Customizing Reports: Researcher to CISO

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

@jareddemott www.vdalabs.com

Overview

Recap

Reporting

- Data
- Written

Tesla fix?

- Yes, for versions 1-2
- 3-4, not so much
  - Key destroyed in memory
    - Kept on the server side and delivered *only* after payment

Common malware

A next-gen endpoint protection platform

Initial infection vector

Deobfuscation

Dynamic and static analysis

Reporting

Report Findings

APT1: Exposing One of China's Cyber Espionage Units

This report is focused on the most prolific cyber espionage group Mandiant tracks: APT1. This single organization has conducted a cyber espionage campaign against a broad range of victims since at least 2006.

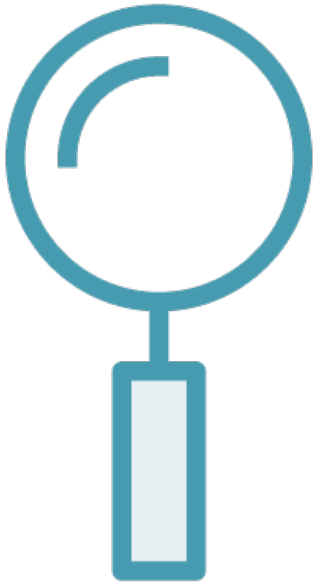
Download Report ▸

Digital Appendix & Indicators

Access more than 3,000 APT1 indicators including domain names, IP addresses, X.509 encryption certificates and MD5 hashes of malware in APT1's arsenal of digital weapons.

Download Appendix ▸

CODE ANALYSIS
Static Analysis (IDA Pro)**:** Strings, CALLs, program flow, loops
Debugging (OllyDbg)**:** Function breakpoints, monitor stack, memory map, plugins for unpacking, find OEP
ANALYSIS SUMMARY
Key Host and Network Indicators of Compromise (IOCs):
Key Functionality:
Purpose:
Persistence:
Environment-specific Impact:
Root Cause:
Attribution:



High level summary

Technical details

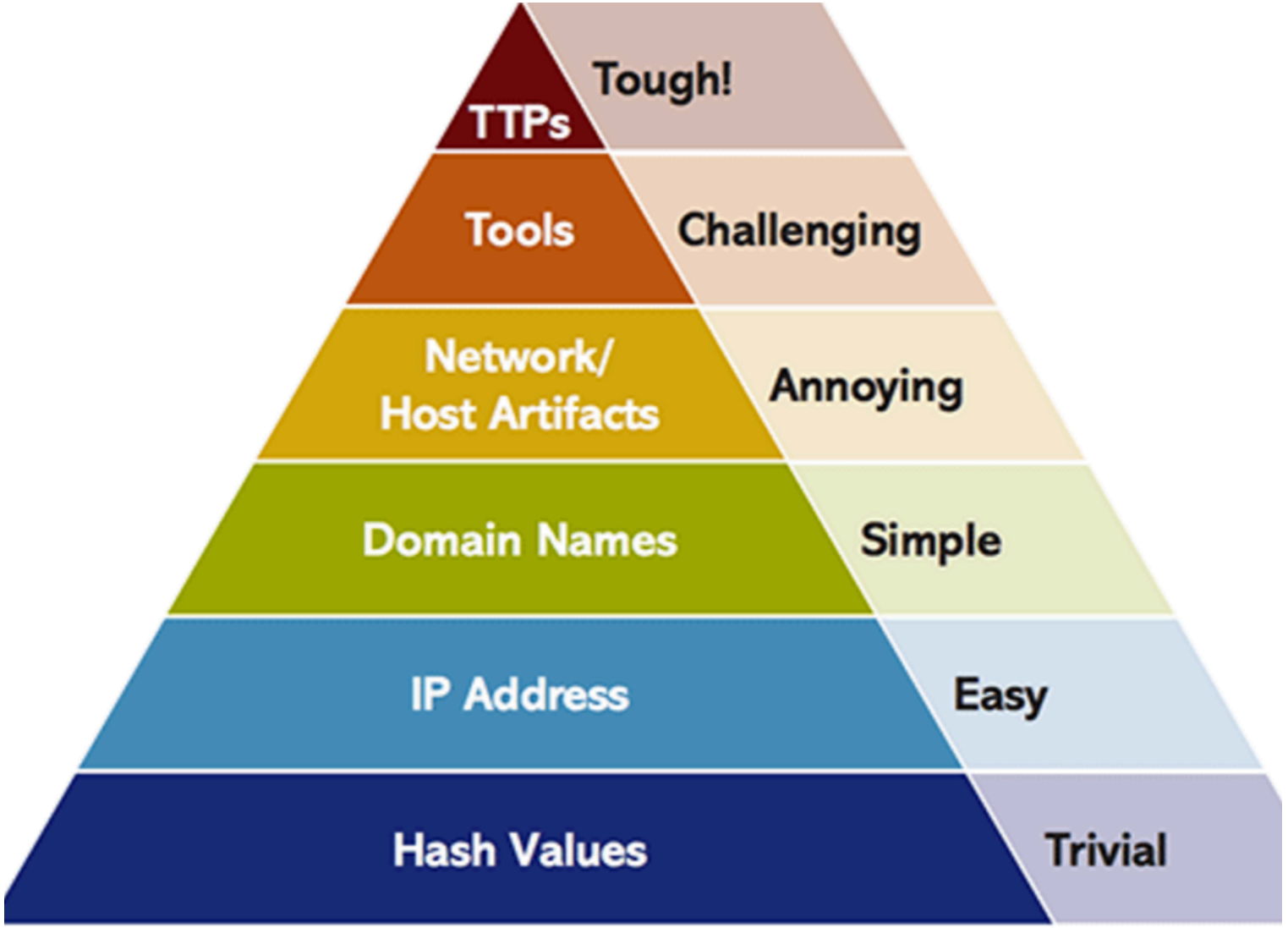
Remediation plan

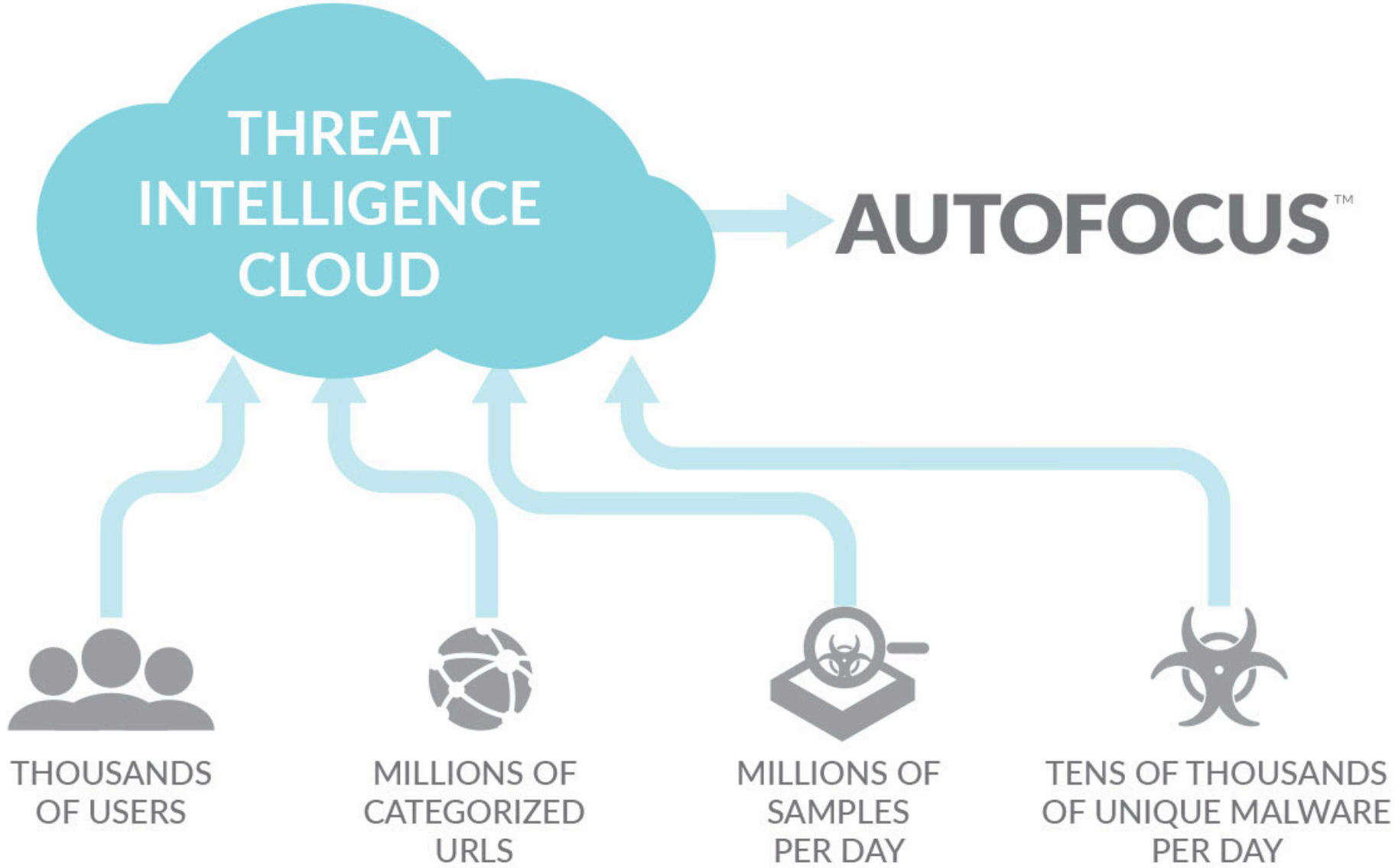
Attribution?

- Five W's

Actionable?

- Integrate into security controls
- Search (IR)



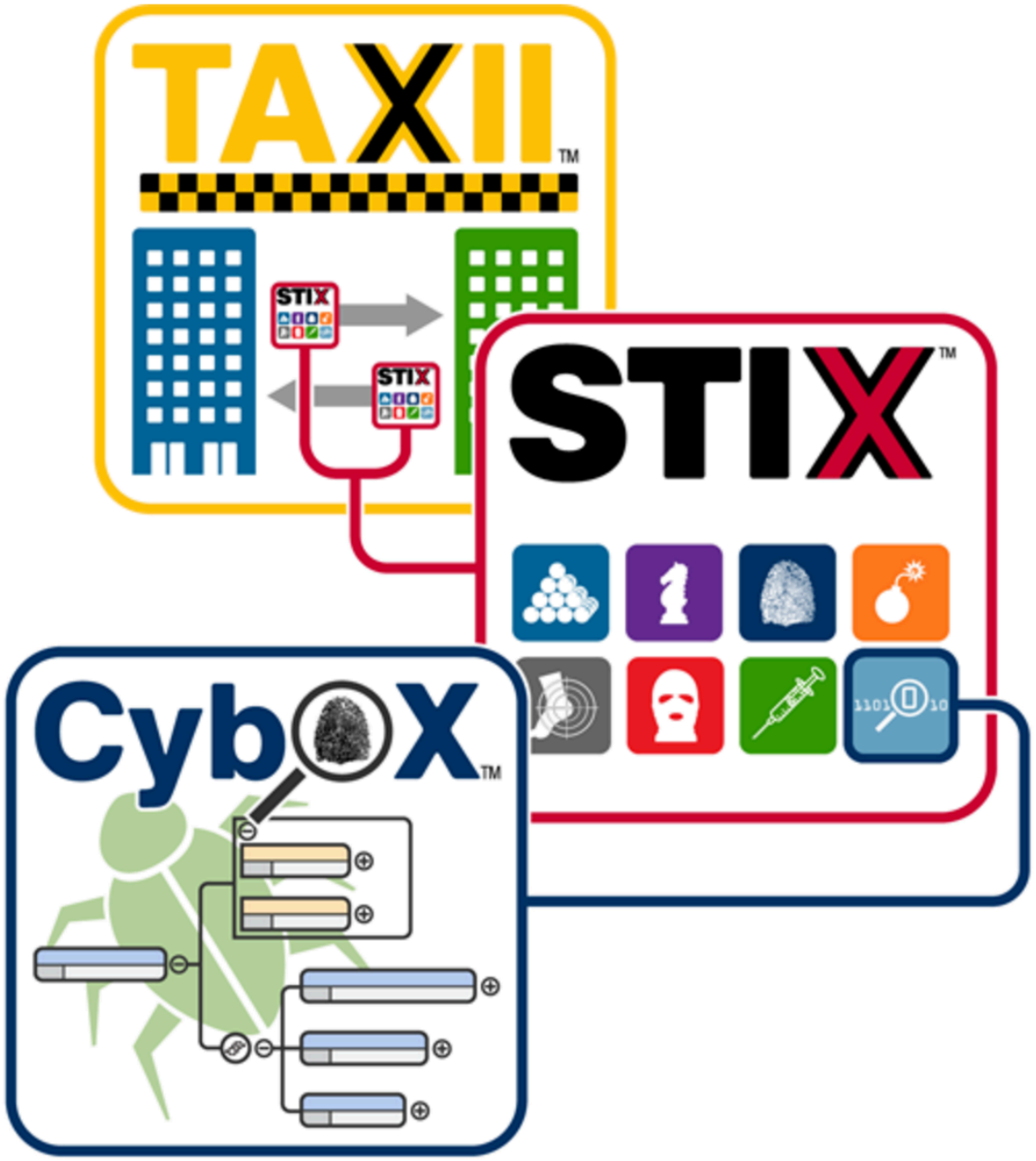

THREAT INTELLIGENCE CLOUD
AUTOFOCUS™
THOUSANDS OF USERS
MILLIONS OF CATEGORIZED URLS
MILLIONS OF SAMPLES PER DAY
TENS OF THOUSANDS OF UNIQUE MALWARE PER DAY

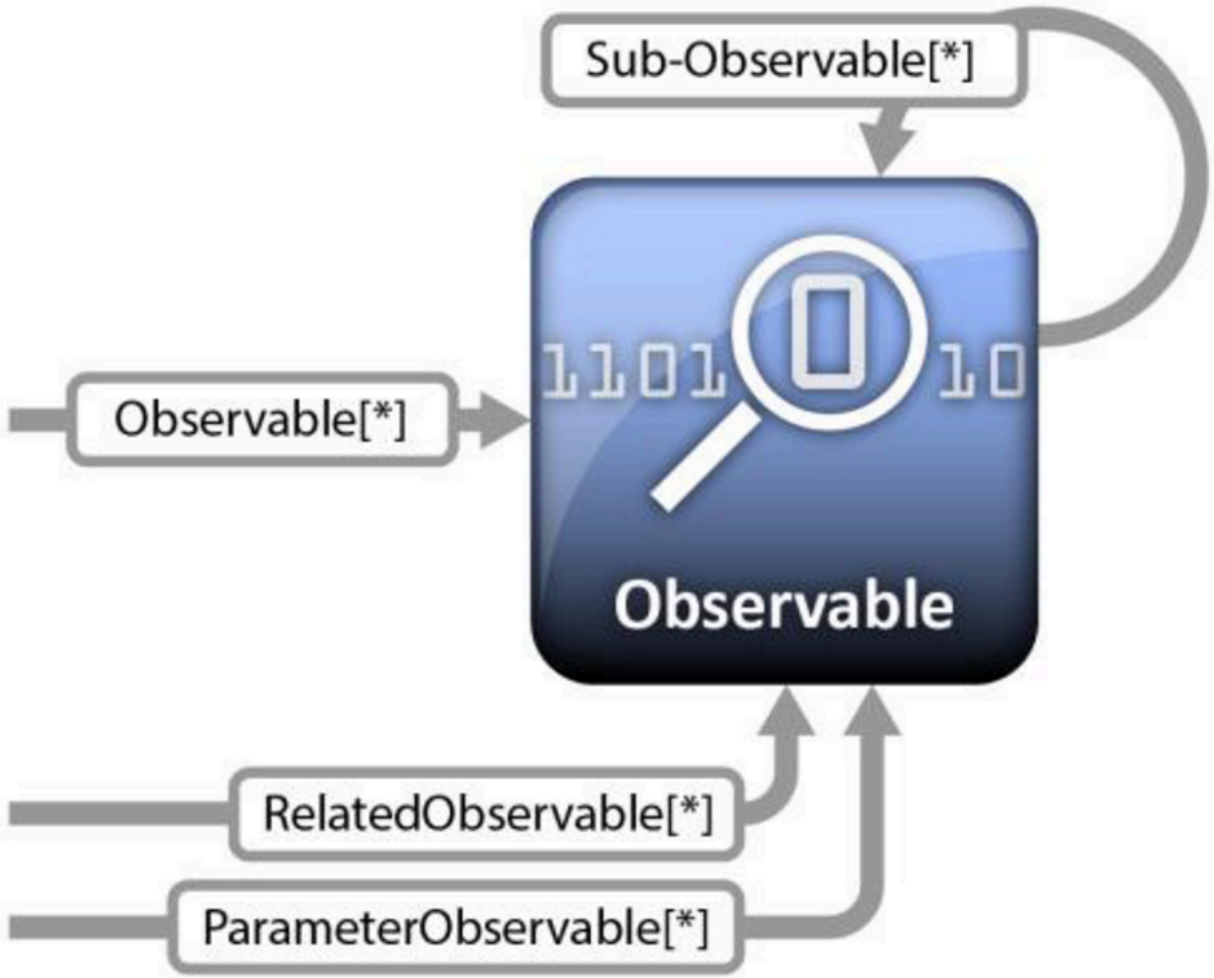
www.misp-project.org/#myCarousel

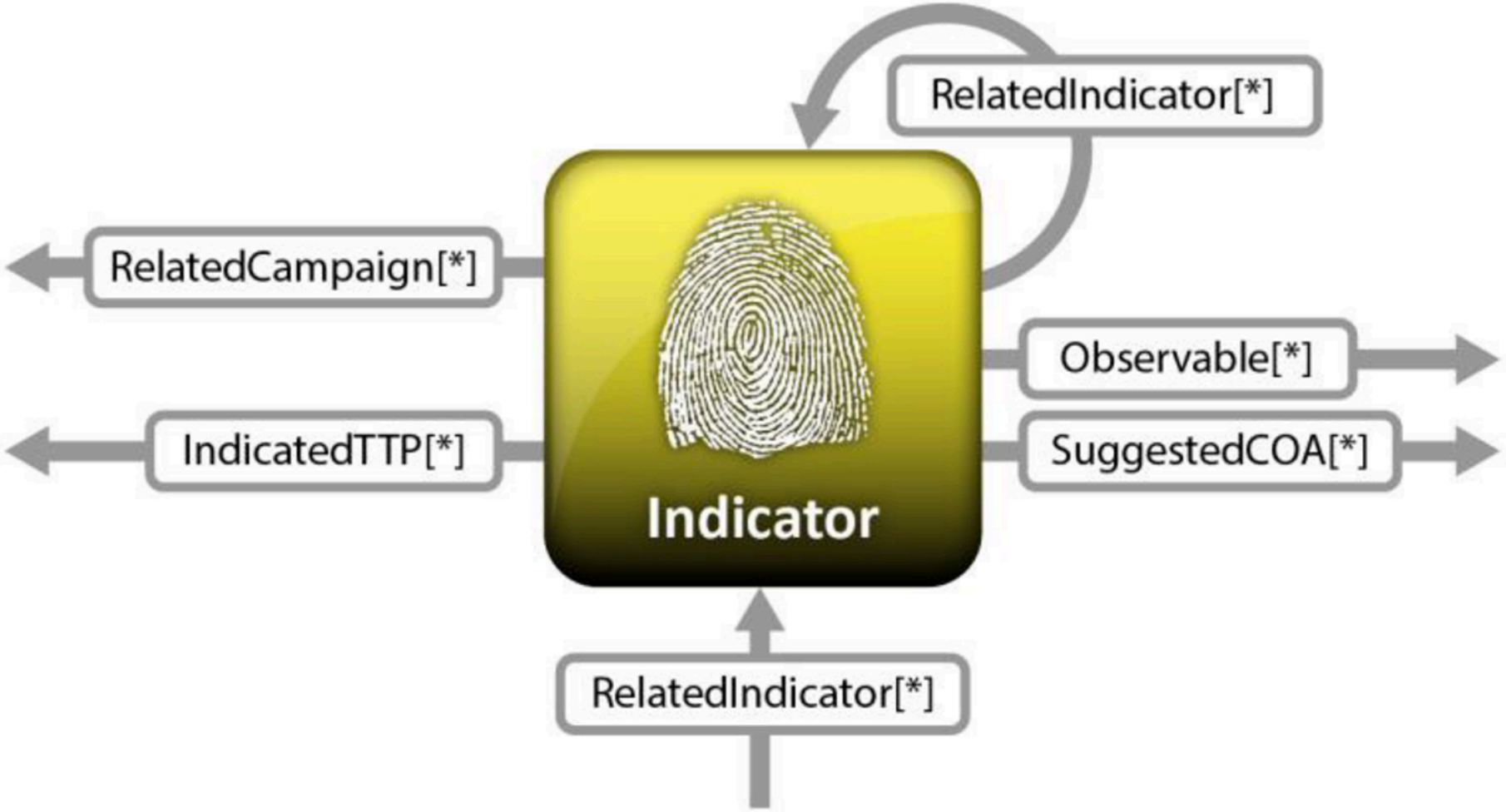
Malware Information Sharing Platform

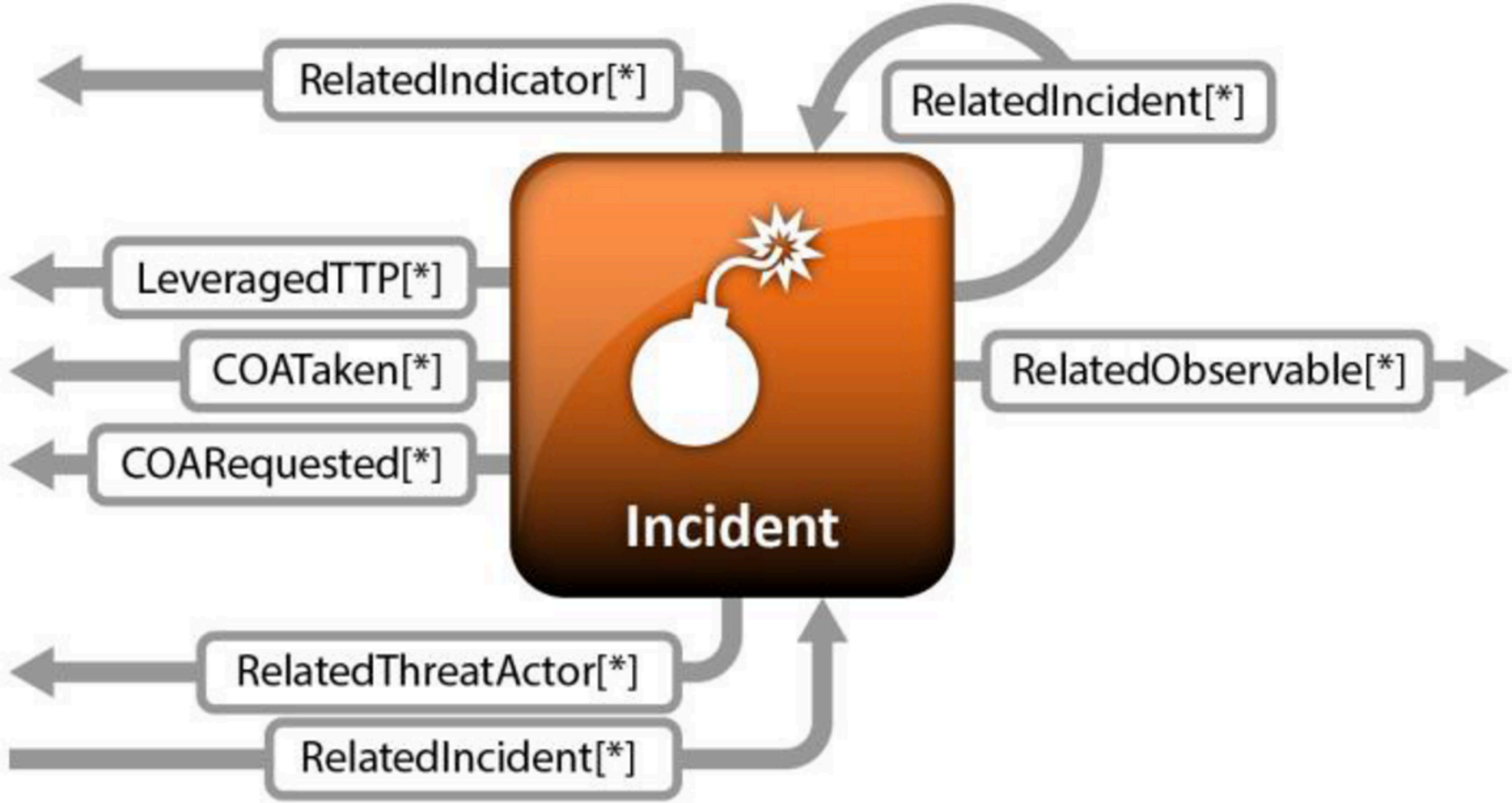
Home | Features | Use-cases | Roadmap | Screenshots | Download | Support

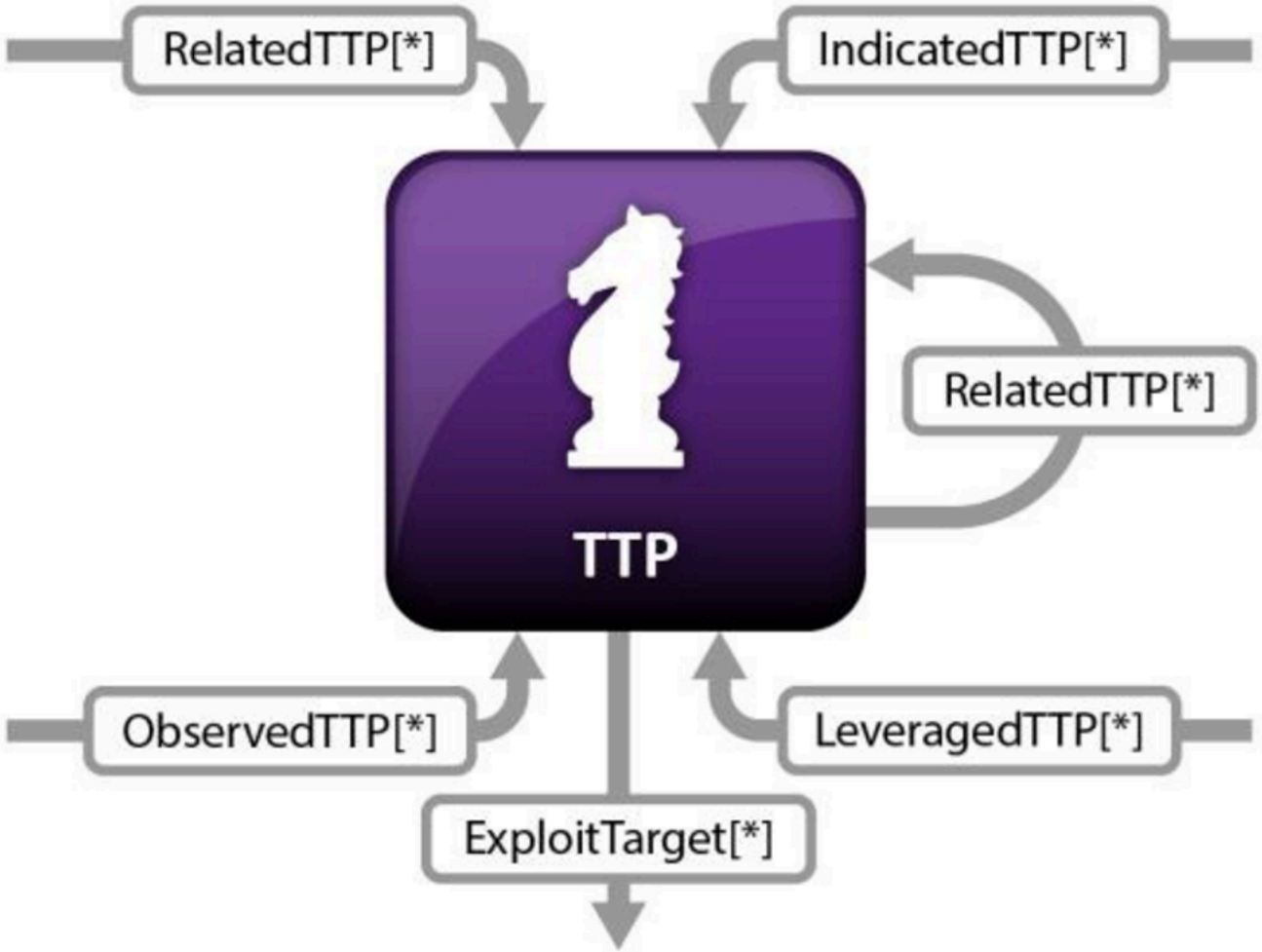
https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity



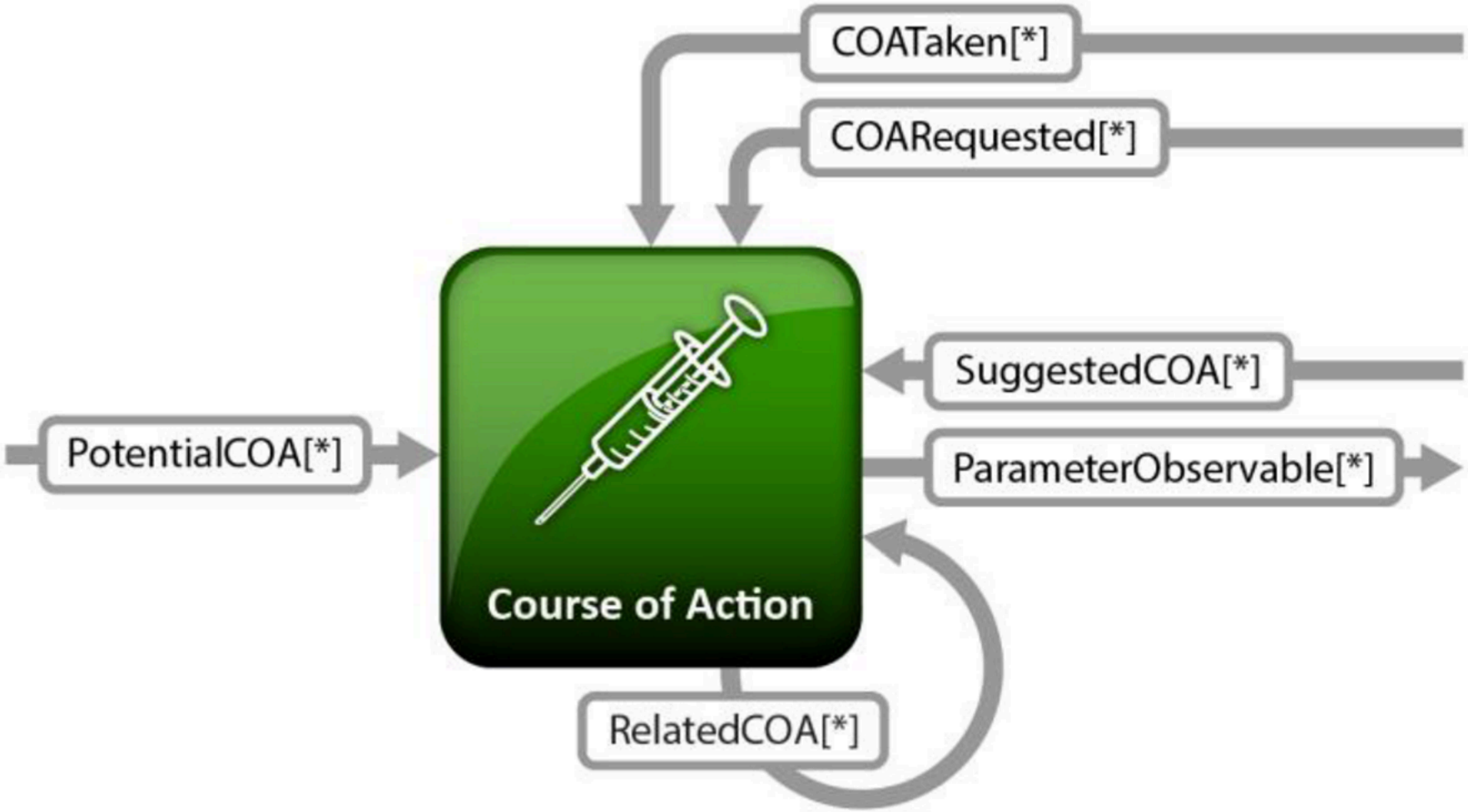

Sub-Observable[*]
Observable[*]
1101 0 10
Observable
RelatedObservable[*]
ParameterObservable[*]

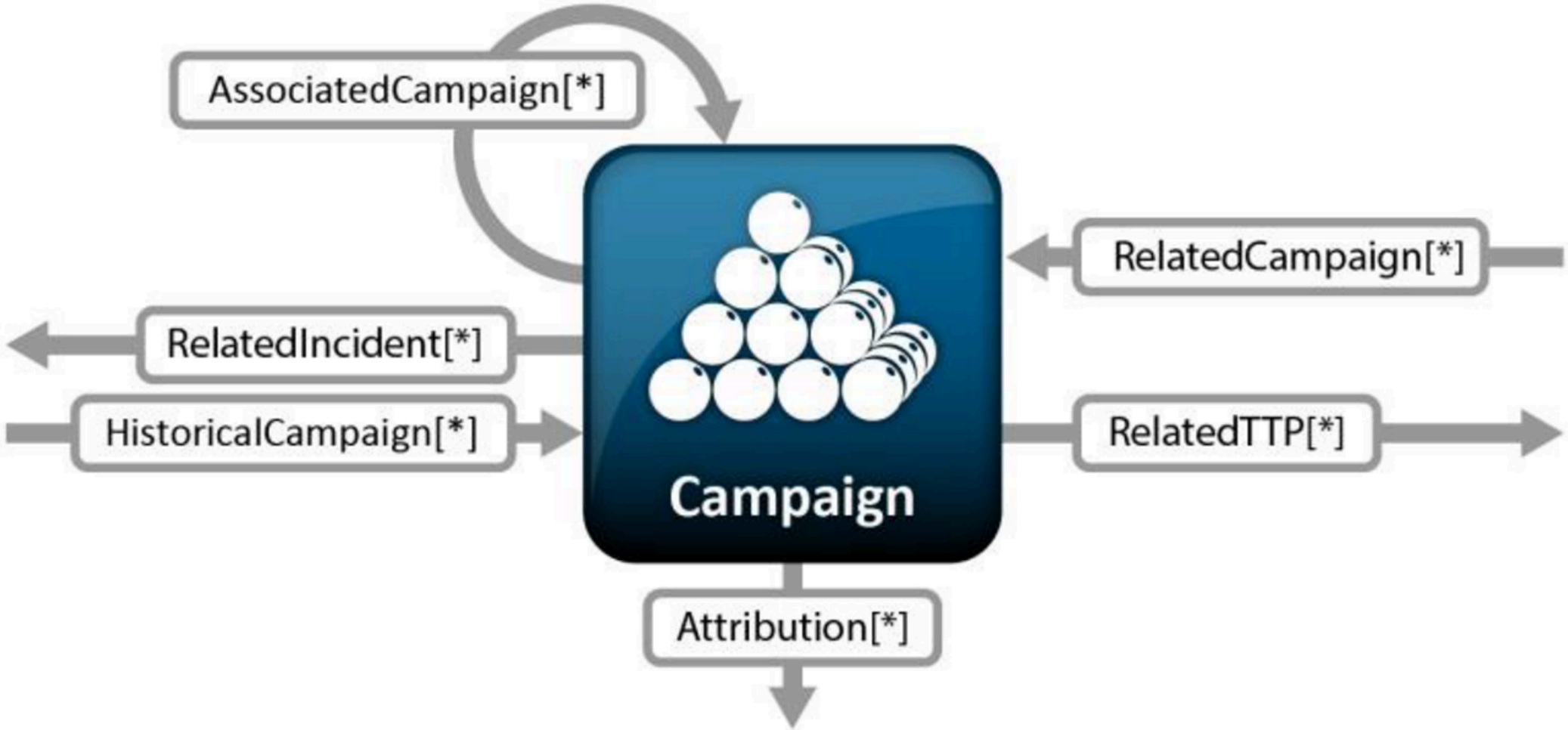

RelatedIndicator[*]
RelatedCampaign[*]
Observable[*]
IndicatedTTP[*]
SuggestedCOA[*]
Indicator
RelatedIndicator[*]

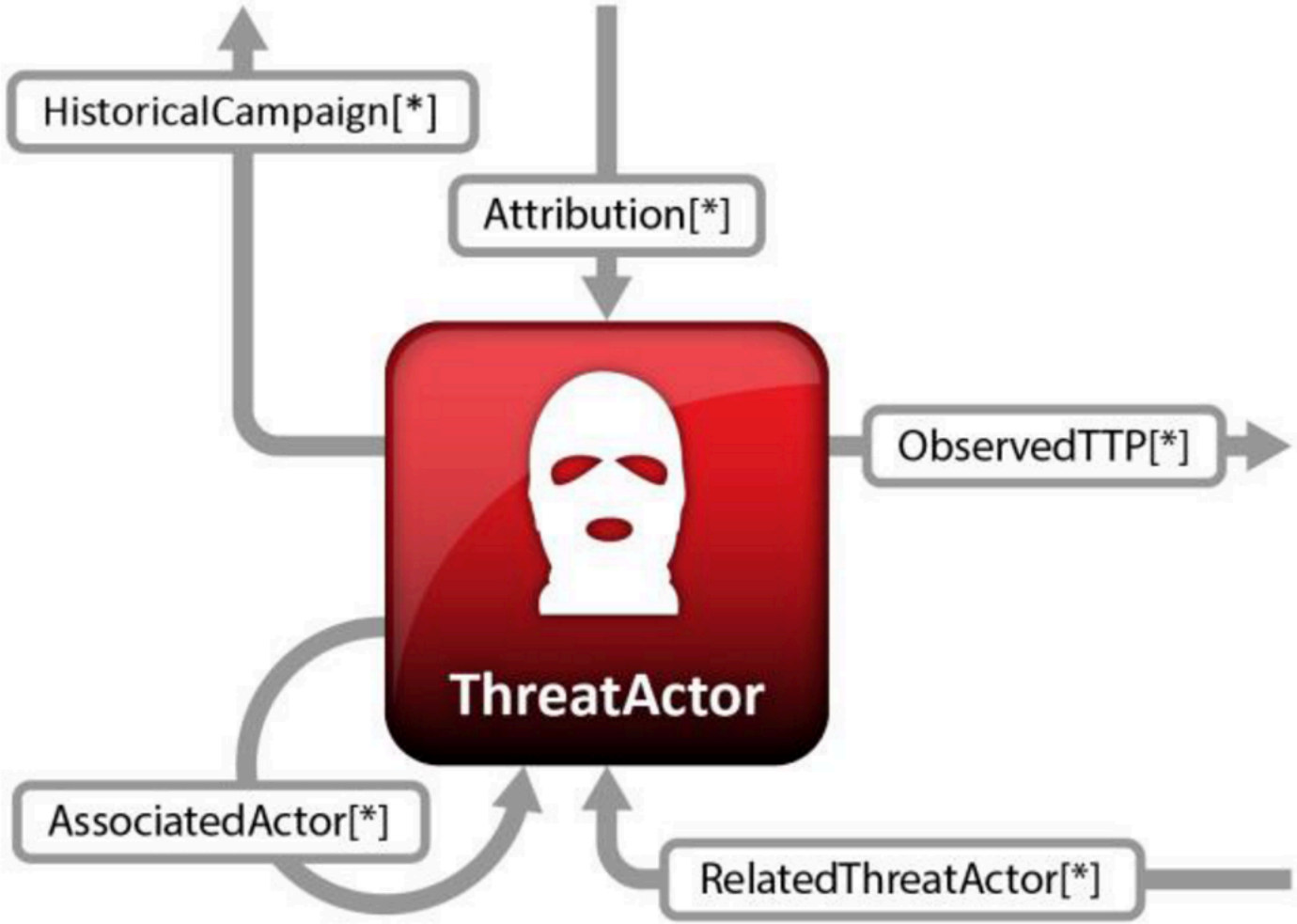

RelatedIndicator[*]
RelatedIncident[*]
LeveragedTTP[*]
COATaken[*]
COARequested[*]
RelatedObservable[*]
Incident
RelatedThreatActor[*]
RelatedIncident[*]

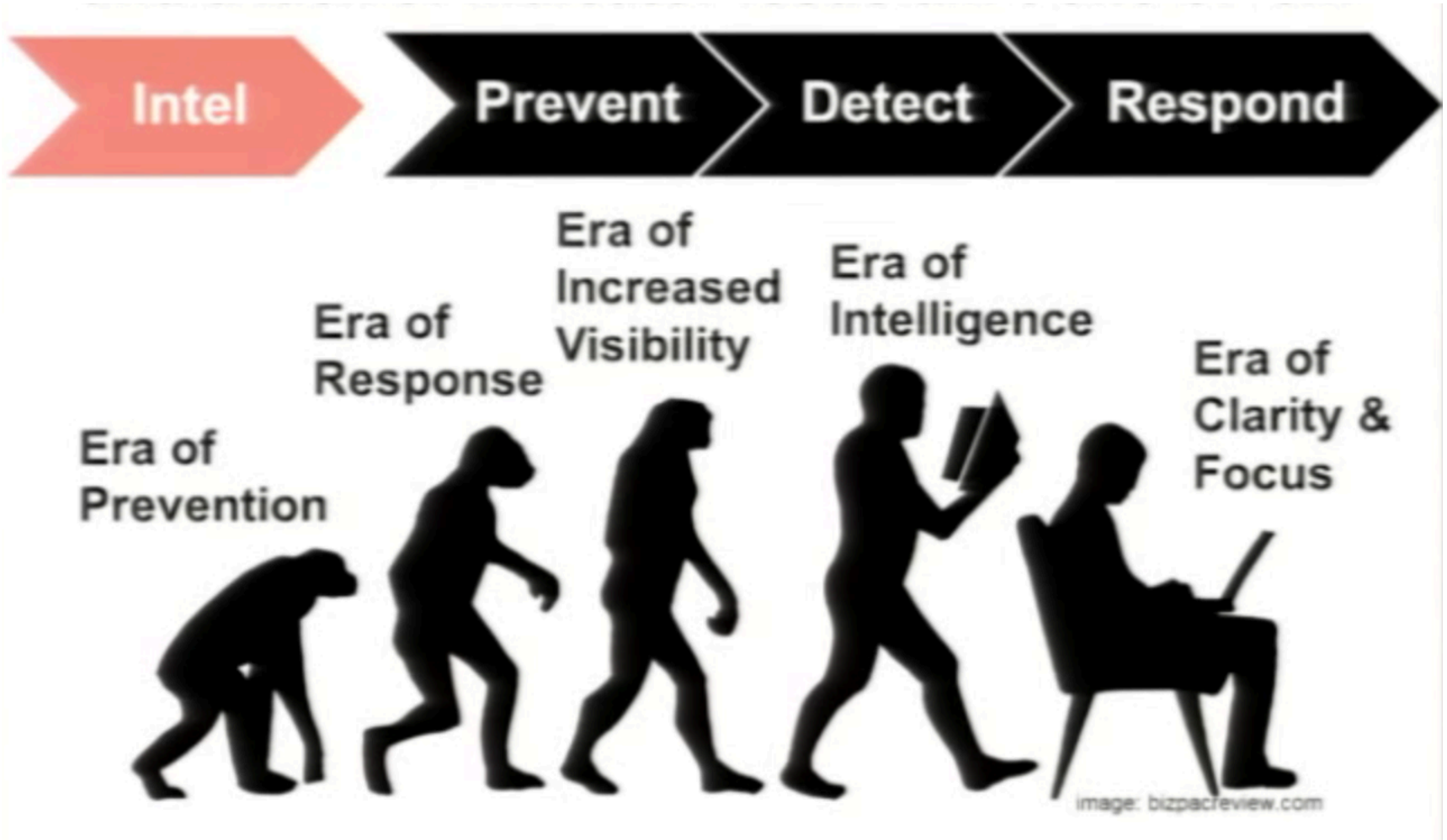

RelatedTTP[*]
IndicatedTTP[*]
RelatedTTP[*]
TTP
ObservedTTP[*]
LeveragedTTP[*]
ExploitTarget[*]


ExploitTarget[*]
ExploitTarget
RelatedExploitTarget[*]
PotentialCOA[*]


COATaken[*]
COARequested[*]
PotentialCOA[*]
SuggestedCOA[*]
ParameterObservable[*]
Course of Action
RelatedCOA[*]


AssociatedCampaign[*]
RelatedIncident[*]
HistoricalCampaign[*]
Campaign
RelatedCampaign[*]
RelatedTTP[*]
Attribution[*]


HistoricalCampaign[*]
Attribution[*]
ObservedTTP[*]
ThreatActor
AssociatedActor[*]
RelatedThreatActor[*]


Intel
Prevent
Detect
Respond
Era of Prevention
Era of Response
Era of Increased Visibility
Era of Intelligence
Era of Clarity & Focus
image: bizpacreview.com

Summary

Finished filling in the malware template

- Place it where?