The lifecycle of zero-day vulnerabilities;

knowledge driven escalation between attacker and defender

Sander Zeijlemaker,

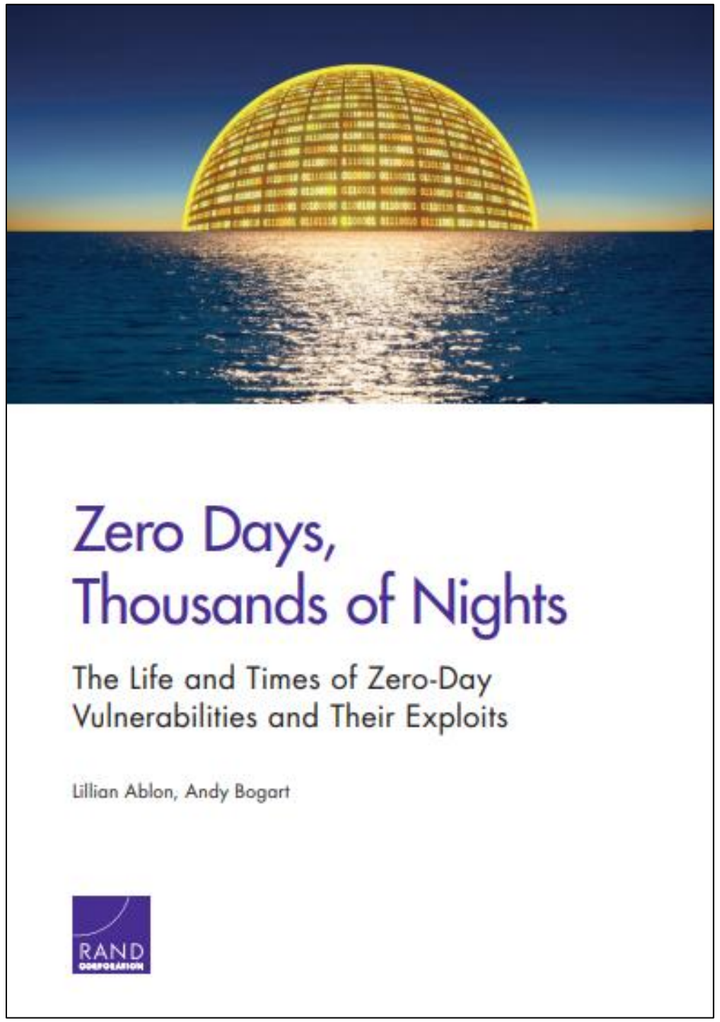
Managing Director Disem Institute

PhD Student Radboud University

DISEM INSTITUTE

Radboud University

Introduction



Rand report (2017):

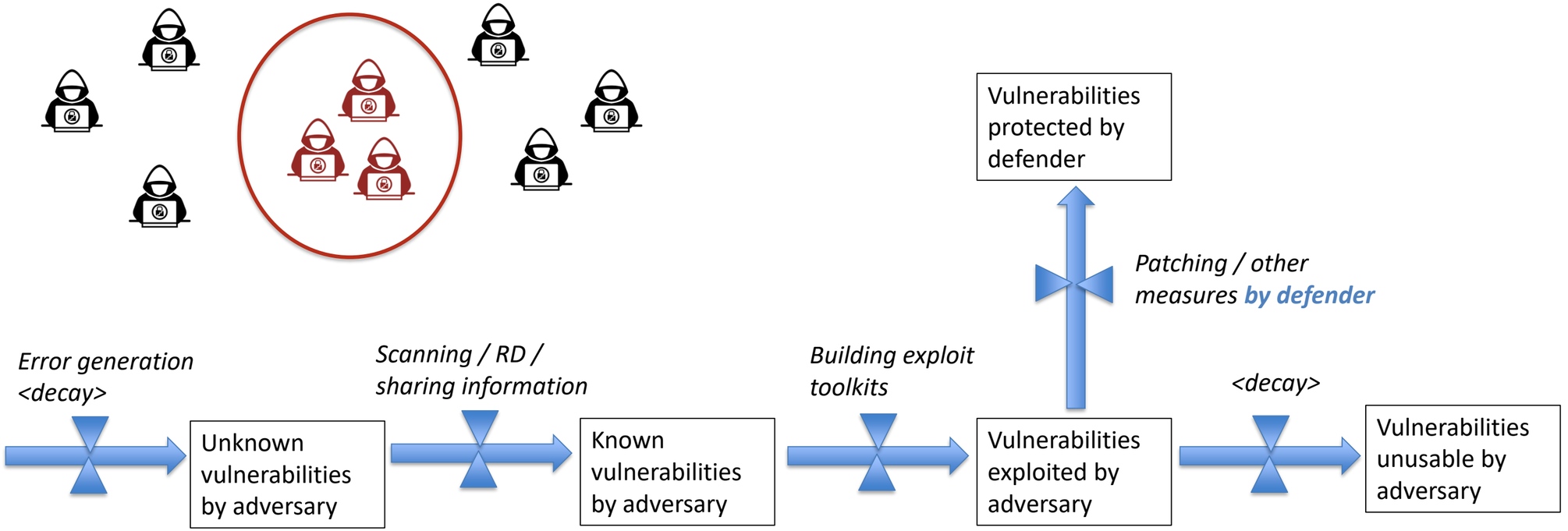
- Provides meaningful static data analyses
- Describes interaction between adversary and defender

Literature:

- Cyber-security is recognized by two dynamic structures: (Zeijlemaker 2016, 2017)
- Interaction between adversary and defender (Clayton, Moore, and Christin, 2015; Libicki, Ablon, & Webb, 2015; Su, 2006; Böhme & Moore, 2016; Barth, Rubinstein, Surandararajan, Mitchell, Song, Bartlett, 2012; Martinez-Moyano, Morrison, & Sallach, 2015).
- Response of the resilient organization (Vogus & Sutcliffe, 2007; Reinmoeller & Baardwijk, 2005; Martinez-Moyano et al., 2015)

Session with 30 IT risk professional of global operating organization.

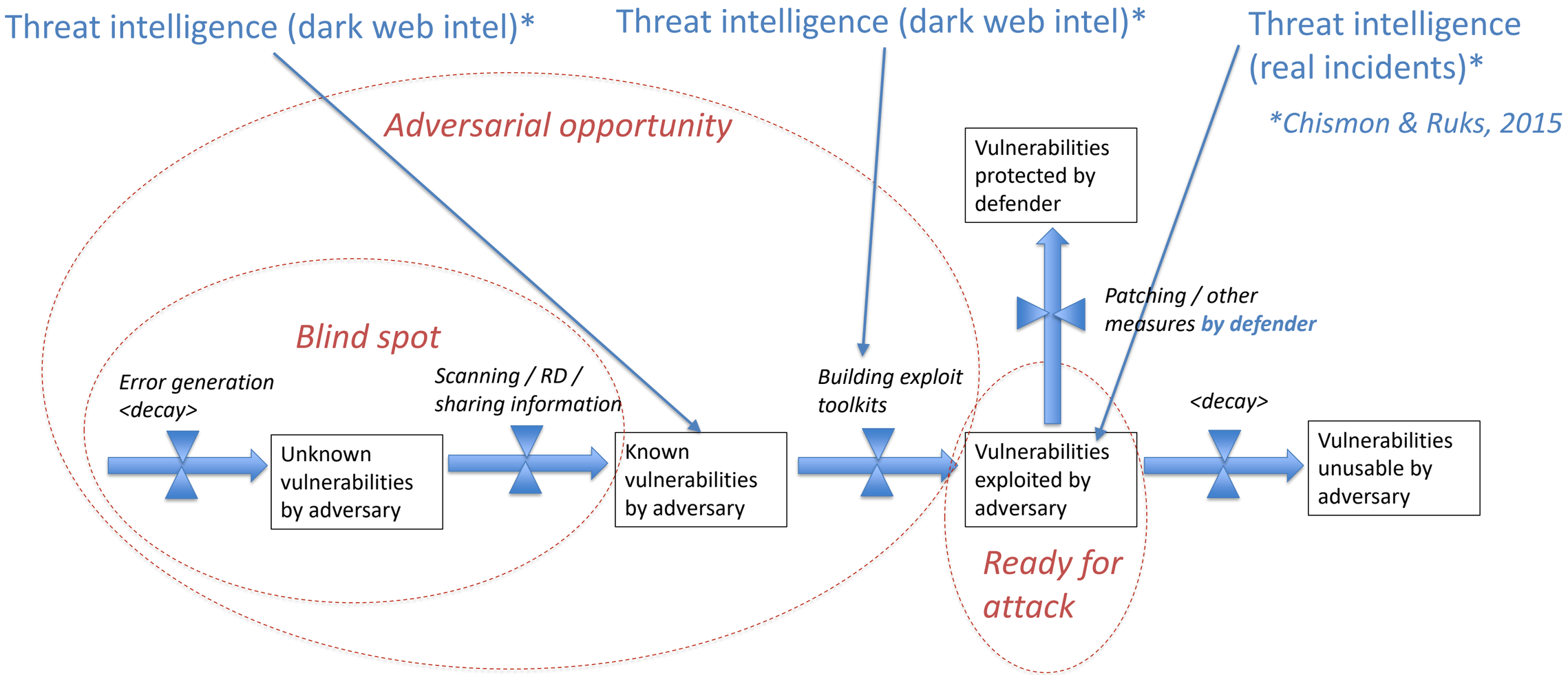
The dynamic life-cycle of a vulnerability from an adversary perspective (1 of 2)



Adversary organization:

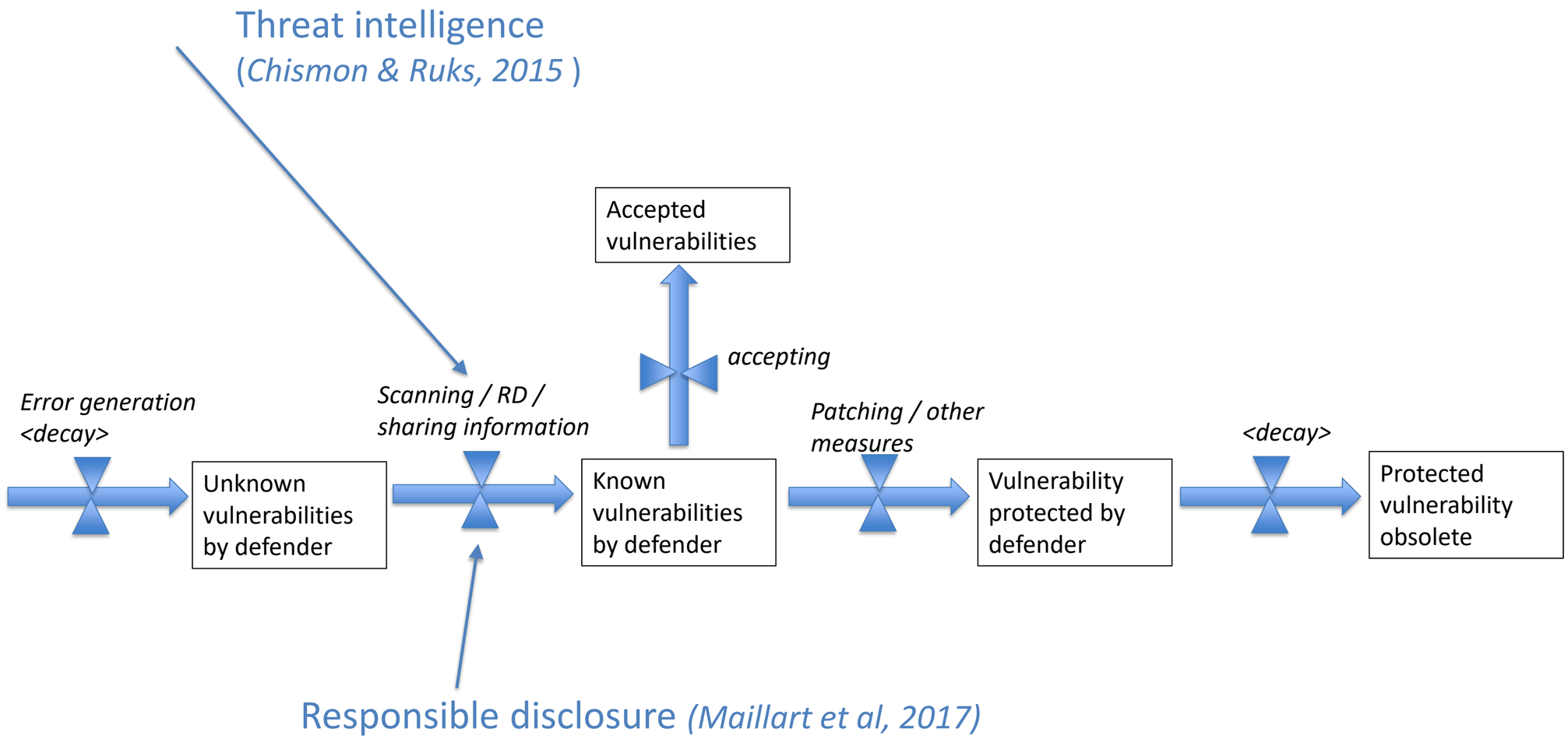
- *Value chain (*Huang, Siegel and Madnick, 2018*)*
- *Dynamic network around a core ((*Odinot, De Poot and Verhoeven, 2018*)*
- *Darkweb shielded from normal search engines (*Balduzzi and Ciancaglini, 2015*)*

The dynamic life-cycle of a vulnerability from an adversary perspective (2 of 2)

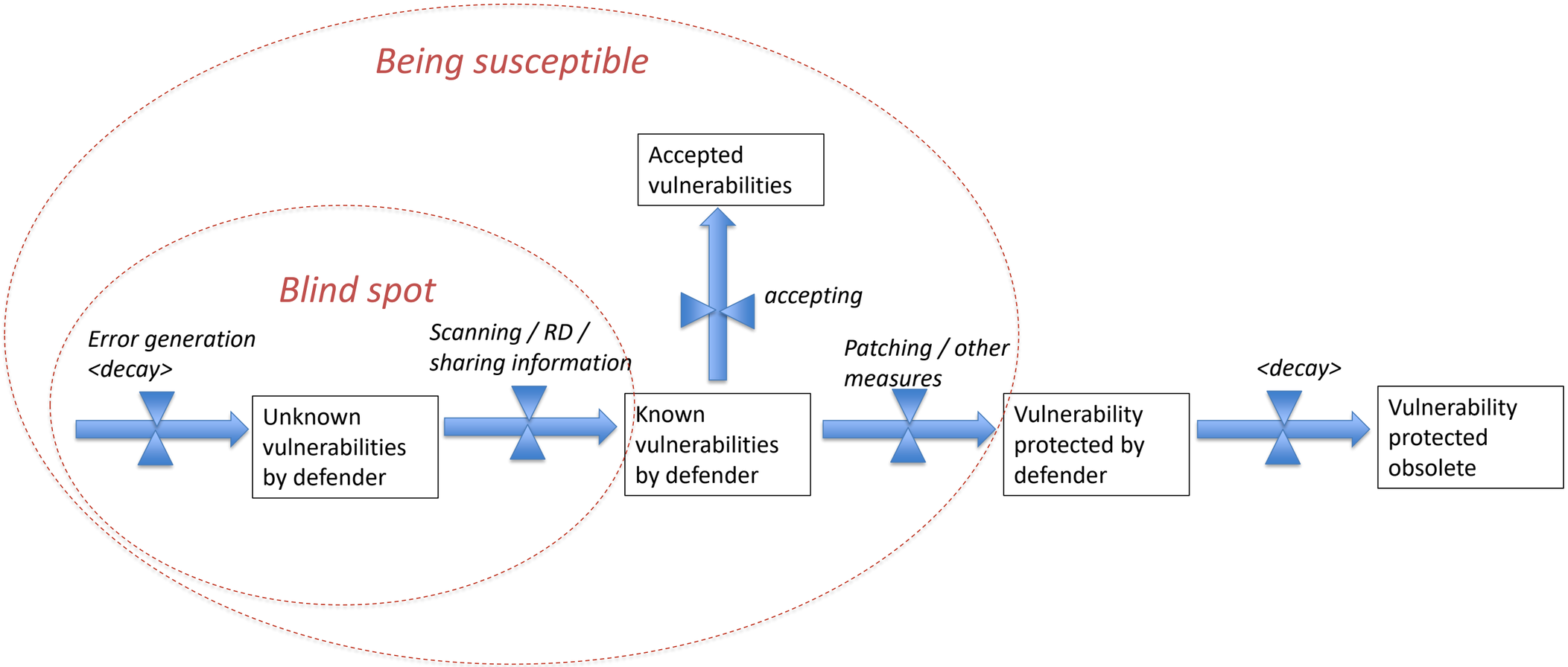


Only a limited number of vulnerabilities are actually being actively exploited by attackers or targeted for exploit kit development (Jacobs, Romanosky, Adjerid, and Baker 2020)

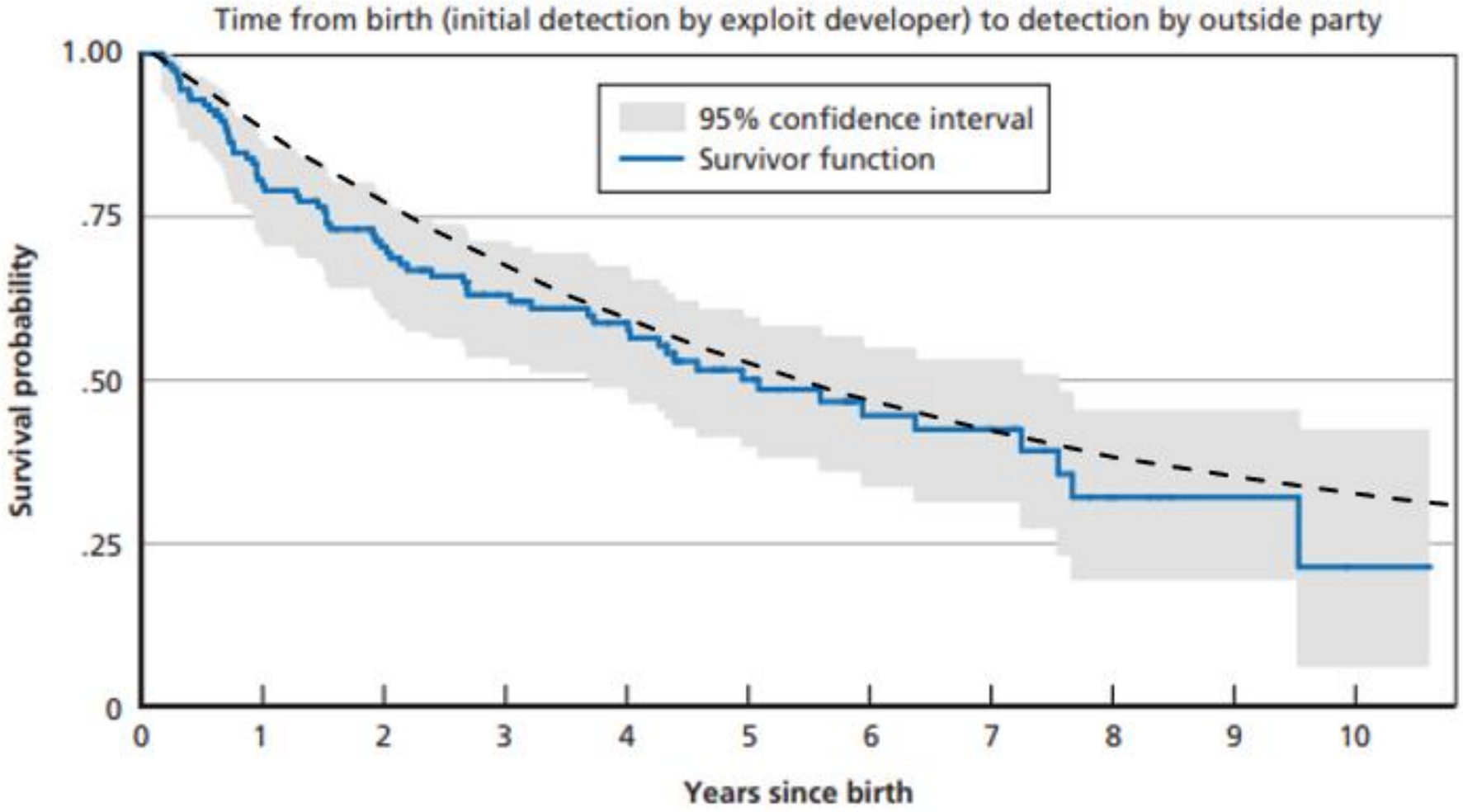
The dynamic life-cycle of a vulnerability from a defender perspective (1 of 2)



The dynamic life-cycle of a vulnerability from a defender perspective (2 of 2)



Validation of structure and output



Comparison model output and report results

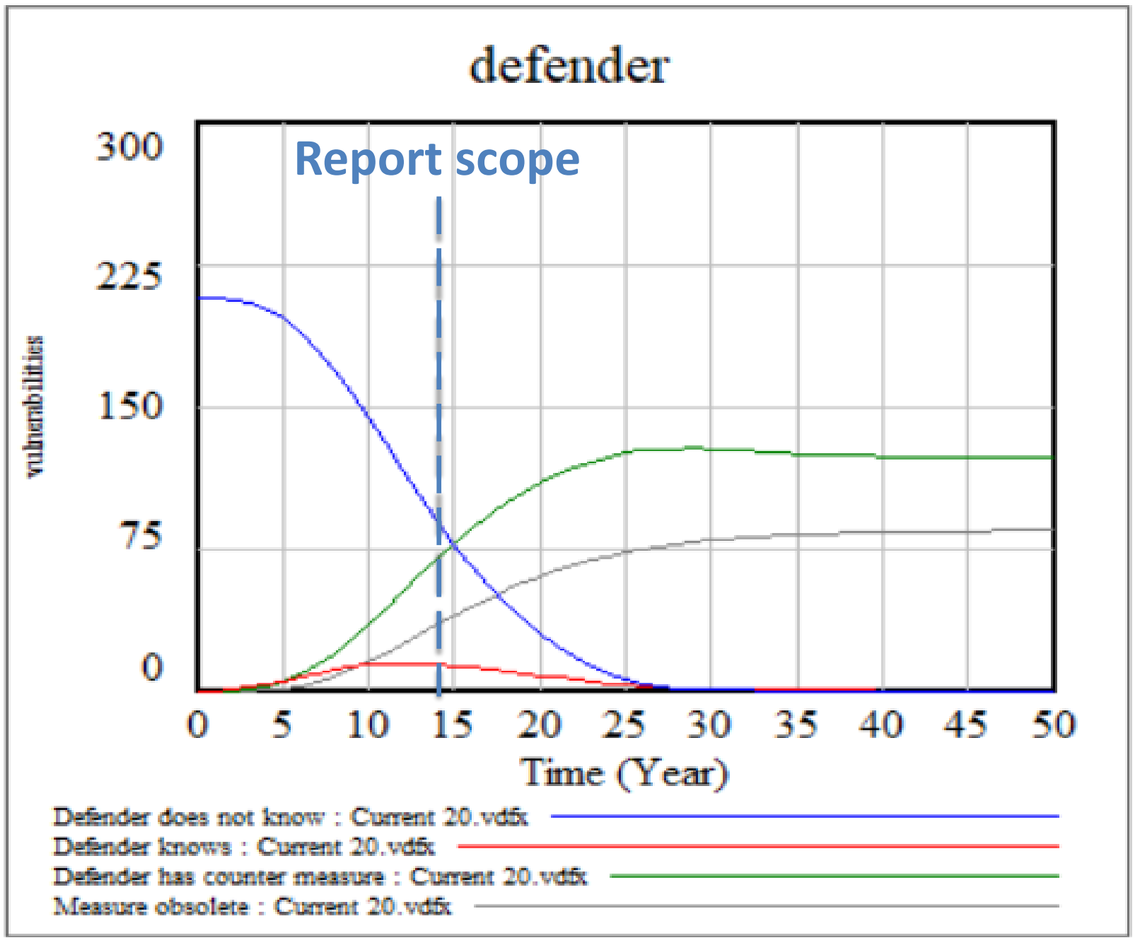
Validation of structure and output

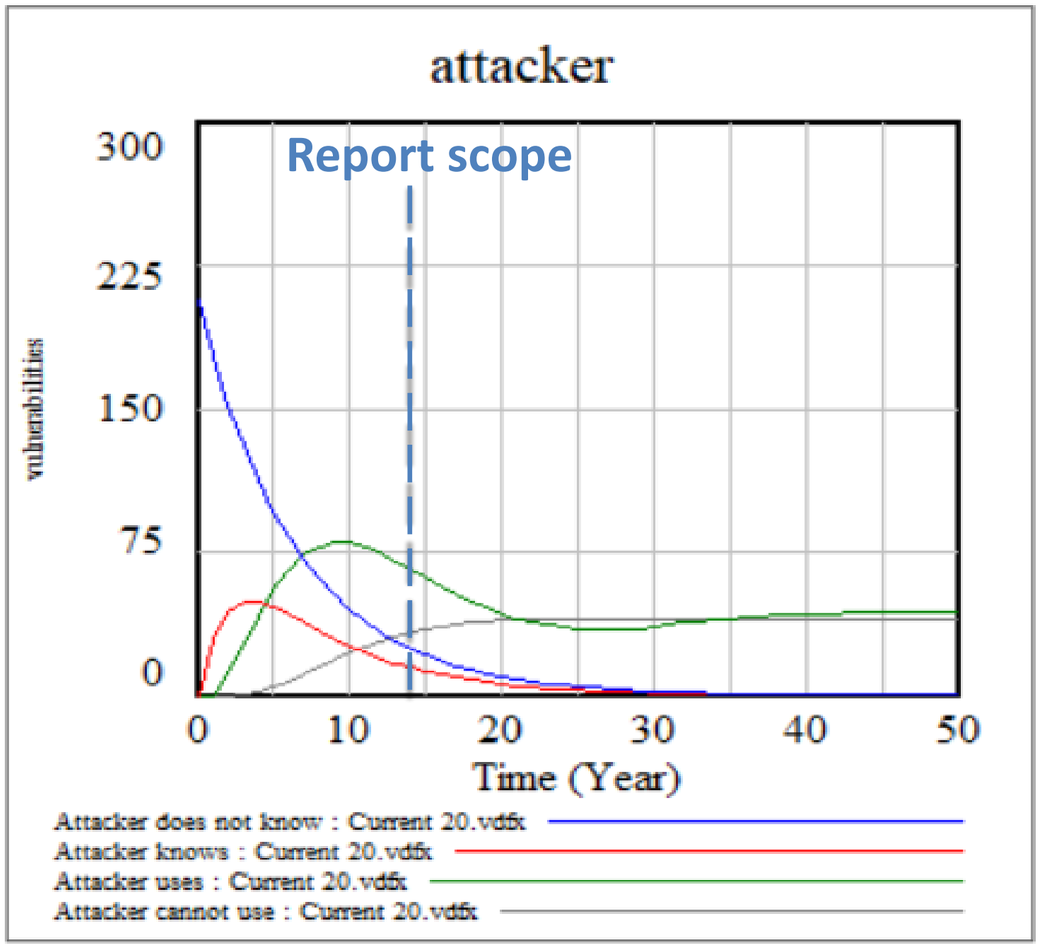
Survival probability

Report category	Rand Adversary	Model Adversary	Report category	Rand Defender	Model Defender
Unknown	*24*		*Unknown*	*24*	
Living			*Living*	*66*	
Unknown vulnerability by adversary	**24**	**24** (12%)	**Unknown vulnerability by defender**	**90**	**90** (44%)
Immortal	*13*		*Immortal*	*13*	
Code refactor	*21*		*Code refactor*	*21*	
Vulnerability unusable by adversary	**34**	**33** (16%)	**Protected vulnerability obsolete**	**34**	**34** (16%)
Security patch	*69*		*Security Patch*	*69*	
Vulnerability protected by defender	**69**	**69** (33%)	**Vulnerability protected by defender**	**69**	**69** (33%)
Publicly shared	*6*		*Publicly shared*	*6*	
Found by security researcher	*8*		*Found by security researcher*	*8*	
Vulnerability known by adversary	**14**	**14** (7%)	**Vulnerability known by defender**	**14**	**14** (7%)
Living	*66*				
Vulnerability exploited by adversary	**66**	**66** (32%)			

Comparison model output and report results

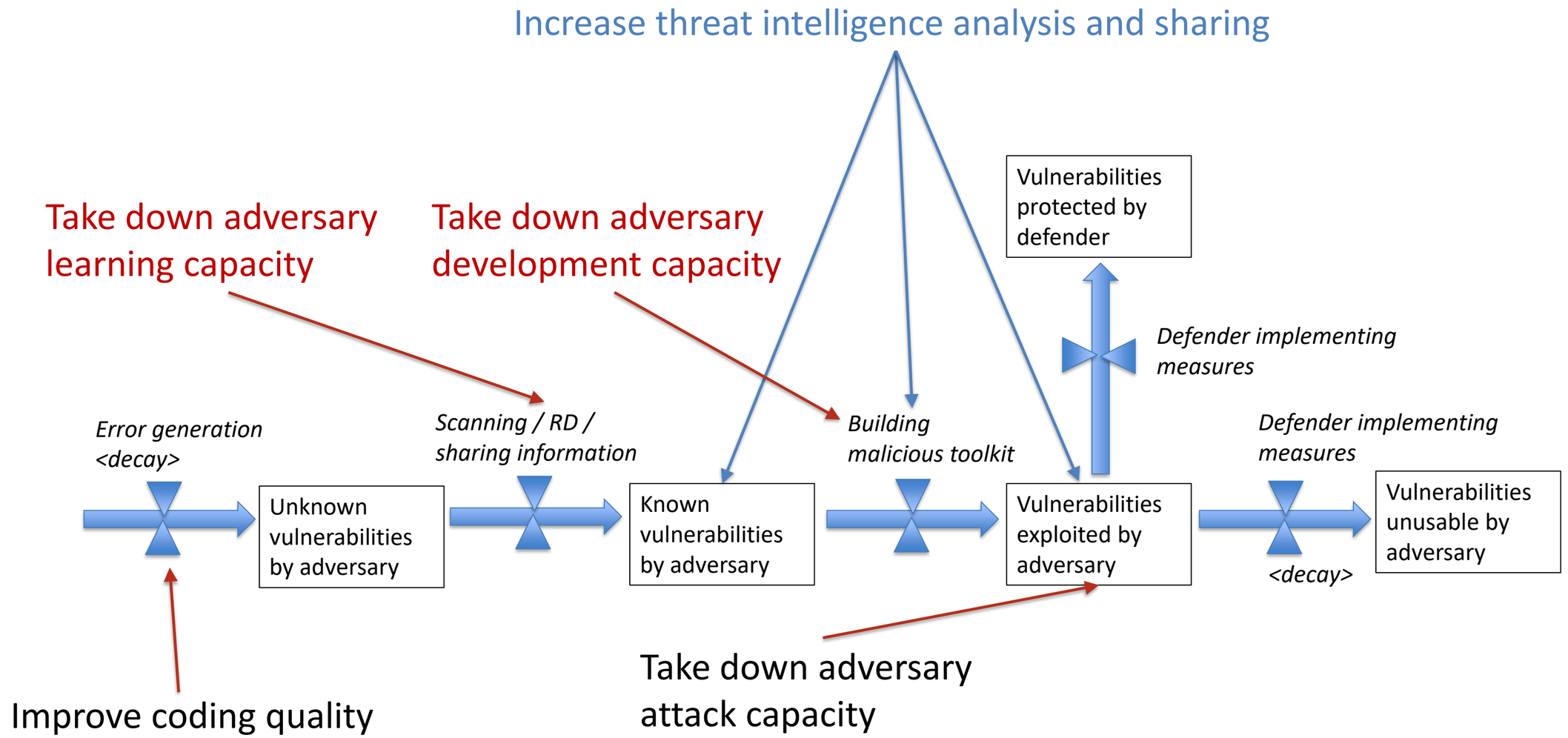
Model reach equilibrium (40 y) far beyond the time horizon of the zero-day report (14 y)





In real life there is ongoing supply of unknown zero-days due to ongoing software and hardware development

Potential policy interventions



! In defender sub-model: Defender increase responsible disclosure and active error scanning !

End state after 50 years and a total of approx. 11.000 zero-days

End-state output	Base case	Responsible disclosure Code scanning	Threat Intelligence	Take down adversary learning cap	Take down adversary development cap.
Unknown vulnerability by adversary	39%	39%	39%	58%	57%
Known vulnerability by adversary	12%	12%	12%	8%	14%
Vulnerability exploited by adversary	29%	28%	25%	18%	14%
Vulnerability protected by defender	8%	11%	20%	12%	11%
Vulnerability unusable by adversary	12%	10%	4%	4%	4%
Unknown vulnerability by defender	70%	57%	22%	37%	43%
Known vulnerability by defender	3%	4%	7%	5%	5%
Vulnerability protected by defender	8%	11%	20%	12%	11%
Protected vulnerability obsolete	19%	28%	51%	46%	41%

Threat intelligence yield:

- Highest number of vulnerabilities being protected.
- Lowest number of unknown vulnerabilities by the defender.

Limiting adversary capabilities reduces the vulnerabilities that are being exploited yet introduces offensive security.

Research limitations

- Effects of good coding practices are not considered
- Vulnerability severity and accepted vulnerabilities are not considered
- Actual vulnerability exploitation by an cyber-attack and detection and response efforts of the defender are not included in the model
- Economics / benefits evaluation for defender and adversary are not considered
- Adversary attack capacity take down is not considered