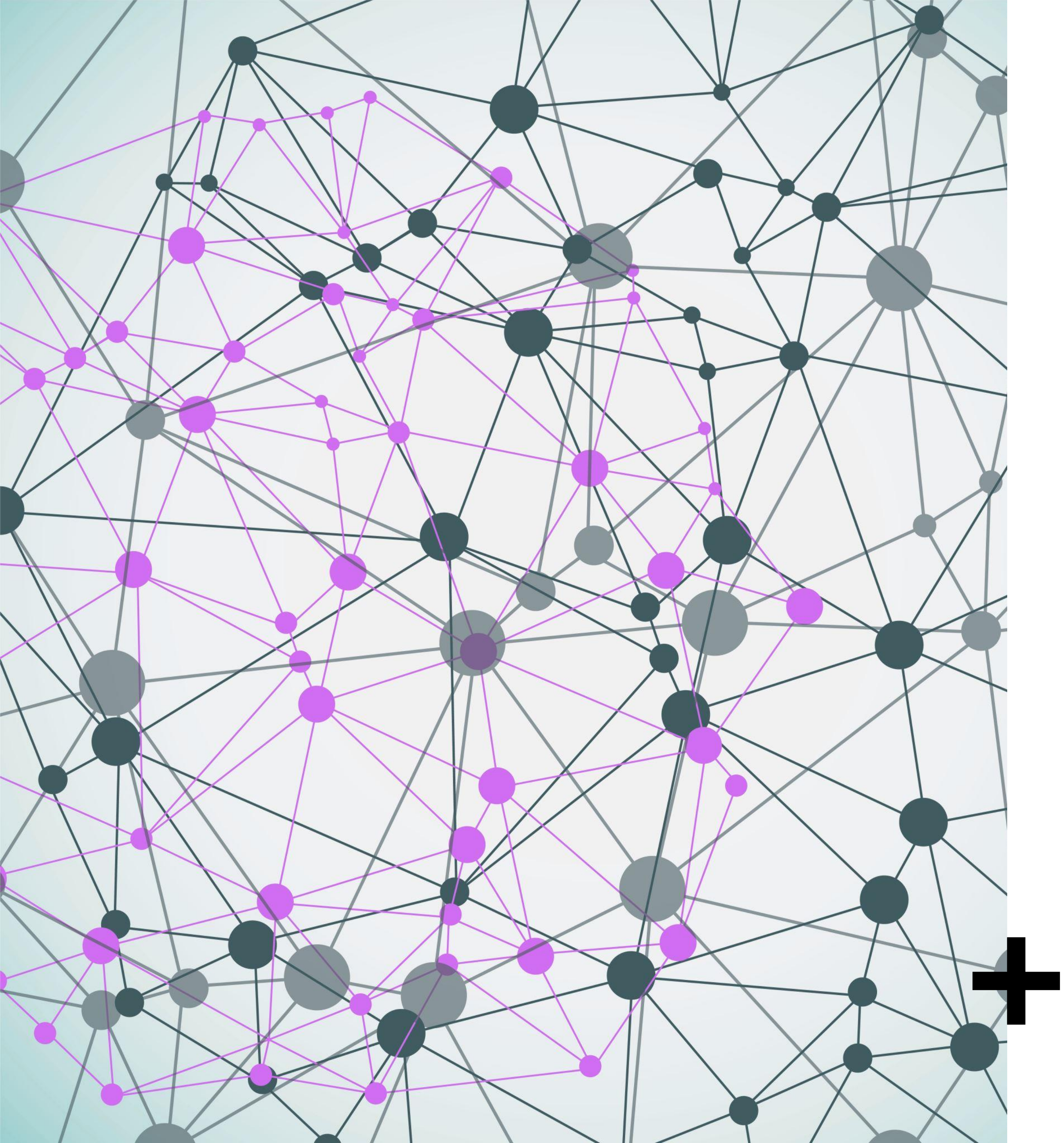


Threat Hunting Introduction PT.1

Joas Antonio

https://www.linkedin.com/in/joas-antonio-dos-santos

Build Lab Threat Hunting

- https://activecm.github.io/threat-hunting-labs/
- https://www.youtube.com/watch?v=_-Bgz9ejLUs
- https://www.youtube.com/watch?v=J8KAIpDXQvk
- https://blueteamlabs.online/

What is Threat Hunting?

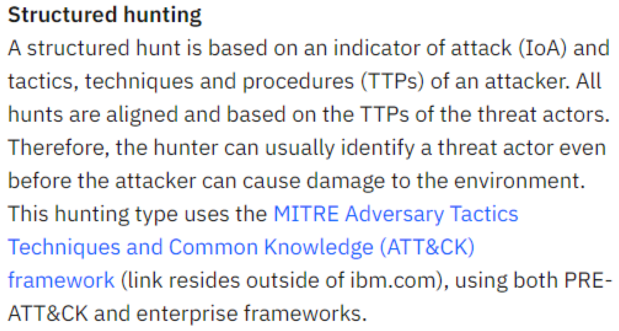
- A successful threat hunting program is based on an environment's data fertility. In other words, an organization must first have an enterprise security system in place, collecting data. The information gathered from it provides valuable clues for threat hunters.
- Cyber threat hunters bring a human element to enterprise security, complementing automated systems. They are skilled IT security professionals who search, log, monitor and neutralize threats before they can cause serious problems. Ideally, they're security analysts from within a company's IT department who knows its operations well, but sometimes they're an outside analyst.
- The art of threat hunting finds the environment's unknowns. It goes beyond traditional detection technologies, such as security information and event management (SIEM), endpoint detection and response (EDR) and others. Threat hunters comb through security data. They search for hidden malware or attackers and look for patterns of suspicious activity that a computer might have missed or judged to be resolved but isn't. They also help patch an enterprise's security system to prevent that type of cyberattack from recurring.
- https://www.ibm.com/topics/threat-hunting

What is Threat Hunting?

- Um programa de caça a ameaças bem-sucedido é baseado na fertilidade de dados de um ambiente. Em outras palavras, uma organização deve primeiro ter um sistema de segurança empresarial instalado, coletando dados. As informações coletadas fornecem pistas valiosas para caçadores de ameaças.
- Os caçadores de ameaças cibernéticas trazem um elemento humano para a segurança corporativa, complementando os sistemas automatizados. Eles são profissionais de segurança de TI qualificados que pesquisam, registram, monitoram e neutralizam ameaças antes que possam causar problemas sérios. Idealmente, eles são analistas de segurança do departamento de TI de uma empresa que conhecem bem suas operações, mas às vezes são analistas externos.
- A arte de caçar ameaças encontra as incógnitas do ambiente. Ele vai além das tecnologias tradicionais de detecção, como gerenciamento de informações e eventos de segurança (SIEM) , detecção e resposta de endpoint (EDR) e outros. Os caçadores de ameaças vasculham os dados de segurança. Eles procuram malwares ou invasores ocultos e procuram padrões de atividades suspeitas que um computador pode ter perdido ou considerado resolvido, mas não foi. Eles também ajudam a corrigir o sistema de segurança de uma empresa para evitar que esse tipo de ataque cibernético se repita.
- https://www.ibm.com/topics/threat-hunting

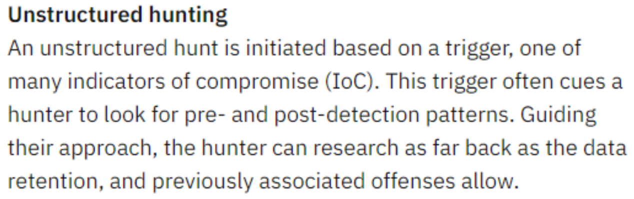
Types of threat hunting

– Hunters begin with a hypothesis based on security data or a trigger. The hypothesis or trigger serve as springboards for a more in-depth investigation into potential risks. And these deeper investigations are structured, unstructured and situational hunting.



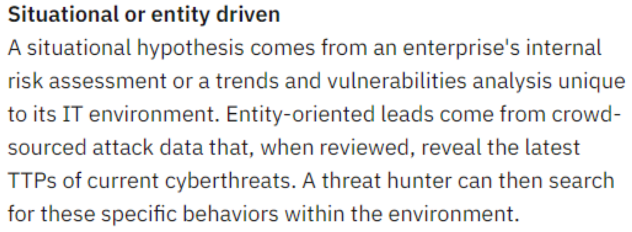
Structured hunting

A structured hunt is based on an indicator of attack (IoA) and tactics, techniques and procedures (TTPs) of an attacker. All hunts are aligned and based on the TTPs of the threat actors. Therefore, the hunter can usually identify a threat actor even before the attacker can cause damage to the environment. This hunting type uses the MITRE Adversary Tactics Techniques and Common Knowledge (ATT&CK) framework (link resides outside of ibm.com), using both PRE-ATT&CK and enterprise frameworks.



Unstructured hunting

An unstructured hunt is initiated based on a trigger, one of many indicators of compromise (IoC). This trigger often cues a hunter to look for pre- and post-detection patterns. Guiding their approach, the hunter can research as far back as the data retention, and previously associated offenses allow.



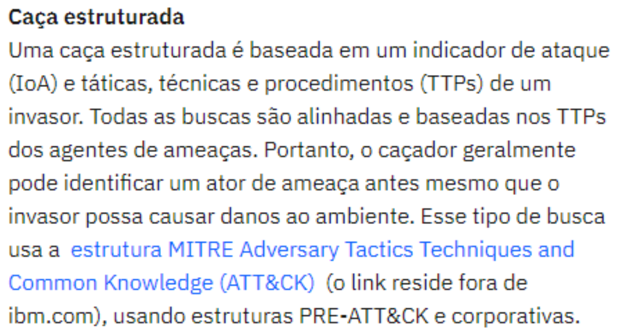
Situational or entity driven

A situational hypothesis comes from an enterprise's internal risk assessment or a trends and vulnerabilities analysis unique to its IT environment. Entity-oriented leads come from crowd-sourced attack data that, when reviewed, reveal the latest TTPs of current cyberthreats. A threat hunter can then search for these specific behaviors within the environment.

Types of threat hunting

- Os caçadores começam com uma hipótese baseada em dados de segurança ou em um gatilho. A hipótese ou gatilho serve como trampolim para uma investigação mais aprofundada dos riscos potenciais. E essas investigações mais profundas são uma caça estruturada, não estruturada e situacional.

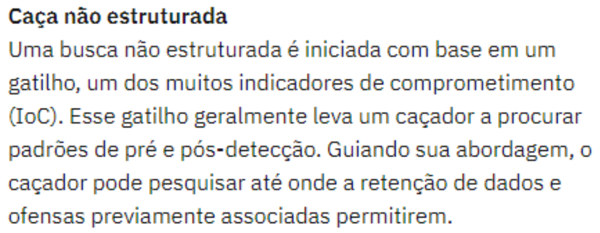
□



Caça estruturada

Uma caça estruturada é baseada em um indicador de ataque (IoA) e táticas, técnicas e procedimentos (TTPs) de um invasor. Todas as buscas são alinhadas e baseadas nos TTPs dos agentes de ameaças. Portanto, o caçador geralmente pode identificar um ator de ameaça antes mesmo que o invasor possa causar danos ao ambiente. Esse tipo de busca usa a estrutura MITRE Adversary Tactics Techniques and Common Knowledge (ATT&CK) (o link reside fora de ibm.com), usando estruturas PRE-ATT&CK e corporativas.

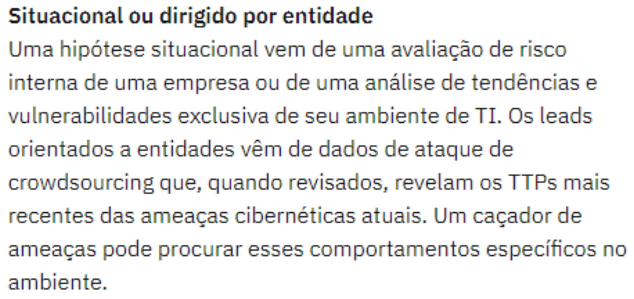
□



Caça não estruturada

Uma busca não estruturada é iniciada com base em um gatilho, um dos muitos indicadores de comprometimento (IoC). Esse gatilho geralmente leva um caçador a procurar padrões de pré e pós-detecção. Guiando sua abordagem, o caçador pode pesquisar até onde a retenção de dados e ofensas previamente associadas permitirem.

□



Situacional ou dirigido por entidade

Uma hipótese situacional vem de uma avaliação de risco interna de uma empresa ou de uma análise de tendências e vulnerabilidades exclusiva de seu ambiente de TI. Os leads orientados a entidades vêm de dados de ataque de crowdsourcing que, quando revisados, revelam os TTPs mais recentes das ameaças cibernéticas atuais. Um caçador de ameaças pode procurar esses comportamentos específicos no ambiente.

Intel-based hunting

- Intel-based hunts can use IoCs, hash values, IP addresses, domain names, networks, or host artifacts provided by intelligence sharing platforms such as computer emergency response teams (CERT). An automated alert can be exported from these platforms and input into the SIEM as structured threat information expression (STIX) (link resides outside of ibm.com) and trusted automated exchange of intelligence information (TAXII) (link resides outside of ibm.com). Once the SIEM has the alert based on an IoC, the threat hunter can investigate the malicious activity before and after the alert to identify any compromise in the environment.

Intel-based hunting

- As buscas baseadas em Intel podem usar IoCs, valores de hash, endereços IP, nomes de domínio, redes ou artefatos de host fornecidos por plataformas de compartilhamento de inteligência, como equipes de resposta a emergências de computador (CERT). Um alerta automatizado pode ser exportado dessas plataformas e inserido no SIEM como expressão de informações de ameaças estruturadas (STIX) (o link reside fora de ibm.com) e troca automatizada confiável de informações de inteligência (TAXII) (o link reside fora de ibm.com) . Uma vez que o SIEM tenha o alerta baseado em um IoC, o caçador de ameaças pode investigar a atividade maliciosa antes e depois do alerta para identificar qualquer comprometimento no ambiente.

Hypothesis hunting

- Hypothesis hunting is a proactive hunting model that uses a threat hunting library. It's aligned with the MITRE ATT&CK framework and uses global detection playbooks to identify advanced persistent threat groups and malware attacks.
- Hypothesis-based hunts use the IoAs and TTPs of attackers. The hunter identifies the threat actors based on the environment, domain and attack behaviors employed to create a hypothesis aligned with the MITRE framework. Once a behavior is identified, the threat hunter monitors activity patterns to detect, identify and isolate the threat. This way, the hunter can proactively detect threat actors before they can do damage to an environment.

Hypothesis hunting

- A caça de hipóteses é um modelo de caça proativa que usa uma biblioteca de caça a ameaças. Ele está alinhado com a estrutura MITRE ATT&CK e usa manuais de detecção global para identificar grupos avançados de ameaças persistentes e ataques de malware.
- As caçadas baseadas em hipóteses usam os IoAs e os TTPs dos invasores. O caçador identifica os atores de ameaças com base no ambiente, domínio e comportamentos de ataque empregados para criar uma hipótese alinhada com a estrutura MITRE. Depois que um comportamento é identificado, o caçador de ameaças monitora os padrões de atividade para detectar, identificar e isolar a ameaça. Dessa forma, o caçador pode detectar proativamente os agentes de ameaças antes que eles possam causar danos a um ambiente.

Custom hunting

- Custom hunting is based on situational awareness and industry-based hunting methodologies. It identifies anomalies in the SIEM and EDR tools and is customizable based on customer requirements.
- Custom or situational hunts are based on customers' requirements, or they're proactively executed based on situations, such as geopolitical issues and targeted attacks. These hunting activities can draw on both intel- and hypothesis-based hunting models using IoA and IoC information

Custom hunting

- A caça personalizada é baseada na consciência situacional e nas metodologias de caça baseadas no setor. Ele identifica anomalias nas ferramentas SIEM e EDR e é personalizável com base nos requisitos do cliente.
- As buscas personalizadas ou situacionais são baseadas nos requisitos dos clientes ou são executadas proativamente com base em situações, como problemas geopolíticos e ataques direcionados. Essas atividades de caça podem se basear em modelos de caça baseados em inteligência e hipóteses usando informações de IoA e IoC

How to become a threat hunter

- The barrier for entry to threat hunting is relatively low, according to Gangwer. Anyone with access to endpoint, network or security telemetry can threat hunt by using that data to test hypotheses or answer questions that interest them. "If you ever think, 'this looks odd,' and hours later find yourself still working on the same problem, you have a possible career as a threat hunter," he said.
- Collins suggested security professionals and others interested in threat hunting consider learning coding and scripting skills in a language such as Python, Go or Perl, thus gaining a level of technological autonomy.

How to become a threat hunter

- "Learn something that will enable you to create those queries and go beyond what the tool set in front of you offers," Collins said. "Some of the best hunters I've seen in action will just sit down and quickly script something custom to grab data on an ad hoc basis if it's not already available to them."
- Aspiring threat hunters would also do well to build cloud networking and cloud security expertise since many of today's organizations struggle with incident response and threat hunting in those environments. "That's a big opportunity," Collins said. "Cloud will be the predominant skill set in the future."

How to become a threat hunter

– In addition to pattern recognition, deductive reasoning, coding and cloud networking skills, experts said aspiring threat hunters would benefit from some understanding of the following:

- data forensics
- incident response
- network administration
- network traffic analysis
- systems administration

– Communication and collaboration skills are also important for anyone interested in how to become a threat hunter. Collins said the best threat hunters are independent thinkers but not lone rangers, working with other IT professionals to access operations data and identify hunting leads. Once hunters have discovered a threat or vulnerability, they must also communicate efficiently and effectively with the rest of the security team and other organizational stakeholders to mitigate the problem.

How to become a threat hunter

- A barreira de entrada para a caça a ameaças é relativamente baixa, de acordo com Gangwer. Qualquer pessoa com acesso ao endpoint, rede ou telemetria de segurança pode caçar ameaças usando esses dados para testar hipóteses ou responder a perguntas que lhes interessam. "Se você pensa 'isso parece estranho' e horas depois ainda está trabalhando no mesmo problema, você tem uma possível carreira como caçador de ameaças", disse ele.
- Collins sugeriu que profissionais de segurança e outros interessados em caçar ameaças considerem aprender habilidades de codificação e script em uma linguagem como Python, Go ou Perl, ganhando assim um nível de autonomia tecnológica.

How to become a threat hunter

- "Aprenda algo que permitirá que você crie essas consultas e vá além do que a ferramenta definida à sua frente oferece", disse Collins. "Alguns dos melhores caçadores que já vi em ação simplesmente sentam e escrevem rapidamente um script personalizado para coletar dados ad hoc, se ainda não estiverem disponíveis para eles."
- Aspirantes a caçadores de ameaças também fariam bem em construir rede em nuvem e experiência em segurança em nuvem, já que muitas das organizações de hoje lutam com resposta a incidentes e caça a ameaças nesses ambientes . "Essa é uma grande oportunidade", disse Collins. "A nuvem será o conjunto de habilidades predominante no futuro."

How to become a threat hunter

– Além do reconhecimento de padrões, raciocínio dedutivo, codificação e habilidades de rede em nuvem, especialistas disseram que aspirantes a caçadores de ameaças se beneficiariam de alguma compreensão do seguinte:

- forense de dados
- resposta a incidentes
- Administração de rede
- análise de tráfego de rede
- administração de sistemas

How to become a threat hunter

- As habilidades de comunicação e colaboração também são importantes para qualquer pessoa interessada em como se tornar um caçador de ameaças. Collins disse que os melhores caçadores de ameaças são pensadores independentes, mas não guardas-florestais solitários, trabalhando com outros profissionais de TI para acessar dados de operações e identificar pistas de caça. Depois que os caçadores descobrem uma ameaça ou vulnerabilidade, eles também devem se comunicar de maneira eficiente e eficaz com o restante da equipe de segurança e outras partes interessadas da organização para mitigar o problema.
- Do ponto de vista corporativo, os líderes de segurança cibernética que procuram atrair e reter os principais talentos de caça a ameaças devem oferecer oportunidades de crescimento profissional e acesso a telemetria cada vez mais rica, sugeriu Gangwer.
- https://www.techtarget.com/searchsecurity/feature/How-to-become-a-threat-hunter

Cyber Threat Hunting

How to use Threat Hunting in your Cyber Security Strategy

Incident Response & Prevention Mechanisms

Intelligence gathered during the hunt provides context around a cyber threat which could be malware or a large scale Advanced Persistent Threat (APT). This information allows Incident response teams to proactively perform targeted threat response, minimising the duration and impact of a breach. These findings can then be used to enrich analytics, allowing defenders to automate future prevention mechanisms.

Advanced Analysis & Visualisation

Advanced analytics and multidimensional visualisation should provide up-to-date actionable insight, so defenders can stay ahead of the evolving cyber threats in the network. SecOps and NetOps teams need rapid alerting and query capabilities, facilitating both machine led analytics with human led analysis to mitigate threats.

New Patterns, Behaviours & Techniques

Uncovering indicators of compromise (IoCs) at a very basic level is a good starting point but is not enough for defenders who are tasked with uncovering a sophisticated adversaries techniques, tactics and procedures (TTP's). Understanding TTP's using models such as Lockheed Martin Cyber Kill Chain or the Mandiant Attack Lifecycle can be helpful to determine where in the attack tree an adversaries' activities occurred. This type of behavioural analysis allows defenders to maximise their anomaly threat detection abilities and streamline response action.

Access to Data

Collecting and consolidating data from numerous physical and logical network assets such as switches/routers, endpoint data such as process execution meta-data and security data e.g. alerts. This data gives defenders an accurate view of the network, and a starting point to pre-process, using techniques such as entity sets, grouping and stack counting (stacking).

Threat Hunting Tools

Employing the right threat hunting and anomaly detection tools for your network will depend on a number of variables but whatever your requirements those tools should fall in to three categories: Intelligence driven, which combines all gathered data and reporting for the hunt. Analytics driven, that uses behaviour analytics and machine learning to create risk scores etc. Situational awareness driven, that measures risk to the network by evaluating company and user trends.

Baseline 'Normal' Behaviour

During the process of threat hunting it is essential to develop a picture of what looks normal for your network, this will provide a snapshot of normal network behaviour, data and user activity. Analysis of current and historic baselines will indicate comparative changes over time. The SANS Institute found that focusing on data sets such as IP addresses, DNS activity file monitoring, user behaviour and analysis, and software baseline monitoring supports successful threat hunting.

telesoft

Incident Response

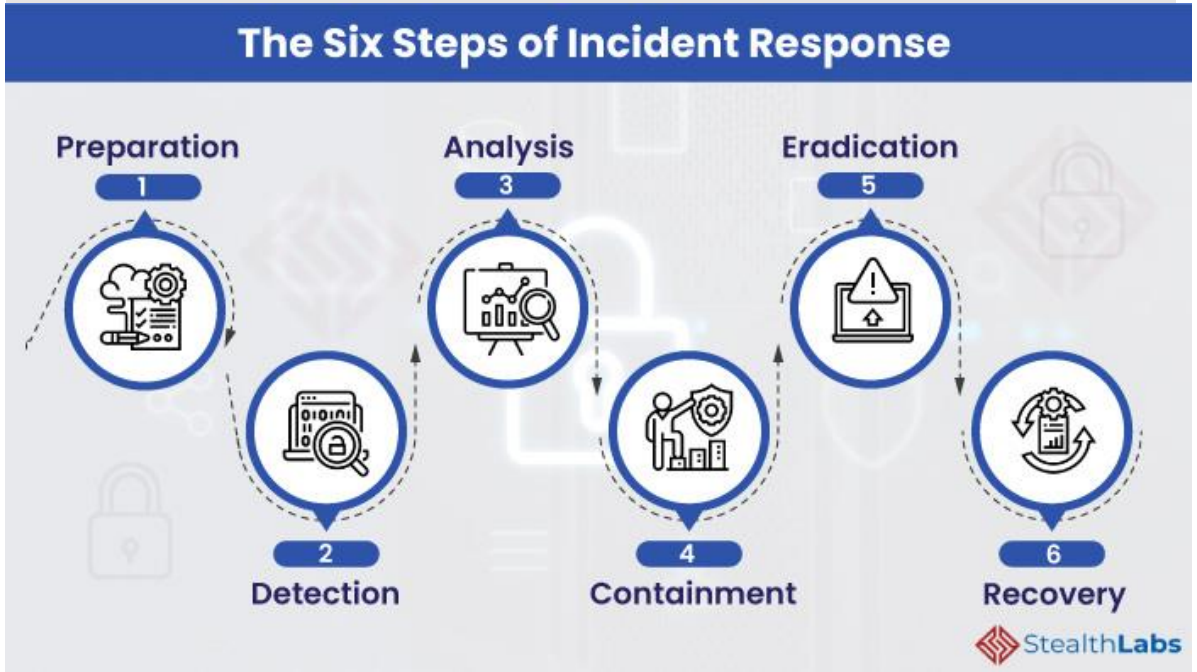
1) Preparation

Preparation is crucial to effective incident response. Even the best Cyber Security Incident Response Team (CSIRT) cannot effectively respond to an incident without predetermined instructions. Preparedness involves:

•Design, development, training, and implementation of enterprise-wide IR plan

•Creating communication guidelines to enable seamless communication during and after an incident

•Conducting cyber simulation exercises to evaluate the effectiveness of incident response plan



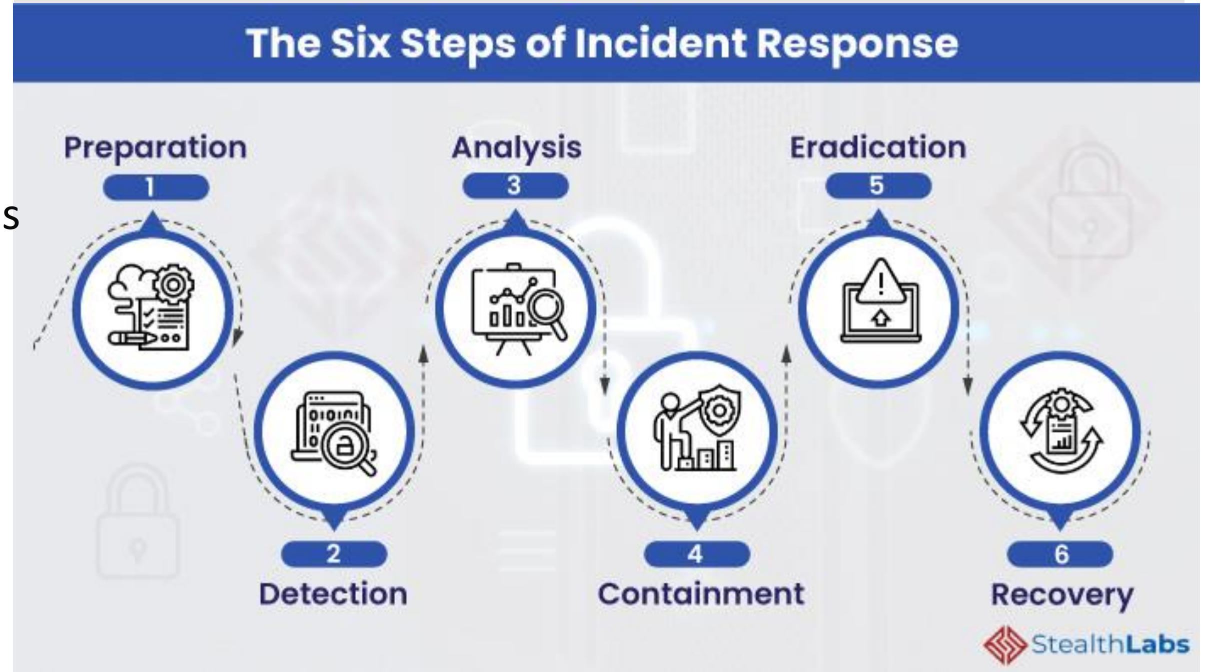
Incident Response

2) Detection

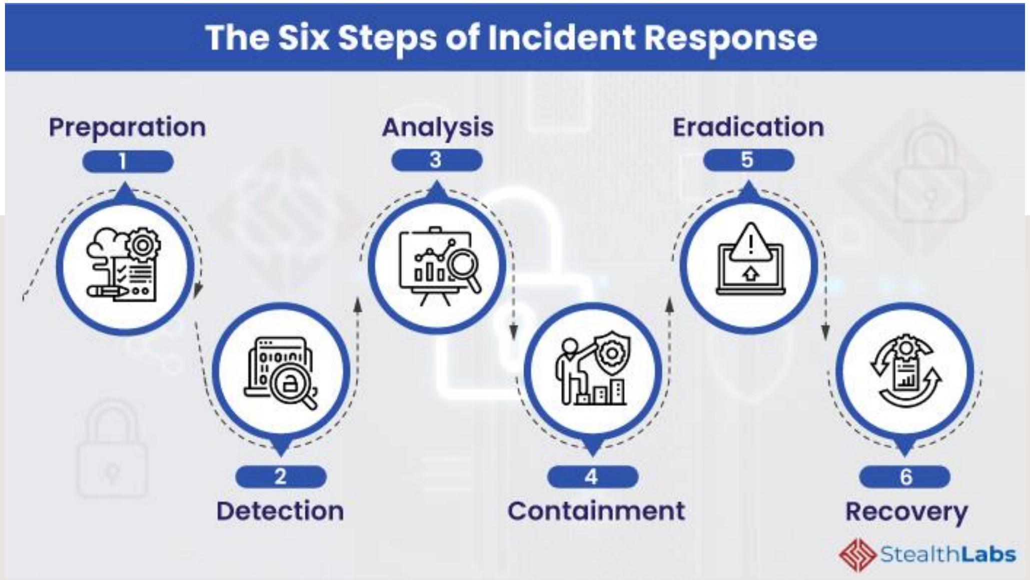
The objective of this phase is to monitor networks and systems to detect, alert, and report on potential security incidents.

•Adopt cyber threat intelligence (CTI) capabilities to develop a comprehensive cyber monitoring program and to support ongoing monitoring and detection

•Conduct cyber compromise assessments to detect unknown compromises



Incident Response



3) Analysis

The majority portion of the efforts to properly understand the security incident take place during this step.

It involves:

•Gathering information and then prioritizing individual incidents and steps for a response.

•Forensic preservation and analysis of data to determine the extent and impact of the incident.

During the event of an incident, the incident response team should focus on three areas:

•Endpoint Analysis

- Determine tracks left behind by the malicious actor.
- Analyze a bit-for-bit copy of systems to determine what occurred on a device during the incident.

•Binary Analysis

- Analyze malicious tools or binaries used by the malicious actor and document the functionalities of those programs. The analysis can be performed through Behaviour Analysis or Static Analysis.

•Enterprise Hunting

- Analyze existing systems and event logs to determine the scope of the incident.
- Document all the compromised systems, devices, and accounts.

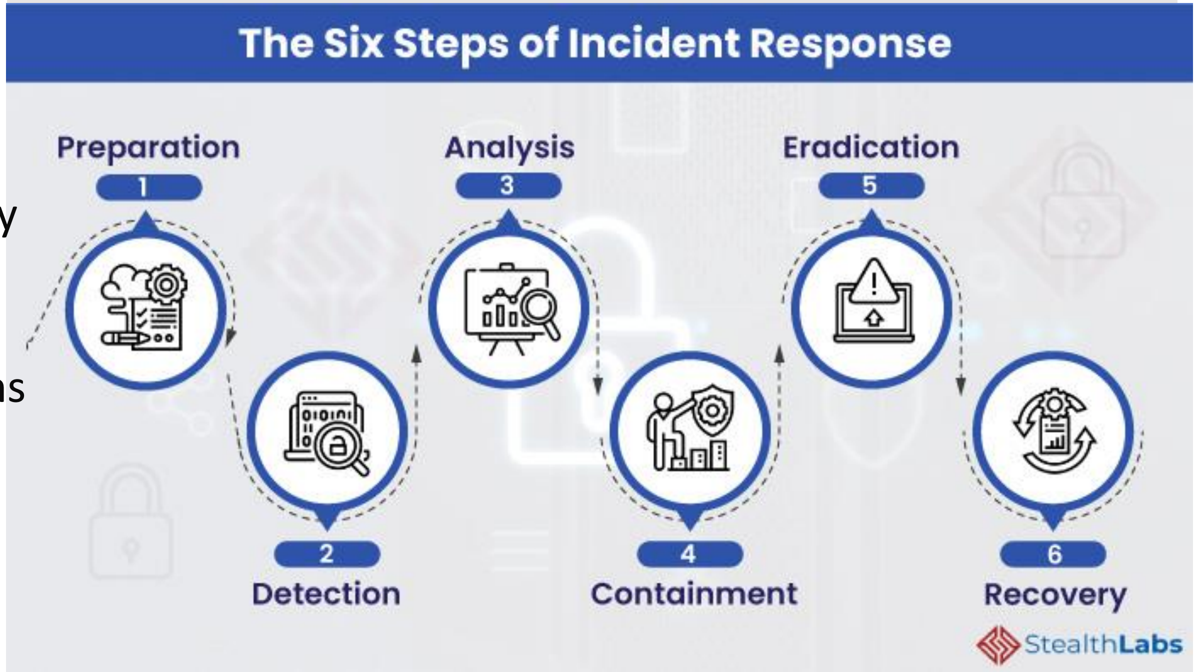
Incident Response

4) Containment

This is the most critical stage of incident response. The strategy for containing an incident is based on the intelligence and indicators of compromise gathered during the analysis phase. The security team should focus on taking risk-mitigating actions to prevent further impact and damage to the organization.

•**Coordinated Shutdown:** Once identifying the compromised systems, perform a coordinated shutdown of these devices. The IR team should be instructed to ensure proper timing.

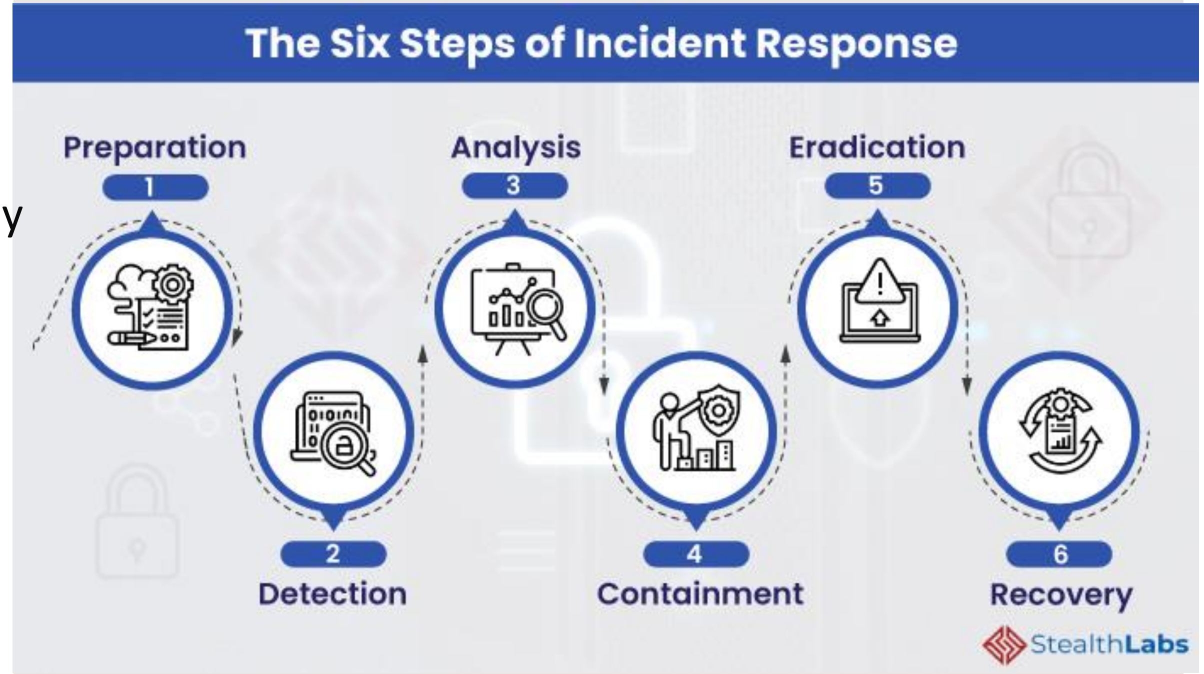
•**Wipe and Rebuild:** Wipe the compromised systems and rebuild the operating systems from scratch. Change the login credentials of all the compromised accounts.



Incident Response

5) Eradication

Once you have identified domains or IP addresses leveraged by the malicious actors for command and control, issue ‘threat mitigation requests’ to block the communication from all channels connected to these domains. The IR team should remove the known existing threats from the networks.

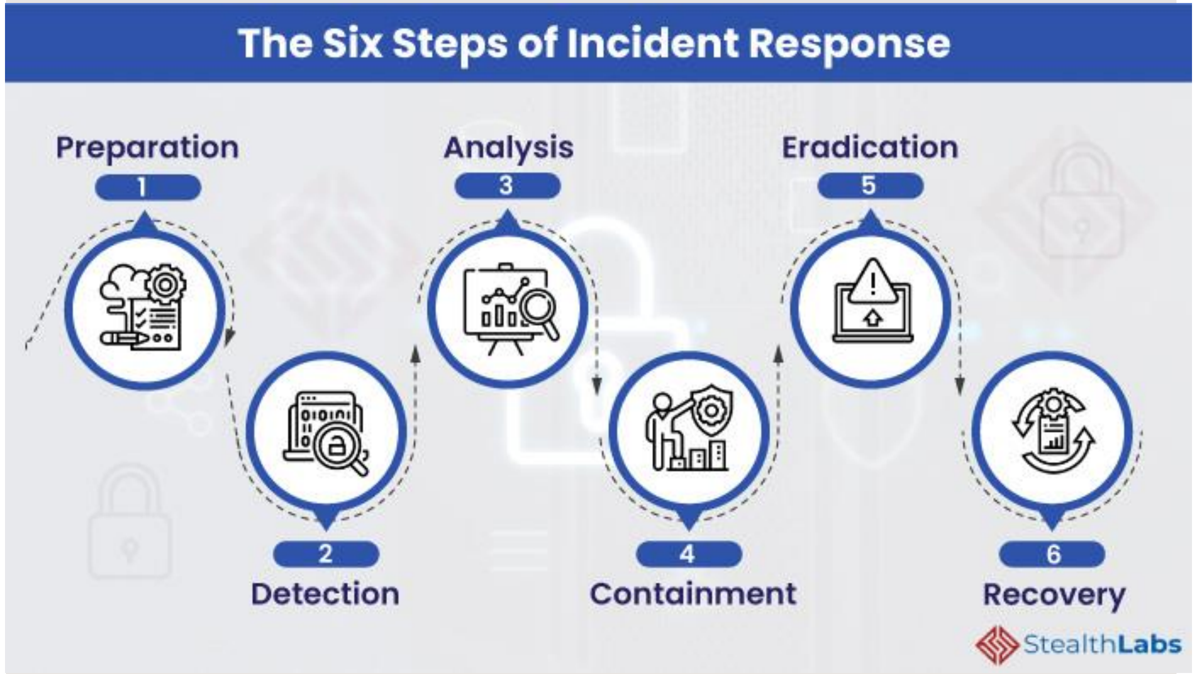


Incident Response

6) Recovery

- Develop a near-term remediation strategy and roadmap
- Focus on resuming normal business operations
- Develop a long-term risk mitigation strategy
- Document the incident to improve the IR plan and update security measures to avoid such incidents in future

- https://www.stealthlabs.com/blog/the-six-steps-to-build-an-effective-cyber-incident-response-plan/


The Six Steps of Incident Response

What are Indicators of Compromise?

- Indicators of compromise (IOCs) are “pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.” Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity. By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent breaches from occurring or limit damages by stopping attacks in earlier stages.

- Indicators of compromise act as breadcrumbs that lead infosec and IT pros to detect malicious activity early in the attack sequence. These unusual activities are the red flags that indicate a potential or in-progress attack that could lead to a data breach or systems compromise. But, IOCs are not always easy to detect; they can be as simple as metadata elements or incredibly complex malicious code and content samples. Analysts often identify various IOCs to look for correlation and piece them together to analyze a potential threat or incident.

What are Indicators of Compromise?

- Indicadores de comprometimento (IOCs) são “partes de dados forenses, como dados encontrados em entradas ou arquivos de log do sistema, que identificam atividades potencialmente maliciosas em um sistema ou rede”. Os indicadores de comprometimento ajudam os profissionais de segurança da informação e de TI a detectar violações de dados, infecções por malware ou outras atividades de ameaças. Ao monitorar os indicadores de comprometimento, as organizações podem detectar ataques e agir rapidamente para evitar a ocorrência de violações ou limitar os danos interrompendo os ataques em estágios anteriores.

- Os indicadores de comprometimento agem como migalhas que levam os profissionais de segurança e TI a detectar atividades maliciosas no início da sequência de ataque. Essas atividades incomuns são as bandeiras vermelhas que indicam um ataque potencial ou em andamento que pode levar a uma violação de dados ou comprometimento de sistemas. Mas os IOCs nem sempre são fáceis de detectar; eles podem ser tão simples quanto elementos de metadados ou códigos maliciosos incrivelmente complexos e amostras de conteúdo. Os analistas geralmente identificam vários IOCs para procurar correlação e juntá-los para analisar uma possível ameaça ou incidente.

What are Indicators of Attack?

- Indicators of attack are similar to IOCs, but rather than focusing on forensic analysis of a compromise that has already taken place, indicators of attack focus on identifying attacker activity while an attack is in process. Indicators of compromise help answer the question “What happened?” while indicators of attack can help answer questions like “What is happening and why?” A proactive approach to detection uses both IOAs and IOCs to discover security incidents or threats in as close to real time as possible.

What are Indicators of Attack?

- Os indicadores de ataque são semelhantes aos IOCs, mas em vez de se concentrar na análise forense de um comprometimento que já ocorreu, os indicadores de ataque se concentram na identificação da atividade do invasor enquanto um ataque está em andamento. Os indicadores de comprometimento ajudam a responder à pergunta "O que aconteceu?" enquanto indicadores de ataque podem ajudar a responder perguntas como "O que está acontecendo e por quê?" Uma abordagem proativa de detecção usa IOAs e IOCs para descobrir incidentes ou ameaças de segurança o mais próximo possível do tempo real.
- https://digitalguardian.com/blog/what-are-indicators-compromise

STIX and TAXII

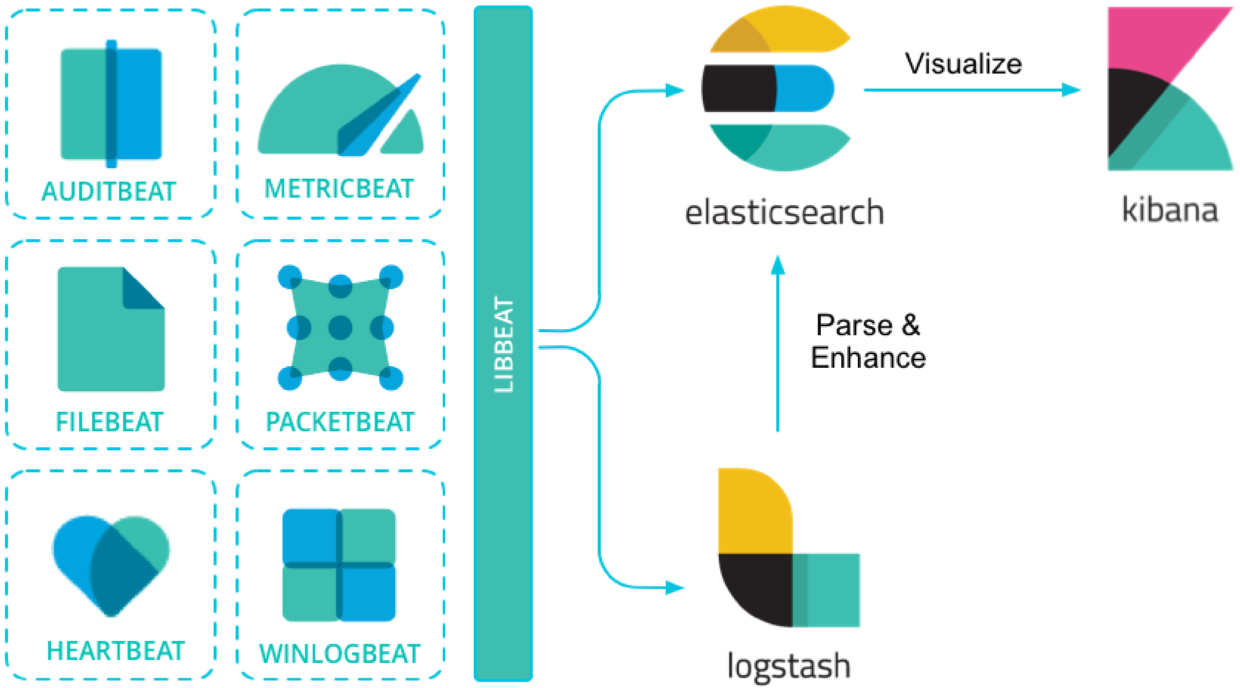
- https://www.anomali.com/pt/resources/what-are-stix-taxii
- https://www.anomali.com/resources/what-are-stix-taxii
- https://www.eclecticiq.com/stix-taxii
- https://www.first.org/resources/papers/munich2016/wunder-stix-taxii-Overview.pdf
- https://medium.com/sekoia-io-blog/stix-and-taxii-c1f596866384

Practical Concepts

What is ELK?

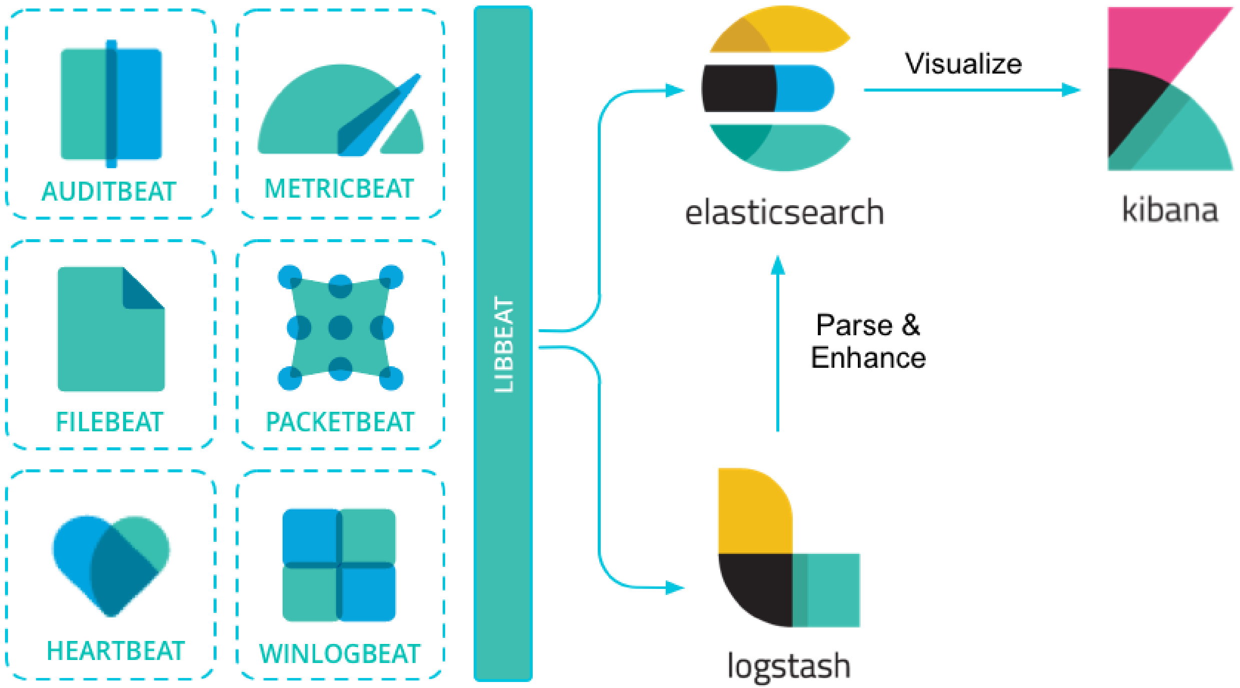
- ELK stands for the monitoring solution which is mainly consist of **Elasticsearch**, **Logstash** and **Kibana**;
- It has been renamed as **Elastic Stack**, since it has expanded its functions greatly through the use of **beats** and some other addons like APM servers. But people still tend to call it ELK;
- It is a distributed monitoring solution suiteable for almost any **structured** and **unstructured** data source, but not limited to log;
- It supports centralized **logging/metric/APM** monitoring;
- It is open source and can be extended easily.

–



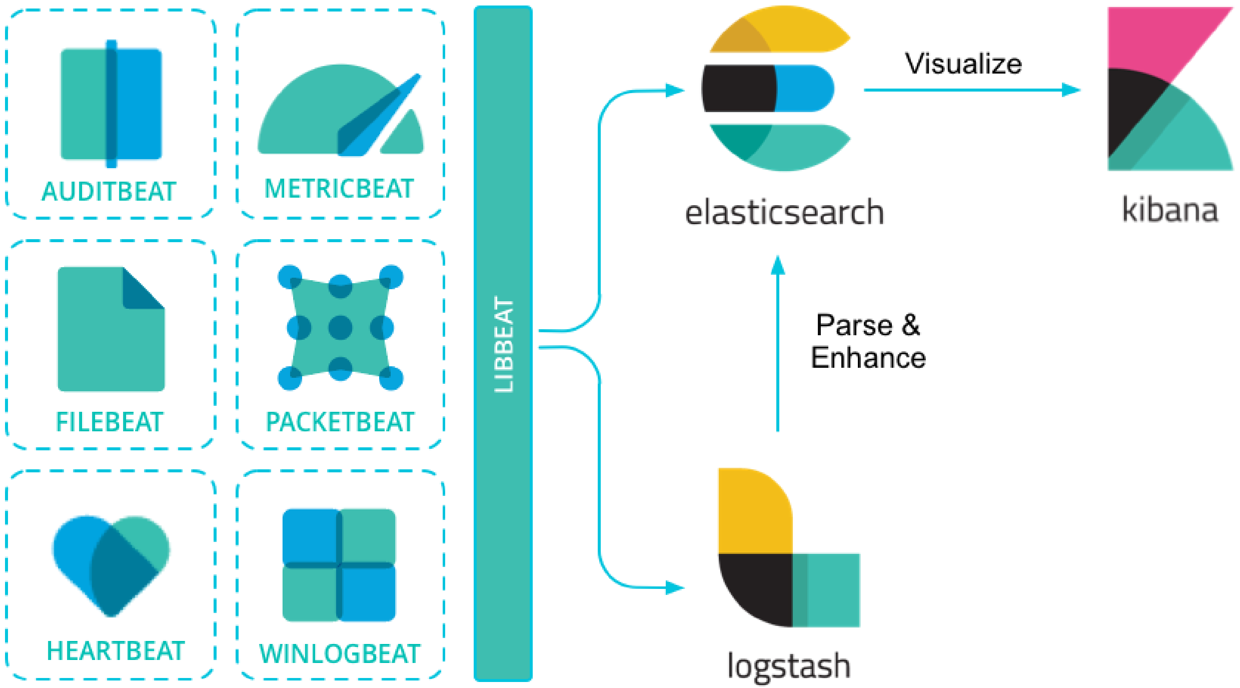
What is ELK?

- ELK significa a solução de monitoramento que consiste principalmente
em **Elasticsearch** , **Logstash** e **Kibana** ;
- Ele foi renomeado como **Elastic Stack** , pois expandiu bastante suas funções através do uso de **batidas** e alguns outros complementos como servidores APM. Mas as pessoas ainda tendem a chamá-lo de ELK;
- É uma solução de monitoramento distribuída adequada para quase qualquer fonte de dados **estruturada** e **não estruturada** , mas não limitada a log;
- Ele suporta monitoramento centralizado de **log/métrica/APM ;**
- É de código aberto e pode ser estendido facilmente.



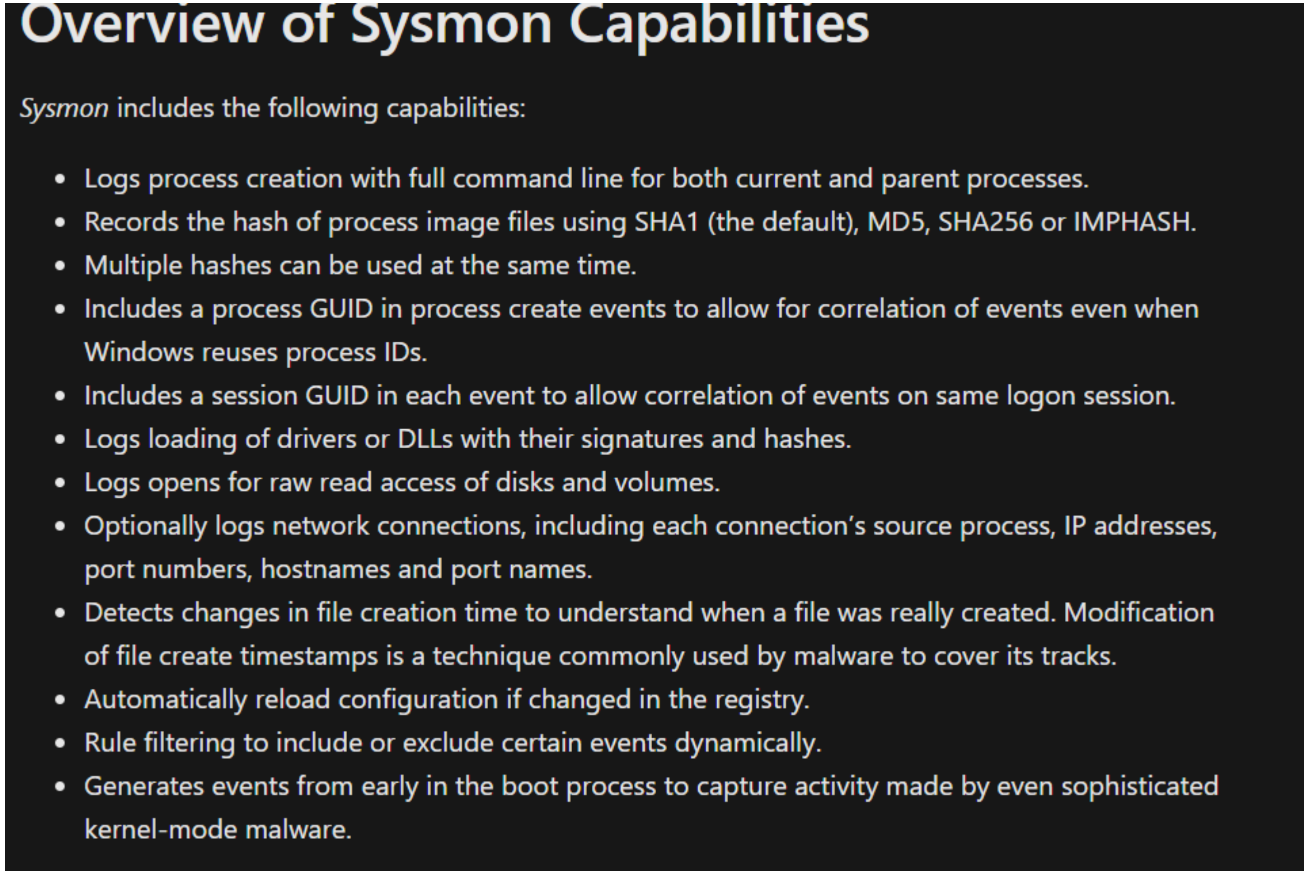
What is ELK?

- ELK significa a solução de monitoramento que consiste principalmente em **Elasticsearch** , **Logstash** e **Kibana** ;
- Ele foi renomeado como **Elastic Stack** , pois expandiu bastante suas funções através do uso de **batidas** e alguns outros complementos como servidores APM. Mas as pessoas ainda tendem a chamá-lo de ELK;
- É uma solução de monitoramento distribuída adequada para quase qualquer fonte de dados **estruturada** e **não estruturada** , mas não limitada a log;
- Ele suporta monitoramento centralizado de **log/métrica/APM ;**
- É de código aberto e pode ser estendido facilmente.
- https://elastic-stack.readthedocs.io/en/latest/introduction.html



Sysmon

- System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.
- Note that Sysmon does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.



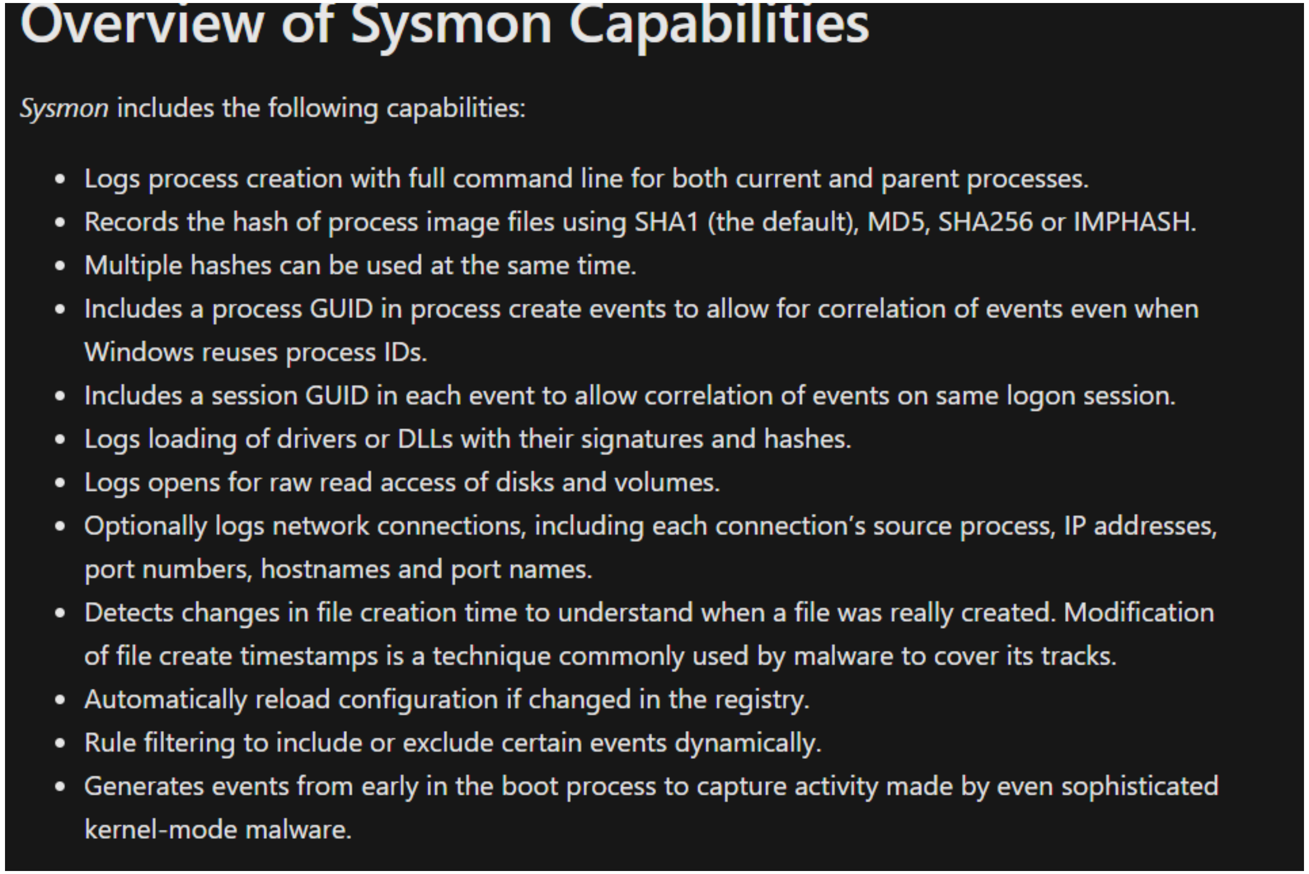
Overview of Sysmon Capabilities

Sysmon includes the following capabilities:

- Logs process creation with full command line for both current and parent processes.
- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- Multiple hashes can be used at the same time.
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process IDs.
- Includes a session GUID in each event to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Logs opens for raw read access of disks and volumes.
- Optionally logs network connections, including each connection’s source process, IP addresses, port numbers, hostnames and port names.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Automatically reload configuration if changed in the registry.
- Rule filtering to include or exclude certain events dynamically.
- Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.

Sysmon

- O System Monitor (Sysmon) é um serviço do sistema Windows e um driver de dispositivo que, uma vez instalado em um sistema, permanece residente nas reinicializações do sistema para monitorar e registrar a atividade do sistema no log de eventos do Windows. Ele fornece informações detalhadas sobre criações de processos, conexões de rede e alterações no tempo de criação de arquivos. Ao coletar os eventos gerados usando a Coleção de Eventos do Windows ou agentes SIEM e posteriormente analisá-los, você pode identificar atividades maliciosas ou anômalas e entender como invasores e malwares operam em sua rede.
- Observe que o Sysmon não fornece análise dos eventos que gera, nem tenta se proteger ou se esconder dos invasores.
- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon



Overview of Sysmon Capabilities

Sysmon includes the following capabilities:

- Logs process creation with full command line for both current and parent processes.
- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- Multiple hashes can be used at the same time.
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process IDs.
- Includes a session GUID in each event to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Logs opens for raw read access of disks and volumes.
- Optionally logs network connections, including each connection's source process, IP addresses, port numbers, hostnames and port names.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Automatically reload configuration if changed in the registry.
- Rule filtering to include or exclude certain events dynamically.
- Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.

Wireshark

- Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

- You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

- In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Wireshark

- Wireshark é um analisador de pacotes de rede. Um analisador de pacotes de rede apresenta dados de pacotes capturados com o máximo de detalhes possível.
- Você pode pensar em um analisador de pacotes de rede como um dispositivo de medição para examinar o que está acontecendo dentro de um cabo de rede, assim como um eletricista usa um voltímetro para examinar o que está acontecendo dentro de um cabo elétrico (mas em um nível mais alto, é claro).
- No passado, essas ferramentas eram muito caras, proprietárias ou ambas. No entanto, com o advento do Wireshark, isso mudou. O Wireshark está disponível gratuitamente, é de código aberto e é um dos melhores analisadores de pacotes disponíveis atualmente.
- https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs

Wireshark Cheatsheet

- https://www.comparitech.com/net-admin/wireshark-cheat-sheet/
- https://packetlife.net/blog/2008/oct/18/cheat-sheets-tcpdump-and-wireshark/
- https://www.stationx.net/wireshark-cheat-sheet/
- http://freedevelop.org/wp-content/uploads/Wireshark_cheatsheet3.pdf

ELK Create Visualization

- https://logz.io/blog/kibana-tutorial-2/#newkibanavisualization
- https://www.youtube.com/watch?v=DzGwmr8nKPg
- https://www.youtube.com/watch?v=5oF2rJPAZ-M
- https://www.youtube.com/watch?v=mpugiMItwpQ

IOCs Editor

- https://www.fireeye.com/content/dam/fireeye-www/services/freeware/ug-ioc-editor.pdf
- The FireEye Indicators of Compromise (IOC) Editor is a free tool that provides an interface for managing data and manipulating the logical structures of IOCs. IOCs are XML documents that help incident responders capture diverse information about threats, including attributes of malicious files, characteristics of registry changes and artifacts in memory. The IOC Editor includes:

- Manipulation of the logical structures that define the IOC
- Application of meta-information to IOCs, including detailed descriptions or arbitrary labels
- Conversion of IOCs into XPath filters
- Management of lists of “terms” used within IOCs

IOCs Editor

- https://www.fireeye.com/content/dam/fireeye-www/services/freeware/ug-ioc-editor.pdf
- O FireEye Indicators of Compromise (IOC) Editor é uma ferramenta gratuita que fornece uma interface para gerenciar dados e manipular as estruturas lógicas de IOCs. IOCs são documentos XML que ajudam os respondentes de incidentes a capturar diversas informações sobre ameaças, incluindo atributos de arquivos maliciosos, características de alterações de registro e artefatos na memória. O Editor do COI inclui:

- Manipulação das estruturas lógicas que definem o IOC
- Aplicação de meta-informação aos IOCs, incluindo descrições detalhadas ou rótulos arbitrários
- Conversão de IOCs em filtros XPath
- Gerenciamento de listas de “termos” usados nos IOCs

Creating IOCs

- https://be4sec.com/2021/07/25/creating-iocs-with-mandiant-ioce/
- https://www.mandiant.com/resources/openioc-basics
- https://www.iocbucket.com/openioceditor
- https://jonahacks.medium.com/thm-creating-iocs-7cf03d8fc768
- https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-iocs/create-an-ioc-rule

Hunting mimikatz with sysmon

- https://medium.com/kminthein/threat-hunter-diary-part-1-hunting-mimikatz-4b24f10a65f4
- https://blog.3or.de/hunting-mimikatz-with-sysmon-monitoring-openprocess.html
- https://www.youtube.com/watch?v=gKa_CZAz3Jc

Hunting mimikatz with ELK

- https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-hunter-hunting-for.html
- https://malwarenailed.blogspot.com/2017/10/hunting-mimikatz-using-sysmon-elk-part.html
- https://jordanpotti.com/2018/01/03/automating-the-detection-of-mimikatz-with-elk/

Hunting Code Injection with Sysmon

- https://www.youtube.com/watch?v=2xA5Sm0Xdd0
- https://letsdefend.io/blog/process-injection-detection-with-sysmon/
- https://holdmybeersecurity.com/2021/06/02/part-3-intro-to-threat-hunting-hunting-the-imposter-among-us-with-the-elastic-stack-and-sysmon/
- https://cyberpolygon.com/materials/threat-hunting-in-action/
- https://www.giac.org/paper/gcfa/11563/hunting-ghosts-fileless-attacks/150888
- https://jsecurity101.medium.com/injecting-into-the-hunt-185af9d56636

Hunting Code Injection with ELK

- https://www.elastic.co/pt/blog/hunting-memory
- https://www.elastic.co/pt/blog/hunting-memory-net-attacks
- http://www.ijcse.com/docs/INDJCSE19-10-05-008.pdf
- https://medium.com/@chenerlich/threat-hunting-using-yeti-and-elastic-stack-29735c51195f
- https://github.com/jsecurity101/Detecting-Process-Injection-Techniques
- https://alparslanakyildiz.medium.com/understanding-and-detecting-dll-1nj3ct0n-process-hollowing-fcd87676d36b

Yara and Yara Rules

- YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a. rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example:
- https://www.varonis.com/blog/yara-rules
- https://yara.readthedocs.io/en/stable/

Yara and Yara Rules

- YARA é uma ferramenta que visa (mas não se limita a) ajudar pesquisadores de malware a identificar e classificar amostras de malware. Com o YARA, você pode criar descrições de famílias de malware (ou o que você quiser descrever) com base em padrões textuais ou binários. Cada descrição, também conhecida como regra, consiste em um conjunto de strings e uma expressão booleana que determina sua lógica. Vejamos um exemplo:
- https://www.varonis.com/blog/yara-rules
- https://yara.readthedocs.io/en/stable/

Redline Analysis

- Redline®, FireEye's premier free endpoint security tool, provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis and the development of a threat assessment profile.

With Redline, you can:

- Thoroughly audit and collect all running processes and drivers from memory, file-system metadata, registry data, event logs, network information, services, tasks and web history.
- Analyze and view imported audit data, including the ability to filter results around a given timeframe using Redline's Timeline functionality with the TimeWrinkle™ and TimeCrunch™ features.
- Streamline memory analysis with a proven workflow for analyzing malware based on relative priority.
- Perform Indicators of Compromise (IOC) analysis. Supplied with a set of IOCs, the Redline Portable Agent is automatically configured to gather the data required to perform the IOC analysis and an IOC hit result review.

Redline Analysis

- Redline®, a principal ferramenta gratuita de segurança de endpoints da FireEye, fornece recursos de investigação de host para que os usuários encontrem sinais de atividade maliciosa por meio da análise de memória e arquivos e do desenvolvimento de um perfil de avaliação de ameaças.

Com Redline, você pode:

- Faça uma auditoria completa e colete todos os processos e drivers em execução da memória, metadados do sistema de arquivos, dados do registro, logs de eventos, informações de rede, serviços, tarefas e histórico da web.
- Analise e visualize dados de auditoria importados, incluindo a capacidade de filtrar resultados em um determinado período de tempo usando a funcionalidade Timeline do Redline com os recursos TimeWrinkle™ e TimeCrunch™.
- Simplifique a análise de memória com um fluxo de trabalho comprovado para analisar malware com base na prioridade relativa.
- Realizar análise de Indicadores de Comprometimento (IOC). Fornecido com um conjunto de IOCs, o Redline Portable Agent é configurado automaticamente para coletar os dados necessários para realizar a análise de IOC e uma revisão de resultado de acerto de IOC.
- https://www.fireeye.com/services/freeware/redline.html

Redline Analysis File

- https://resources.infosecinstitute.com/topic/memory-analysis-using-redline/
- https://www.youtube.com/watch?v=HXv45dsL8xI
- https://www.youtube.com/watch?v=pNZqb9JPv7k
- https://isc.sans.edu/forums/diary/Introduction+to+Memory+Analysis+with+Mandiant+Redline/17797/
- https://www.admin-magazine.com/Articles/Acquiring-a-Memory-Image/(offset)/3
- https://www.toolwar.com/2014/01/mandiant-redline-memory-and-file.html

Redline Analysis Code Injection

- https://resources.infosecinstitute.com/topic/redline-stealer-malware-full-analysis/
- https://www.proofpoint.com/us/blog/threat-insight/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign
- https://securityboulevard.com/2022/03/drawing-the-redline-insider-threats-in-cybersecurity/
- https://isc.sans.edu/forums/diary/RedLine+Stealer+Delivered+Through+FTP/28258/
- https://blog.minerva-labs.com/redline-stealer-masquerades-as-telegram-installer
- https://socprime.com/blog/redline-stealer-malware-detection/

Threat Hunting Fileless Malware

- https://blog.f-secure.com/threat-hunting-for-fileless-malware/
- https://www.socinvestigation.com/threat-hunting-using-powershell-and-fileless-malware-attacks/
- https://www.pandasecurity.com/en/mediacenter/pandalabs/threat-hunting-fileless-attacks/
- https://pt.slideshare.net/OlgaPasko/hunting-fileless-malware-149129867

Threat Hunting Persistence

- https://www.elastic.co/pt/blog/hunting-for-persistence-using-elastic-security-part-1
- https://www.cyborgsecurity.com/cyborg-labs/hunting-for-persistence-registry-run-keys-startup-folder/
- https://www.elastic.co/pt/blog/hunting-for-persistence-using-elastic-security-part-2
- https://www.istrosec.com/pl/blog/osquery-threat-hunt-1/

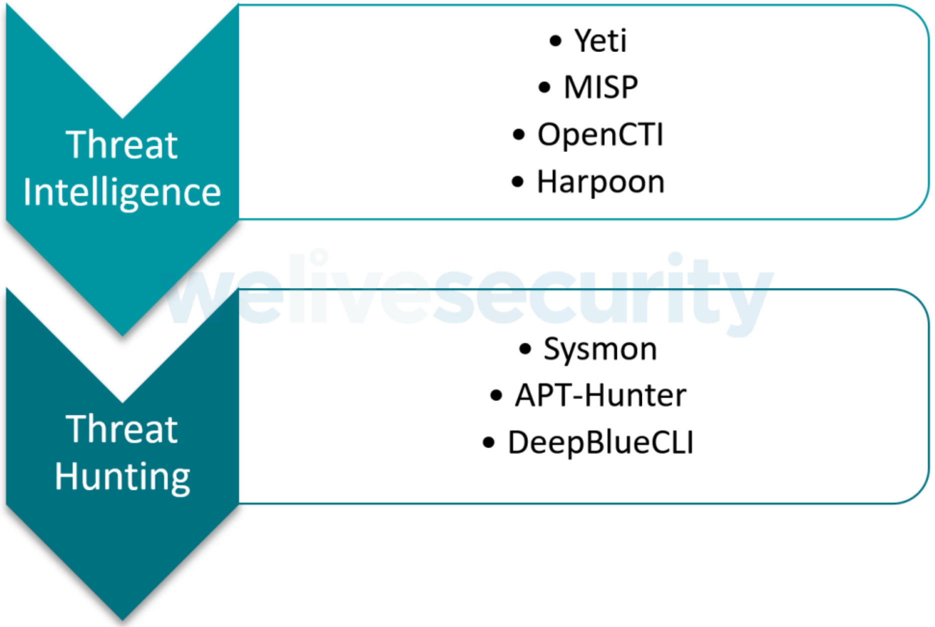
Threat Hunting Lateral Movement

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=512062
- https://www.cybersecurity-insiders.com/threat-hunting-for-lateral-movement/
- https://www.elastic.co/pt/blog/hunting-for-lateral-movement-using-event-query-language
- https://www.slideshare.net/sqrrl/how-to-hunt-for-lateral-movement-on-your-network

Threat Hunting Tools

- https://www.guidepointsecurity.com/education-center/threat-hunting-tips-and-tools-2/
- https://github.com/0x4D31/awesome-threat-detection
- https://github.com/A3sal0n/CyberThreatHunting
- https://github.com/GossiTheDog/ThreatHunting
- https://github.com/SoulSec/resource-threat-hunting

Threat Hunting Maturity

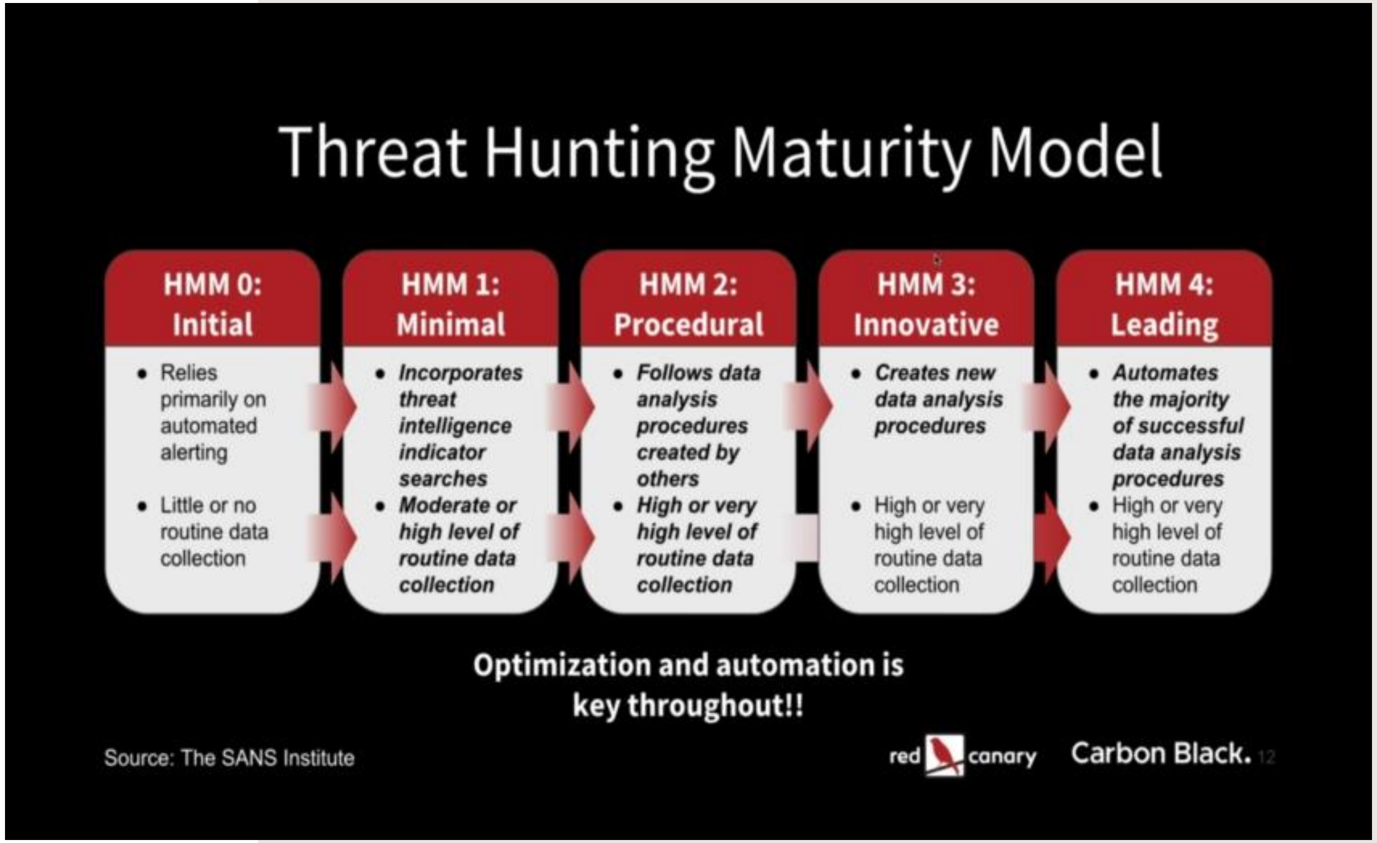


Threat Intelligence

- Yeti
- MISP
- OpenCTI
- Harpoon

Threat Hunting

- Sysmon
- APT-Hunter
- DeepBlueCLI



Threat Hunting Maturity Model

HMM 0: Initial

- Relies primarily on automated alerting
- Little or no routine data collection

HMM 1: Minimal

- *Incorporates threat intelligence indicator searches*
- *Moderate or high level of routine data collection*

HMM 2: Procedural

- *Follows data analysis procedures created by others*
- *High or very high level of routine data collection*

HMM 3: Innovative

- *Creates new data analysis procedures*
- High or very high level of routine data collection

HMM 4: Leading

- *Automates the majority of successful data analysis procedures*
- High or very high level of routine data collection

Optimization and automation is key throughout!!

Source: The SANS Institute

red canary Carbon Black. 12