Empowering your defence with our offensive security expertise

Stay ahead of potential threats with comprehensive and customised offensive security testing and recommendations for remediation.

devoteam
Cyber Trust

The past decade has seen an explosive growth in the use of digital technology across all industries, as companies have embraced the advantages of greater efficiency, convenience, and connectivity that digital tools can provide. This has led to an increased reliance on digital communication channels for everything from customer interactions to internal team collaboration to supply chain management.
At the same time, cybercrime has grown at an alarming rate, with hackers and other bad actors increasingly targeting digital systems and data as a means of gaining access to sensitive information, intellectual property, financial assets, and more.
According to recent research, cybercrime damages are expected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015.

In today's digital age, organisations have come to recognise that cybersecurity is a critical part of doing business, and that it must be actively managed to protect against the growing threat of cyber attacks. To this end, the majority of companies are using industry standards and best practices to implement a risk management approach that helps to identify and mitigate potential vulnerabilities and risks.

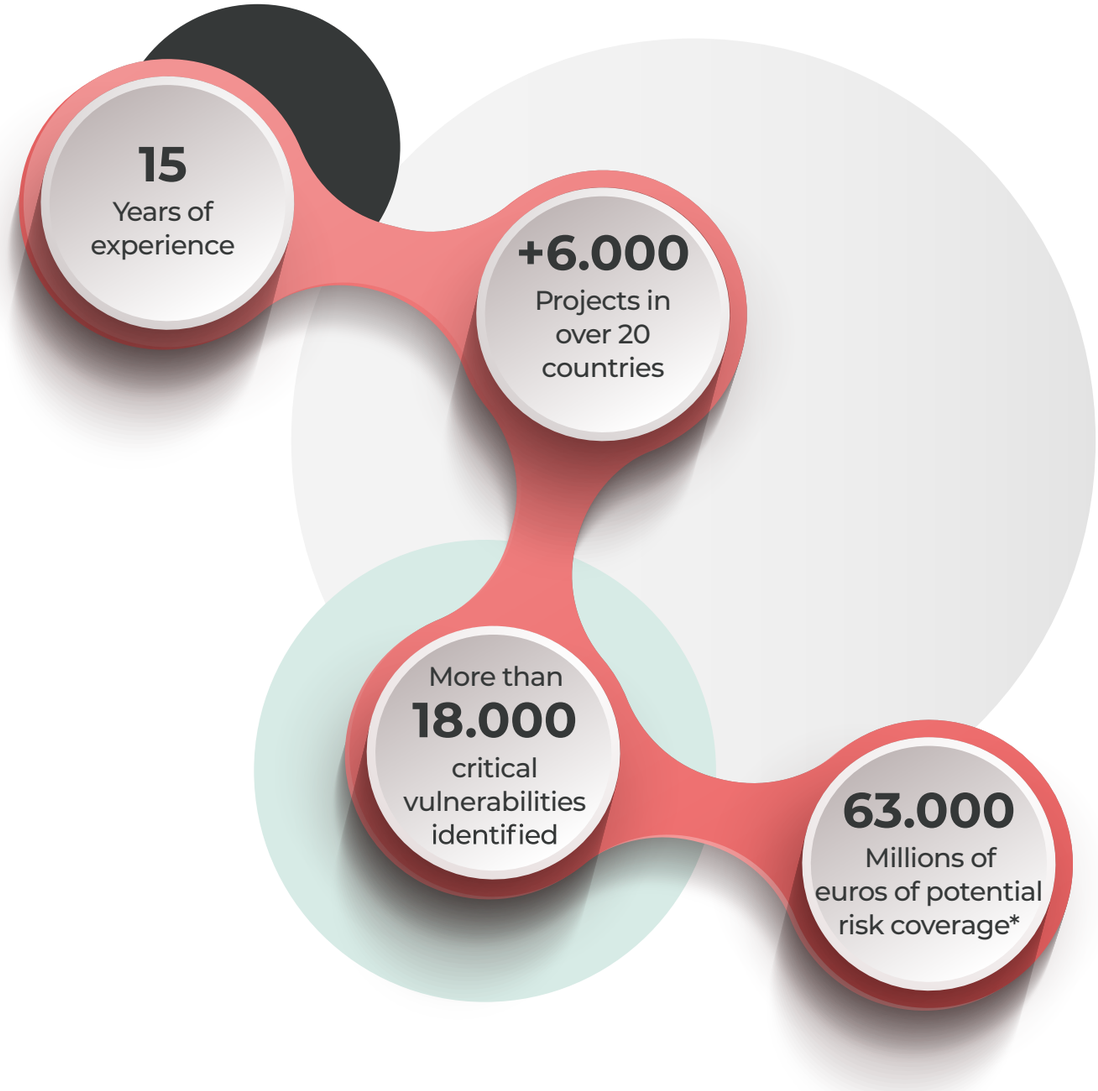
However, while these measures are an essential part of an overall cybersecurity management practice, they are often reactive in nature and can fall short in detecting more advanced and persistent threats.
This is where offensive security comes in - by proactively testing systems and applications to identify potential vulnerabilities and weaknesses before they can be exploited by bad actors.

Devoteam Cyber Trust
experience

At Devoteam Cyber Trust, we have over 15 years of experience in providing cutting-edge offensive security services to organisations of all sizes across a wide range of industries. Our expert consultants are highly skilled and certified in industry standards such as PCI QSA, CREST, and ISO 27001, and have deep knowledge of the latest methodologies and tools used by potential attackers.

With our tailor made approaches, along with our persistent pentesting approach and vulnerability management platform, we provide continuous visibility into your security posture and can help you stay ahead of potential threats by proactively identifying and mitigating vulnerabilities and risks.

By working with us, you can have the confidence that comes with knowing that you are partnering with a leader in the field of offensive security.



(*) According to a recent report by IBM Security and the Ponemon Institute, the average cost of a data breach in 2021 was $4.24 million, or roughly 3.53 million euros

Offensive Security
Standards & Regulations

Beyond its operational benefits in identifying vulnerabilities and mitigating potential risks, offensive security testing is also becoming increasingly important for organisations from a regulatory and compliance perspective.

By engaging in offensive security testing and vulnerability management, organisations can demonstrate their commitment to meeting regulatory and compliance requirements, as well as aligning with best practices for information security management.

- **ISO 27001:** Annex A of the standard contains a set of controls that relate to information security risk management, including requirements for regular risk assessments and the implementation of appropriate controls to mitigate identified risks. Offensive security testing can help organisations to achieve compliance with these requirements.
- **NIS2:** The directive includes specific requirements for regular penetration testing and vulnerability assessments for operators of essential services and digital service providers. This is covered in Article 14 of the directive.
- **GDPR:** Article 32 of the regulation requires companies to implement appropriate measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, and recommends offensive security testing as a method for achieving this.
- **NIST CSF:** The Framework emphasizes the importance of proactive identification and mitigation of potential vulnerabilities and risks, and includes requirements for regular vulnerability assessments and penetration testing, which are covered in the Identify and Protect functions.
- **PCI-DSS:** Requirement 11.3 of the standard mandates regular external and internal penetration testing and vulnerability scanning to identify and mitigate potential vulnerabilities in systems that process or store payment card data. Offensive security testing is a key tool for meeting these requirements and ensuring the security of payment card data.

"it's not if, but when"

With cyber attacks being a constant threat, it's no longer a question of if an attack will occur, but when.

To effectively manage this risk, organisations need to adopt a proactive approach to cybersecurity, including regular offensive security testing and vulnerability management.

Offensive Security

Services Portfolio

- Persistent Penetration Testing
- Traditional Penetration Testing
- WIFI security testing
- SCADA / Operational Technologies Penetration Testing
- Red Teaming
- Web Applications / APIs and Mobile Applications Penetration Testing
- Penetration Testing of IoT devices
- Reverse Engineering
- Infrastructure - External or Internal Penetration Testing
- Active Directory Penetration Testing
- Physical Security and Dropped Media exercises
- Digital footprint (OSINT)
- Social Engineering - Phishing / Spearphishing exercises
- VPN Remote Access Penetration Testing
- Source Code Review
- Ransomware

Our most in-demand service

Let's begin with KEEP-IT-SECURE-24: our star service

Effective Persistent Penetration Testing service and platform

KEEP-IT-SECURE-24 provides continuous services in terms of Pentesting, by a professional team of qualified and certified auditors, customised according to the needs and objectives of the client. This type of project can either focus on the technical component, processes and/or people, or more.

Our expert consultants use methodologies and attack tools the same way potential persistent attackers do, and will provide you with continuous feedback and a management platform showing your current vulnerabilities and risk levels.

	Traditional approach	Keep IT Secure 24
Penetration testing Applications/Systems	✓	✓
Continued Regular Testing	✗	✓
Deep Pen Testing	✗	✓
Scope	Limited	Not limited/dynamic
Change Management Integration	✗	✓
Re-testing After Correction	✗	✓
Vulnerability Management Framework	✗	✓
Online Metrics Regarding Risk Levels	✗	✓
Reporting	✗	✓
Correction Process Follow-Up	✗	✓

The service covers:

- Continuous penetration testing to identify and address potential vulnerabilities in real-time (including retesting).
- Customizable approach tailored to the specific needs and objectives of each client.
- Manual deep testing to greater and more accurate results.
- Access to our proprietary vulnerability management platform for easy and effective management of identified risks.
- Ongoing feedback and support from our expert consultants to ensure the highest level of security.
- Cost-effective managed services approach, providing long-term security benefits for our clients.

Know more about KEEP-IT-SECURE-24 at: www.keepitsecure24.com

Our most in-demand services

Pentesting Project

Our comprehensive and customisable penetration testing projects cover a wide range of areas, from infrastructure and web applications to mobile, Wi-Fi, IoT, and beyond, ensuring that our clients receive the most thorough and effective offensive security services available.

Red Teaming

Our Red Teaming exercises, designed to meet the rigorous standards of TIBER-EU, provide a holistic view of our clients' security posture, testing not only their technical defences but also their people and processes, and delivering a comprehensive set of recommendations to enhance their overall security.

Social Engineering

Our expert social engineering services test the human element of our clients' security, using a variety of techniques (phishing, smishing, dropped media) to simulate real-world attacks and identify vulnerabilities that can be addressed with targeted awareness training and other measures.

Digital Footprint (OSINT)

Our digital footprint (OSINT) services provide a comprehensive view of our clients' online presence, identifying potential vulnerabilities and areas of exposure that can be addressed through enhanced security measures, including targeted training and awareness programs.

Reporting Deliverables

At Devoteam Cyber Trust, we offer both traditional and dynamic reporting options for our offensive security services, giving our clients the flexibility to choose the format that best suits their needs.

Traditional

1. **Executive Summary:** A high-level overview of the key findings, including identified vulnerabilities, risks, and recommendations.
2. **Methodology:** A description of the approach and techniques used during the engagement, including tools and tactics employed, and any limitations or scope restrictions.
3. **Findings:** A detailed analysis of identified vulnerabilities, including severity, impact, and likelihood of exploitation, as well as potential attack vectors and scenarios.
4. **Risk Assessment:** An overall assessment of the risks posed by the identified vulnerabilities, including potential impact on the organisation, likelihood of exploitation, and recommended mitigation strategies.
5. **Recommendations:** Specific recommendations for remediation and mitigation of identified vulnerabilities, including technical solutions, process improvements, and training or education initiatives.
6. **Conclusion:** A summary of the key findings and recommendations, as well as any additional insights or observations from the engagement.
7. **Appendices:** Additional technical details, charts, graphs, and other supporting information to supplement the findings and recommendations in the main report.

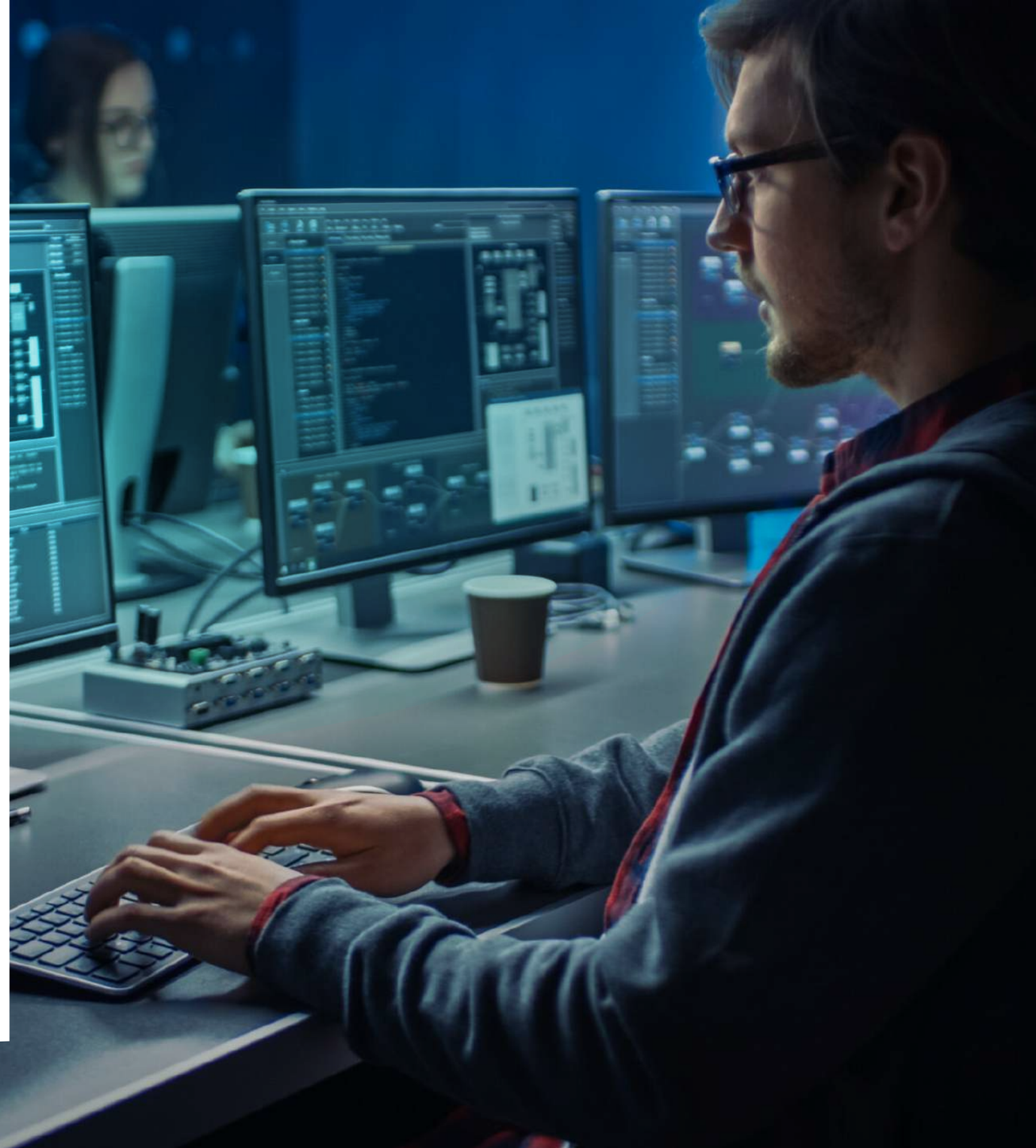
// Structure might vary depending on specific service

Dynamic

Our powerful vulnerability management platform, which also has an API, offers a real-time overview of your security risks and vulnerabilities, along with intuitive tools to track, report, and prioritise remediation efforts. Additionally, clients can integrate our platform with their existing systems to streamline their cybersecurity management process.

Know the Benefits

- Identifying and mitigating potential vulnerabilities before they can be exploited by attackers.
- Improved overall security posture, with a deeper understanding of system and application weaknesses.
- Compliance with industry regulations and best practices, including PCI-DSS, ISO 27001, NIS2, and GDPR.
- Greater confidence and trust from clients, partners, and stakeholders in your organisation's security capabilities.
- Enhanced risk management, with a proactive approach to cybersecurity that reduces the likelihood and impact of successful attacks.
- More efficient use of resources and budgets, with a focus on targeted testing and prioritisation of vulnerabilities.
- Continuous testing and monitoring, with persistent penetration testing providing ongoing feedback and risk management capabilities.
- Greater flexibility and customisation, with offensive security testing tailored to the specific needs and goals of your organisation.



Certifications & Clients

Backed by a diverse portfolio of global clients and a wide range of certifications, including CREST, ISO 27001, ISO 27701, ISO 9001 and PCI QSA, Devoteam Cyber Trust is the premier choice for organisations seeking the highest level of experti - se in offensive security services.

ISO 27001 (2012)

CREST (2014)

ISO 9001 (2014)

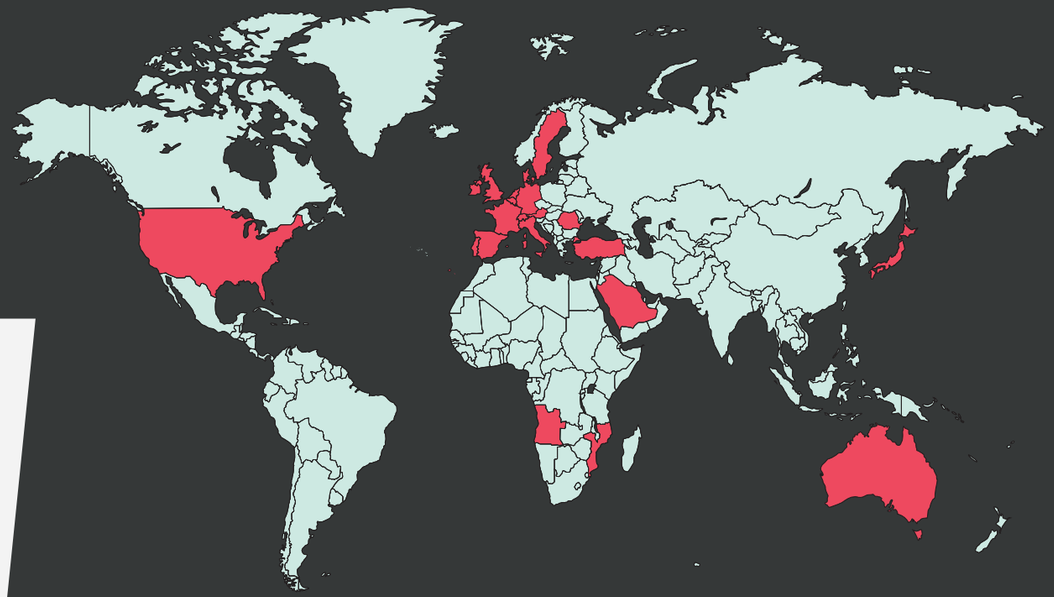
PNSC (2017)

PCI (2020)

Bancontact (2021)

ISO 27701 (2023)

EPi (2024)



More than 20 countries over the world

With HQ in Lisbon, we provide services to a wide **number of large and medium-sized companies**, both at a national and international level.

Case Studies

Risk Management of Strategic Partners

Type of Client: Pharmaceutical / Biotechnology with more than 15,000 employees and global presence

Challenge: The Client has a set of strategic partners that provide technological solutions, mainly in CaaS (Cloud as a Service) model, and the client did not have the structure nor the in-depth knowledge to regularly perform the assessment of the cybersecurity posture of its partners and the potential risks that may arise from this.

Red Teaming

Type of Client: Utilities

Challenge: The client sought to improve its security posture and response protocols to better defend against cyber threats. They engaged our team to conduct a red teaming exercise, with the goal of identifying weaknesses in their systems and processes. Our team conducted a Red Team Exercise on the company's networks and systems using a range of techniques, including social engineering, phishing, and lateral movement.

Persistent Pentesting Security Services

Type of Client: Financial Entity with more than 35,000 employees and with global presence

Challenge: The Client has a very considerable set of business applications, with very sensitive data and financial transaction support, and with a high dynamic of updates.
The Client felt that the traditional test model could not keep up with the dynamics of their business requirements, as well as felling a lack of agility in the reporting process and management of the results of their Pentesting actions.

What our clients are saying about us

"

The project is a success, the team has loads of technical expertise, they performed above expectations.

HEALTH

"

This is a win-win service and the report level is amazing.

ENERGY

"

It's very easy and reliable to work with Devoteam Cyber Trust.

BANKING

Click **here** to know more about these and other case studies, the solutions applied and the impact

Why engage with Devoteam Cyber Trust

- Deep expertise and experience in offensive security testing, with over 15 years of industry-leading experience
- A team of highly certified and experienced security professionals, with certifications including OSCP, CISSP, and CREST
- Comprehensive coverage and flexibility, with a wide range of offensive security services and methodologies customised to the specific needs and goals of your organisation
- A commitment to quality and excellence, with a focus on delivering the highest levels of service and customer satisfaction
- Access to advanced technology and tools, including a vulnerability management platform with 10 years of maturity and a range of specialised testing frameworks and software
- Compliance with industry standards and regulations, including PCI-DSS, ISO 27001, NIS2, GDPR, and other relevant guidelines and frameworks management capabilities
- A focus on long-term partnerships and ongoing support, with persistent penetration testing and regular reporting providing ongoing feedback and risk management capabilities services
- A global footprint and reputation, with clients in over 20 countries and a proven track record of delivering effective and high-quality offensive security testing services

How to Engage

01

Schedule an initial conversation with our expert consultants to discuss your needs, goals, and concerns.

02

Review and approve our customised proposal outlining the scope of our services, timeline, and costs.

03

Finalize the details of the engagement, including testing methodologies and scope.

04

Gain real-time insights into your security risks and vulnerabilities through our vulnerability management platform.

05

Receive regular updates on our progress, including detailed reports and remediation recommendations.

06

Access ongoing support and guidance from our team as needed.

Devoteam Cyber Trust is the right partner to support your organisation in this intense and evolving threat landscape, with best-in-class Offensive Security Services.

This is why dozens of medium-large clients from over 20 countries worldwide trust our services.

We are happy to share **our experience** and help you improve your **cyber security practice.**

Contact us

info@integrity.pt

Present in more than 12 countries across EMEA

www.integrity.pt

devoteam Cyber Trust

About devoteam Cyber Trust

www.integrity.pt

www.devoteam.com/expertise/cyber-trust

Devoteam Cyber Trust is the Cybersecurity specialist arm of the Devoteam Group. With our 800+ experts located across EMEA, we aim to establish cybersecurity as an enabler of business success rather than a gatekeeper. We leverage an end-to-end approach to Cyber Resillience, Applied Security, and Managed Security services to secure the tech journey of large and medium-sized companies from all sectors and industries.

Since 2009, previously known as INTEGRITY, our team based in Portugal is specialised in providing cutting-edge Managed Security Services that combine its expertise and proprietary technology to consistently and effectively reduce the cyber risk of our clients. The comprehensive service range includes Persistent intrusion Testing, ISO 27001, PCI-DSS, GRC Consulting and Solutions, and Third-Party Risk Management, ISO 27001 (Information Security), ISO 27701 (Privacy Information Management) and ISO 9001 (Quality) certified, PCI-QSA, and member os CREST and CIS - Centre for Internet Security, we provide services to a considerable number of clients, operating in more than 20 countries.

About devoteam

www.devoteam.com

Devoteam is a leading consulting firm focused on digital strategy, tech platforms and cybersecurity.

By combining creativity, tech and data insights, we empower our customers to transform their business and unlock the future.

With 25 years' experience and 10,000 employees across Europe, the Middle East and Africa, Devoteam promotes responsible tech for people and works to create better change.

Creative tech for Better Change