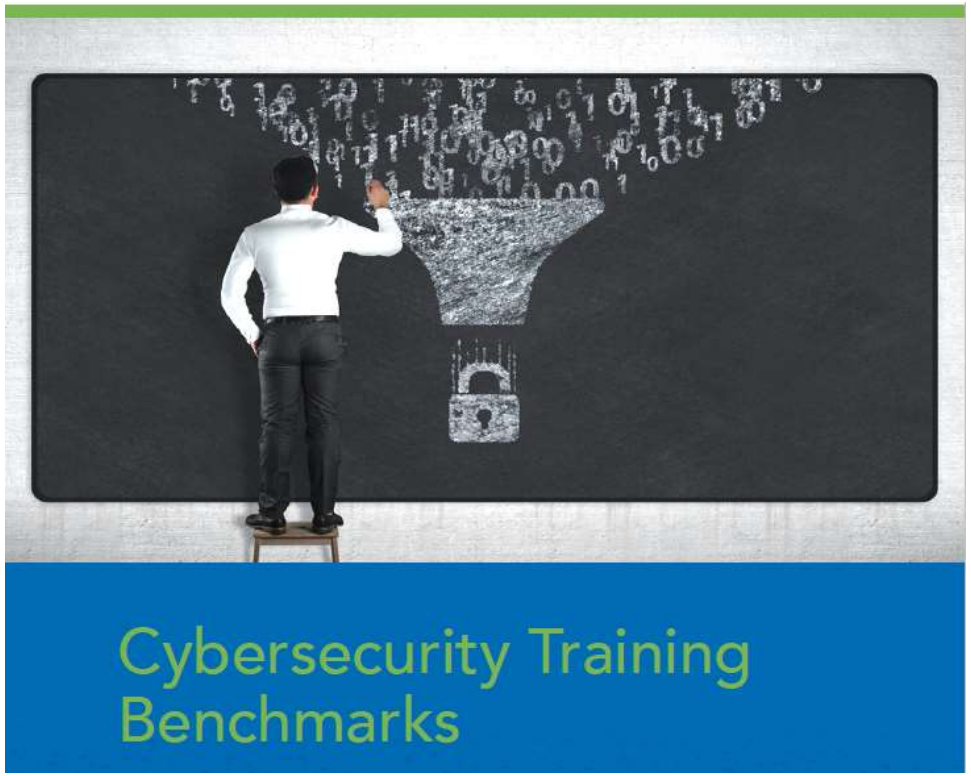
Over
3 Million
Users

Authored
18
Books

Named
6x
Gartner MQ

SECURITY INNOVATION

Recent Research from The Ponemon Institute



- Assessed programs on 17 key elements
- Measures Security Effectiveness Score (SES)
  - High SES Score Correlates to Lower *Mean Time to Find & Fix* and *Data Breaches*
- Some training practices proven more effective than others

https://web.securityinnovation.com/hubfs/cybersecurity-training-benchmarks-2020.pdf

SECURITY INNOVATION

17 Elements (aka “best practices)

Content

1. Training includes realistic simulation
2. Training content fits the learner's role
3. Training is attached to actual events
4. Self-study option is available
5. Content is in the natural language of the learner

Measurement

6. Methods are available to measure effectiveness
7. Learning gains and retention are measured
8. Immediate feedback is given to the learner

Governance and delivery

9. Results are reported to C-level executives
10. Training is mandatory
11. Training is part of the on-boarding process
12. Rollout of the program is top down
13. Training program is updated at least once a year
14. Training requirements cannot be waived
15. Training is conducted at least once per year
16. Training venue is an in-person meeting or classroom
17. Train-the-trainer and/or apprenticeship delivery options are available

Training Benchmarks - What's Most Effective

- 1 = low effectiveness
- 10 = high effectiveness

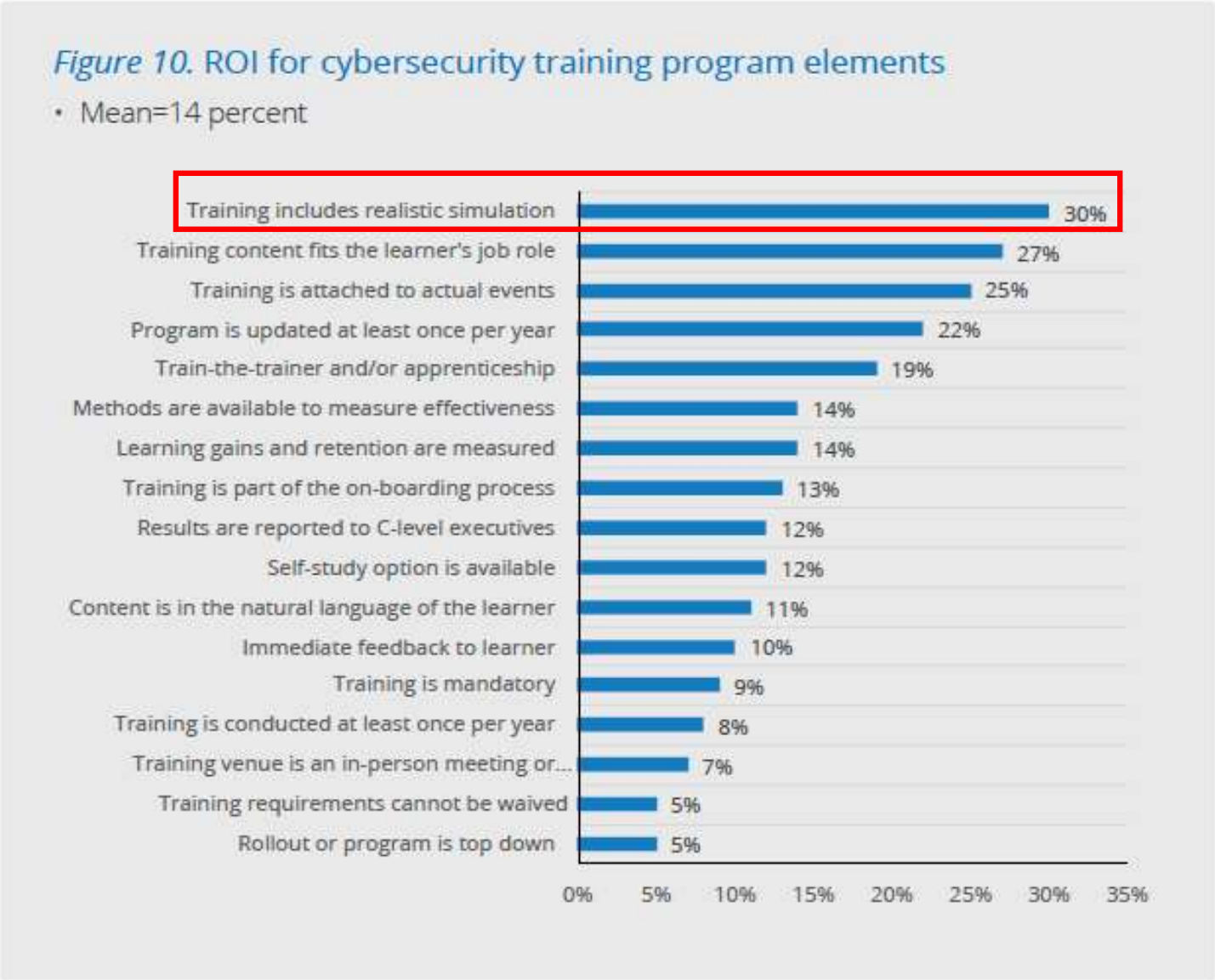
Realistic Simulation

and

Training Tied to Job Role

are most effective

Realistic Simulation Yields 2X ROI vs. Average Element



"Regardless of spend or program size, realistic simulation and job-specific training are the most effective way to build lasting skills, raise security effectiveness scores (SES) and yield higher ROI."

- Dr. Larry Ponemon

SECURITY INNOVATION

Simulation Training in Practice – Does it Work?

Which values did you receive from Cyber Range events? (check all that apply, 120 surveyed)

"By 2022, 15% of large enterprises will be using cyber ranges to Develop Security Skills"

- *Gartner Boost Resilience and Digital Dexterity With Cyber Ranges*

SECURITY INNOVATION

Why Job Specific Training is Necessary

Take the concepts behind modern cryptography

Role	Needs to Know
Developer	• Which cryptographic standards to use and which to avoid • Homegrown cryptography is always a bad idea
IT Operator	• Details about appropriate key management • Why they should never put keys on publicly accessible cloud stores
GRC Manager	• Basics in how cryptography works • For which data and risk environments encryption is necessary for compliance or mandated by law

"Not only is job specific training a critical success factor, but it's important that all technical stakeholders are trained because attackers exploit mistakes your team makes collectively"

- Dr. Larry Ponemon

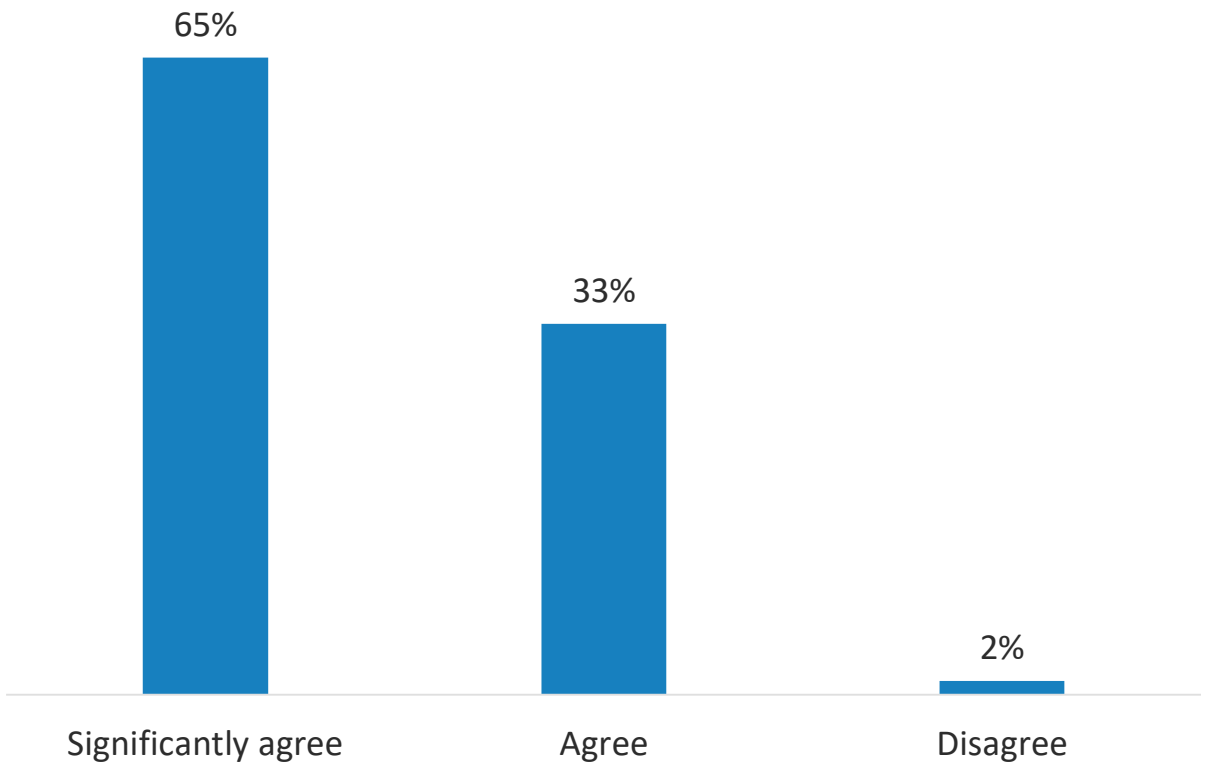
SECURITY INNOVATION

Sample Role-Based Training

	ARCHITECT	DEVELOPER	TESTER/QA	SECURITY MANAGER
INTRODUCTORY	Fundamentals of Secure Architecture	Fundamentals of Application Security	Fundamentals of Security Testing	Fundamentals of Application Security
CORE	Architecture Risk Analysis	Creating Secure .NET Code	Classes of Security Defects	SDLC Gap Analysis & Remediation
SPECIALIZED	Attack Surface Reduction	Conducting a Security Code Review	AppSec Testing – Tools & Techniques	Creating AppSec Design Requirements

Blended Training Reaches Different Learners

To what level do you agree the combination of hands-on Cyber Range experience with Computer Based Training will maximize the knowledge adoption?



Nearly 2/3 respondents "significantly agree" the combination of Cyber Range with CBT will maximize the knowledge adoption

- 98% agree or significantly agree

SECURITY INNOVATION

Poster Child for Best Practices

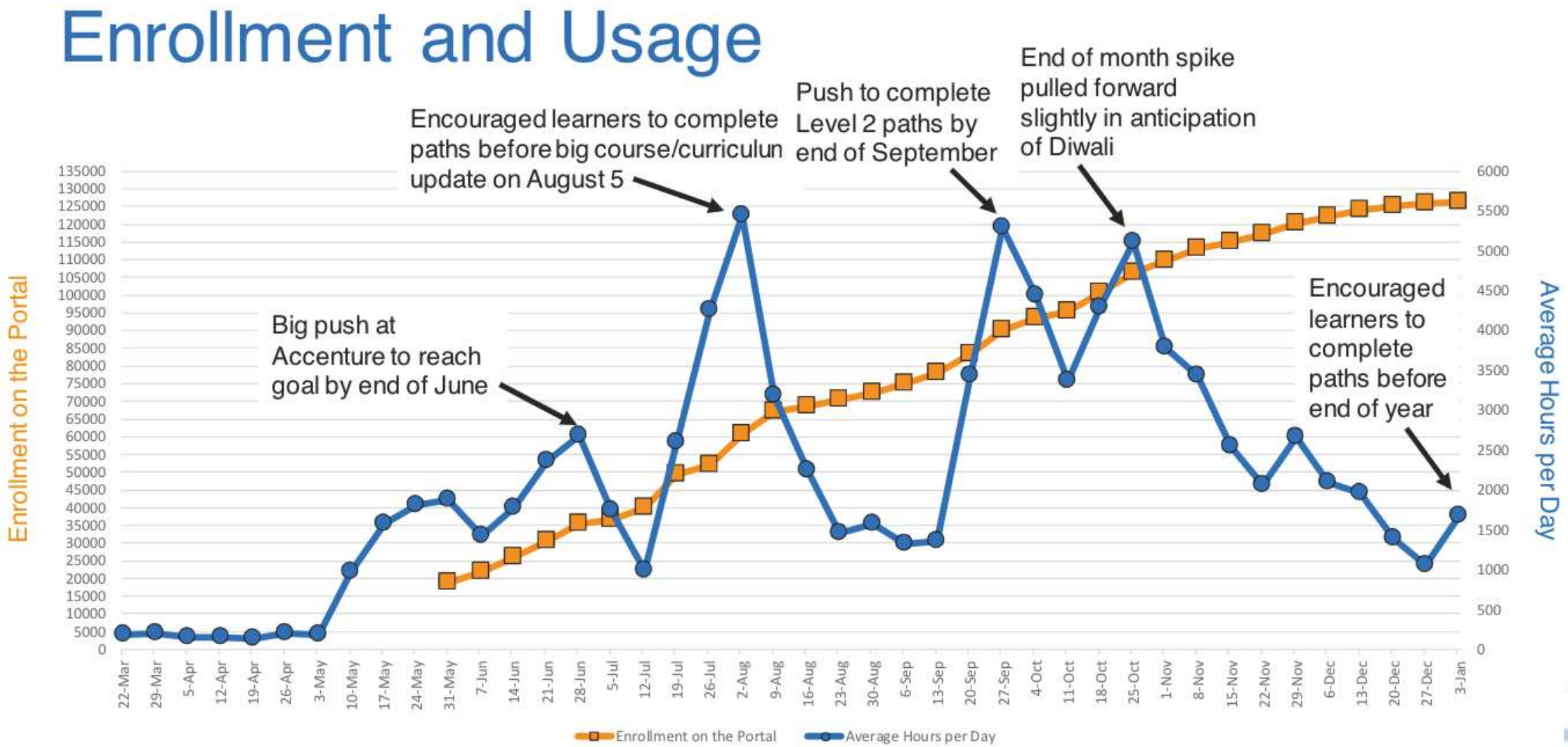
accenture

- Sought to train 80,000 dev team members
  - Staff in 12 different countries
  - Over 50 job functions
  - Varying maturity levels

	Actual Number of Learners Completed	Goal
Level 1	96,551	70,000
Level 2	7,902	7,000
Level 3	5,818	350

- We devised a plan with:
  - Learning paths for 24 roles based on 3 skill levels
  - CBT coupled with a “practice area” using CMD+CTRL Cyber Range
  - Pilot programs to ensure seamless rollout for larger audiences
  - Post-training assessments to determine if users should advance to next level
  - Communication plans with emails, social media posts, and scheduled prompts

Why Goal Setting is Critical



Motivate Teams

- Learning media should be ***mixed*** and ***tailored*** to specific roles
  - ILT, CBT, standards, reference guides
- Use examples from your own environment if possible
- Add Learning Milestones to make goals feel reachable
- Short, focused modules to maintain attention span
- Use incentives like belts, badges, and other recognition

SECURITY INNOVATION

Gartner recommends “Belt” program*

Level	Guideline Training Prerequisites	Advancement and Improvement	Application Security Task to Maintain Level
Blue Belt	• Completed **10** training courses • Basic secure coding training including OWASP Top 10	• Compete in **3** CTFs and average score of **500** • **10** code sprints with no high-severity vulnerabilities	• Assist in gathering security testing requirements for applications relevant to their domain
Purple Belt	• Completed **15** training courses • Advanced training on specific vulnerability types, security architecture and/or language specifics	• Compete in **5** CTFs and average score of **1,000** • **25** code sprints with no high-severity vulnerabilities	• Provide feedback into secure coding practices and annual reviews • Assist with AST remediation activity for applications relevant to their domain
Brown Belt	• Completed **20** training courses	• Compete in **5** CTFs and place in **top 10**. • **50** code sprints with no high-severity vulnerabilities	• Assist with drafting secure coding practices • Perform AST remediation activity independently for applications relevant to their domain
Black Belt	• Completed **25** training courses • Industry certification or presented on topics related to secure coding or design	• Train others • Create improved practices	• Serve as authors or custodians for secure coding practices in their domain • Generate threat models for applications relevant to their domain

- Citrix had 80% participation in 2-year belt program
- Combined belt program with financial compensation
- Tied black belt status to promotion eligibility

**Report: “3 Steps to Integrate Security into DevOps”*
- 2020

SECURITY INNOVATION

6 Techie Training Program Best Practices

1. Executive Management sets the mandate
2. Root in company goals, policies, and standards
3. Ensure company-culture relevance
4. Tie to HR/advancement programs
5. Ensure content is relevant to technologies and platforms teams work with/in
6. Start with 5-20% target audience and adjust

SECURITY INNOVATION

Quick-start Steps

Assessment

Stakeholders, roles, and technologies to create objectives

Pilot Program

Few learners representing different audiences delineated by the assessment.

Rapid Prototyping

Use pilot results to tweak modules included within certain learning plans

Feedback Loop

Examine feedback on modules to further tweak paths and expand to other roles

Concept Reinforcement

Reinforce training with blended learning opportunities wherever possible

Putting it All Together

- Deploys Blended Learning
  - CBT plus hands-on Cyber Range exercises
- Measures Knowledge Gains and Retention
  - When combined with CBT, Cyber Range scores increased avg of 25%
  - Benchmark: Cyber Range scores 2,000+ for software engineers → no additional training
- Features Simulation, relevant to role and company culture
  - Hands-on cyber range events are challenging, fun, cool/trendy
  - Corporate executive always kicks-off/endorses program
- Recurring Training (not point-in-time)
  - Blended learning program offered every month
  - Average score *increase* for second cyber range event was 71%