# The Cycle of Cyber Threat Intelligence

Katie Nickels (@LiketheCoins)
SANS Instructor

# Intelligence

Intelligence is the collecting and processing of information about a competitive entity and its agents, needed by an organization or group for its security and well-being.

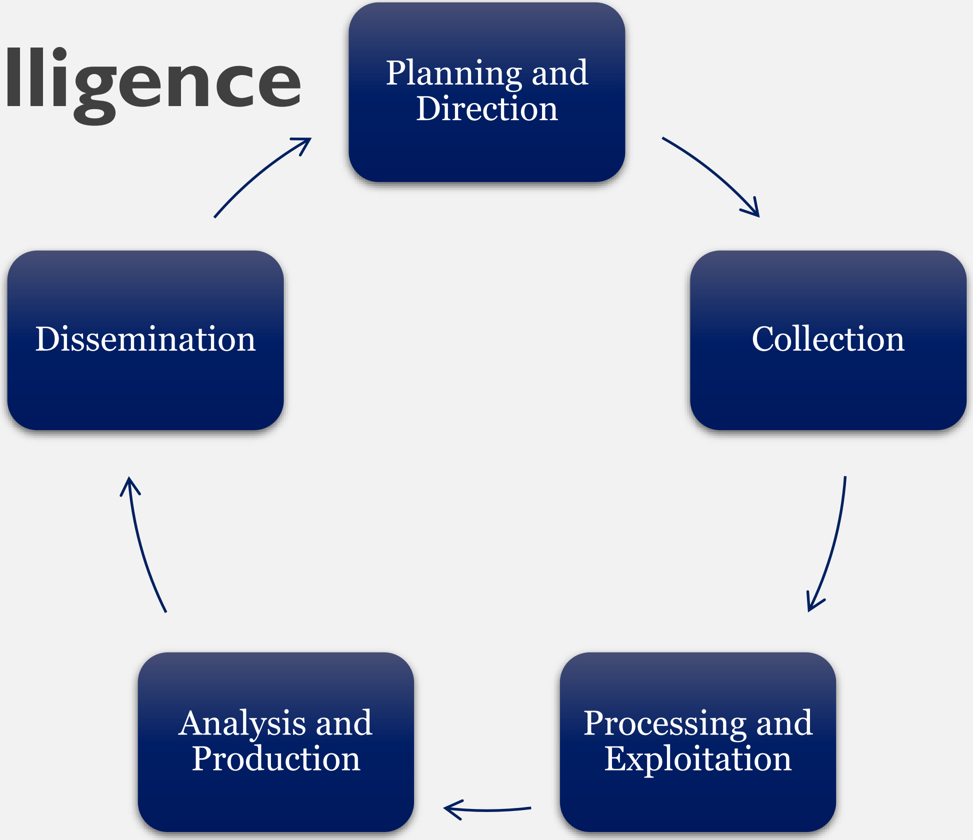
Intelligence is both a product and a process.

# Defining Cyber Threat Intelligence

- Simply defined here as:
  *Analyzed information about the hostile intent, capability, and opportunity of an adversary that satisfies a requirement*

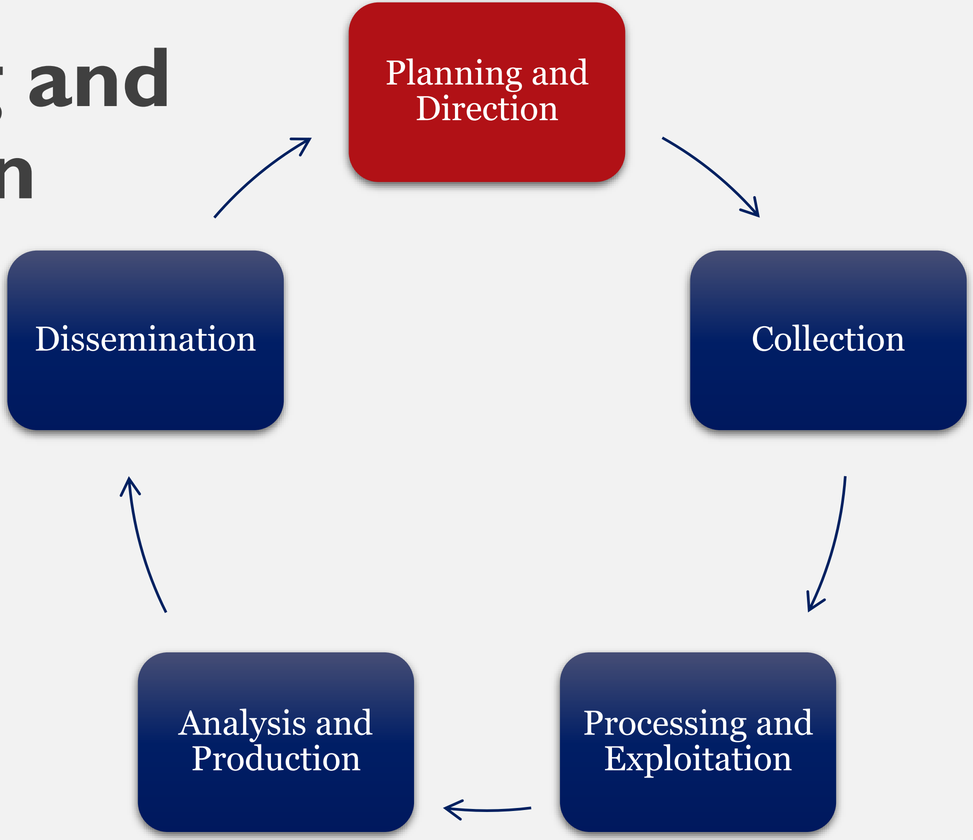
- The focus is on the threat (human)

# The Intelligence Cycle



SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

# Planning and Direction



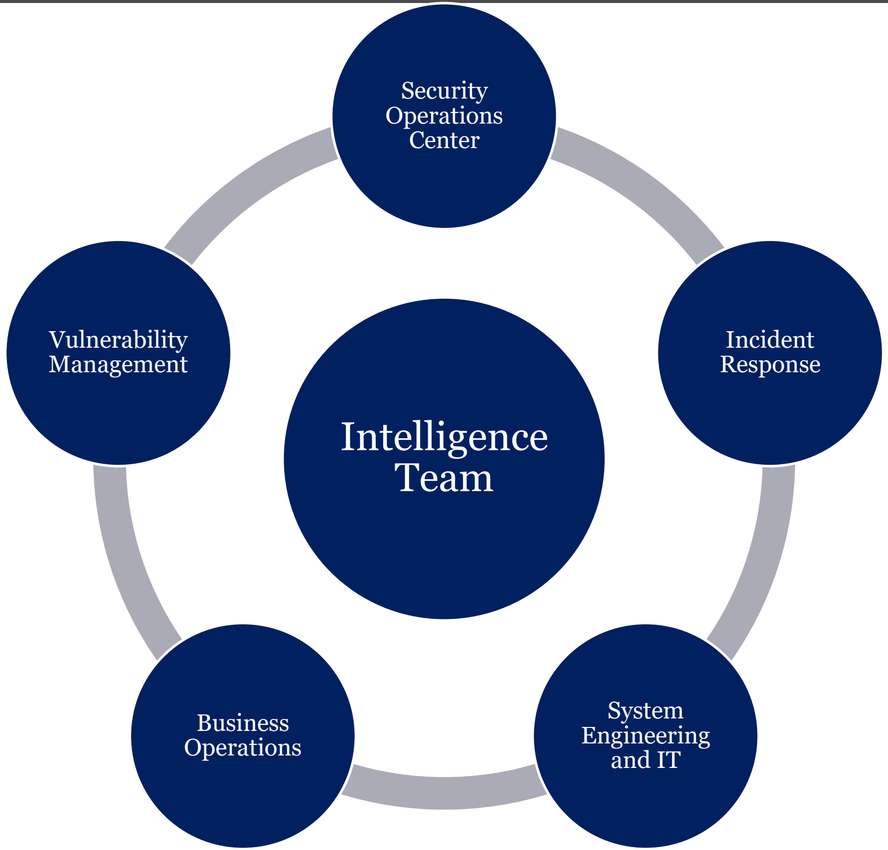
# A Few Sample Purposes of a Cyber Threat Intelligence Team

- Preventative Function: Security Operations Center (SOC) support, alerting, and triage
  - Triaging alerts
  - Enriching IOCs and artifacts
  - Providing information to vulnerability and risk management

- Response Function: Incident Response support
  - Enriching IOCs and artifacts
  - Facilitating information sharing

- Strategic Support Function
  - Supporting business decisions
  - Informing resource prioritization

# Structuring Your Team to Generate Intelligence



Strive for diversity in the team: backgrounds, focus areas, culture, etc.

# Planning and Direction Fundamentals

1. Intelligence Requirements
2. Threat Modeling
3. Collection Management Framework

# Intelligence Requirements

- Intelligence Requirements (IRs) are objectives that analysts seek to satisfy through the intelligence process
- A simple definition: “A request to satisfy a knowledge gap about the threat or the operational environment”
- Teams should have a clearly articulated list of IRs available to the intelligence team and its consumers

# Generating Intelligence Requirements

- Seek input from intelligence consumers
- Should ask only one question
- Offer sample expected results
- Leverage pain points in the org as a starting place

Intelligence requirements help to avoid the self-licking ice cream cone problem (Useless Intelligence)

# Intelligence Requirement Examples

**Strategic**

- What business units are at most risk to cyber crime?

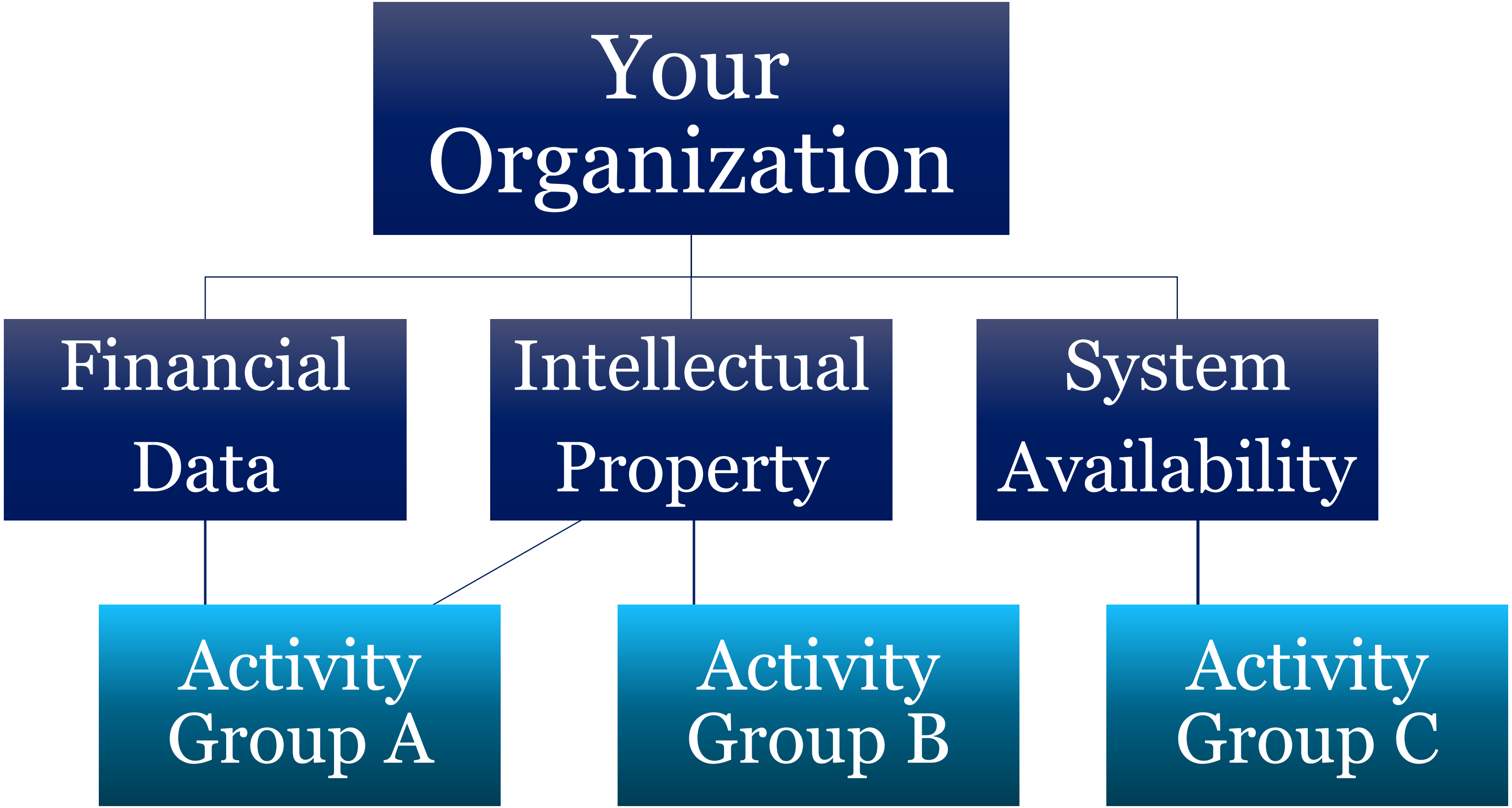
**Operational**

- What activity groups are currently active in our industry?

**Tactical**

- What adversary behaviors should security focus on to identify threats that are the most likely to breach our organization?

# Threat Modeling



Your Organization

Financial Data

Intellectual Property

System Availability

Activity Group A

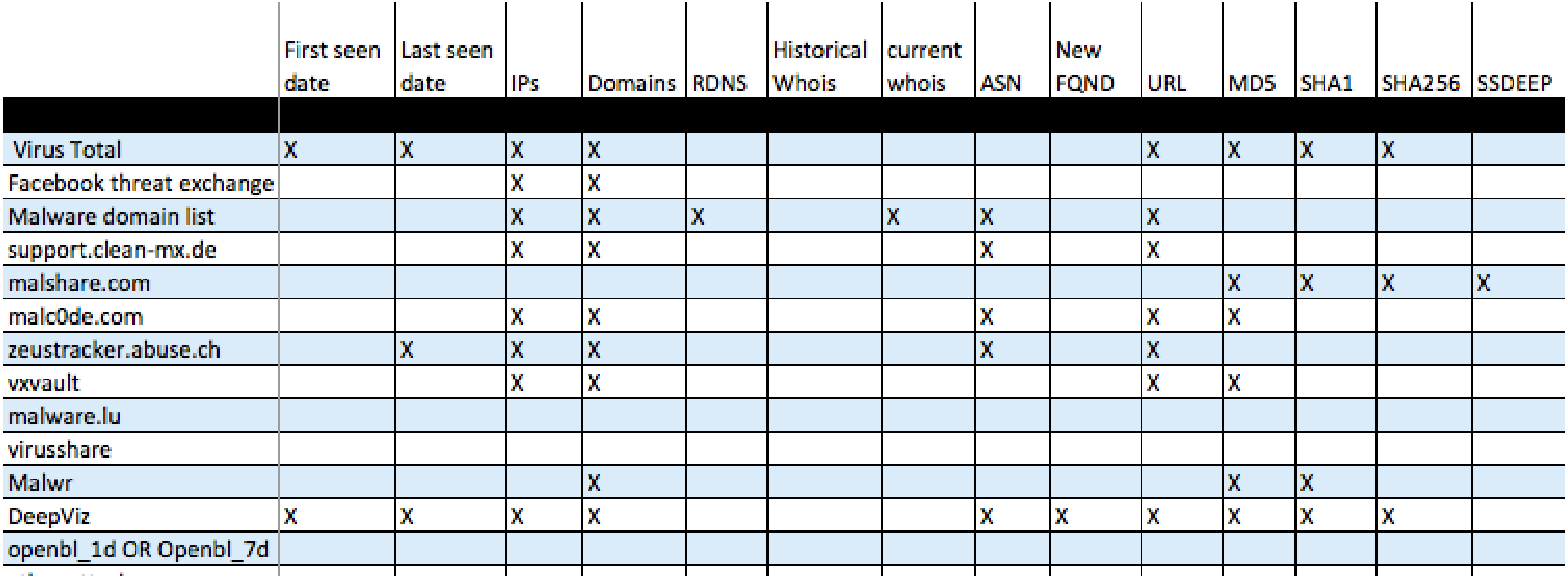
Activity Group B

Activity Group C

# Collection Management Framework

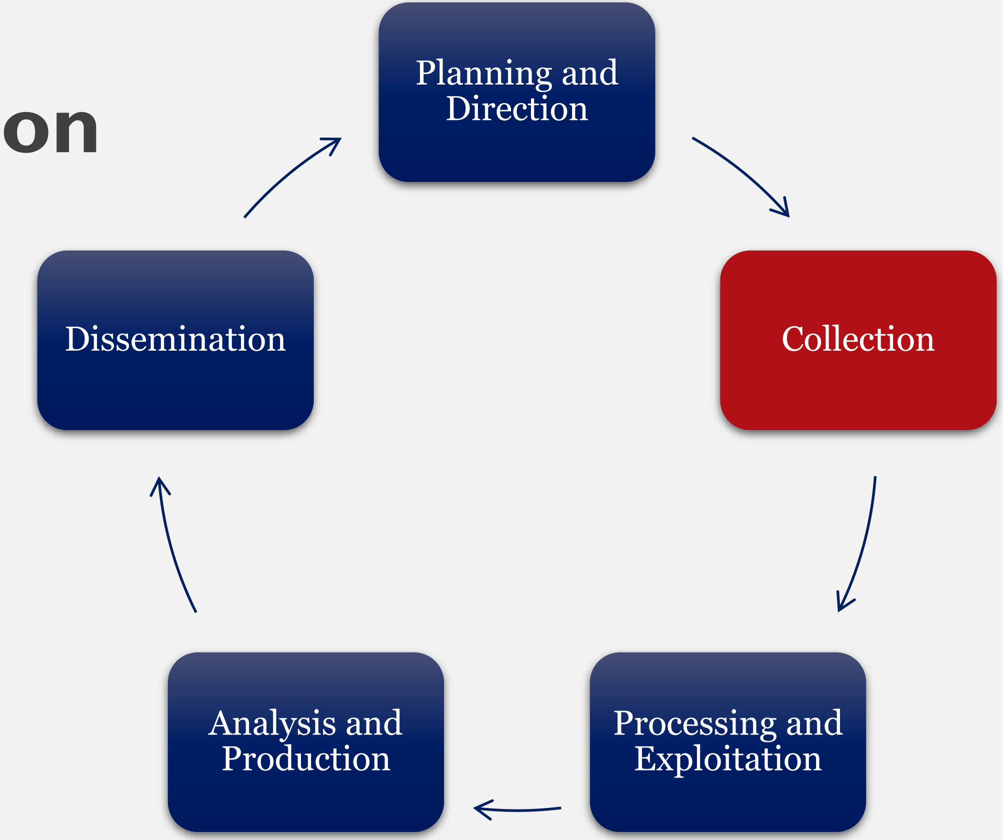
- Analysts must understand where they are getting data, how it is processed and delivered to them, and what questions they can reasonably ask of the data
  - *What requirements can we fulfill?*
- A Collection Management Framework is a view of sources of data, what is available in the data, and how that data is processed and exploited

# A Sample External Collection Management Framework on Malware Data



| | First seen date | Last seen date | IPs | Domains | RDNS | Historical Whois | current whois | ASN | New FQND | URL | MD5 | SHA1 | SHA256 | SSDEEP |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Virus Total | X | X | X | X | | | | | | X | X | X | X | |
| Facebook threat exchange | | | X | X | | | | | | | | | | |
| Malware domain list | | | X | X | X | | X | X | | X | | | | |
| support.clean-mx.de | | | X | X | | | | X | | X | | | | |
| malshare.com | | | | | | | | | | | X | X | X | X |
| malc0de.com | | | X | X | | | | X | | X | X | | | |
| zeustracker.abuse.ch | | X | X | X | | | | X | | X | | | | |
| vxvault | | | X | X | | | | | | X | X | | | |
| malware.lu | | | | | | | | | | | | | | |
| virusshare | | | | | | | | | | | | | | |
| Malwr | | | | X | | | | | | | X | X | | |
| DeepViz | X | X | X | X | | | | X | X | X | X | X | X | |
| openbl_1d OR Openbl_7d | | | | | | | | | | | | | | |

# Collection

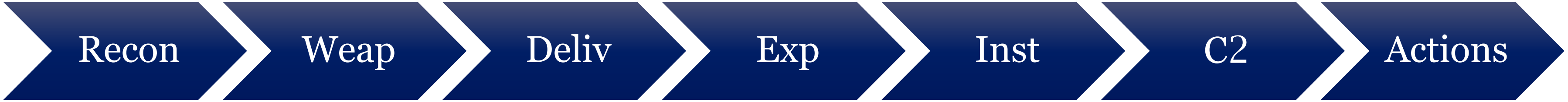

Planning and Direction
Collection
Processing and Exploitation
Analysis and Production
Dissemination

## Key Collection Sources

- Intrusion Analysis
- Malware
- Domains
- External Datasets
- TLS Certificates

# Intrusion Analysis: The Lockheed Martin Kill Chain

- Look to your own internal information!
- Describes stages of a single intrusion
- Seven stages to defend



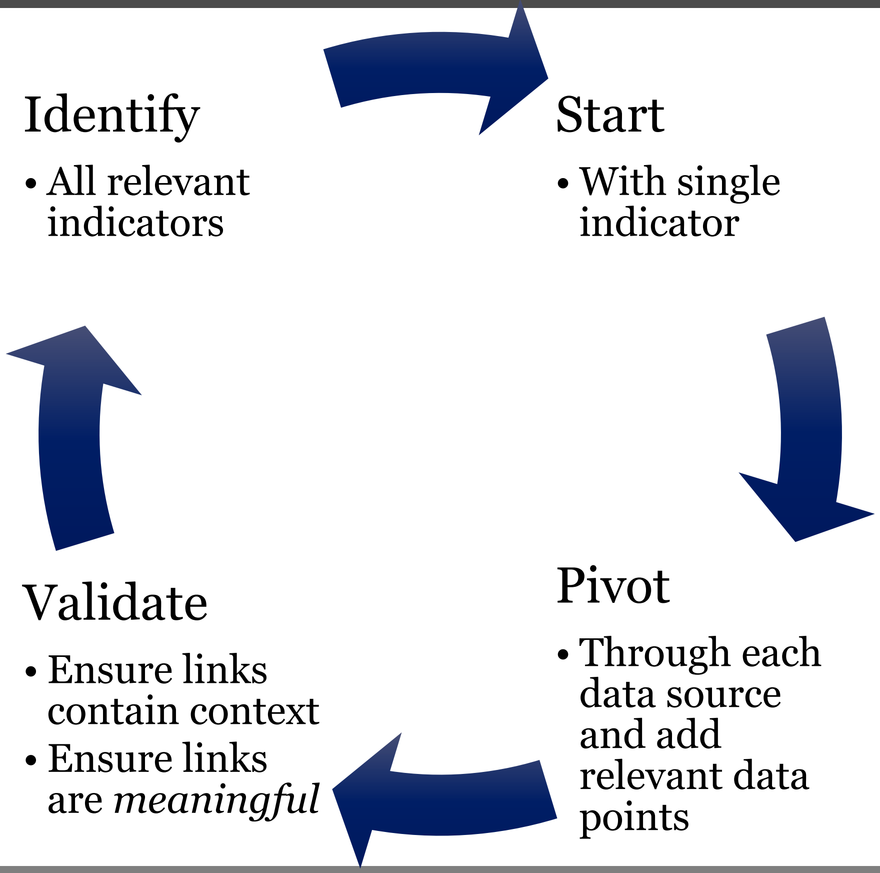
## Malware Collection

- Historically, public threat intelligence reports have been malware reports
  - Strong focus on malware analysis in the community
  - Can be misleading as a sole source of collection, but highly valuable

# Malware Zoos

- Leveraged by organizations as a free malware sandbox
  - Makes the data available to others, *including adversaries*
- Some popular sites:
  - VirusTotal
  - Hybrid-Analysis
  - Joe Sandbox
- Can create your own
- Useful as a CTI collection source

# Domains: Data Pivoting



## Start

- With single indicator

## Pivot

- Through each data source and add relevant data points

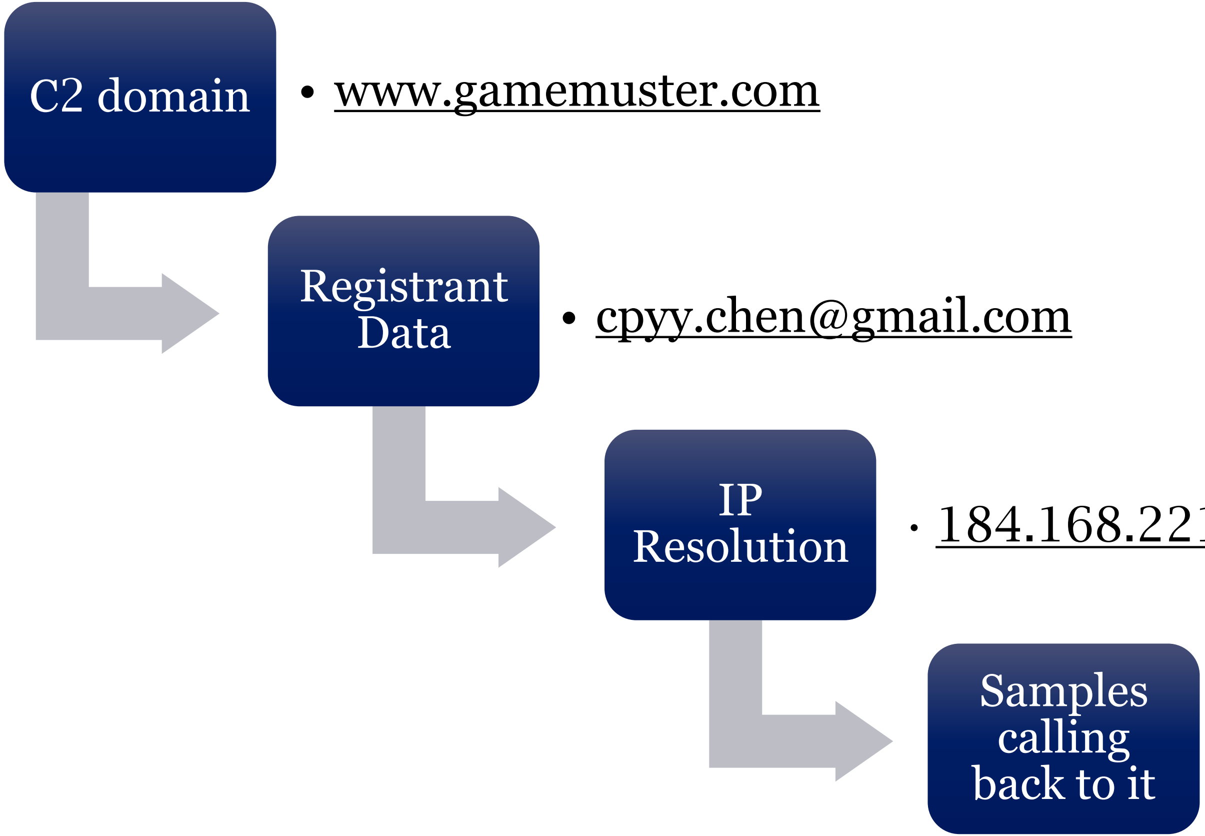
## Validate

- Ensure links contain context
- Ensure links are *meaningful*

## Identify

- All relevant indicators

# Data Pivoting: Example



C2 domain

- www.gamemuster.com

Registrant Data

- cpyy.chen@gmail.com

IP Resolution

- 184.168.221.96

Samples calling back to it

- [MD5 1]
- [MD5 2]

# Beware of the “Kevin Bacon” effect

# External Data Sets: Threat Data Feeds

- Usually exist in the form of IP addresses, digital hashes, filenames, and other Atomic and Computed threat indicators
- Key aspects to watch for:
  - Where is the data coming from?
  - Is the threat data applicable to the type of threats your organization cares about?
  - How is the threat data going to be used?
- Highly trusted sources' threat data can be plugged directly into many organization's security architecture to actively identify or block validated threats, but **be cautious**

# Measuring Threat Feeds

+

- Pivots into higher-order context (blog/report)

- Is focused on your industry or threats

- Has well-articulated understanding of the Collection Management Framework feeding it

- Openly values quality and accuracy over quantity and speed

−

- Ever contains RFC 1918 addresses or public trusted domains like Microsoft.com

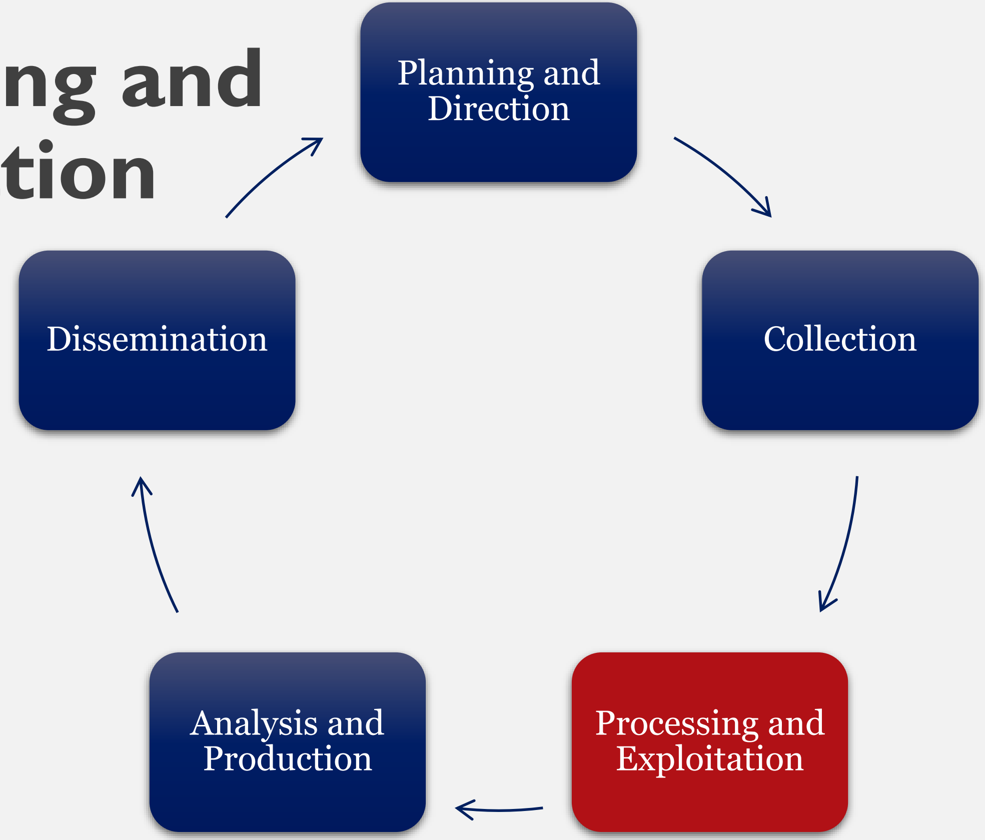
- No context behind info

- Expectation is plug and play

# TLS Certificates

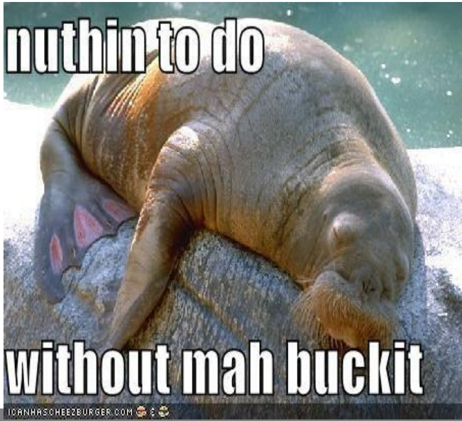
- A digital certificate used in secure host-to-host network communications (previously called SSL)
- Collections of TLS certificates (free/paid options):
  - Censys.io
  - Scans.io
  - Circl.lu
  - PassiveTotal
- Can be used to find C2 infrastructure

# Processing and Exploitation

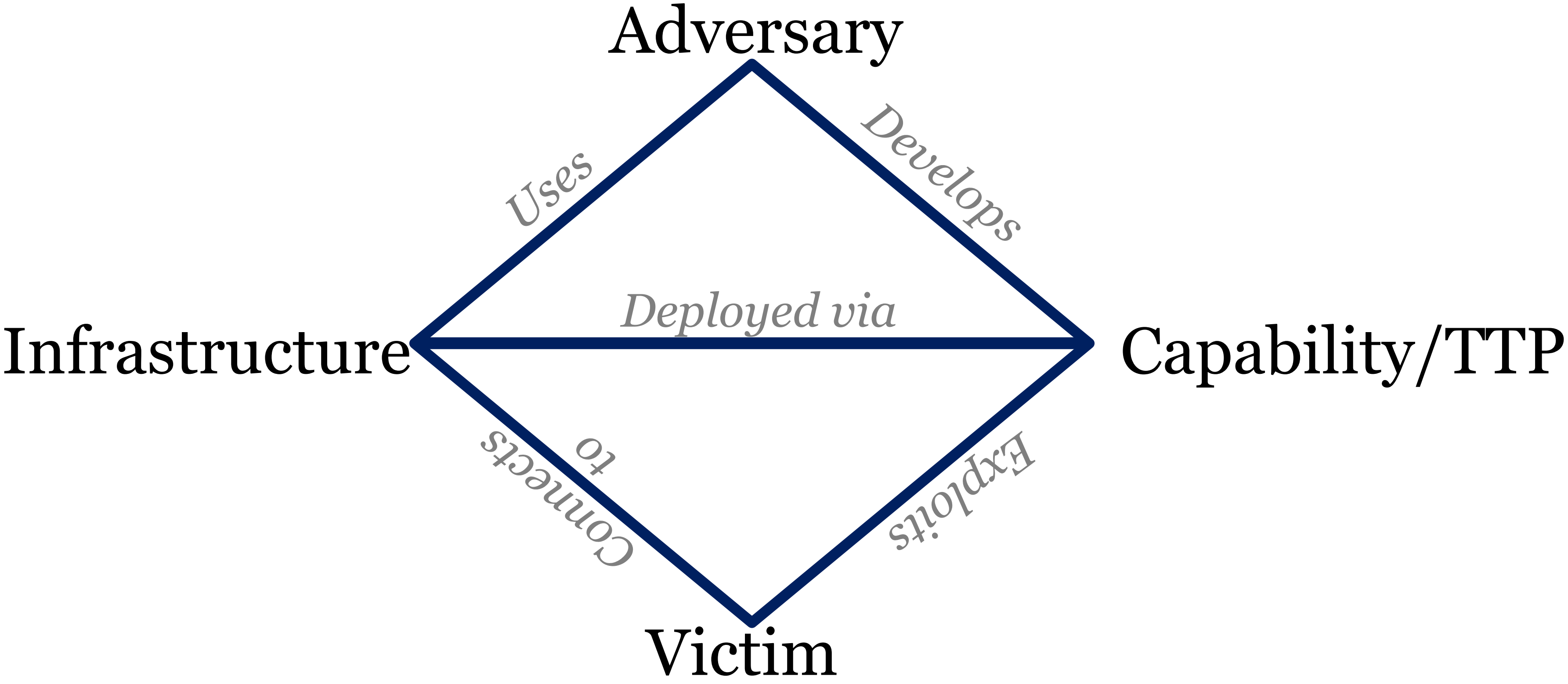


# Structured Models: Data into Buckets

- Structured models are useful to analysts for many reasons, but a chief reason is simply: data into buckets
  - Allows for the abstraction of the analyst and identification of patterns
  - Kill Chain, Diamond Model, MITRE ATT&CK, VERIS

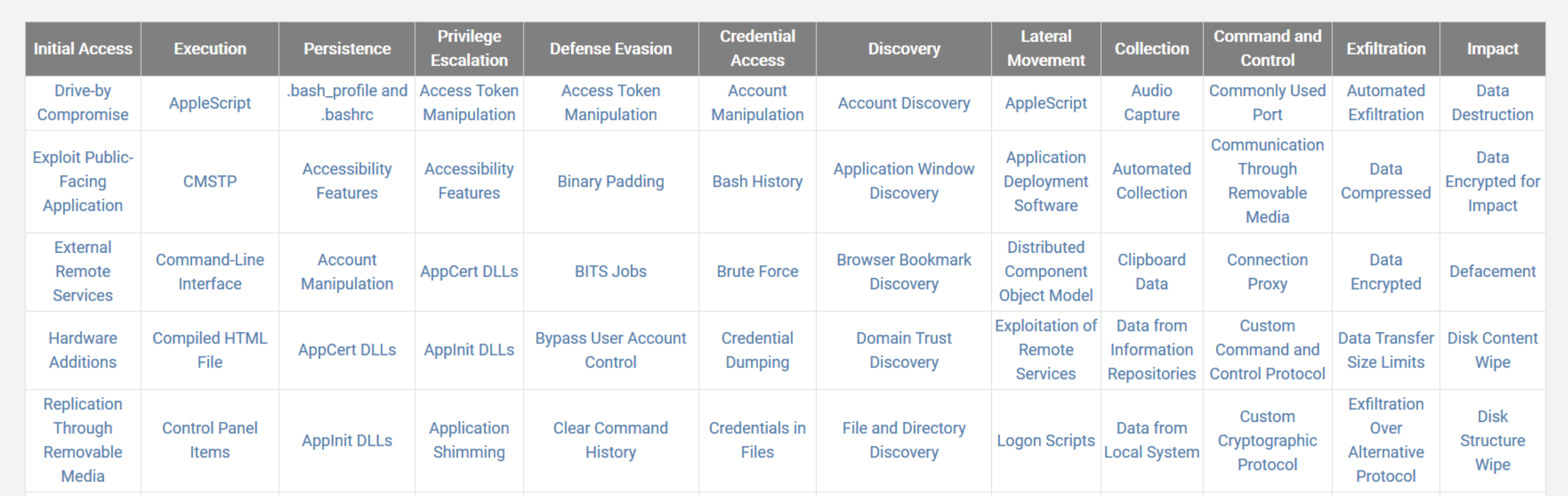


# The Diamond Model



# MITRE ATT&CK™

- MITRE's ATT&CK is a documentation of tactics and techniques
  - A useful framework for expressing and documenting tactics and techniques
  - Supported by MITRE and contributed to through many in the community
  - Focuses on tactics and techniques that have been observed in the real world



| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Commonly Used Port | Automated Exfiltration | Data Destruction |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | Binary Padding | Bash History | Application Window Discovery | Application Deployment Software | Automated Collection | Communication Through Removable Media | Data Compressed | Data Encrypted for Impact |
| External Remote Services | Command-Line Interface | Account Manipulation | AppCert DLLs | BITS Jobs | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Connection Proxy | Data Encrypted | Defacement |
| Hardware Additions | Compiled HTML File | AppCert DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | Domain Trust Discovery | Exploitation of Remote Services | Data from Information Repositories | Custom Command and Control Protocol | Data Transfer Size Limits | Disk Content Wipe |
| Replication Through Removable Media | Control Panel Items | AppInit DLLs | Application Shimming | Clear Command History | Credentials in Files | File and Directory Discovery | Logon Scripts | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Alternative Protocol | Disk Structure Wipe |

# Storing Collected Intel

- Often discussed in the context of “threat intelligence platform”
- The focus is on storing information in a quickly accessible and useful format
- Pros and cons to each
  - Consider your requirements!

# Storing Platforms

Open Source

- CRITS
- MISP
- Threat_Note
- YETI

Pros: Free, ample storage, open source sharing communities

Cons: Difficult to implement and maintain

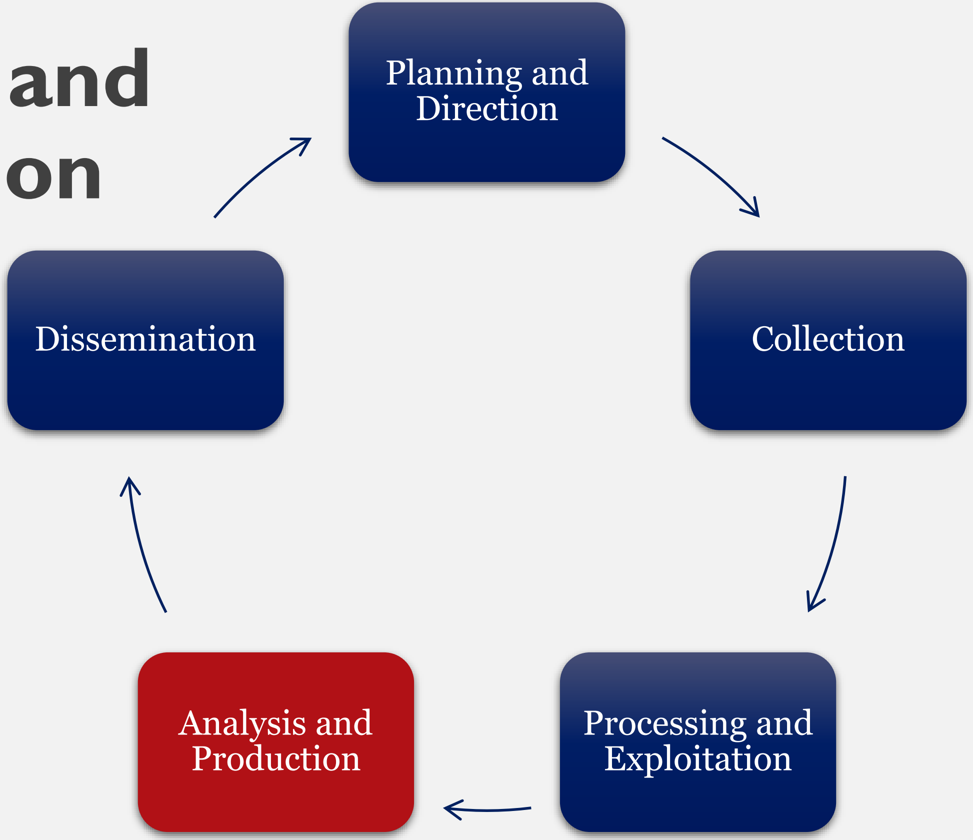
Commercial

- Many options!

Pros: Fully supported, ease of installation, integration with other tools, data analytics

Cons: Can be pricey, may not fit established workflows

# Analysis and Production



# Identifying and Defeating Bias

- All analysts have bias
- Cognitive biases are constraints on how we as analysts think that influence incorrect decisions, assessments, or rationale
- They allow analysts to create their own version of reality where inaccurate judgments and illogical interpretations occur

# Confirmation Bias

## Selectively Supporting One Hypothesis

## Evidence Inclusion

- Seek supporting evidence
- Reject refuting evidence

## Significance Biasing

- Greater significance to supporting data
- Lesser significance to contradicting data

# Structured Analytic Techniques

- Structured analytic techniques (SATs) are analyst approaches to better evaluate information while reducing the impact of bias
  - Analysts leverage models to abstract data as much as possible from ourselves

## Sample SATs

- Analysis of Competing Hypotheses
- Devil’s Advocacy
- Team A/Team B
- Brainstorming
- Red Team Analysis

# Leveraging Different Types of Analysis

## Know Thyself

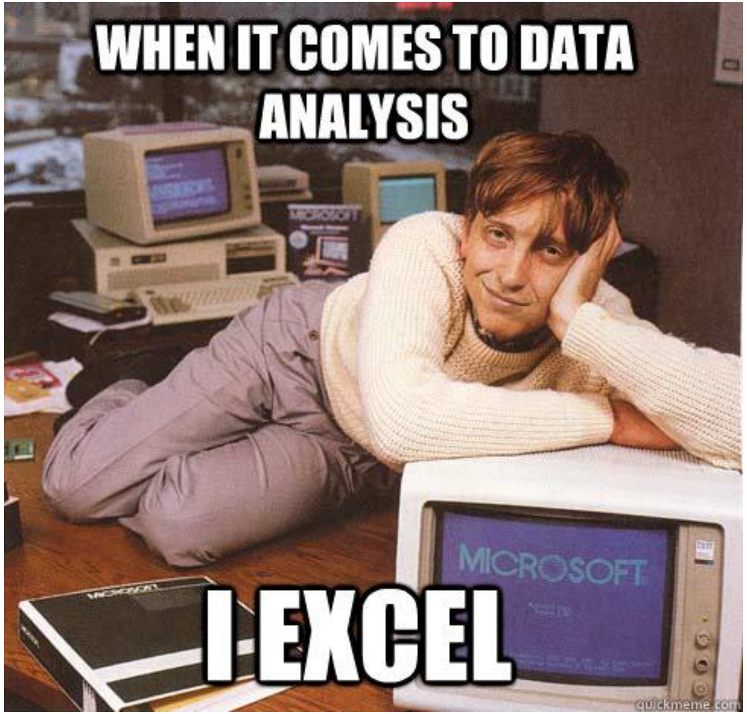
- Everyone has a favorite type of analysis for given situations
- Learn what analysis types facilitate your process

## Know the Team

- Learn your team members' analysis types
- Ensure your tools and approaches play to everyone's strengths

## Inject New Approaches

- Try new types of analysis, especially on critical cases
- Ensure you do not only leverage one type of analysis

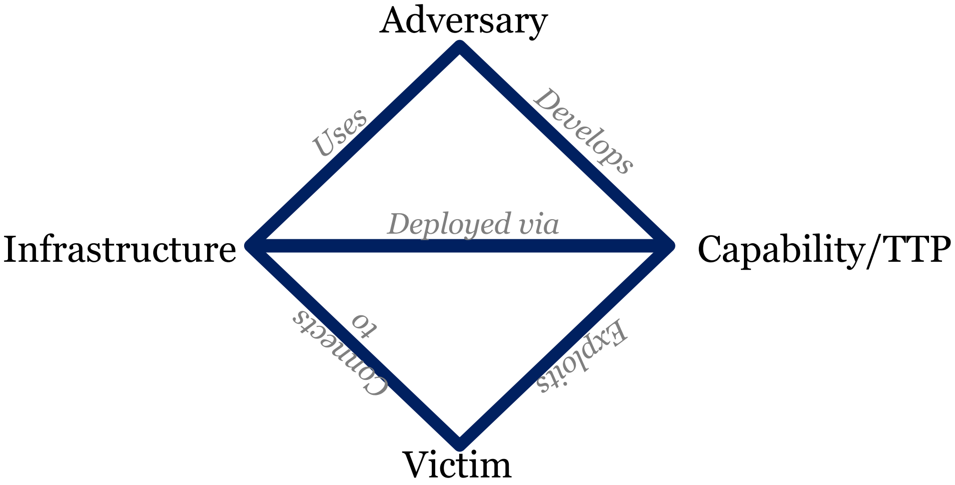


## Analysis: Correlating Clusters

- Many terms for clusters:
  - Threat actors
  - Activity groups
  - Campaigns
  - Intrusion sets
- Different methodologies to do this

# Activity Groups

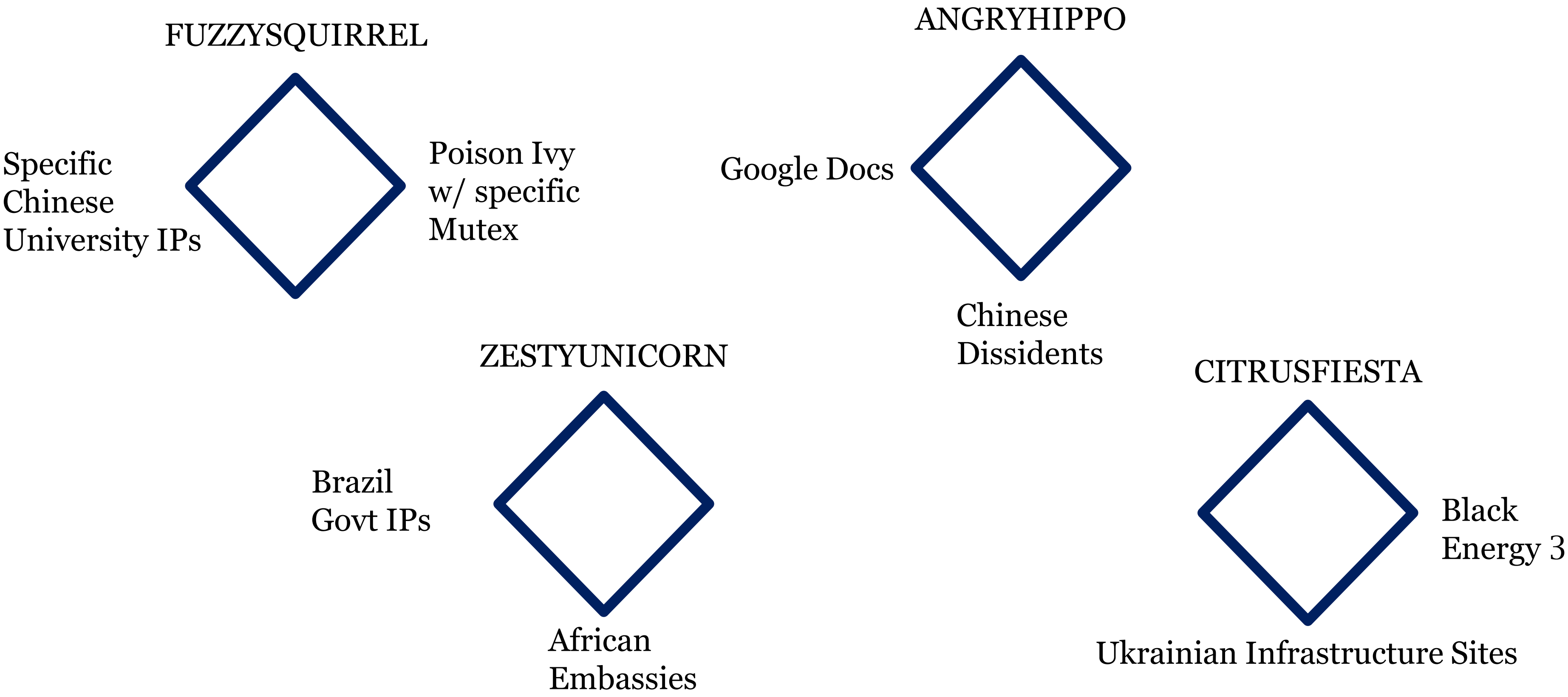
- Concept introduced in the "Diamond Model of Intrusion Analysis" paper by Sergio Caltagirone, Andrew Pendergast, and Chris Betz
- Activity Groups are unique clusters of intrusions mathematically defined by the analyst/team's analytical weighting (confidence scoring)



# Shortcut: The Rule of 2

- One shortcut to clustering is simply applying the Diamond Model
  - Look for overlaps between two vertices in intrusions or campaigns
- The goal is to identify unique characteristics
- Map the unique characteristics to the Diamond Model

# Rule of 2: Forming an Activity Group



FUZZYSQUIRREL

Specific Chinese University IPs

Poison Ivy w/ specific Mutex

ANGRYHIPPO

Google Docs

Chinese Dissidents

ZESTYUNICORN

Brazil Govt IPs

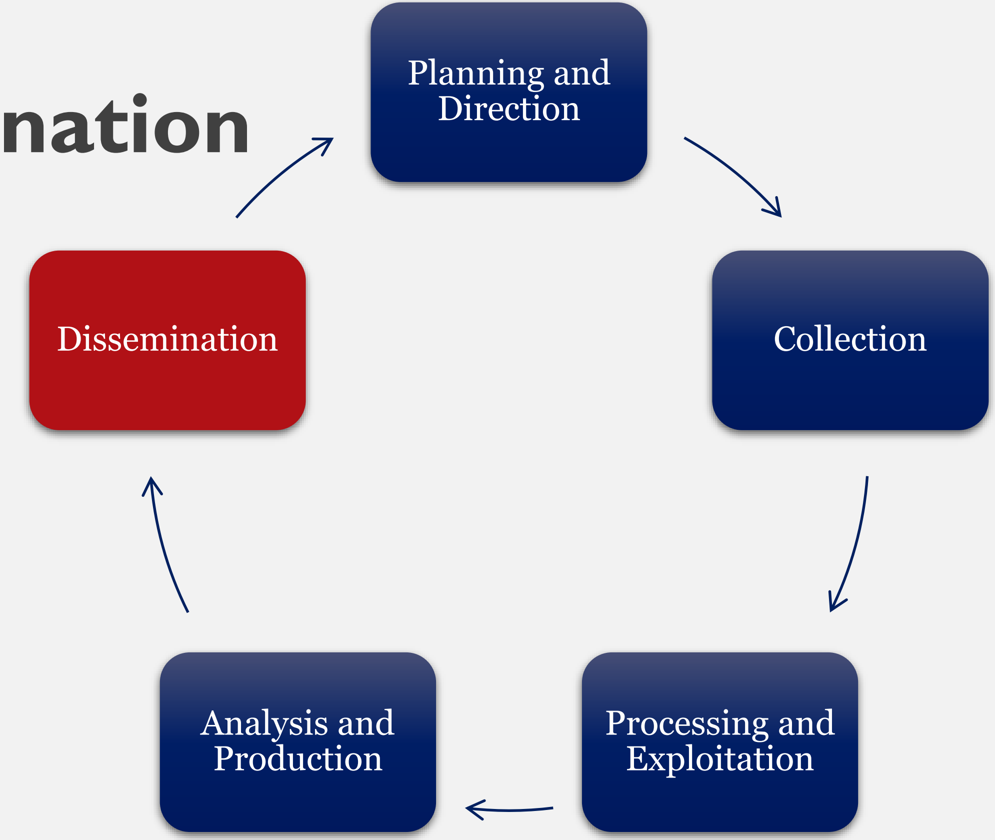
African Embassies

CITRUSFIESTA

Black Energy 3

Ukrainian Infrastructure Sites

# Dissemination



# Know the Audience

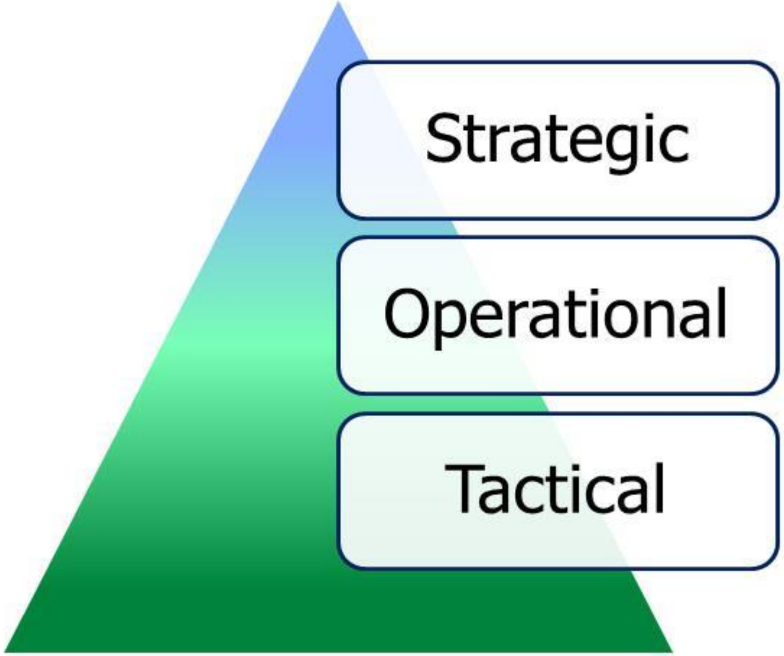
- #1 key to sharing threat intelligence:
  Know your audience

- The audience shapes the delivery:
  - Different audiences have different intel needs
  - Different audiences require data in different formats

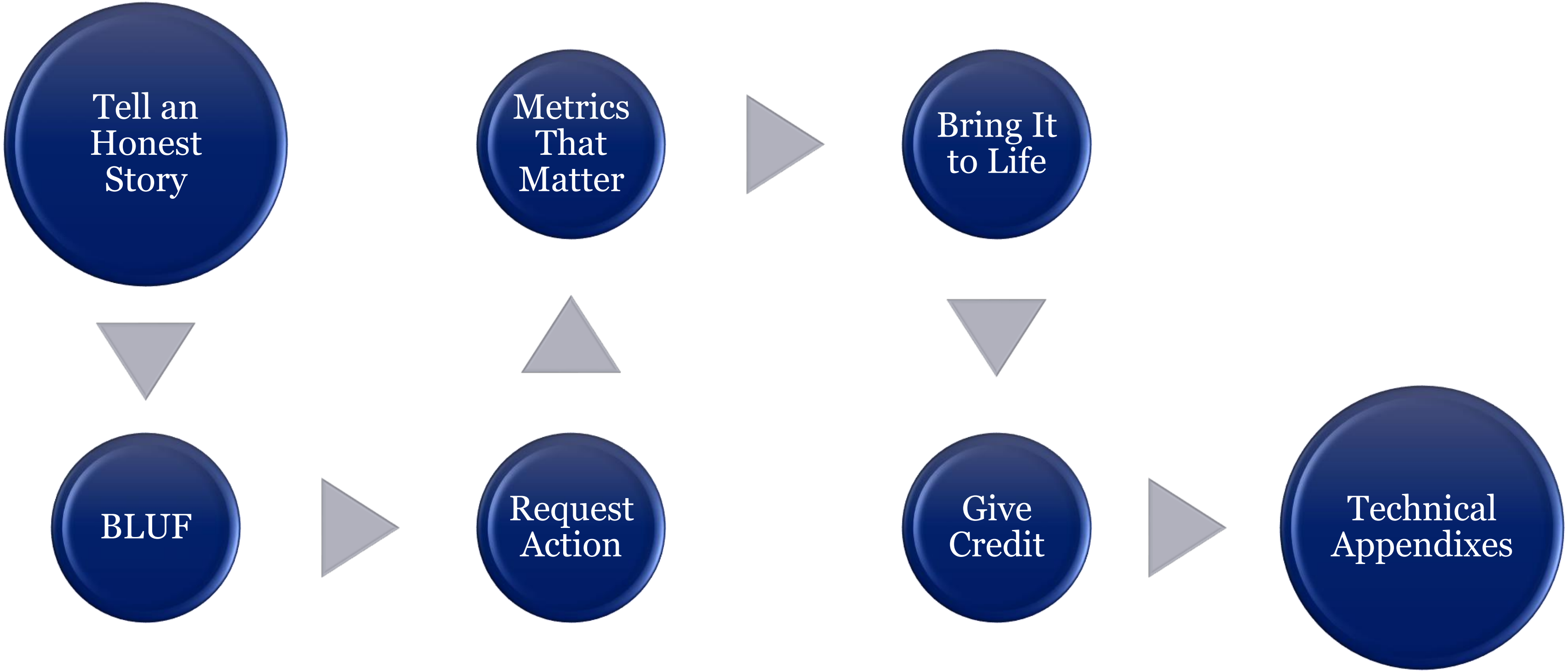
Pretty pictures and maps on an SOC operations screen are usually more for visitors than the SOC analysts

# Intended Audience

The intended audience and their goals determine the type of threat intelligence generated and how it is to be used



# Tips on Effective Report Writing



Tell an Honest Story

BLUF

Request Action

Metrics That Matter

Bring It to Life

Give Credit

Technical Appendixes

# Constructing Assessments

- Can be viewed as an equation

Assessment =
confidence + analysis + evidence + sources

- We assess with <insert confidence> that <insert assessment> because of <insert evidence> <insert sources>

# Confidence Assessments

**High Confidence**

- Supported by preponderance of evidence
- No evidence against
- All but certain

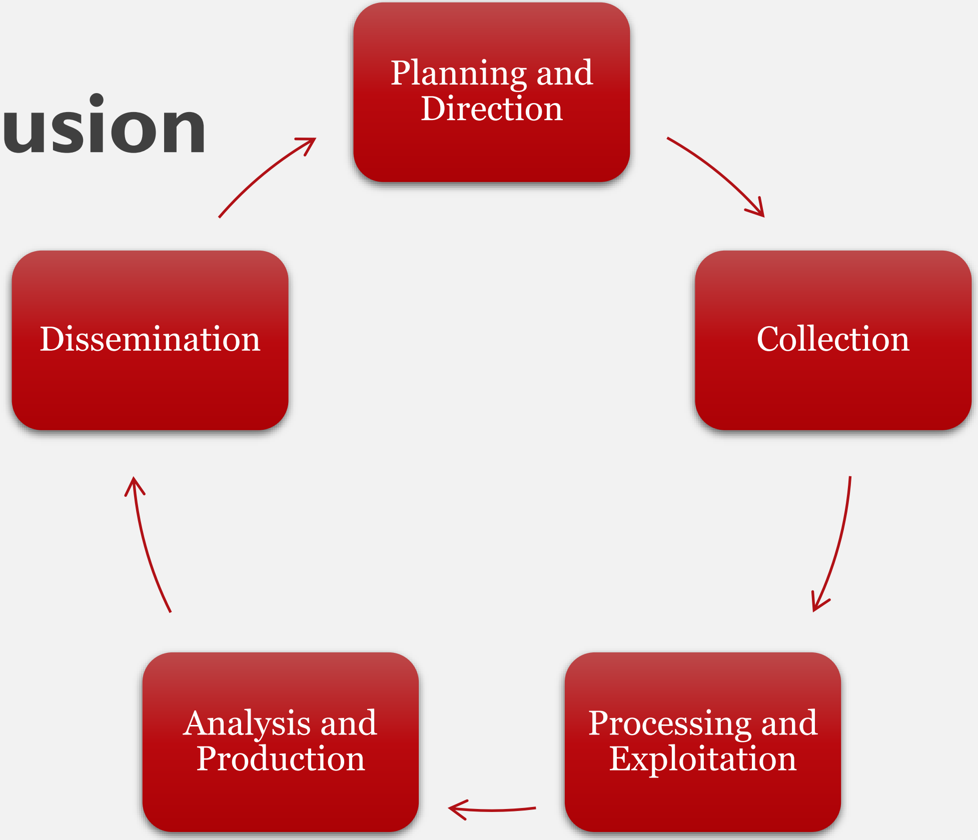
**Moderate Confidence**

- Significant evidence missing
- New evidence could invalidate

**Low Confidence**

- Other equally likely hypotheses exist
- Little evidence available to support

# In Conclusion



Planning and Direction

Collection

Processing and Exploitation

Analysis and Production

Dissemination

Washington, DC

SUMMIT: Jan 20-21

TRAINING: Jan 22-27

# SANS DFIR CYBER THREAT INTELLIGENCE

## SUMMIT & TRAINING

CALL FOR PRESENTATION NOW OPEN

sans.org/CTI-Summit

# Upcoming Live Offerings of FOR578

**September**

- Las Vegas, NV
- Dallas, TX* (with Katie)

**October**

- New Orleans, LA

**November**

- Sydney, Australia
- Coral Gables, FL

**December**

- San Francisco, CA* (with Katie)

**sans.org/ FOR578**

**Katie Nickels (@LiketheCoins)**

# SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

FOR500
**Windows Forensics**
GCFE

FOR518
**Mac and iOS Forensic Analysis and Incident Response**

FOR526
**Advanced Memory Forensics & Threat Detection**

FOR585
**Advanced Smartphone Forensics** GASF

## OPERATING SYSTEM & DEVICE IN-DEPTH

## INCIDENT RESPONSE & THREAT HUNTING

FOR508
**Advanced Incident Response and Threat Hunting** GCFA

FOR572
**Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response** GNFA

FOR578
**Cyber Threat Intelligence**
GCTI

FOR610
**REM: Malware Analysis**
GREM

SEC504
**Hacker Tools, Techniques, Exploits, and Incident Handling** GCIH

@sansforensics

sansforensics

dfir.to/DFIRCast

dfir.to/gplus-sansforensics

dfir.to/MAIL-LIST