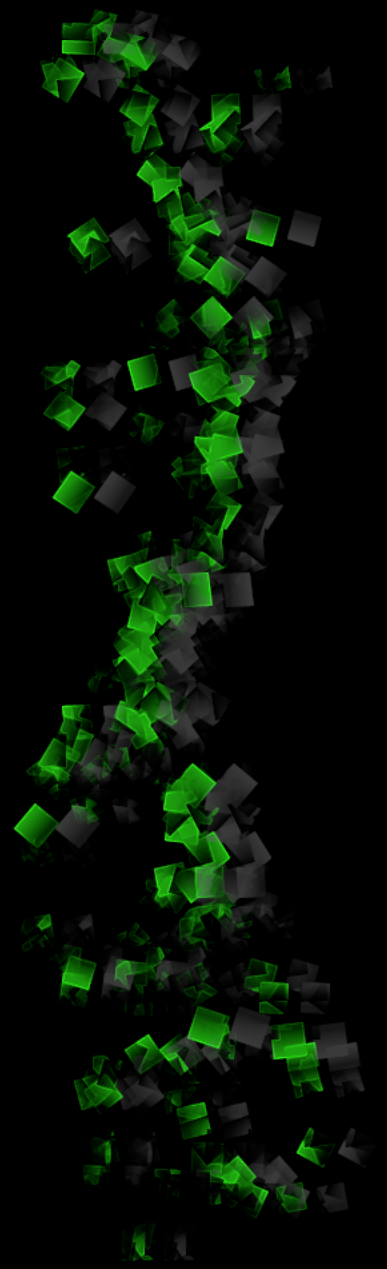
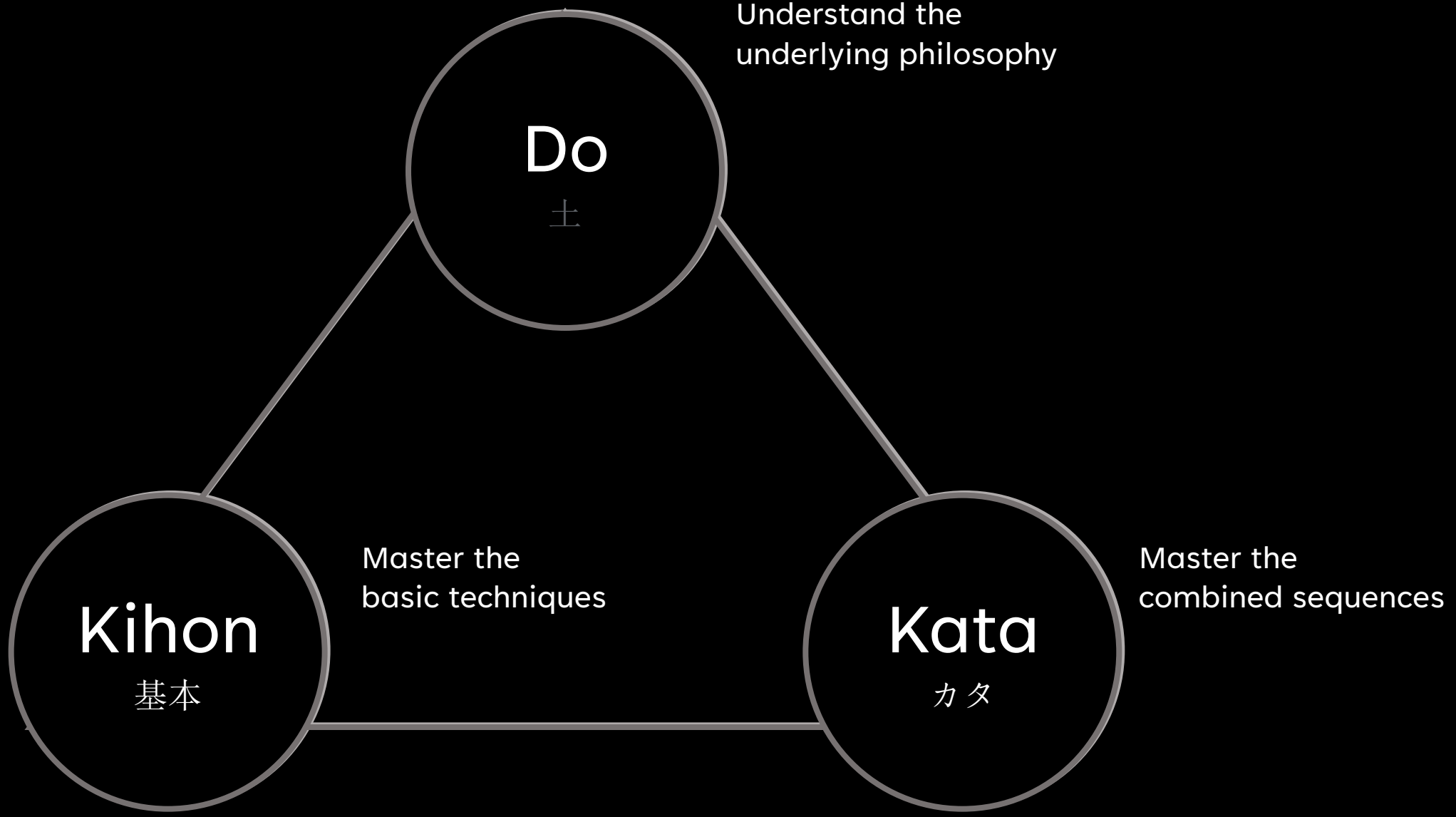
HITCHHIKER'S GUIDE FOR THREAT MODELING

Michael Bernhardt




Do
土
Understand the
underlying philosophy
Kihon
基本
Master the
basic techniques
Kata
カタ
Master the
combined sequences

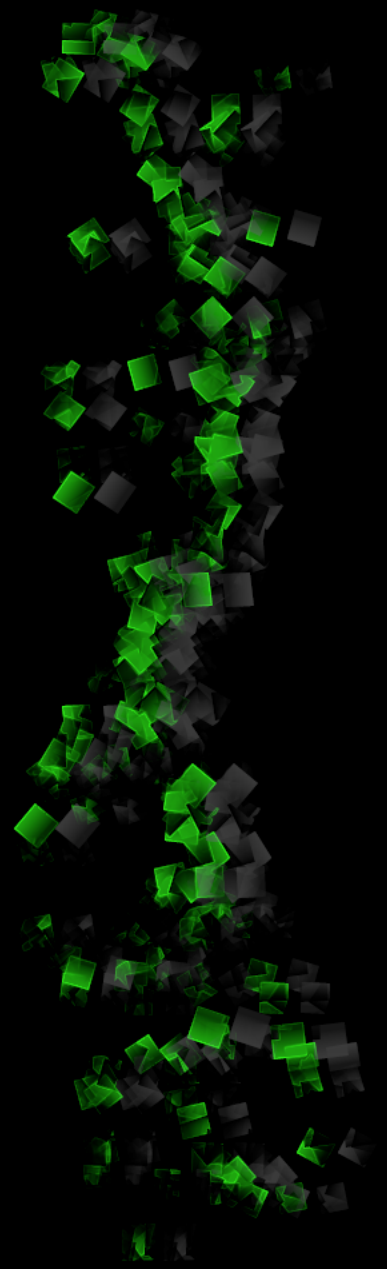
PART 1- REVIEW OUR AMBITION:

HOW DO WE TEACH PRACTITIONERS TO DO IT?

Look at what guidance is already there

Look at how we guide as a community

See how it relates to the Threat Modeling Hitchhiker Guide



Kihon

- Attack Trees
- STRIDE
- DREAD
- Misuse Cases
- Data Flow Diagrams / TAM
- …

Kata

- Books (Adam, Brook, Izar, …)
- Sample Threat Models
- Resource compilations / Blogs / Newsletters
- Papers (SANS, …)
- NIST Standard (Draft Status)
- Communities

Do

- Historic Microsoft Blog
- Threat Modeling Manifesto
- Adam's Jenga paper

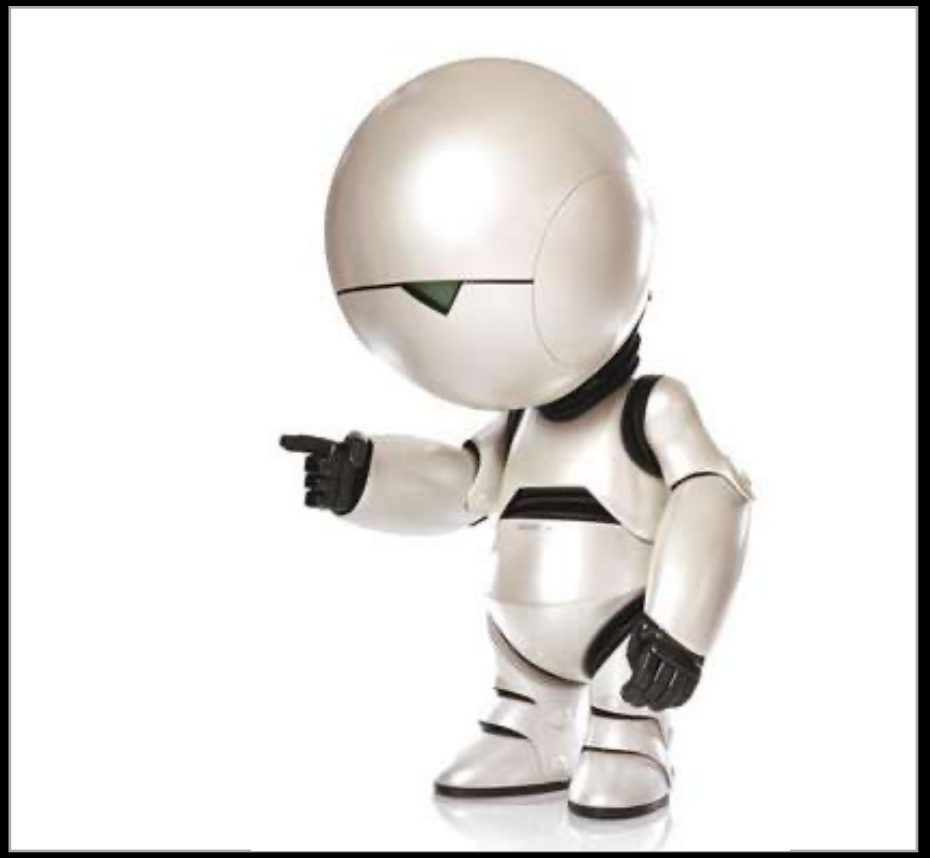
TMC – DID WE DO A GOOD JOB?

Word Cloud Generator (jasondavies.com)

HITCHHIKER'S GUIDE FOR FAILING THREAT MODELING

The Security Expert

Go to blog article



The Developer

PART 2- REVIEW OUR AMBITION:

HOW DO WE GET THE BUY-IN FOR PRACTITIONERS TO DO IT?

How do we enable practitioners to get the buy-in?

What does the expert community see as the missing parts for better acceptance?

PILLARS OF A TM PROGRAM - ADAM'S JENGA MODEL

Organizational

Interpersonal

Technical

[The Jenga View of Threat Modeling]

TMC – DID WE DO A GOOD JOB?

Word Cloud Generator (jasondavies.com)

TO WHICH EXTEND DOES THE FRAMEWORK PROVIDE PRACTITIONERS TO GET THE BUY-IN FROM THE *BUSINESS*?

- Basic concepts (Attack Trees, STRIDE, …)
- Best practices
- Tools
- Reputation
- …

How do we make it *measurable*? Which metrics/KPIs could we promote to advertise the *value* of Threat Modeling?

Do

TO WHICH EXTEND IS THE VALUE KNOWN TO OUR *SECURITY PEERS* OUTSIDE APPSEC?

- SOC/Incident Response
- GRC
- BCM
- Network Security
- …

What is required to make the outcome of a Threat Modeling *meaningful to other security disciplines*? What are the fine twists and enhancements that would bring it closer to their work?

> TO FIGHT IN ALL YOUR BATTLES AND WIN IS NOT THE GREATEST ACHIEVEMENT. THE BIGGEST ACHIEVEMENT IS TO BREAK THE RESISTANCE WITHOUT HAVING TO FIGHT.
>
> [Kam Leung, Kung-Fu Master]

- Kim Wuyts, KU Leuven
- Nick Kirtley, Aristiun
- Koen Yskout, KU Leuven
- Izar Tarandach, Datadog
- Sebastien Deleersnyder, Toreon
- Jan-Philipp Schmitz, Capgemini
- Jasmin Mair, Leica Microsystems
- Grant Ongers, OWASP/SecureDelivery
- Brook Schoenfield
- Maurício Ariza, SAP
- Juliane Reimann / Joshua Holmes, SecureIO

Michael Bernhardt – www.linkedin.com/in/michael-bernhardt-cyber


THREAT MODELING
CONNECT
THREAT MODCON 2023
THREAT MODELING IS FOR EVERYONE