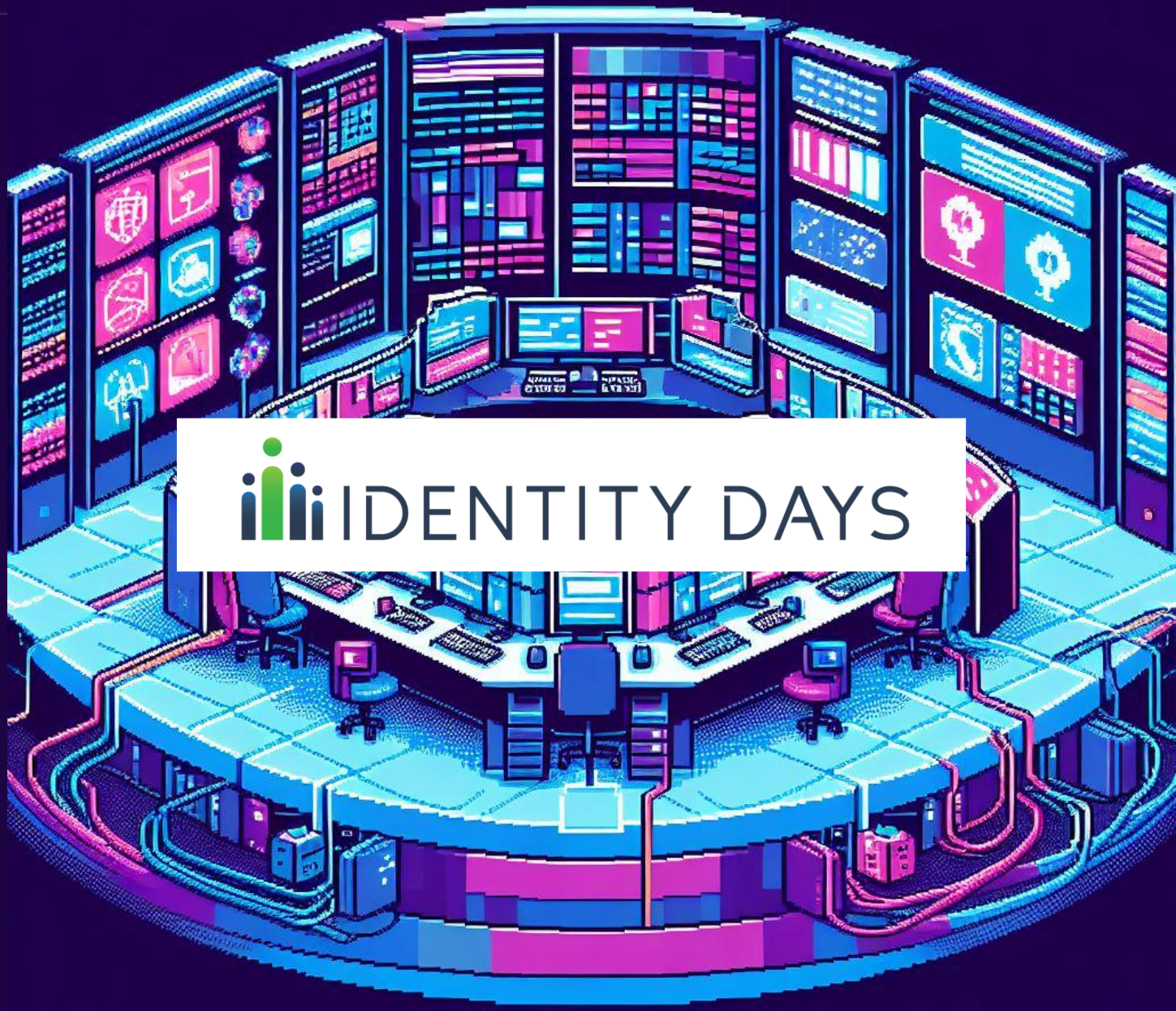
/ hackuity

VOC

Vulnerability Operations Center

19.12.2024

Sylvain CORTES



* overview *

I. WHAT IS A VOC?

Academic definition

A Vulnerability Operations Center (VOC) is a **centralized** facility or unit within an organization that is responsible for **identifying**, **assessing**, **managing**, and **mitigating** vulnerabilities in the organization's systems, networks, software, and infrastructure.

The VOC typically monitors **various sources for information** on security vulnerabilities, such as open-source intelligence, private advisories, security alerts, and research findings, and then coordinates efforts to address these vulnerabilities effectively.

Its primary goal is to **proactively** identify potential weaknesses and take necessary measures to prevent security breaches or mitigate their impact to ensure the overall security posture of the organization.

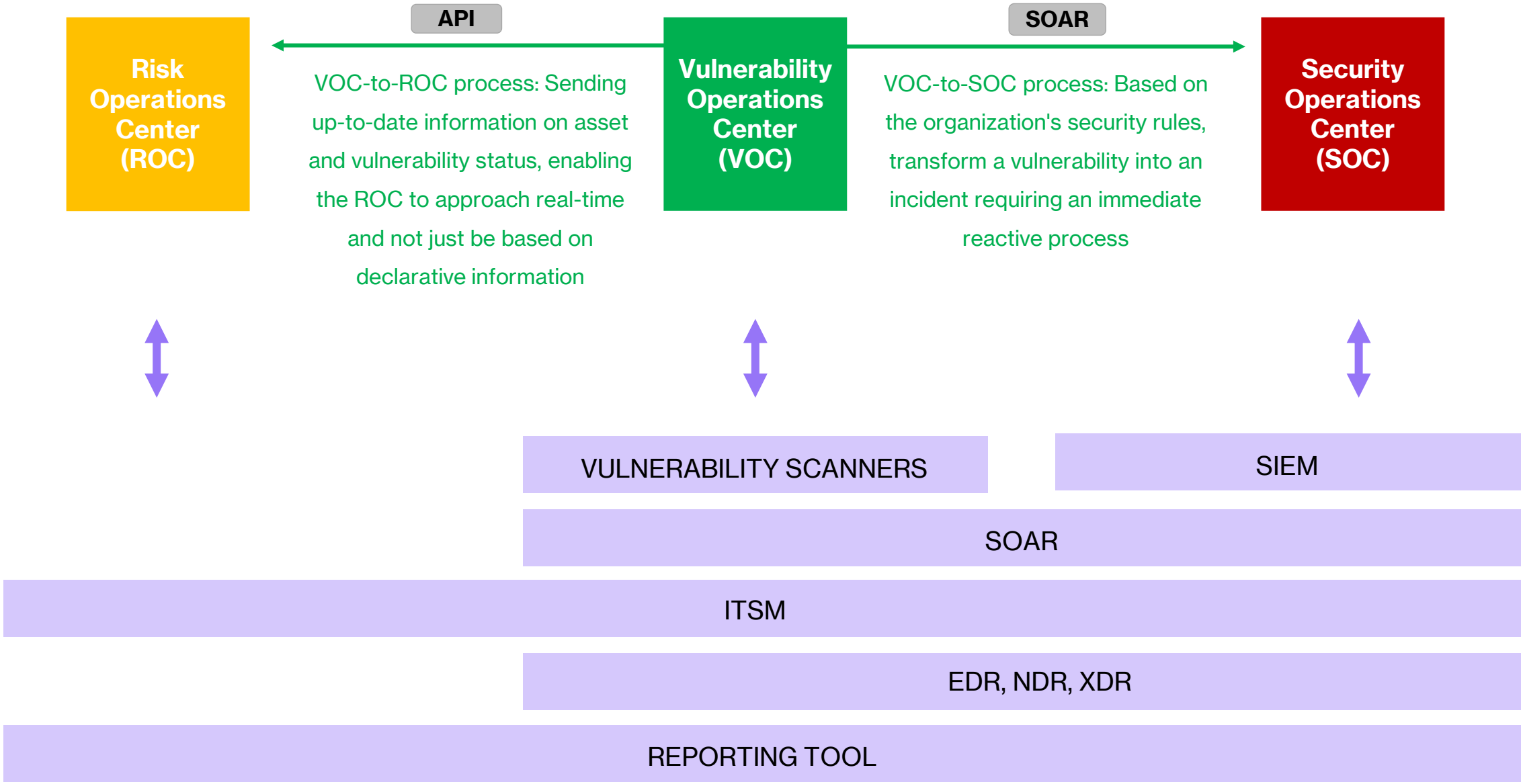
ROC, VOC & SOC

Continuous Threat Exposure Management (CTEM) Program

GOVERNANCE: People & process	PROACTIVE: Pre-attack risk reduction	REACTIVE: Post-attack threat detection
"Alignment & collaboration to manage risk & compliance"	"Near real-time vulnerability intelligence, assessment & mgmt"	"Near real-time detection & response"
Risk Operations Center (ROC)	**Vulnerability Operations Center (VOC)**	**Security Operations Center (SOC)**
Governance, Risk & Compliance	Vulnerability Centralization, Risk-Based Prioritization & Remediation	Threat Detection & Incident Response
Indicators of Compliance	Indicators of Exposure	Indicators of Compromise
AUDIT & SECURITY POLICIES	**VULNERABILITIES & ASSETS**	**EVENTS & LOGS**

Data Center | IT Assets | Public Cloud | Code & Apps | Workloads | Identities | ICS

ROC, VOC & SOC: Interaction matrix



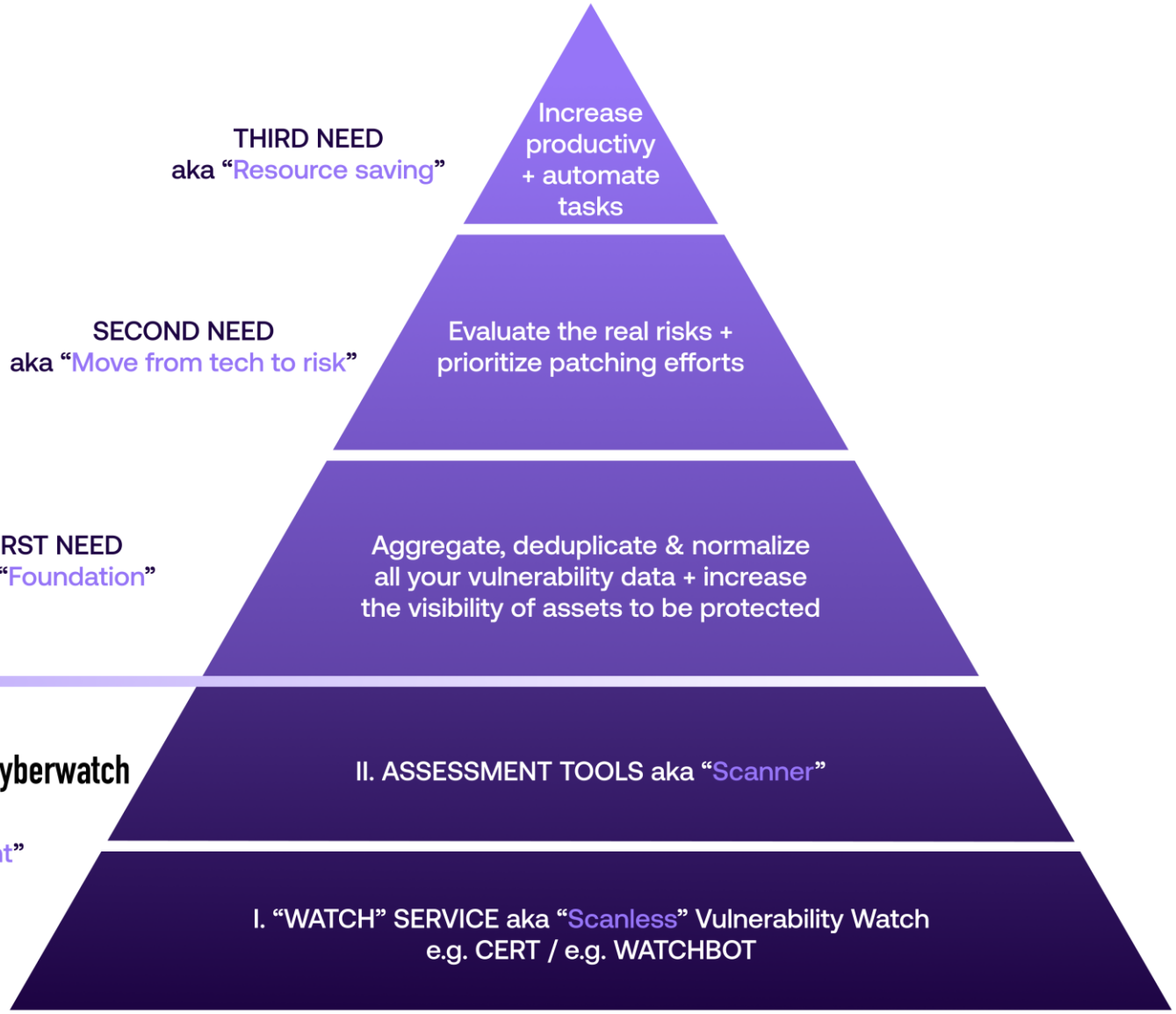
Why SOC is not the right organization to manage Vulnerabilities?

- Too much events/information to manage
- When you're dealing with incidents, prevention and vulnerability management take a back seat
- The consequence is that because of the SOC's overload, vulnerabilities are never managed
- We have tried, through a collective mistake, to have the SOC manage the vulnerabilities, and we all know the current situation... it doesn't work
- The right organization to manage vulnerabilities is VOC

II. THE VOC FOUNDATION

The VOC satisfies three progressive needs

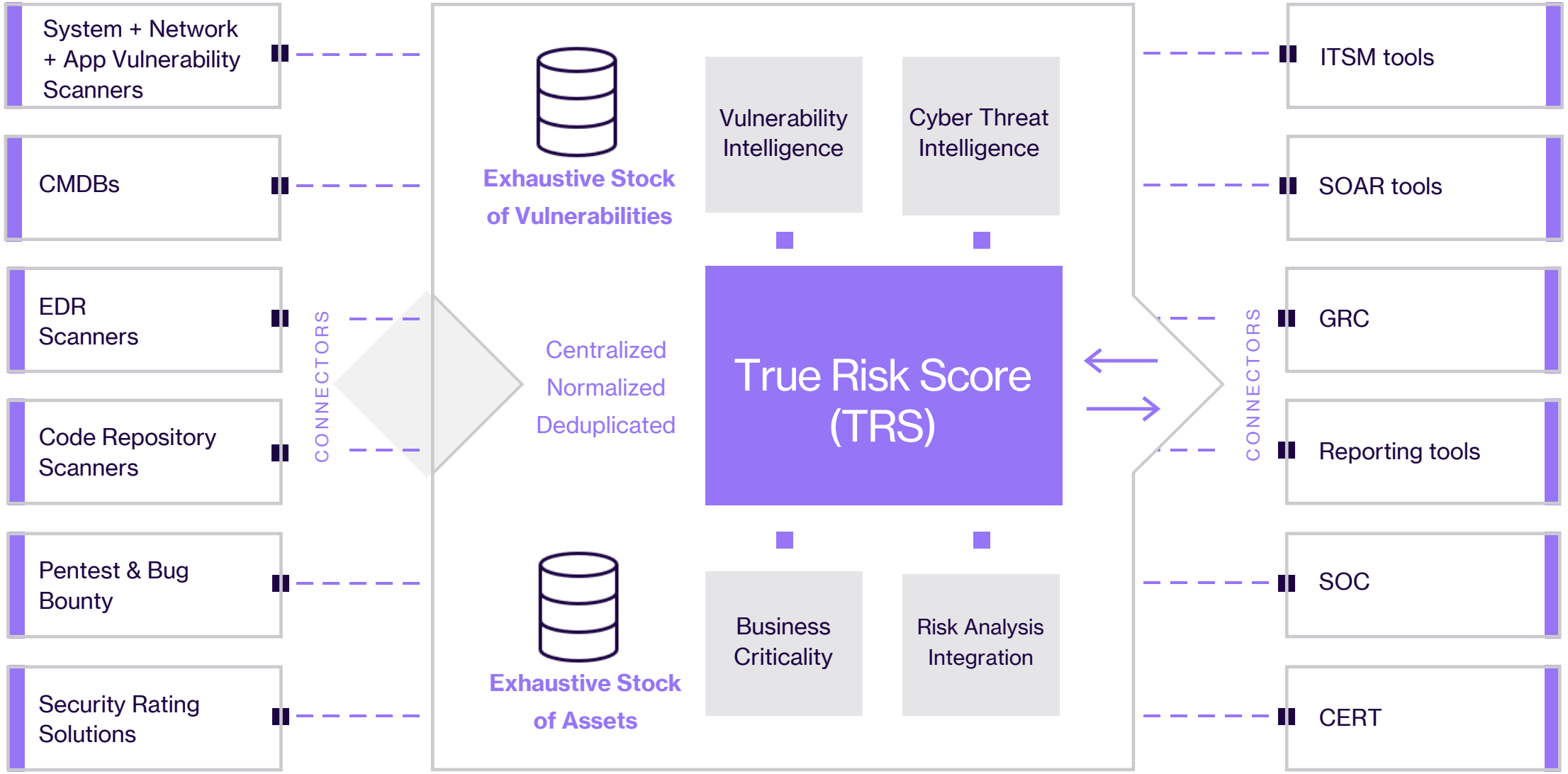
VOC platform



tenable Qualys WIZ TANIUM Cyberwatch

WatchBots CERT-FR CERT-IST INDUSTRIE I SERVICES I TERTIAIRE

Hackuity, the “VOC enabler platform”



Orchestrate Detection Arsenal

On-prem Full Cloud Hybrid

Automate Remediation Workflow

Démonstration par l'exemple

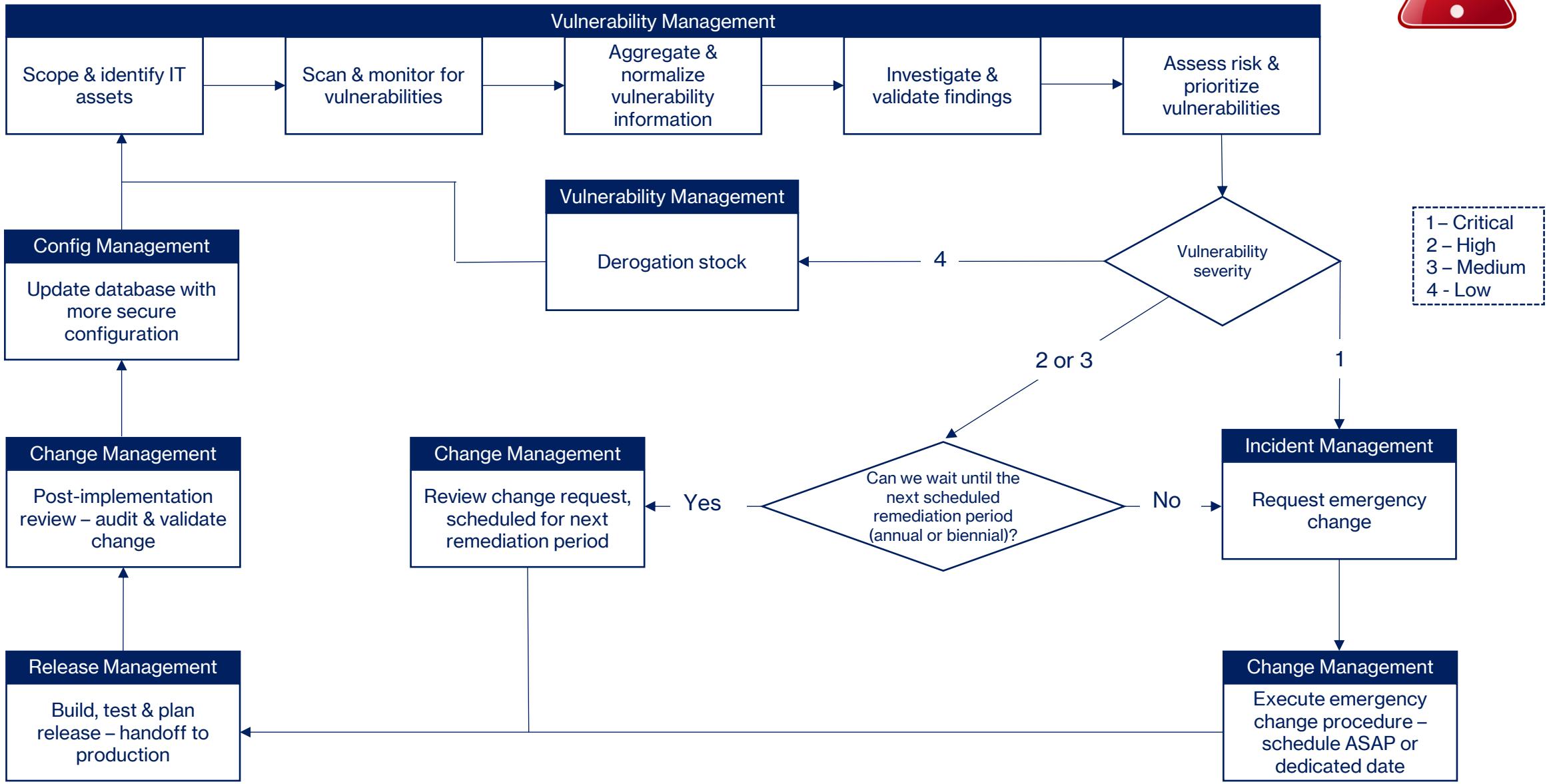
Agrégation
Déduplication
Normalisation

VOC brings flexibility

The VOC delivers strong competitive advantages to an organization and enables a coherent approach to risk:

- No need to depend on scan tools, you can easily change suppliers according to your needs, all without changing your processes or having to retrain your teams
- Streamlines M&A processes
- C-level people don't think in technical terms, they think of financial and business risks: speak the same language
- Sustain your investments in existing security tools and unleash the ROI of each tool
- Pilot risks, not vulnerabilities

Global process overview



III. SSVC OVERVIEW

SSVC foundation

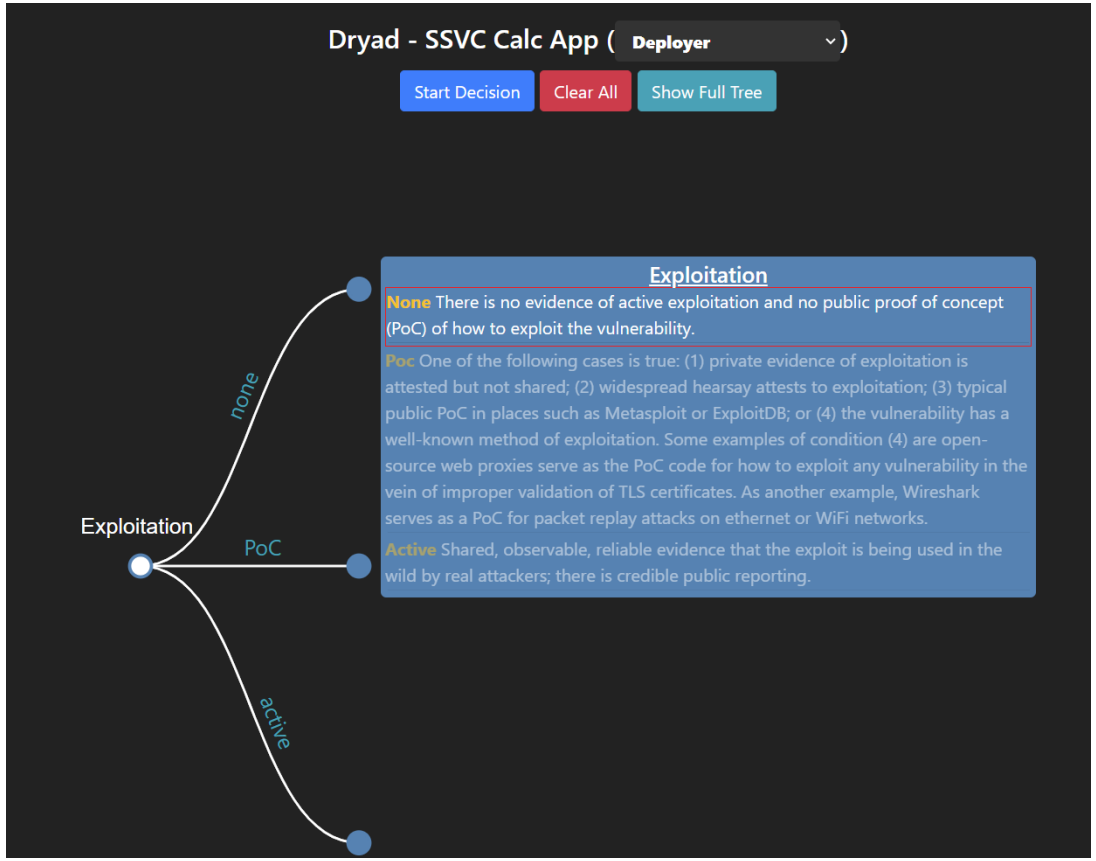
The SSVC methodology can enable organizations to distribute findings to each remediation pool.

Three elements should guide the creation of the SSVC decision tree:

1. Processing capacity, i.e. how many people can be mobilized on a regular basis to carry out corrective actions

2. The organization's risk appetite, i.e. whether or not the organization can take risks, and on what scale

3. Regulations applying to the organization, i.e. some organizations are subject to regulations that require a certain level of security, and the organization must provide adequate processing capacity or risk fines and deregistration



Source: https://certcc.github.io/SSVC/ssvc-calc/

Remediation Pools

At the end of the risk-based qualification cycle, each organization must decide in which remediation pool to place the evaluated finding. There are generally four defined possible pools:

IMMEDIATE

The finding(s) is/are considered extremely dangerous and must be corrected within an extremely short timeframe.

Usually, these are vulnerabilities that can be exploited and actively used by attackers – and more often than not, they are findings carried by assets exposed on the Internet and directly accessible by attackers.

OUT OF CYCLE

The finding(s) is/are considered dangerous, treatment cannot wait until the next scheduled patching period. However, immediate remediation is not required.

The remediation must be planned between the risk assessment date and the next scheduled patching period.

Planning will depend on the urgency of the treatment and the associated risk assessment but is generally between 2 weeks and 2 months from the date of risk assessment.

SCHEDULED

A programmed remediation period exists in the organization. This is often a period of 2 - 3 days scheduled in advance once or twice a year. The scheduling of this period depends on the organization's activity and is generally scheduled during periods of lower activity.

Example of a scheduled remediation period: December 20 & 21 + June 28 & 29

During this period, the business knows in advance that the systems will be patched, and that the service provided by these systems will potentially be disrupted.

DEFER

This silo contains the least dangerous findings, very often non-exploitable vulnerabilities and/or vulnerabilities with a CVSS base score of less than 4.

This stock of exemptions can be considered temporary, and the content of this stock can be regularly re-evaluated, particularly if the Exploitability criteria have evolved over time.

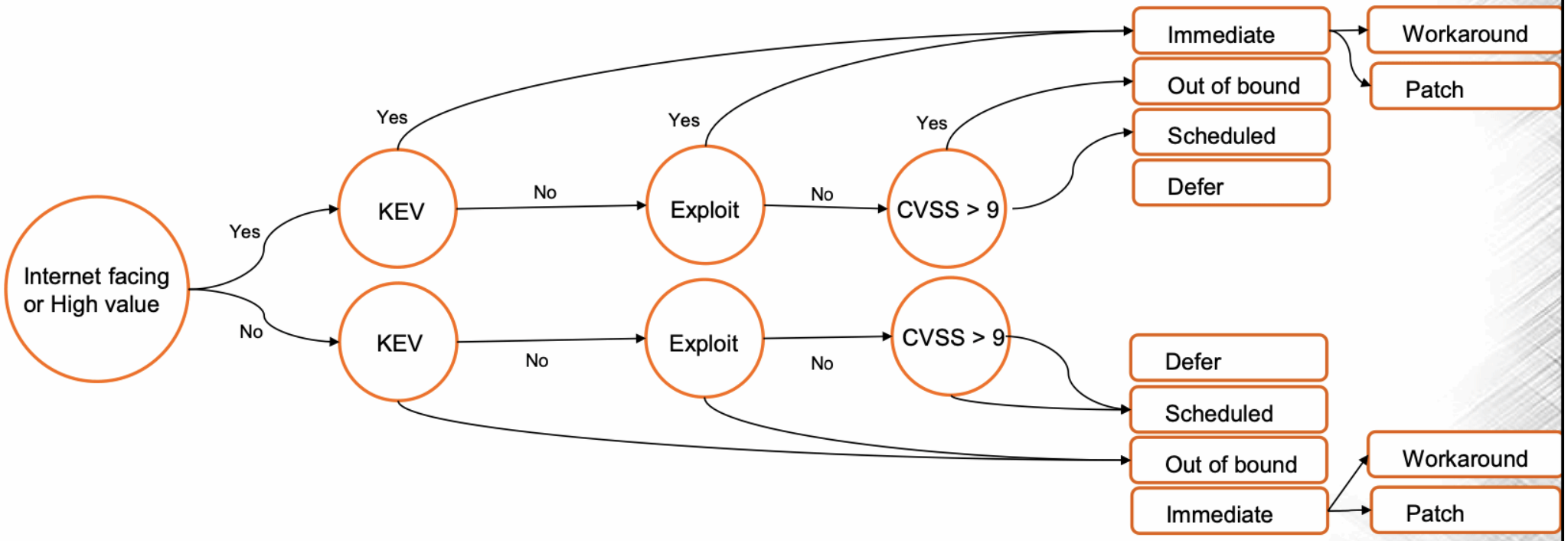
Recertification of this stock is an important activity, as certain vulnerabilities can be "forgotten" but used by attackers years after they first appeared.

CERT-IST Example

CERT-IST
INDUSTRIE | SERVICES | TERTIAIRE

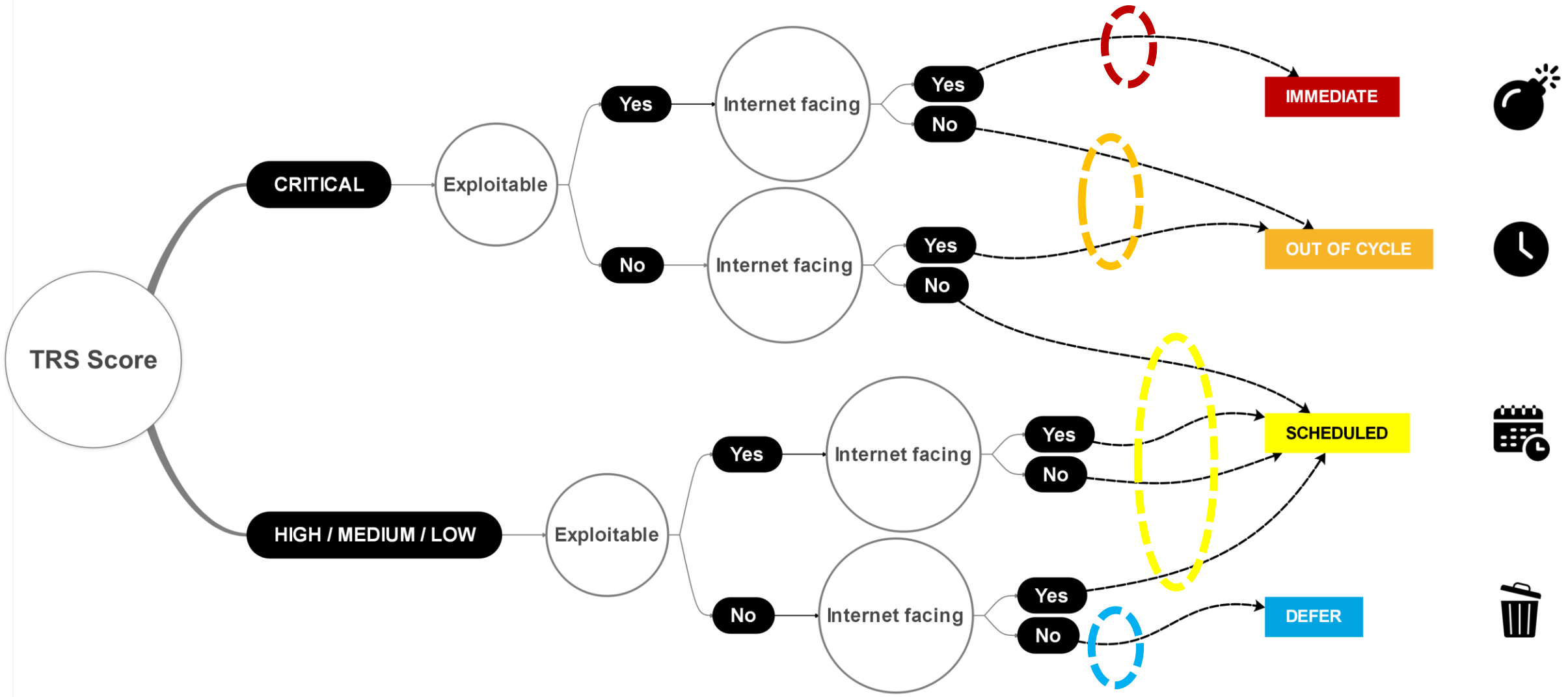
Au-delà de SSVC ?

- Construire un arbre de décision avec le même modèle que SSVC ?



IV. SSVC tree examples

SSVC-like process: example #1 - Organization with high remediation capacity



SSVC-like process: example #1 - Organization with high remediation capacity

NO ENTRIES

SSVC #1 - IMMEDIATE

SSVC #1 - IMMEDIATE

	Finding - Ignored	is	False True	
And	Finding - Deactivated	is	False True	
And	Finding - TRS v2 score	In	Critical	
And	Finding - Exploitable	is	False True	
And	Asset (TRS Metrics) - Exposure	In	Internet	

+ Rule + Group

SSVC-like process: example #1 - Organization with high remediation capacity

2 ENTRIES

SSVC #1 - OUT OF CYCLE

SSVC #1 - OUT OF CYCLE

Finding - Ignored | is | False | True

And

Finding - TRS v2 score | In | Critical

And | Finding - Exploitable | is | False | True

And | Asset (TRS Metrics) - Exposure | Not in | Internet

+ Rule | + Group | Delete group

Or

Finding - TRS v2 score | In | Critical

And | Finding - Exploitable | is | False | True

And | Asset (TRS Metrics) - Exposure | In | Internet

+ Rule | + Group | Delete group

+ Rule | + Group | Delete group

And | Finding - Deactivated | is | False | True

+ Rule | + Group

SSVC-like process: example #1 - Organization with high remediation capacity

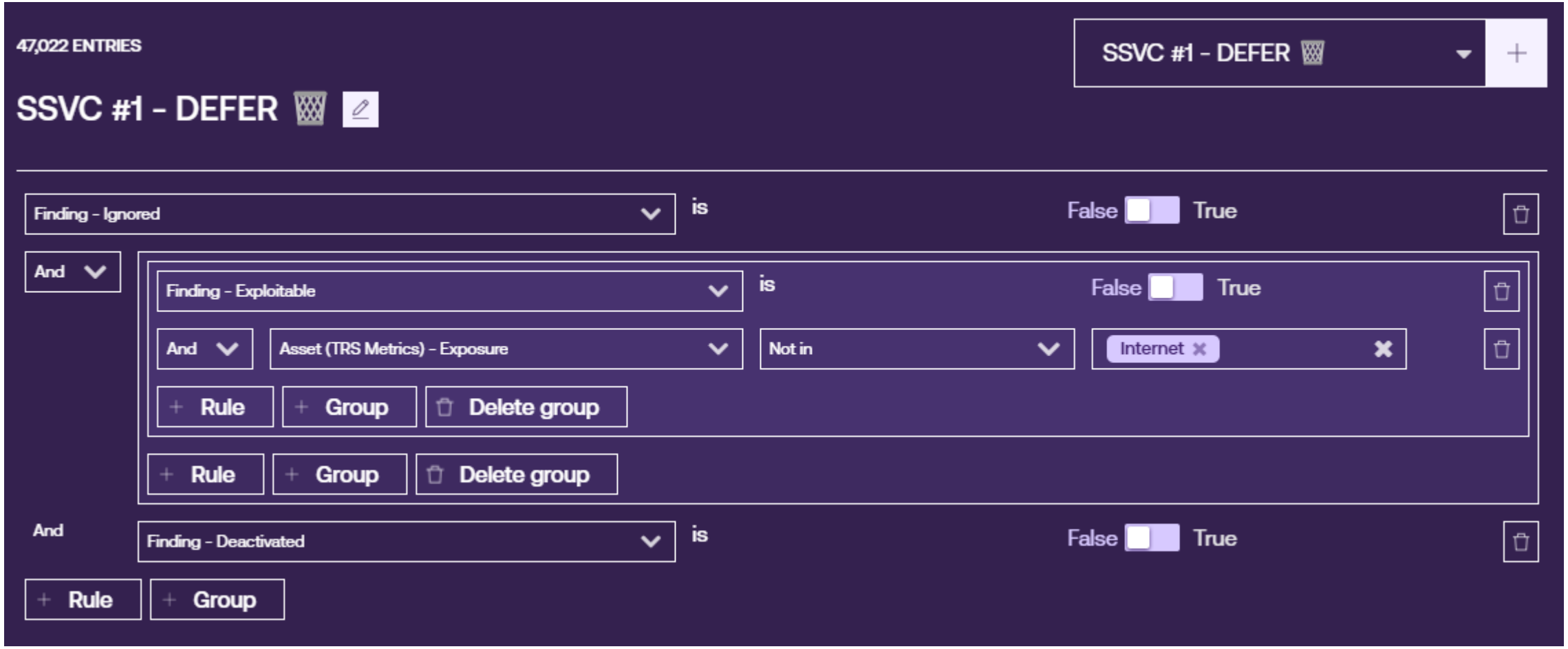
NO ENTRIES

SSVC #1 - SCHEDULED

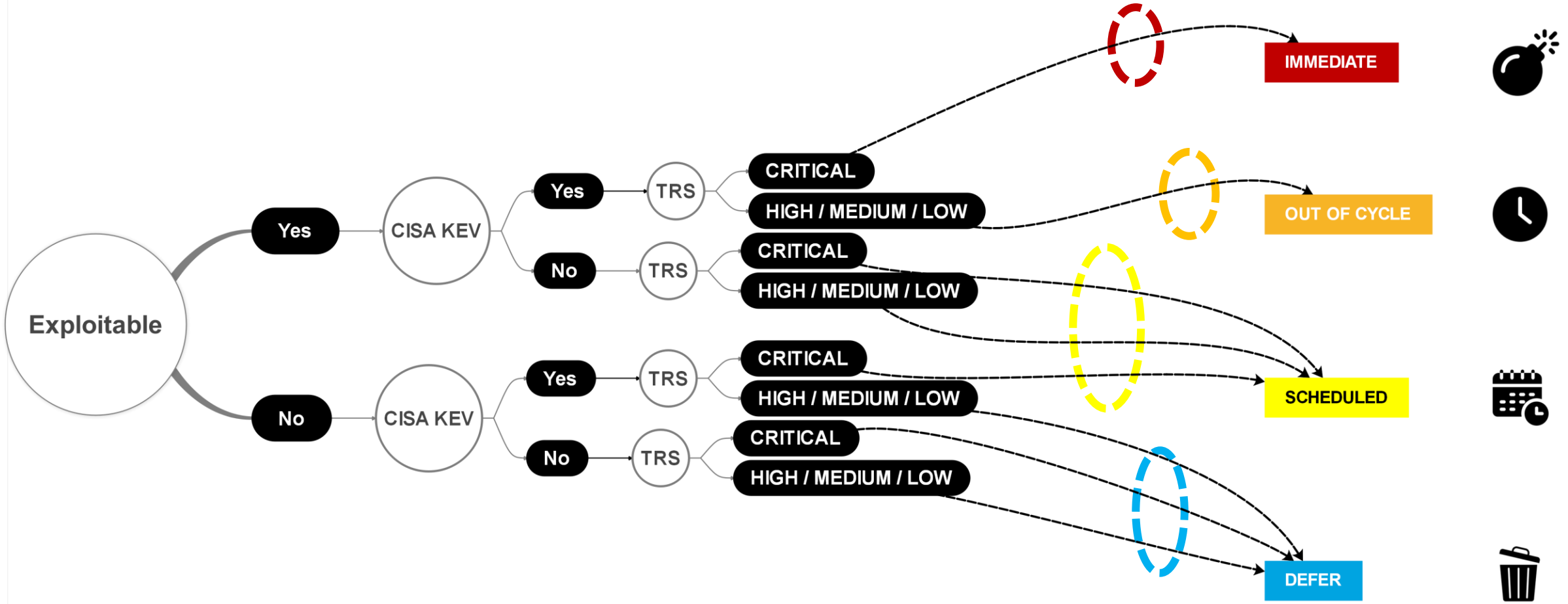
SSVC #1 - SCHEDULED

- Finding - Ignored is False True
- And
  - Finding - TRS v2 score In Critical
  - And Finding - Exploitable is False True
  - And Asset (TRS Metrics) - Exposure Not in Internet
  - Rule Group Delete group
  - Or
    - Finding - TRS v2 score Not in Critical
    - And Finding - Exploitable is False True
    - And Asset (TRS Metrics) - Exposure In Internet
    - Rule Group Delete group
  - Or
    - Finding - TRS v2 score Not in Critical
    - And Finding - Exploitable is False True
    - And Asset (TRS Metrics) - Exposure Not in Internet
    - Rule Group Delete group
  - Or
    - Finding - TRS v2 score Not in Critical
    - And Finding - Exploitable is False True
    - And Asset (TRS Metrics) - Exposure In Internet
    - Rule Group Delete group
  - Rule Group Delete group
- And Finding - Deactivated is False True
- Rule Group

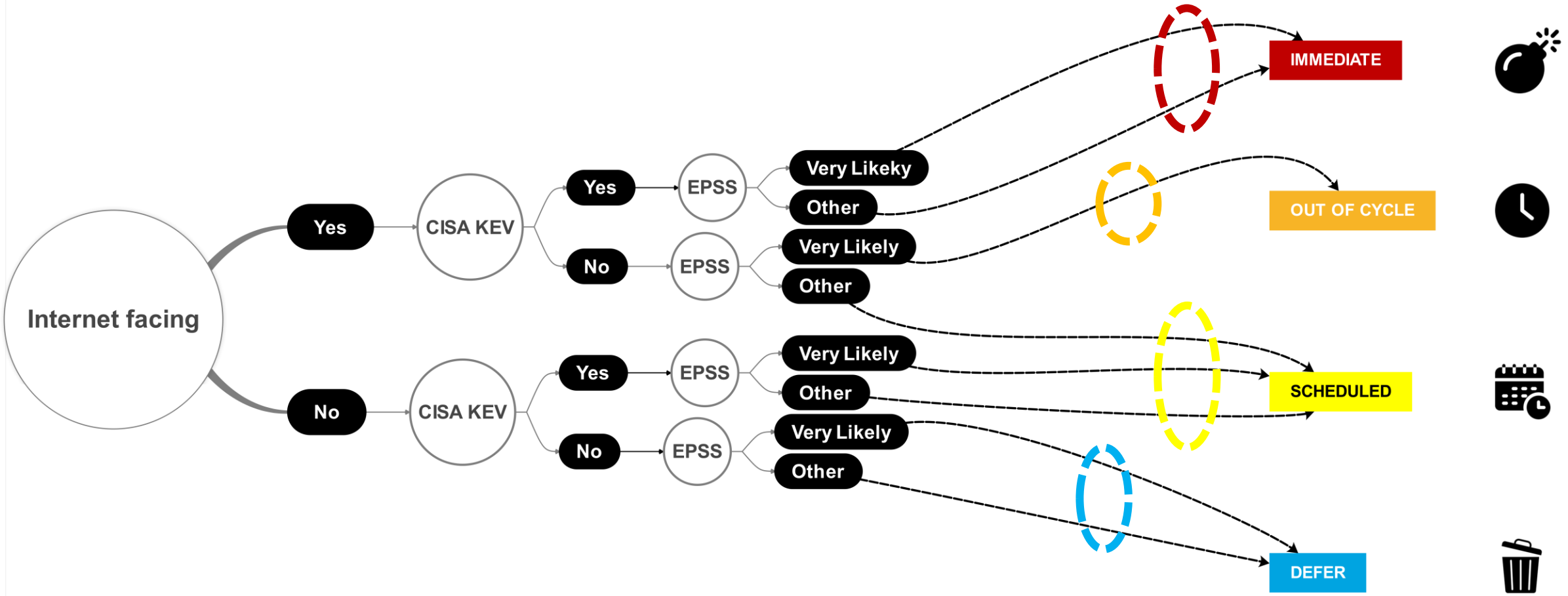
SSVC-like process: example #1 - Organization with high remediation capacity



SSVC-like process: example #2 - Organization with very limited remediation capabilities



SSVC-like process: example #3 - Organization running an Internet business with a high dependency on resilient cloud services



Démonstration par l'exemple

Evaluation du risque & Priorisation des efforts

V. TICKETING STRATEGY

Major steps to achieve the SSVC & ticketing strategy

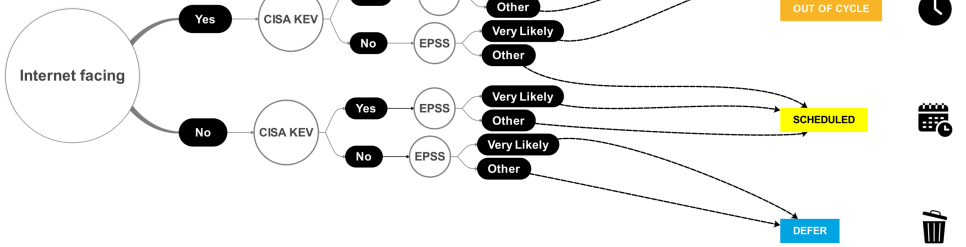
1. **Define your prioritisation strategy**
   You need to define which attributes and attribute values you want to use in your definition of the four remediation pools, and your choices depend mainly on this:
   - Your compliance constraints
   - Your security objectives
   - Your remediation capability
   - Your ITSM organization (how ticketing projects are organized, by OS team, by BU, etc.)

2. **Create a query by remediation pool and by team/project on the ITSM side + link your queries with Remediation Groups**
   You need to create a query that considers all the branches of the SSVC tree leading to the same Remediation Pool - in addition, if several teams are set up on the ITSM side, you need to create a subquery for each of the separate remediation teams on the ITSM side.
   In short, if you have three different ITSM teams dealing with a given Remediation Pool, you will have three queries.

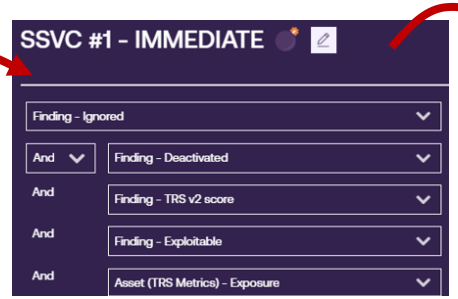
3. **Define and apply rules for monitoring ticket processing and remediation pools**
   You need to write consistent rules that define how the various tickets are tracked and how you monitor the actions taken. It's a good idea to use 2 or 3 KPIs that are easy to understand, but that will give you a clear picture of your organization's efficiency.

Overview – Example with the IMMEDIATE remediation pool for the 'Windows ITSM Team'

SSVC attributs definition



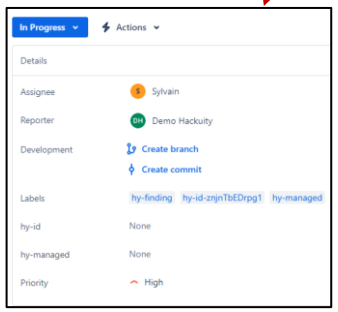
Query



+ Additional attribute to select the Windows Technology Stack

Remediation Group creation

HACKUITY REMEDIATION GROUP



Link with a ticket to the right team

Expired on July 26th 2024

2 months ago R2-3834

Follow-up of the remediation task since Hackuity & evolution of the risk over time

Detailed strategy considering ITSM organization: following example is for IMMEDIATE remediation pool & three different ITSM teams

IMMEDIATE

IMMEDIATE	Windows Technology stack	Filter: OS: *windows*	Windows ITSM project
IMMEDIATE	UNIX Technology stack	Filter: OS: *unix*	UNIX ITSM project
IMMEDIATE	MacOS Technology stack	Filter: OS: *macos*	MacOS ITSM project

For each Remediation Pool (in this example with IMMEDIATE), each team will receive a different ticket. Depending on the Remediation Pool and the organization's internal strategy, these tickets will be created once a day, once a week, etc. In this example, IMMEDIATE, the recommendation is to open a different ticket every day, with a Target Date of “Day+3”.

Windows ITSM project

Ticket R28287

UNIX ITSM project

Ticket R38232

MacOS ITSM project

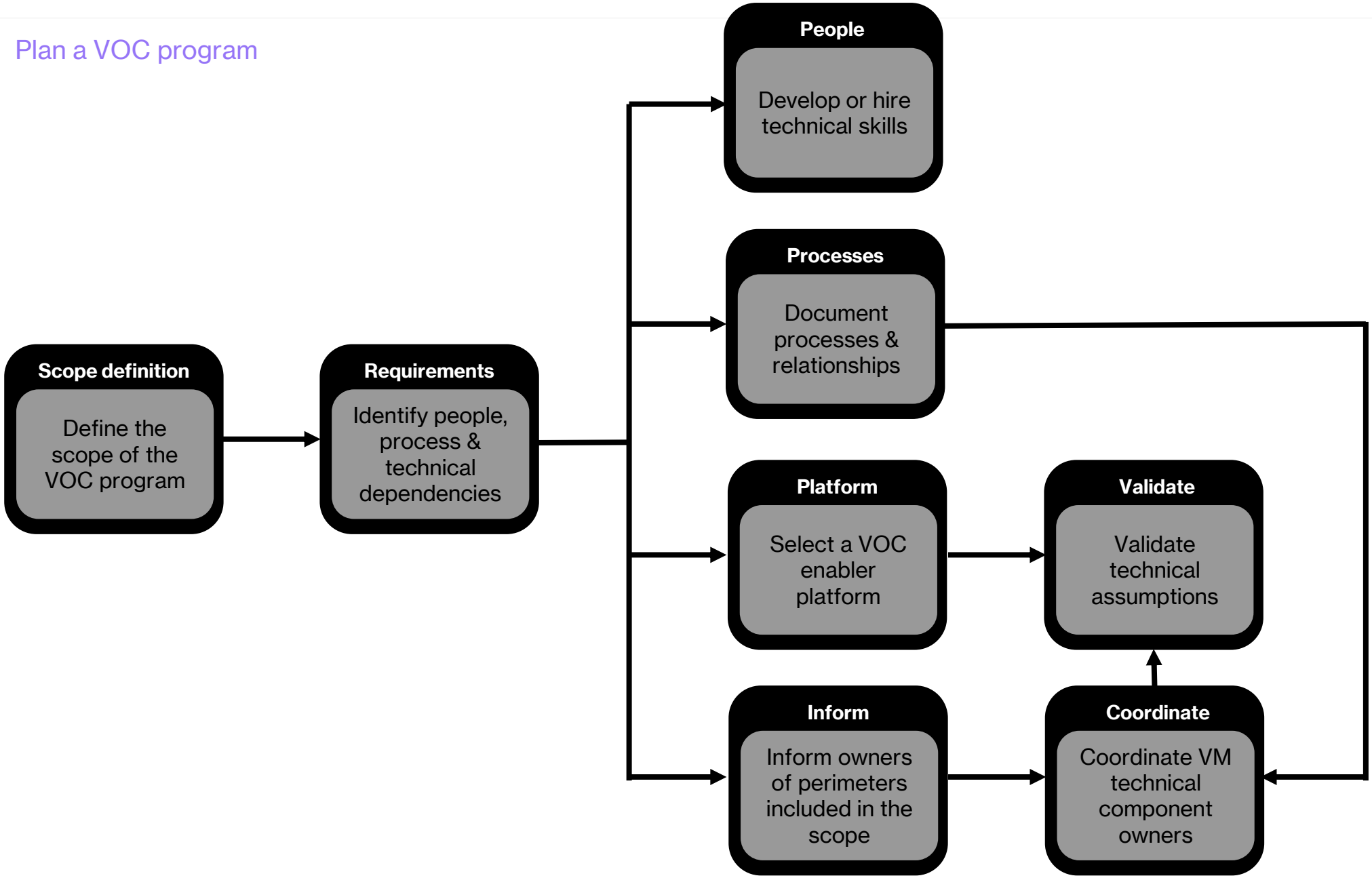
Ticket R99352

Démonstration par l'exemple

Automatisation des tâches & Ticketing

VI. THE VOC MATURITY

Plan a VOC program



What is needed for a VOC?

Mandatory	Optional
Connect all vulnerability data sources	Automated patching
Data deduplication	Automated virtual patching
Bidirectional ITSM connection	Advanced automated scenarios with SOAR
Automated prioritization	Transform Finding into Incident (SOC relay)
Automated findings lifecycle	Advanced Vulnerability Intelligence

VOC Maturity steps

CHAOS	COMMITTED	PROACTIVE	INTEGRATED & ALIGNED	STRATEGIC BUSINESS PARTNER
No VOC	Main components of the VOC are deployed Aggregation is ready Deduplication is ready Visibility on the Vulnerability dept VM technical KPIs are defined	The VM data lake is connected to the ITSM system VOC is used to execute the Vulnerability dept reduction, following a plan or campaigns Prioritization process is effective All VM processes are documented	CTI is considered in the prioritization process Connection to the SOC is effective Global VM KPIs cover all VOC practices Compliance solution is connected	Business Context is considered in the prioritization process The VOC is able to pilot the business dependencies (SOAR is ready) Move KPIs to the next level (VM to Business)

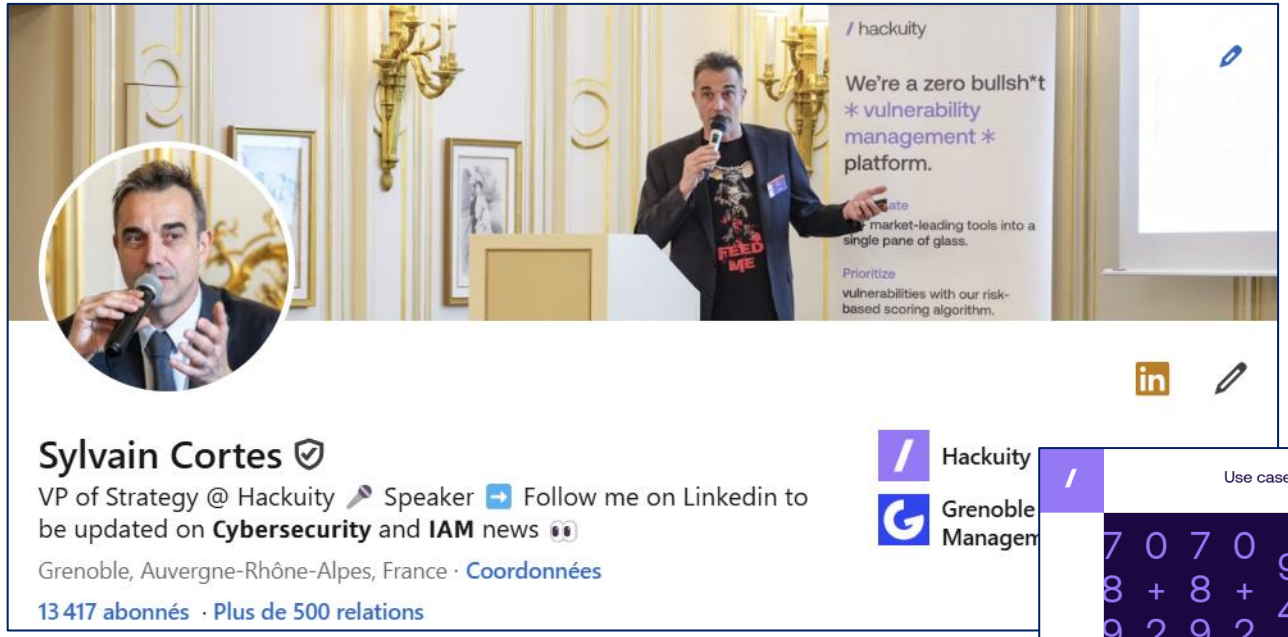
Mission is achievable by most organizations

Significant effort to reach these stages

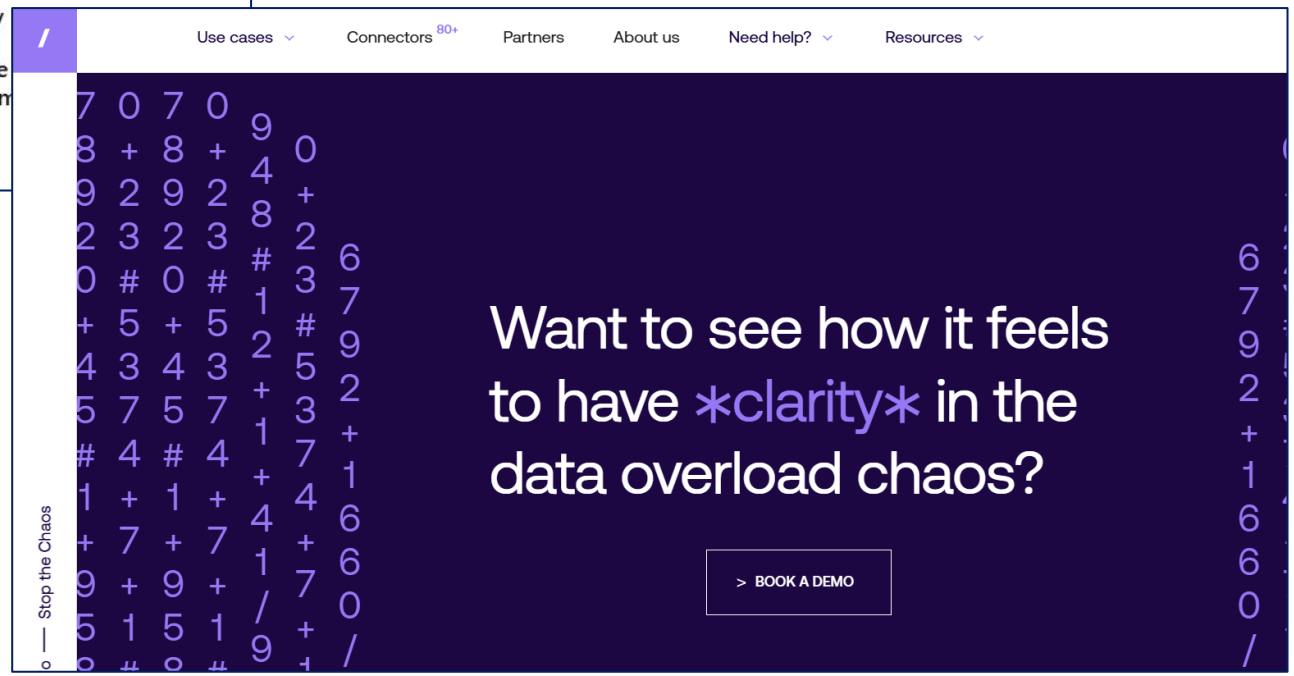
TAKEAWAYS

- VOC ≠ SOC
- Dans l’équilibre prévention/détection, attention à ne pas tout miser sur la détection
- Le VOC sera l’un des « big thing » de l’année 2025

TAKEAWAYS



https://www.linkedin.com/in/sylvaincortes/



https://www.hackuity.io/

hackuity

Thank you

https://www.hackuity.io →