STROZ FRIEDBERG
A LevelBlue Company

SERVICE BRIEF

Adversary Simulation and Red Teaming

Stroz Friedberg's Adversary Simulation Services

At Stroz Friedberg, we combine the expertise of multiple cyber disciplines to help our clients understand the threats their business faces. We identify these threats by gaining insights into your business operations, industry, location, and data assets.

We help our clients by creating threat models and attack path maps to identify their key controls, developing realistic scenarios that impact their business, and providing specialized red teaming services to simulate how an attacker might target their organization.

Core Adversary Simulation Services

THREAT INTELLIGENCE

It's essential that an organisation understands the key threats to its operations based on real intelligence. Our global threat intelligence team undertakes research across a range of sources to understand the threat actors operating in your industry, their mode of operation, and the attack vectors that are being used to target your business.

RED TEAM TESTING

Stroz Friedberg's offensive red team simulates the tactics, techniques and procedures (TTPs) of an attacker to test the defensive controls in place, mitigating the risk of a successful compromise. This end-to-end assessment starts with gaining the initial foothold in your environment via techniques such as phishing or physical entry to your sites, through to targeting the identified objectives.

THREAT MODELLING AND ATTACK PATH MAPPING

A threat model can be built around your entire organisation or discrete elements within it to provide a structured representation of the risks you face alongside the essential controls necessary to protect your key assets. This can include a visual representation of the pathway an attacker could use.

PURPLE TEAMING

Stroz Friedberg's red team works directly with your defensive (blue) teams, collaborating and sharing knowledge to identify blind spots, control efficacy, and help refine your capabilities to protect against your key risks.

Stroz Friedberg's Approach

We offer a flexible delivery approach to meet your primary needs – whether that's comprehensive end-to-end services or specific priorities like understanding your key risks and simulating a realistic attack to evaluate your controls' effectiveness.

See below the key stages involved, with clients having the ability to start and finish where best fits their specific needs and objectives.

Threat Intelligence

Uncover the most probable and impactful threats currently affecting your organisation and any specific vulnerabilities or threats related to your critical functions. Based on this research, the team develops realistic attack path scenarios that inform the red team.

Scenario Development

Our red team managers develop the threat intelligence information into a test scenario specific to your organisation, clearly addressing the objectives you have set.

Initial Compromise

The first stage of compromise often includes gaining a foothold in your environment through techniques such as social engineering, or in the case of scenarios such as insider threat or a supply chain attack, the initial foothold is within the network.

Red Team Execution

Once a foothold is established, our team moves towards the set objectives. This may include escalation of privileges, lateral movement and persistence while remaining undetected by the blue team.

Report and Debrief

Our reporting for red team engagements includes detailed descriptions of the approach taken and clear recommendations to mitigate risks. Formal debrief sessions with key stakeholders at executive and technical levels also offer an opportunity for feedback.

Retesting (Replay Attacks)

Once recommendations have been implemented, we advise that successful attacks are replayed to ensure that the remediation will be effective in preventing future attacks.

FAQ

Given the complexity of securing your environment against threat actors, understanding which services are most relevant to you can be complicated. Below, we list the questions we are often asked about our adversary simulation services.

How does red teaming differ from penetration testing?

Penetration testing looks to find as many vulnerabilities as possible in a defined scope, whereas red teaming simulates the way a threat actor would target an organisation, moving towards a particular objective and testing your detection and response capabilities.

Why should you perform a red team exercise?

Red teams take a proactive, real-world approach to identify potential risks and weaknesses, testing your defences under realistic attack scenarios and ensuring that your organisation is prepared for whatever threats might come its way.

How effective are the defensive capabilities of your organisation?

Companies often invest significantly in the people, process and technology required to protect their data. Red teaming is a key tool in helping to determine the efficacy of your implemented controls and understand the necessary improvements.

When should you perform a red team?

Once your organisation has an effective vulnerability management programme in place that includes regular penetration testing and you have implemented effective defensive controls, red team engagements should then be considered.

Other typical triggers that may necessitate an engagement include:

- Major infrastructure changes
- A security incident
- Audit or compliance requirements
- Testing a new security programme or control
- Preparation for high profile events
- Assessment of new tools or processes
- Changes in the threat landscape
- Organisational change

Stroz Friedberg's Team and Experience

Stroz Friedberg was one of the original companies involved in developing the Bank of England's CBEST programme. We have conducted red team engagements across various industry sectors, with different levels of complexity and scenarios.

Our team is certified to deliver testing under the Bank of England's CBEST scheme (CBEST Threat Intelligence-Led Assessments | Bank of England) and CREST's STAR and STAR-FS schemes (Stroz Friedberg | CREST) for intelligence-led testing. Our consultants hold the CREST CC-SAM and CC-SAS certifications, demonstrating the very highest capability within red team consulting services.

Over a quarter of the work delivered by our testing team is based around adversarial simulation and red teaming, having delivered these services for over 15 years.

Typical Scenarios

SUPPLY CHAIN ATTACK

Simulating the risks posed if a critical supplier was breached by an attacker that consequently gains access to your systems.

RANSOMWARE

Targeting your organisation's data, typically exfiltrating sensitive data and encrypting it within the organisation's network.

CLOUD SERVICES

The available attack surface is increasing as more organisations move to the cloud and hybrid infrastructure deployments and configurations.

INSIDER THREAT

Insider threat or malicious insider simulation focuses specifically on identifying and assessing the risks posed by internal staff within an organisation.

STOLEN DEVICE

Assess how well the organisation can protect sensitive information and mitigate potential risks when a device falls into unauthorised hands.

PHYSICAL ENTRY

Assess the organisation's ability to prevent unauthorised access, detect intrusions, and respond effectively to physical security threats such as tailgating, or policies related to office visitors.

NEXT STEPS

Contact our team to discuss how Stroz Friedberg's services can test the real-world capabilities of your cyber defences and progress your cyber strategy. A scoping call with our team will establish your requirements and build a bespoke package of work designed to meet your objectives.

SF STROZ FRIEDBERG
A LevelBlue Company

About Stroz Friedberg

Stroz Friedberg, a LevelBlue company, delivers intelligence-driven digital risk management with expert-led services designed for adaptive resilience.

With over 25 years of leading the resolution of the most complex, high-stakes digital risk issues, we manage the entire digital risk lifecycle – from cyber threats and insider risks to IP theft and regulatory compliance. Our approach combines managed security services with expert analysis and strategy, supported by threat intelligence gathered from thousands of engagements across various industries.

We translate complex technical and legal risks into actionable strategies, helping CISOs and legal teams turn digital risks into board-ready insights. Our comprehensive services include managed cyber defense, digital forensics and incident response, trade secret protection, expert witness support, threat intelligence, security strategy and governance, attack path mapping and testing, and resilience engineering.

Operating as one trusted partner, we align technical precision with business priorities to protect critical assets, adapt to evolving threats, and maximize ROI through proven outcomes. Through LevelBlue's portfolio, these specialized services integrate seamlessly with 24/7 managed security operations and AI-driven threat detection for comprehensive digital risk protection.

Cybersecurity. Simplified.

levelblue.com/strozfriedberg