Integrity360
your **security** in mind

CASE STUDY:
Red Teaming a leading European payments provider

The customer

A leading European payments and card-services provider engaged Integrity360's Red Team to run a realistic, attack-grade assessment over a six-month period. The engagement combined full-scope Red Teaming (external and internal attack paths), controlled Physical Penetration and Social Engineering, and scenario work mapped to the TIBER-EU framework to test the organisation's ability to detect, respond and protect its crown-jewel assets.

Key objectives included

- Demonstrating detection readiness across internal and external attack vectors.
- Testing resilience against human-based attacks such as social engineering and physical intrusion.
- Assessing whether privileged access could be obtained and used to move laterally.
- Producing actionable remediation guidance to strengthen their security posture.

By setting these goals, the company sought not only to uncover vulnerabilities but also to validate whether its investments in controls and awareness were delivering real protection.

Industry

Payments, banking and card services provider

Challenge

The organisation recognised that traditional penetration testing and vulnerability assessments were not enough to uncover the kinds of weaknesses exploited by motivated adversaries. They needed a realistic simulation that tested their entire defensive ecosystem.

Why Integrity360

The client chose Integrity360 because of its:

- Proven experience in delivering Red Team operations aligned to European regulatory frameworks such as TIBER-EU and DORA.
- Multi-disciplinary expertise spanning technical, physical and social-engineering attacks.
- Ability to run a prolonged, stealthy campaign that emulates real-world attacker behaviour over months rather than days.

CASE STUDY:
Red Teaming a leading European payments provider

Integrity360's solution

Over a six-month engagement, **Integrity360's Red Team executed:**

- **Reconnaissance & external attack attempts:** The team began with open-source intelligence gathering and probing of public-facing infrastructure. This phase highlighted areas such as forgotten services and unpatched systems, testing the organisation's ability to spot and react to low-and-slow intrusion attempts.
- **Insider simulation:** In line with the agreed scope, a controlled insider foothold was provided to replicate a scenario where an attacker had gained access through phishing or a compromised laptop. From this starting point, the team sought to escalate privileges, harvest credentials, and test whether network segmentation would slow or stop lateral movement.
- **Physical & social engineering:** Operators conducted controlled social-engineering engagements by impersonating staff or contractors. On multiple occasions, they were able to gain entry past reception and even connect to the corporate Wi-Fi. These actions revealed how seemingly small lapses in process and awareness could open the door to major compromises.
- **Controlled payloads & exfiltration:** To validate detection and response, the red team deployed custom implants and simulated data exfiltration in a highly controlled way. These actions tested SOC visibility, alerting thresholds and escalation procedures without putting production at risk.
- **Objective-driven testing:** Throughout, the campaign was structured around pre-agreed "flags" — symbolic objectives such as reaching sensitive file-shares, obtaining privileged credentials, and demonstrating potential access to core payment systems. This made it possible to clearly communicate progress and impact to stakeholders.

> "Working on this engagement was illuminating with patience and meticulousness, we highlighted how seemingly innocuous configurations and everyday habits can be exploited to build a path to compromise. The realism inherent in these operations clearly demonstrates how every finding can be turned into concrete action"

Alessandro Gugliandolo,
Red Team Operator, Integrity360

> "It was intense and very close to how a real threat actor operates: small details — a forgotten file share, an overlooked procedure — can throw open doors that seemed closed. Well-crafted social-engineering techniques turned everyday interactions into opportunities for attack"

Leonardo Pace,
Red Team Operator, Integrity360

Integrity360
your security in mind

CASE STUDY:
Red Teaming a leading European payments provider

Results & benefits

The Red Team uncovered critical gaps but also confirmed areas of strength, giving the client a balanced picture of their security maturity.

- **Credential & data hygiene issues:** Developer file-shares were found to contain sensitive credentials, including some plaintext administrative passwords. These were used to escalate privileges and move laterally, demonstrating how a single overlooked repository could undermine strong perimeter defences.
- **SOC performance under stress:** Certain high-risk actions, such as privilege escalation to domain controllers, were detected and blocked by the SOC. However, earlier activities — like reconnaissance and credential harvesting — went unnoticed, highlighting areas for improved rule-tuning and logging.
- **Physical & human vulnerabilities:** Social-engineering exercises showed that reception staff and employees could be manipulated into granting access or providing network credentials. While no malicious intent existed, the findings proved how quickly trust could be exploited.
- **Remediation & uplift:** Immediate fixes were applied, including the retirement of vulnerable systems and the rotation of exposed credentials. The findings were also fed into new tabletop exercises and detection engineering sessions to improve SOC playbooks. Security awareness training was updated with real-world examples from the engagement, making it more impactful for employees.

Conclusion

This engagement demonstrated that even organisations with mature defences can be compromised when people, processes and technology are not equally robust. By engaging **Integrity360's Red Team,** the client gained critical visibility into its true vulnerabilities, implemented immediate fixes, and established a roadmap to strengthen resilience against real-world adversaries.

About Integrity360

Integrity360 is Europe's leading cyber security and PCI specialist, with offices across Ireland, the UK, Bulgaria, Italy, Sweden, Spain, Lithuania, Ukraine, Africa, and the Caribbean. The company operates six Security Operations Centres (SOCs) in Dublin, Sofia, Stockholm, Naples, Madrid and Cape Town.

With an expert team of over 350 dedicated cyber security professionals, Integrity360 offers a full suite of professional, support, and managed security services. These services cover every aspect of cyber risk management, from identification and prevention to detection, response, and recovery.

2500+ Enterprise Clients

350+ Cyber Professionals

AMTIVO ISO 9001 Certified Quality Management
AMTIVO ISO 27001 Certified Information Security Management
AMTIVO ISO 20000-1 Certified IT Service Management