Simulação de Ataques em Cenários Realistas

Sumário

Para navegar pelos capítulos deste estudo, **clique nos botões na margem superior**. A qualquer momento, **clique no logo do Distrito no canto inferior direito para voltar a esta página.**

Metodologia

As startups delineadas no report foram selecionadas a partir de um trabalho minucioso de pesquisa e consulta ao banco de dados de startups proprietário do Distrito. Também foram realizadas consultas a bancos abertos e informações públicas do governo.

As startups foram examinadas individualmente para verificar adequação ao tema do report e aos critérios de seleção estabelecidos. São eles:

- **Ter a inovação no centro do negócio, seja na base tecnológica, no modelo de negócios ou na proposta de valor;**
- **Estar em atividade no momento da realização do estudo, medida pelo status do site e atividade em redes sociais;**
- **Desempenhar atividade diretamente relacionada ao setor estudado;**
- **Ter nacionalidade brasileira e operar atualmente no Brasil.**

O trabalho de definição das categorias foi baseado em análise da literatura relevante e das classificações utilizadas amplamente no mercado, no Brasil e no mundo.

A definição da categoria a que pertence cada startup foi feita por nossa equipe, e, quando uma startup opera em mais de uma categoria, a situamos na que interpretamos como sua atividade principal ou de maior visibilidade.

Também temos uma preocupação em incluir somente aquilo que consideramos startups—e, por mais que nosso critério para defini-las seja bastante amplo, excluímos alguns tipos de negócio que, embora muitas vezes se autodenominam startups, acabam fugindo do conceito. Isso inclui empresas que têm como característica principal serem:

- **Software Houses (desenvolvimento de software sob demanda);**
- **Consultorias;**
- **Agências de marketing, publicidade e design.**

Enfatizamos aqui que os números expostos podem sofrer alterações conforme a evolução da acurácia das informações e maior capacidade de interação com as próprias startups ao longo do tempo.

Entrevistados

Nelson Brito
Security Technical Solutions Architect
Cisco

Carlos Rust
CEO e Presidente
RustCon

Felipe Morgado
Gerente Executivo de Educação Profissional e Tecnológica
SENAI

Genivaldo Araújo
CEO
3CON

Introdução

Introdução

Longe de nós desmentir o clássico ditado popular de que “a prática leva à perfeição”. Quando o assunto é segurança cibernética, a experiência do cotidiano é indispensável e insubstituível para garantir que o profissional do setor saiba lidar com as mais desafiadoras situações de crise. É só após anos combatendo ameaças em seu dia a dia, elaborando planos de ação e forçando seu intelecto para resolver problemas complexos que um especialista se tornará, de fato, conhecedor o suficiente para garantir a segurança de sistemas da informação computadorizados. E, é claro, mesmo assim, precisará de atualizações constantes de conhecimento!

Porém, tal como fizemos nas duas últimas edições do CyberTech Report, vamos pensar no apagão de talentos em cibersegurança enfrentado pelo Brasil e pelo resto do mundo. Vimos, ao longo dos relatórios anteriores, uma série de iniciativas inovadoras — em nosso país e a nível internacional — que visam preparar novos profissionais para esse mercado cada vez mais crucial. Isso inclui cursos acadêmicos tradicionais (graduações), plataformas educacionais 100% online, laboratórios virtuais para aprendizagem mão-na-massa e ações que visam democratizar a entrada de minorias no mercado de trabalho — incluindo mulheres, afrodescendentes, a comunidade LGBTQIA+ e pessoas com deficiências.

Dessa forma, estamos caminhando para um futuro com equipes de segurança mais diversas e capazes de unir seus diferentes backgrounds culturais para contra atacar o crime cibernético.

Há, porém, um pequeno detalhe: voltamos ao início de nossa linha de pensamento sobre a prática levar à perfeição. É crucial que todos esses novos talentos estejam preparados para lidar com situações cotidianas para que estejam preparados para lidar com cenários de alto risco, e, para isso, nada melhor do que usar plataformas e soluções de simulação de ataques em ambientes realistas.

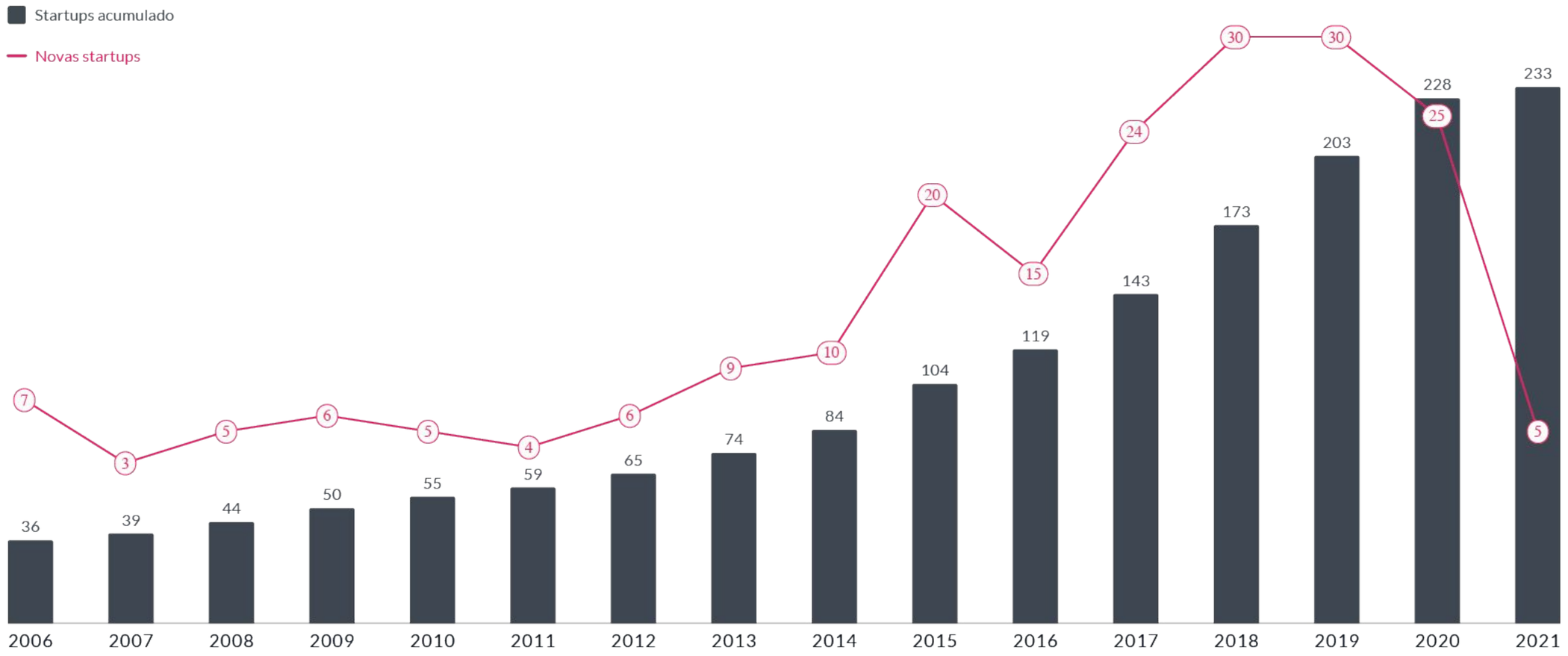
Usadas não apenas por iniciantes, mas também por profissionais experientes para garantir uma capacitação continuada, essas simulações emulam cenários de ataques e invasões cibernéticas com o máximo de fidelidade possível, reproduzindo técnicas, táticas e procedimentos (TTP) utilizados por atores maliciosos no mundo real. No mercado estrangeiro, há um segmento inteiro dedicado para tais plataformas, conhecido como “cyber range”.

Neste relatório, vamos analisar o que há de state-of-art em plataformas, frameworks e soluções — a nível nacional e internacional — para que os profissionais do setor calibrem suas habilidades.

Boa leitura!

Ecossistemas Cybertech

Evolução Cybertechs



Highlights

233
Startups

12
Categorias

9.000
Funcionários empregados

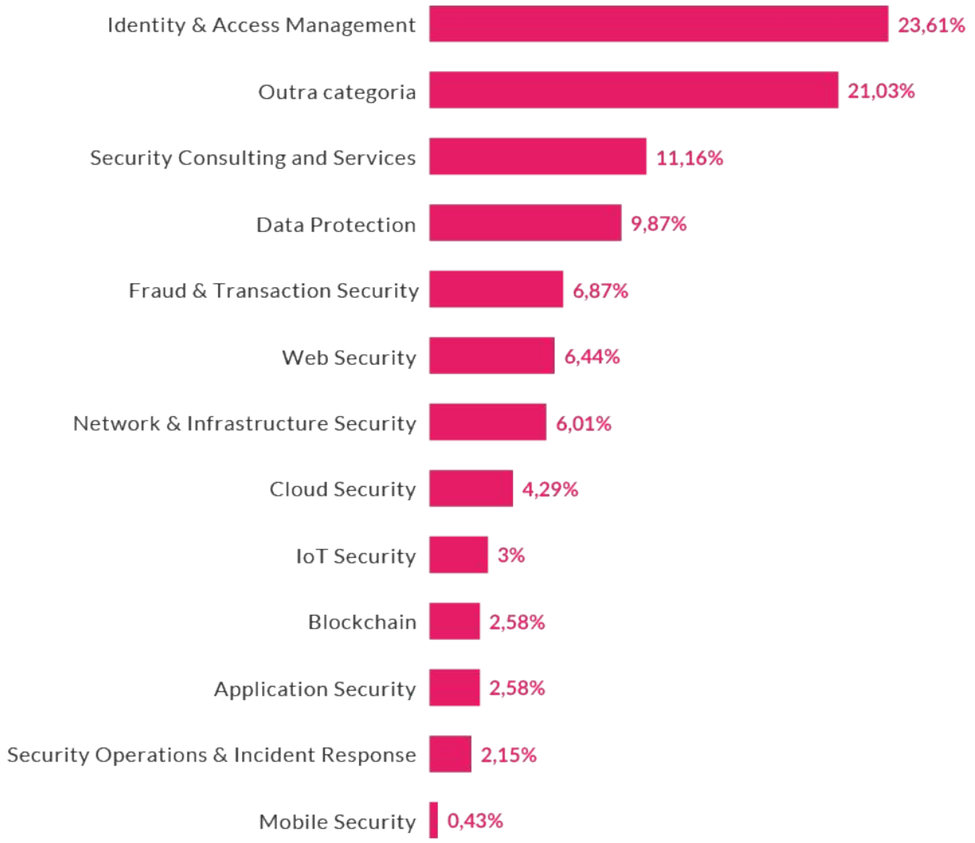
75
Startups com investimento recebido

US$ 412,5M
Investimento recebido desde 2013

US$ 294M
Investimento recebido nos últimos 2 anos

15
M&A's desde 2012

Divisão Cybertechs por categoria



RADAR: CYBERTECHS

DISTRITO

Data protection

36ZERO · a2f · ADDERE SOLUTIONS · beAnalytic · CLAVIS · DADOS LEGAIS · dogma · ethquo · GLOBAL DATA BANK · guardSI · Intelivix · IT2SGROUP · leadcomm · LOGS360 · MODULO · NETTIME · sentnella · PHISHX · Privacy tools · PRIVALLY · riskex · SAFE WAY · senhasegura · SENSR. · Simply. · ST3TAILOR · FlashSafe

Cloud Security

ADTsys · BrasilCloud · DDMX · nuvic · RedeHost · CleanCloud

Mobile Security

BluePex

Security Consulting and Services

SOTO · CECyber · Collision · CROMISOFT · Deep.bbl · DESEC · ESTUARIO · HACK3R_RANGERS · IBLISS · iCybersec · INFOSAFE · INtroduce · SOLVIMM · nova8 · OPTRA SECURITY · REDBELT · RUSTCON · STRONG SECURITY · TEMPEST · Unbroken Cyber Security

Fraud & Transaction Security

B2e Group · bigdatacorp. · BrScan · CQuantt · EXATO DIGITAL BETA · ZAIG · infodatos · konduto · legiti · MOST · Neoway · VIVALISTO · NeuroBanco · NEXTCODE · TRANSFERO SWISS AG

Network, Infrastructure Security

CONNECT · ISM · lumiun CLOUD MANAGED NETWORK · munio SECURITY · oktopus · ProFUSION embedded systems · StartLink · TI Safe · Virti · WEDOIT Working Together · Ztec

Security Operations & Incident Response

AXUR · gocache next-gen CDN

RADAR: CYBERTECHS

DISTRITO

Identity & Access Management

acert · AIKNOW · akiyama · Assine Online · autentique · AutoSeg · BeCloudx · BRy Tecnologia · CH tecnologia · Formalizar e-signature · FULLFace A sua segurança é você · griaule big data biometrics · GrupoCloud · GRYFO · HDDBOX · contract · ID ESSENTIALS · idwall · MEERKAT · NATOSAFE · nexti · nTokens · DITI · payface · qriar · QualiSign · PONT marcação móvel · unike · UNISEC Segurança, tecnologia e conforto · VSOFT · welcome · COMBATE A FRAUDE · contraktor · CRED DEFENSE · D4S · FIVE VALIDATION · mavie · INOVACODE · JURIDOC · Let's Work · .ai · SHIELDER · SimpleID IDENTIDADE CONFIRMADA! · SVATECH smart video analytics · T-SHIELD · UNICO

IoT Security

GAVB · LATOS · Ochain · TrackerThings · POLSEC · PREVISIOWN · ROBBIOT

Governance, Risk and Compliance

GAT InfoSec · NeuralMind · certo · REFINARIA DE DADOS

Application Security

Berghem Smart Information Security · CONVISO · BugHunt

Blockchain

2LEDGER · c4 4D4 .4 · amachains · bitshopp · BLOCKc · BlockNobre · BLOCO1 · bom valor · MARKETPLACE · COSMOS · CRIPTONOMIA · EOSRIO · Go Blockchain · GoBlock · growthTech · InspireIP · ORIGINALMY BLOCKCHAIN · QUAN · rhizom · safe TRACE · health · GoLedger · HubChain

Web Security

apura · AuditSafe · CromiWAF cyber defense · ERRORSEC · <u> · XLabs | ON SECURITY · SITE BLINDADO · Gatefy · UPX TECHNOLOGIES · XLabs · MBSEC

Simulação de Ataques em Cenários Realistas

Contexto e Panorama Nacional

Cyber Range: um “campo de tiro” para armas cibernéticas

Ao ler a introdução deste relatório e se deparar com as palavras “simulação de ataques cibernéticos”, caso seja uma pessoa acostumada com conceitos de cibersegurança, é natural que você tenha se lembrado das práticas de red team ou pentesting. Na primeira, uma equipe interna ou terceirizada tenta invadir constantemente os sistemas computadorizados da companhia em busca de eventuais brechas que possam ser exploradas pelos criminosos, utilizando todos os TTPs catalogados através de frameworks como o ATT&CK, da The MITRE Corporation. O pentesting é similar, sendo uma varredura pontual que também copia as técnicas adotadas por atores maliciosos.

Tais conceitos, porém, são bem diferentes das simulações de ataque em ambientes realistas. Estes ganharam, no mercado internacional, o nome popular de cyber range, em alusão ao termo shooting range — ou campo de tiro, em português, aquele ambiente controlado e seguro no qual atiradores desportivos podem reproduzir operações militares usando armas de fogo.

O cyber range (ou “campo cibernético”) é similar. Trata-se de um cenário configurado especialmente para simular, da maneira mais fiel possível, um ambiente corporativo que está sob ataque de criminosos cibernéticos ou até mesmo sendo alvo de um episódio de guerra cibernética. Dessa forma, seus participantes conseguem testar suas habilidades de reação de maneira altamente realista em comparação com uma situação de crise no mundo real.

O site Cybersecurity Guide possui uma descrição bastante acertada e completa a respeito de plataformas de cyber range:

Um campo cibernético é um ambiente tecnológico controlado e interativo no qual os profissionais de segurança cibernética em ascensão podem aprender como detectar e mitigar ataques cibernéticos usando o mesmo tipo de equipamento que terão no trabalho.

A gama simula os piores ataques possíveis à infraestrutura de TI, redes, plataformas de software e aplicativos. A configuração engloba tecnologias capazes de operacionalizar e monitorar o progresso e o desempenho de um trainee à medida que ele cresce e aprende por meio de experiências simuladas. Se utilizado da maneira correta, um campo cibernético pode incutir confiança nos profissionais de segurança cibernética.

Isto posto, um cyber range possui dois usos principais: a capacitação de profissionais dentro de empresas privadas e o treinamento continuado de forças militares cibernéticas. Estes precisam estar sempre a postos para um eventual conflito com outra nação no âmbito digital, já que podem causar disrupções em infraestruturas críticas como sistemas de distribuição de energia elétrica, telecomunicações e afins.

ECG 3.0: o maior exercício cibernético militar do hemisfério sul é do Brasil!

Como dissemos, simulações realistas de crises cibernéticas são importantes não apenas para empresas privadas, mas também para forças militares que precisam defender uma nação no caso de uma ciberguerra. Isto posto, o Brasil promove anualmente, desde 2018, o Exercício Guardião Cibernético, que utiliza soluções de ponta para criar os cenários de ataque e defesa mais fidedignos que for possível. Ele é organizado pelo Comando de Defesa Cibernética (ComDCiber), organização militar subordinada ao Exército Brasileiro.

Após uma pausa em 2020 por conta da pandemia do novo coronavírus (SARS-CoV2), o ComDCiber realizou, em 2021, o Exercício Guardião Cibernético 3.0 ou simplesmente ECG 3.0, que foi considerado o maior exercício cibernético militar do hemisfério sul. O evento foi realizado em parceria com a Cisco, com o Serviço Nacional de Aprendizagem Industrial (SENAI) e com a RustCon, empresa nacional pioneira no desenvolvimento da plataforma de cyber range Simulador Nacional de Operações Cibernéticas (SIMOC).

Entre os dias 5 e 7 de outubro, foram reunidos 350 participantes das três Forças Armadas (Exército Brasileiro, Marinha do Brasil e Força Aérea Brasileira) e de 70 empresas de diversos setores considerados críticos para a correta manutenção da sociedade, como nuclear, financeiro, telecomunicações, transportes etc. A ação ocorreu simultaneamente na base do ComDCiber, localizada no Forte Marechal Rondon (em Brasília), e na sede do Comando Militar do Sudeste (em São Paulo).

A dinâmica foi relativamente simples: os participantes tinham a missão de proteger o país fictício Azul, que estava em plena guerra cibernética contra o país Cinza. Além das simulações de ataque em si, chama atenção o fato de que o exercício forçou as entidades a lidar com situações de crise criadas por um comitê de cada setor, incluindo notícias de caos que abalavam a população e alertas de hostilidade.

Após o dia 7, foi realizado ainda a Análise Pós-Ação (APA), na qual cada entidade elaborou relatórios analisando resultados de pontos fortes e fracos. No momento em que este relatório foi escrito, o ComDCiber já havia aberto o chamamento público para o ECG 4.0, a ser realizado entre os dias 16 e 19 de agosto de 2022.

Defendendo a infraestrutura cibernética digital

Nelson Brito
Security Technical Solutions Architect
Cisco

A Cisco, junto com o SENAI e com a RustCon, foi uma peça central fundamental para o Exercício Guardião Cibernético 3.0 (ECG 3.0). Institucionalmente falando, o que levou a companhia a participar dessa simulação tão importante e de quais outras formas a Cisco se posiciona como player disposta a auxiliar no desenvolvimento das capacidades de respostas a incidentes junto ao Governo Federal?
A Cisco, através de iniciativas próprias, vem apoiando uma transformação digital, não somente sobre questões de segurança cibernética, mas também através do seu programa chamado "Brasil Digital e Inclusivo". Desta forma, logicamente, faz todo o sentido apoiar a iniciativa EGC 3.0, uma vez que há muito capital intelectual que pode, e deve, ser compartilhado com órgãos federais.

Esta iniciativa, apoiar o EGC 3.0, demonstrou a habilidade em coordenar, juntamente com o SENAI e a RustCon, estratégias de segurança cibernética, auxiliando não somente com soluções, mas colocando em prática toda a experiência na criação de ambientes reais e instrumentalização das equipes que participaram.

Responder a incidentes vem se tornando, com o passar do tempo, uma tarefa estratégica em diversos setores da economia, principalmente com o grande movimento de digitalização dos negócios, imposto indiretamente pela pandemia. E, para atender aos desafios desta nova realidade, a Cisco tem se posicionado tanto em eventos públicos, como no caso do EGC 3.0, quanto em situações que requerem maior sigilo.

Sabemos que tais exercícios são altamente importantes para capacitar as forças nacionais de defesa cibernética (no caso, a COMDCIBER) a estarem aptas a lidar com eventuais ataques cibernéticos contra infraestruturas críticas do país. Como a Cisco avalia o nível de realismo do ECG 3.0 em comparação com outros exercícios de simulação que existem ao redor do mundo?
O EGC 3.0, assim como as edições anteriores, tornou-se o maior exercício do hemisfério sul, e isso pode ser visto, na prática, com a edição de 2021. Os cenários são ultra realísticos, contato com maquetes para simulações de infraestruturas críticas, assim como o enredo criado possibilita uma contextualização →

→ das ações de ataque e defesa. Tudo isso muito bem coordenado pelo ComDCiber.

De que forma, de maneira prática, a Cisco apoiou o ECG 3.0? Quais tecnologias proprietárias da companhia foram empregadas no cenário de simulação e como isso fez diferença para torná-lo mais eficaz?
Foram centenas de horas investidas em toda a preparação e coordenação das ações para disponibilizar um ambiente de simulação. Dentre estas horas, não somente uma arquitetura foi desenhada e implementada, mas, também, horas de definição de cenários, elaboração de treinamentos (workshops), configurações, ajustes e validação.

Dentre as soluções utilizadas, buscando instrumentalizar as equipes dos setores envolvidos com o EGC 3.0, podemos listar:

- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco AnyConnect com Cisco Duo (MFA)
- Cisco Secure Firewall
- Cisco Secure Network Analytics
- Cisco Umbrella
- Cisco SecureX

Todos foram implementados nos ambientes de simulação, assim como foram realizados os treinamentos (workshops) para todos os participantes.

No cenário de uma guerra cibernética, diferente do que ocorre em uma guerra física tradicional, todos os setores da sociedade possuem um papel crucial para impedir maiores danos à infraestrutura nacional. Isso significa que empresas estatais e privadas também têm que cumprir seu dever de casa para que o cidadão comum esteja em segurança. Como essas simulações podem atingir esses outros setores e serem úteis para, por exemplo, uma empresa privada?
Quando levamos em consideração cenários de guerra cibernética, com no EGC 3.0, todos são relevantes, uma vez que a nação é definida pelas empresas que atuam no território nacional. Um exemplo:

- Um país inimigo (chamaremos de País X) decide iniciar uma campanha de ataques contra outro país (chamaremos de País Y);
- Os alvos estratégicos, neste cenário fictício, são: abastecimento de água e energia;
- Independentemente de serem do setor privado ou público, todas as empresas do País Y, responsáveis pelo abastecimento de água e energia, serão alvo desta campanha de ataques.

Então é necessário que estas empresas estejam preparadas para ações hostis do País X e, consequentemente, consigam coordenar, através de comunicação direta com as forças de defesa, as ações necessárias.

Como é possível ver, através do exemplo, é necessário que todos estejam alinhados com Política Nacional de Defesa, a Estratégia Nacional de Defesa e a Estratégia Nacional de Segurança Cibernética, independentemente de serem empresas privadas ou públicas. →

Defendendo a infraestrutura cibernética digital

Nelson Brito
Security Technical Solutions Architect
Cisco

→ Um bom exemplo disso foram as empresas que participaram ativamente do EGC 3.0, de diferentes setores, tais como: Águas, Defesa, Elétrico, Financeiro, Telecom e Transporte.

Embora naturalmente envolva empresas privadas no processo, o Exercício Guardião Cibernético (ECG) tem claro foco em garantir um treinamento anualmente atualizado para as Forças Armadas do Brasil. Ainda é difícil, em nosso país, encontrar fornecedores que disponibilizem ferramentas de livre uso para uma simulação realista de um ataque cibernético patrocinado por uma nação estrangeira. Como você enxerga essa questão?
Nas palavras do Coronel de Artilharia Luiz Cláudio de Souza Cunha, subchefe do Estado-Maior Conjunto do Comando de Defesa Cibernética e coordenador Executivo do Exercício Guardião Cibernético (EGC) 3.0: "O EGC é uma atividade de alto nível equiparada aos principais exercícios internacionais, como por exemplo o Locked Shields (OTAN) e Ciber Perseu (Portugal). [...] Está alinhado com a Política Nacional de Defesa, a Estratégia Nacional de Defesa e a Estratégia Nacional de Segurança Cibernética. O EGC é baseado no incentivo à atuação colaborativa envolvendo Governo Federal, Ministério da Defesa, comunidade acadêmica, agências ligadas ao setor cibernético, nações amigas, organismos internacionais e IC das seguintes áreas prioritárias: água, energia, comunicações, financeiro, transporte e nuclear."

Fica claro que o EGC não se limita ao treinamento das Forças Armadas do Brasil, mas sim de todos os setores participantes, buscando ações coordenadas. Em resumo, grandes empresas enviam profissionais para participarem ativamente no EGC, permitindo corroborar a colaboração entre os setores.

Em meio a este ambiente, a Cisco, assim como quaisquer outras empresas, sejam elas nacionais ou estrangeiras, podem e devem apoiar estas iniciativas, seja através de instrumentalização das equipes, seja através de compartilhamento de experiência e capital intelectual.

Defendendo a infraestrutura cibernética digital

Nelson Brito
Security Technical Solutions Architect
Cisco

Nome: RustCon

Público: B2B

Sobre

Desenvolvedora da única solução 100% nacional de cyber range, a RustCon é uma empresa brasileira fundada em 2013 justamente para ser uma parceira certificada do Ministério da Defesa. Para isso, ela criou o SIMOC, simulador ultra realista que possibilidade a criação de réplicas fiéis de infraestruturas para emular vulnerabilidades e ataques cibernéticos. A ferramenta já era usado pelo Exército Brasileiro desde a sua criação em 2013, mesmo antes do estabelecimento do Exercício Guardião Cibernético.

Seu diferencial é a facilidade de uso. É possível instalá-la em qualquer máquina-cliente (ou até mesmo disponibilizá-la de forma remota como aplicação em nuvem) e configurar a simulação de acordo com a necessidade, definindo objetivos, desafios e regras. O progresso dos exercícios pode ser monitorado em tempo real, com análise e classificação dos participantes. Há ainda um módulo de experimentação que conta com uma sandbox para análise segura de arquivos suspeitos, laboratório de malwares e orquestração de ferramentas de detecção de ataques.

Embora a RustCon tenha nascido especificamente para atender aos órgãos governamentais, a natural procura por plataformas de simulação hiper realista por parte de grandes corporações privadas incentivou a companhia a disponibilizar o SIMOC para um público mais amplo.

Hoje, qualquer empresa interessada em promover um exercício de forma privada — otimizando os conhecimentos de sua própria equipe e treinando seu time de segurança para incidentes graves — pode utilizar a plataforma da maneira que desejar.

Pioneirismo e qualidade a nível internacional

Carlos Rust
CEO e Presidente
RustCon

A RustCon é, até onde conseguimos levantar informações, a única empresa brasileira que atua no segmento de cyber range; isto é, simulações realistas e customizáveis de guerra cibernética e ciberataques. Como a companhia foi fundada e o que levou vocês a investirem especificamente neste setor, que infelizmente até os dias de hoje não é muito valorizado no Brasil?

Começamos a operar em 2010 com o objetivo de desenvolver uma tecnologia nacional para o segmento de Defesa. Participamos de diversos projetos, como o Sistema de Monitoramento de Fronteira, o Simulador de Comando e Controle, o Simulador de Combate e diversos outros. Um dos projetos foi o desenvolvimento de um Simulador de Ataque e Defesa Cibernética para ser usado pelo recém criado Centro de Defesa Cibernética (há 10 anos), com o objetivo de formação de competência em Defesa Cibernética. Em outras palavras, o simulador (que ganhou o nome SIMOC) foi criado para que o Brasil pudesse atuar na Defesa Cibernética, formar os guerreiros cibernéticos, desenvolver os processos e as doutrinas de ataque e defesa, entre outras atividades. Nessa época, as Forças armadas de diversos países, começavam a criar suas organizações de combate na dimensão cibernética... Uma dimensão de conflito que começava a ser quase tão importante quanto o ar, a água e a terra.

Não existia simuladores de ataque e defesa cibernética estrangeiros disponíveis para compra que também atendessem às nossas necessidades. Participamos de um edital de contratação dessa tecnologia, ganhamos e desenvolvemos um dos primeiros simuladores do mundo.

Não foi um desenvolvimento tranquilo; tivemos várias questões e dificuldades tecnológicas inerentes a um projeto de inovação, mas superamos todas elas. Implantamos a primeira versão em 2012 e estamos até hoje evoluindo esse produto que tem qualidade superior ou, no mínimo, comparável a seus concorrentes estrangeiros. Não existe um similar nacional.

Por outro lado, começamos a perceber que a mesma necessidade dos militares aprimorar conhecimento para se defender de ataques cibernéticos seria também percebida pela indústria e demais setores da sociedade civil. Nos Estados Unidos, por volta de 2015 e 2016, começavam a surgir os cyber ranges ou Centros de Competência em Segurança Cibernética. Nesse mesmo momento, começamos um trabalho de introduzir essa nova ferramenta nas empresas brasileiras.

No início, éramos bem recebidos a abordagem era bem aceita, mas as empresas não tinha a segurança cibernética nas suas lista de prioridades. →

→ Foram anos de muito investimento e de frustrações. Aprimoramos o produto para atender melhor a sociedade civil e suas características específicas.

Recentemente a sociedade e as empresas acordaram para o tema de cibersegurança. A digitalização segue em uma velocidade absurdamente alta. Até a pandemia da COVID-19 acelerou o movimento de home office e os criminosos aproveitaram esse momento. Em resumo, hoje não existe risco maior para qualquer organização diferente do risco de ataque cibernético. Não existe mais nenhum executivo que não tenha esse tema no topo da lista de suas prioridades.

Atualmente o maior gap que existe são profissionais de segurança cibernética adequadamente treinados, são executivos que sabem reagir corretamente no caso de um ataque cibernético e demais funcionários que se comportem adequadamente para evitar ataques e que também saibam reagir.

Em resumo hoje todo mundo precisa do que as Forças Armadas precisavam há 10 anos. Precisam treinar seus técnicos, executivos e funcionários. Precisam ter processos de segurança bem estabelecidos e divulgados. Precisam de um cyber range.

Atualmente, como é a estrutura da RustCon enquanto empresa, visto que é difícil encontrar tais informações de forma pública? Quantos funcionários possuem? Já receberam investimentos de fundos de capital ou similares?
Atualmente, a RUSTCON é um empresa brasileira, com tecnologia própria, classificada como pequena (igual a 95% das empresas brasileiras), saudável e com grande potencial de crescimento.

Temos aproximadamente 15 colaboradores, prestamos serviços para grandes organizações brasileiras e multinacionais. Não temos capital estrangeiro e nem de fundos de investimento.

A RustCon é uma empresa de um produto só: o SIMOC, plataforma de simulação realista que é usado pelas Forças Armadas do Brasil desde 2013 e, desde a criação do Exercício Guardião Cibernético (ECG), virou uma peça crucial para tal treinamento anual. Porém, a SIMOC é fornecida exclusivamente para uso militar ou empresas privadas também conseguem se beneficiar treinando seus times de segurança em cenários realistas?
Como dito anteriormente, desenvolvemos uma versão do SIMOC mais adequada para uso civil que já é utilizada por grandes organizações (indústria, bancos, serviços, energia) e continuamos atualizando e mantendo a versão que é utilizada pelas Forças Armadas.

Foi recentemente utilizado no Guardião Cibernético 3.0 que contemplou os segmentos de Telecomunicações, Energia Elétrica, Energia Nuclear, Transporte, Água e Bancos.

Atualmente somos uma empresa de segurança cibernética com um produto e tecnologia própria como diferencial. →

Pioneirismo e qualidade a nível internacional

Carlos Rust
CEO e Presidente
RustCon

→ Como citado anteriormente, a área de cyber range é desconhecida no Brasil; lá fora, existem diversos players oriundos dos mais variados países ao redor do globo (sendo que alguns possuem presença indireta por aqui através de revendedores). Estrategicamente falando, como a RustCon enxerga esse mercado em nosso país e quão desafiador é atuar nele de forma, digamos, monopolista (mesmo sem querer)?
Não podemos afirmar mais que a área de cyber range é desconhecida no Brasil. A necessidade de formação de pessoas em cibersegurança é tão alta por aqui quanto em outros países. A diferença é que começamos a desenvolver tecnologia brasileira ao mesmo tempo que os outros países, diferente do que aconteceu em outras áreas da tecnologia.

Hoje temos um produto de alta qualidade tecnológica e de enorme importância para o mercado, o que nos orgulha muito. Essa área também é unanimemente reconhecida como muito crítica e é importante que o Brasil tenha alguma independência. Nosso produto é, definitivamente, competitivo mesmo em escala internacional.

O cyber range é importantíssimo na formação da pessoas e dos processos, e essas pessoas utilizam as tecnologias de informática e de proteção cibernética disponíveis no mercado. Não é automática a aplicação de um cyber range qualquer no mercado brasileiro. Estamos falando de pessoas e processos que, no Brasil, são bem peculiares. O SIMOC tem mais de 10 anos de vida no país, desenvolvido por técnicos locais.

Nossas dificuldades são as conhecidas por todos os empresários brasileiro: o famoso “custo Brasil”, dificuldade de crédito, dificuldade para internacionalização, incertezas etc.

Até o momento, superamos essas dificuldades. A empresa tem vida longa e temos muito orgulho de tudo que fizemos e dos empregos de alta qualidade que criamos. Temos muitos planos para o futuro.

Pioneirismo e qualidade a nível internacional

Carlos Rust
CEO e Presidente
RustCon

SENAI: educando novos talentos com simulações hiper realistas

Outra organização que está promovendo iniciativas inovadoras para capacitar profissionais na área de cibersegurança com habilidades de alto nível é o complexo educacional SENAI. Em 2020, a instituição lançou o curso “Simulação hiper-realista de Ataques Cibernéticos”, que é 100% à distância e aberto para qualquer estudante interessado em aprimorar as suas habilidades de defesa cibernética. Obviamente, embora seja um curso livre, estamos falando de uma formação de nível avançado; logo, é crucial que os alunos já possuam conhecimentos básicos da área.

O objetivo é que o aprendiz, ao final da grade, seja capaz de propor estratégias preventivas, reconhecer técnicas de ataque, estar habituado com metodologias e fundamentos de segurança em rede e até mesmo explorar vulnerabilidades de forma ofensiva utilizando metasploit. São, no total, 40 horas de estudo.

O simulador utilizado também é o SIMOC da RustCon, sendo que, ao longo do curso, são apresentados 20 cenários diferentes inspirados em casos reais. As simulações não se limitam a exercícios de defesa, mas também de ataque, permitindo que o profissional esteja apto a realizar também manobras de red team e/ou testes de intrusão dentro de companhias.

Embora seja online, o curso permite interações frequentes com docentes qualificados, que estão à disposição para instruir e tirar dúvidas dos alunos em relação aos materiais e exercícios de simulação.

Embora seja perfeitamente possível aproveitar o curso no conforto de sua casa, o SENAI inaugurou, também em 2020, cinco unidades de sua Academia SENAI de Segurança Cibernética. São espaços físicos através dos quais é possível aprender de forma presencial, além de servirem como palco para palestras e competições. As unidades estão localizadas nos estados do Ceará, Espírito Santo, Paraná, Rio Grande do Sul e Distrito Federal.

E, por falar em competições, a instituição de ensino promoveu, entre os dias 1º e 3 de junho de 2021, o Desafio Cyber Capture the Flag (CTF). Tais como outros desafios cibernéticos do tipo "capture a bandeira", os participantes foram divididos em dois times que concorreram entre si realizando manobras de defesa e de ataque através do SIMOC. O torneio também foi online, com uma taxa de inscrição no valor de R$ 100; os vencedores ganharam uma bolsa integral para o curso de simulação hiper-realista.

Por fim, vale a pena comentar também sobre o curso SENAI de Segurança Cibernética Aplicada à Indústria 4.0; este sim é autoinstrucional e com conteúdo mais acessível, abordando os principais riscos e cuidados a serem tomados para evitar vulnerabilidades no ambiente industrial.

Treinando hoje para ir à guerra amanhã

Felipe Morgado
Gerente Executivo de Educação Profissional e Tecnológica
SENAI

O curso "Simulação Hiper Realista de Ataques Cibernéticos" foi lançado pelo SENAI em agosto de 2020. O que motivou a instituição a elaborar tal curso? Desde a sua inauguração até o momento desta entrevista, saberia apontar quantos profissionais já foram certificados finalizando o curso com sucesso?
Em dezembro de 2020, foram inauguradas as Academias SENAI de Segurança Cibernética, localizadas em cinco pontos estratégicos no Brasil: em Brasília, Porto Alegre, Fortaleza, Londrina e Vitória. O diferencial das Academias é fornecer acesso ao simulador hiper realista de ataques cibernéticos para a realização de cursos com o acompanhamento de especialistas do SENAI com formação e experiência em cibersegurança.

No final de 2020, começou a oferta do "Curso Prático de Simulação Hiper-realista de Ataques Cibernéticos", que é uma imersão de 40 horas no ambiente digital do simulador, com a realização de desafios estruturados para os alunos praticarem procedimentos de diferentes níveis de complexidade visando detectar ataque, bloquear ataque, defender rede e web e identificar vulnerabilidades.

Durante o curso, os profissionais também têm a oportunidade de colocar em prática as ações dos criminosos cibernéticos que usualmente são conhecidas na teoria, como burlar proteções, atacar redes e vazar informações.

Até o início de 2022, mais de 250 alunos participarem do curso. Foram turmas fechadas para empresas e organizações que buscam o curso prático para elevar a qualificação de seu time de defesa e turmas abertas para profissionais de TI que estão no mercado de trabalho buscando o autodesenvolvimento para ingressar em novas oportunidades.

Muito se discute sobre o déficit de talentos em cibersegurança, questão que também afeta o Brasil. Existe um agravante que é o fato de que muitos profissionais iniciantes não possuem conhecimento prático para lidar com incidentes no mundo real. O curso do SENAI é capaz de suprir esse gap no mercado?
A formação que o SENAI oferece em diversas áreas tecnológicas destaca as competências práticas para o exercício profissional. No caso da cibersegurança não é diferente e o simulador hiper realista é realmente uma ferramenta muito adequada para os alunos praticarem os seus conhecimentos. →

→ Estamos ampliando o portfólio de cursos práticos que são realizados no simulador hiper realista. Além do curso prático de simulação de ataques cibernéticos, também estão em preparação o curso prático de testes de invasão em aplicações web e o curso prático de técnicas de computação forense.

Outras ações realizadas com o simulador hiper realista ampliam o número de profissionais que se aprimoram por meio da vivência prática de eventos de defesa cibernética.

Alguns exemplos são os jogos do tipo capture the flag (CTF), os exercícios práticos com grande número de participantes — como o Guardião Cibernético promovido pelo Comando de Defesa Cibernética do Brasil — e as demonstrações de ataque e defesa, como será feito no estande do SENAI no 9º Congresso Brasileiro de Inovação para Indústria, que será promovido pela Confederação Nacional da Indústria (CNI) em março.

Experiências práticas em simuladores variados são muito importantes para ampliar o número de profissionais bem preparados para a segurança cibernética das empresas.

Globalmente falando, temos um segmento inteiro de startups, plataformas e soluções que simulam cenários de riscos cibernéticos com perfeição; segmento este conhecido como "cyber range". Quais características do curso Simulação Hiper Realista de Ataques Cibernéticos fazem com que ele possa ser considerado, de fato, hiper realista?
Uma plataforma de cyber range fornece um ambiente virtual multifuncional no qual as organizações podem testar recursos essenciais e revelar a eficácia com que integram pessoas, processos e tecnologia para proteger suas informações, serviços e ativos estratégicos.

O simulador utilizado pelo SENAI é um laboratório totalmente digital, hospedado em nuvem e que, por isso, pode ser acessado por alunos e instrutores de qualquer localidade.

A característica de hiper realismo é consequência da composição por ativos reais (roteadores, servidores, estações de trabalho, firewall, etc.), softwares de negócios e de defesa cibernética. Nesse ambiente, os alunos executam ações de ataque cibernético que efetivamente alteram o funcionamento dos elementos instalados no ambiente do simulador. Da mesma forma, os alunos são orientados para executar ações que restabelecem o funcionamento dos ativos, identificam a origem e impedindo o prosseguimento do ataque.

Por se tratar de um complexo integrado de ativos reais, não há uma única solução para o problema. O que ocorre é a orientação dos alunos para executarem os procedimentos mais eficientes e mais rápidos. Na interface gráfica do simulador, os instrutores acompanham todo o processo e podem criar, modificar, apagar e resetar ambientes complexos com muita velocidade, permitindo que os exercícios sejam realizados e replicados quantas vezes forem necessários para o aprendizado. →

Treinando hoje para ir à guerra amanhã

Felipe Morgado
Gerente Executivo de Educação Profissional e Tecnológica
SENAI

→ Todo o conteúdo do curso é oferecido na modalidade à distância (EAD). Isso certamente facilita os estudos e torna o curso mais acessível, mas pode tornar os exercícios de simulação menos eficientes do que aqueles efetuados presencialmente. Há planos para uma modalidade presencial?
A oferta do curso presencial já é possível nas Academias SENAI de Segurança Cibernéticas que estão localizadas nas cidades de Brasília, Porto Alegre, Fortaleza, Londrina e Vitória, em laboratórios especializados.

No período de restrição de cursos presenciais devido à pandemia, foi disponibilizado acesso para os alunos utilizarem a integralidade dos recursos do simulador por meio de internet segura.

Da mesma forma, durante o exercício Guardião Cibernético, os profissionais de mais de 50 empresas estavam localizados remotamente e realizaram todos os procedimentos de defesa cibernética em cenários virtuais instalados no mesmo simulador utilizado pelo SENAI em seus cursos práticos.

Não há diferença entre acessar o simulador a partir das Academias ou a partir da residência ou empresa na qual os alunos estão, bastando seguir as configurações de computadores e de acesso seguro à internet. Quanto à interação, também é possível realizar todo acompanhamento das atividades dos alunos e fornecer feedback imediato por meio de aplicativos de webconferência.

Além deste novo curso, de quais formas o SENAI está fomentando o mercado de cibersegurança e a formação de novos talentos da área no Brasil?
Há duas novas soluções lançadas pelo SENAI nesse início de 2022 para intensificar a qualidade da formação de profissionais de cibersegurança. Uma delas é a formação do Encarregado de Proteção de Dados, profissional requisitado pelas empresas para atender às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD).

Esse profissional também é conhecido como DPO — Data Protection Officer. O escopo da ação desse profissional ganhou mais visibilidade a partir da inclusão recente, na Constituição Brasileira, da proteção de dados pessoais como direito fundamental.

A outra solução é a formação do Information Security Officer (ISO). No mercado de trabalho, essa formação habilita os profissionais de TI para atuarem como analistas e gestores de segurança cibernética, a depender do porte das empresas.

Nos próximos dias, o SENAI vai realizar a live sobre “Escola segura, Indústria segura”. Um dos especialistas convidado vai esclarecer para o público a importância desses dois profissionais para a segurança cibernética das empresas brasileiras.

Para a formação desses profissionais, o SENAI criou trilhas com cursos online com conteúdo atualizado, vídeos, exercícios e testes simulados de preparação para as provas de certificação internacional. A certificadora EXIN é parceira do SENAI no Brasil e o voucher para realização das provas é disponibilizado para os alunos que se matriculam nos cursos oferecidos pelo SENAI.

Treinando hoje para ir à guerra amanhã

Felipe Morgado
Gerente Executivo de Educação Profissional e Tecnológica
SENAI

No estrangeiro, crescem os investimentos

Panorama Internacional

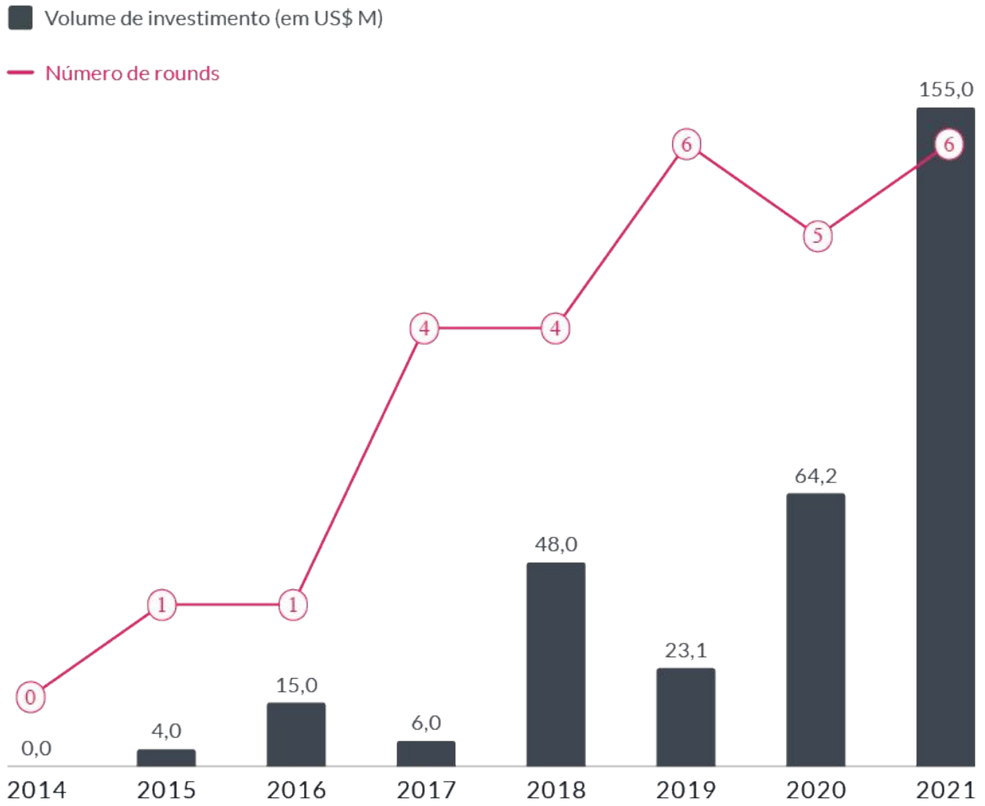
Investimentos em cyber range vêm crescendo exponencialmente a cada ano

Os números globais levantados pelo Distrito não deixam que Carlos Rust, anteriormente entrevistado neste mesmo relatório, conte mentiras. Até 2014, aparentemente, não havia qualquer preocupação global com ferramentas de simulação realista de ataques cibernéticos.

Tal como o fundador da RustCon afirmou, os investimentos começam a surgir — ainda tímidos — entre 2015 e 2016. Após uma leve queda em 2017, os aportes e números de rodadas em startups do setor vêm aumentando exponencialmente ao longo dos últimos anos. Só em 2021, tivemos um total de seis rodadas que levantaram um total de US$ 155 milhões em plataformas do gênero.

Vale lembrar que, no momento em que este relatório é escrito, estamos em fevereiro de 2022 e já contamos com uma rodada de US$ 5,66 milhões — mais do que o dinheiro movimentado em 2015. Podemos encarar isto como um sinal de que este ano também será promissor para as soluções de cyber range.

Valores investidos e números de rodadas em startups de cyber range



Startups têm pouco aporte em estágios iniciais

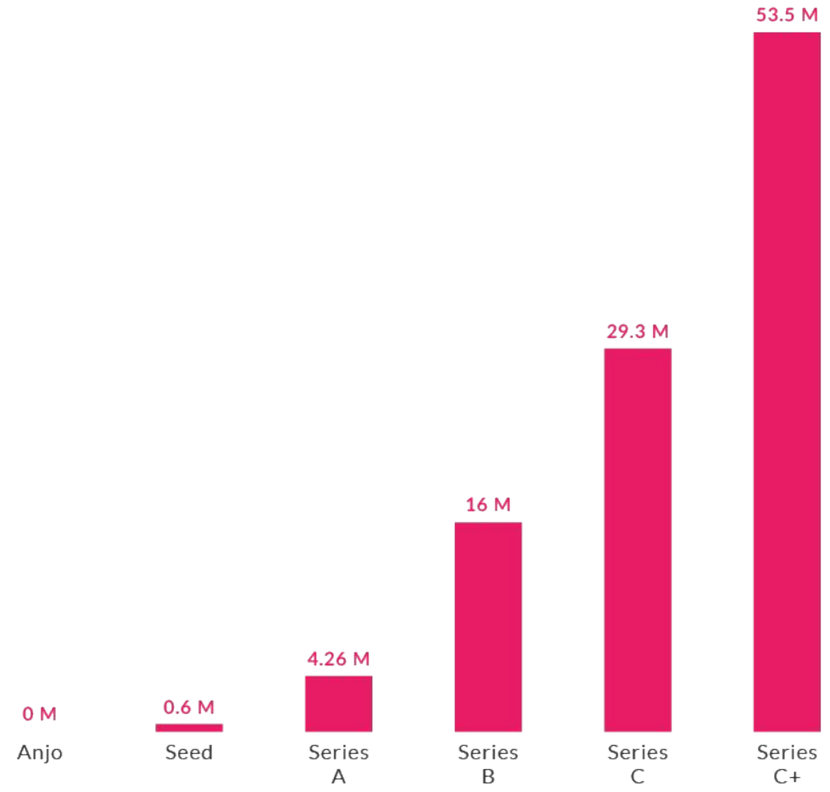
Embora o crescimento no número e volume de investimentos em startups de cyber range seja animador, é crucial observarmos uma particularidade desse mercado: as companhias recebem pouquíssimo aporte em seus estágios iniciais (anjo, pré-seed e seed).

Isso pode explicar o porquê de termos tão poucas opções no mercado — os fundos de investimento apenas aplicam dinheiro em negócios estabelecidos, capazes de demonstrar um crescimento estável e um faturamento interessante.

Apenas para fins de curiosidade, no intervalo de 2013 a 2021, não foi registrado nenhum investimento anjo e apenas US$ 600 mil em rodadas seed. Até mesmo em Series A, o volume é baixo: US$ 4,26 milhões registrados de forma "picada" ao longo de sete longos anos.

A maior parte dos aportes fica mesmo para rodadas Series C+, que representam US$ 53,5 milhões em apenas um ano (2020).

Valores investidos de acordo com o estágio das rodadas



Exercícios militares cibernéticos ao redor do mundo

Engana-se quem pensa que o Brasil é o único país a contar com um exercício militar de defesa cibernética apoiado em simuladores realistas. Diversos outros países, organizações e associações mantêm programas similares. Confira alguns destaques que selecionamos:

- **Cyber Defense Exercise (CDX):** embora sua última edição com este nome tenha ocorrido em 2017, o CDX merece figurar nesta lista por ser um dos primeiros exercícios anuais do mundo — ele foi organizado pela primeira vez em 2001. Era mantido pela Agência de Segurança Nacional dos Estados Unidos (National Security Agency ou NSA) e convocava os cadetes de todos os colégios militares do país para um treino em simulador próprio. A maioria das edições foram vencidas pela Academia Militar dos Estados Unidos de West Point, mas, na última delas, em 2017, a Academia Naval dos Estados Unidos de Annapolis ficou no topo do pódio;
- **NSA Cyber Exercise (NCX):** a partir de 2018, o CDX foi reformulado e rebatizado como NCX. O público, porém, continua o mesmo — estudantes de academias militares ao redor do país. O objetivo, segundo a agência, é "ajudar a educar, treinar e testar as habilidades cibernéticas dos cadetes do serviço acadêmico dos EUA [...] para que se tornem futuros guerreiros e líderes cibernéticos". Após uma edição cancelada em 2020 por conta da COVID-19, o treino de 2021 foi vencido mais uma vez pela Academia Naval dos Estados Unidos de Annapolis.
- **NATO Cyber Coalition:** mantido desde 2008 pela Organização do Tratado do Atlântico Norte (OTAN/NATO), o Cyber Coalition também é anual e reúne membros da aliança (tal como parceiros) com o objetivo de aumentar as suas habilidades de defesa e de contra-ataque no que tange às ameaças no espaço cibernético. Sua mais recente edição (2021) ocorreu no Centro de Exercícios e Treinos de Segurança Cibernética da Estônia, popularmente conhecido simplesmente como CR14, embora algumas nações também participado remotamente. No total, mais de mil militares marcaram presença no evento, que incluiu simulações realistas de ataques a dutos de gás, quartéis militares, centros logísticos e um laboratório fictício que trabalhava na produção de vacinas imunizantes.
- **EDA Cyber Ranges Federation:** aqui, não estamos falando exatamente de um exercício repetido anualmente, mas sim de um programa mantido pela Agência Europeia de Defesa (European Defense Agency ou EDA) que busca usar ferramentas de cyber range de forma constante para otimizar as capacidades de defesa cibernética dos estados-membro da União Europeia. Sua mais recente ação, em fevereiro de 2021, reuniu os Grupo de Resposta a Incidentes de Segurança (Computer Security Incident Response Team ou CSIRT) de 18 país, totalizando 200 profissionais participantes, e contou com a supervisão do ministro da Defesa da Estônia.

Uma parceria que deu certo

Genivaldo Araújo
CEO
3CON

A 3CON é a mais respeitada revendedora da Cymulate no Brasil; que, por sua vez, é a segunda startup de cyber range (simulação realista de ciberataques) mais bem-sucedida do mundo, tendo recebido US$ 71 milhões em investimento. Como se deu a origem da parceria para trazer essa solução para o nosso país?
A 3CON tem um histórico de parcerias com empresas israelenses desde 2014, porque o país é um produtor indiscutível de alta tecnologia. Por outro lado, definimos a área de cibersegurança como prioritária e passamos a construir um portfólio completo para atender ao mercado brasileiro.

Inclusive, um dos nossos objetivos era trazer uma solução de Breach and Attack Simulation (BAS) para o Brasil. Então, foi até natural, quando nossa área de P&D/Inovação passou a buscar as melhores soluções e encontrou produtos muito interessantes. O Cymulate foi um deles.

Vocês certamente tiveram contato e/ou estudaram outras plataformas de cyber range que oferecem simulações de ciberataques além da Cymulate. Quais pontos da solução você apontaria como diferenciais e como ela se sobressai em comparação com competidores do mercado?
Entre os principais diferenciais, destacamos os relatórios gerados automaticamente. O Cymulate produz dois tipos: um técnico e um executivo. O técnico é bem completo e aponta, por exemplo, falhas de configuração no firewall, no sistema operacional, entre outros, e mostra como resolvê-las. Já o relatório executivo é de fácil compreensão para quem não é da área de TI.

Outra vantagem revela-se na hora da implementação: ela é extremamente fácil. Basta fazer o download de um agente, instalar na máquina que queremos testar e pronto. Algumas soluções concorrentes exigem a compra de equipamentos, criação de VPN, instalação de agentes em cada endpoint e outras dificuldades.→

→ Também destacamos o Immediate Threat, um recurso que deixa as empresas sempre atualizadas sobre os mais recentes ataques ao redor do mundo. O Cymulate Research Lab monitora e identifica ameaças assim que são disseminadas, e dispara e-mails diários com informações importantes e dicas de correção para todos seus usuários.

Vale citar ainda uma característica que o coloca na vanguarda tecnológica: todos os vetores do Cymulate são aderentes ao MITRE ATT&CK — Massachusetts Institute of Technology Research & Engineering Adversarial Tactics Techniques and Common Knowledge —, um framework que se tornou popular, pois é uma base de conhecimento globalmente acessível de táticas e técnicas adversárias baseadas em observações do mundo real.

O MITRE é também conhecido como Think Tank, e vai muito além da cibersegurança, com inovações nos campos de computação e na área militar.

Por fim, trata-se de um produto totalmente customizável, que possibilita integração amigável com SIEM e SOC.

Isso faz do Cymulate não só uma solução diferenciada de BAS, mas de validação contínua de postura de segurança com forte componente de gestão.

Na sua visão, qual é a importância de uma ferramenta de assessment e simulação de ataques cibernéticos para empresas e profissionais do setor? Esse tipo de plataforma pode ajudar na capacitação de talentos ao permitir que eles enfrentem situações de risco que imitam cenários reais?
Acreditamos que esse tipo de plataforma acaba ajudando a aperfeiçoar os times de segurança da informação. As brechas nas defesas surgem, normalmente, de controles mal configurados ou processos inadequados. Com esses problemas apontados e corrigidos, os CISOs e suas equipes terão muitas oportunidades de aprender o que fazer e o que não fazer. Mas, evidentemente, o propósito primordial de uma solução BAS não é treinar equipes.

Justamente por isso, estamos firmando parceria com uma empresa israelense de cybertraining. Ela possui sistemas para treinamento de red team e blue team, treinamento para conscientização de funcionários

por meio de games, além de uma solução completa para universidades, com cursos de dois a quatro anos de duração. Revolucionará os treinamentos de segurança, sem sombra de dúvida.

Uma das reações naturais de empresas com pouco conhecimento quando falamos sobre exercícios realistas de defesa é que tal investimento não seria necessário, uma vez que elas já possuem uma estratégia de red team e de blue team ou mesmo fazem pentest regularmente. Como você explicaria a diferença entre essas estratégias?
As soluções BAS não substituem o pentest ou vice-versa. Os testes de intrusão, podemos dizer, trazem uma fotografia da segurança em um →

Uma parceria que deu certo

Genivaldo Araújo
CEO
3CON

→ determinado momento. Os pentests também têm um escopo definido e, normalmente, são voltados para aplicações; além disso, são caros e demorados.

Já as soluções BAS possibilitam a simulação, avaliação e mitigação o tempo todo nas redes, endpoints, máquinas e nuvem de forma automática e contínua. As soluções BAS também podem ser aproveitadas como um kit de ferramentas para os blue e red teams. Assim, não existe, de fato, conflito entre essas estratégias, mas complementaridade.

O Brasil ainda é fraco como produtor de soluções que facilitem exercícios cibernéticos. Não existe, por aqui, um setor desenvolvido de cyber range como existe globalmente. Como você avalia a procura por esse tipo de plataforma pelas corporações brasileiras? Os clientes costumam ser de maior porte ou o público é variado?
As empresas brasileiras estão, neste momento, adquirindo maturidade em relação à adoção de soluções de simulação de ataques para avaliação de sua postura global de segurança. No Brasil, as soluções de Pentest, SOC e SIEM são mais disseminadas, mas a procura por soluções BAS está em expansão.

Nesse sentido, fornecedores como a 3CON e a própria Cymulate, é claro, têm uma grande missão no sentido de chamar a atenção e conscientizar o mercado. Evidentemente, temos mais respostas das médias e grandes empresas, até porque são as que mais têm a perder, seja em termos financeiros ou de reputação, o que é quase a mesma coisa.

Do nosso ponto de vista, o importante é que as empresas compreendam que a segurança da informação, atualmente, faz parte do valor do produto ou serviço que as corporações vendem. A maioria dos funcionários das empresas não têm ideia do prejuízo que pode causar por conta de um link que abriu ou ao compartilhar uma senha indevidamente.

Os elos fracos da cadeia de segurança continuarão existindo, por isso, os gestores precisam se antecipar e se prevenir. O BAS é parte fundamental de uma estratégia consistente de prevenção e mitigação de incidentes de segurança da informação.

Uma parceria que deu certo

Genivaldo Araújo
CEO
3CON

Cymulate

Local
Rishon Lezion, Israel

Ano de Fundação
2016

Público
B2B

Investimento Recebido
US$ 71 milhões

Investidores
Dell Technologies Capital, Vertex Ventures Israel, Susquehanna Growth Equity, One Peak Partners, Vertex Growth

Sobre

Embora se auto-intitule uma solução de Simulação de Ataque e Violação (Breach and Attack Simulation ou BAS), a Cymulate é, na verdade, nada mais do que uma plataforma de cyber range. Podemos considerá-la uma das mais bem-sucedidas a nível global, contando com toda a expertise reconhecida no mercado por especialistas de Israel.

Diferente da SIMOC (que já nasceu com foco em exercícios militares), a Cymulate oferece um produto 100% projetado para empresas privadas. Utilizando o framework MITRE ATT&CK, as corporações podem realizar assessments contínuos através de cenários simulados que validam defesas em email, web, firewall, endpoint etc. É possível reproduzir toda a cadeia de movimentos de atores maliciosos publicamente reconhecidos.

Tendo entre seus maiores investidores fundos de capital específicos de Israel, a startup já captou US$ 71 milhões em cinco rodadas de financiamento — sendo que, desse montante, US$ 45 milhões foram arrecadados no round mais recente em Series C.

A Cymulate possui parceiros estratégicos no mundo inteiro, sendo representada, no Brasil, pela 3CON.

SafeBreach

Local
Sunnyvalle, EUA

Ano de Fundação
2014

Público
B2B

Investimento Recebido
US$ 106 milhões

Investidores
DTCP, DNX Ventures, OCV Partners, Sonae IM, Israel Growth Partners, Sequoia Capital, PayPal, Cerca Partners, Sands Capital, Maverick Ventures, ServiceNow, T-Venture, Hewlett Packard Pathfinder, Leumi Partners, Emerald Development Managers

Sobre

Atacar, analisar, refinar e repetir: é com esse mindset que a SafeBreach vem se destacando como a plataforma BAS/cyber range com maior investimento do mundo. Já em Series D, a companhia possui, entre sua carta de clientes, empresas como Johnson & Johnson, Deloitte, Netflix, Experian e Pepsi.

De forma similar à Cymulate, esta ferramenta permite que corporações emulem diferentes cenários de ataques cibernéticos através de uma biblioteca de exercícios constantemente atualizada com as mais recentes ameaças identificadas. Após as simulações, relatórios automatizados possibilitam uma análise clara das fraquezas de seu sistema de segurança e remediar as brechas encontradas antes que seja tarde demais.

Vale destacar também a capacidade da SafeBreach de se integrar com outras soluções de controle de segurança, incluindo plataformas de Gerenciamento e Correlação de Eventos de Segurança (SIEM) e de Orquestração, Automação e Resposta de Segurança (SOAR).

Local
Tallinn, Estônia

Ano de Fundação
2016

Público
B2B/B2G

Investimento Recebido
US$ 5,66 milhões

Investidores
Karma Ventures, First Fellow Partners

Sobre

Lembra do mais recente exercício da EDA Cyber Ranges Federation que ocorreu na Estônia? A simulação foi feita através de uma plataforma da CybExer, companhia estoniana especializada em fornecer esse tipo de experiência para órgãos governamentais e empresas privadas.

Diferente das demais startups, a CybExer não trabalha apenas com um produto pronto — ela se diferencia no mercado justamente por personalizar o cenário de simulação de acordo com a necessidade de cada cliente ou parceiro, ficando responsável também pela sua operação e manutenção.

Recentemente, a companhia também inovou ao lançar o University Cyber Ranges, oferta exclusiva para instituições de ensino que desejam organizar exercícios realistas para seus estudantes. Novamente, todas as suas características são personalizadas para se adequar à necessidade do contratante.

Apesar de seu louvável sucesso no mercado, a CybExer só recebeu aporte de dois investidores e ainda se encontra em Series A, com um público bastante localizado em seu país de origem.

Local
Nanjing, China

Ano de Fundação
2013

Público
B2C/B2G

Investimento Recebido
US$ 52 milhões

Investidores
Addor Capital, Qihoo 360 Technology, Cornerstone Venture Partners Fund, Balancing Capital, Nanjing Gaoke, DynamicCap

Sobre

Seu nome "oficial" é Nanjing Suning Information Technology, mas pode chamá-la simplesmente de Cyber Peace. É muito provável que você jamais tenha sequer ouvido falar sobre esta startup, mas saiba que, além de ser líder de segmento em seu país de origem, ela também organiza o XCTF, segunda maior liga de segurança de redes do mundo e que já atraiu cerca de 150 mil talentos oriundos de mais de 100 países diferentes. Com ares de evento esportivo, trata-se de um campeonato de CTF para jogador nenhum botar defeito.

Além da liga, a Cyber Peace também oferece uma plataforma robusta de cyber range para empresas privadas e entidades governamentais do país, já tendo sido parceira em exercícios militares.

Com um total de US$ 52 milhões recebidos em investimento, a startup conta com o apoio de grandes corporações, com destaque para a Qihoo 360 Technology, respeitada fornecedora chinesa de soluções para proteção de endpoint e cujos pesquisadores possuem renome global.

Tendências

Brasil se destaca com exercício militar, mas setor de cyber range precisa de amadurecimento

Não há dúvidas de que o Exercício Guardião Cibernético 3.0 provou que o Brasil está em um estágio avançado quando falamos sobre exercícios cibernéticos militares. O evento contou com tecnologias de ponta, incluindo as soluções Cisco e o SIMOC, que pode ser considerado um verdadeiro orgulho autoral por conta de sua alta qualidade que não deixa em nada a desejar.

Contudo, há de convir que, em comparação com o mercado estadunidense, por exemplo, é triste não termos mais startups desenvolvendo esse tipo de tecnologia de forma 100% independente em nosso país.

Claro, qualquer corporação interessada em promover exercícios cibernéticos realistas pode recorrer aos parceiros locais de plataformas estrangeiras ou até mesmo firmar contratos diretamente com fornecedores de outros países. Porém, a criação de um ecossistema nacional facilitaria o acesso à esse tipo de ferramenta e consequentemente aumentaria a sua adoção por parte de mais times de segurança, incluindo os mais enxutos que trabalham em pequenas e médias empresas (ou até mesmo em outras startups).

O trabalho do empreendedor que se aventurar a explorar tal segmento desconhecido pelos brasileiros, porém, certamente enfrentará alguns desafios pela frente. Afinal, sem conhecimento não há demanda, sem demanda não há público e sem público não há investimento. Infelizmente, a falta de conhecimento sobre os benefícios do cyber range parece afetar até mesmo os gringos.

Felizmente, iniciativas como o novo curso apresentado pelo SENAI podem ajudar a virar esse jogo. A formação de novos talentos através de simulações realistas pode fazer com que a próxima geração de profissionais entenda a importância de contar com tais exercícios de forma contínua e atualizada, tornando-se uma extensão, complemento ou — quem sabe — até mesmo um substituto para os formatos atuais de red team/blue team e testes de intrusão.

Aliás, seria muito bem-vindo que mais instituições brasileiras de ensino, incluindo universidades e plataformas de aprendizagem livre, passassem a utilizar plataformas de simulação realista de defesa cibernética. Isso eliminaria o problema de que muitos recém-formados vão ao mercado com pouca ou nula experiência sobre como agir e aplicar corretamente os seus conhecimentos em um cenário de crise.

Temor de ciberguerras faz crescer investimentos em cyber range

Globalmente falando, embora ainda temos uma quantidade diminuta de startups no setor de cyber range, é importante analisarmos como os investimentos em fornecedores já consolidados estão em pleno crescimento. Isso pode ser justificado pelo fato de que estamos vivendo em tempos de tensão no que diz respeito às guerras cibernéticas. Veículos de mídia especializados noticiam o tempo todo manobras e campanhas maliciosas realizadas por hackers de elite patrocinados por entidades estatais — seja para causar disrupções em infraestruturas críticas, para exfiltrar informações altamente sensíveis ou simplesmente disseminar desinformações através de redes altamente organizadas.

São os famosos grupos conhecidos como APT, sigla para Advanced Persistent Threat ou Ameaça Persistente Avançada. A ação desses grupos vem crescendo a um ritmo assustador, a ponto de vislumbrarmos governantes de grandes potências realizando discursos inflamados sobre atividades cibernéticas maliciosas de outras nações.

Com isso, é natural que exércitos e organizações militares passem a ser mais exigidas no campo cibernético, e a melhor forma de garantir o seu preparo é com exercícios em simuladores realistas. Não é à toa que vemos programas desse tipo na América do Norte, na Europa e até na Ásia. Eventualmente, essa responsabilidade militar de defender a infraestrutura crítica de seu país também será compartilhada com as empresas privadas que fornecem serviços essenciais, tornando o cyber range algo crucial para um público ainda mais amplo de profissionais de cibersegurança.

Cybertechs

Glossário de categorias

Categorias

NETWORK & INFRASTRUCTURE SECURITY
Companhias que apliquem processos de proteção da infraestrutura da rede, instalando medidas preventivas para negar acessos não-autorizados, modificações, exclusões e roubo de recursos e dados. Essas medidas de segurança podem incluir controle de acesso, segurança de aplicativos , firewalls, redes virtuais privadas (VPN), análise comportamental, sistemas de prevenção de intrusão e segurança sem fio. Se relaciona com a camada física de transmissão e conexão. Também englobamos soluções de endpoint e messaging security nesta categoria.

WEB SECURITY
Medidas e protocolos de proteção que empresas utilizam para proteger suas organizações de criminosos e ameaças que usam a web como canal. Se relaciona com a camada não-física de segurança, o que engloba internet e segurança de sites.

APPLICATION SECURITY
Medidas de segurança que impedem o roubo/sequestro de dados e códigos dentro de dentro de aplicativos e plataformas.

DATA PROTECTION
Engloba empresas e serviços responsáveis pela proteção de informações sensíveis à empresa (banco de dados, informações de corporações) pelo enquadramento (compliance) às regulamentações de proteção de dados..

MOBILE SECURITY
Empresas que atuam com produtos e serviços voltados a garantir a segurança de dispositivos móveis, independente de seu sistema operacional. Via de regra, são companhias que visam a proteção contra ameaças associadas à conexões wireless.

SECURITY OPERATIONS & INCIDENT RESPONSE
Empresas que desenvolvem soluções estruturadas para responder a vazamentos de dados ou ciberataques. A solução visa minimizar os impactos de ataques cibernéticos já realizados, possibilitando um controle da situação com o menor tempo e custo.

IOT SECURITY
Empresas que atuam com segurança relacionada a internet das coisas, aparelhos e networks que estão conectados entre si.

Categorias

IDENTITY & ACCESS MANAGEMENT
Empresas que desenvolvem soluções que garantem a veracidade das informações e identidades de todas as partes envolvidas em um processo. Aqui se encontram empresas de Identidade como Serviço, que capturam, armazenam e asseguram a veracidade do usuário, e companhias de assinatura digital, que trazem inovação e segurança para todo o ciclo de documentos.

BLOCKCHAIN
Blockchain-as-a-Service (BaaS) são empresas que possibilitam o desenvolvimento de produtos digitais com a tecnologia blockchain, instalando, hospedando e/ou mantendo redes desse tipo em nome de outras organizações.

FRAUD & TRANSACTION SECURITY
Empresas que aplicam tecnologias de análise de dados para gerar avaliações e insights sobre clientes, permitindo mapear riscos, analisar a conformidade com leis e regulamentações e se prevenir contra perdas, desvio, fraude e ataques cibernéticos.

SECURITY CONSULTING & SERVICES
Refere-se às startups que prestam serviços para testar e/ou aprimorar serviços de cibersegurança. Um bom exemplo aqui são as empresas que atuam com simulações de ataques cibernéticos (pentest ou teste de intrusão) como forma de identificar possíveis falhas nos sistemas.

GOVERNANCE, RISK AND COMPLIANCE
Soluções GRC (Governança, Risco e Compliance) são compostas por ferramentas que abrangem a gestão de riscos, governança corporativa e práticas de auditoria e controle, com o objetivo de garantir a conformidade com leis, regulamentos, frameworks e padrões de boas práticas.

CLOUD SECURITY
Cloud security refere-se às iniciativas que atuam com políticas, tecnologias, aplicativos e outros mecanismos de controle utilizados para proteger IP virtualizado, dados, aplicativos, serviços e a infraestrutura associada de computação em nuvem.

Corporates members

APOIO