# Best Practices CTI Sharing

## Forum Analisis dan Berbagi Informasi Keamanan Siber Sektor Keuangan
## 2 Oktober 2025

**Digit Oktavianto**
**@digitoktav**
**https://threathunting.id**

# Who Am I

- Infosec Consulting Manager at FPT Metrodata Indonesia
- Co-Founder BlueTeam.ID (https://blueteam.id)
- Community Lead @ Cyber Defense Community Indonesia (https://cdef.id)
- Cyber Security Training Instructor
- Member of Indonesia Honeynet Project Community
- Member at Asosiasi Forensik Digital Indonesia (AFDI)
- Member of High Tech Crime Investigation Association (HTCIA) APAC
- Opreker and Researcher

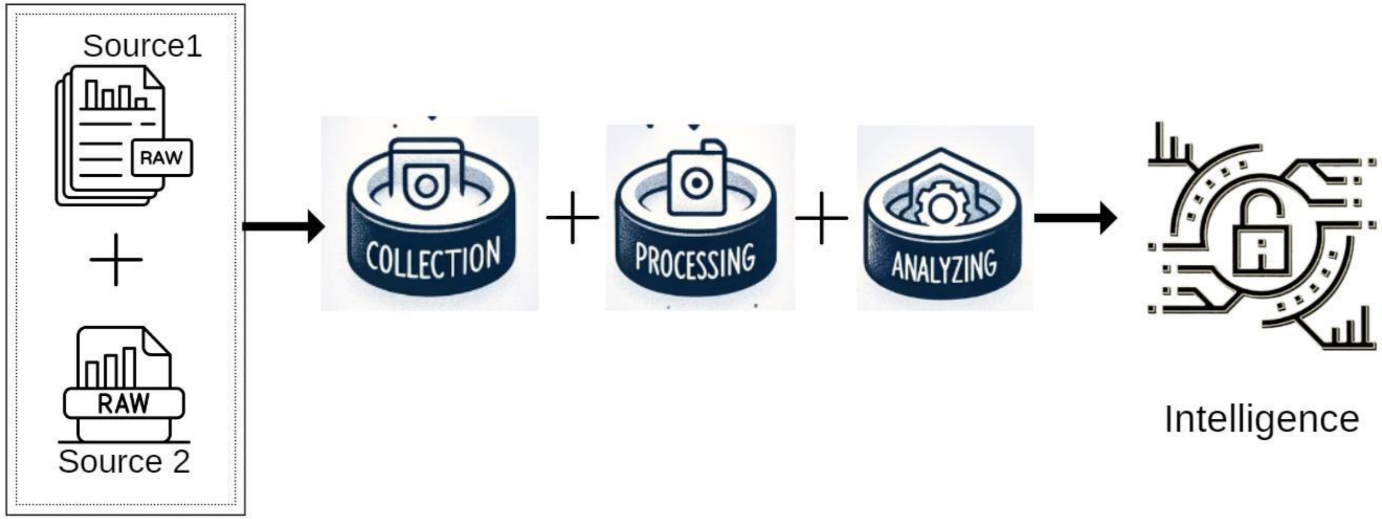
# Module

- Cyber Threat Intelligence Revisited
- Cyber Threat Information Sharing
- Best Practice Cyber Threat Information Sharing
- Threat Intelligence Platform

# Cyber Threat Intelligence

# Threat Intelligence

- RAW data -> collected + processed + analyzed -> CTI
- Information on the occurrence of cyber and physical threats
- Assessment of cyber and physical threats
- Analysis of threat actors involved



# What is Threat Intelligence?

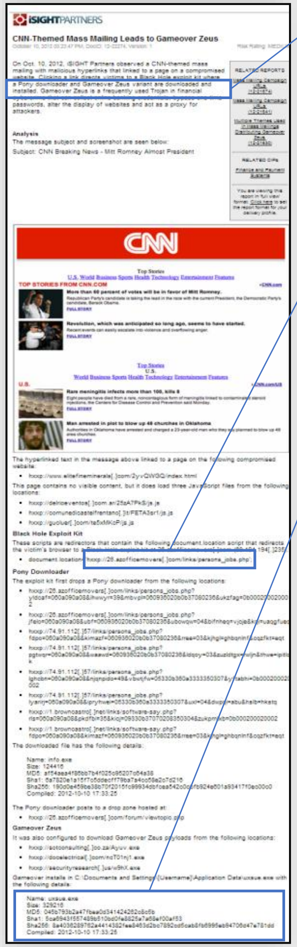
- Information about malicious actors

- Helps you make better decisions about defense

- Examples: IP addresses, Domains, URL’s, File Hashes, TTP’s, victim’s industries, countries..

# What is threat intelligence?

## Technical



iSIGHTPARTNERS

**CNN-Themed Mass Mailing Leads to Gameover Zeus**

October 10, 2012 03:23:47 PM, DocID: 12-22274, Version: 1 Risk Rating: MEDI

On Oct. 10, 2012, iSIGHT Partners observed a CNN-themed mass mailing with malicious hyperlinks that linked to a page on a compromised website. Clicking a link directs victims to a Black Hole exploit kit where a Pony downloader and Gameover Zeus variant are downloaded and installed. Gameover Zeus is a frequently used Trojan in financial cybercrime that can collect online banking credentials, bypass one-time passwords, alter the display of websites and act as a proxy for attackers.

RELATED REPORTS

Mass Mailing Campaign URLs (12-21674)

Mass Mailing Campaign URLs (12-21641)

Multiple Themes Used in Mass Mailings Distributing Gameover Zeus (12-21630)

RELATED CIPs

Finance and Payment Systems

You are viewing this report in 'full view' format. Click here to set the report format for your delivery profile.

**Analysis**

The message subject and screenshot are seen below:

Subject: CNN Breaking News - Mitt Romney Almost President

CNN

Top Stories
U.S. World Business Sports Health Technology Entertainment Features

TOP STORIES FROM CNN.COM »CNN.com

**More than 60 percent of votes will be in favor of Mitt Romney.**
Republican Party's candidate is taking the lead in the race with the current President, the Democratic Party's candidate, Barack Obama.
FULL STORY

**Revolution, which was anticipated so long ago, seems to have started.**
Recent events can easily escalate into violence and overflowing anger.
FULL STORY

Top Stories
U.S.
World Business Sports Health Technology Entertainment Features

U.S. »CNN.com/US

**Rare meningitis infects more than 100, kills 8**
Eight people have died from a rare, noncontagious form of meningitis linked to contaminated steroid injections, the Centers for Disease Control and Prevention said Monday.
FULL STORY

**Man arrested in plot to blow up 48 churches in Oklahoma**
Authorities in Oklahoma have arrested and charged a 23-year-old man who they say planned to blow up 48 area churches.
FULL STORY

The hyperlinked text in the message above linked to a page on the following compromised website:

- hxxp://www.elitefineminerals[.]com/2yvQWGQ/index.html

This page contains no visible content, but it does load three JavaScript files from the following locations:

- hxxp://delrioeventos[.]com.ar/25zA7PkS/js.js
- hxxp://comunedicastelfrentano[.]it/FETA3sr1/js.js
- hxxp://guoluer[.]com/te5xMKoP/js.js

**Black Hole Exploit Kit**

These scripts are redirectors that contain the following document.location script that redirects the victim's browser to a Black Hole exploit kit at 26.azofficemovers[.]com (50.194.194[.]235):

- document.location='hxxp://26.azofficemovers[.]com/links/persons_jobs.php';

**Pony Downloader**

The exploit kit first drops a Pony downloader from the following locations:

- hxxp://26.azofficemovers[.]com/links/persons_jobs.php?yldoaf=060a090a08&ihwwyr=39&mbvpl=0609360200b0b37080236&ukzfag=0b0002000200002
- hxxp://26.azofficemovers[.]com/links/persons_jobs.php?jfelo=060a090a08&ubf=060936020b0b37080236&ubowqw=04&bifnheq=vjoje&kqj=uaqgfued
- hxxp://74.91.112[.]57/links/persons_jobs.php?fdpo=060a090a08&kimazf=060936020b0b37080236&rree=03&kjhgl=ghbqninf&oqzfkt=eqt
- hxxp://74.91.112[.]57/links/persons_jobs.php?pgtwqr=060a090a08&waawd=060936020b0b37080236&ldqoy=03&zuzldtgx=rwljn&thwe=ipitlo k
- hxxp://74.91.112[.]57/links/persons_jobs.php?lghcbn=060a090a08&njqnpido=49&vbwtjfw=05330b360a3333350307&yfabhi=0b000200020002
- hxxp://74.91.112[.]57/links/persons_jobs.php?lyanrj=060a090a08&ipryhwei=05330b360a3333350307&uxl=04&dwpqj=abu&halb=hkstq
- hxxp://1.browncastro[.]net/links/software-say.php?rls=060a090a08&pkdfbi=35&kiqj=09330b370702083503048zukpmkbm=0b000200020002
- hxxp://1.browncastro[.]net/links/software-say.php?fdpo=060a090a08&kimazf=060936020b0b37080236&rree=03&kjhgl=ghbqninf&oqzfkt=eqt

The downloaded file has the following details:

Name: info.exe
Size: 124416
MD5: af54aea4f86bb7b4f025c95207c64a36
Sha1: 6a7820e1a15f7c5ddecff79ba7a4cc58e2c7d216
Sha256: 190d0e459be38b70f2015fc99934dbfcea542c0cbfb924e501a93417f0ec00c0
Compiled: 2012-10-10 17:33:25

The Pony downloader posts to a drop zone hosted at:

- hxxp://26.azofficemovers[.]com/forum/viewtopic.php

**Gameover Zeus**

It was also configured to download Gameover Zeus payloads from the following locations:

- hxxp://sotconsulting[.]co.za/Ayuv.exe
- hxxp://docelectrical[.]com/ncT01nj1.exe
- hxxp://securityresearch[.]us/w9hX.exe

Gameover installs in C:\Documents and Settings\[Username]\Application Data\uxsue.exe with the following details:

Name: uxsue.exe
Size: 329216
MD5: 045b793b2a47fbea0d341424262c8c5b
Sha1: 5ca69431557489b510bd0fe8825a7a68ef00af53
Sha256: 8a4036289762a4414382fee8463d2bc7892cd5cab8fb6995eb94706d47e781dd
Compiled: 2012-10-10 17:33:25

## Basic Context:

Gameover Zeus is a frequently used Trojan in financial cybercrime

## Exploitation Vector:

hxxp://26.azofficemovers.com/links/persons_jobs.php

## Malware Payload Indicators:

Name: uxsue.exe
Identifier: Gameover Zeus
Extension: exe
Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Size: 329216

## Bottom Line:

Zeus Malware Author Probably Working with Gameover Zeus Operators, but Current Level of Involvement Remains Uncertain

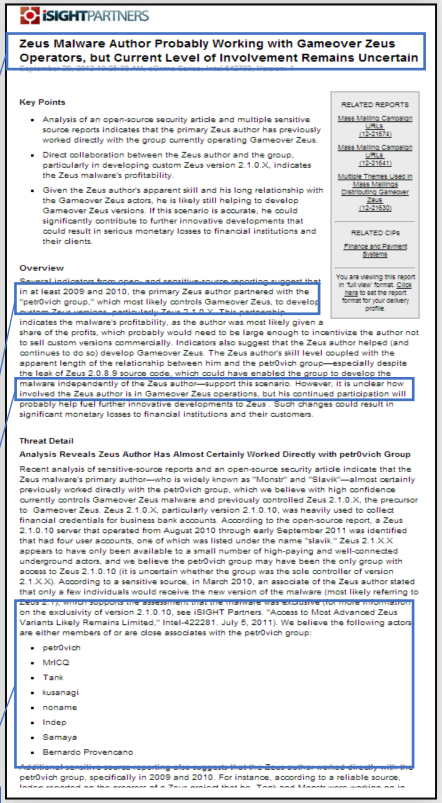
## Contextual Analysis:

...the primary Zeus author partnered with the "petrovich group," which most likely controls Gameover Zeus, to develop custom Zeus versions.... his continued participation will probably help fuel further innovative developments to Zeus.

## Unique Threat-focused information:

We believe the following actors are either members of or are close associates with the petr0vich group: …

## Threat



iSIGHTPARTNERS

**Zeus Malware Author Probably Working with Gameover Zeus Operators, but Current Level of Involvement Remains Uncertain**

September 28, 2012 10:25:38 AM, eCrime Series, Intel 642792, Version: 1

**Key Points**

- Analysis of an open-source security article and multiple sensitive source reports indicates that the primary Zeus author has previously worked directly with the group currently operating Gameover Zeus.
- Direct collaboration between the Zeus author and the group, particularly in developing custom Zeus version 2.1.0.X, indicates the Zeus malware's profitability.
- Given the Zeus author's apparent skill and his long relationship with the Gameover Zeus actors, he is likely still helping to develop Gameover Zeus versions. If this scenario is accurate, he could significantly contribute to further innovative developments that could result in serious monetary losses to financial institutions and their clients.

RELATED REPORTS

Mass Mailing Campaign URLs (12-21674)

Mass Mailing Campaign URLs (12-21641)

Multiple Themes Used in Mass Mailings Distributing Gameover Zeus (12-21630)

RELATED CIPs

Finance and Payment Systems

You are viewing this report in 'full view' format. Click here to set the report format for your delivery profile.

**Overview**

Several indicators from open- and sensitive-source reporting suggest that in at least 2009 and 2010, the primary Zeus author partnered with the "petr0vich group," which most likely controls Gameover Zeus, to develop custom Zeus versions, particularly Zeus 2.1.0.X. This partnership indicates the malware's profitability, as the author was most likely given a share of the profits, which probably would need to be large enough to incentivize the author not to sell custom versions commercially. Indicators also suggest that the Zeus author helped (and continues to do so) develop Gameover Zeus. The Zeus author's skill level coupled with the apparent length of the relationship between him and the petr0vich group—especially despite the leak of Zeus 2.0.8.9 source code, which could have enabled the group to develop the malware independently of the Zeus author—support this scenario. However, it is unclear how involved the Zeus author is in Gameover Zeus operations, but his continued participation will probably help fuel further innovative developments to Zeus . Such changes could result in significant monetary losses to financial institutions and their customers.

**Threat Detail**

**Analysis Reveals Zeus Author Has Almost Certainly Worked Directly with petr0vich Group**

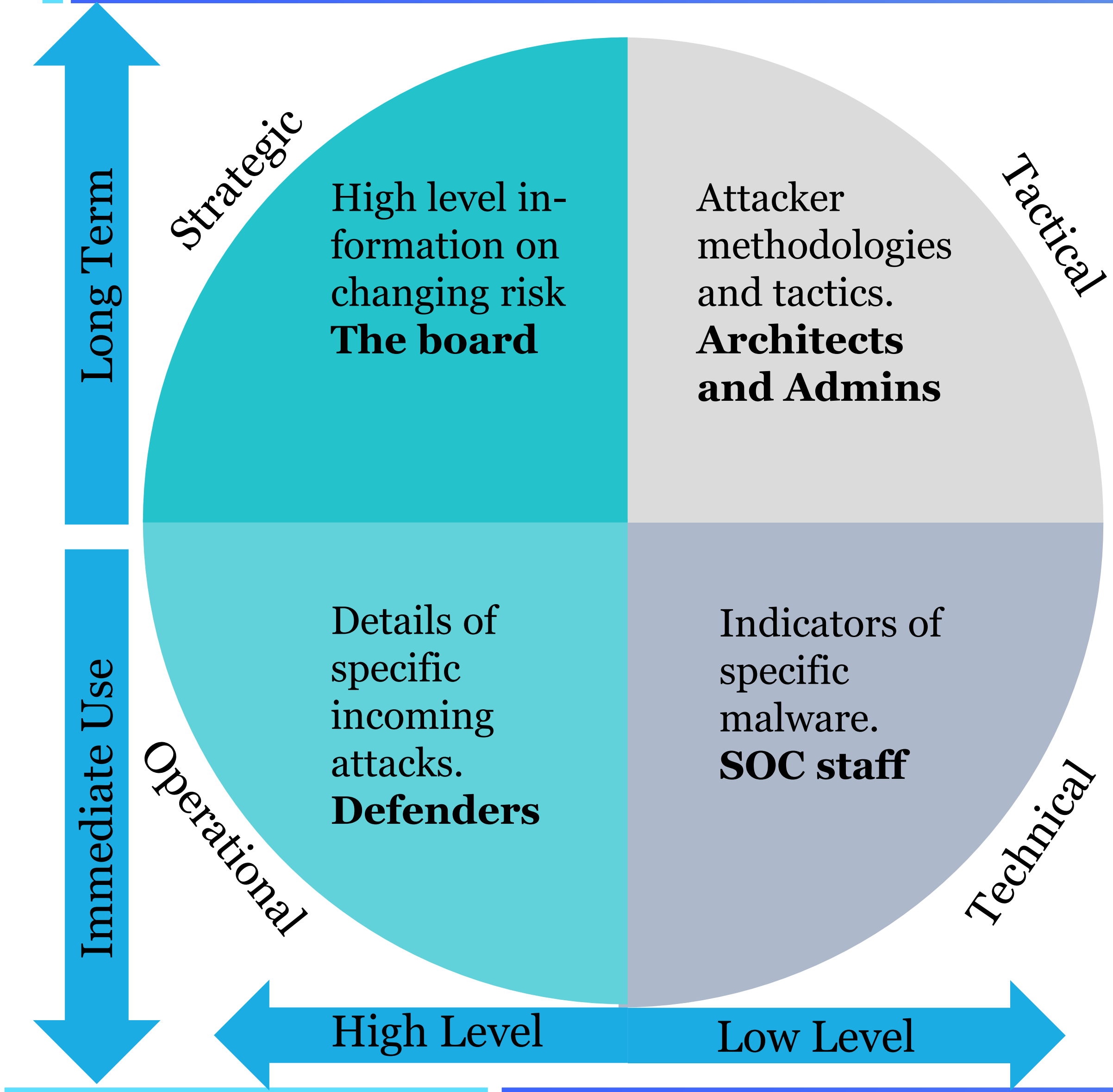
Recent analysis of sensitive-source reports and an open-source security article indicate that the Zeus malware's primary author—who is widely known as "Monstr" and "Slavik"—almost certainly previously worked directly with the petr0vich group, which we believe with high confidence currently controls Gameover Zeus malware and previously controlled Zeus 2.1.0.X, the precursor to  Gameover Zeus. Zeus 2.1.0.X, particularly version 2.1.0.10, was heavily used to collect financial credentials for business bank accounts. According to the open-source report, a Zeus 2.1.0.10 server that operated from August 2010 through early September 2011 was identified that had four user accounts, one of which was listed under the name "slavik." Zeus 2.1.X.X appears to have only been available to a small number of high-paying and well-connected underground actors, and we believe the petr0vich group may have been the only group with access to Zeus 2.1.0.10 (it is uncertain whether the group was the sole controller of version 2.1.X.X). According to a sensitive source, in March 2010, an associate of the Zeus author stated that only a few individuals would receive the new version of the malware (most likely referring to Zeus 2.1), which supports the assessment that the malware was exclusive (for more information on the exclusivity of version 2.1.0.10, see iSIGHT Partners. "Access to Most Advanced Zeus Variants Likely Remains Limited," Intel-422281. July 5, 2011). We believe the following actors are either members of or are close associates with the petr0vich group:

- petr0vich
- MrICQ
- Tank
- kusanagi
- noname
- Indep
- Samaya
- Bernardo Provencano

Additional sensitive-source reporting also suggests that the Zeus author worked directly with the petr0vich group, specifically in 2009 and 2010. For instance, according to a reliable source, Indep reported on the progress of a Zeus project that he, Tank and Monstr were working on in

**Knowledge and context, not just data**

# Type of Cyber Threat Intelligence


Long Term
Immediate Use
Strategic
Tactical
Operational
Technical
High level information on changing risk
**The board**
Attacker methodologies and tactics.
**Architects and Admins**
Details of specific incoming attacks.
**Defenders**
Indicators of specific malware.
**SOC staff**
High Level
Low Level

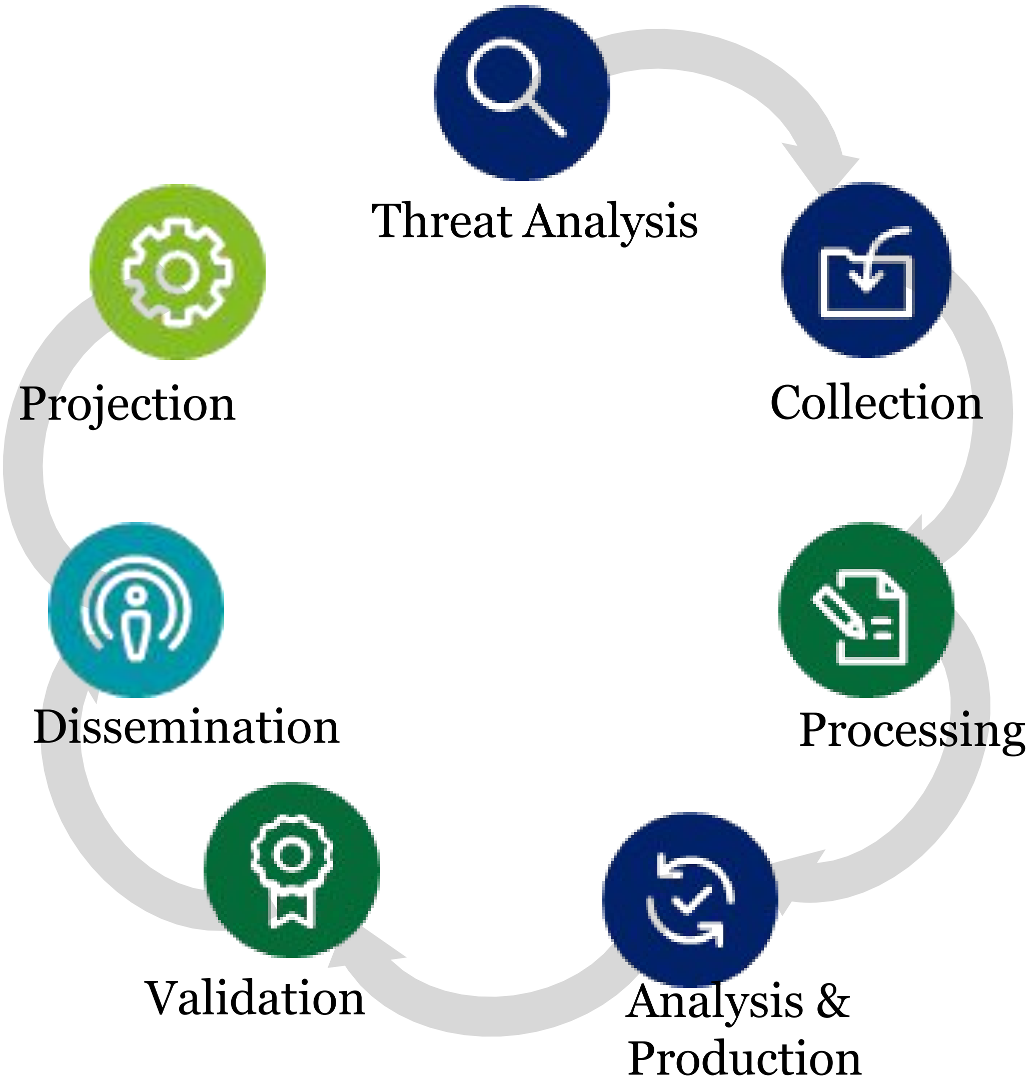
- **Definition** - Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
- **Expectation** - Understanding the threat landscape from a dynamic and strategic perspective helps an organisation to prepare for and react appropriately to Cyber events

# Key Questions

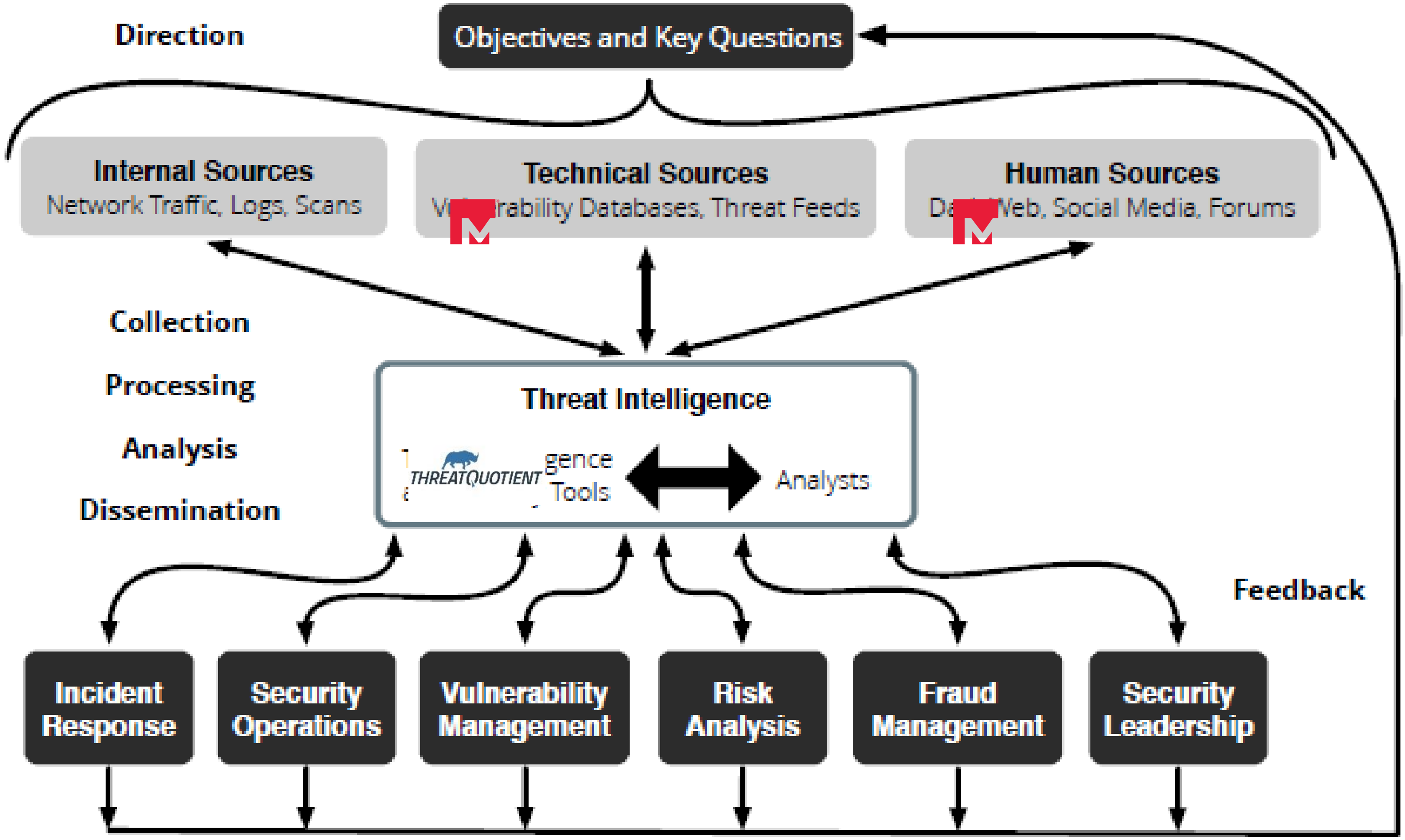
- **Who's** Attacking You?
  - Identify the threat actors/group targeting the organization.
- **What** Are Their Motivations?
  - Uncover the motives driving the attacks for targeted response.
- **What** Are Their Capabilities?
  - Assess the adversaries' technical and strategic capabilities.
- **What** Artefacts and IOCs/IOAs to Look For?
  - Define and monitor indicators of compromise/attack for early threat detection.

# Use Case Examples

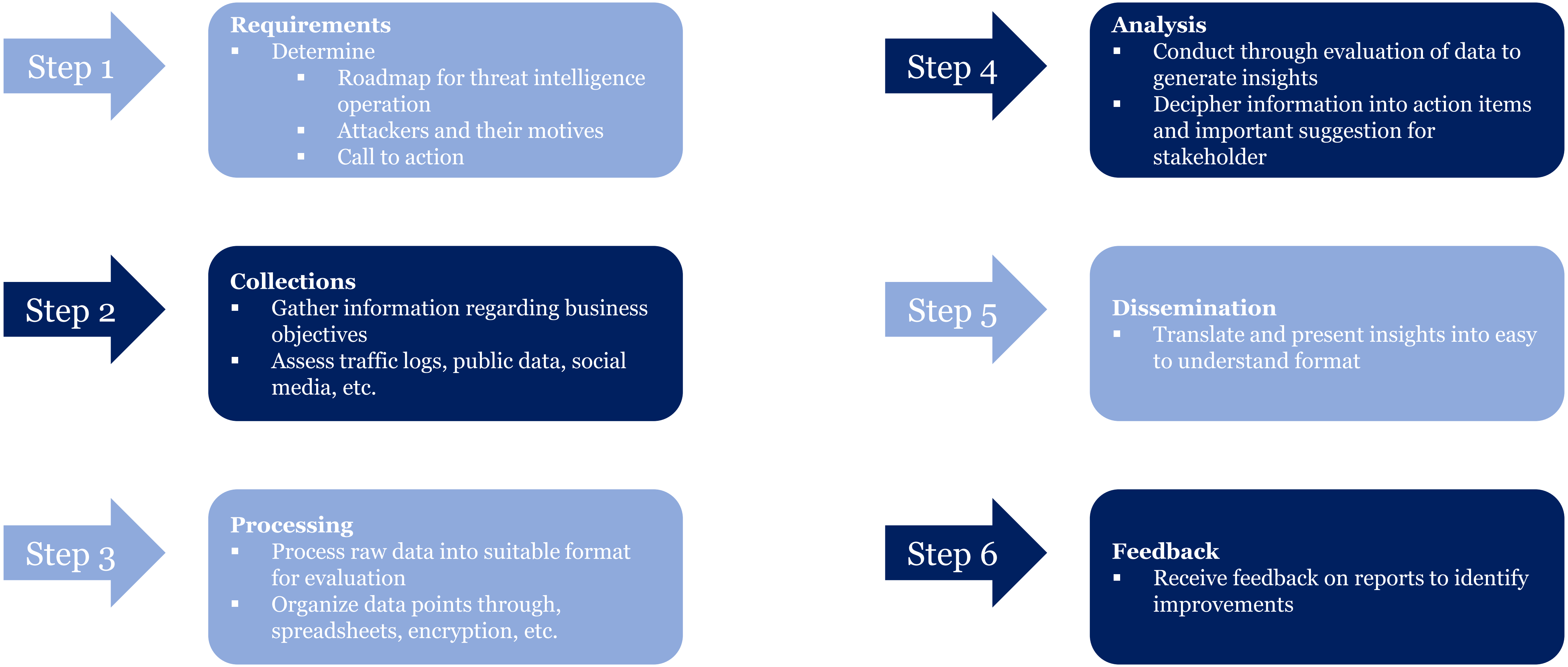
- Phishing detection
- Incident Response knowledge base
- Vulnerability prioritization
- Brand monitoring
- Fraud detection



# Six Phase of Threat Intelligence



# Steps for Cyber Threat Intelligence Lifecycles



Step 1

**Requirements**

- Determine
  - Roadmap for threat intelligence operation
  - Attackers and their motives
  - Call to action

Step 2

**Collections**

- Gather information regarding business objectives
- Assess traffic logs, public data, social media, etc.

Step 3

**Processing**

- Process raw data into suitable format for evaluation
- Organize data points through, spreadsheets, encryption, etc.

Step 4

**Analysis**

- Conduct through evaluation of data to generate insights
- Decipher information into action items and important suggestion for stakeholder

Step 5

**Dissemination**

- Translate and present insights into easy to understand format

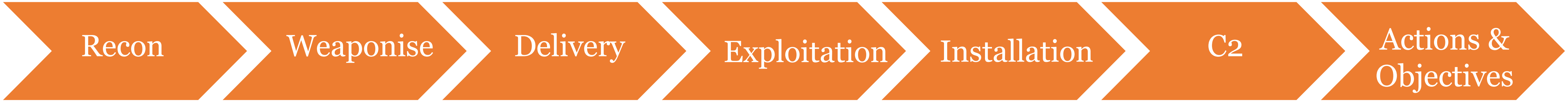
Step 6

**Feedback**

- Receive feedback on reports to identify improvements

# Kill Chain Analysis

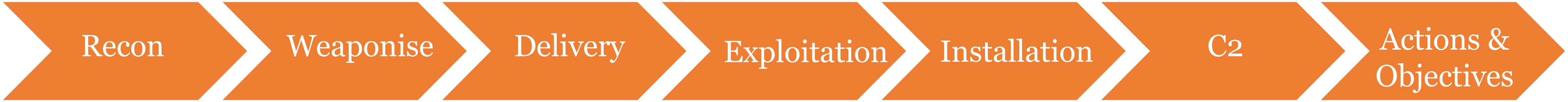
- **Task**: Identify the Attackers’ Step by Step Process
- **Goal**: Disrupting Attackers’ operations



| Recon | Weaponise | Delivery | Exploitation | Installation | C2 | Actions & Objectives |
|---|---|---|---|---|---|---|
| ▪ Motivation<br>▪ Preparation | ▪ Configuration<br>▪ Packaging | ▪ Mechanisme of Delivery<br>▪ Infection Vector | ▪ Technical or human?<br>▪ Applications affected<br>▪ Method & Characteristics | ▪ Perssitence<br>▪ Characteristics of change<br>▪ Acquiring additional components | ▪ Communication between victim & adversary | ▪ What the adversary does when they have control of the system |

# MITRE ATT&CK MATRIX

- Builds on the Kill Chain
- Provides deeper level of granularity



**MITRE ATT&CK:**
- Active Scanning
- Passive Scanning
- Determine Domain and IP Address Space
- Analyze Third-Party IT Footprint

**MITRE ATT&CK:**
- Malware
- Scripting
- Service Execution

**MITRE ATT&CK:**
- Spearphishing Attachment/Link
- Exploit Public-Facing Application
- Supply Chain Compromise

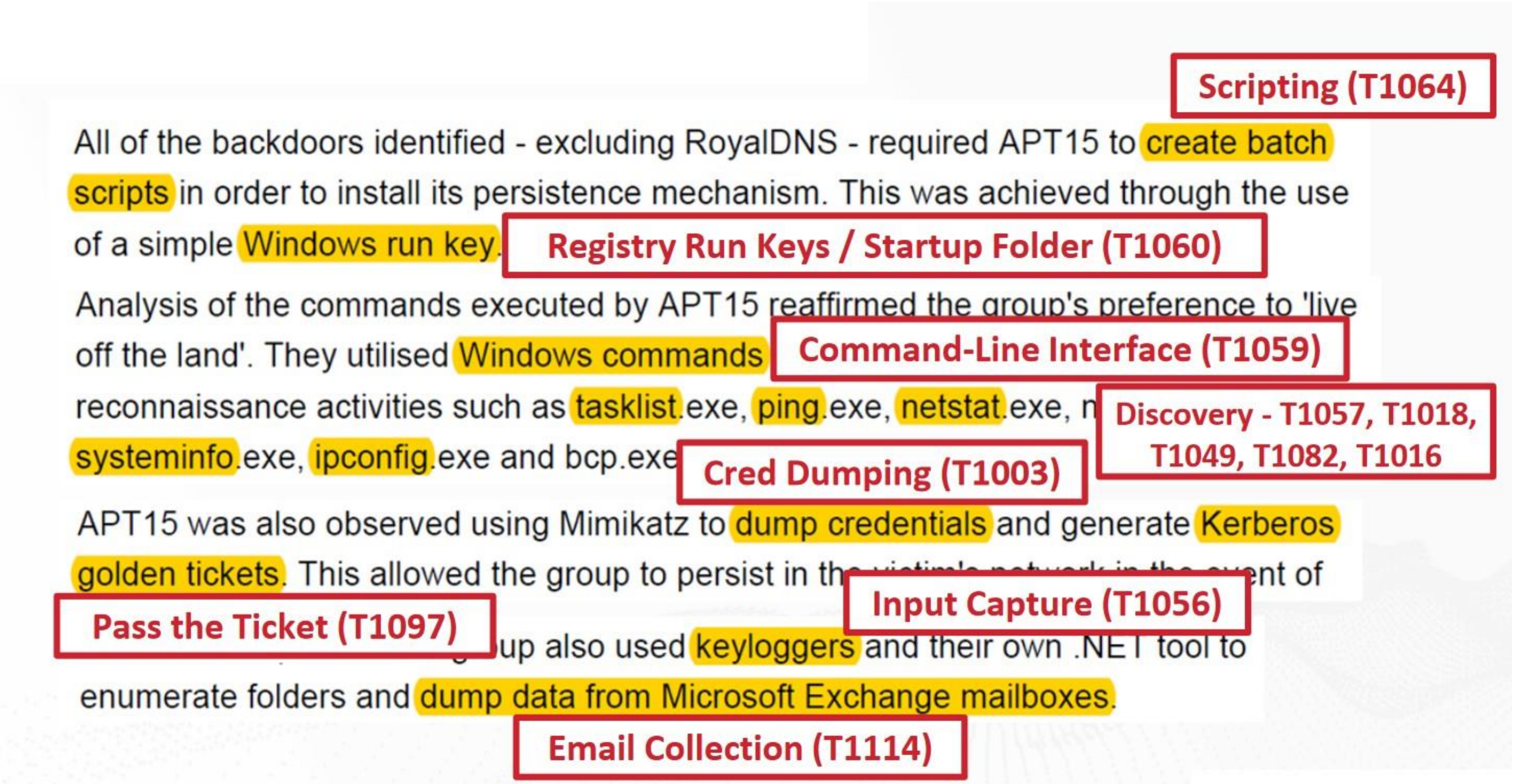
**MITRE ATT&CK:**
- Local Job Scheduling
- Scripting
- Rundll32

**MITRE ATT&CK:**
- Application Shimming
- Hooking
- Login Items

- **MITRE ATT&CK:**
- Data Obfuscation Domain Fronting
- Web Service

**MITRE ATT&CK:**
- Email Collection
- Data from LocalSystem/Network Share

# Aligning Actionable CTI into MITRE ATT&CK



All of the backdoors identified - excluding RoyalDNS - required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved through the use of a simple Windows run key.

Analysis of the commands executed by APT15 reaffirmed the group's preference to 'live off the land'. They utilised Windows commands

reconnaissance activities such as tasklist.exe, ping.exe, netstat.exe, n

systeminfo.exe, ipconfig.exe and bcp.exe

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in th

ent of

up also used keyloggers and their own .NET tool to enumerate folders and dump data from Microsoft Exchange mailboxes.

Scripting (T1064)

Registry Run Keys / Startup Folder (T1060)

Command-Line Interface (T1059)

Discovery - T1057, T1018, T1049, T1082, T1016

Cred Dumping (T1003)

Pass the Ticket (T1097)

Input Capture (T1056)

Email Collection (T1114)

https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

# CTI and Blue Team Engagement

THIS is what the adversary is doing! The Run key is AdobeUpdater.

Registry Run Keys / Startup Folder (T1060)

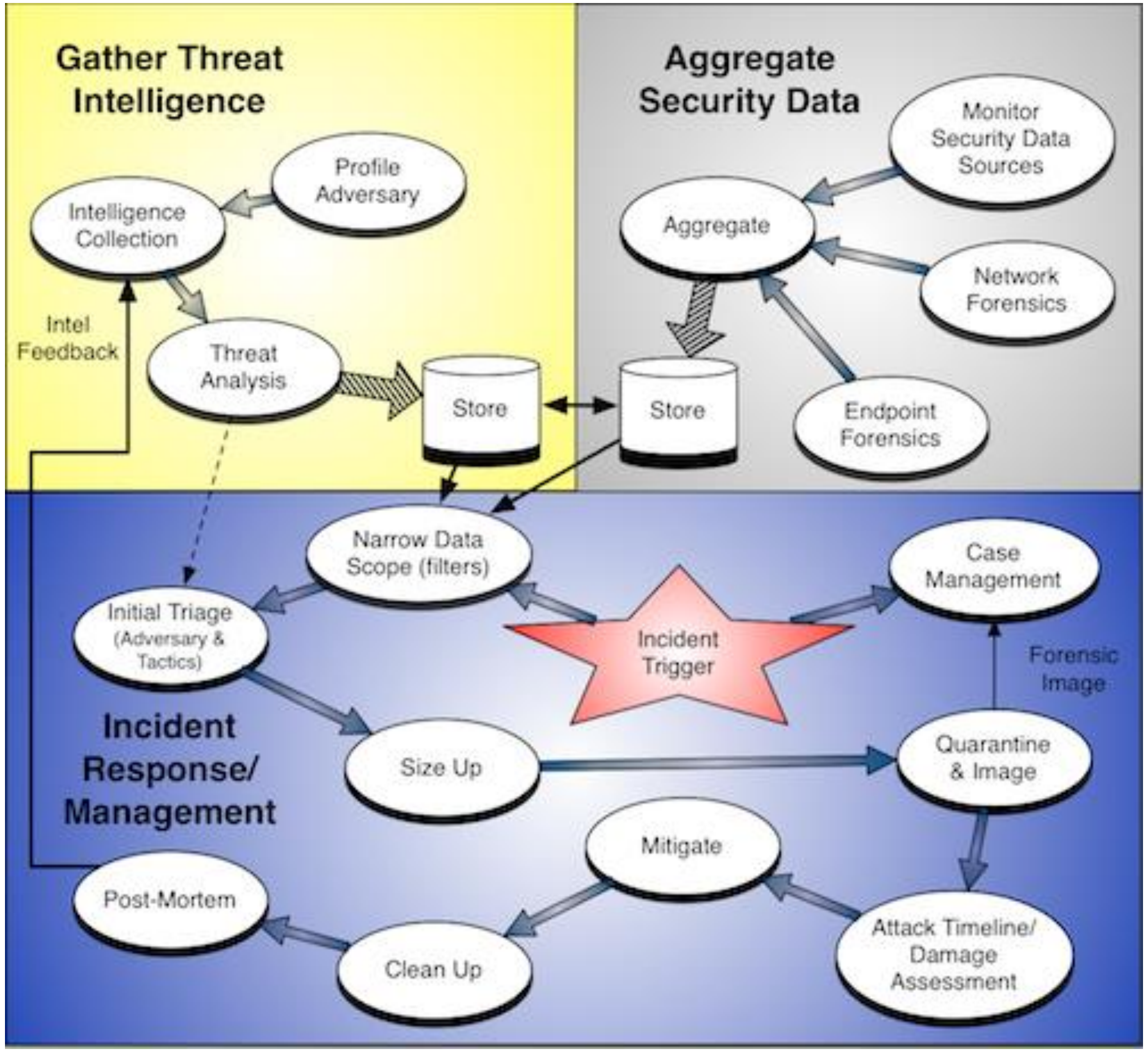
ATT&CK

Oh, we have Registry data, we can detect that!

CTI Analyst

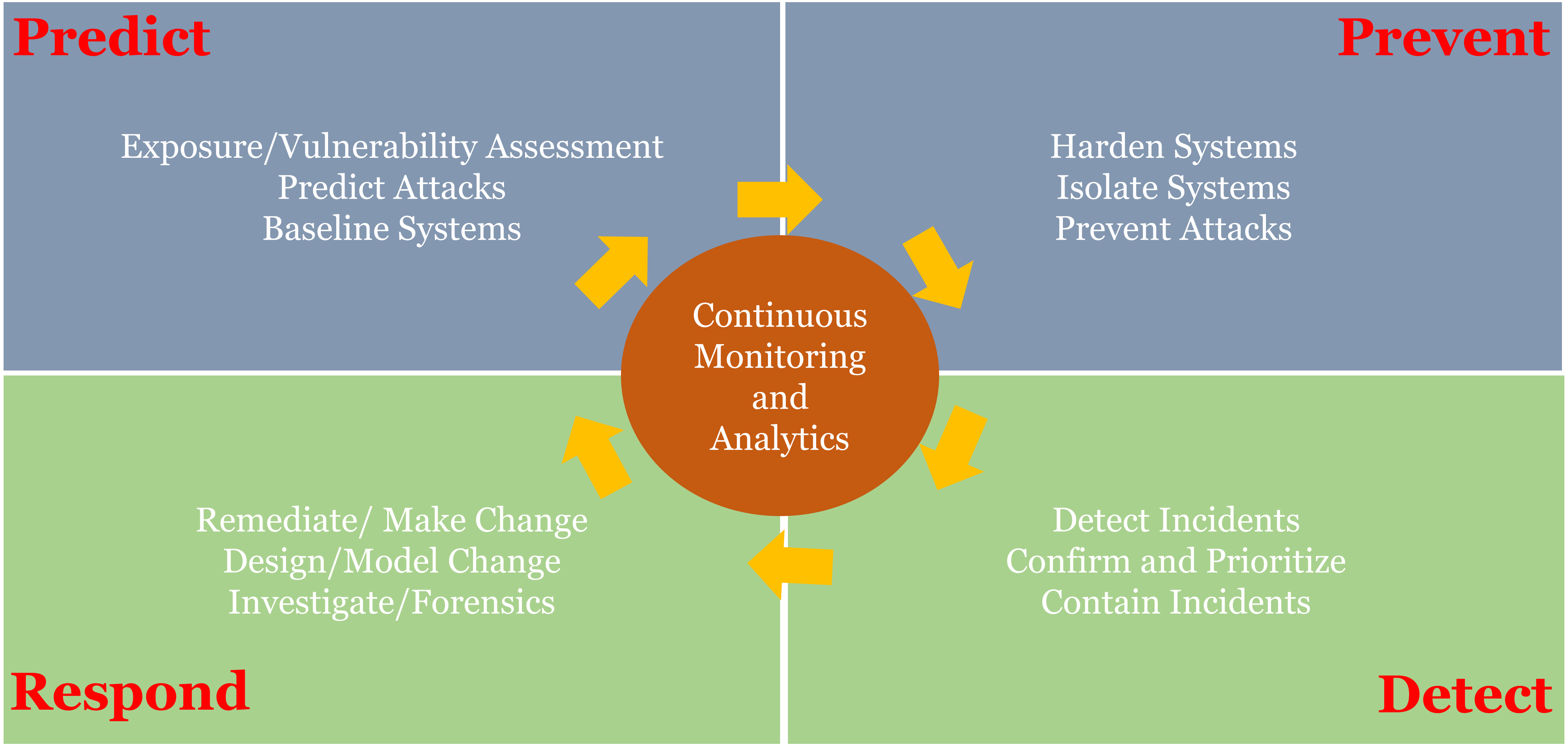
Defender

# Use Case : CTI for Incident Response



https://securosis.com/research/publication/leveraging-threat-intelligence-in-incident-response-management

# Defensive Security Capabilities



Predict

Exposure/Vulnerability Assessment
Predict Attacks
Baseline Systems

Prevent

Harden Systems
Isolate Systems
Prevent Attacks

Continuous Monitoring and Analytics

Remediate/ Make Change
Design/Model Change
Investigate/Forensics

Respond

Detect Incidents
Confirm and Prioritize
Contain Incidents

Detect

# Advantages of utilizing CTI throughout Cybersecurity Ecosystem

## Function

| | Sec/IT Analyst | Security operations center | Cybersecurity incident response team | Intel Analyst | Executive manager |
|---|---|---|---|---|---|
| Benefits | ▪ Optimize prevention and identification capabilities<br>▪ Develop robust defense strategies | ▪ Prioritize incidents based on risk and outcome on business<br>▪ Add text here | ▪ Accelerate incident analysis<br>▪ Manage and prioritize various uncertainties | ▪ Identify threat factors<br>▪ Monitor them to determine vulnerable targets | ▪ Understand internal organizational vulnerabilities<br>▪ Identify solutions to overcome them |
| Use Cases | ▪ Integrate TI feeds with security products<br>▪ Block malware from Lps, URLs, etc. | ▪ Utilize TI to improve alert<br>▪ Link alert notifications to incidents | ▪ Look for information on attackers motives<br>▪ Asses root cause to identify scope of incident | ▪ Gather deeper understanding regarding intrusion evidence<br>▪ Review reports on threats | ▪ Evaluate overall threat level for company<br>▪ Build security roadmap |

# Cyber Threat Information Sharing

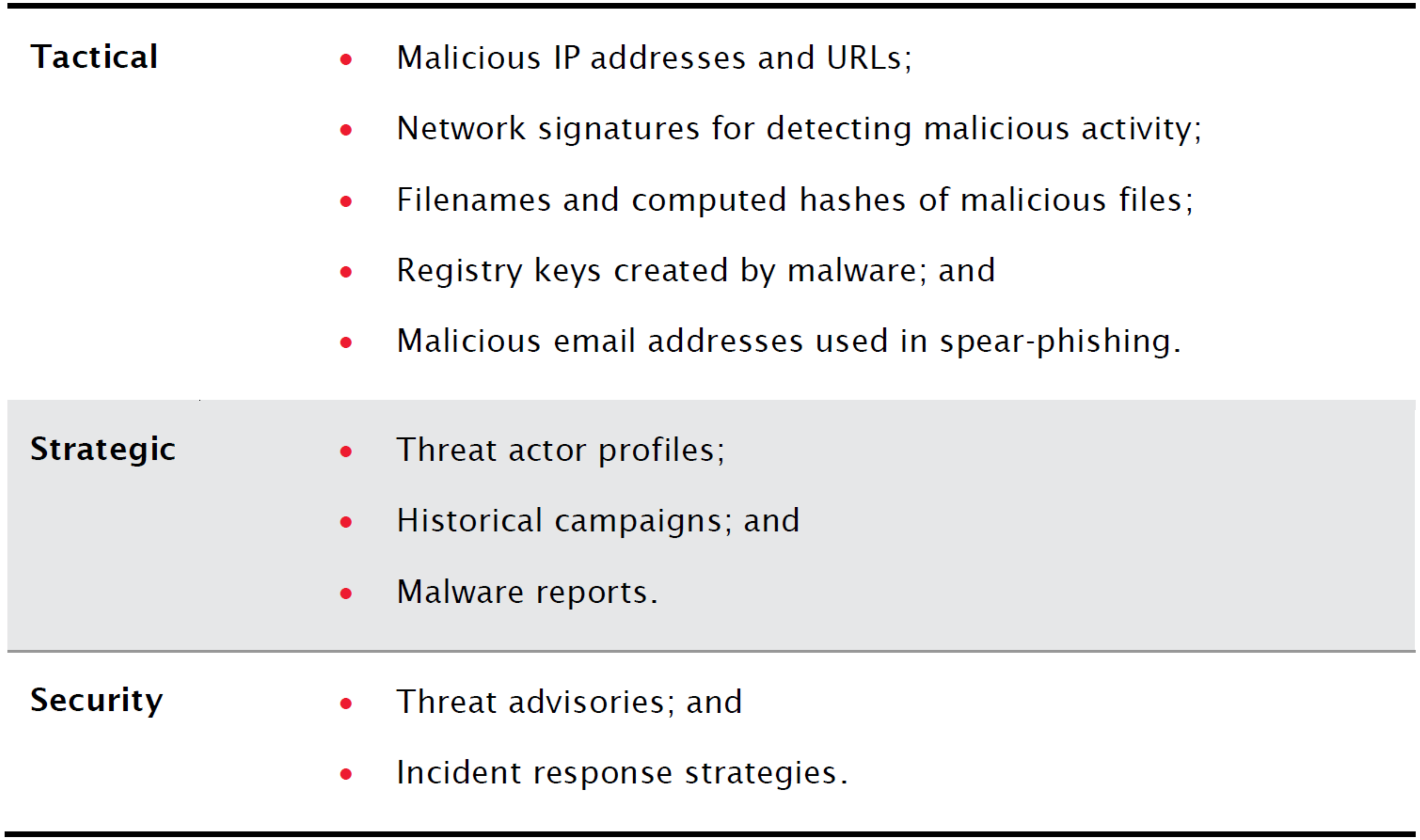
# Importance of CTI Sharing

- **Collective Defense Principle**: Sharing intelligence enables all participants to raise their defensive posture.
- **Early Warning Advantage**: Detection of Indicators of Compromise (IoCs) and TTPs before widespread exploitation.
- **Operational Efficiency**: Reduce duplication in malware analysis and incident response.
- **Strategic Impact**: Supports national cyber resilience and protection of critical infrastructure sectors

# Benefit of Effective CTI Sharing

- **Faster Incident Detection:** Reduced MTTD (Mean Time to Detect) across participating organizations.
- **Increased Situational Awareness:** Real-time visibility into global attack campaigns.
- **Enhanced Resilience:** Collective defense model strengthens entire ecosystems, not just individual entities.
- **Policy Alignment:** Facilitates joint response at national and international levels.

# Type of Shared Intelligence



| | |
|---|---|
| **Tactical** | • Malicious IP addresses and URLs;<br>• Network signatures for detecting malicious activity;<br>• Filenames and computed hashes of malicious files;<br>• Registry keys created by malware; and<br>• Malicious email addresses used in spear-phishing. |
| **Strategic** | • Threat actor profiles;<br>• Historical campaigns; and<br>• Malware reports. |
| **Security** | • Threat advisories; and<br>• Incident response strategies. |

# Example from DHS For Sharing Information :

Among examples of information that contain cyberthreat indicators businesses could submit to DHS:

- Security researchers reporting a discovery of a technique that permits unauthorized access to an industrial control system;
- Managed security service companies disclosing a pattern of domain name lookups that is believed correspond to malware infection;
- Manufacturers reporting unexecuted malware found on its network;
- Investigators reporting on the domain names associated with botnet command and control servers;
- Engineering companies victimized by computer intrusions describing the types of engineering files that appear to have been exfiltrated, as a way of warning other companies with similar assets; and
- News websites suffering distributed denial of service attacks reporting the IP addresses send malicious traffic.

# Threat Information Types

*Threat information* is any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include the following:

- ***Indicators*** are technical artifacts or observables[1] that suggest an attack is imminent or is currently underway or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message.
- ***Tactics, techniques, and procedures (TTPs)*** describe the behavior of an actor. *Tactics* are high-level descriptions of behavior, *techniques* are detailed descriptions of behavior in the context of a tactic, and *procedures* are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit.
- ***Security alerts***, also known as advisories, bulletins, and vulnerability notes, are brief, usually human- readable, technical notifications regarding current vulnerabilities, exploits, and other security issues. Security alerts originate from sources such as the United States Computer Emergency Readiness Team (US-CERT), Information Sharing and Analysis Centers (ISACs), the National Vulnerability Database (NVD), Product Security Incident Response Teams (PSIRTs), commercial security service providers, and security researchers.
- ***Threat intelligence reports*** are generally prose documents that describe TTPs, actors, types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organization. Threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
- ***Tool configurations*** are recommendations for setting up and using tools (mechanisms) that support the automated collection, exchange, processing, analysis, and use of threat information. For example, tool configuration information could consist of instructions on how to install and use a rootkit detection and removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.

# Notable Cyber Threat Information Sharing Organizations

Sharing cyber threat information between organizations has become increasingly important in recent years. Here are a few notable examples of organizations that have successfully implemented cyber threat intelligence sharing programs:

- The National Cyber Security Centre (NCSC) in the UK launched the Cyber Threats Sharing Program, which enables organizations to share threat intelligence with the NCSC in a secure manner.
- CERT-EU has also launched a secure platform that enables public and private organizations to share threat intelligence data.
- In 2015, the Obama administration directed the Cybersecurity & Infrastructure Security Agency to initiate an informational sharing and analysis initiative, which promotes threat intelligence sharing between private and public organizations.
- CISA Automated Indicator Sharing : https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais

# DHS Issues Guidance on How to Share Cyberthreat Data

Seeing Is Believing: Visualizing Best Ways to Share Threat Info

Eric Chabrow (GovInfoSecurity) • February 18, 2016

# Best Practice Cyber Threat Information Sharing

# Best Practices for Cyber Threat Information Sharing

While sharing information can be beneficial, organizations should consider a few best practices. Here are a few critical tips for successful cyber threat information-sharing:

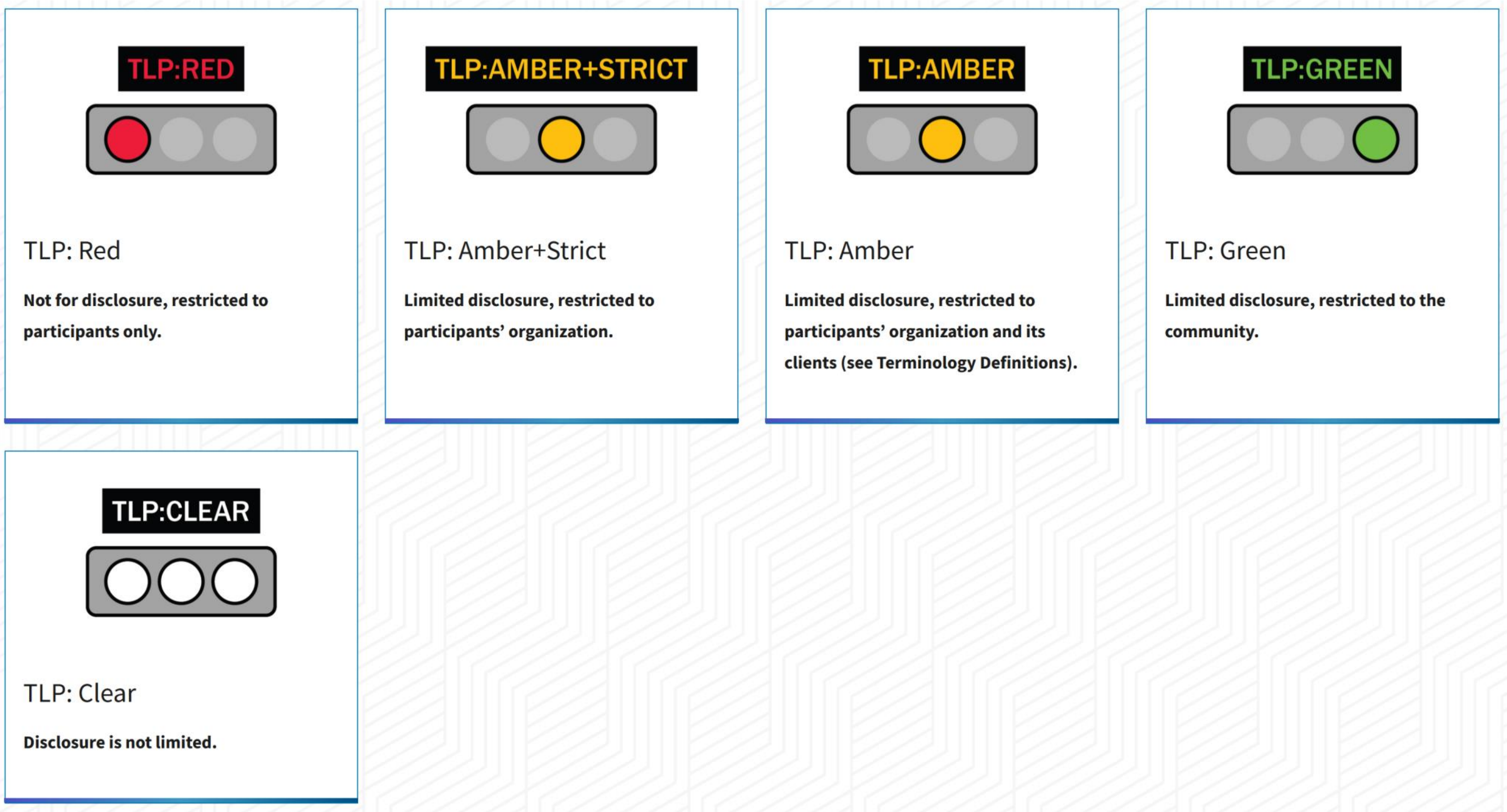
- Designate an individual or team to coordinate information sharing within the organization.
- Have protocols to ensure your organization keeps shared data secure and confidential.
- Develop a process for verifying incoming information and confirming its accuracy.
- Establish a system to track the data shared by all participating organizations.
- Develop policies and procedures for responding to threats quickly and effectively.

By taking these steps, organizations can ensure that they are effectively sharing cyber threat information in a secure manner while also staying one step ahead of would-be attackers.

# NIST SP 800-150 : Guide to Cyber Threat Information Sharing

- Identify existing internal sources of cyber threat information.
- Specify the scope of information sharing activities
- Establish information sharing rules.
- Join and participate in information sharing efforts.
- Actively seek to enrich indicators by providing additional context, corrections, or suggested improvements.
- Use secure, automated workflows to publish, consume, analyze, and act upon cyber threat information.
- Proactively establish cyber threat sharing agreements.
- Protect the security and privacy of sensitive information.

# Traffic Light Protocol V.2.0 in Information Sharing



TLP:RED

TLP: Red

**Not for disclosure, restricted to participants only.**

TLP:AMBER+STRICT

TLP: Amber+Strict

**Limited disclosure, restricted to participants' organization.**

TLP:AMBER

TLP: Amber

**Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).**

TLP:GREEN

TLP: Green

**Limited disclosure, restricted to the community.**

TLP:CLEAR

TLP: Clear

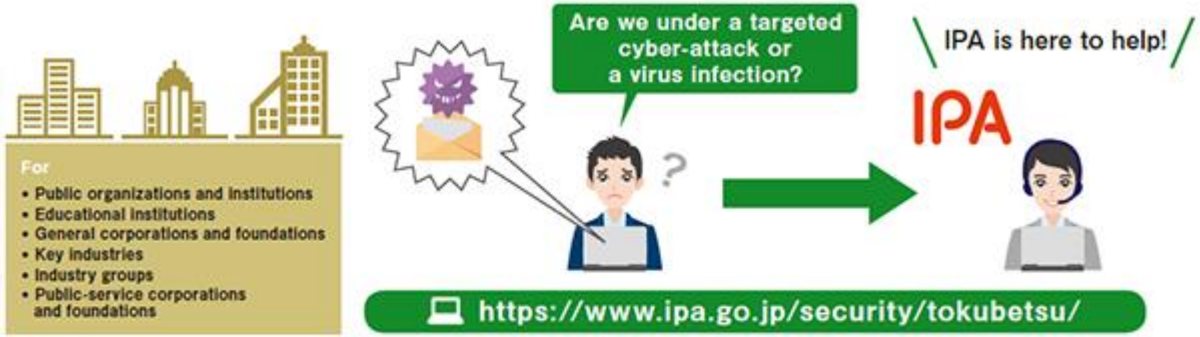
**Disclosure is not limited.**

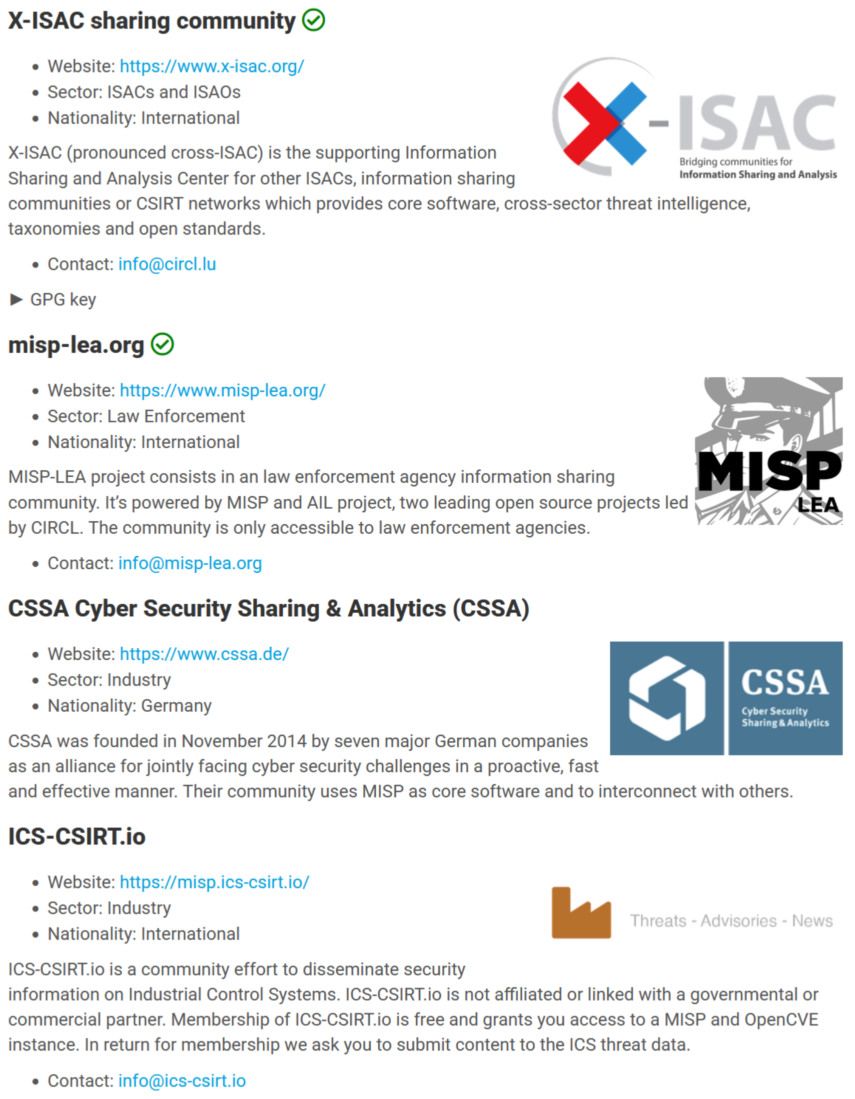
# Industry Best Practice

- **Sector-specific ISACs**: Finance, Energy, Healthcare, Aviation all use ISACs to centralize CTI.
- **Automation & Standards**: Adoption of STIX/TAXII for machine-to-machine intelligence exchange.
- **Operationalization**: Intel feeds must be integrated into SIEM/SOAR for immediate use.
- **Community Building**: Trust-based forums (closed groups, vetted memberships) enhance quality of shared data.

# International Practice

- **United States:** DHS CISA’s AIS program shares machine-readable indicators in real time.
- **European Union:** ENISA facilitates cross-border CTI exchange with a focus on GDPR compliance.
- **Asia-Pacific:** Japan’s J-CSIP promotes manufacturer collaboration, Singapore’s CTI framework integrates with ASEAN partners.
- **Global Platforms:** MISP (open-source) and threat intel alliances like Cyber Threat Alliance (CTA).


For
• Public organizations and institutions
• Educational institutions
• General corporations and foundations
• Key industries
• Industry groups
• Public-service corporations and foundations
Are we under a targeted cyber-attack or a virus infection?
?
IPA is here to help!
IPA
https://www.ipa.go.jp/security/tokubetsu/



X-ISAC
Bridging communities for Information Sharing and Analysis
MISP LEA
CSSA
Cyber Security Sharing & Analytics
Threats - Advisories - News

### X-ISAC sharing community ✓

- Website: https://www.x-isac.org/
- Sector: ISACs and ISAOs
- Nationality: International

X-ISAC (pronounced cross-ISAC) is the supporting Information Sharing and Analysis Center for other ISACs, information sharing communities or CSIRT networks which provides core software, cross-sector threat intelligence, taxonomies and open standards.

- Contact: info@circl.lu

► GPG key

### misp-lea.org ✓

- Website: https://www.misp-lea.org/
- Sector: Law Enforcement
- Nationality: International

MISP-LEA project consists in an law enforcement agency information sharing community. It’s powered by MISP and AIL project, two leading open source projects led by CIRCL. The community is only accessible to law enforcement agencies.

- Contact: info@misp-lea.org

### CSSA Cyber Security Sharing & Analytics (CSSA)

- Website: https://www.cssa.de/
- Sector: Industry
- Nationality: Germany

CSSA was founded in November 2014 by seven major German companies as an alliance for jointly facing cyber security challenges in a proactive, fast and effective manner. Their community uses MISP as core software and to interconnect with others.

### ICS-CSIRT.io

- Website: https://misp.ics-csirt.io/
- Sector: Industry
- Nationality: International

ICS-CSIRT.io is a community effort to disseminate security information on Industrial Control Systems. ICS-CSIRT.io is not affiliated or linked with a governmental or commercial partner. Membership of ICS-CSIRT.io is free and grants you access to a MISP and OpenCVE instance. In return for membership we ask you to submit content to the ICS threat data.

- Contact: info@ics-csirt.io

# Key Challenge in Implementation

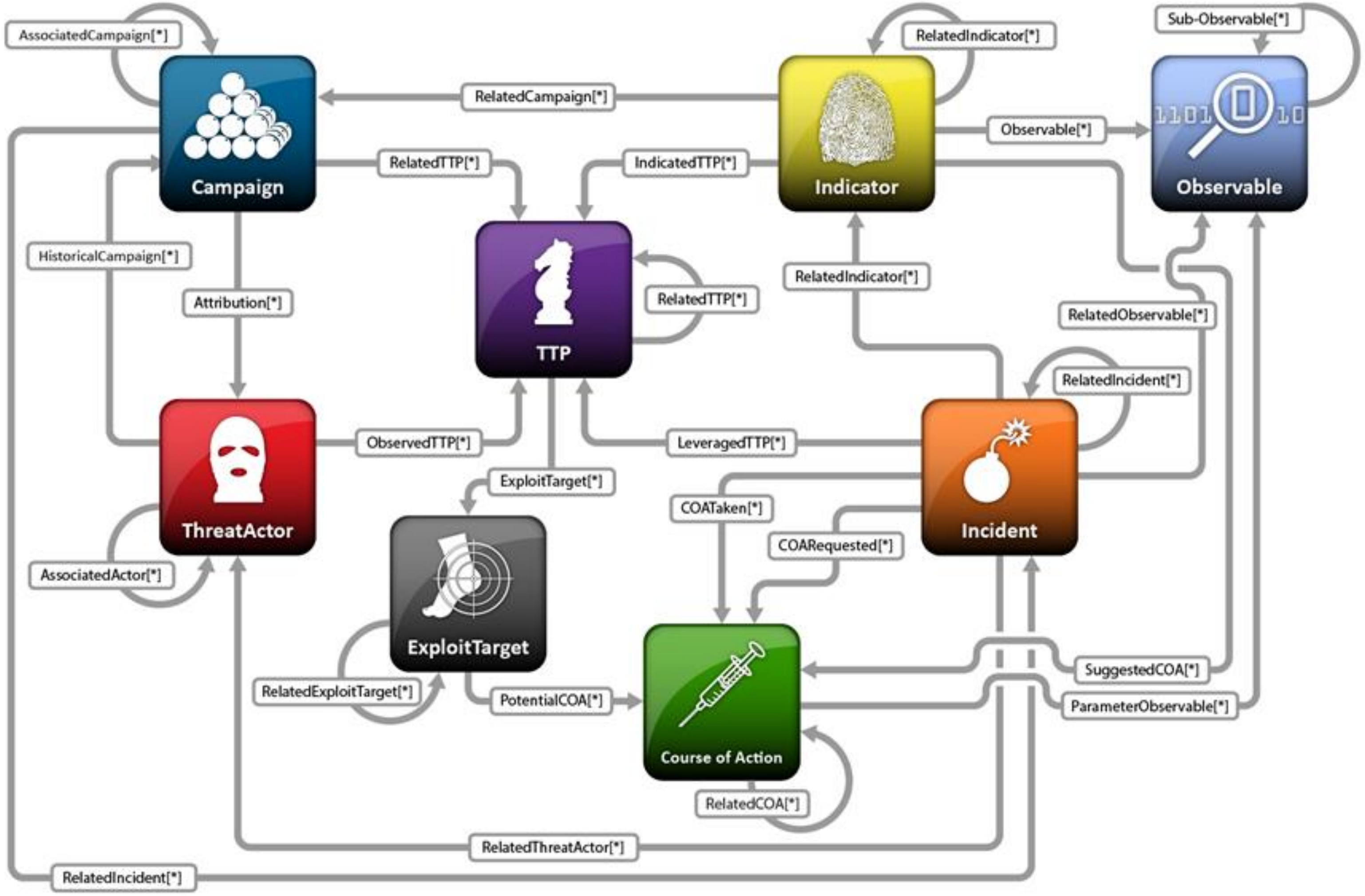
- **Trust Deficit:** Concerns about reputational damage or misuse of shared intelligence.
- **Data Sensitivity:** IoCs may contain confidential or privacy-sensitive data.
- **Legal/Regulatory Barriers:** Data protection laws (GDPR, HIPAA) limit sharing.
- **Lack of Standardization:** Different formats (CSV, JSON, PDF) slow automation.
- **Information Overload:** Low-quality feeds create “alert fatigue.”
- **Evaluating the Quality of Received Information :** Before acting on threat information, an organization needs to confirm that the information is correct, that the threat is relevant, and that the risks of using or not using the information

# Standardization and Technical Enablers

- **STIX & TAXII**: Enable structured, machine-readable intelligence exchange.
- **MISP**: Widely adopted open-source platform supporting global collaboration.
- **Automation & SOAR Integration**: Turn intelligence into automated detection & response playbooks.
- **APTs & TTPs Mapping**: Using MITRE ATT&CK to contextualize shared intelligence.

**Example**: European CERTs use MISP + ATT&CK mapping for cross-border incident coordination.

# STIX (Structured Threat Information Sharing Expression)



# Bad Intel Lives Forever!

However, threat intelligence sharing does have some disadvantages:

- Trusting other organisations
  - their analysis capabilities
  - making good decision, e.g., not submitting malware to open-source repos
- Possible intelligence gaps
- Tools simply cannot keep up with the volume
- Knowledge is power, sharing could quickly de-value the shared threat intelligence, –lifespan of OSINT vs. commercial vs. internal discovery

# Threat Intelligence Platform

# Threat Intelligence Platform

- A Threat Intelligence Platform (TIP) is an advanced cybersecurity solution designed to aggregate, analyze, and act upon threat data from various sources. By centralizing threat intelligence, a TIP helps organizations understand and mitigate potential cyber threats more effectively.
- These platforms collect data from multiple sources, including open-source intelligence, commercial threat feeds, internal security logs, and other relevant information.
- This data is then normalized, enriched, and analyzed to identify patterns, trends, and indicators of compromise (IOCs), providing security teams with actionable insights.

# Main Functions Of Threat Intelligence Platform

- The primary functions of a TIP include data aggregation, threat analysis, and integration with existing security infrastructure. Data aggregation involves collecting and consolidating threat data from diverse sources into a single platform.
- Threat analysis uses advanced algorithms and machine learning techniques to correlate and prioritize threats, enabling security teams to focus on the most critical issues.
- Furthermore, a TIP integrates with other security tools, such as Security Information and Event Management (SIEM) systems, firewalls, and intrusion detection systems, to automate responses and enhance overall security posture.
- This integration helps streamline workflows, reduces the time to detect and respond to threats, and improves the efficiency of security operations.

# Threat Intelligence Platform Features

Much of the Blue Team alerting will be based on indicator lists

- Known bad IPs, domains, hashes, etc.

Need a solution to:

- **Store analysis** and **threat information** for known indicators
- Perform **automated/fast lookups** via API
- Record context about stored items (NOT just list)
  - Ex: IP 1.2.3.4 resolved to evilsite.com serving exploit kit on 2020-02-19
- **Find associations** across multiple events
- **Sharing** of indicators with other organizations

# Threat Intelligence Platform Requirements

Indicators or low-level configuration details?

- Most TIPs handle indicators of compromise with ease
  - IP Addresses, filenames, domains, hash values, URLs, etc.
  - Important feature: **easy bulk entry and integration**
- Some TIPs do a better job with additional features
  - Are you storing **malware configurations? Non-standard fields?**
  - How do you want to **correlate** across items stored?
  - Is **sharing** a required function?
  - What **volume** of indicators will you be storing?

# Summary : Actionable Cyber Threat Intelligence

- Cyber Threat Intelligence (CTI) sharing initiatives—whether through government platforms like AIS, community-driven programs like CiSP, or sector-based ISACs—have demonstrated that **collaboration is a powerful enabler of collective defense**. However, sharing alone is not the final goal. The true value emerges when shared intelligence is **transformed into actionable insights** that directly guide security teams, policy makers, and executives in their decision-making.
- Actionable Threat Intelligence bridges the gap between **data exchange and concrete defense outcomes**. It ensures that organizations are not overwhelmed by the volume of indicators, but are instead empowered with **context-rich knowledge** that highlights relevance, urgency, and specific mitigation steps. In this sense, effective CTI sharing networks are not just information pipelines—they are catalysts for **operational resilience, strategic foresight, and adaptive defense**.
- As cyber threats continue to evolve, the future of intelligence sharing will depend on two critical factors: **trust among stakeholders** and the ability to convert shared data into intelligence that is truly actionable. In closing, it is not the act of sharing alone that secures us, but the **collective ability to act swiftly and decisively** on the intelligence we share.

“one organization’s detection to become another’s prevention”

# THANKYOU