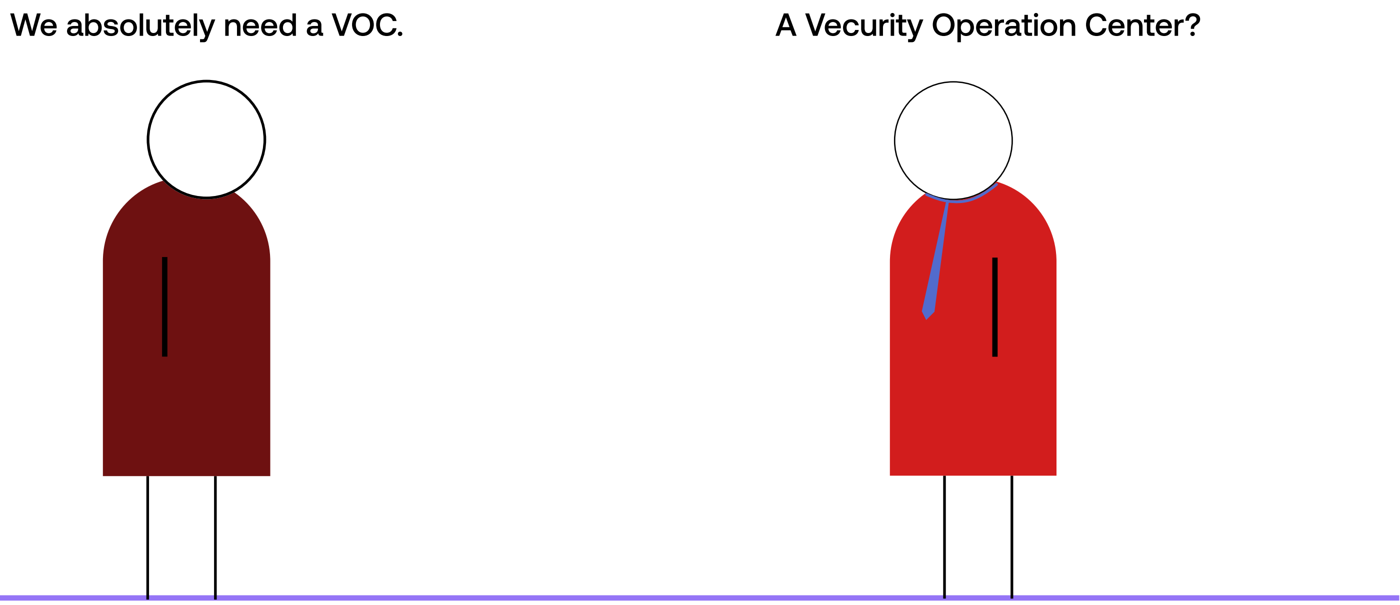
A CISO Guide to Building a Vulnerability Operations Center (VOC)



By hackuity

#Summary#

#01 What the VOC?!

A Vulnerability Operations Center (VOC) is an integrated function within, or alongside, your SOC that is dedicated to the continuous **identification**, **triage**, **prioritization**, **remediation**, and **reporting** of vulnerabilities across the organization.

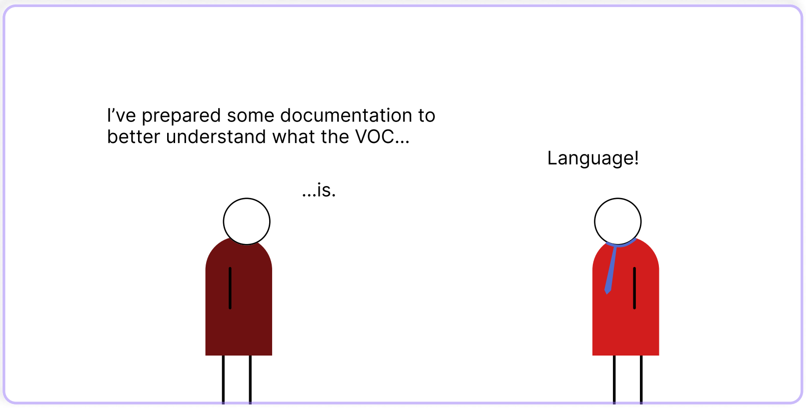

I've prepared some documentation to better understand what the VOC...
Language!
...is.

fig.1 - Trying to be cyber-polite.

Unlike traditional approaches that rely solely on periodic scans and siloed teams, a VOC offers a centralized, proactive, and risk-based methodology to manage vulnerabilities more efficiently and strategically.

Where classic models often treat vulnerabilities in isolation or according to static severity scores, a VOC introduces structured decision-making processes and context-aware analysis. This enables organizations to focus remediation efforts on vulnerabilities or assets that pose the most significant operational and business risks.

By establishing a VOC, security teams can:

- Reduce their attack surface
- Master risk exposure
- Streamline operations through automation, orchestration, and repeatable workflows
- Communicate value to executives and regulators via measurable metrics and outcomes

_In essence, a VOC acts as a mission control center for vulnerability operations—replacing fragmented, ad hoc practices with a scalable, sustainable program that bridges the gap between cybersecurity and business objectives.

#02 Why this guide?

CISOs often struggle with fragmented data, limited resources, and alert fatigue.

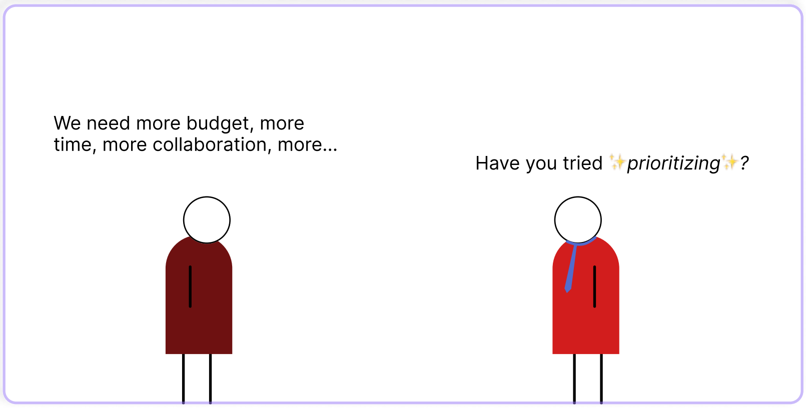
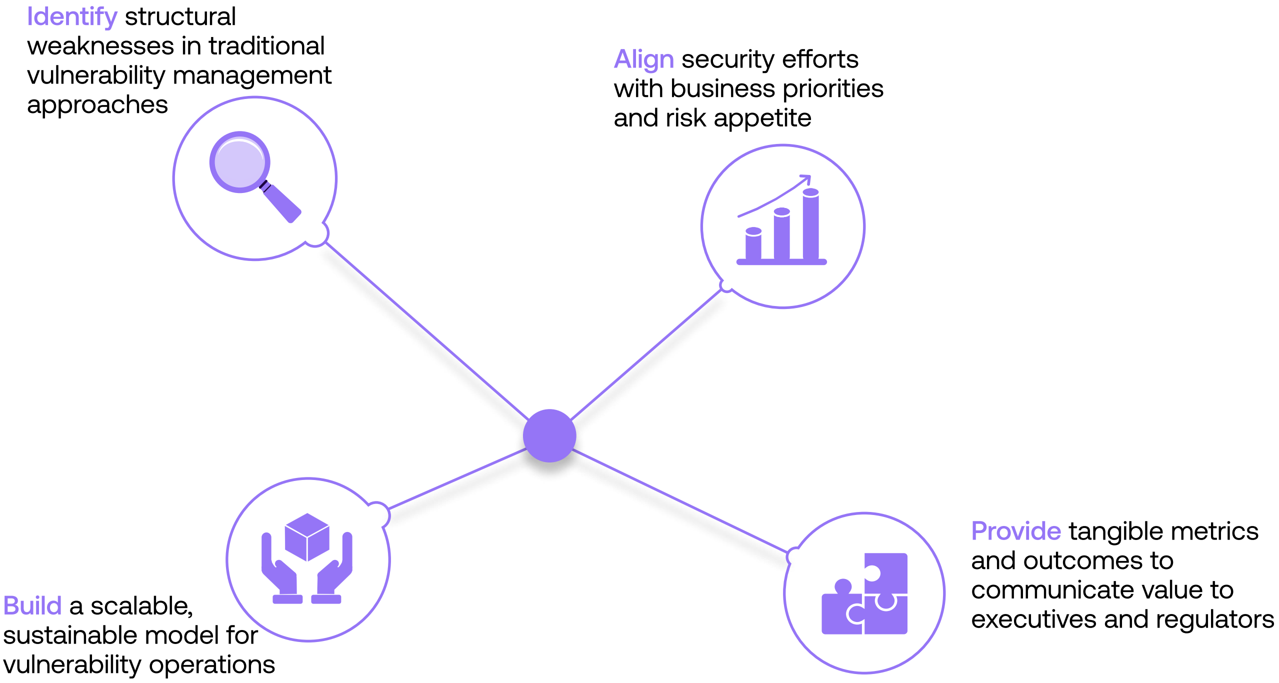

We need more budget, more time, more collaboration, more...
Have you tried ✨*prioritizing*✨?

fig.2 - "Try eating in front of your computer."

Security teams are overwhelmed with scan results and dashboards, yet still lack the visibility and clarity to act decisively. Despite their efforts, vulnerabilities pile up while execs and auditors keep asking questions.

This guide is for security leaders facing that challenge.

It offers a practical roadmap to build and run a VOC: a dedicated function to make vulnerability operations structured, scalable, and aligned with real-world business priorities.



Identify structural weaknesses in traditional vulnerability management approaches

Align security efforts with business priorities and risk appetite

Build a scalable, sustainable model for vulnerability operations

Provide tangible metrics and outcomes to communicate value to executives and regulators

_In short, this guide helps you move from reactive firefighting to proactive, risk-driven vulnerability management.

#03 The Case for a VOC

Modern security teams face an uncomfortable truth: despite all the tools, scans, and dashboards, vulnerabilities remain open for months, sometimes years, before being remediated.

+76%

of vulnerabilities being exploited by ransomware gangs were discovered more than three years ago.

> According Jay Jacobs, the EPSS father: "If we study the data related to post-exploitation cases, it turns out that 6% of exploitations are linked to CVEs that are less than 12 months old, while 94% of exploitations are associated with CVEs discovered more than 12 months ago."

38.2%

year-over-year growth in the total number of known vulnerabilities (CVEs) was reported by the NIST NVD.

367

is the average number of technologies used by large enterprises.

VOC vs. SOC

Different Focus, Shared Goal

The SOC is built for real-time detection and response. It manages alerts, investigates incidents, and contains active threats and breaches. It’s *reactive* by nature, often overwhelmed by noise, and focused on the present.

The VOC is *proactive*. It identifies and prioritizes vulnerabilities before they can be exploited, focusing on risk context, exposure, and specific business impact. It ensures structured remediation and reduces the attack surface over time.

Where the SOC defends, the VOC fortifies.

Together, they form a complete defence strategy: the SOC handles the now, the VOC prepares for what’s next.

Key Challenges in VM

1. **Overwhelming volume of vulnerabilities**
Security tools may report thousands of vulnerabilities per scan, many of which are low-risk or duplicates.

2. **Inconsistent prioritization**
Prioritization frameworks are not comprehensive or too rudimentary, teams may focus on the wrong vulnerabilities.

3. **Disconnected tools and workflows**
Lack of integration between security tools and IT workflows leads to inefficiencies and delays & lack of communication between functional teams.

4. **Delayed remediation**
Vulnerabilities often remain unaddressed due to unclear ownership, lack of visibility, or slow ticketing processes.

Benefits of a VOC

Measurable outcomes

Use KPIs and dashboards to demonstrate risk reduction, remediation efficiency over time and identify areas for improvement.

Centralized visibility

One unified platform to view and act on vulnerabilities across infrastructure, applications, and cloud.

VOC

Streamlined workflows

Integrate scanning, ticketing, and remediation tools to remove friction.

Risk-based prioritization

Focus on vulnerabilities that are most likely to be exploited and that would cause the most damage.

Making Remediation Actionable

Counting critical vulnerabilities is useful, but it is far better to focus on the remediation plan.

#04 VOC Framework Overview

A VOC is not just a dashboard or a new tool—it's a complete operational framework. It transforms scattered vulnerability data into coordinated, risk-driven action across people, processes, and technologies.

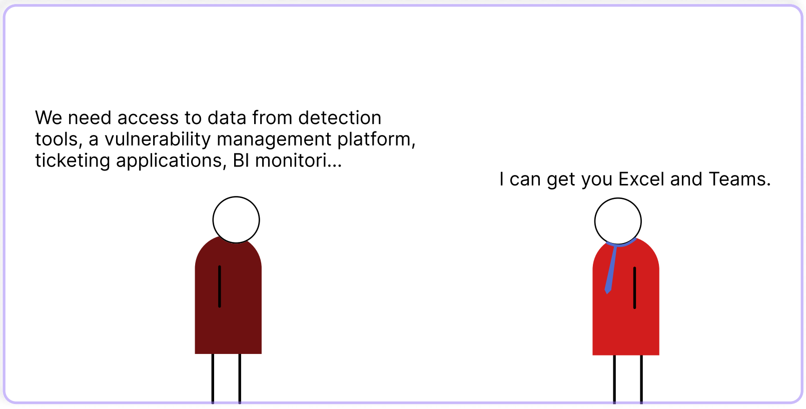

We need access to data from detection tools, a vulnerability management platform, ticketing applications, BI monitori...
I can get you Excel and Teams.

fig.3 - "And don't forget to check notification during the weekend."

Assessment (Monitoring & Discovery)

Ingest vulnerability data from all relevant sources—scanners, cloud platforms, applications, threat intel, pentests, bug bounty.

Consolidate, Deduplicate & Normalize (CDN)

Clean and standardize the data across relevant formats and tools (VM tools, cloud, apps, etc.).

Prioritization

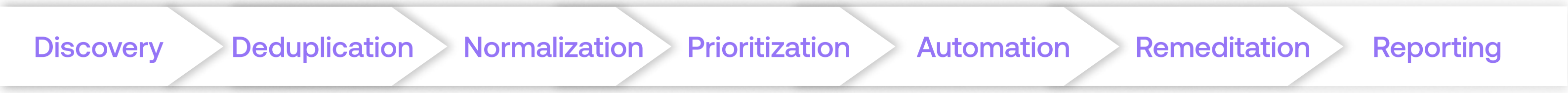
Prioritize vulnerabilities using risk scoring that combines CVSS, threat intelligence, asset context, and exploitability; enhanced by TRS (True Risk Score) to reflect the evolving nature of real-world risks

Workflow Automation & Remediation

Route remediation tasks to the right teams with SLAs. Ensure accountability, track progress, and automate reporting.

Reporting & Metrics

Deliver insights at tactical, operational, and strategic levels, enabling informed decisions and continuous improvement.


Discovery
Deduplication
Normalization
Prioritization
Automation
Remeditation
Reporting

The VOC Pyramid

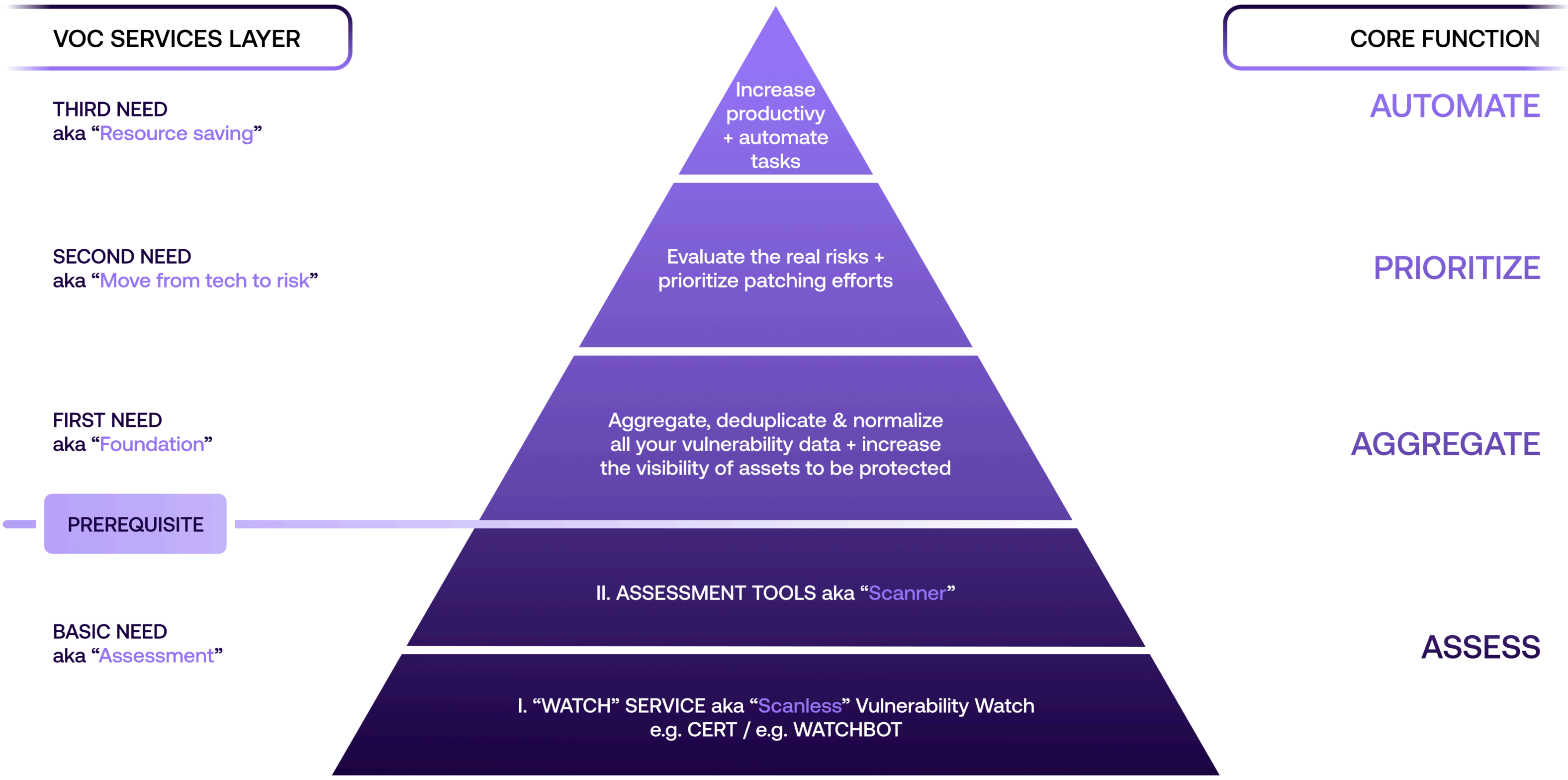

VOC SERVICES LAYER
CORE FUNCTION
THIRD NEED
aka "Resource saving"
Increase productivy + automate tasks
AUTOMATE
SECOND NEED
aka "Move from tech to risk"
Evaluate the real risks + prioritize patching efforts
PRIORITIZE
FIRST NEED
aka "Foundation"
Aggregate, deduplicate & normalize all your vulnerability data + increase the visibility of assets to be protected
AGGREGATE
PREREQUISITE
II. ASSESSMENT TOOLS aka "Scanner"
BASIC NEED
aka "Assessment"
I. "WATCH" SERVICE aka "Scanless" Vulnerability Watch e.g. CERT / e.g. WATCHBOT
ASSESS

fig.4 - The different stages of the VOC pyramid

The VOC Operating Model

<Technology>

A strong VOC integrates scanners, asset management systems, CMDBs, ticketing tools, and threat intelligence platforms to enable automation and context-rich analysis.

<People>

Key roles include VOC analysts, vulnerability managers, product security, IT support, and DevOps teams, all aligned under shared remediation objectives.

<Process>

Governance includes SLAs, exception handling, remediation workflows, and risk acceptance.

#05 Step 1 | Assessment

GOAL | Establish **foundational visibility** into your IT environment, attack surface, existing vulnerabilities, and the external threat landscape.

To begin, let's list all of our assets, and let's move forward methodologically by...
Let's not loose time, patch all findings. Here, take that and off to work!

fig.5 - Done isn't always better than perfect

Key actions

1. **Baseline Asset Discovery**
   Build a complete and up-to-date IT inventory across on-prem, cloud, and hybrid environments.

2. **Identify Shadow IT and Unmanaged Assets**
   Unmanaged systems represent blind spots often missed in security coverage—and are frequently exploited first.

3. **Deploy Vulnerability Scanning Tools**
   Use a layered approach with tools covering:
   - Infrastructure (network scanners, agents)
   - Applications (SAST, DAST, SCA)
   - Cloud workloads and containers

4. **Subscribe to Threat and Vulnerability Feeds**
   Integrate trusted sources into your detection pipeline:
   - CISA KEV Catalog
   - NIST NVD
   - Vendor security advisories
   - CERT bulletins
   - Private CTI feeds (if available)

TIPS | Document gaps and build a business case for assessment/security tools

#06 Step 2 | Consolidate, Normalize & Deduplicate

GOAL | Break down silos and build a **unified, reliable vulnerability dataset** to support accurate risk analysis and decisive action. Consolidation transforms scattered technical data into a solid foundation for effective VOC operations.

Key actions

1. Integrate vulnerability scanners across all layers: infrastructure, cloud, containers, applications.
2. Connect asset management tools or CMDB to enrich each vulnerability.
3. Incorporate threat intelligence feeds and asset inventory metadata.
4. Normalize vulnerability metadata.
5. Deduplicate findings by comparing asset ID, IP, hostname, location.
6. Tag assets based on business criticality.

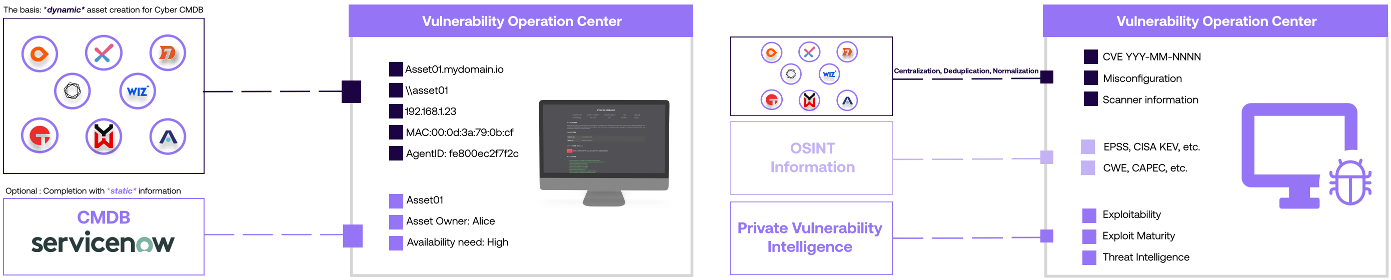


fig.6 - Explanatory graph on how the VOC is powered.

TIPS

Use APIs and webhooks for real-time data ingestion.

Conduct periodic reconciliation with CMDB and asset inventory

Include shadow IT and third-party assets to avoid blind spots.

Map vulnerabilities to real-time asset ownership and criticality using CMDB or scanner tagging.

#07 Step 3 | Risk-Based Prioritization with Full Context

GOAL | Identify and address the vulnerabilities that pose **the highest actual risk**, not just the highest technical severity.

Key Risk Factors to Consider

Threat Intelligence
Is there active exploitation in the wild?

Exploitability
Use indicators like CVSS score, EPSS likelihood, CISA KEV listing.

Asset Exposure
Is the system internet-facing? Part of a regulated workload?

Business Impact
What would be the impact on confidentiality, integrity, and availability if this vulnerability were exploited on this asset?

Key approaches

1. Build a weighted scoring model that includes internal and external risk signals.
2. Use automation to continuously re-rank vulnerabilities as context changes.
3. Define your proritization strategy based on risk appetite

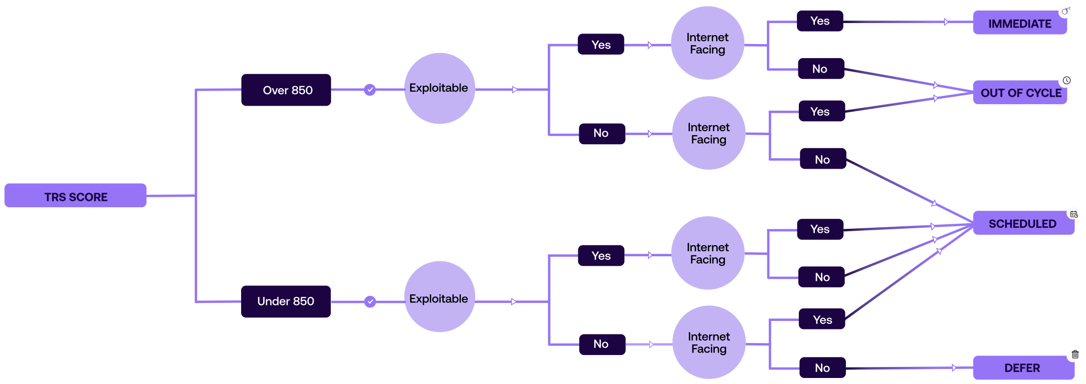


fig.7 - Example of a SSVC-like process for an organization with high remediation capacity

#08 Step 4 | Automate your Tracking and Remediation

GOAL | Eliminate **manual handoffs,** reduce **remediation delays,** and ensure **closure and accountability** at every stage of the vulnerability lifecycle.

Key actions

1. **Integrate with ITSM, ticketing, and communication channels**
   Seamlessly connect the VOC with the likes of Jira, ServiceNow, Slack, Microsoft Teams...

2. **Auto-group vulnerabilities**
   Use business context and asset metadata to group findings by owner, environment, or application stack.

3. **Auto-assign tickets based on ownership**
   Route issues directly to the teams responsible for the impacted asset.

4. **Set SLAs based on risk level**
   Define deadlines aligned to risk and exposure.

5. **Track remediation status automatically**
   Monitor progress across tools, teams, and environments.

6. **Escalate overdue items**
   Notify responsible managers or trigger workflows with the change board.

7. **Enable compensating controls**
   Where patching is not possible, support risk acceptance, mitigation, segmentation, or virtual patching.

Best Practice

> **Align remediation SLAs with risk tiers and exposure:**
> - *Critical + Internet-facing → 7 days*
> - *High + Intranet → 21 days*

> **Set up automated closure verification, e.g., confirm patch is effective via new scan results.**

#09 Step 5 | Reporting and Metrics

GOAL | Translate technical remediation work into **clear, business-relevant** insights. Show progress, risk posture, compliance aligment, and drive continuous improvement in vulnerability management.

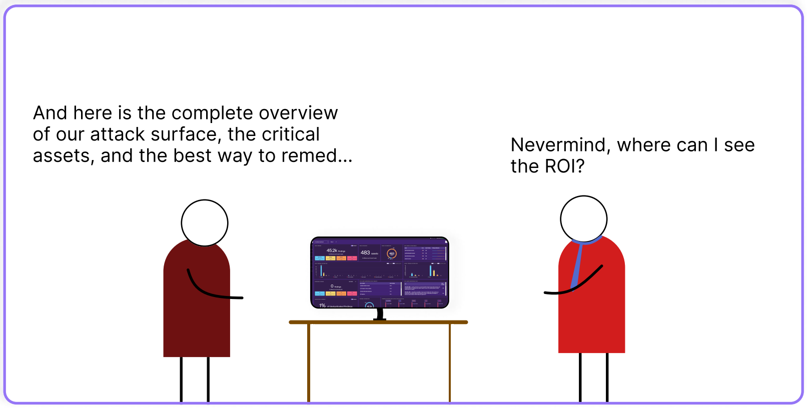

And here is the complete overview of our attack surface, the critical assets, and the best way to remed...
Nevermind, where can I see the ROI?

fig.8 - Priorities first.

Tailor reporting by audience

1. **Executives**
   Focus on high-level risk posture, top business impact, and risk reduction over time.

2. **Security Teams**
   Provide visibility into prioritization effectiveness, remediation blockers, and backlog trends.

3. **Auditors & Compliance**
   Deliver structured evidence of timely remediation, exception processes, and SLA adherence.

Key Metrics to Track

- MTTR (Mean Time to Remediate)
- SLA Adherence Rate
- Remediation Success Rate
- Open vs. Closed Vulnerability Trend

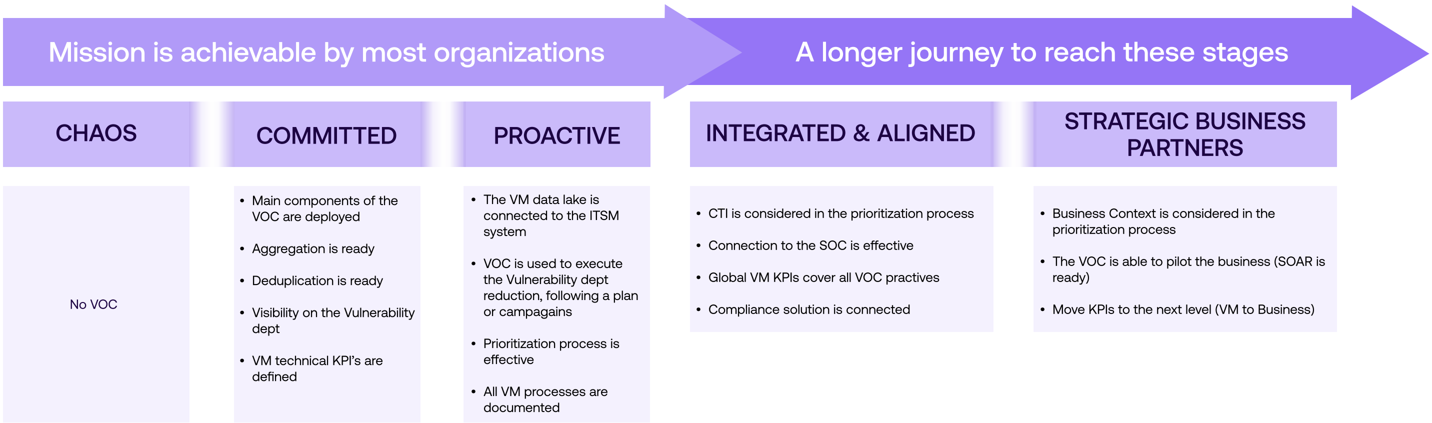
Recommended Dashboards

- Risk heatmaps by business unit or environment
- Top 10 vulnerabilities by risk score or exposure
- SLA performance and breach reports
- Trends in newly discovered, remediated, and overdue issues.

#10 VOC Maturity Model

Not all organizations need a fully optimized VOC from day one. The goal is **progressive**, **measurable maturity**—with the **right steps, tooling, and structure** at each level. This model helps teams benchmark their current posture and define a roadmap for growth.

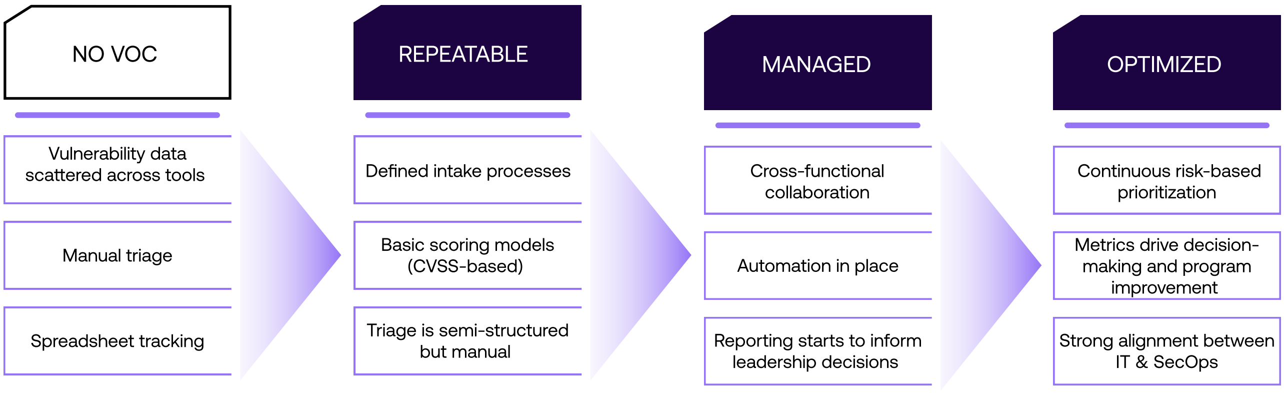
VOC maturity steps



Mission is achievable by most organizations			A longer journey to reach these stages	
CHAOS	COMMITTED	PROACTIVE	INTEGRATED & ALIGNED	STRATEGIC BUSINESS PARTNERS
No VOC	• Main components of the VOC are deployed • Aggregation is ready • Deduplication is ready • Visibility on the Vulnerability dept • VM technical KPI's 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 campagains • 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 practives • Compliance solution is connected	• Business Context is considered in the prioritization process • The VOC is able to pilot the business (SOAR is ready) • Move KPIs to the next level (VM to Business)

fig.9 - The steps of VOC Maturity and how to reach them.

Levels of VOC maturity



NO VOC	REPEATABLE	MANAGED	OPTIMIZED
Vulnerability data scattered across tools	Defined intake processes	Cross-functional collaboration	Continuous risk-based prioritization
Manual triage	Basic scoring models (CVSS-based)	Automation in place	Metrics drive decision-making and program improvement
Spreadsheet tracking	Triage is semi-structured but manual	Reporting starts to inform leadership decisions	Strong alignment between IT & SecOps

fig.10 - The different stages of VOC Maturity.

Assessment & Progression

Run VOC maturity assessments every 6 to 12 months to evaluate process, coverage, tooling, and outcomes.

Define quarterly KPIs to drive improvement—for example:
- Reduce MTTR on critical findings by 20%
- Contextualized risk-score (e.g. TRS) < 8/10 across all entities

#11 Getting the Buy-In

Because great ideas still need a green light, a successful VOC initiative requires more than just good tooling, it needs **strategic alignment** and **executive sponsorship**. Getting leadership buy-in early can accelerate funding, unlock resources, and embed the VOC into broader resilience and risk strategies.

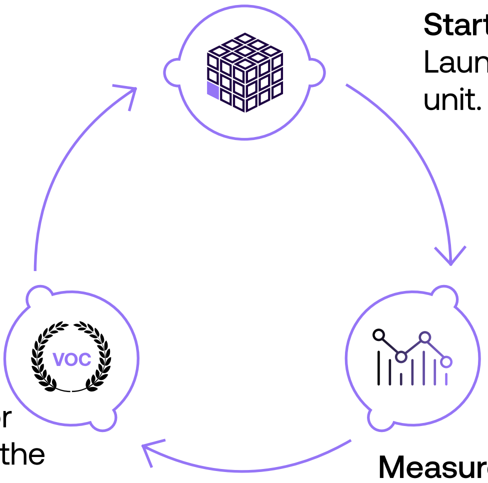
Key messages

1. **VOC reduces breach risk and enhances compliance readiness**
   By addressing vulnerabilities proactively and proving SLA adherence, the VOC strengthens both cyber resilience and audit posture.

2. **It delivers cost savings**
   Less rework, fewer escalations, and better coordination between security, IT, and DevOps reduce operational friction and human effort.

3. **It improves security team efficiency**
   Automation frees up analyst time, reduces alert fatigue, and brings clarity to remediation workflows.

Tips for securing <Buy-In>



Start small
Launch a pilot VOC in one business unit. Show tangible impact.

Measure impact
Track quantifiable outcomes such as SLA adherence or exposure reduction.

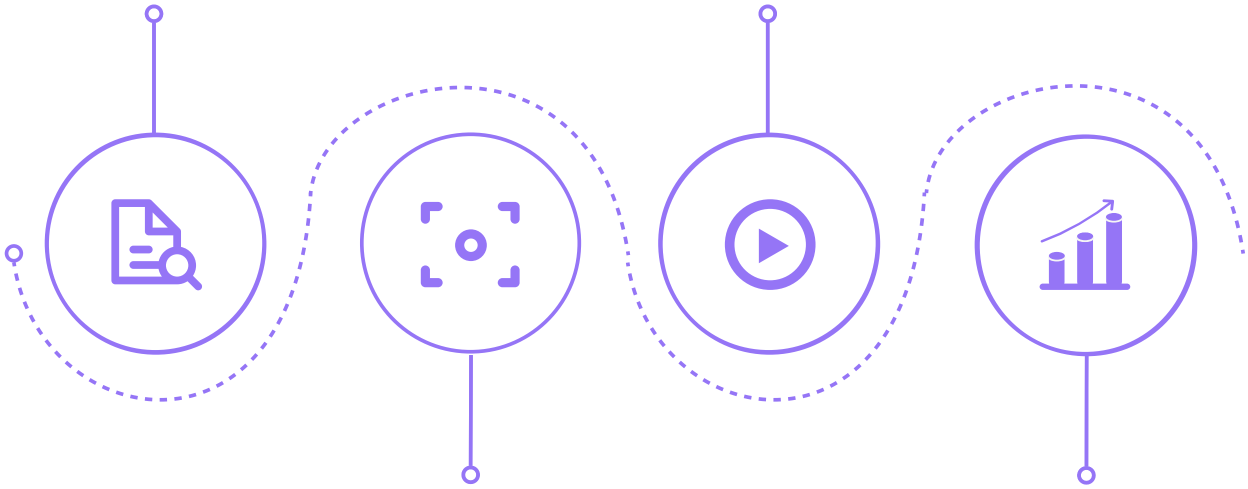
Tie outcomes to strategic goals
Align the VOC as an enabler of operational resilience, regulatory or readiness. Terms that resonate at the board level.

#12 Conclusion and Next Steps

Building a VOC is not about implementing a single tool—it’s about creating a **long-term operational capability** that changes how your organization manages cyber risk.

But success depends on leadership, cross-team collaboration, and a commitment and a mindset to continuous improvement.

Next steps



Assess your current state
Review your existing tools, workflows, gaps and existing sources of vulnerability data.

Define your VOC vision and scope
Tailor it to your origanization size and risk profile.

Start fast
Launch a pilot focused on a critical asset group or business unit.

Go deep & scale gradually
Use quick wins to drive adoption across techno stacks and teams.

Ready to put it into action?

Building a resilient and efficient VOC starts with one conversation.

Speak with Hackuity's VOC experts to explore your roadmap, pilot ideas, and tools to scale with confidence. Find out how you can take the first step towards building a resilient and efficient VOC.