O avanço dos ataques cibernéticos

Sua opinião é muito importante!

Sua opinião é muito importante para o Distrito. Por isso, queremos saber quais foram as suas impressões, críticas e sugestões sobre este relatório. Além disso, gostaríamos de saber quais outros estudos você gostaria que o Distrito Dataminer realizasse.

Quer falar com a gente? É só encaminhar um e-mail para: inside@distrito.me

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

Marcelo Bezerra
Executivo Sênior
Cisco

Josemando Sobral
Co-Founder
Unxpose

Pedro IVO
CEO
PhishX

Marcos Sêmola
Co-Founder
EY

Introdução

Introdução

No Inside Cybertechs #4, focamos em compilar um pouco do que trazemos nos últimos reports e focar especificamente nas ameaças cibernéticas que estão ameaçando os empreendimentos no Brasil e no mundo. O país foi o mais afetado na América Latina por ciberataques e um dos principais alvos no mundo, dessa forma o Distrito destaca algumas startups que estão dentro do ecossistema que estão na luta diária contra os crescentes crimes cibernéticos.

LGPD, Blockchain e temas futuros a serem abordados no Inside Cybertech estão sempre focados em proteger as empresas de criminosos cada vez mais habilidosos que se aproveitam de falhas para conseguir informações sigilosas, destruir arquivos e, quando não, paralisar por completo sistemas utilizados dentro das organizações. Nesse sentido, além de trazer um panorama atualizado do ecossistema das startups de Cyber, são destacados alguns cases e entrevistas de especialistas do mercado de cibersegurança que abordam as principais ameaças, o combate à elas, como o Brasil está frente a um panorama internacional e quais são os próximos passos.

Por fim, o relatório traz algumas tendências para o setor, com o intuito de entender como o ecossistema de inovação irá ser parceiro na luta diária contra os ciberataques.

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!

Ecossistemas Cybertechs

Highlights

223
Startups

US$ 395M
Investimento recebido desde 2013

14
Categorias

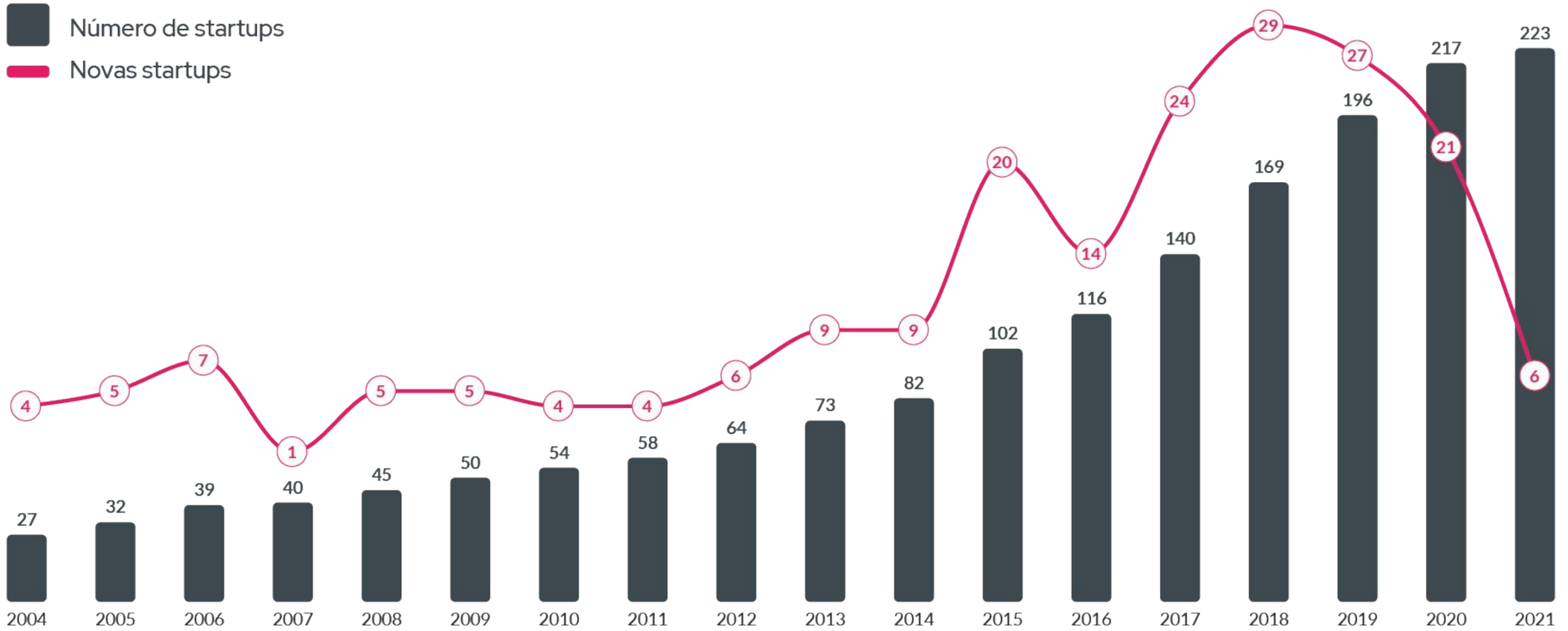
US$ 287M
Investimento recebido nos últimos 2 anos

7.200
Funcionários empregados

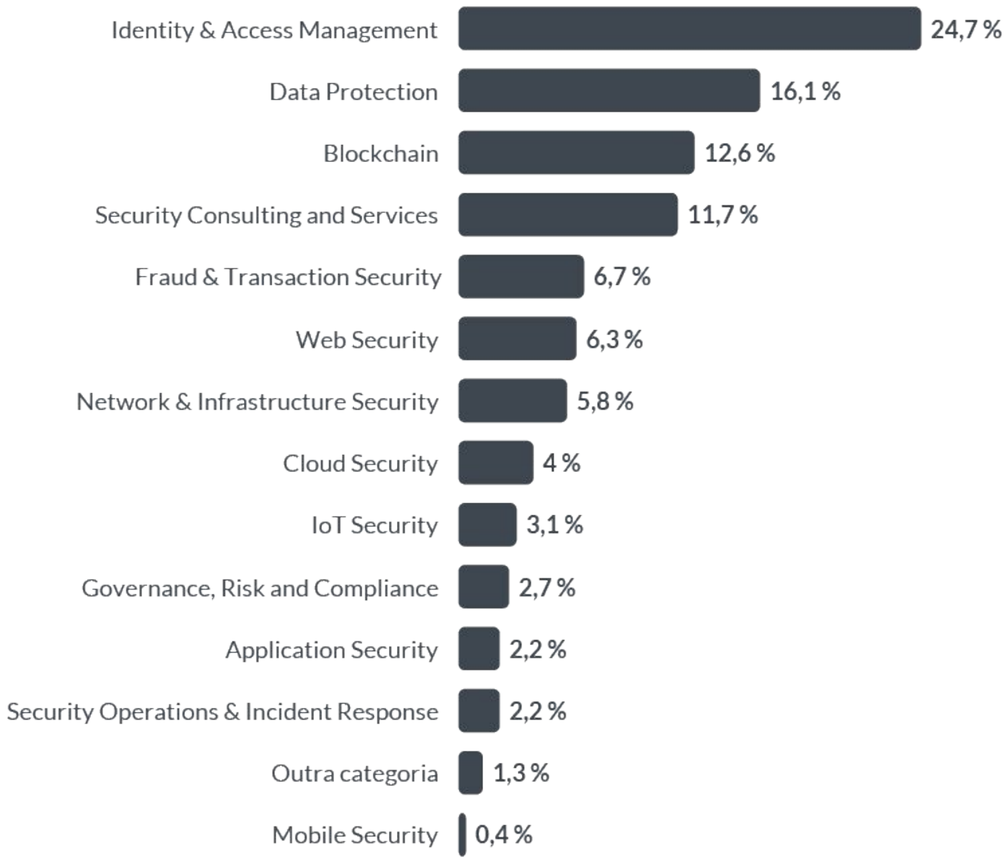
11
M&A's desde 2012

41
Startups com investimento recebido

Evolução Cybertechs



Divisão Cybertechs por categoria



CATEGORIAS	REPRESENTATIVIDADE
Identity & Access Management	24,7%
Data Protection	16,1%
Blockchain	12,6%
Security Consulting and Services	11,7%
Fraud & Transaction Security	6,7%
Web Security	6,3%
Network & Infrastructure Security	5,8%
Cloud Security	4,0%
IoT Security	3,1%
Governance, Risk and Compliance	2,7%
Application Security	2,2%
Security Operations & Incident Response	2,2%
Outra categoria	1,3%
Mobile Security	0,4%

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, PHISHX, Privacy tools, PRIVALLY, riskex, SAFE WAY, senhasegura, SENSR., Simply., ST3TAILOR

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 · SVA TECH · T-SHIELD · acesso digital

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 · 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 · <u> · XLabs ON SECURITY · SITE BLINDADO · Gatefy · UPX TECHNOLOGIES · XLabs

Ameaças cibernéticos

Contexto e Panorama Nacional

Ataques cibernéticos cresceram globalmente na pandemia

Com o avanço da vacinação no mundo e a retomada das economias depois de uma queda do PIB global, muitas organizações voltaram a algumas rotinas praticadas antes da pandemia. Entretanto, com a aceleração da transformação digital em muitas empresas e a consolidação do home-office ou regime híbrido de trabalho, a volta completa aos padrões antes da pandemia é praticamente impossível. Nesse contexto, criminosos cibernéticos continuam explorando os principais fatores de risco dentro das organizações, atacando supply chains e brechas dentro da rede para atingir seus objetivos

Embora a transformação digital acelerada tenha trazido diversos benefícios para as empresas, globalmente **ataques do tipo ransomware subiram 93% no ano de 2021**, e essas investidas ficaram cada vez mais complexas. As ameaças bem sucedidas estão implementando uma técnica de extorsão dupla, que além de roubar dados sensíveis das organizações e exigir resgates milionários em cripto para devolver as informações, estão também mirando clientes e parceiros das empresas, exigindo contrapartidas financeiras de ambas partes.

No mundo todo, o volume de ataques ransomware só no primeiro semestre de 2021 já ultrapassou a soma do ano passado inteiro, e o **Brasil foi o quinto país mais atingido, com 9,1 milhões de ataques** registrados, ficando atrás apenas de Estados Unidos, Reino Unido, Alemanha e África do Sul. Apenas em junho desse ano, globalmente foram registrados mais de 78 milhões de ataques.

É nesse cenário que estimativas da Cybersecurity Ventures afirmam que crimes cibernéticos vão custar às empresas no mundo tudo cerca de US$ 10,5 trilhões anualmente até 2025. Além disso, com uma taxa de crescimento de **15% ao ano, crimes cibernéticos representam a maior transferência de riqueza de toda a história da humanidade**, e não existem indícios que esse volume irá reduzir.

Assim, como exposto em edições anteriores do Inside Cybertechs, as organizações estão investindo cada vez mais em soluções de cybersecurity, que é um requisito básico para um bom funcionamento de uma companhia sem tomar grandes riscos. Destaca-se que cerca de 43% dos ciber ataques são direcionados para pequenas empresas, entretanto somente 14% afirmam estar preparadas para lidar com essas ameaças. Em 2016, foi registrado um ataque Ransomware a cada 40 segundos, **já em 2021 esse número foi reduzido para 11 segundos**.

Independente do tipo de ameaça cibernética que afeta uma organização, um ataque desse tipo pode trazer perdas financeiras para empresa, perda ou impossibilidade de produtividade por tempo indeterminado, danos à reputação, danos legais e problemas na continuidade de diversas parcerias. Assim, globalmente nos próximos 3 anos a EMBROKER destaca que o **orçamento destinado para cybersecurity deve crescer cerca de 71%**, de acordo com a necessidade das organizações.

Ransomware se destaca como principal ameaça, mas existem outras

Muito se fala em ransomware como principal ameaça cibernética em ascensão no mundo, e não é por acaso. No Brasil, ataques do tipo ransomware afetaram algumas grandes corporações brasileiras durante a pandemia, e em 2021 o número de ocorrências subiu cerca de 92%. Os principais setores mais afetados foram educação, saúde e varejo, e o prejuízo dessa ameaça globalmente atingiu US$ 20 bilhões. Esse tipo de investida entrou para história como o primeiro ataque a causar uma morte, quando em um hospital alemão todos os sistemas foram paralisados e uma paciente não resistiu por não poder ser atendida. Essas e outras evidências indicam que essa modalidade de ciberataque será a principal ameaça digital nos próximos anos.

Entretanto, é necessário destacar que existem uma série de outros ataques cibernéticos que também causam danos consideráveis àqueles afetados, e que precisam serem divulgados e adereçados de maneira correta. Alguns exemplos como:

Phishing: Envio de mensagens fraudulentas que parecem ser inofensivas e seguras, geralmente por e-mail. O usuário pode preencher informações sensíveis ou dar acesso aos invasores para roubar dados pessoais, muito utilizado para conseguir informações de cartão de crédito, por exemplo;

Injeção de SQL: Inserção de um código malicioso em um servidor que se utiliza de SQL (onde geralmente estão diversas informações de uma organização) para revelar informações sensíveis;

Ataque de negação de Serviço (DDoS): Provoca a saturação dos sistemas, servidores e redes de tráfego para esgotar os recursos e a largura de banda . Dessa forma, o sistema fica inutilizável.

Claro, além do ransomware temos outros **malwares** (softwares maliciosos), que se aproveitam da vulnerabilidade da rede, como Bots, Worms, Spywares, Adwares e o famoso cavalo de tróia.

Além dos citados, existem inúmeras outras formas de ataques cibernéticos, como man-in-the-middle, zero-day, encapsulamento do DNS, e várias outras. Dessa forma, quando se pensa em uma estrutura de segurança e proteção dentro das organizações, é necessário ter em mente todos os possíveis ciberataques passíveis de acontecer. Quando se pensa em contratação de produtos de cibersegurança e detecção de ameaças cibernéticas, a solução deve compreender todos os pontos de brecha, para mitigar radicalmente a possibilidade de qualquer invasão do sistema.

O avanço dos ataques cibernéticos dentro das corporações

Marcelo Bezerra
Executivo Sênior
Cisco

O mundo observa nos últimos anos um avanço de uma série de ameaças cibernéticas, que em escalas distintas ameaçam o bom funcionamento da nova economia digital. Como a Cisco vê esse movimento e quais são as principais preocupações que os agentes econômicos devem estar atentos?
Esse é um movimento natural do crime organizado, acompanhando o movimentos dos agentes econômicos na digitalização dos negócios, além dos rentáveis mercados criminosos digitais, como o criptomining e o ransomware, e outros. O principal ponto a estar atento é que, diferente do passado, não há mais alvos típicos das ações criminosas. Todas as empresas, de todos os tamanhos e segmentos, são alvos, seja para rentabilizar algum negócio paralelo (como é o caso típico do criptomining) seja para o pagamento de resgate do ransomware, ou para quaisquer outras ameaças.

Outro ponto é que os criminosos digitais estão continuamente aperfeiçoando suas técnicas, ou buscando novas técnicas a serem alugadas de outros grupos, o que forma outro mercado extremamente rentável. Dessa forma, qualquer criminoso tem acesso fácil a malware extremamente sofisticado. As empresas precisam avaliar continuamente se sua segurança está em linha com as tecnologias mais recentes em uso pelos criminosos digitais.

Durante a pandemia, crimes cibernéticos cresceram muito globalmente em comparação a médias históricas anteriormente datadas. Sabemos que o trabalho remoto e mais pontos de acesso para criminosos são um ponto principal nesse aumento, mas com a volta gradual à normalidade, devemos esperar que os cibercrimes continuem em patamares elevados?
Os criminosos digitais são hábeis em identificar novos vetores de ataque e se aproveitar deles. O trabalho remoto é apenas um, e a velocidade de adoção no início da pandemia levantou questões das medidas de segurança adotadas. Dessa forma, as quadrilhas apenas aproveitaram a oportunidade, como continuarão a aproveitar qualquer oportunidade que surja, seja o trabalho híbrido ou alguma nova tendência. É preciso entender que assim como a digitalização provê condições mais eficientes para as empresas fazerem seus negócios, ela provê condições mais eficientes para os criminosos realizarem suas ações. O crime cibernético sempre continuará em patamares elevados, tal qual outros crimes, não digitais, rentáveis. →

→ Quais são as principais ameaças cibernéticas que você destacaria em 2021? E para os próximos 10 anos?
Para fins estatísticos podemos dizer que o ransomware está sendo a principal ameaça em 2021. No entanto, para fins de segurança digital, é um grande erro destacar uma ameaça cibernética em detrimento da outra, porque o fato de uma ameaça ter sido a mais comum em um ano não significa que continuará sendo no ano seguinte, ou mesmo no mês seguinte. Os criminosos são oportunistas e podem variar seu ataque a qualquer momento. O ransomware é um ataque em que o criminoso irá criptografar o computador para pedir resgate, mas para chegar a esse intento o criminoso pode usar centenas de técnicas e malware diferentes. Um ataque pode ser completamente diferente do outro. Além disso, algo que pareça ser um ransomware pode ser na verdade um ataque de exfiltração de dados.

Dessa forma, as empresas necessitam ficar alertas para quaisquer indícios de ação suspeita ou maliciosa em sua rede, aplicações, dispositivos e computadores; sem se importar em nomear a atividade, pois no fim serve apenas para fins estatísticos. Nesse sentido, é completamente impossível dizer a principal ameaça nos próximos 10 anos. Será o que estiver funcionando para os criminosos ganharem dinheiro.

O Brasil vem subindo de patamar nos rankings internacionais de cibersegurança nos últimos anos, e com o avanço da LGPD no país, privacidade de dados e segurança da informação são temas que as empresas precisam se atentar cada vez mais. Como o Brasil se compara no mercado internacional no combate às ameaças cibernéticas? As perspectivas de longo prazo são positivas?
O Brasil possui setores extremamente avançados em segurança digital, como financeiro e telecomunicações, e outros mais atrasados, como elétrico e abastecimento. O desenvolvimento da segurança digital nesses setores irá acompanhar a sua digitalização nos negócios. O país possui a capacidade humana e tecnológica para tal, e a LGPD acabou contribuindo por uma maior maturidade das empresas e instituições. Nesse mês, sob liderança do Comando de Defesa Cibernética – COMDCIBER, 350 integrantes das Forças Armadas e de 65 empresas dos setores de Finanças, Telecomunicações, Transporte, Energia Nuclear, Elétrico, Águas e Defesa, realizaram durante três o maior exercício de defesa cibernética do hemisfério sul, o Exercício Guardião Cibernético 3.0. O evento contou com o apoio da Cisco em parceria com o Senai.

A longo prazo o grau de maturidade e preparação das empresas só tende a aumentar, acompanhando o desenvolvimento da economia digital no Brasil.

Como a Cisco está trabalhando para conscientizar seus clientes para garantir pequenas políticas que ajudam na segurança da informação?
A Cisco possui um dos maiores programas de educação tecnológica do Brasil – o Networking Academy. Disponível para qualquer pessoa, de qualquer lugar, o programa fornece capacitação tecnológica em diferentes áreas do conhecimento, incluindo segurança digital. ◉

O avanço dos ataques cibernéticos dentro das corporações

Marcelo Bezerra
Executivo Sênior
Cisco

Como o Brasil está enfrentando os criminosos cibernéticos, e o que fazer para evitar ataques?

No Brasil, como destacado no Inside Cybertech #3, a LGPD e ascensão dos ataques cibernéticos ligaram um alerta das empresas brasileiras para um maior investimento em cibersegurança. Além disso, a ascensão das startups de cibersegurança no Brasil é um movimento novo, e essas empresas estão sendo procuradas pelo mercado para solucionar problemas de segurança da informação que são cada vez mais necessários .

Soluções de monitoramento de ameaças cibernéticas, proteção de redes, proteção de dispositivos, cloud security, proteção de dados e identity centric solutions têm ganhado cada vez mais espaço no mercado, o que ajudam empresas a combaterem todas as facetas das ameaças cibernéticas. Obviamente existe um grande apoio das grandes corporações de segurança da informação, como a Cisco, que fornecem soluções completas de estrutura em cibersegurança, e se beneficiam do ecossistema de inovação que cada vez mais traz atenção ao tema.

Cybersecurity, como já foi bem destacado, precisa estar em presentes em todos os setores produtivos da economia e com um investimento pesado, principalmente pela ascensão das ameaças cibernéticas no país e no mundo, como descrito nas anteriormente.

Setores muito visados por criminosos cibernéticos

Indústria

Indústrias transformadoras e energéticas foram muito visadas para ataques em 2020

Saúde

Ataques no setor subiram 715% na comparação entre 2019 e 2020 globalmente

Educação

478 instituições de ensino latino-americanas sofreram invasões no primeiro semestre de 2020

Agronegócio

84% dos produtores utilizam tecnologia, por ser um setor altamente lucrativo, é altamente visado por criminosos

‹unxpose›

Categoria
Web Security

Local
São Paulo, São Paulo

Ano de Fundação
2020

Público
B2B

Investidores
Canary, Norte Ventures

Sobre

A Unxpose é uma startup que disponibiliza alguns serviços de cybersegurança. Dentre eles estão, descoberta de ativos digitais, correções de vulnerabilidade, monitoramento de falhas de segurança, priorização inteligente e score de exposição em websites, apps e sistemas de nuvem.

Através de Inteligência Artificial, a empresa é capaz de monitorar em tempo real brechas de segurança e vazamento de informações. Inclusive a IA consegue fazer certas correções nos sistemas automaticamente.

Basicamente, essa startup traz soluções para desmistificar o que é cibersegurança e como implementá-la nas empresas

GAT InfoSec

Categoria
GRC

Local
São Paulo, São Paulo

Ano de Fundação
2020

Público
B2B

Investimento Recebido
R$500 mil

Investidores
NDA Capital

Sobre

A GAT InfoSec foi fundada no começo de 2020 e presta diversos serviços relacionados a cibersegurança. Seus produtos e serviços incluem de maneira geral avaliação da segurança, painéis de gestão e monitoramento de segurança. Inclusive, a empresa atende também riscos relacionados ao fator humano.

Ademais, recentemente a empresa está apostando em estratégias relacionadas com outros aspectos ligados ao tema através de um canal de parcerias, por exemplo pontes com escritórios de advocacia que ganham espaço nesse mercado, tendo em vista questões como a LGPD e normas de órgãos reguladores.

A GAT se enquadra na categoria de Governança, Risco e Compliance, como uma plataforma que atua nessas diferentes frentes e entregando valor para o cliente de diversas formas.

PHISHX

Categoria
Data Protection/ Peoople Centric Security

Local
São Paulo, SP

Ano de Fundação
2016

Público
B2B

Investidores
ACE Startups

Sobre

A PhishX é uma plataforma SaaS de Cibersegurança que foi desenvolvido para empresas que buscam treinar e educar seus funcionários sobre segurança cibernética, protegendo o ambiente corporativo contra ataques.

Através de APIs, a startup simula ataques cibernéticos, disparando aos colaboradores emails com mensagens maliciosas, simulando ataques de phishing — ataques virtuais em que conteúdos maliciosos induzem o usuário a clicar em links, abrir anexos e instalar aplicativos a fim de capturar informações confidenciais das companhias. A plataforma da PhishX é conectada à ferramentas das empresas para obter acesso aos emails dos colaboradores e medir o nível de resposta.

A empresa se considera como uma startup de People Centric Security, uma categoria que diz respeito a soluções que focam em tratar a segurança cibernética, colocando as Pessoas no Centro.

///AXUR

Categoria
Security Operations & Incident Response

Local
Porto Alegre, Rio Grande do Sul

Ano de Fundação
2008

Público
B2B

Investidores
DGF Investimentos

Sobre

A Axur é uma startup gaúcha de monitoramento e reação a riscos digitais, visando preservar a imagem e relação de empresas com seus clientes. Entre os riscos monitorados estão: apropriação de identidade, phishing, aplicativos fraudulentos e vendas não autorizadas. Assim, a Axur protege o consumidor durante toda a jornada de compra e nas experiências de contato digital com as marcas.

A empresa oferece uma gama de serviços ligados à fraudes digitais, vendas abusivas, presença digital, inteligência de ameaças, vazamento de dados e ameaça a executivos.

Com o uso de inteligência artificial, vasculham a internet em busca de fraudes e simulam o comportamento online de consumidores das marcas buscando encontrar ameaças antes de ferirem os consumidores e a marca.

Hoje, a startup tem grandes corporações nacionais como clientes, entre elas estão Azul, NuInvest, Méliuz, Porto Seguro, Natura, Via, entre muitas outras.

As startups na luta contra ataques cibernéticos

Josemando Sobral
Co-Founder
Unxpose

Sabemos que o Brasil, seguindo uma tendência mundial, tem sofrido bastante com ameaças cibernéticas. Qual a importância da solução da Unxpose dentro das empresas para garantir que as organizações fiquem cada vez mais protegidas?
Unxpose chega para cobrir essa lacuna com uma proposta de democratizar o acesso à cibersegurança, especialmente para Startups e PMEs, e o faz a partir de 2 importantes pilares: automatização e simplicidade. A solução funciona como um braço adicional no time ao monitorar ativos expostos 24/7 e identificar falhas de segurança e vazamentos de dados, priorizar essas falhas, avisar sobre aquilo que é crítico e deve ser visto primeiro, e atuar na correção delas por meio de passo a passos simples — tudo de forma contínua e automatizada.

A Unxpose nasce da junção muito interessante: eu, que sou Founder e CEO, já fui CTO e conheço de perto o dilema de ter um time reduzido e não ter tempo, nem braço para olhar para a cibersegurança, apesar de ela ser um dor constante. Já o Tiago Assumpção e o Patrick Costa, outros 2 founders, são profissionais reconhecidos de cibersegurança que colocam a sua expertise à disposição para automatizar processos de segurança.

Democratizar a segurança digital é importante, pois ela tem impacto direto nos negócios. Além de evitar vazamentos e roubos de dados que podem, de fato, destruir uma empresa do dia para a noite, a segurança tem relação direta com o aumento do valuation de uma empresa. Além disso, ajuda a fazer negócios com grandes organizações, que exigem diligência de segurança de seus parceiros.

Quais são as principais ameaças cibernéticas mais destacadas pelos clientes de vocês? O Brasil se difere do resto do mundo nessa questão, ou os ataques cibernéticos têm acontecido de forma homogênea pelos países?
O Brasil está no TOP 5 de países que mais sofreram ataques de ransomware e isso deve continuar, atingindo também PMEs e Startups. Importante destacar que um atacante procura janelas de oportunidade, independente do tamanho da empresa. Entre as falhas de segurança mais comuns que temos visto estão a exposição de aplicações e sites de uso interno que não deveriam estar expostos na internet, como por exemplo, ferramentas de BI, de integração/entrega contínua (CI/CD) ou até backoffices! Também vemos muitos problemas relacionados à má-configuração de serviços em →

→ provedores de cloud. Essas má-configurações acontecem devido a complexidade inerente aos próprios serviços de nuvem, falta de padronização entre eles e, claro, a exigência de agilidade na entrega de novas funcionalidades pelos times de desenvolvimento. Essas brechas podem expor dados confidenciais da empresa até mesmo de clientes. Um relatório da Netskope de julho/2021 mostrou que mais de 35% dos workloads da AWS, Azure e GCP estão expostos à internet de forma completamente pública. Isso só reforça que é necessário haver um monitoramento contínuo tanto dos ativos expostos da empresa quanto dos serviços de nuvem.

Como empresa de cibersegurança que recebeu aporte, como vocês acreditam que as startups e o ecossistema de inovação como um todo podem ajudar nos principais problemas relacionados aos ataques cibernéticos? Você acredita que um crescimento como um todo no setor de cibersegurança pode ajudar ainda mais no crescimento e nos próximos passos da Unxpose?
Com certeza. Uma pesquisa recente mostrou que apesar de 80,6% das empresas afirmarem dar muita importância para os seus dados, apenas 31% priorizam a área no plano de negócios. O crescimento do setor ajuda a educar o mercado sobre a importância de encarar a cibersegurança como investimento prioritário. Outro ponto importante é que o cibercrime é complexo e tem vários tipos de técnicas. O mercado tem apresentado soluções que buscam proteger empresas respondendo a esses diferentes tipos de crime.

Do mesmo jeito que existem diferentes startups que substituem conta bancária, cartão de crédito, seguros, investimentos, entre outras, estamos vendo o nascimento de startups que atuam em áreas como antifraude, antivírus, e até a Unxpose que atua na proteção da infraestrutura, inclusive da Cloud. Além de também ajudar a educar o mercado sobre a diferença entre essas empresas, a variedade delas aponta para um cenário de maior segurança para fazer negócios.

O que você gostaria de destacar no padrão dos ataques cibernéticos nos últimos 10 anos? Muita coisa mudou em uma década?
Aqui na Unxpose temos visto uma tendência onde o uso de Cloud acaba aumentando a superfície de exposição das empresas e consequentemente os ataques. No início da década passada, os atacantes buscavam descobrir novas vulnerabilidades (as chamadas "zero-days"), hoje eles vão em busca de portas de entradas já conhecidas, porém não monitoradas, e a Cloud é um prato cheio para isso. Isso tem impactado cada vez mais startups e PMEs, que usam massivamente serviços de nuvem, mas não contam com uma infraestrutura de proteção. Infelizmente, elas acreditam que apenas por estarem na Cloud estão seguras, o que absolutamente não →

As startups na luta contra ataques cibernéticos

Josemando Sobral
Co-Founder
Unxpose

→ é verdade. E os atacantes sabem disso. Outra mudança é que o crescimento exponencial de uso das redes sociais, que trouxe junto um volume absurdo de dados pessoais e de comportamento, vem permitindo um uso cada vez mais elaborado de engenharia social. Os atacantes usam as informações disponibilizadas e se fazem passar por outras pessoas.

Além de contar com um sistema de segurança eficaz, que outras medidas as empresas podem tomar para prevenir os ataques?
No mundo pós GDPR e LGPD, a preocupação com a privacidade dos dados é uma realidade de qualquer negócio. Por isso é importante repensar na quantidade de dados que são coletados e se todos são essenciais para o sucesso da empresa. O seu nível de risco é proporcional aos dados que você guarda.

Outra medida é a conscientização dos colaboradores para que eles se tornem agentes de segurança por meio de treinamentos periódicos, e também colocando o tema da cibersegurança nas conversas com os times. É preciso que a segurança seja um tema de toda a empresa.

Além disso, é de extrema importância ter uma boa Política de Segurança da Informação, que estabeleça diretrizes. Mas é importante salientar que ela precisa ser exequível e jogar a favor do negócio. Para isso, é preciso que seja feita a muitas mãos, unindo áreas técnicas e áreas de negócios. Uma PSI é vital para evitar vazamentos e incidentes, protegendo os pilares do seu negócio. ◉

As startups na luta contra ataques cibernéticos

Josemando Sobral
Co-Founder
Unxpose

Ameaças cibernéticas

Panorama Internacional

Qual o panorama brasileiro em comparação ao cenário internacional?

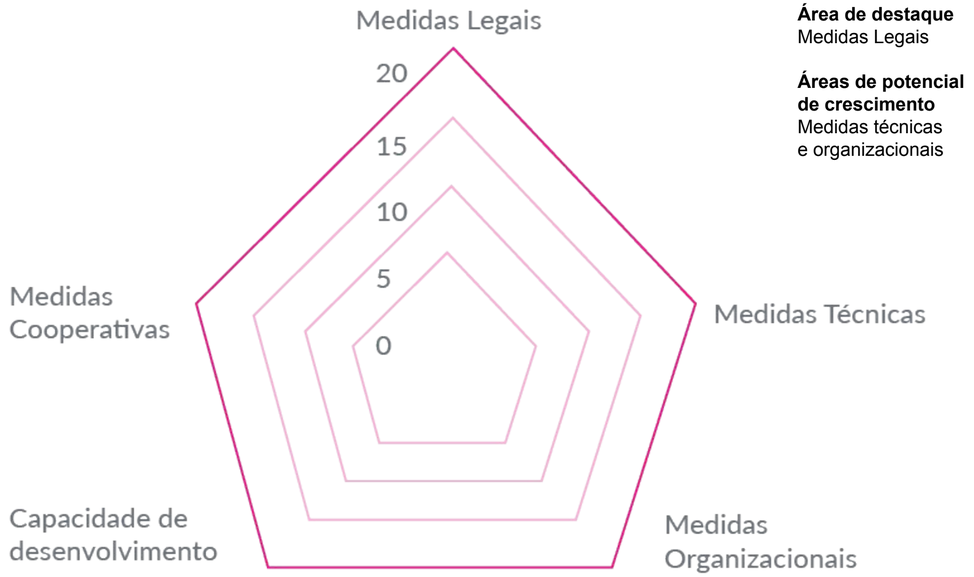
O Brasil subiu 53 posições desde o último *Globay Cybersecurity Index*, índice que mede a qualidade da cibersegurança no país na esfeta pública e privada, o que o colocou na 18º posição entre todos os países analisados no ranking (182), e se tornou o país mais bem colocado da América Latina. Grandes pontos de destaque para a subida do país frente ao panorama nacional foram a digitalização dos serviços públicos e a implementação da Lei Geral de Proteção de Dados (LGPD), que garantiu nota máxima no critério de medidas legais.

Além disso, a Estratégia Nacional de Segurança Cibernética vem ganhando força no país, porque apesar dos riscos advindos pelo aumento da digitalização de vários serviços, os esforços para tornar as aplicações cada vez mais seguras tiveram um aumento. Leis federais como o Marco Civil da Internet, em 2013, e a lei dos crimes cibernéticos, em 2021, auxiliaram na elucidação e divulgação do tema, além de estabelecer precedentes corretos de como tratar o assunto no país.

Embora os resultados do índice sejam animadores, o país é um dos mais visados globalmente por criminosos cibernéticos, por ainda ter diversas fragilidades dentro das organizações. Mesmo estando fora das 7 principais economias do mundo, o Brasil está entre os 5 países mais visados por criminosos, o que indica que o ecossistema de cibersegurança no país ainda está em desenvolvimento e precisa de investimento e atenção.

Pontuações do Brasil: Global Cybersecurity Index

BRASIL (República Federativa)



Nível de desenvolvimento
País em desenvolvimento

Área de destaque
Medidas Legais

Áreas de potencial de crescimento
Medidas técnicas e organizacionais

Pontuação Total	Medidas Legais	Medidas Técnicas	Medidas Organizacionais	Capacidade de desenvolvimento	Medidas cooperativas
96,6	20	18;73	18,98	19,48	19,41

Cybertechs brasileiras com atuação dentro e fora do Brasil

Predro IVO
CEO
PhishX

A PhishX já conta com uma trajetória de sucesso, estando em mais de 90 países e levando conhecimento em cibersegurança para as organizações. O que vocês gostariam de destacar na solução de vocês?
A nossa atuação global é muito importante. Estamos trabalhando cada dia mais na disseminação dos conhecimentos sobre segurança digital, para ajudar as organizações do mundo todo com a conscientização das pessoas sobre cybersecurity, privacidade, compliance e governança, temas correlatos.

Para fazer isso, temos uma equipe dedicada em produzir conteúdos em diversos idiomas, que estão alinhados com os temas mais atuais. Também acompanhamos cada cliente, para que possam utilizar nossos produtos e tecnologias da melhor forma possível, foco na experiência e sucesso do cliente para nós é 100% colocada em prática, desde o primeiro dia. Dessa maneira, fazemos com que todos possam usufruir da nossa biblioteca de materiais.

Além disso, contamos com tecnologias desenvolvidas para desafogar equipes de TI que sofrem com a quantidade de chamados para identificar ameaças internas e/ou externas, como o PhishX Assistant, nosso assistente pessoal contra fraudes, e, o My PhishX, nossa plataforma de gamification. Nossas soluções são focadas em facilitar a conscientização sobre segurança digital, permitindo que as organizações gerenciem seus próprios indicadores e façam com que as pessoas participem ativamente das estratégias de segurança, sendo verdadeiros ativos de segurança cibernética. Através de pessoas empoderadas de conhecimento sobre cybersecurity, governança, privacidade e compliance, estabelecemos a integração da inteligência humana à inteligência artificial, através de meios colaborativos e humanizados, como bots, add-ons e integrações, com o uso do PhishX API em diversas variações de aplicabilidade.

O Brasil tem um problema sério de falta de preparo e de informação dos colaboradores dentro das organizações quando o assunto é cibersegurança. Como vocês vêem a realidade brasileira frente a todos os países que vocês já trabalharam? Tem algum país que você gostaria de destacar em relação à conscientização dos colaboradores mesmo antes da solução de vocês entrar em prática?
No Brasil a cybersecurity ainda é vista como gasto, e não investimento. Essa é uma das grandes →

→ barreiras que as organizações vêm enfrentando para encontrar estratégias de segurança da informação. E é aí que mora o problema. As consequências de ataques cibernéticos trazem gastos ainda maiores do que as soluções que estão disponíveis no mercado. E basta que apenas uma pessoa clique em um link comprometido para abrir as portas. Por isso a cibersegurança deve ser vista como um investimento. Organizações que adotam as melhores práticas, inclusive a conscientização das pessoas, evitam prejuízos financeiros e de imagem, além de evitarem gastos ainda maiores para se recuperar de ataques cibernéticos, como os ataques de ransomware.

Qual é o principal desafio que vocês enfrentam com a solução de vocês hoje? Os desafios são diferentes no Brasil em comparação a outras regiões do globo?
Acredito que o principal desafio no Brasil seja quebrar a percepção limitada de que a tecnologia por si só resolverá os problemas, sem o envolvimento das Pessoas. Além disso, treinamentos sobre segurança da informação e/ou segurança cibernética não devem ocorrer somente através de palestras anuais e/ou imersões pontuais. Golpes e ataques cibernéticos fazem parte do dia a dia das organizações e das pessoas, 24 horas por dia ativos e disponíveis, com automação e inteligência artificial ao seu favor. A segurança cibernética dentro de todas as organizações e ciclos de convivência deve se tornar um assunto recorrente e habitual, não há como fugir e/ou negligenciar o tema.

É muito importante que as equipes possam enxergar métricas e relatórios, como as pessoas estão absorvendo os treinamentos, simulados, comunicados e outras interações, de que forma elas estão criando aproximação com os temas da segurança, privacidade, compliance e governança.

Somente com gerenciamento recorrente de indicadores é possível saber se as pessoas estão realmente absorvendo os conteúdos. Então a PhishX propõe enxergar a conscientização de outra maneira, através de interações contínuas, recorrência, multidisciplinariedade de assuntos, omnichannel e, fazendo uso de inteligência artificial aplicada à coleta de informações preditivas, que possam antever ataques cibernéticos.

Em relação aos desafios do Brasil em comparação com outras regiões do globo, é possível afirmar que existe uma diferença de maturidade dentro das organizações. As maneiras e costumes variam entre os países, e isso também afeta os nossos desafios.

Por exemplo, nos Estados Unidos as pessoas não utilizam as redes sociais da mesma forma que em Angola. Isso proporciona novos desafios para a PhishX. Como abordar a conscientização sobre segurança da informação em diferentes culturas? Também buscamos estar atualizados com as formas que as organizações multinacionais tratam esses assuntos em suas matrizes e em diferentes nações. Assim podemos conhecer as verdadeiras necessidades de quem queremos impactar. →

Cybertechs brasileiras com atuação dentro e fora do Brasil

Pedro Ivo
CEO
PhishX

→ Pedro, se você pudesse dar dicas para organizações ao redor do mundo sobre como mitigar riscos dentro da organização para que não haja um ataque cibernético por conta de uma falha de segurança humana, o que você falaria?
Conscientize as pessoas. Criminosos são oportunistas, eles precisam de apenas uma brecha para operar ataques que geram prejuízos milionários, e muitos desses ataques começam em estratégias que abordam pessoas. Seja através de uma mensagem falsa, com um link malicioso, ou por meio de uma propaganda. Apenas um clique pode abrir as portas da sua organização.

Então, além de ter e atualizar frequentemente as soluções de segurança, mantenha as pessoas treinadas e habituadas com temas de segurança digital, privacidade, compliance e governança. Faça com que elas sejam parte ativa da sua estratégia de segurança da informação e/ou segurança cibernética. Tornar as pessoas capazes de reconhecer um phishing, ou um golpe dentro de um aplicativo de mensagens, pode salvar recursos financeiros e a reputação da sua organização.

Por fim, quais são os próximos passos da empresa?
Seguimos firmes e fortes em nosso único Propósito: Levar o conhecimento de Segurança Digital, Privacidade, Compliance e Governança para todas as Pessoas, em qualquer lugar, a qualquer momento e em qualquer dispositivo. Manteremos o foco em nosso propósito e ampliaremos nossa relevância global no mercado de PCS (Peopl-Centric Security). Já somos líderes na LATAM, mas ampliaremos nossas iniciativas nos EUA, Europa, África e Oriente Médio.

Cybertechs brasileiras com atuação dentro e fora do Brasil

Josemando Sobral
Co-Founder
Unxpose

Ataques cibernéticos ao redor do mundo

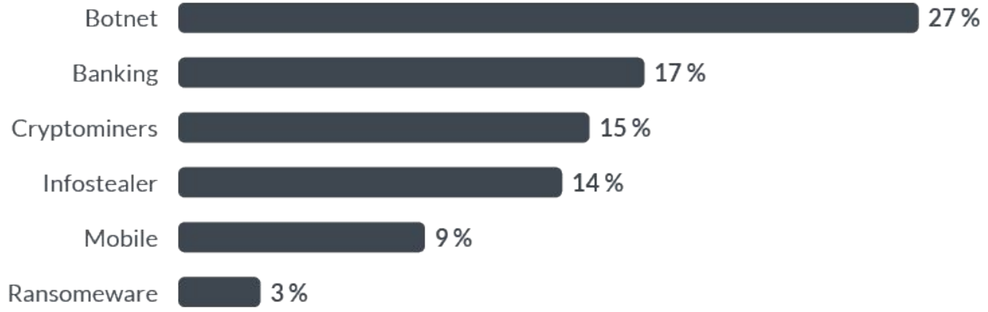
Em 2021, as organizações dos EUA viram uma média de 443 ataques semanais, marcando um aumento de 17% em relação ao início deste ano. Na EMEA (que engloba países da Europa, Oriente Média e África), a média de ataques foi de 777, um aumento de 36%. E na APAC (órgão que engloba países da Ásia e do Pacífico), as organizações sofreram 1338 ataques semanais, um aumento de 13%. Apesar do crescimento mundial na média de ataques, a Europa tem sido o foco principal, elevando os ataques para o dobro do patamar, se comparado aos outros blocos.

Dentre malwares mais utilizados no mundo, o tipo botnet foi o mais visto, atingindo quase 30% das redes corporativas mundiais. Um botnet consiste em uma rede de bots, capazes de executar ataques como DDoS, roubar dados, enviar spam, ou ainda permitir o acesso aos dispositivos atacados.

Em segundo lugar está o tipo banking que, como o nome sugere, tem os serviços de bancários digitais como alvo do ataque, mapeados em quase 20% das redes corporativas. Este malware busca roubar informações como dados do cartão de crédito e do saldo, assim como existem alguns que tomam o controle e o acesso à conta.

Em terceiro lugar temos os tipos cryptominers, que são malwares que instalam programas para minerar cripto ativos, consumindo o processamento das máquinas afetadas, muitas vezes sem o usuário saber.

Porcentagem de redes corporativas atacadas por cada tipo de malware



Porém vale destacar que este cenário vem mudando e que o cenário e os acontecimentos globais influenciam na tendência dos tipos de ataque, como pode ser observado nos dados levantados pela SonicWALL.

Tipo de ataque	Número de ataques	Diferença 2019 - 2020
Ataques de malwares	5,6 bilhões	- 43%
Ameaças encriptografadas	3,8 milhões	+ 4%
Tentativas de invasão	4,8 trilhões	+ 20%
Ataques cryptojacking	81,9 milhões	+ 28%
Ataques de ransomeware	304,6 milhões	+ 62%
Ataques em IoT	56,9 milhões	+ 66%

Hunters.

Local
Tel Aviv,
Israel

Ano de Fundação
2018

Público
B2B

Investimento Recebido
US$ 50,4M

Investidores
Bessemer Venture Partners; U.S Venture Partners; M12; YL Ventures

Sobre

A Hunters é uma startup israelense que está transformando a forma como os times de segurança respondem a ameaças e ataque cibernéticos. Seu modelo de negócio combina engenharia de dados com camadas de inteligência e automação para tornar as empresas e seus clientes mais ágeis nas respostas aos ataques.

Fundada em 2018, a startup vem apresentando forte crescimento, tendo captado mais de US$ 50,4 milhões de fundos como a Bessemer Venture Partners e a U.S. Venture Partners. Desde então, a empresa já atingiu um tamanho de time de mais de 80 funcionários.

Atualmente a startup foca em quatro pilares para desenvolver seus produtos:

- Atualização e modernização de SIEMs (Security and Information Event Management)
- Construção de um Data Lake de Segurança conectado com uma plataforma de analytics
- Analytics para segurança
- Caça de Ameaças

Blumira

Local
Ann Arbor, Michigan,
Estados Unidos

Ano de Fundação
2018

Público
B2B

Investimento Recebido
US$ 12,9M

Investidores
Ten Eleven Ventures; M25; Mercury; Array Ventures

Sobre

A startup Blumira desenvolve uma plataforma de detecção e resposta a ameaças digitais, permitindo que empresas se previnam de ataques de ransomware .

A empresa vem se destacando por utilizar métodos bastante inovadores na parte de detecção avançada de ameaças, reduzindo interferências e os chamados “falso-positivos”.

A Blumira que nasceu de forma próxima a Universidade de Michigan já recebeu cerca de US$ 13 milhões em investimentos, com a participação de fundos relevantes como a Ten Eleven Ventures. O modelo de negócio da startup se assemelha bastante a maioria das plataformas de detecção e resposta a ataques cibernéticos surgidas depois de 2015.

Local
Boston, Massachusetts, Estados Unidos

Ano de Fundação
2015

Público
B2B

Investimento Recebido
US$ 25 mil

Investidores
Hartford InsurTech Hub

Sobre

A Yaxa é uma startup focada em fornecer proteção em tempo real através de algoritmos próprios de machine learning.

Com pouca necessidade de intervenção da área de TI, a empresa monitora o tráfego de usuários criando um perfil com base no comportamento apresentado. Essa pré-classificação auxilia no monitoramento para um possível ataque nas informações protegidas. Esse sistema também ajuda na identificação de "falso alarme".

Além disso, no caso de um acesso não reconhecido, o sistema encaminha uma solicitação de verificação que pode ser personalizada com base na política da empresa o que melhora a segurança interna.

Por fim, com a incorporação de feedbacks constantes, a empresa consegue acompanhar mudanças de comportamento gerais de quem acessa a plataforma, assim consegue ser mais precisa de quando está ocorrendo um acesso que comprometa as informações.

Local
Bochum, Renânia do Norte-Vestfália, Alemanha

Ano de Fundação
2013

Público
B2B

Investimento Recebido
US$ 28,9 mi

Investidores
eCAPITAL ENTREPRENEURIAL PARTNERS, Digital+ Partners, Hight-Tech Grunderfonds

Sobre

A VMRay foi fundada para colocar pesquisas sobre combate a malwares na prática. Através de seus produtos e serviços a startup detecta, notifica, analisa e responde a ameaças cibernéticas.

Através do seu sandbox, mesmo que o malware consiga passar por alguma barreira ele será capturado por outra, não permitindo que ele saia e leve os dados com ele.

Ademais, diversos mecanismos de proteção desenvolvidos por outras empresas são visíveis aos malwares o que permite que eles possam escapar. No entanto, o que foi desenvolvido pela VMRay não consegue ser visto pelo malwares enquanto procura a sua presença, desta forma sendo mais fácil para impedi-los.

Quais são os principais investidores internacionais em soluções de Cyber Threat Detection?

MACH37 CYBER ACCELERATOR

techstars_

LORCA

CYLON

PLUGANDPLAY

Tendências

Blockchain em soluções de segurança para conter ransomwares e resgates em cripto

No começo de 2021, cerca de 48% dos hospitais dos Estados Unidos tiveram que ficar offline por conta de um ransomware que sequestrou dados e exigiu pagamentos para devolver acessos e dados médicos. Esse evento levantou diversas discussões sobre as razões desse tipo de ataque terem aumentado e quais as formas de se proteger perante tal cenário.

Na última década, o ransomware tornou-se um dos modelos de negócios criminosos mais prolíficos do mundo, afetando de usuários padrão até grandes organizações ou órgãos governamentais. O ransomware se propaga através de anexos de e-mail maliciosos, aplicativos de software infectados, dispositivos de armazenamento externos infectados e sites comprometidos.

Um dos motivos da volta desse tipo de ataque foi o surgimento do bitcoin e outras criptomoedas. Isso ocorre principalmente porque essas criptomoedas permitem que os invasores consigam grandes somas de dinheiro enquanto permanecem anônimos longe do rastreio como em moedas mais tradicionais.

Porém, a mesma rede que sustenta o anonimato do bitcoin é capaz de promover segurança e confiabilidade para soluções que visam proteger o usuário desses ataques.

O blockchain é uma das soluções para esse ataques, uma vez que a descentralização e distribuição são suas características fundamentais. A descentralização significa que a rede não conta com um servidor central para hospedar todos os dados, mas distribui eles entre todos os usuários da rede, também conhecidos como nós. Existem muitos tipos de nós em uma rede blockchain, nós completos, por exemplo, armazene uma cópia de toda a blockchain.

Como resultado, todo o sistema não tem um único ponto de falha. Se um nó estiver comprometido, os administradores apenas terão que lidar com a vulnerabilidade que permitiu o usuário mal-intencionado acessar a rede e restaurar o nó à sua versão anterior, ou eles podem simplesmente cortar o nó da rede. Tendo a rede toda interligada, se torna tecnicamente impossível realizar um sequestro massivo de dados.

Data Protection e regulações ao redor do mundo irão se intensificar

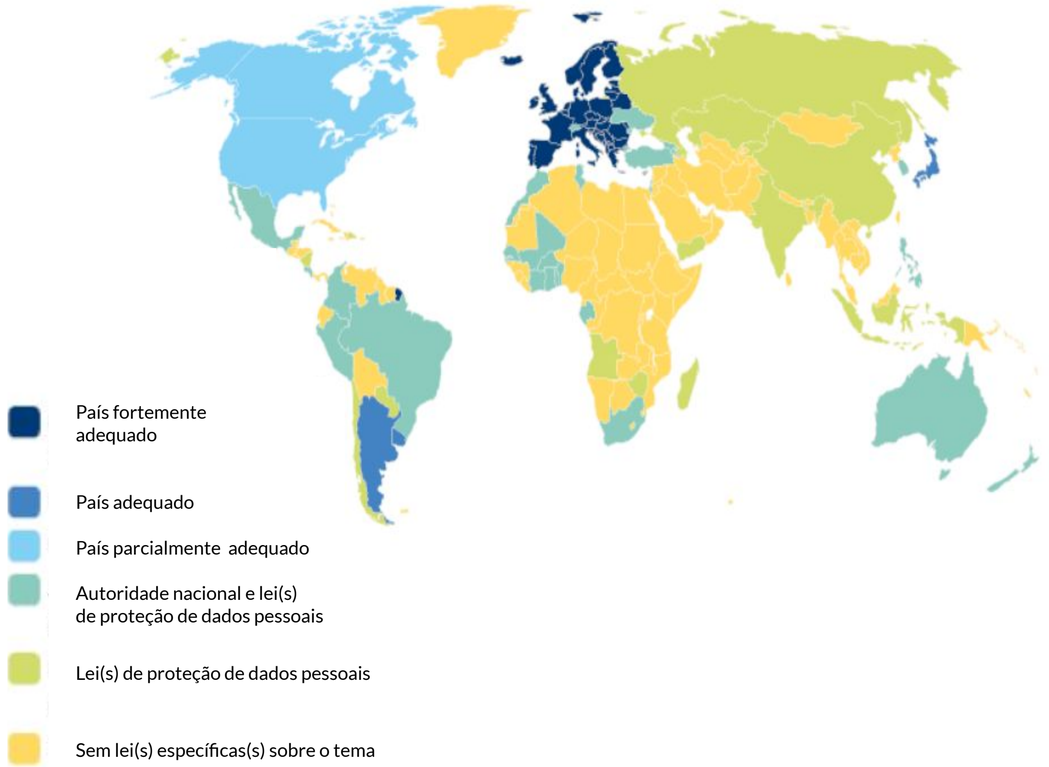
A preocupação com a proteção de dados já não é uma preocupação exclusiva de grandes empresas, uma vez que clientes estão cada vez mais cientes da importância do bom uso de seus dados pessoais.

Além da pressão direta dos clientes, os poderes legislativos também estão aprimorando leis e pondo em execução projetos de regulamentações para que empresas e corporações sejam legalmente responsáveis pela captação, armazenamento e segurança desses dados. No Brasil, apesar da LGPD já estar em vigência desde novembro de 2020, ainda é possível encontrar empresas que não estão de acordo com as normas federais.

Como consequência, todos empreendimentos que atuam no formato digital, sejam eles MEI's ou grandes corporações, terão que se adequar a essas novas regras. Para empresas que já tinham uma grande base de dados, o desafio se torna ainda maior por haver a necessidade de realizar essas alterações em grande escala, enquanto simultaneamente redesenha suas estratégias para trabalhar com informações mais generalistas.

Dentro desse contexto, as startups de privacidade e segurança estão ganhando popularidade, pois além de já terem o know-how sobre legislações, elas conseguem ajustar o banco de dados da empresa de forma rápida e eficiente sem a necessidade de realocar funcionários do time de T.I. para executar essa atividade.

Grau de adequação



Identity Centric Solutions em um mundo cada vez mais digital

Tema do nosso próximo Inside Cyber #5, as empresas de Identity and Access Management são essenciais para uma política de cibersegurança forte dentro das organizações. Deve-se destacar as solução de Network Security, Web security, Cloud Security e afins, no entanto o acesso privilegiado à informação tem que estar como centro das políticas de privacidade e segurança.

Com o poder de acessar sistemas, bancos de dados, aplicações e recursos variados, acessos não bem-vindos podem facilmente comprometer a integridade de qualquer ativo, e é um dos pontos de falha para a entrada de softwares maliciosos. Uma política de segurança baseada em identidade no centro (Identity Centric Security) já é um termo bastante utilizado, que parte dos princípios de autenticação, autorização, acesso a dados e auditoria, e precisa ser pilar dentro das empresas para garantir que apenas pessoas desejadas estejam acessando informações privilegiadas.

O ecossistema brasileiro de inovação em cibersegurança destaca as soluções de Identity and Access Management como a categoria mais investida. Vamos explorar o tema, sua importância e seus desdobramentos no nosso próximo report.

25%
Das Cybertechs brasileiras estão na categoria de Identity and Access Management

Confira a entrevista realizada no **Inside VC**/Setembro !

Guilherme Cervieri
VP Strategy & M&A
unico

Próximos anos

Marcos Sêmola
Partner
EY

Marcos, como você avalia o crescimento do número de ataques cibernéticos nos últimos anos, especialmente na pandemia? Quais medidas poderiam ser tomadas para evitar esses ataques?
Previsível. O crime acompanha o dinheiro e uma vez que as empresas e seus modelos de negócio dependam tanto de ativos digitais, estes passam a ser alvo de ataques mai sofisticados e com maior volumetria.

Não há como evitar um ataque, a não ser que a empresa optasse pelo retrocesso de voltar a operar offline, o que não é, de fato, uma opção. Portanto, risco é um vetor onipresente. O segredo está em tornar seu negócio menos interessante aos criminosos pelo esforço e investimento que teriam que fazer para obterem ganhos.

Quais são as principais tecnologias que vão ser nossas aliadas no combate às principais ameaças nos próximos anos?
A tecnologia é apenas parte da solução. As empresas operam em seu próprio micro ecossistema e que depois se conecta ao um macro ecossistema, e onde uma peça de dominó derrubada pode produzir efeitos em cascata.

Esses dominós podem ser representados por ativos físicos, tecnológicos e humanos e, portanto, todos devem estar debaixo do guarda-chuva da gestão de riscos de segurança da informação.

Quais são os pontos que você gostaria de destacar que você acredita que serão pauta chave para a contenção das principais ameaças cibernéticas nos próximos 10 anos?
Governança é a palavra. As empresas precisam desenvolver alguma habilidades como a de conhecer o seu risco, e seu apetite, para então elaborar sua própria solução de segurança capaz de exercer 5 funções: 1) identificar riscos, 2) proteger ativos, 3) detectar um risco em trajetória de materialização, 4) responder a um incidente em curso e 5) recuperar os danos produzidoS pelo incidente que não pôde ser evitado.

Estamos prontos para nos defendermos da quantidade de ciberataques que virão já em 2022?
Não e nunca estaremos. O que pode ser feito é desenvolver nosso próprio sistema operacional de riscos cibernéticos onde as decisões de negócio são tomadas com base no risco residual, após medidas compensatórias ou mitigatórias, e o apetite ou tolerância ao risco/impacto da empresa.

Cybertechs

Glossário de categorias

Categorias

NETWORK & INFRASTRUCTURE SECURITY
Companhias que apliquem processos de proteção da infraestrutura de rede, instalando medidas preventivas para negar acesso não autorizado, 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 cyber 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 roubo/sequestro de dados e códigos dentro de dentro de aplicativos e plataformas.

DATA PROTECTION
Data protection engloba empresas responsáveis pela proteção de informações sensíveis à empresa (Banco de Dados, Informações de Corporações) e enquadram às corporações na LGPD.

MOBILE SECURITY
Empresas que atuam com produtos e serviços voltados a garantir a segurança do device (dispositivo móvel), IoS, Android. 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 as a Service, 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 Secutiry refere-se às startups 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
Security Consulting and Services refere-se a startups que prestam serviços para testar ou aprimorar serviços de cibersegurança. Um exemplo aqui são empresas que atuam com simulações de ataques cibernéticos como forma de identificar possíveis falhas nos sistemas.

GOVERNANCE, RISK AND COMPLIANCE
Soluções GRC (Governança, Risco e Cokmpliance) 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

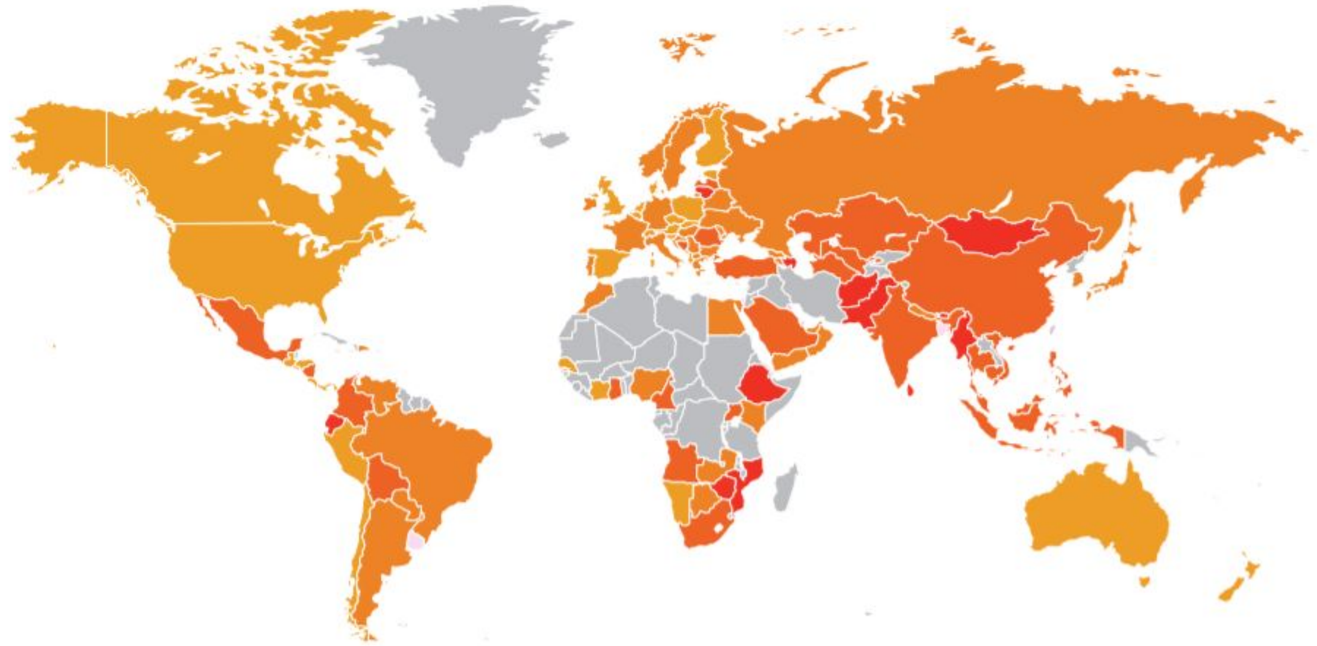
Classificação dos países em relação ao risco de ataques

A partir da análise de dados do seu sistema, a Check Point levantou um índice de ameaça cibernética global, baseado na probabilidade de uma máquina ser atacada por um malware em um determinado país. O mapa exibe o índice de risco de ameaças cibernéticas globalmente, demonstrando as principais áreas de risco ao redor do mundo.

Podemos ver que a Ásia é uma das regiões com maior risco, dando destaque para a Mongólia, Afeganistão, Paquistão e Mianmar.

Apesar da falta de dados para o mapeamento completo, a África também se mostra como uma região vulnerável, com destaques para a Etiópia, Moçambique e Zimbabuê.

Nas Américas, o risco é considerado moderado apesar do número de incidentes, com destaque para o Equador.

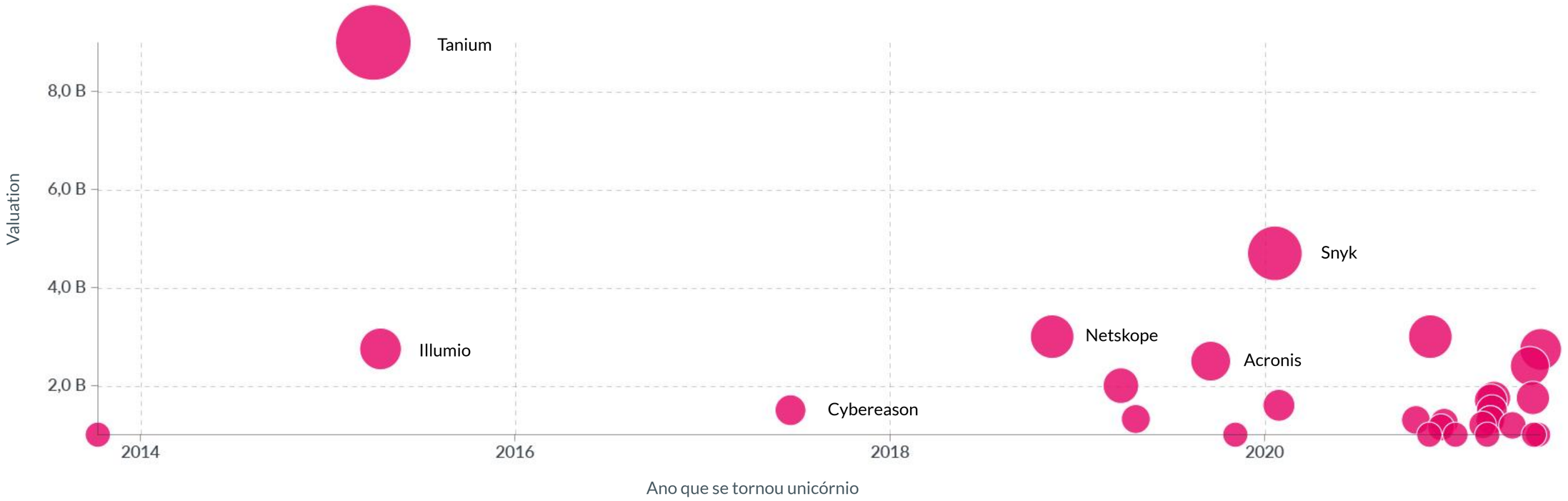


Quando mais escuro, maior o risco
Cinza = dados insuficientes

Dos mais de 750 unicórnios ao redor do mundo, 30 são empresas de cibersegurança

Por uma necessidade mundial, o mercado cyber vem apresentando nos últimos anos um crescimento notável, que é refletido diretamente no número de startups que atingiram o patamar de unicórnio (empresas com valor de mercado acima de US$ 1 B). Não à toa, o setor representa cerca de 5% do total de unicórnios. Interessante notar que 21 das 30 empresas alcançaram este patamar em 2020 ou 2021, o que evidencia a crescente preocupação com a segurança digital. Espera-se que nos próximos anos mais empresas de cibersegurança cresçam a patamares de unicórnio, como foi o caso da Unico, de acesso e controle de identidades, no Brasil.

Unicórnios em cybersecurity



LINKS

2021 Cyber Security Statistics. The Ultimate List of Stats, Data & Trends https://purplesec.us/resources/cyber-security-statistics/

What is a Cyber attack? https://searchsecurity.techtarget.com/definition/cyber-attack

7 Types of Cyber Security Threats https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

2021 Top Ten Cybersecurity Trends https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends

2021 Must-Know Cyber Attacks Statistics and Trends https://www.embroker.com/blog/cyber-attack-statistics/

Ataques cibernéticos: Quais são os principais e como se proteger deles? https://www.iberdrola.com/inovacao/ciberataques

Ameaças cibernéticas Brasil 2021: https://www.gat.digital/wp-content/uploads/2021/05/datasheet-relatorio-ameac%CC%A7as.pdf

Brasil é o quinto país mais afetado com ataques cibernéticos em 2021:
https://www.poder360.com.br/tecnologia/brasil-e-o-5-pais-mais-afetado-com-ataques-ciberneticos-em-2021/

Relatório de ameaças cibernéticas da SONICWALL 2021 https://www.sonicwall.com/pt-br/2021-cyber-threat-report/

https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Entrevistas: **https://docs.google.com/document/d/115NHloYhTFxGjQ0MWzoaevSAzrwgJZbL2G_2-SX9y4o/edit?usp=sharing**

Docs: https://docs.google.com/document/d/1wkcHi7EaXjt8NNrDJrsP0v8e1MueXx4_trx8TIxQzRw/edit

Report CISCO
https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/602/original/CTIR_TAR__Q2_2021_one_pager.pdf?1626852906