Investigation using OSINT with a focus on Intelligence operations and Dark Web operations - Training

Joas Antonio dos Santos

Whoami

- Name:
- Job Title:
- Company:

Introduction OSINT

O que é OSINT?

- Open Source Intelligence (OSINT). É um modelo de inteligência que visa encontrar, selecionar e adquirir informações de fontes públicas e analisá-las para que junto com outras fontes possam produzir um conhecimento. Na comunidade de inteligência (IC), o termo "aberto" refere-se a fontes disponíveis publicamente.
- As fases que abrangem a coleta especializada segundo fontes e meios utilizados para a obtenção das informações englobam basicamente quatro técnicas. Convencionalmente separadas em três de cunho sigiloso e uma de natureza ostensiva. Nos países centrais, cerca de 80 a 90% dos investimentos governamentais na área de Inteligência são absorvidos por este estágio do ciclo. Os trabalhos acadêmicos que versam sobre Inteligência definem as técnicas de coleta através de acrônimos derivados do uso norte-americano: HUMINT (Inteligência de fontes humana), SIGINT (Inteligência de sinais), IMINT (Inteligência de imagens) e OSINT (Inteligência de fontes abertas).

What is OSINT?

- Open source intelligence (OSINT). It is an intelligence model that aims to find, select and acquire information from public sources and analyze it so that, together with other sources, it can generate knowledge. In the intelligence community (IC), the term "open" refers to publicly available sources.

- The sources encompass the collection according to techniques and means used to collect basic information four. Conventionally separated into three of a confidential nature and one of an ostensible nature. In central countries, about 80 to 90% of government investments in the area of intelligence are integrated by this stage of the cycle. The liaison works that deal with Intelligence define as collection techniques through acronyms results of the American use: HUMINT (Intelligence of human sources), SIGINT (Intelligence of northern sources), IMINT (Intelligence of images) and OSINT (Intelligence of sources open).

Sobre o OSINT?

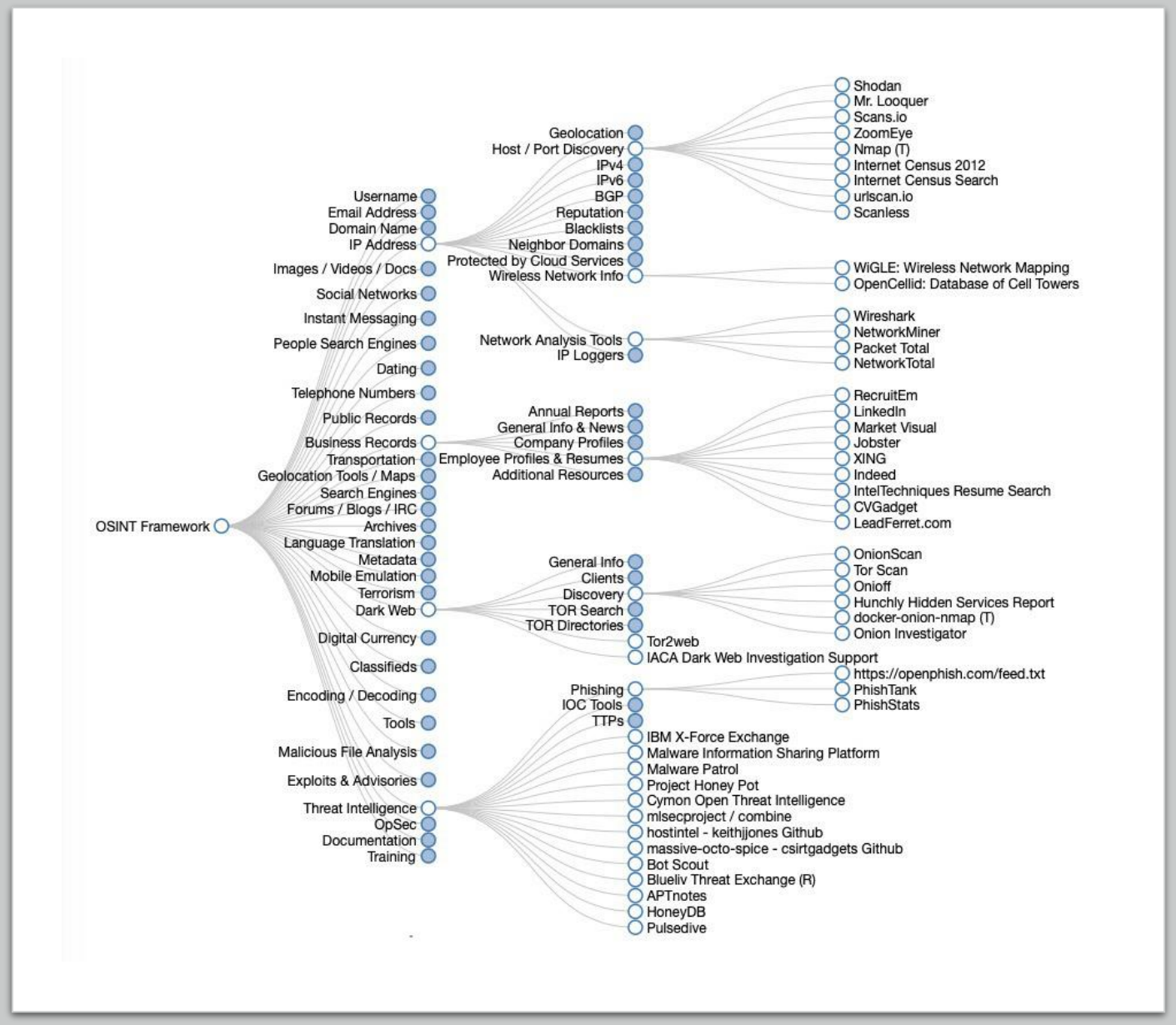
- A inteligência de código aberto é anterior à Internet. Os governos há muito usam jornais e transmissões posteriores para rastrear os planos e atividades militares, políticas ou econômicas de adversários em potencial.
- OSINT é de baixo risco, barato e muitas vezes altamente eficaz, como o consultor de inteligência corporativa Cameron Colquhoun escreveu em um artigo da Bellingcat sobre a história do OSINT.
- Como sugere Colquhoun, o OSINT saiu de moda após a Segunda Guerra Mundial, com as agências de inteligência se concentrando no mundo mais glamoroso e perigoso de HUMINT – inteligência humana ou espionagem – e SIGINT: sinais e inteligência eletrônica.
- Mas com o surgimento da internet e das mídias sociais e ferramentas online que podem filtrar grandes quantidades de informações, o OSINT agora é mais relevante do que nunca.

About OSINT?

- Open source intelligence predates the internet. Governments have long used newspapers, and later broadcasts, to track potential adversaries' military, political, or economic plans and activities.
- OSINT is low risk, cheap, and often highly effective, as corporate intelligence consultant Cameron Colquhoun has written in a Bellingcat article on the history of OSINT.
- As Colquhoun suggests, OSINT fell out of fashion after World War Two, with intelligence agencies instead focusing on the more glamorous and dangerous world of HUMINT – human intelligence or spying – and SIGINT: signals and electronic intelligence.
- But with the rise of the internet and social media, and online tools that can sift through vast amounts of information, OSINT is now more relevant than ever.

OSINT Framework

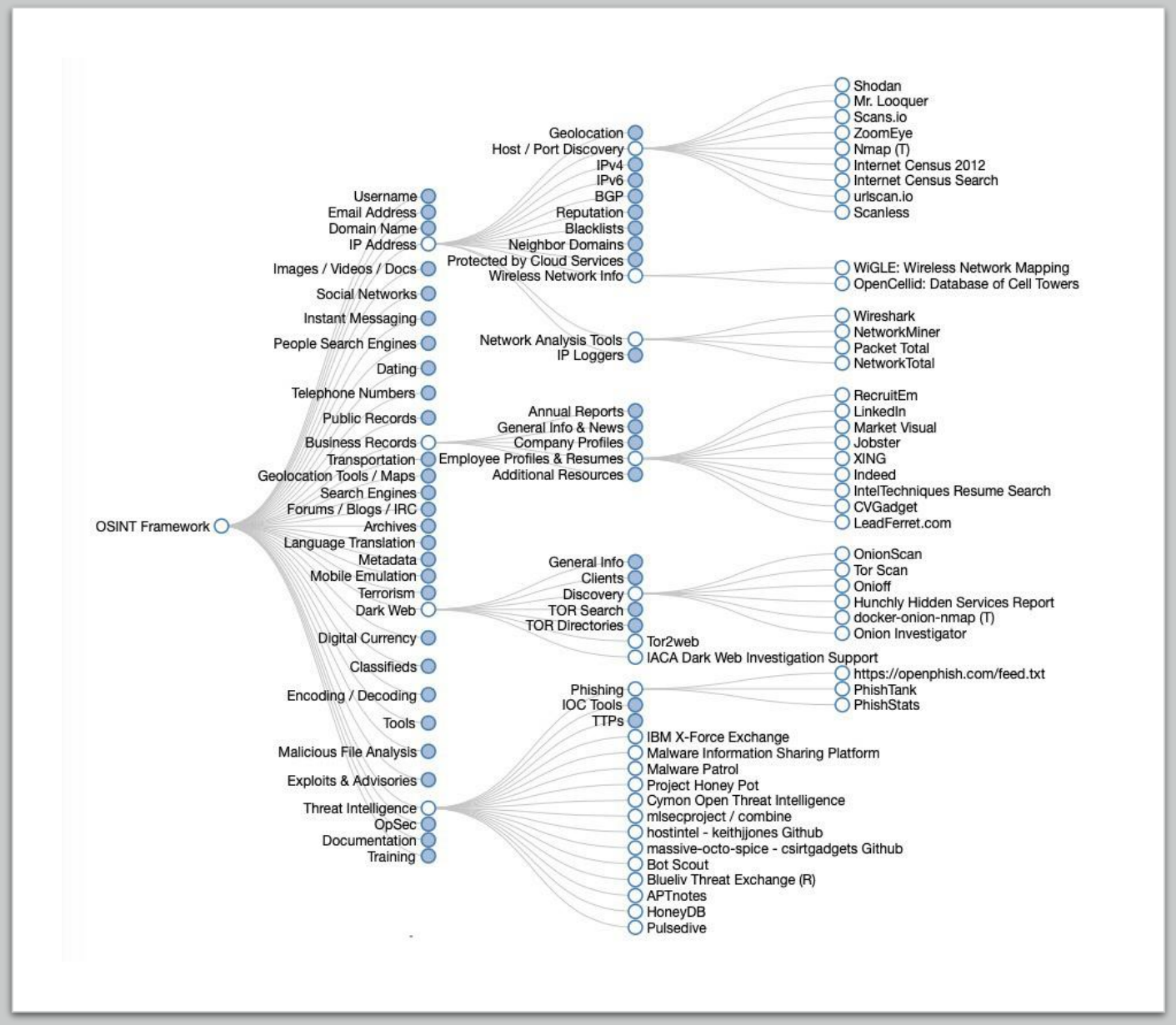
- OSINT framework focused on gathering information from free tools or resources. The intention is to help people find free OSINT resources. Some of the sites included might require registration or offer more data for $$$, but you should be able to get at least a portion of the available information for no cost.
- https://github.com/lockfale/OSINT-Framework

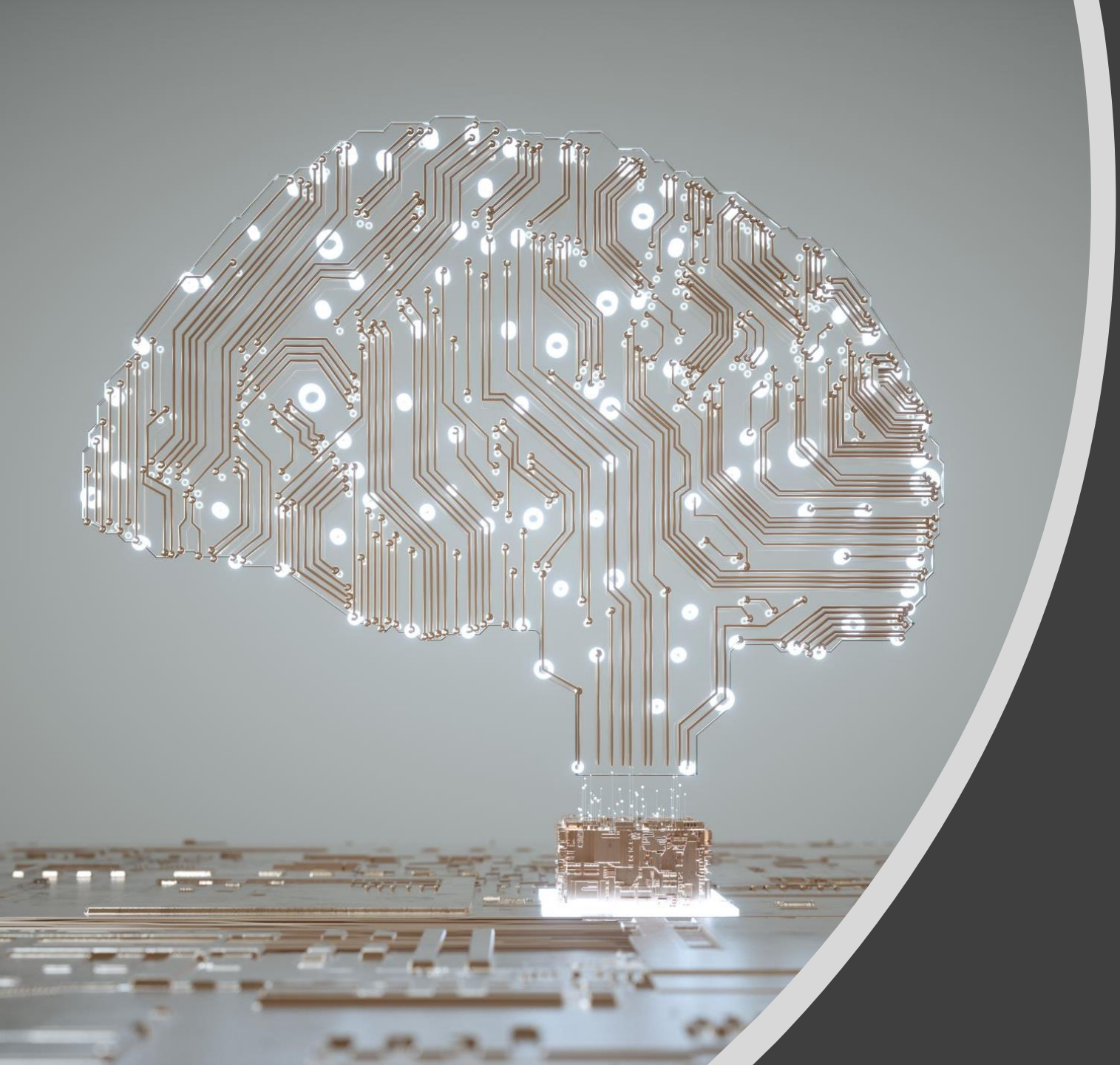


OSINT Framework

- Estrutura OSINT focada na coleta de informações de ferramentas ou recursos gratuitos. A intenção é ajudar as pessoas a encontrar recursos OSINT gratuitos. Alguns dos sites incluídos podem exigir registro ou oferecer mais dados por $$$, mas você poderá obter pelo menos uma parte das informações disponíveis gratuitamente.

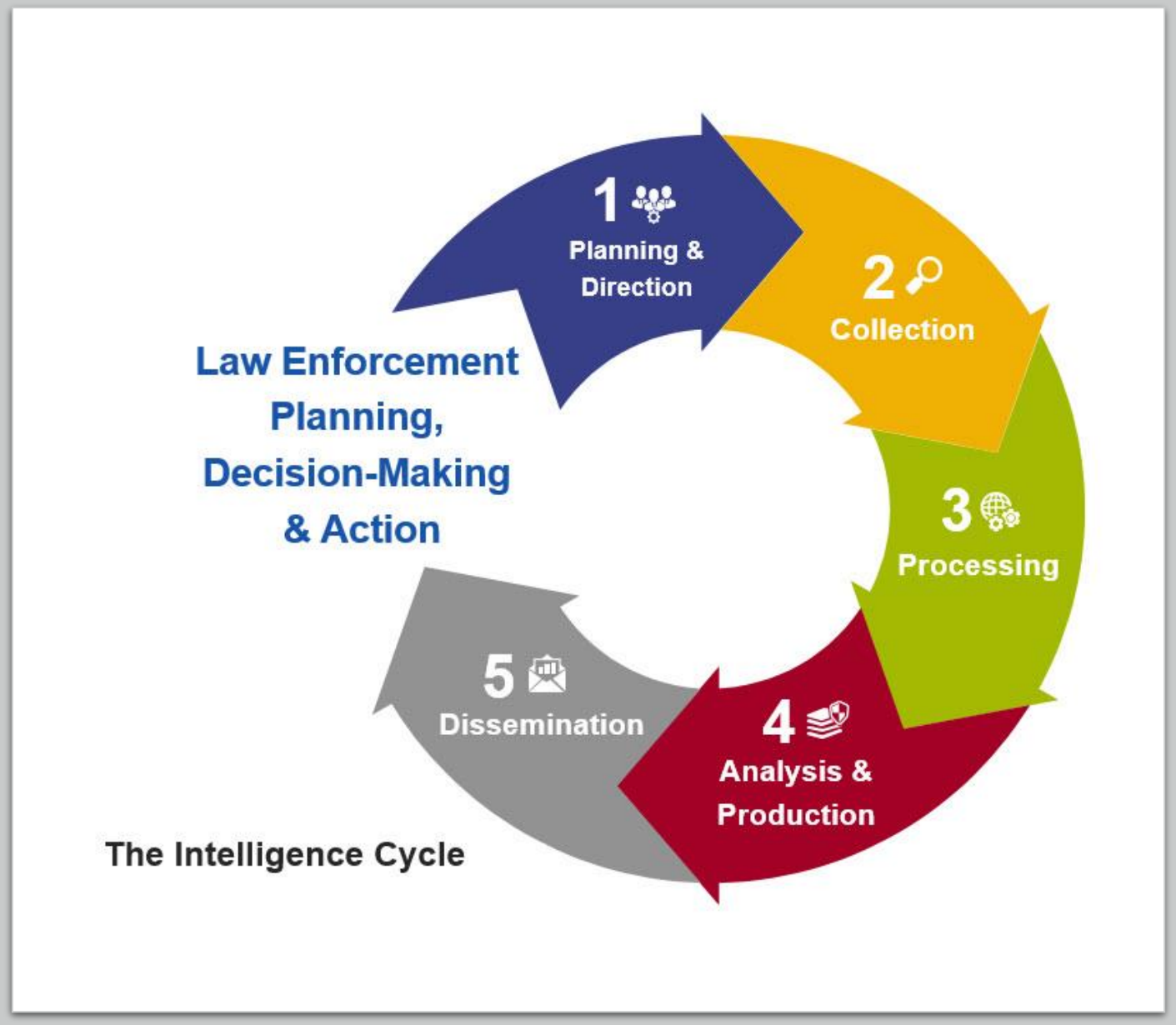
- https://github.com/lockfale/OSINT-Framework





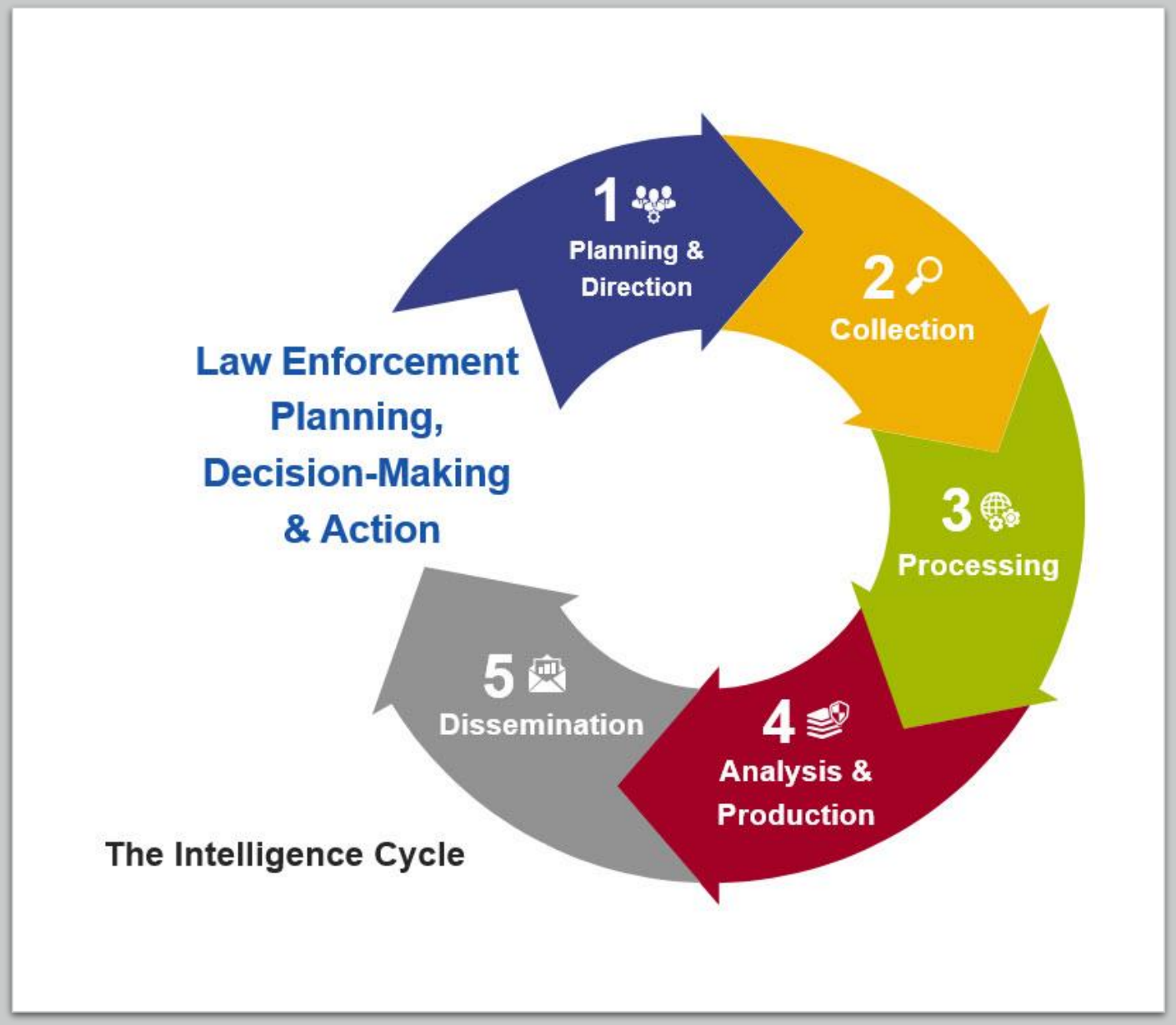
The Intelligence Concepts and Critical Thiking

The Intelligence Cycle



The Intelligence Cycle - Planning and Direction

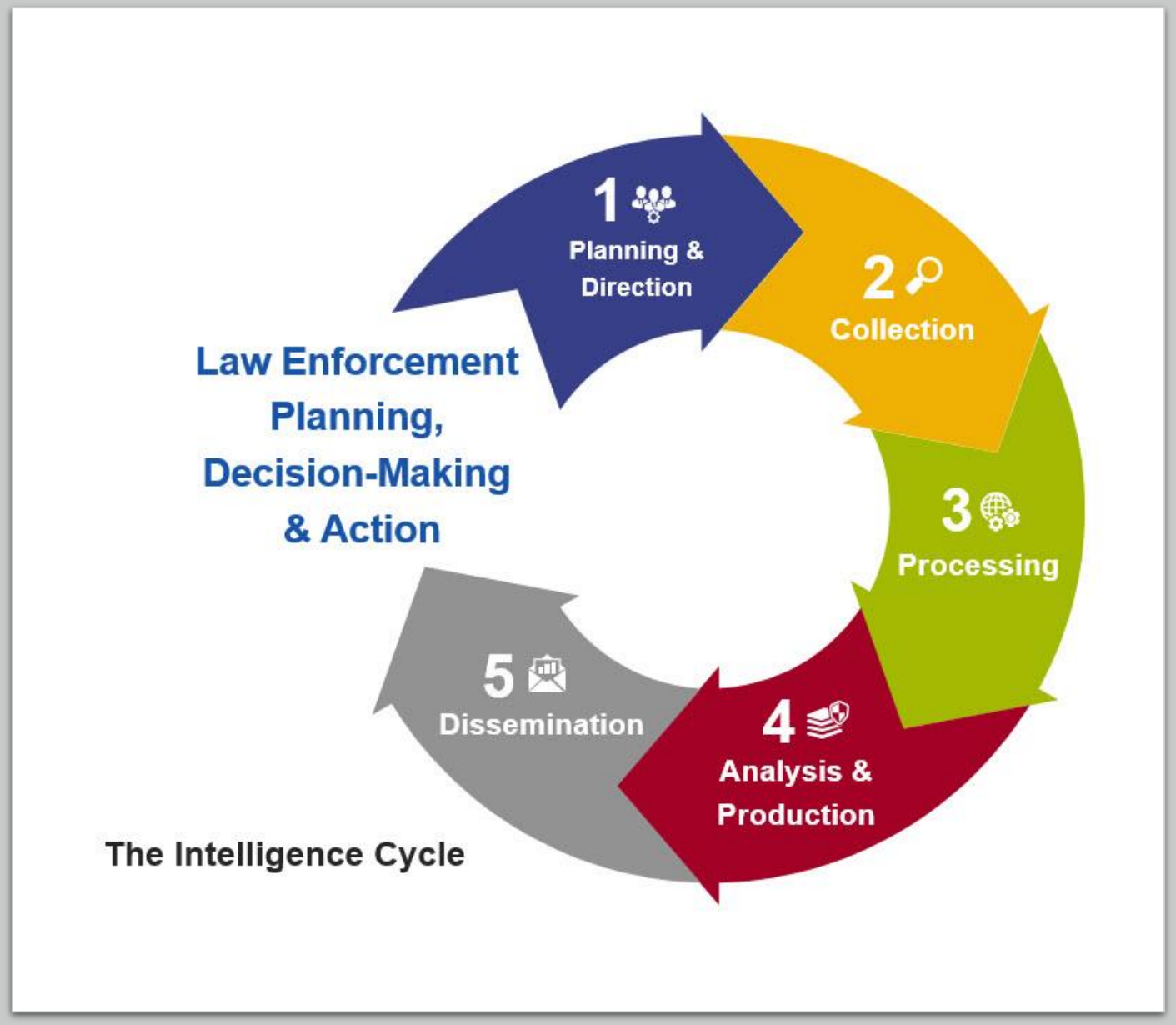
- Planning and direction involves management of the entire intelligence effort, from identifying the need for data to delivering an intelligence product to a consumer. It is both the beginning and the end of the cycle. It is the beginning because it involves formulating specific collection, processing, analysis, and dissemination requirements. It is the end because finished intelligence, which must support decision-making and action, frequently generates new information requirements.
- The intelligence process is consumer-driven. That is, the entire process depends on guidance from the consumer -- the end-user -- of the intelligence. Consumers from all levels of government -- federal, state, and local -- may initiate requests for intelligence. In addition, policymakers, executives, investigators, and patrol officers usually have different information needs. Thus, the effective planning and direction of the intelligence effort requires an understanding of the needs of a variety of consumers.



The Intelligence Cycle - Planning and Direction

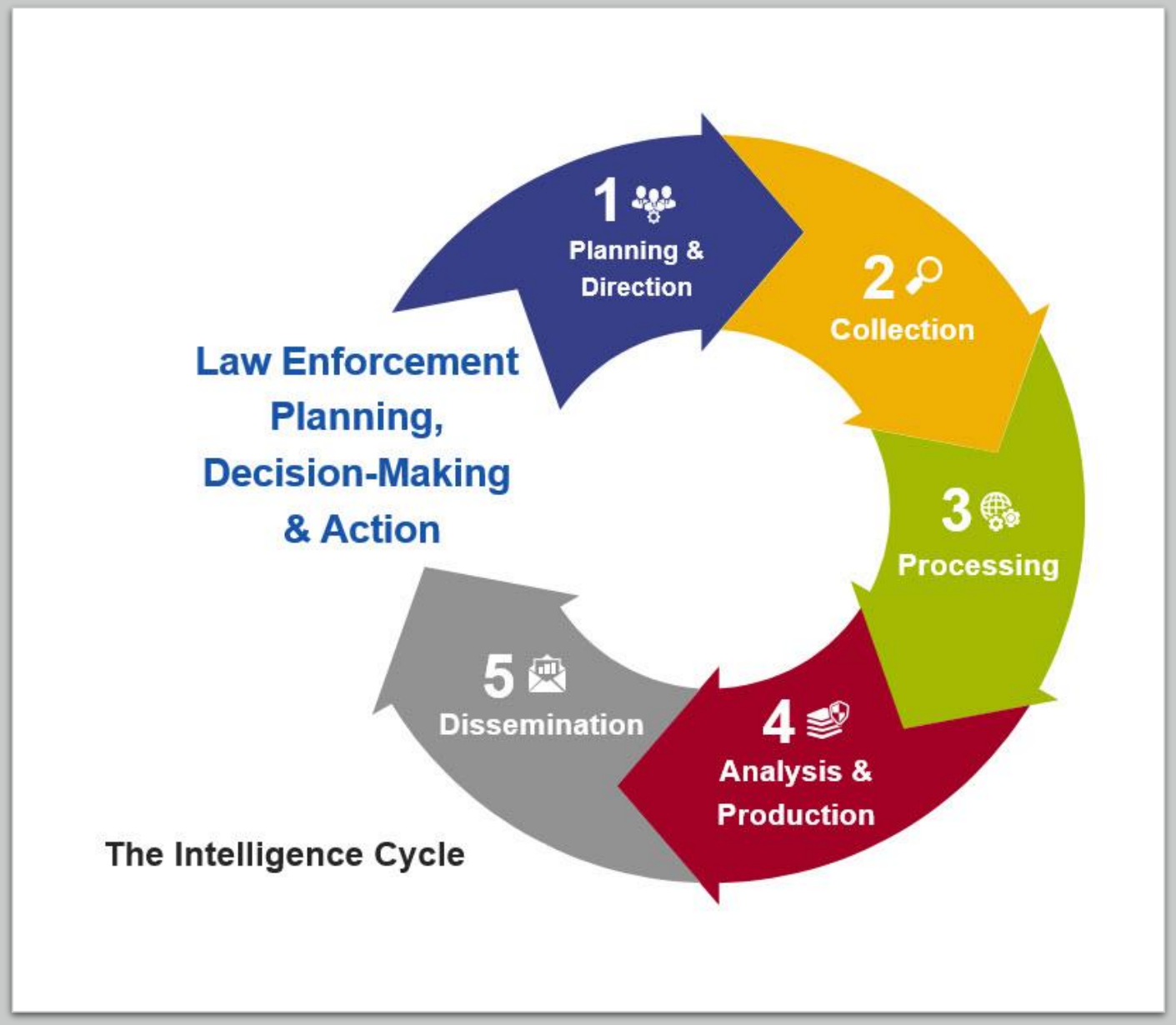
- O planejamento e a direção envolvem o gerenciamento de todo o esforço de inteligência, desde a identificação da necessidade de dados até a entrega de um produto de inteligência ao consumidor. É o início e o fim do ciclo. É o começo porque envolve a formulação de requisitos específicos de coleta, processamento, análise e disseminação. É o fim porque a inteligência acabada, que deve apoiar a tomada de decisão e a ação, frequentemente gera novos requisitos de informação.

- O processo de inteligência é orientado ao consumidor. Ou seja, todo o processo depende da orientação do consumidor – o usuário final – da inteligência. Consumidores de todos os níveis de governo - federal, estadual e local - podem iniciar solicitações de inteligência. Além disso, formuladores de políticas, executivos, investigadores e oficiais de patrulha geralmente têm necessidades de informação diferentes. Assim, o planejamento e a direção eficazes do esforço de inteligência requerem um entendimento das necessidades de uma variedade de consumidores.



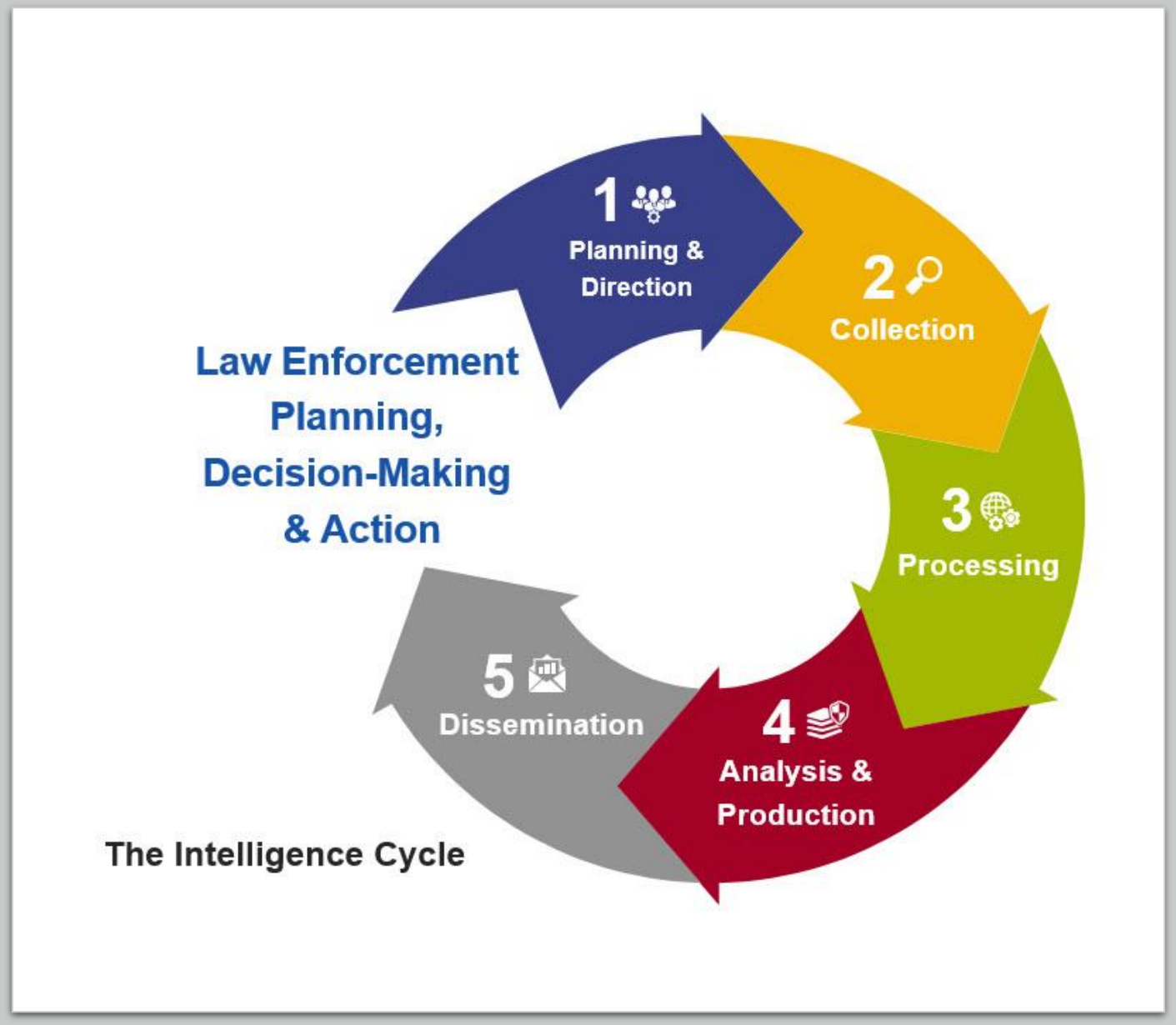
The Intelligence Cycle - Collection

- Collection is the gathering and reporting of the raw information that is needed to produce finished intelligence. To be effective, collection should be planned, focused, and directed. There are many sources of raw information, including open sources such as governmental public records, media reports, the Internet, periodicals, and books. Although often underestimated, open source collection is important to an intelligence unit's analytical capabilities. There are also confidential sources of information. Law enforcement officers collect such information from various sources, including citizens who report crime, investigations that are conducted, and speaking with persons who participate in criminal activity. To gather this information, law enforcement officers use a variety of collection methods such as interviews, undercover work, and physical or electronic surveillance.



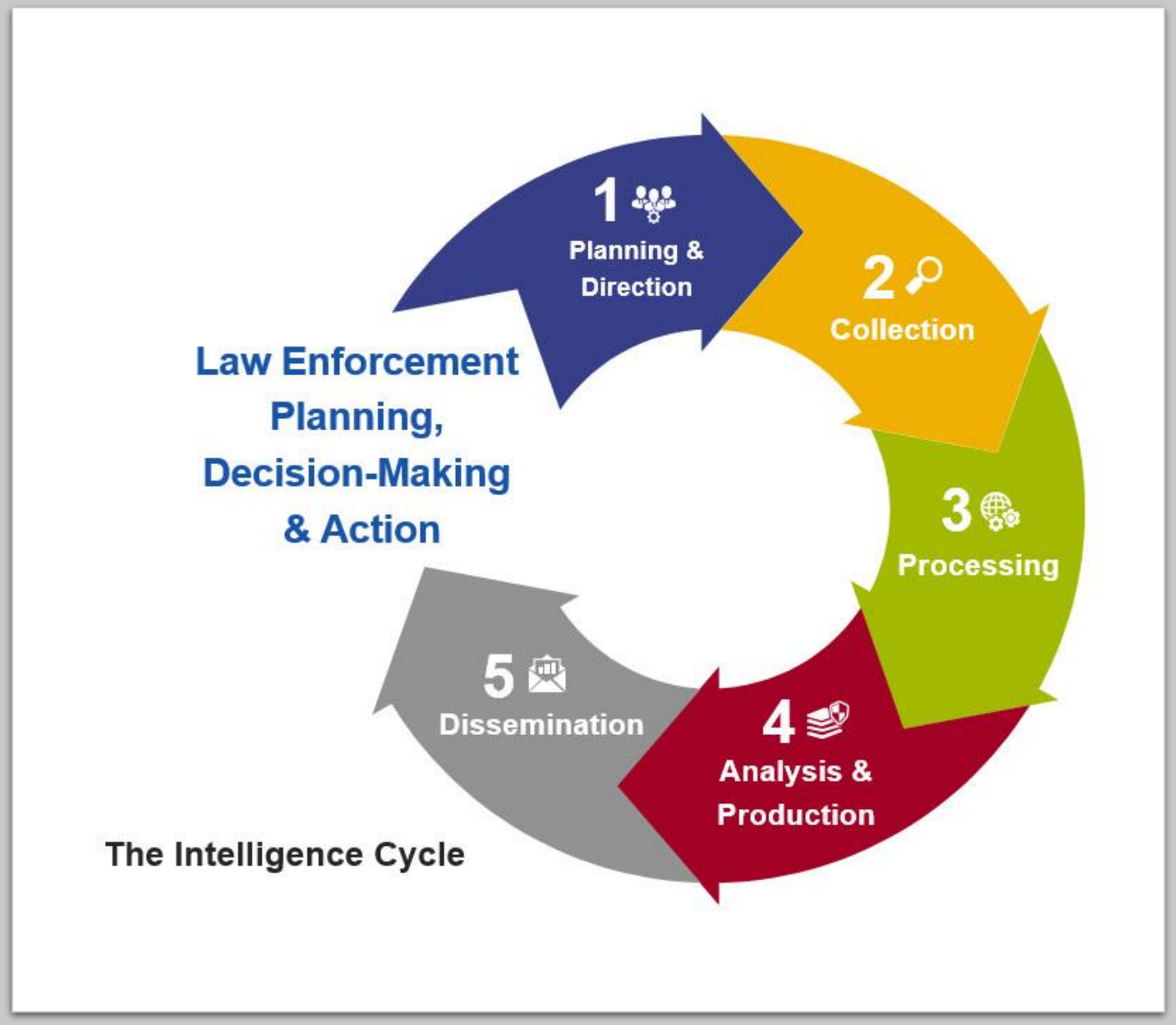
The Intelligence Cycle - Collection

- A coleta é a coleta e o relatório das informações brutas necessárias para produzir inteligência finalizada. Para ser eficaz, a coleta deve ser planejada, focada e direcionada. Existem muitas fontes de informações brutas, incluindo fontes abertas, como registros públicos governamentais, relatórios da mídia, Internet, periódicos e livros. Embora muitas vezes subestimada, a coleta de código aberto é importante para os recursos analíticos de uma unidade de inteligência. Existem também fontes de informação confidenciais. Os policiais coletam essas informações de várias fontes, incluindo cidadãos que denunciam crimes, investigações conduzidas e conversas com pessoas que participam de atividades criminosas. Para coletar essas informações, os policiais usam uma variedade de métodos de coleta, como entrevistas, trabalho disfarçado.



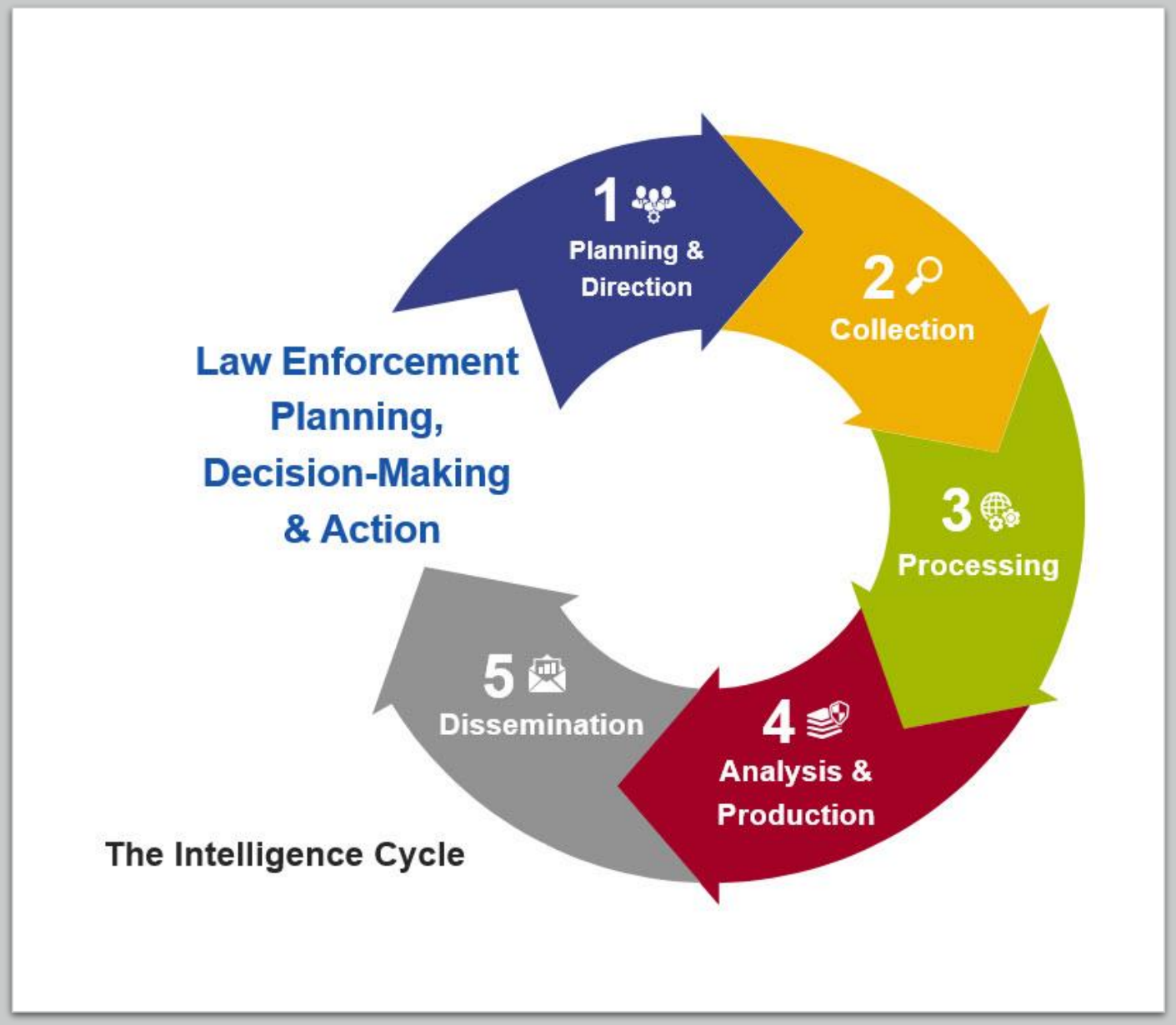
The Intelligence Cycle - Processing

- Processing and collation involves conversion of raw information into a form usable by analysts. This is accomplished through information management. Information management is the indexing, sorting, and organizing of raw data into files so that the information can be rapidly retrieved. For example, the processing step includes entry of data into a computer, reduction of data, collation of paper files, and other forms of information management. Effective processing and collation requires an understanding of the consumers' needs, the types of information that are being processed, the collection plan, and the analytic strategy.



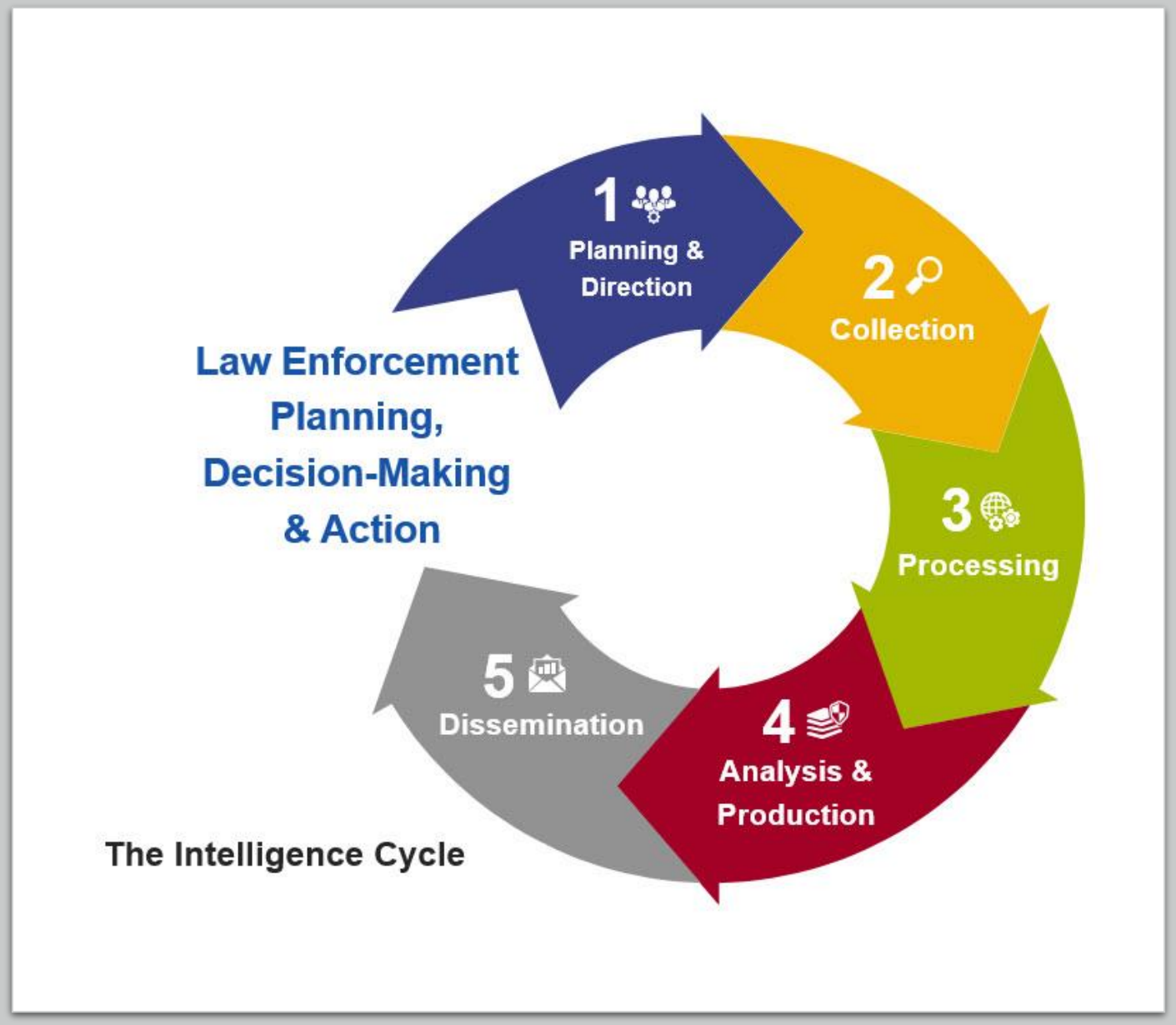
The Intelligence Cycle - Processing

- O processamento e o agrupamento envolvem a conversão de informações brutas em um formato utilizável pelos analistas. Isso é feito por meio do gerenciamento de informações. O gerenciamento de informações é a indexação, classificação e organização de dados brutos em arquivos para que as informações possam ser recuperadas rapidamente. Por exemplo, a etapa de processamento inclui entrada de dados em um computador, redução de dados, agrupamento de arquivos em papel e outras formas de gerenciamento de informações. O processamento e o agrupamento eficazes requerem uma compreensão das necessidades dos consumidores, os tipos de informações que estão sendo processadas, o plano de coleta e a estratégia analítica.



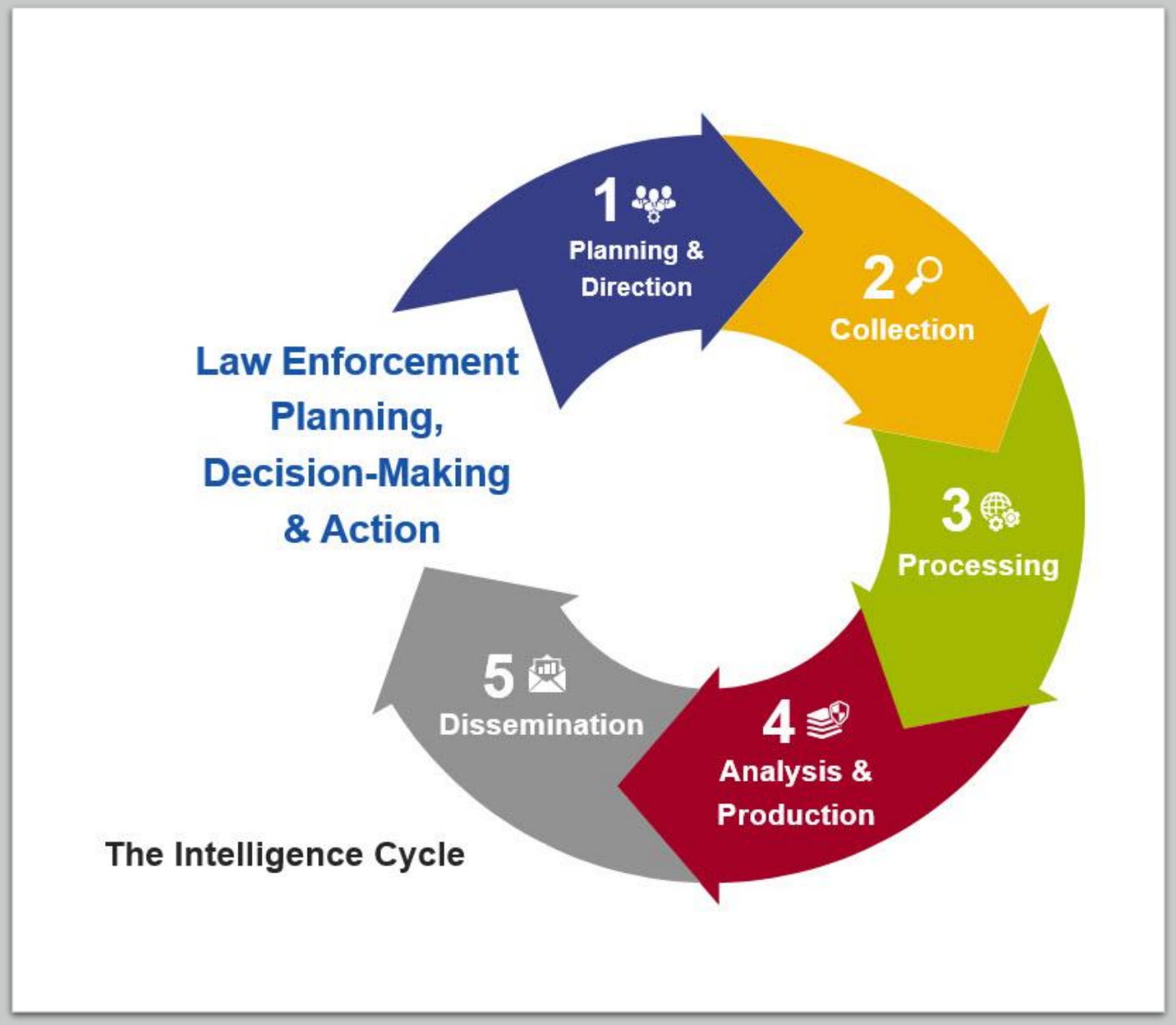
The Intelligence Cycle – Analysis and Production

- Analysis and production is the conversion of basic information from all sources into finished intelligence. It includes integrating, evaluating, and analyzing all available data--which is often fragmentary and even contradictory - and preparing intelligence products. In short, analysis gives additional meaning to the raw information. Analysts, who are subject-matter-specialists, consider the information's reliability, validity, timeliness, and relevance. They integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications of the information for consumers. Intelligence and analysis units may devote their resources to producing strategic intelligence for policymakers and executives, providing operational intelligence to continuing investigations, or making available tactical intelligence for an immediate law enforcement need. These important functions are performed by monitoring current crime and non-crime events, warning decision makers about actual and potential threats to public safety and order, and forecasting developments in the area of criminal activity. Intelligence and analysis units may produce numerous written reports, which may be brief - one page or less--or lengthy studies. They may involve current intelligence, which is of immediate importance, or long-range assessments.



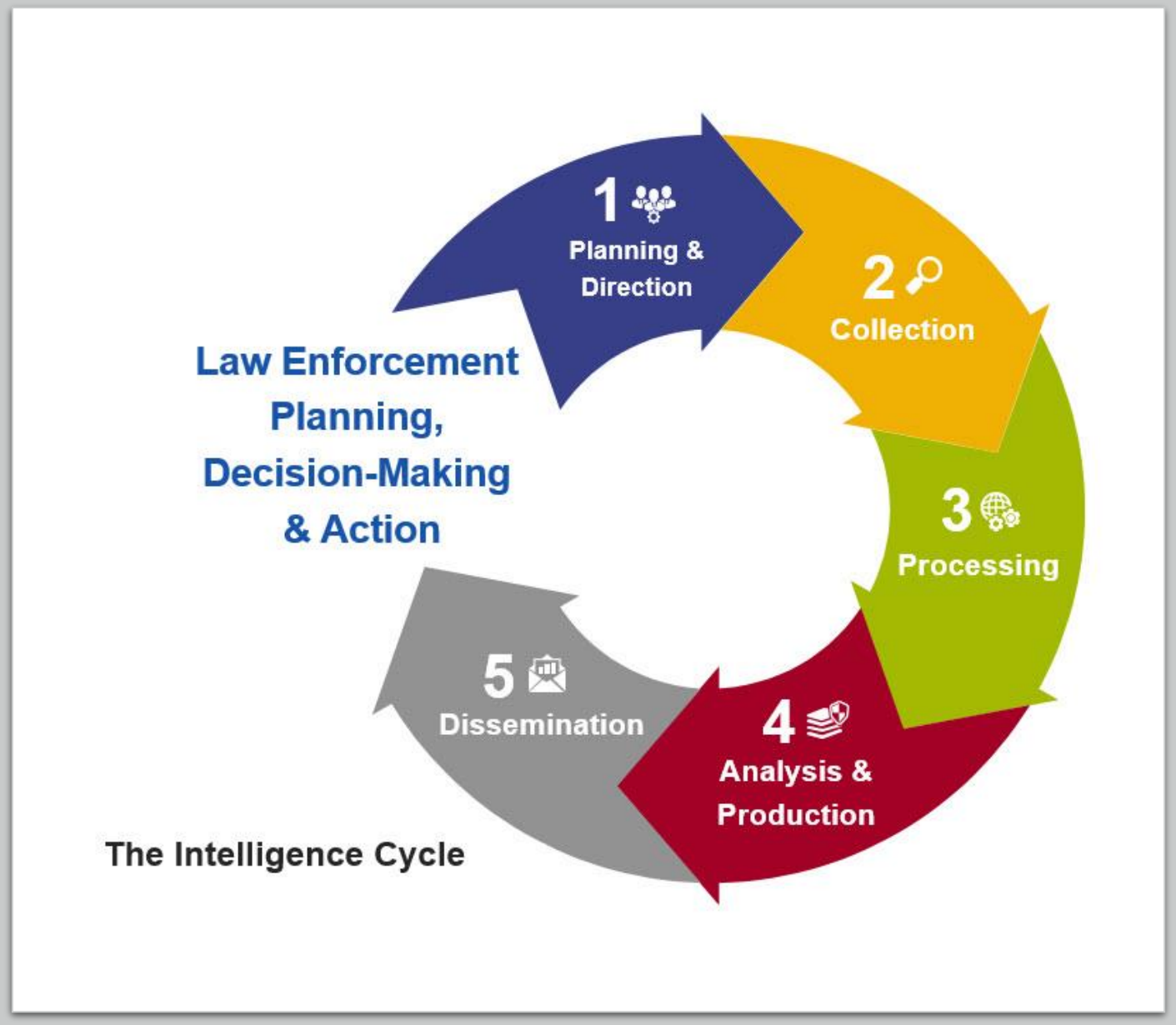
The Intelligence Cycle - Processing

- Análise e produção é a conversão de informações básicas de todas as fontes em inteligência acabada. Inclui integrar, avaliar e analisar todos os dados disponíveis – muitas vezes fragmentados e até contraditórios – e preparar produtos de inteligência. Em suma, a análise dá significado adicional à informação bruta. Os analistas, que são especialistas no assunto, consideram a confiabilidade, validade, oportunidade e relevância das informações. Eles integram dados em um todo coerente, colocam as informações avaliadas em contexto e produzem inteligência final que inclui avaliações de eventos e julgamentos sobre as implicações das informações para os consumidores. As unidades de inteligência e análise podem dedicar seus recursos à produção de inteligência estratégica para formuladores de políticas e executivos, fornecer inteligência operacional para investigações contínuas ou disponibilizar inteligência tática para uma necessidade imediata de aplicação da lei. Essas importantes funções são desempenhadas monitorando eventos criminais e não criminais atuais, alertando os tomadores de decisão sobre ameaças reais e potenciais à segurança e ordem públicas e prevendo desenvolvimentos na área de atividade criminosa. As unidades de inteligência e análise podem produzir numerosos relatórios escritos, que podem ser breves - uma página ou menos - ou estudos longos. Eles podem envolver inteligência atual, que é de importância imediata, ou avaliações de longo alcance. alertando os tomadores de decisão sobre ameaças reais e potenciais à segurança e ordem públicas e prevendo desenvolvimentos na área de atividade criminosa. As unidades de inteligência e análise podem produzir numerosos relatórios escritos, que podem ser breves - uma página ou menos - ou estudos longos. Eles podem envolver inteligência atual, que é de importância imediata, ou avaliações de longo alcance. alertando os tomadores de decisão sobre ameaças reais e potenciais à segurança e ordem públicas e prevendo desenvolvimentos na área de atividade criminosa. As unidades de inteligência e análise podem produzir numerosos relatórios escritos, que podem ser breves - uma página ou menos - ou estudos longos. Eles podem envolver inteligência atual, que é de importância imediata, ou avaliações de longo alcance.



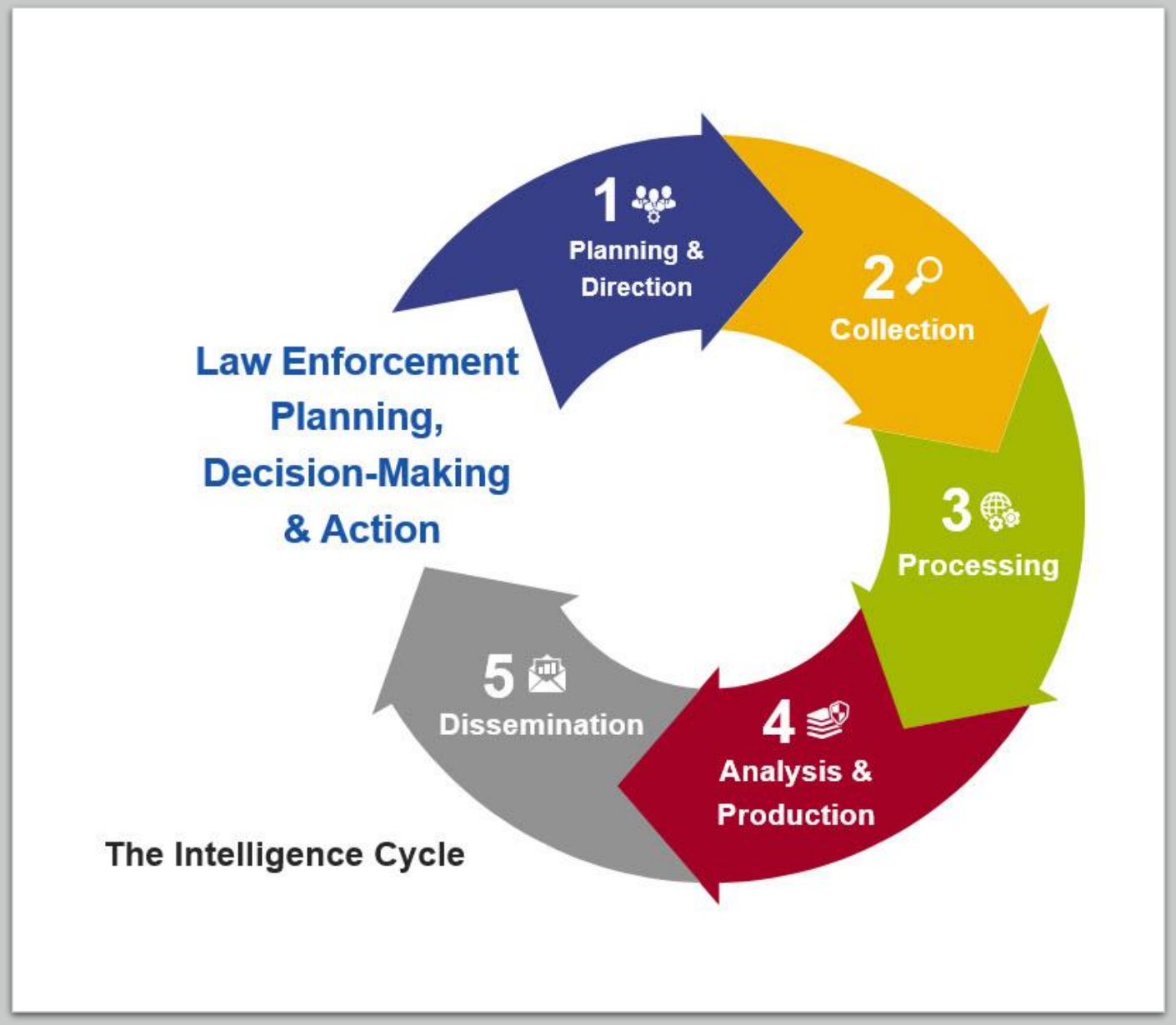
The Intelligence Cycle - Dissemination

- The last step, which logically feeds into the first, is the distribution of the finished intelligence to the consumers -- the same consumers whose needs initiated the intelligence requirements. These recipients of finished intelligence then make decisions or take action based on the intelligence that has been provided. This step should also include an opportunity for feedback, to assess the value of the intelligence that has been provided. The decisions, actions, and feedback may lead to the levying of more information requirements, thus triggering the intelligence cycle once again.



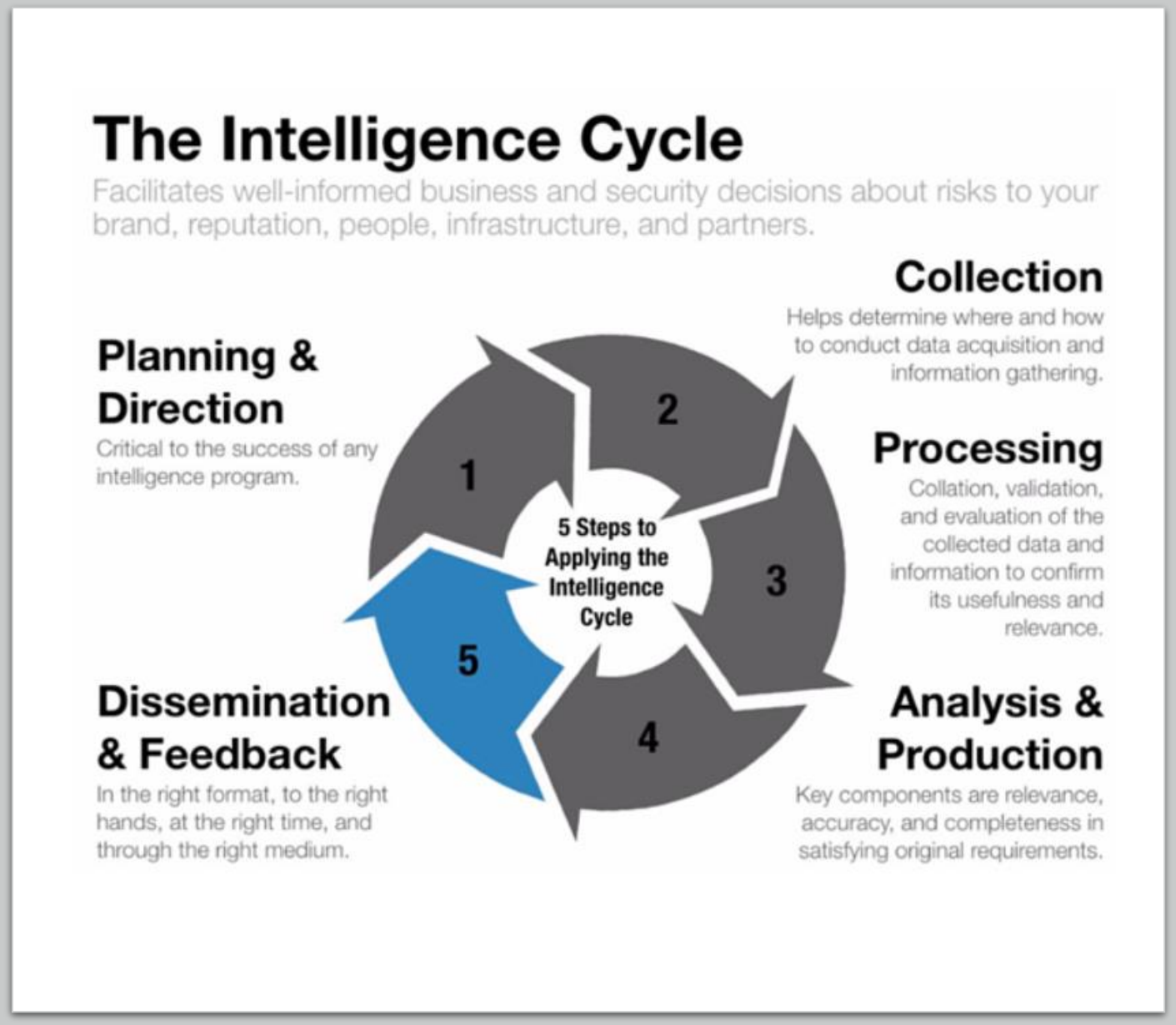
The Intelligence Cycle - Dissemination

- A última etapa, que logicamente alimenta a primeira, é a distribuição da inteligência final para os consumidores – os mesmos consumidores cujas necessidades iniciaram os requisitos de inteligência. Esses destinatários da inteligência finalizada então tomam decisões ou agem com base na inteligência que foi fornecida. Esta etapa também deve incluir uma oportunidade de feedback, para avaliar o valor da inteligência que foi fornecida. As decisões, ações e feedback podem levar à cobrança de mais requisitos de informação, acionando novamente o ciclo de inteligência.



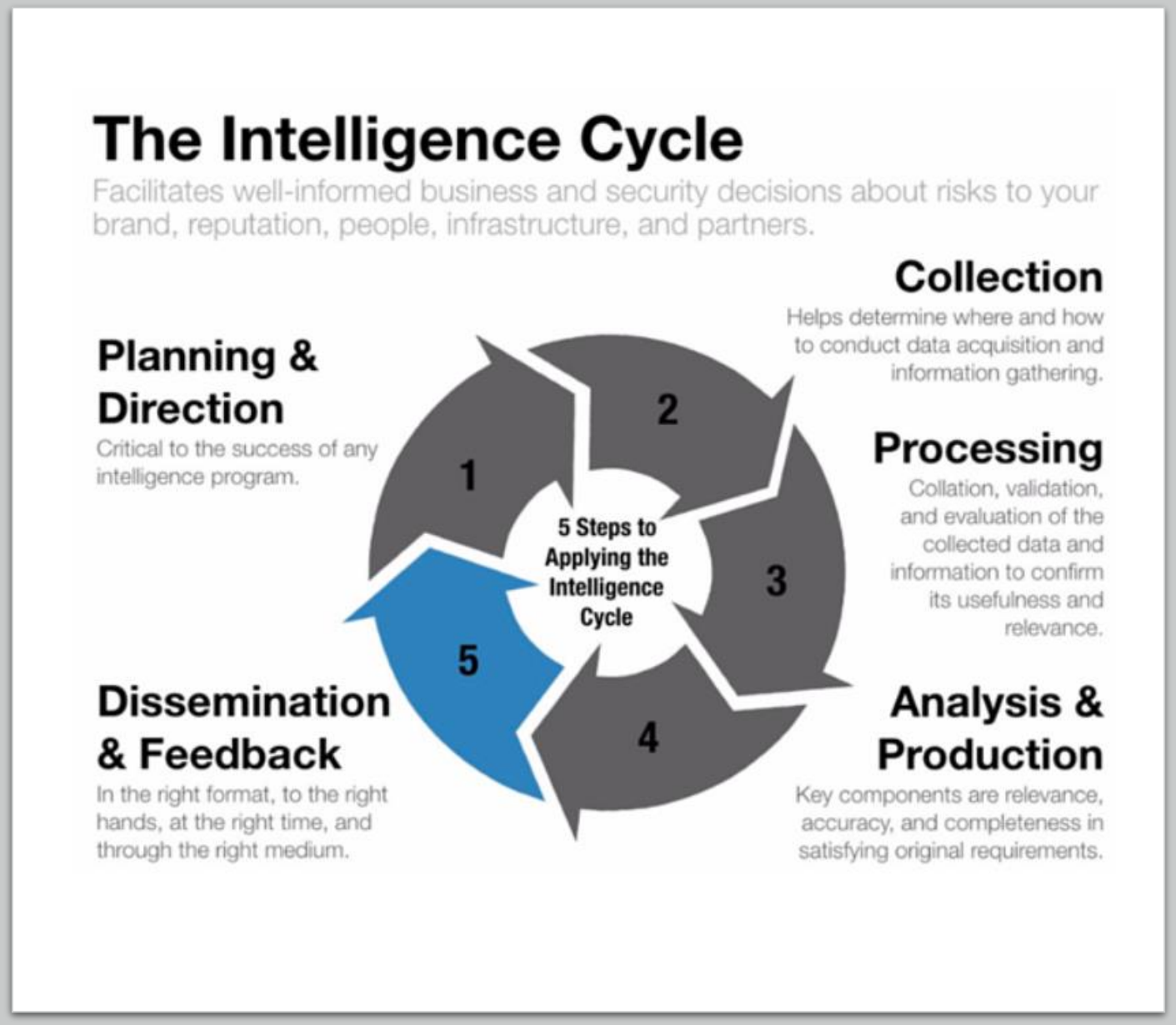
The Intelligence Cycle

- The Intelligence Cycle is the process of developing raw information into finished intelligence for policymakers or business leaders to use in decision making and policy action. The Intelligence Cycle is cyclical in nature, with previous findings influencing subsequent avenues of investigation, the goal is not only to determine what one wants to know and learning it, but to remain ever receptive to new information and how it may impact the status quo.

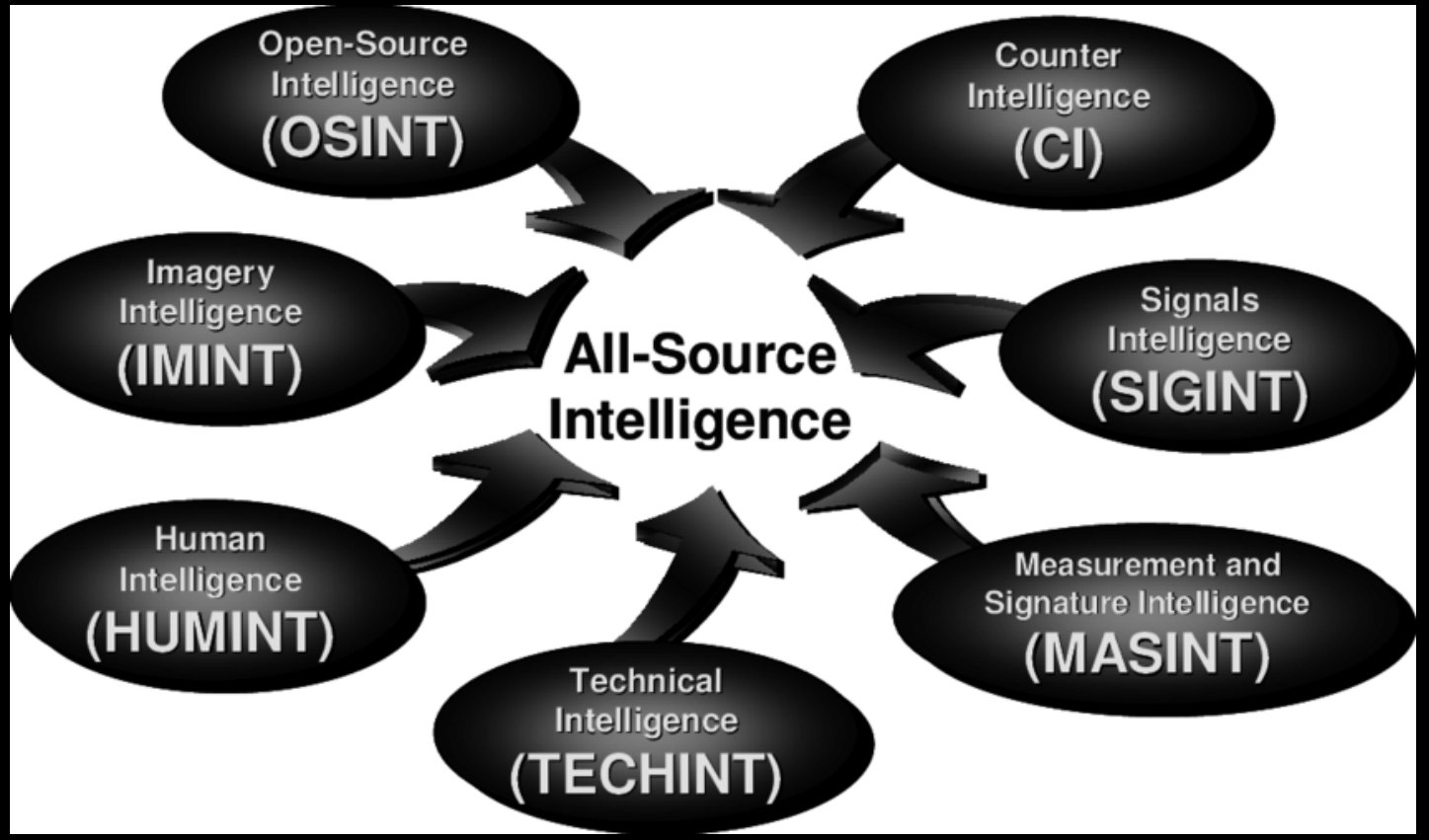


The Intelligence Cycle

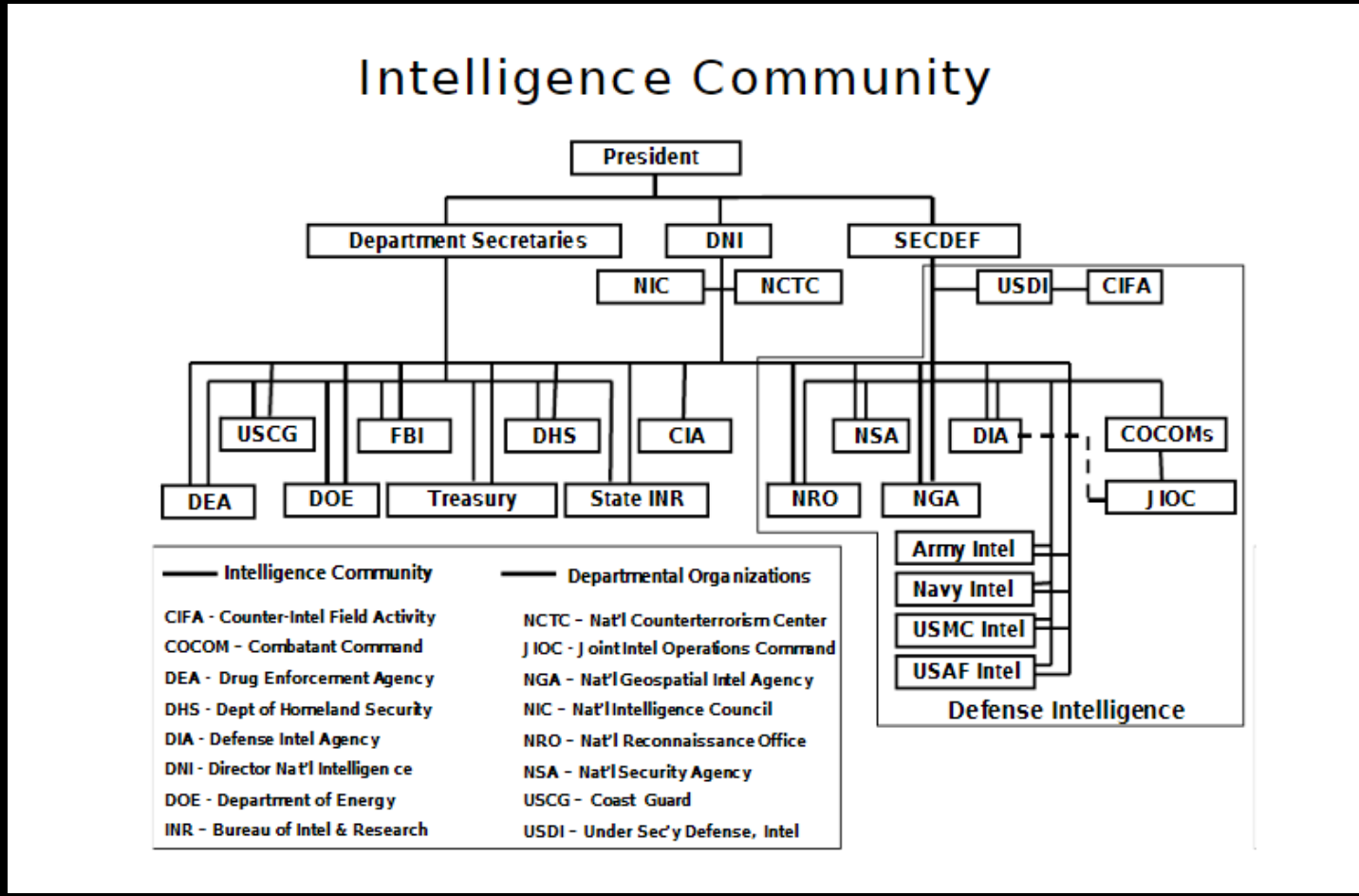
- O Ciclo de Inteligência é o processo de desenvolvimento de informações brutas em inteligência acabada para os formuladores de políticas ou líderes empresariais usarem na tomada de decisões e na ação política. O Ciclo de Inteligência é de natureza cíclica, com descobertas anteriores influenciando avenidas subsequentes de investigação, o objetivo não é apenas determinar o que se quer saber e aprender, mas permanecer sempre receptivo a novas informações e como isso pode afetar o status quo.



Intelligence Disciplines



Intelligence Community



Critical Thinking

- *Critical thinking is the ability to think in an organized and rational manner in order to understand connections between ideas and/or facts. It helps you decide what to believe in. In other words, it's "thinking about thinking"—identifying, analyzing, and then fixing flaws in the way we think.*
- *O pensamento crítico* é a capacidade de pensar de forma organizada e racional para compreender as conexões entre ideias e/ou fatos. Isso ajuda você a decidir em que acreditar. Em outras palavras, é "pensar sobre pensar" – identificar, analisar e corrigir falhas na maneira como pensamos.

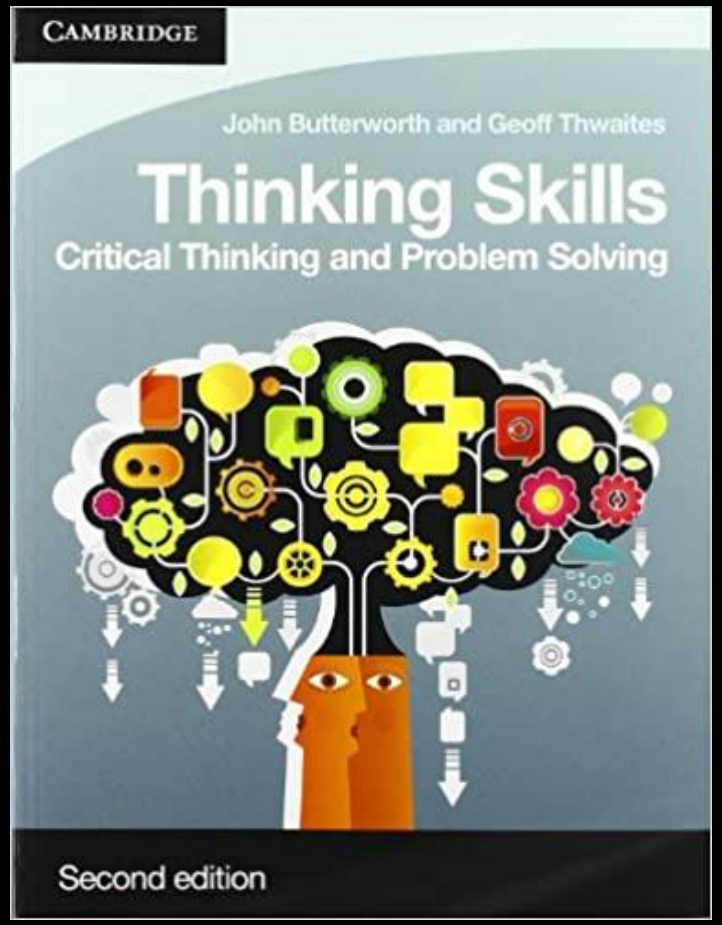
Critical Thinking - Steps

- **1. Identify the problem or question.**
- Be as precise as possible: the narrower the issue, the easier it is to find solutions or answers.
- **2. Gather data, opinions, and arguments.**
- Try to find several sources that present different ideas and points of view.
- **3. Analyze and evaluate the data.**
- Are the sources reliable? Are their conclusions data-backed or just argumentative? Is there enough information or data to support given hypotheses?
- **4. Identify assumptions.**
- Are you sure the sources you found are unbiased? Are you sure you weren't biased in your search for answers?
- **5. Establish significance.**
- What piece of information is most important? Is the sample size sufficient? Are all opinions and arguments even relevant to the problem you're trying to solve?
- **6. Make a decision/reach a conclusion.**
- Identify various conclusions that are possible and decide which (if any) of them are sufficiently supported. Weigh strengths and limitations of all possible options.
- **7. Present or communicate.**
- Once you've reached a conclusion, present it to all stakeholders.

Critical Thinking - Steps

- **1. Identifique o problema ou a pergunta.**
- Seja o mais preciso possível: quanto mais restrita a questão, mais fácil será encontrar soluções ou respostas.
- **2. Reúna dados, opiniões e argumentos.**
- Tente encontrar várias fontes que apresentem ideias e pontos de vista diferentes.
- **3. Analise e avalie os dados.**
- As fontes são confiáveis? Suas conclusões são baseadas em dados ou apenas argumentativas? Existem informações ou dados suficientes para apoiar determinadas hipóteses?
- **4. Identifique suposições.**
- Tem certeza de que as fontes que você encontrou são imparciais? Tem certeza de que não foi tendencioso em sua busca por respostas?
- **5. Estabeleça significado.**
- Que informação é mais importante? O tamanho da amostra é suficiente? Todas as opiniões e argumentos são relevantes para o problema que você está tentando resolver?
- **6. Tome uma decisão/chegue a uma conclusão.**
- Identifique várias conclusões possíveis e decida quais delas (se houver) são suficientemente apoiadas. Pesar pontos fortes e limitações de todas as opções possíveis.
- **7. Apresentar ou comunicar.**
- Depois de chegar a uma conclusão, apresente-a a todas as partes interessadas.

Critical Thinking - Book



OSINT CONFIGURATIONS

Password Management

- A password manager is a program that is used for a large number of password names. The database where this information is unique cryptographic access key using a password that the user just memorizes has access to all others
- Um gerenciador de senha é um programa que é usado para armazenar uma grande quantidade de nomes/senhas. O banco de dados onde esta informação é armazenada é criptografado usando uma única chave, para que o usuário apenas tenha de memorizar uma senha para acesso a todos as outras

Virtual Private Network

- VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.
- VPN significa "Rede Privada Virtual" e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas. As VPNs criptografam seu tráfego de internet e disfarçam sua identidade online. Isso torna mais difícil para terceiros rastrear suas atividades online e roubar dados. A criptografia ocorre em tempo real .

Virtual Private Network - Benefits

- A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.
- Secure encryption: To read the data, you need an encryption key . Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack . With the help of a VPN, your online activities are hidden even on public networks.
- Disguising your whereabouts : VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities. Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.
- Access to regional content: Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home. With VPN location spoofing , you can switch to a server to another country and effectively “change” your location.
- Secure data transfer: If you work remotely, you may need to access important files on your company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Virtual Private Network - Benefits

- Uma conexão VPN disfarça seu tráfego de dados online e o protege de acesso externo. Os dados não criptografados podem ser visualizados por qualquer pessoa que tenha acesso à rede e queira vê-los. Com uma VPN, hackers e criminosos cibernéticos não conseguem decifrar esses dados.
- Criptografia segura: para ler os dados, você precisa de uma chave de criptografia . Sem um, levaria milhões de anos para um computador decifrar o código no caso de um ataque de força bruta. Com a ajuda de uma VPN, suas atividades online ficam ocultas mesmo em redes públicas.
- Disfarçar seu paradeiro: os servidores VPN atuam essencialmente como seus proxies na internet. Como os dados de localização demográfica vêm de um servidor em outro país, sua localização real não pode ser determinada. Além disso, a maioria dos serviços VPN não armazena registros de suas atividades. Alguns provedores, por outro lado, registram seu comportamento, mas não repassam essas informações a terceiros. Isso significa que qualquer registro potencial do seu comportamento de usuário permanece permanentemente oculto.
- Acesso ao conteúdo regional: o conteúdo regional da web nem sempre é acessível de todos os lugares. Os serviços e sites geralmente contêm conteúdo que só pode ser acessado em determinadas partes do mundo. As conexões padrão usam servidores locais no país para determinar sua localização. Isso significa que você não pode acessar conteúdo em casa enquanto viaja e não pode acessar conteúdo internacional em casa. Com a falsificação de localização VPN, você pode alternar para um servidor para outro país e efetivamente “alterar” sua localização.
- Transferência segura de dados: Se você trabalha remotamente, pode precisar acessar arquivos importantes na rede da sua empresa. Por motivos de segurança, esse tipo de informação requer uma conexão segura. Para obter acesso à rede, geralmente é necessária uma conexão VPN. Os serviços VPN se conectam a servidores privados e usam métodos de criptografia para reduzir o risco de vazamento de dados.

TRACELABS OSINT VM

Download:

- https://www.tracelabs.org/initiatives/osint-vm

Configuration

- https://www.youtube.com/watch?v=jjK0nvmOeUA

FIREFOX ADDON

- **Firefox Addon: Firefox Containers**
- **Firefox Addon: UBlock Origin**
- **Firefox Addon: Downloadthemall**
- **Firefox Addon: VideoDownloadHelper**
- **Firefox Addon: Full Web Page Screenshots**
- **Firefox Addon: Nimbus**
- **Firefox Addon: HTTPS Everywhere & Smart HTTPS**
- **Firefox Addon: User-Agent**
- **Firefox Addon: Exif Viewer**
- **Firefox Addon: Copy Selected Links**
- **Firefox Addon: Link Gopher**
- **Firefox Addon: Right Click Copy**
- **Firefox Addon: Perceptual Image Analysis**
- **Firefox Addon: Singe File**
- **Firefox Addon: Privacy Badger**
- **Firefox Addon: Search by Image**

TOR BROWSER

What is TOR

Tor—short for "The Onion Routing" project—is an open source privacy network that enables anonymous web browsing. The network of computers worldwide in the Tor network uses secure, encrypted protocols to ensure that users' online privacy is protected. Tor users' digital data and communications are shielded using a layered approach that resembles the nested layers of an onion.

The Tor technology was initially developed and solely used by the U.S. Navy, to protect sensitive government communications. The network was later made available to the public as an open-source platform, meaning that Tor's source code is accessible to everyone. Tor is upgraded and enhanced by volunteer developers in the Tor network.

What is TOR

Tor - abreviação de projeto "The Onion Routing" - é uma rede de privacidade de código aberto que permite navegação anônima na web. A rede de computadores em todo o mundo na rede Tor usa protocolos seguros e criptografados para garantir que a privacidade online dos usuários seja protegida. Os dados e comunicações digitais dos usuários do Tor são protegidos usando uma abordagem em camadas que se assemelha às camadas aninhadas de uma cebola.

A tecnologia Tor foi inicialmente desenvolvida e usada exclusivamente pela Marinha dos EUA para proteger comunicações confidenciais do governo. A rede foi posteriormente disponibilizada ao público como uma plataforma de código aberto, o que significa que o código-fonte do Tor é acessível a todos. O Tor é atualizado e aprimorado por desenvolvedores voluntários na rede Tor.

More Details about TOR

https://www.investopedia.com/terms/t/tor.asp

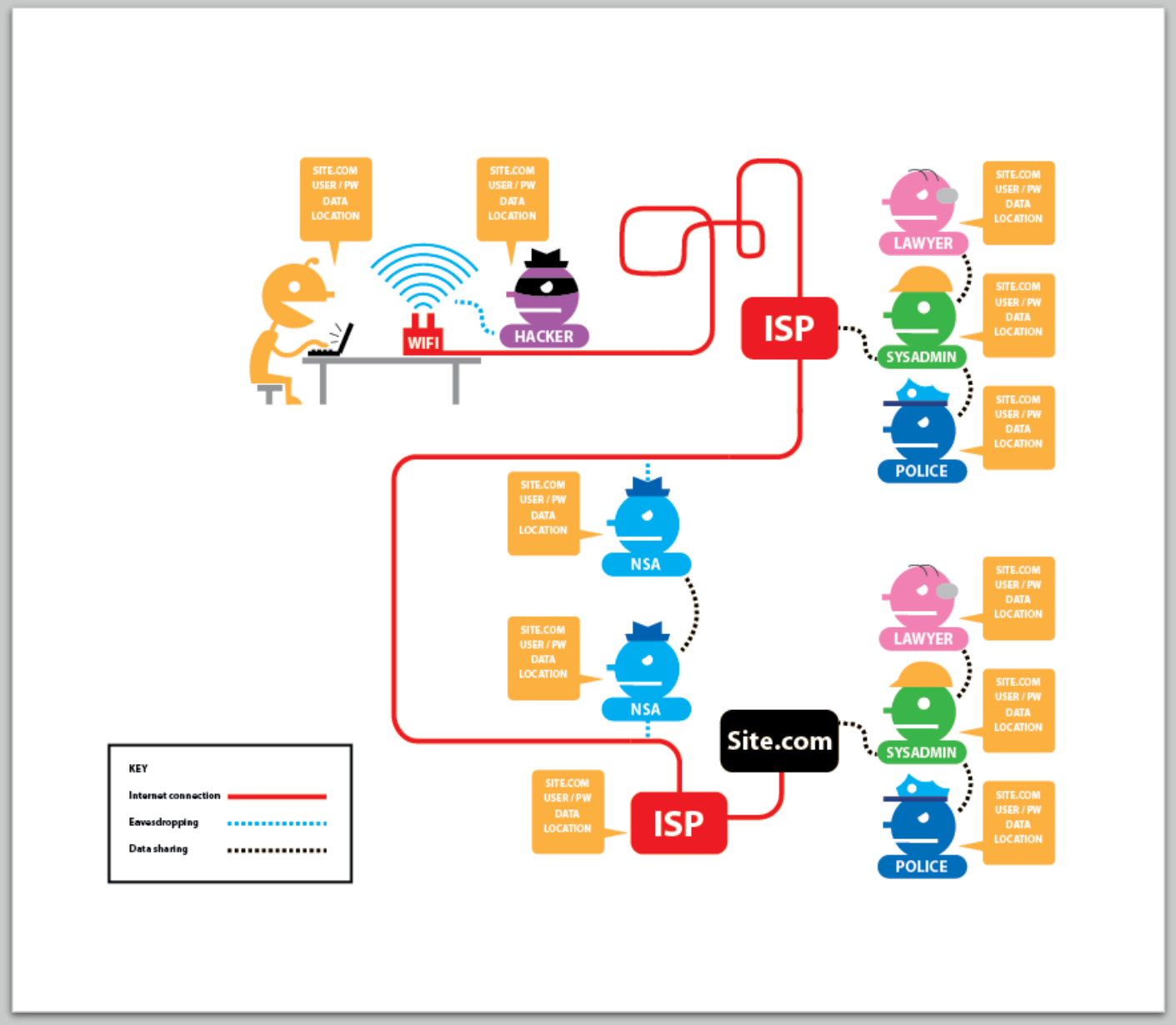
https://www.torproject.org/

https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

Configuration Tor Browser

https://thesafety.us/tor-browser-setup

https://tb-manual.torproject.org/running-tor-browser/



TOR Browser Vulnerabilities

https://www.cvedetails.com/product/50922/Torproject-Tor-Browser.html?vendor_id=12287

https://www.privacyaffairs.com/cve-2021-39246-tor-vulnerability

https://www.bleepingcomputer.com/news/security/tor-browser-fixes-vulnerability-that-tracks-you-using-installed-apps/

https://www.pcmag.com/news/tor-browser-has-a-flaw-that-governments-may-have-exploited

https://www.techradar.com/news/tor-browser-is-wrestling-with-a-major-security-problem

https://medium.com/codex/protecting-tor-on-linux-from-malicious-exit-relays-1f28635ba2c9

Other Privacy Networks

What is Freenet

- Freenet is free software which lets you anonymously share files, browse and publish "freesites" (web sites accessible only through Freenet) and chat on forums, without fear of censorship. Freenet is decentralised to make it less vulnerable to attack, and if used in "darknet" mode, where users only connect to their friends, is very difficult to detect.
- Communications by Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is.
- Users contribute to the network by giving bandwidth and a portion of their hard drive (called the "data store") for storing files. Files are automatically kept or deleted depending on how popular they are, with the least popular being discarded to make way for newer or more popular content. Files are encrypted, so generally the user cannot easily discover what is in his datastore, and hopefully can't be held accountable for it. Chat forums, websites, and search functionality, are all built on top of this distributed data store.
- Freenet has been downloaded over 2 million times since the project started, and used for the distribution of censored information all over the world including countries such as China and in the Middle East. Ideas and concepts pioneered in Freenet have had a significant impact in the academic world. Our 2000 paper "Freenet: A Distributed Anonymous Information Storage and Retrieval System" was the most cited computer science paper of 2000 according to Citeseer, and Freenet has also inspired papers in the worlds of law and philosophy. Ian Clarke, Freenet's creator and project coordinator, was selected as one of the top 100 innovators of 2003 by MIT's Technology Review magazine.

What is Freenet

- Freenet é um software gratuito que permite compartilhar arquivos anonimamente, navegar e publicar "freesites" (sites acessíveis apenas através do Freenet) e conversar em fóruns, sem medo de censura. O Freenet é descentralizado para torná-lo menos vulnerável a ataques e, se usado no modo "darknet", onde os usuários se conectam apenas a seus amigos, é muito difícil de detectar.
- As comunicações dos nós da Freenet são criptografadas e roteadas através de outros nós para tornar extremamente difícil determinar quem está solicitando as informações e qual é o seu conteúdo.
- Os usuários contribuem para a rede fornecendo largura de banda e uma parte de seu disco rígido (chamado de "armazenamento de dados") para armazenar arquivos. Os arquivos são mantidos ou excluídos automaticamente dependendo de quão populares eles são, com os menos populares sendo descartados para dar lugar a conteúdos mais novos ou mais populares. Os arquivos são criptografados, portanto, geralmente o usuário não pode descobrir facilmente o que está em seu armazenamento de dados e, esperançosamente, não pode ser responsabilizado por isso. Fóruns de bate-papo, sites e funcionalidade de pesquisa são todos construídos sobre esse armazenamento de dados distribuído.
- Freenet foi baixado mais de 2 milhões de vezes desde o início do projeto e usado para a distribuição de informações censuradas em todo o mundo, incluindo países como China e Oriente Médio. Ideias e conceitos pioneiros na Freenet tiveram um impacto significativo no mundo acadêmico. Nosso artigo de 2000 "Freenet: A Distributed Anonymous Information Storage and Retrieval System" foi o artigo de ciência da computação mais citado de 2000, de acordo com o Citeseer, e o Freenet também inspirou artigos nos mundos do direito e da filosofia. Ian Clarke, criador e coordenador do projeto Freenet, foi selecionado como um dos 100 maiores inovadores de 2003 pela revista Technology Review do MIT.

What is i2P

- The Invisible Internet Project (I2P) is a fully encrypted private network layer that has been developed with privacy and security by design in order to provide protection for your activity, location and your identity. The software ships with a router that connects you to the network and applications for sharing, communicating and building.
- I2P hides the server from the user and the user from the server. All I2P traffic is internal to the I2P network. Traffic within I2P does not interact directly with the Internet. It's a layer on top of the Internet. It uses encrypted one-way tunnels between you and your peers. No one can see where the traffic comes from, where it goes, or what the content is. In addition, I2P offers resistance to pattern recognition and blocking by censors. As the network depends on the peers, the location blocking is also reduced.

What is i2P

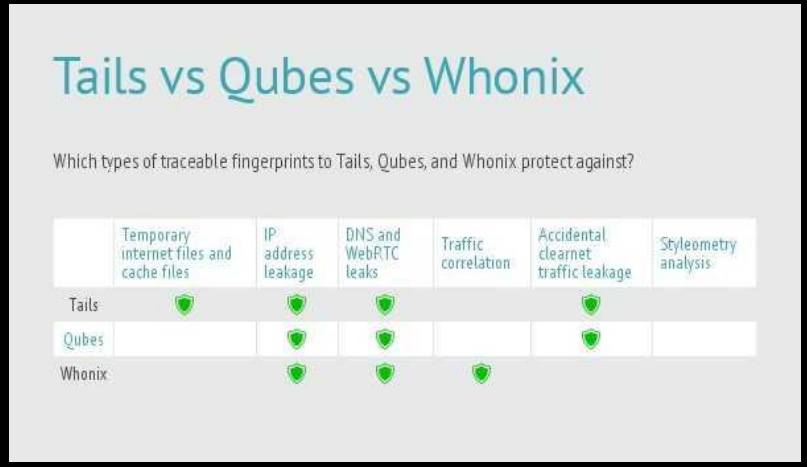
- O Invisible Internet Project (I2P) é uma camada de rede privada totalmente criptografada que foi desenvolvida com privacidade e segurança por design para fornecer proteção para sua atividade, localização e identidade. O software é fornecido com um roteador que conecta você à rede e aplicativos para compartilhamento, comunicação e construção.
- I2P esconde o servidor do usuário e o usuário do servidor. Todo o tráfego I2P é interno à rede I2P. O tráfego dentro do I2P não interage diretamente com a Internet. É uma camada no topo da Internet. Ele usa túneis unidirecionais criptografados entre você e seus pares. Ninguém pode ver de onde vem o tráfego, para onde ele vai, ou qual é o conteúdo. Além disso, I2P oferece resistência ao reconhecimento e bloqueio de padrões por censores. Como a rede depende dos pares para encaminhar o tráfego, o bloqueio de localização também é reduzido.

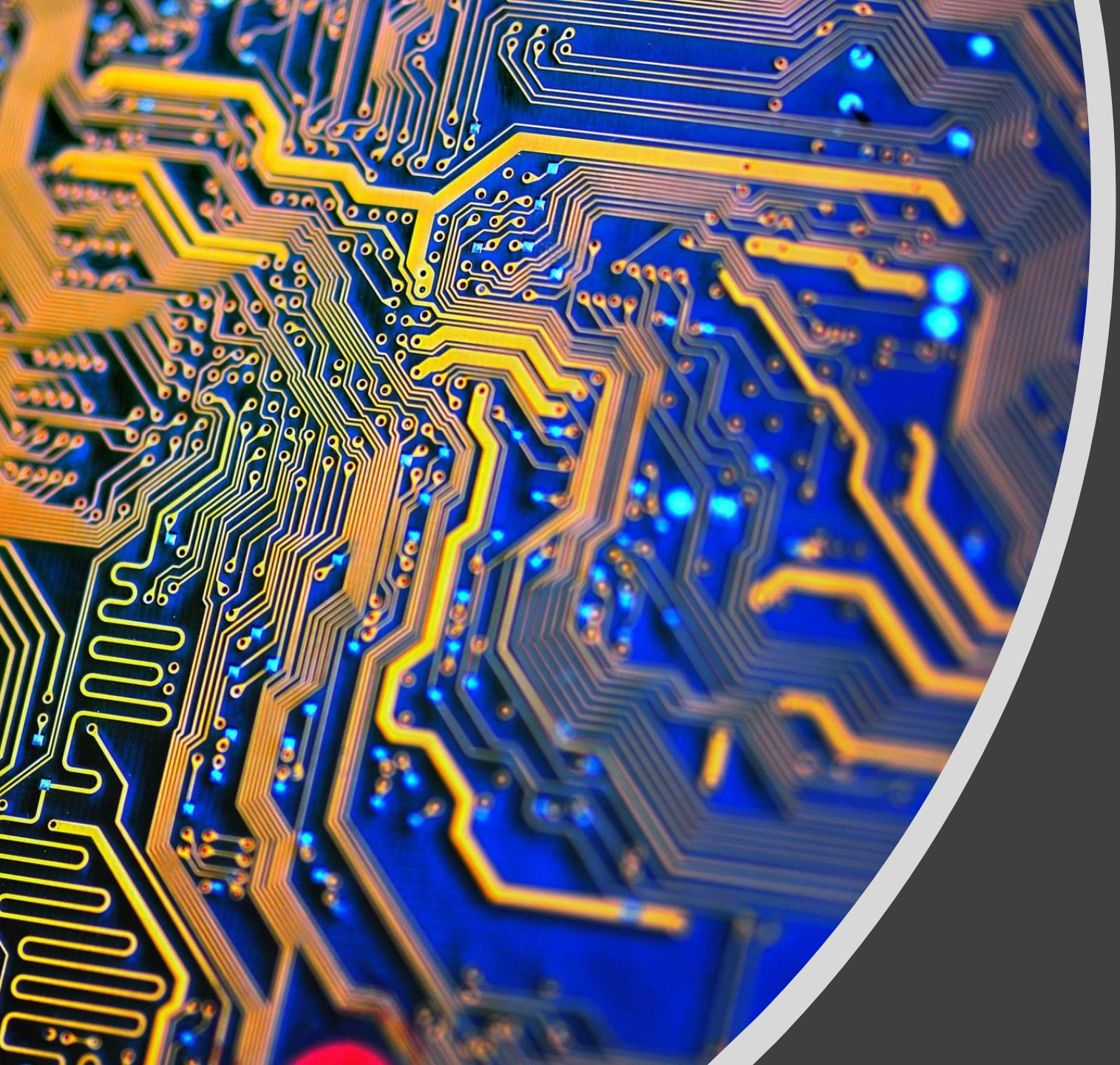
i2P and Freenet Configuration

- https://geti2p.net/pt-br/about/browser-config
- https://freenetproject.org/pages/help.html

Whonix vs Tails

- https://www.whonix.org/wiki/Comparison_with_Others
- https://www.whonix.org/wiki/Manually_Create_Whonix_VM_Settings
- https://tails.boum.org/contribute/design/Tor_network_configuration/
- https://tails.boum.org/





OSINT Process and Intelligence Investigation

Create Process OSINT

Phase 1: Setup

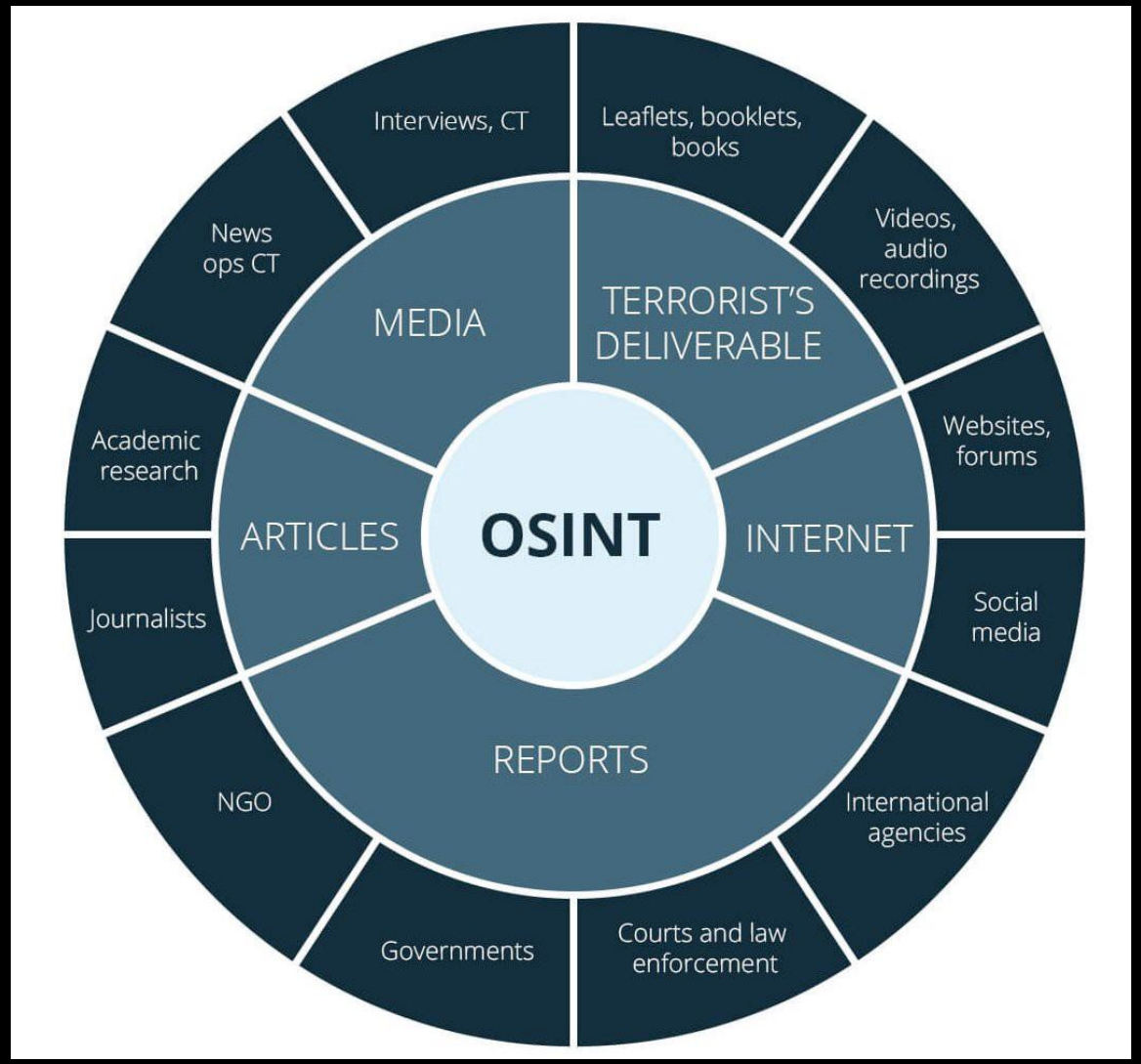
- Create a secure working environment
- Create new email addresses
- Create social media puppet accounts

Phase 2: Learning and Ingesting Information

- Read papers, blogs and articles on OSINT methodology and techniques

Phase 3: Use anonymity tools

- VPNs, Proxys, Network Privacy



Create Process OSINT

Fase 1: Configuração

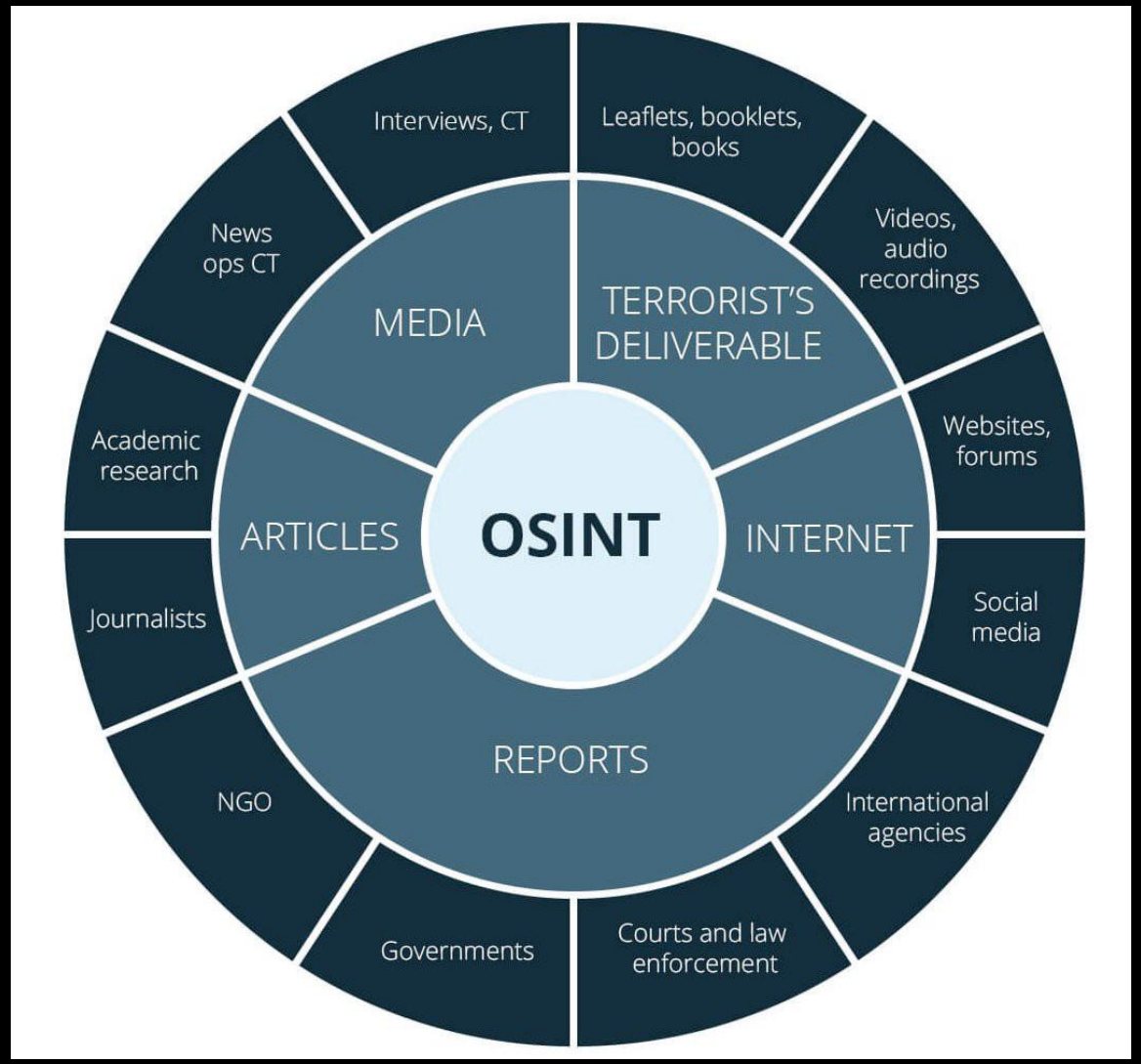
- Crie um ambiente de trabalho seguro
- Criar novos endereços de e-mail
- Crie contas de fantoches de mídia social

Fase 2: Aprendizagem e ingestão de informações

- Leia artigos, blogs e artigos sobre metodologia e técnicas OSINT

Fase 3: use ferramentas de anonimato

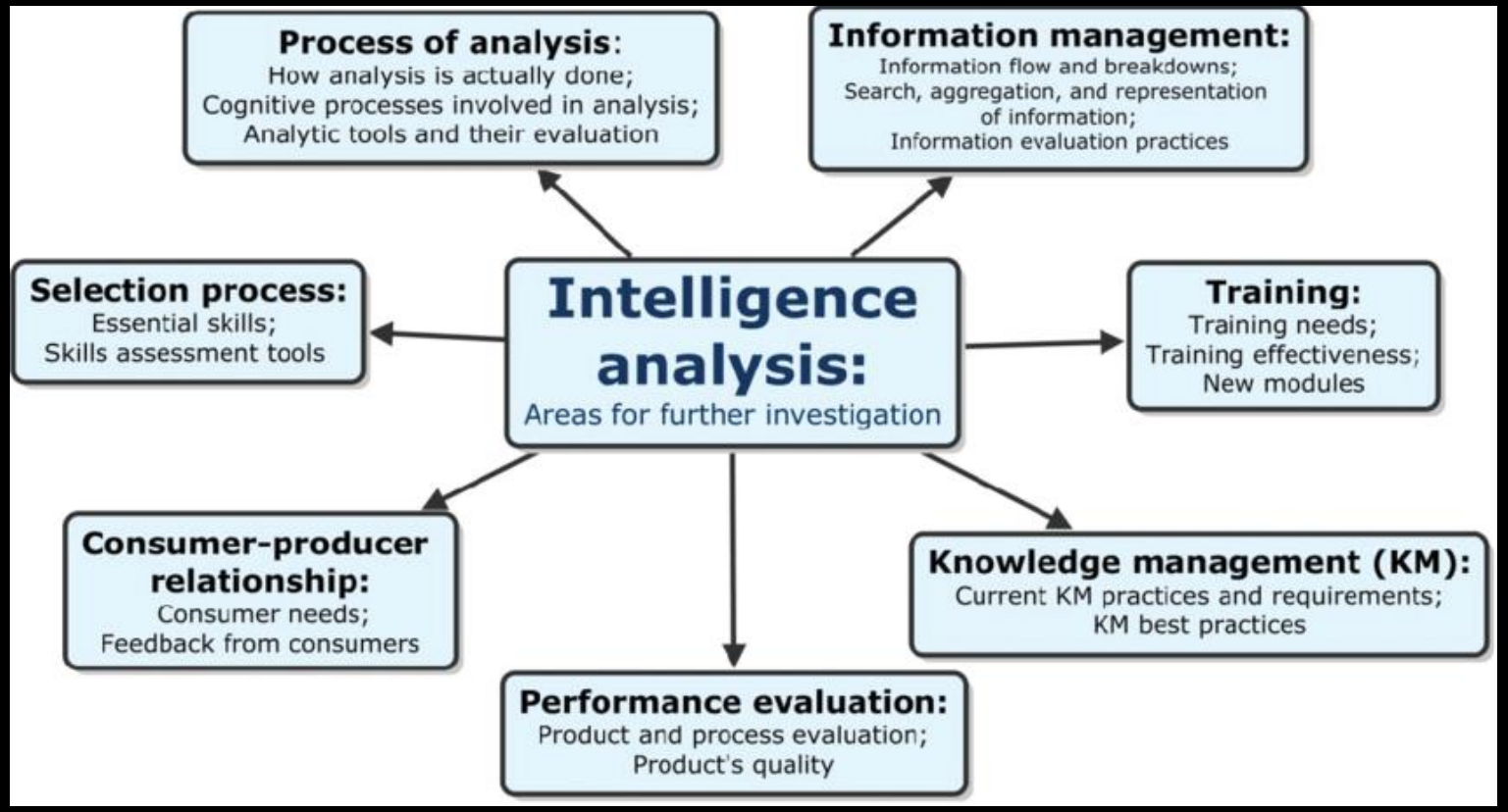
- VPNs, proxies, privacidade de rede



Online Investigation Toolkit

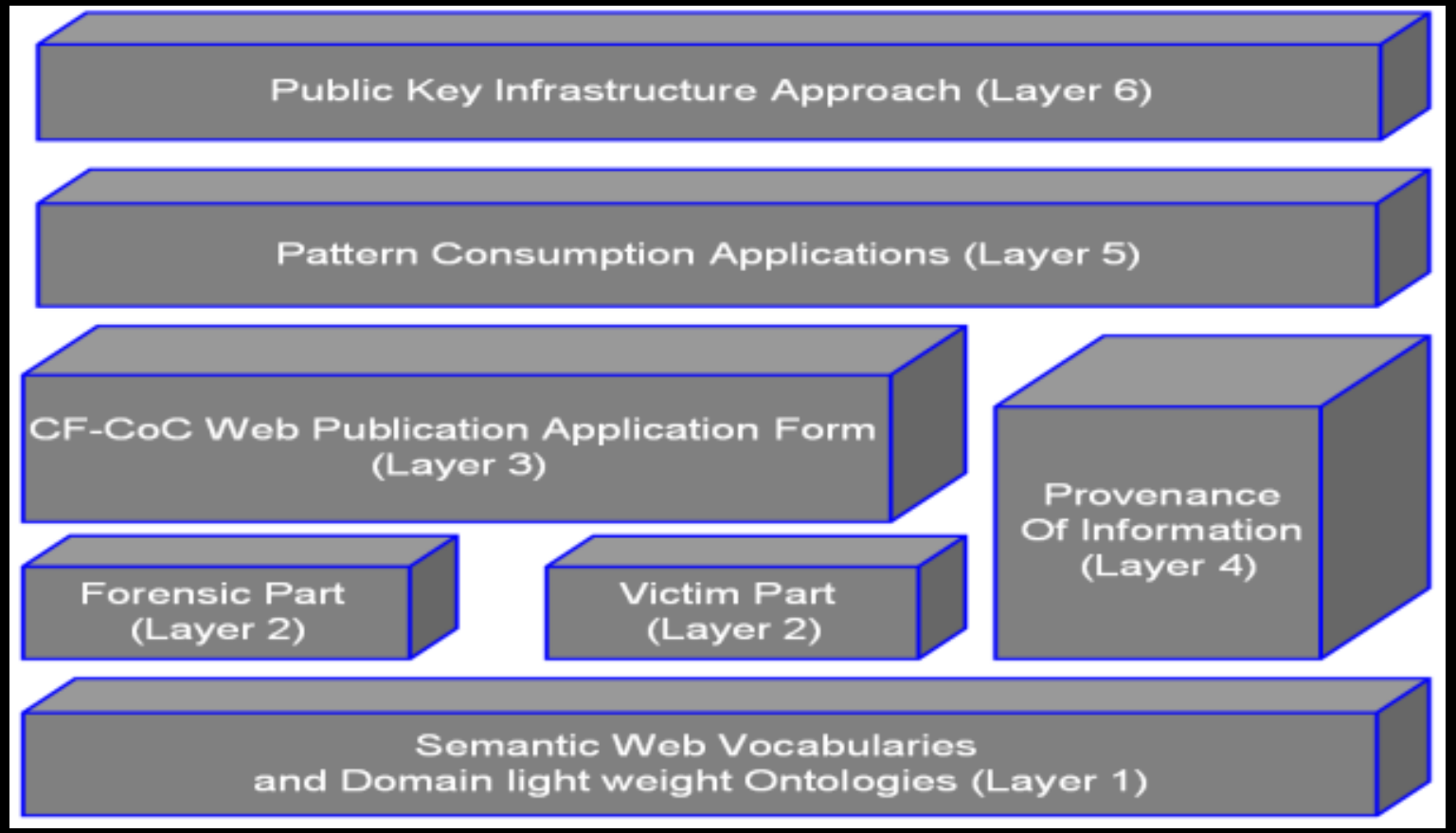
https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit#

Intelligence Analysis



Process Investigation

Chain of Custody



Chain of Custody

CHAIN OF CUSTODY: 8 KEY GUIDELINES

- Preparation of tools and techniques.
- Approach Strategy: Collect maximum number of evidence.
- Preservation of physical and digital evidence and isolate them to ensure their integrity.
- Collection and duplication of all digital evidence.
- Examination. In-depth search of evidence.
- Analysis of all evidence.
- Presentation. Explanation and a summary of the whole process.
- Returning evidence and accessing what lessons were learned. Final step of the investigation process.

OSINT Techniques and Intelligence Investigation - Commons

Open Source Intelligence Research

- Search Engine Research
- Reverse Image Research
- Archive Search Engine Research
- Email Address Research
- Username Research
- People Search Engines Research
- Telephone Number Research
- Online Map Research
- Domain Name Research
- IP Address Research
- Govt & Business Record Research
- Video Research

Search Engine

- Google
- Bing
- Yahoo
- AOL
- Infospace
- Lycos
- Exalead
- ASK
- Ecosia
- entireweb
- teoma
- yippy
- I Search From: simulate using Google Search from a different location or device, or perform a search with custom search settings.
- millionshort: Allows you to remove the top of the search engine results (e.g Remove top 100,1000,10000)

National Search Engines

- Yandex: Russia
- Search: Switzerland
- Alleba: Philippines
- Baidu | so | bhanvad China
- Eniro: Sweden
- Daum: South Korea
- Goo: Japan
- Onet: Poland
- Parseek: Iran
- SAPO: Portugal
- AONDE: Brazil
- Lableb: Arabic based search engine
- arabo: Arabic Search engine

Reverse Image Search

- Google reverse search
- Karmadecay
- TinEye
- Yandex reverse image search
- Bing visual search
- REVERSE IMAGE SEARCH
- Cam finds App: this is an App available for both Android and Apple devices. It uses visual search technology to recognize uploaded picture and give instant results about it like related images, local shopping results and a vast selection of web results.
- Image Identification Project
- Picsearch
- Yahoo search engine

File Search

- Global file search
- Archie
- File watcher
- Mamont
- NAPALM FTP Indexer
- Faganfinder
- DOCUMENT SEARCH ENGINE
- grayhatwarfare: Search for Open Amazon s3 Buckets and their contents.

Stock Photo Search

- ImageFinder
- istockphoto
- stocksnap
- gettyimages
- shutterstock
- pikwizard
- mostphotos
- photopin

Video Search

- YouTube
- Google video
- Yahoo video search
- Bing videos
- AOL videos
- StartPage video search
- Veoh
- Vimeo
- 360daily
- Official Facebook video search
- Crowd tangle (Facebook video search)
- Internet archive open source movies
- Live Leak
- Facebook live video map
- Meta Tube
- Geo Search Tool: Search for all movies according to a specific query entered by the user – the result set will be further filtered according to the distance from a specific location (city, village, intersection) and according to a specific time frame (past hour, past two or three hours ..etc.).
- Earth Cam
- Insecam

Custom Search Engine

- Google Custom Search Engines Finder
- 300+ Social Networking Sites
- 250+ Video Sharing Sites
- File Sharing Sites Search
- FTP and File Search Engine
- Github Awesome Custom Search Engine
- OSINT Tools, Resources & News Search
- Torrent Search
- Social Media Custom Search Engine
- IFTTT Applet Finder
- WordPress Content Hacker Search Engine
- Short URL Search Engine
- Raw Git Hacker Custom Search Engine

Devices Search Engine

- Shodan: Shodan is the world's first search engine for Internet-connected devices.
- Airport webcams
- Insecam
- Lookr
- Earthcam
- Openstreetcam
- Opentopia
- Pictimo
- Thingful
- Webcam.nl (NL)
- Webcams.travel
- Worldcam
- censys

Exploit Search Engine

- sploitus
- exploit-db
- Vulnerability Assesment Platform
- CVE Details
- nmmapper
- Vulmon
- exploits.shodan
- vulnerability-lab
- 0day.today

Data Leak Search Engine

- Leak.sx
- breachchecker
- Intelligence X
- 4iq
- leak-lookup
- leakcheck
- nuclearleaks
- weleakinfo
- leakpeek
- haveibeenpwned
- snusbase
- Have I Been Sold?
- leakedsource
- WikiLeaks
- Joe Black Security
- Black Kite
- scatteredsecrets
- dehashed
- Cryptome
- GlobaLeaks: is an open-source, free software intended to enable secure and anonymous whistleblowing initiatives
- Al Jazeera's Investigative Unit
- ghostproject
- Have I Been Facebooked? : Check if your data was part of the Facebook April 2021 breach.
- spycloud
- raidforums
- Have I Been Zucked? : Check if your details are included in the 2019 Facebook data breach.
- leakhispano
- Fasterbroadband
- F-Secure Identity Theft Checker
- Firefox Monitor
- Amibreached
- inoitsu
- Password Checkup by Google

Dark Web Search Engine

- ahmia
- Onion Search Engine
- darksearch
- Torch
- Not Evil
- Candle
- The Uncensored Hidden Wiki
- Parazite
- TorLinks
- gibiru
- HayStack
- TorDex

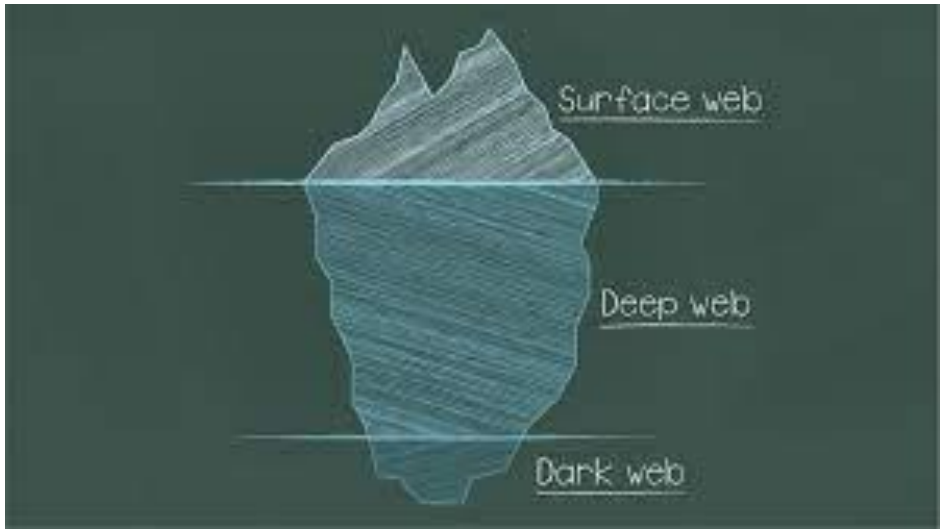
Offensive OSINT

https://www.offensiveosint.io/offensive-osint-s01e03-intelligence-gathering-on-critical-infrastructure-in-southeast-asia/

https://www.offensiveosint.io/offensive-osint-s01e02-deobfuscation-source-code-analysis-uncovering-cp-distribution-network/

https://www.offensiveosint.io/offensive-osint-s01e01-osint-rdp/

Dark Web Investigation



Memex

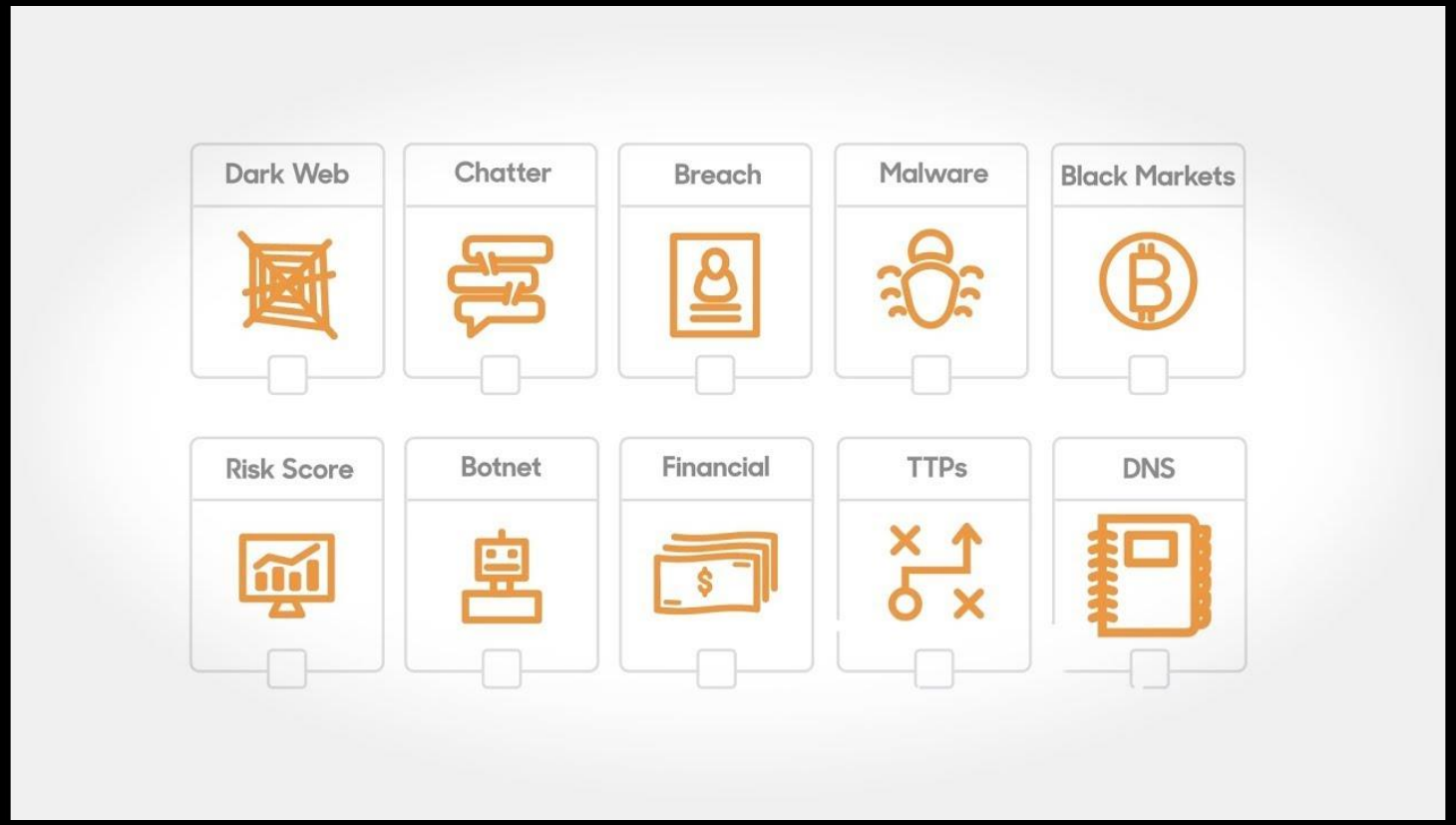
- Memex would ultimately apply to any public domain content; initially, DARPA plans to develop Memex to address a key Defense Department mission: fighting human trafficking. Human trafficking is a factor in many types of military, law enforcement and intelligence investigations and has a significant web presence to attract customers. The use of forums, chats, advertisements, job postings, hidden services, etc., continues to enable a growing industry of modern slavery. An index curated for the counter-trafficking domain, along with configurable interfaces for search and analysis, would enable new opportunities to uncover and defeat trafficking enterprises.
- Memex plans to explore three technical areas of interest: domain-specific indexing, domain-specific search, and DoD-specified applications. The program is specifically not interested in proposals for the following: attributing anonymous services, deanonymizing or attributing identity to servers or IP addresses, or accessing information not intended to be publicly available. The program plans to use commodity hardware and emphasize creating and leveraging open source technology and architecture.
- https://www.youtube.com/watch?v=SX0MJ2ACbPk

Memex

- A Memex acabaria se aplicando a qualquer conteúdo de domínio público; inicialmente, a DARPA planeja desenvolver o Memex para atender a uma missão-chave do Departamento de Defesa: combater o tráfico de seres humanos. O tráfico de pessoas é um fator em muitos tipos de investigações militares, policiais e de inteligência e tem uma presença significativa na web para atrair clientes. O uso de fóruns, chats, anúncios, vagas de emprego, serviços ocultos, etc., continua a permitir uma crescente indústria da escravidão moderna. Um índice com curadoria para o domínio de combate ao tráfico, juntamente com interfaces configuráveis para pesquisa e análise, permitiria novas oportunidades para descobrir e derrotar empresas de tráfico.
- A Memex planeja explorar três áreas técnicas de interesse: indexação específica de domínio, pesquisa específica de domínio e aplicativos especificados pelo DoD. O programa especificamente não está interessado em propostas para o seguinte: atribuição de serviços anônimos, desanonimização ou atribuição de identidade a servidores ou endereços IP, ou acesso a informações não destinadas a serem publicamente disponíveis. O programa planeja usar hardware comum e enfatizar a criação e alavancagem de tecnologia e arquitetura de código aberto.
- https://www.youtube.com/watch?v=SX0MJ2ACbPk

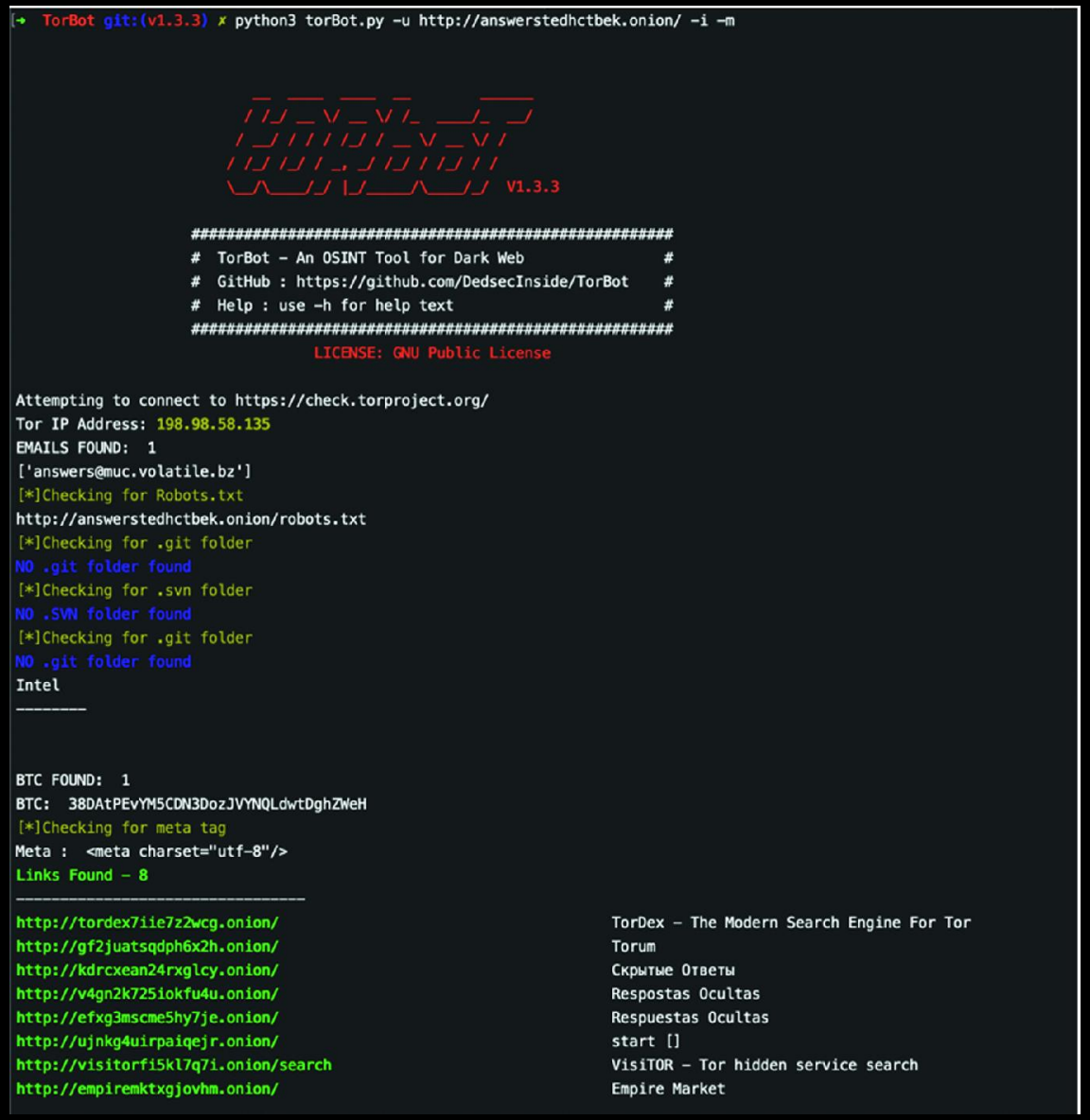
Dark Web Monitoring

- https://intsights.com/solutions/dark-web-monitoring
- https://www.youtube.com/watch?v=jKxySrFQCzk
- https://www.comparitech.com/net-admin/best-dark-web-monitoring-tools/



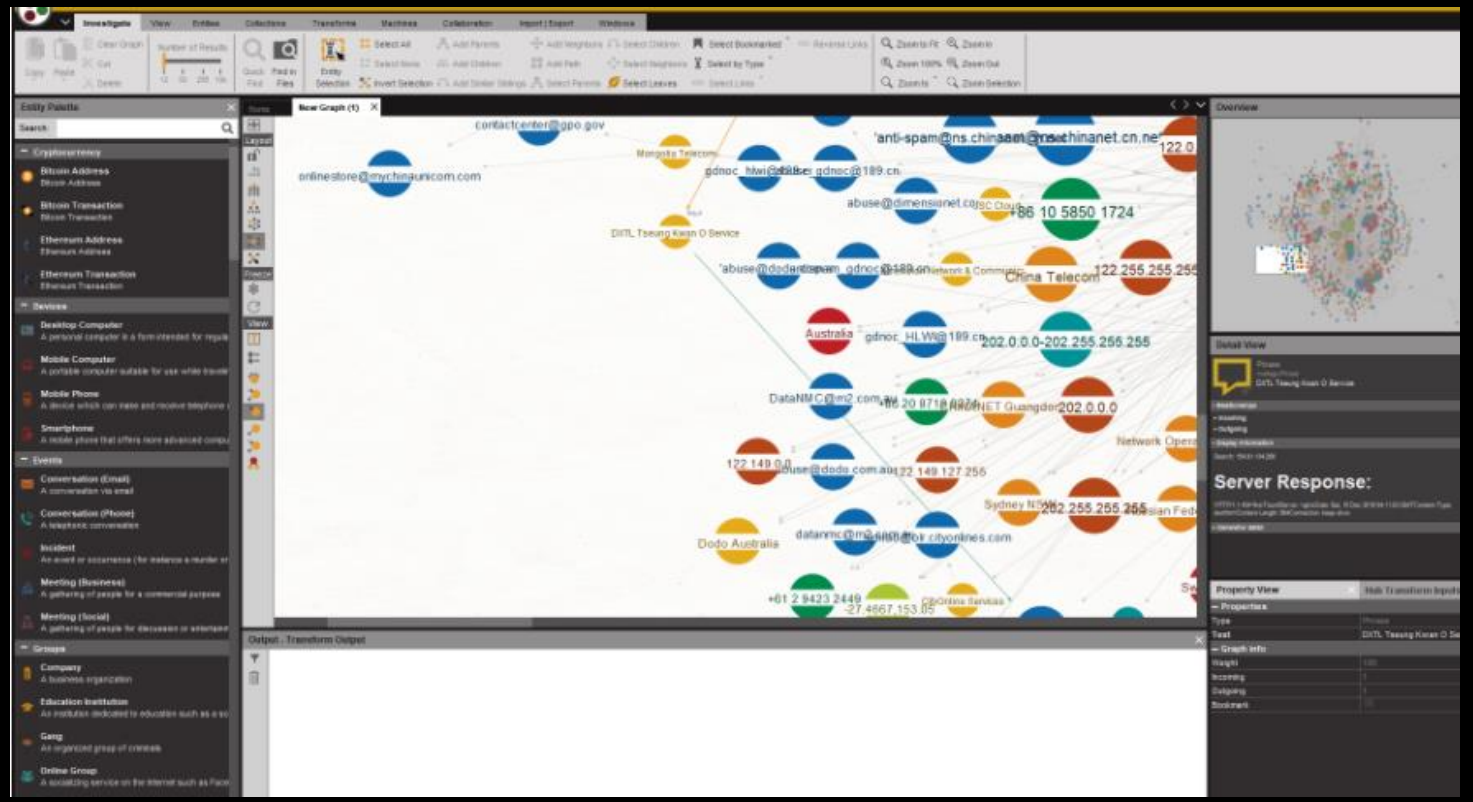
TorBot

- https://github.com/DedSecInside/TorBot
- https://haxf4rall.com/2019/06/27/torbot-osint-dark-web/



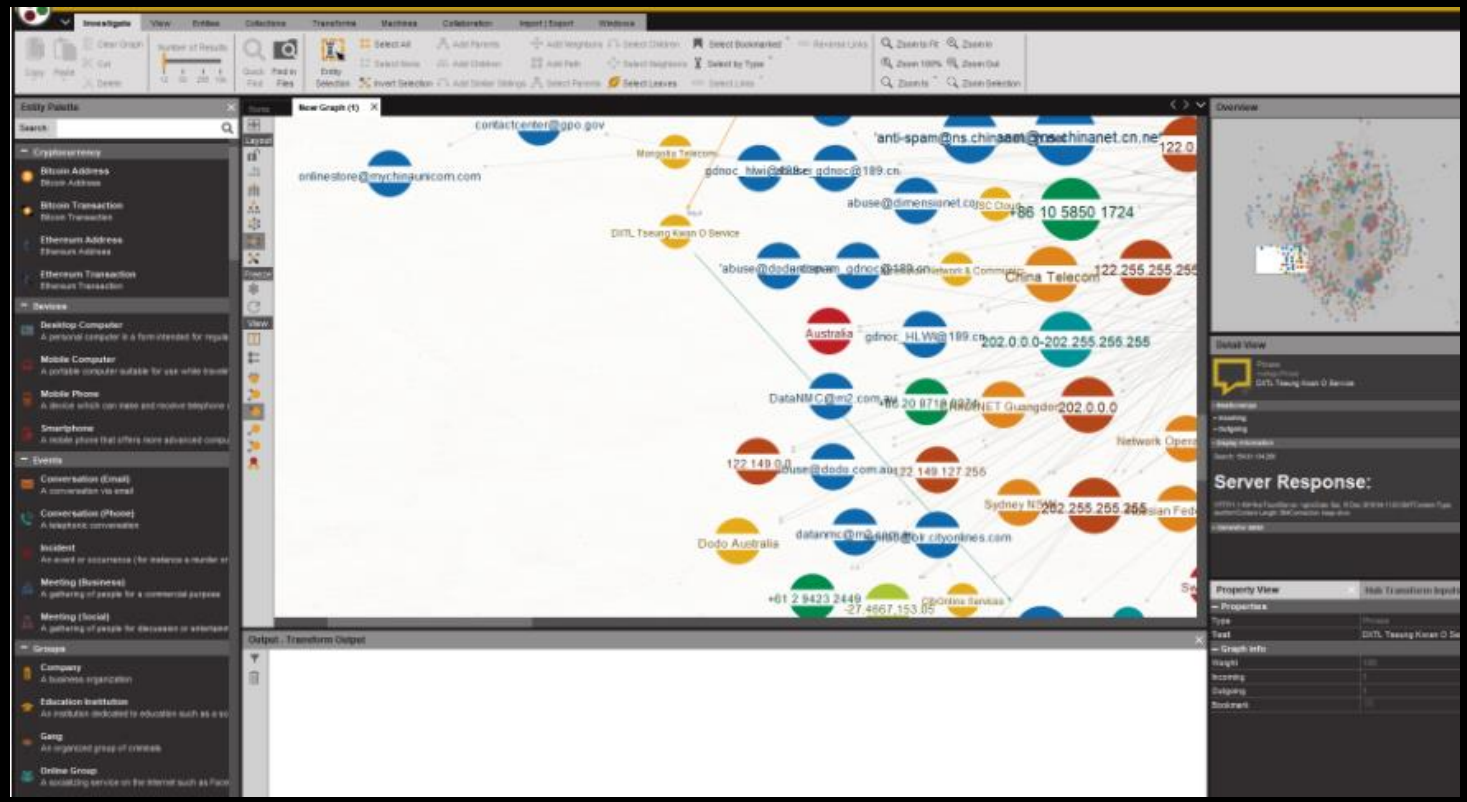
Maltego Case File

- CaseFile was born as a result of many Maltego users using the tool to build graphs with offline data that they have from their investigations. These users weren't using the Transforms available in Maltego and just needed the flexibility and performance of Maltego's graphing capability.
- CaseFile is a visual intelligence application that can be used to determine the relationships and real world links between hundreds of different types of information.
- CaseFile can be used to plot relationships between pieces of information - making it possible to see hidden connections even if they are multiple degrees of separation apart.
- CaseFile comes bundled with many different types of Entities that are commonly used in investigations allowing you to act quickly and efficiently. CaseFile also has the ability to add custom Entity types allowing you to extend the product to your own data sets.



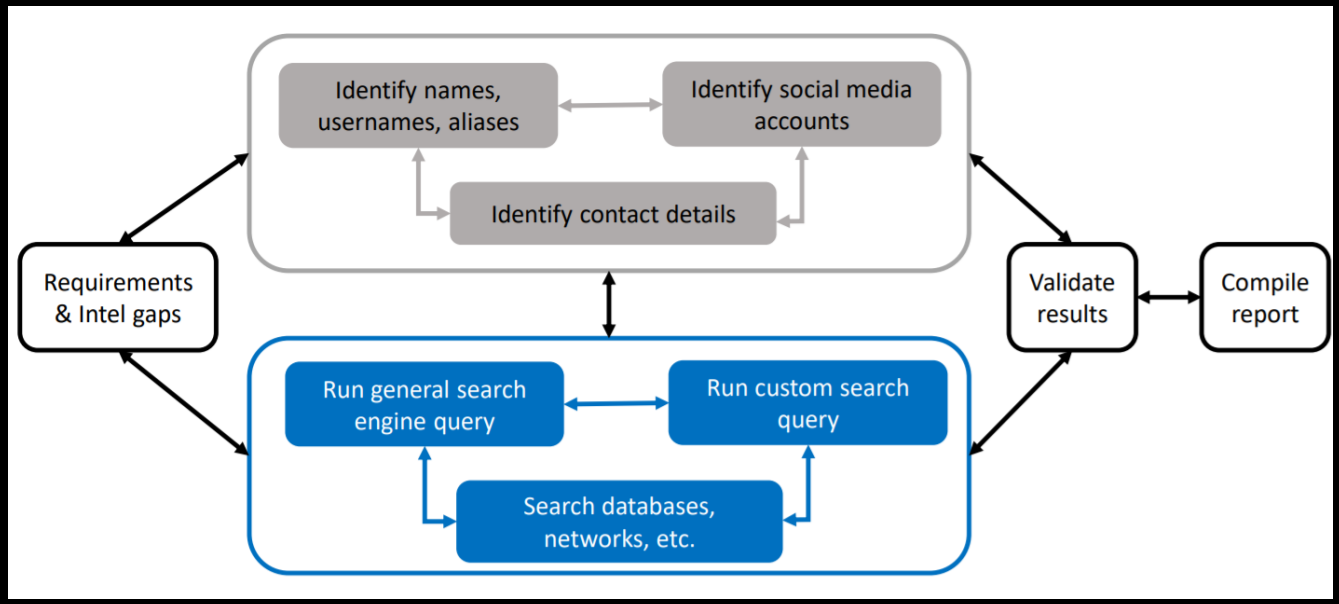
Maltego Case File

- CaseFile nasceu como resultado de muitos usuários Maltego usando a ferramenta para construir gráficos com dados offline que eles têm de suas investigações. Esses usuários não estavam usando os Transforms disponíveis no Maltego e só precisavam da flexibilidade e desempenho dos recursos gráficos do Maltego.
- CaseFile é um aplicativo de inteligência visual que pode ser usado para determinar os relacionamentos e links do mundo real entre centenas de diferentes tipos de informações.
- CaseFile pode ser usado para traçar relacionamentos entre informações - tornando possível ver conexões ocultas, mesmo que estejam em vários graus de separação.
- O CaseFile vem com muitos tipos diferentes de Entidades que são comumente usadas em investigações, permitindo que você aja com rapidez e eficiência. O CaseFile também tem a capacidade de adicionar tipos de Entidade personalizados, permitindo que você estenda o produto para seus próprios conjuntos de dados.



People Search Investigation

- Decide how to organize / collate data
- Don’t break the law
- Identify formal names
- Identify titles and honorifics
- Identify the target’s social media profiles
- Identify the target’s contact details
- Identify the target’s usernames
- Identify the target’s locations
- Identify the target’s affiliations



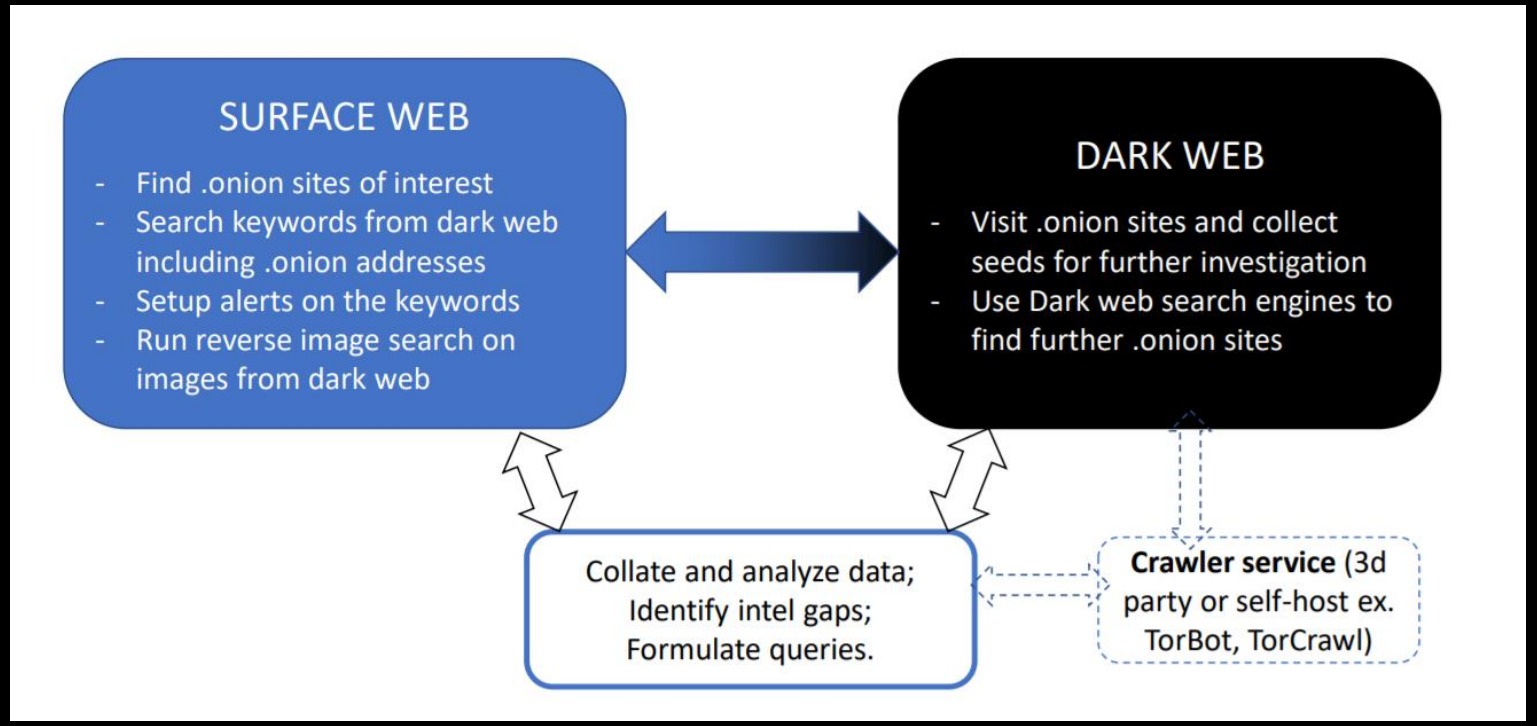
Email Search Investigation

- Usernames often associate with emails
- Run Google queries / setup Google Alerts
- Check breached data (https://haveibeenpwned.com etc)
- Find private email address (constructs and guesses, socmint)
- Find professional email address (www.hunter.io etc)
- Run email validator (www.email-validator.net etc)
- Reverse email checks (www.pipl.com etc)
- Check email provider for business emails (www.mxtoolbox.com etc)
- Check blacklists (www.mxtoolbox.com etc)

Digital data hierarchy

Individual Data	Organisational Data	Network Data
• Key personnel • Contact details • Email addresses • Email conventions • Phone numbers	• Business locations • Company addresses • Phone numbers • Security policies • Web service providers • Social media assets	• IP Data • Internal domain names • Name servers • Email servers • Web technologies • System technologies

Tor Investigation Framework



Tor Security Tips

- Before opening the Tor browser, close all other software running on your system and disable any plugins in the browser
- Generate “New Identity” or “New Tor Circuit” every time you access a new .onion link
- Do not download any content unless necessary
- Use sock puppet accounts

Data Mining

https://github.com/SimonDele/Enlighten-DarkWeb-Markets-with-Data-Mining

https://www.cyberwatching.eu/projects/1690/cybersane/news-events/blog-post-web-crawlers-data-mining-and-extraction-knowledge-news-articles-and-dark-web

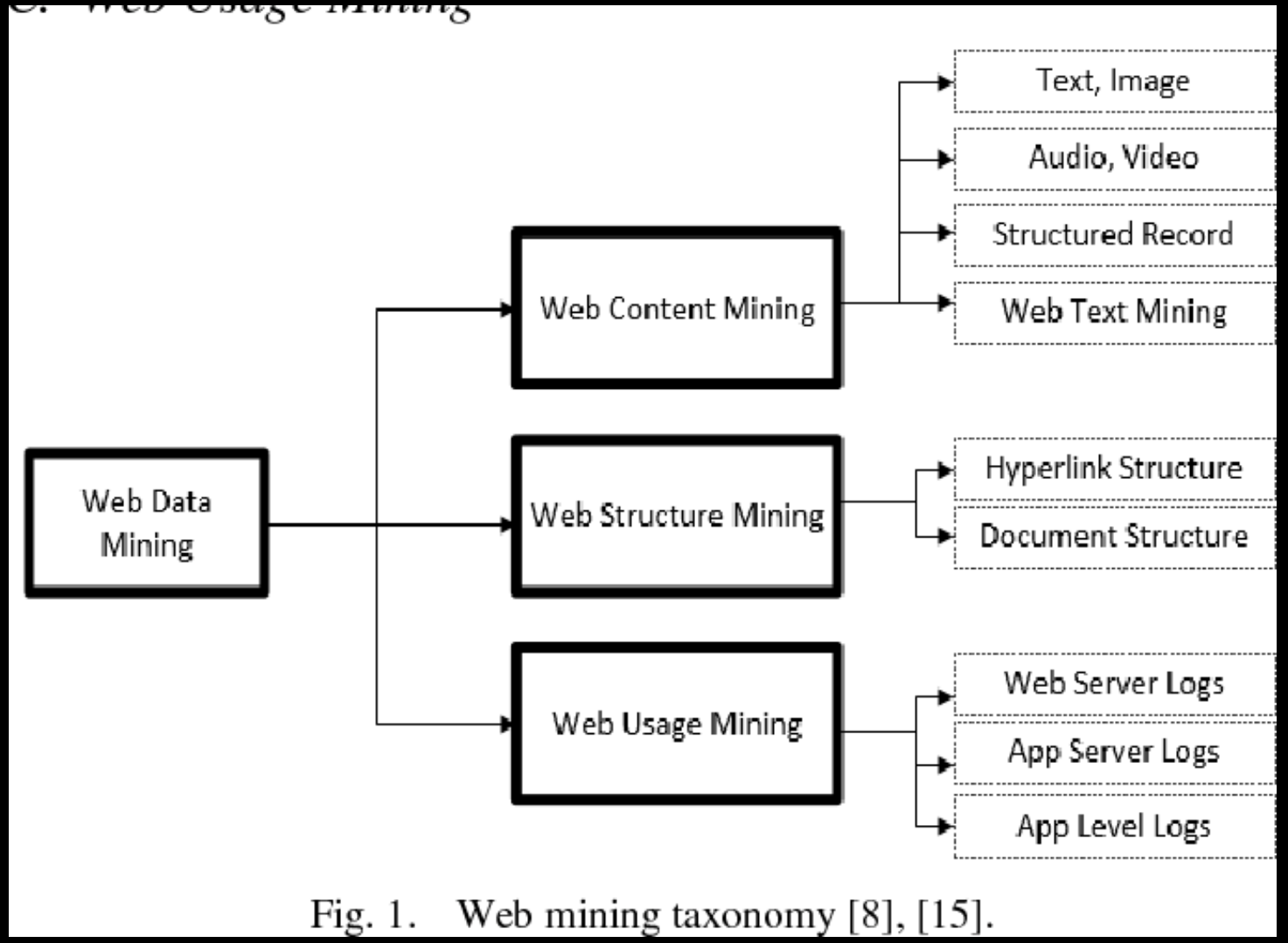
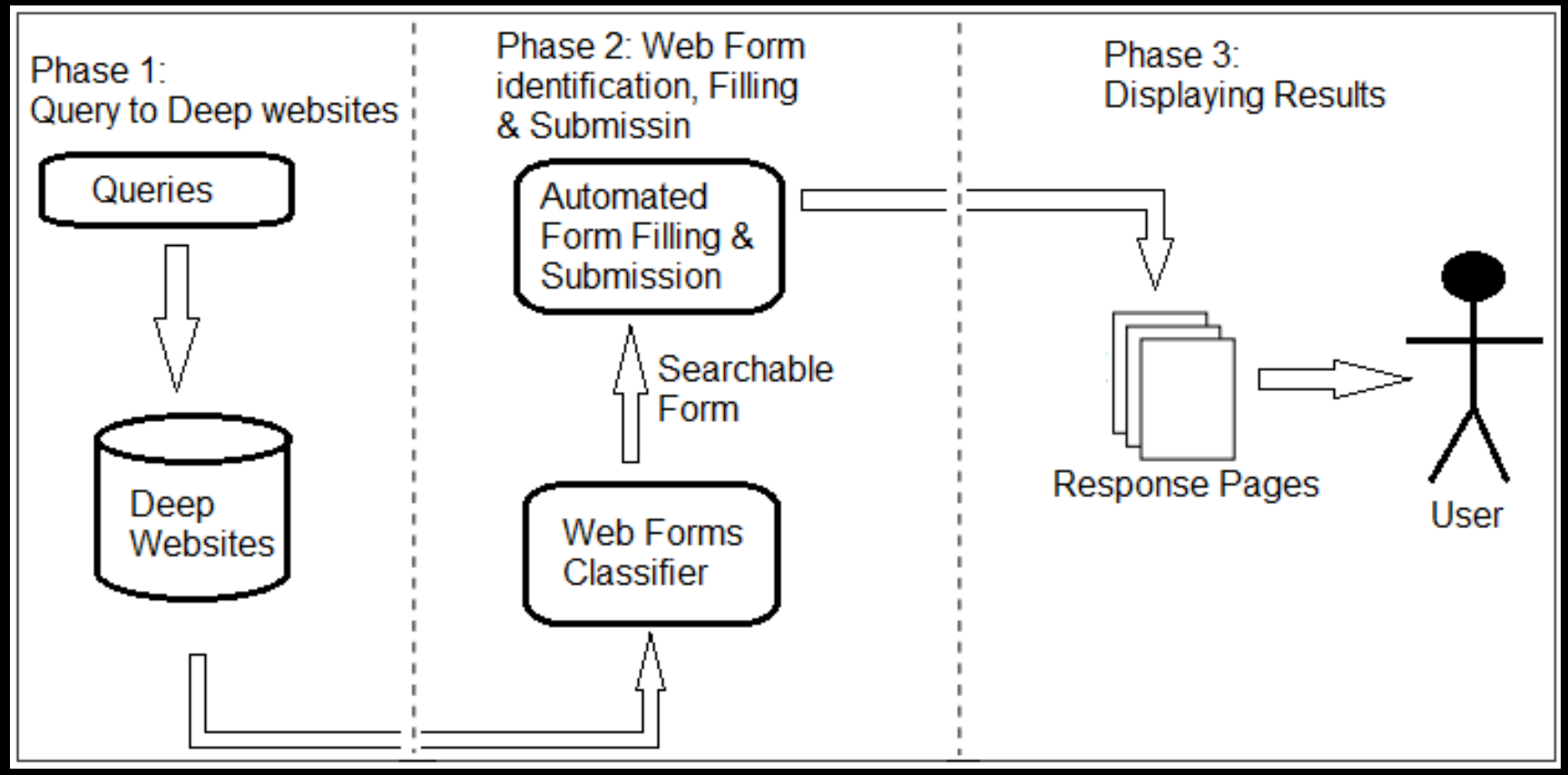


Fig. 1. Web mining taxonomy [8], [15].

DEEP WEB EXTRACTOR



NIT

- *"The NIT was a* Flash based *application that was developed by H.D.Moore and was released as part of Metasploit. The NIT, or more formally,* Metaspolit *Decloaking Engine was designed to provide the real IP address of web users, regardless of proxy settings."* states *the forensic report.*
- *"O NIT era um aplicativo baseado em Flash que foi desenvolvido pela H.D.Moore e lançado como parte do Metasploit. O NIT, ou mais formalmente, Metaspolit Decloaking Engine, foi projetado para fornecer o endereço IP real dos usuários da Web, independentemente das configurações de proxy." declara o relatório forense.*
- The NIT itself consists of three major components: the exploit which takes over the Tor browser (a customized copy of FireFox), the payload which conducts the search needed to deanonymize the target, and server support infrastructure which not only hosts the NIT but modifies each copy sent to include a unique identifier.
- O NIT em si consiste em três componentes principais: a exploração que assume o navegador Tor (uma cópia personalizada do FireFox), a carga útil que conduz a pesquisa necessária para desanonimizar o alvo e a infraestrutura de suporte ao servidor que não apenas hospeda o NIT, mas modifica cada cópia enviada para incluir um identificador exclusivo.

- https://nakedsecurity.sophos.com/2016/05/19/firefox-users-left-feeling-vulnerable-as-judge-keeps-tor-hack-under-wraps/
- https://www.lawfareblog.com/end-nit

Malware Development Dark Web Investigation

- https://www.secjuice.com/osint-daily-dose-of-malware/
- https://portswigger.net/daily-swig/fbis-dark-web-investigations-hampered-by-inefficiencies-overlapping-objectives-of-different-units
- https://www.pulsarsecurity.com/services/dark-web-assessment
- AbuseHelper - Uma estrutura open-source para receber e redistribuir feeds de abuso e ameaça Intel.
- AlienVault Open Threat Exchange - Compartilhe e colabore no desenvolvimento de Threat Intelligence.
- Combinar - Ferramenta para reunir indicadores de Inteligência de ameaças de fontes publicamente disponíveis.
- Fileintel - Puxe inteligência por hash de arquivo.
- Hostintel - Puxe a inteligência por host.
- IntelMQ - Uma ferramenta para CERTs para o processamento de dados de incidentes usando uma fila de mensagens.
- IOC Editor - Um editor gratuito para arquivos XML IOC.
- Ioc_writer - Biblioteca Python para trabalhar com objetos OpenIOC, de Mandiant.
- Massa Octo Spice - Anteriormente conhecido como CIF (Collective Intelligence Framework). Acumula IOCs de várias listas. Curated pela fundação dos dispositivos de CSIRT .
- MISP - Plataforma de Compartilhamento de Informações de Malware com curadoria do Projeto MISP .
- PassiveTotal - Pesquise, conecte, marque e compartilhe IPs e domínios.
- PyIOCe - Um editor Python OpenIOC.
- Threataggregator - agrega ameaças de segurança de várias fontes, incluindo algumas das listadas abaixo em outros recursos .
- ThreatCrowd - Um motor de busca de ameaças, com visualização gráfica.
- ThreatTracker - Um script Python para monitorar e gerar alertas baseados em IOCs indexados por um conjunto de motores de busca personalizados do Google.
- TIQ-test - Visualização de dados e análise estatística de feeds de Threat Intelligence.

Malware Development Dark Web Investigation

- AbuseHelper - An open-source framework for receiving and redistributing Intel abuse and threat feeds.
- AlienVault Open Threat Exchange - Share and collaborate on Threat Intelligence development.
- Combine - Tool for gathering Threat Intelligence indicators from publicly available sources.
- Fileintel - Pull intelligence by file hash.
- Hostintel - Pull intelligence by host.
- IntelMQ - A tool for CERTs for processing incident data using a message queue.
- IOC Editor - A free editor for IOC XML files.
- Ioc_writer - Python library for working with OpenIOC objects, by Mandiant.
- Pasta Octo Spice - Formerly known as CIF (Collective Intelligence Framework). Accumulates IOCs from multiple lists. Curated by the CSIRT Devices Foundation .
- MISP - Malware Information Sharing Platform curated by the MISP Project .
- PassiveTotal - Search, connect, tag and share IPs and domains.
- PyIOCe - A Python OpenIOC editor.
- Threataggregator - aggregates security threats from various sources, including some of those listed below under Other Resources .
- ThreatCrowd - A threat search engine, with graphical visualization.
- ThreatTracker - A Python script to monitor and generate alerts based on IOCs indexed by a set of Google's custom search engines .
- TIQ-test - Data visualization and statistical analysis of Threat Intelligence feeds.

About Investigation Dark Web

- https://www.vice.com/en/article/jpgm7d/how-the-fbi-identified-suspects-behind-the-dark-webs-largest-child-porn-site-playpen
- https://www.youtube.com/watch?v=L5YYHJ35vHE
- https://www.youtube.com/watch?v=UXfqMVCALJk
- https://calert.info/details.php?id=1270
- https://bitcoinist.com/darkweb-dream-market-now-a-bitcoin-payment-fbi-honeypot/
- https://latesthackingnews.com/2017/06/11/20297
- https://www.digitaltrends.com/computing/fbi-running-darknet-child-port-sites-tor-malware/
- https://www.independent.co.uk/life-style/gadgets-and-tech/news/dark-web-drug-dream-market-fbi-honeypot-a8843456.html

About Investigation Dark Web - Brazilian

- https://www.youtube.com/watch?v=mDzqdv3VjKE
- https://www.youtube.com/watch?v=ywUxkvCK96w
- https://www.youtube.com/watch?v=edcFMhUwCkY
- https://www.youtube.com/watch?v=0UuHn27dFpE
- https://www.youtube.com/watch?v=p2IC4VQcxyo
- https://www.youtube.com/watch?v=Pzg-BnrUYXI
- https://www.youtube.com/watch?v=u6mCVB19rfc
- https://www.youtube.com/watch?v=IvoVww0smfc
- https://www.youtube.com/watch?v=HTgl_wEUjN4

Dark Web OSINT Tools

- Hunchly - https://www.hunch.ly/darkweb-osint/
- Tor66 Fresh Onions - http://tor66sewebgixwhcqfnp5inzp5x5uohhdy3kvtnyfxc2e5mxiuh34iid.onion/fresh
- Onionscan - https://github.com/s-rah/onionscan
- Onioff - https://github.com/k4m4/onioff
- Onion-nmap - https://github.com/milesrichardson/docker-onion-nmap
- TorBot - https://github.com/DedSecInside/TorBot
- TorCrawl - https://github.com/MikeMeliz/TorCrawl.py
- VigilantOnion - https://github.com/andreyglauzer/VigilantOnion
- OnionIngestor - https://github.com/danieleperera/OnionIngestor

HoneyPots Dark Web

- In computer terminology, a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site and contain information or resources of value to attackers. It is actually isolated, monitored, and capable of blocking or analyzing the attackers. This is similar to police sting operations, colloquially known as "baiting" a suspect.
- Na terminologia de computador, um honeypot é um mecanismo de segurança de computador definido para detectar, desviar ou, de alguma forma, neutralizar tentativas de uso não autorizado de sistemas de informação . Geralmente, um honeypot consiste em dados (por exemplo, em um site de rede) que parecem ser uma parte legítima do site e contêm informações ou recursos de valor para os invasores. Na verdade, é isolado, monitorado e capaz de bloquear ou analisar os invasores. Isso é semelhante às operações policiais , coloquialmente conhecidas como "iscando" um suspeito.
- https://ieeexplore.ieee.org/document/9265528
- https://www.quora.com/Is-Tor-essentially-an-NSA-honeypot
- https://www.youtube.com/watch?v=Up5xl7BLihc
- https://www.reddit.com/r/TOR/comments/3ci3po/14_days_running_a_secret_dark_web_pedophile/

HoneyPots Tools

HoneyTrap

- Combine multiple services to one honeypot, eg a LAMP server
- Honeytrap Agent will download the configuration from the Honeytrap Server
- Use the Honeytrap Agent to redirect traffic out of the network to a seperate network
- Deploy a large amount agents while having one Honeytrap Server, configuration will be downloaded automatically and logging centralized
- Payload detection to determine which service should handle the request, one port can handle multiple protocols
- Monitor lateral movement within your network with the Sensor listener. The sensor will complete the handshake (in case of tcp), and store the payload
- Create high interaction honeypots using the LXC or remote hosts directors, traffic will be man-in-the-middle proxied, while information will be extracted
- Extend honeytrap with existing honeypots (like cowrie or glutton), while using the logging and listening framework of Honeytrap
- Advanced logging system with filtering and logging to Elasticsearch, Kafka, Splunk, Raven, File or Console
- Services are easily extensible and will extract as much information as possible
- Low- to high interaction Honeypots, where connections will be upgraded seamless to high interaction
- https://github.com/honeytrap/honeytrap
- Awesome HoneyPots: https://github.com/Fedex100/awesome-honeypots

HoneyPots Tools

HoneyTrap

- Combine vários serviços em um honeypot, por exemplo, um servidor LAMP
- O Honeytrap Agent baixará a configuração do Honeytrap Server
- Use o Honeytrap Agent para redirecionar o tráfego da rede para uma rede separada
- Implante uma grande quantidade de agentes enquanto tiver um Honeytrap Server, a configuração será baixada automaticamente e o registro centralizado
- Detecção de carga útil para determinar qual serviço deve lidar com a solicitação, uma porta pode lidar com vários protocolos
- Monitore o movimento lateral dentro de sua rede com o ouvinte Sensor. O sensor completará o handshake (no caso de tcp) e armazenará a carga útil
- Crie honeypots de alta interação usando o LXC ou diretores de hosts remotos, o tráfego será man-in-the-middle proxy, enquanto as informações serão extraídas
- Estenda o honeytrap com honeypots existentes (como cowrie ou glutton), enquanto usa a estrutura de registro e escuta do Honeytrap
- Sistema de registro avançado com filtragem e registro em Elasticsearch, Kafka, Splunk, Raven, File ou Console
- Os serviços são facilmente extensíveis e extrairão o máximo de informações possível
- Honeypots de baixa a alta interação, onde as conexões serão atualizadas sem interrupção para alta interação
- https://github.com/honeytrap/honeytrap
- Awesome HoneyPots: https://github.com/Fedex100/awesome-honeypots

Subreddits

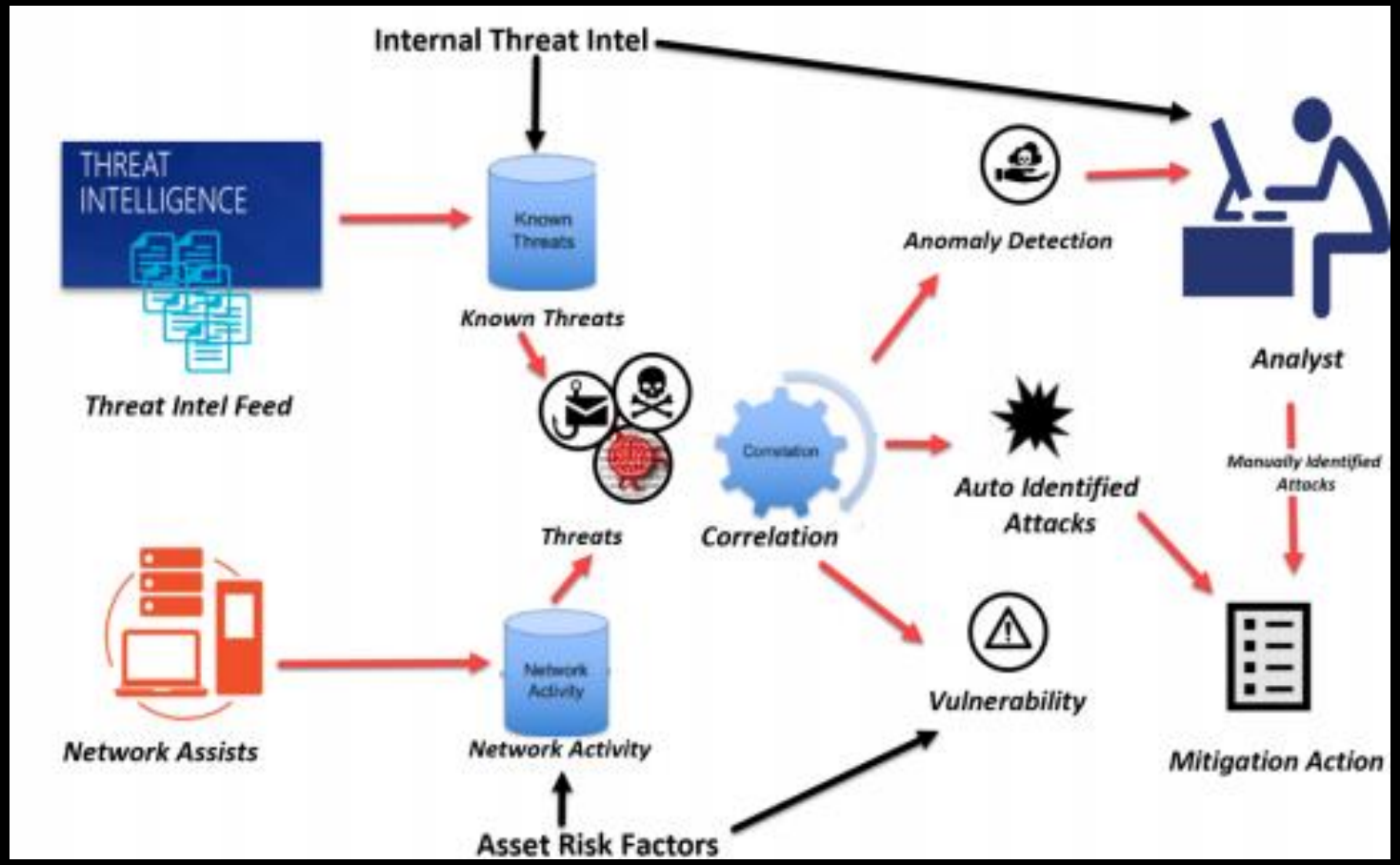
- r/Onions - https://www.reddit.com/r/onions/
- r/DNMBusts - https://www.reddit.com/r/DNMBusts/
- r/deepweb - https://www.reddit.com/r/deepweb/
- r/TOR - https://www.reddit.com/r/TOR/
- r/Darknet - https://www.reddit.com/r/darknet/

TheHarvester

- theHarvester is a very simple to use, yet powerful and effective tool designed to be used in the early stages of a
penetration test or red team engagement. Use it for open source intelligence (OSINT) gathering to help determine a
company's external threat landscape on the internet. The tool gathers emails, names, subdomains, IPs and URLs using
multiple public data sources
- theHarvester é uma ferramenta muito simples de usar, mas poderosa e eficaz, projetada para ser usada nos estágios iniciais de um
teste de penetração ou envolvimento da equipe vermelha. Use-o para coleta de inteligência de código aberto (OSINT) para ajudar a determinar
o cenário de ameaças externas de uma empresa na Internet. A ferramenta reúne e-mails, nomes, subdomínios, IPs e URLs usando
várias fontes de dados públicas

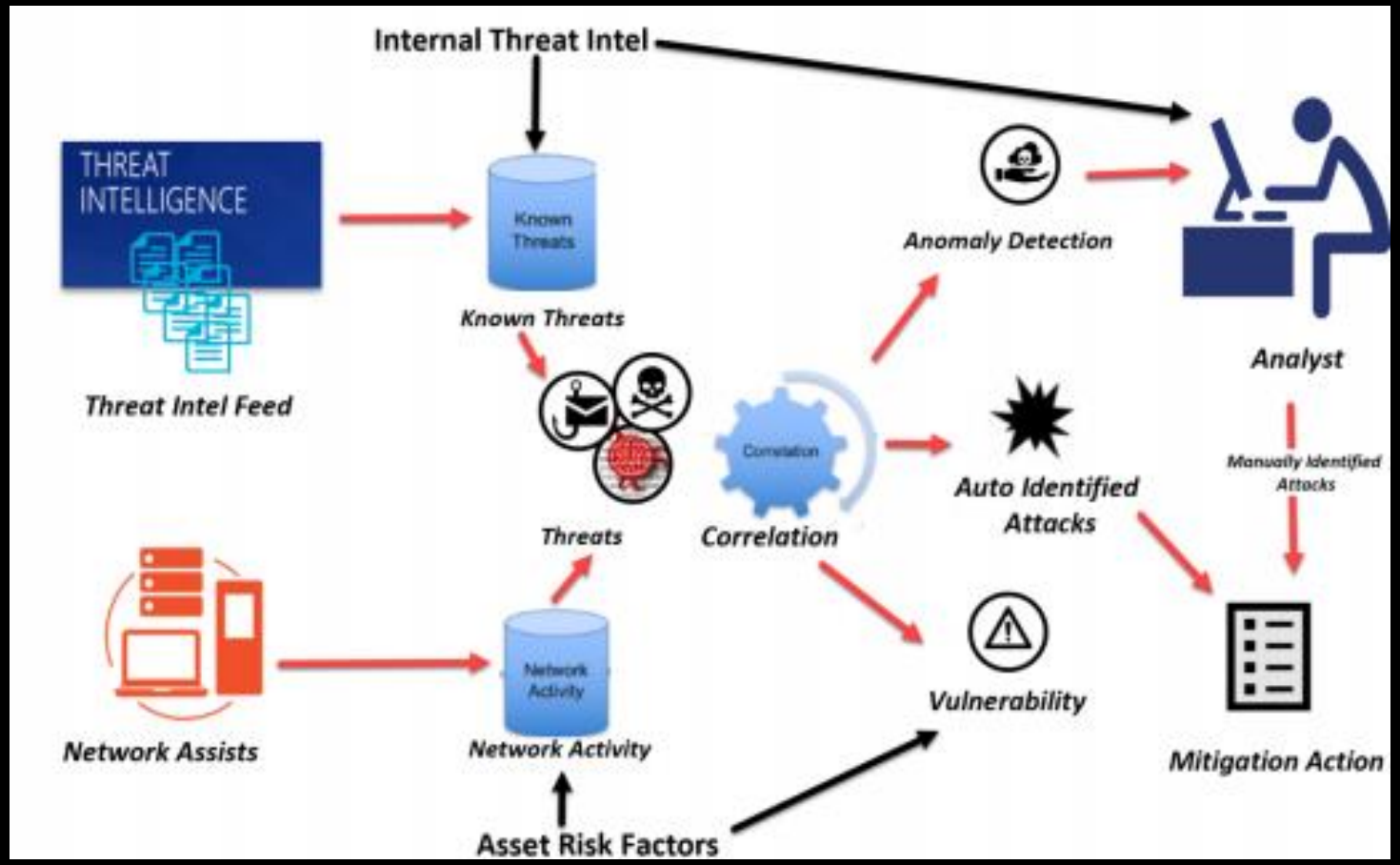
Threat Intelligence Platforms

- Threat Intelligence Platform is an emerging technology discipline that helps organizations aggregate, correlate, and analyze threat data from multiple sources in real time to support defensive actions. TIPs have evolved to address the growing amount of data generated by a variety of internal and external resources (such as system logs and threat intelligence feeds) and help security teams identify the threats that are relevant to their organization. By importing threat data from multiple sources and formats, correlating that data, and then exporting it into an organization's existing security systems or ticketing systems, a TIP automates proactive threat management and mitigation. A true TIP differs from typical enterprise security products in that it is a system that can be programmed by outside developers, in particular, users of the platform. TIPs can also use APIs to gather data to generate configuration analysis, Whois information, reverse IP lookup, website content analysis, name servers, and SSL certificates.
- https://www.esecurityplanet.com/products/threat-intelligence-platforms/



Threat Intelligence Platforms

- A Threat Intelligence Platform é uma disciplina de tecnologia emergente que ajuda as organizações a agregar, correlacionar e analisar dados de ameaças de várias fontes em tempo real para apoiar ações defensivas. Os TIPs evoluíram para lidar com a crescente quantidade de dados gerados por uma variedade de recursos internos e externos (como logs do sistema e feeds de inteligência de ameaças) e ajudar as equipes de segurança a identificar as ameaças relevantes para sua organização. Ao importar dados de ameaças de várias fontes e formatos, correlacionar esses dados e exportá-los para os sistemas de segurança ou sistemas de tíquetes existentes de uma organização, um TIP automatiza o gerenciamento e a mitigação proativos de ameaças. Um verdadeiro TIP difere dos produtos de segurança corporativos típicos, pois é um sistema que pode ser programado por desenvolvedores externos, em particular, usuários da plataforma. TIPs também podem usar APIs para coletar dados para gerar análise de configuração , Whoisinformações, pesquisa reversa de IP , análise de conteúdo de sites, servidores de nomes e certificados SSL
- https://www.esecurityplanet.com/products/threat-intelligence-platforms/



Framework for More Accessible Dark Web Marketplace Investigations

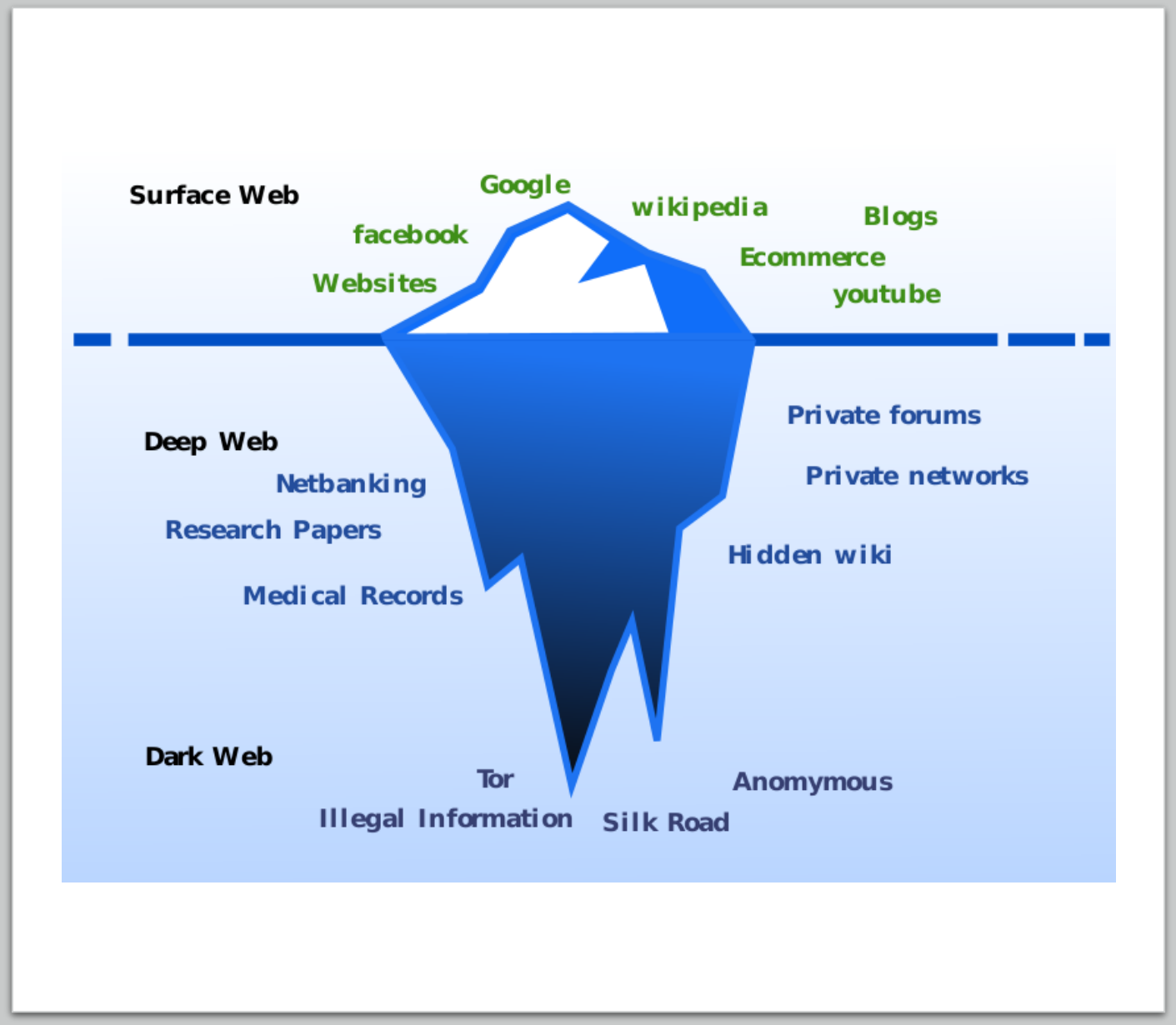
Bulk Extractor

- bulk_extractor is a high-performance digital forensics exploitation tool. It is a "get evidence" button that rapidly scans any kind of input (disk images, files, directories of files, etc) and extracts structured information such as email addresses, credit card numbers, JPEGs and JSON snippets without parsing the file system or file system structures. The results are stored in text files that are easily inspected, searched, or used as inputs for other forensic processing. bulk_extractor also creates histograms of certain kinds of features that it finds, such as Google search terms and email addresses, as previous research has shown that such histograms are especially useful in investigative and law enforcement applications.
- bulk_extractoré uma ferramenta de exploração forense digital de alto desempenho. É um botão "obter evidências" que verifica rapidamente qualquer tipo de entrada (imagens de disco, arquivos, diretórios de arquivos, etc.) e extrai informações estruturadas, como endereços de e-mail, números de cartão de crédito, JPEGs e trechos JSON sem analisar estruturas do sistema de arquivos. Os resultados são armazenados em arquivos de texto que são facilmente inspecionados, pesquisados ou usados como entradas para outros processamentos forenses. bulk_extractor também cria histogramas de certos tipos de recursos que encontra, como termos de pesquisa do Google e endereços de e-mail, pois pesquisas anteriores mostraram que esses histogramas são especialmente úteis em aplicativos de investigação e aplicação da lei.
- https://www.youtube.com/watch?v=5MTzP7THNKQ

Building a Dark Web Scraper

- A coleta de dados web, ou raspagem web, é uma forma de mineração que permite a extração de dados de sites da web convertendo-os em informação estruturada para posterior análise. O tipo mais básico de coleta é o download manual das páginas, copiando e colando o conteúdo, e isso pode ser feito por qualquer pessoa.
- Web harvesting, or web scraping, is a form of mining that allows for the conversion of data from structured web site data into further analysis information. The most basic type of collection is manual page downloading, copying and pasting content, and this can be done by anyone.

- https://justhackerthings.com/post/building-a-dark-web-scraper/
- https://insec.in/2020/07/06/dark-web-how-to-scrape-part-1/
- https://www.cybersixgill.com/blog/dark-web-scraping/
- https://www.youtube.com/watch?v=BCzx5tj2PIo
- https://www.youtube.com/watch?v=Wtzino26yyk

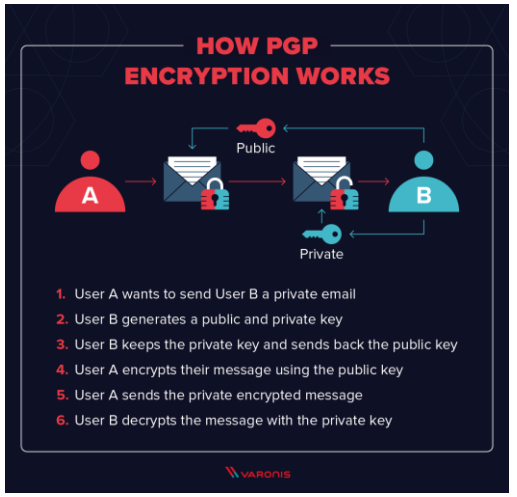


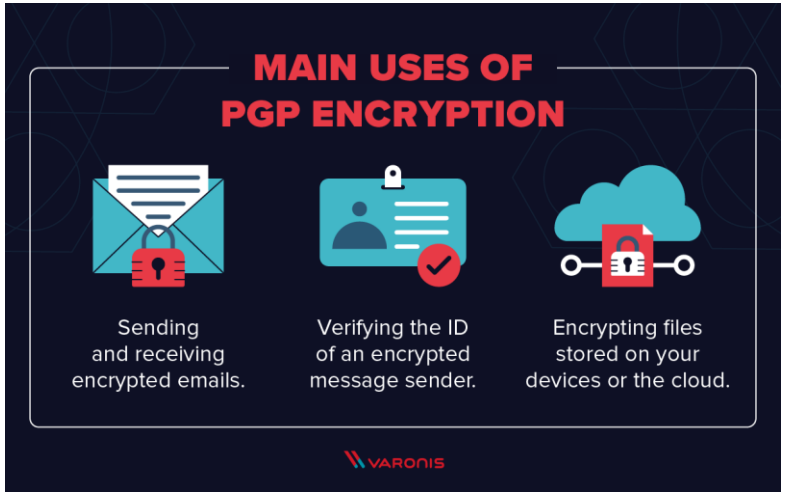
DarkScrape Tool

- https://github.com/itsmehacker/DarkScrape
- https://www.geeksforgeeks.org/darkscrape-osint-tool-for-scraping-dark-websites/
- Download Media
- Scrape From Single Url
- Face Recognition
- Scraping From Files
  - Txt
  - Csv
  - Excel

PGP Encryption

- PGP encryption is a data encryption methodology used for encrypting, decrypting, and authenticating digital files and online communication. It uses a combination of encryption methodologies such as hashing, data compression, symmetric private-key cryptography, and asymmetric public-key cryptography to keep data secure.
- A criptografia PGP é uma metodologia de criptografia de dados usada para criptografar, descriptografar e autenticar arquivos digitais e comunicação online . Ele usa uma combinação de metodologias de criptografia, como hash, compactação de dados, criptografia de chave privada simétrica e criptografia de chave pública assimétrica para manter os dados seguros.
- https://www.reddit.com/r/OSINT/comments/lfvzl8/extracting_information_from_public_pgp_keys/
- https://nixintel.info/osint-tools/using-pgp-keys-for-osint/
- https://www.sans.org/white-papers/1092/
- https://www.blackhat.com/presentations/bh-europe-05/bh-eu-05-callas-up.pdf

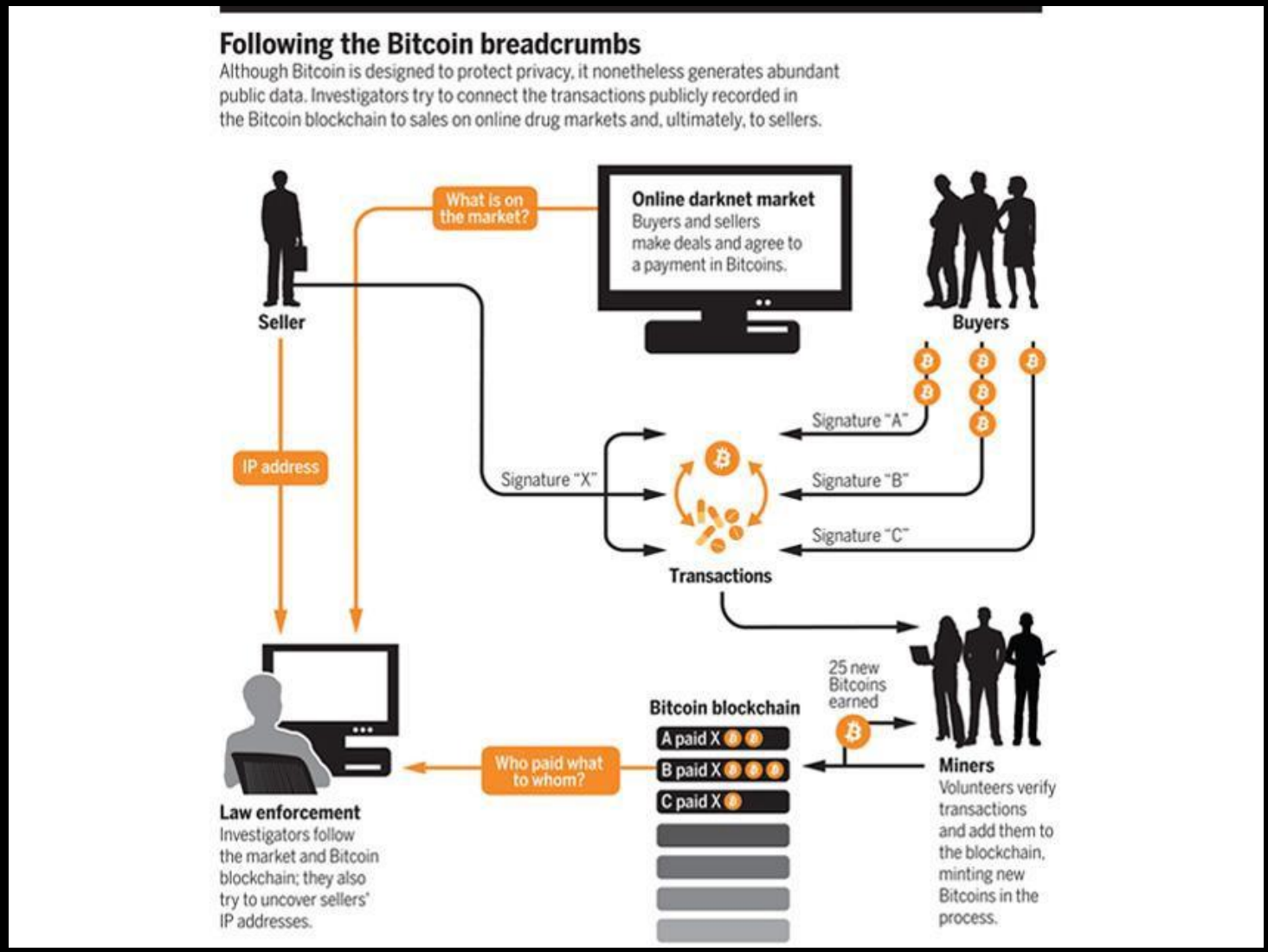




Cryptocurrency Investigation

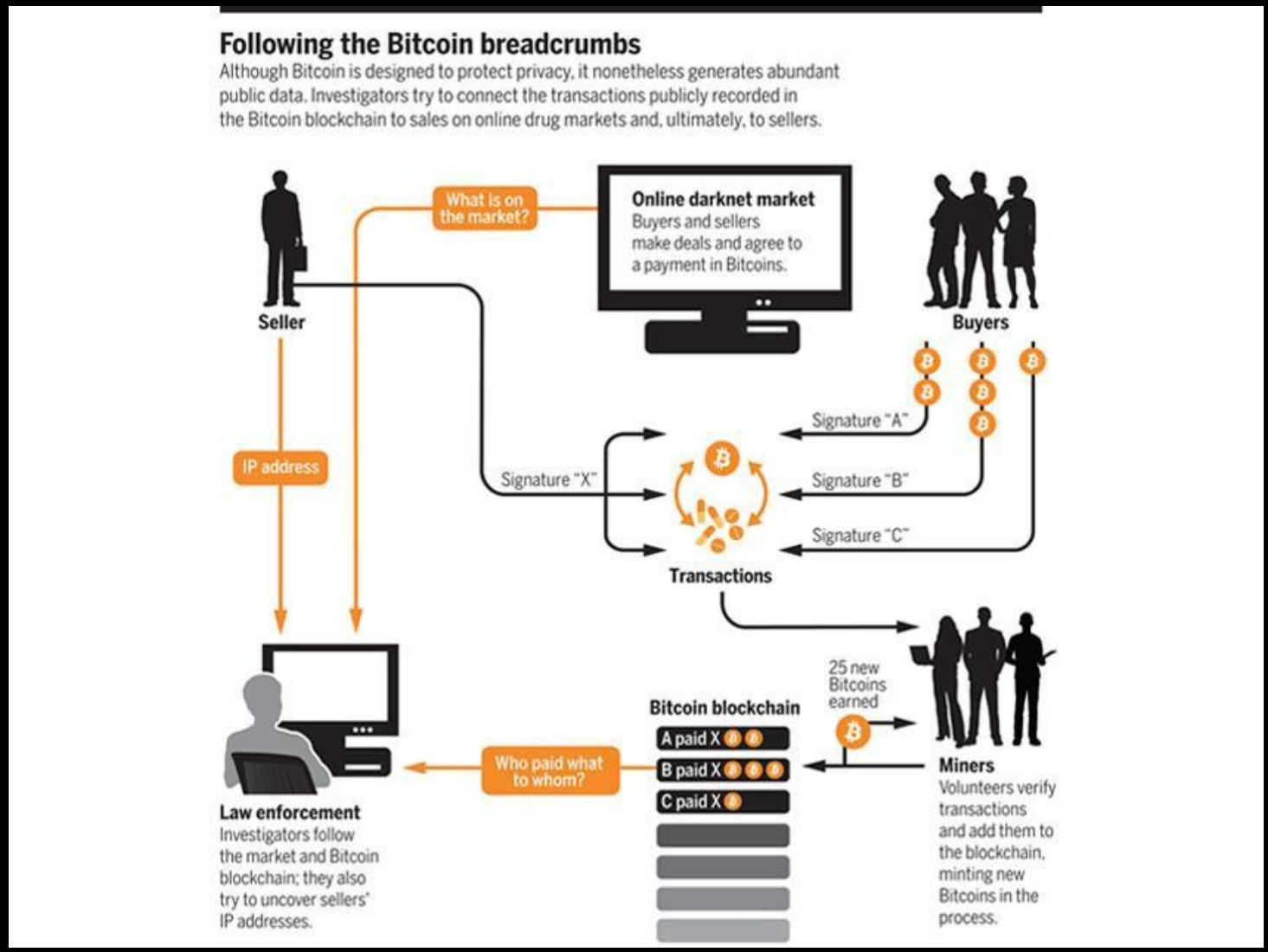
Bitcoin Transactions

- The most basic framework of any financial investigation consists of identifying a target, searching for information related to them, identifying the target's associates, and then searching for information on them. Cryptocurrencies fit perfectly to this investigation. Cryptocurrencies have become the favored means of exchange for cybercriminals and those avoiding restrictions of traditional banking, due to being increasingly dependent on cryptographic protection and a decentralized P2P system, money ownership is tacitly pseudonymous, while its flow is publicly accessible and perceptible.



Bitcoin Transactions

- A estrutura mais básica de qualquer investigação financeira consiste em identificar um alvo, buscar informações relacionadas a ele, identificar os associados do alvo e, em seguida, buscar informações sobre eles. As criptomoedas se encaixam perfeitamente nessa investigação. As criptomoedas tornaram-se o meio de troca preferido dos cibercriminosos e daqueles que evitam as restrições do sistema bancário tradicional, por serem cada vez mais dependentes da proteção criptográfica e de um sistema P2P descentralizado, a propriedade do dinheiro é tacitamente pseudônima, enquanto seu fluxo é publicamente acessível e perceptível.



Analyzing Wallet Addresses using Blockchain Explorers

- In cryptocurrency investigations, blockchain ledgers play a significant role. To render it simpler to comprehend and make sense of the information, investigators use Wallet explorers to conduct analysis on wallet addresses and transactions.
- Transaction analysis is crucial in cryptocurrency investigations since it not merely permits investigators to follow the money, but also determine the source and what sort of tools the suspect employed
- One of the more known Explorers is Blockchain.com. It allows us to look up the wallet address and see all of its past transactions. It also shows how much currency it currently holds. Blockchain transactions are simple to track in the case of public ledgers like Bitcoin or Ethereum.
- *WalletExplorer*
- *BitcoinWho'sWho*
- *BitcoinAbuse*
- *IntelX*

Wallet explorers usually update in real-time with the details of each transaction, comprising of:

- Hash: The transaction ID which serves as a way to look up a particular transaction on the blockchain. (Not to be confused with Cryptographic Hashes)
- From/To: The sender's address and the recipient's address.
- Time Stamp: Each block includes the precise time for when the transaction entered the blockchain. Thus, the time the block was mined.
- Actual Cost/Fee: The price of the transaction.
- Transaction Receipt Status: Confirmation of the transaction's status.
- Value: How much cryptocurrency was sent and the equivalent USD value.

Analyzing Wallet Addresses using Blockchain Explorers

- Nas investigações de criptomoedas, os livros de blockchain desempenham um papel significativo. Para simplificar a compreensão e a compreensão das informações, os investigadores usam os exploradores de carteiras para realizar análises em endereços e transações de carteiras.
- A análise de transações é crucial nas investigações de criptomoedas, pois não apenas permite que os investigadores acompanhem o dinheiro, mas também determinem a fonte e que tipo de ferramentas o suspeito empregou.
- Um dos exploradores mais conhecidos é o Blockchain.com. Ele nos permite procurar o endereço da carteira e ver todas as suas transações anteriores. Ele também mostra quanta moeda possui atualmente. As transações Blockchain são simples de rastrear no caso de livros públicos como Bitcoin ou Ethereum.
- *WalletExplorer*
- *BitcoinWho'sWho*
- *BitcoinAbuse*
- *IntelX*

Os exploradores de carteiras geralmente atualizam em tempo real os detalhes de cada transação, incluindo:

- Hash: O ID da transação que serve como uma maneira de pesquisar uma transação específica no blockchain. (Não confundir com Hashes Criptográficos)
- De/Para: O endereço do remetente e o endereço do destinatário.
- Time Stamp: Cada bloco inclui a hora exata de quando a transação entrou no blockchain. Assim, o tempo em que o bloco foi minerado.
- Custo/Taxa Real: O preço da transação.
- Status de Recebimento da Transação: Confirmação do status da transação.
- Valor: Quanta criptomoeda foi enviada e o valor equivalente em USD.

Identifying Risky Bitcoin Transactions with Maltego and CipherTrace Blockchain Intelligence

- Maltego has been instrumental in supporting various types of fraud investigations through a wide range of data integrations into our Transform Hub. With Maltego, fraud investigators can deepen and further contextualize their analysis with specific data sources by combining millions of attribution data points from OSINT or third-party intelligence providers.
- As part of our Transform Hub, CipherTrace Transforms provide investigators, analysts and researchers with access to a wealth of cryptocurrency intelligence from the different digital tokens, including Bitcoin, Ethereum, Bitcoin Cash and Litecoin. Leveraging open and closed source blockchain attribution and machine learning algorithms, CipherTrace Blockchain Intelligence assists law enforcement investigators and financial fraud specialists to de-anonymize transactions and obtain solid evidence on individuals involved in money laundering, financial terrorism, drug dealing, extortion and other crimes.

- https://www.maltego.com/blog/bitcoin-forensics-with-maltego-and-ciphertrace-blockchain-intelligence/

Identifying Risky Bitcoin Transactions with Maltego and CipherTrace Blockchain Intelligence

- A Maltego tem sido fundamental no apoio a vários tipos de investigações de fraude por meio de uma ampla gama de integrações de dados em nosso Transform Hub . Com a Maltego , os investigadores de fraude podem aprofundar e contextualizar ainda mais suas análises com fontes de dados específicas, combinando milhões de pontos de dados de atribuição da OSINT ou de provedores de inteligência terceirizados.
- Como parte do nosso Transform Hub, o CipherTrace Transforms fornece aos investigadores, analistas e pesquisadores acesso a uma riqueza de inteligência de criptomoedas de diferentes tokens digitais, incluindo Bitcoin, Ethereum, Bitcoin Cash e Litecoin. Aproveitando a atribuição de blockchain de código aberto e fechado e algoritmos de aprendizado de máquina, o CipherTrace Blockchain Intelligence auxilia investigadores policiais e especialistas em fraudes financeiras a anonimizar transações e obter evidências sólidas sobre indivíduos envolvidos em lavagem de dinheiro, terrorismo financeiro, tráfico de drogas, extorsão e outros crimes.

- https://www.maltego.com/blog/bitcoin-forensics-with-maltego-and-ciphertrace-blockchain-intelligence/

CTF (Capture the Flag)

How would the challenge work?

- Será criado um falso site .onion simulando um Black Market;
- Vamos utilizar técnicas de OSINT para coletar informações desse Black Market;
- Nele vai conter um painel de login, usuários cadastrados e brechas de seguranças para serem exploradas;
- Vamos se aproveitar das vulnerabilidades existentes para injetar códigos malicioso;
- Realizar data mining no site;
- E criar e configurar nosso honeypot;

How would the challenge work?

- A fake .onion site will be created simulating a Black Market;
- We will use OSINT techniques to collect information from this Black Market;
- It will contain a login panel, registered users and security holes to be explored;
- We will take advantage of existing vulnerabilities to inject malicious code;
- Perform data mining on the website;
- And create and configure our honeypot;

Content source

Fonts

- https://portswigger.net/daily-swig/osint-what-is-open-source-intelligence-and-how-is-it-used
- https://dps.iowa.gov/divisions/intelligence/intel-cycle
- https://www.researchgate.net/publication/277742692_National_Intelligence_Focus_on_Latin_America_Is_It_Adequate#pf7
- https://zety.com/blog/critical-thinking-skills
- https://www.investopedia.com/terms/t/tor.asp
- https://freenetproject.org/pages/about.html
- https://medium.datadriveninvestor.com/open-source-intelligence-osint-101-d96f47ff2ff1
- https://www.echosec.net/blog/osint-strategy
- https://cassiusxiii.medium.com/how-to-get-started-in-osint-e99d21833650
- https://www.researchgate.net/figure/Areas-for-further-investigation_fig4_265876925
- https://www.flickr.com/photos/tsbcanada/26304697670
- https://www.intelligenthq.com/revolutionising-cybersecurity-with-digital-forensics-part-1/

Fonts

- https://osint.link/
- https://static.googleusercontent.com/media/www.google.com/pt-BR//pdf/GoogleSearchGuide-back.pdf
- https://ahrefs.com/blog/google-advanced-search-operators/
- https://help.bing.microsoft.com/#apex/18/en-us/10002/0
- https://titanwolf.org/Network/Articles/Article?AID=af8ee16d-0d5e-4453-9dce-2b67ba477532
- https://www.osintcombine.com/post/dark-web-searching
- https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CyberDrill-2020/How%20to%20conduct%20effective%20OSINT%20investigation%20online.pdf
- https://osintbrasil.blogspot.com/2017/03/uma-lista-curada-de-ferramentas-e-de_21.html

Fonts

- https://www.pentesteracademy.com/course?id=29
- https://www.mcafeeinstitute.com/products/certified-osint
- https://www.osintcombine.com/cyber-investigator-course-1
- https://medium.com/ax1al/using-osint-to-investigate-cryptocurrency-transactions-7229f64c671a
- https://www.hackers-arise.com/post/open-source-intelligence-osint-osint-tools-for-bitcoin-investigations
- https://www.youtube.com/watch?v=C8um3JcCQuQ
- https://www.youtube.com/watch?v=eLL6BPKvwlg