Offensive Security & Stress Testing

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. As the threat evolves and grows in impact, organizations also face pressure from regulators and stakeholders to quantify the effectiveness of cybersecurity controls in place across their systems.

Offensive security and stress testing, also known as "penetration testing," involves simulating a malicious attack on a computer system or network to identify vulnerabilities. Our offensive security and stress testing services uses the same tools, techniques, and protocols, as witting and unwitting malicious actors to help identify vulnerabilities and improve security.

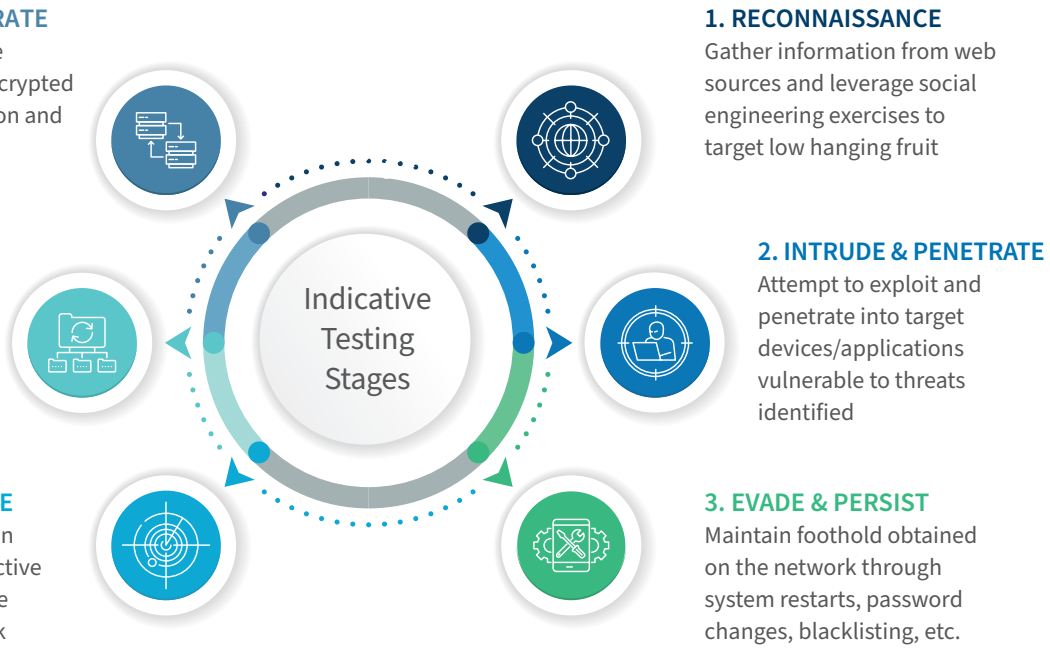
Our Expertise

Our approach to cybersecurity testing is unique because we focus on scenario-based, objective- driven tests that replicate the techniques used by real-world threat actors. Our team of experts are recognised by leading industry accreditations such as CREST, hold certifications from leading entities such as OffSec, Global Information Assurance Certification (GIAC) and SANS, and possess strong academic credentials in science, mathematics, engineering, and computer science.

Additionally, the FTI Cybersecurity team has extensive experience working alongside regulators, setting requirements and analyzing results, and has actively participated in developing threat intelligence-led penetration testing frameworks and approaches (such as CBEST, TIBER and iCAST) for regulators and financial sector organizations.

Our offensive security and stress testing services typically help CISOs and business leaders answer the following critical questions:

1. Will my company's existing combination of security controls protect against a ransomware attack in practice?
2. Do existing risk assessments, budgets and technology transformation initiatives appropriately reflect the cybersecurity risks facing my business?
3. Can my organization be breached due to security weaknesses in the supply chain or third parties?
4. What data can office visitors, contractors, employees, and threat actors find on the corporate network?



Our Services

Our experts leverage an intelligence-driven approach to these objective-based penetration tests, to allow clients practice responding to the most severe situations without exposing them to the associated risks.

Red Teaming

Red Teaming simulates attacks to bolster cybersecurity controls by accessing high-value assets or stealing privileged credentials.

Purple Teaming

Purple Teaming allows a client's SOC team to collaborate with our red team to identify improvement opportunities for enterprise level threat detection and response. Leveraging both our attack simulation and incident response expertise, FTI Cybersecurity focuses on improving breadth and depth of internal security operations capabilities and processes through continuous simulation of attack techniques and stress testing of response plans.

Internal Capability Program Development

FTI Cybersecurity offers effective solutions for mature organizations seeking to build new adversary detection and simulation teams or enhance existing cybersecurity competencies. Our comprehensive approach prioritizes the integration of technical components into overall security operations programs.

Penetration Testing

Application Penetration: Combines automated security testing with manual vulnerability analysis to evaluate an application's security controls. This is done through authenticated and unauthenticated attacks to test against threat actors attempting to obtain access to sensitive data and resources.

Infrastructure Testing: Evaluates enterprise environment controls against relevant adversaries using internal or external attack vectors. The goal is to assess the effectiveness of controls in preventing access to sensitive data and resources based on the business context.

'Assume Breach' Assessments: Evaluate a system's security posture from the viewpoint of a malicious insider or after an external perimeter breach. These assessments help system owners consider how far a threat actor could penetrate and the extent of the damage they could cause once inside the network.

CASE STUDY

PENETRATION TEST FOR A GLOBAL PRIVATE EQUITY COMPANY

SITUATION

A global private equity firm made several cybersecurity investments, including implementation of new "detect and respond" technologies, password-less authentication schemes, and on-boarding experienced certified hires on the security operations team. However, the firm also wanted to ensure they were prepared to respond to a significant cyber attack in a timely manner. The firm hired FTI Cybersecurity to perform an internal penetration test against their New York City and London offices to help their board determine if a disgruntled employee or malicious contractor could obtain unauthorized access to key systems and sensitive data. The client also wanted to assess whether the security operations team could accurately detect threat actors within the network.

OUR ROLE

FTI Cybersecurity completed the penetration test over a period of two weeks. Our offensive security team was able to bypass enterprise security technologies such as privileged identity management, endpoint threat detection, and response controls to compromise several employee and server administrator accounts to gain full control over the client's global enterprise environment. Our experts also held debrief sessions with the Global CTO and Information Security Lead at the end of every day of fieldwork to discuss key areas for improvement and address any indicators of compromise observed by the security operations team. We also provided additional recommendations to improve incident detection and response times for the SOC team.

OUR IMPACT

It took less than two days for our team to compromise the first employee workstation and obtain an initial foothold on the firm's internal network, and only six more hours to gain full control of the firm's global IT infrastructure and business systems. We identified several weaknesses that could be used by threat actors to install ransomware, facilitate fraud, share sensitive information, or cause operational outages.

Working with our offensive security team has helped the firm quickly and reliably highlight where what cybersecurity measures are working, and where they need to improve. The offensive security team was able to exploit weaknesses in core configurations and obtain administrator rights to the entire global network from the New York office in a safe and controlled manner, without impacting regular business operations during the tests.

KEY BENEFITS

- Communicate security vulnerabilities within your organization to stakeholders and develop effective strategies to defend against real-world attacks, improving breach preparedness.
- Evaluate the effectiveness of security tools, technology, and processes through tailored, scenario-based controlled incidents.
- Identify gaps in incident response plans and build a remediation plan to address root cause issues, reducing risk exposure across the enterprise.
- Rehearse and prepare people, processes, and tools to respond to cyber attacks, building 'muscle memory' for quick response.
- Assess employee response to real-world threats and provide targeted training to proactively identify and respond to security threats in a timely manner.

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

No other firm in the space has a crisis communications practice

Integration of FTI Consulting's expertise across the platform

1982

Year Founded and $6.2B Equity Market Cap*

Top 50

Advisor to the world's top 50 bank holding companies

7,700+

Employees Worldwide

NYSE:FCN

Publicly traded

**Number of total shares outstanding as of April 20, 2023, by the closing price per share on April 20, 2023.*

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

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

DAVID DUNN
Head of Cybersecurity, EMEA & APAC
Senior Managing Director
+1 267 507 2863
david.dunn@fticonsulting.com

06012023 | VN02739-v07