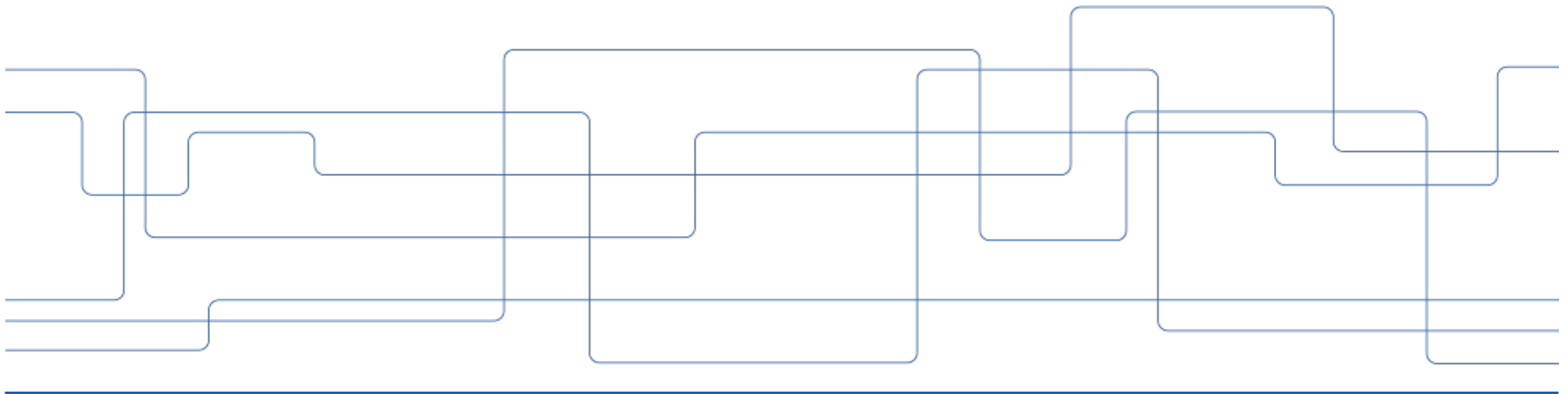




Attack Simulations for Cyberdefense

Viktor Engström
Mathias Ekstedt





Cybersecurity management is difficult!

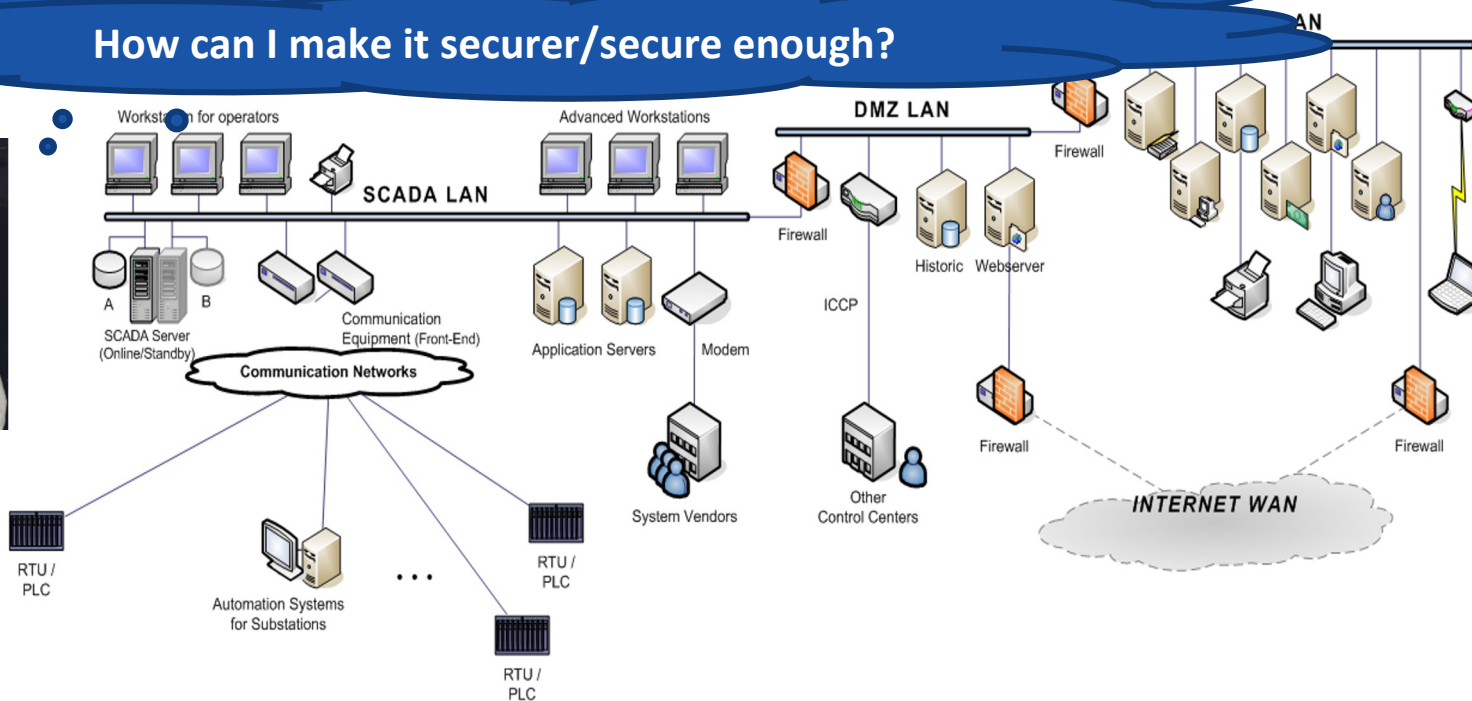
Is my ICT infrastructure secure (enough)?

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

How can I make it securer/secure enough?



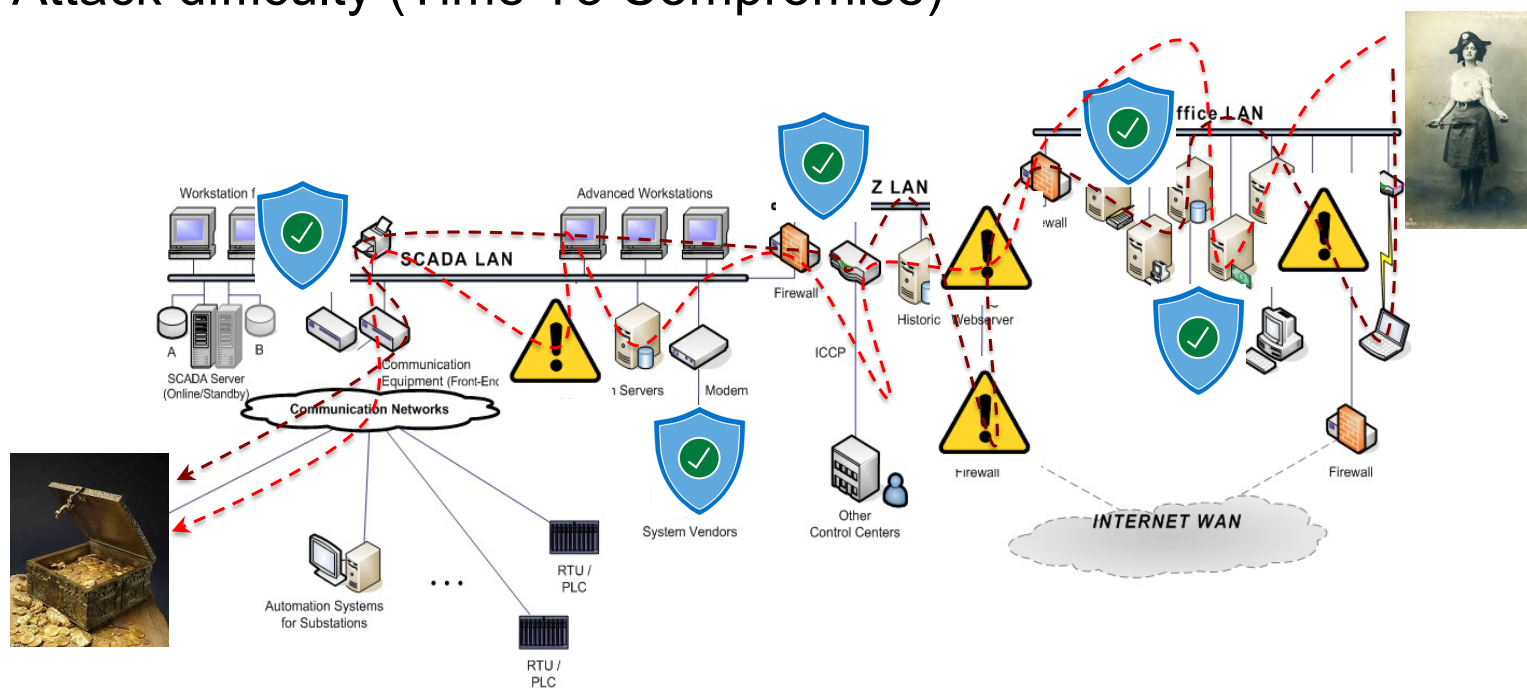
security architect (etc.)



Cybersecurity analysis of ICT infrastructures

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

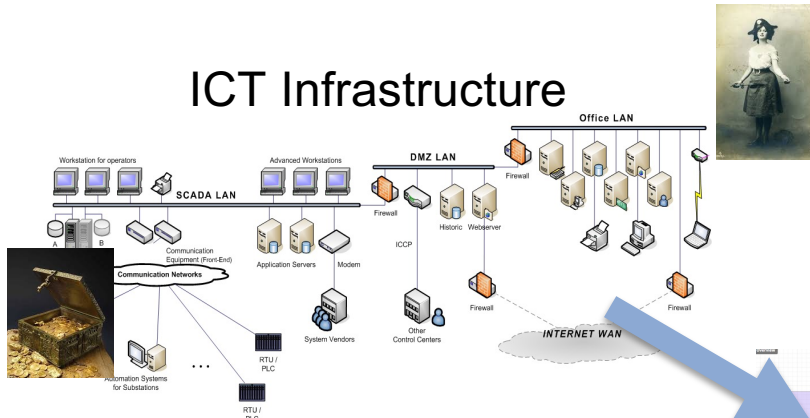
- Attack vector
- Attack difficulty (Time To Compromise)





Model-based cybersecurity analysis

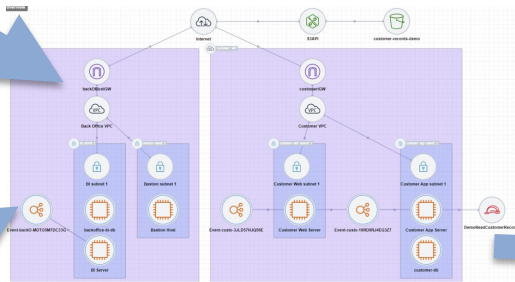
ICT Infrastructure



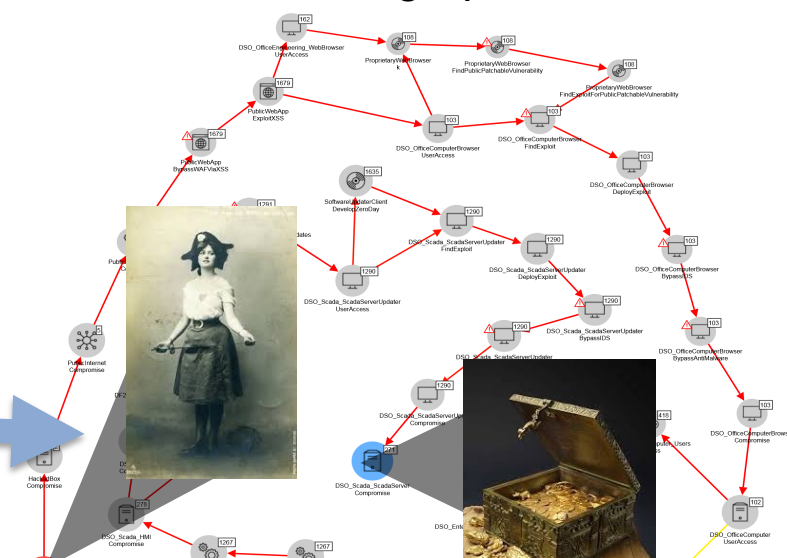
Domain Specific Language (Meta Attack Language)

```
asset ServiceMP2
info: "A service API... structures"
{
  create
  info: "An example service API... request for an... bucket."
}
{
  request
  -> transactRequest,
  transactResponse
  statistics: {lowPrivilegeAccounts V highPrivilegeAccounts} | DMRole, assume
}
transactRequest
->
// Interface subsets
let: subnets = ipRanges.superDMZanges+subnets,
// IP range services
// The union of ipRangesServices and ipRangesServices2 is used because of a bug in the old MML compiler
let: ipRangesServices = ipRanges(ipRangesDMZanges, networkInterface.services,
let: ipRangesServices2 = ipRanges(subDMZanges+subDMZanges(ipRangesDMZanges), networkInterface.services,
let: ipRangesServices = ipRangesServices1 V ipRangesServices2,
//let: ipRangesServices = ipRanges(subDMZanges+subDMZanges(ipRangesDMZanges), networkInterface.services,
// Part range services
let: portRangeServices = portRange(subDMZanges+services,
```

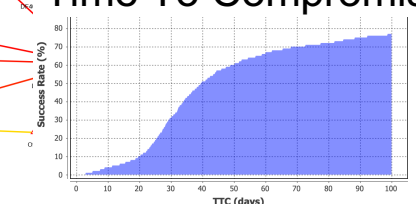
Domain Specific Model



Attack graph



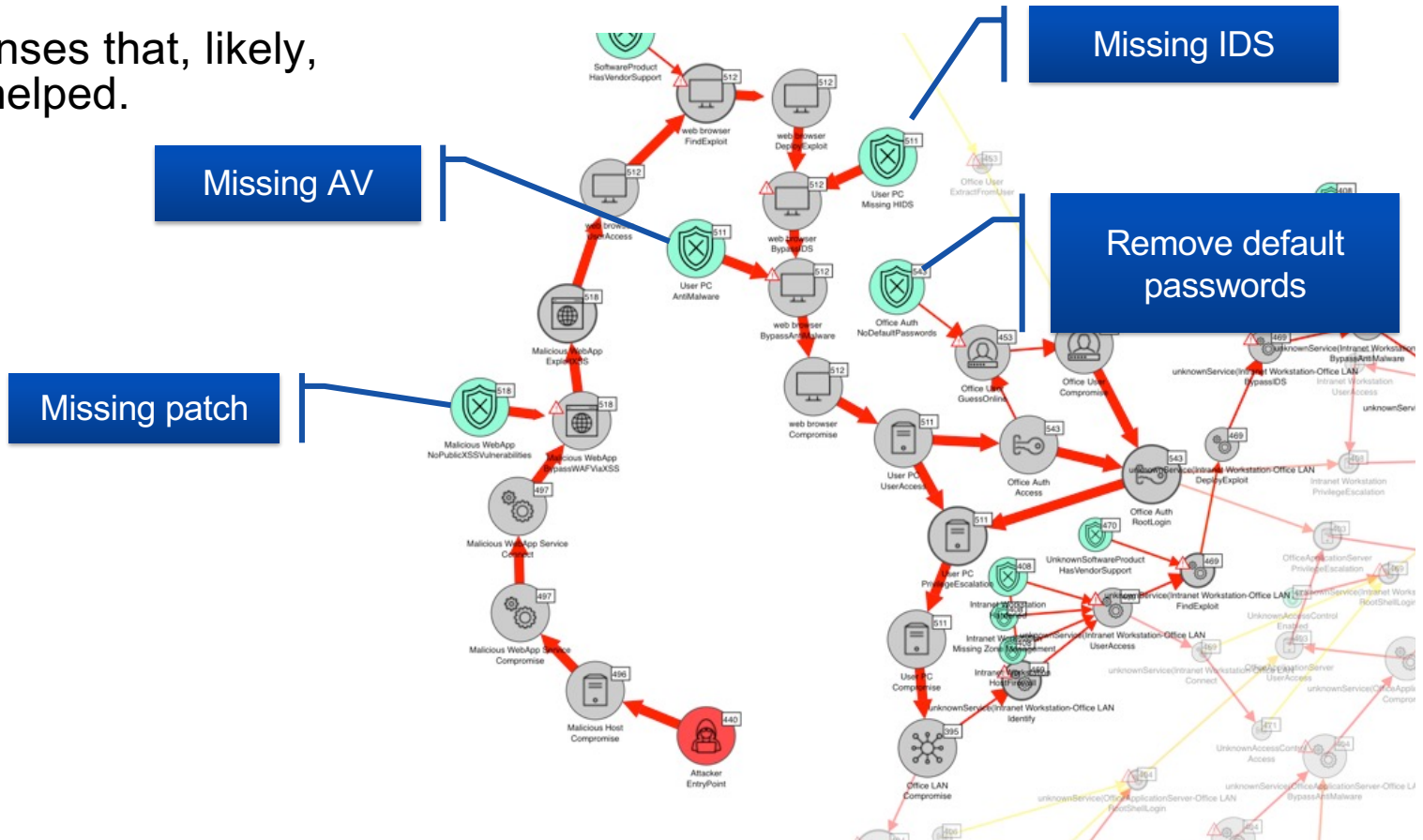
Time To Compromise





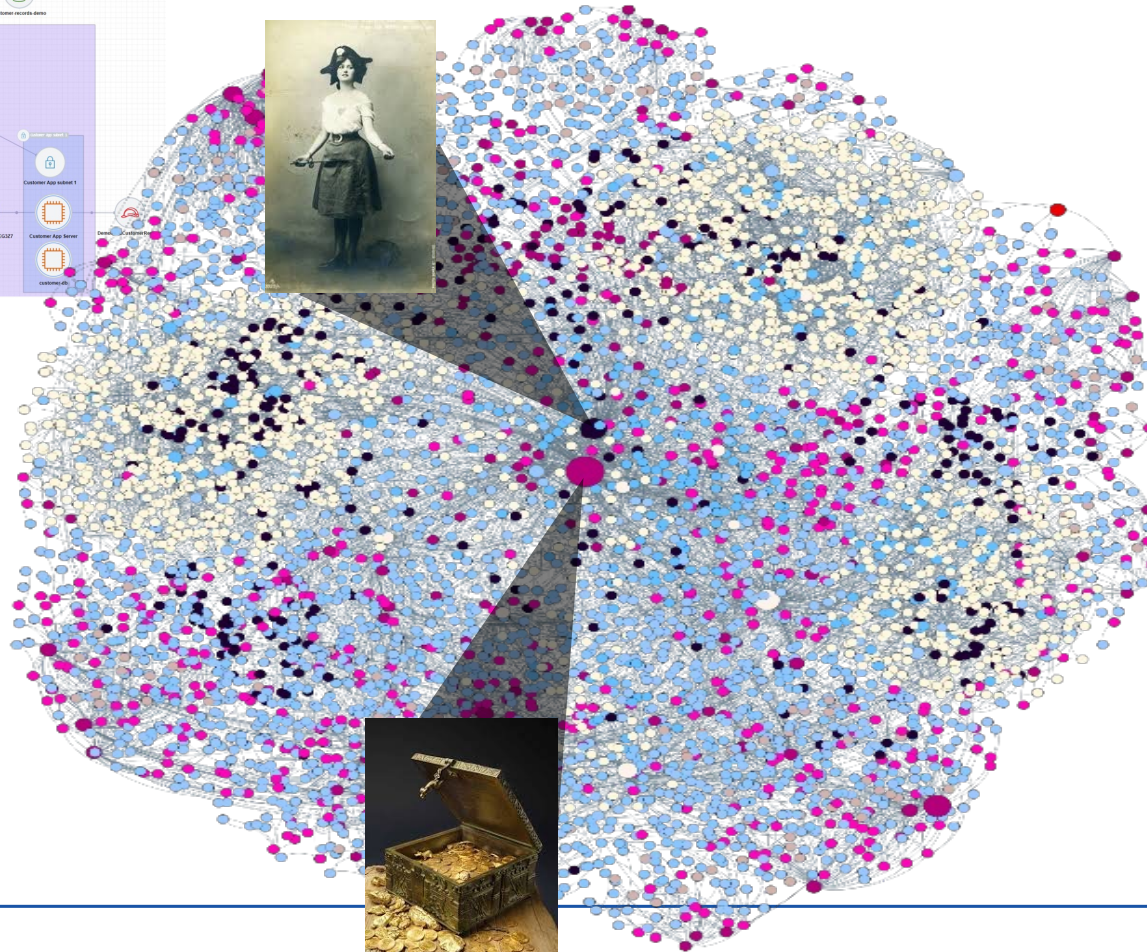
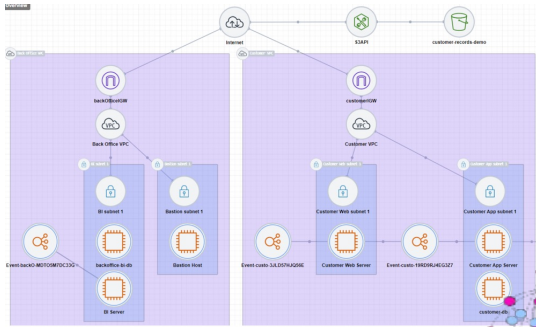
Aimed to serve as design support

Missing defenses that, likely, would have helped.

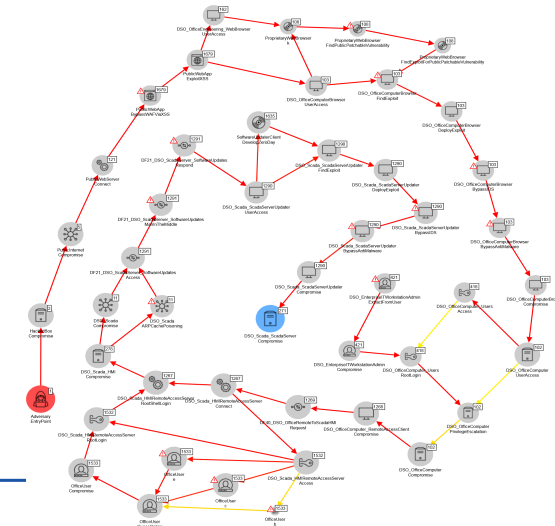




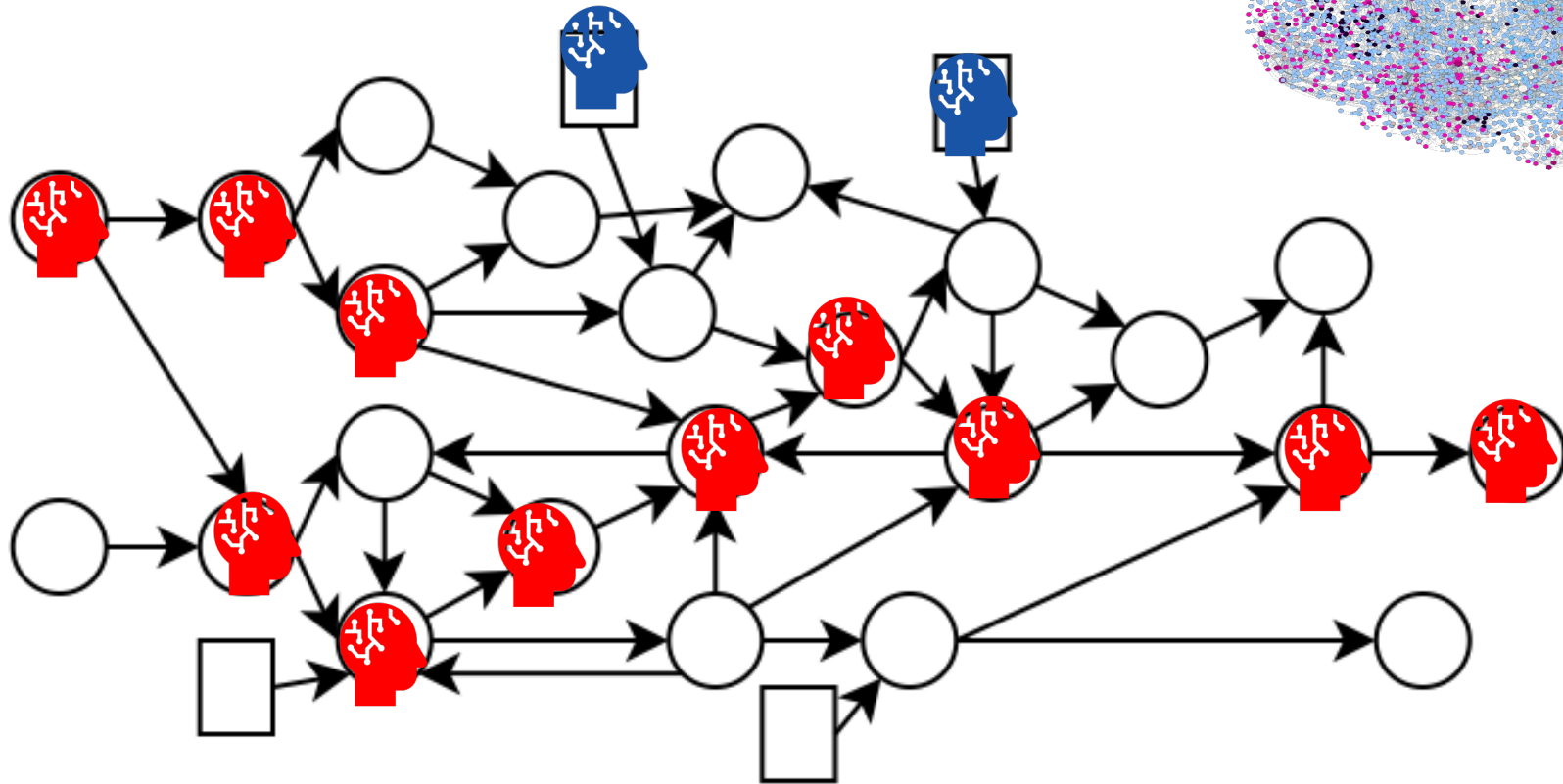
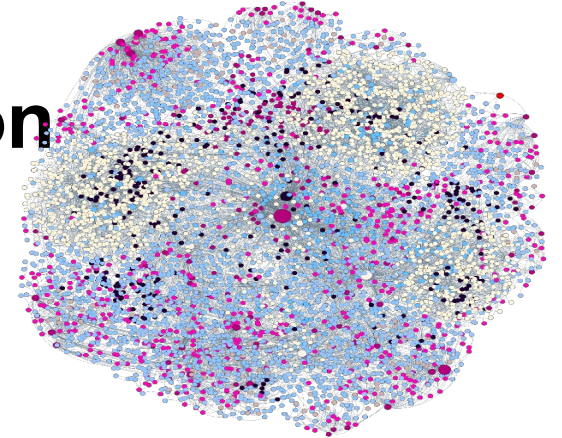
Attack graph generation and computation



(Monte Carlo based) shortest path calculation

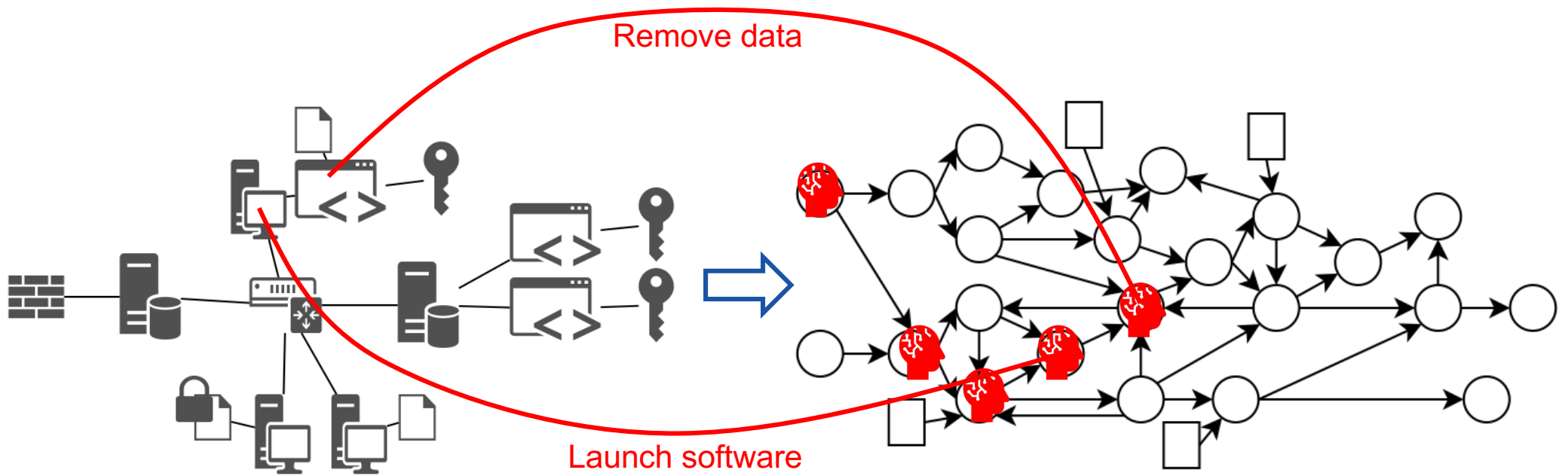


Agent- and game-oriented simulation

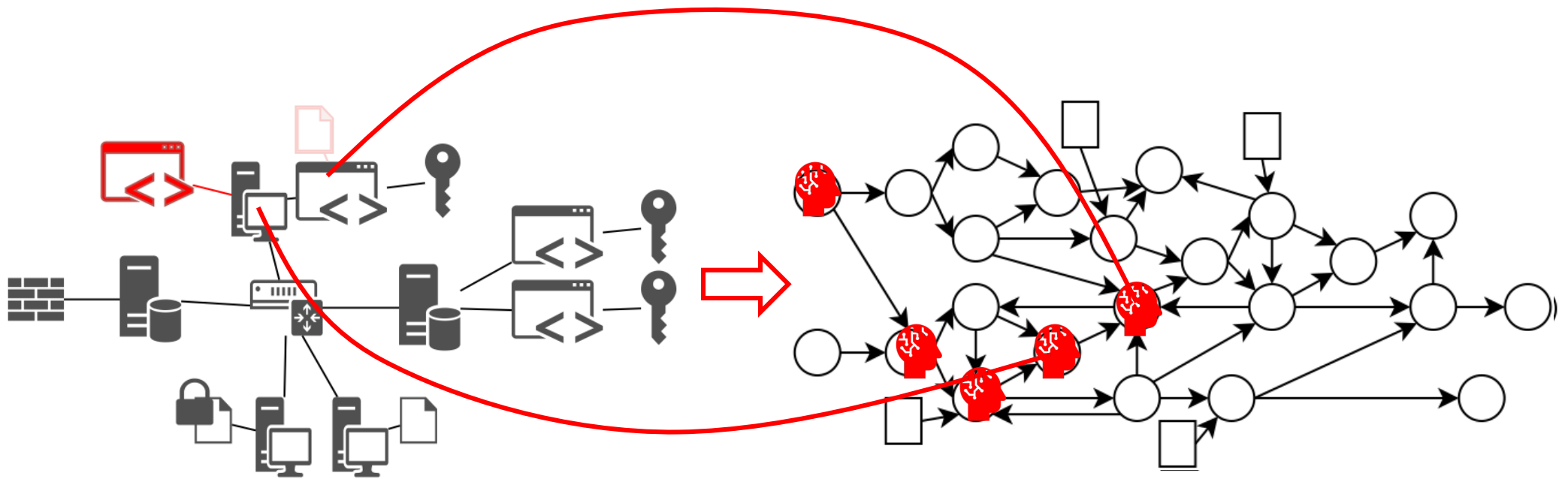




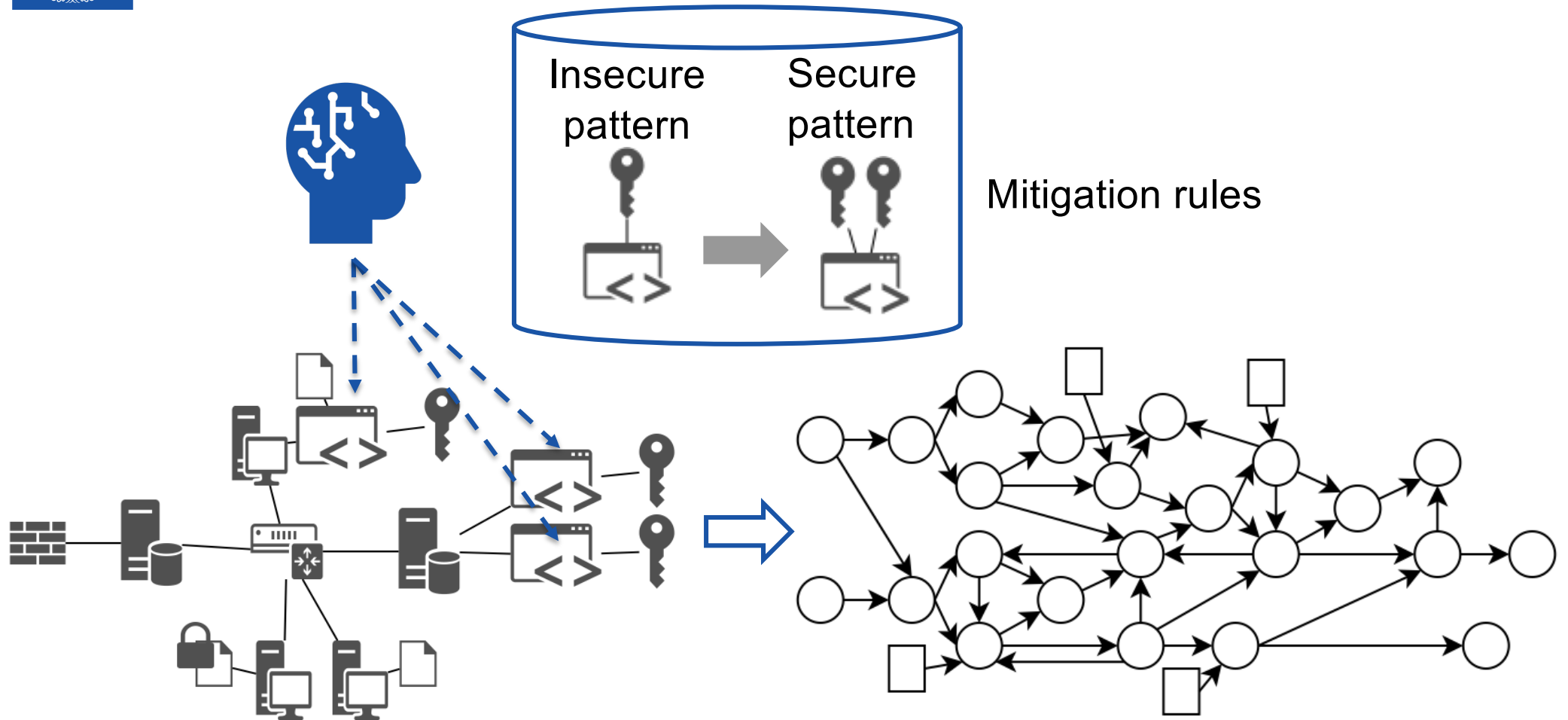
Structural changes



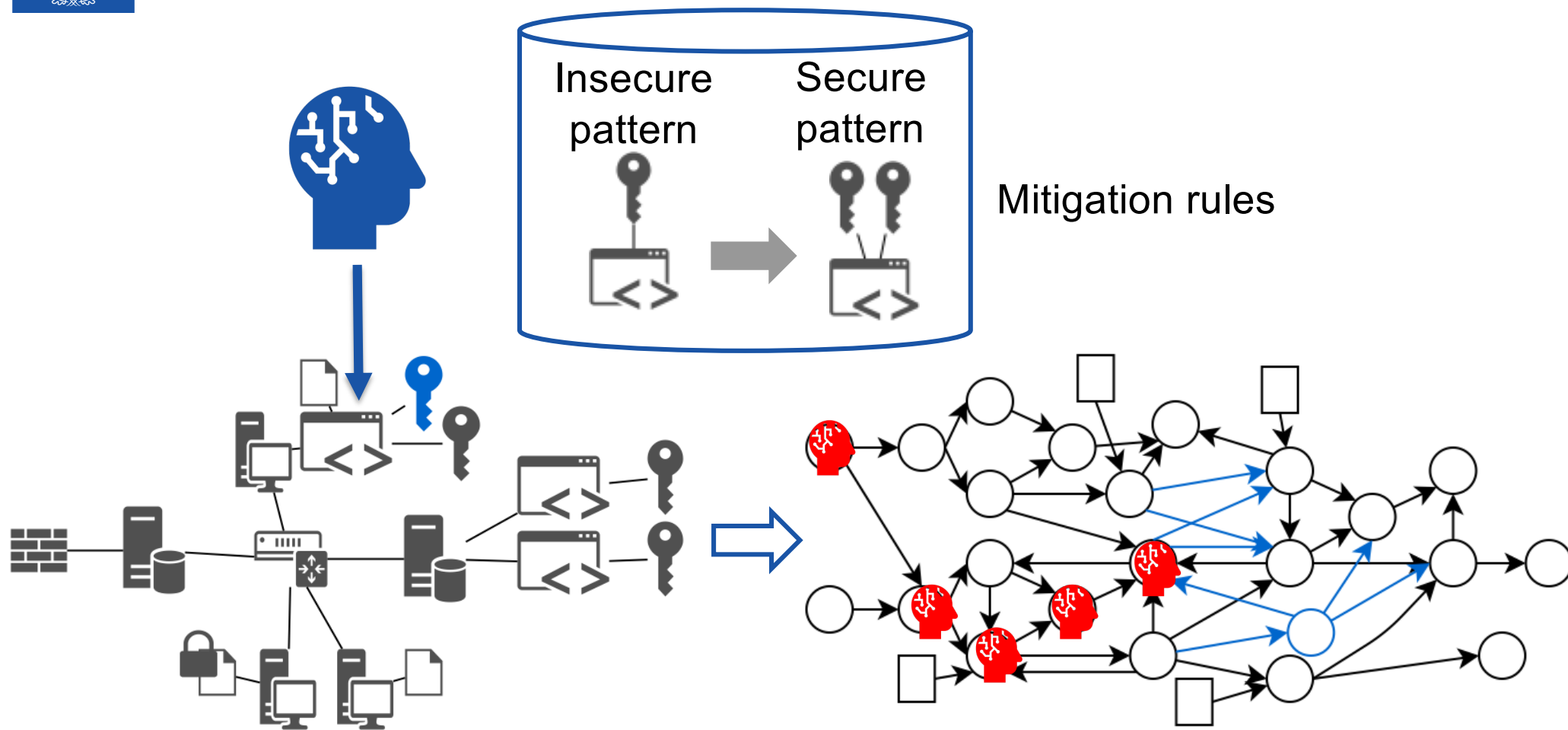
Structural changes



Also the defender can change structure

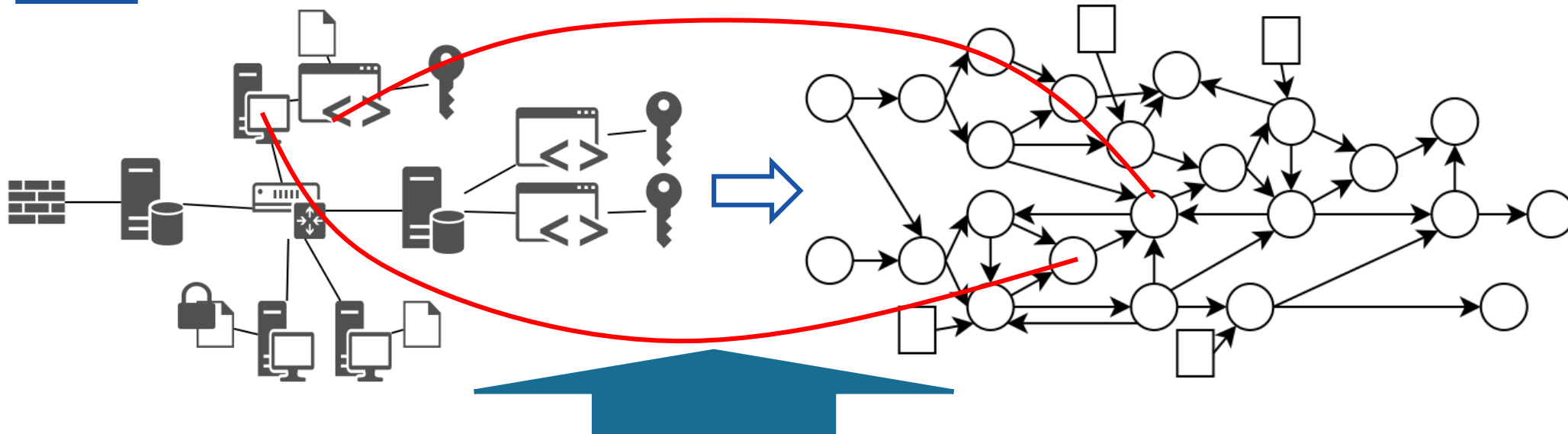


Also the defender can change structure





Extend formalism with dynamic structural change



Domain Specific Language

```
asset ServiceAPI
  info: "A service API is a mechanism for exposing the capabilities of a service infrastructure."
  {
  }
  invoke
  info: "An example service API invocation that requests a subject in an S3 bucket."
  }
}

//set NetworkInterface extends Request
// Interface is
let ipRanges = ipRanges.subnets

// IP range services
// The union of ipRangeServices1 and ipRangeServices2 is used because of a bug in the old MAL compiler
let ipRangeServices1 = ipRanges.privateRange1.networkInterface.services
let ipRangeServices2 = ipRanges.subIPRanges.subIPRanges.privateRange1.networkInterface.services
let ipRangeServices = ipRangeServices1 ∪ ipRangeServices2
//let ipRangeServices = (ipRanges.subIPRanges+privateRange1).networkInterface.services

// Port range services
let portRangeServices = portRange.subPortRanges+services
```

(Meta)Attack Language
DynaMAL



But why?

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