# CYBERNEWSFEED TECHNOLOGY: REVEAL
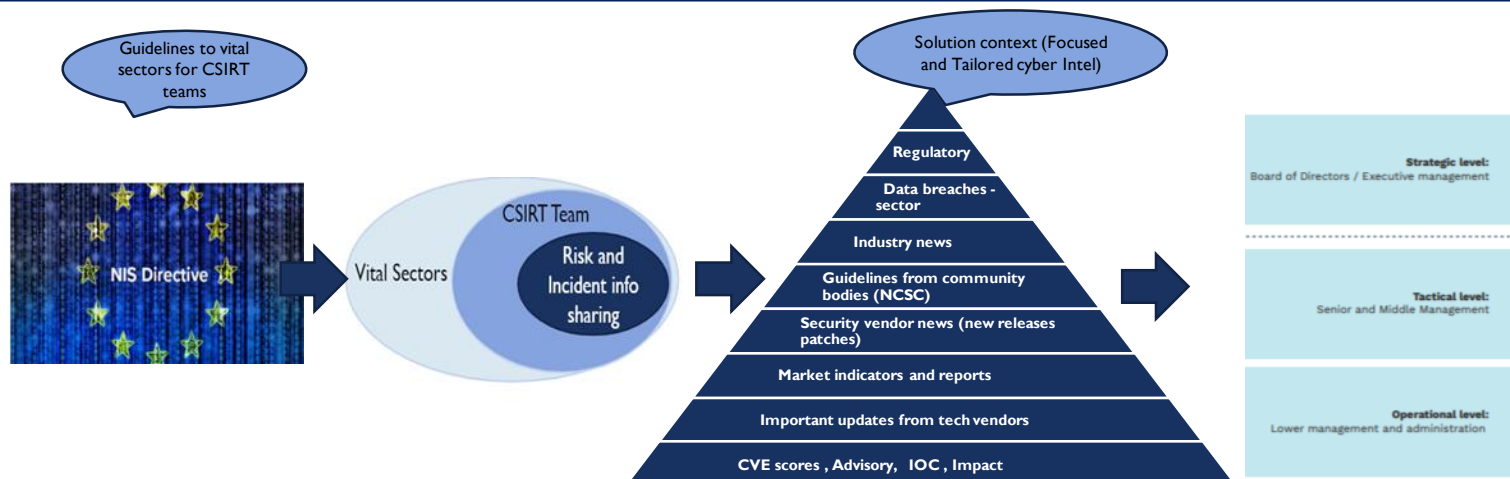
OVERVIEW, DEMO & FUTURE?

# Agenda

Incubation

Problem: An example & demo.
Problem context at European level.
Requirement and Solution Design.
Survey: Market sentiments about the prototype.
Survey: Market demand for the product.
Roadmap: POC, pilot and production.

Scattered Raw Cyber Information

CYBERNEWSFEED TECHNOLOGY

Actionable Cyber Intelligence for CISO





**Ransomware in Hospitals - Targeted with Trickbot delivering Ryuk**

**Description**

Ransomware are still targeting hospitals despite the global pandemic using Ryuk Russian ransomware. Security intelligence believes that the initial compromise is performed through TrickBot, which is typically distributed via spam email.

**Advice**

Keep regular backups, make sure they are intact, and more.

Generally: prepare for disaster and implement and test disaster recovery.

**References**

- https://twitter.com/AltShiftPrtScn/status/1243166479903834112
- https://blog.reversinglabs.com/blog/exposing-ryuk-variants-using-yara
- https://www.willbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/

**Feedback us:** How was this advisory

| Actionable | Valuable | Quality |
|---|---|---|
| 🙁 😐 🙂 | 🙁 😐 🙂 | 🙁 😐 🙂 |

Want a DEMO?

---

Guidelines to vital sectors for CSIRT teams

Solution context (Focused and Tailored cyber Intel)

NIS Directive

Vital Sectors

CSIRT Team — Risk and Incident info sharing

Regulatory
Data breaches - sector
Industry news
Guidelines from community bodies (NCSC)
Security vendor news (new releases patches)
Market indicators and reports
Important updates from tech vendors
CVE scores , Advisory,  IOC , Impact

**Strategic level:**
Board of Directors / Executive management

**Tactical level:**
Senior and Middle Management

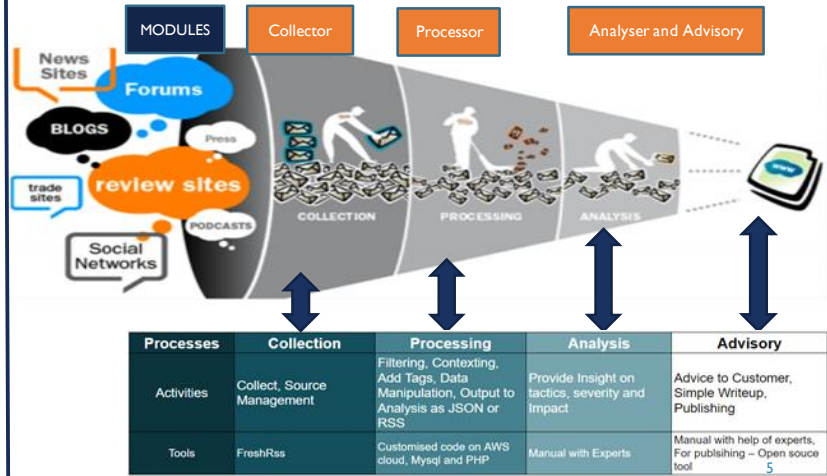**Operational level:**
Lower management and administration

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
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**

# PRODUCT REQUIREMENTS AND SOLUTION:
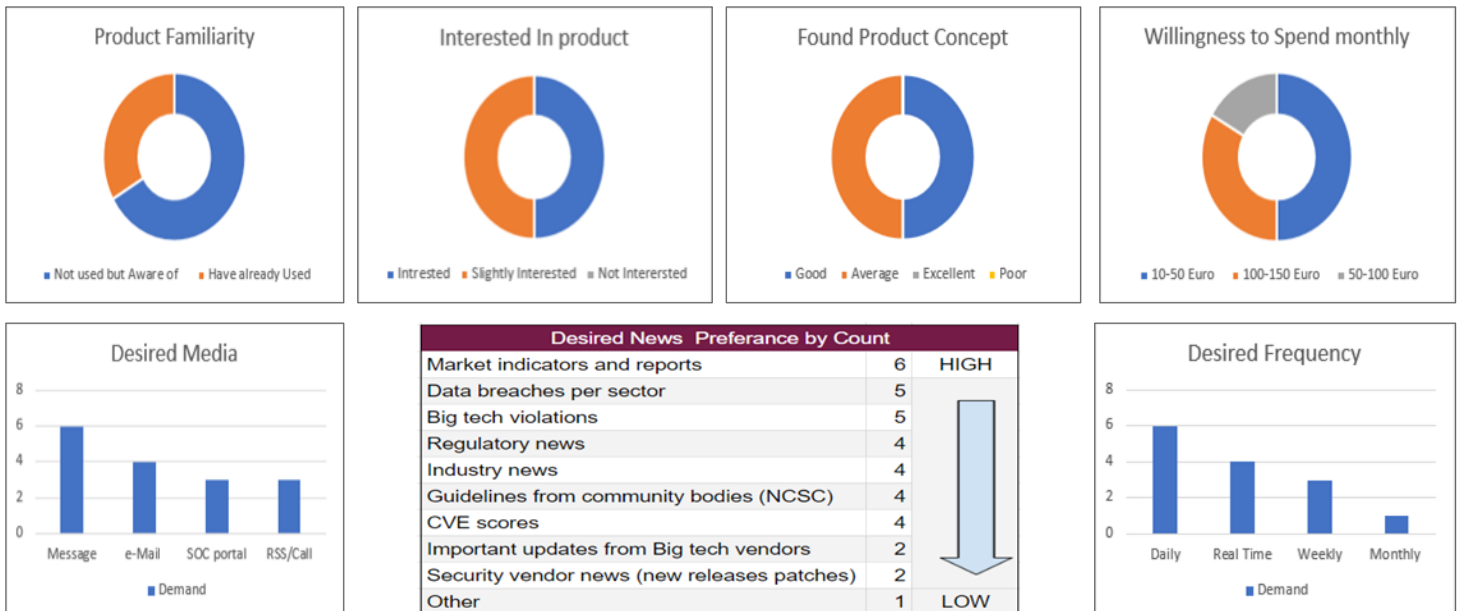## MODULE LEVEL MAPPING-PROCESSES, ACTIVITIES AND TOOLS

## REQUIREMENT NEEDS

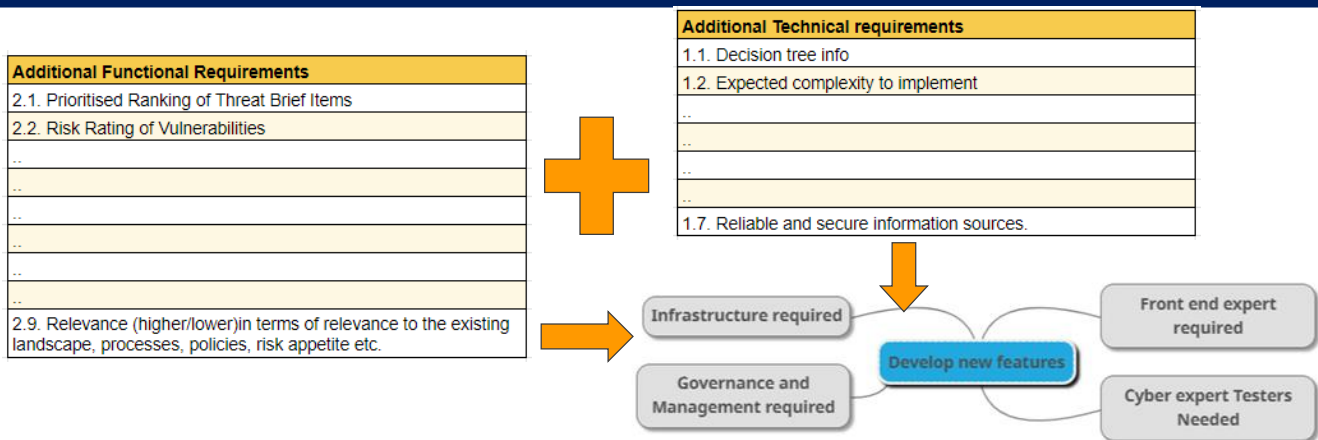| High Level Modules | Requirements: | What? | Why? | MoSCoW (priority) |
|---|---|---|---|---|
| Collector | Language Support | Support various languages. | To not miss intel in other languages | Must have |
| | Data Formats | Allow multiple data formats | To collect and process standard and recent 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 |

## SOLUTION MODEL



| 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 |

# MARKET SENTIMENTS: PROTOTYPE SURVEY INDICATIONS



### Product Familiarity
- Not used but Aware of
- Have already Used

### Interested In product
- Intrested
- Slightly Interested
- Not Interrested

### Found Product Concept
- Good
- Average
- Excellent
- Poor

### Willingness to Spend monthly
- 10-50 Euro
- 100-150 Euro
- 50-100 Euro

### Desired Media
- Demand (Message, e-Mail, SOC portal, RSS/Call)

| Desired News  Preference by Count | | |
|---|---|---|
| Market indicators and reports | 6 | HIGH |
| Data breaches per sector | 5 | |
| Big tech violations | 5 | |
| Regulatory news | 4 | |
| Industry news | 4 | |
| Guidelines from community bodies (NCSC) | 4 | |
| CVE scores | 4 | |
| Important updates from Big tech vendors | 2 | |
| Security vendor news (new releases patches) | 2 | |
| Other | 1 | LOW |

### Desired Frequency
- Demand (Daily, Real Time, Weekly, Monthly)

# MARKET DEMAND: ON NEW PRODUCT FEATURES

| Additional Functional Requirements |
| --- |
| 2.1. Prioritised Ranking of Threat Brief Items |
| 2.2. Risk Rating of Vulnerabilities |
| .. |
| .. |
| .. |
| .. |
| .. |
| .. |
| 2.9. Relevance (higher/lower)in terms of relevance to the existing landscape, processes, policies, risk appetite etc. |

| Additional Technical requirements |
| --- |
| 1.1. Decision tree info |
| 1.2. Expected complexity to implement |
| .. |
| .. |
| .. |
| 1.7. Reliable and secure information sources. |

Infrastructure required

Front end expert required

Develop new features

Governance and Management required

Cyber expert Testers Needed

**The product needs incubation so that it can mature itself for the market.**
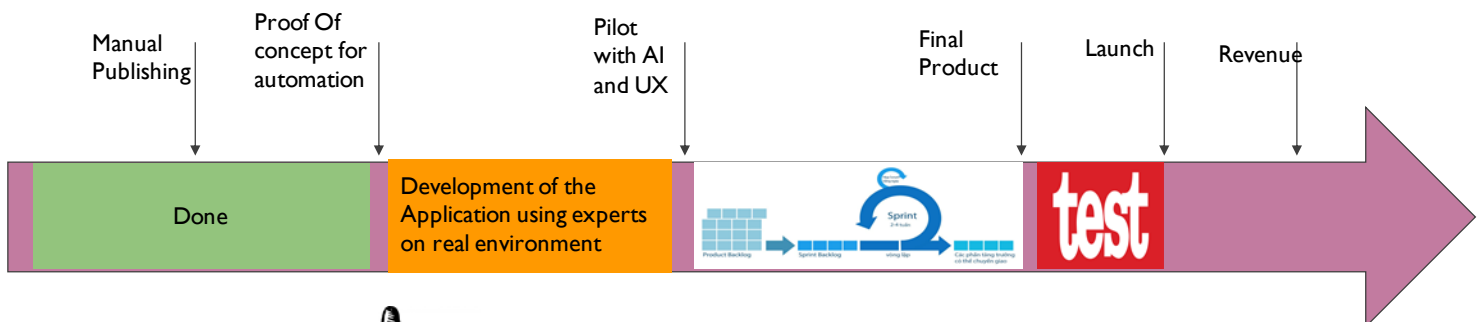
I think the product has a good foundation.

I like the Idea very much, Its Unique

With some improvements, the tool can become excellent.

# ROADMAP: The Future

Manual Publishing

Proof Of concept for automation

Pilot with AI and UX

Final Product

Launch

Revenue

Done

Development of the Application using experts on real environment

Product Backlog    Sprint Backlog    Sprint 2-4 tuần    vòng lặp    Các phần tăng trưởng có thể chuyển giao

test

We are Here

# YOUR OPINION ?