Cyber Risk Management in DevSecOps

Fuelling Business Decision-makers with Meaningful Metrics

Estevan Chaves

May/2024

THE PROBLEM

Getting attention to **what really matters** in Cyber Security is not as always easy as it should be.

The **usual suspects** business actors are loaded of their own goals, tasks, processes and problems to pay attention on things that are not *explicit* connected to their objectives.

On the other hand, **security professionals** (I am one) have been smashing those actors with several requirements, from mandatory to recommended security controls, sometimes with (near) zero business appeal.

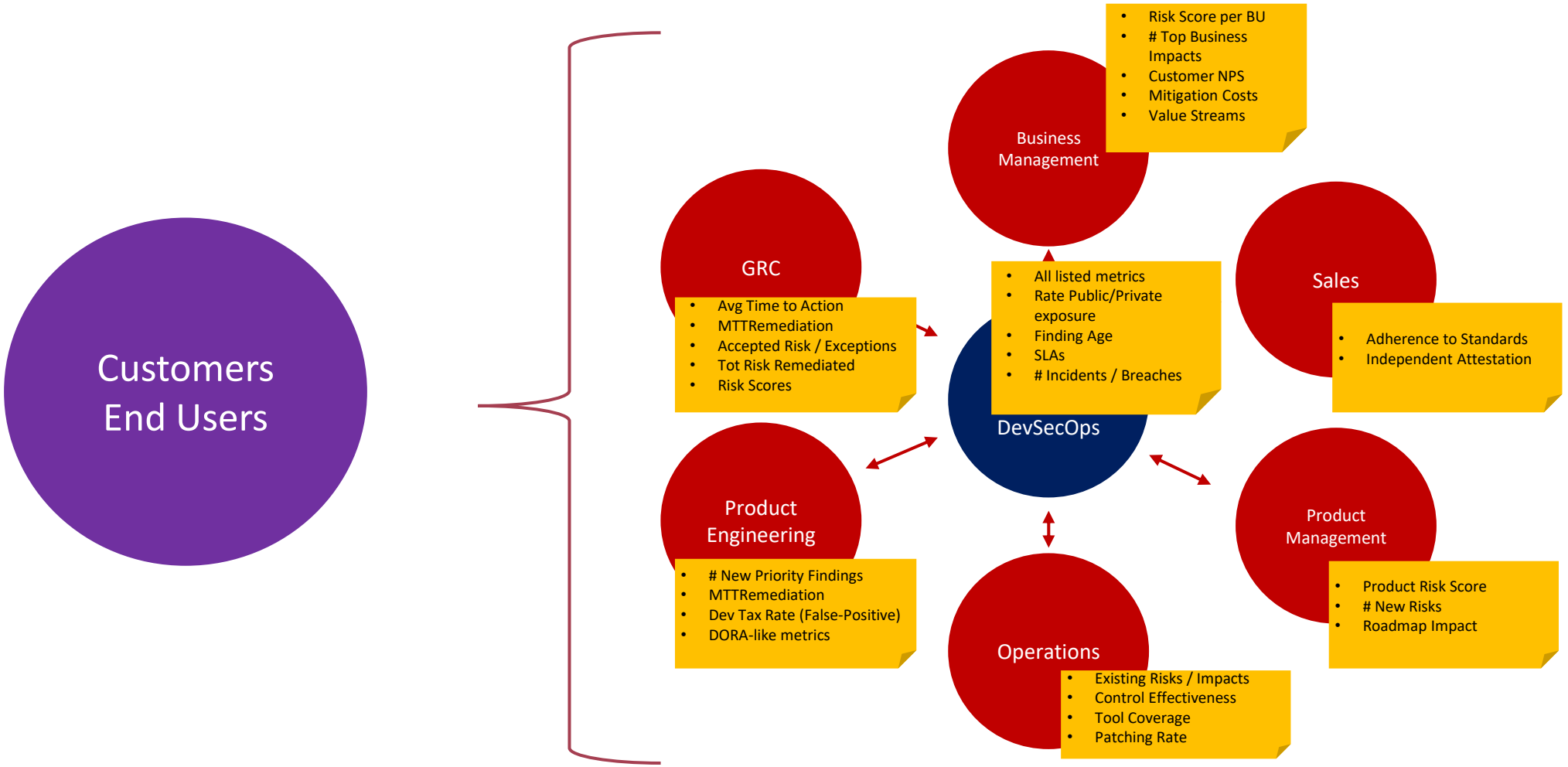
The big questions are:

How to make cyber security concerns more attractive to business actors?

How to transform the business actors in security advocates?

Help me (them), help you!

THE USUAL SUSPECTS



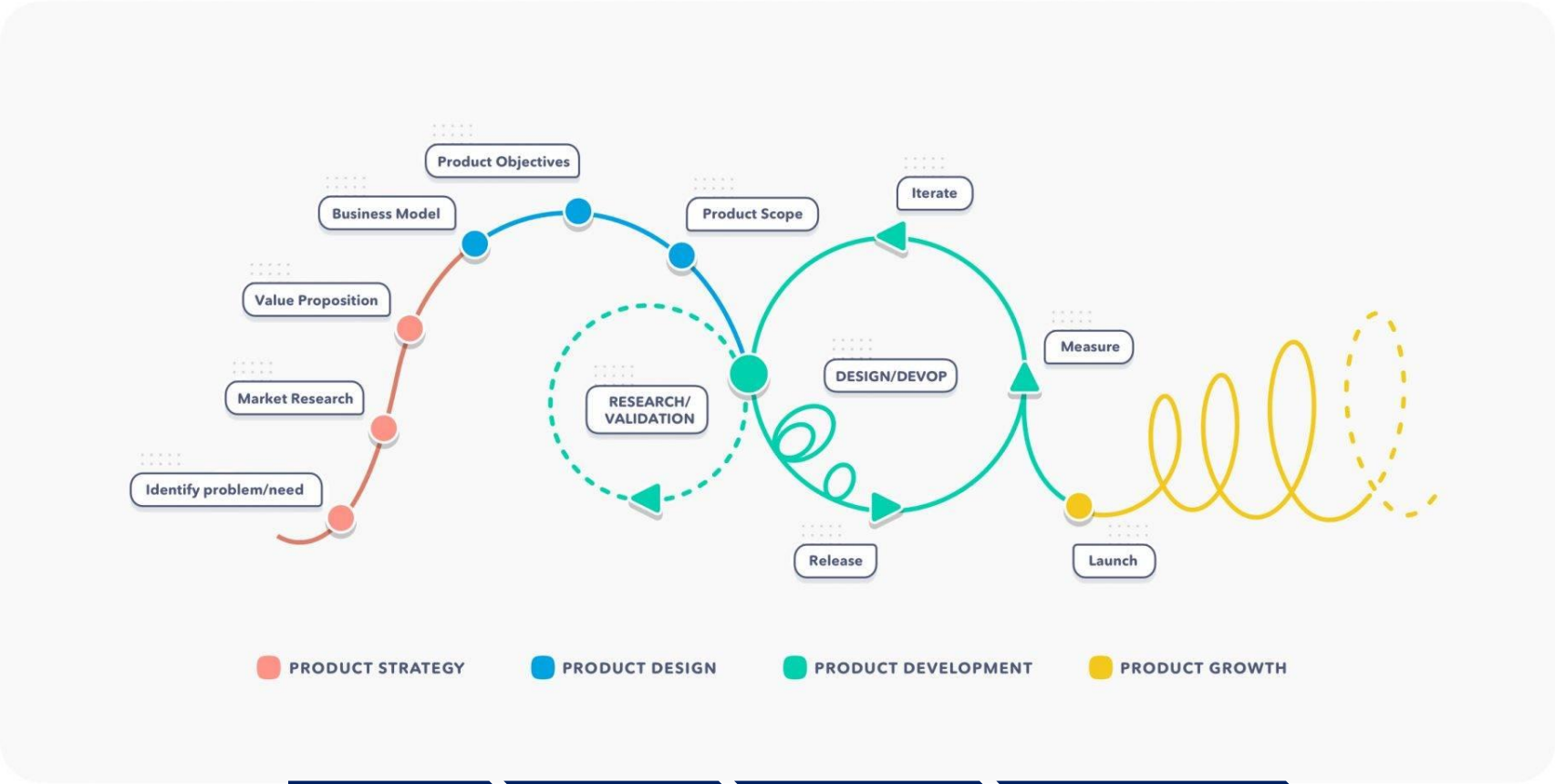
HOW TO ENGAGE BUSINESS

As part of our work, we need to connect with our internal customers and speak their language – it means understand what they value and how we can deliver information (metrics / artifacts) that helps their goals.

Also, in many organizations, all the other parts of the business speak another single language: *the risk language*.

- Understand their goals and issues (first listen, speak after)
- Propose risk metrics / security information they can use to achieve their goals (not only yours)
- Report based on the organization existing risk frameworks (risk team is your friend)
- Educate them on reading your reports (the obvious is not always obvious)
- Re-engage and review the metrics …

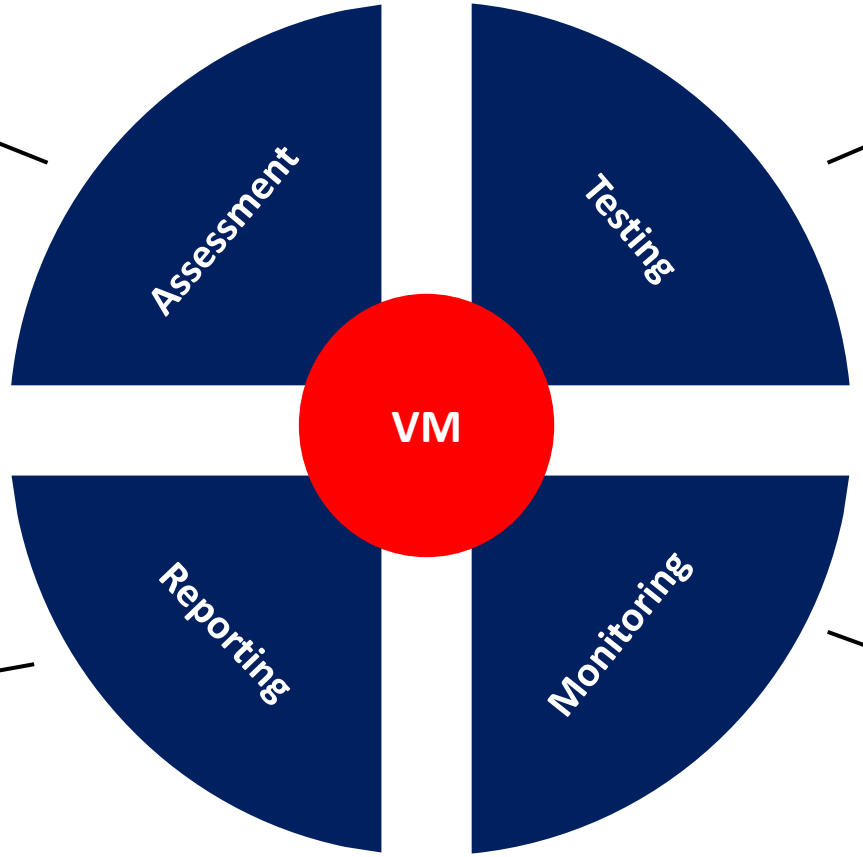
DIGITAL PRODUCT LIFECYCLE



Ideation | Design | Development | Operations

VULNERABILITY MANAGEMENT (FINDINGS)

- Audits
- Maturity Checks
- Control Effectiveness
- Self-Assessment
- Security Requirements
- Threat Modelling



- Security Testings
- Pentesting
- Bug-Bounties
- Scans (ongoing / ad-hoc)
- Manual testing (any sort)

- User reports
- Customer reports
- Researchers reports

- Runtime sensors
- Continuous Sec Monitoring
- In-line security controls
- XDR-like sensors
- Threat Intelligence
- Attack Surface Management

USUAL FINDING DILEMMA

Product/Application Perspective

```
IF (FINDING.environment != PRODUCTION) {
    It is not PRIORITY
    FINDING.Class = "Development Bug"
    IF (FINDING.RiskScore < RISK APPETITE) {
       FINDING.Status = "Risk Accepted"
    } ELSE {
       Call to fix before release
    }
} ELSE {
    FINDING.Class = "Production Bug"
    IF (FINDING.RiskScore >= HIGH) {
         FINDING.Priority = "Severity 1"
         Call for action to fix ASAP / VM Sch
    } ELSE IF (FINDING.RiskScore = MEDIUM) {
         FINDING.Priority = "Severity 2"
         Monitor risk score
         Plan for next release
    } ELSE {
         FINDING.Priority = "Severity 3"
         Plan for further delivery in the roadmap
    }
}
```

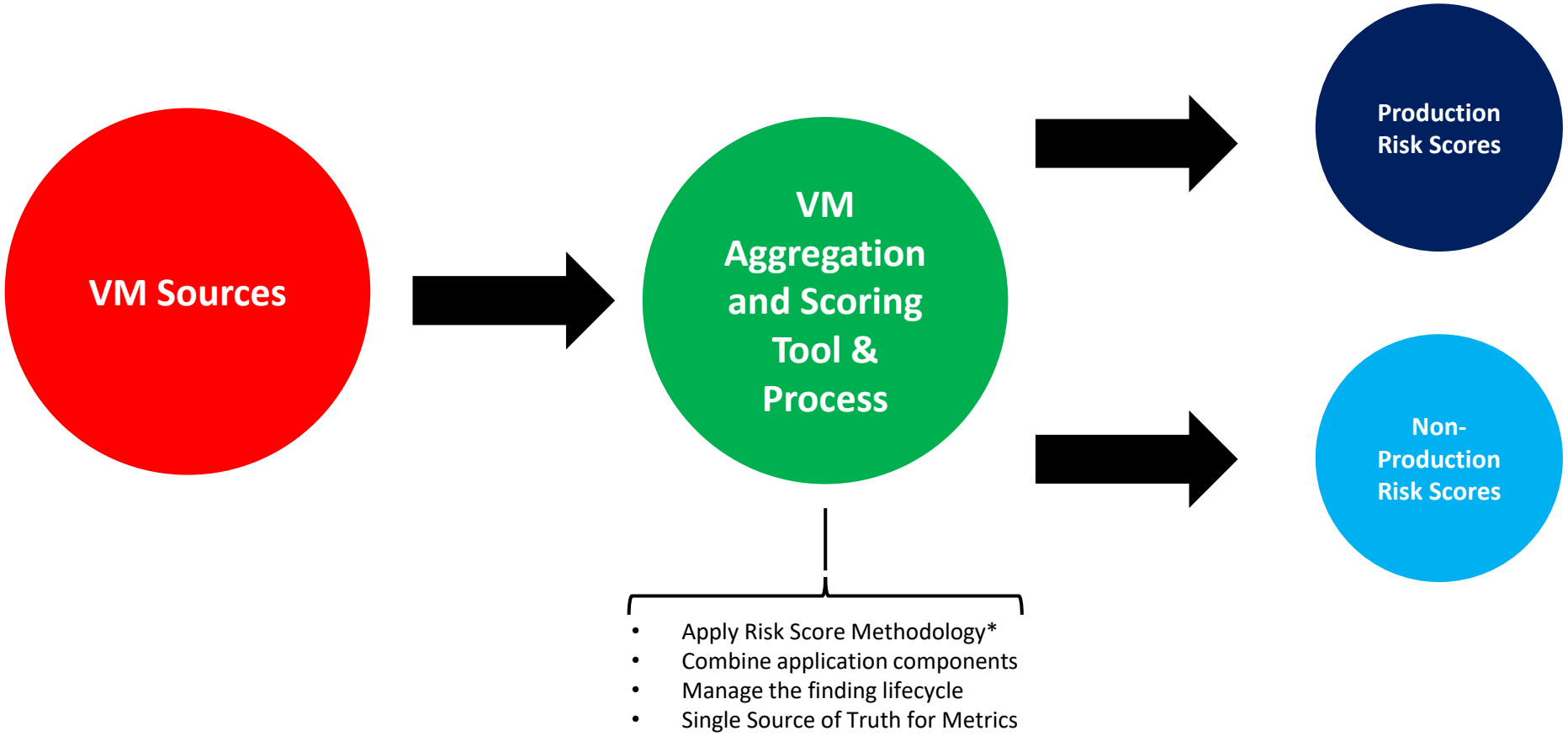
Security/Ops/IT Perspective

```
IF (FINDING.Status = OPEN) {
   Teams need to fix according to VM schedule
}
```

Security/Ops/IT teams need to provide consultancy and risk-based views to Product/Applications teams.

If it's in the risk appetite, it is OK to keep monitoring or accept risks.

VM ADDING VALUE TO BUSINESS



TAKEAWAYS

Business Engagement

- MUST be a relational engagement
- Help them, Help you!
- Always EDUCATE them in cyber risks
- GIVE them metrics / documentation that make sense for their goals

Vulnerability Management

- BE a consultant and solution provider to business
- AGGREGATE findings per application/product
- Build a RISK SCORE methodology (or grab from risk teams one)
- MANAGE the findings from a CENTRAL solution
- Split reports based on what is PRIORITY

THANK YOU

Estevan Chaves

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