www.pwc.com/ao/academy
www.pwc.pt/cybersecurity

Cyber Arena

PwC's Academy em Angola
De profissionais para profissionais

CyberArena: uma experiência real de cibersegurança

O Cyber Arena é um jogo online em ambiente web que simula o ambiente de segurança da sua organização e o dia a dia da mesma, através de um conjunto de ataques cibernéticos aos quais terá de dar resposta.

Através do jogo pode testar as suas sensações, respostas e ideias. Todas as opções são válidas, mas cada uma tem o seu impacto.

Destinatários

Executivos C-Level - Colaboradores que não pertencem ao IT, mas que no seu trabalho lidam com áreas de IT. No jogo serão responsáveis por decisões estratégicas (e.g. aprovar aquisições)

IT Operations - Responsáveis por garantir a contínua operação dos sistemas

IT Security - Responsáveis por analisar as ameaças e articular com IT Operations as acções (e.g. aquisição SW/HW)

***Online* com formador**

pwc

Leia o QR Code para saber mais sobre a PwC's Academy em Angola.

Programa

1 Boas vindas e instruções de acesso

2 Cyber Security Awareness

3 O que é o Cyber Arena?

4 Realização do jogo: Cyber Arena

5 **Análise de outputs/jogo**

O jogo e aprendizagens (estratégias de sucesso usadas, ataques bloqueados, etc)

Comportamentos que existem e serão mudados

Reflexão sobre o que percepciona estar menos correto na estratégia de Cyber da sua organização e deve ser mudado

Duração: 6 horas

Horário: A definir
Valor: 600 euros*

Inclui: envio de materiais de apoio e certificado de formação PwC

Inscreva-se em:
www.pwc.com/ao/academy **ou envie um email para:** ao_pwcsacademy@pwc.com

A PwC reserva-se ao direito de admissão

* Acresce o IVA aos valores apresentados.

A presença na acção de formação fica sujeita ao pagamento antecipado do valor da inscrição.

Como funciona?

A PwC fará um *setup* de um cenário standard com o objetivo de garantir que reflete os sistemas mais comuns nas empresas. Trata-se de um passo importante, porque as ameaças são particulares de determinada tecnologia, e permite criar uma experiência real, envolvente, em ambiente de simulação.

Divisão dos elementos por 3 equipas, onde cada uma terá acesso a um *dashboard* distinto com ações relacionadas com o seu dia-a-dia.

Arranque do jogo, com duração média de 2 horas. Haverá um ecrã com o progresso do jogo. O CyberArena tem um motor de ameaças de cibersegurança que serão geradas de acordo com o tipo de assets, e o seu impacto (financeiro e reputacional) irá variar de acordo com o ambiente de segurança da organização e com as acções tomadas em conjunto pelos 3 grupos que estão a participar na experiência.

O jogo é terminado com sucesso, caso consigam manter um elevado nível de reputação e tenham capacidade de aumentar o *cashflow* da empresa.

Benefícios do jogo para ajudar a potenciar e identificar estratégias de defesa

Benefícios

- **Criação de um ambiente realista e totalmente customizado(1)** do ambiente de **IT e OT** da sua organização. - somos capazes de espelhar a infraestrutura.
- **Simulação em tempo real de ataques cibernéticos** e cenários pós-incidentes que afetam o negócio principal e a capacidade de cumprir os objectivos corporativos (e.g indicadores financeiros, reputação, etc).
- **Verificar a eficácia da atual estratégia de segurança cibernética** da sua organização.
- **Compreender as necessidades e motivações das diferentes equipas** e funções (Top management, IT Security e IT Operations).
- **Reconhecer novas ameaças relevantes** e aplicáveis à sua infraestrutura de IT e OT.
- **Aprender com os erros** tendo por base o *feedback* da simulação / análise pós-simulação.
- **Criar canais de comunicação** entre diferentes equipas e funções.
- **Prioritize tarefas** enquanto estiver sob pressão.

Vantagens estratégicas do CyberArena

Avaliar
Avalie a eficácia atual da segurança cibernética de sua empresa

Definir
Crie uma estratégia de defesa cibernética para o seu ambiente

Responder
Avalie a resposta a incidentes dos seus funcionários

Experienciar
Experiencie o impacto das decisões sem riscos reais

Medir
Meça a sua defesa cibernética contra eventos de ataque simulados

Comunicar
Crie canais de comunicação entre diferentes equipas e funções na organização

O CyberArena adaptado à sua realidade

Personalização (1)
Personalização completa de toda a simulação para as especificações e necessidades do cliente

Ataques cibernéticos
Simular ataques cibernéticos em diversos ambientes já pré-criados

Comunicação
Dinâmica da ferramenta permite a comunicação constante dos intervenientes potenciando uma reflexão sobre o ambiente de cibersegurança

Configuração
Templates *standard* de **configuração** de ambiente da organização já **existentes** por indústria (serviços financeiros, energia, telecomunicações)

Pensar o cyber
Executar **cenários personalizados** de "*what-if*" para mostrar aos formandos os **benefícios de investimentos** potenciais em segurança

Multi-propósito
Solução excelente para **formações** de security awareness, **eventos** de recrutamento, **conferências** e muito mais

Uma experiência real na gestão de riscos decorrentes de ameaças cibernéticas

(1) - Dada a especificidade de customização, a componente de personalização para espelhar o cenário da sua empresa apenas se encontra disponível, para formações acima de 10 elementos.

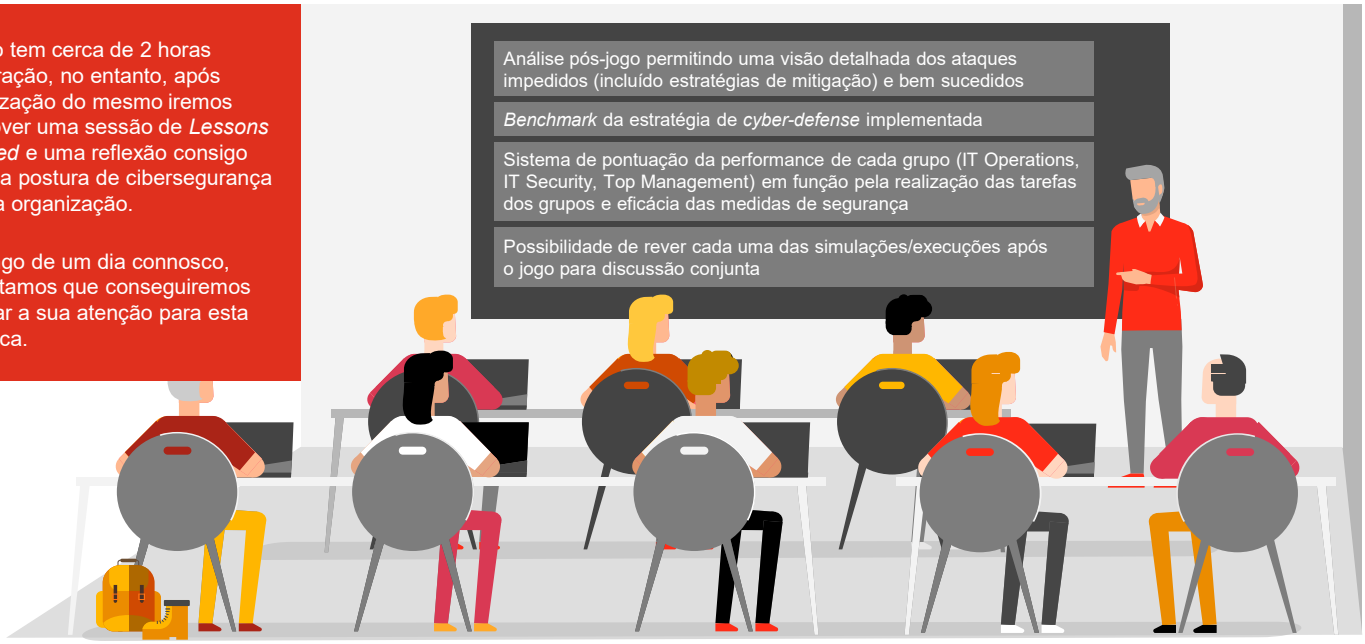
O CyberArena em 4 passos

Passo 1: Definir o ambiente	**Passo 2:** Definir as equipas	**Passo 3:** Executar a simulação	**Passo 4:** Avaliar a abordagem
A infraestrutura de IT ou OT da organização é criada na ferramenta Cyber Arena - criada via CMDB ou utilização de questionários caso haja necessidade de configuração específica do ambiente da empresa.. A defesa cibernética é adaptada na ferramenta Cyber Arena ao contexto - serão usados questionários personalizados e elementos. CyberArena pode ser adaptado a qualquer infraestrutura - não há limites. Podem ser utilizados Templates predefinidos para IT/OT e defesa cibernética.	Os participantes são divididos em 3 grupos com base nos seus conhecimentos e experiência em IT / Segurança. Cada grupo representa um dos seguintes grupos/funções: Top management, IT/OT operations, Cyber Security. Cada participante pode ter o seu próprio PC / tablet com um painel personalizado para a sua função específica no jogo. As principais informações do jogo são exibidas no painel principal, visível a todos os participantes.	Uma simulação dura cerca de uma hora (toda a sessão da Cyber Arena tem a duração de pelo menos 2 horas) e requer: • Construir a defesa cibernética • Lidar com ataques cibernéticos • Cumprir os objetivos financeiros • Comunicar no seio da equipa O objetivo da simulação é cumprir os objetivos financeiros e outros indicadores (e.g. reputação). Apenas uma empresa "saudável" é capaz de atingir a meta e uma estratégia adequada de segurança cibernética é crucial.	Depois da simulação terminar, um dashboard individual e para as funções é exibido e avaliado em conjunto. Este sumário apresenta: • Indicadores de *benchmarking* • *Best practices* da indústria • Recomendações Durante o processo de avaliação e reflexão, os principais *gaps* são identificados e o risco é avaliado conjuntamente.

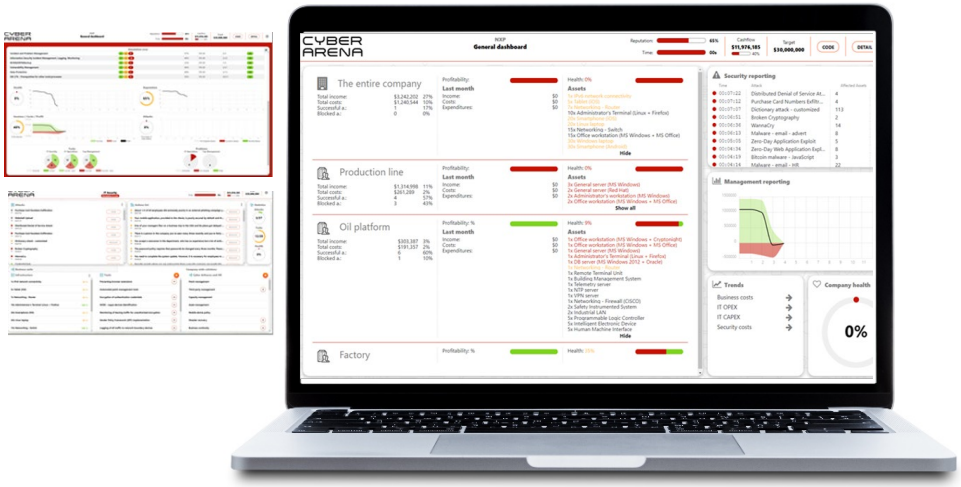
Que lições tirar para promover a discussão interna na sua organização?

O jogo tem cerca de 2 horas de duração, no entanto, após a realização do mesmo iremos promover uma sessão de *Lessons Learned* e uma reflexão consigo sobre a postura de cibersegurança da sua organização.

Ao longo de um dia connosco, acreditamos que conseguiremos chamar a sua atenção para esta temática.



O ambiente de jogo



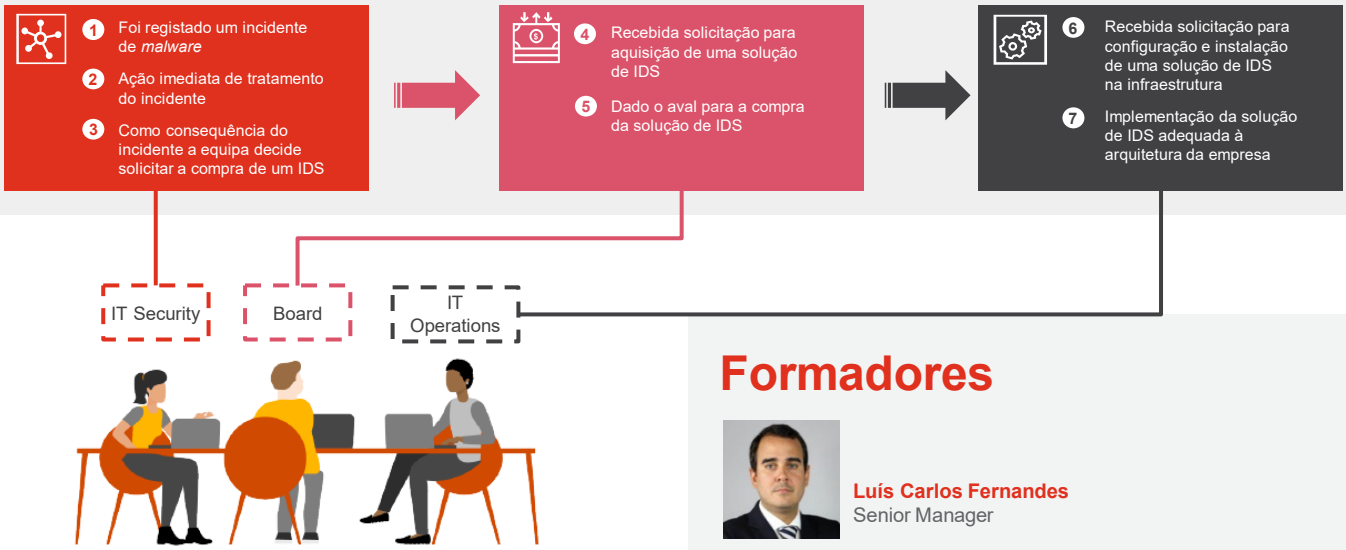
Se quiser saber mais, assista ao vídeo de introdução abaixo

https://www.youtube.com/watch?v=VoXPnCkWndo

CyberArena

Exemplo da dinâmica de jogo, através de um evento registado na equipa de Segurança

Ambiente de Jogo



Óscar Peres
Senior Associate

Senior Associate de Risk Assurance Services na PwC. Tem mais de 14 anos de experiência em auditoria de TI em várias indústrias

Tem o 5º Ano de engenharia informática, pela Faculdade de Engenharia da Universidade Agostinho Neto e é membro do ISACA - Information Systems Audit and Control Association.

Certificado Information Security Management System – ISO/IEC 27001 -

Tem participado ao longo da sua carreira em em diversos projectos relacionados com Controlo interno, Auditoria interna, Auditoria de sistemas de informação e processos de gestão de risco e continuidade de negócio.

Formadores

Luís Carlos Fernandes
Senior Manager

Senior Manager de Risk Assurance Services da PwC com 10 anos de experiência em auditoria e assessoria nas temáticas de sistemas de informação, segurança, processos e riscos/controlos.

Licenciado em Engenharia Informática e de Computadores pelo Instituto Superior Técnico. Encontra-se a frequentar o Advanced Development Program na Nova School of Business & Economics. Certificado ISO 27001 Lead Auditor, ITIL v3 Foundation e membro do ISACA - Information Systems Audit and Control Association.

Experiência relevante em processos de auditoria de sistemas e segurança de informação, Compliance Regulatório, Cibersegurança, Gestão de Risco, Continuidade de Negócio. Tem desenvolvido a sua prática auxiliando os clientes na implementação e no cumprimento de diversos frameworks e requisitos regulatórios tais como ITIL, Cobit, ISO 27001, ISO 20000, NIST CSF, EBA Guidelines (ICT & security risk management; outsourcing arrangements), ESMA Guidelines (Cloud Outsourcing Guidelines).

Marcelo Rodrigues
Director

Diretor de Risk Assurance Services da PwC com mais de 15 anos de experiência em auditoria de sistemas de informação, programação e Administração de Sistemas. É Licenciado em Ciência de Computadores na Faculdade de Ciências da Universidade do Porto e detentor das seguintes certificações:

Certificado CISA "Certified Information Systems Auditor" pela ISACA;

Certificado CISM "Certified Information Security Manager" pela ISACA; e

Certificação ITIL V3/2011, pela APMG.

Experiência profissional em sistemas em auditoria e segurança de informação. Tem coordenado equipas na realização de auditorias de segurança, testes de intrusão e análises de vulnerabilidades de sistemas de informação nos diversos formatos (caixa preta/branca), bem como na realização de diferentes tipos de testes (rede interno ou rede externa)

Contactos

Informações
PwC's Academy Luanda
Tel: +244 227 286 109
ao_pwcsacademy@pwc.com

Luanda
PricewaterhouseCoopers|Edifício Presidente,
Largo 17 de Setembro, nº 3, 1º andar - Sala 137
Luanda - República de Angola

Visite-nos nas redes sociais

www.pwc.com/ao/academy
www.pwc.pt/cybersecurity

© 2021 PricewaterhouseCoopers (Angola), Limitada. Todos os direitos reservados. Neste documento "PwC" refere-se a PricewaterhouseCoopers (Angola), Limitada que pertence à rede de entidades que são membros da PricewaterhouseCoopers International Limited, cada uma das quais é uma entidade legal autónoma e independente.