STROZ FRIEDBERG
A LevelBlue Company

SERVICE BRIEF

Application Security Testing

Enhance Your Security Posture with Comprehensive Product Security Assessments

As technology advances, security threats also grow across hardware, firmware, applications, cloud, and network services. A fragmented approach to product security can create vulnerabilities that attackers may exploit. Our Full Stack Product Security Testing offers comprehensive security assessments to identify risks throughout the entire product stack – from silicon to software.

Typical Use Cases for Purple Team Engagements

Our clients use purple teaming for a variety of different reasons, represented below with some typical use cases:

SECURITY PROGRAM VALIDATION

Test the effectiveness of the organisation's security program to help shape the direction and find existing strengths and weaknesses. This can also take place when significant changes are being made to ensure that security controls, policies, and procedures are working as intended.

PRE-EMPTIVE DEFENCE

Proactively identify weaknesses in your security defences before they are exploited by an attacker. By simulating real-world attack scenarios an organisation can uncover hidden risks and improve defences.

COMPLIANCE REQUIREMENTS

Are you subject to specific regulatory or industry compliance standards? The purple team engagement can help assess your adherence to those requirements, simulating attacks and evaluating the effectiveness of any security controls, ensuring compliance and mitigating potential risks.

POST-INCIDENT EVALUATION

A post-incident evaluation can be conducted after a breach to analyse the incident response procedures and processes. This helps to identify any gaps in detection, response or mitigation that contributed to the incident, and provide insights for strengthening the overall strategy.

SECURITY PROGRAM VALIDATION

Deploying new technologies, such as data loss prevention, intrusion detection systems or endpoint protection solutions. This allows you to test the effectiveness of these technologies in real-world attack scenarios, identify configuration weaknesses, and fine-tune them for optimal protection and performance.

Stroz Friedberg's Purple Team Approach

Whether we're working to understand the detection and response capabilities for a new service or technology, assessing a new SOC service, or performing purple teaming as part of a red team follow-up, we follow the same approach to ensure that the objectives of the engagement are met.

1 ATTACK PATH IDENTIFICATION AND THREAT MODELLING

This stage is used to develop a threat model for the target environment / system / platform / process / company.

We review all the supporting documentation relevant to the target, interview key stakeholders from the business, technology teams, security, and blue teams. This is supplemented with threat intelligence information from our in-house team, based on the industry, geography, and company-specific information.

This stage allows us to develop a threat model and identify likely attack paths based on your profile.

2 TEST CASE DEVELOPMENT ASSESSMENT

Gain a better telemetry of a particular solution or the entirety of your defensive-based tooling and a more robust detection capability with the involved technologies. The main objective of this engagement is to perform simulations of expected "good" traffic to identify expected behaviour and telemetry, as well as a multi-layered attack simulation.

Stroz Friedberg will review your deployments to identify which telemetry sources are being ingested, mapping this to critical assets and probable attack vectors. Where relevant, Stroz Friedberg will recommend other data sources that would enhance your capabilities against the previously identified attack vectors.

3 EXECUTION AND REPORTING

Working in direct contact with your blue team, our red team will systematically progress through the test cases developed to understand what (if any) telemetry is generated against each attack, timestamp of execution, source host, destination host, username and the result of the execution.

As this execution phase is consultant-led by a member of our accredited red team, we add additional sophistication to the attack in an effort to evade detection. Results are fed back throughout the engagement. However, we also provide a fully documented report identifying the efficacy of the controls in place, any blackspots, recommendations for improvement, and a full debrief with ongoing dialogue.

4 RETESTING

Our testing often highlights several changes that the blue team will have to implement. This often extends to our team, working directly with security vendors to implement fixes to their products.

Once this is completed, a round of retesting is essential to ensure that attacks are now being identified and responded to in an effective manner.

Stroz Friedberg's Team and Experience

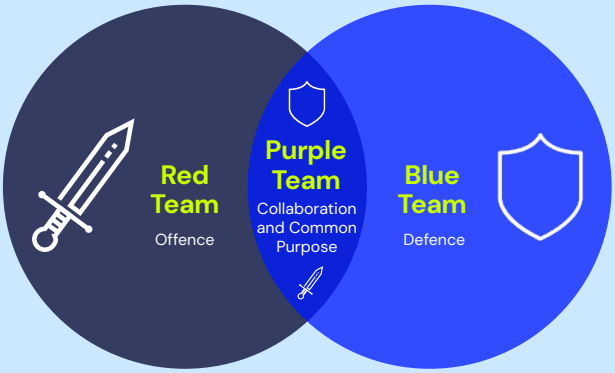
Stroz Friedberg's team has been involved in delivering red and purple teaming for over 15 years and was one of the original companies that helped create the Bank of England's CBEST programme. In recent years, many of our clients have shifted toward conducting collaborative purple team engagements to gain a better understanding of overall defensive capabilities and to receive recommendations for improving control effectiveness.

Our team operates in some of the world's most cyber-advanced industries and high-profile organisations. We have experience with deploying leading technology solutions, regularly testing their capabilities and integrations across people, processes, and technology.

We work with clients who are on the path to maturity and are looking to safeguard themselves against key threat scenarios that impact them, their industry, and the types of data assets they aim to protect.

The Benefits of Purple Teaming

- Help tune defensive controls
- Review technology and process deployments
- Assess specific controls associated with the real-world cyber threats you face
- Provide actionable recommendations to improve your cyber maturity
- Evaluate efficacy of technologies being considered
- Collaboration between our offensive specialists and your blue team



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 to counter the risks you face. A scoping call with our team will establish your requirements and build a bespoke package of work designed to meet your objectives.

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