Exploring the Value of Different Threat Intelligence Sources

JESSICA LEE | INFOSECJESS@GMAIL.COM

About Me

Threat hunter on 24/7/365 managed threat hunting team

Over 7 years of experience in information security

Helped build threat intelligence capabilities at global oil and gas and financial services companies

Certifications: GCFA, GCIA, GCTI, GSEC

Studied Linguistics and Applied Linguistics

Started career as a technical writer

Agenda

Threat Intelligence Fundamentals

- Threat Intelligence Lifecycle
- Types of Threat Intelligence
- Threat Modeling

Types of Threat Intelligence Sources

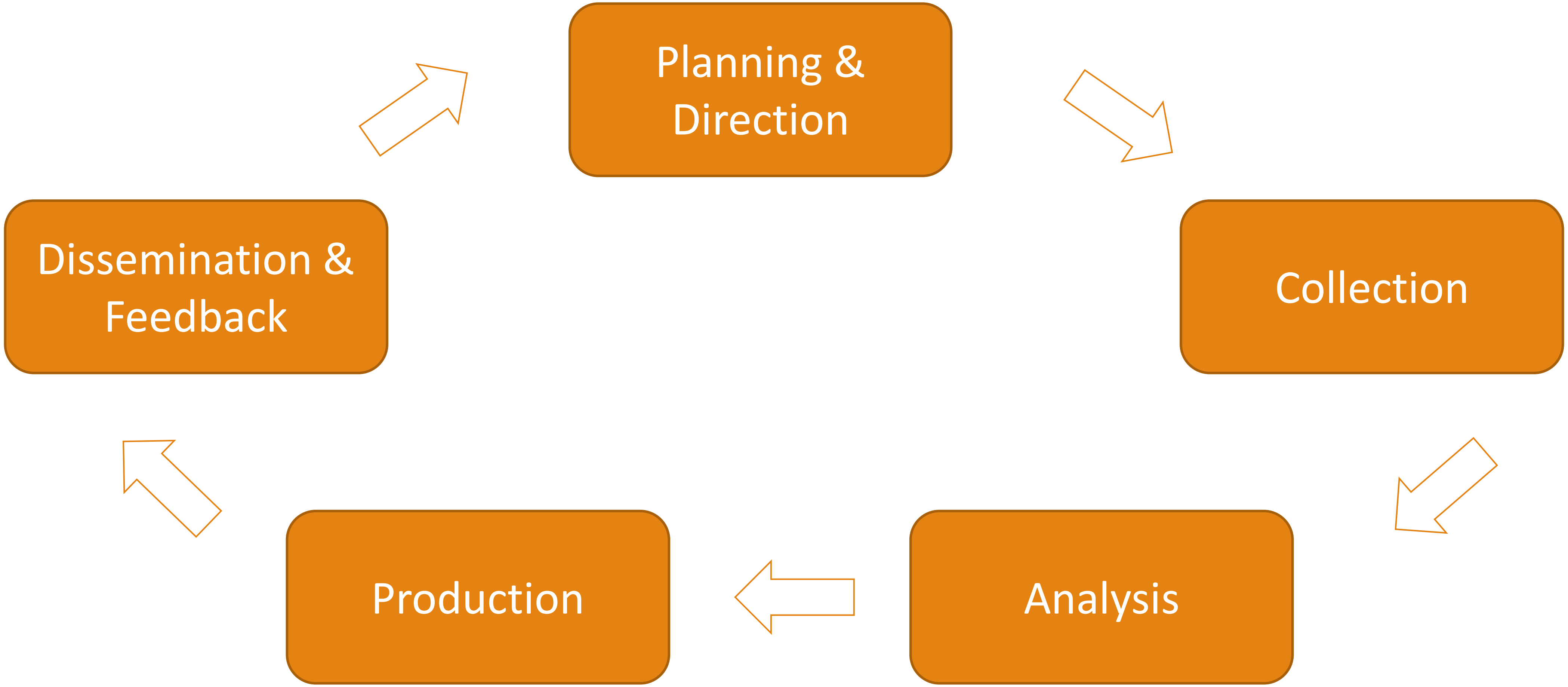
- Threat Intelligence Sources Matrix
- Source Deep Dives

Thinking Critically About Threat Intelligence Sources

- Critical Thinking Techniques
- Primary, Secondary, and Tertiary Sources
- Timely, Accurate, Relevant, Actionable

Threat Intelligence Fundamentals

Threat Intelligence Lifecycle



Planning & Direction

Collection

Analysis

Production

Dissemination & Feedback

Types of Threat Intelligence

Technical: Machine-readable threat data that can be ingested into security technologies, which is often short-term with short shelf-life. (Technical intelligence is not a focus of this presentation)

Tactical: Geared toward incident responders and other hands-on technical analysts that are involved in day-to-day operations. Is used to generate and enrich Indicators of Compromise (IOCs) and Indicators of Attack (IOAs) and provide a quick turnaround to make the Security Operations Center (SOC) more efficient and more effective.

Operational: Geared toward SOC managers, vulnerability management, the red team, and others who may benefit from understanding information about campaigns and adversary behaviors. This level of threat intelligence often provides attribution on intrusion activity and helps others to understand which threats are most pressing to the organization.

Strategic: Geared toward senior leadership and is used to drive strategic business decisions based on the cyber threats that may impact your organization. This is the least technical type of intelligence.

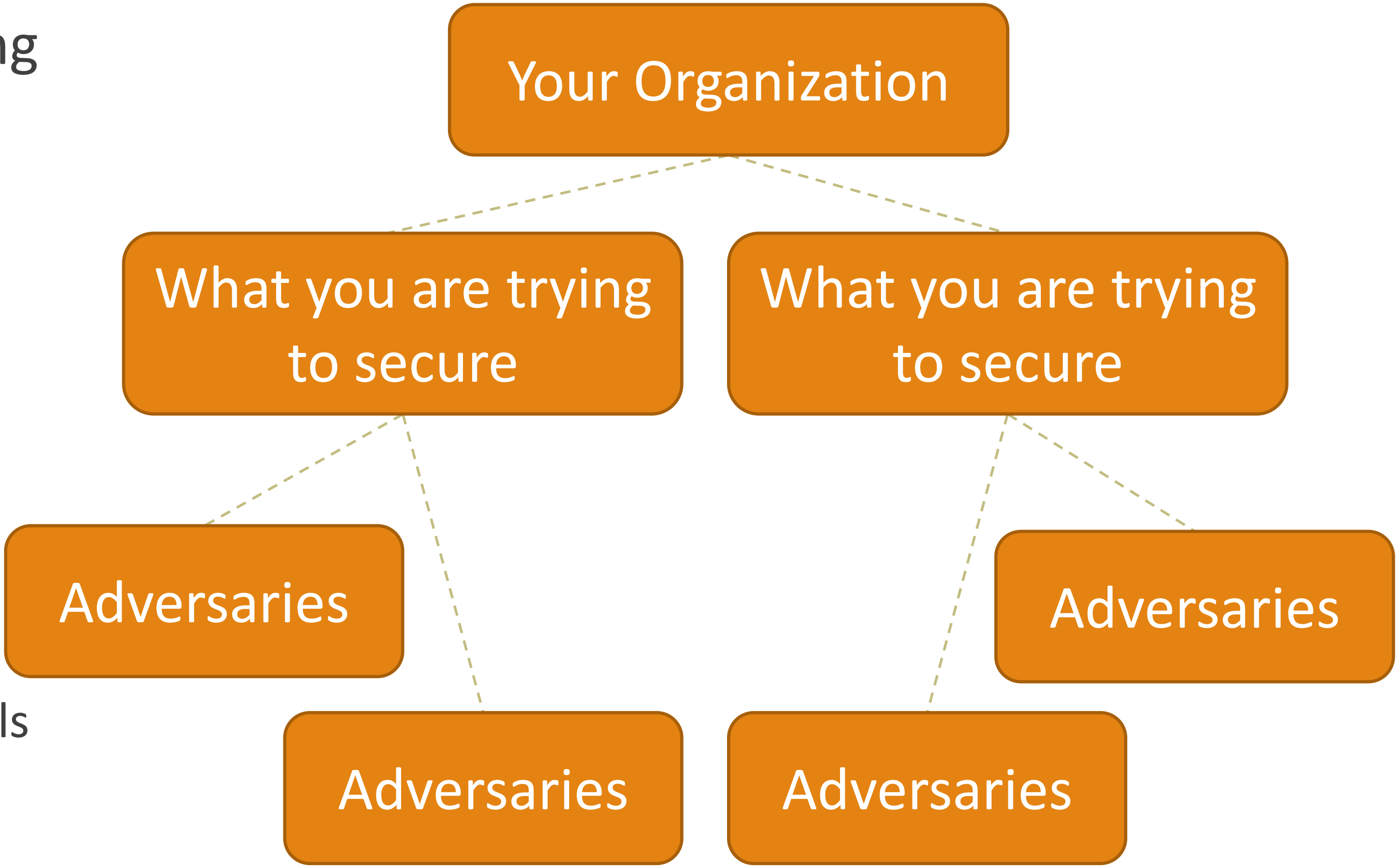
Threat Modeling

What is your organization working to secure?

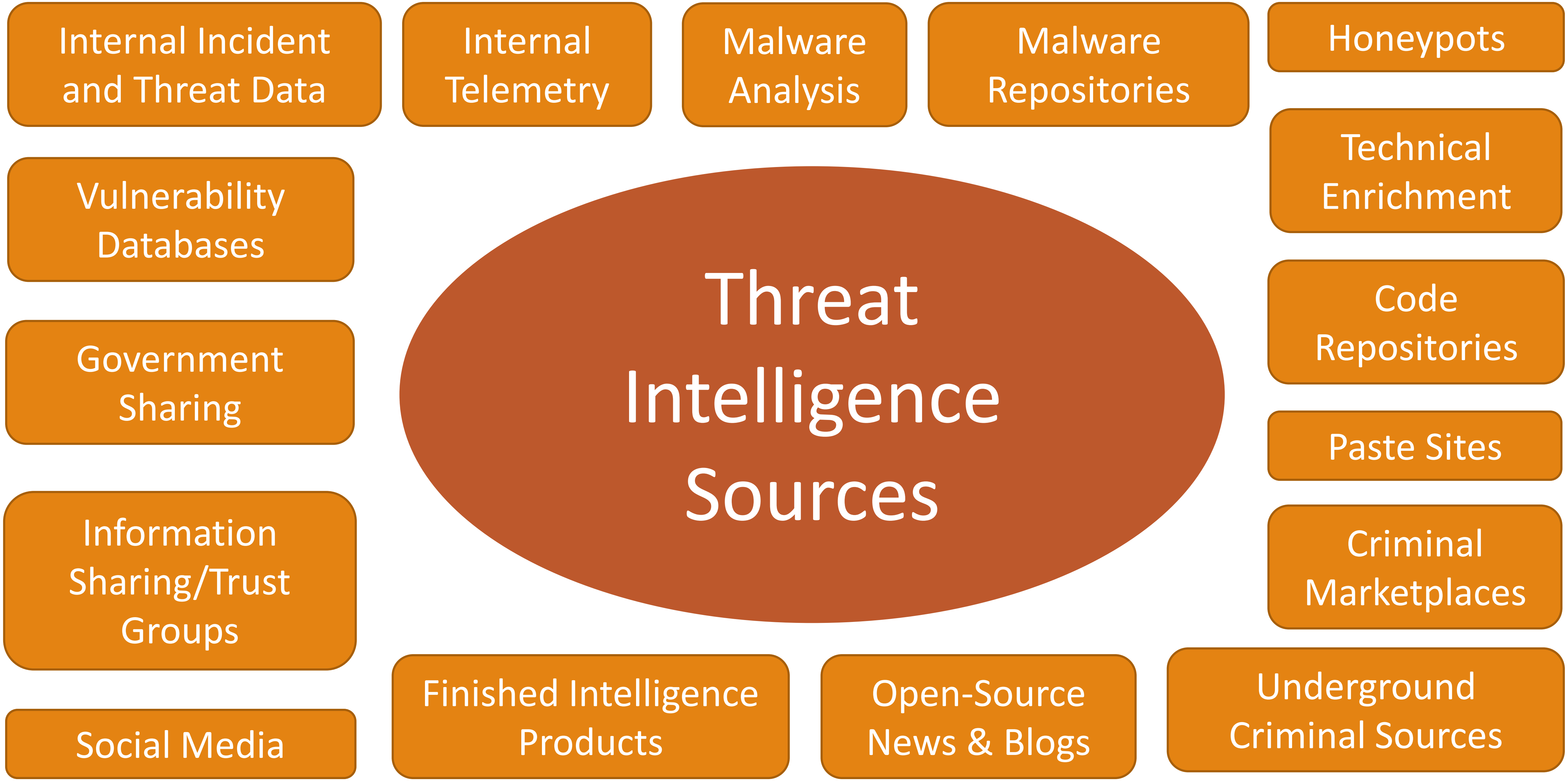
- Trade Secrets
- Customer Data
- Payment Card Information
- Other?

What types of adversaries may target your organization or have historically targeted your organization?

- Targeted/Nation-State
- Financially Motivated Cyber Criminals
- Hacktivists
- Unidentified Adversaries

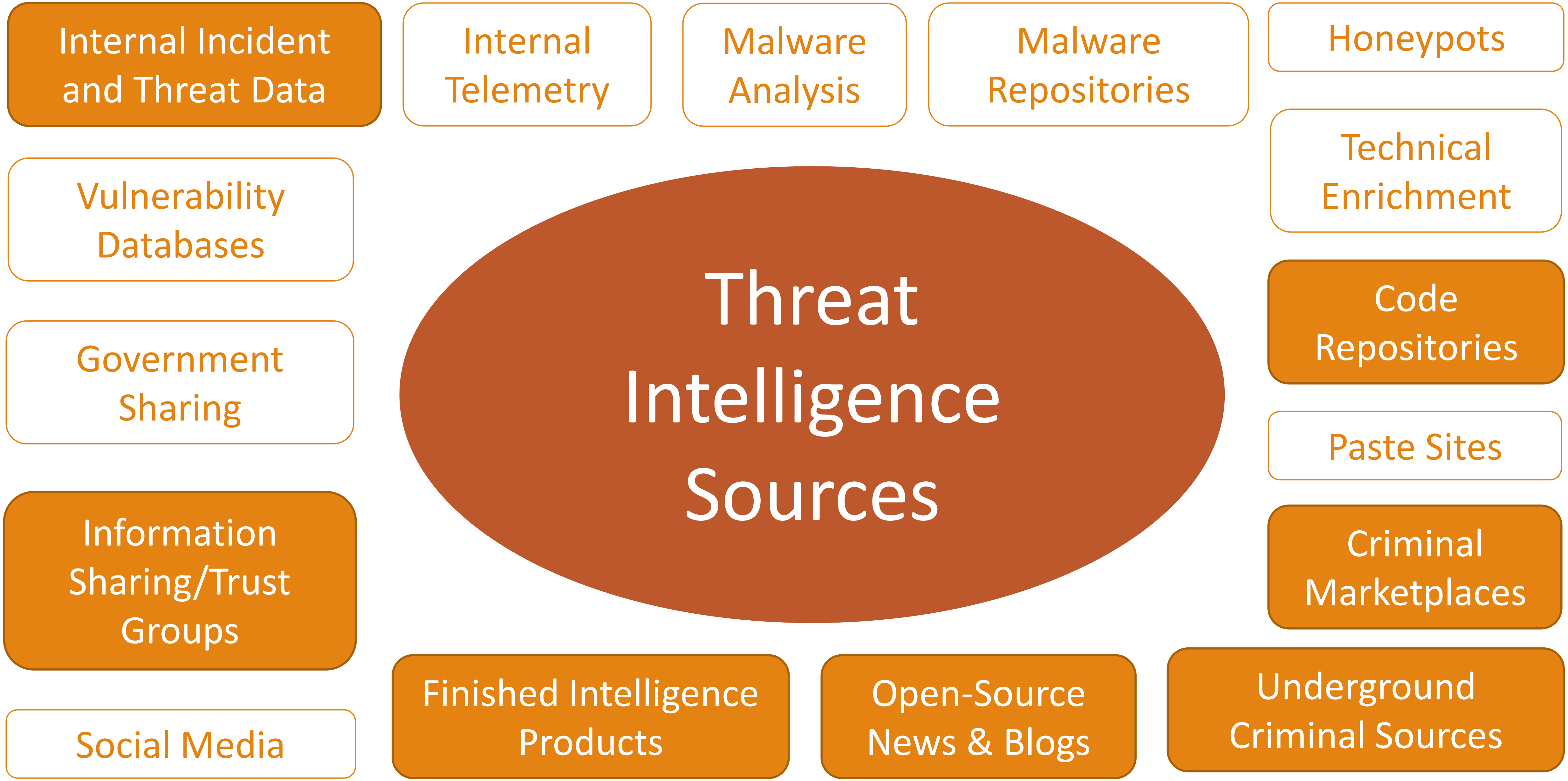


Types of Threat Intelligence Sources



Threat Intelligence Sources

- Internal Incident and Threat Data
- Internal Telemetry
- Malware Analysis
- Malware Repositories
- Honeypots
- Vulnerability Databases
- Technical Enrichment
- Code Repositories
- Government Sharing
- Paste Sites
- Information Sharing/Trust Groups
- Criminal Marketplaces
- Social Media
- Finished Intelligence Products
- Open-Source News & Blogs
- Underground Criminal Sources



Threat Intelligence Sources

- Internal Incident and Threat Data
- Internal Telemetry
- Malware Analysis
- Malware Repositories
- Honeypots
- Technical Enrichment
- Vulnerability Databases
- Code Repositories
- Government Sharing
- Paste Sites
- Information Sharing/Trust Groups
- Criminal Marketplaces
- Social Media
- Finished Intelligence Products
- Open-Source News & Blogs
- Underground Criminal Sources

Internal Incident and Threat Data

One of the most valuable sources for refining threat model

Helps your organization identify which adversaries have targeted your organization as well as which malware families and tools have impacted your environment

Dependent on quality of data collected during incident response

Processing internal incident data can be very time-consuming, and your team needs a technical repository to store and correlate data

Attribution can be difficult, but your team can defend against Tactics, Techniques, and Procedures (TTPs) observed that have impacted your organization

Can be used to drive organizational change, such as implementing new policies, tuning security technologies, or purchasing new security tools

Finished Intelligence

Medium to high confidence intelligence analysis that can reduce analysis time spent by internal threat intelligence teams

Can provide insight into other organizations and industries without identifiable information

Finished intelligence often requires context before content can be shared across your organization. Others will want to know whether the organization was impacted, whether your organization is vulnerable to this activity, and what the information security teams are doing in response to this information, for example

Potentially not as valuable if you are in an industry or region that is not heavily reported on. In that case, your organization may prefer access to more raw data and enrichment sources to generate original intelligence for your organization

Underground Criminal Sources

Sources that are not easily accessible by average people or are not safe or easy to access for security professionals

Can include criminal forums where adversaries share information and techniques, criminal marketplaces that sell data, and other places where data can be dumped or shared

Not easy to directly collect in-house. Most organizations probably prefer to purchase access

- Operational security is very important to protect the identity of individuals and organizations
- Some sources require participants to be vouched for to gain access
- Cannot always be scraped regularly by intelligence providers

Commonly useful for organizations with large amounts of customer data or accounts

Data advertised for sale is often not actionable without purchasing the listings

Can tip companies off to potential data breaches, but data needs to be validated

Access brokers are a pressing threat to many organizations

Open-Source News & Blogs

Often the easiest to gain access to, but the easiest to overload analysts with information

Some sources are very valuable for providing overviews on trending industry news, such as ongoing incidents, major vulnerabilities, and new security research

- While these types of articles are often tertiary sources, they will site the primary or secondary source. Find the original source for more in-depth analysis and to remove one level of potential inaccuracies

Can be very technical in nature, such as blogs by security vendors. Can provide details on campaigns and adversary groups that can fill gaps in your collections without paying for information from every vendor

This source type can be very valuable for individuals not in threat intelligence roles who want to stay up to date on the latest industry news

Executive Freakout Factor: Wall Street Journal, New York Times, and other major news outlets can often grab the attention of executives when they publish information security content

Code Repositories

Code repositories such as GitHub can be rich sources for a variety of objectives

- Code leaks or misconfigurations involving sensitive company code
- Leaked passwords and private keys
- Proof-of-Concept code for vulnerabilities that could potentially impact your organization, such as vulnerabilities with low patch saturation rate or that cannot be patched in your environment
- Malicious tools with your infrastructure mentioned in their code
- New versions of penetration testing tools that may be abused

Must have allow list capability to filter out noise, such as test data sets or sample code

Sometimes these use cases are not in scope for threat intelligence, but this can fall under threat intelligence because that team collects the most external data

Information Sharing/Trust Groups

These groups are often created based on shared characteristics, such as the industry

Can help fill gaps in collections for smaller industries where finished intelligence is not available

Data is not often validated before shared, but over time, you can more easily recognize what types of data will be valuable to your organization

Often have agreements in place for how to safely and ethically share data

Can be less beneficial if members do not actively participate or if your organization does not have a similar threat model to other participants

Incorporate how to share data into your intelligence workflows to reduce time spent on information sharing (tagging IOCs to be pulled out of Threat Intelligence Platform (TIP), templates for copying and pasting sharable portions of data)

Thinking Critically About Sources

Thinking Critically About Sources

Who created this content?

Why did they create the content?

Are there any secondary motivations for why this content was created?

How is this content valuable to your organization?

Is the information actionable?

What are the reasons why this content may not be trustworthy?

What can you do to validate this information?

Is this primary, secondary, or a tertiary source?

Primary, Secondary, and Tertiary Sources

Primary Sources: The source type that is closest to the raw data or the event of interest
Examples: Indicators of Compromise, Indicators of Attack, incident data, telemetry from security tools, communications on criminal forums, interview transcripts

Secondary Sources: Sources that include analysis of data and other primary sources
Examples: Finished intelligence, technical blogs, internal incident reports

Tertiary Sources: Summaries or condensed versions of materials, usually including information from primary and secondary sources
Examples: Online blogs and new articles, adversary profiles, wikis, social media posts announcing technical blogs

Each degree of separation introduces the opportunity for inaccuracies. On the other hand, the more sources that are used for research, the more accurate the final product may be

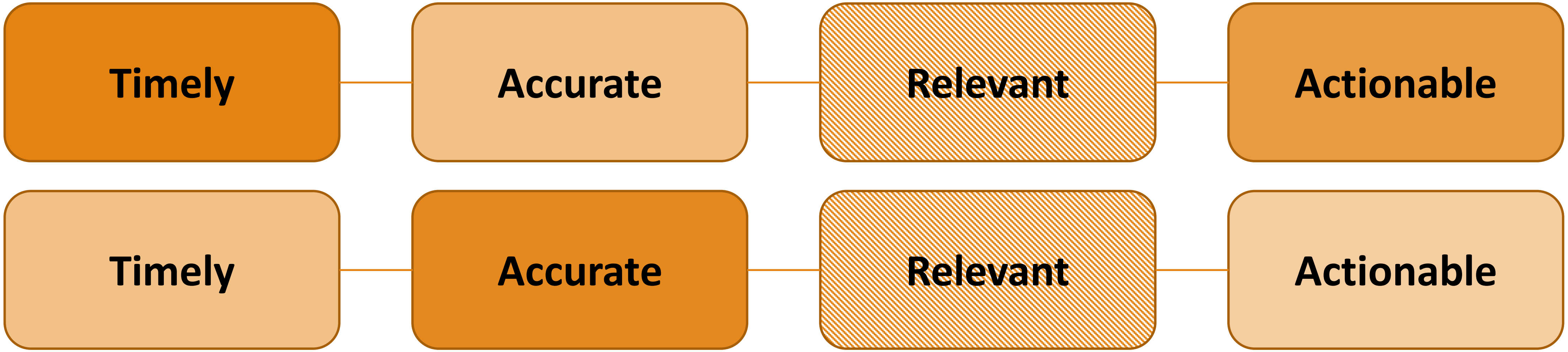
TARA

Timely: How quickly was this content created after the event of interest?

Accurate: How accurate is this content?

Relevant: How relevant is this content to the audience?

Actionable: Can the audience act on this information to strengthen security posture?



Timely — Accurate — Relevant — Actionable

Timely — Accurate — Relevant — Actionable

Key Considerations

Threat intelligence teams are often overloaded with data. Assessing what sources are valuable can help the team focus

Assess how each source supports your threat model

Ensure you have business processes in place to support the new collections capability

- Who do you contact for code exposures?
- Can you force password resets?
- Does your team have reporting templates and mechanisms to distribute intelligence reporting?

The intelligence work you do today should be accessible years from now, and you should be able to search for and correlate data

Even if you aren’t in a threat intelligence role, how are these sources valuable to you and your organization?

Jessica Lee

INFOSECJESS@GMAIL.COM

Thank you!