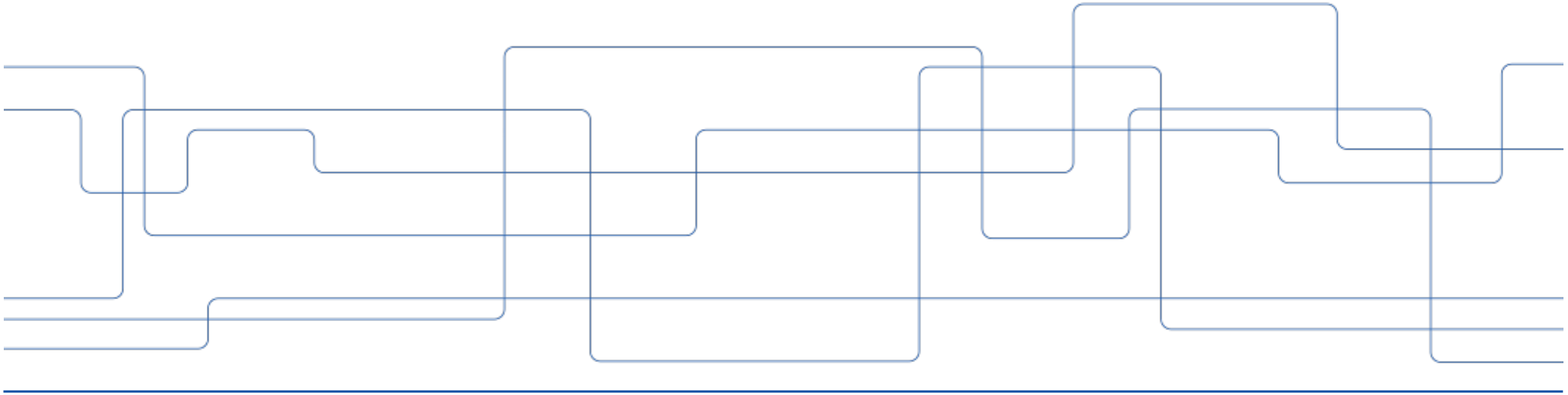
Attack Simulations for Cyberdefense

Viktor Engström
Mathias Ekstedt



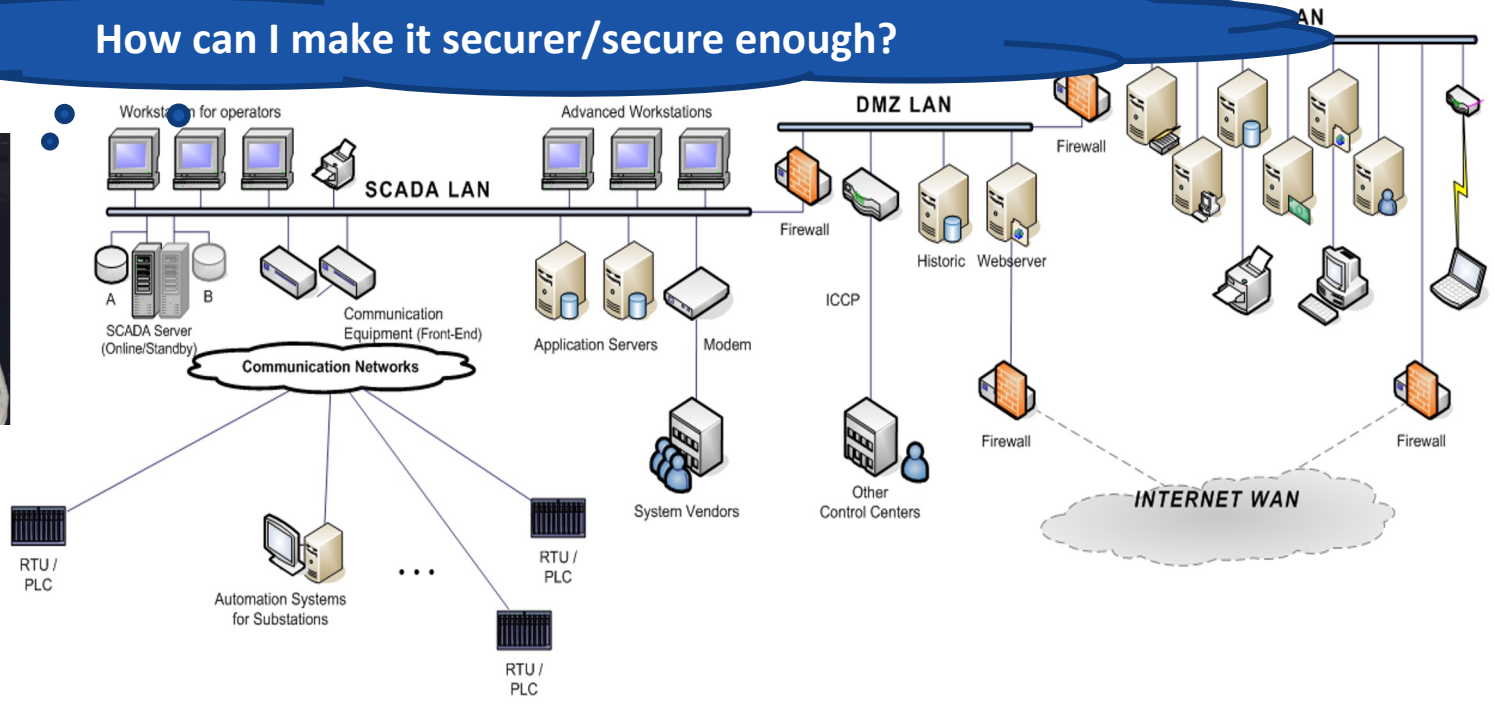
Cybersecurity management is difficult!

Is my ICT infrastructure secure (enough)?

What exactly makes the system as a whole (in)secure?

How can I make it securer/secure enough?

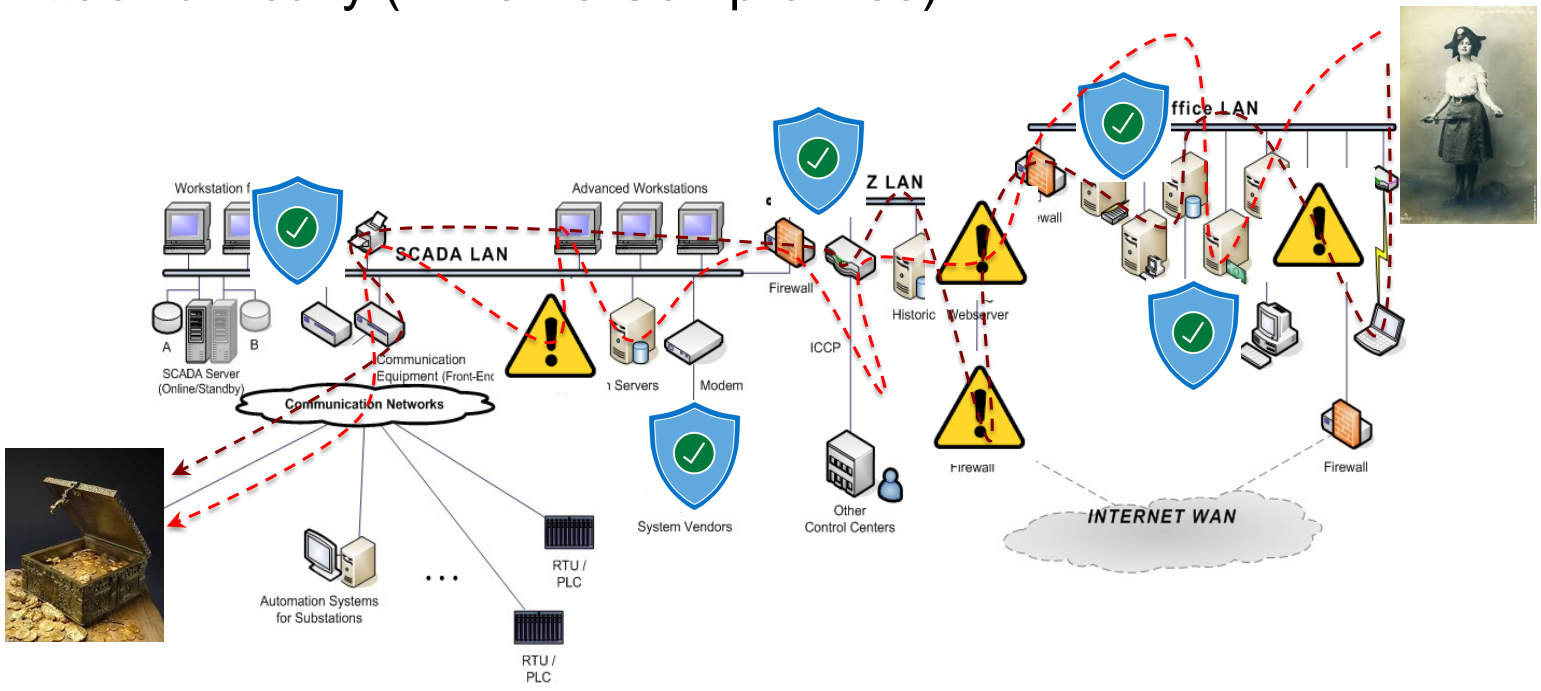
security architect (etc.)



Cybersecurity analysis of ICT infrastructures

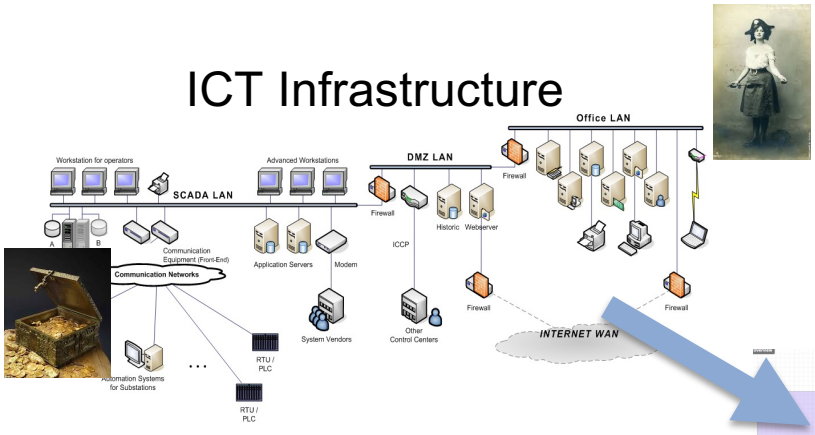
Attacks will vary with vulnerabilities and defenses (and architectural design)

- Attack vector
- Attack difficulty (Time To Compromise)

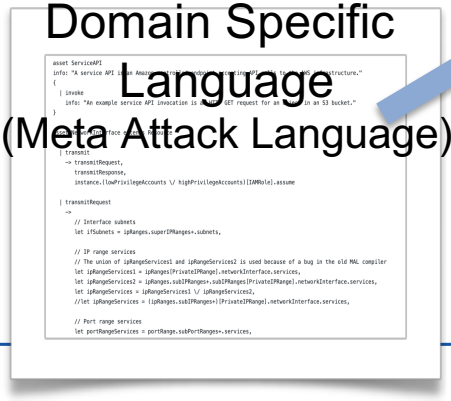


Model-based cybersecurity analysis

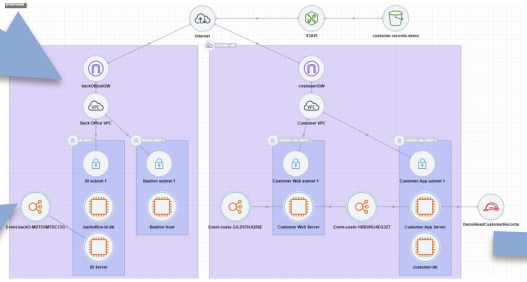
ICT Infrastructure



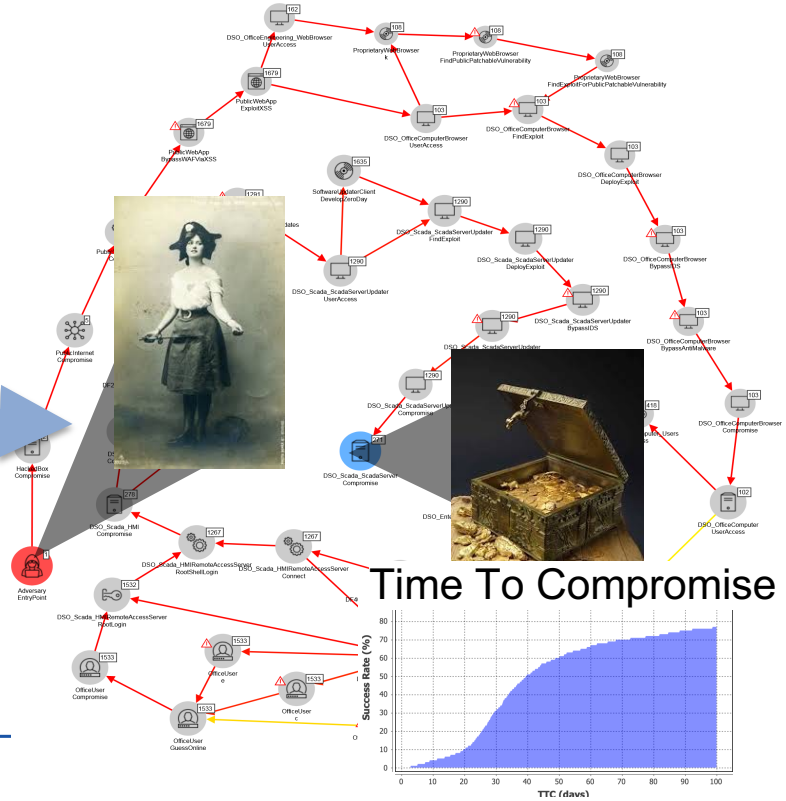
Domain Specific Language (Meta Attack Language)



Domain Specific Model

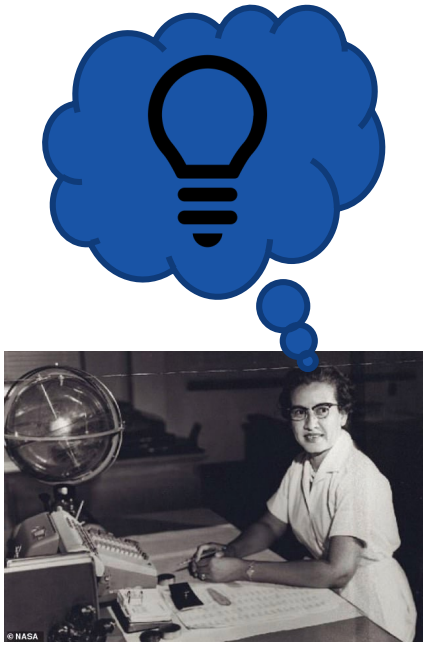


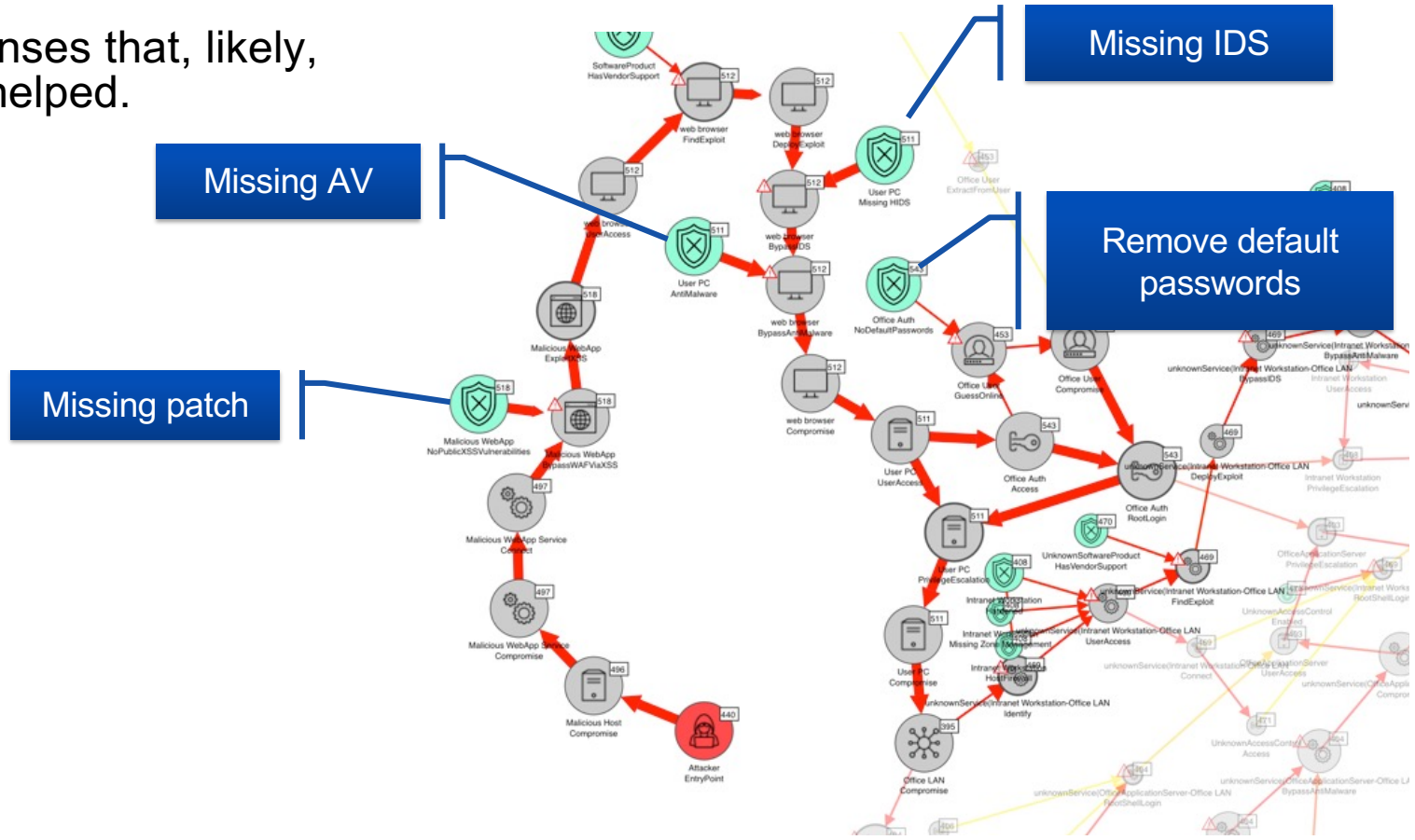
Attack graph



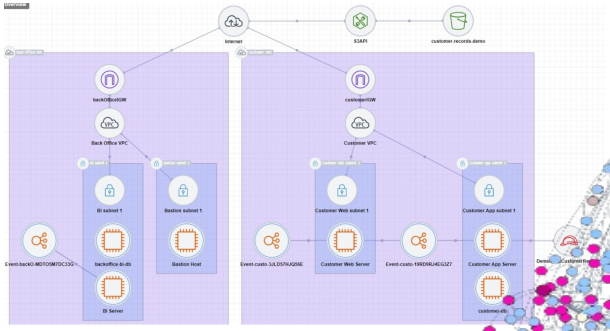
Aimed to serve as design support

Missing defenses that, likely, would have helped.

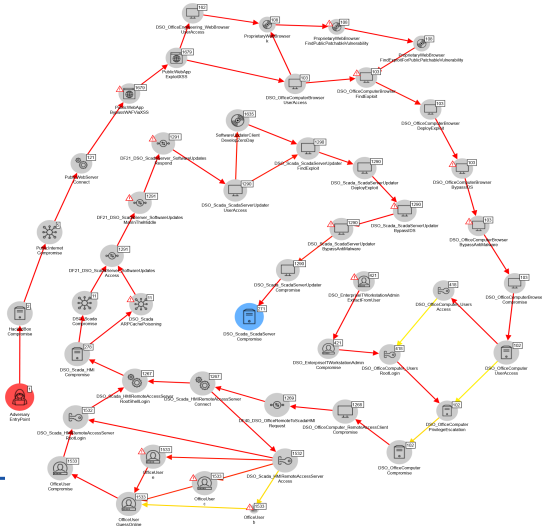




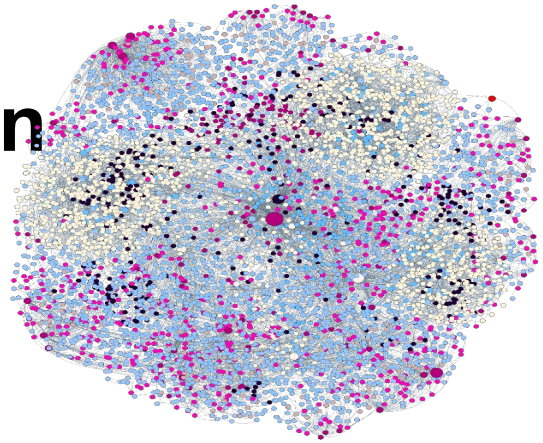
Attack graph generation and computation

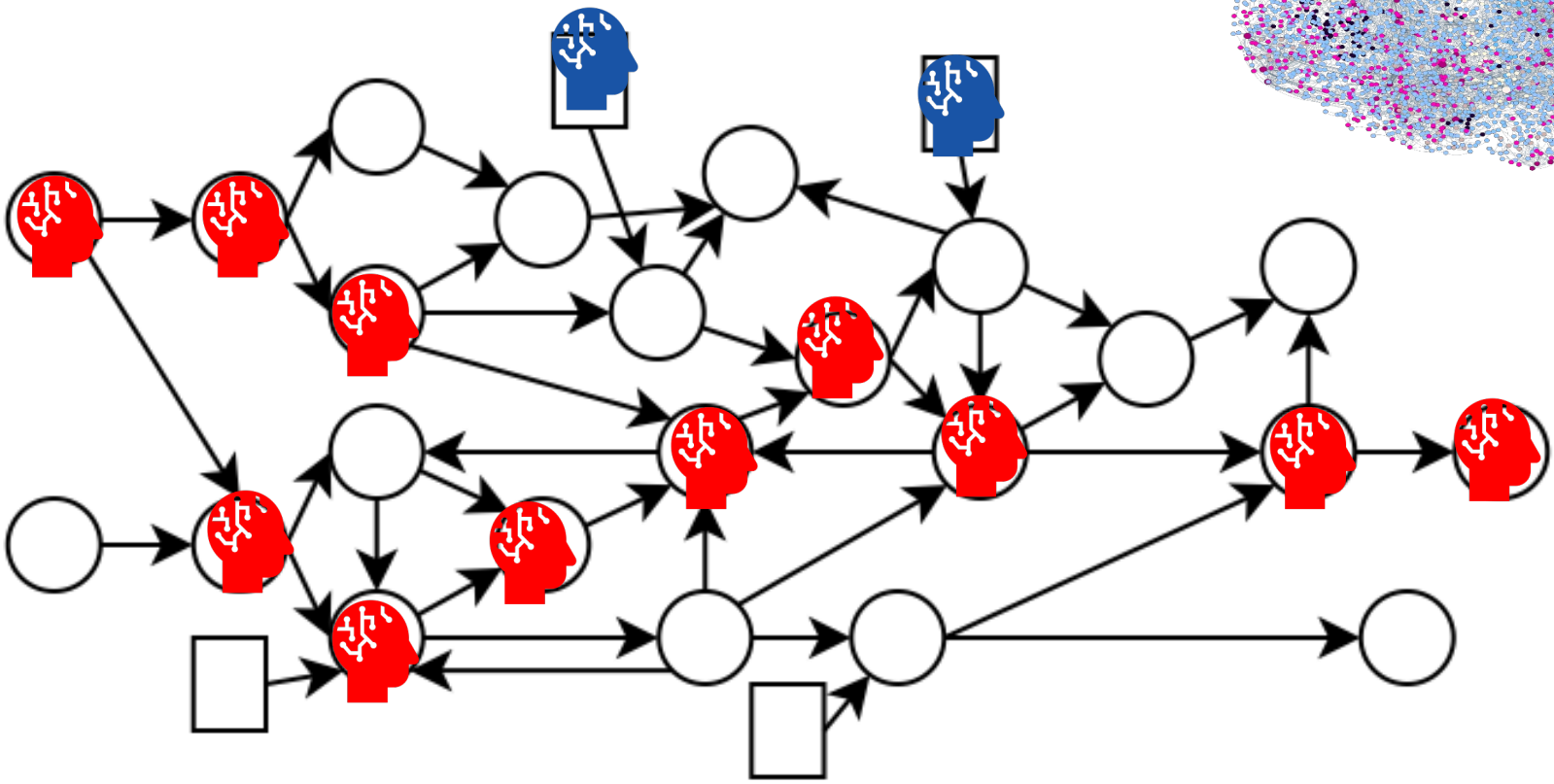


(Monte Carlo based) shortest path calculation

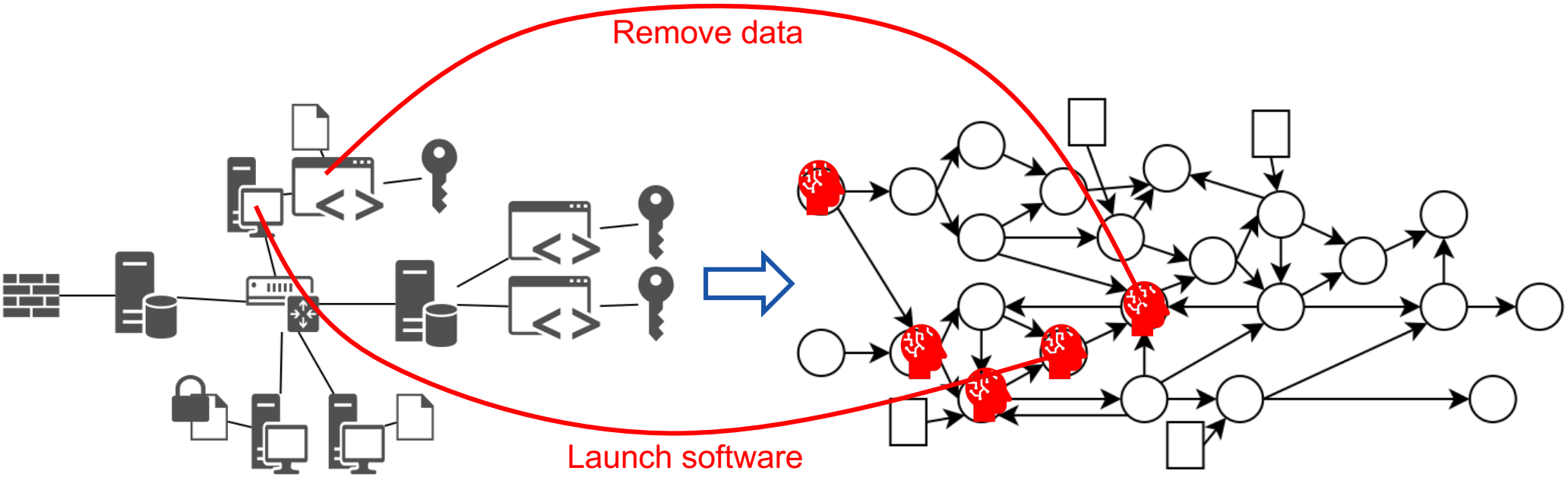


Agent- and game-oriented simulation

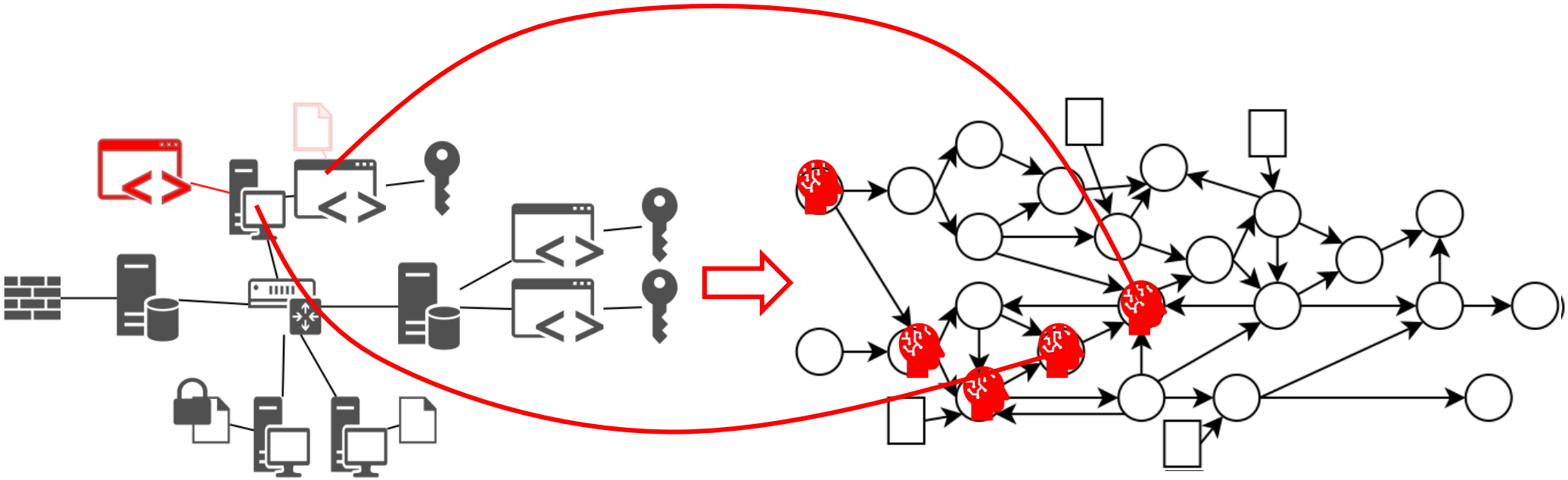




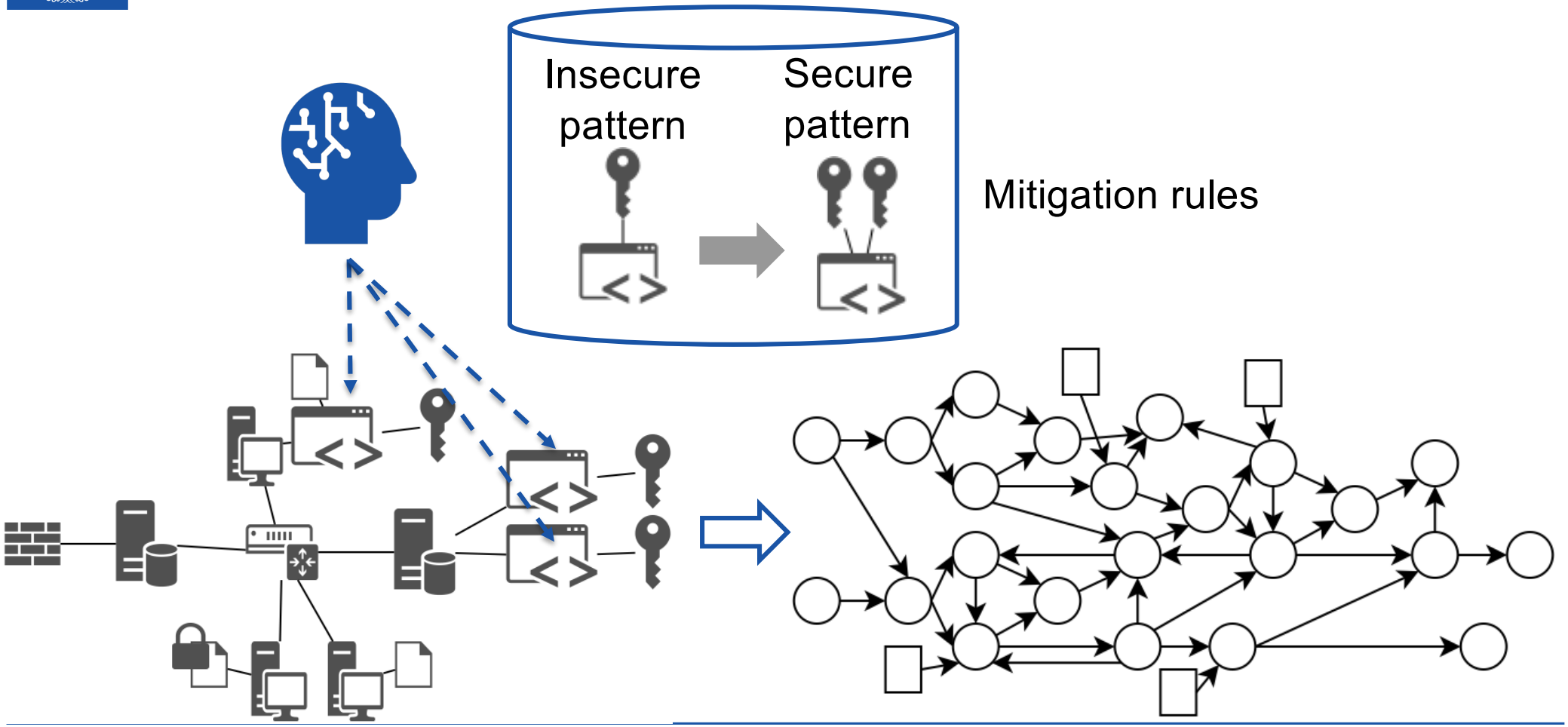
Structural changes



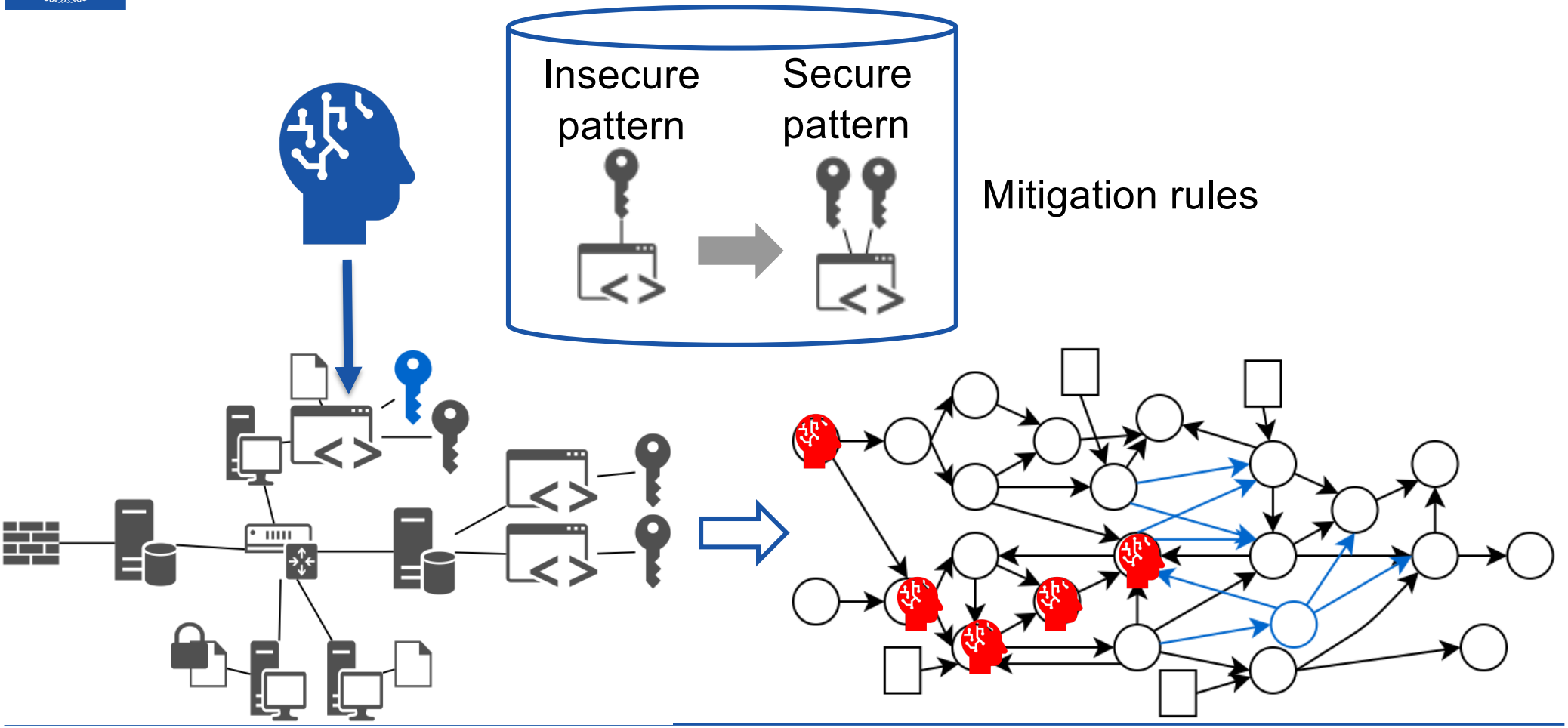
Structural changes



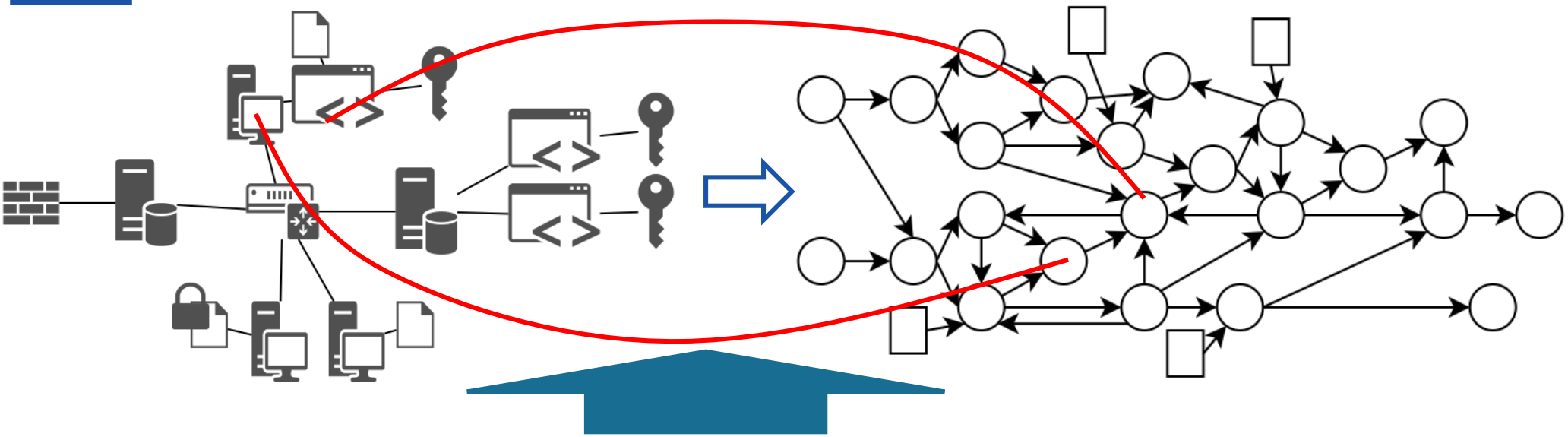
Also the defender can change structure



Also the defender can change structure

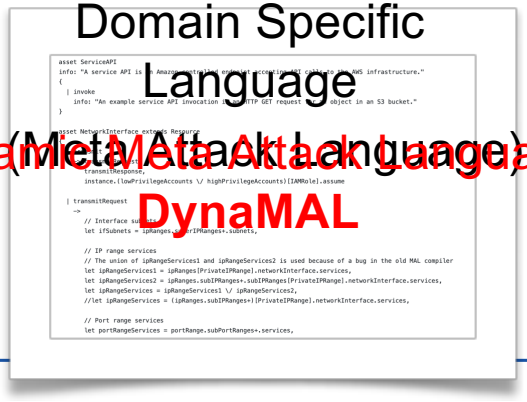


Extend formalism with dynamic structural change



Domain Specific Language (MetaAttackLanguage)

DynaMAL: Dynamic Meta Attack Language



But why?

…To get a more capable and attack simulation formalism that can better represent reality.