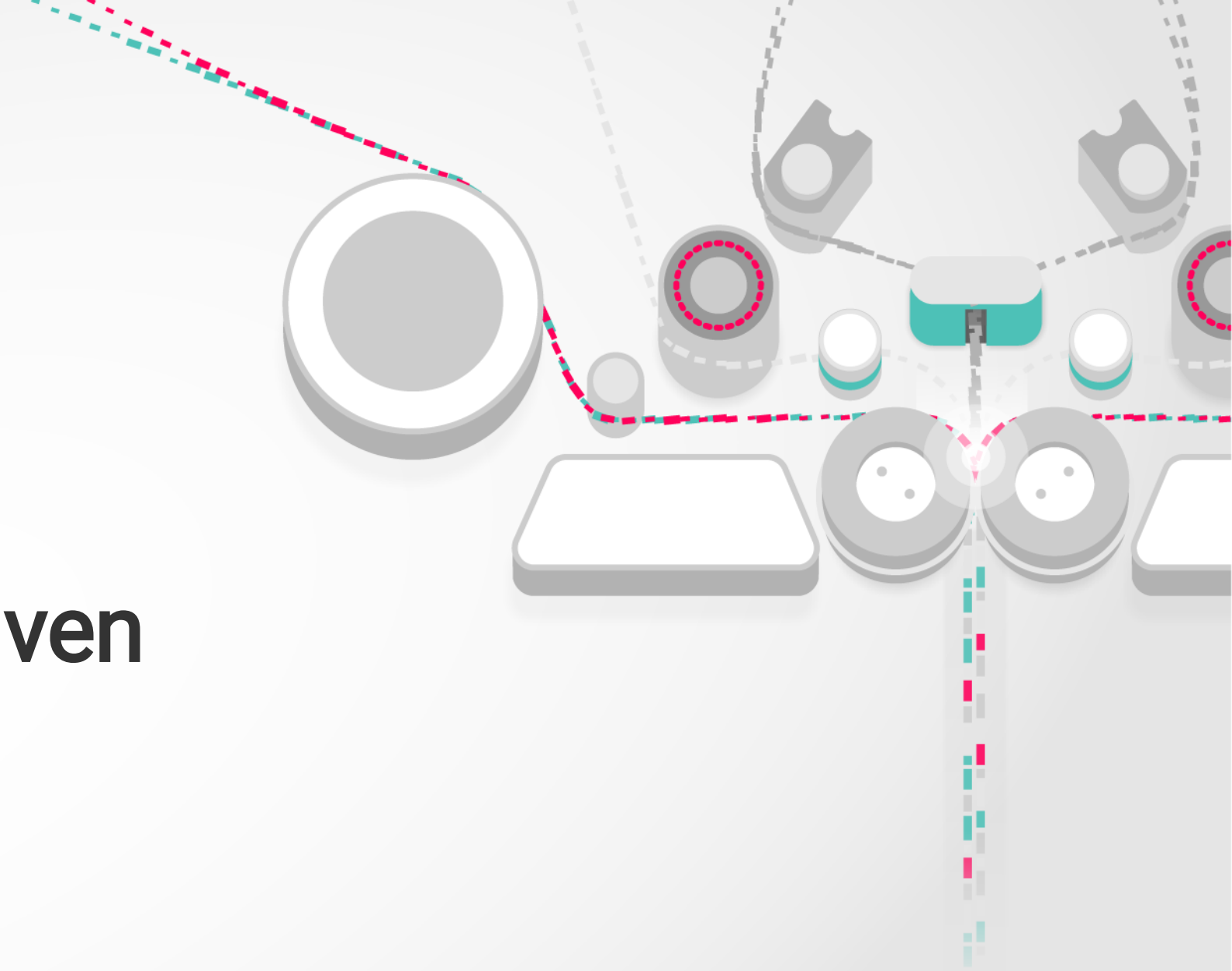
ISACA
Netherlands Chapter



Intelligence driven Cyber Defense

Herro Zoutendijk CISM, CDPSE
Regional Director EclecticIQ

⚠ views are my own

EclecticIQ

Agenda

April 29th 2021
The Netherlands

Today threats require an Intelligence driven response

- Trends in Threats
- What is Cyber Threat Intelligence (CTI)
- Example: phishing incident

CTI within your Information Security Program

- The Intelligence Cycle
- CTI Beyond IOC's
- Example: Diamond Model and a VIP data breach case

The evolution of CTI

- From early adaptors to collaboration
- From TIP to TIM
- Best practices when starting a CTI initiative

Today threats require an Intelligence driven response

EclecticIQ

Trends in Threats

Intelligent response to these challenges

BI, AI,…. Threat Intelligence

"If you know the enemy and know yourself, you need not fear the result of a hundred battles".

The Art of War by Sun Tzu (544-496 BC)

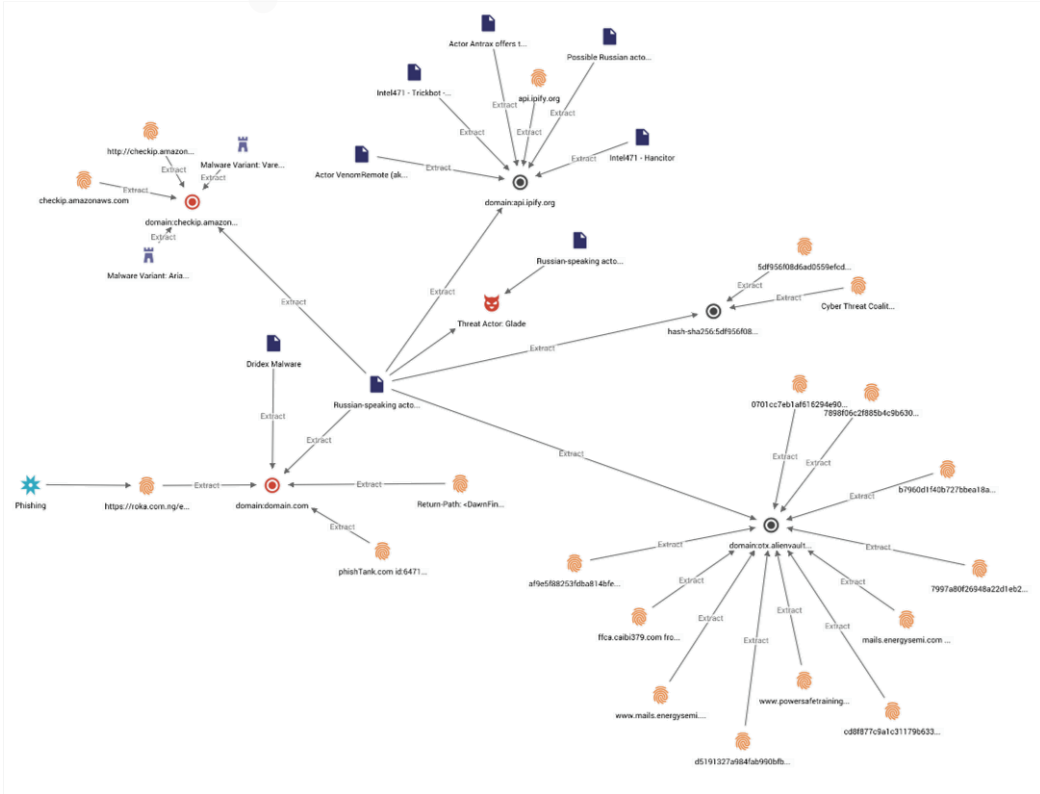
Cyber Threat Intelligence is all about knowing what your adversaries do and using that information to improve decision-making

EclecticIQ

HZ: views are my own

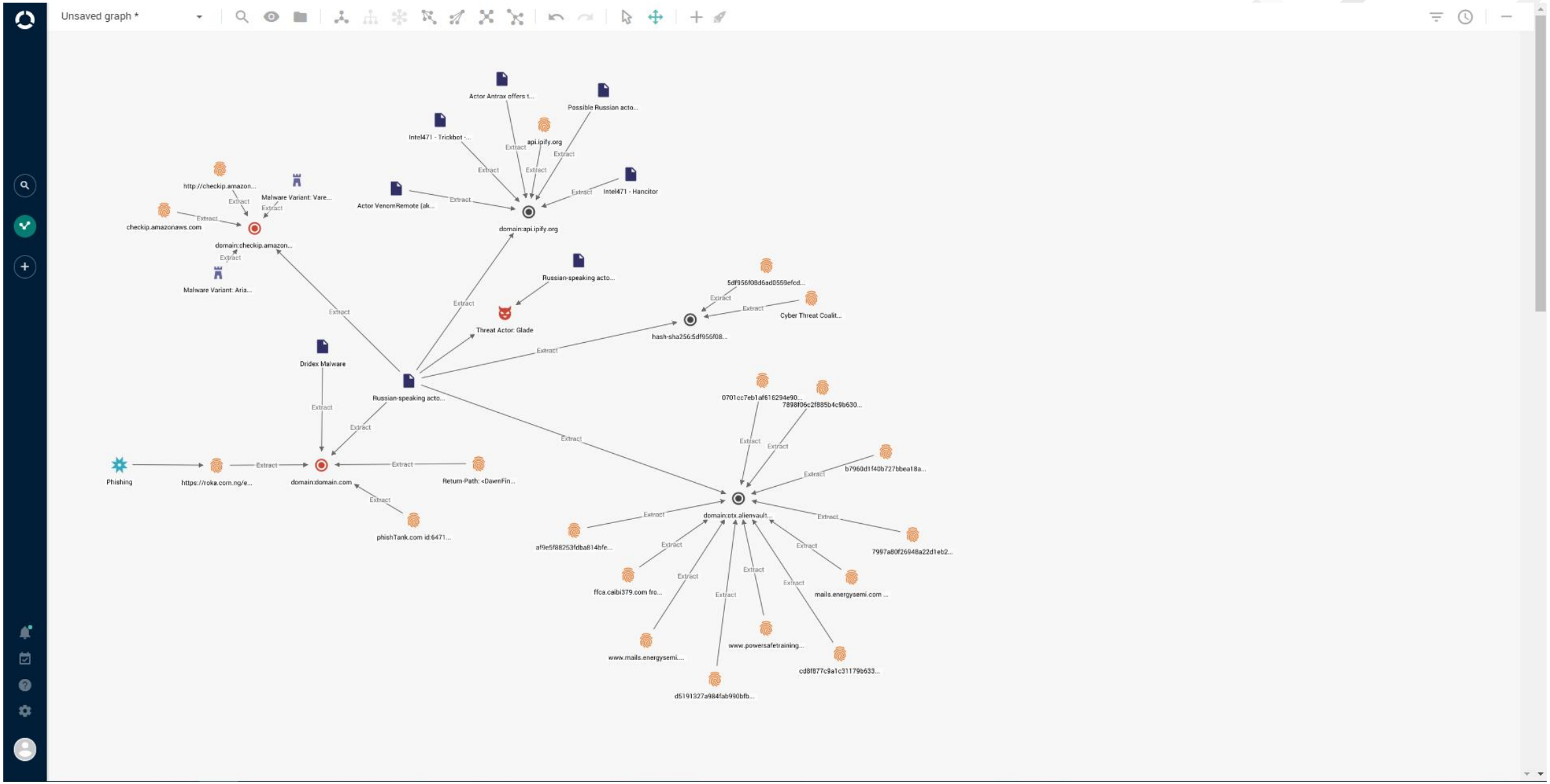
Intelligent response to these challenges

- Complexity
  - Vast amount of data
  - Connecting the dots
  - Understand what matters
- Timeliness
  - Data ingestion and automation
  - Analyst time-to-intelligence
  - Disseminate actionable intelligence
- Collaboration
  - Collective knowledge and skills
  - Frameworks and standards
  - Awareness across the organization



EclecticIQ

HZ: views are my own



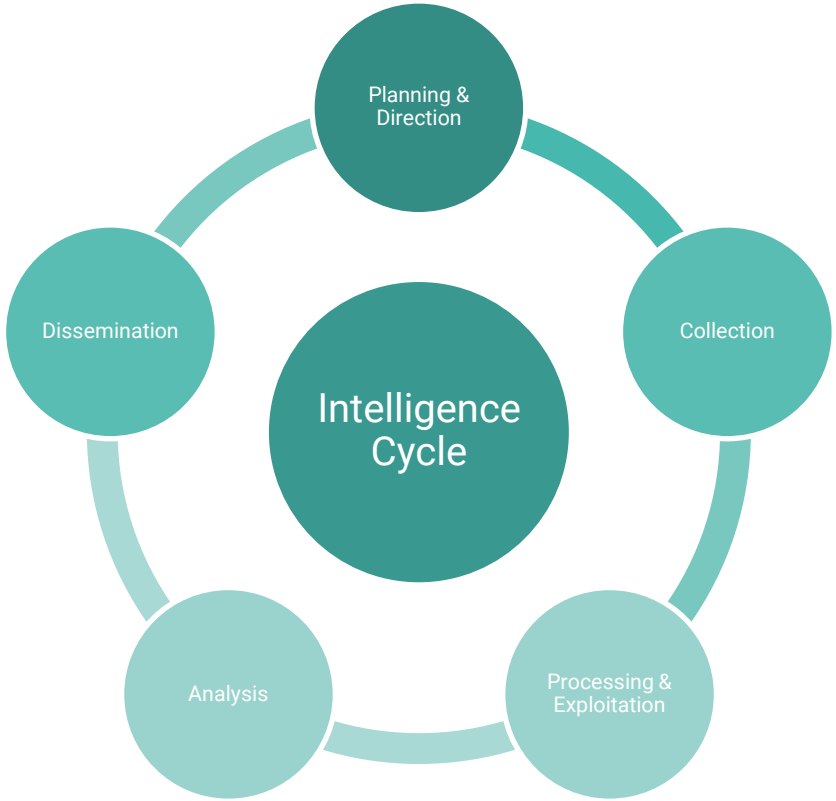
EclecticIQ

HZ: views are my own

CTI within your Information Security Program

EclecticIQ

Organizing the intelligence process



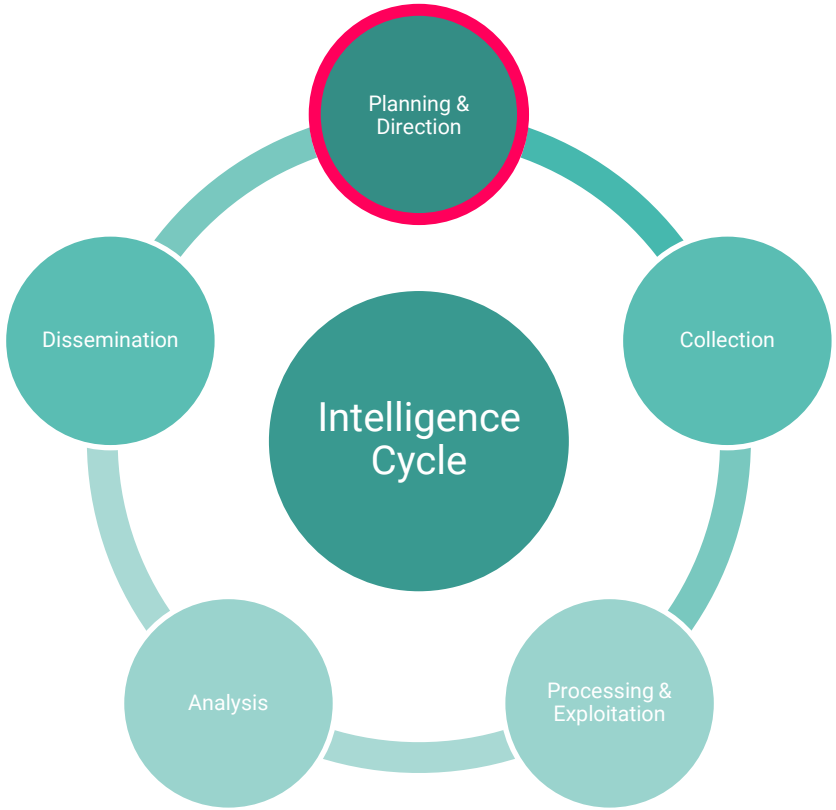
Organizing the intelligence process

Planning & Direction

1. Business Objectives, Characteristics, and Risk Appetite
2. Information Security Governance
3. Information Security Program
4. Risk Management
   - Asset identification and valuation
   - Threat Identification and scenarios
   - Likelihood and impact analysis

Frameworks

e.g. ISO, NIST, etc

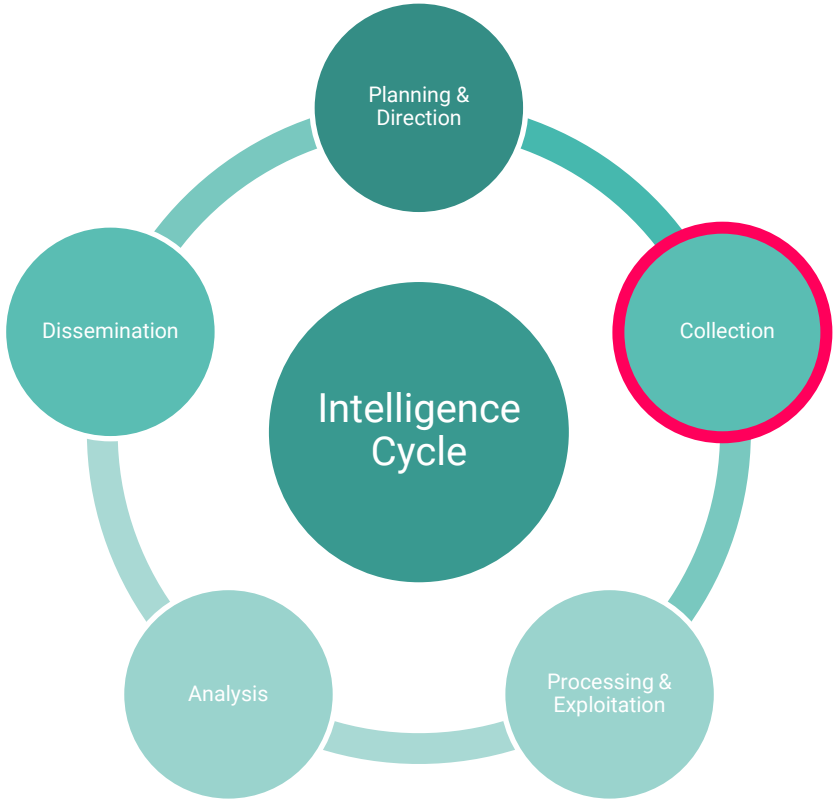


Organizing the intelligence process

Collection

1. Data Collection plan*
   - Priority Intelligence Requirement
   - Indicator
   - Specific Information Request
   - Detection Point

2. Data Acquisition plan
   - Internal: Telemetry, Reports
   - External: OS, Communities, Peers, Partners
   - External: Commercial Vendors

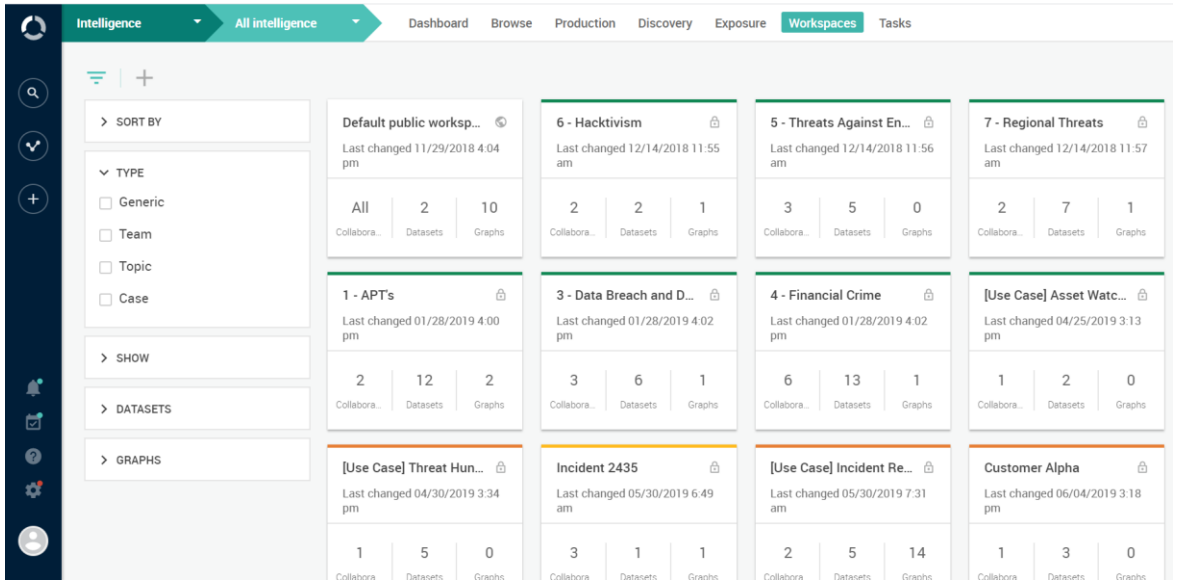


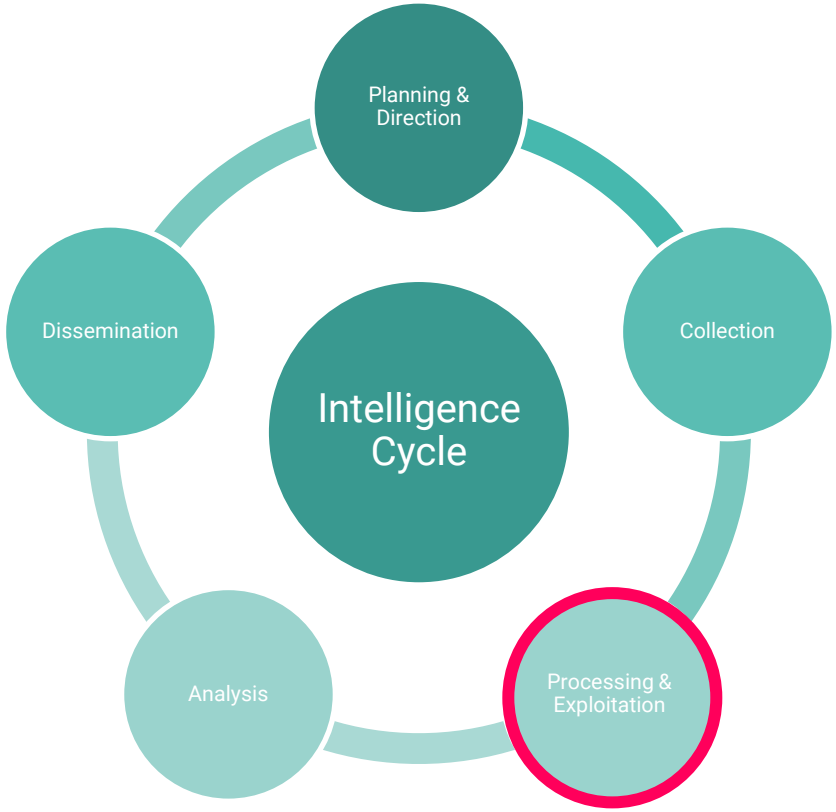
* Publicly available example at: https://www.sans.org/reading-room/whitepapers/threatintelligence/threat-intelligence-planning-direction-36857

Organizing the intelligence process

Processing & Exploitation

- Process data streams into unified Knowledge Base
- Organize along Threat Scenarios, PIRs, Teams
- Automation, Enrichment, Fusion and Discovery





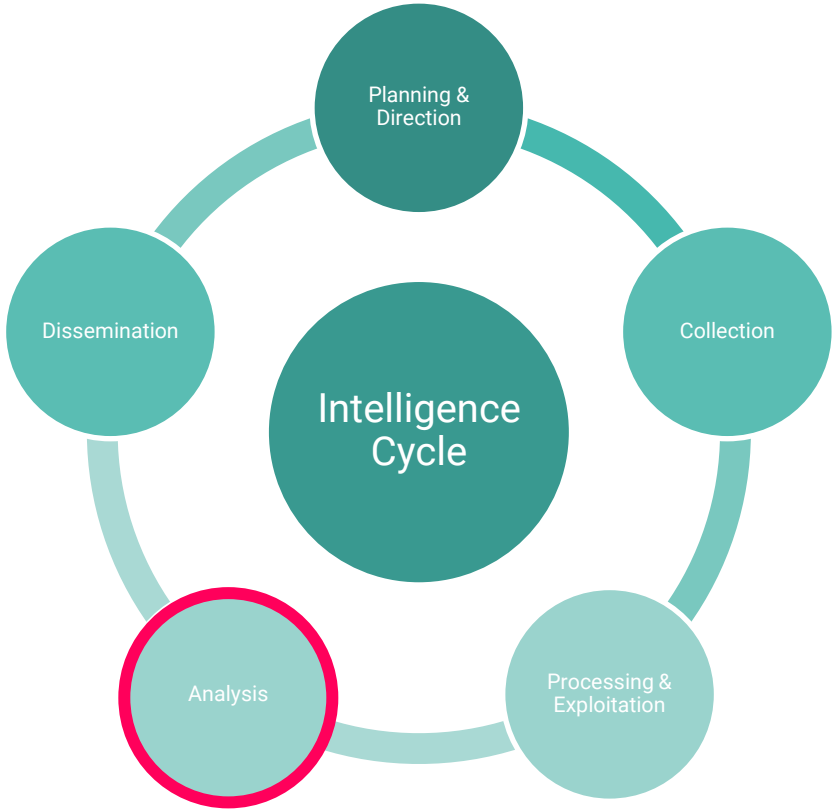
EclecticIQ

HZ: views are my own

Organizing the intelligence process

Analysis

- Standing and Specific information requirements
- IOCs, TTPs, Campaigns, Adversaries, Capabilities and Motivations
- Correlations, relevance and timely
- Team collaboration



EclecticIQ

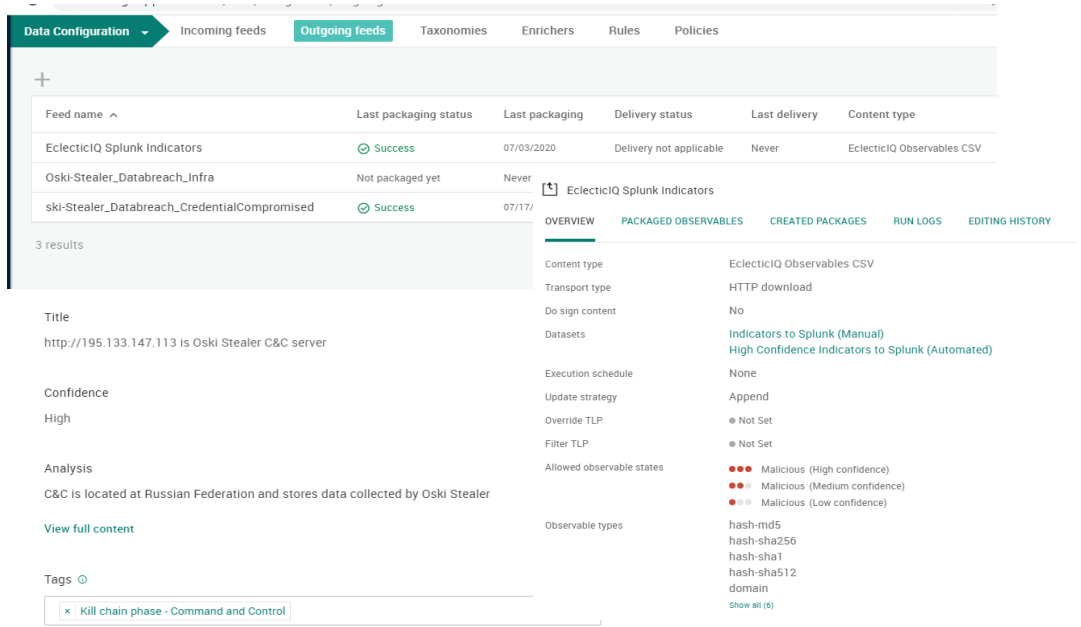
HZ: views are my own

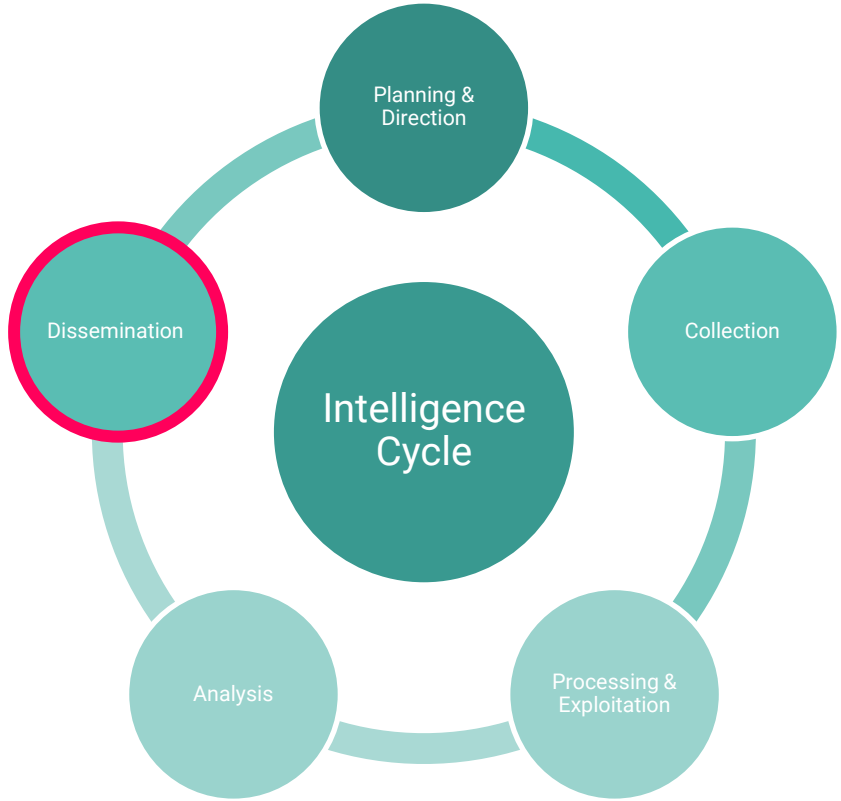
Organizing the intelligence process

Dissemination

Human Readable
- Awareness
- Mitigation Decisions
- VM, Dev, TPRM, IR & BC

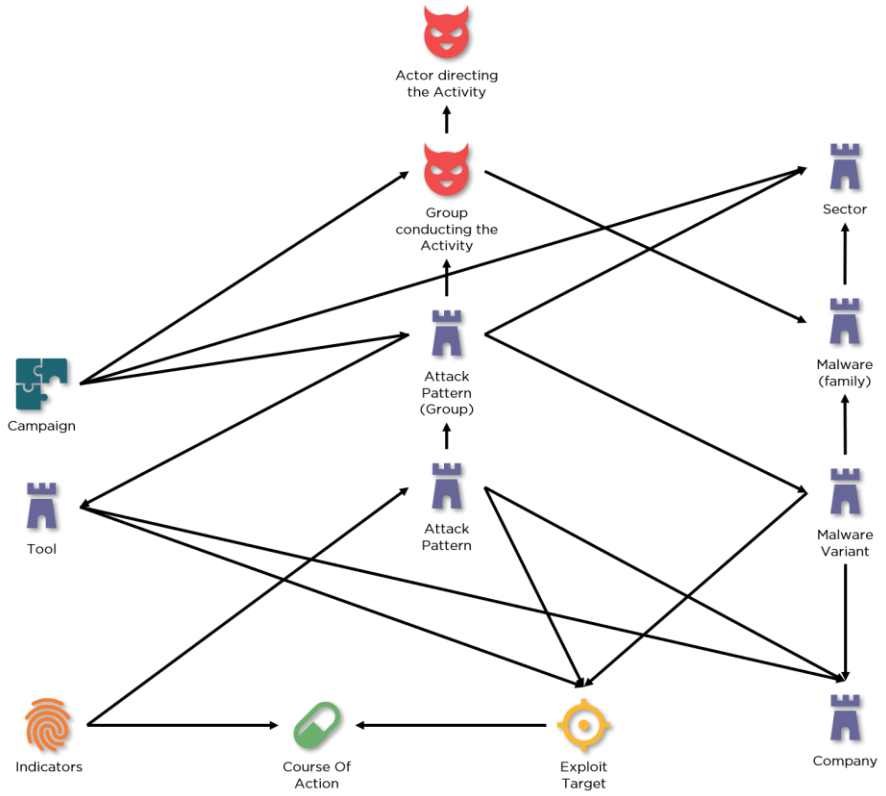
Machine Readable
- Monitoring Systems
- Network and Endpoint
- Orchestration





EclecticIQ
HZ: views are my own

On the spot

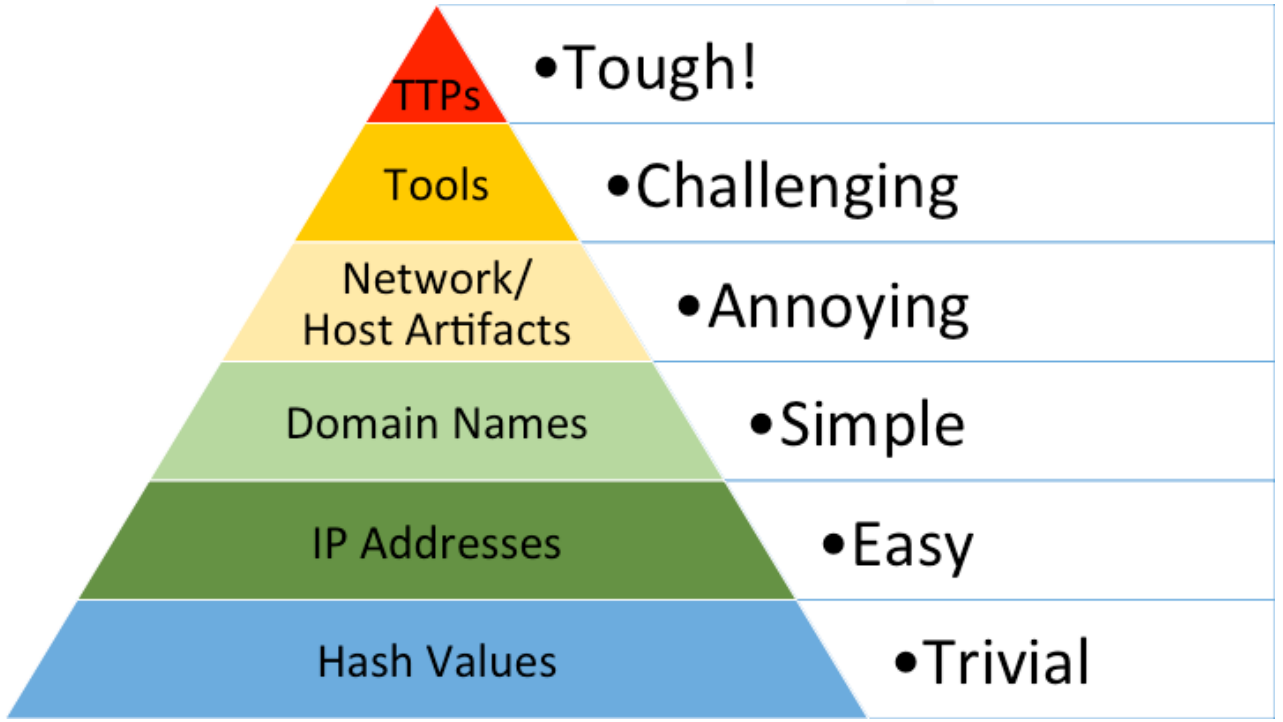


Further reading: **Beyond the IOC blog and report**

EclecticIQ
HZ: views are my own

The Pyramid of Pain

By David J Bianco



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

SingHealth Case Study

What happened?

- The database of Singapore's largest healthcare institution, SingHealth, was compromised, in what was described as a "very serious and unprecedented, massive cyberattack."

- As a result, the names, IC numbers, addresses, gender, race and dates of birth of some 1.5 million patients — including Prime Minister Lee Hsien Loong and potentially a few other ministers — were stolen.

Spot the features (1)

"About 1.5 million patients who visited SingHealth's specialist outpatient clinics and polyclinics from 1 May 2015 to 4 July 2018 have had their non-medical personal particulars illegally accessed and copied. The data taken include name, NRIC number, address, gender, race and date of birth. Information on the outpatient dispensed medicines of about 160,000 of these patients was also exfiltrated. The records were not tampered with, i.e. no records were amended or deleted. No other patient records, such as diagnosis, test results or doctors' notes, were breached. We have not found evidence of a similar breach in the other public healthcare IT systems."

- Targeting Singapore
- Targeting Health Care
- Data Theft
- Financial Data NOT stolen
- Ransomware NOT used

Spot the features (2)

"Investigations … confirmed that this was a deliberate, targeted and well-planned cyberattack. It was not the work of casual hackers or criminal gangs."

"On 4 July 2018, IHiS' database administrators detected unusual activity on one of SingHealth's IT databases.

It was established that data was exfiltrated from 27 June 2018 to 4 July 2018. SingHealth lodged a police report on 12 Jul 2018. Police investigation is ongoing.

Likely an APT

NOT Financially motivated

Knowledge: Database exfiltration

Meta: Timeframe

Spot the features (3)

"… further measures to tighten the security of SingHealth's IT systems. These include temporarily imposing internet surfing separation. We have also placed additional controls on workstations and servers, reset user and systems accounts, and installed additional system monitoring controls.

CSA has ascertained that the cyber attackers accessed the SingHealth IT system through an initial breach on a particular front-end workstation. They subsequently managed to obtain privileged account credentials to gain privileged access to the database. Upon discovery, the breach was immediately contained, preventing further illegal exfiltration.

- Phishing
- Watering Hole
- Privilege Escalation
- Lateral Movement

Spot the features (4)

“As they ransacked the system for data on PM Lee, the thieves also stole the personal data of some 1.5 million patients. What aided the hackers' plans was that they did not just look for things to steal once they entered the system - they also planned ahead. In the week prior to being discovered on July 4, they had stolen log-in credentials, covered their tracks and probed for more entry points. These entry points became windows through which other attackers could enter. These meant that when the initial attack was detected and halted, the threat did not stop. The hackers had initially entered the system via a malware-infected SingHealth front-end workstation.


Targeting Gov Official


Long Term Access > Exfil


Worked in Teams

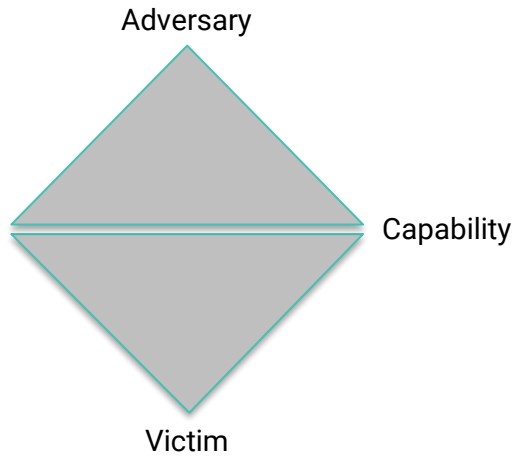

Persistent


Malware

EclecticIQ
HZ: views are my own

Diamond Model

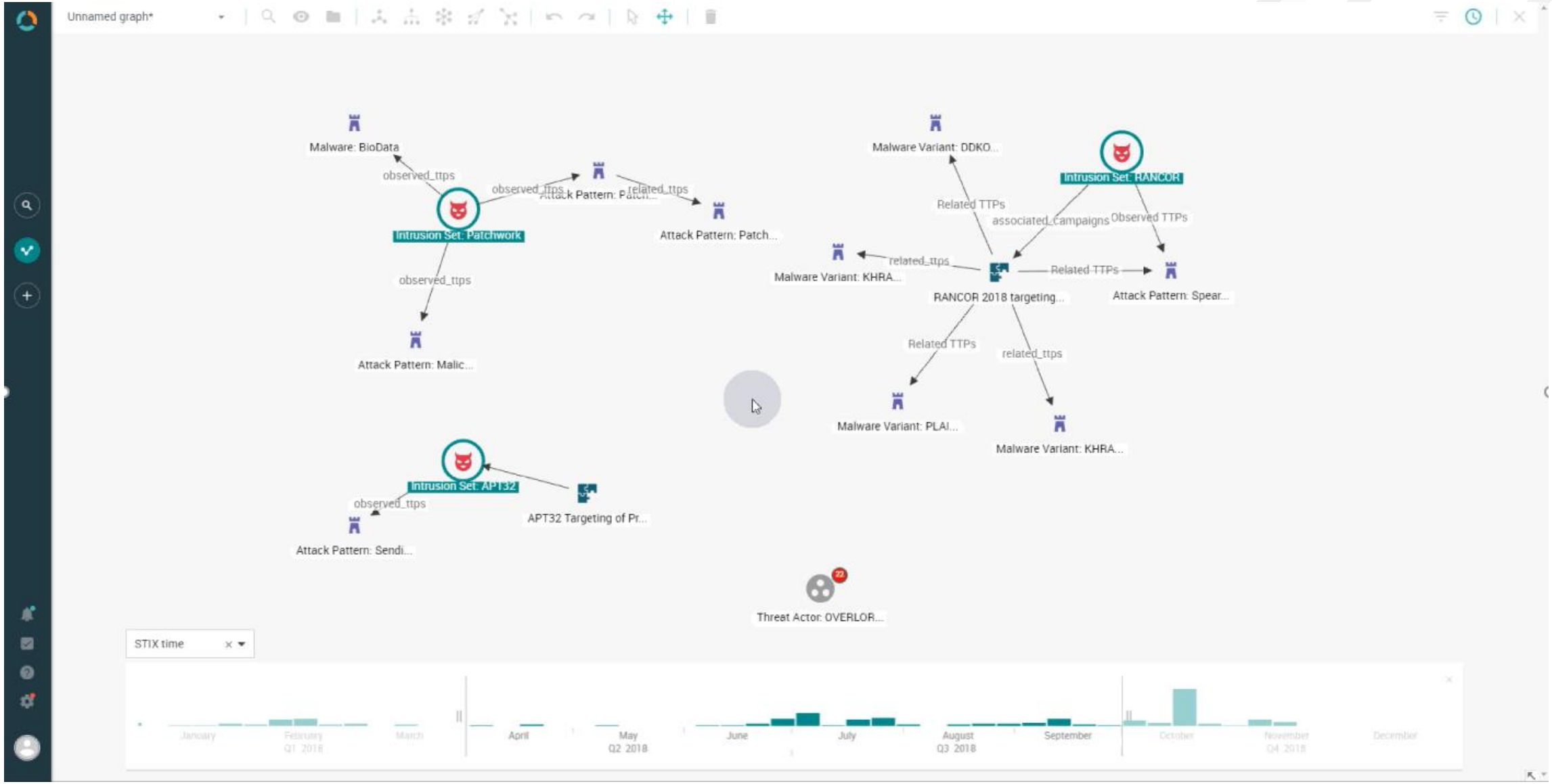
- Long Term Access > Exfil
- Worked in Teams
- Likely an APT, especially persistent
- NOT Financially motivated



- Malware

- Knowledge: Database exfiltration
  - Phishing
  - Watering Hole
  - Privilege Escalation
  - Lateral Movement
  - Ransomware NOT used
  - Data Theft
  - Financial Data NOT stolen

- Targeting Singapore Gov Official
- Targeting Health Care

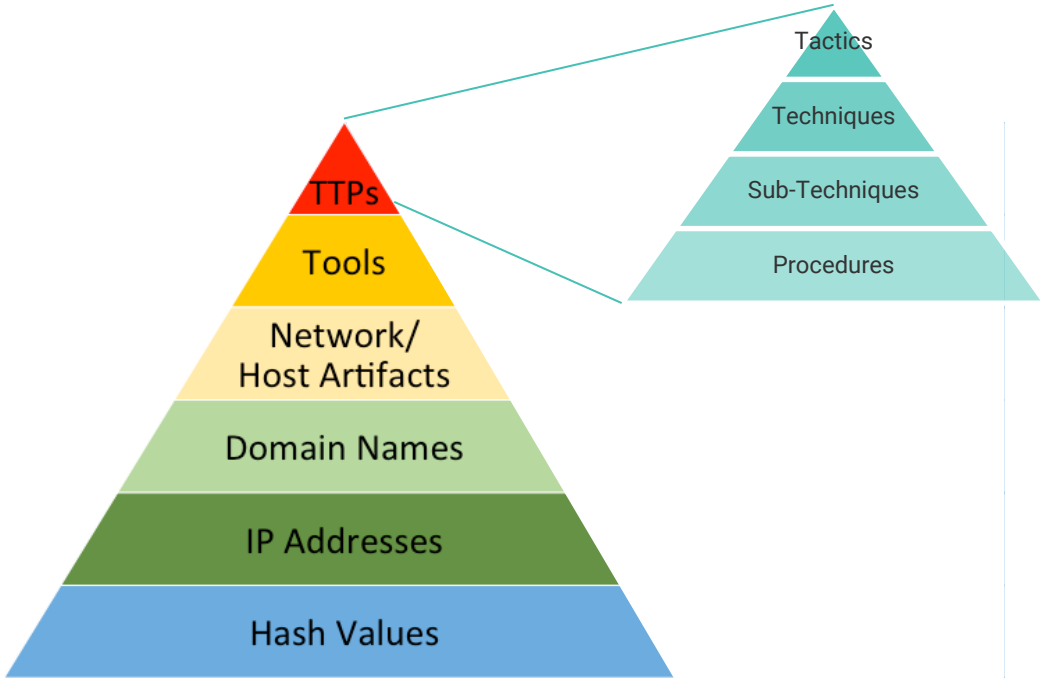


EclecticIQ

HZ: views are my own

MITRE | ATT&CK®

- Knowledge base of adversary behaviors
- Based on real-world observations
- Free, open and globally accessible
- Community contribution driven
- Framework updated 2x per year



MITRE | ATT&CK®

Enterprise Matrix

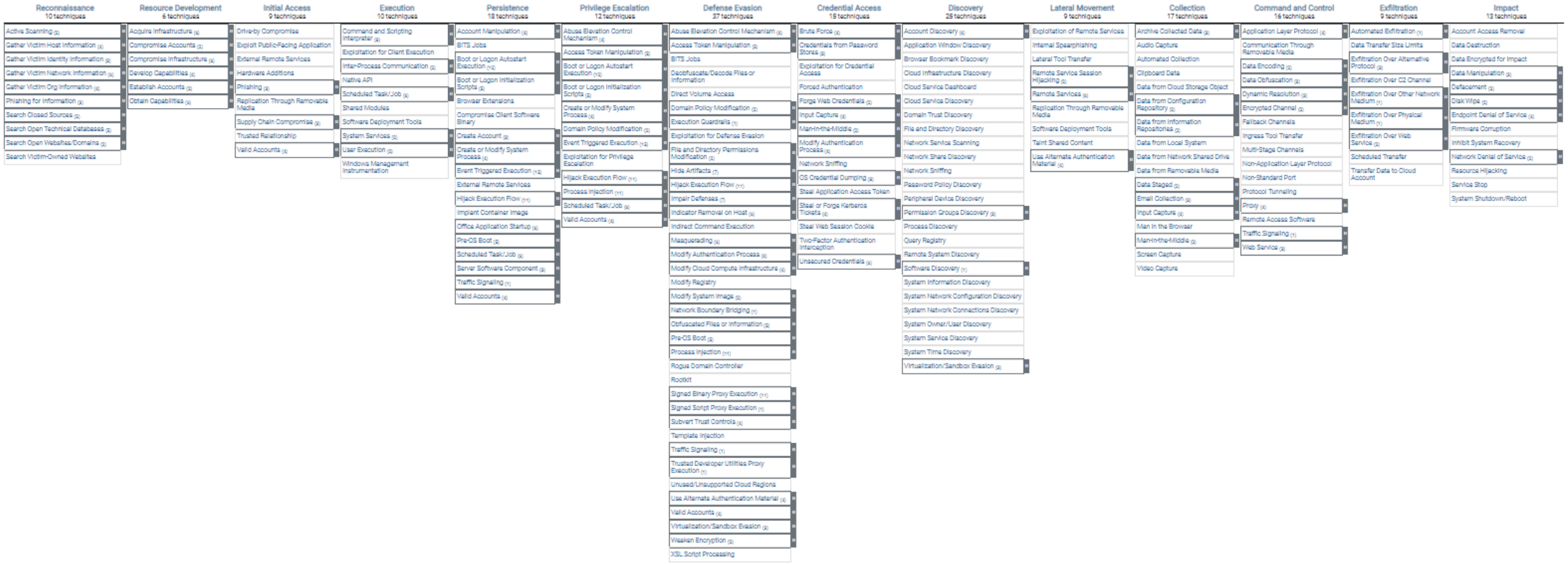
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Network.

View on the ATT&CK® Navigator

About the Enterprise domain

Version Permalink

layouts | show sub-techniques | hide sub-techniques | help



icIQ

HZ: views are my own

The evolution of CTI

EclecticIQ

Threat Intelligence Market Evolution

CTI Practice with TIP
Threat Intelligence Platform

- Threat intelligence content and management
- Collaboration and exchange

Security Operations with TIM
Threat Intelligence Management

- Threat intelligence content and management
- Threat detection and SecOps enablement
- Threat hunting
- End-point detection and response
- Threat detection
- Security event storage and analytics

EclecticIQ
HZ: views are my own

TIM-enabled NextGen SOC Platforms

DtSR Episode 428 - TPA TIM-enabled NextGen SOC Platforms

DOWN THE SECURITY RABBITHOLE PODCAST

DtSR Episode 428 - TPA TIM-enabled NextGen SOC Platforms

30 00:00:00 / 00:33:39 30 libsyn

Jan 5, 2021

Prologue

Let's start 2021 off right with a returning guest whose name you will want to remember. Joep (pronounced like "soup" but with a "you") Gommers the founder and CEO of EclecticIQ joins Rafal to talk about threat intelligence - from platforms to TIPs, use-cases, implementations, limitations, and the move to TIM. It's a fun conversation that looks at where "threat intelligence" started, and where it's gone over the last 5 years or so. If you're a threat intel analyst, another consumer, or even a vendor, you'll want to listen up carefully and maybe take notes.

By the way we need a "TIM-enabled NextGen SOC Platform" sticker to be made up, with "Tim the Enchanter" as the key figure ... this should happen. Someone has to have the talent!

Guest

- **Joep Gommers**
  - LinkedIn: https://www.linkedin.com/in/joepgommers/
  - Twitter: https://twitter.com/joepgommers

http://podcast.wh1t3rabbit.net/dtsr-episode-428-tpa-tim-enabled-nextgen-soc-platforms

Best practices when starting a CTI initiative

- Make room on the org chart. Lock down IT capacity;
- Build a well-balanced core team;
- Manage the right collection of CTI feeds;
- Bootstrap with technology platforms;
- Deliver stakeholder-focused CTI solutions;
- Achieve stakeholder buy-in;
- Provide specific support to stakeholder groups.

- Security Operations Centers (SOCs)
- Vulnerability Management teams
- Incident Response and Operations (IR)
- Network Operations
- IT and Security Architects
- Risk Management Team
- Business stakeholders
- Executives and decision-makers
- Constituents, Customers

More at https://go.eclecticiq.com/resources/white-paper-building-cyber-threat-intelligence-practice

EclecticIQ

HZ: views are my own

Other considerations

Business context

- Strategy, Risk Appetite, Threat Scenarios

Use Cases

- IOC aggregation, Discovery, Threat Actor Monitoring, SOC augmentation, Collaboration, …..

Data Sources

- Volume & variety & velocity → sets reqs for completeness and robustness of the ingestion process

Team

- Maturity, teamwork, efficiency, tools

CTI Vendor

- Content / DRP / TIP, TIP emphasis, journey

Questions

Intelligence driven Cyber Defense

If a next session in 2H 2021, what topic do you prefer?

- Intelligence and collaboration
- Intelligence & Hunting & Responding
- Intelligence Tradecraft
- ……

Herro Zoutendijk CISM CDPSE
Regional Director @ EclecticIQ
herro@eclecticiq.com
https://www.linkedin.com/in/herrozoutendijk/