Canva

Understanding and improving detection coverage using MITRE ATT&CK

M3asuring the threat

Raymond & Jasmina

おはようございます Magandang umaga शुभ प्रभात

早上好 Good morning Καλημέρα Buenos

Buongiorno Magandang Hapon สวัสดีตอนบ่าย

rde こんにちは Buon Pomeriggio 下午好 Dob

Good Afternoon 안녕하세요 Boa tarde おは

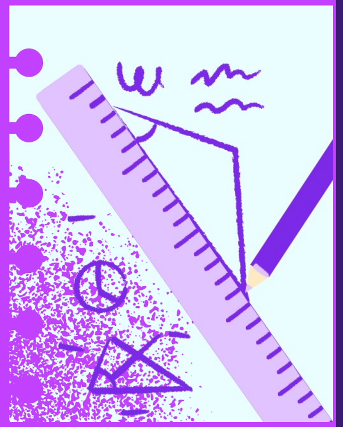
Boa Noite सुसंध्या Canva Good evening Boa ta

Today's agenda

01

Who are we?

02

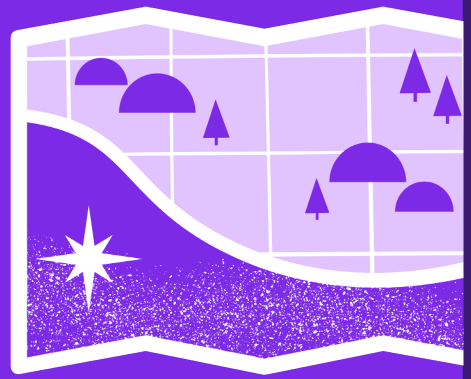


Why measure?

03

How do we collaborate?

04



What are the pitfalls?

05

Where to next?

1

Who are we

Jasmina Zito

Raymond Schippers

1

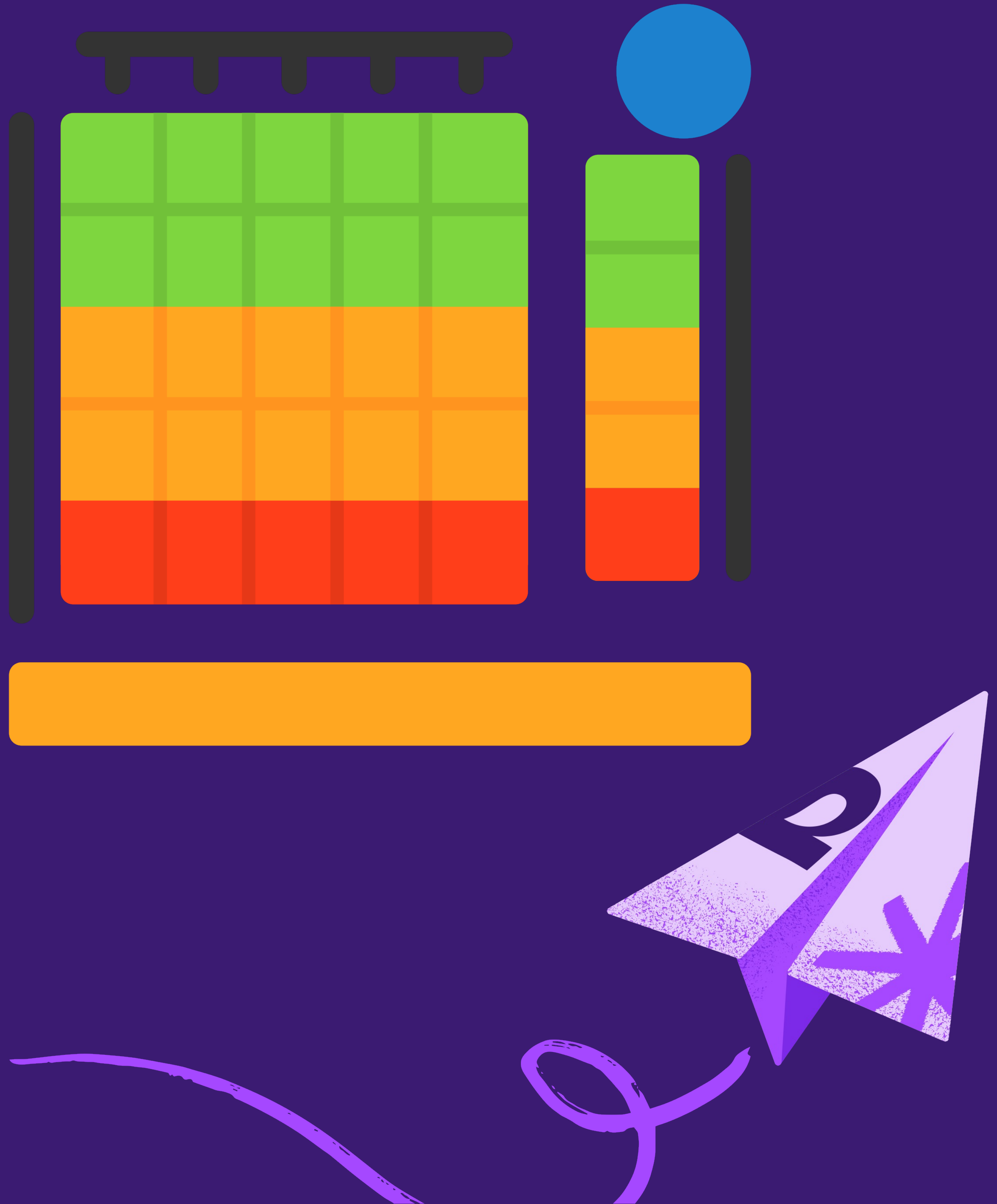
Why measure?

why m3asure?

Can’t manage what you don’t measure

What does good or great security look like?

What should we invest our research efforts into?



Detection Questions

1. How has our protections in AWS improved?

2. What is our coverage for Hopping Kangaroo?

3. Can we detect identity based attacks ?

3

Collab - CTI & Detections

CTI

Understands and tracks adversaries & their TTP

Creates profiles and bulletins on adversaries of concern

Advises detection & hunting team on TTPs and adversaries

Detections

How do we turn TTP into a detection?

What does it look like in our logs?

How can we overplay our coverage with the adversary and understand gaps?

Example

Adversary uses technique X

Do we detect X?

Can simulate it? Analytics?

ATT&CK Challenges

1

What is a platform vs service?

2

Analytics and attacks across providers vary

3

Coverage for a service vs a platform vs a technique

4

How to measure with generic platforms

Human Factors

If something is only high on Product complexity, is this the best use of a TPM? or do we need to solve for that first?

1

Tagging a detection with technique

2

Coverage a detection provides

3

Different people selecting different techniques

4

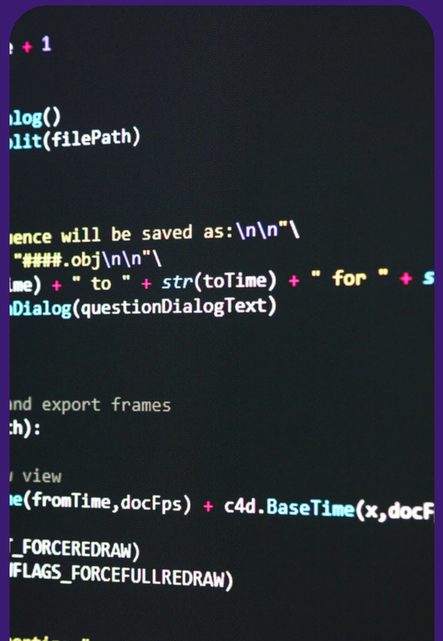
Different tooling using different ATT&CK versions

Solutions speak louder than problems

Automate

Navigator

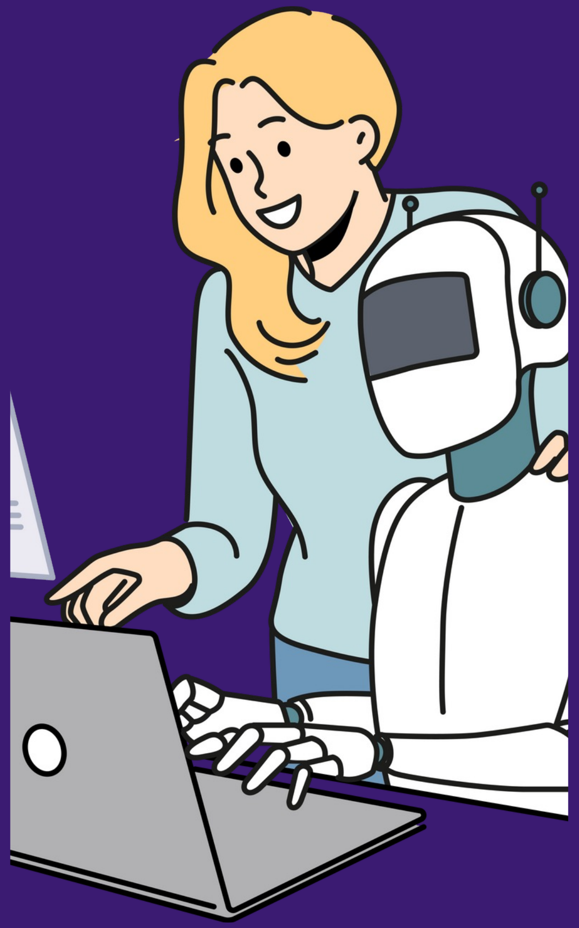
Layer creation per detection based on source system



```
 + 1

log()
lit(filePath)

ence will be saved as:\n\n"\
 "####.obj\n\n"\
me) + " to " + str(toTime) + " for " + s
Dialog(questionDialogText)

nd export frames
h):

 view
e(fromTime,docFps) + c4d.BaseTime(x,docF

_FORCEREDRAW)
FLAGS_FORCEFULLREDRAW)
```

Automate Testing

Test that rules logic still works
Test that logs have changed
Test if the alerting flows works



Threat Bulletins

Ensure Threat Bulletins result in actions and include MTIRE mappings for techniques.

Leverage NLP tools to speed up identification of techniques in text.

Outcomes

Deeper understanding of coverage per systems

Can drill up or down on coverage

Coverage evolves as threats evolve

Prioritise research & detection efforts.

What’s next

Custom of MITRE techniques

More log focused coverage not just system

Using log coverage to drive log onboarding priority

Sharing with the community

Questions?

Thank you!

Canva