Potencie a sua defesa com a nossa competência em segurança ofensiva

Mantenha-se à frente de potenciais ameaças com testes de segurança ofensiva abrangentes e personalizados e recomendações para remediação.

devoteam
Cyber Trust

A última década assistiu a um crescimento explosivo na utilização de tecnologia digital em todas as indústrias, à medida que as empresas abraçaram as vantagens de maior eficiência, conveniência e conectividade que as ferramentas digitais podem proporcionar. Isso levou a uma maior dependência de canais de comunicação digital para tudo, desde interações com clientes até colaboração interna de equipas e gestão da cadeia de fornecimento.
Ao mesmo tempo, a cibercriminalidade cresceu a uma taxa alarmante, com hackers e outros atores mal-intencionados cada vez mais a direcionar os seus ataques a sistemas e dados digitais como meio de obter acesso a informações confidenciais, propriedade intelectual, ativos financeiros e muito mais. De acordo com pesquisas recentes, os danos causados pela cibercriminalidade devem chegar a US$ 10,5 trilhões anualmente até 2025, um aumento em relação aos US$ 3 trilhões em 2015.

Na era digital de hoje, as organizações reconhecem que a segurança cibernética é uma parte crítica dos negócios e que ela deve ser gerida ativamente para proteger contra a crescente ameaça de ataques cibernéticos. Para isso, a maioria das empresas está a usar padrões do setor e melhores práticas para implementar uma abordagem de gestão de risco que ajuda a identificar e mitigar potenciais vulnerabilidades e riscos.

No entanto, embora essas medidas sejam uma parte essencial de uma prática geral de gestão de segurança cibernética, elas são frequentemente reativas por natureza e podem falhar na deteção de ameaças mais avançadas e persistentes.
É aqui que a segurança ofensiva entra em jogo - através de testes proativos de sistemas e aplicações para identificar potenciais vulnerabilidades e fraquezas antes que possam ser exploradas por atores mal-intencionados.

Experiência da Devoteam Cyber Trust

Na Devoteam Cyber Trust, temos mais de 15 anos de experiência em fornecer serviços de segurança ofensiva de ponta para organizações de todos os tamanhos numa ampla gama de setores. Os nossos consultores especializados são altamente qualificados e certificados em standards do setor, como PCI QSA, CREST e ISO 27001, e têm amplo conhecimento das últimas metodologias e ferramentas utilizadas por potenciais atacantes.

Com as nossas abordagens personalizadas, juntamente com a nossa prática persistente de testes de intrusão e plataforma de gestão de vulnerabilidades, fornecemos visibilidade contínua à sua postura de segurança e podemos ajudá-lo a manter-se à frente de possíveis ameaças, identificar e mitigar proativamente vulnerabilidades e riscos.

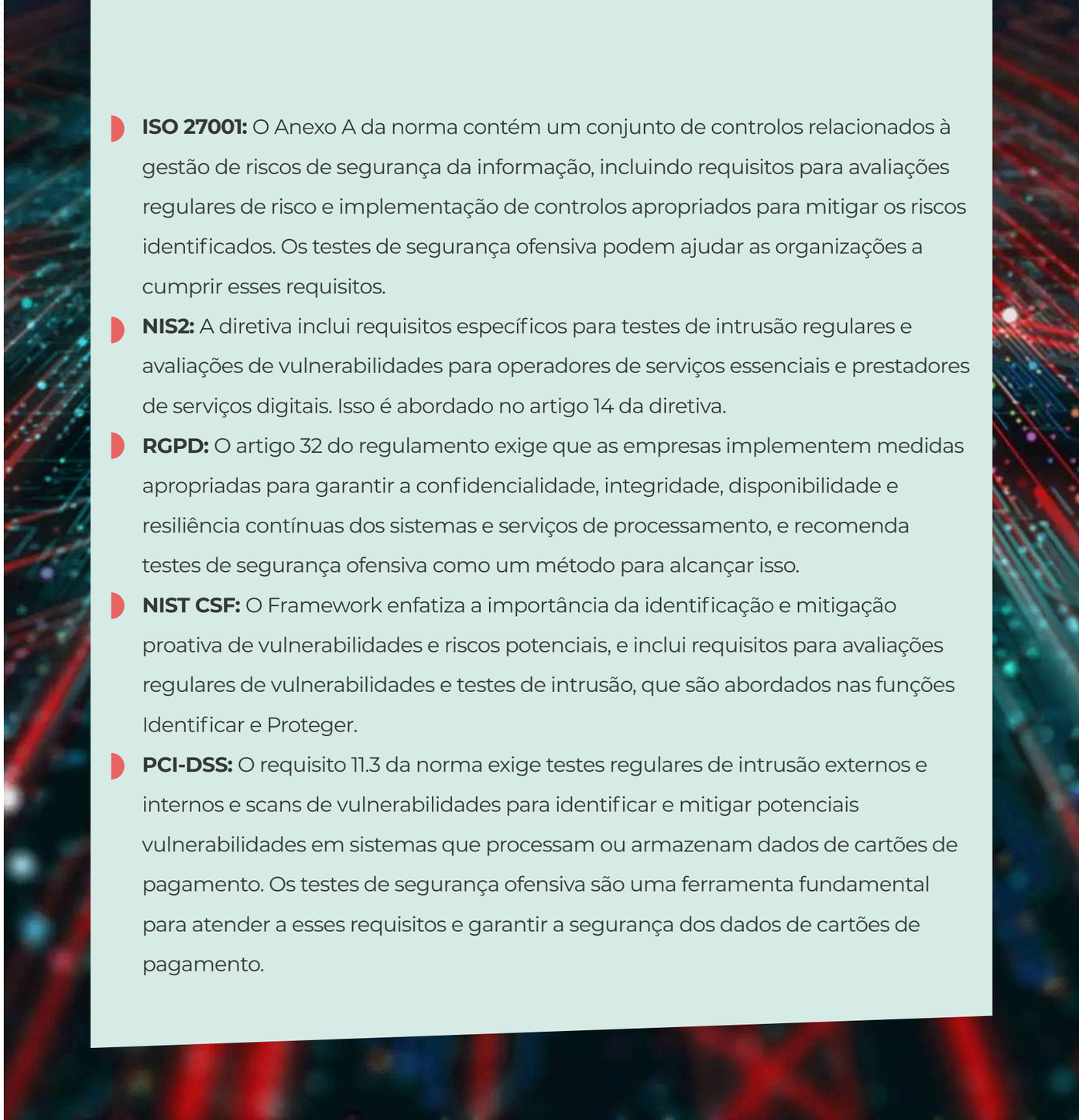
Ao trabalhar connosco, pode ter a confiança que estará associado a um líder no campo da segurança ofensiva.

(*) De acordo com um relatório recente da IBM Security e do Ponemon Institute, o custo médio de uma violação de dados em 2021 foi de US$ 4,24 milhões, ou aproximadamente 3,53 milhões de euros.

Segurança Ofensiva
Normas e Regulamentos

Além dos benefícios operacionais na identificação de vulnerabilidades e mitigação de riscos potenciais, os testes de segurança ofensiva estão a tornar-se cada vez mais importantes para as organizações do ponto de vista regulatório e de conformidade.

Ao realizar testes de segurança ofensiva e gestão de vulnerabilidades, as organizações podem demonstrar o seu compromisso em atender aos requisitos regulatórios e de conformidade, bem como alinhar-se às melhores práticas para a gestão da segurança da informação.



- **ISO 27001:** O Anexo A da norma contém um conjunto de controlos relacionados à gestão de riscos de segurança da informação, incluindo requisitos para avaliações regulares de risco e implementação de controlos apropriados para mitigar os riscos identificados. Os testes de segurança ofensiva podem ajudar as organizações a cumprir esses requisitos.
- **NIS2:** A diretiva inclui requisitos específicos para testes de intrusão regulares e avaliações de vulnerabilidades para operadores de serviços essenciais e prestadores de serviços digitais. Isso é abordado no artigo 14 da diretiva.
- **RGPD:** O artigo 32 do regulamento exige que as empresas implementem medidas apropriadas para garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de processamento, e recomenda testes de segurança ofensiva como um método para alcançar isso.
- **NIST CSF:** O Framework enfatiza a importância da identificação e mitigação proativa de vulnerabilidades e riscos potenciais, e inclui requisitos para avaliações regulares de vulnerabilidades e testes de intrusão, que são abordados nas funções Identificar e Proteger.
- **PCI-DSS:** O requisito 11.3 da norma exige testes regulares de intrusão externos e internos e scans de vulnerabilidades para identificar e mitigar potenciais vulnerabilidades em sistemas que processam ou armazenam dados de cartões de pagamento. Os testes de segurança ofensiva são uma ferramenta fundamental para atender a esses requisitos e garantir a segurança dos dados de cartões de pagamento.

"Não é uma questão de se, mas de quando"

Sendo os ataques cibernéticos uma ameaça constante, não é uma questão se um ataque irá ocorrer, mas sim quando.

Para gerir efetivamente esse risco, as organizações precisam de adotar uma abordagem proativa em relação à cibersegurança, incluindo testes regulares de segurança ofensiva e gestão de vulnerabilidades.

Portfólio de serviços de
Segurança Ofensiva

- 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

O nosso serviço mais procurado

Comecemos com o KEEP-IT-SECURE-24: o nosso principal serviço

Serviço e plataforma eficazes de Testes de Intrusão Persistentes

O KEEP-IT-SECURE-24 oferece serviços contínuos de PenTest, realizados por uma equipa profissional de auditores qualificados e certificados, personalizados de acordo com as necessidades e objetivos do cliente. Este tipo de projeto pode focar-se apenas na componente técnica, nos processos e/ou pessoas, ou em todos eles.

Os nossos consultores especializados utilizam metodologias e ferramentas de ataque da mesma forma que os potenciais atacantes, e fornecem feedback contínuo através de uma plataforma de gestão que apresenta os seus níveis atuais de vulnerabilidades e risco.

	Abordagem tradicional	Keep IT Secure 24
Testes à segurança dos Sistemas e Aplicações	✓	✓
Testes Continuados / Regulares	✗	✓
Deep Pen Testing	✗	✓
Âmbito	Limitado	Sem limites/dinâmico
Integração com Change Management	✗	✓
Re-testes após Correção	✗	✓
Ferramenta de Gestão de Vulnerabilidades	✗	✓
Métricas Online	✗	✓
Reporte dinâmico	✗	✓
Acompanhamento na Correção	✗	✓

O serviço inclui:

- Testes de Intrusão contínuos para identificar e gerir potenciais vulnerabilidades em tempo real (incluindo retestes).
- Abordagem personalizada adaptada às necessidades e objetivos específicos de cada cliente.
- Testes manuais em profundidade para resultados mais precisos e efetivos.
- Acesso à nossa plataforma proprietária de gestão de vulnerabilidades para uma gestão fácil e eficaz dos riscos identificados.
- Feedback e suporte contínuo dos nossos consultores especializados para garantir o mais alto nível de segurança.
- Abordagem de gestão de serviços rentável, proporcionando benefícios de segurança a longo prazo para os nossos clientes.

Saiba mais sobre o KEEP-IT-SECURE-24 em: www.keepitsecure24.com

Os nossos serviços mais procurados

Pentesting Project

Os nossos projetos abrangentes e personalizáveis de teste de intrusão cobrem uma ampla gama de áreas, desde infraestrutura e aplicações web, até dispositivos móveis, Wi-Fi, IoT, garantindo que os nossos clientes recebam os serviços de segurança ofensiva mais completos e eficazes disponíveis.

Red Teaming

Os nossos exercícios de Red Teaming, projetados para atender aos rigorosos padrões do TIBER-EU, fornecem uma visão holística da postura de segurança dos nossos clientes, testando não apenas as suas defesas técnicas, mas também as pessoas e os processos envolvidos, e fornecendo um conjunto abrangente de recomendações para melhorar a sua segurança geral.

Social Engineering

Os nossos serviços especializados de engenharia social testam o elemento humano da segurança dos nossos clientes, utilizando uma variedade de técnicas (phishing, smishing, dropped media) para simular ataques do mundo real e identificar vulnerabilidades que podem ser abordadas com formação/treino de consciencialização direcionado entre outras medidas.

Digital Footprint (OSINT)

Os nossos serviços de pegada digital (OSINT) fornecem uma visão abrangente da presença online dos nossos clientes, identificando possíveis vulnerabilidades e áreas de exposição que podem ser abordadas por meio de melhorias dos controlos de segurança, incluindo programas de formação e consciencialização direcionados.

Entregáveis

Na Devoteam Cyber Trust, oferecemos opções de relatórios tradicionais e dinâmicos para os nossos serviços de segurança ofensiva, que permite aos nossos clientes a flexibilidade de escolher o formato que melhor se adapta às suas necessidades.

Tradicionais

1. **Resumo Executivo:** Uma visão geral de alto nível das principais descobertas, que inclui vulnerabilidades, riscos identificados e recomendações.
2. **Metodologia**: Uma descrição da abordagem e técnicas utilizadas durante o decorrer do projeto, incluindo ferramentas e táticas utilizadas, bem como quaisquer limitações ou restrições de âmbito.
3. **Descobertas**: Uma análise detalhada das vulnerabilidades identificadas, incluindo gravidade, impacto e probabilidade de exploração, bem como possíveis vetores e cenários de ataque.
4. **Avaliação de Risco**: Uma avaliação geral dos riscos apresentados pelas vulnerabilidades identificadas, incluindo o potencial impacto na organização, a probabilidade de exploração e as estratégias de mitigação recomendadas.
5. **Recomendações**: Recomendações específicas para remediação e mitigação de vulnerabilidades identificadas, incluindo soluções técnicas, melhorias de processos e iniciativas de formação/treino ou educação.
6. **Conclusão**: Um resumo das principais descobertas e recomendações, bem como quaisquer informações adicionais ou observações resultantes do processo.
7. **Apêndices**: Detalhes técnicos adicionais, gráficos, tabelas e outras informações de suporte para complementar as descobertas e recomendações no relatório principal.

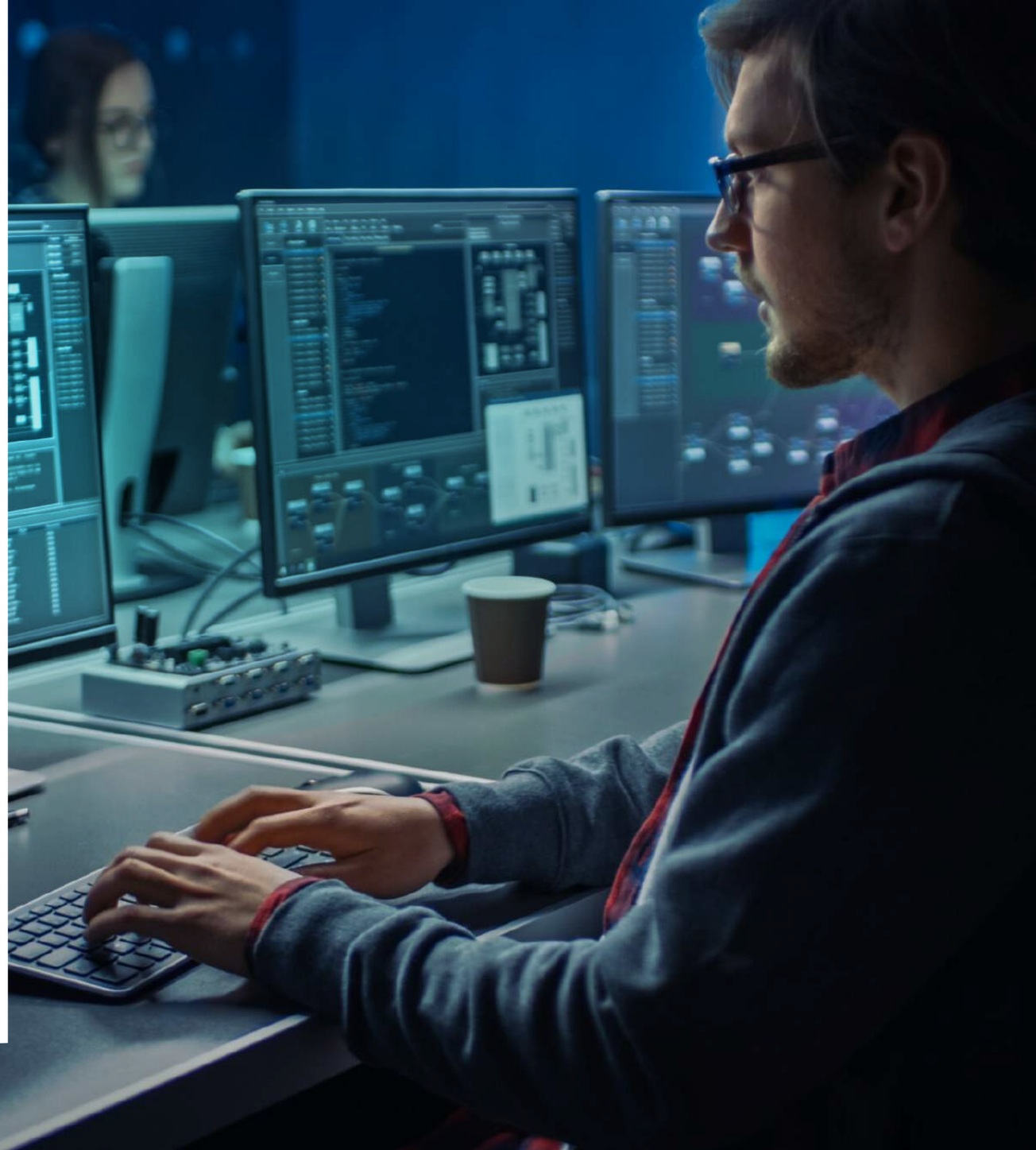
// A estrutura pode variar dependendo do serviço específico.

Dinâmicos

A nossa poderosa plataforma de gestão de vulnerabilidade, que também possui uma API, oferece uma visão em tempo real dos seus riscos e vulnerabilidades de segurança, juntamente com ferramentas intuitivas para rastrear, relatar e priorizar os eforços de remediação. Além disso, os clientes podem integrar a nossa plataforma com os seus sistemas existentes para simplificar o seu processo de gestão de cibersegurança.

Conheça os Benefícios

- Identificar e mitigar potenciais vulnerabilidades antes que possam ser exploradas por atacantes.
- Melhoria da postura geral de segurança, com uma compreensão mais profunda das fraquezas do sistema e aplicativos.
- Conformidade com regulamentações e melhores práticas da indústria, incluindo PCI-DSS, ISO 27001, NIS2 e RGPD.
- Maior confiança e confiabilidade de clientes, parceiros e stakeholders nas capacidades de segurança da sua organização.
- Gestão de riscos aprimorada, com uma abordagem proativa à segurança cibernética que reduz a probabilidade e o impacto de ataques bem-sucedidos.
- Uso mais eficiente de recursos e orçamentos, com foco em testes direcionados e priorização de vulnerabilidades.
- Testes e monitorização contínuos, com testes de intrusão persistentes fornecendo feedback contínuo e capacidades de gestão de riscos.
- Maior flexibilidade e personalização, com testes de segurança ofensivos adaptados às necessidades e objetivos específicos da sua organização.



Certificações & Clientes

Apoiada numa carteira diversificada de clientes globais e numa ampla gama de certificações, incluindo CREST, ISO 27001, ISO 27701, ISO 9001 e PCI QSA, a Devo - team Cyber Trust é a principal opção para organizações que procuram o mais alto nível de especialização em serviços de segurança ofensiva.

ISO 27001 (2012)

CREST (2014)

ISO 9001 (2014)

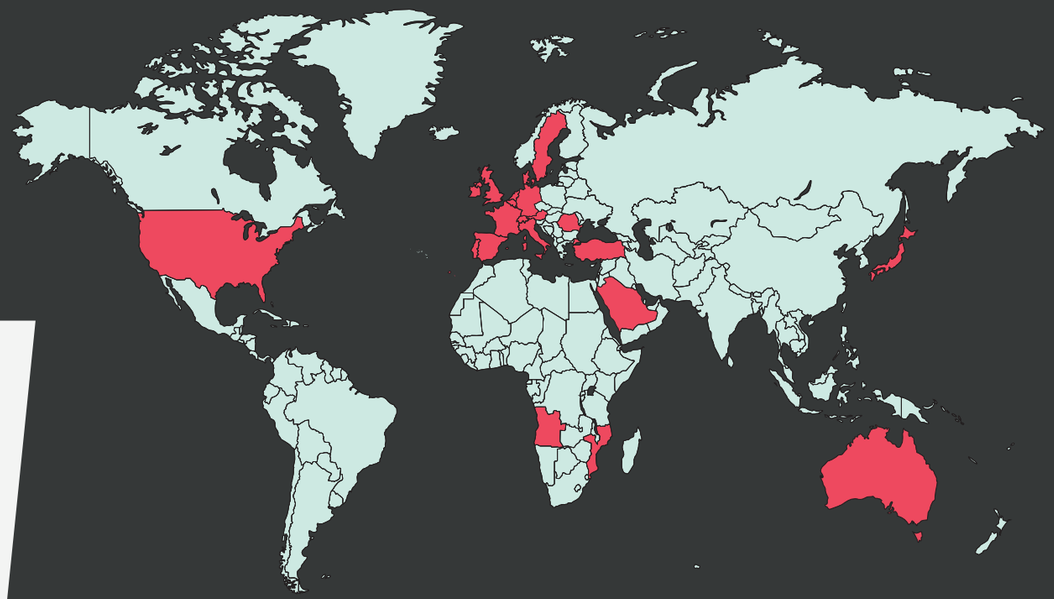
PNSC (2017)

PCI (2020)

Bancontact (2021)

ISO 27701 (2023)

EPi (2024)



Mais de 20 países em todo o mundo

Com sede em Lisboa, prestamos serviços a um **grande número de empresas de grande e média dimensão**, tanto a nível nacional como internacional.

Casos de Estudo

Gestão de Risco de Parceiros Estratégicos

Tipo de Cliente: Farmacêutica/Biotecnologia com mais de 15.000 funcionários e presença global

Desafio: O Cliente possui um conjunto de parceiros estratégicos que fornecem soluções tecnológicas, principalmente no modelo CaaS (Cloud as a Service), e o cliente não tinha a estrutura nem o conhecimento aprofundado para realizar regularmente a avaliação da postura de cibersegurança dos seus parceiros e os potenciais riscos que possam surgir disso.

Red Teaming

Tipo de Cliente: Instituição no setor da Energia

Desafio: O cliente procurava melhorar a sua postura de segurança e protocolos de resposta para se defender melhor contra ameaças cibernéticas. A nossa equipa foi contratada para conduzir um exercício de Red Teaming, com o objetivo de identificar falhas nos seus sistemas e processos. A nossa equipa realizou um exercício de Red Team nos sistemas e redes da empresa e utilizou uma variedade de técnicas, incluindo engenharia social, phishing e movimento lateral.

Serviço de Testes de Segurança Persistentes

Tipo de Cliente: Entidade Financeira com mais de 35.000 colaboradores e com presença global

Desafio: O Cliente detém um conjunto muito considerável de aplicações de negócio, com dados muito sensíveis e de suporte a transações financeiras, e com uma elevada dinâmica de atualizações.
O Cliente sentia que o modelo de teste tradicional não conseguia acompanhar a dinâmica dos seus requisitos de negócio, bem como sentia pouca agilidade no processo de reporting e gestão dos resultados das suas ações de testes de intrusão.

O que dizem os nossos clientes

"

O projeto é um sucesso, a equipa tem muito conhecimento técnico, superou as expectativas.

SAÚDE

"

Este é um serviço win-win e o nível de análise é incrível.

ENERGIA

"

É muito fácil e fiável trabalhar com a Devoteam Cyber Trust.

BANCO

Clique **aqui** para saber mais sobre estes e outros casos de estudo, as soluções aplicadas e o impacto.

Porquê trabalhar com a Devoteam Cyber Trust

- Profundo conhecimento e experiência em testes de segurança ofensiva, com mais de 15 anos de experiência líder da indústria
- Uma equipa de profissionais de segurança altamente certificados e experientes, com certificações como OSCP, CISSP e CREST
- Cobertura abrangente e flexibilidade, com uma ampla gama de serviços e metodologias de segurança ofensiva personalizados às necessidades e objetivos específicos da sua organização
- Compromisso com qualidade e excelência, com foco na entrega dos mais altos níveis de serviço e satisfação do cliente
- Acesso à tecnologia e ferramentas avançadas, que inclui uma plataforma de gestão de vulnerabilidades com 10 anos de maturidade e uma variedade de estruturas e software de teste especializados
- Conformidade com padrões e regulamentos do setor, incluindo PCI-DSS, ISO 27001, NIS2, RGPD e outras diretrizes e normas relevantes
- Foco em parcerias de longo prazo e suporte contínuo, com testes de Intrusão persistentes e relatórios regulares fornecendo feedback contínuo e capacidades de gestão de riscos
- Presença global e reputação, com clientes em mais de 20 países e um histórico comprovado de fornecer serviços eficazes e de alta qualidade de testes de segurança ofensiva

Como Começar

01

Agende uma conversa inicial com os nossos consultores especializados para discutir as suas necessidades, objetivos e preocupações.

02

Analise e aprove a nossa proposta personalizada delineando o âmbito dos nossos serviços, prazos e custos.

03

Finalize os detalhes da proposta, incluindo metodologias e âmbito de testes.

04

Obtenha informações em tempo real sobre os seus riscos e vulnerabilidades de segurança através da nossa plataforma de gestão de vulnerabilidades.

05

Receba atualizações regulares sobre o nosso progresso, incluindo relatórios detalhados e recomendações de remediação.

06

Receba suporte e orientação contínuos da nossa equipa, conforme necessário.

Devoteam Cyber Trust é o parceiro certo para apoiar a sua organização neste cenário de ameaças intenso e em constante evolução, com Serviços de Segurança Ofensiva de classe mundial.

É por isso que dezenas de clientes de média e grande dimensão em mais de 20 países em todo o mundo confiam nos **nossos serviços.**

Estamos disponíveis para partilhar a nossa **experiência** e ajudá-lo a melhorar as suas práticas de **cibersegurança**.

A gestão equilibrada dos riscos requer uma estratégia sólida.

Fale connosco.

Contacte-nos

info@integrity.pt

Presentes em mais de 12 países da EMEA

www.integrity.pt

devoteam Cyber Trust

Sobre devoteam Cyber Trust

www.integrity.pt

www.devoteam.com/expertise/cyber-trust

A Devoteam Cyber Trust é a unidade especializada em cibersegurança do Grupo Devoteam. Com mais de 800 especialistas localizados na região EMEA, o nosso objetivo é estabelecer a cibersegurança como um facilitador do sucesso dos negócios, em vez de um obstáculo. Utilizamos uma abordagem abrangente de Resiliência Cibernética, Segurança Aplicada e Gestão de Serviços de Segurança para proteger a jornada tecnológica de empresas de grande e média dimensão de todos os setores e indústrias.

Desde 2009, anteriormente com a denominação INTEGRITY, a nossa equipa sediada em Portugal é especializada em fornecer Serviços Geridos de Segurança de ponta, que combina a sua expertise e tecnologia proprietária para reduzir de forma consistente e eficaz o risco cibernético dos nossos clientes. A ampla gama de serviços abrange Testes Persistentes de Intrusão, ISO 27001, PCI-DSS, Consultoria e Soluções de GRC e Gestão de Riscos de Terceiras Partes. Certificados em ISO 27001 (Segurança da Informação), ISO 27701 (Gestão de Informação Privada) e ISO 9001 (Qualidade), PCI-QSA e membros da CREST e CIS - Centro de Segurança na Internet, prestamos serviços a um número considerável de clientes, operando em mais de 20 países.

Sobre devoteam

www.devoteam.com

A Devoteam é uma consultora líder focada em estratégia digital, plataformas tecnológicas e cibersegurança.
Ao combinar criatividade, tecnologia e insights de dados, capacitamos os nossos clientes a transformar os seus negócios e desbloquear o futuro.
Com 25 anos de experiência e 10.000 funcionários em toda a Europa, Oriente Médio e África, a Devoteam promove tecnologia responsável para as pessoas e trabalha para criar mudanças positivas.
Creative tech for Better Change