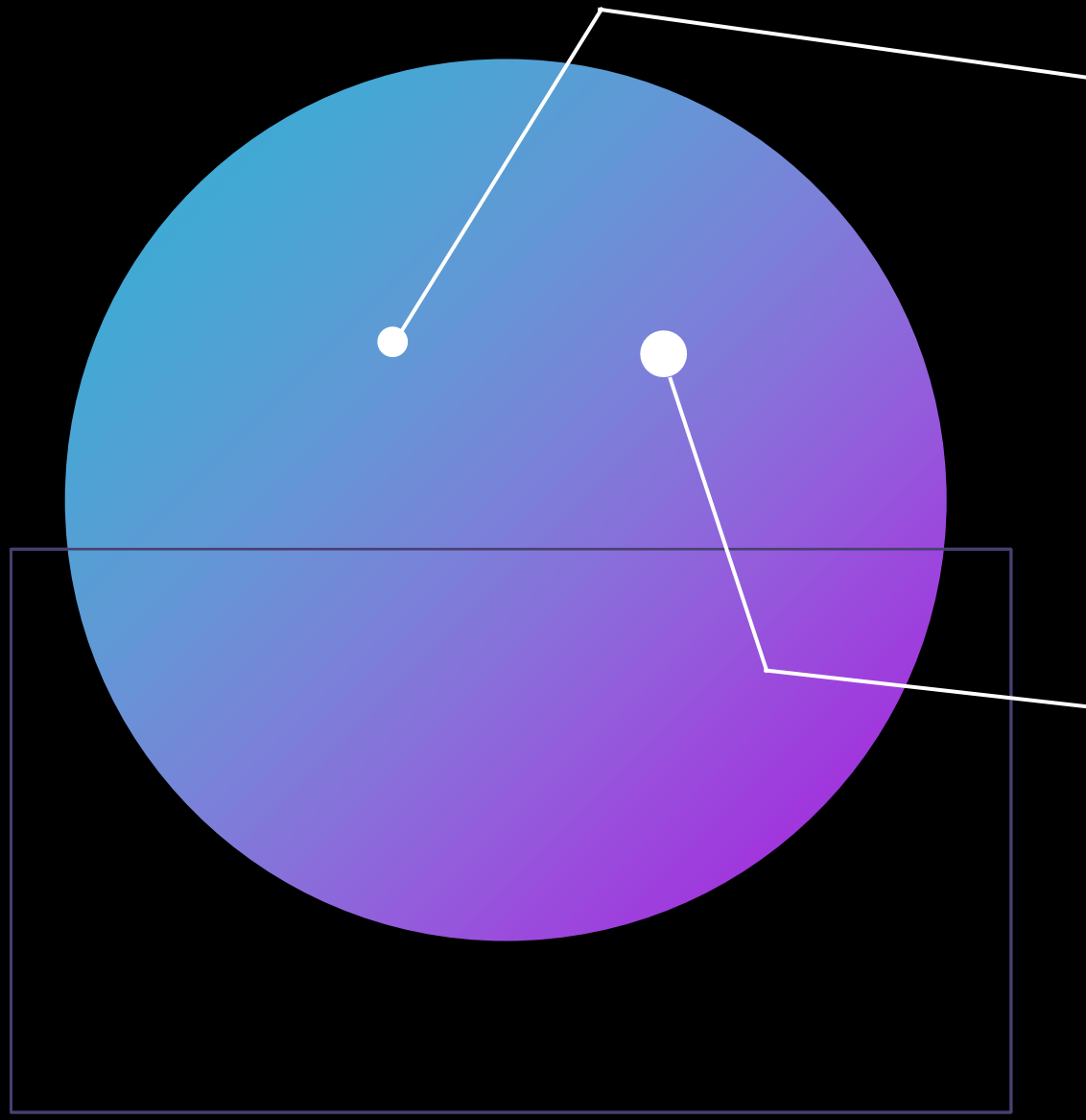
Prime

CCS-A

Vetores e Fontes de Inteligência

Vetores

- Termo para os métodos ou meios que um invasor pode utilizar para comprometer um sistema.
- Exemplos:
  - Wireless;
  - Email;
  - Mídia social;
  - Cadeia de Suprimentos;
  - Fontes de dados externa;
  - Mídia removível;
  - Nuvem.
- Ou seja, se houver uma maneira de mover dados para o seu sistema, isso pode se tornar um vetor.



Acesso Direto

- O invasor tem acesso direto ao sistema.
- Pode ser:
  - Ataque interno;
  - Ataques externos, por meio de servidores web.
- Por conta do acesso direto, precisamos pensar no princípio do privilégio mínimo.
- Se um estranho de fora acessa o sistema, automaticamente todas as entradas são potencialmente perigosas.

Wireless

- Exploração do sistema por meio de uma rede ou dispositivo wireless vulneráveis.
- Pode incluir uma wireless 802.11 ou outra tecnologia sem fio como o Bluetooth.

Wireless/Redes sem fio são simples.

- A facilidade de conexão traz uma série de problemas de segurança.

O acesso sem fio proporciona ao invasor:

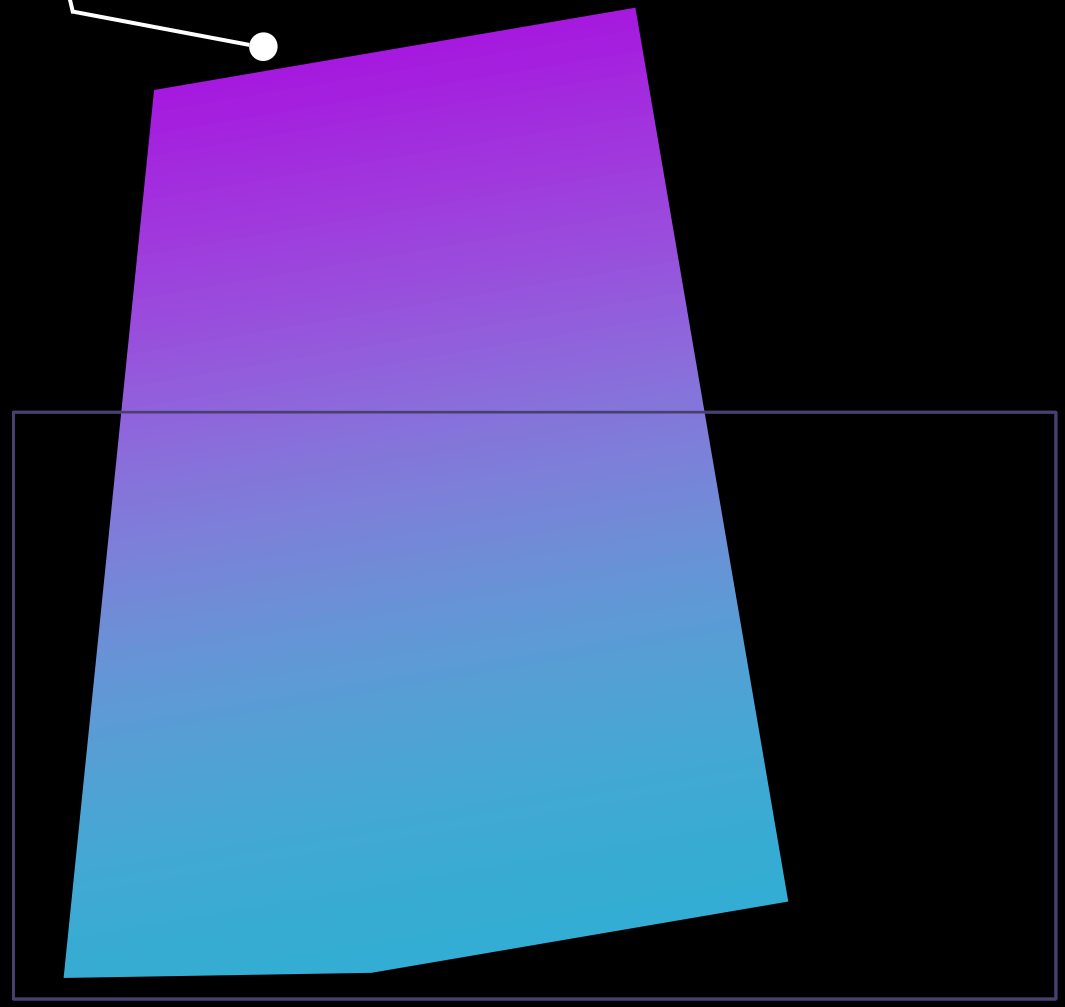
- Não precisar mais de acesso físico.

E-mail

Um dos vetores preferidos para ataques de engenharia social.

É querido pela interação que gera com o usuário.

- Se uma mensagem convincente é incluída, os usuários podem clicar nos links ou abrir o anexo.



Cadeia de Suprimentos

- Método para comprometer a segurança de sua organização, invadindo os fornecedores.
- Inserção de exploit nos componentes dos fornecedores.
- Usa a cadeia de suprimentos como um agente involuntário no ataque.

Um invasor pode encontrar um meio para inserir seu código de ataque na cadeia de suprimentos.

- Exemplo:

O caso SolarWinds Orion (18k clientes).

- Os ataques contra cadeia de suprimentos são ameaças reais e não podem ser interrompidos com políticas ou contratos.

Mídias Sociais

- Pode ser um vetor para ataques de engenharia social.
- Características:

Conecta um invasor diretamente a um usuário;

Não há verificações de segurança como vistas com e-mail corporativo.

- Invasores podem fazer pessoas clicarem em URLs abreviadas, com um redirecionamento indesejado.

Mídia Removível

- Como um vírus inserido em um pen drive ou flash card.
- Vantagens para o invasor:
  - Armazenamento pequeno;
  - Onipresente;
  - Não requer habilidades para serem conectadas a um PC.
- Um invasor pega um dispositivo de armazenamento USB e coloca o módulo de ataque para que o mesmo possa ser executado.
- Colocar o dispositivo USB em um local propenso à descoberta é um tipo de ataque comum.

Nuvem

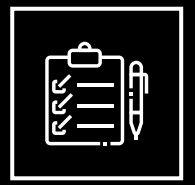
- Normalmente protegemos mais nossa rede local do que a nuvem.
- Tal motivo para os hackers tentarem invadir é a relação de confiança que temos na nuvem.

Busque soluções em nuvem que terão uma conexão VPN entre a nuvem e sua rede local.

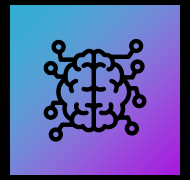
- Servidores em nuvem precisam estar tão protegidos quanto seus sistemas locais.
- É preciso incluir proteções antivírus nos arquivos.

Fontes de Inteligência de Ameaças

Nenhuma empresa tem os recursos para se proteger de tudo.



É preciso apostar seus recursos na inteligência de ameaças.

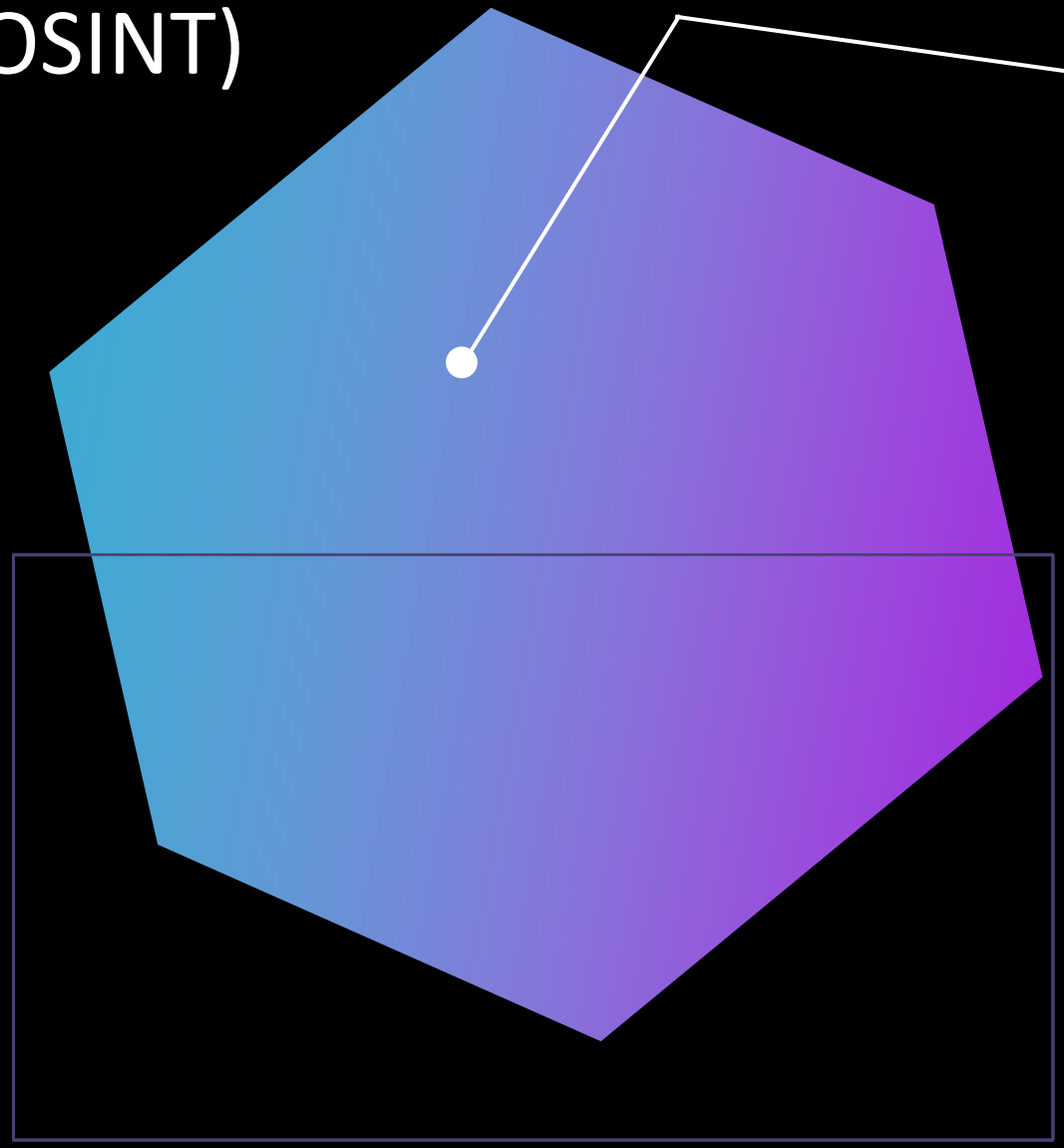


A inteligência de ameaças é a coleta de informações de várias fontes, incluindo:

- Fontes de inteligência de ameaças, onde obtemos essas informações (e.g. Fontes públicas).

Inteligência de Código Aberto (OSINT)

- Dados de inteligência coletados de fontes públicas sem violar quaisquer leis de direitos autorais ou privacidade.
- Ampla gama de fontes públicas de informação sobre a atividade atual de segurança cibernética.
- Muitas estão “escondidos” na deep e na dark web (96%).
- Existe uma grande variedade de feeds de código aberto:
  - Compartilhamento Automatizado de Indicadores do Departamento de Segurança Interna (DHS);
  - Portal InfraGard do Federal Bureau of Investigation (FBI);
  - SANS - Internet Storm Center (ISC);
  - VirusTotal;
  - Cisco;
  - Shodan.



Ferramentas Fechadas ou Proprietárias

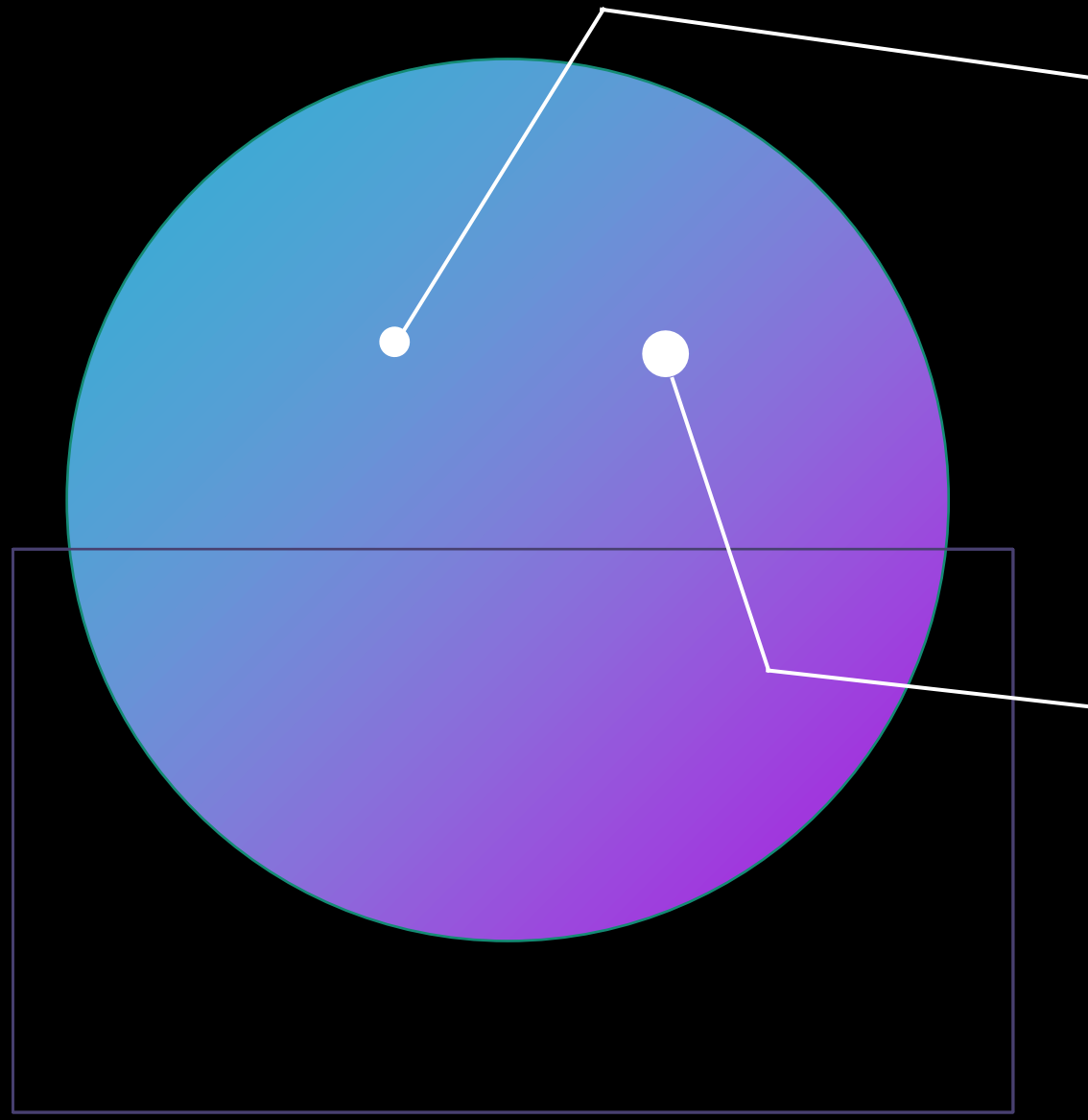
- Ferramentas comerciais como fontes de inteligência de ameaças, semelhante à OSINT, porém, pagas.
- Normalmente coletam e exibem as mesmas informações que as ferramentas OSINT, mas têm um custo para as empresas.
- Formatos comuns incluem:
  - CSV;
  - XML;
  - JSON;
  - STIX.
- Outros fatores importantes incluem:
  - Frequência com que os dados são atualizados;
  - Quais setores são foco dos dados.
- Agentes de ameaças têm padrões e operam por setor, fazendo com que as exposições de setor difiram de um para o outro.

Banco de Dados de Vulnerabilidades

- Útil para pesquisar vulnerabilidades de um determinado produto.
- Relata cada uma das vulnerabilidades e fornece uma classificação de risco baixo, médio ou alto.
- Para corrigir vulnerabilidades ou fornecer uma solução defensiva.
- Existem vários bancos de dados de vulnerabilidades – Exemplo:
  - National Vulnerability Database (NVD).
  - Metasploit.
- NVD faz parte da NIST (Publicação de um Framework de boas práticas de Cybersecurity).

Centros de Compartilhamento de Informações (Públicos/Privados)

- Sites para compartilhar informações sobre ameaças comuns às organizações;
- Público para qualquer um ou privado à uma empresa. Exemplos de centros públicos e privados:
  - Centros de Compartilhamento e Análise de Informações (ISACs);
  - Organizações de Compartilhamento e Análise de Informações (ISAOs);
  - Infragard (FBI) – Free.
- O compartilhamento é anonimizado.
- A análise é realizada por profissionais altamente qualificados e é compartilhado o custo entre membros.



Dark Web

Parte da Internet que tem seu acesso restrito por meio de métodos específicos (Tor) de ofuscação (anonimato).

Quando um navegador está na dark web, o acesso é anônimo, por conta do protocolo .onion (domínio).

Dark Web não é Deep Web:

- Deep Web não é indexada pelos mecanismos de pesquisa,.
- Deep Web tem acesso restrito.
- Deep Web é facilmente acessível pelo navegador.

Indicadores de Comprometimento (IoCs)

- Indicações de que um sistema foi comprometido por atividade não autorizada.
- Os IoCs deixam rastros para ajudar a identificar a presença de um ataque em um sistema.
  - Quem atende um incidente precisa coletar e processar dados destintos e criar uma imagem significativa do estado atual de um sistema.
- Ferramentas como o YARA podem usar um conjunto de assinaturas/IoCs e escanear seu ambiente.
- Se o comprometimento é detectado: o atendente pode se concentrar nas informações e documentar totalmente a natureza e o escopo do problema.

Compartilhamento Automatizado de Indicadores (AIS)

- Compartilhamento de informações sobre ameaças em tempo real. A inteligência é enviada e consumida.

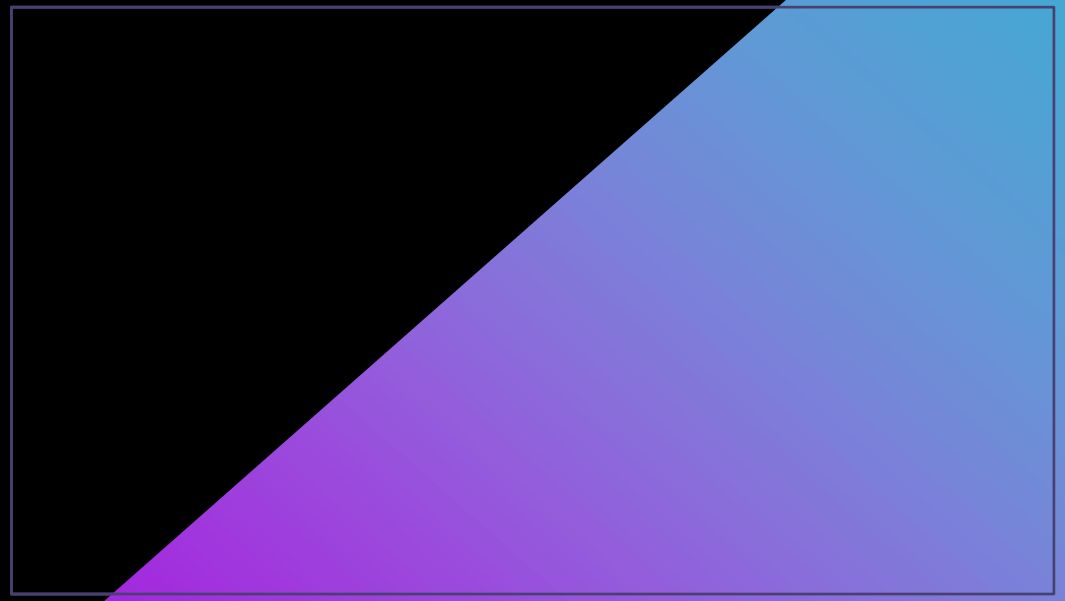
Método de indicador de ameaças cibernéticas automatizado e bidirecional utilizado para relatórios.

Objetivo:
Comoditizar a coleta de informações de inteligência de ameaças.

- O sistema AIS usa as especificações:
  - Structured Threat Information Expression (STIX);
  - Trusted Automated Exchange of Intelligence Information (TAXII).

STIX e TAXII

- Criados para comunicar informações sobre ameaças cibernéticas.
- Ambos fornecem um conjunto de padrões orientados pela comunidade:
  - STIX (Expressão Estruturada de Informações sobre Ameaças) – Linguagem estruturada padronizada.
  - TAXII (Troca Automatizada Confiável de Informações de Inteligência) – Serviço de mensagem que permitem= o compartilhamento de informações sobre ameaças.



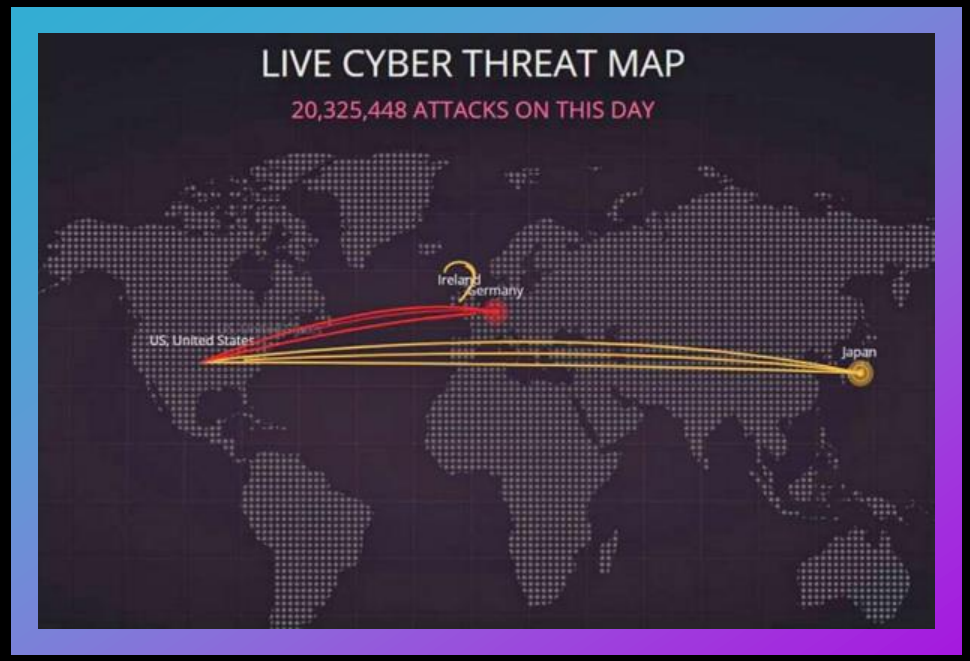
Análise Preditiva

- Função: examinar novas ameaças que surgem por algum fator específico.
- Prever e determinar as etapas futuras envolvidas em uma ameaça.
- Ativar medidas de proteção antecipadamente.
- Uso de informações de inteligência de ameaças para antecipar o próximo movimento de uma ameaça.
- Como é feito:

Curadoria de grandes quantidades de dados de várias fontes;

Cada setor tem diferentes agentes de ameaças, e cada conjunto de agentes de ameaças tende a utilizar métodos específicos.

Mapas de Ameaças



https://threatmap.checkpoint.com/

Repositórios de Arquivos/Códigos

- Exemplo: GtiHub. Com código ou um arquivo que você pode usar para testar e rastrear problemas.

Repositórios funcionam como locais comunitários para as pessoas trabalharem juntas e desenvolverem software.

Podem oferecer uma fonte de informações aos adversários sobre como o software é construído.

Podemos usar as mesmas fontes para examinar as capacidades de algumas ferramentas que poderão ser usadas contra você.

No desenvolvimento interno de software, mantém-se um repositório (e versões) de onde todos os módulos vieram para rastrear problemas.

Fontes de Pesquisa

- Uma alternativa é encontrar fontes de informação que sejam verificadas quanto à veracidade.
- A inteligência de ameaças possui várias fontes.
- **Exemplos:**

Fornecedores e grupos locais do setor;

Feeds de vulnerabilidades e ameaças;

Conferências e revistas acadêmicas;

Entradas de solicitações de comentários (RFCs).

Sites de Fornecedores

- Todo fornecedor quer ser um parceiro valioso em seu problema de segurança e te enviar um orçamento.
- Eles têm equipes de marketing (um site lindo) que vendem seus serviços.
- Sites de fornecedores parecem estar repletos de informações.

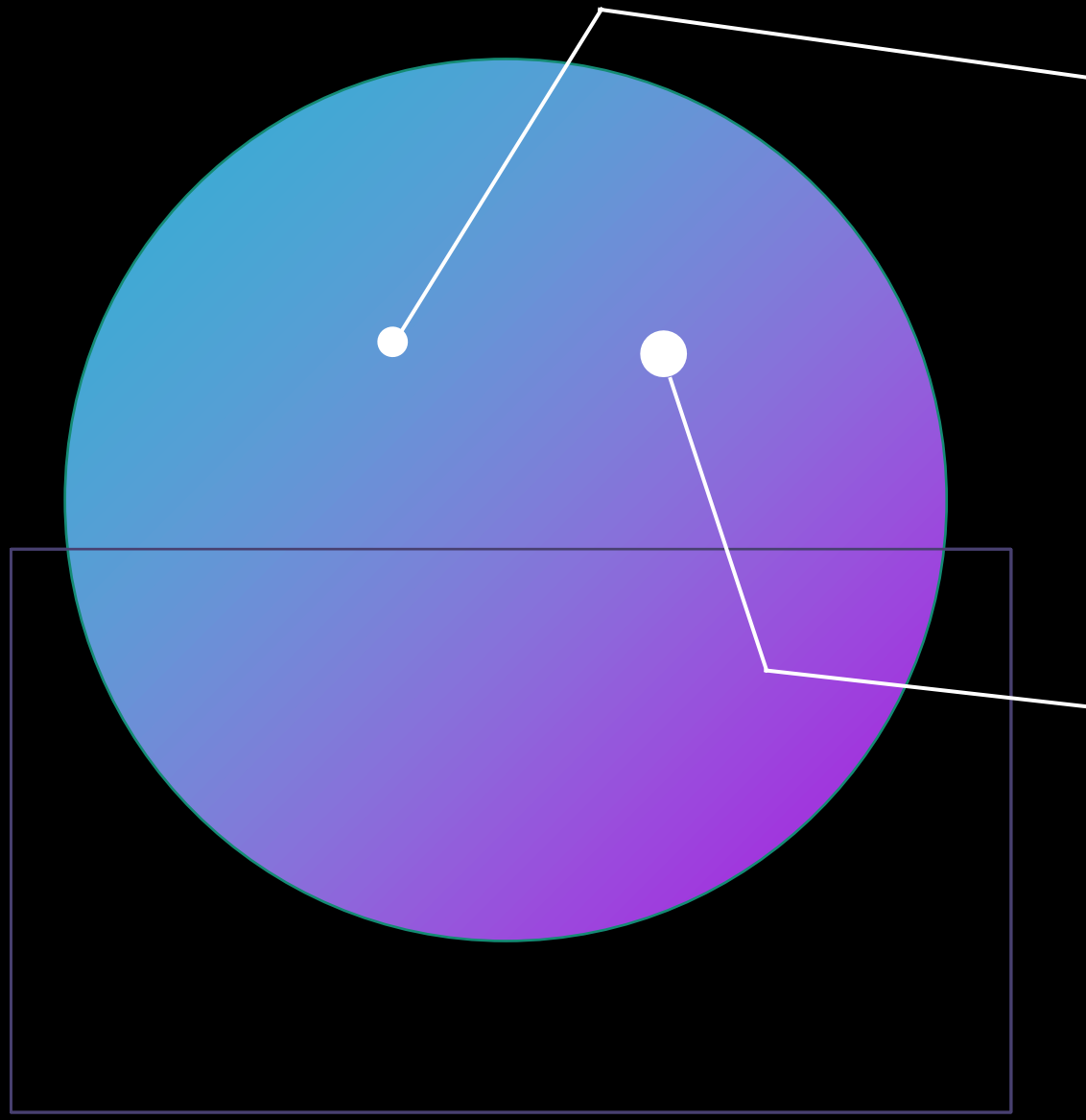
Dica: Você precisa descobrir quais são as fontes deles.

Feeds de Vulnerabilidades

- A qualidade dos feeds de vulnerabilidades pode variar muito de uma fonte pra outra.
- Para garantir que você tenha boas fontes, é importante verificar vários problemas em seus feeds, incluindo:
  - Qual é a fonte dos dados?
  - Quais características específicas do feed?
- Vários feeds são quase que obrigatórios para se manter atualizado continuamente sobre ameaças encontradas.
- **Exemplos:**

https://cve.mitre.org/cve/data_feeds.html

https://nvd.nist.gov/vuln/data-feeds



Feeds de Ameaças

Muito parecidos com os feeds de vulnerabilidade.

Importante: Entender de onde vêm e como a informação foi verificada.

Existe a necessidade de vários feeds não sobrepostos.

Conferências

- Acadêmicos realizam pesquisas e apresentam seus artigos nestes eventos.
- Discutem as tendências atuais em relação a ameaças e vulnerabilidades.

Vantagens:

- Os prazos para submissão de conferências são mais curtos que revistas;
- A apresentação do material da conferência é um bom jeito de obter feedback;
- Networking.

Revistas Acadêmicas

- As revistas acadêmicas tem duas questões delicadas:
  - Atualidade;
  - Aplicabilidade.
- **Desvantagens:**
  - Publicações podem durar meses ou anos para serem concluídas;
  - A revista pode estar desatualizada no momento em que for publicado;
  - Acadêmicos raramente são especialistas na prática.

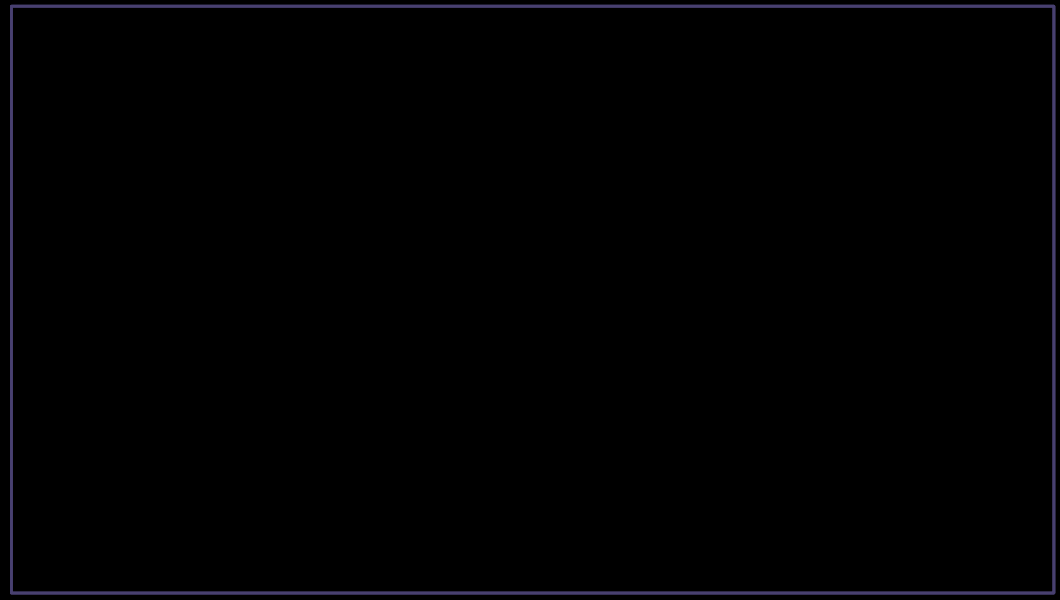
Solicitações de Comentários (RFC)

- Conjuntos de padrões para definir como a Internet e os protocolos do World Wide Web são estabelecidos e gerenciados.
- Características:

Gratuitos e disponíveis abertamente.

Documentos formais, atualizados e aprovados.

Listam detalhes, por exemplo, dos padrões dos protocolos.



Grupos de Indústria Local

- Recurso valioso sob algumas perspectivas.
- Características:

Boa fonte de informações práticas sobre ameaças;

Sólida fonte de informações em rede;

- Motivo para adotar essa prática: A segurança cibernética gira em torno do compartilhamento de informações.

https://digitalguardian.com/blog/top-50-infosec-networking-groups-join

Mídia Social

A mídia social é onipresente.

A comunicação com um contato em um site voltado para negócios como o LinkedIn pode levantar boas discussões.

A chave está na verificação das fontes de informação!

Lembre-se que o*caveat emptor* de advertência se aplica às redes sociais.
(o risco é do comprador)

VETORES E FONTES DE INTELIGÊNCIA

Táticas, Técnicas e Procedimentos Adversários (TTP)

- TTP – Descreve como os agentes de ameaças se organizam e orquestram seus esforços.
- Os hackers evoluem para utilizar métodos repetíveis que são eficazes.
- Os TTPs, ou padrões usados pelos adversários, são fundamentais em um programa de inteligência de ameaças.

A fonte é tudo!

OBRIGADO!

VETORES E FONTES DE INTELIGÊNCIA