IMMERSIVELABS

Cyber Workforce Optimization

Three Steps to Ultimate Cyber Resilience

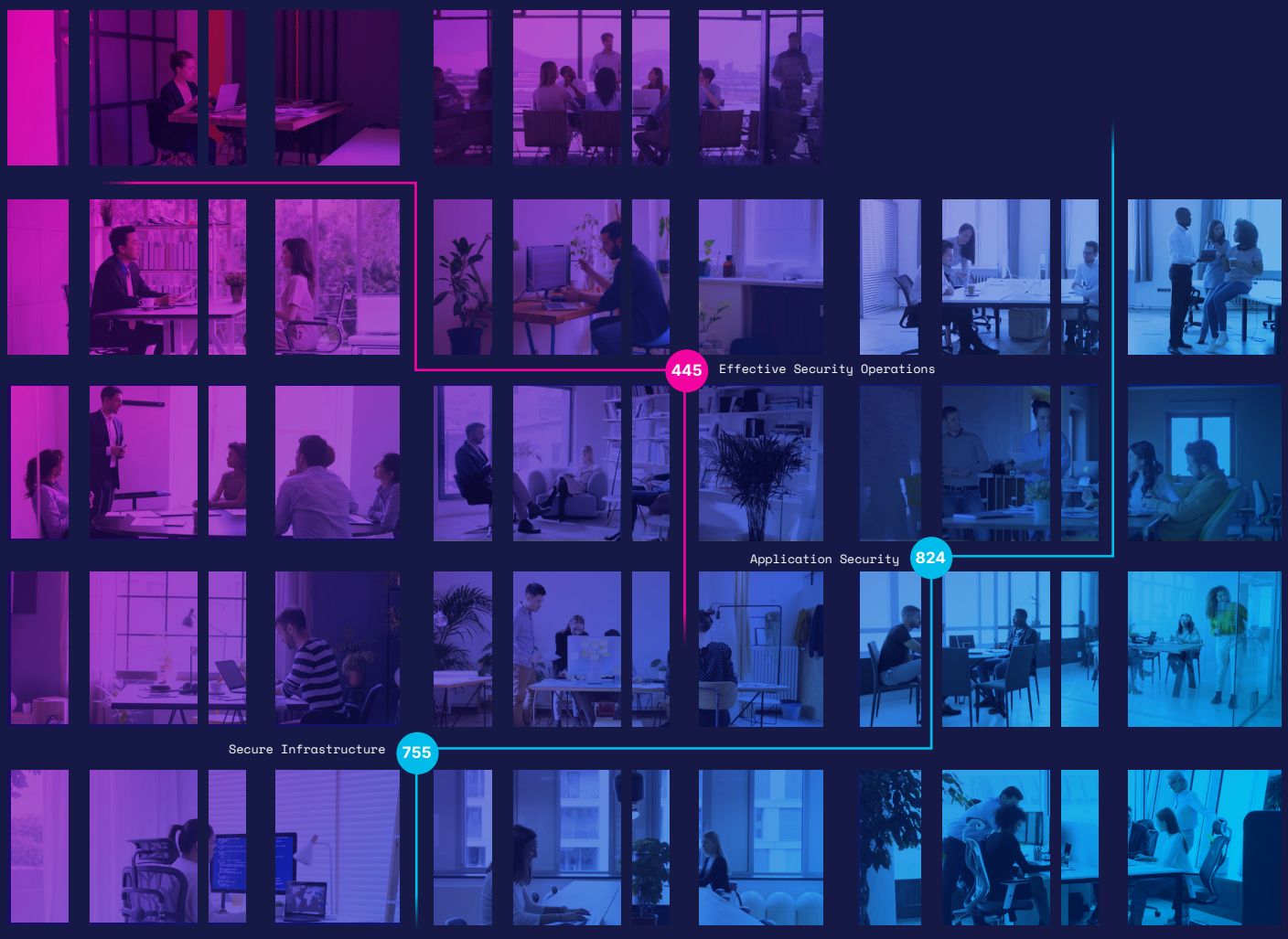
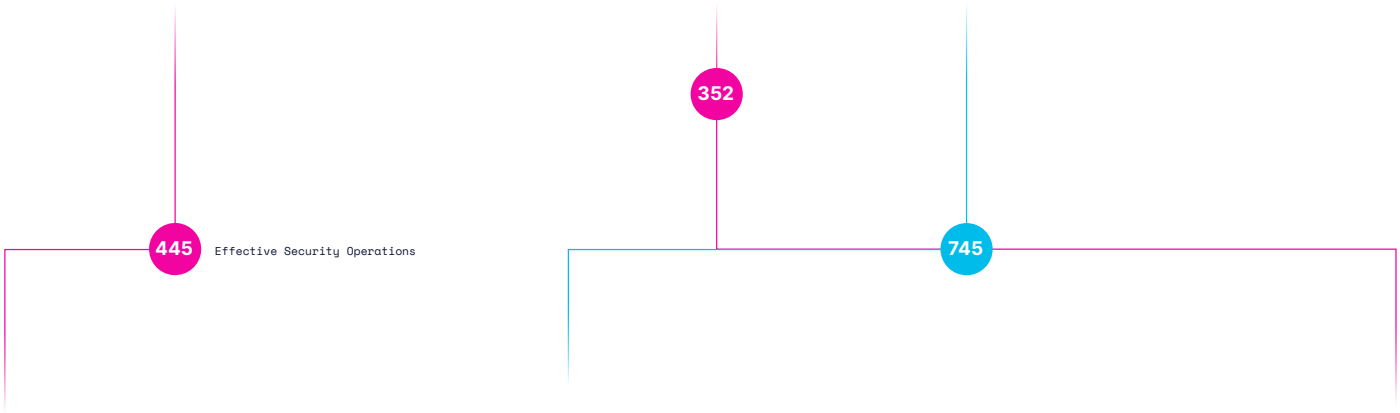


Table of Contents



Introduction

Security breaches have become a fact of corporate life over the past few years. Cyberattacks are accelerating at an alarming rate as hackers and their use of technology, techniques and procedures become more sophisticated and more cunning. The statistics bear it out: the total number of data breaches through September 2021 exceeded the total number of events in all of 2020 by 17%, with 1,291 breaches in 2021 compared to 1,108 breaches in 2020.

The cost is equally alarming. In a global study by IBM Security, data breaches now cost companies $4.24 million per incident on average—the highest cost of the 17-year history of the report. While drastic operational shifts during the pandemic were cited for costs rising 10% compared to the prior year, data breaches undoubtedly come at a high cost—financially and otherwise.

So what, if anything, can be done about them, immediately and for the long term? Are technological countermeasures enough? Can organizations "counter-attack" these ever-growing threats and successfully keep them at bay, or will they forever be playing catch up in the race to defend themselves?

17%

exceeded the total amount of data breaches from 2020 by the time September 30 of 2021 arrived.

1,291

breaches in 2021 compared to 1,108 breaches in 2020.

$4.24 M

average cost of data breaches for companies per incident.

10%

cost increase for drastic operational shifts during the pandemic compared to the previous year.

Yesterday's Solutions vs. Today's Attacks

Fact is, cyber criminals are clever, creative and focused on one thing—developing and refining new, effective threats with far-reaching consequences.

Consider the Chinese hacking group, Hafnium. When Hafnium found vulnerabilities in Microsoft Exchange, they gained access to the email accounts of at least 30,000 organizations in the U.S. and 250,000 globally. The implications of this event went far beyond just financial, as the group primarily targets entities in the U.S. "for the purpose of exfiltrating information from a number of industry sectors," said Microsoft's Tom Burt, corporate VP for customer security and trust. These sectors include infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks and NGOs.

Apple was also hit with a devastating blow last April. Apple supplier Quanta suffered a $50 million ransomware attack by Russian ransomware-as-a-service gang REvil. It's estimated that REvil made at least $123 million in profits in 2020 and stole around 21.6 terabytes of data. Originally, the group demanded Apple pay the ransom to regain access to encrypted data. However, after gaining access to Apple's networks and stealing future product designs, REvil became increasingly more aggressive and also threatened to leak even more stolen blueprints for the yet-to-be-released devices.

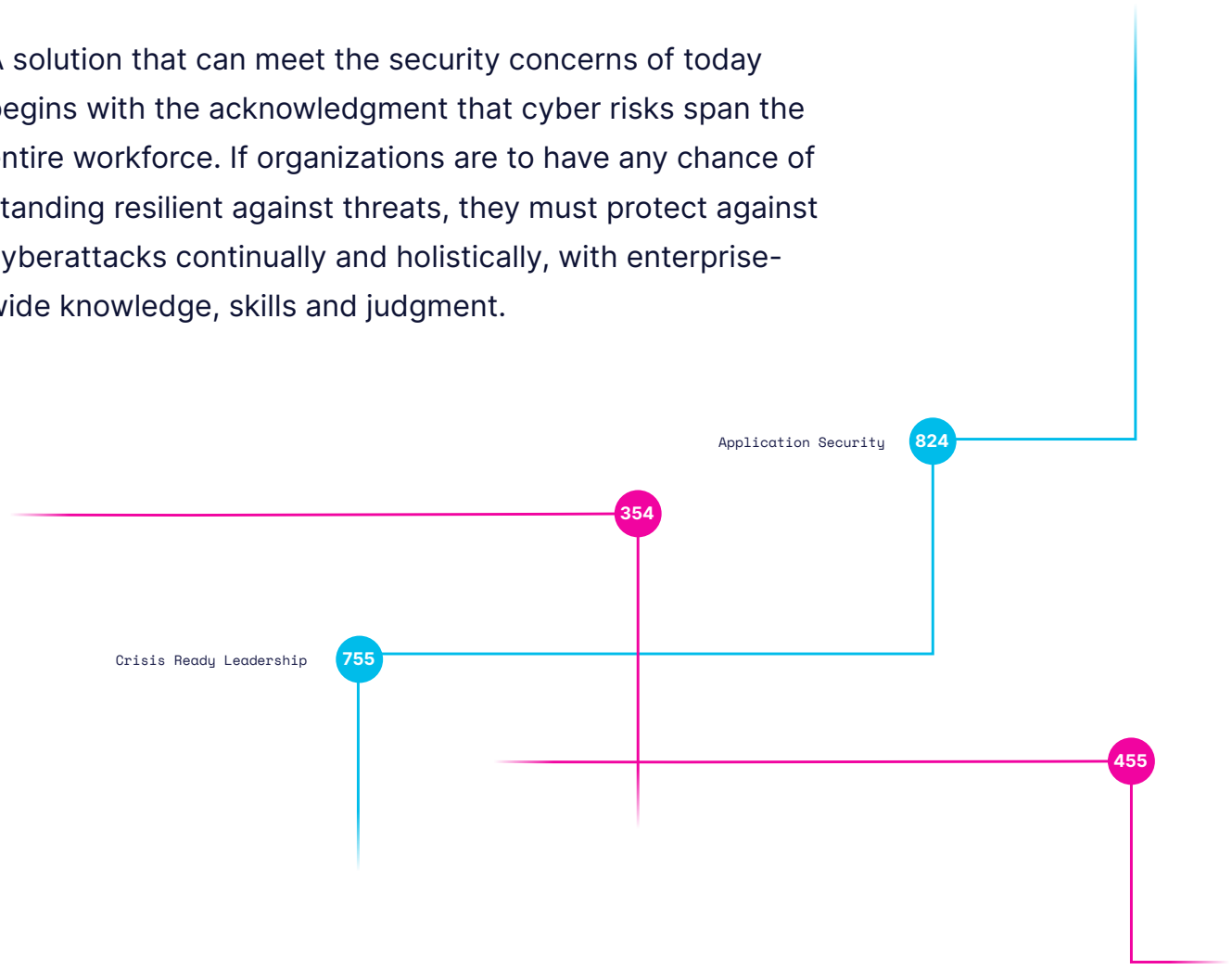
From these two examples alone, we can see that cyberattacks of today are sophisticated, widespread and potentially devastating. It follows, then, that organizations must embrace a defensive solution that can match these attacks and meet them head on.

Traditionally, large enterprise organizations have relied upon expensive technology, enhanced tech stacks and additional processes to help keep them safe. Static mechanisms such as external audits and certification schemes to measure the company's readiness have created a false sense of security. And the workforce—the people behind the screens—are largely forgotten and left to complete once-a-year training that's out of date just as soon as it's completed. Cyber resilience feels like a guessing game.

Static mechanisms such as external audits and certification schemes create a false sense of security.

With every hack that hits the headlines, it's clear that these strategies are leaving organizations extremely vulnerable. They belong in the past.

A solution that can meet the security concerns of today begins with the acknowledgment that cyber risks span the entire workforce. If organizations are to have any chance of standing resilient against threats, they must protect against cyberattacks continually and holistically, with enterprise-wide knowledge, skills and judgment.



Cyber Resilience as a Solution

Cyber resilience is about being able to continuously deliver business outcomes in the face of ever-changing, ever-growing risk—relying on both technical and non-technical teams for prevention, response and remediation. In the past, this goal existed primarily within the enterprise security team—the “geeks”—but more recently, it has emerged as a holistic concern.

Cyber resilience lies in the hands of every business function—from the executives who must make rapid, confident decisions when facing a cyberattack, to the legal, comms and customer teams who must be able to effectively communicate the issue, to developers who must write secure code from the outset. Everyone has a part to play.

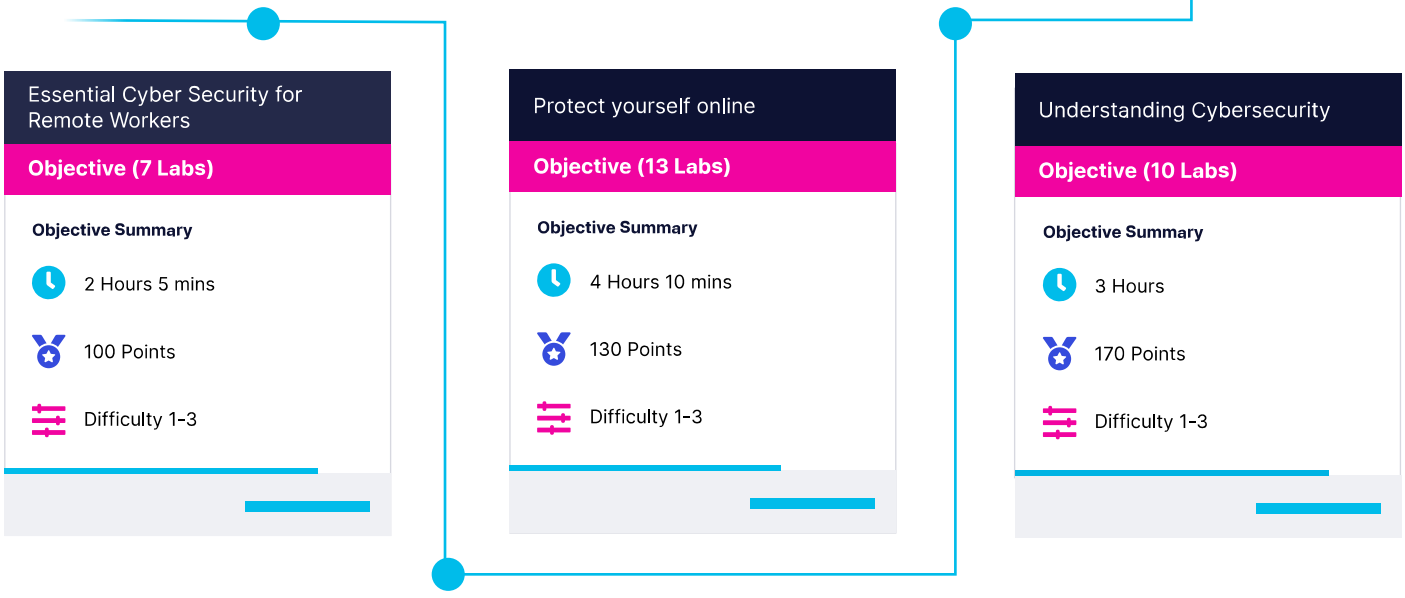
424

Yet how do you prove you’re resilient and secure? How do you measure it? How can you see how your people’s knowledge, skills and judgment impact your overall cyber resilience? Can you prove it to a third party, your regulators, customers, investors and shareholders?

Got Something to Prove?

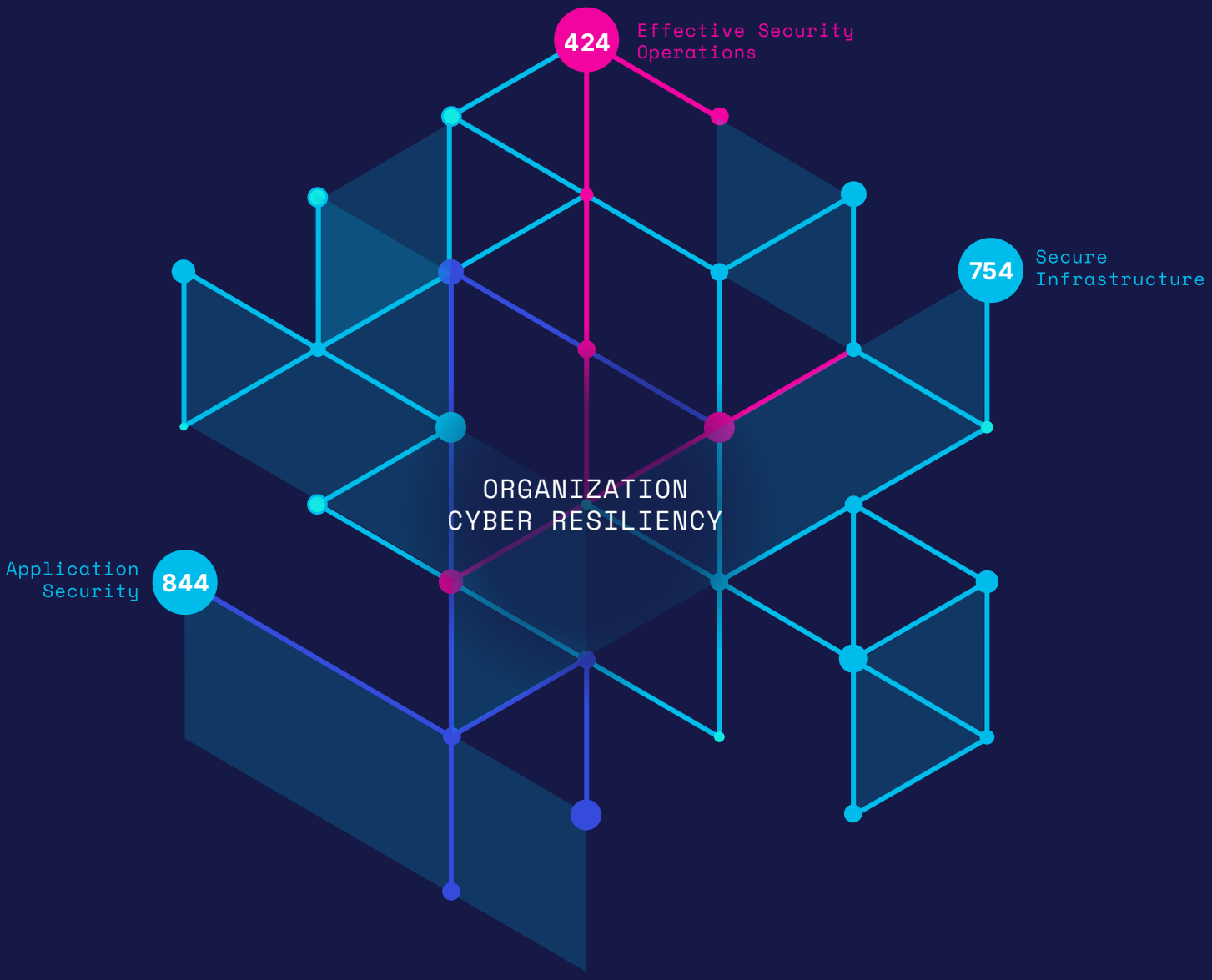
Workforce capability is notoriously difficult to measure, which is why organizations fall back on certificates and qualifications to assess whether their people are capable. But these date just as soon as they're awarded. That leaves organizations in a position to rely on the solutions of the past to meet the threats of today—unless they become cyber resilient.

Building the technical knowledge of your people is just one aspect of a continuous cycle of cyber workforce optimization. It starts with training, but people must be elevated to the same level as technology in the push toward cyber resilience. Just as you would patch, update and continuously optimize your software, an organization must do the same for its people's cyber capabilities, with continuous cyber training, complemented with measurement.



Maximizing Cyber Resilience—Step by Step

To be truly cyber resilient, an organization must be able to assess and measure workforce cyber capabilities, see exactly where their strengths and weaknesses are at any given point, and inject targeted simulations and exercises to optimize the knowledge, skills and judgment.

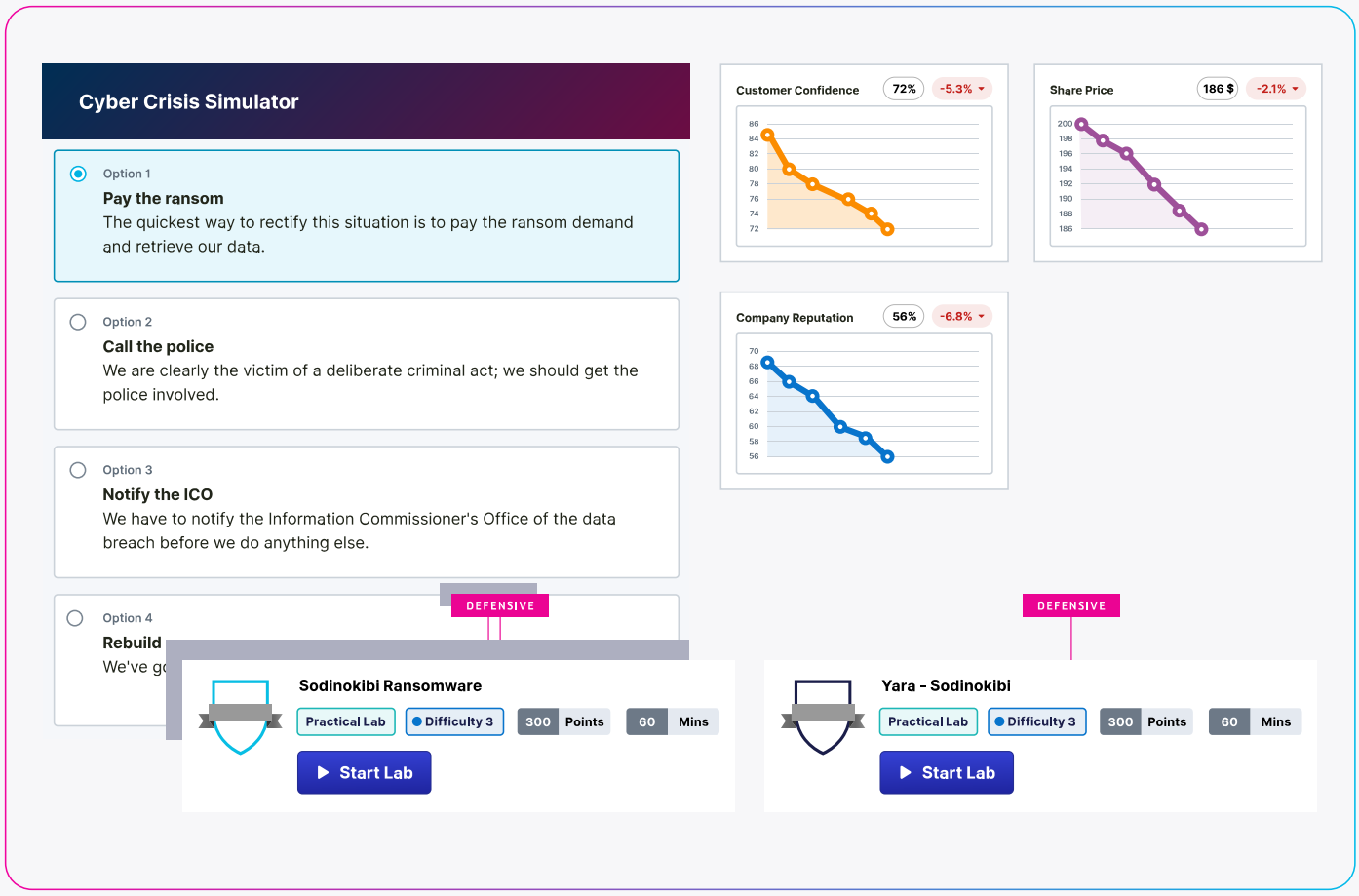


1. Exercise

Benchmark current knowledge, skills and judgment through realistic, role-specific cyber simulations across the entire workforce, with minimal impact on resources.

Benefit from:

- Dynamic crisis scenarios that test organizational decision-making and impact against relevant threats
- Role-specific content experiences that enable micro-drilling and generate data towards a workforce capability baseline
- Screening functionality that demonstrates job candidates' ability in place of a reliance on certifications and CVs

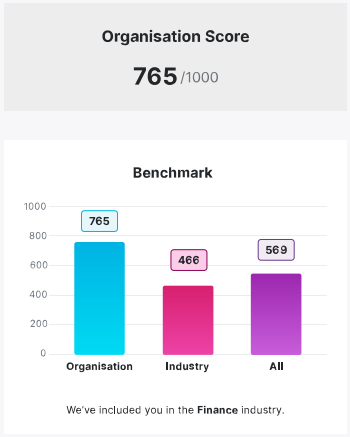


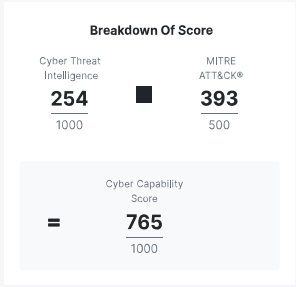
2. Evidence

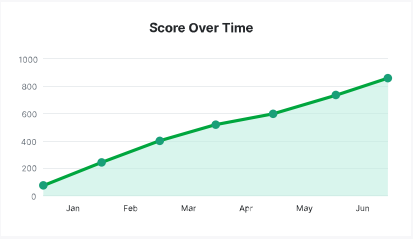
In addition, the organization must be able to easily map workforce capability data and insights to accepted risk frameworks for a real-time picture of cyber resilience and risks, benchmarked to peers.

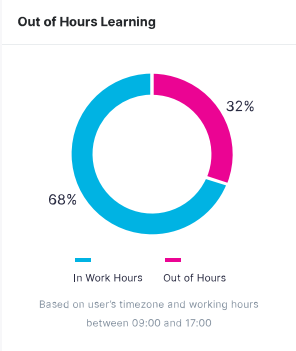
Benefit from:

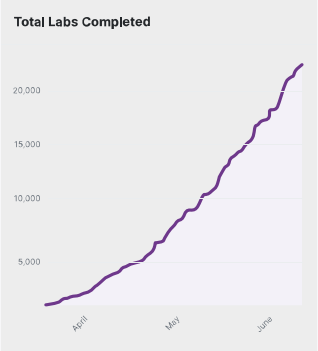
- Data dashboards that organize platform telemetry by focus, visualizing knowledge, skills and judgment over time
- MITRE | ATT&CK® framework mapping that can illustrate threat coverage and identify gaps
- Real-time insights for up to the minute reporting and to inform strategic decision-making

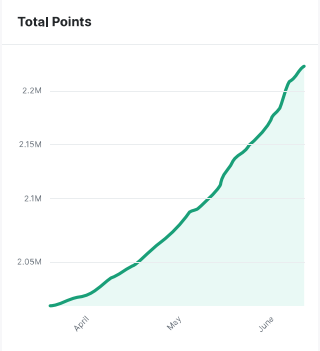










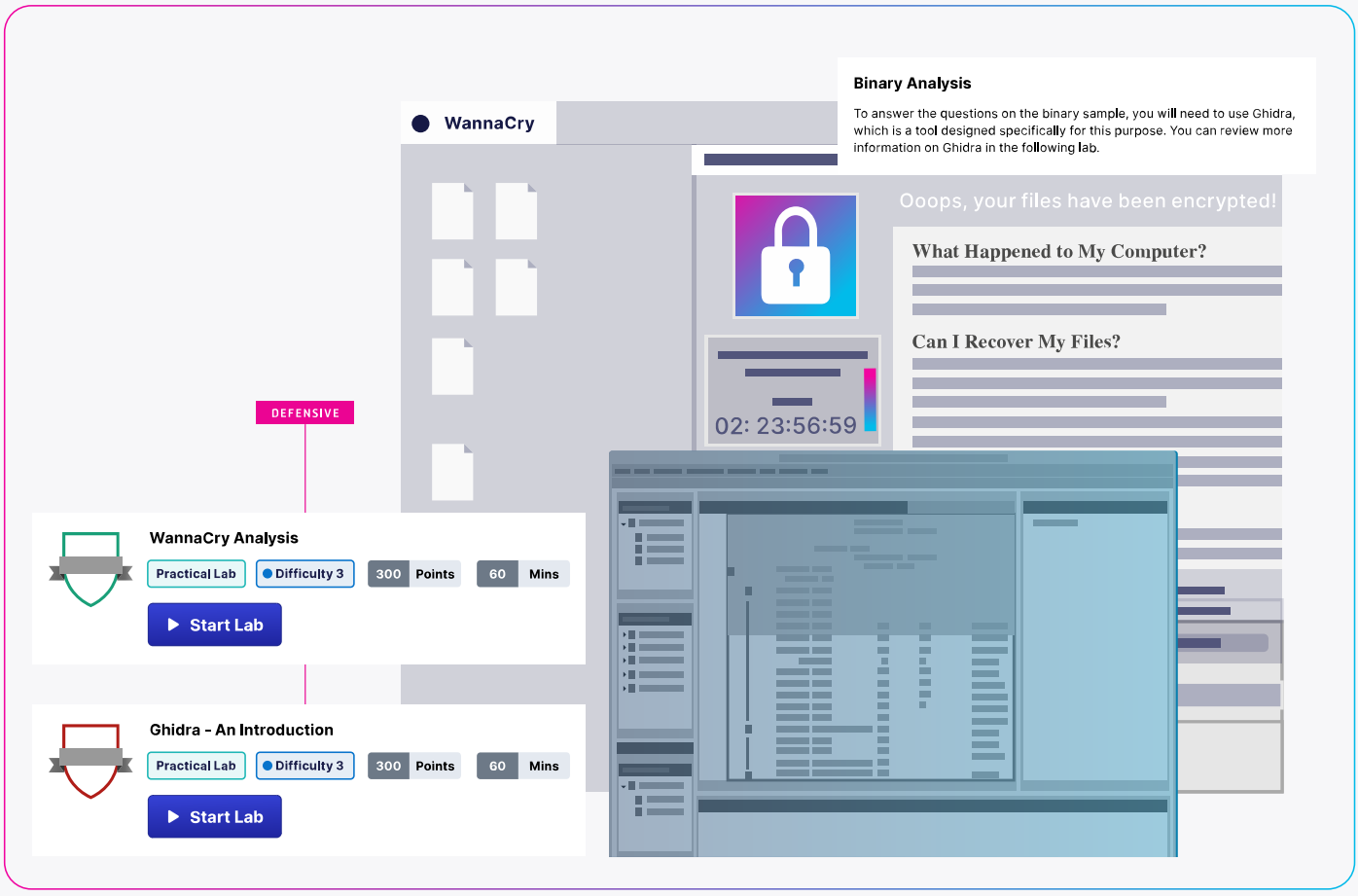


3. Equip

Lastly, the organization must plug gaps in knowledge, skills and judgment using scalable content experiences tailored to each individual dependent on role and business risk.

Benefit from:

- Bite-sized labs and content series for targeted upskilling across multiple individuals, teams, and roles
- Complex environments for the realistic exploration of emerging threats by security teams
- Customizable crisis scenarios to continuously refine confidence and points of weakness in incident response



Seeing the Bigger Picture

It's also vital that organizations maintain a complete real-time visualization of their resilience position that adapts and matures in line with risk. By tracking the effectiveness of cross-functional incident response teams, coverage of governance, risk and compliance and emerging technical threats, the organization can continually adapt in line with strategic goals. And for the very first time, your people can be elevated to the same level as your technology as defensive assets.

For the first time ever, workforce knowledge, skills and judgment are transformed into powerful security controls.

All Together. More Resilient.

Bottom line—cyber workforce optimization is critical for organizations to continually protect against, and effectively respond to, the growing number of cyberattacks. Immersive Labs is a pioneer in Cyber Workforce Optimization, redefining how technical and non-technical measure, map to risk, and optimize workforce cyber capabilities.

Cyber Workforce Optimization is a single solution that enables organizations to continually exercise teams relevant to their role to get the evidence they need about where they stand, and equips them with knowledge, skills and judgment. The result—organizations can be confident that their workforce has the knowledge, skills, and judgment to stand up to every cyber threat, every time.

IMMERSIVELABS

Cyber Resilience, Readiness, Confidence. Let's Get Started.

Talk to an expert about building your cyber resilience with Immersive Labs today. Contact enquiries@immersivelabs.com