VOC: the future of vulnerability management?

26 447

Vulnerabilities were disclosed in 2023

26.5%

With a PoC exploit available

31%

of CERT-W interventions in 2023 had an unpatched vulnerability as the entry point of the attacker

All IS components are affected: **OS, middleware, applications, network and security components,** etc.

In particular, assets **exposed on the Internet** (websites, services, etc.) and **core infrastructures** (AD, etc.) are targeted.

Vulnerability management, a pillar for IT security

Sources

- *2023_10 CERT-Wavestone 2023 Report: Ransomware, Geopolitical risk, and Artificial intelligence*
- *2023_03 Forrester The state of vulnerability risk management*
- *2023_12 Qualys - Threat landscape year in review : if everything is critical, nothing is*

A quick glossary for what follows

Vulnerability

Vulnerabilities are security flaws in production. *Vulnerabilities are reported, for example, by Qualys-type scanning tools, pentests and/or security flaws that have passed into production.*

Security defect / flaw

During project phase, it's only considered as a security flaw; ***a project should not go into production with security flaws****. Security flaws are identified through code reviews for example.*

Vulnerability management

Capability *to* ***identify and remediated*** *vulnerabilities on devices* ***that are likely to be used by attackers to compromise a device*** *and use it as* ***a platform*** *from which to* ***extend compromise to the network.***

Patch Management

The ***systematic*** *notification, identification, deployment, installation, and verification of* ***operating system*** *and* ***application software code revisions****. These revisions are known as patches, hot fixes, and service packs.*

6 typical challenges faced by our clients…

1. Scoping & defining the sources of inputs
2. Managing tools that are not standardized and overlapping
3. Dealing with insufficient or unreliable inputs to move forward
4. Prioritizing a large backlog of vulnerabilities
5. Meeting remediation SLAs
6. Reporting to Senior Management

VOC is the future of Vulnerability Management

A **VOC** (Vulnerability Operation Center) is an **orchestrator for vulnerability management** as it **combines** a **platform for centralizing vulnerabilities** detected by a variety of tools (such as SAST, DAST and IAST) in order to **better manage their remediation by rationalizing and prioritizing them** and a **governance system** defined with a **clear organization of tasks and assignments** (e.g. OnPrem, Cloud, Entities, remediation team, detection team, vulnerability responsibilities etc.)

VOC main objectives are

AUTOMATION

Build use cases to automate detection and remediation and leverage on integration with SOAR and ITSM tools
(e.g replay of a security test to validate vulnerabilities have been fixed on the whole chain).

EFFICIENCY

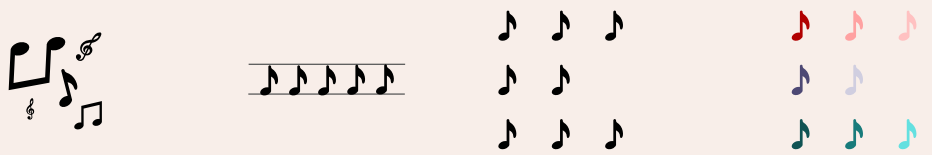
Aim for quality of remediation and not quantity! Vulnerabilities are prioritized according to risk appetite (assets criticality, scope…).

One Platform to remediate them all!

CMDB

Inside the centralization and prioritization tool

- Vulnerability scanners
- Penetration testing
- Threat Vulnerability Intelligence (TVI)
- Code review
- Configuration review
- Etc.



Centralization

Ensure integration with multiple data source
Centralization is reached through **connectors** / APIs with **various type of third parties**

Rationalization

Ensure consistency between the sources
Remove **duplicates** (between pentests & vuln scan for instance) and allow **unified scoring**

Prioritization 1

Through CVSS classic scoring
Or other referentials

Prioritization 2

Provide contextualized information
Prioritization aims at assessing the **exploitability** (ex: internet-facing) of the vulnerability & the **criticality** for the business

Automated workflow with administration tool

Remediation

Dashboard & KPI
- Asset view
- Pre defined reporting for management
- KPI – vulnerability score average, remediation time, etc.

Qualys · Nucleus · VULCAN. · ArmorCode · RAPID7 · Balbix · hackuity · ARMIS. · CISCO

Automation for remediation with production & dev teams is key

Automate ticket creation with automatic assignment to the right teams, respecting their usual tools and processes:

Infrastructure team

Tickets must be adapted to production teams (ServiceNow for example)

Applicative team

Tickets should be materialized as **user stories** of vulnerability corrections intended for developers (e.g., Jira), followed by Security Champions

*Using **CI/CD controls in blocking mode** is essential to minimize the backlog of application vulnerabilities.*

Automatically reconcile remediation and detection

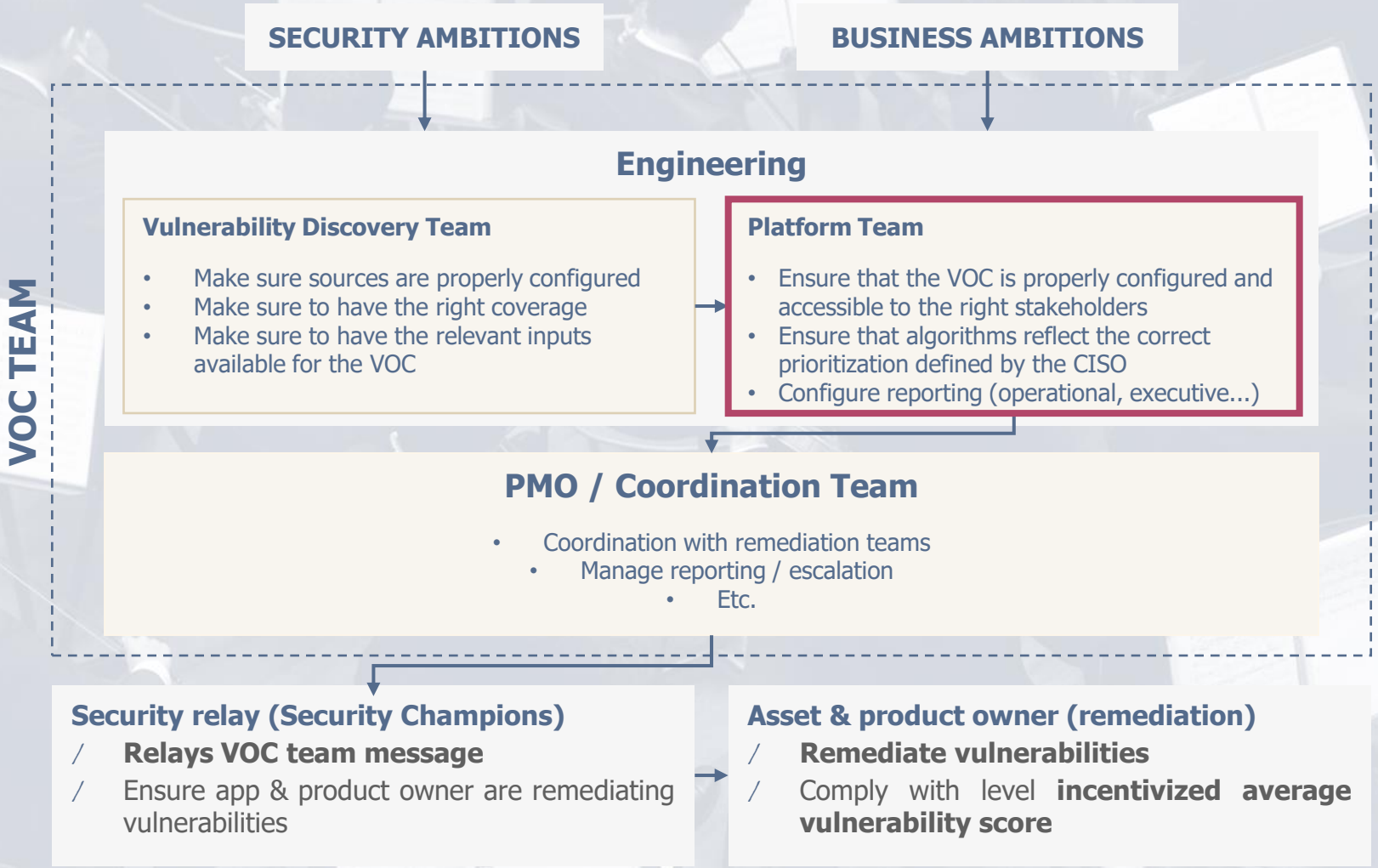
Key success factors

Must be **integrated into the classic life cycle** of the teams concerned.

SLAs must be clearly established, and form part of the service commitment of production and/or development teams, depending on the criticality of the vulnerability.

It's **impossible to mitigate everything**. Remediation is not just about patching or modifying code and might require a **risk reduction approach.**

A proper VOC governance to set the pace



Rely on VOC to clarify responsibilities among the various stakeholders.

But concretely how to start the journey to VOC ?

What's next?

1. **Generalize** to other business stakeholders
2. And then, only once the business stakeholders are well onboarded, **extend the data sources**

Design remediation workflows

Work closely with the **infrastructure and application remediation teams** to create an integrated remediation workflow **aligned with their existing processes**.

04

Fine-tuning prioritization

Focus on a single business scope to test prioritization (and remediation) and **define the necessary requirements** (up-to-date CMDB, context of the corresponding asset and the business chain).

03

Define the initial data sources

Start by integrating **only 2 vulnerability sources** while **ensuring formatting consistency** and **defining the pre-sorting level** before sending to the VOC.

02

Review the prioritization strategy

Identifying the criteria to consider for prioritization: CVSS only, internet-facing, technology, exploit, etc.

01

Build the VOC in POC mode

Thank you !

Hélène DUTILLEUL
Senior Manager

M +33 (0)6 88 94 38 17
helene.dutilleul@wavestone.com

Lauren MASSONI
Senior Consultant

M +33 (0)7 60 17 73 47
lauren.massoni@wavestone.com