SECURITY INNOVATION

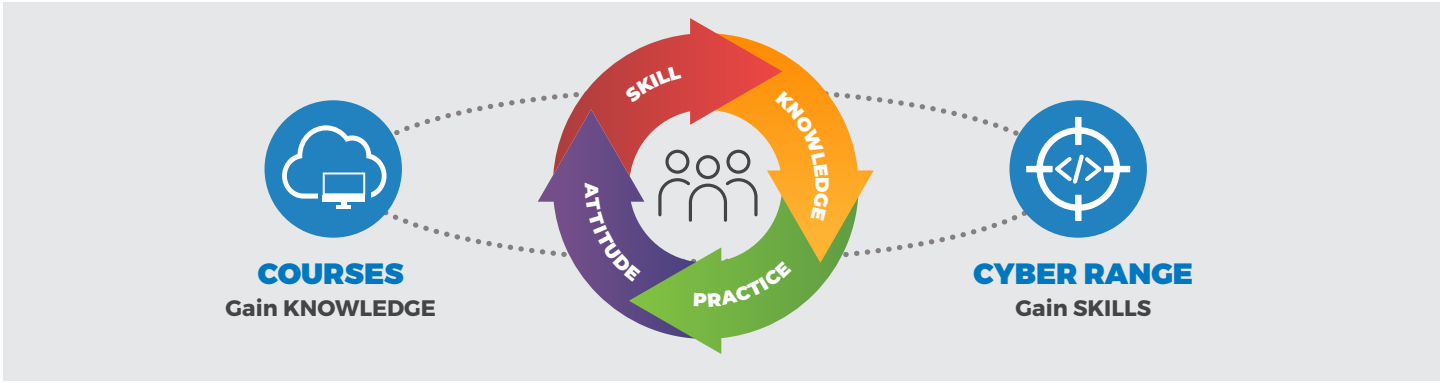
CMD + CTRL TRAINING - CLIENT SUCCESS

Reducing IoT & Cloud Risk in HealthTech

Ramping teams up with the right training blend

Cloud migration is happening fast across most businesses. For this growing healthcare company, what once could be handled by the InfoSec team became problematic as more lines of business accelerated cloud adoption. Additionally, recent attacks on Healthcare Devices fueled the need to build and maintain secure software.

To up level skills in an engaging way, a blend of self-paced courses and hands-on cyber ranges was the solution.



Getting to the Payoff: A Complex but Achievable Task

Like many organizations, disparate groups handled security differently. Some utilized DevOps, others had hybrid IoT/ cloud deployments, and all were struggling to secure APIs.This common scenario creates risk if not addressed holistically.

This company had added complexities including:

- Multiple roles and shared resources for cloud systems
- New technologies being rolled out regularly, with little understanding of risk
- Developers not utilizing cloud security controls when building applications
- Risk management pushing alignment with OWASP, MITRE ATT&CK and ISO

Above all, management sought a phased approach that would enable attainment of short-term goals without overwhelming teams in the process.

The training plan included role- and technology-specific learning paths for the development, operations and security teams. Those paths were complemented by real-time assessments on cyber range technology environments that provided valuable insight into how each team was progressing.

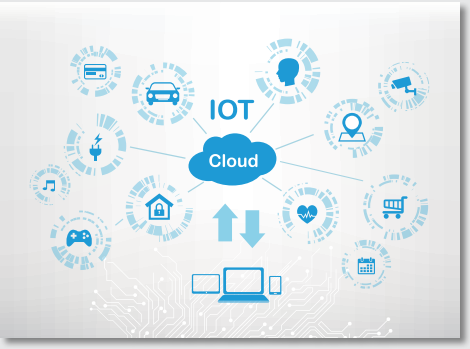
The Journey to Healthcare Cloud Security Excellence

1 Build Cloud & IoT Security Awareness

PURPOSE - Ensure security basics (including DevOps) are understood across teams.

HOW - CBT courses applicable to all roles and responsibilities

- Fundamentals of Application Security
- Fundamentals of Secure Cloud Development
- Fundamentals of DB Security
- Fundamentals of DevSecOps
- OWASP IoT Top Ten
- Meeting Cloud Governance Requirements

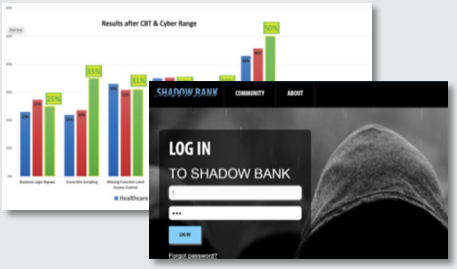


2 Benchmark Skills

PURPOSE - Baseline against industry standards, set goals for outcomes, and design individual learning paths from results.

HOW - ShadowBank cyber range, a fully-featured Web application with poorly implemented security principles and vulnerabilities.

Detailed reports baselined staff risk, described next steps, and tracked against goals.



3 Milestone- Status Check

Driven by cyber range performance and target goals, learning paths were tweaked. Those needing deeper expertise moved on to specialized training.

Rank	Points	Handle	Full Name
1	11230	3.WonderWoman	Jane Doe
2	10330	0_hackman	Joe Doe
3	8770	0_Malwark	Jeff Doe
4	8730	2-PillPushrMorpheus	John Doe
5	8430	2-IceGal	Jen Doe

4 Build Specialized Skills

PURPOSE - Ensure staff can conduct security activities specific to their job function and tech stack. This is critical to engagement and knowledge retention - a"one size fits all" approach would not yield the desired results.

HOW - Role- and technology-specific courses:

Developers
- Creating Secure AWS, Web API, Python Apps
- Protecting Java Backend Services
- Securing API Gateways in DevSecOps
- DevSecOps in the AWS Cloud

Operations/IT
- Automating Security Updates, Testing and CI/CD
- Securing Infrastructure Architecture
- Protecting Cloud Infrastructure
- Hardening Linux/Unix Systems

Architects
- Threats to Containers and Data in DevSecOps
- Fundamentals of IoT Architecture & Design
- Protecting Microservices and Orchestration

InfoSec
- Implementing Controls within the RMF
- Application & Infrastructure Pen Testing
- Orchestrating Secure System & Service Configuration

5 Elevate Expertise with Cyber Ranges

PURPOSE

Move towards cloud security excellence by further honing the skill sets to bring specific teams to elite status utilizing organizational and industry benchmarks.

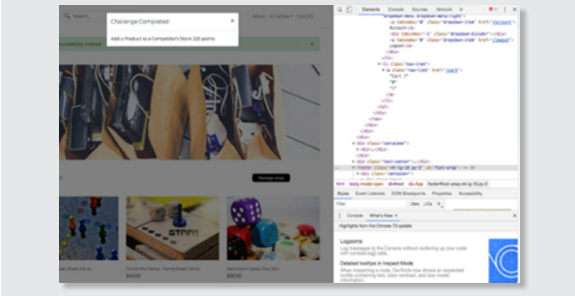
Compare against industry-leading DEFCON players

HOW

Role-based cyber range play

Builders

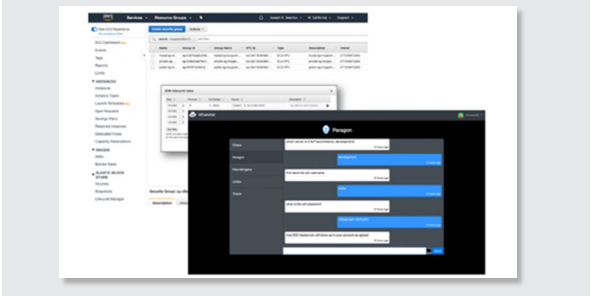
LetSee Marketplace
Single page application (SPA)



Advanced builders played LetSee cyber range that focuses on code, design, and API vulnerabilities.

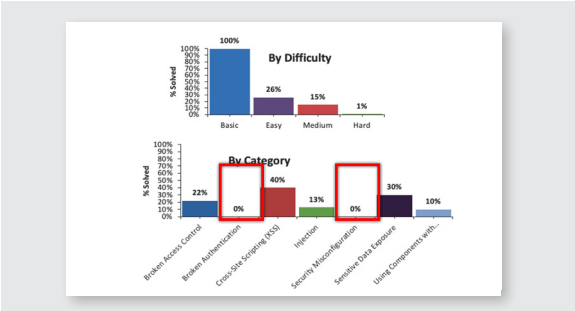
Operators & Defenders

Forescient Portal
Fully featured AWS Infrastructure

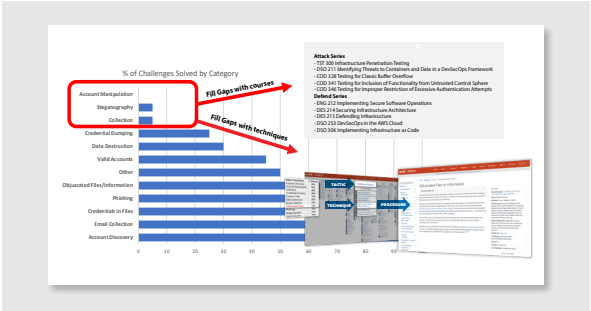


Engineers played Forescient, a range replete with misconfigurations, data disclosures and faulty controls.

6 Milestone - Optimization



With results mapped to standards like OWASP API Top Ten, additional vulnerability-specific courses were taken for developers needing the highest level of security acumen.



With cyber range results mapped to specific MITRE ATT&ACK techniques, IT teams learned more about how attackers penetrate systems similar to theirs, and how to master defense.

Advanced & Sustained Training: Continuing to Pay Dividends

With a concerted and well-executed security training program, this company was able to quickly overcome critical skills gaps, align to industry frameworks, and zero-in on the exact role-based security training requirements across disparate groups. Overall, this approach has greatly reduced the company's risk profile for cloud and IoT security.

Additionally, they recognized that security wasn't a 'one and done' effort. Phase 2 includes expanding to a larger audience, focusing on data privacy, and aligning with ISO.

Get in Touch

187 Ballardvale Road, Suite A195
Wilmington, MA 01887
877-839-7598 x1

SecInnovation
Security Innovation
SecInnovation
securityinnovation.com