2025 CVE/FIRST VulnCon

Raleigh (NC), USA
April 7-10

Towards a Minimum Viable Vulnerability Enumeration (MVVE)

Jay Jacobs
jay@empiricalsecurity.com

Art Manion
zmanion@protonmail.com

Hey Jay wait up...

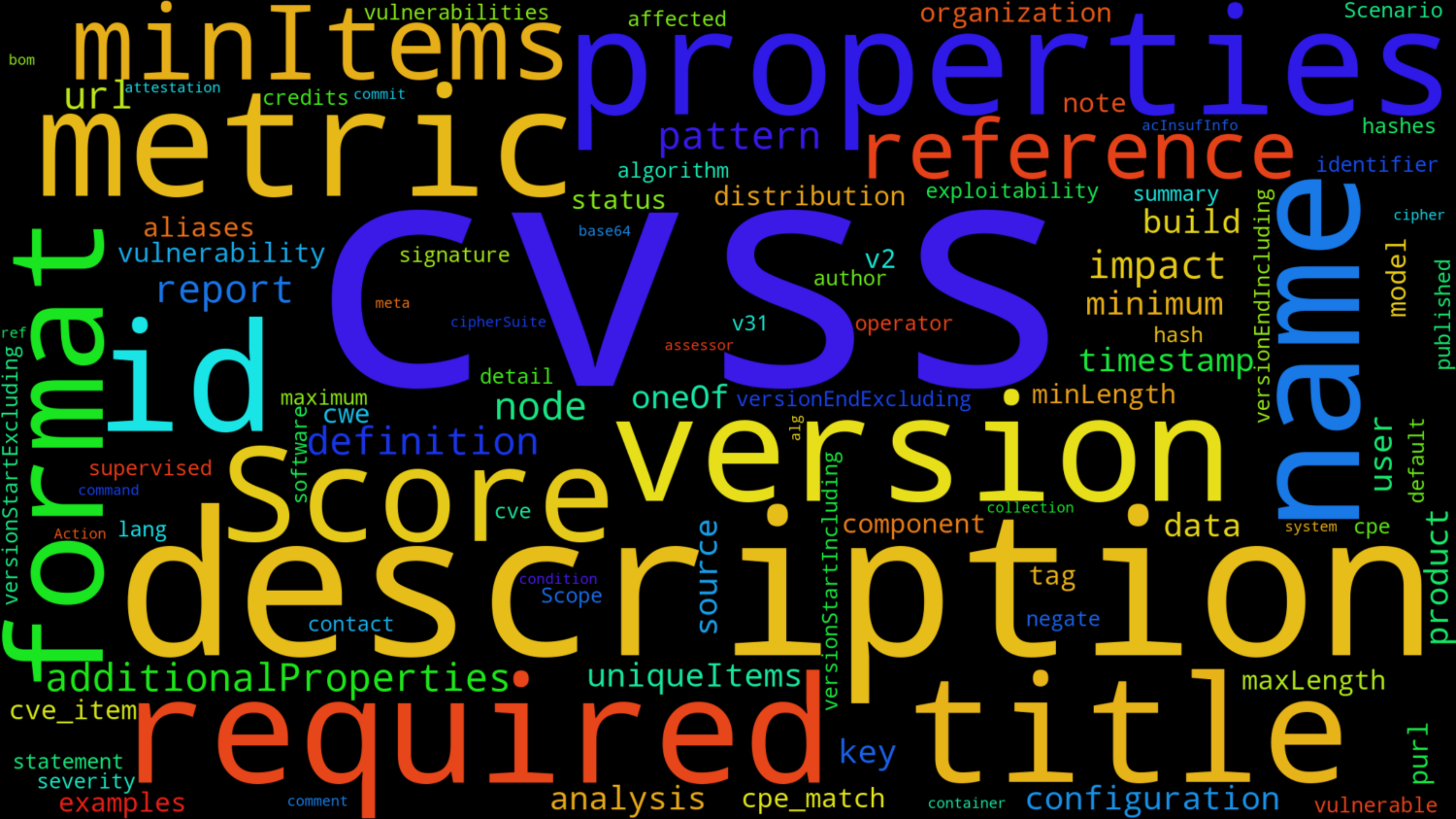
What information do we need in a vulnerability record to uniquely identify a vulnerability?

No really, the absolute minimum?

Necessary, but perhaps not sufficient for vulnerability management

A note on vulnerability management:

- Risk management, scoped to vulnerabilities
- “Zero vulnerabilities” is an illusion


CVSS
description
properties
metric
version
required
title
name
Score
format
id
minItems
reference
pattern
additionalProperties
uniqueItems
definition
node
report
vulnerability
impact
minimum
timestamp
minLength
maxLength
configuration
analysis
cpe_match
cve_item
component
data
build
distribution
status
oneOf
source
key
versionEndIncluding
versionStartIncluding
versionStartExcluding
versionEndExcluding
aliases
organization
note
url
vulnerabilities
affected
credits
algorithm
exploitability
summary
identifier
hashes
Scenario
attestation
commit
bom
acInsufInfo
cipher
signature
base64
v2
author
meta
cipherSuite
v31
operator
assessor
detail
maximum
cwe
software
alg
hash
model
published
user
default
product
supervised
command
cve
lang
Action
collection
system
cpe
condition
Scope
tag
negate
contact
statement
severity
examples
comment
container
purl
vulnerable
ref

Towards a Common Enumeration of Vulnerabilities

David E. Mann, Steven M. Christey

The MITRE Corporation

202 Burlington Rd., Bedford MA 01730

January 8, 1999

Abstract

In this paper, we discuss the use of multiple vulnerability databases in our operational enterprise security environment and we consider some of the roadblocks we see to achieving interoperability between them. We introduce the concept of a Common Vulnerability Enumeration (CVE) as a mechanism that we believe will help to foster easier data sharing. We consider some historical examples of the development of taxonomies in other fields and relate them to current efforts in representing and sharing vulnerability information. We present a simplified representation of a "vulnerability" and discuss how we anticipate using it to mitigate the problem of interoperability. We also describe some of the practical issues that may be involved in the development and use of a CVE.

MVVE defined

- Must contain a unique and public identifier for each record.
- Must contain enough information to initiate the vulnerability management process for the product consumer.
- Must contain enough information to disambiguate each vulnerability from other vulnerabilities.
- Removal of any one information element from the record negates the value.
- All information is represented once and only once.

Framing

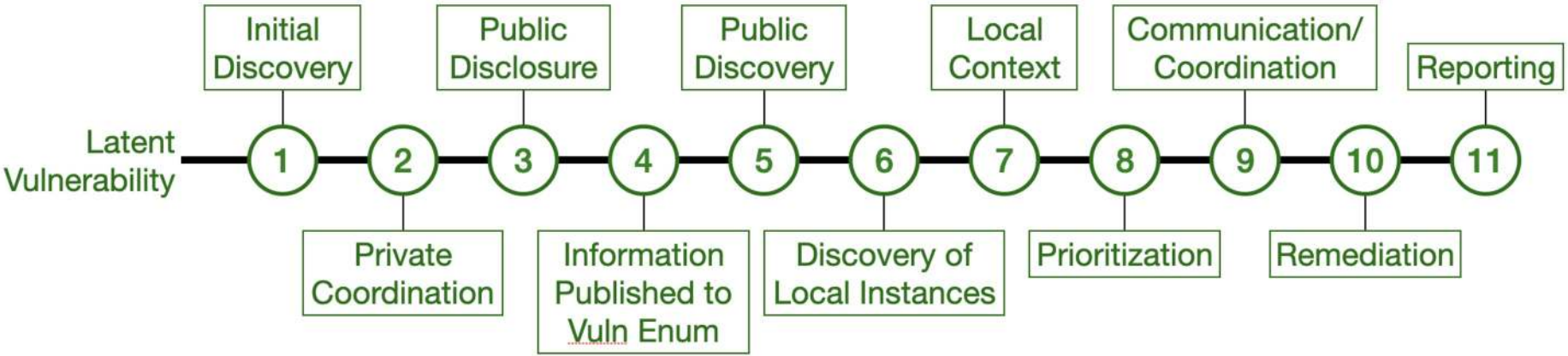
Vulnerability management

Information elements

Phases

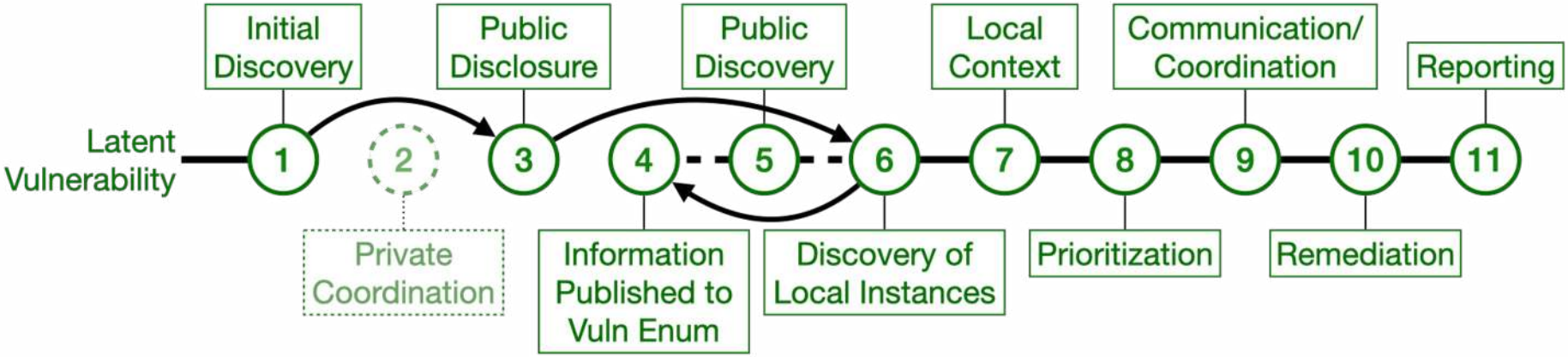
Stakeholder roles

Phases



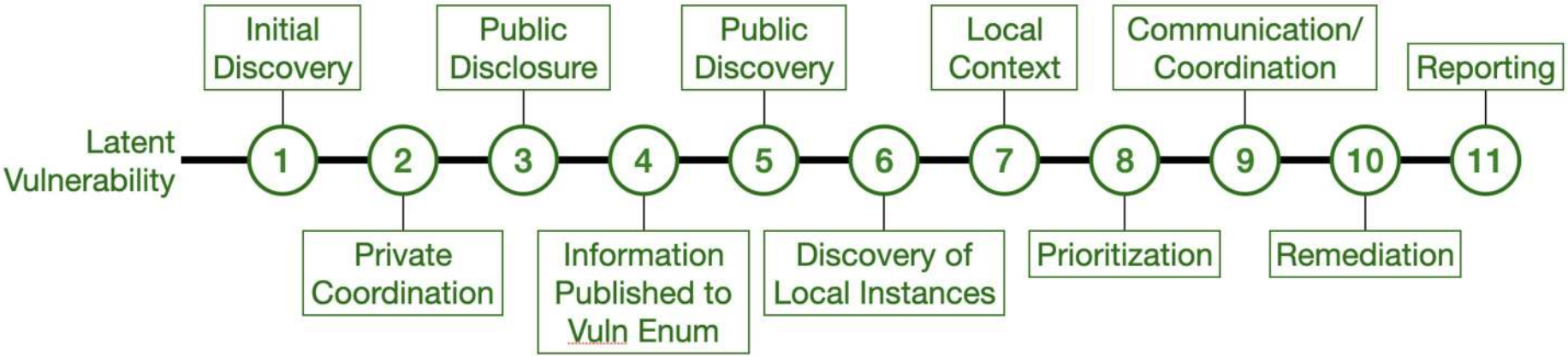
Risk-minimizing, defensive CVD and idealized vulnerability management

Phases

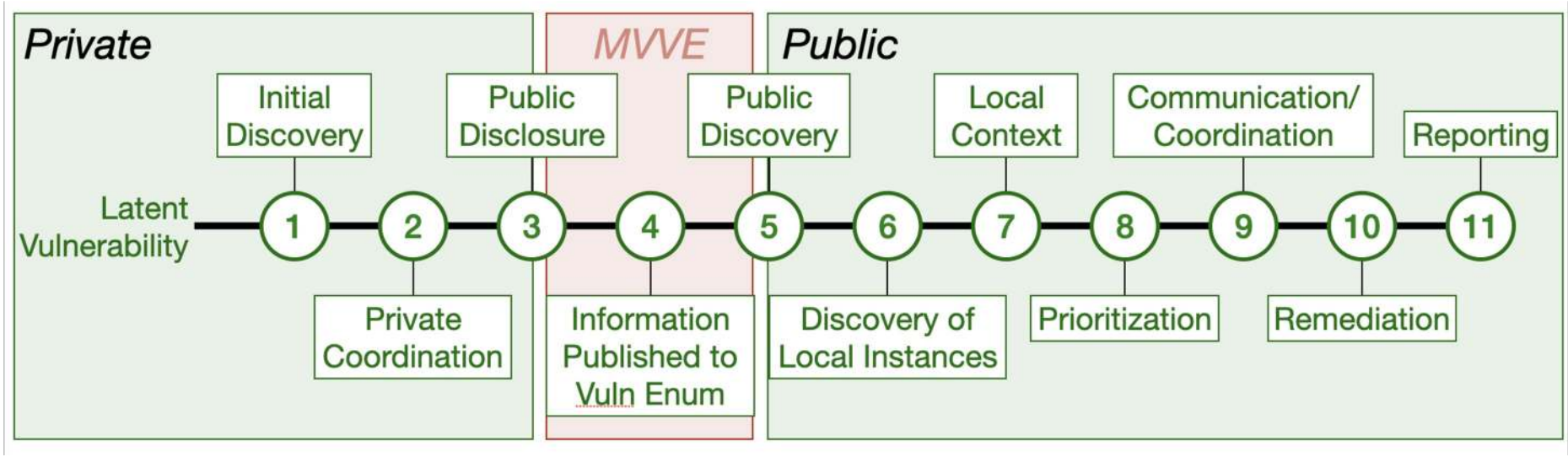


Or, EITW

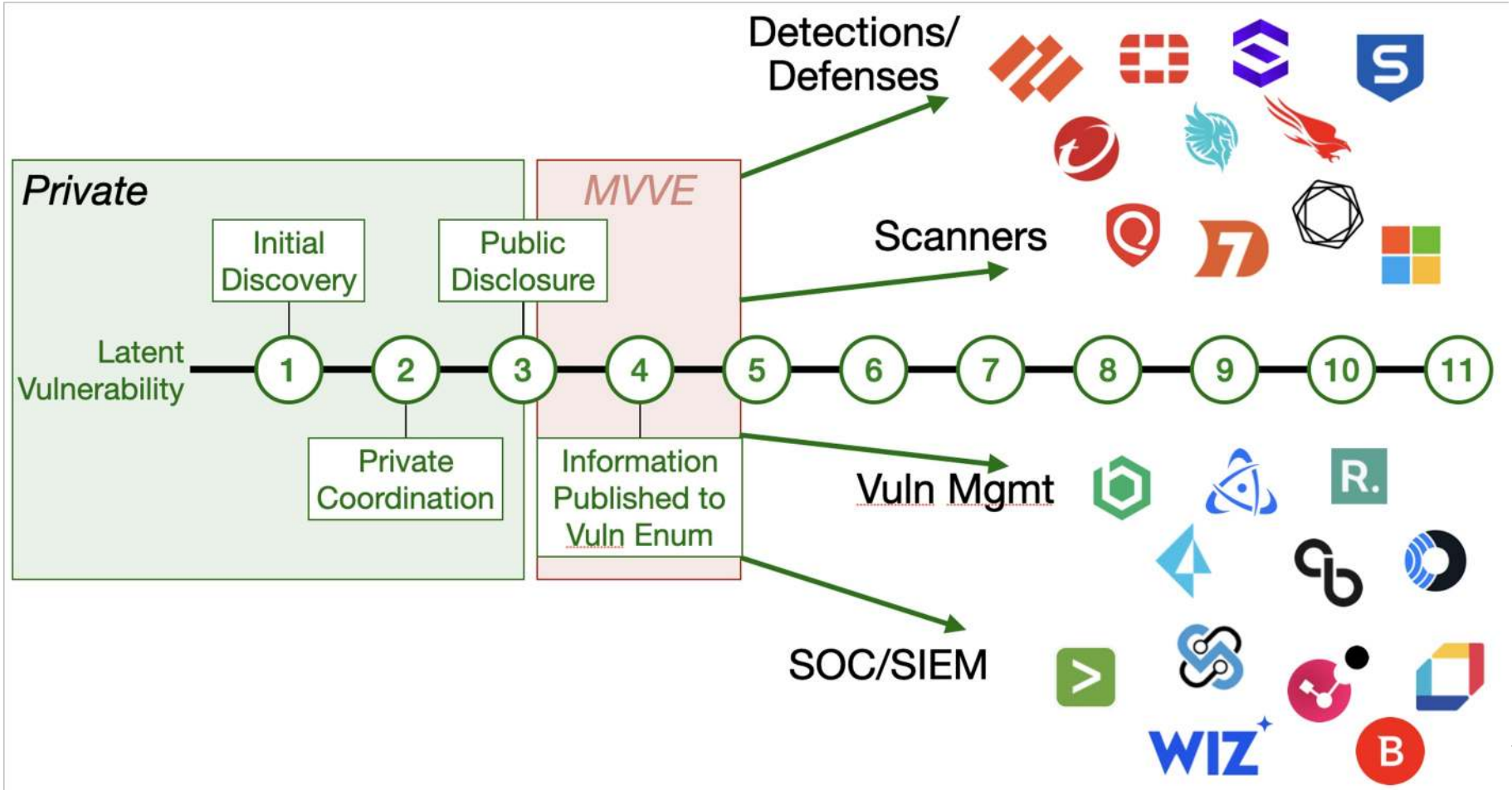
Phases


Latent Vulnerability
1
Initial Discovery
2
Private Coordination
3
Public Disclosure
4
Information Published to Vuln Enum
5
Public Discovery
6
Discovery of Local Instances
7
Local Context
8
Prioritization
9
Communication/ Coordination
10
Remediation
11
Reporting

Phases


Private
MVVE
Public
Initial Discovery
Public Disclosure
Public Discovery
Local Context
Communication/ Coordination
Reporting
Latent Vulnerability
1
2
3
4
5
6
7
8
9
10
11
Private Coordination
Information Published to Vuln Enum
Discovery of Local Instances
Prioritization
Remediation

Vulnerability Management Providers



Stakeholder roles

Producer, Product Producer - the individual or organization that created or maintains the Product

Consumer, Product Consumer - the individual or organization that is primarily responsible for deploying a patch and/or other remediation actions.

Vulnerability Manager - A sub-role, traditionally existing within the product consumers, that prioritizes/executes the remediation/treatment of known vulnerabilities.

Vulnerability Management Provider - provides a capability, service or other supporting role.

Information elements

Vulnerability identifier

Product identifier

Remediation

- Update, workaround, mitigation, detection

Attributes, characteristics of a vulnerability (e.g., CVSS vectors)

Classification (e.g., CWE)

References

Zeitgeist (“*spirit of the times*”)

Requires/Provides (attack graph)

MVVE: Minimum Viable Vulnerability Enumeration

Vulnerability identifier

Product identifier

Notably missing from this list: CVSS, SSVC, EPSS, CWE, CAPEC, zeitgeist…

AVE: Adequate Vulnerability Enumeration

Vulnerability identifier (MVVE)

Product identifier (MVVE)

Remediation (AVE)

- Update, workaround, mitigation, detection

References

Attributes, characteristics of a vulnerability (e.g., CVSS vectors)

Classification (e.g., CWE)

Zeitgeist (“*spirit of the times*”)

Requires/Provides (attack graph)

Enumeration or Exposure?

Are we…

- Enumerating technical cybersecurity vulnerabilities?
- Cataloging technical cybersecurity “exposures?”

Depending on the answer, does MVVE change?

- Still need identifiers
- What is needed for “exposure” management?

A look forward

Minimum Viable Vulnerability Enumeration

- Paper coming “real soon now”
  - In depth analysis of vulnerability phases/tasks
  - High level introduction of roles
  - Discussion of Information Elements and their applicability to roles and phases

https://tinyurl.com/3tdux5z2