

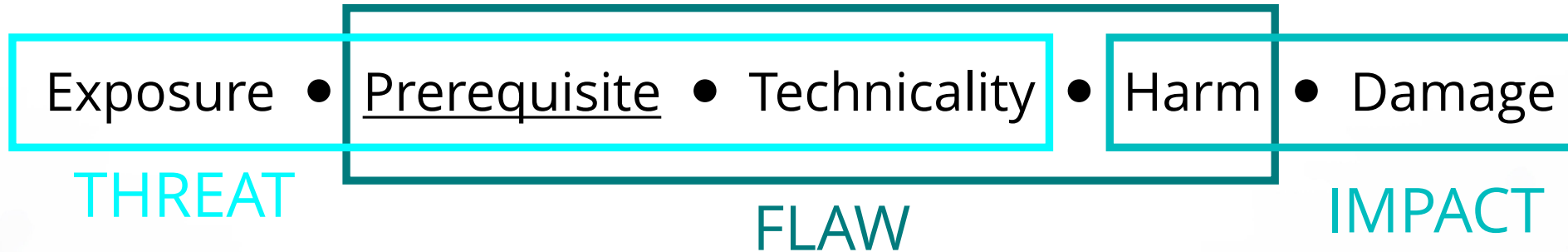
VULNERABILITY SCORING



Exposure *What position the hacker needs to have*

- Remote *When LSDi5Fun hacks you from the TORdjikistan*
- Outside *When Steve (High School student) find your Wifi key to not pay Internet access*
- Inside *You know the malware in your cracked MS Office ? That's inside*
- Physical *When your sales's PC is left behind in the train*

VULNERABILITY SCORING



Prerequisite *What capabilities the hacker needs to have*

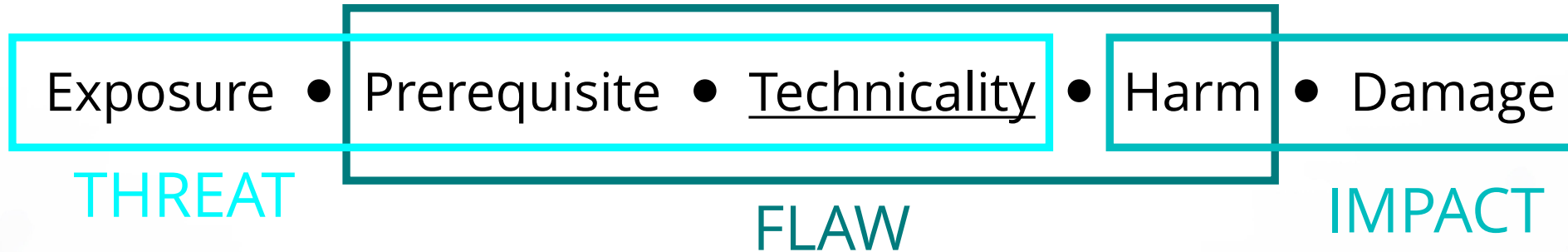
Unauthenticated *A polite word for "open bar"*

Deception *When you click the link in the "Is that you on this picture !!" email"*

Interception *Every router between you and your server, including NSA-US routers*

Authenticated *When the hacker found that Billy uses the password "Billy01!"*

VULNERABILITY SCORING



Technicality *What skills the hacker needs to have*

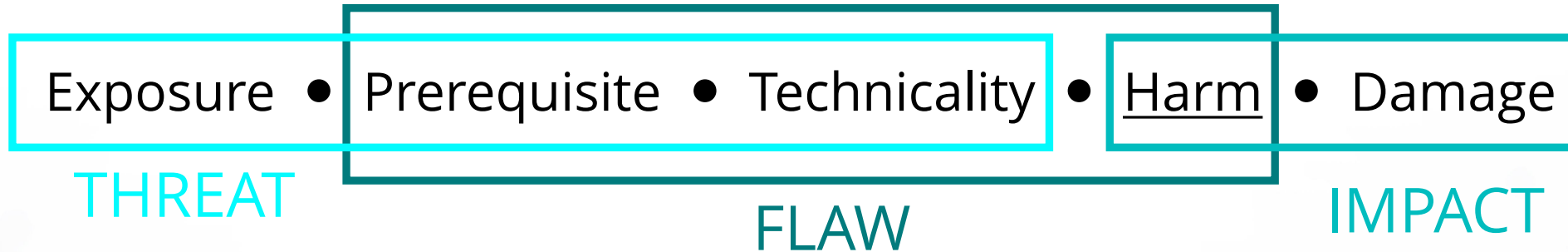
Direct *When the password is password*

Automated *Or fully documented. Actually, all kinds of "available in Kali" cases*

Complex *When you have to read specs and open vim*

Theoretical *When some paper says that SSL is broken*

VULNERABILITY SCORING



Harm *What the hacker can do*

Denial of service *The good news for your electricity bill*

Information disclosure *It's time to read about the GDPR*

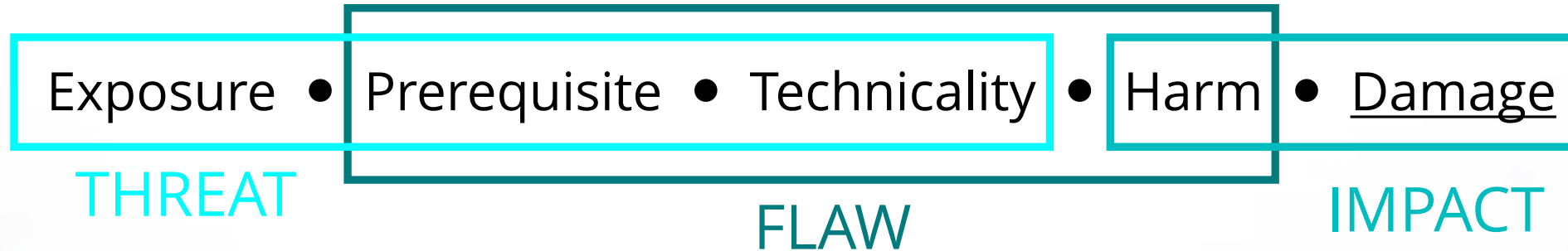
Tampering *When the medication dosage grows from 0,01g to 1337g (non repudiation can be broken)*

Code execution *A sweet way to say "this is not your server anymore"*

Privilege escalation *Authorization bypass, impersonation, spoofing, (not a great news too for non repudiation)*

Scope extension *New playgrounds for the hacker*

VULNERABILITY SCORING



Damage *What kinds of prejudice for the structure*

Reputation *But no one will never know if you get hacked no ?*

Legal *Time for shawshank redemption*

Health / Environmental *When a radioactive substance is released and creates a new superhero*

Strategic *It's all about the money (and secrets)*

Operational *When the IT is down and you are rediscovering the stone age*

VULNERABILITY SCORING

And now, the maths !

Exposure, **Prerequisite** and **Technicality** define together the **likelihood** of the vulnerability exploitation
For each, the top level value represents 4 points and the following: 3, 2, 1. Add those three scores

Score	Likelihood
≥ 11	Maximal
≥ 9	High
≥ 6	Medium
≥ 3	Low

*Exemple: a XSS is remotely exploitable (4), needs a deception (3) and is quite automated (3)
= 10 (High likelihood)*

VULNERABILITY SCORING

And now, the maths !

Harm and **Damage** define the **Impact**

The scoring is more complicated because several options can be involved in the same time

For each **Harm** scenario, the score can be :

- 0 : absent
- 1 : limited and non sensitive part of the target involved
- 2 : broad or sensitive part of the target involved
- 3 : target fully affected

For each **Damage** scenario, the score can be :

- 0 : absent
- 1 : limited prejudice over time
- 2 : significative prejudice over time
- 3 : possible irrecoverable prejudice

VULNERABILITY SCORING

And now, the maths !

Add all the points of **Harm** and **Damage**, the scale is:

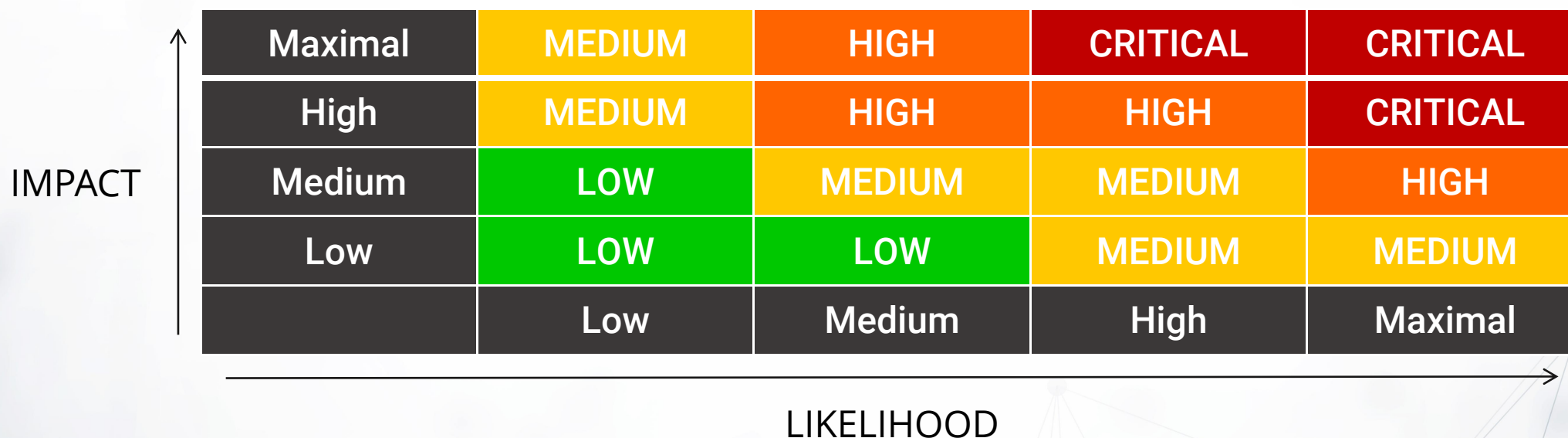
Score	Impact
≥ 22	Maximal
≥ 15	High
≥ 8	Medium
≥ 0	Low

*Exemple: a successfully exploited XSS permits information disclosure, tampering, privilege escalation and scope extension about one account with personal data : $2 + 2 + 1 + 1$
The structure will suffer a limited prejudice in reputation (from the victime who was deceived), potentially a legal prejudice (GDPR or if non repudation was mandatory), a limited obstacle about strategic and operational purposes: $1 + 1 + 1 + 1 = 10$ (Medium Impact)*

VULNERABILITY SCORING

FINAL RISK

The final definition of the vulnerability risk is calculated according to the following table:



A 5x5 matrix for vulnerability scoring. The vertical axis is labeled 'IMPACT' with an upward arrow, and the horizontal axis is labeled 'LIKELIHOOD' with a rightward arrow. The matrix cells contain risk levels: Maximal, High, Medium, Low, and their corresponding final risk scores (MEDIUM, HIGH, CRITICAL, LOW, etc.). The background features a faint network diagram.

Maximal	MEDIUM	HIGH	CRITICAL	CRITICAL
High	MEDIUM	HIGH	HIGH	CRITICAL
Medium	LOW	MEDIUM	MEDIUM	HIGH
Low	LOW	LOW	MEDIUM	MEDIUM
	Low	Medium	High	Maximal