Capacitação de talentos em cibersegurança

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

Rodrigo Uchoa
Digitization & Business Development Lead
Cisco

Paulo Mordehachvili
CEO
CECyber

João Matos
Business Director
Hackaflag

Robson Amicio
Aluno Cisco
Estudante

Introdução

Introdução

Ao longo das últimas edições do Inside Cybertech Report, nossos leitores puderam aprender mais sobre uma série de novos desafios em segurança cibernética que nasceram recentemente, sobretudo por conta da transformação digital acelerada causada pela crise do novo coronavírus (SARS-CoV2). Nesta sexta edição do relatório, porém, abordaremos um problema em comum enfrentado por todos os envolvidos no setor: o apagão global de talentos, o que leva à escassez de mão-de-obra especializada.

Se em muitos setores da economia vemos um batalhão de bons profissionais competindo por uma quantia ínfima de oportunidades, o cenário é bem diferente quando falamos sobre cibersegurança. Faltam candidatos para um número crescente de vagas. Pode fazer o teste: crie um alerta em seu perfil no LinkedIn para receber notificações de novas posições em aberto nessa área e veja seu email ser inundado por avisos ininterruptos.

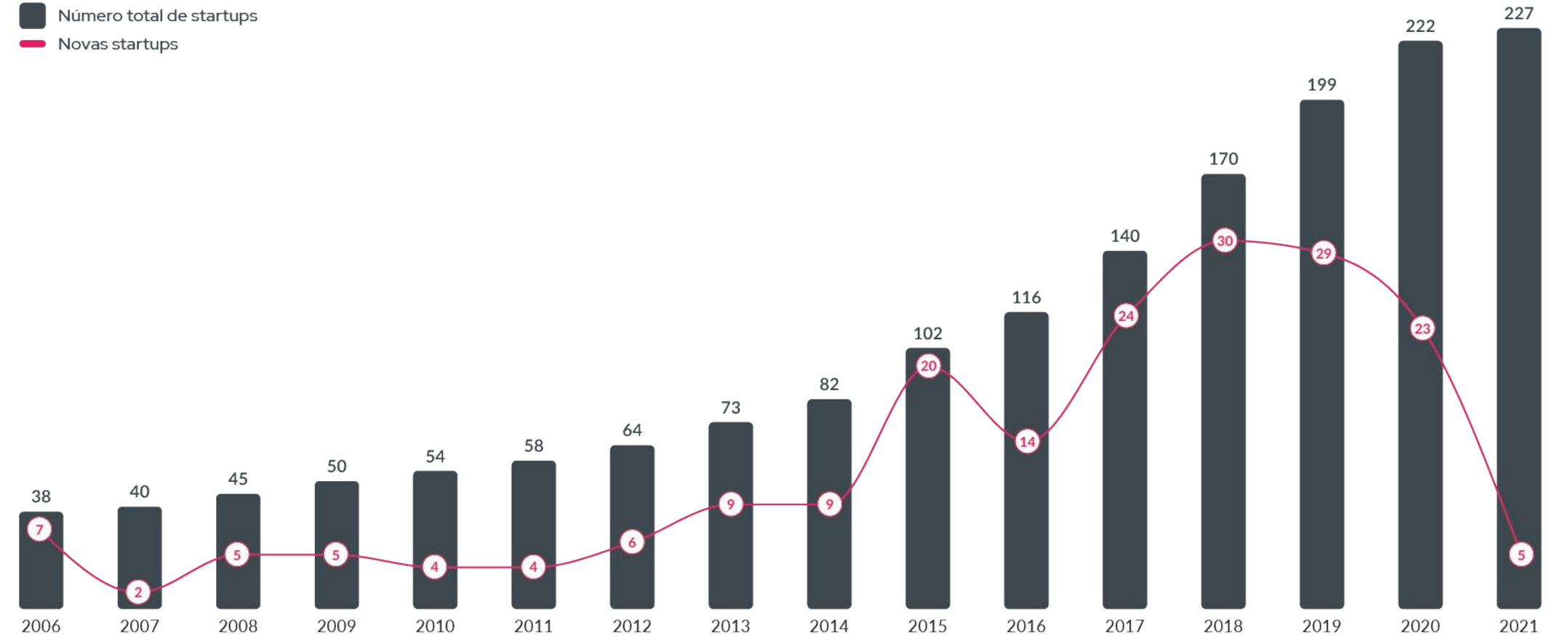
Isso é preocupante sobretudo em uma época na qual novas tecnologias e modelos de infraestrutura estão sendo amplamente adotados, como computação na nuvem, novas soluções de gestão de identidade e acesso e ferramentas de compliance para legislações de proteção de dados pessoais — tal como citamos nos reports anteriores.

Tal situação é global e o Brasil está sendo drasticamente afetado. Neste relatório, entenderemos os fatores que causam tal fenômeno, conheceremos iniciativas (nacionais e globais) que visam preencher essa lacuna e estudaremos algumas tendências do mercado para os próximos anos.

Agradecemos o apoio e o patrocínio da Cisco na confecção do report, que pretende alimentar cada vez mais conteúdos sobre cibersegurança, tema que se torna cada vez mais relevante dentro das corporações.

Boa leitura!

Evolução Cybertechs



Ecossistemas Cybertechs

Highlights

231
Startups

US$ 402M
Investimento recebido desde 2013

12
Categorias

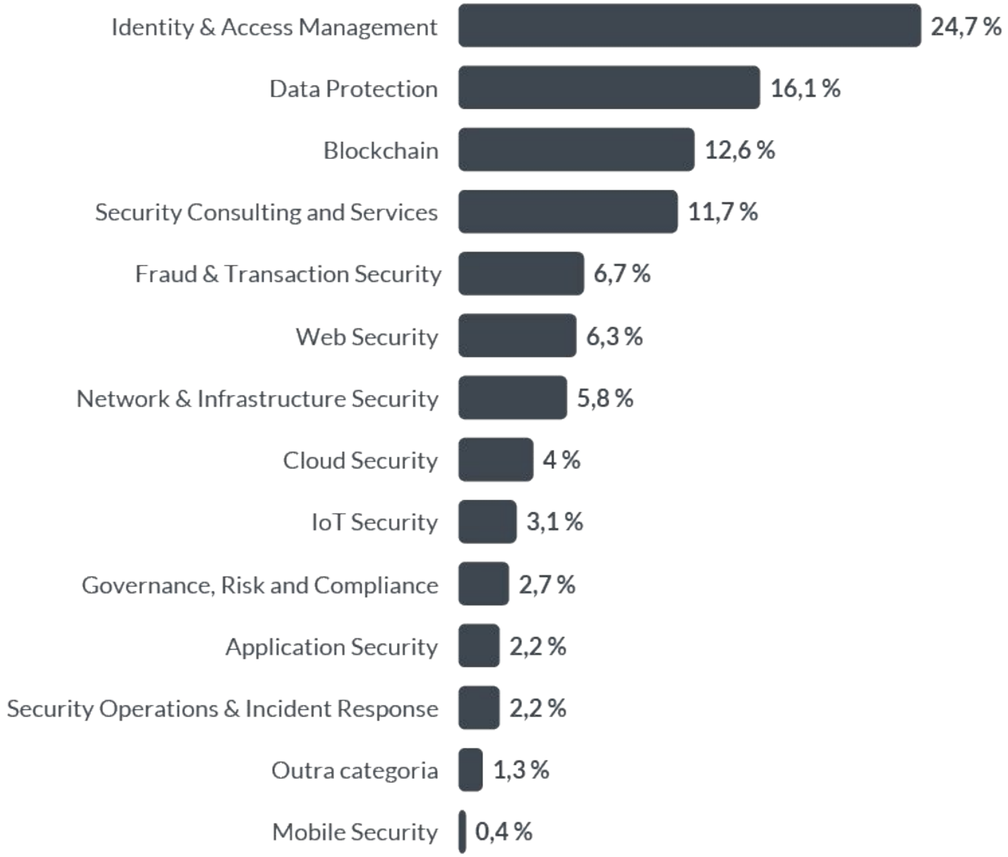
US$ 294M
Investimento recebido nos últimos 2 anos

8.200
Funcionários empregados

13
M&A's desde 2012

43
Startups com investimento recebido

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 · BeCloud · BRy Tecnologia · CH tecnologia · Formalizar e-signature · FULLFace · griaule big data biometrics · GrupoCloud · GRYFO · HDOBOX · contract · ID ESSENTIALS · idwall · MEERKAT · NATOSAFE · nexti · nTokens · DI TI · payface · qriar · QualiSign · PONTO · unike · UNISEC · VSOFT · welcome · COMBATE A FRAUDE · contraktor · CRED DEFENSE · D4S · FIVE VALIDATION · mavie · INOVACODE · JURIDOC · Let's Work · .ai · SHIELDER · SimpleID · SVATECH · 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 · CONVISO · BugHunt

Blockchain

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

Web Security

apura · AuditSafe · CromiWAF · XLabs · SITE BLINDADO · Gatefy · UPX TECHNOLOGIES · XLabs

Capacitação de mão-de-obra em cibersegurança

Contexto e Panorama Nacional

Falta de mão-de-obra: um problema global no mercado de cibersegurança

Não é de hoje que o mercado de cibersegurança se vê preocupado com um verdadeiro apagão de talentos devidamente capacitados para lidar com uma necessidade crescente de bons profissionais. Para mensurar o problema de forma científica, o Consórcio Internacional de Certificação em Segurança de Sistemas da Informação (International Information System Security Certification Consortium), mais conhecido como (ISC)², realiza anualmente uma pesquisa global sobre o tema.

Na edição 2021 de seu estudo Cybersecurity Workforce Study, a organização entrevistou um número recorde de 4,753 profissionais do setor, em empresas de todos os tamanhos, na América do Norte, América do Sul (LATAM), Europa e Ásia-Pacífico (APAC). Surpreendentemente, o relatório indicou a existência de 4,19 milhões de profissionais de segurança da informação ao redor do mundo — um salto de mais de 700 mil novos trabalhadores em comparação com o ano anterior.

Ainda assim, por mais que o gap entre demanda e oferta de mão-de-obra tenha caído em relação a 2020, ela continua assustando: **estima-se ser necessário mais 2,72 milhões de profissionais capacitados** para que o mercado esteja pronto para responder às novas ameaças que surgem diariamente. Estamos falando de um crescimento de 65%.

O maior crescimento registrado em 2021 foi na Alemanha, onde a quantia de profissionais saltou em 165% (de 175 mil para mais de 465 mil).

As consequências dessa falta global de mão-de-obra são gravíssimas, especialmente se levarmos em conta o fato de que estamos enfrentando uma onda de sequestros digitais (ransomware) e ataques à cadeia de suprimentos, que acabam causando disrupções em grande escala em infraestruturas que são críticas para a sociedade.

Dentre os problemas mais comuns da indústria apontadas pelo (ISC)² como consequências diretas da ausência de profissionais qualificados dentro das empresas, nós podemos destacar:

- Sistemas configurados indevidamente (32%);
- Falta de tempo para avaliações e gerenciamento de risco apropriados (30%);
- Lentidão para atualizar sistemas críticos (29%);
- Falta de fiscalização em processos e procedimentos (28%);
- Inabilidade de se manter consciente sobre todas as ameaças que rondam a sua rede corporativa (27%);
- Desenvolvimento apressado (26%).

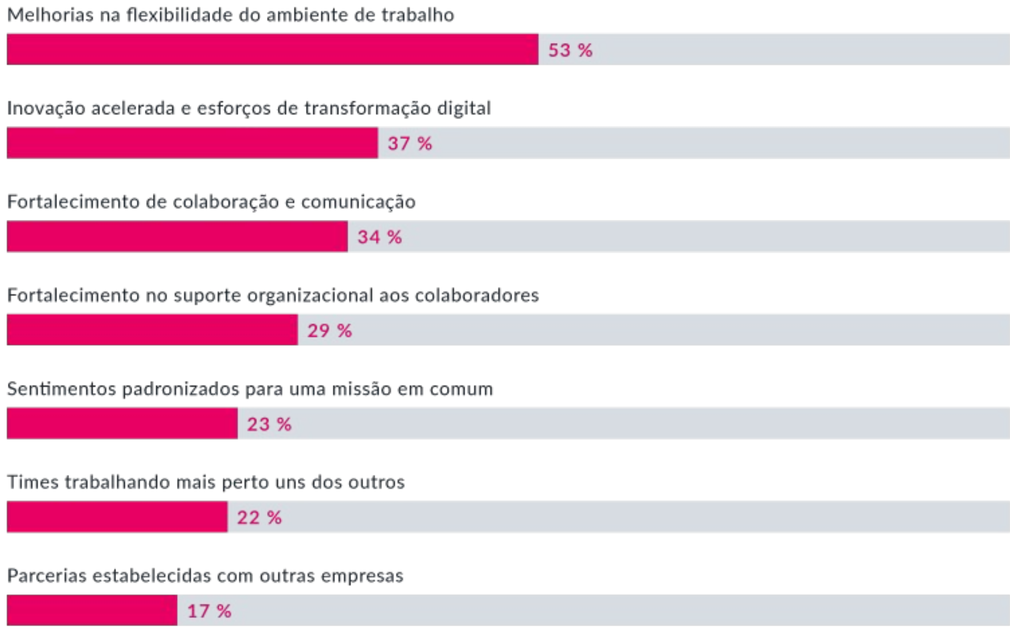
Crise da COVID-19 atrapalha (e ajuda) mais

Como você pôde aprender em nossos relatórios anteriores, a crise do novo coronavírus (SARS-CoV2) causou um estresse ainda maior na área de segurança da informação. A transformação digital acelerada causada pela pandemia forçou companhias a adotarem novas tecnologias e modelos de negócio focados no digital sem o devido preparo para tal; como resultado, tivemos aumentos exponenciais na quantidade de ciberataques e fraudes online por conta do aumento da superfície de ataque.

Porém, a crise da COVID-19 também teve impactos no mercado de trabalho, com 29% dos entrevistados da (ISC)² afirmando terem se ausentado de suas posições entre 2020 e 2021 por motivos que incluem guarda de crianças, recessos coletivos e problemas de saúde particulares ou familiares. Apesar disso, **os participantes do estudo, em sua maioria, relatam um aumento de moral e de produtividade durante esse período**, sendo que o principal motivo disso parece ser uma preferência pessoal pelo trabalho remoto.

Globalmente falando, apenas 24% das empresas pretendem retornar a um formato de trabalho 100% presencial; é provável que elas estejam levando em consideração que "maior flexibilidade no ambiente de trabalho" é o ponto positivo mais citado entre os profissionais como resultados benéficos diretos da pandemia do novo coronavírus.

Como as respostas à COVID-19 melhoraram o ambiente de trabalho



E no Brasil, qual é a situação?

Pode até parecer falta de sorte para nós, mas, dentre os 14 países analisados pelo (ISC)², o Brasil é o que mais sofre com falta de mão-de-obra qualificada. O consórcio certificador estima que o nosso país precisa de 441 mil novos profissionais no mercado para preencher essa lacuna.

Apenas para fins comparativos, temos os Estados Unidos da América em segundo lugar com 377 mil profissionais necessários; México em terceiro com 260 mil trabalhadores ausentes; Alemanha em quarto com um déficit de 68 mil pessoas e Japão em quinto lugar com 50 mil colaboradores em falta.

Diferente da maioria dos países, o Brasil foi um dos poucos a sofrer uma queda no número de profissionais em 2021. Estima-se que, por aqui, existia uma força de trabalho formada por 486 mil profissionais em 2019; essa quantia subiu para pouco mais de 626 mil em 2020, mas sofreu um declínio este ano para cerca de 581 mil. As razões para essa redução são um tanto misteriosas.

Em uma recente entrevista concedida à imprensa, o vice-presidente da Associação Brasileira das Empresas de Software, Paulo Roque, comentou que muitos vezes países estrangeiros acabam "roubando" talentos nacionais, oferecendo uma entrada facilitada no mercado de trabalho (com menos burocracia) e pagamento diretamente em moedas mais valorizadas como dólar ou euro — isso tudo sem que o talento precise sequer sair do Brasil.

"Quando você vai procurar um profissional júnior, tem eles sobrando. Mas na hora que você vai, por exemplo, procurar um programador sênior, você não acha. E o que está acontecendo é que as empresas estrangeiras estão roubando nossa mão-de-obra e o cara não precisa nem sair de casa. Tem caso de grande desenvolvedor pagando em dólar um jovem de 23 anos para trabalhar na casa dele. Ele ganha cinco vezes mais do que ganharia no Brasil, e de casa, ele nem precisa ir para o escritório", explica Roque.

Um ambiente favorável

É importante ressaltar que o Brasil é um alvo predileto do crime cibernético por conta de uma série de características que, quando combinadas, o tornam bastante atraente para os meliantes digitais: uma economia relativamente próspera e uma baixíssima maturidade em segurança da informação, tanto por parte das empresas (independentemente do porte) quanto dos usuários finais.

Isto posto, também é sabido que o Brasil possui graves problemas com inclusão digital e com educação. Por isso, é essencial analisarmos aqui as iniciativas que temos para capacitação de mão-de-obra especializada.

Desafios na capacitação de mão-de-obra especializada

Rodrigo Uchoa
Digitization & Business Development Lead
Cisco

O problema de falta de mão-de-obra qualificada no mercado de cibersegurança é uma questão antiga, mas que torna-se ainda mais preocupante em tempos de transformação digital acelerada no novo normal. Quais seriam os principais motivos para esse apagão de talentos no setor?

Com certeza, é impossível falar de digitalização e transformação dos negócios na era digital sem considerarmos o tema de riscos cibernéticos e segurança da informação. O principal pilar de todo o processo de transformação digital é a hiperconectividade de pessoas e máquinas, a coleta massiva de dados e a análise contínua, holística e em tempo real destes dados através de ferramentas e algoritmos de inteligência artificial.

Com milhões de pessoas e máquinas conectadas e bilhões de dados gerados a cada dia e armazenados em diferentes localidades, na nuvem ou em data centers próprios, imagine o tamanho do desafio que a área de segurança da informação está enfrentando nos dias de hoje. O número exponencial de pessoas, dispositivos, aplicações, servidores e dados reflete a complexidade envolvida com a digitalização e com a gestão da segurança cibernética. E esta complexidade é a resposta para a sua pergunta.

Este cenário e o tamanho do desafio apresentado ao profissional de segurança cibernética se traduz em uma necessidade de alta qualificação, conhecimentos profundos de diferentes domínios tecnológicos e uma capacidade de estudo e aprendizado contínuo que não é simples de se encontrar no mercado.

Eu costumo dizer que, de certa forma, um profissional de segurança cibernética já nasce um profissional de segurança cibernética, pois as principais qualificações necessárias para um bom profissional nesta área não estão associadas apenas com o conhecimento específico, mas com a paixão por tecnologia, capacidade de enfrentar grandes desafios e de trabalhar sob enorme pressão, persistência, personalidade questionadora e investigativa. Concluindo, estamos falando de diversos soft skills difíceis de serem encontrados e combinados em uma única pessoa.

É isso que faz do profissional de segurança cibernética um profissional difícil de ser encontrado e desenvolvido, gerando um apagão de talentos no setor.

A Cisco abrirá, em fevereiro de 2022, mais uma rodada para o Programa CiberEducação Cisco Brasil. Como funciona essa iniciativa e como a Cisco enxerga que ela poderá alterar o panorama atual do mercado de trabalho nacional?

Costumo dizer que o nosso maior desafio é descobrir talentos com o perfil certo para o setor de segurança cibernética e, na minha opinião, a melhor forma de fazermos isso é apresentando ao maior número de jovens e profissionais de tecnologia o que é o setor e qual o papel do profissional de segurança cibernética.

O Programa CiberEducação Cisco Brasil endereça exatamente este ponto, convida milhares de jovens a entrarem neste mundo. O programa é uma porta de entrada, uma red pill para aqueles que querem entrar no mundo desafiador da segurança cibernética. O desafio é grande, mas as recompensas também. O programa está transformando o mercado de trabalho de ciber no Brasil, desenvolvendo a nova geração de profissionais de segurança cibernética do país, já tendo formado mais de 1,7 mil talentos em seu primeiro ano. Além disso, também investimos na formação de 274 docentes para que este conteúdo seja replicado no longo prazo pelas academias Cisco, gerando assim um efeito multiplicador.

No geral, quando falamos de capacitação em cibersegurança, vemos um cenário bastante bagunçado, com diferentes instituições oferecendo diferentes tipos de formações e com foco em diferentes vertentes do mercado, como redes, intrusão etc. Isso é um fator que pode atrapalhar a resolução desse apagão?

Em essência, é extremamente recomendado ao profissional de segurança cibernética um amplo conhecimento dos diferentes domínios tecnológicos, tais como redes de comunicação, nuvem, bancos de dados, aplicações e dispositivos, pois na maioria das vezes as vulnerabilidades, ameaças e ataques envolvem ou impactam diferentes domínios dentro e fora dos muros da empresa. Obviamente, nenhum ser humano é capaz de se especializar e dominar profundamente todos os domínios tecnológicos e seus componentes de hardware e software, exigindo altos níveis de coordenação e colaboração entre diferentes profissionais e equipes.

Além dos diferentes domínios, toda organização de segurança cibernética também é estruturada em diferentes áreas funcionais, que normalmente são exercidas por equipes com perfis e conhecimentos distintos — gestão, engenharia, operações, governança de dados, inteligência de ameaças, investigação & resposta a incidentes.

É fundamental entendermos que iniciativas de capacitação para o setor precisa levar em consideração os diferentes domínios tecnológicos e áreas funcionais, exigindo que a empresa e seus profissionais tenham claramente suas linhas de atuação e desenvolvimento. Além disso, toda posição de TI é uma posição de segurança cibernética.

Desafios na capacitação de mão-de-obra especializada

Rodrigo Uchoa
Digitization & Business Development Lead
Cisco

Cada trabalhador de TI, cada trabalhador de tecnologia, precisa estar envolvido com a proteção e defesa de aplicativos, dados, dispositivos, infraestrutura e pessoas. Por isso, nosso programa de educação Cisco Networking Academy disponibiliza uma jornada educacional nesta área que oferece desde os conhecimentos mais básicos aos mais avançados, apoiando profissionais de várias áreas e interesses.

Como as startups e as grandes corporações podem auxiliar o mercado a capacitar novos talentos e inseri-los no mercado de trabalho?

Como empresa pioneira no mercado de TI e impulsora da transformação digital, a Cisco entendeu faz tempo o desafio social e econômico da brecha de mão-de-obra no mercado de TI. Uma de suas respostas foi justamente a criação do Cisco Networking Academy. Este é o maior programa de responsabilidade social da empresa, focado em trazer estas habilidades profissionais e capacitar novos talentos através de uma plataforma e portfólio educacional robusto e reconhecido pelo mercado. Com mais de 25 anos de história, tem presença em 180 países e impactou mais de 15 milhões de jovens de todo mundo, sendo 440 mil somente no Brasil.

Outra forma de capacitar novos talentos e inseri-los no mercado de trabalho é abrindo oportunidades para um primeiro emprego e entender que o profissional de segurança cibernética é construído com muita mão na massa e com um aprendizado teórico e prático contínuo.

É importante que as empresas entendam que é necessário formar e apoiar estes profissionais ao longo desta jornada de desenvolvimento contínuo.

Na minha opinião, toda empresa, seja ela uma startup ou uma corporação, precisa de um programa específico para atração e desenvolvimento de talentos, partindo de um processo claro de identificação de quem tem o perfil correto para este setor, ou seja, paixão por tecnologia, resiliência, persistência, personalidade questionadora e investigativa.

Desafios na capacitação de mão-de-obra especializada

Rodrigo Uchoa
Digitization & Business Development Lead
Cisco

Empresas brasileiras oferecem conteúdo educacional e certificações

As iniciativas da Cisco são um excelente exemplo de programas de capacitação para profissionais que desejam ingressar nesse mercado, mas não é o único. Primeiramente, dentro do cenário acadêmico tradicional, diversas instituições de ensino já ofertam cursos de graduação na modalidade tecnólogo (com menor duração, geralmente entre dois anos a dois anos e meio) em segurança da informação.

Em consulta realizada ao sistema do Ministério da Educação (MEC), o Distrito constatou que **105 instituições ao redor do Brasil estão credenciadas para oferecer tal curso de graduação**.

Já quando falamos em cursos de especialização (como pós-graduação, MBA e cursos livres), constatamos a existência de nada menos do que 280 opções variadas, incluindo "Especialização em Segurança da Informação", "Gestão da Segurança da Informação", "Computação Forense e Segurança da Informação" e "Segurança da Informação e Perícia Digital".

Mas e fora da academia?

Claro, não é apenas o cenário acadêmico que oferece oportunidades de capacitação para quem deseja se preparar para o mercado de trabalho. Também temos startups, empresas e até docentes independentes.

É interessante perceber que uma particularidade do setor de segurança da informação é que ele se divide em diversas vertentes e não existe um fluxograma específico de conhecimentos para quem deseja trabalhar na área. Embora um background em tecnologia da informação (TI) costume ser a base para novos profissionais, também há quem prefira estudar em seu próprio ritmo, obtenho conhecimentos sobre programação, redes, governança e outras disciplinas de forma não-linear.

Ao pesquisar "segurança da informação" na plataforma de ensino livre Udemy, por exemplo, conseguimos 1,016 resultados de cursos em português nos mais variados preços e níveis de conhecimento prévio.

105
Cursos de Graduação (tecnologia)

280
Cursos de Especialização (pós, MBA e livre)

>1 mil
Resultados de cursos na plataforma Udemy

Investimentos em multiplicadores

Como dissemos anteriormente, é difícil falar em capacitação de mão-de-obra para segurança cibernética sem entrar no mérito de disciplinas mais abrangentes do mercado de tecnologia da informação em geral, como desenvolvimento de aplicações.

Se analisarmos startups que oferecem cursos mais generalistas, mas cujos conhecimentos podem ser perfeitamente aproveitáveis no setor de cibersegurança, podemos perceber investimentos crescentes sobretudo em plataformas de ensino à distância (EAD).

Neste ponto, fica difícil não mesclar a categoria das startups cybertech com as edtech (educational technology, ou tecnologia educacional).

Investimentos em startups brasileiras de educação digital (2021)

MÊS	STARTUP	INVESTIDOR	VALOR	ESTÁGIO
Março	Hotmart	TCV	US$ 130M	Series C
Maio	Tera	Arco Educação	N/A	N/A
Agosto	Driven	Iporanga Ventures	R$ 16M	Seed
Outubro	Trybe	Base Partners & Untitled	US$ 26M	Series B

Nome: CECyber

Público: B2C/B2B

Ano de Fundação: 2019

Tendo como missão “ajudar profissionais e organizações a enfrentarem o crime cibernético através da capacitação prática voltada para o mundo real”, a CECyber (Center of Excellence in Cybersecurity) foi fundada em 2019 e é uma das poucas startups nacionais focadas em capacitar mão de obra qualificada para o mercado de cibersegurança.

Embora conte com DNA brasileiro, ela atua em território tupiniquim em parceria com a israelense Cyberbit para trazer aos seus alunos o Cyberbit Range, um avançado simulador de ataques cibernéticos que recria com perfeição um security operations center (centro de operações de segurança ou SOC) para cenários de prevenção, detecção e resposta a incidentes.

Os cursos são variados. Na área de infraestrutura e redes, temos três tracks (Iniciante, Avançado e Lab Sessions); há também programas na área de Desenvolvimento Seguro, Cloud Security (segurança para ambientes na nuvem) e cursos sob encomenda que abordam cenários bem específicos, como estratégias ofensivas (red team), crimes no setor financeiro, threat hunting, administração de Active Directory e até anatomia de malwares.

O grande destaque, porém, fica para o programa Prep & Placement. Nele, o aluno passa por um alinhamento individualizado, sendo submetido ao programa Cybersecurity Foundation e auxiliado a encontrar um emprego na área.

Após conseguir a sua colocação, o profissional ainda recebe ume mentoria dos especialistas da CECyber durante seis meses, garantindo plenamente uma performance prática satisfatória dentro do mercado de trabalho.

Por fim, empresas também podem contratar o corpo docente da CECyber para realizar treinamentos internos sob-demanda para a sua equipe já existente.

A companhia já recebeu um total de US$ 1 milhão em aporte.

CECyber: capacitando e alocando profissionais

Paulo Mordehachvili
CEO
CECyber

A CECyber pode ser considerada a primeira empresa brasileira a se dedicar exclusivamente à capacitação de profissionais na área de cibersegurança, oferecendo diversos cursos nos mais variados formatos. Quais desafios você enxerga na inserção de novos talentos no setor?

A CECyber pode ser considerada a primeira empresa brasileira dedicada à capacitação de profissionais na área de defesa cibernética. Nossos cursos são voltados para a prática do dia a dia de profissionais, assim como novos entrantes no setor. Estamos endereçando o enorme gap da força de trabalho em cibersegurança do Brasil, tido hoje como o maior do mundo, estimado em 440 mil profissionais.

Além do gap de quantidade, que é o mais óbvio, há também um gap de qualidade (nível dos profissionais atuantes), principalmente no que tange a capacidade de praticar defesa cibernética no dia a dia de organizações e provedores de serviços. Os desafios para a inserção de novos talentos são inúmeros, tais como: a) o baixíssimo número de graduandos de cursos TIC de faculdades; b) a competição pelos graduandos por todas as áreas de TI, e não somente cibersegurança; c) a falta de empregabilidade dos formandos, apesar da alta demanda; d) a baixa qualidade técnica dos cursos, comumente generalistas e pouco voltados para a prática; e e) a falta de disponibilidade de capacitação de prontidão, "for the job", que é a essência da capacitação da CECyber. Além da capacitação técnica em defesa e desenvolvimento seguro, a CECyber tem orgulho da parceria com fundações da Poli-USP no desenvolvimento do MBA em Cibersegurança do PECE-USP e do curso Executivo em Cyber da FDTE-USP, que serão lançados em 2022.

O mercado de trabalho, muitas vezes, superestima grandes certificações do mercado e formações acadêmicas de grandes instituições de ensino, refutando candidatos que possuem formação alternativa. Como a CECyber se posiciona em relação a essa questão?

Países desenvolvidos como Japão, EUA e Alemanha têm na capacitação técnica um enorme contingente de alunos. O mesmo não se aplica ao Brasil. Ainda, apesar da relevância de fundamentos e da teoria, ambos "nice to have", não há substituto para a capacitação prática, um "must have", e que é o foco da CECyber. Nós ensinamos fundamentos desde a base crítica em infra e redes, derivados pela prática, assim como técnicas avançadas de defesa, for the job.

O programa Prep & Placement chama atenção por garantir a colocação profissional do aluno no mercado de trabalho, oferecendo apoio na busca por oportunidades e oferecendo mentoria pós-contratação. Você possui estatísticas de quantos profissionais já foram inseridos no mercado graças a esse programa inovador?

Em 2021, selecionamos 40 de 120 alunos, e destes 40 alunos, 21 já conseguiram sucesso em empresas especializadas do setor, como ISH, Clavis, Daryus, Oi, Proof e Safeway, dentre outras.

Já temos 40 candidatos para próxima turma, e agora o processo de captação está mais seletivo desde a largada, logo, estimamos 30 novos entrantes já em janeiro de 2021.

Nós ajudamos a colocação destes novos profissionais, que se tornam embaixadores da CECyber no mercado. Estimamos 300 alunos ou mais em 2022.

Na sua visão, como podemos resolver esse apagão de talentos em cibersegurança no Brasil, especialmente durante o novo normal, no qual a transformação digital acelerada demanda a adoção de novas tecnologias de forma segura?

Não há substituto para capacitação for the job, mesmo saindo de uma base zero em TI.

Este é programa que estamos desenvolvendo e que será a extensão natural do FIT-C – From IT to Cyber, da CECyber.

Não será possível aguardar a formação de estudantes em universidades, que na sua maioria peca pelo baixo engajamento, graças a formação teórica, de pouca prática, o que resulta em baixa empregabilidade mesmo em mercado aquecido e demandante. Uma tragédia considerando a taxa de desemprego do país, não é?

CECyber: capacitando e alocando profissionais

Paulo Mordehachvili
CEO
CECyber

Nome: Hackaflag

Público: B2C/B2B

Ano de Fundação: 2014

A princípio, o Hackaflag não foi fundado para atuar como um fornecedor de conteúdos educacionais, mas sim como a marca responsável por organizar o campeonato de capture the flag (CTF) homônimo, e que mais tarde ficaria conhecido simplesmente como #HFBR.

O objetivo era reunir entusiastas e pesquisadores em um jogo que colocasse à prova os seus talentos na área de cibersegurança, com desafios inspirados em cenários do mundo real. Ocorrendo junto ao evento itinerante Roadsec, o campeonato visitou, durante anos, dezenas de cidades ao redor do país.

Aos poucos, percebendo os talentos que atraia naturalmente, o Hackaflag passou a atuar também como uma plataforma de bug bounty. Isso significa que empresas brasileiras poderiam se cadastrar no módulo e ter seus sistemas computacionais testados por qualquer pesquisador interessado em encontrar falhas. Quem identificar uma vulnerabilidade (e após esta ser devidamente validada) é recompensado com uma quantia pré-determinada em dinheiro.

Programas de bug bounty podem ser públicos (abertos à participação de qualquer internauta) ou restritos (apenas para pesquisadores selecionados).

No intuito de incentivar uma evolução mais ágil e eficiente da comunidade, em 2018, foi finalmente inaugurada o Hackaflag Academy. O módulo traz diversas opções de cursos rápidos, 100% online e gratuitos, para quem deseja iniciar sobretudo na área de segurança ofensiva.

O HF Academy recebe novos conteúdos educacionais periodicamente, conta com um sistema de ranking para incentivar a competitividade saudável entre os alunos e oferece laboratórios digitais realistas para quem deseja testar suas habilidades recém-adquiridas.

Desenvolvendo skills específicas fora da academia

João Matos
Business Director
Hackaflag

Pesquisas apontam que as novas gerações (Z e millenials) entram no mercado de cibersegurança através de métodos não-convencionais, fora da formação inicial tradicional em TI. A Hackaflag Academy é uma iniciativa que justamente fornece cursos para quem deseja um caminho alternativo. Como a HF Academy enxerga o mercado de capacitação de profissionais no Brasil e a sua própria atuação na resolução desse problema?

Primeiramente é válido lembrar um pouco da trajetória do Hackaflag para contextualizar. Nós nascemos como uma competição dentro da maior conferência de hacking da América Latina, o Roadsec. Com isso, nós visitamos o Brasil todo desde 2014, onde fomos conseguindo visualizar e conhecer a cena de tecnologia regional e nacional. Foi daí que surgiu a ideia de capacitar quem possuía interesse em iniciar na área de segurança da informação com o Academy, preparando-os para começarem a jogar o nosso CTF, que é a maior competição do continente.

Hoje o mercado de capacitação está aquecendo com o surgimento de novas empresas e faculdades voltadas para o setor acadêmico de segurança, além de algumas empresas buscando formar esses profissionais dentro de casa; porém, somos uma área diferente de outras que necessitam de certificações, diplomas e provas de ordem para exercer a profissão.

Tecnologia é um segmento no qual pessoas com capacidades de aprendizado diversas conseguem se destacar, principalmente aquelas que têm facilidade de aprendizado autodidata. Quem demonstra conhecimento prático consegue entrar no mercado de trabalho. O papel do Hackaflag é dar um direcionamento para que pessoas encontrem sua área de atuação. Se ela quer seguir para o caminho mais técnico (como pentester e red team), apontamos quais conhecimentos e requisitos ela necessita para seguir de forma autodidata ou buscar cursos e certificações de acordo com o seu objetivo.

Todos os cursos da plataforma são 100% gratuitos, o que é um ineditismo em comparação aos modelos de negócio de outras startups que oferecem capacitação. O que levou o Hackaflag a decidir por tal modelo?

Antes de tudo mais, o Hackaflag é uma comunidade com mais de 10 mil pessoas que participam dos nossos eventos, campeonatos e ações. Temos como objetivo fomentar a comunidade, capacitar e fornecer profissionais ao mercado. Para que tenhamos uma comunidade e mercado fortes, é necessário oferecer ao menos condições iniciais e conteúdos para os primeiros passos e é esse o nosso papel, atuando desde o início com cursos e laboratórios gratuitos para estudos, sendo uma vitrine para o mercado através dos nossos campeonatos e outros produtos corporativos. Com isso conseguimos alimentar todas as etapas. →

A Academy é apenas um módulo da plataforma Hackaflag, que possui laboratórios virtuais para treino e um sistema no qual qualquer pessoa pode efetivamente ser recompensada financeiramente por encontrar vulnerabilidades em sistemas reais de clientes. Esse formato pode ser uma maneira mais acessível para novos talentos ingressarem no mercado?

Com certeza. Nosso objetivo é atuar em todas as etapas da vida profissional. Auxiliar seus primeiros passos com o Academy gratuito, dar exposição de sua evolução com os campeonatos CTF (onde a participação também é gratuita) e consolidar seu talento em projetos de recrutamento corporativo e nos programas de bug bounty.

O bug bounty, enquanto um programa de recompensas por falhas encontradas em empresas, é hoje uma das maiores provas de capacidade de um profissional. Possui o custo-benefício para a empresa recompensar o pesquisador por bugs e nível de criticidade ao escopo indicado, fazendo com que os possíveis erros sejam corrigidos antes que cheguem em mãos de criminosos. Já o pesquisador cria sua reputação com seus reports ajudando o mercado.

Plataformas de bug bounty, como o próprio Hackaflag, possui o que essas empresas precisam: proximidade e contato dos melhores profissionais, pesquisadores, talentos e estudantes com diversas skills. Por isso essa modalidade vem crescendo cada vez mais no Brasil e muito utilizada como solução de segurança e recrutamento. Quando o Hackaflag trouxe a modalidade ao Brasil em 2018, ainda não era compreendido como essa prática auxiliaria tanto no desafio de encontrar profissionais de segurança. Hoje, as maiores empresas do país já visualizam e possuem seus programas publicados em nossa plataforma.

Quando falamos de apagão de talentos, por parte das empresas, muitas ainda adotam um modelo de avaliação e contratação defasado. Sabemos que dentro de plataformas de bug bounty há muitos "olheiros" de talentos que podem convidar um pesquisador independente para uma posição fixa. Você acredita que parte desse apagão é culpa do próprio mercado de trabalho não se adaptar à nova realidade? Como podemos mudar isso?

Sim, o mercado tem uma boa parcela de culpa nesse apagão. Durante muito tempo, o mercado negligenciou a segurança da informação, visualizando tal área apenas como um departamento (muitas das vezes de uma pessoa só) para gerenciar acessos e firewalls, proibir acessos e reportar para o TI. Hoje, esta área está sendo finalmente colocada como estratégica ao negócio e aplicada em várias frentes: desde corporativa a todos os estágios de um produto, e, com o surgimento de normativas e legislações voltadas à proteção de dados, aceleramos este desafio.

Com isso, estamos vendo essa "corrida maluca" das corporações atrás dos profissionais sem compreender corretamente as personas e necessidades, pois anteriormente esse profissional não estava em evidência. Com a pandemia do novo coronavírus, agravamos ainda mais o problema com empresas estrangeiras capturando os nossos maiores talentos com salários mais atraentes em dólar ou euro sem que o candidato precise sair do Brasil, trabalhando de forma remota.

Desenvolvendo skills específicas fora da academia

João Matos
Business Director
Hackaflag

O caminho para a transformação são as empresas e profissionais mais experientes se aproximarem cada vez mais da comunidade, compreendendo, auxiliando e financiando a formação da nova geração, além de apostar em novos métodos de trabalho, abrindo suas portas para que as pessoas compreendam a cultura de trabalho da empresa e a importância que as pessoas e segurança tem para elas.

Além, é claro, de entender que o mercado precisa de uma maturação e que ela será feita em conjunto e com paciência. Por mais que a necessidade seja para agora, enfim, não adianta abrir uma vaga para estagiário pedindo experiência de um profissional sênior, como infelizmente é comum encontrar por aí.

Desenvolvendo skills específicas fora da academia

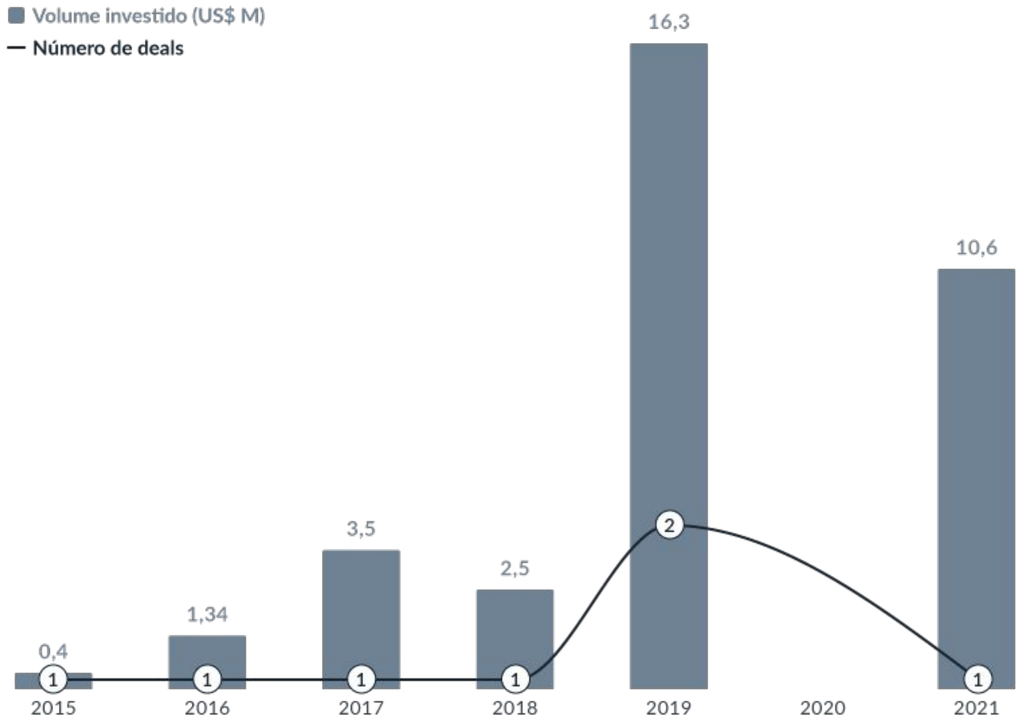
João Matos
Business Director
Hackaflag

Mudanças de paradigmas

Panorama Internacional

Startups de educação especializada ainda recebem pouco investimento na América do Norte e Europa

Investimento em startups de capacitação e educação cibernética



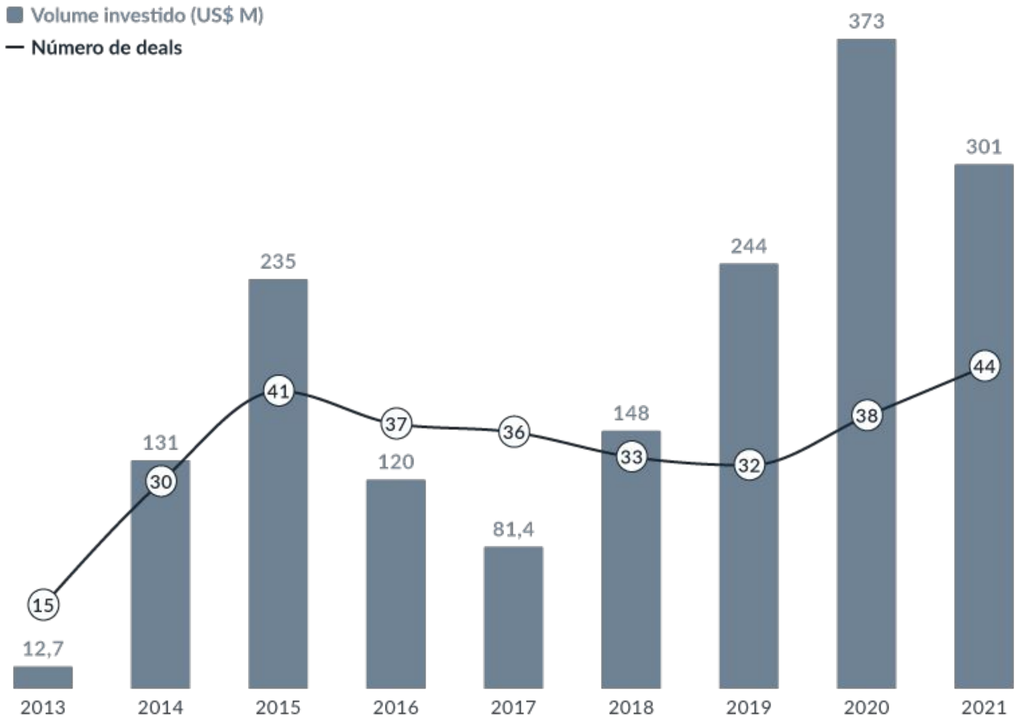
As startups focada em capacitação e conteúdo educacional focadas em segurança da informação ainda formam um mercado bastante tímido no resto do mundo. Ao analisarmos novos empreendimentos nessa área, conseguimos encontrar apenas dez startups fundadas desde 2012.

Da mesma forma, tais negócios não parecem chamar atenção de fundos de investimento. De 2015 a 2021, temos apenas 7 deals e um total de US$ 34,6 milhões investidos em apenas duas startups. Como é possível perceber no gráfico ao lado, apenas o ano de 2019 se destaca por ter registrado dois rounds e um volume de investimento de US$ 16,3 milhões.

Não tivemos deals em 2020, e, neste ano, os valores movimentados também foram bem maiores.

Em educação generalista, o cenário muda para melhor

Investimento em startups de ensino generalista em TI



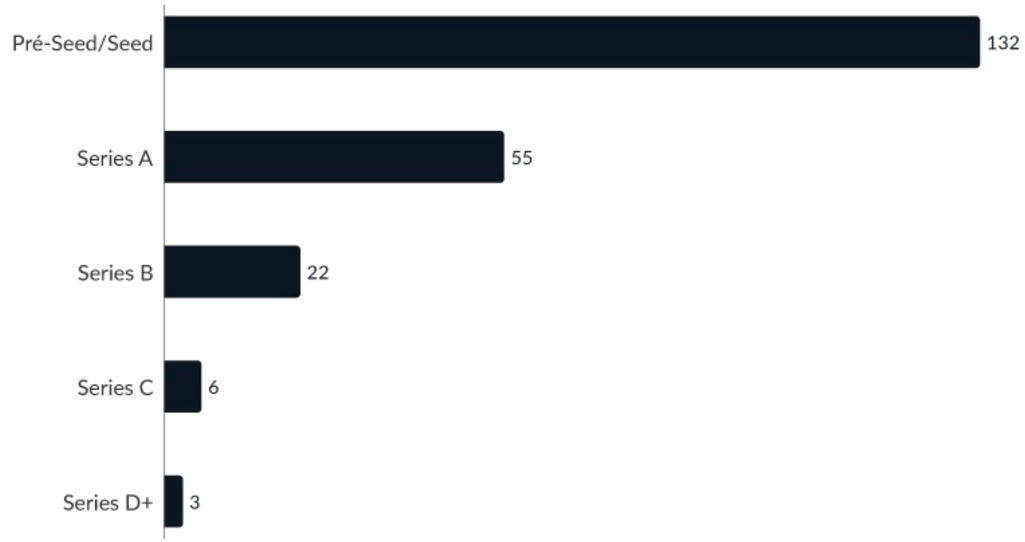
Novamente, fica difícil falar sobre capacitação de mão-de-obra sem entrar no mérito das edtechs que oferecem conteúdos educacionais sobre tecnologias da informação de forma mais generalistas, incluindo cursos de programação, governança, redes, compliance regulatório com legislações de proteção de dados e assim por diante.

Plataformas desse tipo — categoria na qual incluímos nomes conhecidos como Udacity, Codecademy e SoloLearn — já receberam, juntas, um total de US$ 1,75 bilhões em investimento de todos os estágios, sendo que temos 40 companhias acima da Series A e 66 exits (aquisições e ofertas públicas iniciais ou IPO) bem-sucedidos. A Udacity, inclusive, é a única unicórnio nesse segmento.

É possível perceber um aumento nos investimentos a partir de 2019, com um recorde em 2020 e um leve declínio em 2021.

Volume por estágio de aporte

Número de deals por estágio



Embora os investimentos em startups de educação online estejam em alta, a maior parte dos aportes concentram-se nas categorias de investimento-anjo e seed; temos apenas 55 companhias em Series A e apenas 22 em Series B..

Restam apenas 9 edtechs em estágio avançado de investimento, e, como citamos anteriormente, somente um unicórnio.

Principais investidores e deals

	INVESTIDOR	PAÍS	INVESTIMENTOS NA CATEGORIA
1	**Y Combinator**	EUA	19
2	**500 Global**	EUA	9
3	**Techstars**	EUA	7
4	**Learn Capital**	EUA	5
5	**Start-Up Chile**	Chile	4

Observando os 198 investidores que colocaram dinheiro em plataformas de ensino de tecnologia da informação, ao analisarmos os cinco nomes mais proeminentes, percebemos que se tratam de aceleradoras e incubadoras igualmente generalistas — quase todas oriundas dos Estados Unidos. Isso significa que tal setor recebe apoio em seus estágios iniciais para validação de seu MVP e amadurecimento de seu produto inicial, mas não consegue atrair grandes nomes de venture capital.

Há dois pontos a serem destacados aqui: o primeiro é a Learn Capital, que investe unicamente em startups do setor educacional. O segundo é a Start-Up Chile, programa de aceleração financiado pelo governo chileno. Curiosamente, embora a iniciativa tenha sido criada para acelerar empresas da América Latina, apenas uma das quatro startups aportadas está baseada neste continente (a argentina Coderhouse).

Preparando-se para preencher a lacuna

Robson Amicio
Aluno Cisco
Estudante

O que lhe levou a participar do programa CiberEducação Cisco Brasil?

Meu contato com o programa CiberEducação Cisco Brasil ocorreu através da faculdade. Sou estudante do quarto semestre de análise e desenvolvimento de sistemas pela FATEC São Caetano do Sul — Antonio Russo. Durante o desenvolvimento de um projeto de iniciação científica voltado à IoT e smart environments no qual trabalhava em uma solução de monitoração e advisoring para eficiência energética, passei a ter contato com assuntos relacionados à segurança de redes e vulnerabilidades em dispositovos de IoT.

Na mesma época surgiu a oportunidade de realizar o curso para certificação CyberOps Associate da Cisco, e assim foi meu primeiro contato com o programa. Após isso, me tornei frequentador assíduo da plataforma Networking Academy, também da Cisco, onde cursei/estou cursando diversos cursos nas áreas de cibersegurança, redes e programação.

Como você avalia os conteúdos educacionais do programa?

Os conteúdos da Cisco são de altíssimo nível técnico e o mesmo se pode dizer dos instrutores. Os conteúdos são sempre atualizados e permitem que o profissional, mesmo após formado, possa usufruir de programas de reciclagem e atualização.

Além disso, sempre há o direcionamento para conteúdos externos de grande relevância e reconhecimento no mercado, como as organizações profissionais e estudantis de pesquisa e desenvolvimento em cibersegurança, no caso. Todos os cursos da Cisco dos quais participei contam ainda com excelentes labs que permitiram a prática dos conteúdos ministrados.

Um ponto muito importante é que a Cisco disponibiliza todos os conteúdos em português, apesar do idioma inglês ser extremamente necessário no mundo de segurança cibernética, há a preocupação com jovens profissionais que ainda não tenha tal skill.

Você acredita que o programa impulsionou a sua colocação no mercado de trabalho?

Sim, sem dúvidas. Eu tinha a necessidade de rápida entrada no mercado, pois estou em um processo de mudança de área de atuação, e nesse contexto me programei financeiramente para iniciar uma nova faculdade, o que fiz em julho de 2020.

Portanto eu tinha um limite financeiro de suporte e esse limite contemplava a necessidade de conseguir um estágio e, posteriormente, um vaga efetiva para equalização financeira.

Meu contato com o de CiberEducação Cisco Brasil ocorreu no final do segundo semestre de 2020 (primeiro semestre da faculdade) e em abril de 2021 eu consegui minha oportunidade de estágio na Tempest Security Intelligence, empresa especializada em cibersegurança. Sete meses após o início do estágio fui efetivado como analista de segurança.

Posso afirmar que a aprovação no processo seletivo foi totalmente relacionada aos conteúdos técnicos aprendidos no programa e o bom desempenho tem ligação direta com o conceitos e postura de segurança ministrados, além do aprendizado contínuo na Networking Academy.

Como você avalia o atual cenário de capacitação de profissionais de segurança cibernética no Brasil?

Temos excelentes cursos de capacitação na área, especialmente aqueles que têm a iniciativa e participação da comunidade de cibersegurança. Contudo, reais programas de formação, como o CiberEducação Cisco Brasil, ainda são raros. É importante ressaltar que o profissional de segurança cibernética atua em uma infinidade de subáreas, portanto, é necessário conhecer de muitos assuntos diferentes, dentre os quais podemos citar superficialmente redes de computadores, frameworks de segurança e legislação etc., ou seja, há uma vastidão de conhecimento que precisa ser preenchida.

Nesse sentido, programas de formação completa levam em consideração tais necessidades, muitas vezes não supridas por cursos pontuais oferecidos nas plataformas de cursos mais conhecidas, apesar de serem de qualidade, como disse anteriormente, mas que são essenciais para a formação de profissionais que vão começar a atuar no nível 1 da carreira e que são justamente os profissionais mais requisitados pelo mercado atualmente, onde há um déficit enorme entre o número de vagas e a quantidade de colaboradores capacitados disponíveis.

Além do contexto do mercado profissional, é muito importante lembrarmos que o espaço cibernético é considerado como a quinta dimensão do conflito geopolítico, ou seja, há tempos a capacitação de profissionais para atuar na defesa do espaço cibernético tornou-se assunto estratégico e de defesa. O Brasil tem realizado exercícios e tido iniciativas muito interessantes e efetivas, como o exercício Guardião Cibernético, mas ainda há muita necessidade de formação de profissionais de base. Por isso iniciativas como a do programa de CiberEducação Cisco Brasil são realmente importantes.

Preparando-se para preencher a lacuna

Robson Amicio
Aluno Cisco
Estudante

HACKTHEBOX

Local
Folkestone, Inglaterra

Ano de Fundação
2017

Público
B2C/B2B

Investimento Recebido
US$ 11,9 milhões

Investidores
Paladin Capital, Osage University Partners, Brighteye Ventures, Marathon Venture Capital

Sobre

A britânica Hack The Box se auto-intitula como "um playground massivo para hacking". Adotando o formato de fomento à comunidade, trata-se de uma plataforma completa que inclui conteúdos educacionais, laboratórios para a prática de testes de intrusão, campeonatos CTF.

Embora tenha apenas quatro anos de idade, a startup já conseguiu renome internacional pela alta quantidade de conteúdo ofertado (novos materiais são adicionados semanalmente) e pelo realismo de seus laboratórios digitais.

Também chama atenção o fato de que a Hack The Box conta com elementos de gamificação (possuindo até mesmo um ranking global de melhores alunos) e serviços específicos para empresas e universidades, que podem contratar projetos sob demanda para seus funcionários ou alunos.

Trata-se atualmente da startup de capacitação em cibersegurança com o segundo maior volume de aporte recebido a nível global. Seu mais recente investimento recebido foi de US$ 10,6 milhões em Series A em abril de 2021.

CYBRARY

Local
Greenbelt, EUA

Ano de Fundação
2015

Público
B2C

Investimento Recebido
US$ 23 milhões

Investidores
Inner Loop Capital, New Stack Ventures, Arthur Ventures, Blu Venture Investors, Baltimore Angels, Loop Capital, BuildGroup, Gula Tech Adventures

Sobre

Acima da Hack The Box, só mesmo a Cybrary, fundada em 2015 na cidade de Greenbelt, nos Estados Unidos. Já em Series B, seu mais recente aporte foi de US$ 15 milhões em novembro de 2019; em seis anos de existência, a startup acumula US$ 23 milhões em investimentos recebidos.

Seu diferencial é oferecer cursos online que abrangem todos os níveis de conhecimento: é possível encontrar desde programas para iniciantes até materiais preparatórios para quem deseja obter alguma certificação tradicional do setor, como a Certified Information Systems Security Professional (CISSP) e CompTIA Security+.

Além de usufruir de aulas gravadas em vídeo que podem ser assistidas sob demanda, os alunos também contam com laboratórios digitais para praticar seus novos conhecimentos e um time de mentores que estará à sua disposição através de um ambiente hospedado na plataforma Slack.

É possível ter acesso limitado aos cursos da Cybrary de forma gratuita; quem deseja conseguir mais materiais precisa pagar uma taxa mensal ou anual.

UDACITY

Local
Mountain View, EUA

Ano de Fundação
2011

Público
B2C

Investimento Recebido
US$ 238 milhões

Investidores
Charles River Ventures, Andreessen Horowitz, Bertelsmann, Drive Capital, GV, Baillie Gifford, Emerson Collective, Valor, Hercules Capital, Recruit Strategic Partners, Carriage House Rock, SharesPost 100 Fund, Cox Enterprises, DT Unicorn Fund, InvestX, Big Sky Opportunities Fund, Steve Blank, K20 Fund

Sobre

Única unicórnio no setor de edtechs focadas no mercado de TI, a Udacity se transformou em uma velha conhecida até mesmo pelos brasileiros. A startup fundada em 2011 já conseguiu captar US$ 238 milhões, sendo que, deste montante, US$ 105 milhões foram aporte já em estágio Series D.

Seu diferencial é oferecer "nano-graduações" online, ou seja, cursos que teoricamente possuem a mesma qualidade de uma graduação tradicional, mas com um investimento de tempo muito menor. Vários desses programas contam com o apoio de gigantes como Google, NVIDIA e Autodesk.

Na área de cibersegurança, a Udacity possui seis programas distintos, variando de acordo com o nível de conhecimento do aluno: "Introdução à Cibersegurança", "Analista de Segurança", "Engenheiro de Segurança", "Segurança Corporativa", "Arquiteto de Segurança" e "Hacker Ético".

Também chama atenção os programas de nano-graduação em computação na nuvem, que sabemos ser uma área de conhecimento um tanto requisitada no setor de segurança da informação ao longo dos últimos anos.

codecademy

Local
Nova Iorque, EUA

Ano de Fundação
2011

Público
B2C

Investimento Recebido
US$ 82,5 milhões

Investidores
Union Square Ventures, Prosus, Owl Ventures, Kleiner Perkins, Index Ventures, SV Angel, Founder Collective, Naspers, Flybridge Capital Partners, Y Xombinator, Thrive Capital, Initialized Capital, Collaborative Fund, CrunchFund, Social Capital, Bloomberg Beta, O'Reilly AlphaTech Ventures, Bowery Capital, Ascolta Ventures

Sobre

Considerada uma "Soonicorn" (startup que possível se tornará um unicórnio dentro dos próximos anos), a Codecademy já angariou US$ 82,5 milhões , sendo que seu mais recente aporte ocorreu em janeiro deste ano, em Series D, no valor de US$ 40 milhões.

Foca-se em cursos de programação, oferecendo programas para quem deseja aprender diferentes linguagens: Python, JavaScript, Java, SQL, Bash/Shell, Ruby, C++, R, C#, PHP, Go, Swift e Kotlin, além das linguagens de marcação HTML e CSS. É possível estudar pela web ou pelo aplicativo oficial disponível para Android e iOS.

Há também opções de cursos focados na disciplina de segurança da informação. O mais simples, com apenas duas aulas, é o "Introdução em Cibersegurança"; alunos avançados têm à sua disposição os programas "Protegendo Aplicações Express", "Autenticação & Autorização de Usuário em Express" e "Defendendo Aplicações Node contra Injeções SQL, XSS & Ataques CSRF".

É possível aproveitar a maioria dos conteúdos de forma gratuita, com possibilidade de assinar um plano Pro para ganhar mais privilégios.

Tendências

"Skills, not degrees"

Ficou bem claro, através das entrevistas e estatísticas apresentadas ao longo deste relatório, que não existe um "caminho das pedras" para a capacitação do futuro profissional de cibersegurança. Esta figura é formada por **uma série de conhecimentos e soft skills que não necessariamente serão adquiridas em determinado curso de graduação em uma faculdade convencional**, mas sim através de uma série de estudos e práticas combinadas — além de, claro, um interesse nato em tecnologia da informação.

Tal como nos últimos anos, esta edição do estudo da (ISC)² ressaltou que, para diversos profissionais já alocados no mercado de trabalho, essa série de habilidades não-técnicas são críticas para que entrantes no segmento tenham sucesso em suas carreiras, sendo tão ou mais valorizadas do que certificações tradicionais. Por conta disso, **as empresas precisam repensar seus critérios antiquados de avaliação na hora de contratar mão-de-obra**.

Entre as características desejadas para um profissional de cibersegurança, podemos destacar **fortes habilidades de resolução de problemas, ânsia por aprender mais, excelente comunicação interpessoal e uma mentalidade altamente estratégica**.

Certificações introdutórias

Usadas como demonstrativo dos conhecimentos técnicos do profissional de segurança cibernética, as certificações da área são amplamente respeitadas e procuradas, sendo críticas como diferenciais no currículo para os candidatos à uma vaga de emprego. Atualmente, segundo o (ISC)², as certificações mais procuradas em 2021 são:

- **(ISC)² Certified Cloud Security Professional (CCSP)**
- **ISO 27001 Lead Implementer**
- **BS 7799**
- **Cisco Cyber Security Specialist (SCYBER)**
- **Cisco Certified Network Professional Security (CCNP Security)**

Porém, visto que a maioria dessas certificações são um tanto difíceis de se conseguir, a (ISC)² anunciou, em outubro deste ano, planos para criar uma certificação introdutória para profissionais de nível júnior. Ela se posicionaria abaixo da atual graduação mais baixa do consórcio, a CISSP.

Pesquisas concluem que há uma escassez global de profissionais de segurança cibernética qualificados. Embora existam muitos fatores contribuintes, acreditamos que uma solução é criar uma certificação que permita aos candidatos — incluindo estudantes, jovens profissionais e pessoas mudando de carreira — demonstrarem aos empregadores sua familiaridade com os conceitos básicos de segurança cibernética", explicou o órgão.

Home office e outras disrupções no modelo de trabalho

Como citado na introdução deste report, a crise do novo coronavírus aumentou ainda mais a quantidade de profissionais trabalhando em regime remoto. Mesmo com a pandemia se tornando mais branda, as empresas perceberam os benefícios desse modelo e a tendência é uma adoção global de um formato híbrido, no qual os colaboradores se deslocam até o escritório apenas se desejarem.

Pode não parecer, mas essa disrupção também causa impactos positivos na remediação do apagão de talentos. "A mudança global para o trabalho remoto para muitas organizações impactou os profissionais de segurança cibernética de várias maneiras. Primeiro, eles aprenderam a trabalhar em casa, assim como outras pessoas em suas organizações. Em segundo lugar, eles tiveram que enfrentar novas ameaças e superfícies de ataque mais amplas que adicionaram uma nova dimensão a seus trabalhos já desafiadores", explica o (ISC)².

"Apesar dessas novas ameaças, **os participantes citaram vários benefícios de trabalhar remotamente, incluindo laços mais fortes entre as equipes, um renovado senso de missão e uma melhor comunicação**. Quando questionados sobre o que sua organização poderia fazer para ajudar a resolver sua própria lacuna de habilidades, os participantes citaram condições de trabalho flexíveis", complementa o estudo do consórcio.

Também é importante observar que o trabalho remoto abre portas para endereçarmos os problemas de diversidade dentro do mercado de trabalho — estima-se que, de toda a força de trabalho dos EUA e do Reino Unido, 76% é representada pelo sexo masculino e 72% são caucasianos. **As mulheres ainda somam apenas 25% da força global de trabalho**.

"Quando possível, as organizações devem adotar totalmente o trabalho remoto para suas equipes de segurança cibernética. Muitos profissionais de segurança cibernética desejam continuar trabalhando remotamente, mas o mais importante é que o trabalho remoto permite que as organizações criem uma rede muito mais ampla geograficamente durante o recrutamento, o que também promove um grupo mais diversificado de candidatos", concluem os especialistas da (ISC)².

Uma luta que precisamos lutar juntos

Ficou bem claro que o apagão de talentos global no mercado de segurança cibernética é um problema que possui diferentes fatores contribuintes, e é justamente dessa "mistura" de parcelas de culpa que surge a complexidade em resolver tal questão. Vamos ressaltar alguns pontos.

- Embora o Brasil conte com uma grande quantia de cursos acadêmicos em segurança da informação, a grade curricular costuma ser um tanto genérica e incompleta, não preparando o aluno para os desafios da vida real;
- Ao mesmo tempo, tanto no Brasil quanto no resto do mundo, falta interesse no investimento (especialmente de corporate venture capital) em plataformas que oferecem educação online especializada em cibersegurança;
- A hipervalorização de certificações de renome do mercado por parte dos contratantes acaba afastando muitos entrantes que, embora tenham soft skills adequadas, não possuem condições socioeconômicas para conquistá-las;
- Por falar em soft skills, os contratantes precisam urgentemente colocá-las um nível acima em sua lista de prioridades na hora de avaliar candidatos para uma posição, em vez de privilegiar formações acadêmicas;
- Por fim, os candidatos precisam se condicionar a entender as tendências do mercado e se manter devidamente preparados com novos conhecimentos, seja através de graduações formais ou cursos de plataformas alternativas.

Caçando talentos escondidos

Também é interessante lembrar que, hoje, as empresas possuem um novo canal muito interessante para encontrar talentos "perdidos" e que possuem as skills (soft e técnicas) para cumprir sua função no meio corporativo, mas, por algum motivo, ainda não estão inseridos no mercado de trabalho: as plataformas de bug bounty.

Vimos aqui dois excelentes exemplos: a nacional Hackaflag e a norte-americana Hack The Box. Ambas promovem campeonatos, desafios gamificados e uma plataforma de caça de vulnerabilidades que, mais do que resultar na identificação de uma outra falha de segurança nos seus sistemas, também pode revelar um futuro profissional precioso para a sua equipe interna de segurança da informação.

No fim das contas, **ao falarmos do gap na força de trabalho global em cibersegurança, estamos falando de uma batalha que precisamos lutar juntos** — com cada ator fazendo devidamente o seu papel de investir, educar, aprender, praticar e recrutar de acordo com o que o mercado necessita. Trata-se de um esforço conjunto no qual, em um futuro breve, todos nós sairemos ganhando.

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.

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.

Categorias

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.

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.

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.

Corporates members

APOIO

inside Cybertech Report