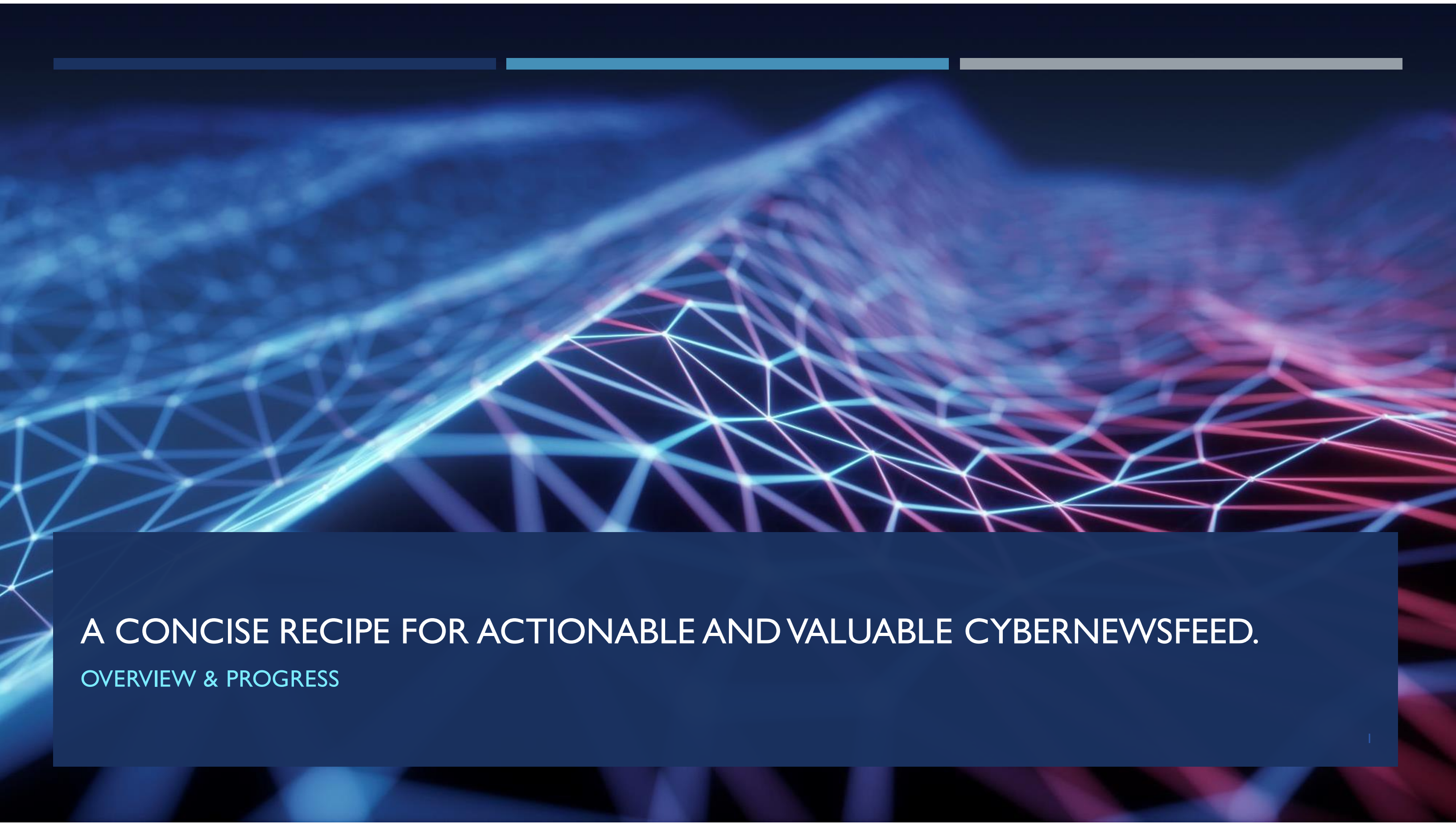


A CONCISE RECIPE FOR ACTIONABLE AND VALUABLE CYBERNEWSFEED.

OVERVIEW & PROGRESS

AGENDA

- RELEVANT CYBER THREAT NEWS? THE PROBLEM
- VISION : SOLUTION APPROACH
- SOLUTION REQUIREMENT COMPONENTS: NEEDS(WHAT? & WHY?) AND PRIORITY
- APPROACH : TAKEN TO BUILD ARTEFACT
- ARGUMENTATION : ON ASSESSMENT & SELECTION
- PRODUCT VISION – PROCESSES, ACTIVITIES AND TOOLS
- PROCESSES EXPLAINED

  1. COLLECTION
  2. PROCESSING
- DELIVERABLES : MAY 2020
- Q&A

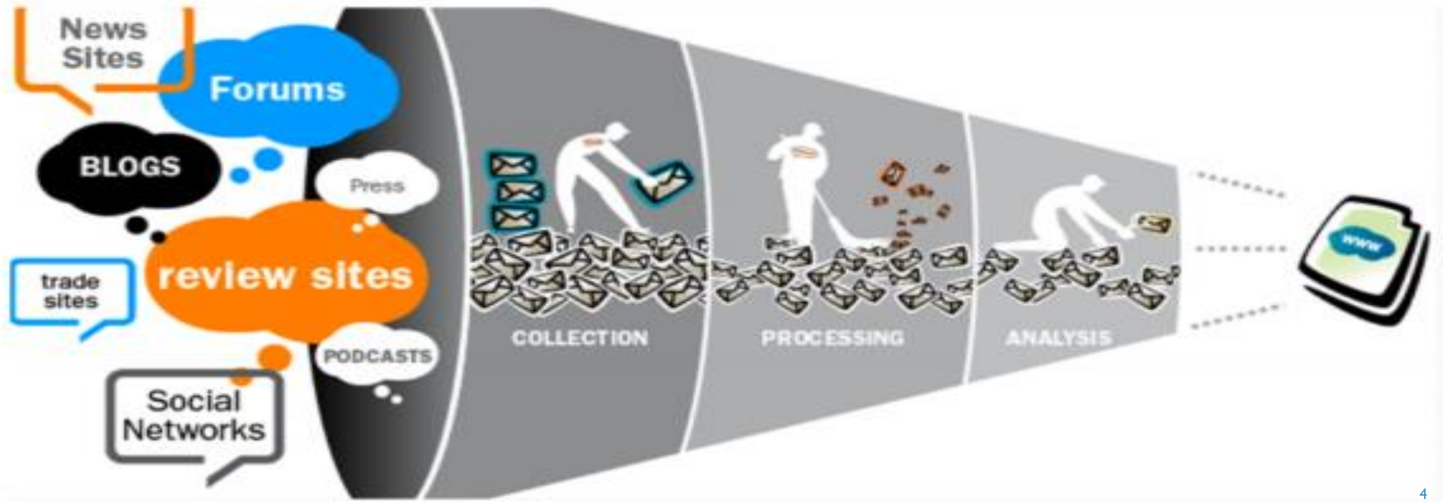
RELEVANT CYBER THREAT NEWS? THE PROBLEM

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

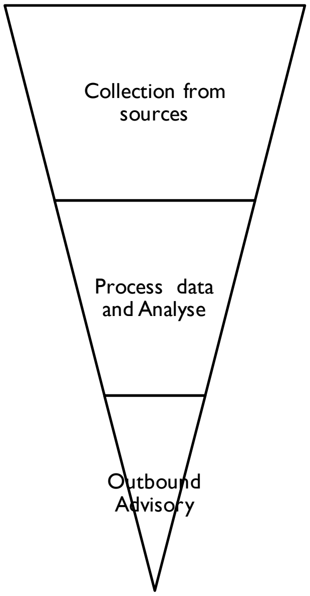
Rapid detection, risk assessment and preventive or mitigative measures is gaining prominence.

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

VISION : SOLUTION APPROACH



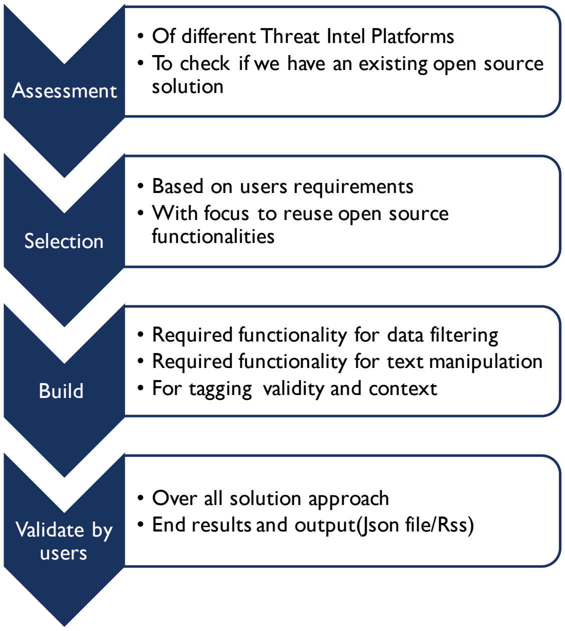
SOLUTION REQUIREMENT COMPONENTS: NEEDS(WHAT? & WHY?) AND PRIORITY



High Level	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
Analyzer	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
	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.

APPROACH : TAKEN TO BUILD ARTEFACT



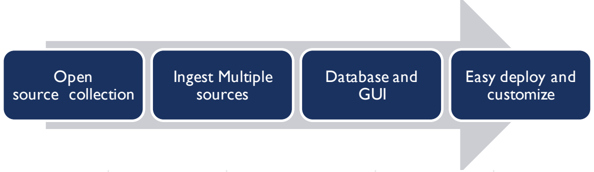
Assessment
- Of different Threat Intel Platforms
- To check if we have an existing open source solution

Selection
- Based on users requirements
- With focus to reuse open source functionalities

Build
- Required functionality for data filtering
- Required functionality for text manipulation
- For tagging validity and context

Validate by users
- Over all solution approach
- End results and output(Json file/Rss)

Assessment Parameters	Distribution	Application Support Forum Available?	Application Active Since years	Application's Last Issue resolved date	Functional Feautures	Database and GUI
Focus	Open Source	Ease of trouble shoot	Old and stable	Most recent is better	More is better	User Friendly



FreshRSS

Custom Build Analyzer and Advisory features	Filtiring	Contextualization	Data manipulation	Source reliability	JSON extraction	RSS feed publication

Demo to: Jean-Hugues Migeon, ON2IT Cybersecurity, Jeroen Scheerder, ON2IT Cybersecurity.
JSON files shared: Jean-Hugues Migeon, ON2IT Cybersecurity, Jeroen Scheerder, ON2IT Cybersecurity, Yuri Bobbert, ON2IT Cybersecurity.
Rss feed: Published on AWS hosted cloud.

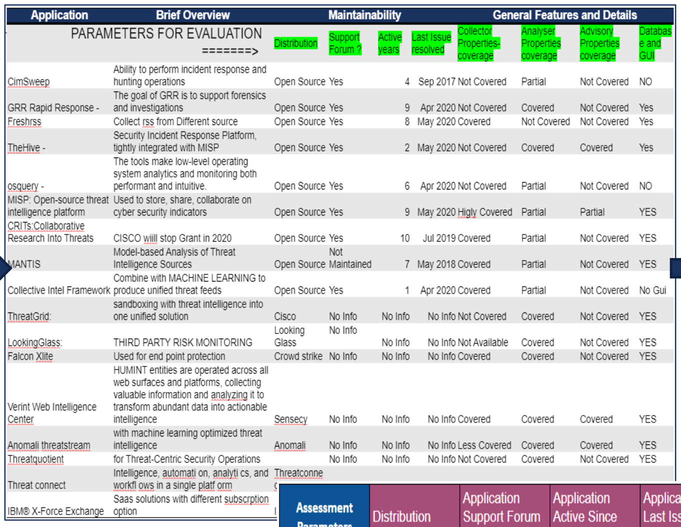
ARGUMENTATION : ON ASSESSMENT & SELECTION

Scanning → Listing → Assessment → Shortlisting → Final selection

Scanned Sources: Literature, Web , White papers, professional Inputs, (Total 23 evaluated, 17 is listed)

Referred Sources: 1 .Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives by Sauerwein, Clemens and Sillaber, Christian and Mussmann, Andrea and Breu, Ruth, Year 2017. 2. Jean-Hugues Migeon, ON2IT Cybersecurity.

Platform Specific Information collection : start from Google, find like to Offcial websites, read Whilepapers, and GitHUb links



Application	Brief Overview	Maintainability				General Features and Details			
	PARAMETERS FOR EVALUATION =======>	Distribution	Support Forum ?	Active years	Last Issue resolved	Collector Properties-coverage	Analyser Properties coverage	Advisory Properties coverage	Database and GUI
CimSweep	Ability to perform incident response and hunting operations	Open Source	Yes	4	Sep 2017	Not Covered	Partial	Not Covered	NO
GRR Rapid Response -	The goal of GRR is to support forensics and investigations	Open Source	Yes	9	Apr 2020	Not Covered	Covered	Not Covered	Yes
Freshrss	Collect rss from Different source	Open Source	Yes	8	May 2020	Covered	Not Covered	Not Covered	Yes
TheHive -	Security Incident Response Platform, tightly integrated with MISP	Open Source	Yes	2	May 2020	Not Covered	Covered	Covered	Yes
osquery -	The tools make low-level operating system analytics and monitoring both performant and intuitive.	Open Source	Yes	6	Apr 2020	Not Covered	Partial	Not Covered	NO
MISP: Open-source threat intelligence platform	Used to store, share, collaborate on cyber security indicators	Open Source	Yes	9	May 2020	Higly Covered	Partial	Partial	YES
CRITs:Collaborative Research Into Threats	CISCO wiill stop Grant in 2020	Open Source	Yes	10	Jul 2019	Covered	Partial	Not Covered	YES
MANTIS	Model-based Analysis of Threat Intelligence Sources	Open Source	Not Maintained	7	May 2018	Covered	Partial	Not Covered	YES
Collective Intel Framework	Combine with MACHINE LEARNING to produce unified threat feeds	Open Source	Yes	1	Apr 2020	Covered	Partial	Not Covered	No Gui
ThreatGrid:	sandboxing with threat intelligence into one unified solution	Cisco	No Info	No Info	No Info	Not Covered	Covered	Not Covered	YES
LookingGlass:	THIRD PARTY RISK MONITORING	Looking Glass	No Info	No Info	No Info	Not Available	Covered	Not Covered	YES
Falcon Xlite	Used for end point protection	Crowd strike	No Info	No Info	No Info	Covered	Covered	Not Covered	YES
Verint Web Intelligence Center	HUMINT entities are operated across all web surfaces and platforms, collecting valuable information and analyzing it to transform abundant data into actionable intelligence	Sensecy	No Info	No Info	No Info	Covered	Covered	Covered	YES
Anomali threatstream	with machine learning optimized threat intelligence	Anomali	No Info	No Info	No Info	Less Covered	Covered	Covered	YES
Threatquotient	for Threat-Centric Security Operations		No Info	No Info	No Info	Not Covered	Covered	Not Covered	YES
Threat connect	Intelligence, automati on, analyti cs, and workfl ows in a single platf orm	Threatconne c							
IBM® X-Force Exchange	Saas solutions with different subscrption option	I							

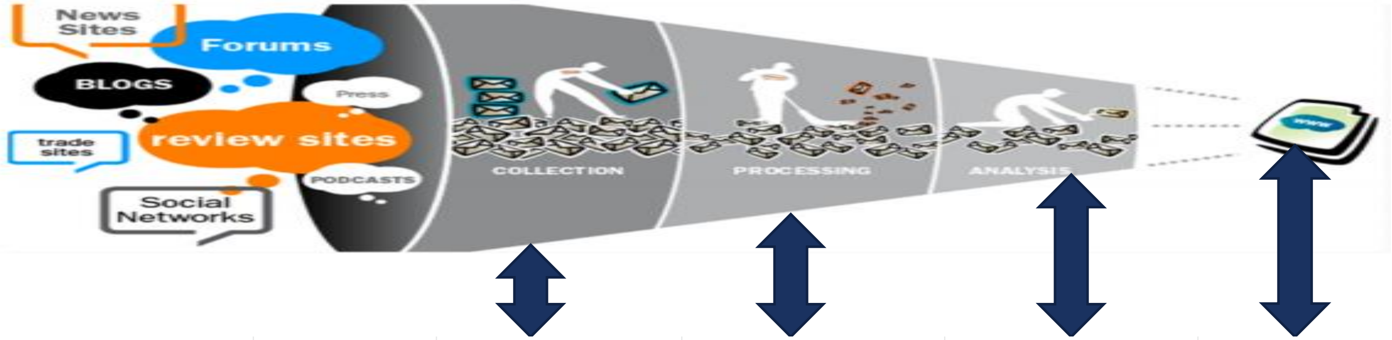
Assessment Parameters	Distribution	Application Support Forum Available?	Application Active Since years	Application's Last Issue resolved date	Functional Feautures	Database and GUI
Focus	Open Source	Ease of trouble shoot	Old and stable	Most recent is better	More is better	User Friendly

Shorlisted Applications	Brief Over View
FreshRss	Only for Collection
MISP: Open-source threat intelligence platform	Used to store, share, collaborate on cyber security indicators
CRITs: Collaborative Research Into Threats	CISCO will stop Grant in 2020
Collection Intel Framework	Combine with MACHINE LEARNING to produce unified threat feeds

Only collection , fast deploy and fit to user purpose

FreshRSS

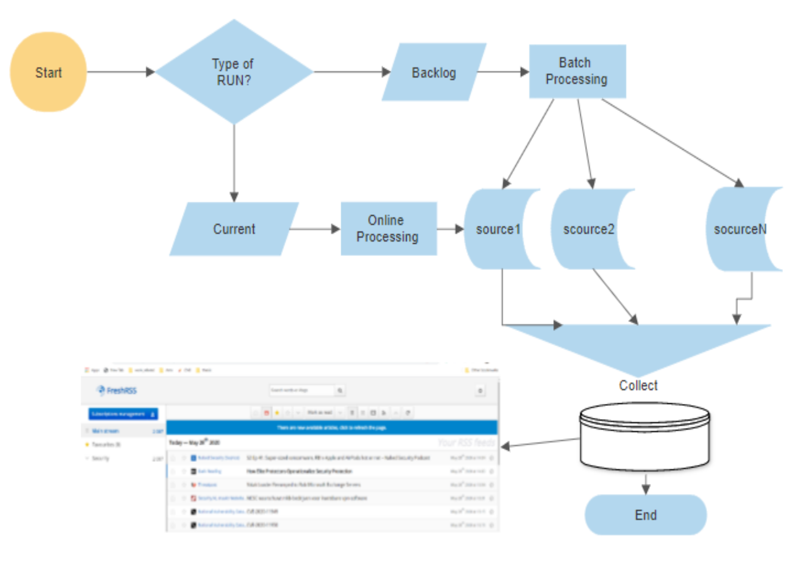
PRODUCT VISION – PROCESSES,ACTIVITIES AND TOOLS



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

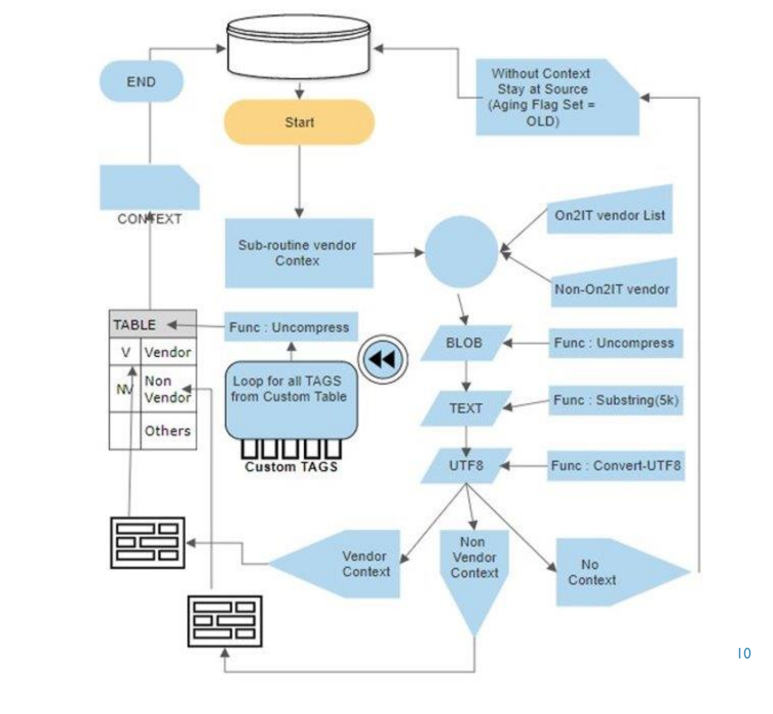
COLLECTION: TOOLS AND ACTIVITIES

Tools: FressRSS build on PHP and MySql
Activities : Supports online and batch collection of rss news feed from configured sources.



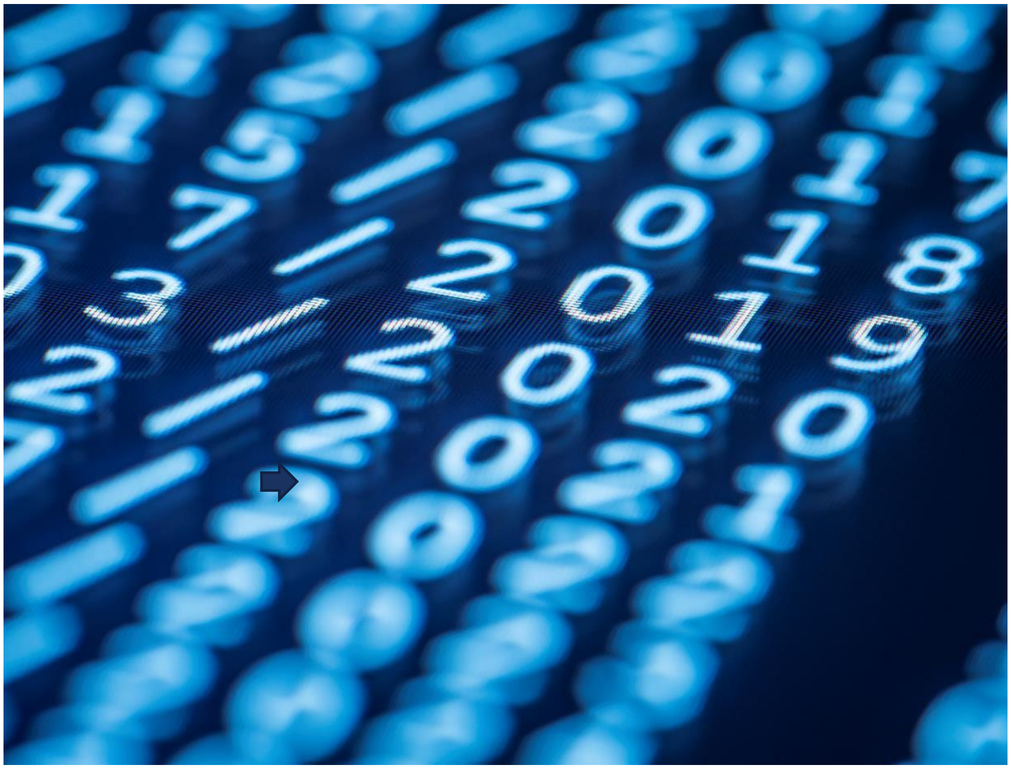
PROCESING: TOOLS AND ACTIVITIES

Tools: Custom written code in PHP and MySql
Activities : Filtering, Contexting, Add Tags, Data Manipulation, Output to Analysis as JSON or RSS



DELIVERABLES : MAY 2020

- Literature Review on Existing Knowledge.
- Assessed List of cybernewsfeed Intel Platforms(Link).
- Demo on progress so far(28th Mar- Recording).
- Algorithms and Visuals used so far(with source code).
- JSON files for purpose of parsing
- List of Sources used so far.
- UI for Internal Feedback(Face/Thumb)
- Questionarie for cost Determination



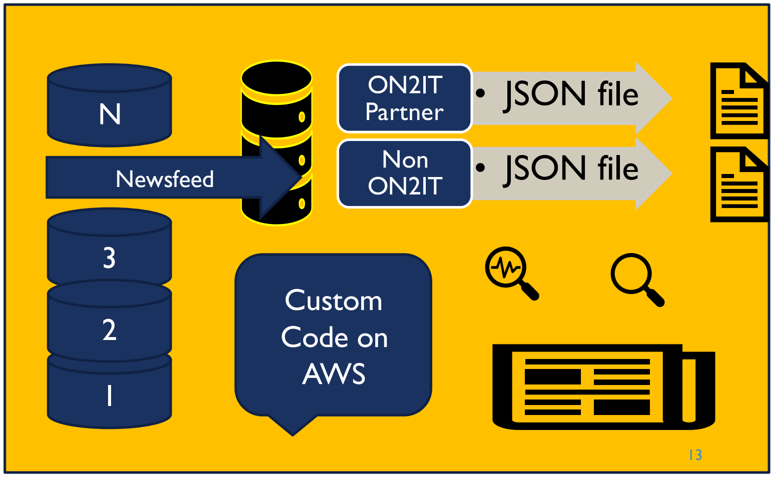
THANK YOU FOR YOUR QUESTIONS

SHORT LISTED SOLUTIONS AND APPLIED SOLUTIONS

Collector : open source

Application	Brief Over View
FreshRss ☛	Only for Collection ✓
MISP: Open-source threat intelligence platform	Used to store, share, collaborate on cyber security indicators ✓
CRITs: Collaborative Research Into Threats	CISCO will stop Grant in 2020 ✓
Collection IIntel Framework	Combine with MACHINE LEARNING to produce unified threat feeds ✓

Vendor specific Contextualisation



LOW HANGING ~~FRUITS~~ MODULES

- Open Source collection engine
- Vendor Contexulization and Tags
- Open Source Publishing

Ideas For Future :

Strategic/Tactic/Operational Tags
Implement logic for source validation
Run similar platform for other Intel

SOLUTIONS : UNDER INCEPTION

WEB ANALYSER- In house

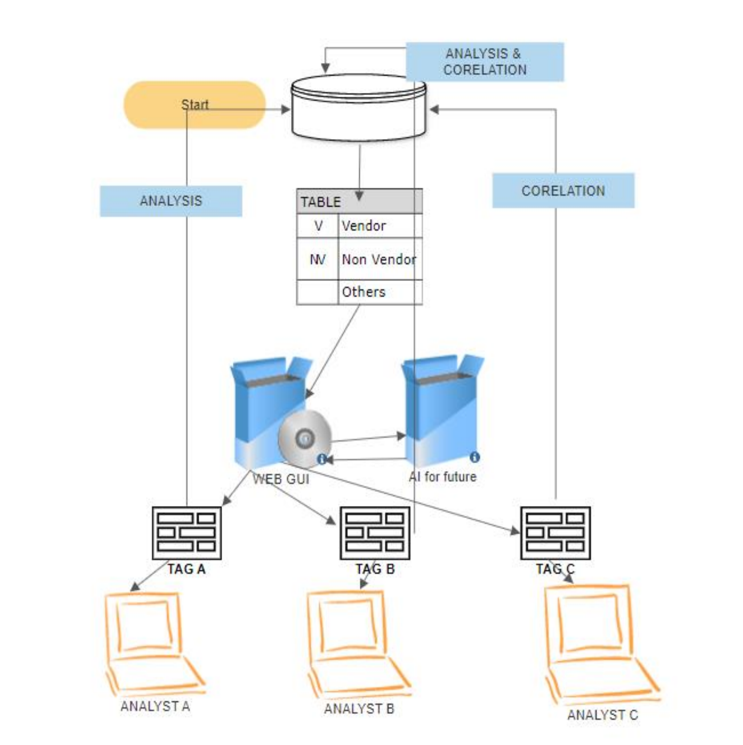
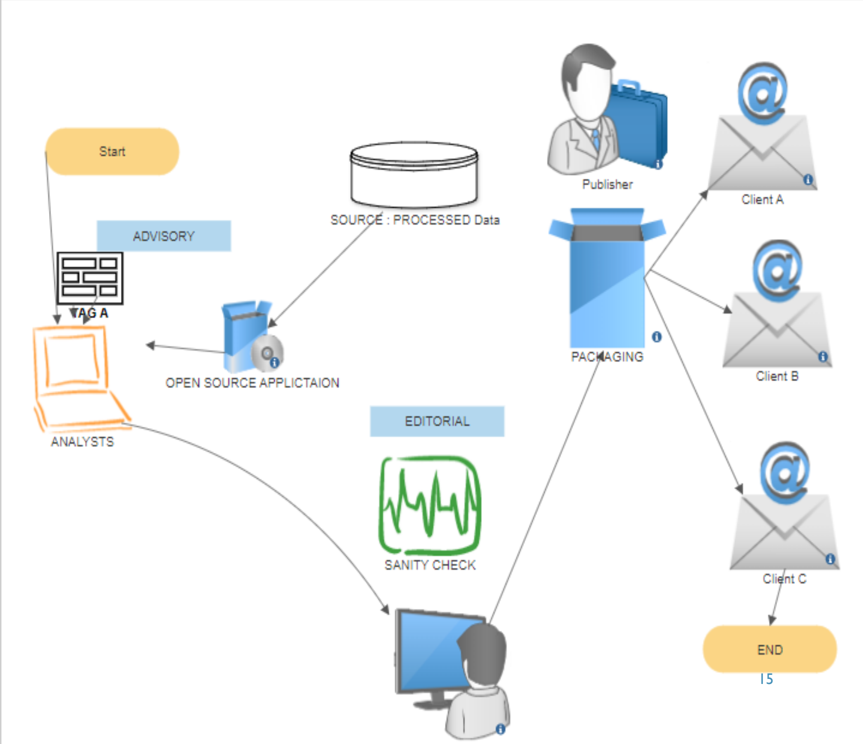


TABLE	
V	Vendor
NV	Non Vendor
	Others

PUBLICATION – Open Souce


Publisher
Client A
Start
SOURCE : PROCESSED Data
ADVISORY
TAG A
PACKAGING
Client B
OPEN SOURCE APPLICTAION
ANALYSTS
EDITORIAL
SANITY CHECK
Client C
END