

Immersive for Financial Services

Feb 2025

Finance



Hone Your Organization's Human Edge Against Cyber Threats

Be ready for financial services-related threats, supply chain risk, and software vulnerabilities.

Securing a financial services organization like yours is a complex challenge, as the industry remains a prime target for cybercriminals. Leaders must navigate the delicate balance between innovation and security, manage outdated technology, and comply with increasingly stringent regulatory requirements.

Additionally, the interconnected nature of today's ecosystem and intricate supply chains heightens vulnerability. There's also mounting pressure to demonstrate resilience to Boards, C-level executives, and customers. In this demanding environment, a comprehensive approach to proving and improving your organization's capabilities is essential.



Challenges

- Industry a top target for cyber crime
- Highly interconnected business ecosystems and supply chains
- Legacy tech risks
- Pressure to ship new code under tight deadlines
- Maintaining customer trust

Benefits

- **Measure and Prove Your Resilience:** Demonstrate, benchmark, and prove resilience to Board and regulators.
- **Be Ready for Threats:** Empower defenders to identify and mitigate financial services-related threats.
- **Pressure-Test Your Teams:** Put your executive and technical teams' judgment to the test against realistic scenarios.
- **Create the Ultimate Offensive and Defensive Cyber Team:** Deploy state-of-the-art, hands-on labs for offensive and defensive cybersecurity training.
- **Drive Secure Development:** Shift Left with cutting-edge, hands-on application security solutions that empower financial services development teams to boost productivity, cut costs, and mitigate threats.

For Individuals

Hands-on labs offer engaging, gamified learning environments

- Defensive Cybersecurity Professionals
- Penetration Testers
- Developers
- Application Security Experts
- Cloud & Infrastructure Security
- Entire Workforce

For Teams

Team-based simulations from the store room to the board room

- Executive Team
- Crisis Management & Incident Response Teams
- Offensive, Defensive & SOC Teams

For the Organizations

Skills development exercises that drive transformative behavioral change

- Senior Leaders
- Front-line Employees
- High-risk Targets of Cyber Attacks

Get the Human Edge

To drive resilience against attacks, financial services organizations must prepare their entire workforce for attacks; upskill and retain top cyber talent; and prove their resilience to customers, Boards, C-level executives, and regulators.

Immersive can help. We're trusted by global financial services firms like Citi and HSBC to upskill their teams against the latest threats and provide reporting to support various Regulatory requirements. We are backed by Goldman Sachs Asset Managements, Summit Partners, Insight partners, Citi Ventures, Ten Eleven Ventures, and Menlo Ventures.



Support Regulatory Compliance and Reporting

We offer exercise and labs that allow you to align with industry frameworks and meet regulatory requirements and standards, such as DORA and PCI-DSS. Learn how Immersive can help you meet and maintain multiple compliance requirements.

Over the past 20 years, nearly one-fifth of all global cyber attacks targeted financial services organizations, resulting in \$12 B in losses.* Most attacks involve the human element**

\$12B

*International Monetary Fund (IMF) Global Financial Stability Report, April 2024
**Verizon 2024 Data Breach Investigations Report, 2024

Understand MITRE ATT&CK Coverage and Close Gaps

RECONNAISSANCE 10 techniques	RESOURCE DEVELOPMENT 7 techniques	INITIAL ACCESS 9 techniques	EXECUTION 12 techniques	PERSISTENCE 19 techniques	PRIVILEGE ESCALATION 13 techniques	DEFENSE EVASION 40 techniques	CREDENTIAL ACCESS 15 techniques	DISCOVERY 29 techniques
Active Scanning 2 sub-techniques	Acquire Infrastructure 6 sub-techniques	Drive-by Compromise L	Command and Scripting Interpreter 8 sub-techniques	Account Manipulation 4 sub-techniques	Abuse Elevation Control Mechanism 4 sub-techniques	Abuse Elevation Control Mechanism 4 sub-techniques	Adversary-in-the-Middle 2 sub-techniques	Account Discovery 4 sub-techniques
Gather Victim Host Information 4 sub-techniques	Compromise Accounts 2 sub-techniques	Exploit Public-Facing Application	Container Administration Command	BITS Jobs L	Access Token Manipulation 5 sub-techniques	Access Token Manipulation 5 sub-techniques	Brute Force 4 sub-techniques	Application Window Discovery
Gather Victim Identity Information 3 sub-techniques	Compromise Infrastructure 6 sub-techniques	External Remote Services	Deploy Container	Boot or Logon Autostart Execution 15 sub-techniques	Boot or Logon Autostart Execution 15 sub-techniques	BITS Jobs L	Credentials from Password Stores 5 sub-techniques	Browser Bookmark Discovery
Gather Victim Network Information 6 sub-techniques	Develop Capabilities 4 sub-techniques	Hardware Additions H	Exploitation for Client Execution	Boot or Logon Initialization Scripts 5 sub-techniques	Boot or Logon Initialization Scripts 5 sub-techniques	Build Image on Host	Exploitation for Credential Access L	Cloud Infrastructure Discovery
Gather Victim Org Information 4 sub-techniques	Establish Accounts 2 sub-techniques	Phishing 3 sub-techniques	Inter-Process Communication 2 sub-techniques	Browser Extensions L	Boot or Logon Initialization Scripts 5 sub-techniques	Deobfuscate/Decode Files or Information L	Forced Authentication L	Cloud Service Dashboard L
Phishing for Information L	Obtain Capabilities 6 sub-techniques	Replication Through Removable Media H	Native API L	Compromise Client Software Binary	Create or Modify System Process 4 sub-techniques	Deploy Container	Forge Web Credentials 2 sub-techniques	Cloud Service Discovery L
	Supply Chain Compromise 3 sub-techniques	Supply Chain Compromise 3 sub-techniques	Scheduled Task/Job L	Create Account L	Domain Policy	Direct Volume Access		Cloud Storage Object Discovery

Identify individual and organizational capabilities according to the MITRE ATT&CK Framework and fill gaps with specifically-tailored labs.

Why Immersive?

<p>Immersive Realism</p> <p>We offer the most realistic, real-world learning environments for all skill levels</p>	<p>Proof of Capability</p> <p>We equip CISOs with the data to be confident that they have a cyber-resilient workforce</p>	<p>Complete Organizational Coverage</p> <p>We foster resilience across the organization, with unparalleled content that offers world-class breadth and depth</p>	<p>A Unified Enterprise Platform</p> <p>We provide a seamless and customized experience for individuals, teams, and the entire workforce</p>	<p>Capability at the Speed of Cyber</p> <p>We ensure your teams are updated on the latest cyber risks, from zero-day exploits to the evolving AI landscape</p>
---	--	---	---	---

Trusted by the world's largest organizations:



Be Ready

Immersive is trusted by the world's largest organizations and governments, including Citi, Pfizer, Humana, HSBC, the UK Ministry of Defence, and the UK National Health Service. We are backed by Goldman Sachs Asset Management, Ten Eleven Ventures, Menlo Ventures, Summit Partners, Insight Partners and Citi Ventures.

