CyberTech Report

CISCO SECURE

Colaboração e Compartilhamento de Inteligência de Ameaças

#9 | MARÇO | 2022

Sumário

Este report conta com o apoio da Cisco Secure.

cisco SECURE

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
Systems Engineering Manager
Cisco

Marcos Sêmola
Cybersecurity Partner
EY

Rafael Narezzi
Especialista em Segurança Cibernética
4CyberSec & Cyber Security Summit

Introdução

Introdução

Você certamente já ouviu falar que o crime cibernético está cada vez mais organizado — e isso é uma verdade indiscutível. Basta levarmos em consideração o alto nível de estruturação e disciplinas dos sindicatos de ransomware-como-serviço (ransomware-as-a-service ou RaaS), que possuem uma composição hierárquica similar à de grandes empresas, com a alta gerência, os gestores de departamentos e os "colaboradores" contratados para tarefas de cunho operacional.

Indo além, é de conhecimento popular que os níveis mais obscuros da internet (dark e deep web) estão repletos de fóruns e comunidades nas quais os meliantes digitais trocam informações e ferramentas entre si, incluindo vulnerabilidades encontradas em softwares, exploits, malwares, páginas falsas prontas (para o disparo de campanhas de phishing) e muito mais. Aliás, já não é preciso sequer descer até as profundezas da WWW para encontrar esses conteúdos: existem grupos em mensageiros instantâneos e comunidades hospedadas na surface web no qual existe o compartilhamento desse tipo de material.

Embora muitos executivos não percebam isso, tal característica do cibercrime é o que o torna tão eficiente em suas artimanhas: os golpistas se ajudam, independentemente de suas origens étnicas, convicções pessoais ou finalidades. Eles se estruturam em uma gigantesca comunidade global e entendem que, auxiliando uns aos outros, ficará mais fácil para todo mundo efetuar seus ataques cibernéticos e obter êxito em suas campanhas maliciosas.

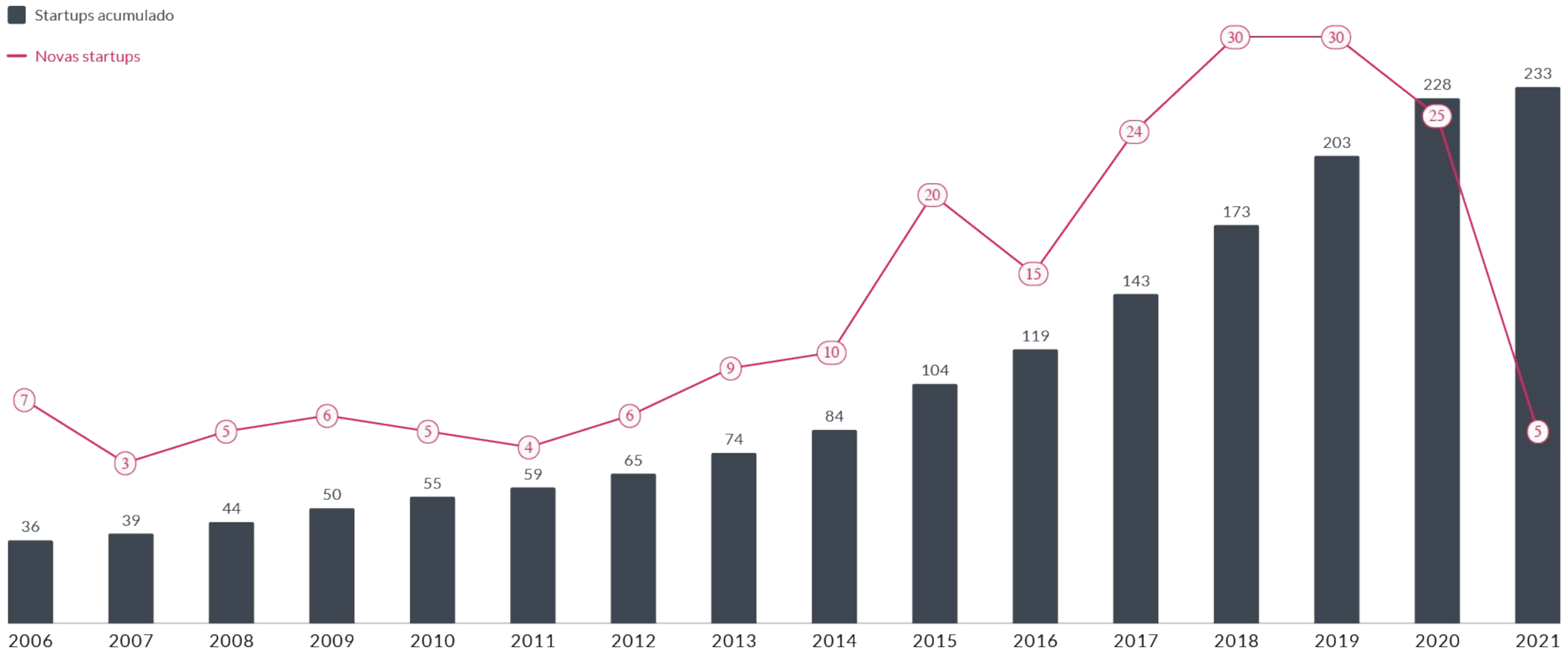
Por outro lado, por algum motivo, o mesmo não ocorre com a comunidade de segurança da informação. Não temos ainda o forte costume — nem a nível federal e nem a mundial — de trocar experiências de forma aberta e compartilhar conhecimento que possa ajudar outros profissionais em situações similares a lidar com uma intrusão em seus sistemas, por exemplo. Parte disso é reflexo de uma cultura que enquadra um incidente de segurança da informação como algo vergonhoso e que deve ser escondido a todo custo, já que pode afetar negativamente a reputação da empresa.

Contudo, o compartilhamento de inteligências sobre ameaças cibernéticas e a colaboração entre profissionais, empresas e outras instituições do setor só traz benefícios. O objetivo deste relatório é justamente abordar quais são esses benefícios, entender os motivos que desestimulam a troca de informações, visualizar as barreiras que precisamos transpor e visualizar insights para um cenário futuro de maior auxílio multidirecional no combate ao cibercrime.

Boa leitura!

Ecossistemas Cybertech

Evolução Cybertechs



Highlights

233
Startups

12
Categorias

9.000
Funcionários empregados

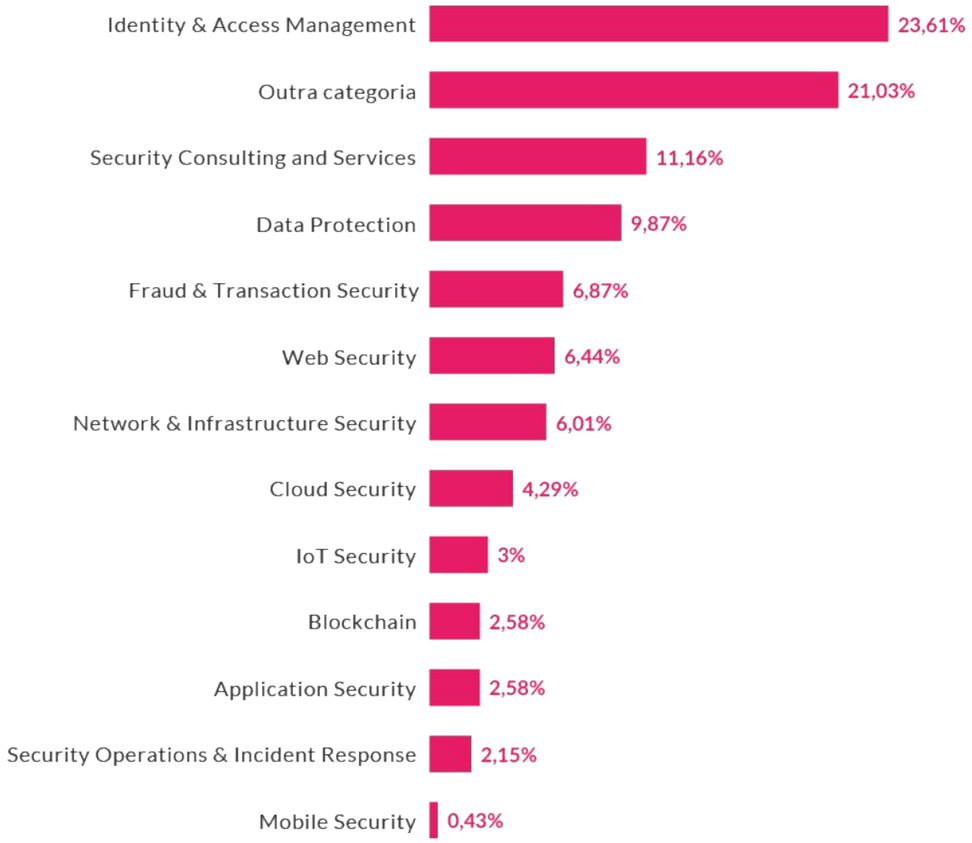
75
Startups com investimento recebido

US$ 412,5M
Investimento recebido desde 2013

US$ 294M
Investimento recebido nos últimos 2 anos

15
M&A's desde 2012

Divisão Cybertechs por categoria



RADAR: CYBERTECHS

DISTRITO

Data protection

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

Cloud Security

ADTsys · BrasilCloud · DDMX · nuvic · RedeHost · CleanCloud

Mobile Security

BluePex

Security Consulting and Services

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

Fraud & Transaction Security

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

Network, Infrastructure Security

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

Security Operations & Incident Response

AXUR · gocache next-gen CDN

RADAR: CYBERTECHS

DISTRITO

Identity & Access Management

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

IoT Security

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

Governance, Risk and Compliance

GAT InfoSec · NeuralMind · certo · REFINARIA DE DADOS

Application Security

Berghem Smart Information Security · CONVISO · BugHunt

Blockchain

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

Web Security

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

Inteligência de Ameaças: vamos compartilhar?

Contexto e Panorama Nacional

O que é inteligência de ameaças cibernéticas?

Também conhecida pelos nomes em inglês threat intelligence ou cyber threat intelligence (de onde surge a sigla CTI, que passaremos a usar neste relatório para maior facilidade de compreensão), a inteligência de ameaças cibernéticas é, basicamente, o uso e a análise de dados crus para gerar conhecimento a respeito de perigos existentes ou emergentes às informações e dados da companhia. Com tal conhecimento prévio, fica mais fácil preparar-se para responder a eventuais incidentes ou até mesmo evitá-los completamente.

A definição do instituto de consultoria Gartner sobre CTI é bastante esclarecedora:

A inteligência contra ameaças é um conhecimento baseado em evidências, incluindo contexto, mecanismos, indicadores, implicações e conselhos úteis, sobre uma ameaça ou perigo existente ou emergente a ativos, que pode ser usado para informar decisões sobre a resposta do sujeito a essa ameaça ou perigo.

Já dizia o sábio Sun Tzu em sua obra "A Arte da Guerra": "Conheces teu inimigo e conhece-te a ti mesmo; se tiveres cem combates a travar, cem vezes serás vitorioso". Certamente você conhece sua própria infraestrutura de segurança, mas e os seus inimigos? Você realmente sabe quem são seus adversários e como eles podem te atacar? Quais são os vetores mais possíveis de serem exploradas? Quais pontos a sua equipe deve ficar mais atenta? Quais atitudes devem ser colocadas em prática para reduzir ao máximo a chance de um ataque cibernético bem-sucedido?

O objetivo do CTI é juntar esforços para responder a todas essas questões da forma mais assertiva e atualizada possível. Um programa de inteligência de ameaças deve contar com feeds sempre atualizados a respeito das mais recentes técnicas, táticas e procedimentos (TTPs) detectados, tal como profissionais especializados em analisar essa quantidade massiva de dados brutos e transformá-los em uma informação digestível.

Recentemente, as capacidades preditivas de soluções de inteligência artificial (I.A.) se mostraram valiosas para facilitar e automatizar grande parte desse trabalho intelectual. Vale a pena ressaltar, porém, que o fator humano continua sendo crucial para uma análise mais sensibilizada sobre as motivações e a contextualização de um possível ataque cibernético.

Também é importante observar que diversas empresas fornecedoras de soluções de segurança cibernética possuem os seus próprios laboratórios, compostos por equipes de pesquisadores altamente capacitados, justamente para coletar e gerar essa inteligência de forma totalmente gratuita ao mercado.

Geralmente, isso ocorre após a detecção de uma vulnerabilidade, ator malicioso ou ameaça persistente avançada (advanced persistent threat ou APT) inédita, sendo fornecidas todas as informações sobre tal perigo no formato de um extenso relatório técnico.

Compartilhamento de ameaças: juntos, somos mais fortes

Nesse sentido, uma prática que poderia nos ajudar no combate ao crime cibernético é justamente uma colaboração maior entre empresas, pesquisadores e entidades governamentais com o objetivo de compartilharmos — de forma multidirecional — a nossa inteligência relativa às ameaças cibernéticas que enfrentamos e incidentes de segurança da informação que sofremos. Toda experiência e toda inteligência, por mais que a priori possa não parecer, é extremamente válida e útil para terceiros. Dessa forma, passamos a ganhar a mesma vantagem estratégica dos cibercriminosos, que têm tanto sucesso justamente pelo costume de se ajudar com o objetivo comum de atacar um alvo.

O mercado costuma dividir o compartilhamento de inteligência de ameaças em duas categorias distintas:

- **Compartilhamento unidirecional:** apenas uma das partes compartilha sua inteligência de forma aberta sem receber uma contribuição das contrapartes que a recebem. Podemos exemplificar isso com os relatórios de download livre disponibilizados por grandes fornecedores de soluções de segurança cibernética;
- **Compartilhamento bidirecional:** embora não existam garantias de que todas as partes irão colaborar, neste modelo, forma-se um ecossistema (fechado ou aberto) no qual dois ou mais membros compartilham inteligência entre si, consumindo materiais alheios e também contribuindo.

Infelizmente, enfrentamos um problema de cunho cultural ao falarmos sobre colaboração e compartilhamento de inteligência em segurança cibernética: no geral, empresas e profissionais não se sentem confortáveis em “abrir a porta de suas casas” e trocar experiências com terceiros. Esse é um problema global, mas que, no Brasil, parece ser ainda mais grave do que em qualquer outro país. Podemos destacar alguns motivos para tal problema cultural.

Antes de mais nada, temos o medo comum de simplesmente admitir que sofremos um episódio de tentativa de ataque, invasão, sequestro digital (ransomware) ou até mesmo um vazamento de dados — este último se tornou especialmente delicado desde que a Lei Geral de Proteção de Dados (LGPD) entrou em vigor. Muitas marcas ainda não entendem que, infelizmente, ser vítima de um ciberataque é algo comum e não representa negligência; ao invés de esconder o incidente, é muito mais saudável assumi-lo e demonstrar o que foi feito para garantir que ele não se repita.

Também existem preocupações em relação à privacidade e segurança de dados, ou seja, no compartilhamento acidental de informações corporativas sensíveis junto com a inteligência de ameaça. Por fim, é possível perceber uma falta generalizada de conhecimento sobre como realizar tal compartilhamento da forma mais eficiente possível — o que, por sua vez, é um resultado direto da falta de discussões sobre o assunto.

Concorrentes sim, inimigos jamais!

Marcelo Bezerra
Systems Engineering Manager
Cisco

Historicamente falando, a comunidade de segurança da informação costuma ter receio de compartilhar inteligência sobre ameaças cibernéticas, preferindo manter sigilo sobre incidentes e atores maliciosos enfrentados. Quais motivos justificam esse medo de uma maior colaboração entre corporações?

Primeiro temos que separar o compartilhamento de informações da publicação de informações de ataques e ameaças. As empresas de um modo geral preferem que seus problemas de segurança não venham a público, mas isso não significa que não haja compartilhamento. Há compartilhamento, e muito.

Alguns setores (e o dos bancos é um exemplo) possuem canais oficiais de compartilhamento; porém, mesmo nos setores que onde não há canais oficiais, os profissionais compartilham informação entre si. Nos últimos casos de ataques de ransomware sofrido por empresas brasileiras, viu-se bastante cooperação, inclusive entre empresas concorrentes.

Os CISOs e gestores, de uma forma geral, participam ao longo do ano de uma série de eventos em que há muita discussão.

Acaba sendo uma comunidade pequena. Em muitos desses eventos, há apresentações de casos de sucesso e painéis de discussão.

Muitas das empresas e profissionais participam também de plataformas de compartilhamento, como o FIRST e o CERT.br, entre outros.

Já na área dos fabricantes, as equipes de inteligência e pesquisa compartilham livremente informações sobre ameaças de modo geral. Os fabricantes também costumam emprestar licenças de seus produtos para ajudar as empresas a responder a ataques. A Cisco, por exemplo, vem liberando licenças de Umbrella, Secure Workload e Secure Endpoint a clientes e não-clientes que estão sofrendo ataques.

Quais benefícios o mercado de cibersegurança desfrutaria em uma realidade na qual todas as empresas compartilhassem entre si os detalhes de incidentes, indicadores de comprometimento, técnicas de busca e defesa etc.? →

→ De maneira geral, os profissionais de segurança trocam entre si informações sobre ameaças, boas práticas, o que funcionou e não funcionou em resposta, e até experiências com produtos de fabricantes. O mercado como um todo se beneficia com o aumento da maturidade, o que influencia diretamente na resiliência das empresas e seus negócios.

Para as empresas que ainda estão fora dessa comunidade, e em segmentos onde não há canais oficiais, o ideal é começar participando de eventos da área, em que gestores e profissionais técnicos poderão formar seu networking.

A Cisco faz parte da Cyber Threat Alliance (CTA), uma organização sem fins lucrativos que visa incentivar o compartilhamento de conhecimento sobre ameaças cibernéticas entre empresas do segmento e organizações. Como funciona a CTA e qual é o papel da Cisco nesse ecossistema?

O Cyber Threat Alliance é um grande exemplo de compartilhamento de informações. Os membros do CTA são concorrentes no mercado de segurança, o que mostra que a prática de compartilhar informações são se mistura com a disputa no mercado, seja ele qual for.

A Cisco faz parte dos “Charter Members” — os membros de maior relevância no ecossistema, e do Conselho de Diretores, através do vice-presidente do Cisco Talos, a equipe de pesquisa e inteligência de ameaças da empresa.

O CTA possui uma plataforma na qual os membros podem compartilhar a qualquer momento informações contextualizadas e acionáveis sobre as campanhas de ameaças que estão acompanhando e/ou pesquisando. Através do programa Early Sharing (“compartilhamento antecipado”), análises e resultados de pesquisas são primeiro compartilhados com os membros antes de se tornarem públicos.

Temos uma grande quantidade de frameworks e plataformas livres disponíveis no mercado para o compartilhamento de inteligência sobre ameaças, incluindo a famosa MISP. Se por um lado tal variedade é positiva, por outro, ela não pode justamente fragmentar as informações sobre ameaças, dificultando a criação de uma biblioteca "universal"?

Não acredito que haverá em algum momento uma biblioteca universal, e talvez não seja mesmo a melhor estratégia.

Uma única e enorme biblioteca universal não necessariamente atenderia demandas específicas de alguns setores ou áreas de especialização, sendo esse o principal motivo para a organização de diferentes fóruns.

O importante é que há opções para troca de informações para todas as necessidades. →

Concorrentes sim, inimigos jamais!

Marcelo Bezerra
Systems Engineering Manager
Cisco

→ Pudemos acompanhar, ao longo dos últimos anos, o nascimento de algumas startups ao redor do mundo que usam a chamada "cibersegurança coletiva" para oferecer soluções de proteção, como bloqueio automático de tráfego oriundo de IPs reportados pelos próprios usuários como sendo maliciosos. Você acredita que esse modelo de negócio é uma tendência de mercado?

As bases de reputação hoje no mercado já são abertas e permitem a colaboração pelo público em geral, tanto para reportar que um IP, domínio web ou de email é malicioso, tanto para reportar erro em alguma classificação que esteja bloqueando um domínio legítimo.

As empresas do mercado, por sua vez, usam diferentes bases para decidir pelo bloqueio ou não de um determinado domínio. Uma startup que oferece essa base, no conceito de "cibersegurança coletiva", terá como principal desafio fazer com que as principais soluções do mercado a utilize em suas soluções.

Uma solução de segurança apenas baseada em uma base de reputação de domínios ou IPs não conseguirá eficiência na detectar e bloquear programas maliciosos, principalmente a nova geração de ataques e malwares.

As maiores tendências em soluções de segurança, como zero trust e SASE, não se baseiam apenas em bases de reputação, sendo elas apenas uma entre mais de uma dezena de técnicas para segurança.

Concorrentes sim, inimigos jamais!

Marcelo Bezerra
Systems Engineering Manager
Cisco

CybOX e STIX: entendendo as linguagens estruturadas de compartilhamento

Acredite ou não, mas existem linguagens desenvolvidas especificamente para facilitar o compartilhamento de threat intelligence. Até poucos anos atrás, tínhamos a Cyber Observable eXpression (CybOX), desenvolvida pela organização sem fins lucrativos MITRE e de código aberto. De acordo com a própria ONG, o objetivo da CybOX era ser um padrão para especificar, capturar, caracterizar e comunicar eventos observáveis no campo cibernético. Confira:

O CybOX é uma linguagem padronizada para codificar e comunicar informações de alta fidelidade sobre observáveis cibernéticos, sejam eles eventos dinâmicos ou medidas de estado observáveis no domínio cibernético operacional. O CybOX não é direcionado a um único caso de uso de segurança cibernética, mas pretende ser flexível o suficiente para oferecer uma solução comum para todos os casos de uso de segurança cibernética que exigem a capacidade de lidar com observáveis cibernéticos.

Porém, a linguagem foi descontinuada e embutida à mais moderna versão 2.0 da Structured Threat Information Expression (STIX), que rapidamente se tornou um padrão de referência para toda a indústria. Ela também é open source e mantida pela MITRE, mas com o apoio de órgãos públicos e empresas privadas, como o Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology ou NIST), a Organização do Tratado do Atlântico Norte (OTAN/NATO), a Verizon, a Lockheed Martin, a CyberIQ, a Mandiant, a CrowdStrike etc.

Um excelente white paper lançado pela MITRE nos primórdios da STIX explica de forma clara o porquê da existência da linguagem:

As informações que estão sendo gerenciadas e trocadas hoje são tipicamente muito atômicas, inconsistentes e muito limitadas em sofisticação e expressividade. Onde estruturas padronizadas são usadas, elas são tipicamente focadas em apenas uma porção individual do problema geral; não se integram bem entre si ou carecem de flexibilidade coerente. Muitas atividades de compartilhamento de indicadores existentes são trocas entre humanos de descrições não-estruturadas ou semi-estruturadas de indicadores potenciais, conduzidas através de portais baseados na web ou email criptografado.

Ou seja, a STIX nasceu para ser uma forma mais bem estruturada e eficiente de incentivar o rateio e gerenciamento de informações sobre ameaças cibernéticas. É importante notar que não estamos falando de uma plataforma em si, mas sim de um padrão que é embutido em soluções de compartilhamento e usado tanto por grupos fechados e abertos para garantir consistência e interoperabilidade entre as informações trocadas.

Claro, visto que estamos falando de um projeto de código aberto e uso livre, é importante ressaltar que nada lhe impede de usar a STIX para criar a sua aplicação, servidor ou instância de compartilhamento de sua propriedade.

Os 18 Objetos do STIX 2.1

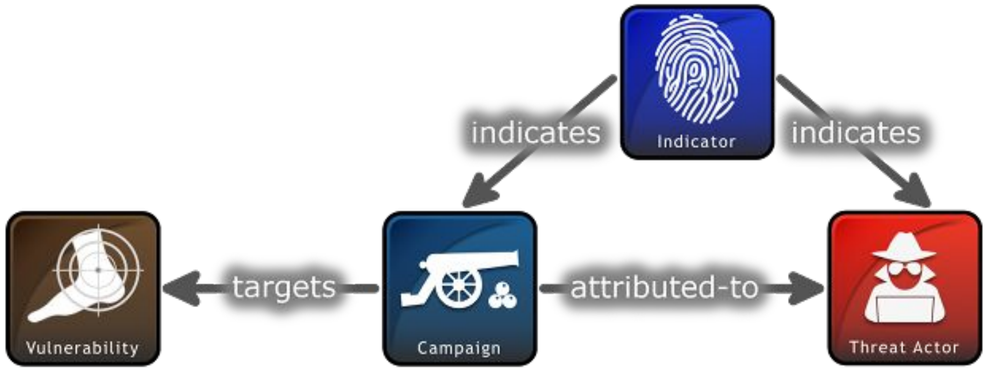
Atualmente, a linguagem STIX está em sua versão 2.1 e possui uma estrutura baseada em Objetos, que categorizam os pedaços de informações que, juntas, formam relações que estruturam representações completas de inteligência de ameaças. Atualmente, temos 18 Objetos:

- **Attack Pattern (Padrão de Ataque):** tipo de tática, técnica e procedimento (TTP) que descreve a forma que o adversário tenta comprometer o alvo;
- **Campaign (Campanha):** grupo de comportamentos adversários que descrevem um conjunto de atividades ou ataques maliciosos que ocorrem em um determinado intervalo de tempo contra um único ou um grupo de alvos;
- **Course of Action (Curso de Ação):** uma recomendação de quem produziu aquele inteligência sobre ações a serem tomadas em resposta àquela ameaça;
- **Grouping (Agrupamento):** afirma explicitamente que os objetos STIX referenciados têm um contexto compartilhado;
- **Identity (Identidade):** indivíduos, organizações ou grupos, tal como classes de indivíduos, organizações, sistemas ou grupos;
- **Indicator (Indicador):** um padrão que pode ser usado para detectar atividades cibernéticas suspeitas ou maliciosas;
- **Infrastructure (Infraestrutura):** representa um tipo de TTP e descreve quaisquer sistemas, softwares e recursos virtuais ou físicos associados desenvolvidos para dar suporte a algum propósito;
- **Intrusion Set (Conjunto de Intrusão):** um conjunto agrupado de comportamentos adversários e recursos com propriedades em comum que acredita-se ser orquestrado por uma única organização;
- **Location (Localidade):** refere-se a uma localidade geográfica;
- **Malware:** um tipo de TTP que representa um código malicioso;
- **Malware Analysis (Análise de Malware):** metadados e resultados de uma análise particular de um malware ou família de malwares;
- **Note (Nota):** usado para textos informativos adicionais que ofereçam maior contexto ou análises adicionais que não se categorizam em outros Objetos;
- **Observed Data (Dados Observados):** diz respeito às informações sobre entidades de cibersegurança como arquivos, sistemas e redes;
- **Opinion (Opinião):** uma correção ou crítica adicionada por outra entidade da instância STIX sobre determinado Objeto;
- **Report (Relatório):** coleção estruturada de inteligência de ameaças focada em um ou mais tópicos, como descrições de um ator malicioso, um malware ou TTPs, incluindo contextos e detalhes relacionados;
- **Threat Actor (Ator Malicioso):** indivíduos, grupos ou organizações com intenções maliciosas;
- **Tool (Ferramenta):** software legítimo usado por atores maliciosos para ataques;
- **Vulnerability (Vulnerabilidade):** falha em um software que pode ser explorada por um ator malicioso.

Peças de um quebra-cabeça

Os Objetos do STIX são estruturados em um JSON e, novamente, podem ser combinados de forma a criar um diagrama de relacionamento. A ideia por trás desse padrão é que tais diagramas de relacionamento criem ligações de inteligência cada vez mais amplos e interconectados. Confira abaixo um exemplo de JSON de um Objeto do tipo Campanha:


```
{
  "type": "campaign",
  "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "spec_version": "2.1",
  "created": "2016-04-06T20:03:00.000Z",
  "modified": "2016-04-06T20:03:23.000Z",
  "name": "Green Group Attacks Against Finance",
  "description": "Campaign by Green Group against targets in the financial services sector."
}
```

Logo acima, temos um exemplo gráfico de relacionamento entre diferentes objetos estruturados pela linguagem STIX que pode ser usado para entender como tais peças do quebra cabeça se encaixam para gerar inteligência compartilhada de ameaças. Um Indicador indica tanto um Ator Malicioso quanto uma Campanha, que, por sua vez, é atribuída ao Ator Malicioso e tem como alvo uma determinada Vulnerabilidade. Idealmente, cada peça desse quebra-cabeça seria adicionada por um membro em uma instância STIX — eis a importância da colaboração bidirecional para que todos consigam se proteger contra riscos cibernéticos.

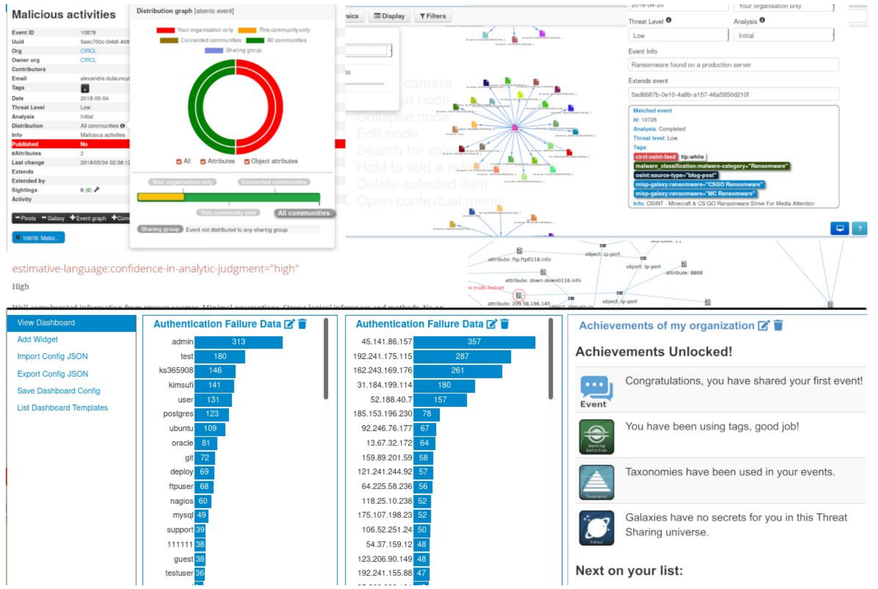
MISP: o maior framework de compartilhamento de inteligência do mundo

Outra plataforma altamente conhecida no mercado — e uma das mais utilizadas — é a Malware Information Sharing Platform (MISP). Diferente da CybOX e da STIX, não se trata de uma linguagem, mas sim de uma solução de código aberto para compartilhar, armazenar, correlacionar e analisar indicadores de comprometimento (Indicators of Compromise ou IoC). Ela possui uma interface de usuário bem mais amigável e podem ser criadas diversas instâncias para grupos específicos — trata-se da solução utilizada, aliás, pelo **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)**.

O projeto foi iniciado em junho de 2011 por Christophe Vandeplas, que estava frustrado com a forma, na época, em que os IoCs eram compartilhados: de forma não-organizada por emails ou via documentos PDF que não poderiam ser lidos e compreendidos de forma automática por um sistema computadorizado. A guinada veio em 2012, quando a OTAN se interessou pelo projeto e contratou um desenvolvedor para atuar no sistema em regime full-time.

Como já citamos, o grande trunfo do MISP é sua interface gráfica mais amigável e acessível, facilitando a criação, atualização e colaboração em eventos e atributos de indicadores. Além disso, sua API é flexível o suficiente para permitir sua integração com outras soluções, oferecendo uma biblioteca em Python (PyMISP) que é de fácil operação. Também é possível exportar dados no padrão STIX, caso haja necessidade.

Hoje já existem incontáveis comunidades MISP que aceitam novos membros, sendo que a maioria delas é focada em setores, interesses ou regiões gráficas específicas. Como exemplo, podemos citar a **NATO MISP Community** (instância oficial da OTAN para troca de informações entre os países membros da aliança), o **FIRST MISP Community**, o **Danish MISP Community** (específico para empresas dinamarquesas) e o **Cyber Security Sharing & Analytics (CSSA)**, cuja origem é alemã e tem foco em ameaças industriais.



Em busca de um *trade-off* mais justo

Marcos Sêmola
Cybersecurity Partner
EY

Em sua longa trajetória como consultor de cibersegurança com grande vivência no mercado brasileiro, como você avalia o cenário nacional quando o assunto é colaboração entre empresas para troca de conhecimentos e inteligência sobre ameaças? Sabemos que tal colaboração existe, mas ela é bem estruturada e efetivamente eficaz?

Quando a gente fala do mercado brasileiro, nós não podemos ignorar o fato de que o Brasil, uma cultura latina, recebe o efeito de uma baixa maturidade em prevenção de uma maneira geral. Além disso, não podemos descartar as especificidades dos setores; existem alguns mais maduros e mais conscientes, com maior tracionamento para os assuntos ligados à segurança da informação.

Olhando para essas características culturais e as específicas de setores, percebemos um descolamento entre o Brasil e outros países — principalmente aqueles do bloco europeu, onde essa cultura de normas, padrões, conformidade e prevenção é mais madura —, mas também vemos descolamentos entre setores, tendo a área financeira como uma dos mais maduras, acompanhado por um bloco intermediário e depois um bloco retardatário. E último ainda está muito reativo aos assuntos ligados à segurança da informação (mesmo que as notícias dos jornais tenham trazido esse tema para o café da manhã de todo líder empresarial).

Quando começamos a falar de cooperação, elas existem sim. Porém, são, em sua grande maioria, cooperações desestruturadas, quase que ad-hoc, e isso acontece também por essas razões que mencionei antes. O descasamento cultural entre os setores e as empresas faz — e fez — com que as corporações sequer tivessem ainda CISOs que ocupam essa função, mas não têm ainda o empoderamento, o orçamento, a equipe e nem a voz que o executivo ideal deveria ter.

Essa diferença também entre como cada empresa desenha a função de segurança e delimita o alcance, o poder, a voz, a influência, os recursos financeiros e humanos que essa função terá faz com que algumas corporações não encontrem pares compatíveis.

Então, passa a não ser natural trocar informações entre essas empresas e essas funções de CISO tão destoantes. No entanto, setores mais antenados e que têm executivos compatíveis em sua forma, extensão, autonomia e responsabilidade já se organizam sim. Eu mesmo, enquanto sócio da EY e consultor, atuo como uma ponte conectando CISOs que têm essas similaridades (principalmente no setor de energia, onde atuo com muito foco) e eles vêm trocando informações de forma bastante organizada. →

→ Para mim, esse é o cenário atual, e o cenário futuro é o de acelerar essa cooperação; mas lembrando sempre que a cooperação plena e consistente dentro de cada setor (e depois entre setores) só vai de fato acontecer se nós corrigirmos problemas estruturais com antecedência.

Isso inclui dar o tratamento estratégico adequado para a função do CISO, posicioná-lo adequadamente no organograma (colocando essa função, de preferência, lado-a-lado aos outros membros do board) com autonomia e o escopo da abrangência que mencionei.

Quando as empresas tiverem essa função com esse perfil bem posicionado, os CISOs vão olhar para os seus pares com igualdade e vão se sentir ambos motivados a se expor e se abrir para trocar, ajudar, dar e receber. Esse é o conceito.

Existem diversos padrões, frameworks e plataformas abertas (open source) para a criação de silos de compartilhamento de inteligência cibernética, e a impressão que fica é que nem sempre os profissionais de segurança da informação estão dispostos a "gastar" seu tempo aprendendo a operar e alimentando tais padrões, como STIX, TAXII etc. Você partilha dessa visão?

Essa pergunta tem uma complexidade em si própria. Cada empresa e cada CISO, mesmo convivendo com os desafios que citei na resposta anterior, têm problemas de segurança para resolver, têm respostas a dar para a liderança e têm recursos limitados.

Então, quando você olha para esse indivíduo, analisa a rotina dele e o dia-a-dia dele, percebe-se que ele tem o dilema de fazer escolhas: onde alocar seu tempo e os seus recursos financeiros e humanos.

É como se ele estivesse sendo convidado a ser o maestro de uma orquestra com muitos instrumentos diferentes, em um grande volume, operados por instrumentistas com características diferentes, e ele precisa garantir que tudo isso seja executado simultaneamente e produza um resultado harmônico.

Então, o problema é você imaginar que esse indivíduo — que já convive com uma série de problemas de grande porte, muitos deles oriundos de vulnerabilidades até antigas — tem que escolher entre continuar atuando onde ele sabe o que fazer e percebe retorno do investimento de suas ações ou investir em uma plataforma na qual ele vai produzir inteligência para poder estar mais bem preparado.

De certa forma, essa decisão implica em abrir mão de outros investimentos em outras áreas, e também acredito que gera uma sensação nesses CISOs de que eles estão enxugando gelo, pois, de certa forma, ameaça e vulnerabilidade é algo que dá mais do que xuxu na cerca. Você dá as costas, nasceu mais uma.

É muito difícil encontrar ou chegar em um estágio em que você diga: bom, já fiz um investimento e agora vou colher os frutos dele. Trata-se de um investimento contínuo. →

Em busca de um *trade-off* mais justo

Marcos Sêmola
Cybersecurity Partner
EY

→ Então, eu procuro colocar a probabilidade a meu favor nessas análises. Eu acredito que a utilização dessas plataformas e o investimento das pessoas, empresas e CISOs em criar uma inteligência cibernética vai acontecer quando esse for um esforço compartilhado. E eu não me refiro apenas ao compartilhamento entre empresas: eu acho que isso pode até nascer do setor público.

O Exército Brasileiro tem investido muito em defesa cibernética, em laboratórios e centros de estudo, e acho que isso pode ser a amálgama que conectará grandes empresas àquelas que têm compatibilidade em tamanho, energia, budget, equipe etc., para aí sim cada um poder oferecer um pouco de doação de competência e esforço para construir uma base de inteligência cibernética mais rica, ampla e eficiente.

Eu acredito, de fato, que esse é o melhor caminho para tornar viável e efetivo o investimento nesse tipo de plataforma e de conhecimento. Enquanto isso não acontecer, as empresas acabam optando por beber na fonte de parceiros de negócio que tenham esse tipo de serviço e que normalmente são empresas globais, justamente porque se beneficiam dos aprendizados que eles obtêm. Isso gera um conhecimento de ameaças que se converte em um serviço de valor para os clientes.

Os eventos do setor também acabam se tornando, mesmo que sem querer, um espaço para a troca de experiências e inteligência. Ainda assim, levando em consideração vivências em grandes conferências do ramo, nem todas as empresas/executivos se sentem à vontade para falar abertamente sobre como consertaram as infiltrações em suas casas, preferindo escondê-las da visita. Como você enxerga essa questão?

Essa pergunta me acompanha em muitos dos meus 23 anos de experiência em segurança da informação. Eu participo desses eventos há muito tempo, inicialmente aprendendo, assistindo, e posteriormente como keynote. Mas tenho uma análise bastante crítica sobre isso.

Falamos, pregamos e ensinamos que segurança é confiança. Quando uma empresa desenvolve uma governança de segurança da informação ou de riscos, ela está construindo confiança em sua cadeia produtiva: confiança com seus investidores, acionistas, clientes e parceiros. Ela está exalando confiança nas relações governamentais e com outras empresas. Isso não é nenhum segredo.

Quando você fala de um evento, você presume que alguém orquestrou um ambiente que vai reunir pessoas que tenham competências, experiências, práticas, ensinamentos, dúvidas e necessidades, todas no mesmo lugar, ao redor de um único tema: gestão de riscos de segurança da informação. Até aí, tudo bem.

Só que, de certa forma, as empresas, além de serem (em certa medida) concorrentes, a depender do caso, talvez falte um ambiente que ofereça um espaço seguro, justamente de confiança e com pessoas de confiança, para que elas possam se sentir confortáveis em revelar uma fragilidade, uma preocupação, e até mesmo comentar sobre uma decisão equivocada que tenham tomado, para evitar que o colega da empresa amiga possa evitar o mesmo erro. →

Em busca de um *trade-off* mais justo

Marcos Sêmola
Cybersecurity Partner
EY

→ Então, muitas dúvidas passam pela cabeça daqueles que frequentam esses eventos, e eu posso falar isso de carteirinha. Eu também frequentei esses eventos com esse chapéu. Quando estamos ali, todos os que vão querem ensinar e aprender, querem ser ouvidos e querem falar.

Mas aí sempre surge uma questão na cabeça: será que eu estou falando para a pessoa certa? Será que eu deveria expor isso? Qual garantia eu tenho de que essa informação não vai chegar a outros públicos, expondo a minha empresa? Será que estarei sendo irresponsável ao trazer esse nível de detalhes?

É uma pergunta comum e legítima. Todos que vão a um evento desses passam por esse dilema e acabam optando por ficar em silêncio ou simplesmente limitar os detalhes ao nível que não os comprometa, mas que também não ajuda a resolver ou ensinar aos demais sobre o ocorrido. É sempre aquela conversa rasa, e o curioso é que, depois de tantos anos em eventos de segurança, eu percebo a mesma coisa entre os palestrantes.

Quando você ouve alguém falando sobre um case, é um case raso. Por que? Pelas mesmas razões: ele vai falar sobre a empresa dele, mas tem medo de quem vai receber aquilo e como vão usar aquela informação. Ou o palestrante é um fornecedor de soluções que recebeu o "ok" de um cliente para falar do case dele, mas em certo nível, sem ir muito a fundo.

O cliente não quer abrir o diferencial competitivo ou revelar detalhes que, à primeira vista, são positivos, mas podem ser vistos como negativos dependendo do ângulo.

No fim, um vai lá fingindo que vai ensinar e o outro fingindo que vai aprender. O resumo da ópera é: ou os eventos e as próprias pessoas encontram termos e condições para tornar aquele fórum mais seguro e confiável (mesmo que isso represente criar subgrupos de trabalho que possam abertamente falar sobre os temas, ensinar e aprender), ou nós vamos depender — como acontece desde então — que as próprias pessoas se auto-regulem.

Me lembro de centenas de eventos nos quais você passa seis horas ouvindo generalidades e, em algum momento, você puxa duas ou três pessoas para um café que confiam entre si e aí sim temos algo que agrega.

Todo mundo ali troca figurinhas e sai feliz do evento — não necessariamente pelo que o congresso como um todo produziu, mas por ter proporcionado aquele ambiente que rompeu a agenda e permitiu que eles pudessem conversar entre si.

Levando em consideração toda a sua experiência e visão sobre o assunto, quais barreiras esbarramos atualmente na colaboração e compartilhamento de inteligência cibernética? Qual seria o melhor caminho para tornarmos tal troca de informações mais eficiente e frequente?

Vou abusar da minha prepotência de achar que conheço de metaverso, tokenização, NFT, blockchain e inovação — embora eu tenha experiência em investir, mentorear e acelerar startups, além de experiência em todos esses campos que citei. Acho o suficiente para eu arriscar um palpite. →

Em busca de um *trade-off* mais justo

Marcos Sêmola
Cybersecurity
Partner
EY

→ Acho que, além do que falei anteriormente sobre como vencer as barreiras da colaboração e do compartilhamento, poderíamos criar uma governança mais estruturada para que isso acontecesse. E essa governança poderia beber da fonte dessas ferramentas da web 3.0. Vamos pensar no conceito.

É o conceito de garantir, como governança, que todos que se doarem irão de fato se beneficiar na mesma proporção de sua doação.

É como se, por exemplo, fôssemos capazes de criar um ambiente controlado (e por esse motivo mais seguro do que falar abertamento em um congresso ou grupo de WhatsApp) no qual as pessoas, empresas, CISOs e suas equipes fossem estimuladas a compartilhar a informação e contribuir efetivamente com algo de valor.

Isso teria a confiabilidade de um blockchain, um time stamping, uma autenticação e que poderia ser convertido em tokens.

Ou seja, eu vou tokenizar uma atividade colaborativa de troca de conhecimento de segurança da informação. E eu vou remunerar esses voluntários com tokens que podem valer coisas — não apenas dinheiro, mas também acessos privilegiados, seja até mesmo em eventos.

Imagine: a empresa, equipe ou profissional que mais contribuiu com inteligência cibernética neste semestre vai poder participar de uma reunião com os outros cinco CISOs das empresas cujas equipes também contribuíram no mesmo nível.

É uma maneira de conectar o mundo real ao virtual de uma forma estruturada e que produza um benefício mensurável para aqueles que doarem tempo e compartilharem inovação. É quase que um ecossistema baseado no mesmo conceito de organização autônoma descentralizada (DAO), onde inclusive as pessoas, equipes e profissionais que contribuírem, por terem tokens, têm maior influência nas tomadas de decisão sobre a evolução da própria plataforma.

É gamificar a segurança da informação no conceito mais amplo possível. Tirar das empresas e dos CISOs a impressão de que eles, ao se doarem em um evento ou dando informações, estarão se expondo a troco de nada, sem garantia de retorno; mas sim que eles conseguirão uma moeda de troca, nem que tal moeda seja uma orientação similar. Um *trade-off* entre risco e benefício que seja compensador.

Podemos até nos aventurar em uma visão mais ambiciosa, que é plugar essa cooperação ao setor público de tal maneira que o próprio governo reconheça o benefício desse conhecimento e recompense as empresas na forma de redução de tributos. Mais uma vez: tudo com tokenização, de forma segura e controlada.

Em busca de um *trade-off* mais justo

Marcos Sêmola
Cybersecurity
Partner
EY

E no resto do mundo, como estamos?

Panorama Internacional

Conheça o Cybersecurity Information Sharing Act of 2015 (CISA)

Nos Estados Unidos, o compartilhamento entre o setor público e empresas privadas é lei — embora tal cooperação seja 100% opcional, e não mandatória. A norma em si é a Lei de Compartilhamento de Informações Cibernéticas (**Cybersecurity Information Sharing Act ou CISA**) e foi aprovada em 2015 com o objetivo de "melhorar a segurança cibernética nos Estados Unidos por meio do compartilhamento aprimorado de informações sobre ameaças à segurança cibernética". Não confundir com a Agência de Cibersegurança e Segurança de Infraestrutura (Cybersecurity and Infrastructure Security Agency, que também atende pela sigla CISA).

A legislação foi criada justamente porque, até então, uma série de outras barreiras jurídicas dificultavam o compartilhamento de detalhes sobre incidentes cibernéticos. A normativa facilitou essa troca e incentiva que as corporações forneçam ao governo estadunidense inteligência sobre ataques sofridos, vulnerabilidades detectadas e métodos reativos contra atores maliciosos conhecidos — e cujas atividades podem representar perigos à segurança nacional.

Segundo um relatório divulgado em 2020 pelo Departamento de Segurança Interna dos Estados Unidos (Department of Homeland Security ou DHS), porém, o programa ainda precisa progredir para atingir o nível esperado de quando ele foi colocado em prática. O padrão criado pela norma, o Compartilhamento Automatizado de Informações (Automated Information Sharing ou AIS) ainda carece de um número aceitável de usuários e participantes. Confira um trecho de análise realizado por um auditor no dito relatório:

O CISA aumentou o número de participantes do AIS, bem como o volume de indicadores de ameaças cibernéticas compartilhados desde o início do programa em 2016. No entanto, o CISA fez progressos limitados melhorando a qualidade geral das informações que compartilha com os participantes do AIS para reduzir efetivamente as ameaças cibernéticas e proteger contra ataques.

A falta de progresso da CISA na melhoria da qualidade das informações que compartilha pode ser atribuída a vários fatores, como o número limitado de participantes do AIS compartilhando indicadores cibernéticos com a CISA, atrasos no recebimento de padrões de inteligência de ameaças cibernéticas e equipe insuficiente do escritório da CISA. Para ser mais eficaz, o CISA deve contratar a equipe necessária para fornecer divulgação, orientação e treinamento.

Isso significa que, mesmo mais de cinco anos após o estabelecimento da lei, ela ainda sofre de problemas estruturais que podem ser atribuídos à falta de interesse ou confiança das companhias privadas em abrir sua inteligência — mesmo de forma direta para os órgãos governamentais.

ISACs: os centros de compartilhamento ao redor do mundo

Não poderíamos deixar de citar também a existência daquilo que chamamos de Centro de Análises e Compartilhamento de Informações (**Information Sharing and Analysis Center ou ISAC**). Um ISAC nada mais é do que uma organização autônoma, sem fins lucrativos, que utiliza o framework e a linguagem de sua preferência para reunir e incentivar a cooperação na troca de informações sobre ameaças cibernéticas em determinado campo comercial. Existem diversos ao redor do mundo (embora os Estados Unidos seja líder no número de ISACs ativos), e podemos citar alguns dos mais importantes:

CANADÁ

- **Global Mining and Metals Information Sharing & Analysis Centre** (MM-ISAC)

EUROPA

- **European Energy - Information Sharing & Analysis Centre** (EE-ISAC)

ESTADOS UNIDOS

Nos EUA, temos o Conselho Nacional de ISACs, que organiza e padroniza a forma de atuação de todos os centros de compartilhamento existentes no país, mantendo uma lista atualizada em seu site oficial.

- **Automotive Information Sharing & Analysis Center** (Auto-ISAC): focada na colaboração entre montadoras de automóveis;
- **American Chemistry Council** (ACC): específico para empresas do setor químico e relacionados;
- **Aviation ISAC** (A-ISAC): voltado ao setor de aviação comercial;
- **Communications ISAC**: tem foco em informações relevantes ao setor de telecomunicações;
- **Downstream Natural Gas ISAC** (DNG-ISAC): exclusivo para companhias do ramo de distribuição de gás natural;
- **Elections Infrastructure Information Sharing and Analysis Center** (EI-ISAC): formado para pesquisar ameaças ao sistema eleitoral do país;
- **Financial Services ISAC** (FS-ISAC): específico para instituições do ramo financeiro;
- **Healthcare Read**y (antiga RxResponse): específico para o setor de saúde;
- **Health ISAC** (H-ISAC): também focado em questões de saúde;
- **Information Technology ISAC** (IT-ISAC): próprio para colaborações sobre infraestruturas de tecnologias da informação;
- **Maritime Transportation System Information Sharing and Analysis Center** (MTS-ISAC): formado para endereçar os desafios no setor de transporte marítimo.

Dentre muitos outros.

OPENCTI

Nome: OpenCTI

Local: Paris, França

Ano de fundação: 2018

Público: B2B

Sobre

A OpenCTI é um bom exemplo de como as soluções e iniciativas para o compartilhamento de ameaças cibernéticas estão, felizmente, se tornando cada vez mais modernas e com interfaces *user-friendly*. Criada na França em 2018, a plataforma é open source (ou seja, qualquer pessoa pode colaborar com seu desenvolvimento), mas destaca-se por ter uma apresentação digna de produto comercial.

Ela permite que seus usuários armazenem, organizem, visualizem e troquem conhecimentos sobre ameaças, tudo através de um modelo de dados consistente baseado no Stix 2.0 e um hiper gráfico que facilita o entendimento de correlações.

"O primeiro objetivo da plataforma OpenCTI é fornecer um poderoso banco de dados de gerenciamento de conhecimento com um esquema reforçado especialmente adaptado para inteligência de ciberameaças e operações cibernéticas. Com várias ferramentas e recursos de visualização, os analistas podem explorar todo o conjunto de dados girando na plataforma entre entidades e relações", explicam os responsáveis pelo projeto.

Embora já tenha quatro anos de idade, a OpenCTI ainda pode ser considerada "um bebê", com um roadmap ambicioso pelo frente. Novas features planejadas incluem recursos completos de investigação de entidades e melhorias na contextualização de observáveis.

"O objetivo é criar uma ferramenta abrangente que permita aos usuários capitalizar informações técnicas (como TTPs e observáveis) e não-técnicas (como atribuição sugerida, vitimologia etc.) enquanto conecta cada peça de informação à sua fonte primária (um relatório, um evento MISP etc.).

Todos os indicadores estão vinculados às ameaças com todas as informações necessárias para que os analistas compreendam completamente a situação, o papel desempenhado pelos observáveis em relação à ameaça, a fonte da informação e a pontuação do comportamento malicioso", concluem.

Um problema global a ser resolvido

Rafael Narezzi
Especialista em Segurança Cibernética
4CyberSec & Cyber Security Summit

Como um profissional globalmente renomado no mercado de cibersegurança, com interações constantes com outros executivos e grandes empresas da área (além de instituições sem fins lucrativos e órgãos governamentais), como você enxerga, a nível mundial, os esforços em colaboração e compartilhamento de threat intelligence na atualidade?

Primeiramente, nós ainda não possuímos mesma maturidade para compartilhar ameaças. Existe um grande receio em compartilhar certas threats, pois elas podem se tornar inteligência para outros. Por exemplo, imagine que eu sou um banco e você é outro. Obviamente, não vou querer compartilhar com você os meus problemas e as minhas brechas, pois nós competimos no mercado.

No entanto, se você observar o cibercrime, ele é mais organizado do que nós. Isso quer dizer que, da mesma maneira que gostaríamos de poder ter uma threat intelligence aberta, na qual todos poderiam compartilhar informações e vulnerabilidades (inclusive existem até alguns programas que fazem isso), os criminosos infelizmente estão na nossa frente.

Organizações desses criminosos não têm de cumprir leis, eles simplesmente compartilham informações em uma velocidade que, mesmo se nós quiséssemos ter uma plataforma que o mundo inteiro colaborasse, para nós, existiriam grandes barreiras governamentais, barreiras privadas e barreiras de anonimizar dados. São muitos os empecilhos para que isso possa acontecer em uma velocidade tão rápida para nós, que seguimos as leis.

Hoje há fóruns, grupos de Telegram, inúmeras comunidades na internet nos quais incidentes são compartilhados. Inclusive, eu participo de um grupo de especialista de cibersegurança. No entanto, as vulnerabilidades de uma empresa a gente não compartilha. Empresas e organizações não querem que saibam dos seus problemas para não serem atacadas. Mas eu acho que essa maturidade tem de evoluir.

Eu sei que uma grande empresa do ramo petrolífero possui um canal no qual pessoas compartilham esses problemas. Eles ouvem e abrem ao público.→

→ A própria Universidade de Cambridge tem um datawarehouse muito bom de threat intelligence da Inglaterra inteira, mas não global. Ou seja, já começa a ter dificuldades para fins de pesquisas, não para fins comerciais. Vamos supor que eu começo a compartilhar e você começa a ter a parte comercial envolvida, então tudo que a gente compartilha de inteligência tem um valor agregado.

Óbvio que não temos muito tempo, temos muito barulho acontecendo, ao mesmo tempo em que existem muitas coisas boas no sentido que seria inteligência para uma empresa. Mas quem filtra isso e conduz essa parte operacional? Há um custo para isso também.

O custo para o cibercrime é vantajoso e lucrativo. Para nós, já é o contrário: o custo é muito alto e não somos tão eficientes no compartilhamento, então é a nossa grande desvantagem.

Historicamente falando, embora tenhamos frameworks, padrões e plataformas abertas para o compartilhamento desse tipo de inteligência, eles costumam ser pouco intuitivos ou amigáveis, exigindo um esforço para a compreensão de seu funcionamento, o que pode desestimular a prática de colaboração. Porém, nos últimos tempos, temos presenciado o nascimento de soluções e ferramentas mais automatizadas e acessíveis. Você acredita que precisamos de uma maior evolução no mercado com mais startups focadas em tal propósito?

Eu acredito que o modelo de negócio precisa ser transformacional. Vou citar como o cibercrime trabalha e porque para eles é vantajoso, porque para a indústria privada estamos um pouco atrás e isso não é tão vantajoso como gostaríamos, eles estão à frente disso.

Primeiro que, com os criminosos compartilhando informações entre si, a probabilidade dos ataques deles terem sucesso é muito maior.

Com isso, falamos sobre o lucro ser assertivo, ou seja, eles conseguirão atingir o objetivo através da inteligência que criaram entre eles. Logo, também vão conseguir o resultado lucrativo, que é o financeiro que tanto buscam. Então esse é o primeiro ponto.

Mas por que ainda não está tão bom se temos empresas e open? Porque está muito segregado, essa inteligência está muito distribuída. Então, tem uma plataforma que vai ter uma inteligência maior do que a outra, com a chance de ser menos eficaz. Em certo aspecto, tratamos de muitas indústrias, então fica muito difícil agregar esse valor.

Vamos imaginar cinco empresas que são especialistas em cyber threat intelligence e esse é o produto que eles vendem. De certo, eles não vão compartilhar isso, eles ganham agregando esses dados e passando numa visão executiva ou ilustrativa para aquelas empresas; por isso, não terão interesse em compartilhar sem fim lucrativo. Logo, o lucro sempre está à frente. →

Um problema global a ser resolvido

Rafael Narezzi
Especialista em Segurança Cibernética
4CyberSec & Cyber Security Summit

→ Para de repente solucionarmos isso, deveria existir uma multiplataforma na qual as pessoas que compartilham ganham créditos por isso, talvez dinheiro ou investimentos, até mesmo do governo ou da sociedade privada. Dessa forma, quanto mais vocês construíssem, mais fomentam essas informações, esse threat intelligence seria melhor.

Porém, como tudo que é open source de graça ou que não tem valor, torna-se também uma arma na mão dos criminosos, porque da mesma maneira que eu vou ter essa inteligência, ele também poderia ter.

Então, temos que criar um certo benefício, um programa que tenha vantagens para as empresas terem a chance de colaborar. Sobre a vantagem desse programa citado, já sabemos qual é: vamos ter a melhor informação sobre um determinado threat. Porém, ninguém quer pagar para trocar informações ou manter atualizado o custo de operação, então, envolve a questão do custo benefício que não é do interesse das empresas.

Eles provavelmente vão investir em várias outras alternativas ao invés desse intel, algo que se adeque mais aquele particular nicho daquela empresa.

Nesse sentido, não é necessário saber o que está acontecendo em uma indústria, por exemplo, ou em um PLC. De certa maneira, não é muito útil. Então é importante existir um certo incentivo para que possa ser criado um canal. Como também, pode ser que não vai existir, porque entra em dilemas comerciais.

Por exemplo, querer ocultar as fraquezas e as informações de seu competidor. Logo, torna-se uma operação muito complicada, e é justamente onde os criminosos têm vantagens. Uma vez que eles não tem ética, podem compartilhar o que quiserem, fazer o que quiserem, pois para eles compartilhar informação privada é mais fácil. Então, infelizmente a vantagem está do lado criminoso.

Da mesma forma, enquanto nos Estados Unidos temos o Cybersecurity Information Sharing Act (CISA) de 2015 regulamentando o compartilhamento de inteligência sobre ciberameaças, faltam iniciativas governamentais desse tipo em outros países, incluindo aqui no Brasil. Um maior incentivo governamental e legislativo sobre tal assunto poderia impulsionar uma maior colaboração não somente entre empresas, mas também entre o setor público e o privado?

Eu acho um programa interessante, porém, a gente sabe que não são todos que estão se filiando. Não é algo que você vai conseguir fazer, por exemplo, uma escola de natação aderir a esse programa, porque não vai ter recurso. Então é interessante a gente fazer um pouco esse comparativo.

Já as empresas grandes que têm mais capacidade, que têm certo capital e recursos de pessoas para fazer, podem até se associar, compartilhar, informar o governo, fazer o dever de uma empresa perante a sociedade. Mas por que isso não acontece? Porque não são todas as empresas que vão dedicar tempo e esforço para alimentar uma fonte de dados que poderia ser fantástica, →

Um problema global a ser resolvido

Rafael Narezzi
Especialista em Segurança Cibernética
4CyberSec & Cyber Security Summit

→ sem reconhecer qual o retorno que ela vai ter. Então é muito difícil, por via do governo, ter essa essa estrutura. Caso você compare com uma lei de proteção de dados, por exemplo, vamos falar da General Data Protection Regulation (GDPR) aqui da Europa.

Colocamos ela, fizemos um regulamento que deixamos claro que se tratavam de leis, e, caso fossem descompridas, seriam penalizados. O que pudemos acompanhar desde 2008 por dentro dessa lei mudou bem pouco em comparação ao que estava. As empresas estão mais voltadas a se proteger, a não vazar dados por conta das multas. De certa forma, em relação aos danos reputacionais está bom, porém não resolveu o problema.

Eu falo isso, porque a indústria tem que ser aplicada em um todo. E o que eu pude notar na GDPR, por exemplo, é justamente que as empresas grandes que são mais atacadas, possuem certos recursos para poder ter um melhor entendimento da lei e aplicar barreiras ou proteções necessárias, além de saber lidar em casos de incidentes. Vou dar um exemplo, de uma empresa aérea aqui do Reino Unido. O que ela teve de prejuízo por vazamento de dados foi equivalente ao quanto ela gasta de papel higiênico no ano para todas as aeronaves.

Então, será que com o regulamento e com as multas a gente consegue o objetivo principal de parar ou ter uma maturidade melhor de cibersegurança? Pelo que temos visto, as empresas estão aumentando essa capacidade, mas não em um nível que seja apto. Também o nível de vulnerabilidade, o nível de ataque à tecnologia que envolve cada vez mais rápido, é uma corrida que nunca vai ter fim.Então, acredito que estamos muito atrás nesse sentido de inteligência compartilhada.

Outra coisa importante de comentar é sobre os diferentes regulamentos. Mesmo que você tenha um nos Estados Unidos, outros países possuem diferentes leis e diferentes entendimentos da internet.

Existem países que irão entender tal coisa como uma violação da privacidade deles, e não vai te deixar fazer. E se caso esses dados caem numa mão de um stent ou de um outro grupo hacker? Também vai ser usado contra você. Assim, tudo tem o benefício a favor.

De certo, se eu tenho a ciência que todo ano todo mundo está tendo aquele problema, então eu vou atacar naquele problema, usando como uma fonte de inteligência para também criar outros tipos de ataque ou outras situações. Por exemplo, em um banco chileno, eles criaram uma smoke bomb. Ou seja, estava acontecendo um ataque, criando uma visão para que o time se dedicasse a mitigar um incidente, fazendo com que a atenção do banco ficasse em outro local, para que entrassem pela porta do fundo, através de outra vulnerabilidade. Então, a criatividade humana é algo que nunca vamos conseguir competir.

No Brasil, já temos de forma eficientemente estruturada a Lei Geral de Proteção de Dados (LGPD), que obriga a notificação de incidentes de exposição de dados às autoridades competentes; no caso, a Autoridade Nacional de Proteção de Dados (ANPD). →

Um problema global a ser resolvido

Rafael Narezzi
Especialista em Segurança Cibernética
4CyberSec & Cyber Security Summit

→ Você acredita que a lei possa servir como pontapé e evoluir para se tornar uma ferramenta de coleta de inteligência de ameaças com base na análise dos incidentes reportados?

Temos visto muitos incidentes acontecendo no Brasil e como aumentou o nível deles. É igual ao que falei sobre a Lei Geral de Proteção de Dados: até então, as multas vão existir, mas não quer dizer que vão aumentar a segurança. Porém, muitas empresas que já deveriam estar aptas, adequadas e capazes de estarem mais à frente da cibersegurança, na verdade, não estão.

Dessa forma, acredito que a lei não trouxe o impacto que a gente necessitava, justamente pelos incidentes e pelo tempo de demora de recuperação que estamos vendo. E outra, estamos em formação dessa agência para que elas possam executar a sua operação. Então fica muito difícil.

Vou citar um outro exemplo, um comparativo que é muito importante. Veja bem, a Irlanda que é um país significantemente bem menor que o Brasil, teve tando caso de GDPR que não conseguiu lidar com eles. Já o Brasil, como seria? Já que é bem maior que a Irlanda, e estamos falando de uma agência nacional para cobrir todo o país. Se todos os ataques que tivessem fossem declarados (como sabemos muito bem que não são) e sim somente os que caem na mídia, talvez as coisas mudariam. Na mídia, sabemos de muitos incidentes que já aconteceram que não foram declarados, inclusive de órgãos governamentais ou de órgãos de escolas privadas.

Dessa forma, conseguimos ver que ainda existe esse problema, e eu acredito que talvez isso não vai mudar daqui para frente, mesmo estabelecendo essa lei. Porque a demanda vai exigir que a agência tenha braços particulares em toda a sua operação e já sabemos que ela não tem.

É uma agência nova; não que isso tenha alguma coisa a ver, mas imagina se eles tiverem cinco incidentes para liderar, com a equipe que eles têm hoje, como que faz? Então, eles vão acabar escolhendo do mais significativo, para o menor significativo ou talvez do mais impactante, para o menos impactante.

Vamos supor que um laboratório teve vazamento de dados, como são dados pessoais e mais de saúde, a gente talvez vai investigar esse cara primeiro, do que quem estava no hotel que se trata somente de dados pessoais. Um comparativo meio ilustrativo, para a gente pensar.

A lei veio para ajudar sim, mas será que ela está resolvendo todos os problemas? Será que as empresas realmente investiram em contratar todo esse pessoal que era necessário? A gente sabe que a demanda nesse segmento só tem aumentado, sabemos de tudo isso, mas a falta de maturidade das empresas na parte de cibersegurança ainda está muito baixa. →

Um problema global a ser resolvido

Rafael Narezzi
Especialista em Segurança Cibernética
4CyberSec & Cyber Security Summit

→ Inclusive, uma recente pesquisa da Gartner diz que o próximo nível educacional que precisa ser executado é a nível de board para os executivos entenderem o que é cibersegurança, uma coisa que 50% não sabem. E temos que mudar daquela conversa de que o executivo não tem que saber. Pelo contrário, na economia digital ele é obrigado a saber, a entender as consequências e é obrigado a ser responsabilizado pelas mesmas.

De fato, é muito diferente o impacto quando acontece em uma empresa brasileira e quando acontece em uma empresa estrangeira. Então, podemos falar de situações em que o CEO pode ser mandado embora de uma empresa ou ele mesmo pede para sair. Temos que tirar essa cultura que o mundo inteiro possui, às vezes, da falha humana ser penalizado ao time de segurança. Ou também, a antiga frase de alguns falarem para colocar um seguro em tudo que falhar. O seguro ajuda, mas seria ele a sua melhor resposta para toda a situação de cibersegurança que está vivendo?

Ele não vai te trazer a reputação de volta, não vai trazer as noites mal dormidas e também não vai trazer a dor que seu time passou a lidar com uma crise. Então é importante a gente falar disso.

Voltando novamente à sua experiência global com executivos e empresas do setor, em qual estágio de maturidade você encaixaria o Brasil a respeito desse assunto? O quanto estamos mais evoluídos ou atrasados, em comparação com outros mercados, em sermos abertos uns com os outros sobre nossas próprias fraquezas, violações, estratégias de proteção etc.?

Como eu disse anteriormente, não vou citar rankings ou comparativos, porque eu acho que a gente vive um problema global. Então assim como é um problema presente por aqui onde estou e no Brasil também, o nível de maturidade, infelizmente, não está em nível global. Também não está onde deveria estar.

O mundo inteiro não teve uma educação digital, então, existem muitos executivos trabalhando em empresas que não têm o entendimento do que é o mundo digital, do que é a segurança digital e do que é a economia digital. Então, a gente continua vivendo em um mundo onde, talvez, ainda não enxergaram que evoluímos para esse futuro. Apesar de ter melhorado muito nesses últimos anos, continuamos tendo os mesmos problemas que tínhamos antes.

Por exemplo, continuamos trazendo desenvolvedores sem ele nem ter cadeira, inclusive, muitas universidades não tem uma cadeira de segurança. Então, quanto tempo será que ainda vai demorar para termos uma consolidação e mais uma visão de segurança dentro da parte de desenvolvimento? Fica complicado se você já não aplicar em design security dentro de softwares ou capacidades tecnológicas, já que vivemos em uma economia digital.

Não temos um número suficiente de profissionais no mundo para cobrir tudo, por mais que esteja melhor do que o passado, evoluindo cada vez mais, você também consegue ver que o nível de vulnerabilidades e o nível de conhecimento dentro de riscos, dentro de cibersegurança tem triplicado ou quadruplicado no ano. →

Um problema global a ser resolvido

Rafael Narezzi
Especialista em Segurança Cibernética 4CyberSec & Cyber Security Summit

→ Logo, estamos tendo mais pesquisas, mais desenvolvimento nessa área de cibersegurança e mais conhecimento de vulnerabilidades que não tínhamos antes. Porém, ainda estamos em desvantagem, porque o número é superior ao que conseguimos ter de profissionais.

O segundo exemplo vem de cima. Se eu trabalho em uma empresa e mesmo que o executivo invista horrores de dinheiro na página de cibersegurança, mas eu não acredito, eu não entendo. É como se eu transferisse isso e alguma coisa acontecesse por responsabilidade daquela pessoa, em vez de ser mais uma responsabilidade em conjunto.

Então, é importante a gente pensar que a cibersegurança é uma coisa que todos têm que participar, desde o executivo lá de cima, até o cara lá de baixo.

Vimos vários casos de insider threat, então, o que adianta eu falar que a gente faz, sendo que não fazemos nada e qualquer coisa que acontecer eu jogo a culpa para o meu time de segurança que está errado? Então, é importante que, em tudo o que a gente fizer, pensar sempre na parte educacional.

Vivemos uma sociedade hoje totalmente digital, uma grande maioria não teve a educação base do que todos viveram, a era do computador. Óbvio que as novas gerações vão chegar, talvez tenhamos um grande outro problema, que a nova geração que só queira ser consumidor, e também vamos passar grandes problemas no futuro, pois se a nova geração não quer entender como as coisas funcionam, se só quiserem consumir, vamos ter dificuldade em contratar pessoas para manter as coisas funcionando.

Um problema global a ser resolvido

Rafael Narezzi
Especialista em Segurança Cibernética
4CyberSec & Cyber Security Summit

Nome: CrowdSec

Local: Montrouge, França

Ano de fundação: 2019

Público: B2B

Investimento recebido: US$ 6,76 milhões

Investidores: Reflexion Capital, Breega

Sobre

Outra solução interessante que merece ser destacada neste relatório é a CrowdSec, uma plataforma colaborativa de sistema de prevenção de intrusão (Intrusion Prevention System ou IPS) que se baseia em inputs da própria comunidade de cibersegurança para criar a sua própria base de dados de confiança. A ideia é simples: ao compartilhar endereços IP usados para atividades maliciosas contra a sua empresa, você ajuda a criar uma comunidade cada vez mais forte com uma blocklist sempre atualizada em tempo real.

Vale lembrar também que a CrowdSec é open source, podendo ser integrada a diversos sistemas operacionais (Linux, FreeBSD), serviços (IP Tables, NFTables, Nginx, Apache, Caddy), linguagens/frameworks (Wordpress, PHP, JS) e instâncias de outras plataformas como Docker, Amazon Web Services, Google Cloud e Cloudflare.

A CrowdSec se orgulha de já estar presente em 145 países, ostentar 4,9 mil estrelas no GitHub e ter detectado 1,9 milhões de IPs maliciosos nesses poucos anos de vida que possui.

Aliás, apesar dos poucos anos de vida, é interessante perceber que, mesmo se tratando de uma ferramenta livre, sem fins lucrativos e de código aberto, a CrowdSec conseguiu angariar o aporte significativo de US$ 6,76 milhões dos investidores Reflexion Capital e Breega. A companhia também tem feito aparições em diversos eventos (físicos, virtuais e híbridos) de renome no setor, incluindo a edição 2021 da Black Hat USA.

Tendências

Colaboração existe, mas ainda precisa de maior estrutura e organização

As informações levantadas neste relatório e os insights oferecidos pelos especialista entrevistados não deixam dúvidas de que, de fato, já existe sim um cenário de colaboração e cooperação entre empresas e executivos para a troca de inteligência sobre ameaças cibernéticas. Contudo, ela é pouco estruturada e, consequentemente, menos eficaz do que poderia ser.

O compartilhamento de experiências, indicadores de comprometimento, TTPs e práticas defensivas e reativas **ainda é limitado a silos bem específicos que geralmente dizem respeito a um determinado setor comercial ou grupo fechado de corporações** que, por algum motivo, razão ou consequência, consideram justo firmarem uma parceria entre si com esse objetivo em comum.

No geral, a sensação que fica é a de que falta maior confiança — maior confiança dentro de um congresso de cibersegurança para que os participantes se sintam mais confortáveis em se expor, maior confiança entre executivos para comentar sobre suas fragilidades e maior confiança no mercado de segurança da informação como um todo para entender que revelar detalhes sobre um incidente não significa assinar um atestado de fraqueza.

Claro, **a revelação de tais detalhes deve ser sempre feita da maneira mais "limpa" e consciente possível**, sendo removidos todos e quaisquer dados pessoais ou sensíveis antes que esse compartilhamento ocorra.

Além disso, a fragmentação de padrões, frameworks e plataformas disponíveis para criar bibliotecas de inteligência pode ser entendida como uma barreira para fomentar essa atividade — como bem observado pelo especialista Marcos Sêmola, para um perfil "padrão" de CISO, é difícil decidir entre focar seus recursos humanos (geralmente escassos) entre atividades cotidianas de retorno mensurável e a criação dessa threat intelligence.

Nossos leitores certamente perceberam que este é um relatório que não usou gráficos e estatísticas, tampouco apresentou números sobre o crescimento de startups relacionadas à sua temática. O motivo é simples: **esse é um mercado praticamente ignorado, com pouquíssimas iniciativas que visam facilitar a cooperação** entre profissionais de cibersegurança, empresas, fornecedores de soluções e o setor público.

Não há nada no tipo no Brasil e, mesmo a nível internacional, é praticamente impossível mensurar corretamente os investimentos que tal departamento recebe. Apesar disso, é indiscutível que plataformas mais amigáveis e atualizadas, como os exemplos OpenCTI e CrowdSec, podem fazer a diferença em curto e a longo prazo.

Uso de novos conceitos tecnológicos e conexão governamental

Apesar dos problemas preocupantes que citamos na página anterior, há uma luz no fim do túnel. Os insights levantados neste material podem servir como ponto de partida para a criação de frameworks e soluções que utilizem novos conceitos tecnológicos para facilitar o compartilhamento de inteligência cibernética. **A proposta de flertar a colaboração de CTI com a onda da tokenização, por exemplo, é deveras interessante** — dois de nossos especialistas, aliás, concordam que "ter algo em troca" na proporção de sua colaboração é algo que certamente iria incentivar muitas empresas e profissionais.

Uma conexão com o setor governamental e iniciativas públicas podem muito bem ajudar a impulsionar a cooperação. Embora a redução de tributos e impostos para companhias que auxiliem na detecção e resposta de ameaças pareça um cenário bastante distante, é interessante sempre mantermos essas ideias fora da curva em perspectiva para um futuro que pode não estar tão distante.

No fim das contas, a evolução na colaboração e no compartilhamento de inteligência de ameaças cibernéticas depende de uma série de fatores — alguns culturais e alguns tecnológicos. **Trata-se de um desafio que o mercado precisa discutir com maior frequência** e chegar a soluções que tragam benefícios para todos — caso contrário, continuaremos perdendo essa guerra infinita para o cibercrime altamente organizado.

Cybertechs

Glossário de categorias

Categorias

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

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

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

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

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

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

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

Categorias

IDENTITY & ACCESS MANAGEMENT

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

BLOCKCHAIN

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

FRAUD & TRANSACTION SECURITY

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

SECURITY CONSULTING & SERVICES

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

GOVERNANCE, RISK AND COMPLIANCE

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

CLOUD SECURITY

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

Agradecimentos

Este report conta com o apoio da:

Cybertech Report