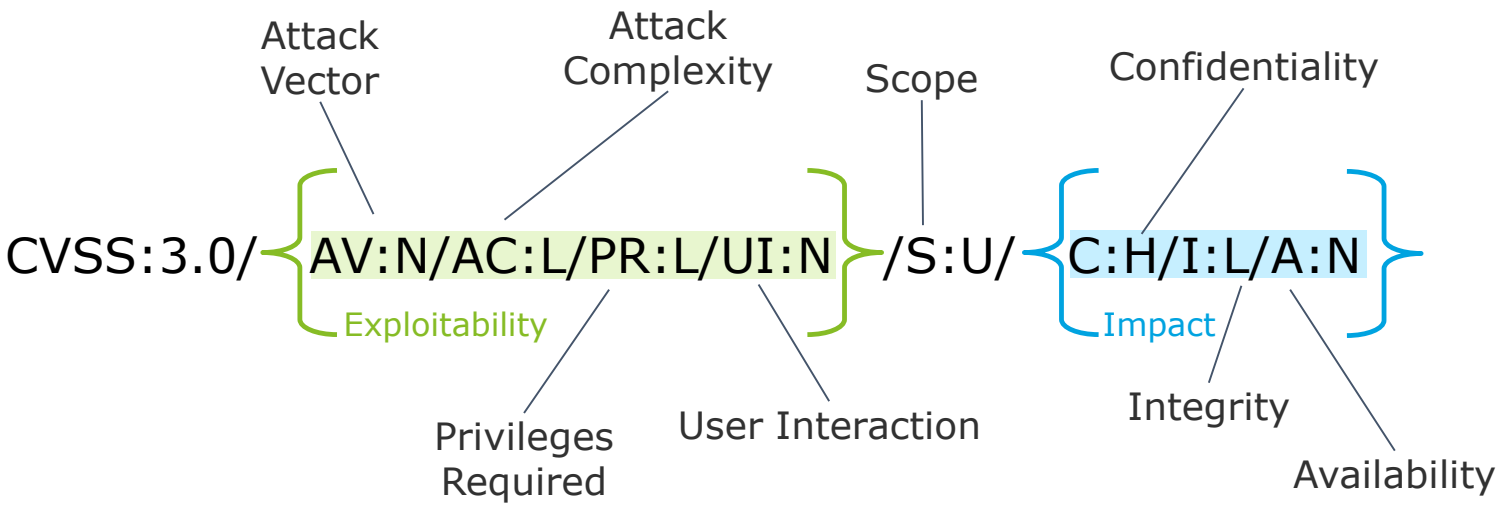
Common Vulnerability Scoring System v3.0

Introduction

Introduction

What is CVSS and why do we have the session?

Introduction
Metrics



The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component.

On the other hand, the Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.

Attack Vector	Network, Adjacent, Local, Physical
Attack Complexity	Low, High
Privileges Required	None, Low, High
User Interaction	None, Required

Scope	Changed, Unchanged

Confidentiality	None, Low, High
Integrity	None, Low, High
Availability	None, Low, High

Empfehlung	0.0
Niedrig	0.1-3.9
Mittel	4.0-6.9
Hoch	7.0-8.9
Kritisch	9.0-10.0

Metrics

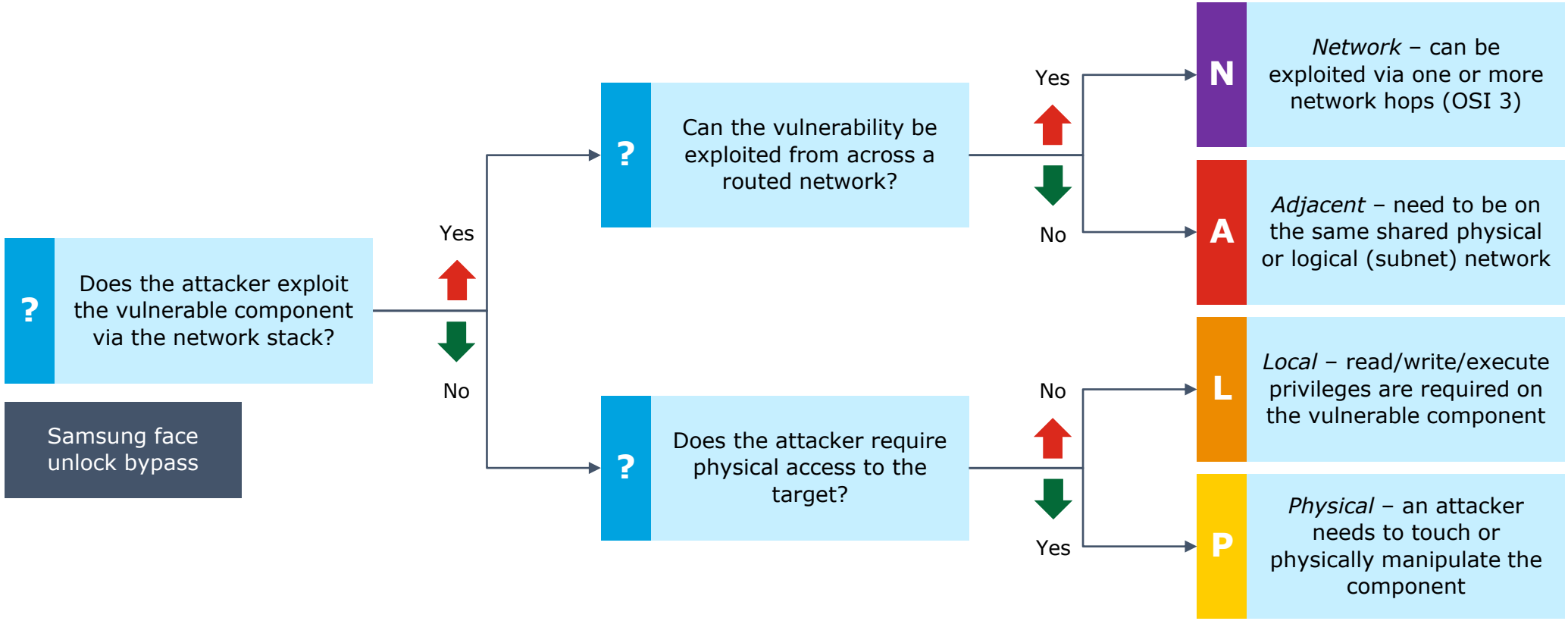
Attack Vector

Issues with the attack vector

- Do I need physical access to the system or is local access sufficient?
- What is the difference between Adjacent and Network?

Attack Vector

Some example to get a better understanding



Attack Complexity

What does it mean, and what does it not mean

High Complex XSS

%3Cscript%3Edocument.body.innerHTML
3Ca%20onmouseover%0B=location=%27\x
61\x76\x61\x53\x43\x52\x49\x50\x54\x26\x63
x6F\x6C\x6F\x6E\x3B\x63\x6F\x6E\x66\x69\x72
\x6D\x26\x6C\x70\x61\x72\x3B\x64\x6F\x63\x7
5\x6D\x65\x6E\x74\x2E\x63\x6F\x6F\x6B\x69\x
65\x26\x72\x70\x61\x72\x3B%27%3E%3Cinput
%20name=attributes%3E%22;%3C/script%3E&d
isable_xss_defense=on&disable_browser_xss_d
ense=on

Low Complex XSS

<script>alert("XSS")</script>

Attack Complexity

What does it mean, and what does it not mean

High Complexity

- The attacker does not have full control over all requirements to exploit the vulnerability
- The victim need to have some specific settings set on the target system
- Man in the middle attack is required in order to execute attacks

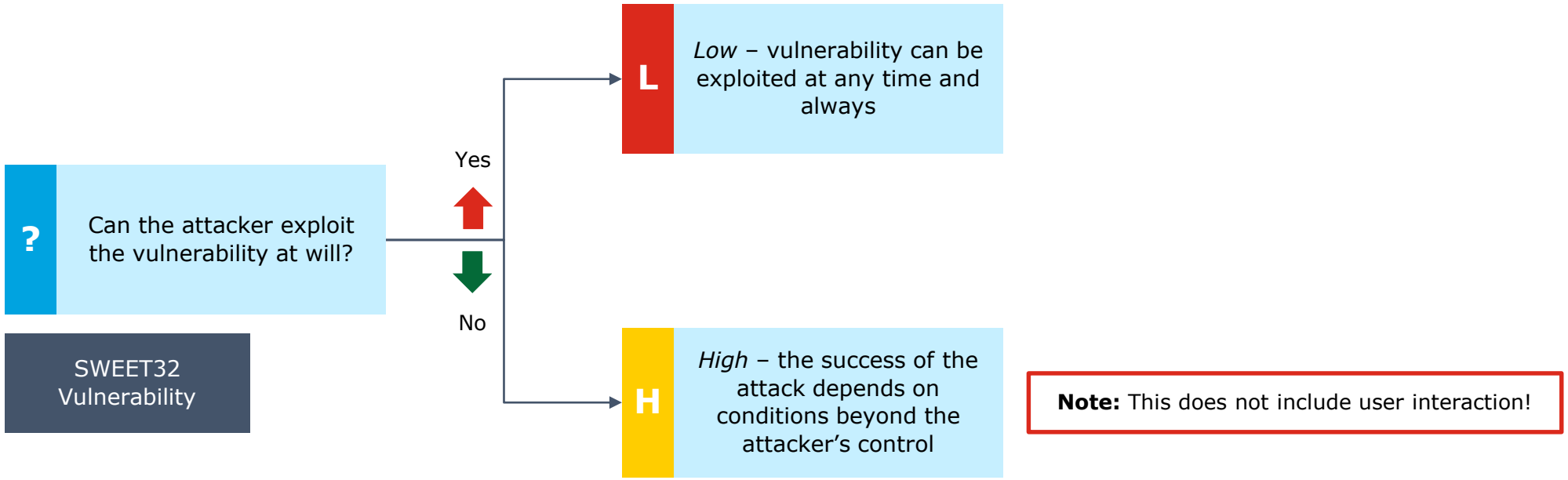
→ The attacker does not have full control over the success of the exploit. (User Interaction is not part of the metric)

Low Complexity

- The attacker can repeat the attacker reliable and as often as he wants

Attack Complexity

How complex is it to fill the attack



Note: This does not include user interaction!

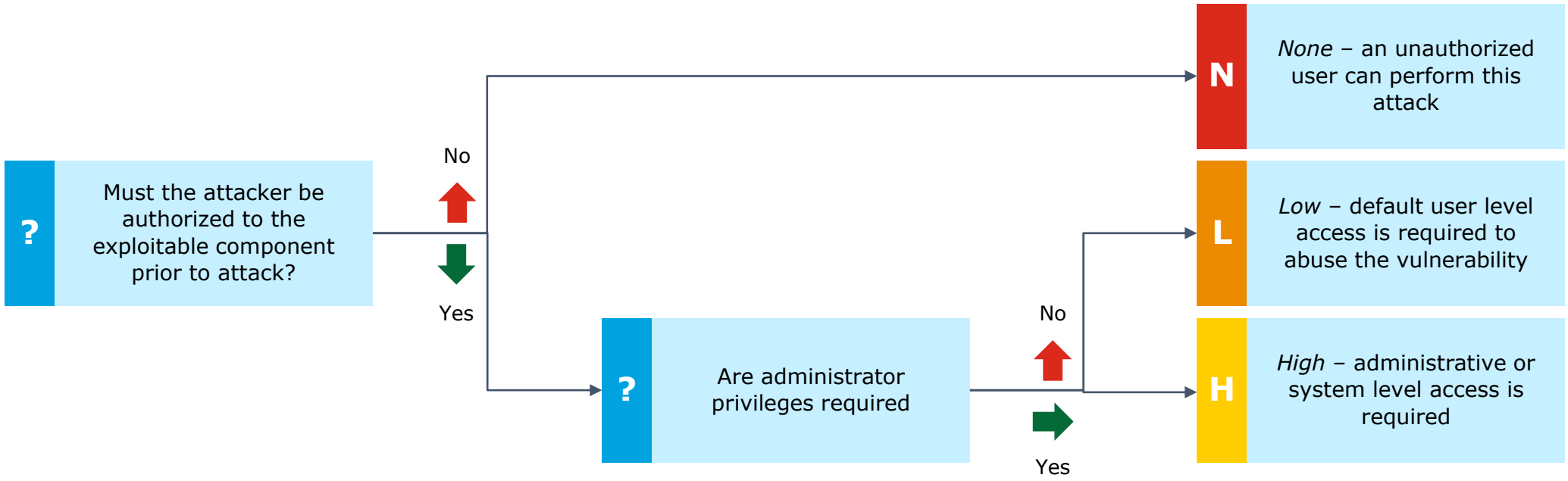
Privileges Required

What is meant by privileges

- Three different level exist (High/Low/None)
- This metric describes the level of privilege an attacker needs **before** conducting the attack on the vulnerable system or application

Privileges Required

How to determine the required privilege level



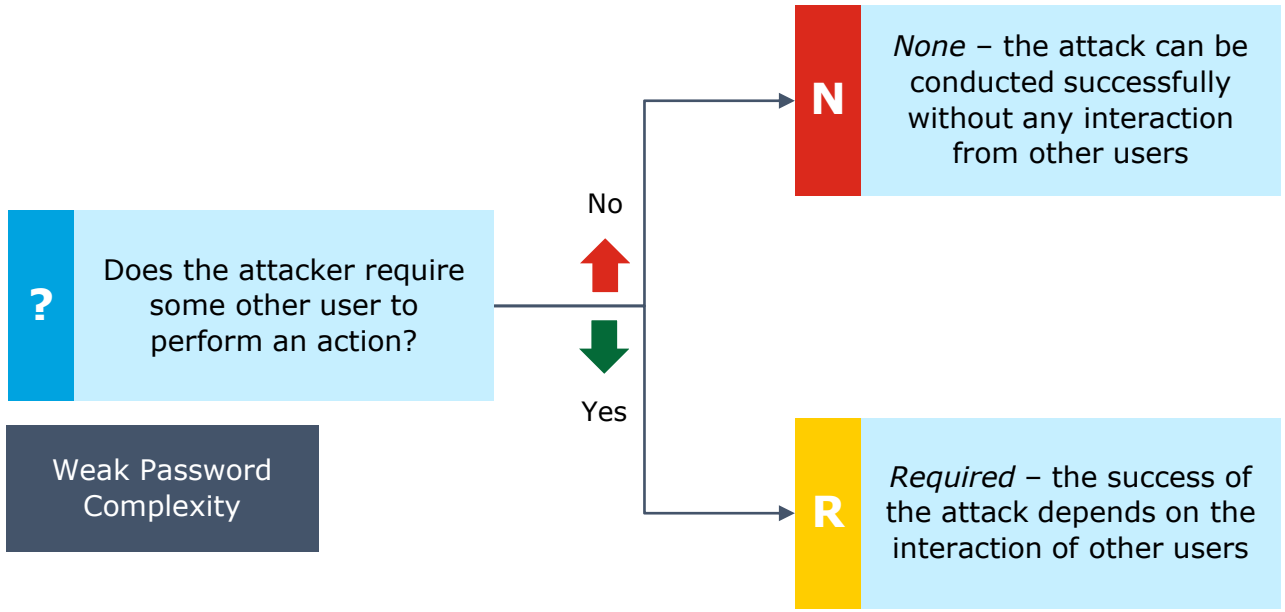
User Interaction

Do we need any user to interact in order to exploit the vulnerability

- no **active** interaction of any other user than the attacker is required
    - ➢ browsing the web page is no interaction, while clicking on a specially crafted link is an interaction
- the attack can be launched at the attackers will at any time

User Interaction

When do we need user interaction



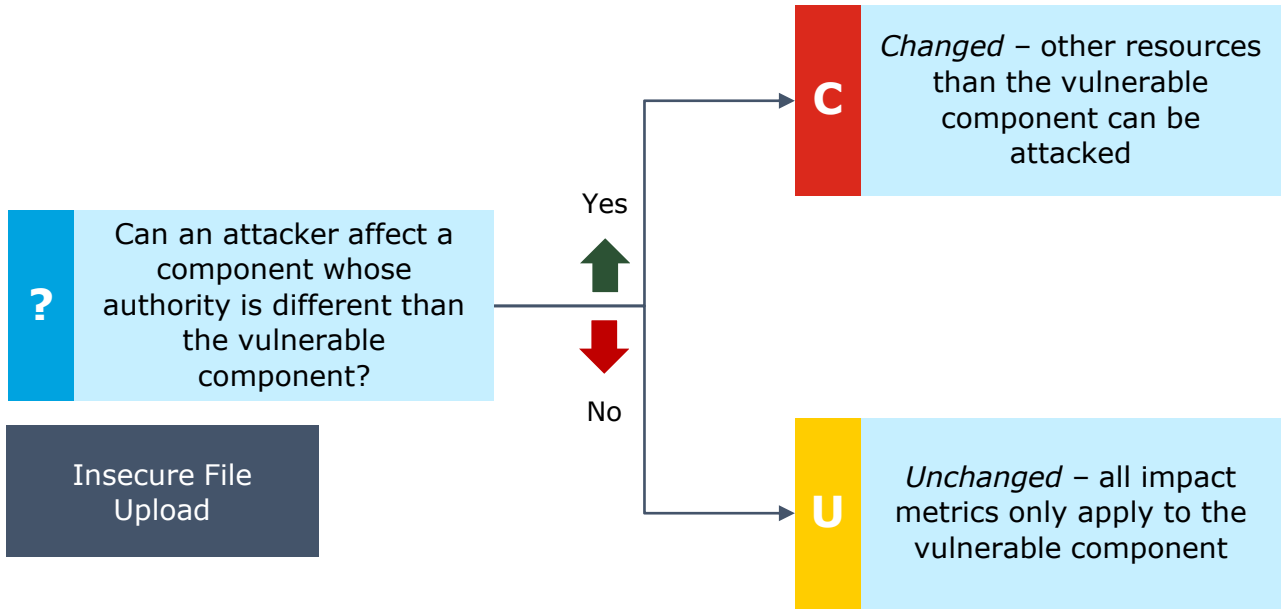
Scope

When does the scope change

- The scope changes, whenever another system is affected than the vulnerable one
- If the infrastructure behind the web application is affected – the scope is changed, since different departments are responsible
- Always look for the *vulnerable* and *impacted* component
- The impact metrics should always apply to the most impacted system

Scope

How do we determine if the scope is changed or not



Impact Metrics

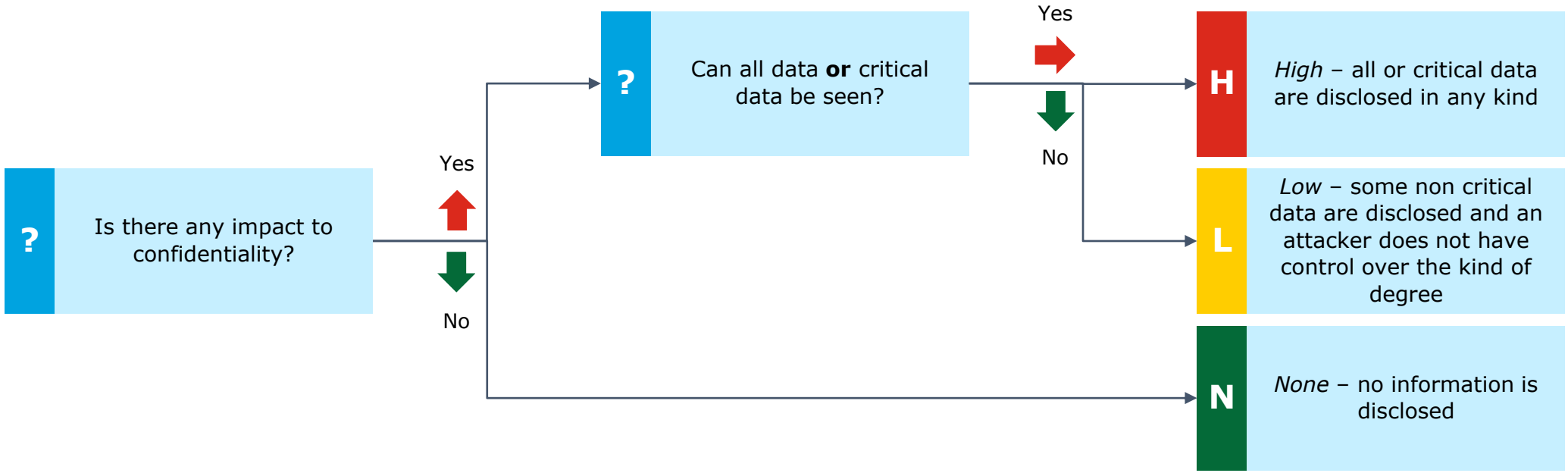
Does it make an impact that matters

 Confidentiality	**High:** All or critical data be seen. **Low:** Just some (uncritical) data can be seen and the attacker does not have control over the kind of degree. **None:** No data can be retrieved due to this vulnerability.
 Integrity	**High:** All or critical data be altered. **Low:** Just some (uncritical) data can be altered and the attacker does not have control over the kind of degree. **None:** No data sensitive can be modified due to this vulnerability.
 Availability	**High:** The service or critical resources can be shut down completely. **Low:** The service can be interrupted or single resources can be shut down. **None:** The availability can not be affected.

Note: Altering data that leads to missing availability (e.g. changing password) will be handled as integrity issue, not as availability issue!

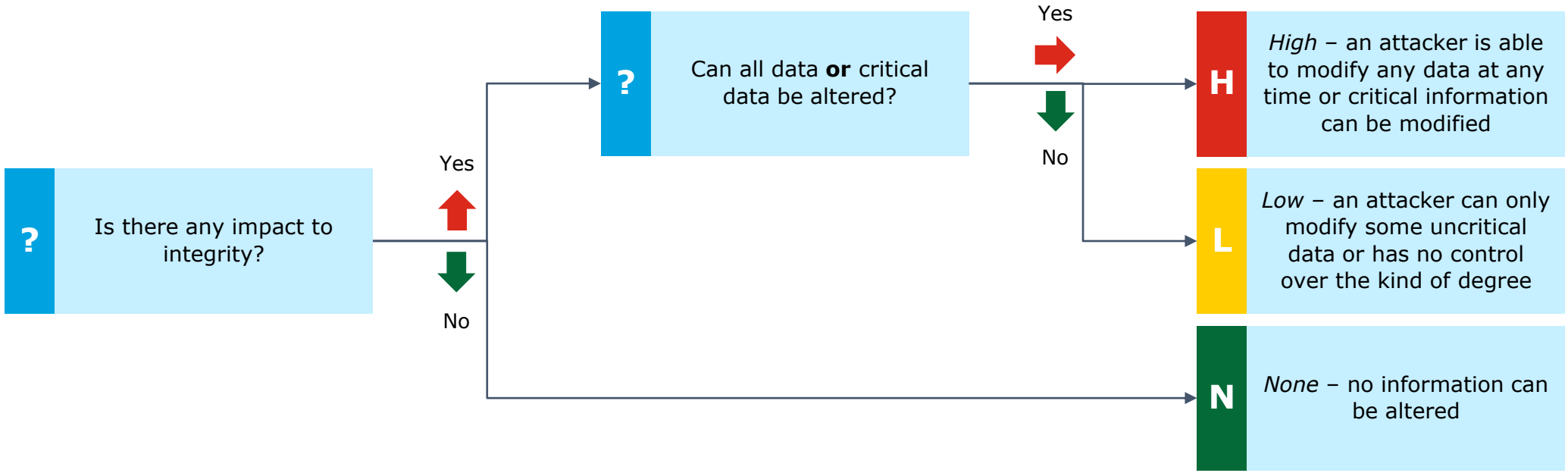
Confidentiality Impact

How to determine the confidentiality impact



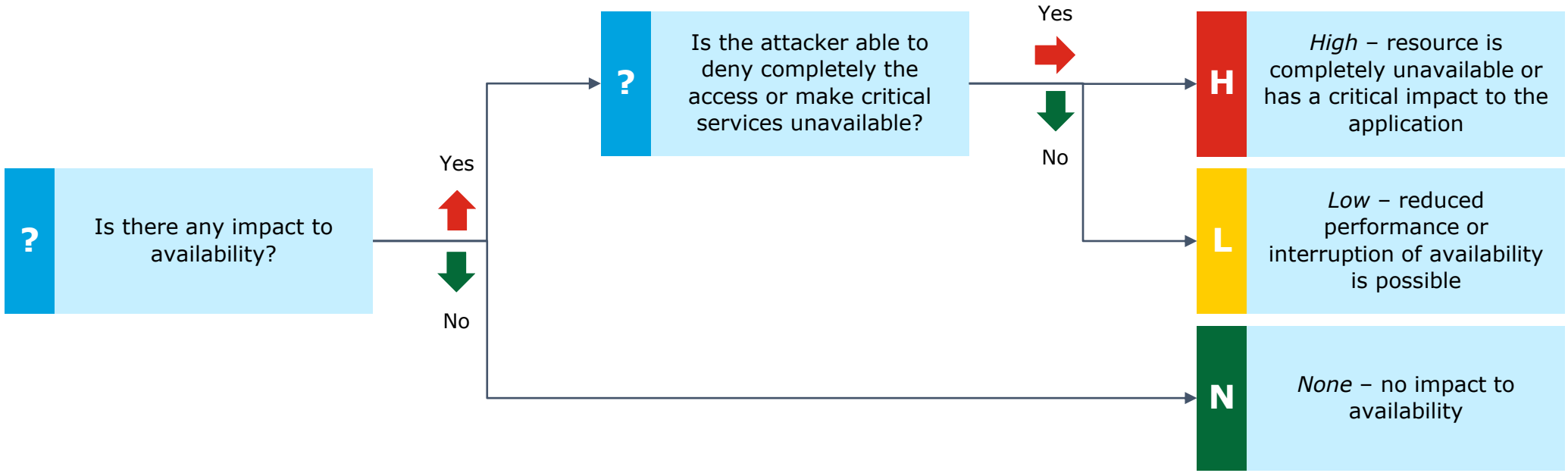
Integrity Impact

How to determine the integrity impact



Availability Impact

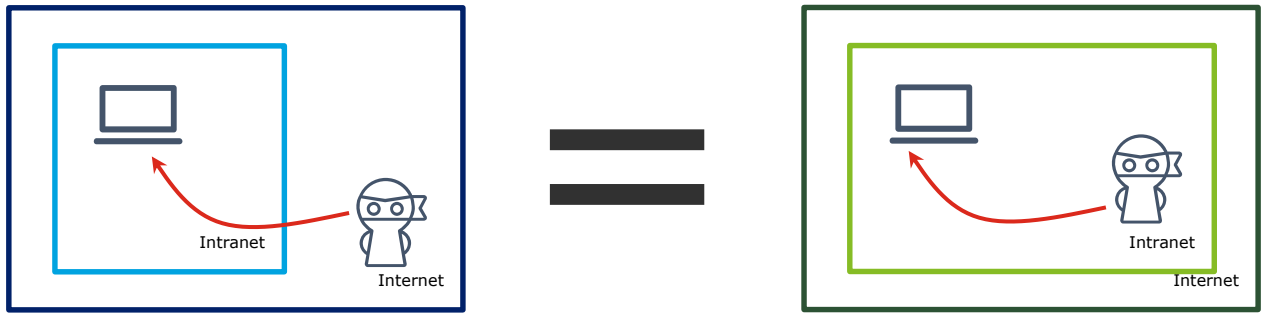
How to determine the availability impact



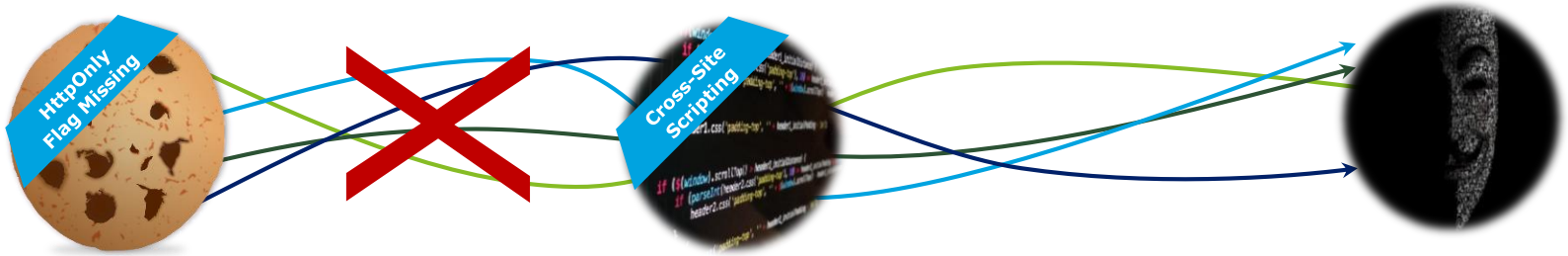
Common Mistakes

Scoring Done Right
Common issues

- There is no distinction between intranet and internet facing systems / applications (already in the list of improvements for CVSS v4.0)



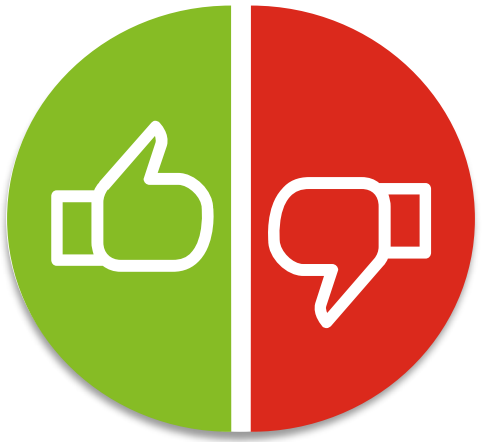
- The dependency between two findings is not reflected within the score



Scoring Done Right
Common mistakes

DO'S

- Apply the impact metrics always to the highest impacted system!
- Put the attack vector for MiTM-attacks as network!
- Apply the rating without looking at the overall severity and score to get an objective result!
- Get a clear understanding of the attack start point and direct impact before applying the vector!
- Have a close look at the application, environment and vulnerability!



DONT'S

- Do not handle limited availability caused by data changes as availability issue!
- Do not rate the technical complexity of an attack!
- Do not rate the preconditions of an attack as impact!
- Do not use confidentiality as all-purpose answer