JSAC2025

Joint Security Analyst Conference

Follow the Clues

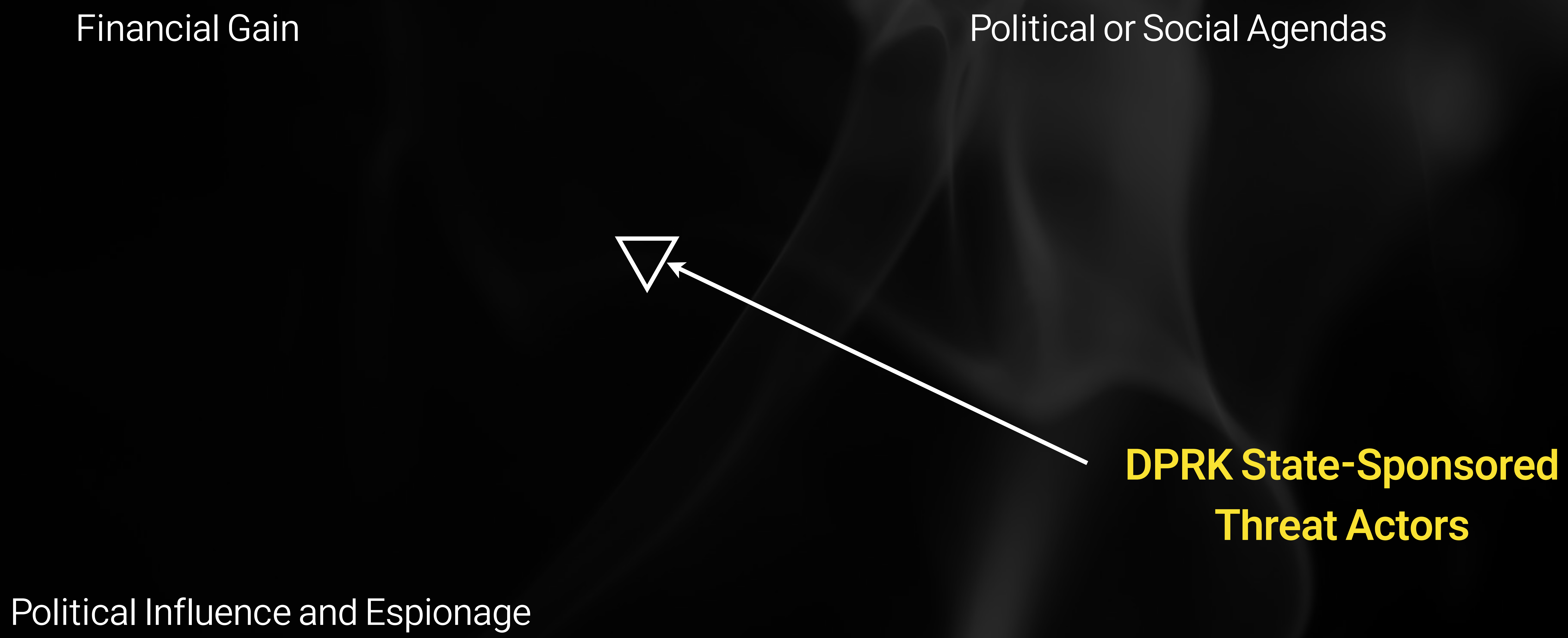
Everyday is lazarus.day

2025-01-21

JeongGak Lyu @lazarusholic

금융보안원
FINANCIAL SECURITY INSTITUTE

The Evolving Threat Landscape



Financial Gain

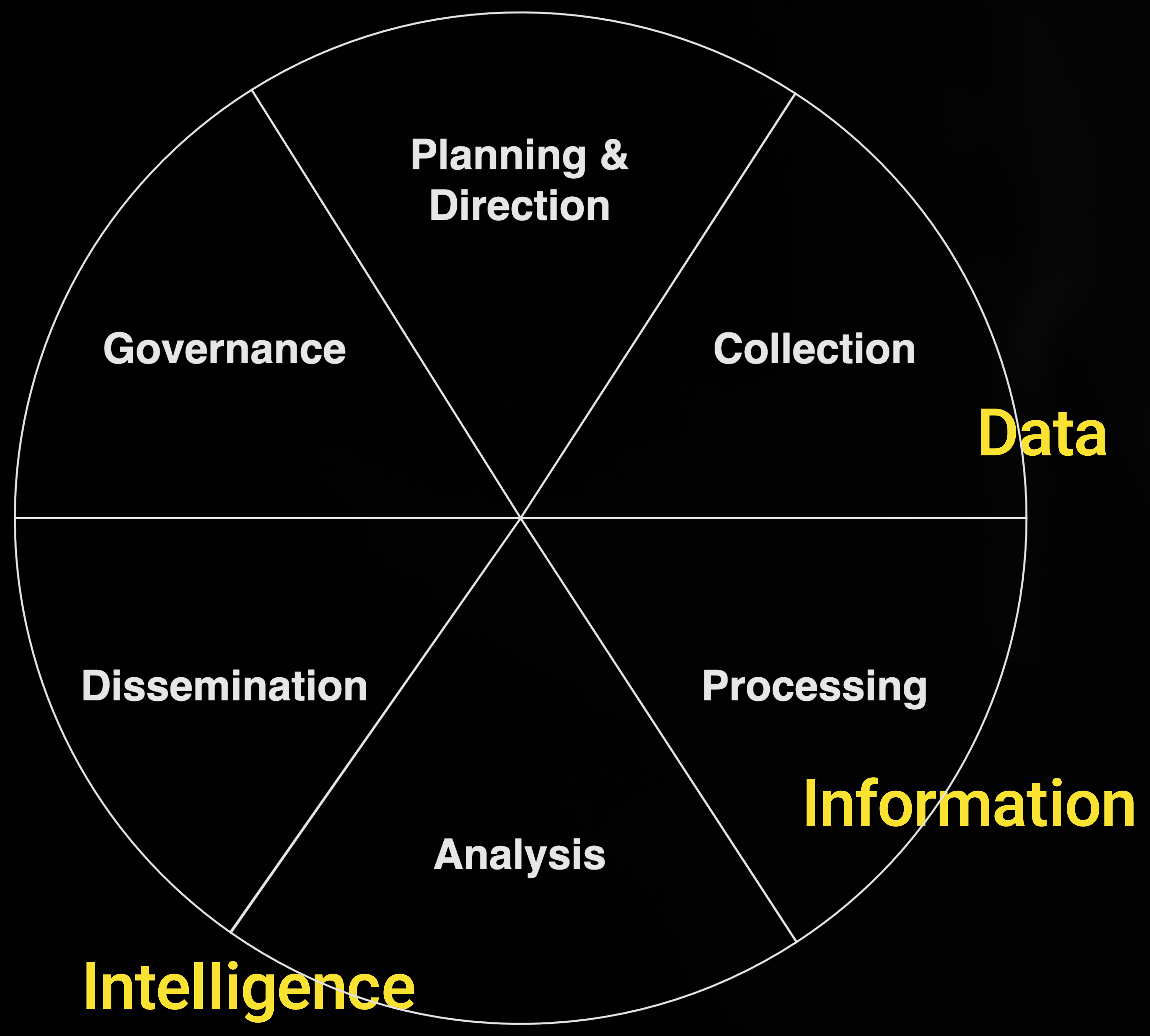
Political or Social Agendas

Political Influence and Espionage

DPRK State-Sponsored Threat Actors

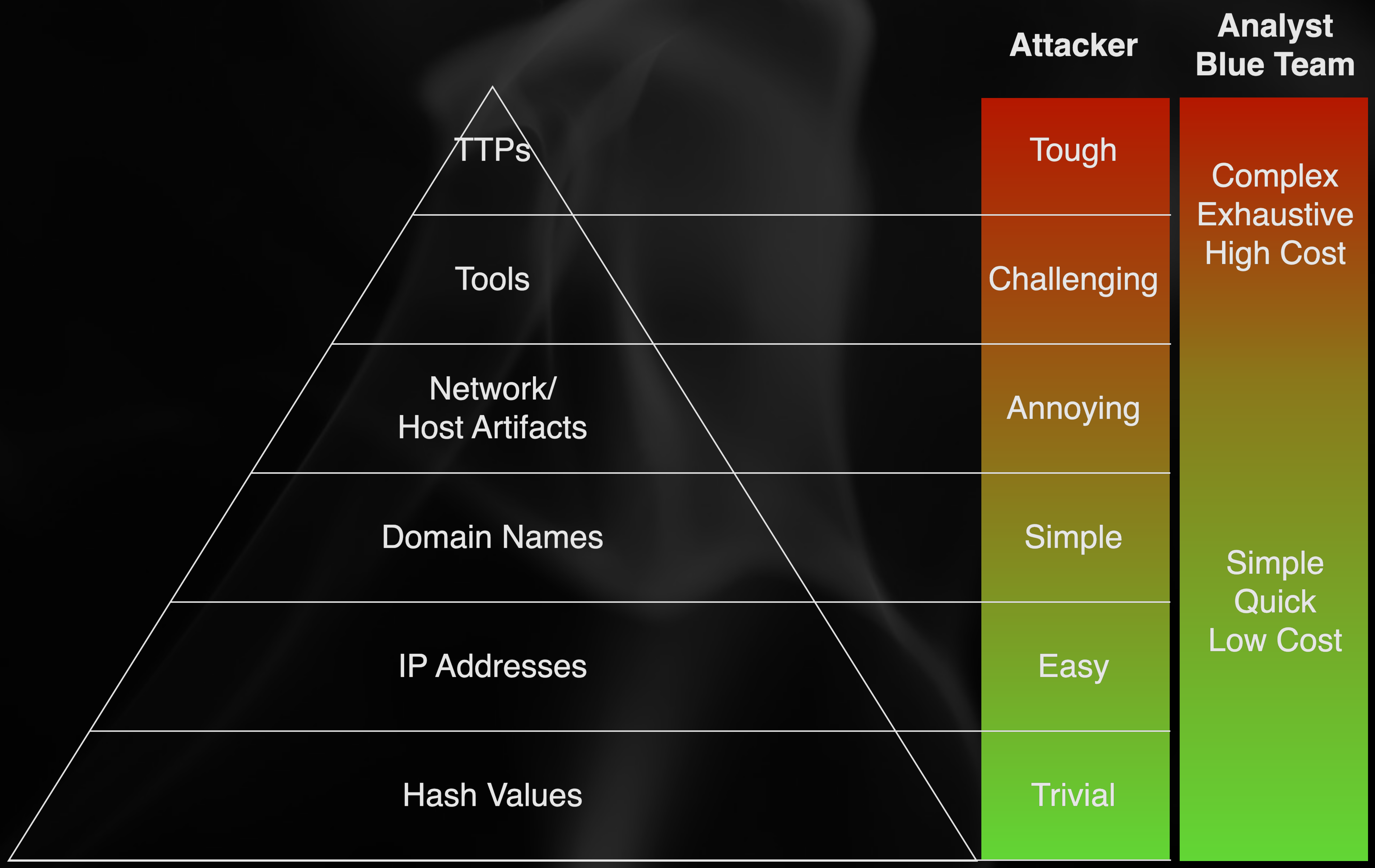
Cyber Threat Intelligence Essentials

CTI Lifecycle



https://www.gartner.com/document-reader/document/4056399

The Pyramid of Pain



https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

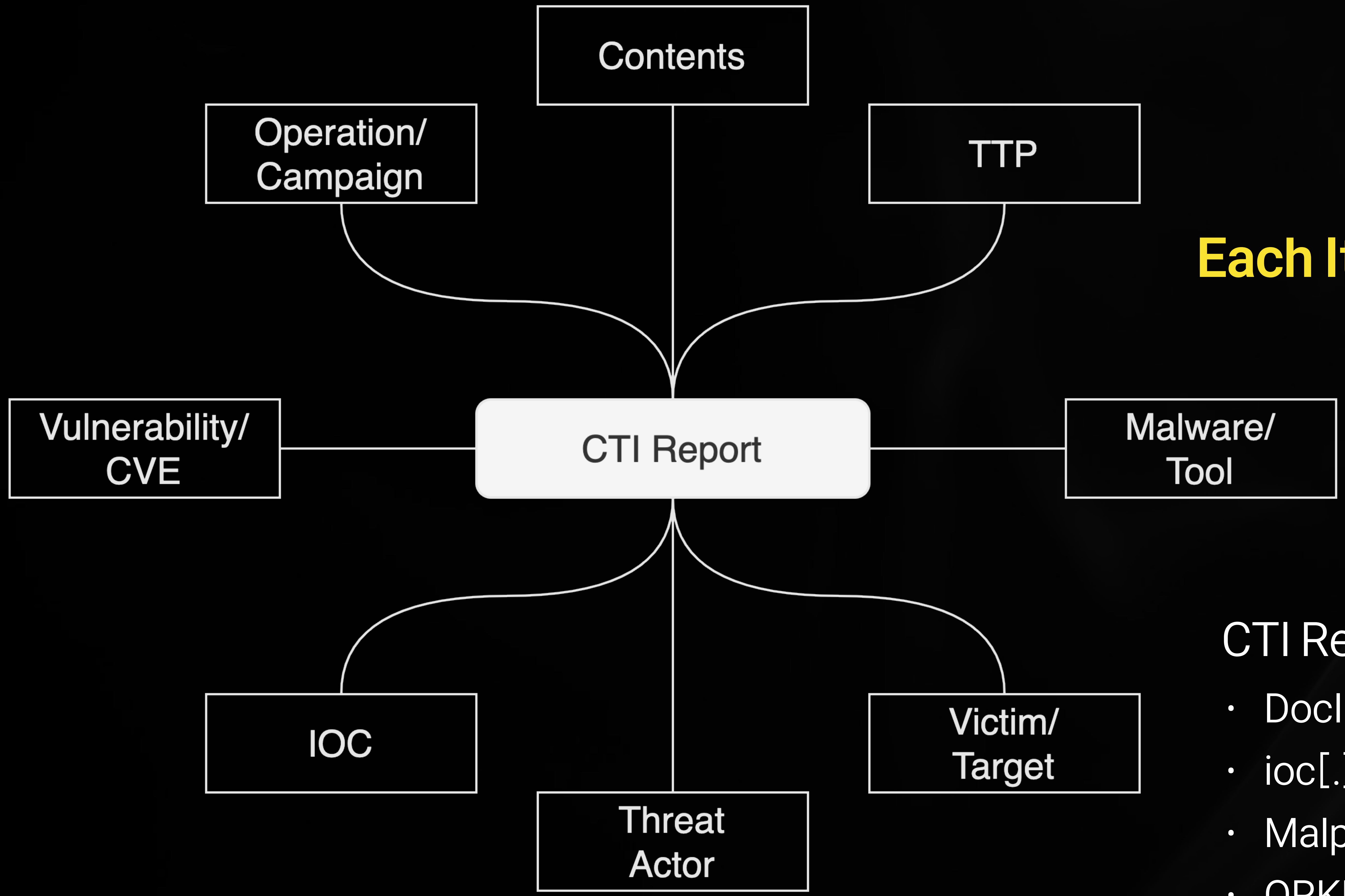
Threat Detection & Threat Hunting

Reactive Approach
Focus on Known Threats
Detecting Evil

Proactive Approach
Targets Unknown Threats
Searching for Evil

Rely on CTI & IOCs
Mitigating Threats

Inside a CTI Report

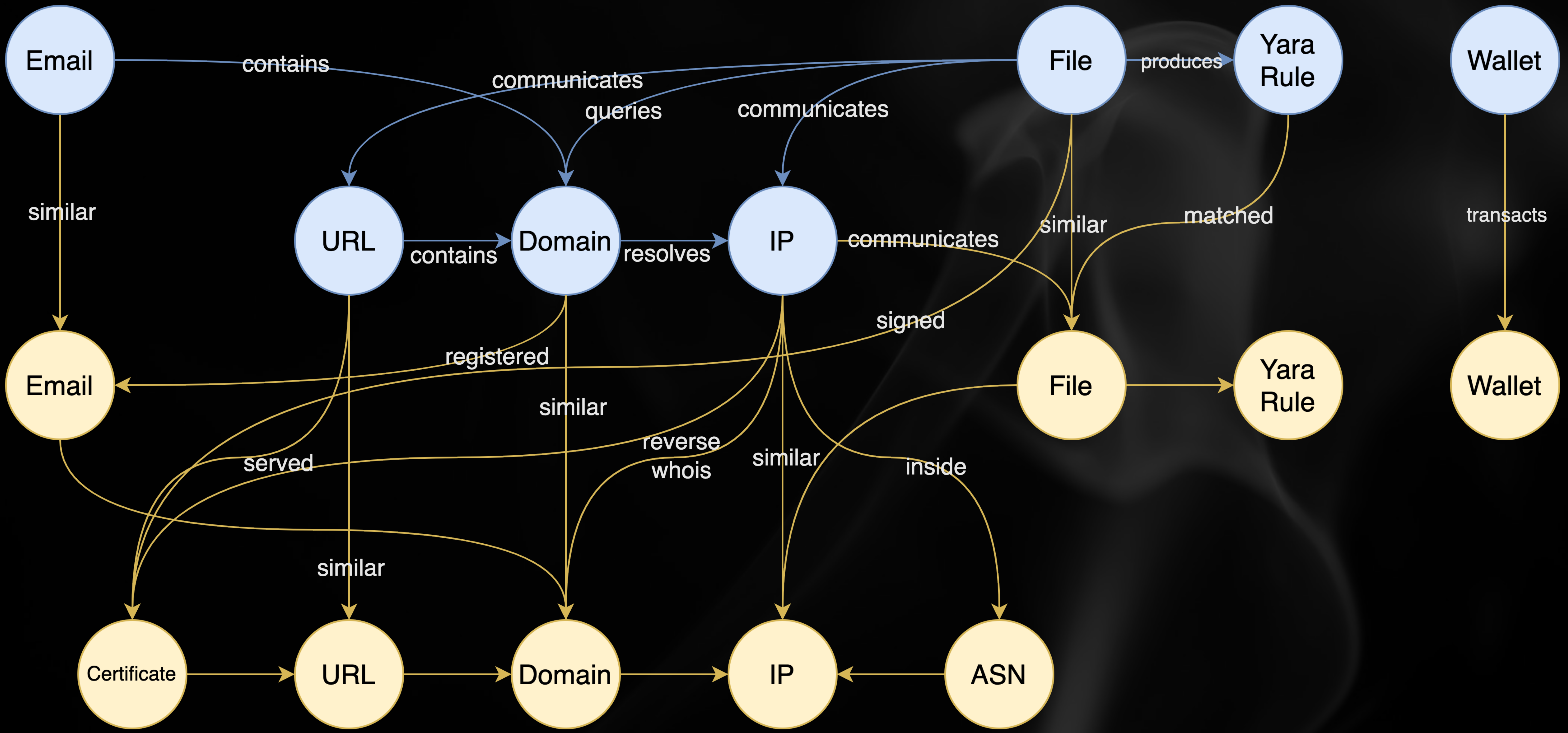


Each Item can be a Clue

CTI Report Collections & Platforms

- DocIntel https://docintel.org/
- ioc[.]one https://ioc.one/
- Malpedia https://malpedia.caad.fkie.fraunhofer.de/
- ORKL https://orkl.eu/
- Threat Intelligence Reports https://mthcht.github.io/ThreatIntel-Reports/
- Vx Underground https://vx-underground.org/

IOC Pivoting / Enrichment



IOC Pivoting with OSINT

Similarity
User Agent
Subject
Common Name
Email
File
Yara Rule
Certificate
AilenVault
AnyRun
Censys
Criminal IP
CTX
GreyNoise
Hybrid Analysis
Intezer
Joe Sandbox
Malware Bazaar
OpenTIP
Pulsedive
Shodan
SSLBL
ThreatFox
Triage
URL DNA
URLHaus
URLScan
Validin
VirusTotal
YARAify
ZoomEye
ASN
IP
Domain
URL
Finger-prints
Whois
Reverse Whois
Registrant
Registra
Similarity
Whois History
Favicon
Path
Response

Introduction to lazarus.day

Reports

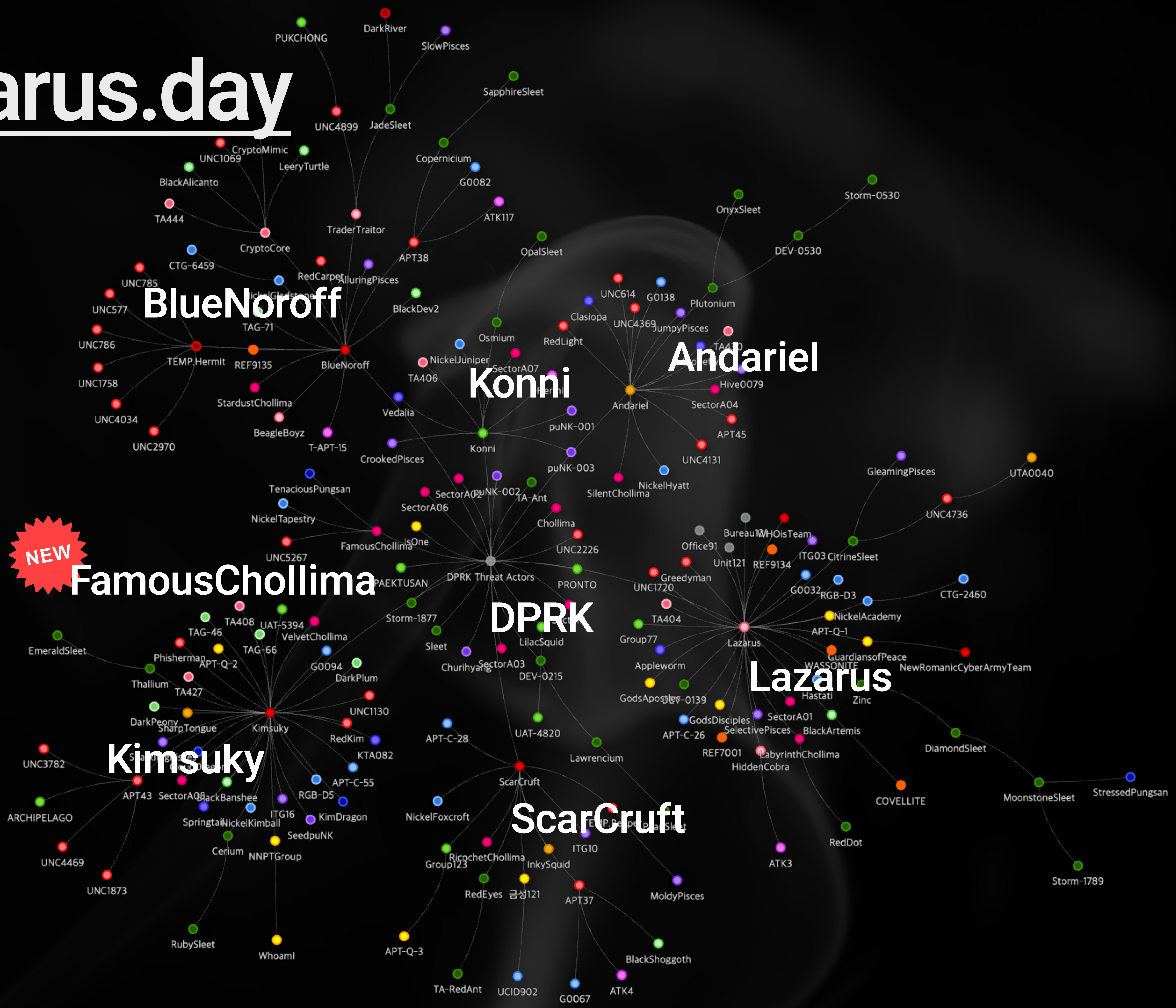
2,470

Incidents

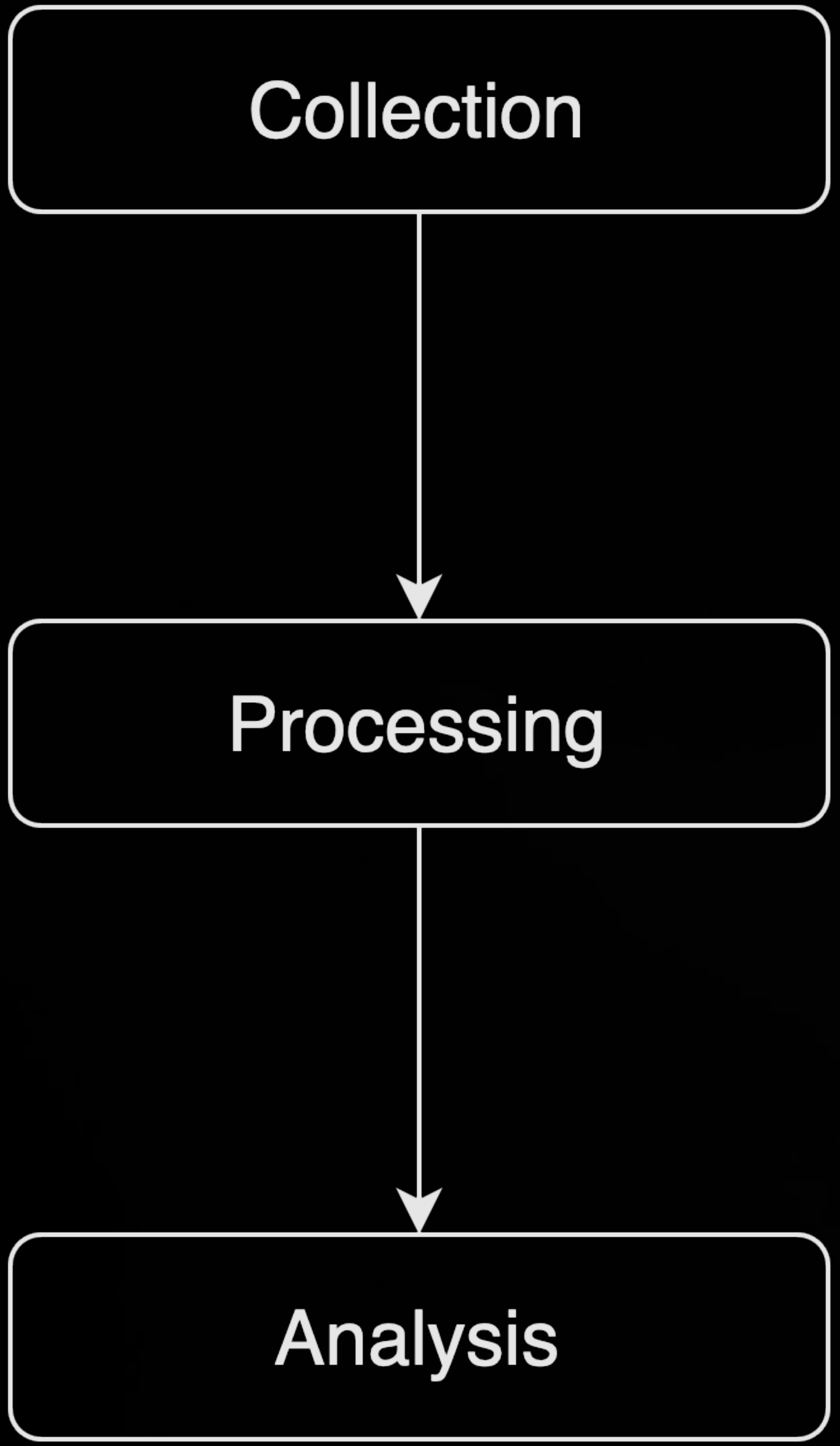
187

Actors

187



Everyday is lazarus.day



Collection

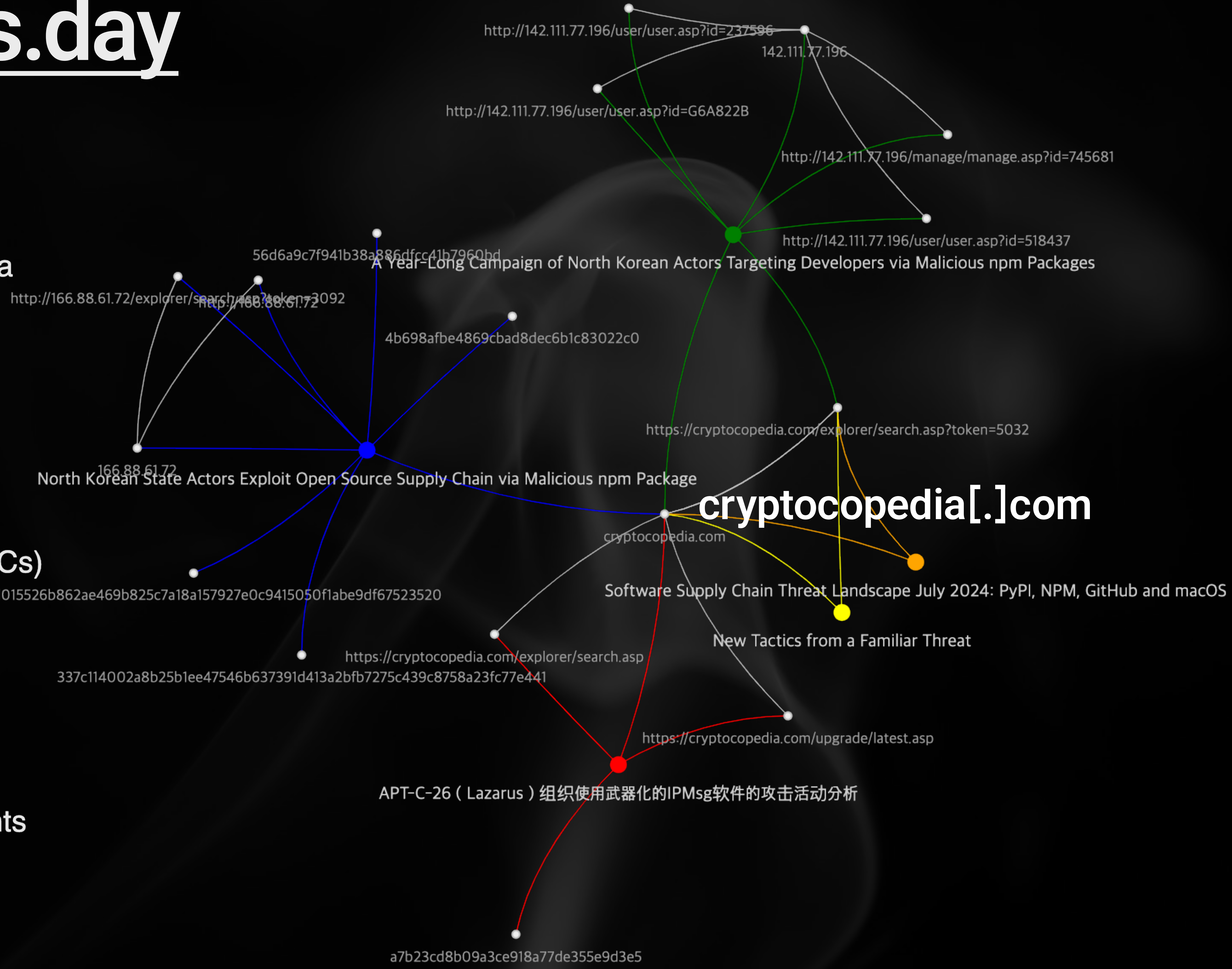
- Monitor RSS Feeds
- Monitor Social Media
- Monitor News

Processing

- Archive Report
- Extract Contents(IOCs)

Analysis

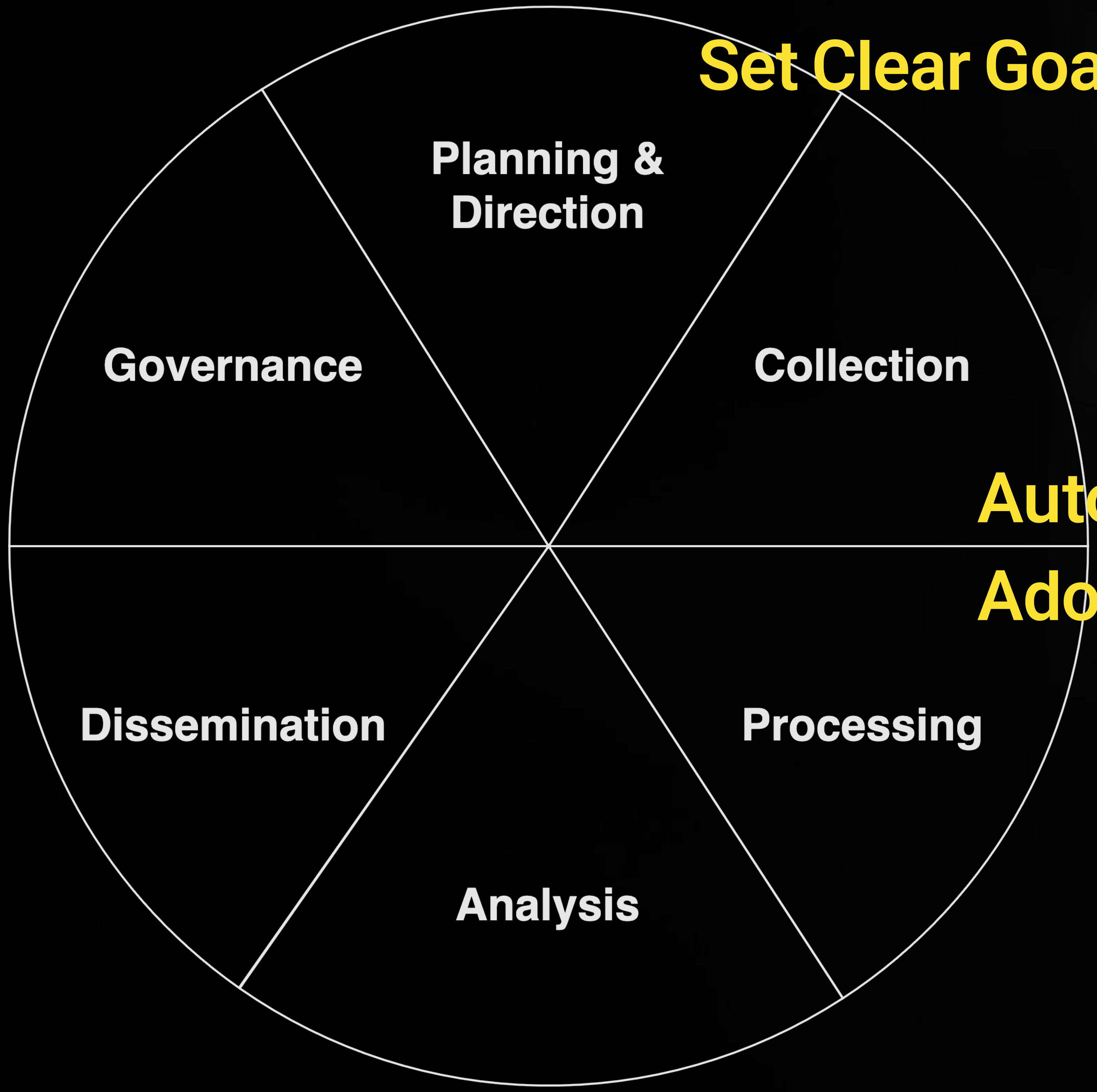
- Summarize Report
- Identify New Actors
- Identify New Incidents
- Manage Tags
- ~~IOCs Pivoting~~


http://142.111.77.196/user/user.asp?id=237596
142.111.77.196
http://142.111.77.196/user/user.asp?id=G6A822B
http://142.111.77.196/manage/manage.asp?id=745681
http://142.111.77.196/user/user.asp?id=518437
56d6a9c7f941b38a886dfcc41b7960bd
A Year-Long Campaign of North Korean Actors Targeting Developers via Malicious npm Packages
http://166.88.61.72/explorer/search.asp?token=3092
http://166.88.61.72
4b698afbe4869cbad8dec6b1c83022c0
https://cryptocopedia.com/explorer/search.asp?token=5032
166.88.61.72
North Korean State Actors Exploit Open Source Supply Chain via Malicious npm Package
cryptocopedia.com
Software Supply Chain Threat Landscape July 2024: PyPI, NPM, GitHub and macOS
B57b75d015526b862ae469b825c7a18a157927e0c9415050f1abe9df67523520
New Tactics from a Familiar Threat
https://cryptocopedia.com/explorer/search.asp
337c114002a8b25b1ee47546b637391d413a2bfb7275c439c8758a23fc77e441
https://cryptocopedia.com/upgrade/latest.asp
APT-C-26（Lazarus）组织使用武器化的IPMsg软件的攻击活动分析
a7b23cd8b09a3ce918a77de355e9d3e5

cryptocopedia[.]com

Strategies for Enhanced Threat Intelligence

CTI Lifecycle



Set Clear Goals!

Automation, Automation, Automation!

Adopt Generative AI!

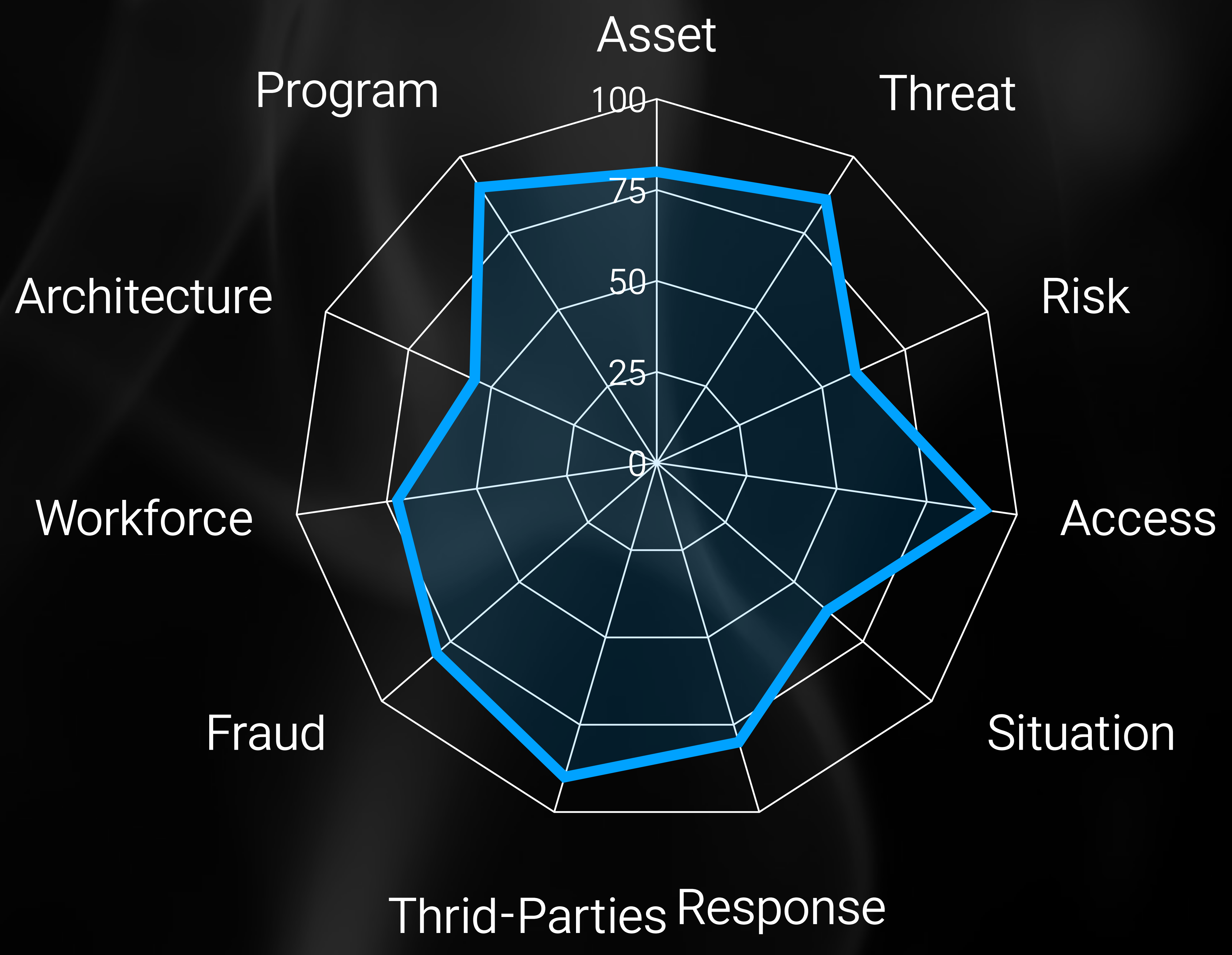
Tools to Spark Ideas

- Harpoon https://github.com/Te-k/harpoon
- IntelOwl https://intelowlproject.github.io/
- Censeye https://github.com/Censys-Research/censeye
- SecAI https://secai.ai/
- TI Mindmap https://github.com/format81/TI-Mindmap-GPT

Conclusion

- Following the Clues is an Endless Journey
  - Requires Patience, Expertise and Investment
- Maximize the Use of OSINT
- Evaluate Your CTI Capability Maturity

CTI Capability Maturity Model



https://cti-cmm.org/

JSAC2025
Joint Security Analyst Conference

Q&A

@lazarusholic

https://lazarus.day

금융보안원
FINANCIAL SECURITY INSTITUTE

Background Images: Unsplash Marek Piwnicki