IT-Sicherheit seit 1996

terreActive terreActive terreActive terreActive

The Cyber Kill Chain

Use it to protect yourself - knowing the limitations!

Agenda

terreActive
terreActive
terreActive
terreActive

1 Introduction

2 The Cyber Kill Chain

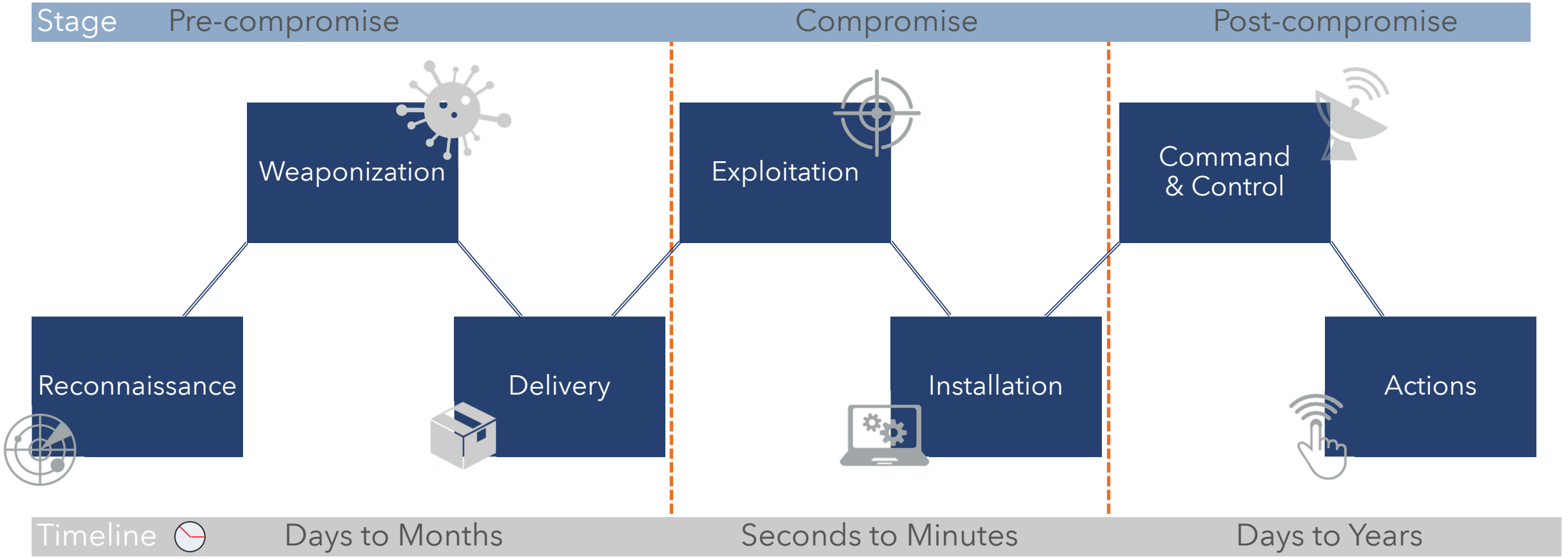
3 Mapping to the Cyber Kill Chain
Course of Action

4 Application: Intrusion Reconstruction

5 The Cyber Kill Chain in Context

6 Conclusion

The Cyber Kill Chain



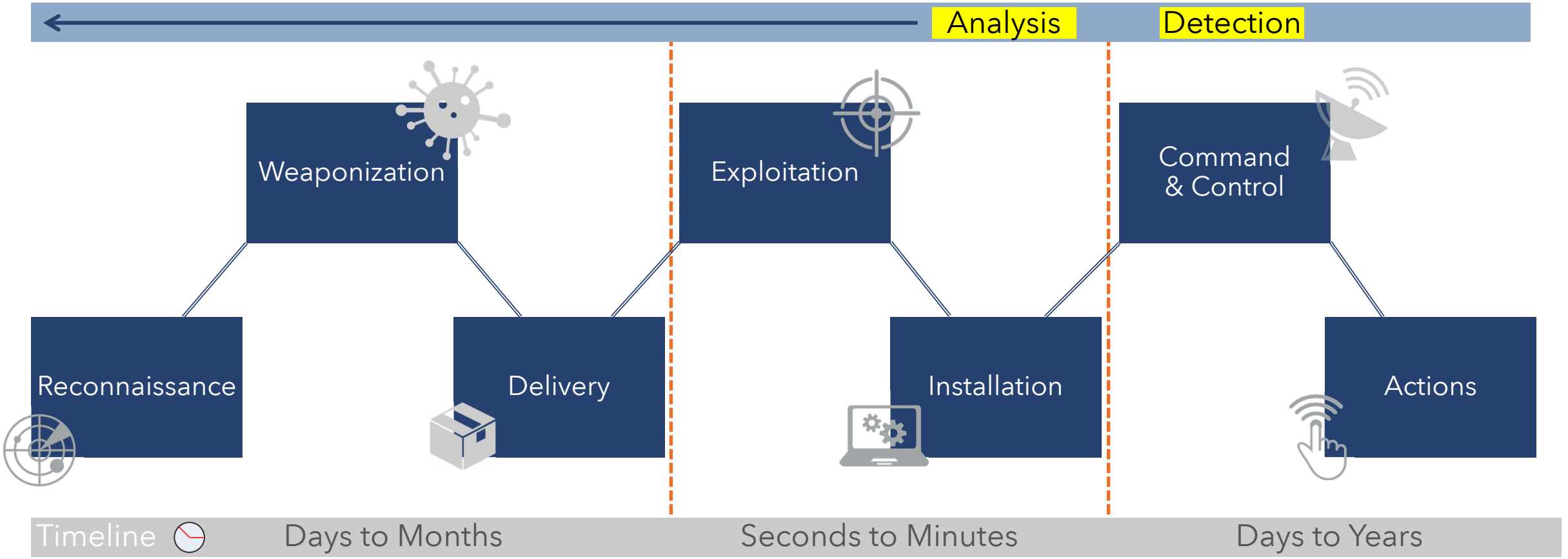
Mapping capabilities to phases

Course of Action Matrix

	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web Analytics	Firewall ACL				
Weaponisation	NIDS	NIPS				
Delivery	Vigilant User	Proxy Filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	chroot jail	AV			
Command & Controll	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit Log			QoS	Honeypot	

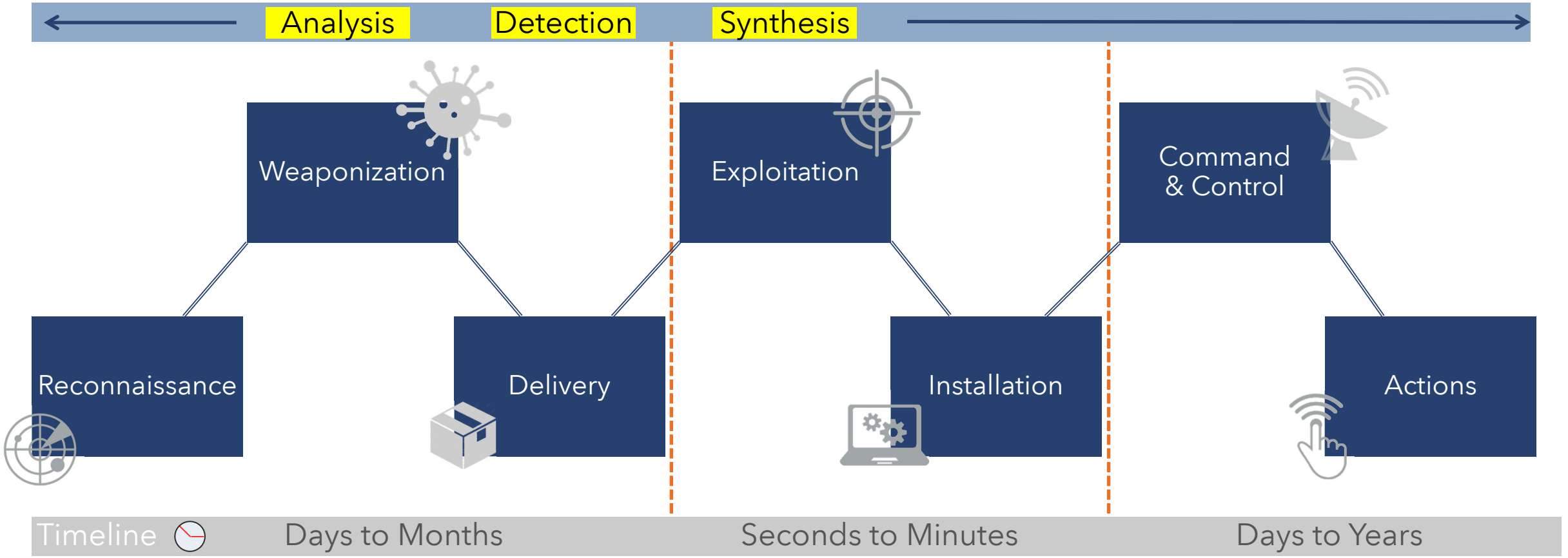
Intrusion Reconstruction

Late Phase Detection



Intrusion Reconstruction

Early Phase Detection



Conclusion

Using the Cyber Kill Chain for your benefit

Uses

- Modelling Tool
- Discover “Blind Spots”
- Intrusion Reconstruction
- Campaign Analysis
- Communication

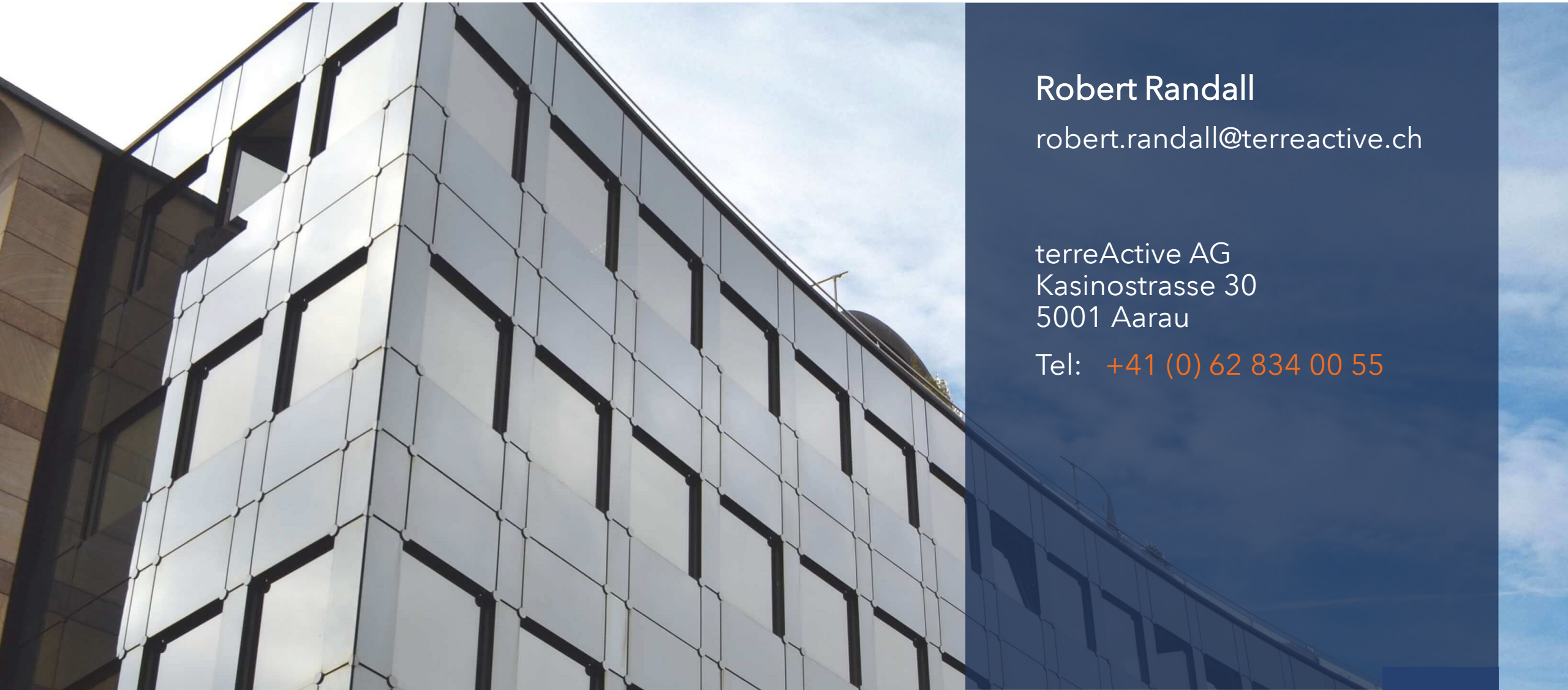
Issues

- Modeling Tool – Not Reality
- Just one tool among many
- Focused on Malware
- Perimeter-focused

Contact

IT-Sicherheit seit 1996

terreActive terreActive terreActive terreActive



Robert Randall

robert.randall@terreactive.ch

terreActive AG
Kasinostrasse 30
5001 Aarau

Tel: +41 (0) 62 834 00 55