TotalTest Simulation Service

Elevating Conventional Penetration Testing into Real-World Live Scenarios

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges affecting your organization – your people, your operations, and your reputation.

The growing digitalization of business operations creates numerous entry points for threat actors to compromise critical systems and expose assets, data, and customer information. To keep pace with threat actors and evolving tactics, organizations need to develop a comprehensive and actionable approach to cybersecurity crisis preparedness. FTI Cybersecurity's TotalTest Simulation Service is a comprehensive solution designed to seamlessly extend traditional penetration testing into real-life scenarios. This service uniquely combines strategic business leadership decision-making with dynamic, real-time technical assessments, offering an actionable approach to fortify readiness and response capabilities.

With costs for cybersecurity incidents escalating into the millions and continuing to soar, a proactive and end-end approach to maintaining readiness is crucial. Organizations cannot afford to rely on traditional testing methods alone. The TotalTest Simulation Service is designed to fortify strategic decision-making by testing business leadership responses in a simulated cybersecurity crisis and reveal technical vulnerabilities and incident response process improvements through threat intelligence-led red team tests.

The TotalTest Simulation Service leverages our **extensive incident response experience**, our **leading cybersecurity readiness solutions**, and our **operational resilience testing expertise** to deliver a comprehensive cybersecurity crisis simulation. This provides our clients with the opportunity to rehearse their business leadership and technical response processes in a controlled setting against plausible and industry-specific, organizationally relevant cybersecurity attack scenarios.

Define realistic threat scenarios that depict the most plausible cyber and physical security threats

Simulate a real-world attack or cyber crisis to test your threat response controls and processes

Elevate your technical and procedural readiness, incorporating learnings into response plans

Offensive Security & Stress Testing

Our 'Red Team' steps into the shoes of sophisticated adversaries. Equipped with a blend of stealthy Tactics, Techniques, and Procedures (TTPs), we challenge your threat detection and response controls. Through relevant attack scenarios, we measure the quality of your technical defense controls and response processes, testing both your technical and business leadership under pressure. This approach offers a tangible measure of your organization's incident readiness posture, combining business continuity testing and technical challenges in a single simulation.

Incident Response

Our 'Blue Team' engages in an assessment of your security defenses and leadership's crisis management throughout the simulation. By simulating advanced threat scenarios, we evaluate the efficacy of your incident response and threat intelligence in real-time. The exercise is designed not just to test but to coach, collaboratively enhancing your teams' ability to effectively detect and respond to threats. Following the simulation, we conclude with a focused debrief session, presenting a concise analysis and clear recommendations for bolstering your cyber incident response capabilities.

Our Approach

Our cybersecurity testing employs scenario-based, objective-driven exercises that replicate current threat actor tactics. Beyond technical assessments, we understand that executive leadership needs to be ready for real incidents. To bridge this gap, our exercises culminate in a hands-on simulation for executives, informed by the preceding Red Team assessment.

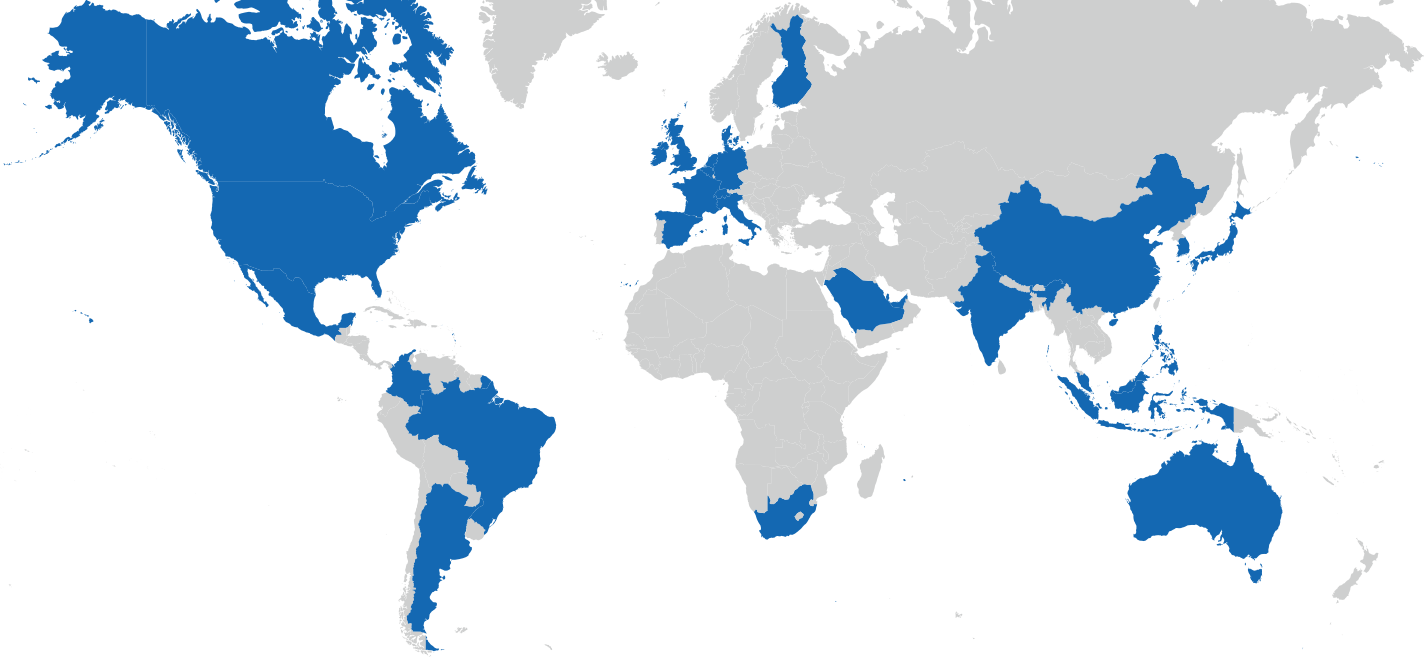
Simultaneously, our incident response and Blue Team experts provide guidance to optimize your technical security processes and communication protocols, ensuring your leadership can navigate the complexities of a live cyber threat.

KEY BENEFITS

- **Holistic Assessment:** A 360-degree view of your readiness and response capabilities, covering and testing both technical and non-technical processes, as well as personnel skills
- **Realistic Simulations:** Engage in real-world attack scenarios to truly understand enterprise vulnerabilities and weaknesses
- **Empower Teams:** Equip both your technical and business leadership teams with hands-on experience and awareness
- **Strategic Decision-Making:** Enhance the executive leadership's capacity to make informed decisions under the stress of cyber crisis scenarios
- **Continuous Improvement:** Identify areas of improvement and iterate, elevating your incident-related processes over time
- **Collaborative Engagement:** Strengthen inter-departmental collaboration and decision-making, fostering a collective sense of responsibility towards cybersecurity

TotalTest for Organizations

Responding to real-world cyber incidents requires coordination amongst multiple stakeholders and suitable strategies for efficiently allocating resources in the midst of an emergency. FTI Cybersecurity's TotalTest Simulation Services provide an opportunity for organizations to train individuals and teams on how to respond to various cyber crisis situations. Regular rehearsals through TotalTest simulations ensures that when a cybersecurity incident does occur, the organization is better equipped to appropriately respond.



Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

Services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

1982

Year Founded and $7.7B Equity Market Cap*

Top 50

Advisor to the world's top 50 bank holding companies

8,000+

Employees Worldwide

NYSE:FCN

Publicly traded

99/100

Advisor to 99 of the world's top 100 law firms

82/100

82 of Fortune Global 100 corporations are clients

**Number of total shares outstanding as of October 19, 2023, by the closing price per share on October 26, 2023.*

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

DAVID DUNN
Head of Cybersecurity, EMEA, APAC
Senior Managing Director
+44 7816 251410
david.dunn@fticonsulting.com

01192024 | VN03182-v04 TotalTest