

# THREAT-LED PENETRATION TESTING

Threat-Led Penetration Testing goes beyond traditional methods by simulating the tactics, techniques, and procedures of real-life threat actors.

It ensures clients meet basic compliance-driven needs while driving additional value through targeted threat intelligence. Our approach prioritises cost-effectiveness through collaboration, providing insight into threats faced by clients and validating controls to mitigate risks effectively.

## Purpose:

Threat-Led Penetration Testing is essential for organisations to assess their cyber resilience against real-world threats. By simulating the tactics of threat actors, organisations gain insights into potential vulnerabilities and weaknesses in their security defences. It helps organisations ensure they meet compliance requirements while effectively mitigating risks posed by threat actors.

## Features:

- **Real-Life Threat Simulation:** Simulation of tactics, techniques, and procedures used by real-life threat actors to identify vulnerabilities and weaknesses in security defences.
- **Targeted Threat Intelligence:** Utilisation of targeted threat intelligence to assess the impact of potential opportunities for adversaries and inform security strategies.
- **Cost-Effective Collaboration:** Cost-effective approach through collaboration, providing insight into threats faced by clients and validating controls to mitigate risks effectively.
- **Technical Validation:** Technical validation of threat paths and controls, extending to key technical milestones to escalate privileges, traverse environments, and perform actions with tangible business impact.
- **Comprehensive Reporting:** Reporting for technical and non-technical audiences, aiding understanding of potential threats and their impact, followed by actionable recommendations to mitigate risks.

## Benefits:



### People:

- **Empowered Security Teams:** Empowers security teams with actionable insights into real-world threats and effective strategies to mitigate risks, enhancing overall cyber resilience.
- **Enhanced Security Awareness:** Increases security awareness among employees by providing insights into real-world threats and vulnerabilities, fostering a culture of cybersecurity within the organisation.

### Technology:

- **Cost-Effective Risk Mitigation:** Provides a cost-effective approach through collaboration, ensuring efficient allocation of resources to mitigate risks effectively.
- **Strategic Decision-Making:** Informs strategic decision-making by providing insight into potential threats and their impact on operations, enabling proactive risk management.

### Commercials:

- **Enhanced Compliance:** Ensures organisations meet compliance requirements while effectively mitigating risks posed by adversaries, enhancing overall security posture.
- **Stakeholder Confidence:** Builds stakeholder confidence by demonstrating proactive measures to address potential threats and vulnerabilities, enhancing trust and reputation.