CYBERNEWSFEED TECHNOLOGY

OVERVIEW & DEMO

AGENDA

- RELEVANT CYBER THREAT NEWS? THE PROBLEM
- PROBLEM AND IMPACT TO STAKEHOLDERS
- FIT INTO BIG PICTURE :CYBER SECURITY LEGISLATION DIRECTIVE FOR EUROPEAN UNION
- REQUIREMENT COMPONENTS: NEEDS(WHAT? & WHY?) AND PRIORITY
- SOLUTION: MODULE MAPPING-PROCESSES,ACTIVITIES AND TOOLS
- OPINIOINS

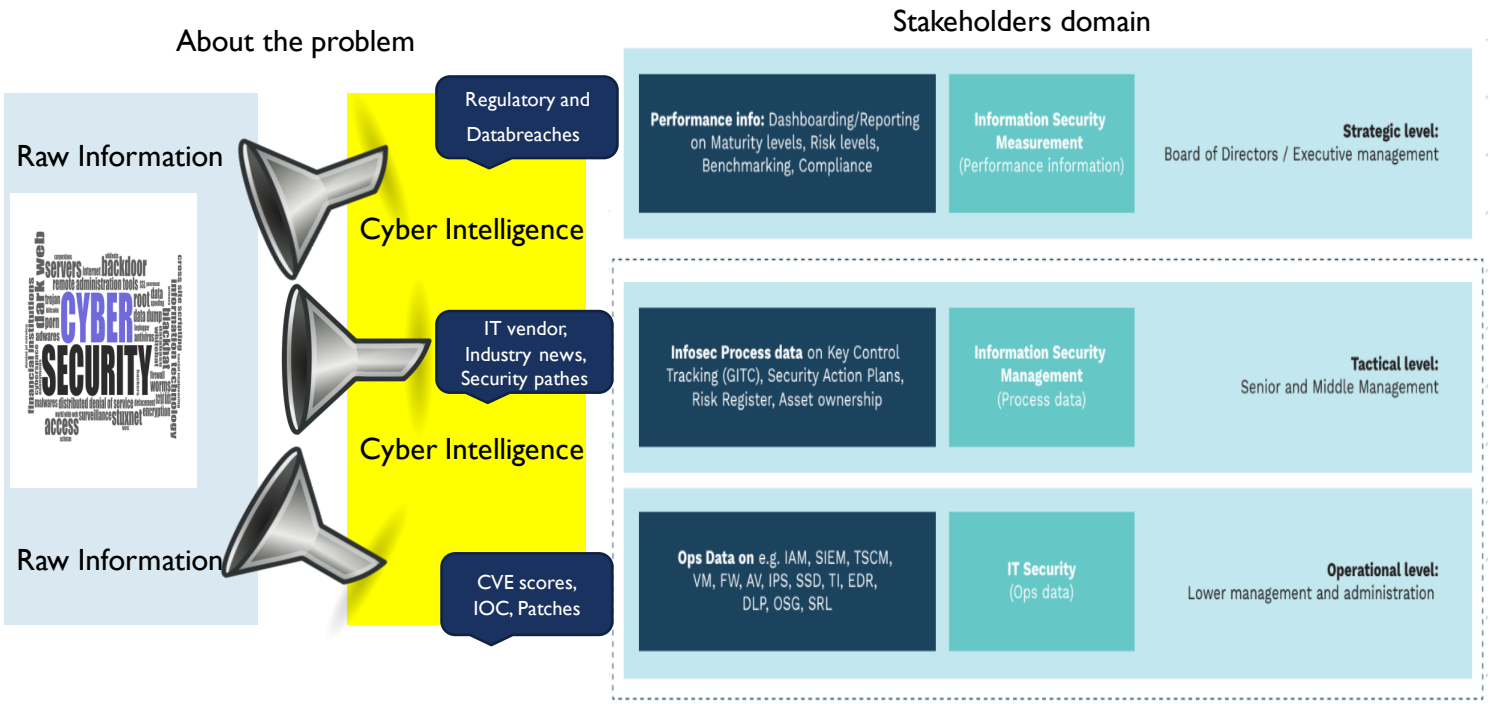
RELEVANT CYBER THREAT NEWS? THE PROBLEM

In current day network security, vigilance with respect to arising new threats and attack vectors is becoming ever more important.

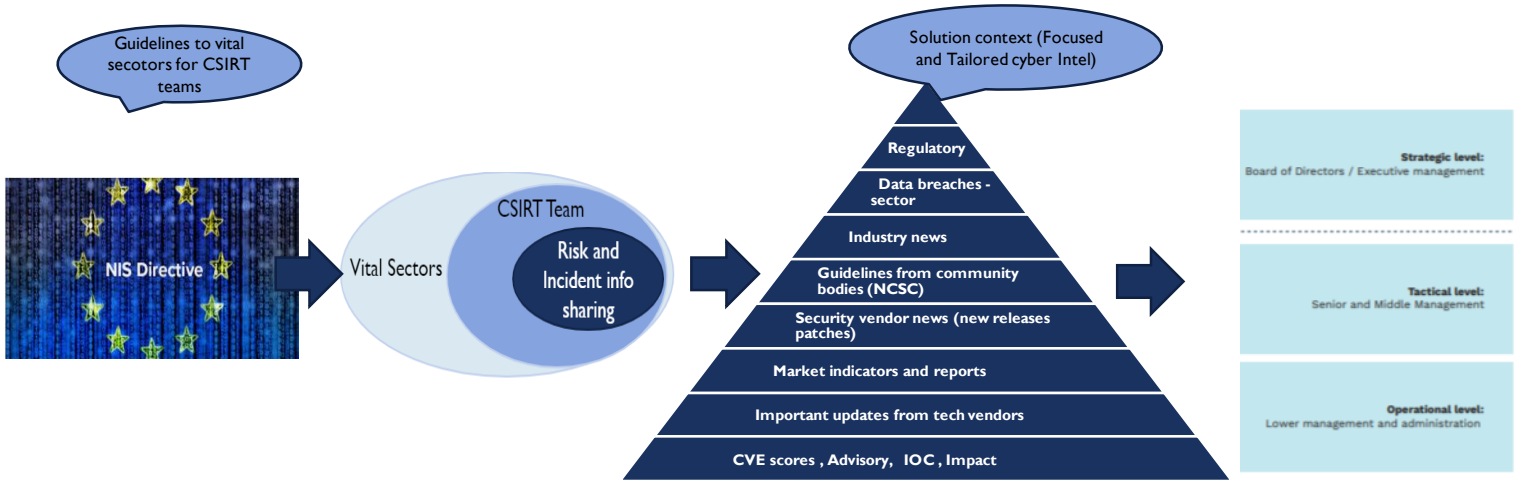
Rapid detection, risk assessment and preventive or mitigative measures is gaining prominence.

Knowing a relevant threat has become important in order to act in right direction

PROBLEM AND IMPACT TO STAKEHOLDERS



FIT INTO BIG PICTURE :CYBER SECURITY LEGISLATION DIRECTIVE FOR EUROPEAN UNION

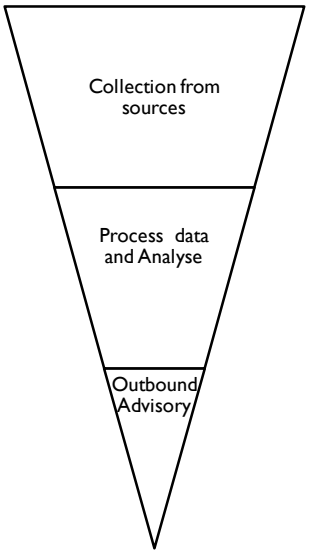


The **Network and Information Systems (NIS) Directive i**s the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

A culture of security across **vital sectors** which rely heavily on ICTs, such as **energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure**

Member States' preparedness by requiring them to be appropriately equipped, e.g. via a **Computer Security Incident Response Team (CSIRT)** and a competent national NIS authority

REQUIREMENT COMPONENTS: NEEDS(WHAT? & WHY?) AND PRIORITY

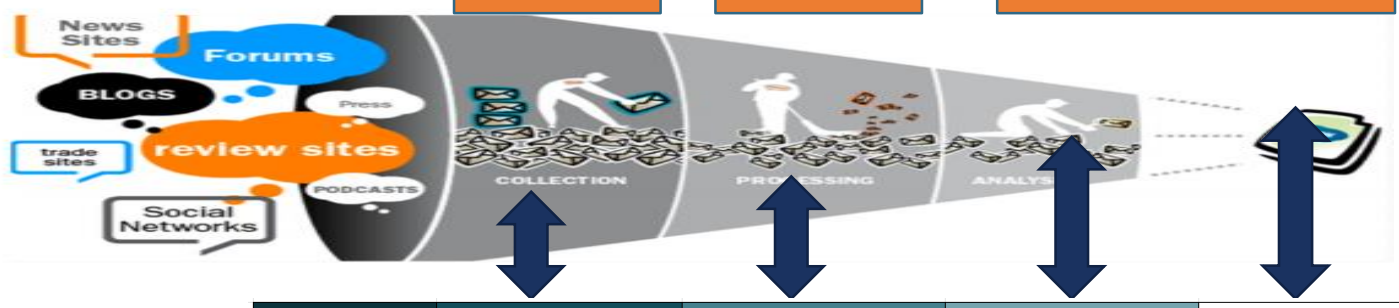


High Level Modules	Requirements:	What?	Why?	MoSCoW (priority)
Collector	Language Support	Support various languages.	To not miss intel in other languages	Must have
	Data Formats	Allow multiple data formats	To collect and process standard and recent formats	Should have
	Data Source types	Ingest from various sources	To cover broader sources of Intel	Must have
	Connection protocol	Support common protocols	To allow actual transfer To data	Must have
Processor	Data structuring	Data mappings and Data format conversion	To ensure a common data format To enable further processing	Should have
	Contextualization	Possible to set context	To convert raw intel To specific intel	Must have
Analyzer	Co-relation	Group similar Intel	To reduce duplicity and improve granularity	Should have
	Analysis	Provide insights on tactics, severity and impact	To make the cyber intel actionable	Must have
Advisory	Writing custom intel	Allow to write a new content for cyber news feed	To ensure that analyst can use his knowledge for providing details on cyber news	Must have
	Template Designing	Make design template for writing cyber intel and advisories	To allow flexibility in presentation of cyber Intel To further streams	Should have
	Feedback Collection	Collect internal and external user feedback	To check the quality and if the news is actionable	Could have
	Outbound Communication	Deliver Cyber news feed to users	To ensure cyber intel with advisory reach To destination	Must have

Sources : 1. Google search 2. Research work on academic papers 3. Discussion with: Jean-Hugues Migeon, ON2IT Cybersecurity, Jeroen Scheerder, ON2IT Cybersecurity.

SOLUTION: MODULE MAPPING-PROCESSES,ACTIVITIES AND TOOLS

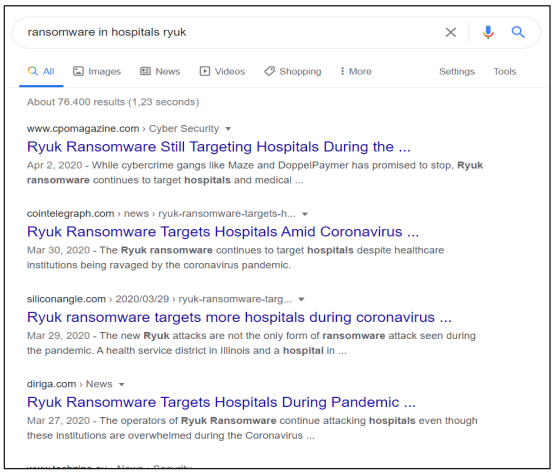
MODULES | Collector | Processor | Analyser and Advisory



Processes	Collection	Processing	Analysis	Advisory
Activities	Collect, Source Management	Filtering, Contexting, Add Tags, Data Manipulation, Output to Analysis as JSON or RSS	Provide Insight on tactics, severity and Impact	Advice to Customer, Simple Writeup, Publishing
Tools	FreshRss	Customised code on AWS cloud, Mysql and PHP	Manual with Experts	Manual with help of experts, For publsihing – Open souce tool

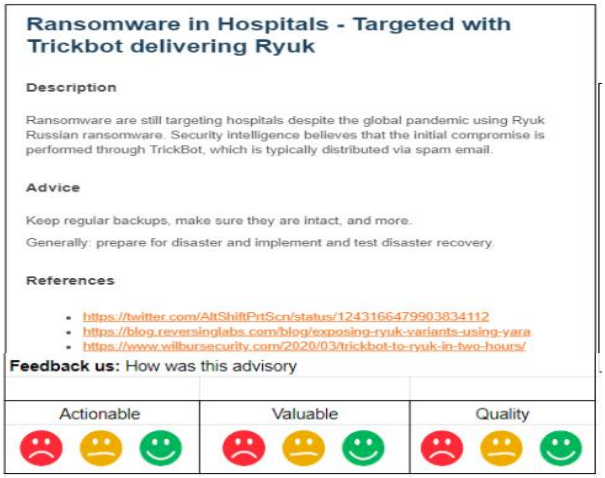
AN EXAMPLE:WHEN RAW BECOMES INTEL.

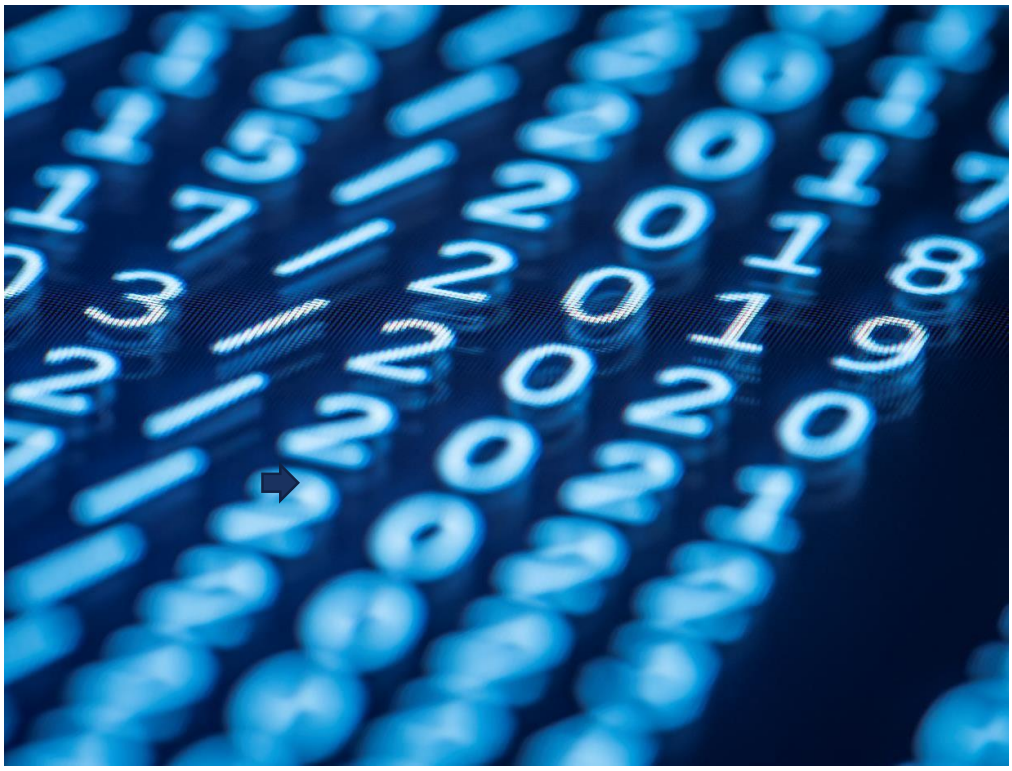
Scattered Raw Cyber Information



CYBERNEWSFEED TECHNOLOGY

Cyber newsfeed Intelligence Item





YOUR OPINION ?