

# Intelligence driven Cyber Defense

Herro Zoutendijk CISM, CDPSE Regional Director EclecticIQ





# Agenda

April 29<sup>th</sup> 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



#### **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".

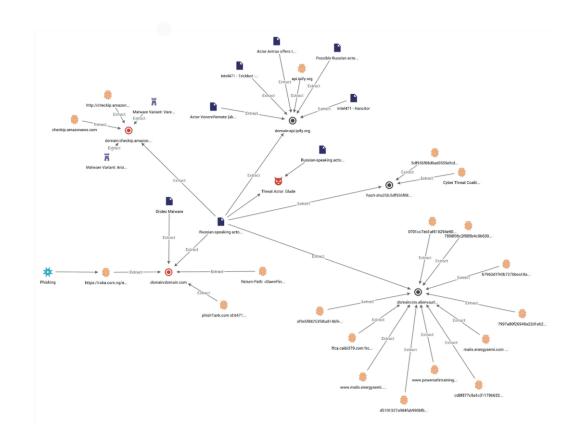
The Art of War by Sun Tzu (544-496 BC)

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

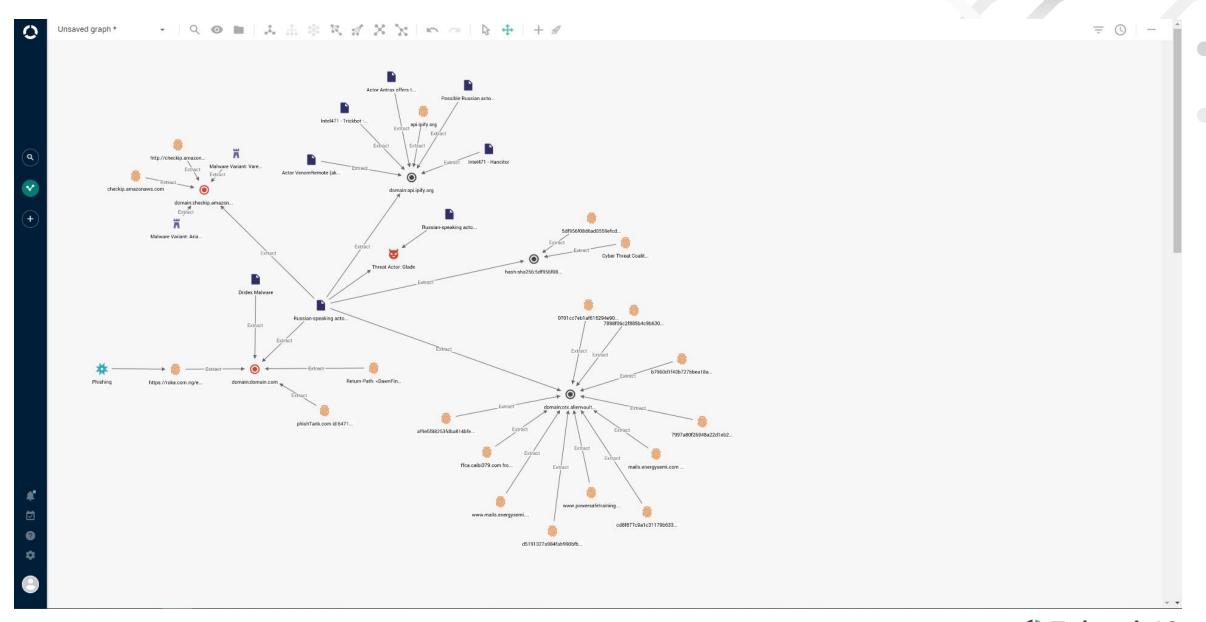


### Intelligent response to these challenges

- 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



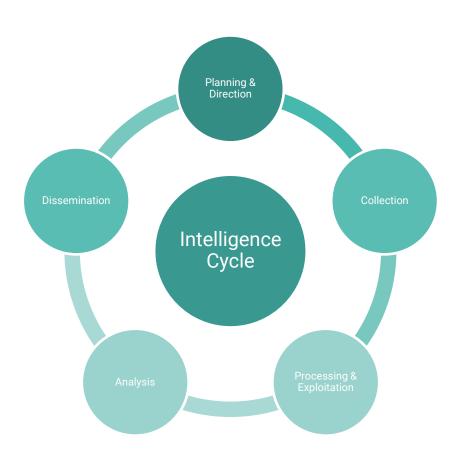






### CTI within your Information Security Program





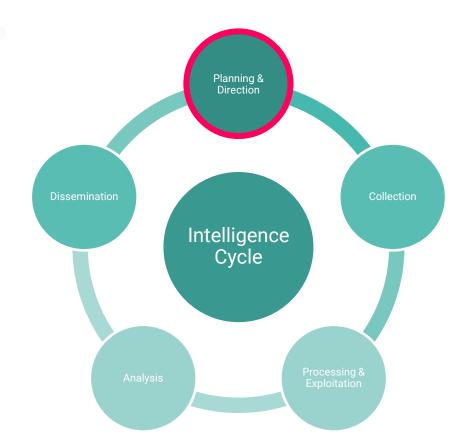


#### **Planning & Direction**

- 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

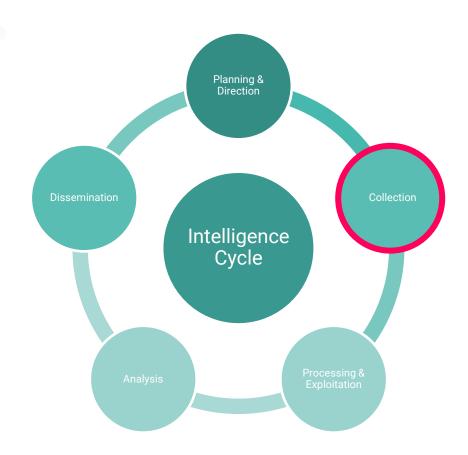
e.g. ISO, NIST, etc





#### **Collection**

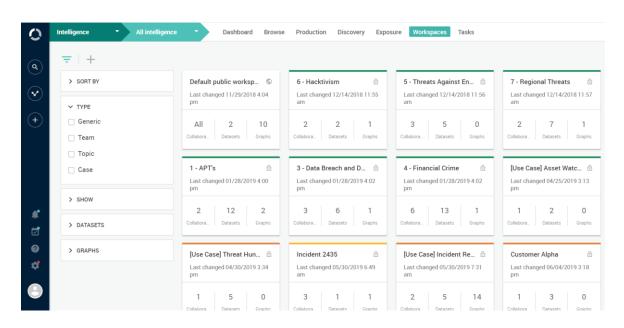
- Data Collection plan\*
  - Priority Intelligence Requirement
  - Indicator
  - Specific Information Request
  - Detection Point
- 2. Data Acquisition plan
  - Internal: Telemetry, Reports
  - External: OS, Communities, Peers, Partners
  - External: Commercial Vendors

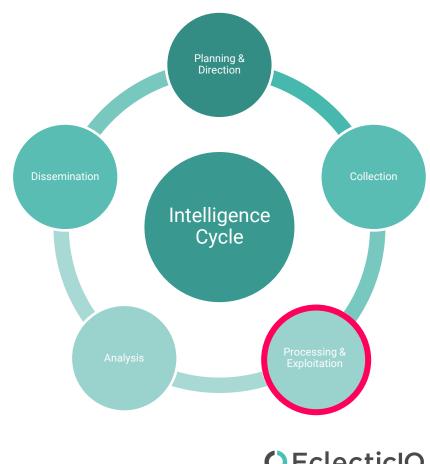




#### **Processing & Exploitation**

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

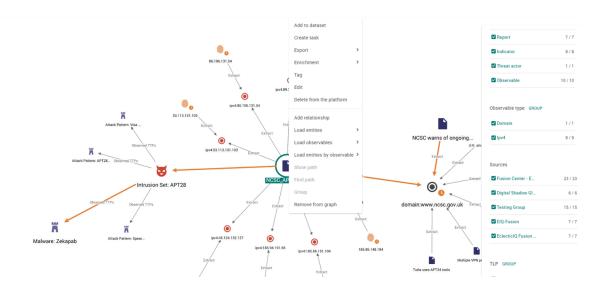


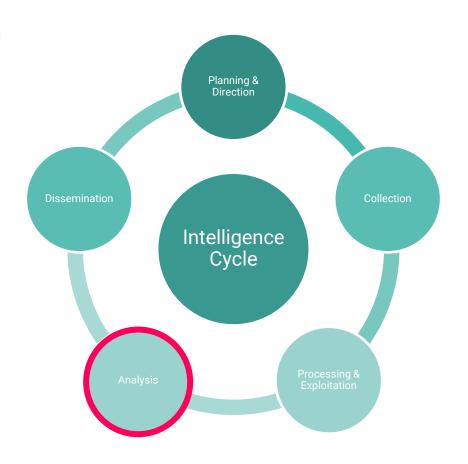




#### **Analysis**

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







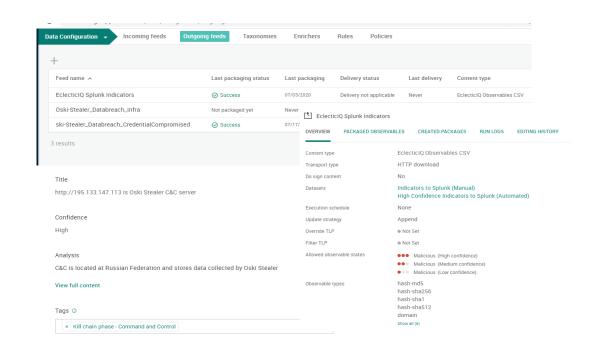
#### **Dissemination**

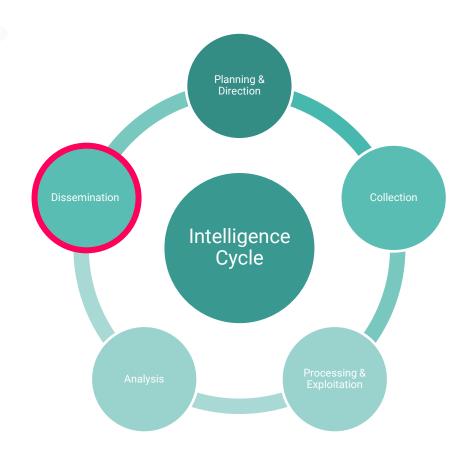
#### **Human Readable**

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

#### Machine Readable

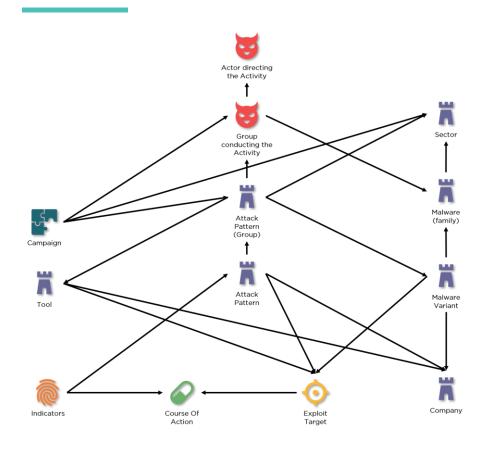
- Monitoring Systems
- Network and Endpoint
- Orchestration







### On the spot

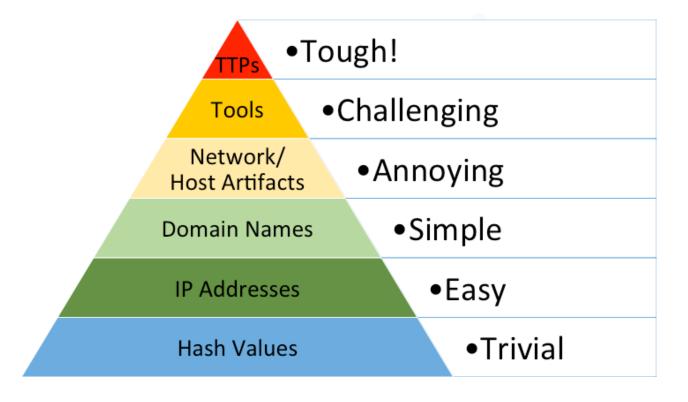






### The Pyramid of Pain

By David J Bianco





### 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."













### 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.







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.











### 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.



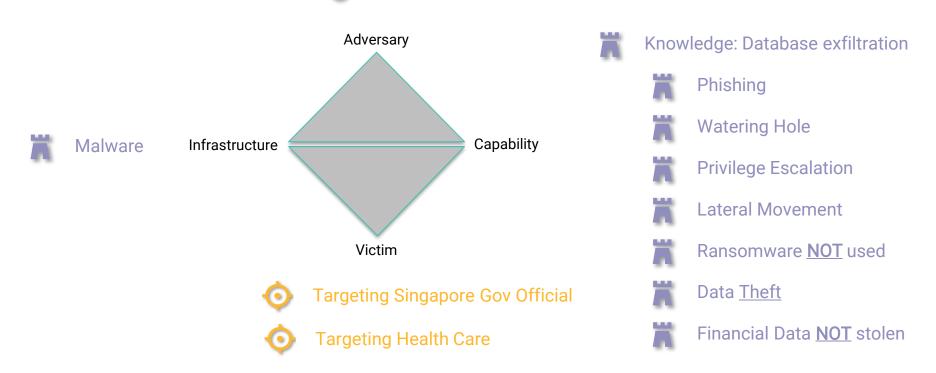


- Worked in Teams
- Persistent
- Malware

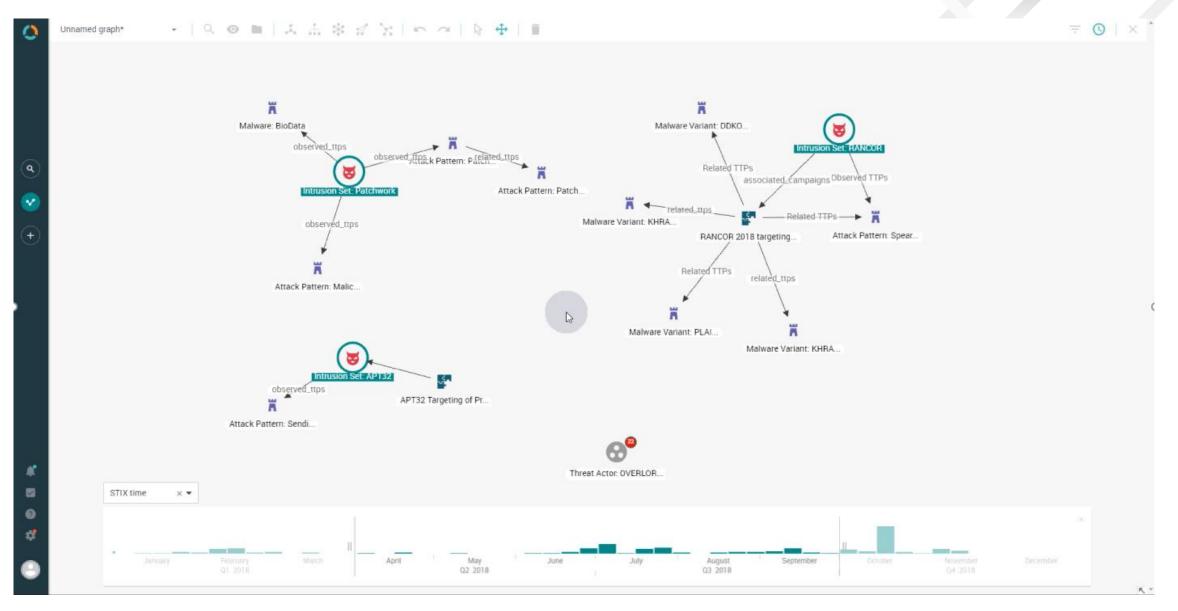


#### **Diamond Model**

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



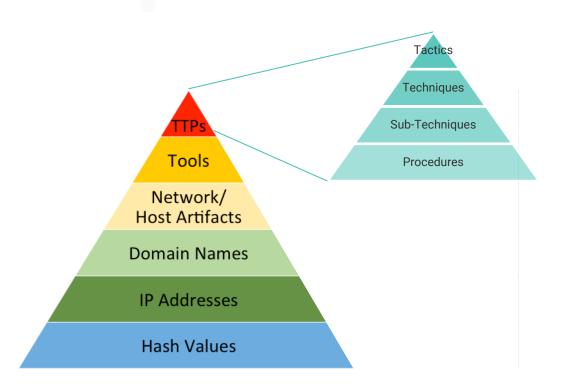






## MITRE | ATT&CK°

- 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<sup>®</sup> Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, AWS, GOP, 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 Reconnaissance 10 techniques Initial Access 9 techniques Execution 10 techniques Persistence 18 techniques Privilege Escalation 12 techniques Defense Evasion 37 techniques Credential Access Discovery 25 techniques Lateral Movement Command and Control Exfiltration 9 techniques Impact 13 techniques Resource Development Collection 6 techniques 15 techniques 9 techniques 17 techniques 16 techniques Active Scenning (3) use Elevation Control se Elevation Control Machanism Exploitation of Remote Services Archive Collected Date (x) tomated Exfiltration (t) ount Access Removal Autometed Collection Data Encoding (2) oot or Logon Autostart Exploitation for Credential Sather Victim Network Information (s ardware Additions bfuscate/Decode Files or Cloud Infrastructure Discovery Remote Service Session lpboard Data velop Capabilities (c) ete Obfuscation (a) tration Over C2 Channel Boot or Logon Initialization Cloud Service Deshboard Gather Victim Org Information (6) stablish Accounts (2) shing (2) ot or Logon Initialization efacement (2) Scheduled Task/Job (s ct Volume Access Remote Services (6) namic Resolution (g) tration Over Other Netw hishing for information (a) btain Capabilities (e) Browser Extensions Forge Web Credentials (2) ud Service Discovery Data from Configuration leplication Through Removable Wipe (S) Create or Modify System Replication Through Removable Compromise Client Software Binary Search Closed Sources (2) main Trust Discovery nout Capture on fitration Over Physical Supply Chain Compromise (a) Data from Information twere Deployment Tools cution Guardralia N Ilback Channels omain Policy Modification (z. fan-In-the-Middle (2) le and Directory Discover Search Open Technical Databases (5) Software Deployment Tools ware Corruption Repositories (2) igress Tool Transfer Orfitration Over Web Trusted Relationship System Services (2) Create Account (g) oftation for Defense Evasion twork Service Scenning Taint Shared Content ibit System Recovery Search Open Websites/Domains on fodify Authentication Date from Local System Valid Accounts on User Execution (2) Create or Modify System le and Directory Permissions Multi-Stage Channels ploitation for Privilege atwork Share Discovery Use Alternate Authentication Date from Network Shared Drive letwork Denial of Service // Search Victim-Owned Websites Scheduled Transfer letwork Sniffing Windows Management Instrumentation ion-Application Laver Protocol Event Triggered Execution As de Artifects 🕾 letwork Sniffing Data from Romovable Media Transfer Date to Cloud Resource Hillacking lack Execution Flow 3S Credential Dumping (g) on-Standard Port Date Steged (2) External Remote Services lack Execution Flow assword Policy Discovery Service Stop cess injection we Steel Application Access Toke tocol Tunneling Email Collection (s). System Shutdown/Reboot Hillack Execution Flow on nneir Defenses 🕾 Perinheral Device Discovery cheduled Task/Job iss Steel or Forge Kerberos Implant Container Image dicator Removal on Host (s rmission Groups Discovery in Input Capture (4) alld Accounts (4) omnto Annoco Software Office Application Startup (s) direct Command Execution Steel Web Session Cookle Process Discovery Man in the Browser Traffic Signaling (t) Pre-OS Boot (8) Masguerading (s) Two-Fector Authentication Query Registry Man-In-the-Middle (3) Web Service (8) Scheduled Task/Job (s) Modify Authentication Process (4) lemote System Discovery Screen Capture nsecured Credentials (s) Server Software Component (x) Modify Cloud Compute Infrestructure Software Discovery (t) Modify Registry Valid Accounts (4) Modify System Image (3) System Network Configuration Discovery Network Boundary Bridging (1) System Network Connections Discovery Obfuscated Files or Information (s) System Owner/User Discovery Pre-OS Boot (2) System Service Discovery Process Injection (10) System Time Discovery Virtualization/Sandbox Evasion (2) Roque Domain Controller Signed Binary Proxy Execution Av Subvert Trust Controls // Termilate Injection Trusted Developer Utilities Proxy Execution (n) /Irtualization/Sandbox Evasion (x) Weaken Encryption (2) XSL Script Processing

### The evolution of CTI



### **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

End-point detection and response

Threat detection and SecOps enablement

Threat detection

Threat hunting

Security event storage and analytics



#### TIM-enabled NextGen SOC Platforms



#### DtSR Episode 428 - TPA TIM-enabled NextGen SOC Platforms



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 Eclectic Q 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 Gommer
  - LinkedIn: https://www.linkedin.com/in/joepgommers/
  - o 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



#### 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/