COORDINATED SCIENCE LABORATORY

ENGINEERING AT ILLINOIS

WiP: A Model-Based Approach for Quantitative Decision-Making in Cybersecurity Incident Response

Hoang Hai Nguyen (Frank), Kartik Palani, David M. Nicol
University of Illinois at Urbana-Champaign

HoTSoS Special Session on Work-in-Progress
April 5-7, 2022

ITI.ILLINOIS.EDU

INFORMATION TRUST INSTITUTE

Cybersecurity incident response (CSIR)

Network breaches are **inevitable**

"widespread recognition that some of these cybersecurity (cyber) events ***cannot be stopped****."* [NIST2016]

[Ponnemon2014] Cyber Security Incident Response: Are we as prepared as we think?
[NIST2016] SP 800-184 Guide for Cybersecurity Event Recovery..
[Onwubiko2020] SOTER: A Playbook for Cybersecurity Incident Management, *Transactions on Engineering Management*.
[Smith2021] The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework, *Computer & Security.*
[Spring2021] Review of Human Decision-making during Computer Security Incident Analysis. *Digital Threats: Research and Practice.*
[MarketWatch] https://www.marketwatch.com/press-release/incident-response-market-size-volume-share-demand-growth-business-opportunity-by-2023-trending-report-2022-01-10, *Last access: March 23, 2022*

Cybersecurity incident response (CSIR)

Network breaches are **inevitable**

*"widespread recognition that some of these cybersecurity (cyber) events **cannot be stopped**."* [NIST2016]

Incident response helps **control the damage** after the breach

68% agreed that *"the **best thing that their organizations could do** to mitigate future breaches is to **improve their incident response capabilities**."* [Ponemon2014]

*"global incident response market size to grow from **USD 13.38 billion** in 2018 to **USD 33.76 billion** by 2023, at a Compound Annual Growth Rate (CAGR) of **20.3%**"* [MarketWatch]

[Ponemon2014] Cyber Security Incident Response: Are we as prepared as we think?
[NIST2016] SP 800-184 Guide for Cybersecurity Event Recovery..
[Onwubiko2020] SOTER: A Playbook for Cybersecurity Incident Management, *Transactions on Engineering Management*.
[Smith2021] The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework, *Computer & Security*.
[Spring2021] Review of Human Decision-making during Computer Security Incident Analysis. *Digital Threats: Research and Practice*.
[MarketWatch] https://www.marketwatch.com/press-release/incident-response-market-size-volume-share-demand-growth-business-opportunity-by-2023-trending-report-2022-01-10, *Last access: March 23, 2022*

Cybersecurity incident response (CSIR)

Network breaches are **inevitable**

*"widespread recognition that some of these cybersecurity (cyber) events **cannot be stopped**."* [NIST2016]

Incident response helps **control the damage** after the breach

68% agreed that *"the **best thing that their organizations could do** to mitigate future breaches is to **improve their incident response capabilities**."* [Ponemon2014]

*"global incident response market size to grow from **USD 13.38 billion** in 2018 to **USD 33.76 billion** by 2023, at a Compound Annual Growth Rate (CAGR) of **20.3%**"* [MarketWatch]

Incident response relies on **playbooks**

*" **incomplete**, **untested**, and **not fit for purpose**"* [Onwubiko2020]

*"**overly prescriptive**, **slow to change,** and often suffer from a **lack of responsible oversight**."* [Smith2021]

*"there are no existing CSIR standards that provide advice on **which analysis heuristic or tool to use at one time** or **in what situation**, given **limited analyst resources**."* [Spring2021]

[Ponemon2014] Cyber Security Incident Response: Are we as prepared as we think?
[NIST2016] SP 800-184 Guide for Cybersecurity Event Recovery..
[Onwubiko2020] SOTER: A Playbook for Cybersecurity Incident Management, *Transactions on Engineering Management*.
[Smith2021] The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework, *Computer & Security*.
[Spring2021] Review of Human Decision-making during Computer Security Incident Analysis. *Digital Threats: Research and Practice*.
[MarketWatch] https://www.marketwatch.com/press-release/incident-response-market-size-volume-share-demand-growth-business-opportunity-by-2023-trending-report-2022-01-10, *Last access: March 23, 2022*

Background

Threat model: cyber kill chain [LockheedMartin] [SANS2015]

- Gain **initial access** to the network
- Propagate in the network via **lateral movement**

[LockheedMartin] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, *Last access: March 23, 2022.*
[NIST2012] SP 800-61 Rev2 Computer Security Incident Handling Guide.
[SANS2015] The industrial control system cyber kill chain.
[NERC/FERC2020] Cyber planning for response and recovery report (CYPRES).
[CISA2021] Cybersecurity incident & vulnerability response playbooks.

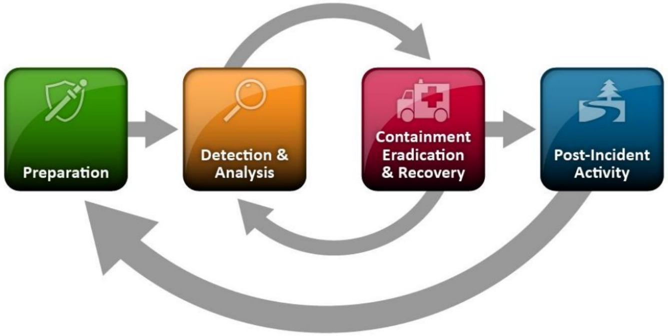
Background

Threat model: cyber kill chain [LockheedMartin] [SANS2015]

- Gain **initial access** to the network
- Propagate in the network via **lateral movement**

Defense model [NIST2012] [CISA2021]

- Confirm **security incident** took place
- **Scope** the attack
- **Contain**, **eradicate**, and **restore**
- Perform **post-incident analysis**



Incident response life cycle [NIST2012]

[LockheedMartin] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, *Last access: March 23, 2022.*
[NIST2012] SP 800-61 Rev2 Computer Security Incident Handling Guide.
[SANS2015] The industrial control system cyber kill chain.
[NERC/FERC2020] Cyber planning for response and recovery report (CYPRES).
[CISA2021] Cybersecurity incident & vulnerability response playbooks.

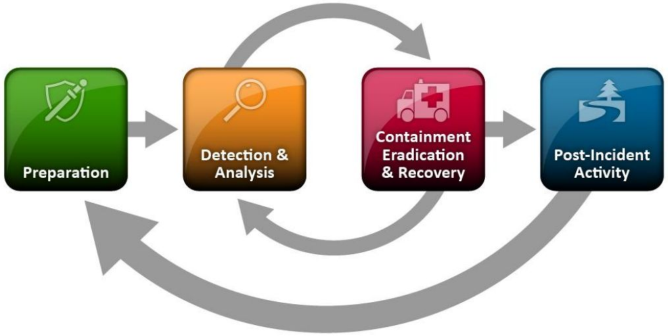
Background

Threat model: cyber kill chain [LockheedMartin] [SANS2015]

- Gain **initial access** to the network
- Propagate in the network via **lateral movement**

Defense model [NIST2012] [CISA2021]

- Confirm **security incident** took place
- **Scope** the attack
- **Contain**, **eradicate**, and **restore**
- Perform **post-incident analysis**



Incident response life cycle [NIST2012]

Key challenges: information uncertainty and **resource allocation**

- Security observations are **noisy**, **incomplete**, and **contradictory**
- **Quick response** may be suboptimal [NERC/FERC2020]
- **Delayed containment** is dangerous [NIST2012]

[LockheedMartin] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, *Last access: March 23, 2022.*
[NIST2012] SP 800-61 Rev2 Computer Security Incident Handling Guide.
[SANS2015] The industrial control system cyber kill chain.
[NERC/FERC2020] Cyber planning for response and recovery report (CYPRES).
[CISA2021] Cybersecurity incident & vulnerability response playbooks.

Research questions (RQs)

During incident response, defenders need to answer the following questions:

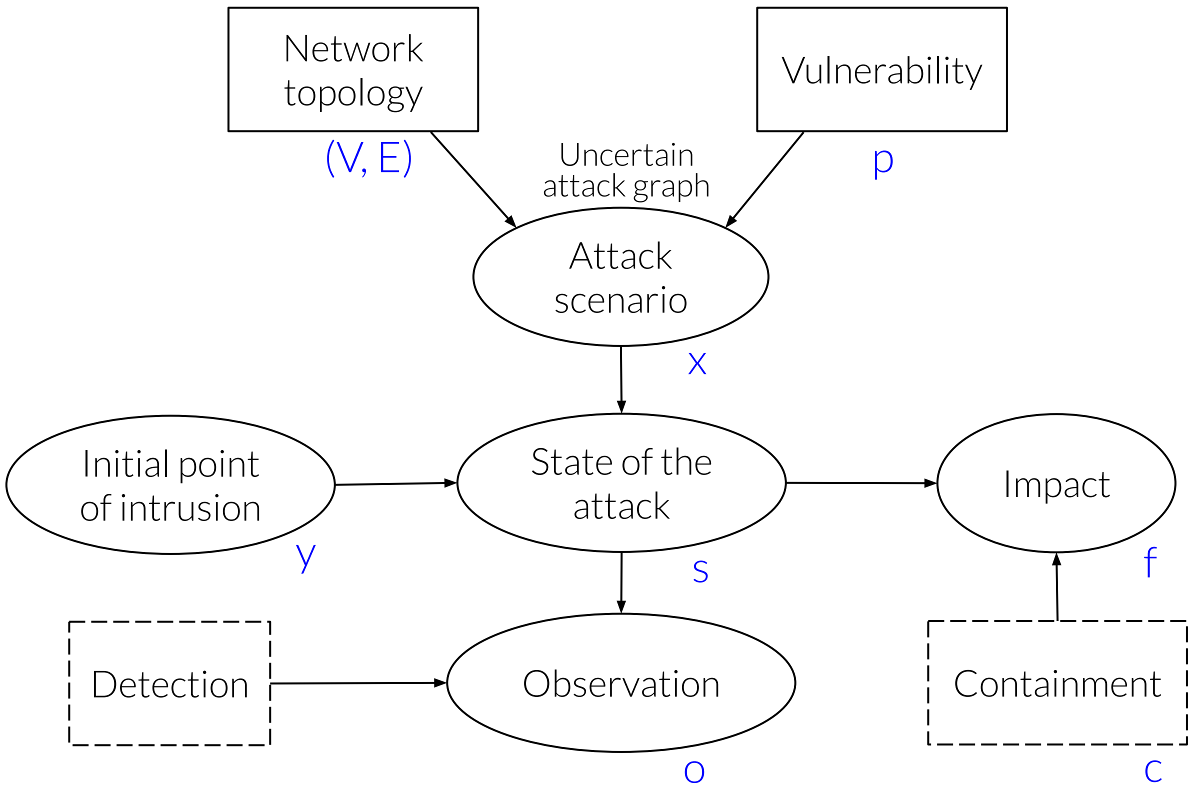
(**RQ1**) What is the **probability of compromise** of the network hosts?

(**RQ2**) What is the containment strategy that **minimizes the overall impact**?

(RQ3) At a given moment, whether to continue the **investigation** or proceed to the **containment**?

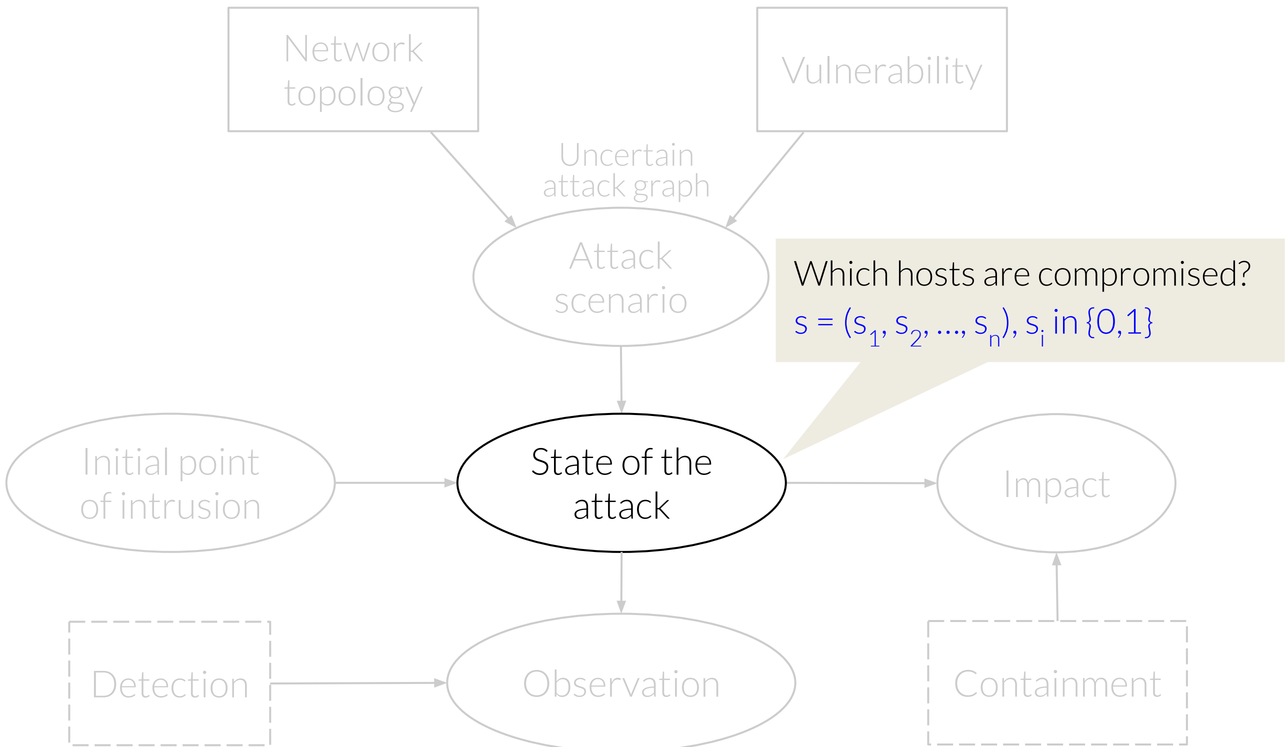
(**RQ4**) If the answer to **RQ3** is to continue the investigation, then **which host should be inspected, using which security tool**, to yield the optimal outcome?

Static incident response model



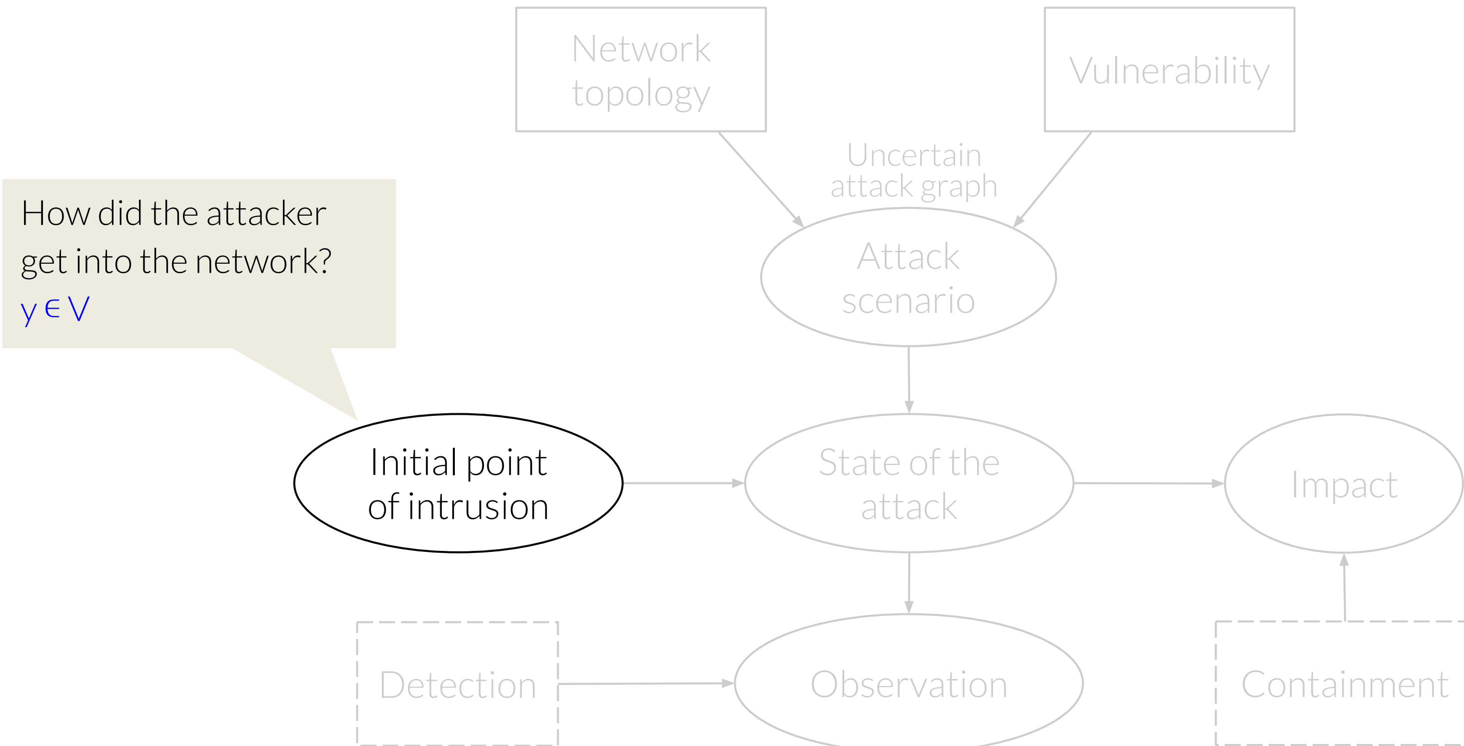
*Relationships between the **basic components** of a **static IR model**. Ovals represent **known unknowns**, solid rectangles represent **known knowns,** and dashed rectangles represent **defense decisions**.*

Static incident response model



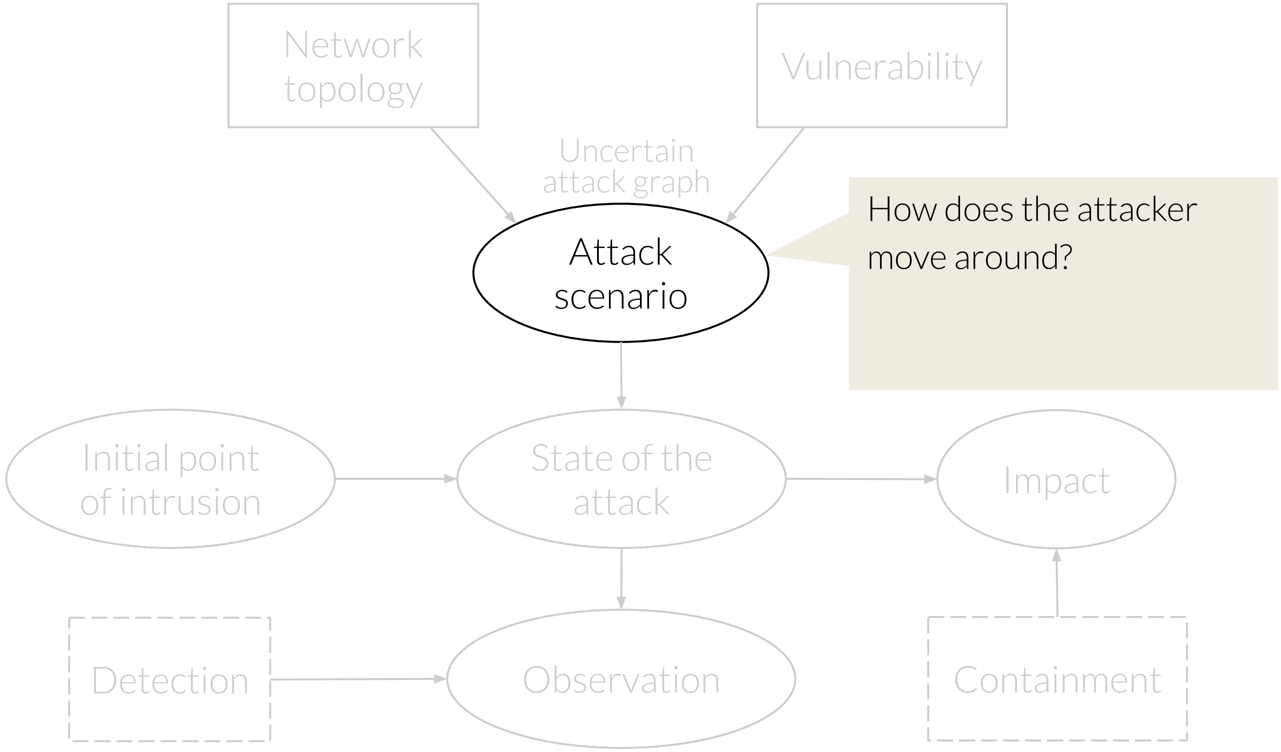
*Relationships between the **basic components** of a **static IR model**. Ovals represent **known unknowns**, solid rectangles represent **known knowns,** and dashed rectangles represent **defense decisions**.*

Static incident response model



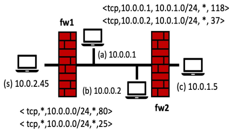
Relationships between the ***basic components*** *of a* ***static IR model****. Ovals represent* ***known unknowns****, solid rectangles represent* ***known knowns,*** *and dashed rectangles represent* ***defense decisions****.*

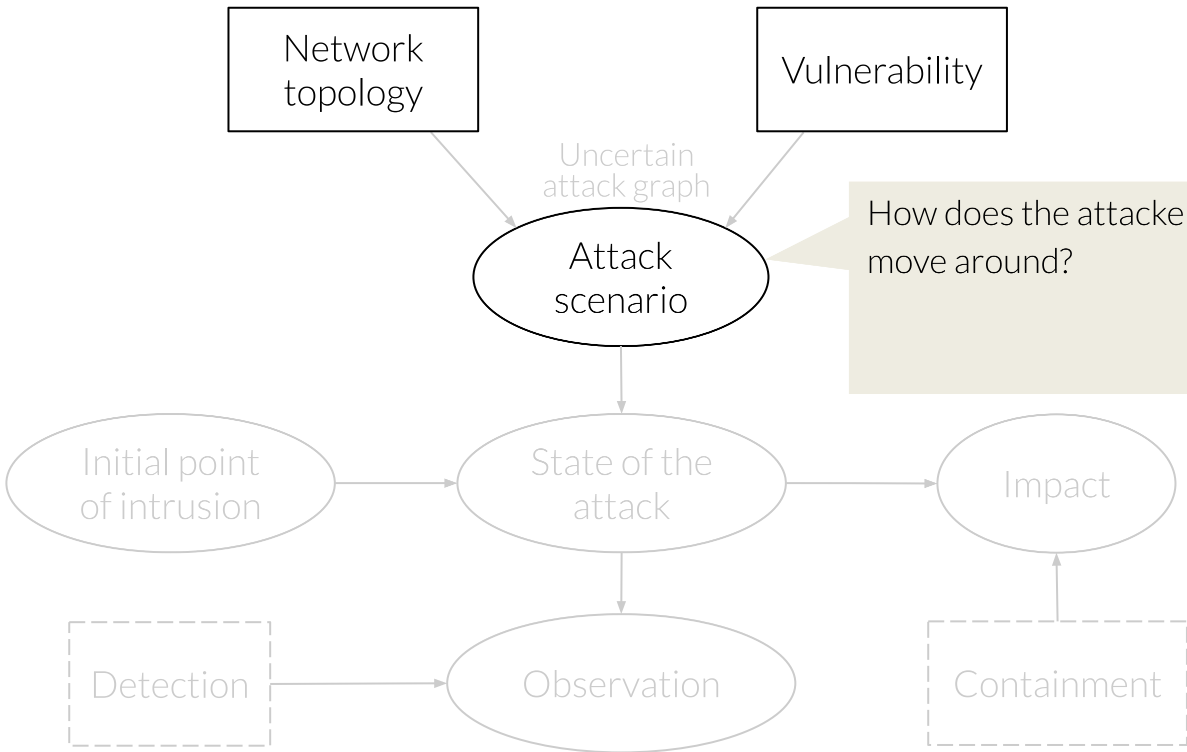
Static incident response model



*Relationships between the **basic components** of a **static IR model**. Ovals represent **known unknowns**, solid rectangles represent **known knowns,** and dashed rectangles represent **defense decisions**.*

Static incident response model

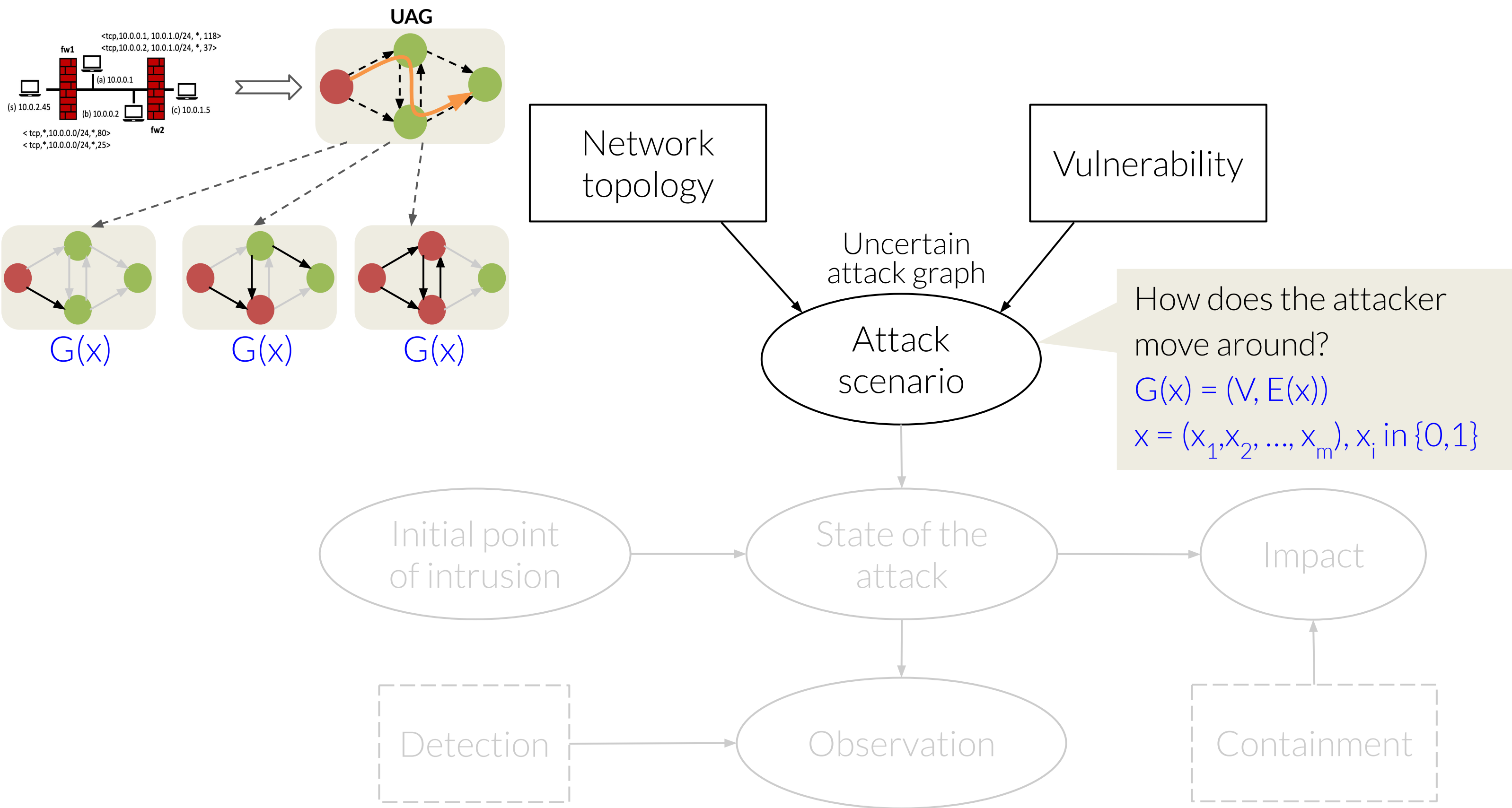




How does the attacker move around?

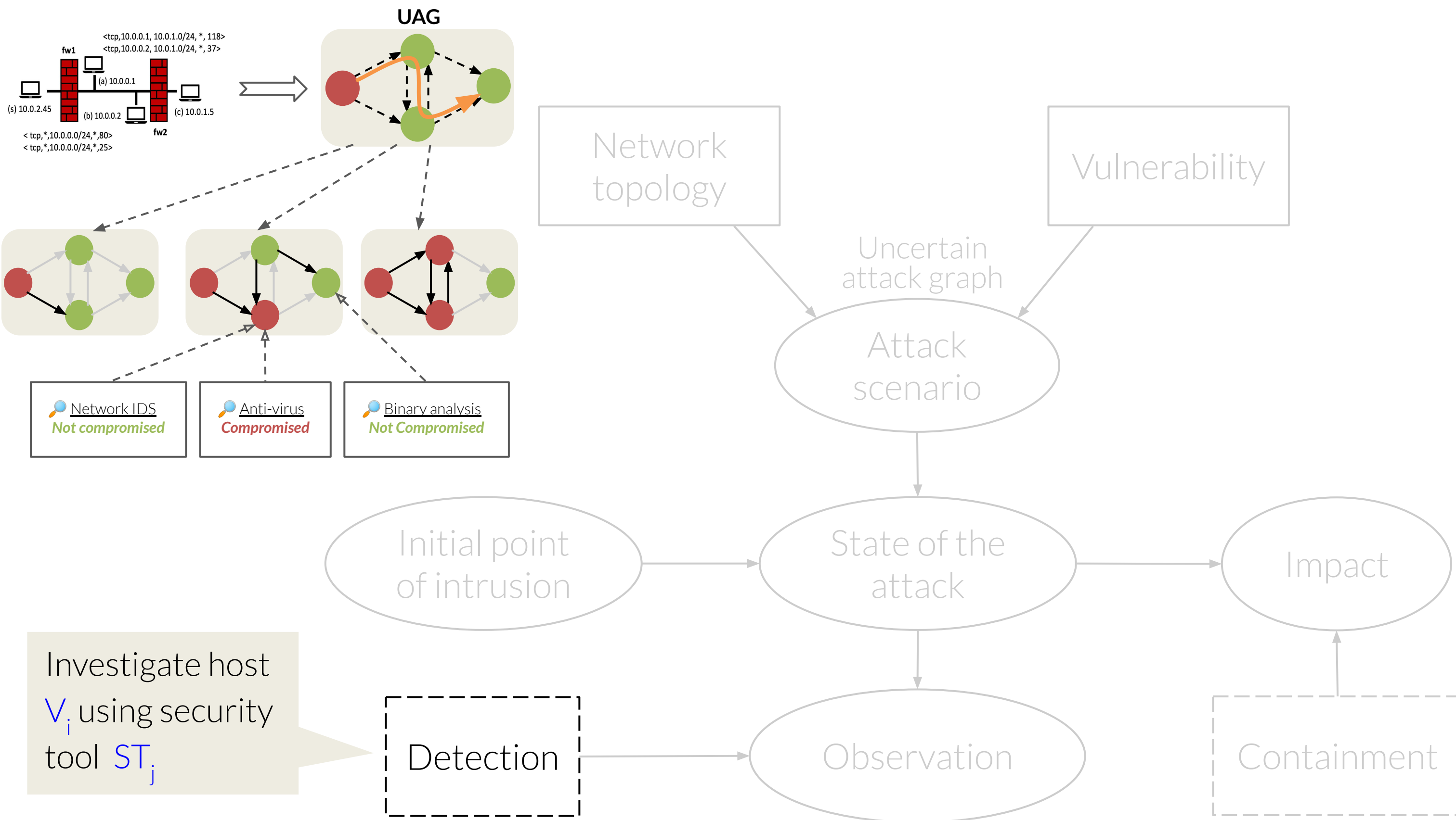
Relationships between the ***basic components*** *of a* ***static IR model****. Ovals represent* ***known unknowns****, solid rectangles represent* ***known knowns,*** *and dashed rectangles represent* ***defense decisions****.*

Static incident response model



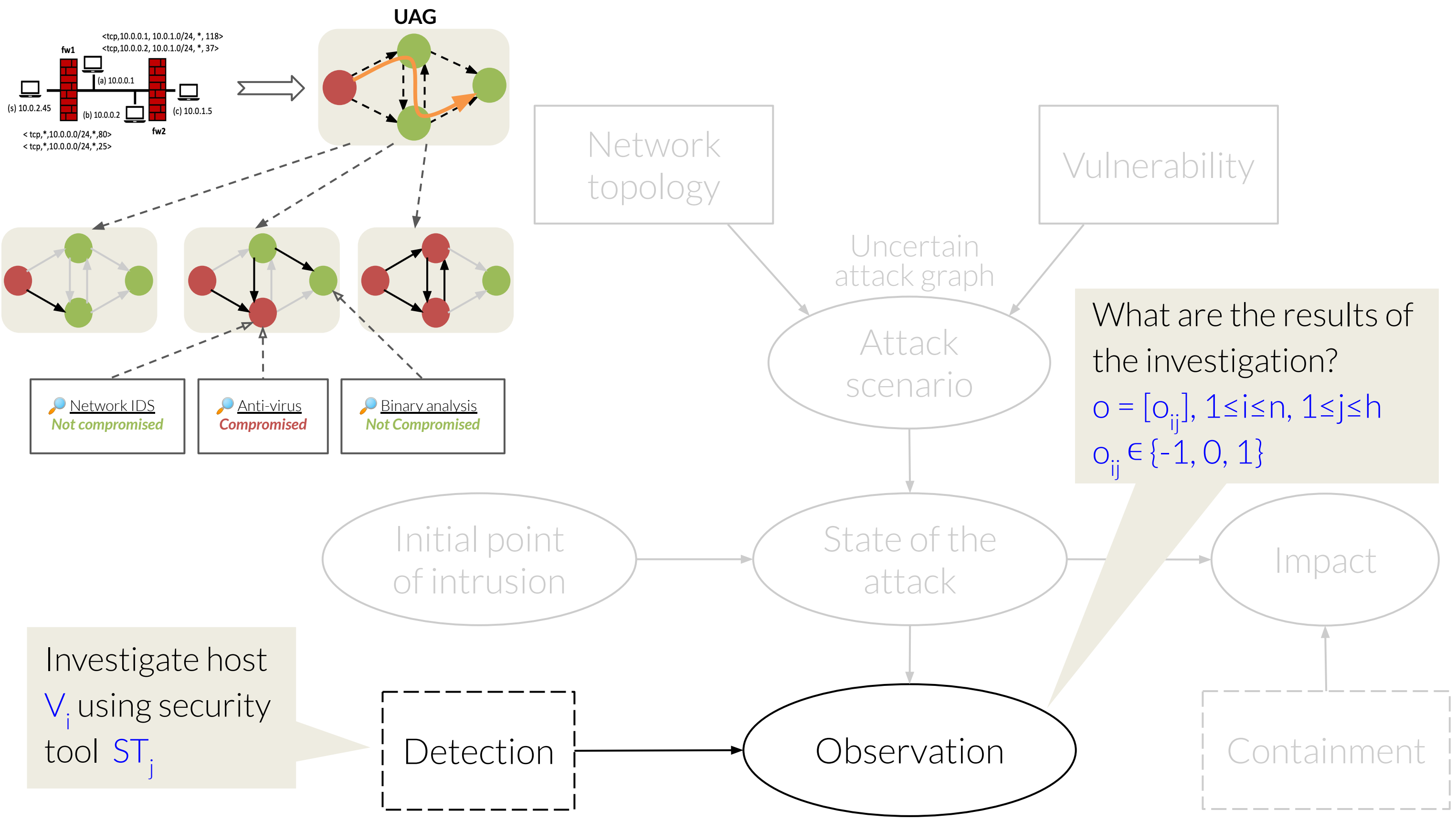
*Relationships between the **basic components** of a **static IR model**. Ovals represent **known unknowns**, solid rectangles represent **known knowns,** and dashed rectangles represent **defense decisions**.*

Static incident response model



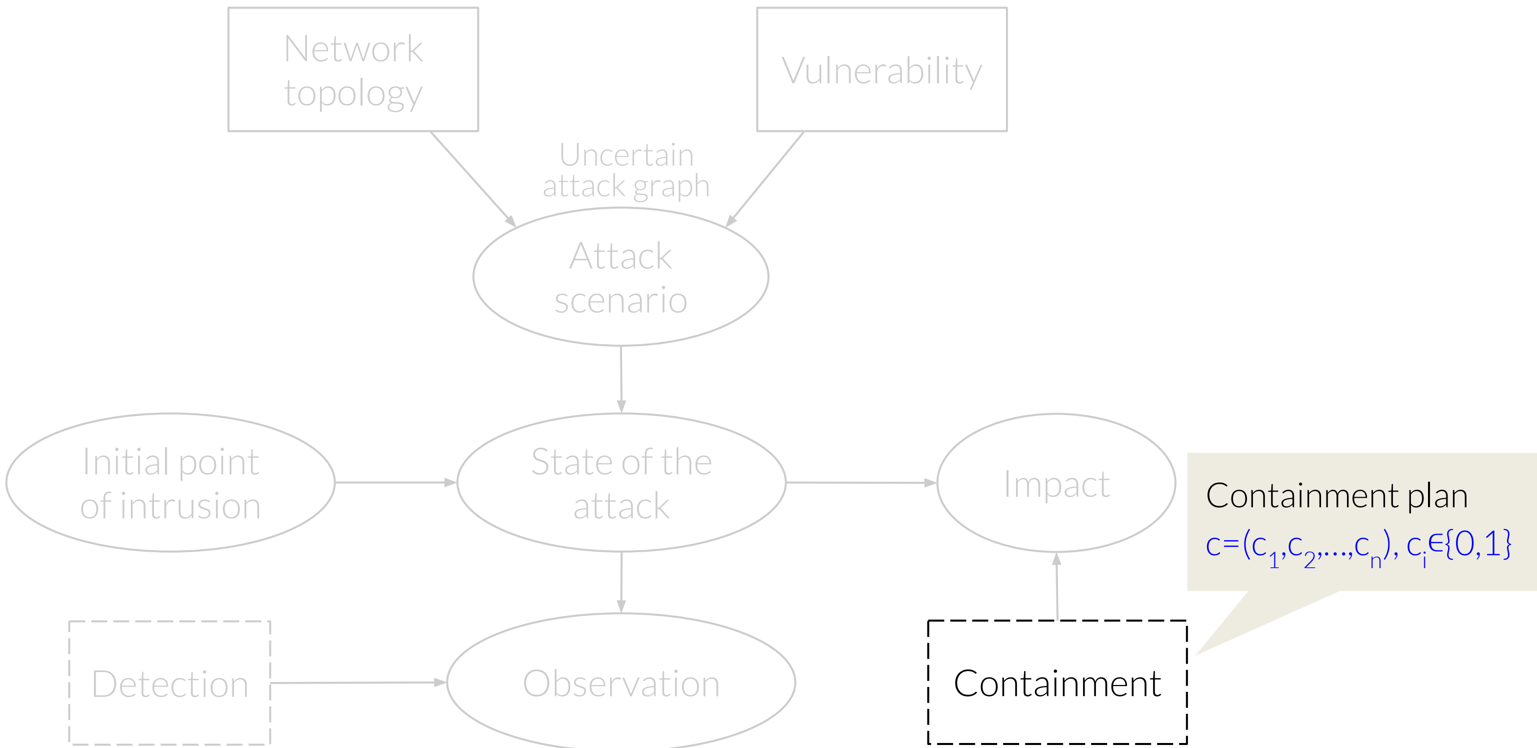
Relationships between the ***basic components*** *of a* ***static IR model****. Ovals represent* ***known unknowns****, solid rectangles represent* ***known knowns,*** *and dashed rectangles represent* ***defense decisions****.*

Static incident response model



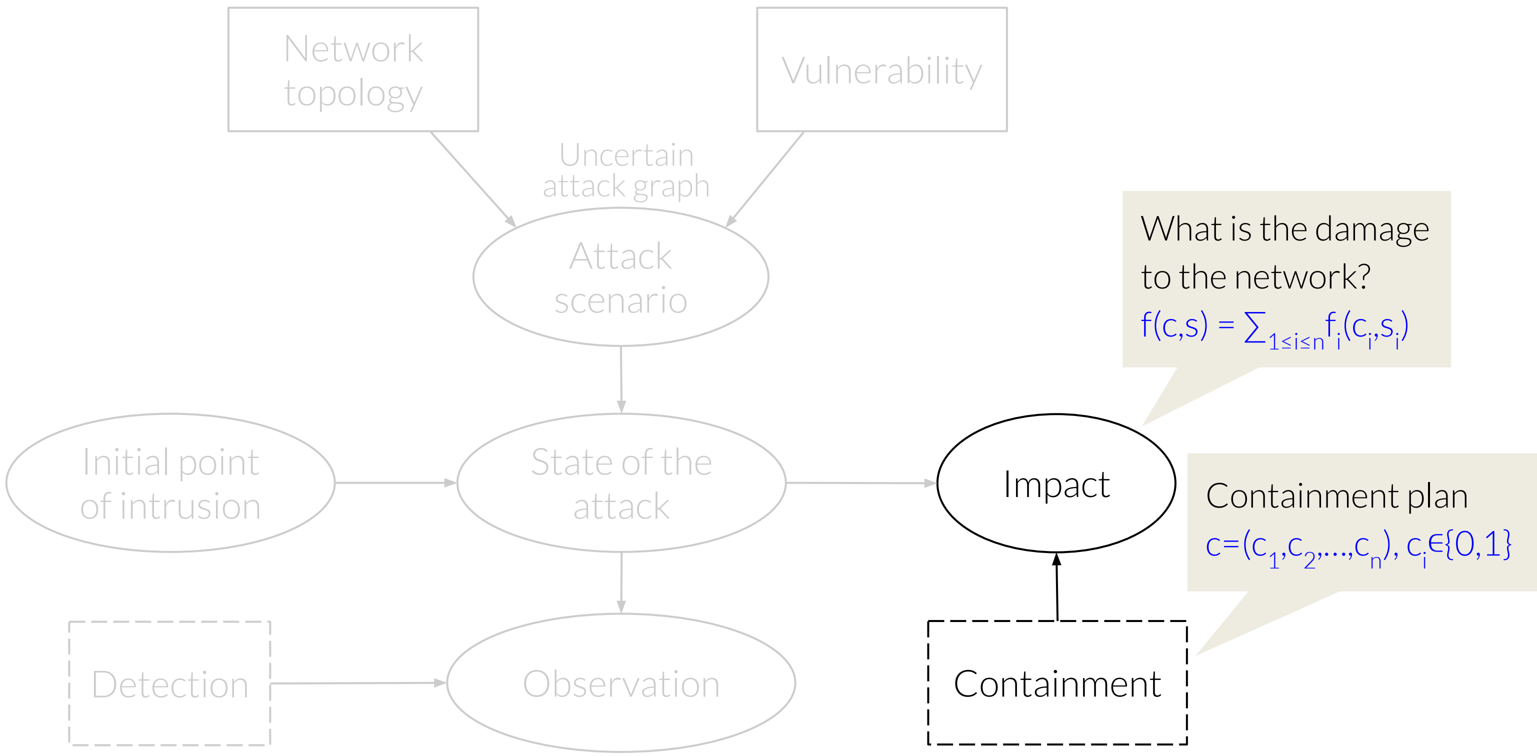
*Relationships between the **basic components** of a **static IR model**. Ovals represent **known unknowns**, solid rectangles represent **known knowns,** and dashed rectangles represent **defense decisions**.*

Static incident response model



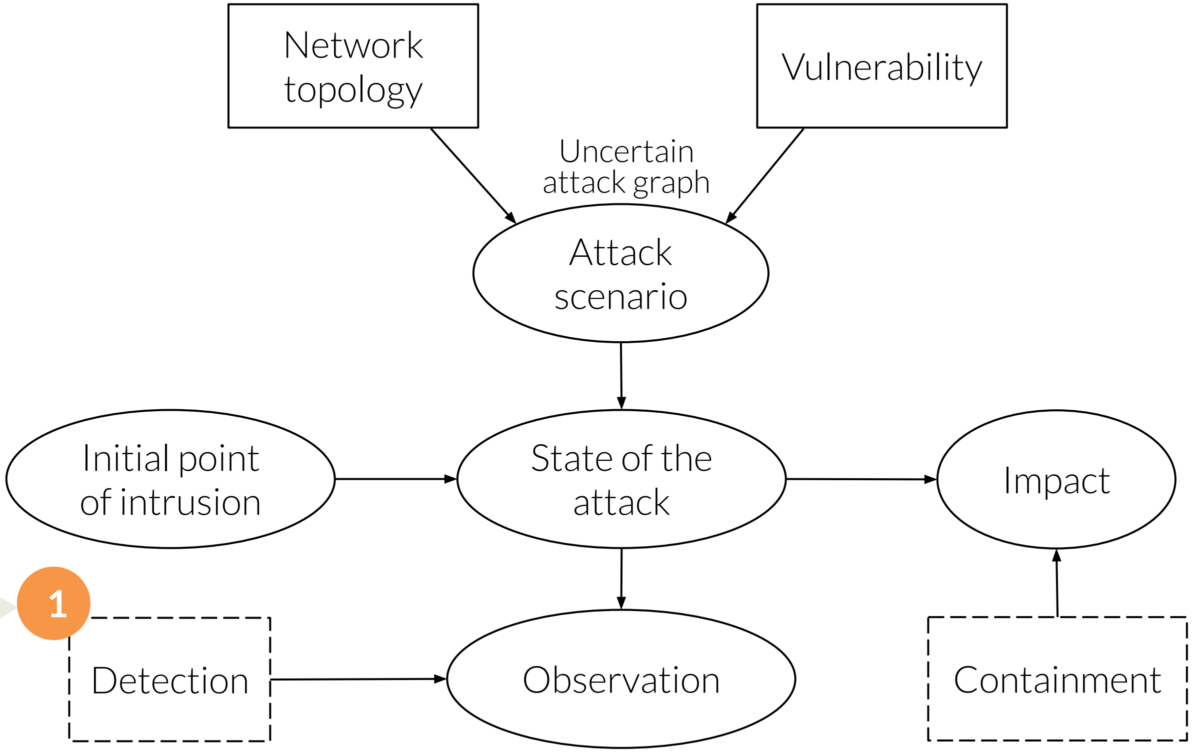
*Relationships between the **basic components** of a **static IR model**. Ovals represent **known unknowns**, solid rectangles represent **known knowns,** and dashed rectangles represent **defense decisions**.*

Static incident response model



Relationships between the ***basic components*** *of a* ***static IR model****. Ovals represent* ***known unknowns****, solid rectangles represent* ***known knowns,*** *and dashed rectangles represent* ***defense decisions****.*

Incident response process

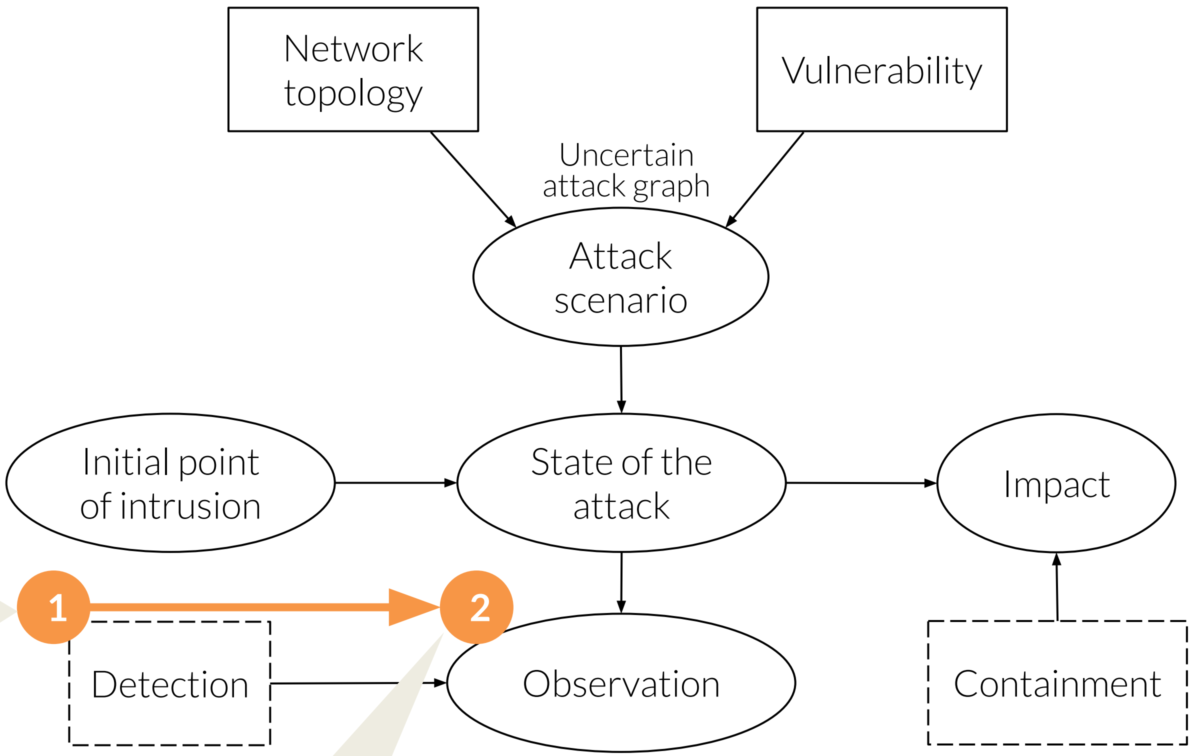


Optimal detection policy

1. V_{i1}, ST_{j1}
2. V_{i2}, ST_{j2}

…

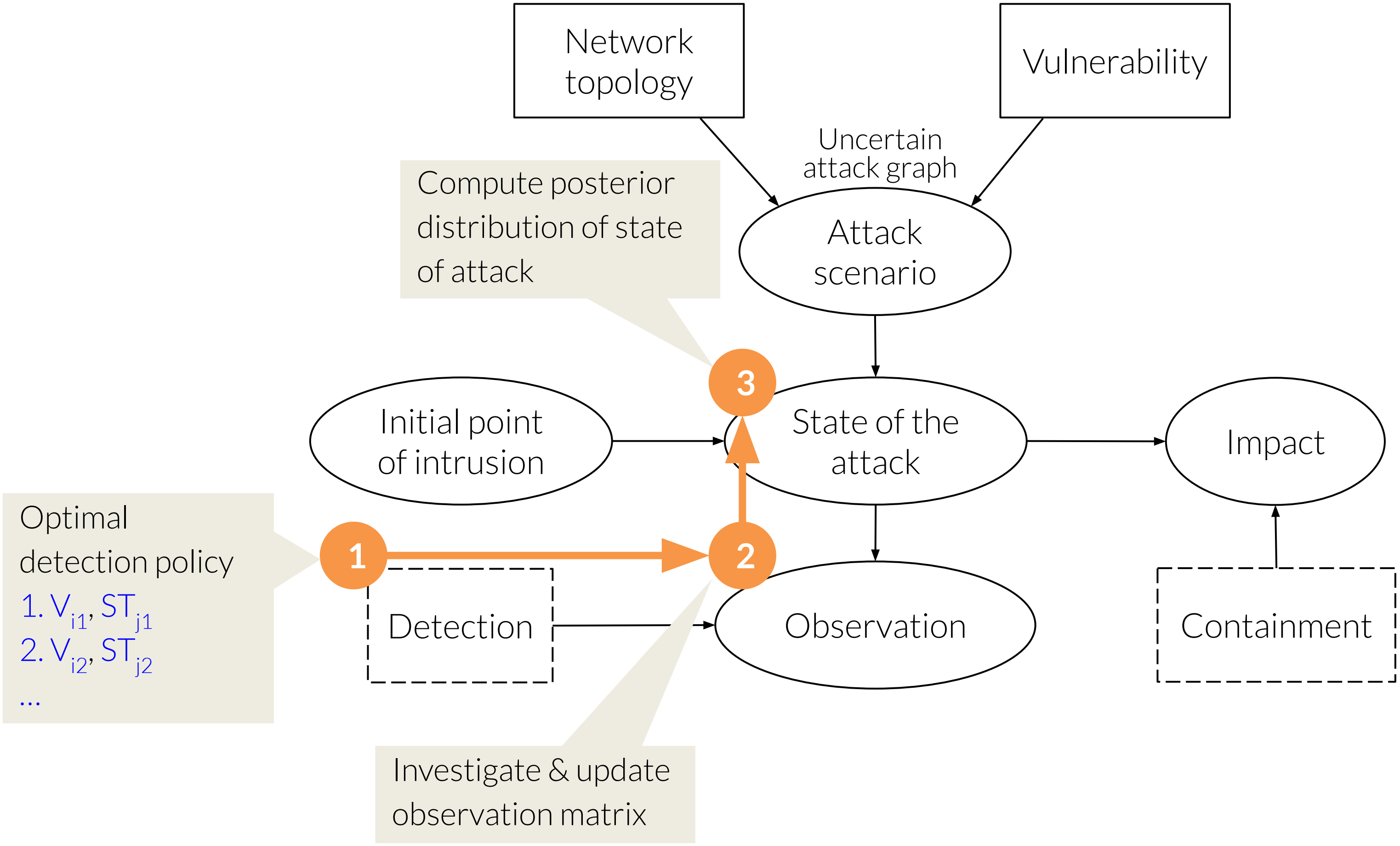
Incident response process



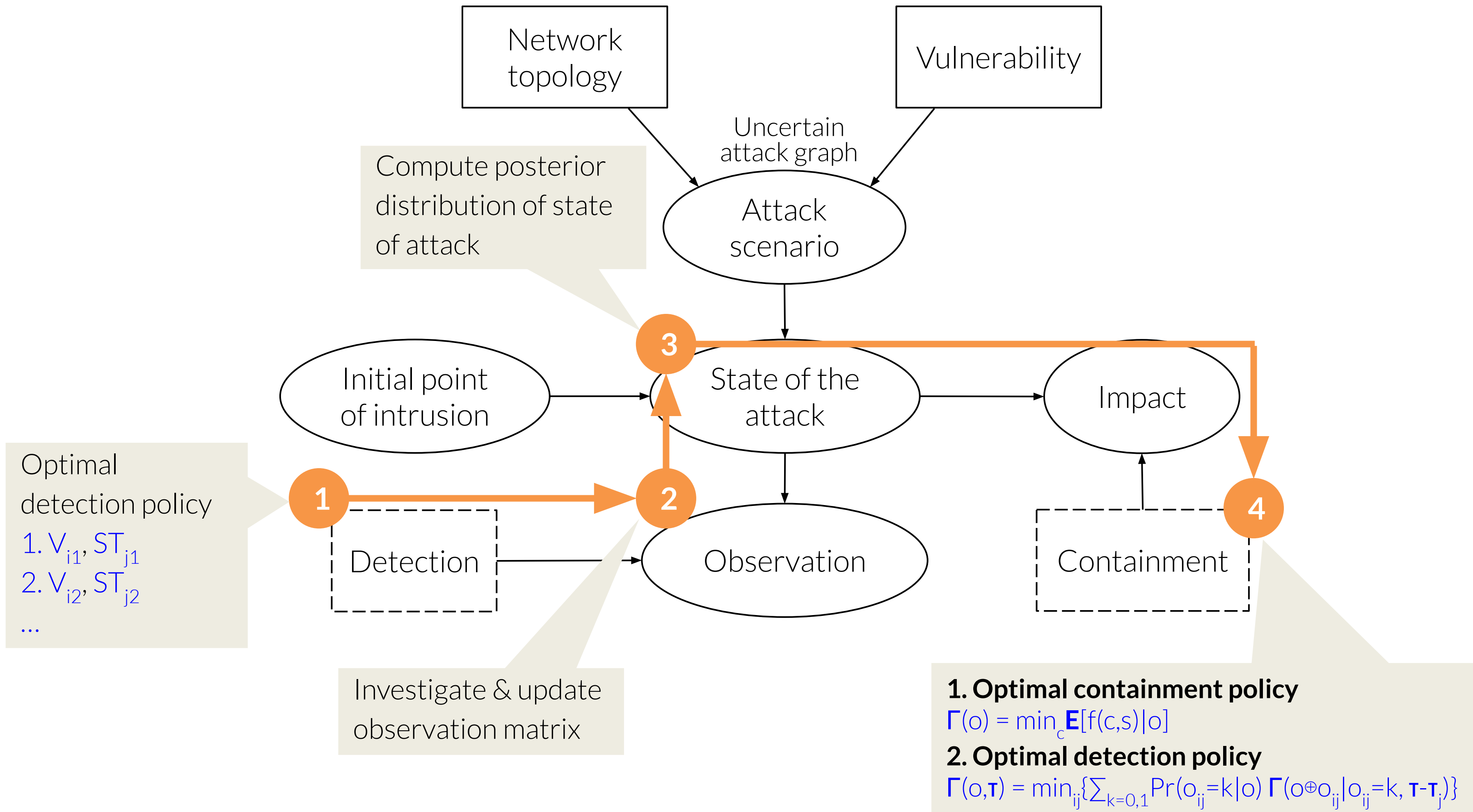
Optimal detection policy
1. V_{i1}, ST_{j1}
2. V_{i2}, ST_{j2}
…

Investigate & update observation matrix

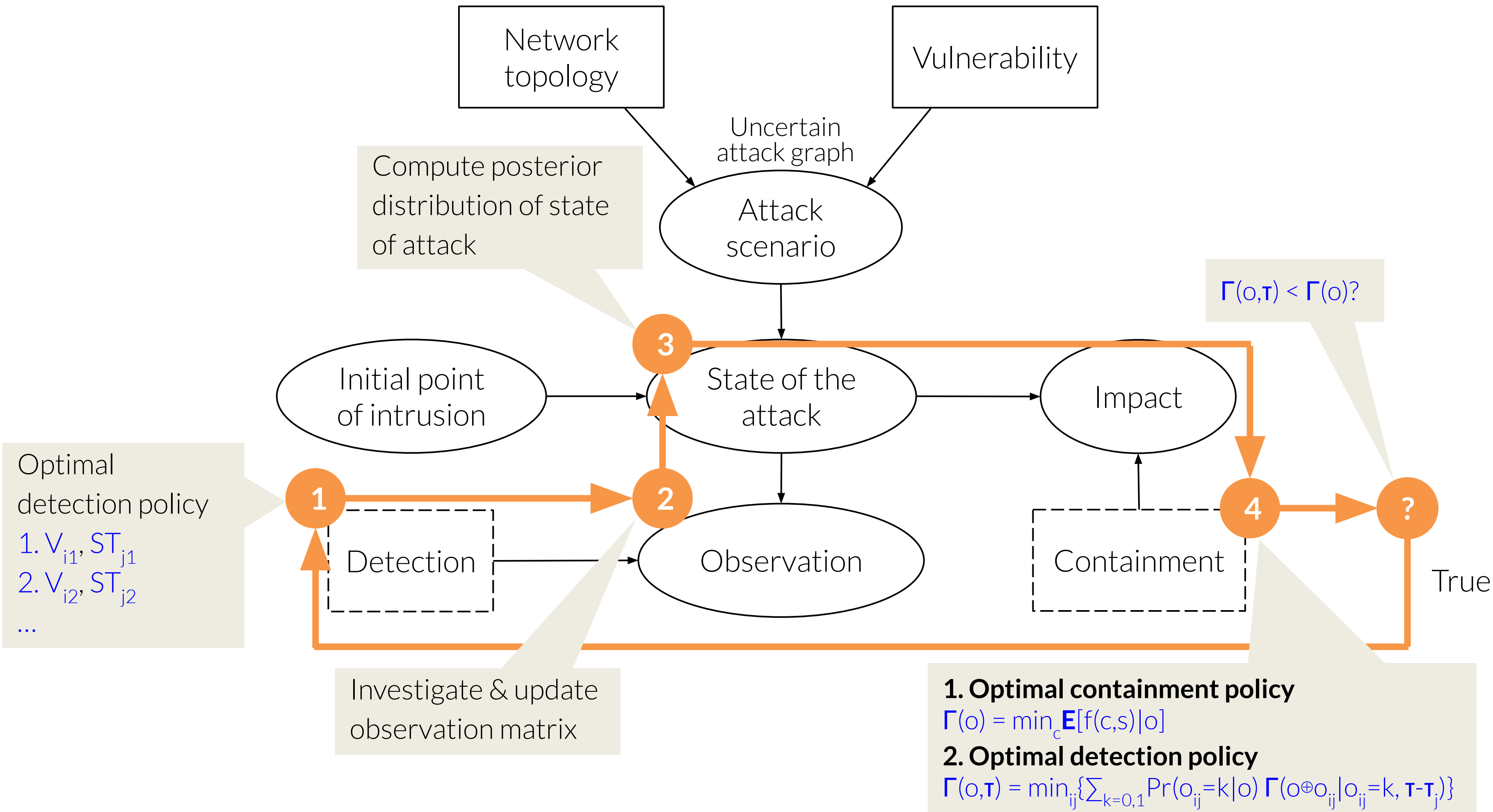
Incident response process



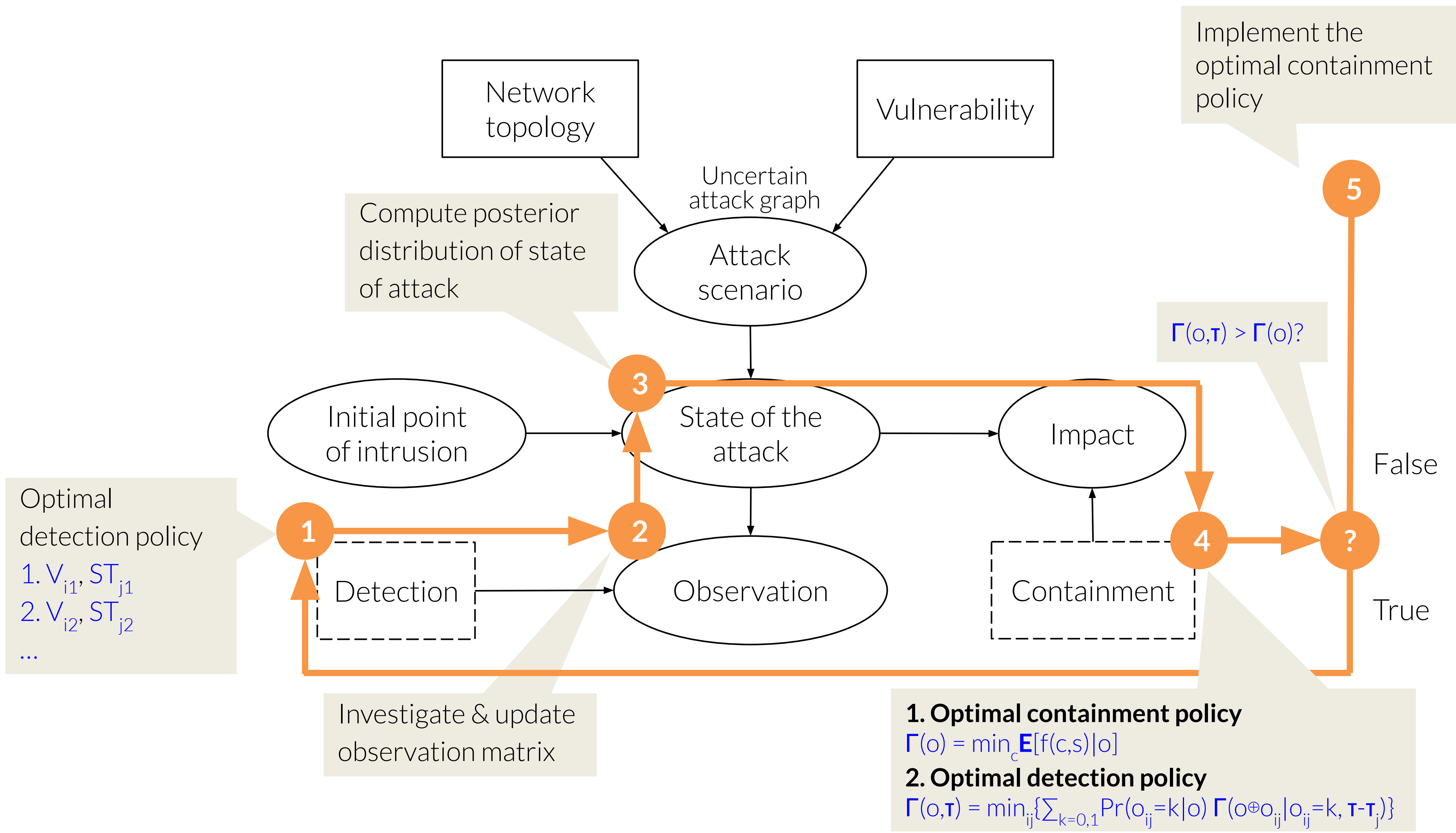
Incident response process



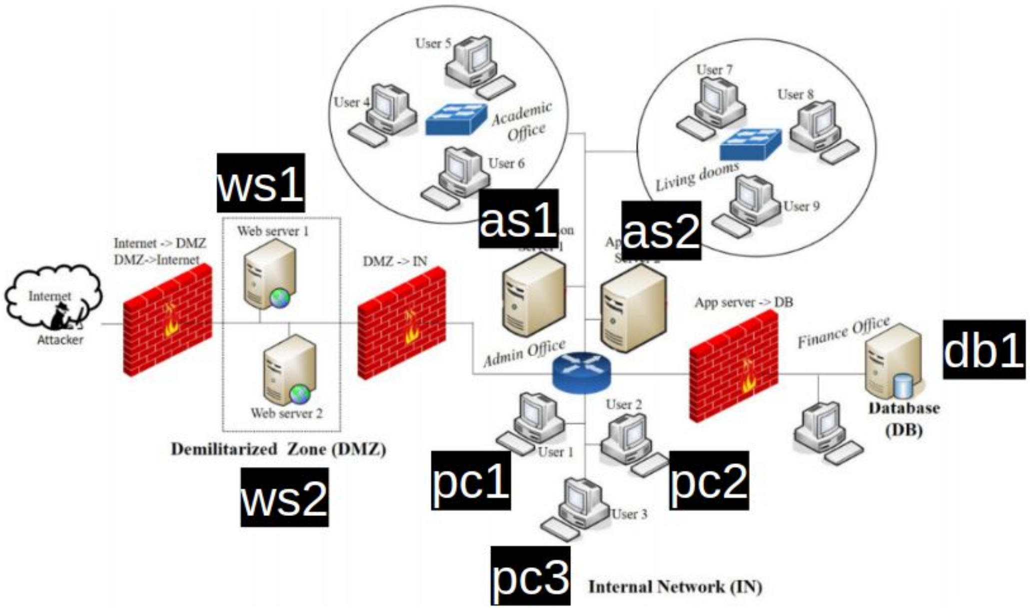
Incident response process



Incident response process



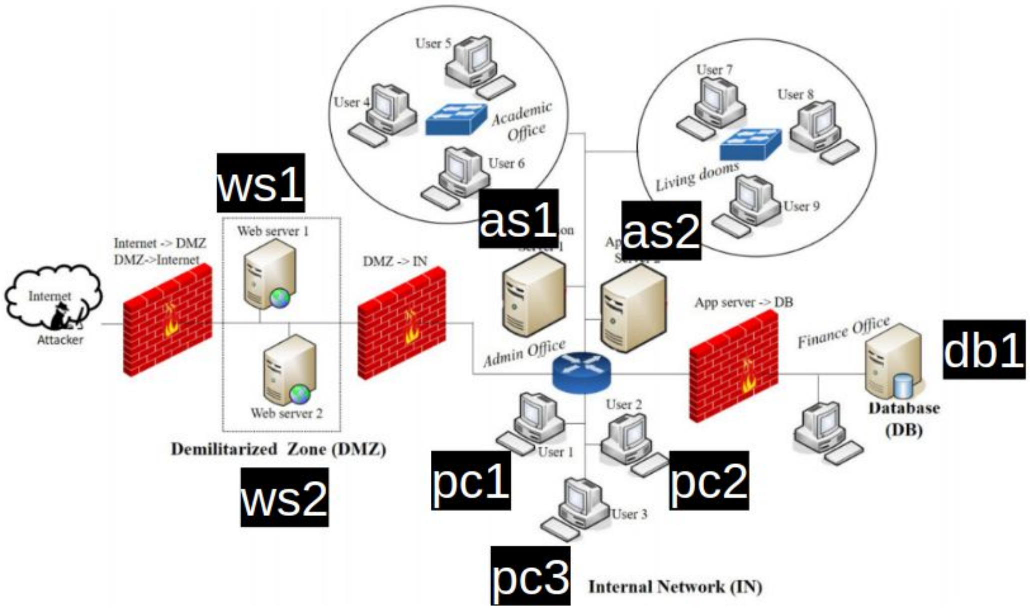
Evaluations



A campus network model [Enoch2019]

[Enoch2019] Security modelling and assessment of modern networks using time independent graphical security models, *Journal of Network and Computer Applications.*

Evaluations



A campus network model [Enoch2019]

Table 1. Lateral movement risks.

	ws→ws	ws→pc	ws→as	pc,as→pc,as	as→db
WEP	very likely	unlikely	very unlikely	likely	even

Table 2. Quantified words of estimative probabilities (WEP).

	very unlikely	unlikely	even	likely	highly likely
exact	.15	.3	.5	.7	.85
range	[.05, .2]	[.2, .45]	[.45, .55]	[.55, .8]	[.8, .95]

Table 3. Investigation results using two security tools, ST_1 and ST_2.

	ws1	ws2	pc1	pc2	pc3	as1	as2	db1
ST_1	1	-1	1	-1	-1	1	-1	-1
ST_2	-1	-1	1	-1	-1	0	0	-1

	ws	pc	as	db
$f_i(0,0)$	0.0	0.0	0.0	0.0
$f_i(1,0)$	1.0	5.0	15.0	25.0
$f_i(1,1)$	2.5	12.5	37.5	62.5
$f_i(0,1)$	5.0	25.0	75.0	125.0

Table 4. Values of the impact functions of each type of network host.

[Enoch2019] Security modelling and assessment of modern networks using time independent graphical security models, *Journal of Network and Computer Applications*.

Experiment 1: probability of compromise

*(**RQ1**) What is the **probability of compromise** of a host given an observation?*

o^0 = no observation
o^1 = observation using ST_1 only
o^{12} = observation using both ST_1 & ST_2

Table 3. Investigation results using two security tools, ST_1 and ST_2.

	ws1	ws2	pc1	pc2	pc3	as1	as2	db1
ST_1	1	-1	1	-1	-1	1	-1	-1
ST_2	-1	-1	1	-1	-1	0	0	-1

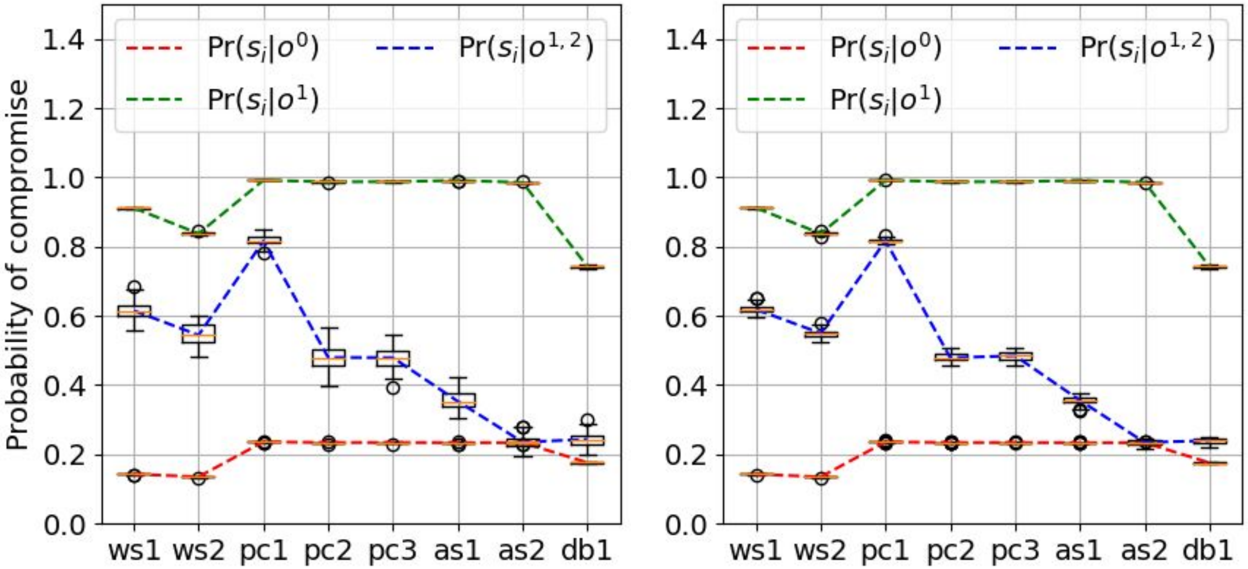
Experiment 1: probability of compromise

*(**RQ1**) What is the **probability of compromise** of a host given an observation?*

o^0 = no observation
o^1 = observation using ST_1 only
o^{12} = observation using both ST_1 & ST_2

Table 3. Investigation results using two security tools, ST_1 and ST_2.

	ws1	**ws2**	**pc1**	**pc2**	**pc3**	**as1**	**as2**	**db1**
ST_1	1	-1	1	-1	-1	1	-1	-1
ST_2	-1	-1	1	-1	-1	0	0	-1

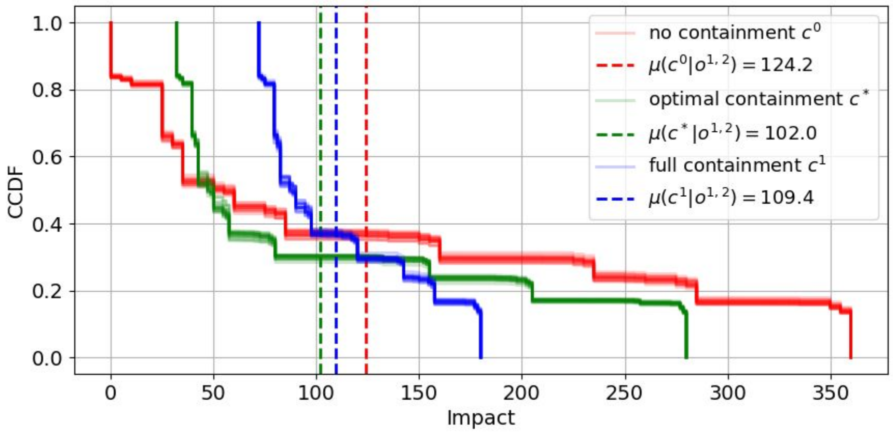


***Probability of compromise** under different observation matrices using **crude Monte Carlo** (left) and **importance sampling** (right).*

Experiment 2: optimal containment policy

*(**RQ2**) What is the **containment decision** that yields the **minimum expected impact**?*

<u>Exp. 2a:</u> optimal containment vs other containment strategies
(i) **no containment** c^0
(ii) **optimal containment** c^*: contain all hosts except **as2** and **db1**
(iii) **full containment** c^1

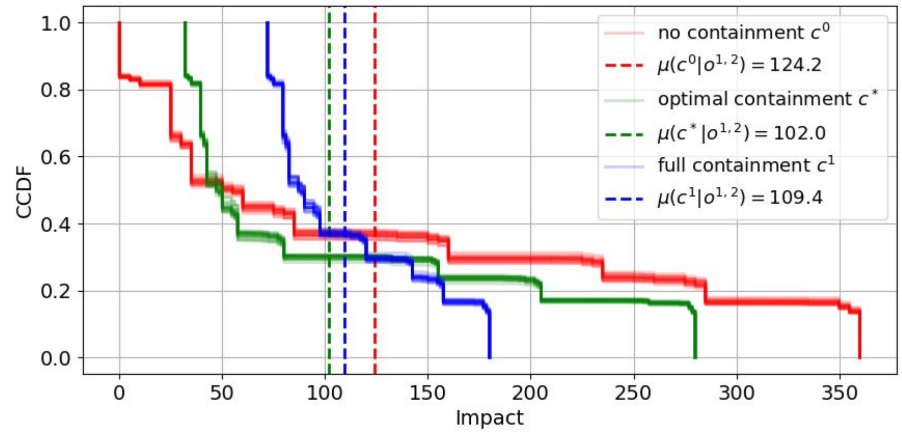


*The **risk curves** of three different containment strategies.*

Experiment 2: optimal containment policy

*(**RQ2**) What is the **containment decision** that yields the **minimum expected impact**?*

Exp. 2a: optimal containment vs other containment strategies
(i) **no containment** c^0
(ii) **optimal containment** c^*: contain all hosts except **as2** and **db1**
(iii) **full containment** c^1



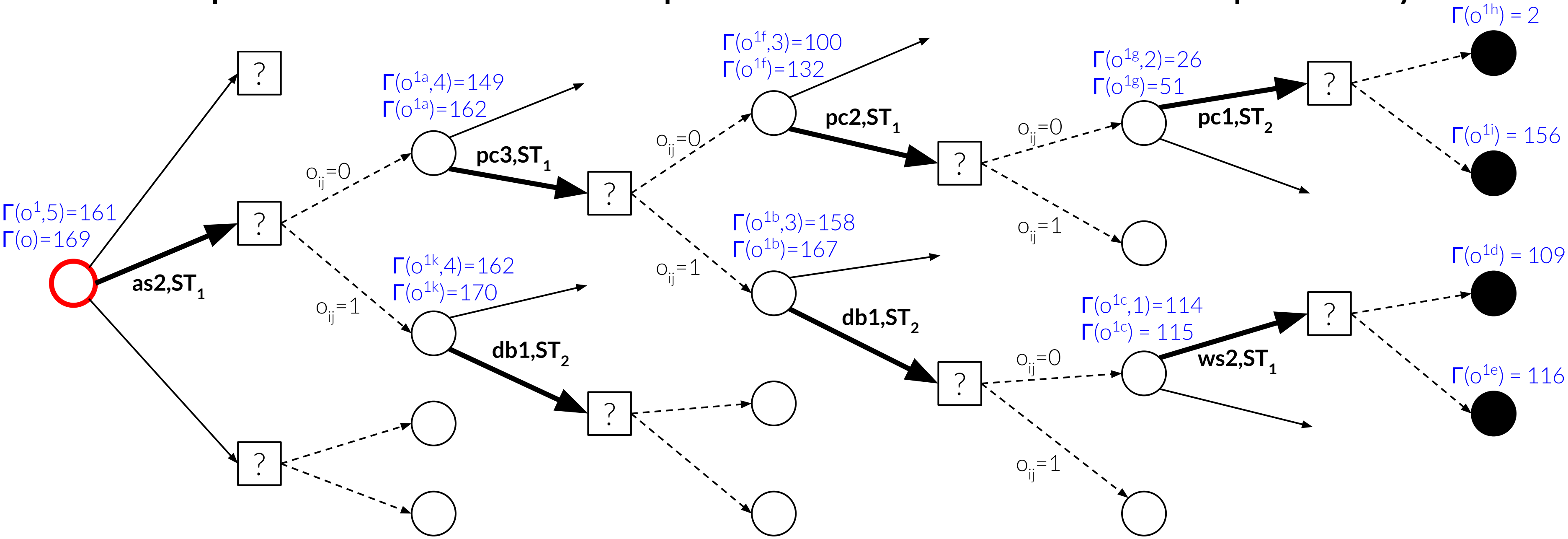
*The **risk curves** of three different containment strategies.*

Exp. 2b: sensitivity analysis
(i) **no variability**
(ii) **variability in probabilities**
(iii) **variability in probabilities & impacts** (70%-130%)

Table 5. Sensitivity analysis of the optimal containment decision subjected to variability in the probabilities and impacts.

	ws1	ws2	pc1	pc2	pc3	as1	as2	db1
(i) no vari.	100%	100%	100%	100%	100%	100%	0%	0%
(ii) prob.	100%	100%	100%	100%	100%	56%	23%	18%
(iii) prob. & impact	98%	97%	100%	92%	92%	59%	31%	27%

Experiment 3: optimal detection policy



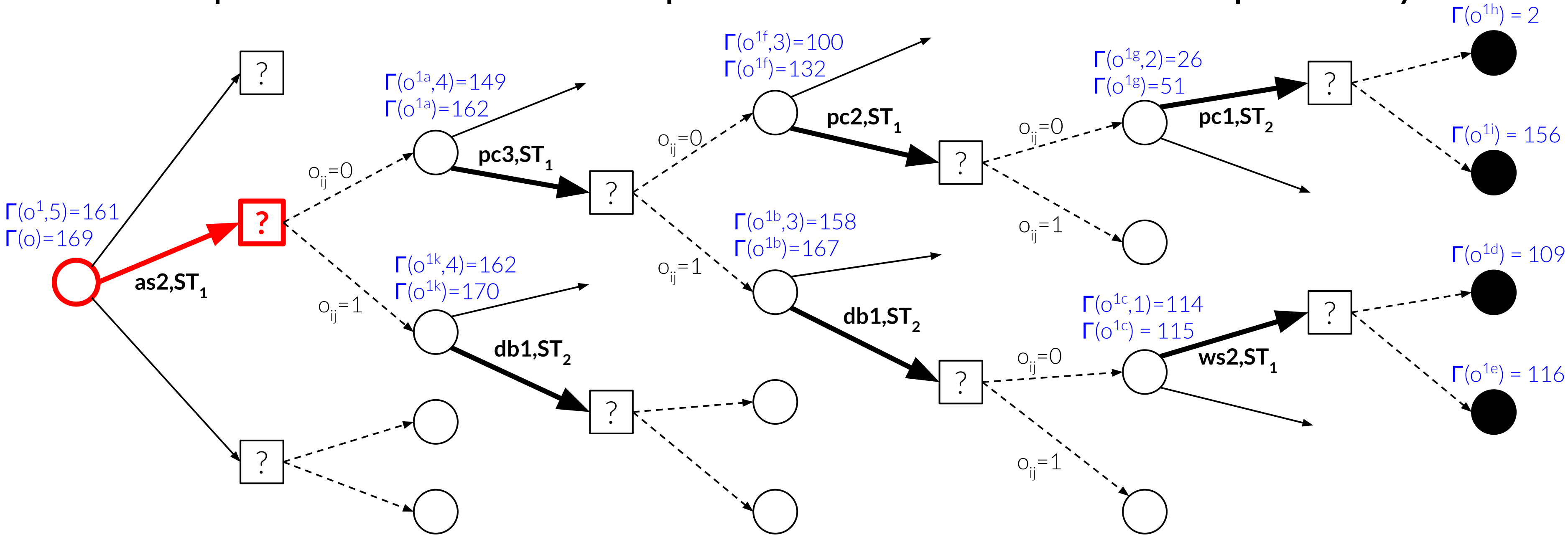
Optimal detection search tree.

o = current **observation matrix,** τ = **remaining time**

Γ(o, τ) = **minimally achievable** reward Γ(o) = **immediate** reward

*(**RQ4**) **Which host** to investigate, using **which security tool**?*

Experiment 3: optimal detection policy



Optimal detection search tree.

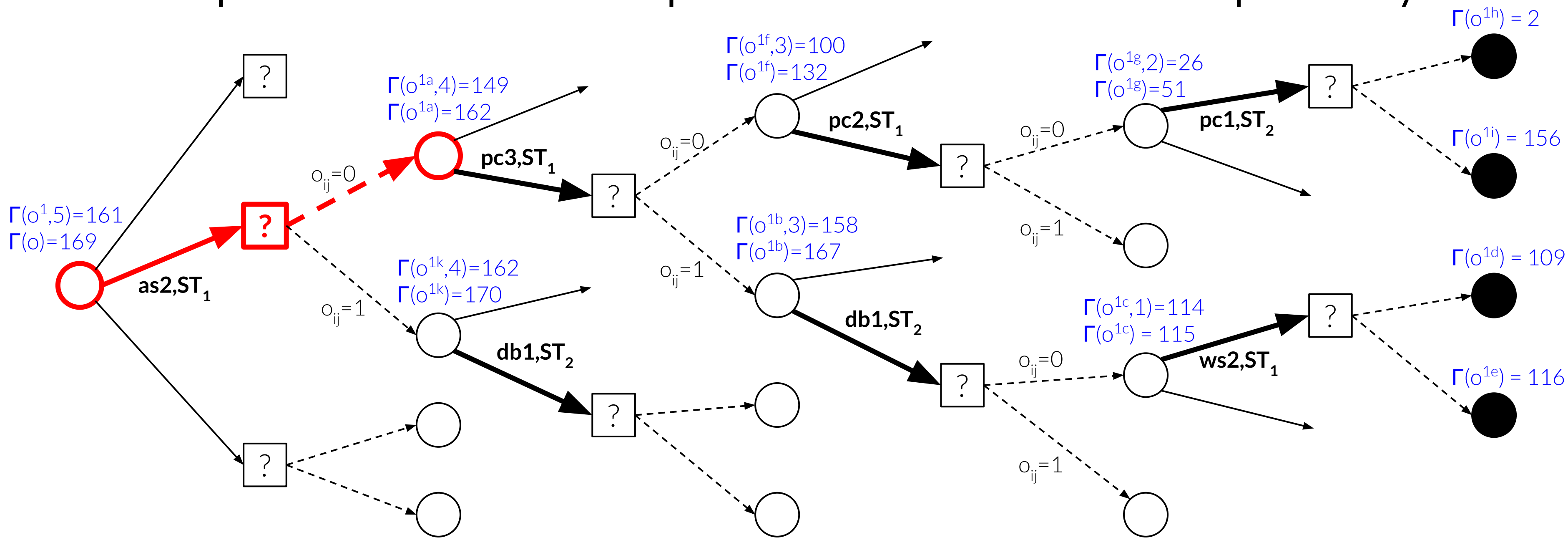
o = current **observation matrix,** τ = **remaining time**

Γ(o, τ) = **minimally achievable** reward Γ(o) = **immediate** reward

*(**RQ4**) **Which host** to investigate, using **which security tool**?*

1. **as2, ST_1**

Experiment 3: optimal detection policy



Optimal detection search tree.

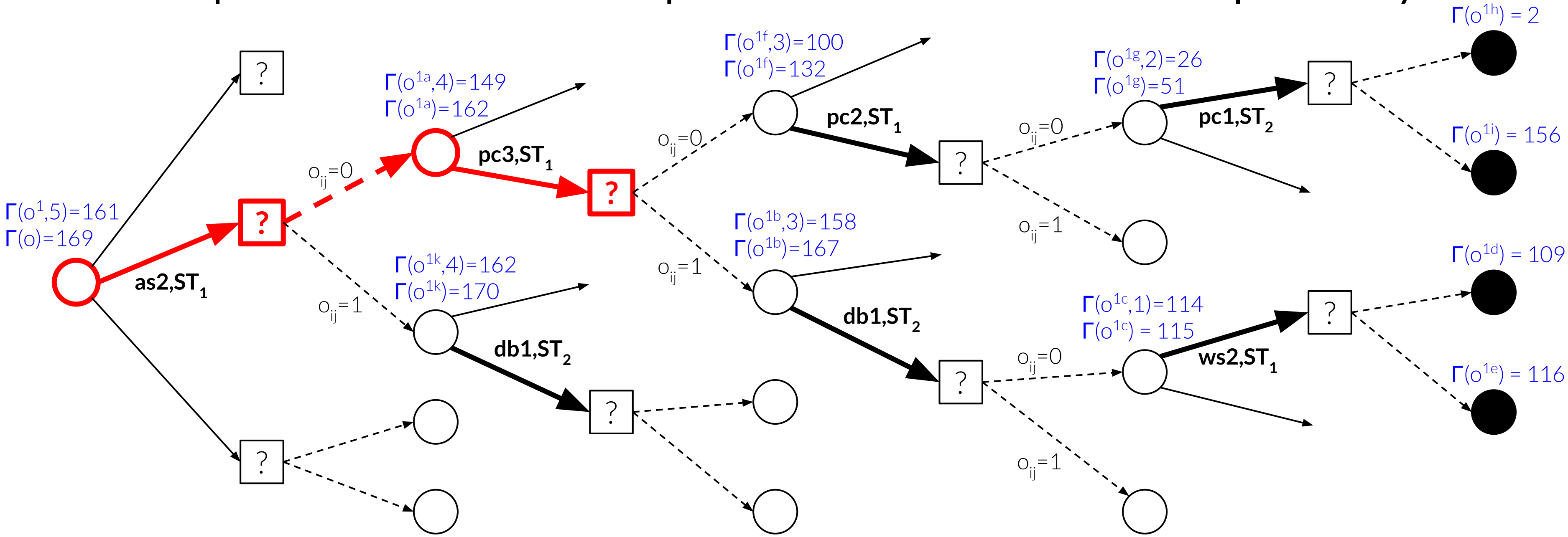
o = current **observation matrix,** τ = **remaining time**

Γ(o, τ) = **minimally achievable** reward Γ(o) = **immediate** reward

*(**RQ4**) **Which host** to investigate, using **which security tool**?*

1. **as2, ST_1**

Experiment 3: optimal detection policy



Optimal detection search tree.

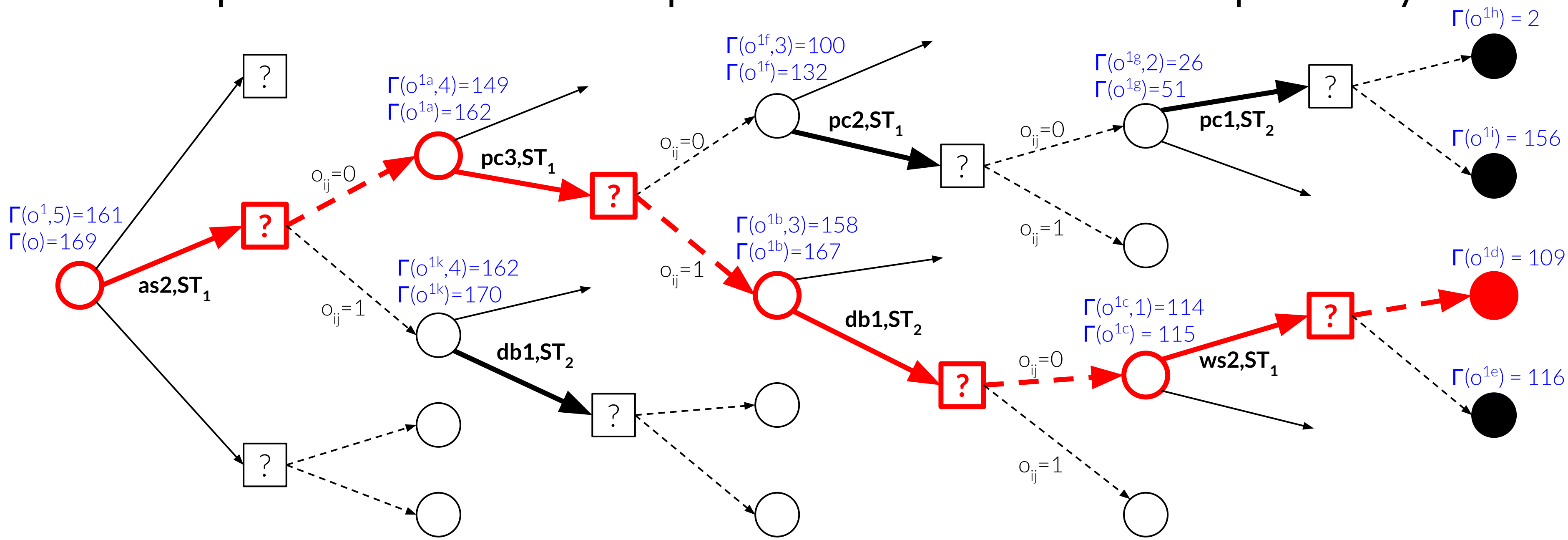
o = current **observation matrix,** τ = **remaining time**

Γ(o, τ) = **minimally achievable** reward Γ(o) = **immediate** reward

*(**RQ4**) **Which host** to investigate, using **which security tool**?*

1. **as2, ST$_1$**
2. **pc3, ST$_1$**

Experiment 3: optimal detection policy



Optimal detection search tree.

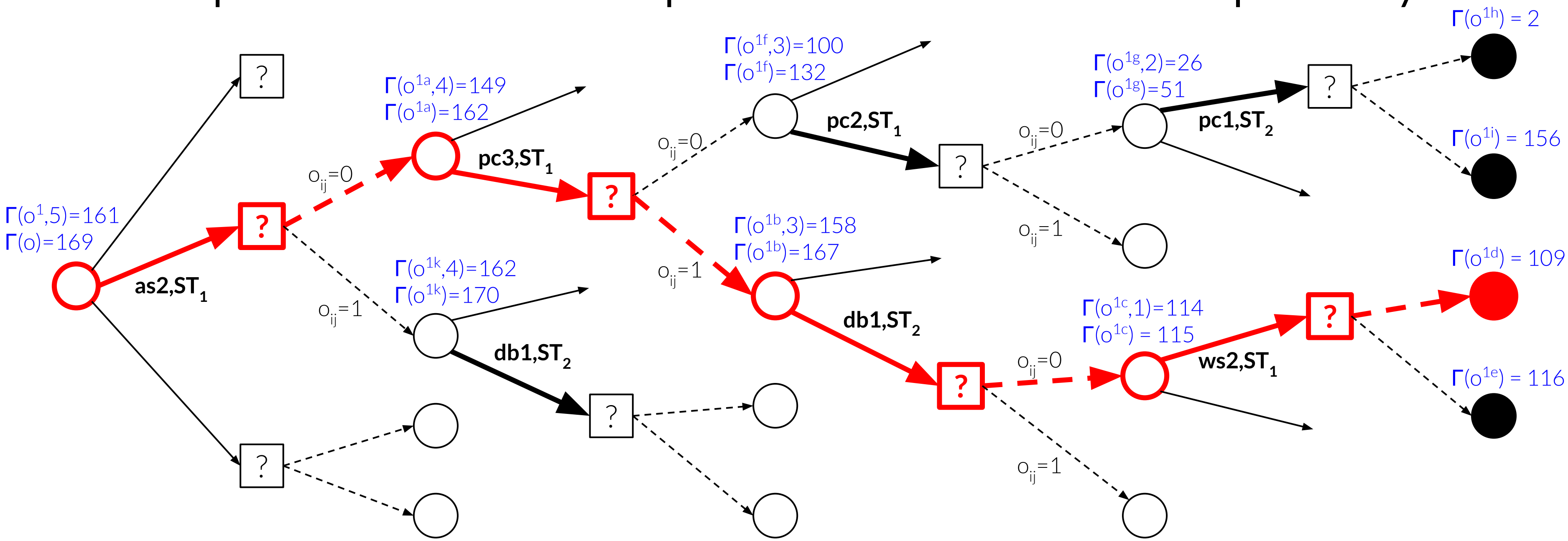
o = current **observation matrix,** τ = **remaining time**

Γ(o, τ) = **minimally achievable** reward Γ(o) = **immediate** reward

*(**RQ4**) **Which host** to investigate, using **which security tool**?*

1. **as2, ST_1**
2. **pc3, ST_1**
3. **db1, ST_2**
4. **ws2, ST_1**

Experiment 3: optimal detection policy



Optimal detection search tree.

o = current **observation matrix**, τ = **remaining time**

Γ(o, τ) = **minimally achievable** reward Γ(o) = **immediate** reward

*(**RQ4**) **Which host** to investigate, using **which security tool**?*

1. **as2, ST_1**
2. **pc3, ST_1**
3. **db1, ST_2**
4. **ws2, ST_1**

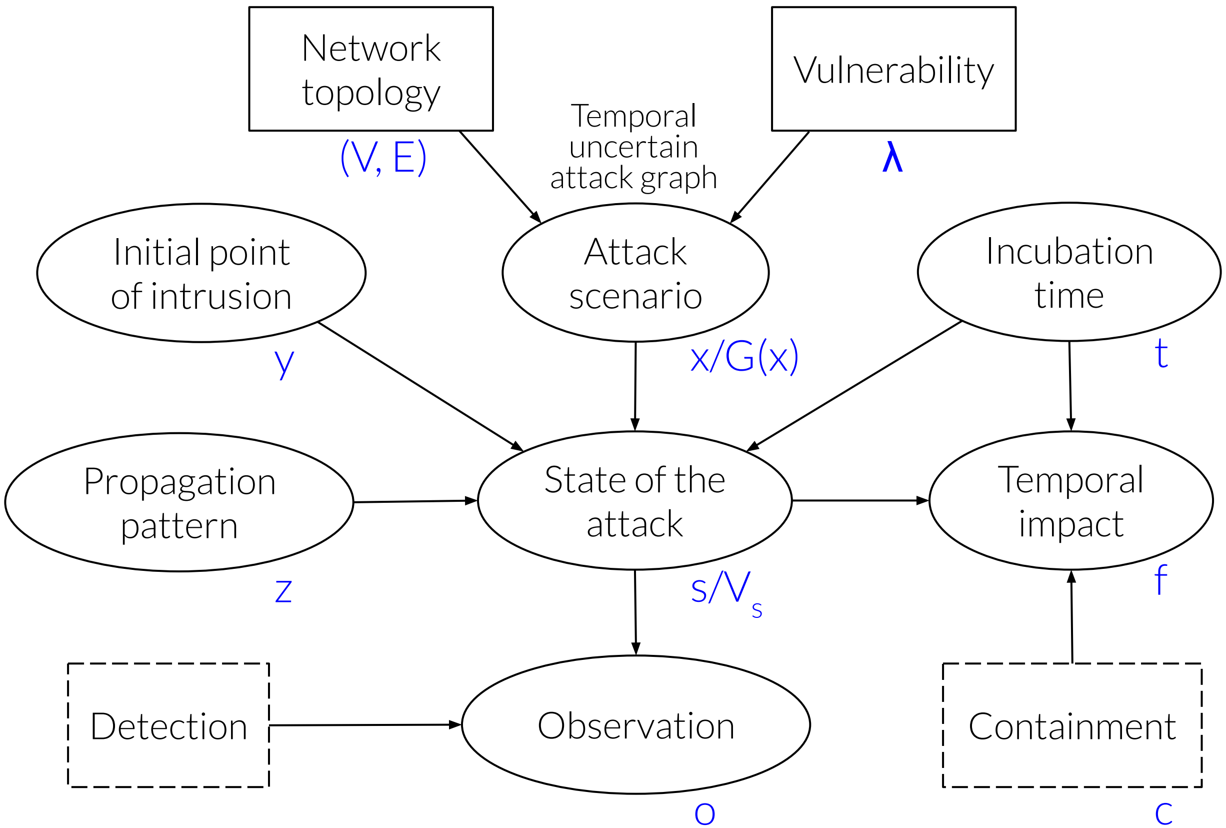
*(**RQ3**) To investigate or to contain?*

$\Gamma(o, \tau) \leq \Gamma(o) \Rightarrow$ investigate until running out of time/option

Extra slides

-

Temporal incident response model



Model assumptions

Assumption 0: the uncertain attack graph faithfully captures the logic of multistep cyberattacks

Assumption 3: the initial point of intrusion and the attack scenario are probabilistically independent

Assumption 4: security observations are probabilistically independent

Assumption 5: the impact function is deterministic

Assumption 6: the impact function is additive