# Heuristic Approach for Countermeasure Selection Using Attack Graphs

Orly Stan[1], **Ron Bitton[1]**, Michal Ezrets[1], Moran Dadon[1] Masaki Inokuchi[2], Yoshinobu Otha[2], Tomohiko Yagyu[2], Yuval Elovici[1], and Asaf Shabtai[1]

1. Cybersecurity Research Center at Ben-Gurion University of the Negev
2. Security Research Laboratories NEC Corporation


CBG | Cyber@ Ben-Gurion University of the Negev | NEC

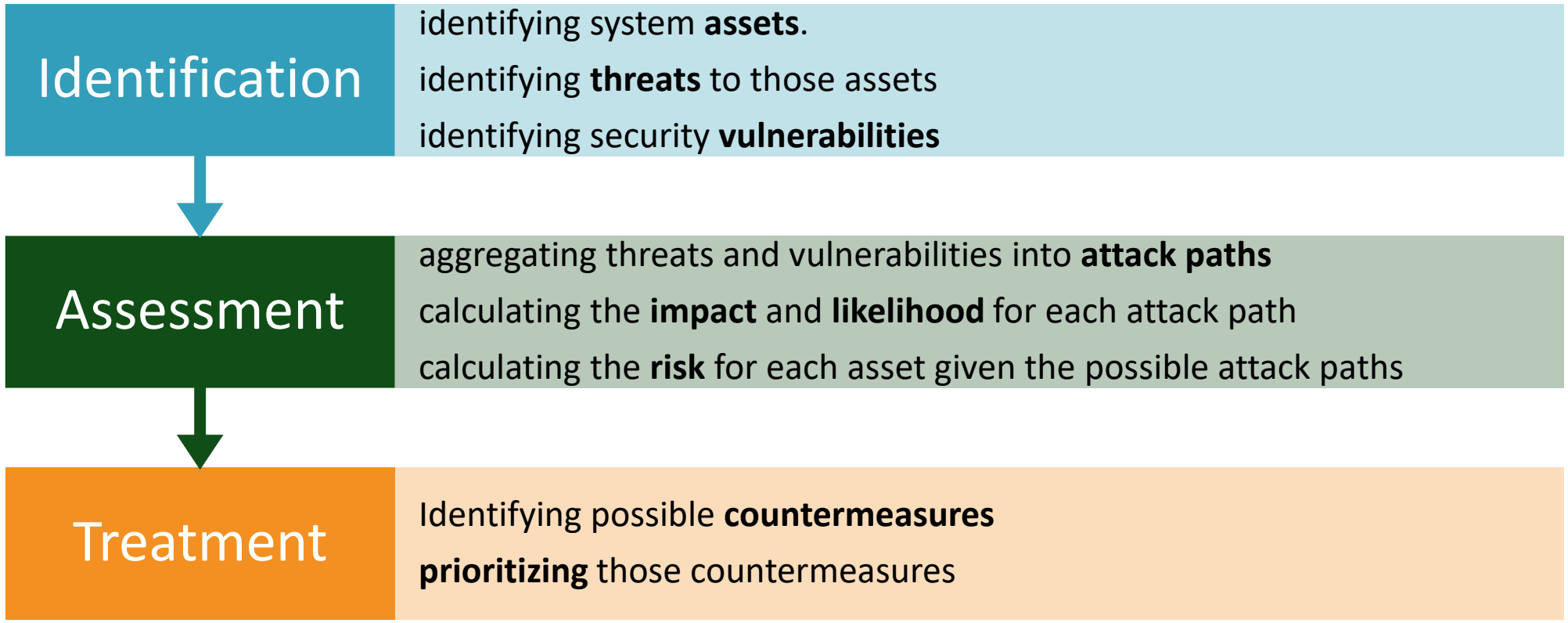
# Cybersecurity risk management lifecycle

| | |
|---|---|
| Identification | identifying system **assets**.<br>identifying **threats** to those assets<br>identifying security **vulnerabilities** |

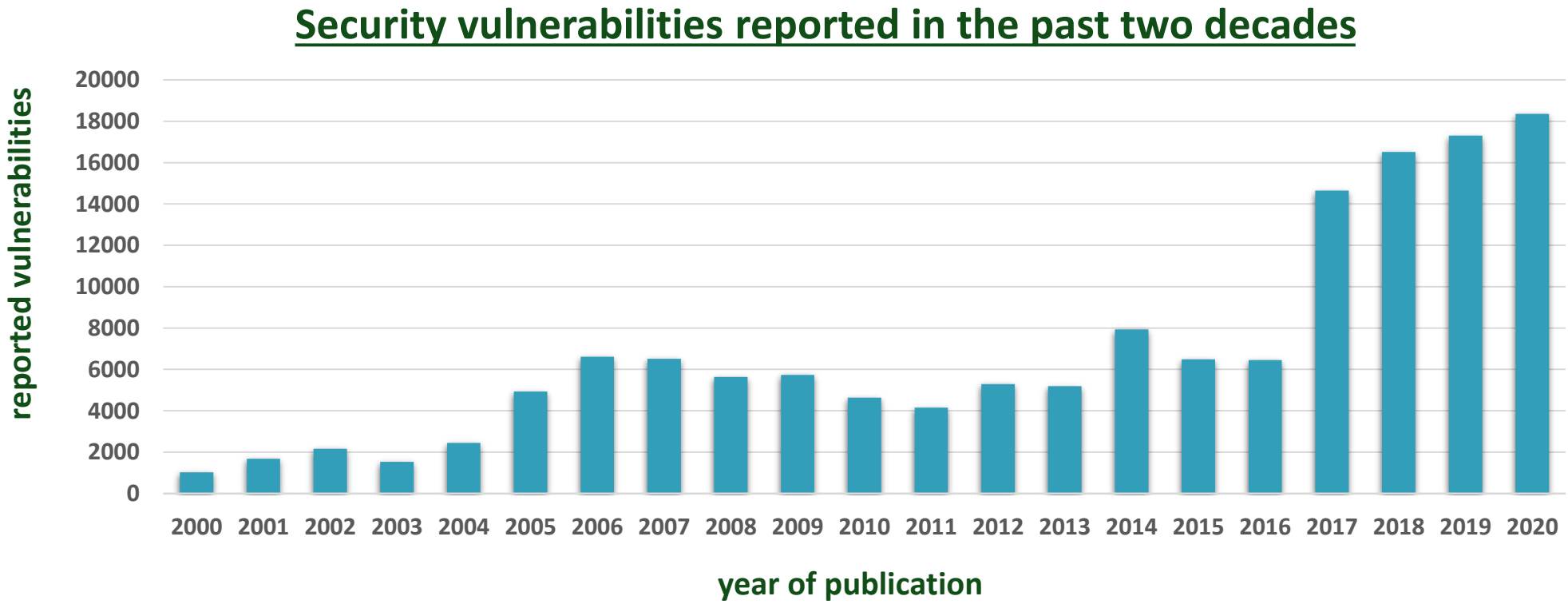
# Cybersecurity risk management lifecycle

| | |
|---|---|
| Identification | identifying system **assets**.<br>identifying **threats** to those assets<br>identifying security **vulnerabilities** |
| Assessment | aggregating threats and vulnerabilities into **attack paths**<br>calculating the **impact** and **likelihood** for each attack path<br>calculating the **risk** for each asset given the possible attack paths |

# Cybersecurity risk management lifecycle



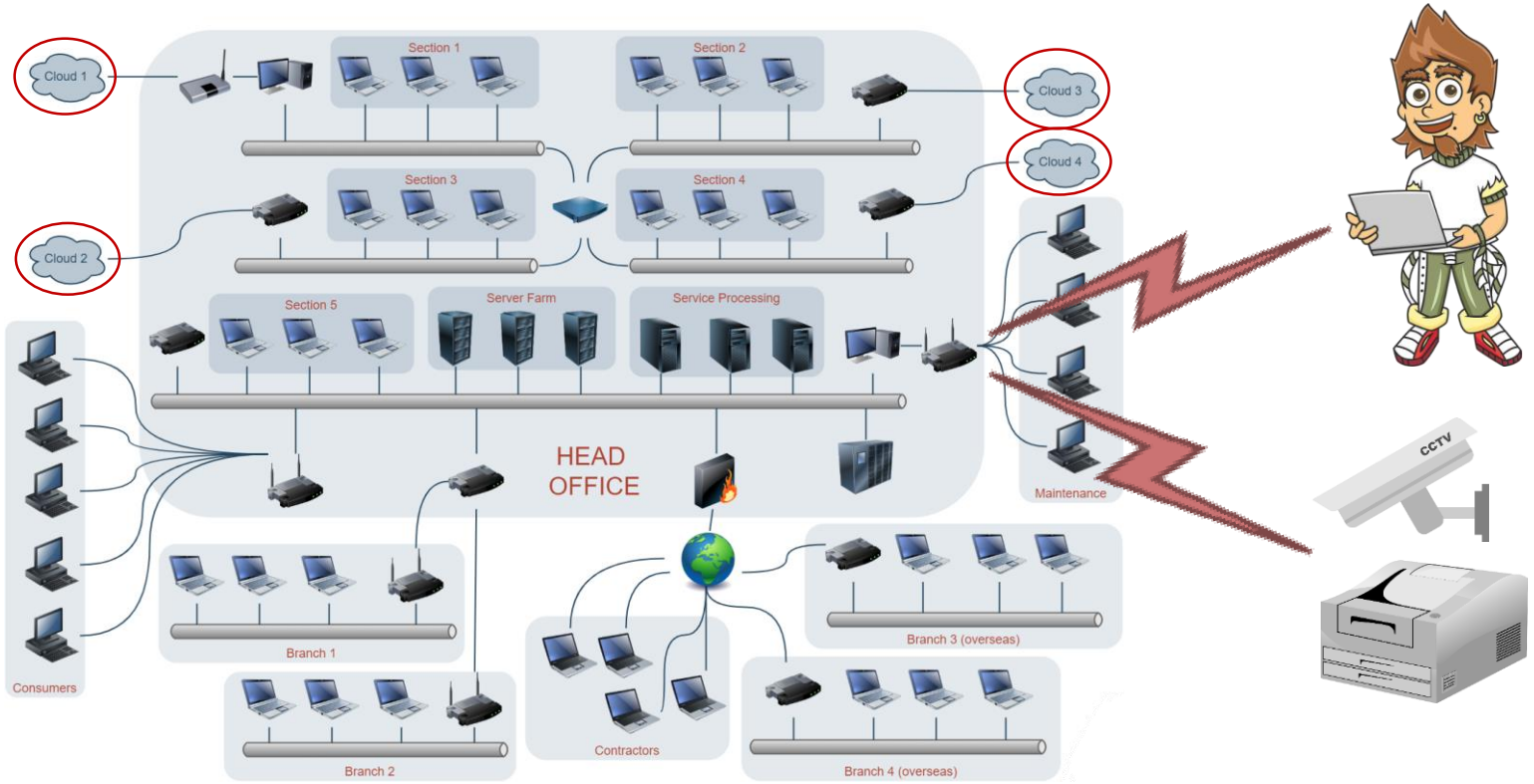
# Why countermeasure planning is a very challenging task?




Source: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time#CVSSSeverityOverTime

NEC CBG Cyber@ Ben-Gurion University of the Negev NEC

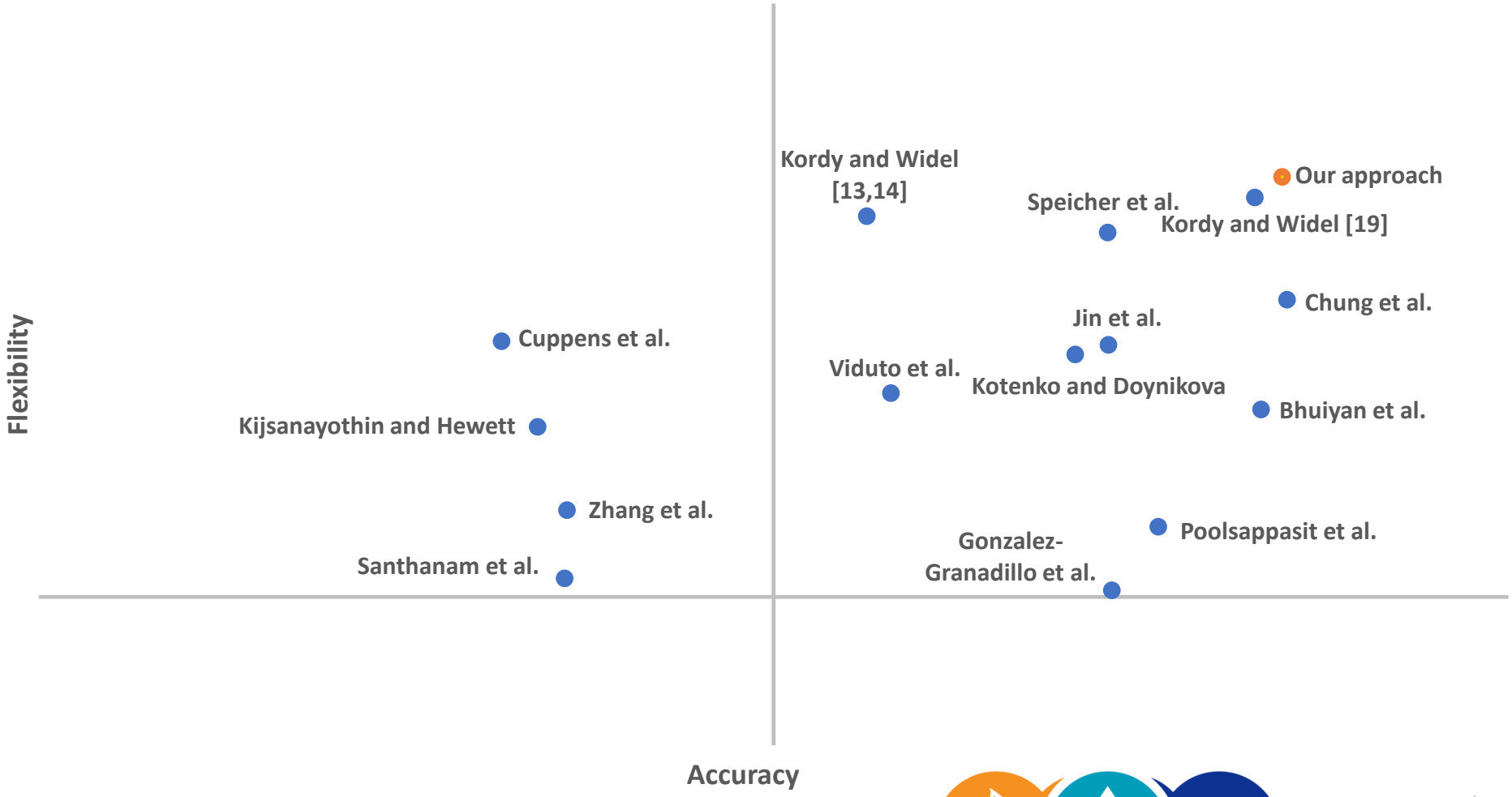
# Why countermeasure planning is a very challenging task?




Cyber@
Ben-Gurion University
of the Negev

NEC

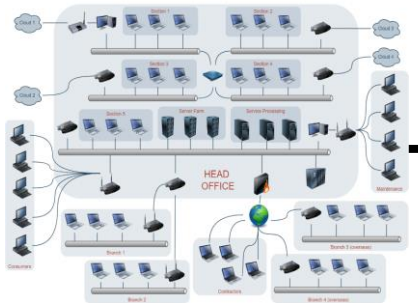
# Related Work



# High-level overview of the proposed method

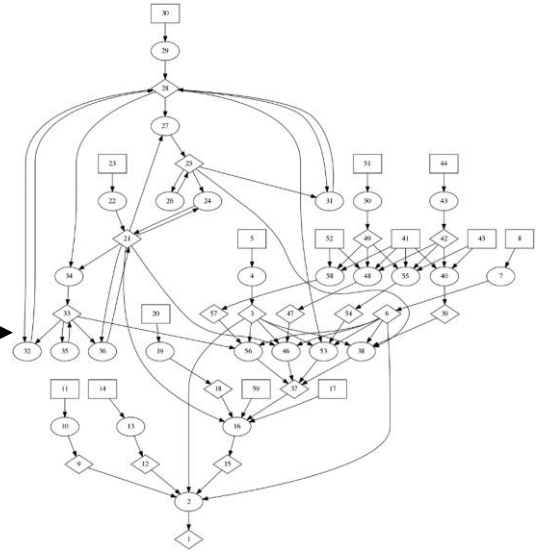
# High-level overview of the proposed method

1

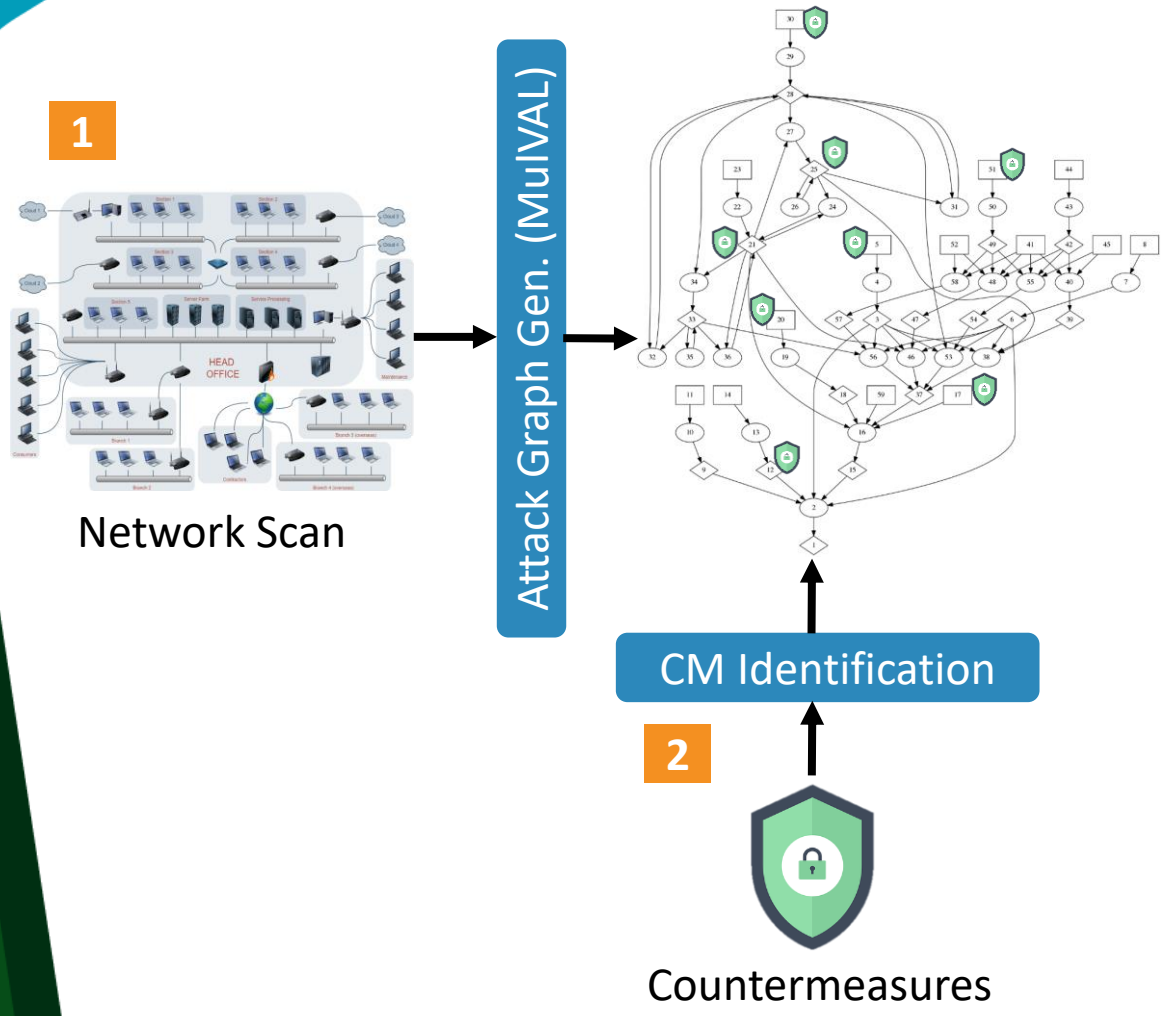



Network Scan

Attack Graph Gen. (MulVAL)



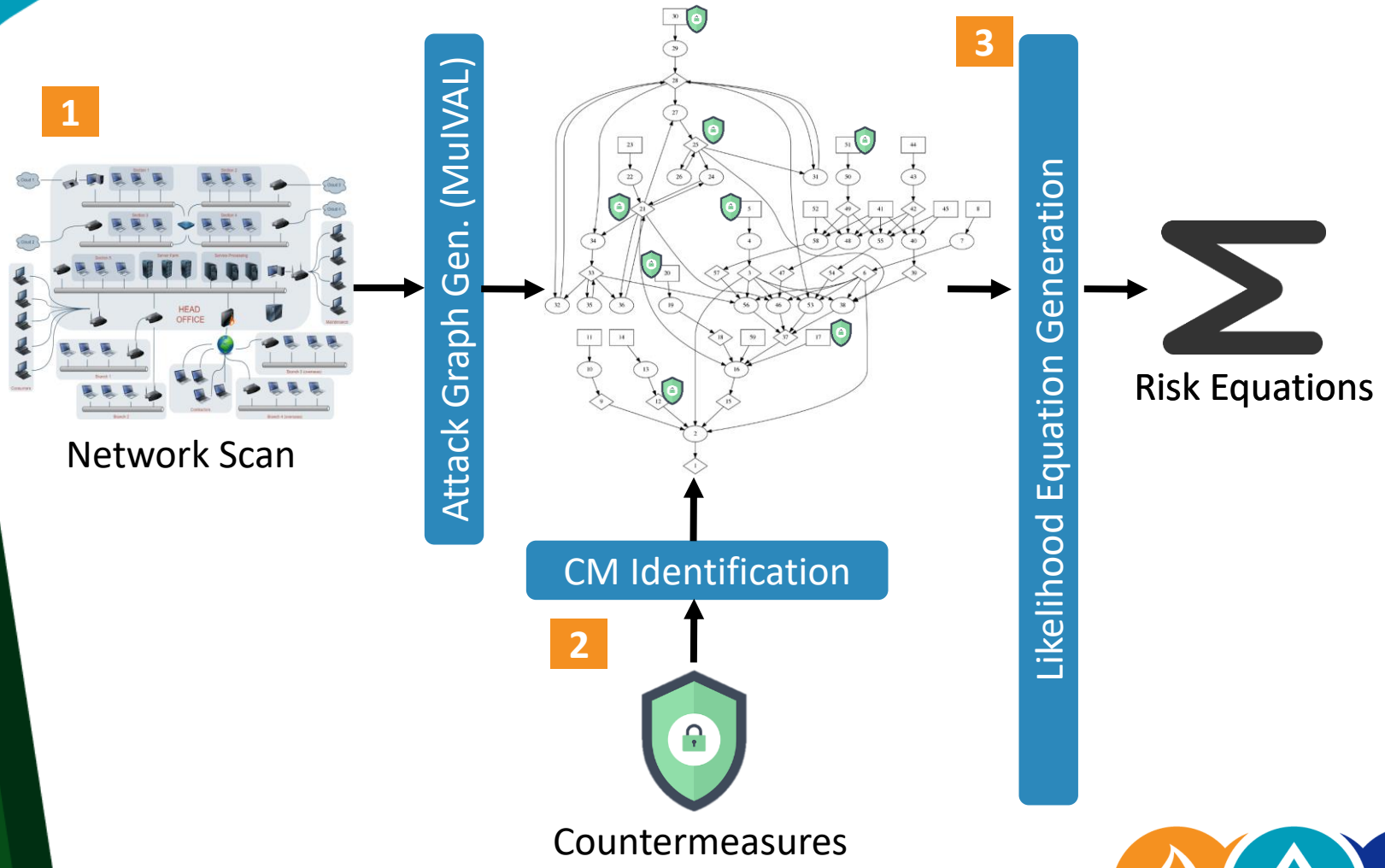
# High-level overview of the proposed method




Cyber@
Ben-Gurion University
of the Negev

NEC

# High-level overview of the proposed method

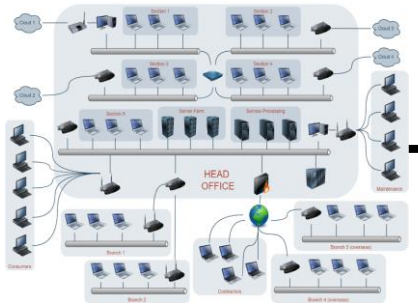



Cyber@ Ben-Gurion University of the Negev

NEC

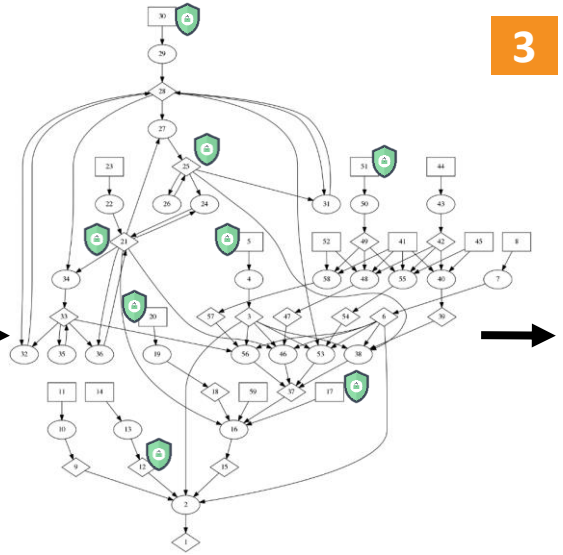
# High-level overview of the proposed method

1




Network Scan

Attack Graph Gen. (MulVAL)



2

CM Identification

Countermeasures

3

Likelihood Equation Generation

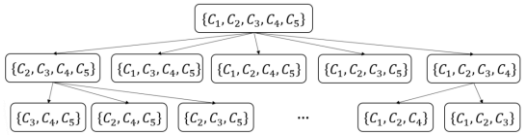
Risk Equations

Budget

4

Path-Finding Problem Formulation

Search Graph




NEC

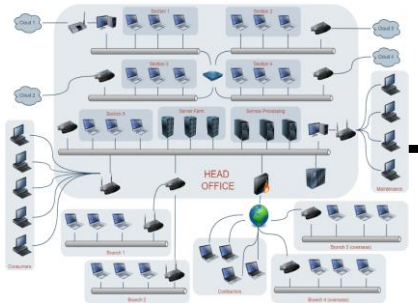
CBG

Cyber@
Ben-Gurion University
of the Negev

NEC

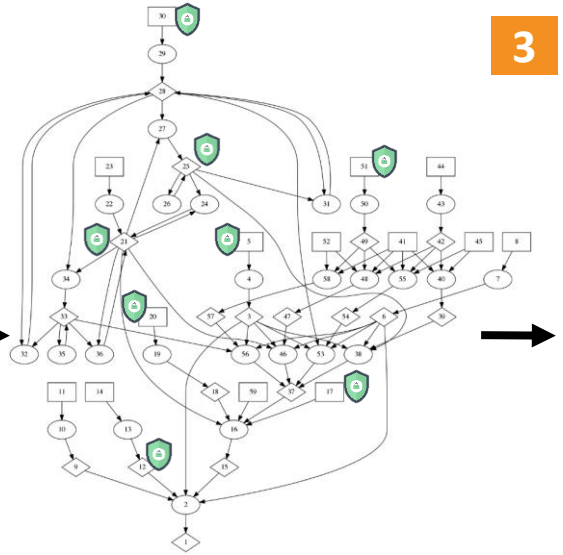
# High-level overview of the proposed method

1




Network Scan

Attack Graph Gen. (MulVAL)



3

Likelihood Equation Generation

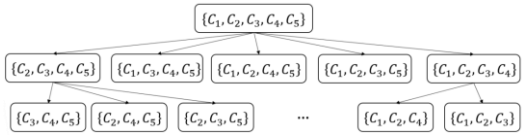
Risk Equations

Budget

4

Path-Finding Problem Formulation

Search Graph




5

A* Solver

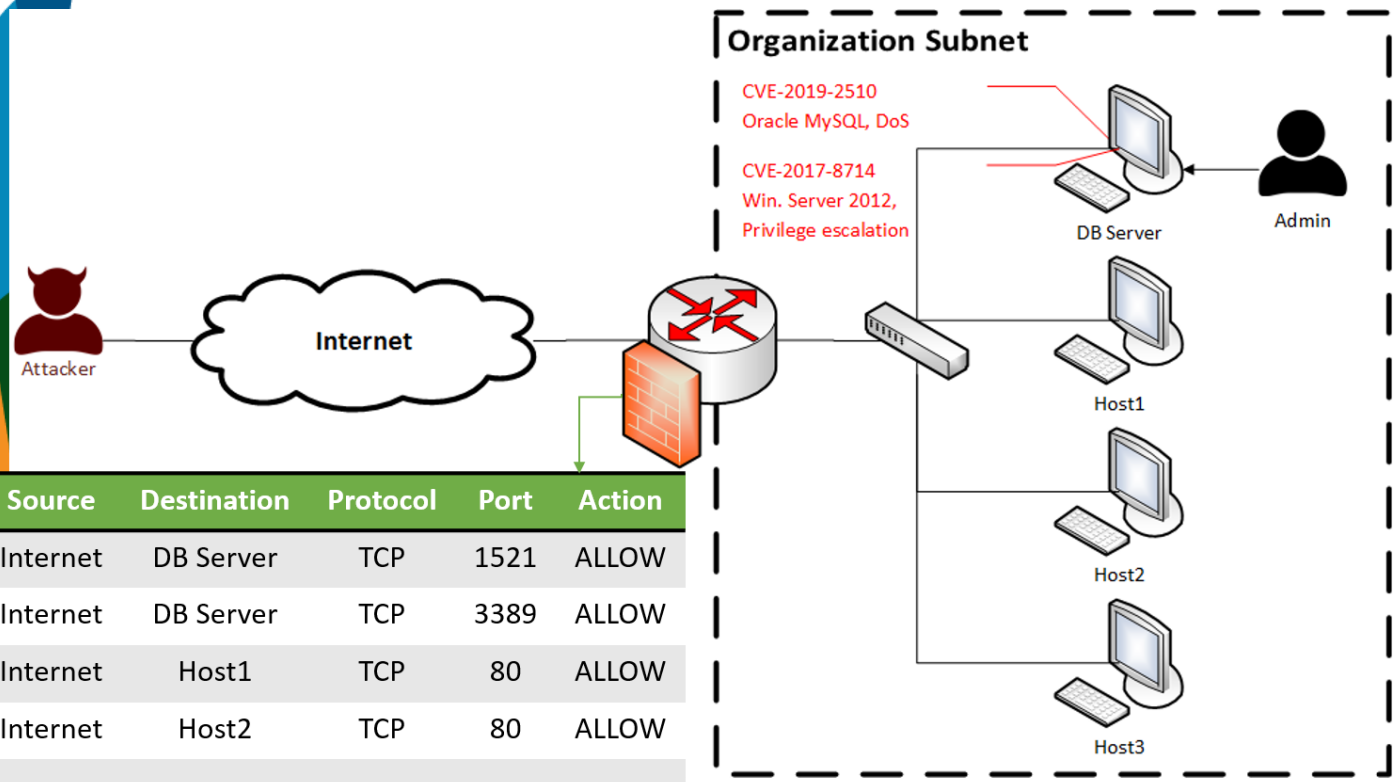
**Optimal Plan**

CM Identification

2

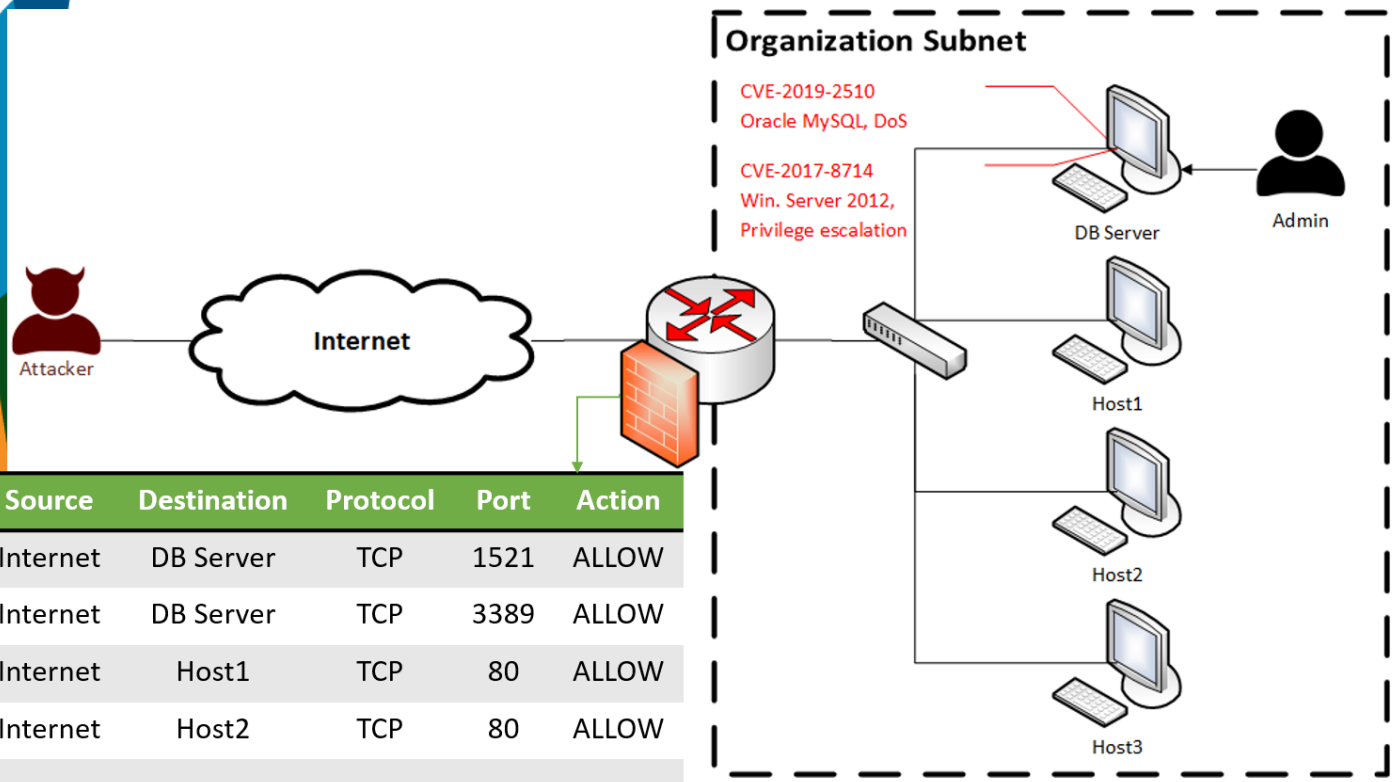
Countermeasures

# Step 1: Attack Graph Generation

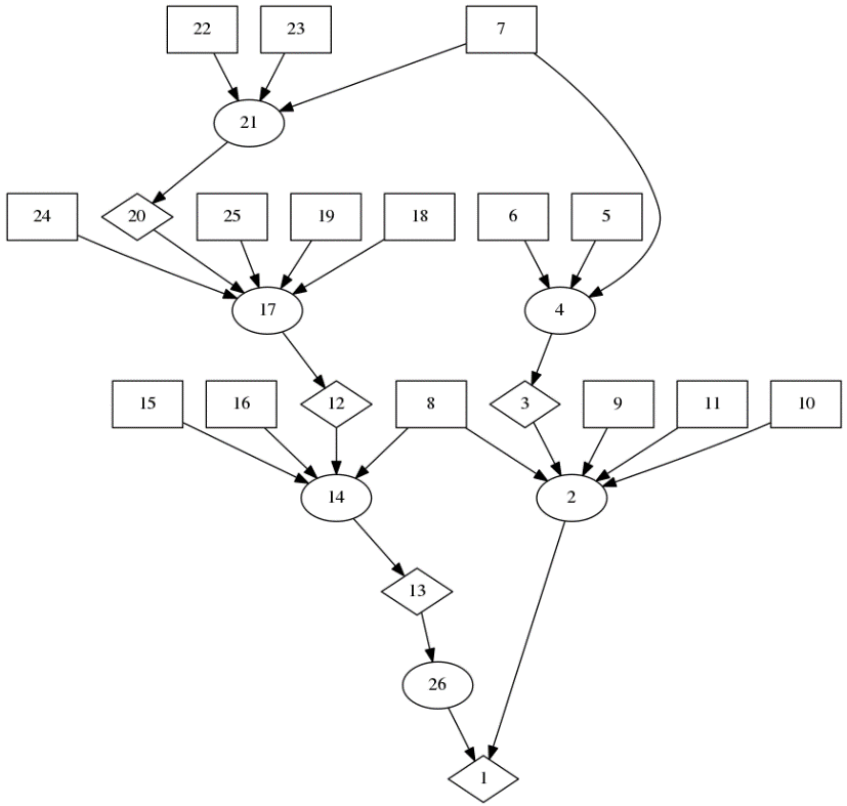



| Source | Destination | Protocol | Port | Action |
|---|---|---|---|---|
| Internet | DB Server | TCP | 1521 | ALLOW |
| Internet | DB Server | TCP | 3389 | ALLOW |
| Internet | Host1 | TCP | 80 | ALLOW |
| Internet | Host2 | TCP | 80 | ALLOW |
| ... | ... | ... | ... | ... |

# Step 1: Attack Graph Generation



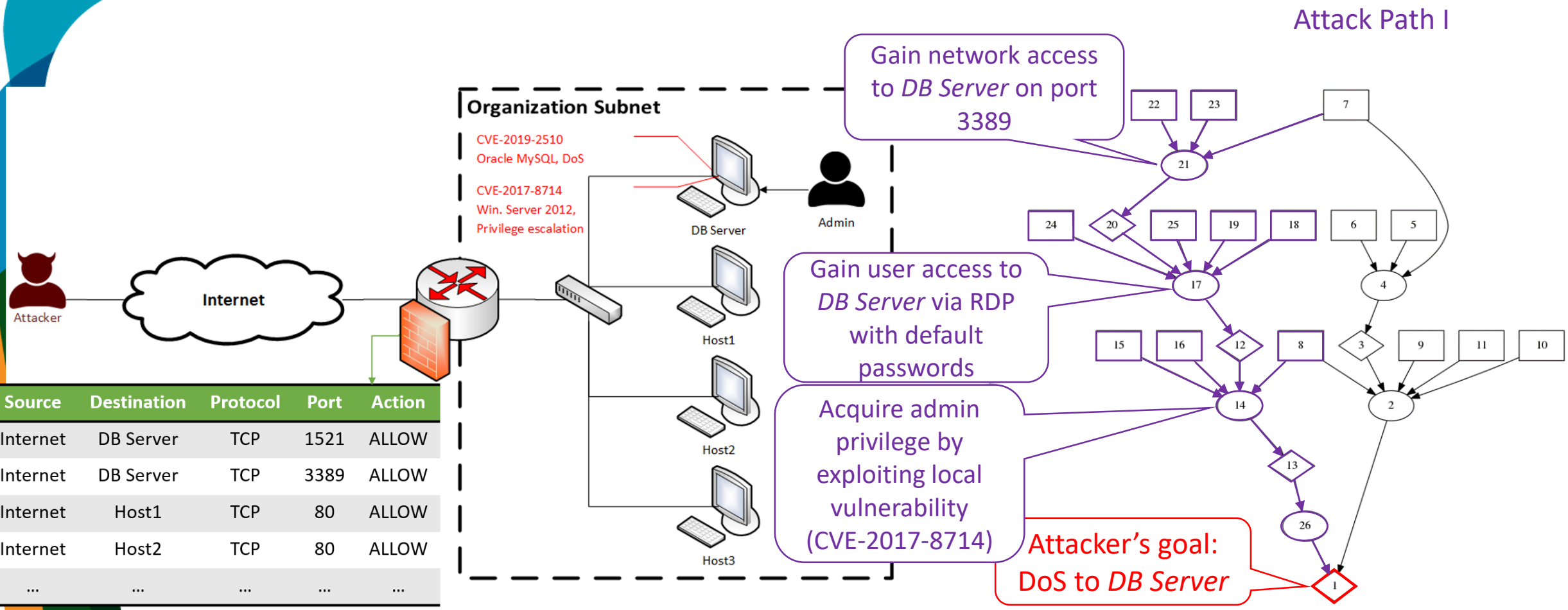

| Source | Destination | Protocol | Port | Action |
|---|---|---|---|---|
| Internet | DB Server | TCP | 1521 | ALLOW |
| Internet | DB Server | TCP | 3389 | ALLOW |
| Internet | Host1 | TCP | 80 | ALLOW |
| Internet | Host2 | TCP | 80 | ALLOW |
| ... | ... | ... | ... | ... |




Cyber@
Ben-Gurion University
of the Negev

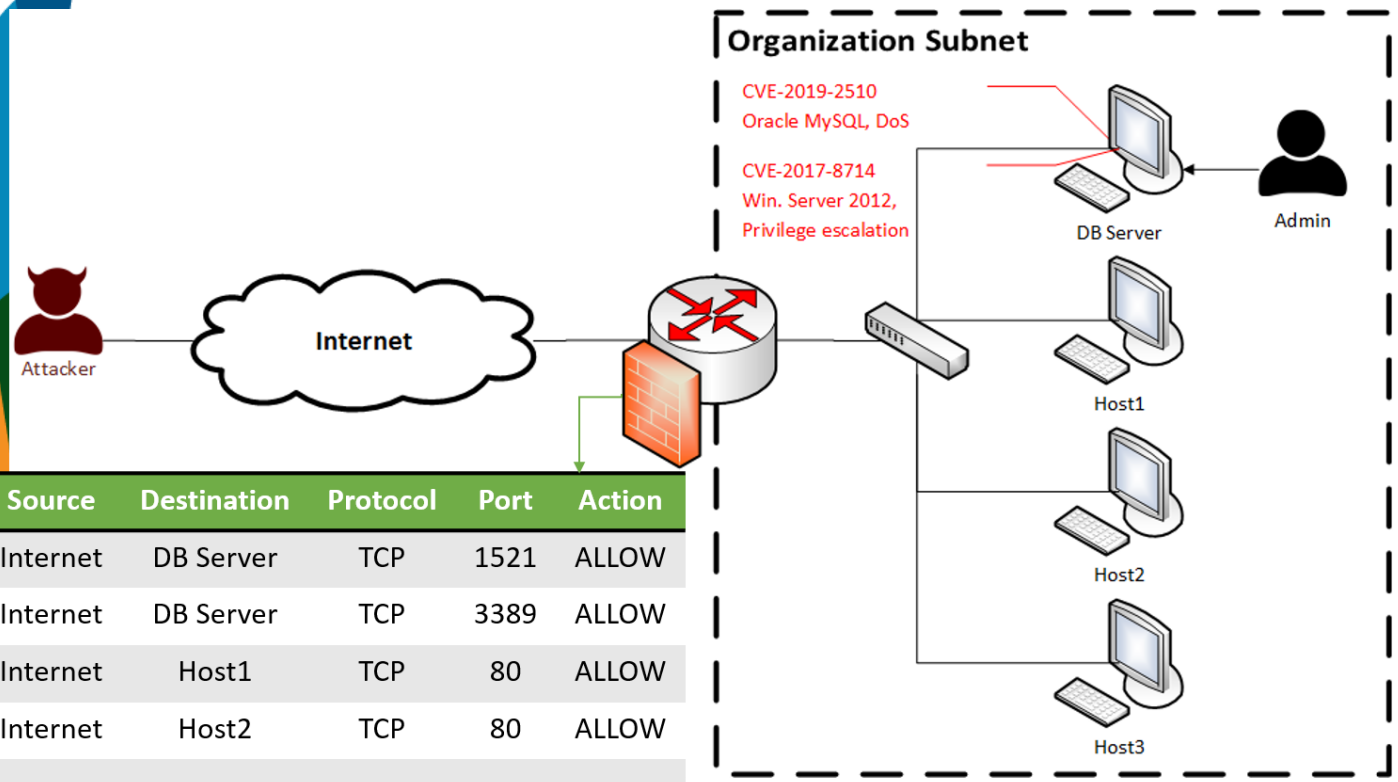
NEC

# Step 1: Attack Graph Generation



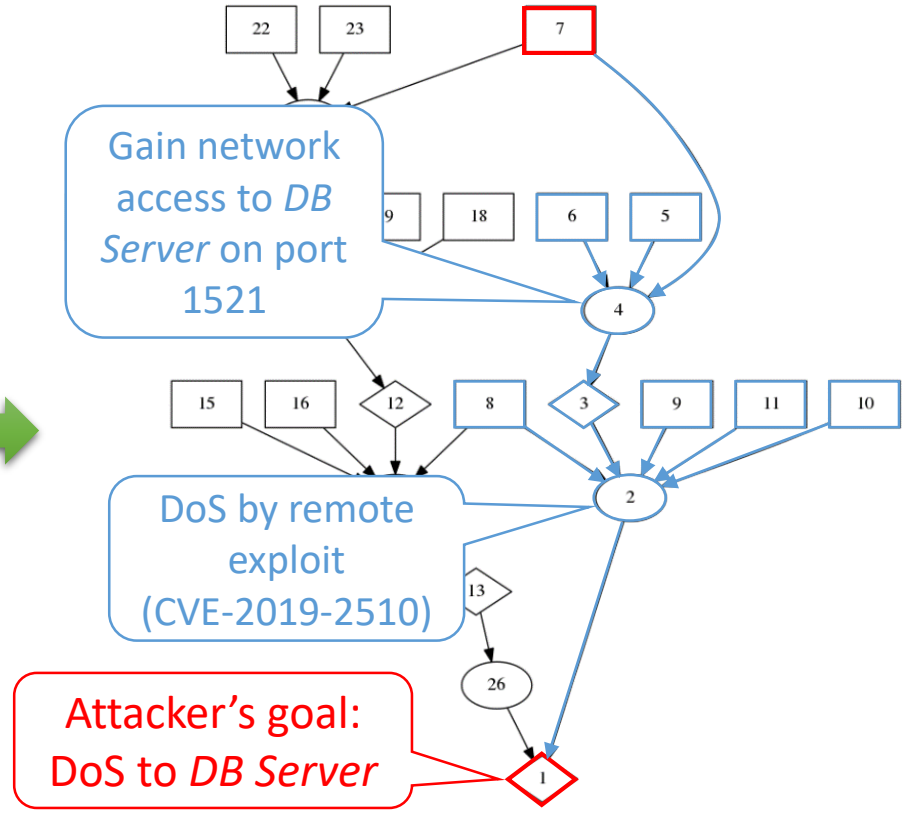

| Source | Destination | Protocol | Port | Action |
|---|---|---|---|---|
| Internet | DB Server | TCP | 1521 | ALLOW |
| Internet | DB Server | TCP | 3389 | ALLOW |
| Internet | Host1 | TCP | 80 | ALLOW |
| Internet | Host2 | TCP | 80 | ALLOW |
| ... | ... | ... | ... | ... |

# Step 1: Attack Graph Generation




| Source | Destination | Protocol | Port | Action |
|---|---|---|---|---|
| Internet | DB Server | TCP | 1521 | ALLOW |
| Internet | DB Server | TCP | 3389 | ALLOW |
| Internet | Host1 | TCP | 80 | ALLOW |
| Internet | Host2 | TCP | 80 | ALLOW |
| ... | ... | ... | ... | ... |

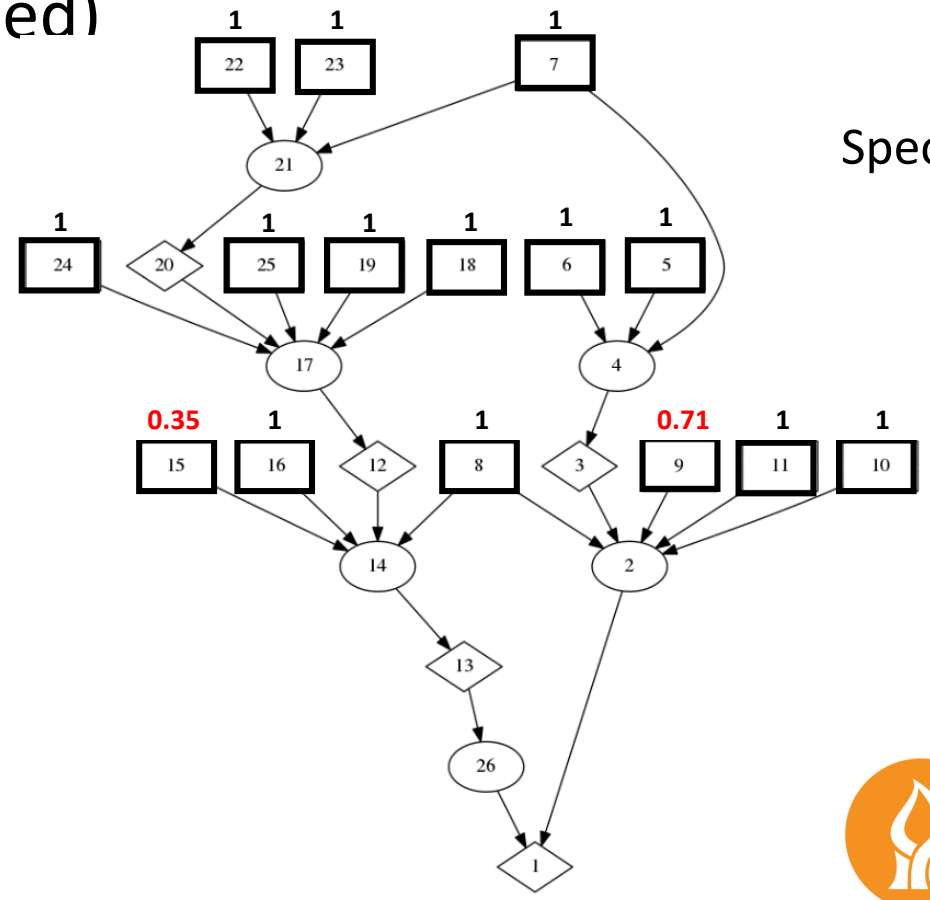
Attack Path II




NEC CBG Cyber@ Ben-Gurion University of the Negev NEC

# Attack Graph-Based Risk Calculation

1. Assign basic probabilities to primitive predicates (CVSS based)




Primitive facts (leaves)

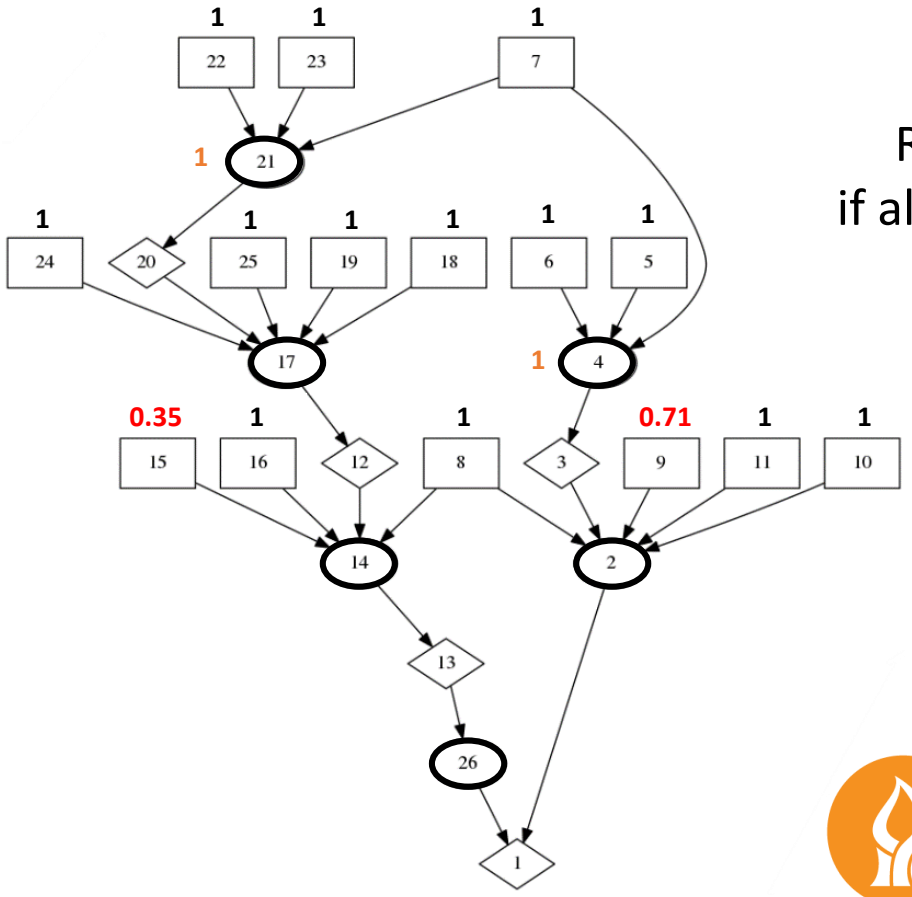
Specify the existing conditions in the system

$$P(n_{vuln}) = \begin{cases} 0.35, & if\ AC = HIgh \\ 0.61, & if\ AC = Medium \\ 0.71, & if\ AC = Low \end{cases}$$

$$P(n_{\overline{vuln}}) = 1$$

# Attack Graph-Based Risk Calculation

2. Recursively compute the probability for succeeding nodes.



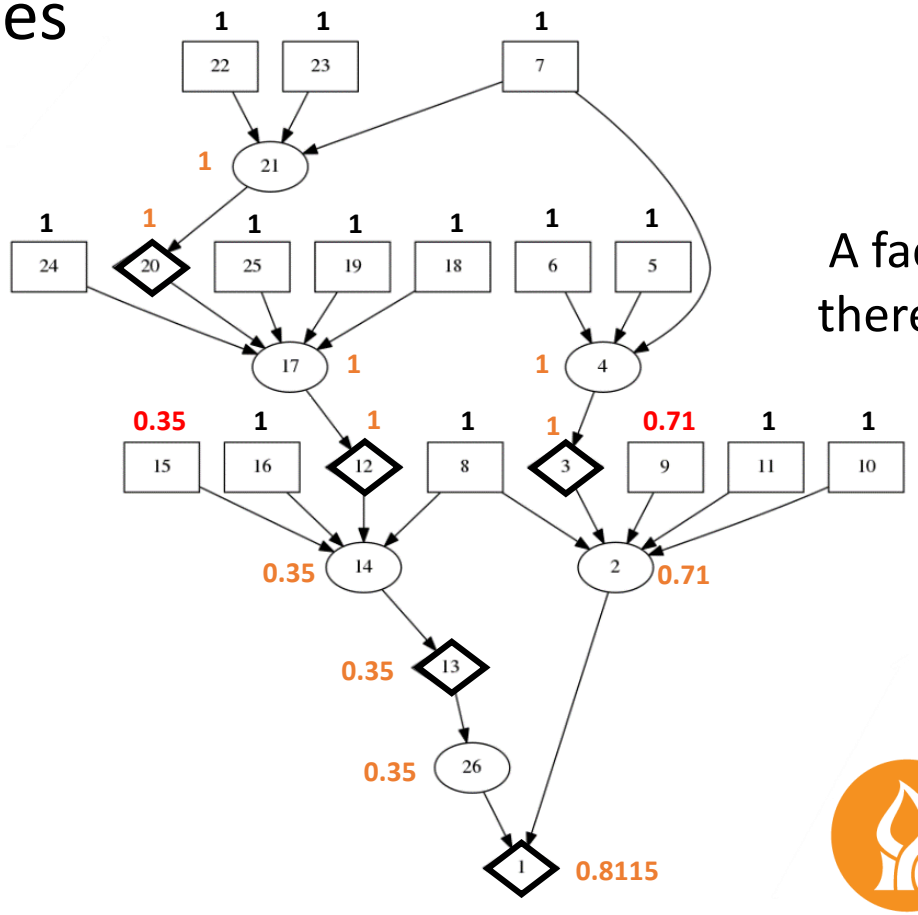

Derivation (AND) nodes

Represent the inference of new facts:
if all patent nodes are true – then the child node is also true

$$P(AND) = \prod_{n \in AND_{IN}} P(n)$$

# Attack Graph-Based Risk Calculation

2. Recursively compute for derivation (AND) and derived (OR) nodes



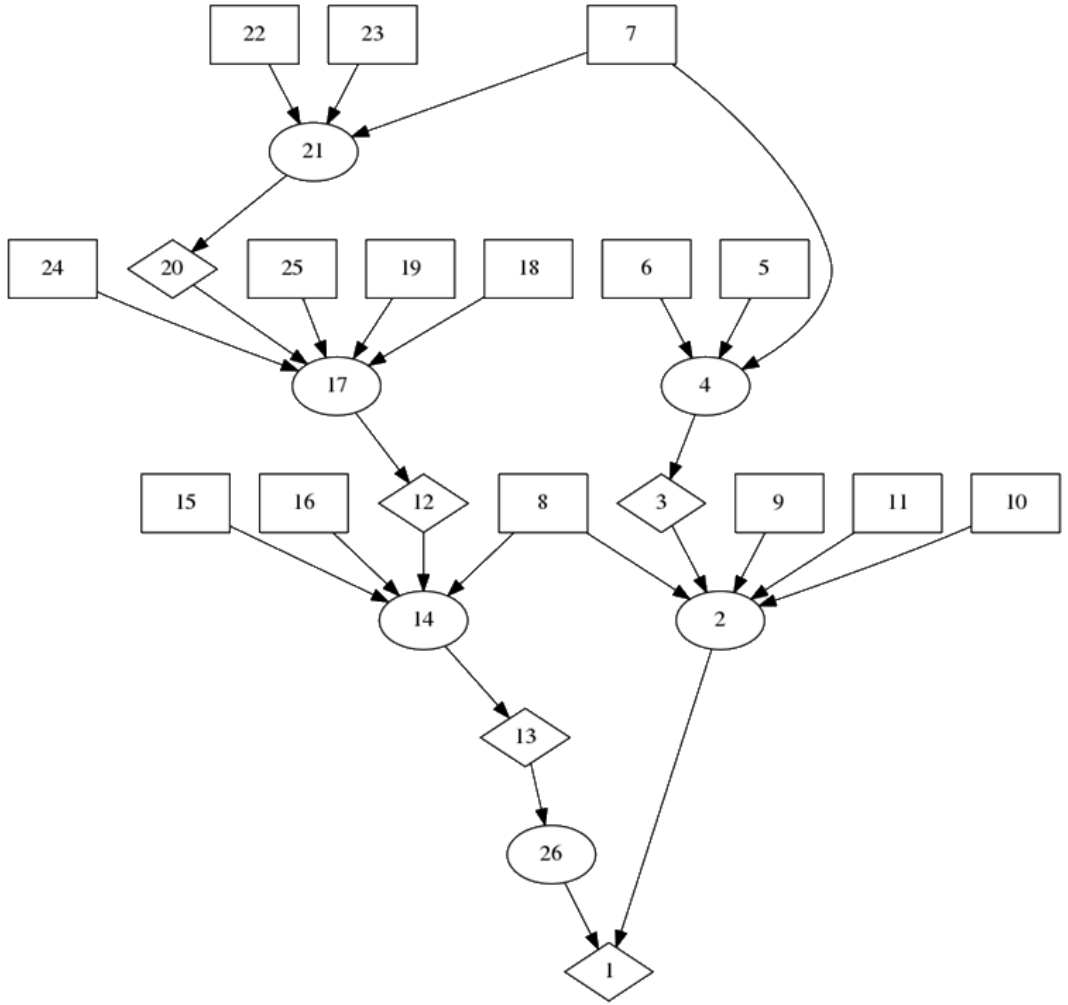

Derived facts (OR nodes)

The facts inferred by AND nodes

A fact can be derived by several AND nodes, therefor it is sufficient that **one** of the parent nodes is true

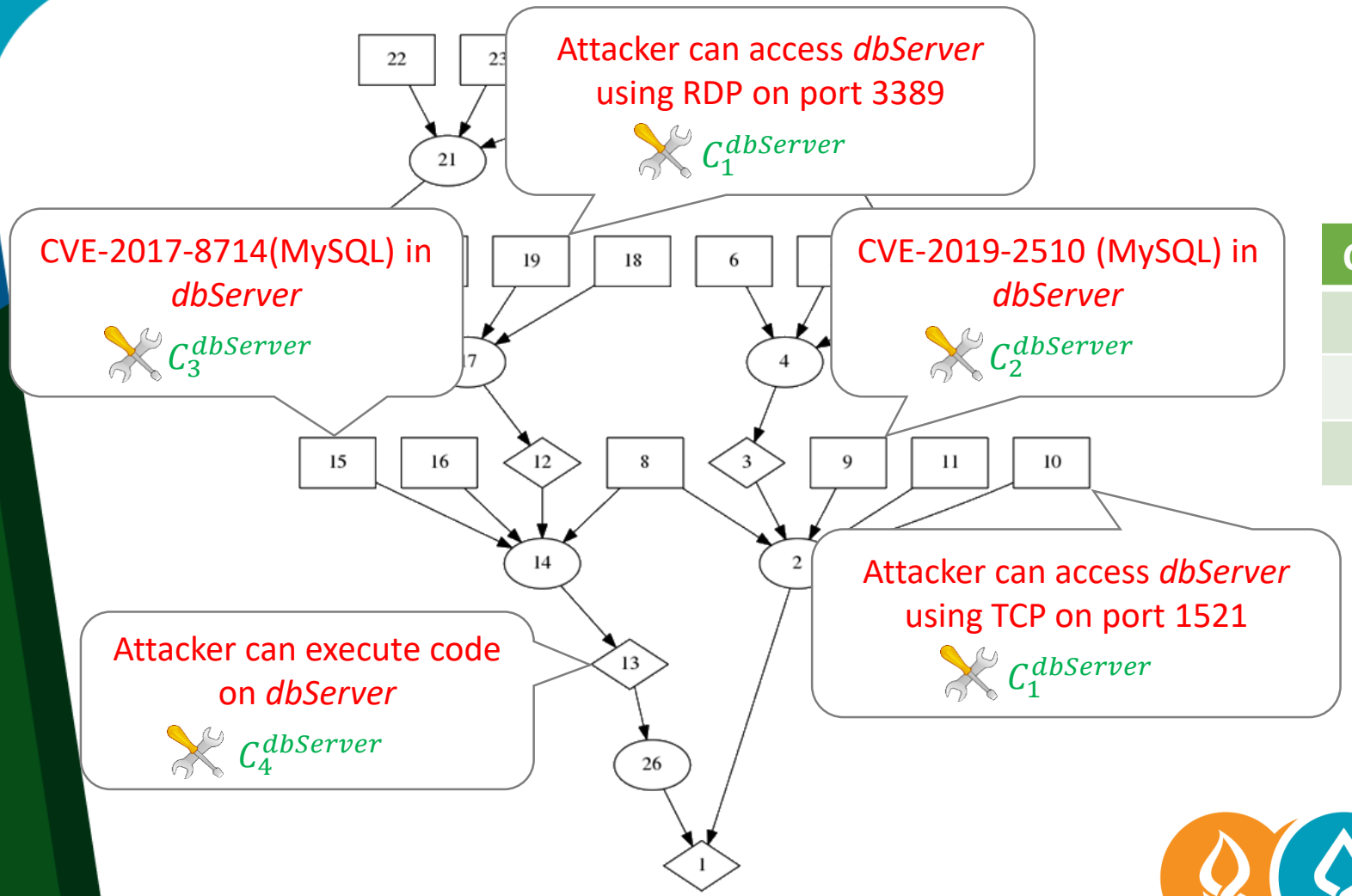
$$P(\mathrm{OR}) = 1 - \prod_{n \in \mathrm{OR}_{IN}} \left(1 - P(n)\right)$$

# Step 2: Countermeasure Identification




| Countermeasure | Type |
|---|---|
| $C_1$ | Host-Based Firewall |
| $C_2, C_3$ | Patch |
| $C_4$ | EDR |

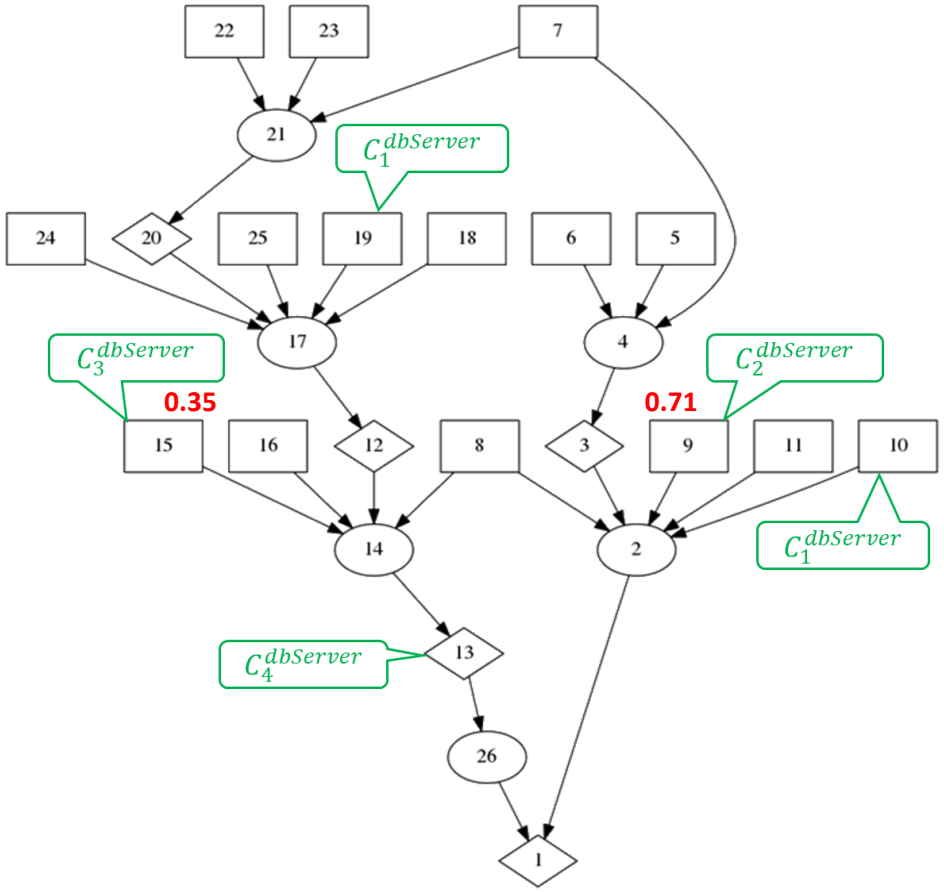
# Step 2: Countermeasure Identification




| Countermeasure | Type |
|---|---|
| $C_1$ | Host-Based Firewall |
| $C_2, C_3$ | Patch |
| $C_4$ | EDR |

# Step 3: Likelihood Equations Generation

- Integrate countermeasures into the likelihood equations




$$cm = \begin{cases} 0, & cm\ is\ implemented \\ 1, & cm\ is\ \boldsymbol{not}\ implemented \end{cases}$$

$$LH(LEAF) = \left( \prod_{cm \in LEAF_{CM}} cm \right) \cdot P(LEAF)$$

$$LH(AND) = \prod_{n \in AND_{IN}} LH(n)$$

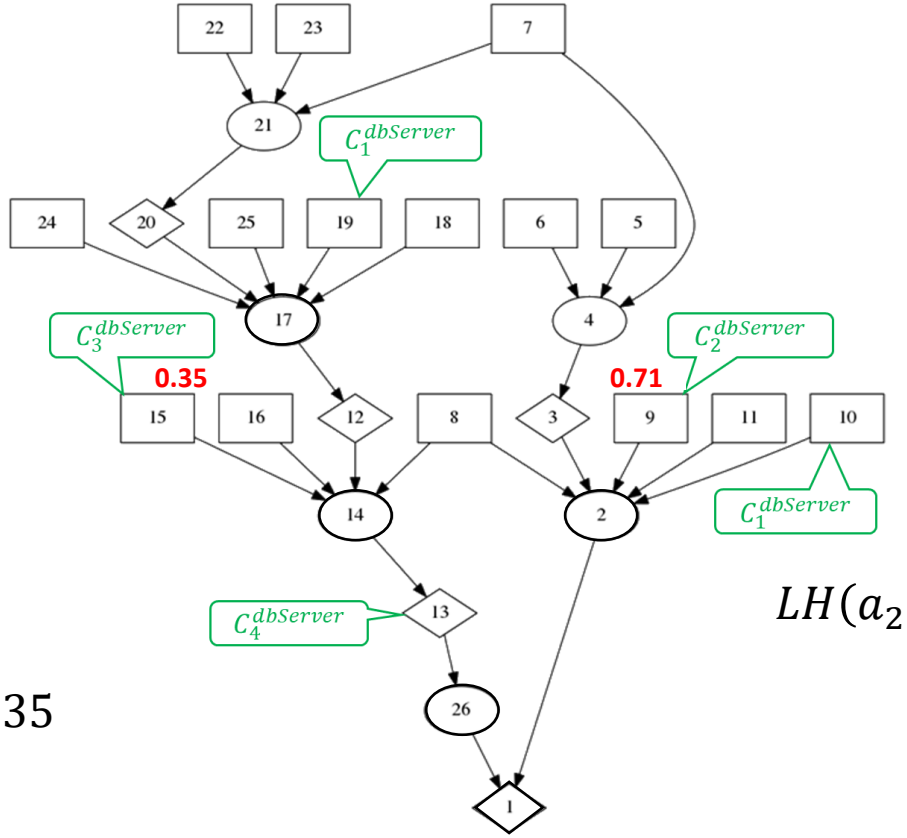
$$LH(\mathrm{OR}) = \left( \prod_{cm \in OR_{CM}} cm \right) \cdot \left( 1 - \prod_{n \in \mathrm{OR}_{IN}} (1 - LH(n)) \right)$$

# Step 3: Likelihood Equations Generation

$LH(a_{17}) = C_1$

$LH(a_{14}) = C_3 \cdot C_1 \cdot 0.35$

$LH(a_{26}) = C_4 \cdot C_3 \cdot C_1 \cdot 0.35$

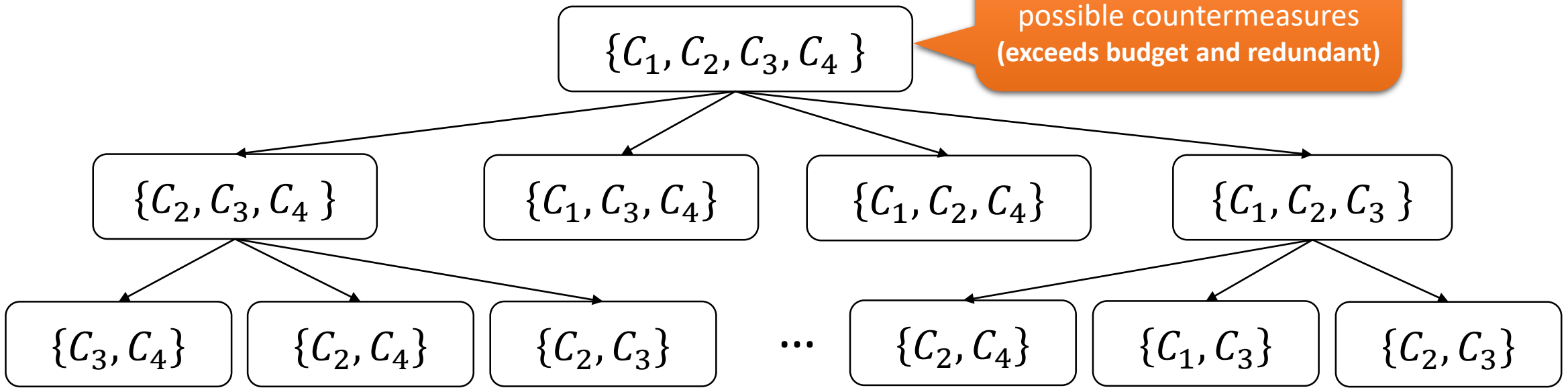



$LH(a_2) = C_2 \cdot C_1 \cdot 0.71$

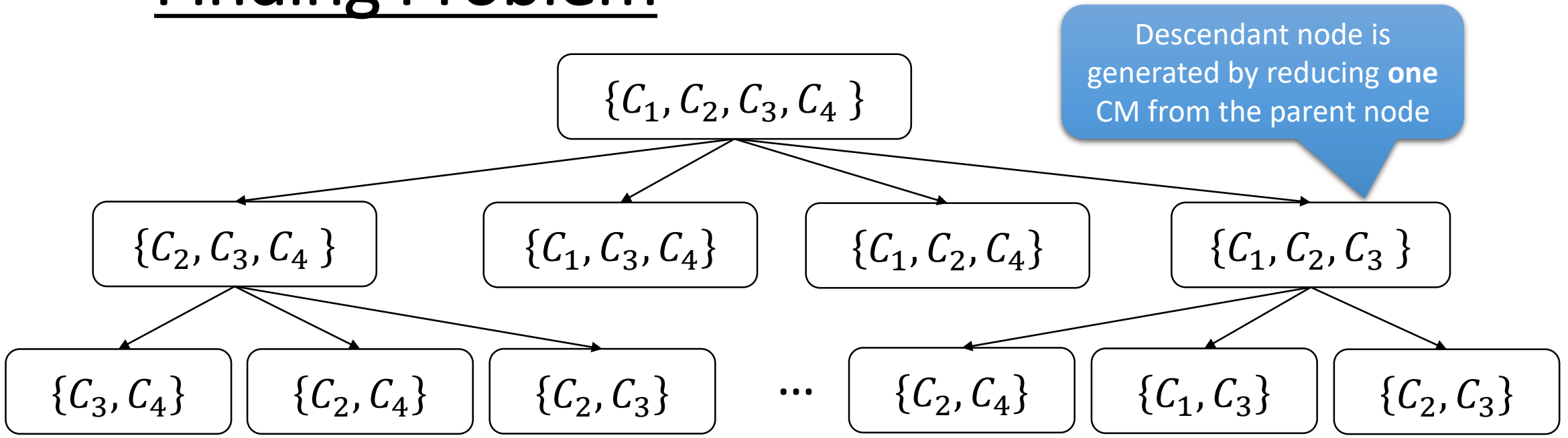
$LH(a_1) = 1 - \left((1 - C_4 \cdot C_3 \cdot C_1 \cdot 0.35) \cdot (1 - C_2 \cdot C_1 \cdot 0.71)\right)$

$Risk(n) = I_{a_1} \cdot LH(a_1|n)$

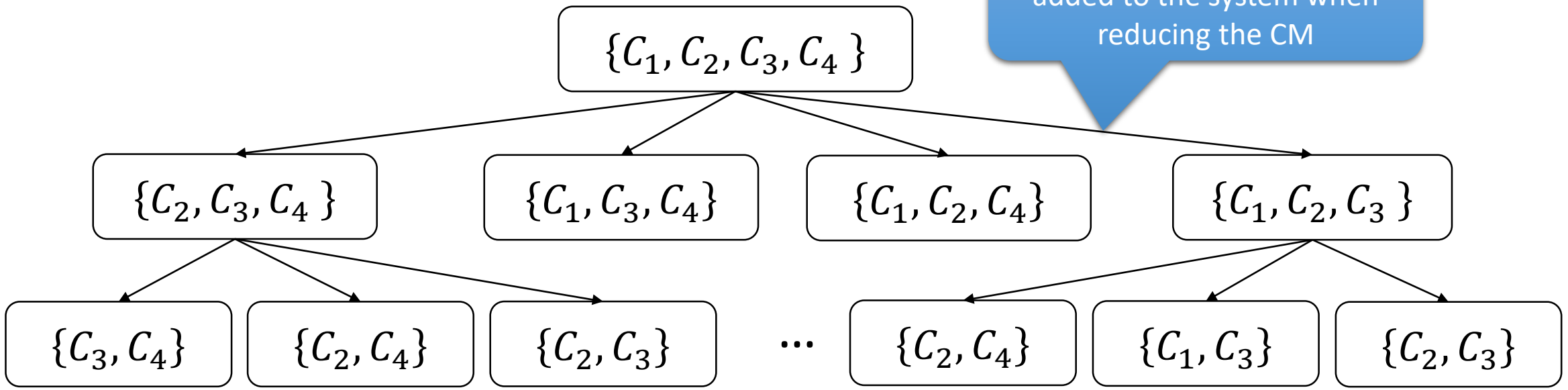
# Countermeasure Selection as a Path-Finding Problem



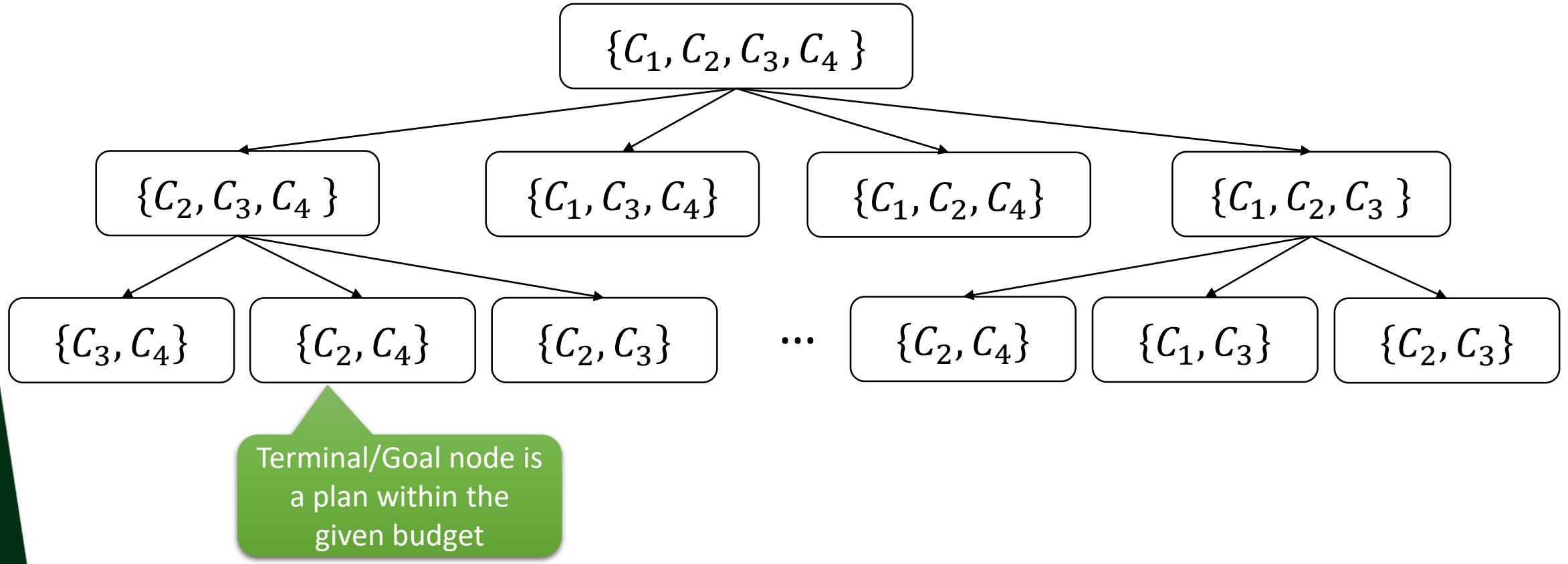
# Countermeasure Selection as a Path-Finding Problem



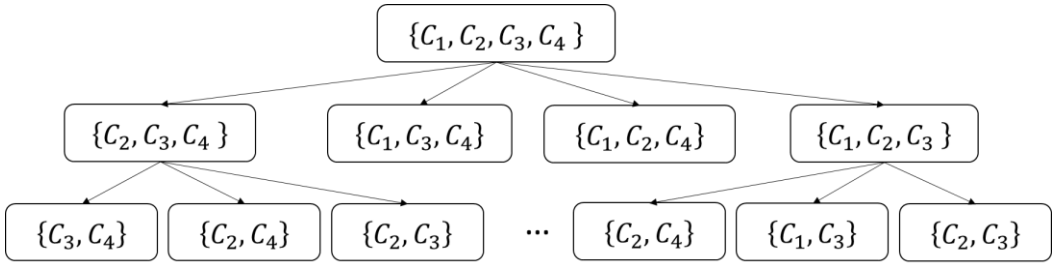
# Countermeasure Selection as a Path-Finding Problem



# Countermeasure Selection as a Path-Finding Problem



# Countermeasure Selection as a Path-Finding Problem




$$f(n) = g(n) + h(n)$$

*f-value* – an estimation of the risk under a subset of the countermeasure plan *n* that is within the budget

*g-value* – the actual risk under countermeasure plan *n*

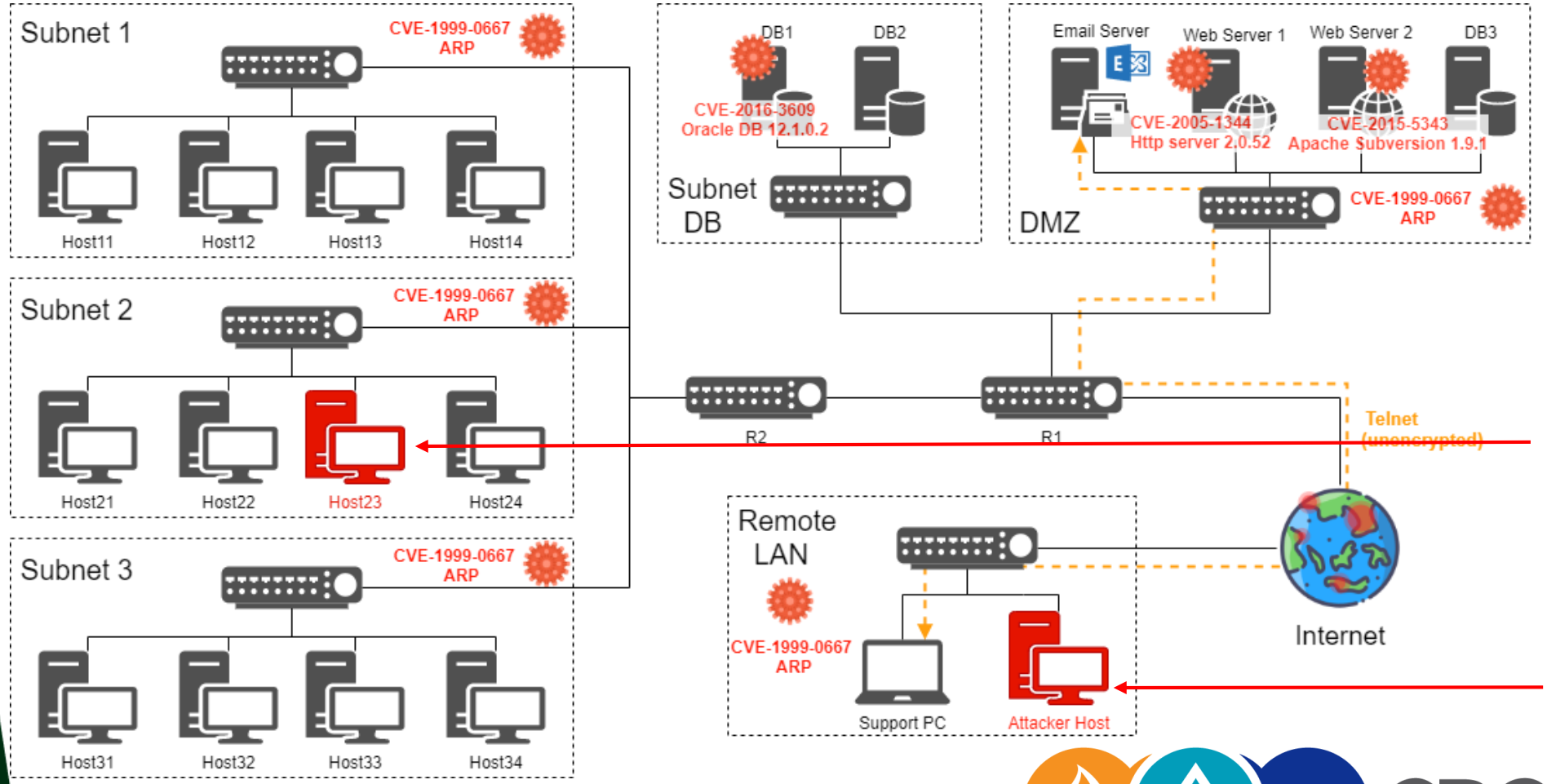
*h-value* – a lower bound of the risk that must be added to plan *n* to satisfy the budget constraint.

# A* Solver

**Algorithm 2** A* Solver

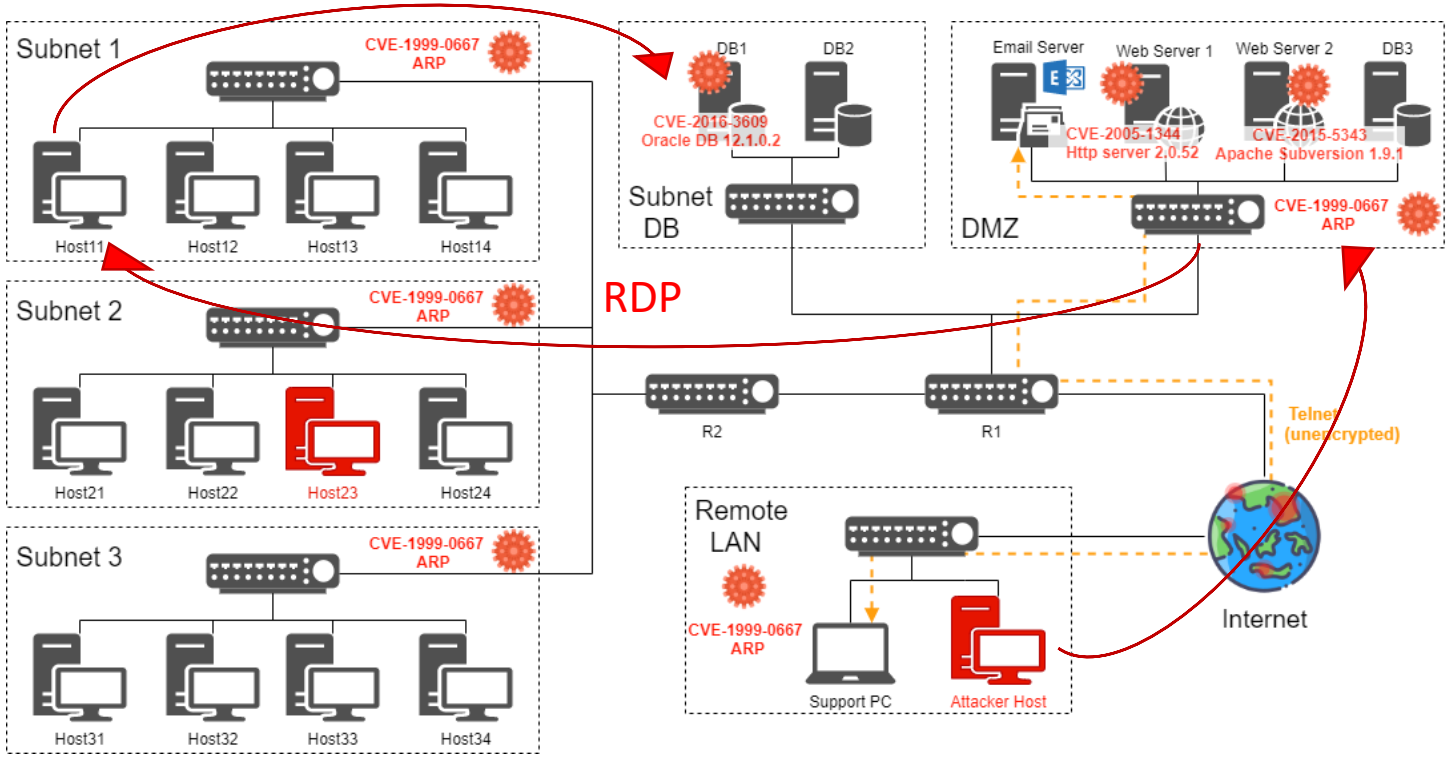
```
1: Inputs:
2:     RiskEq ← Risk equations
3:     initial ← Relevant countermeasures
4:     B ← Budget
5: Initialize:
6:     OpenList ← PriorityQueue()
7:     ClosedList ← []
8: procedure A*-SOLVER(RiskEq, initial, B)
9:     addToOpenList(initial, RiskEq)
10:    while !OpenList.isEmpty() do
11:        plan ← OpenList.poll()
12:        if Cost(plan) ≤ B then
13:            return plan
14:        end if
15:        ClosedList.append(plan)
16:        for each cm ∈ plan do
17:            newPlan ← plan \ {cm}
18:            if !(newPlan ∈ OpenList)&&!(newPlan ∈
   ClosedList) then
19:                addToOpenList(newPlan, RiskEq)
20:            end if
21:        end for
22:    end while
23: end procedure
24: procedure ADDTOOPENLIST(plan,RiskEq)
25:    plan.g ← ComputeRisk(plan, RiskEq)
26:    plan.h ← h(plan, RiskEq)
27:    plan.f ← plan.g + plan.h
28:    OpenList.add(plan)
29: end procedure
```

# Evaluation Environment



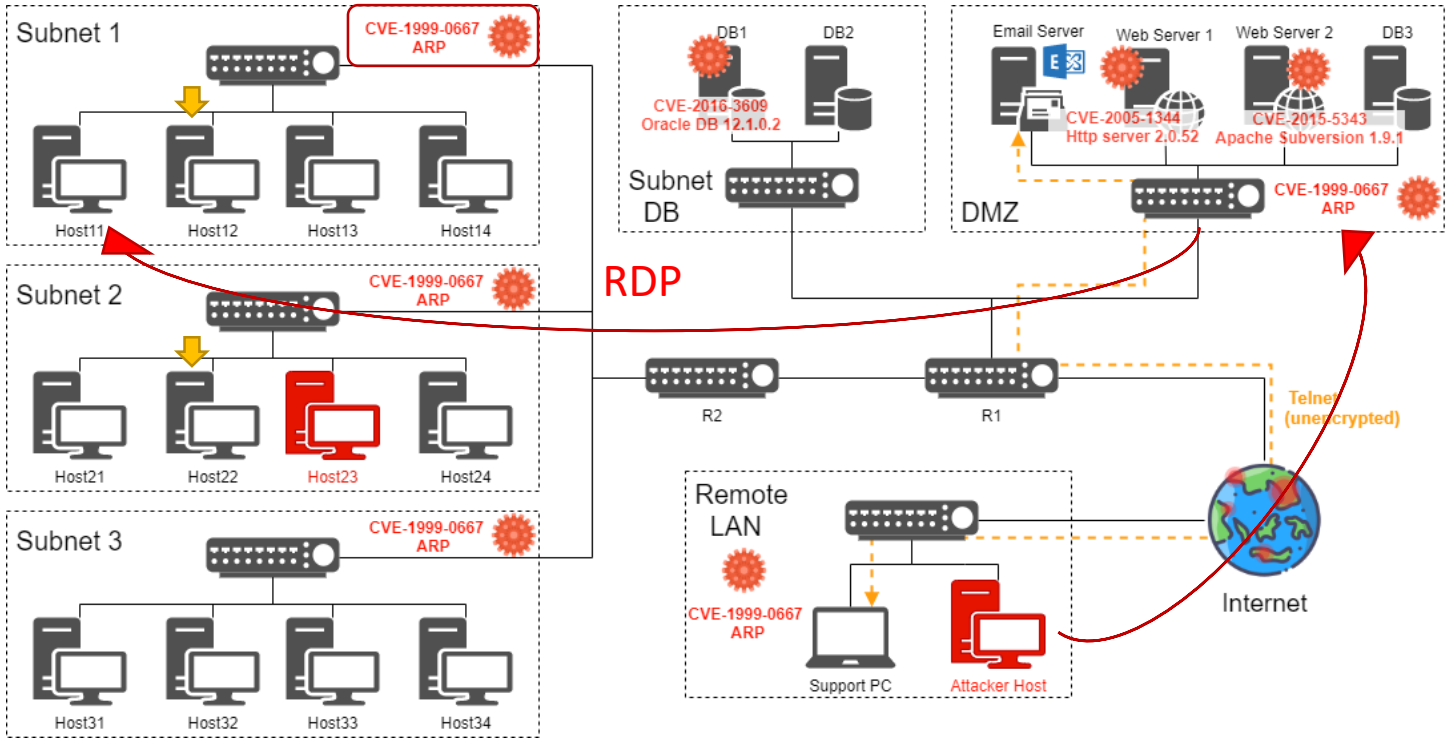
# Evaluation Environment – Attacks

1. Access sensitive information on DB1



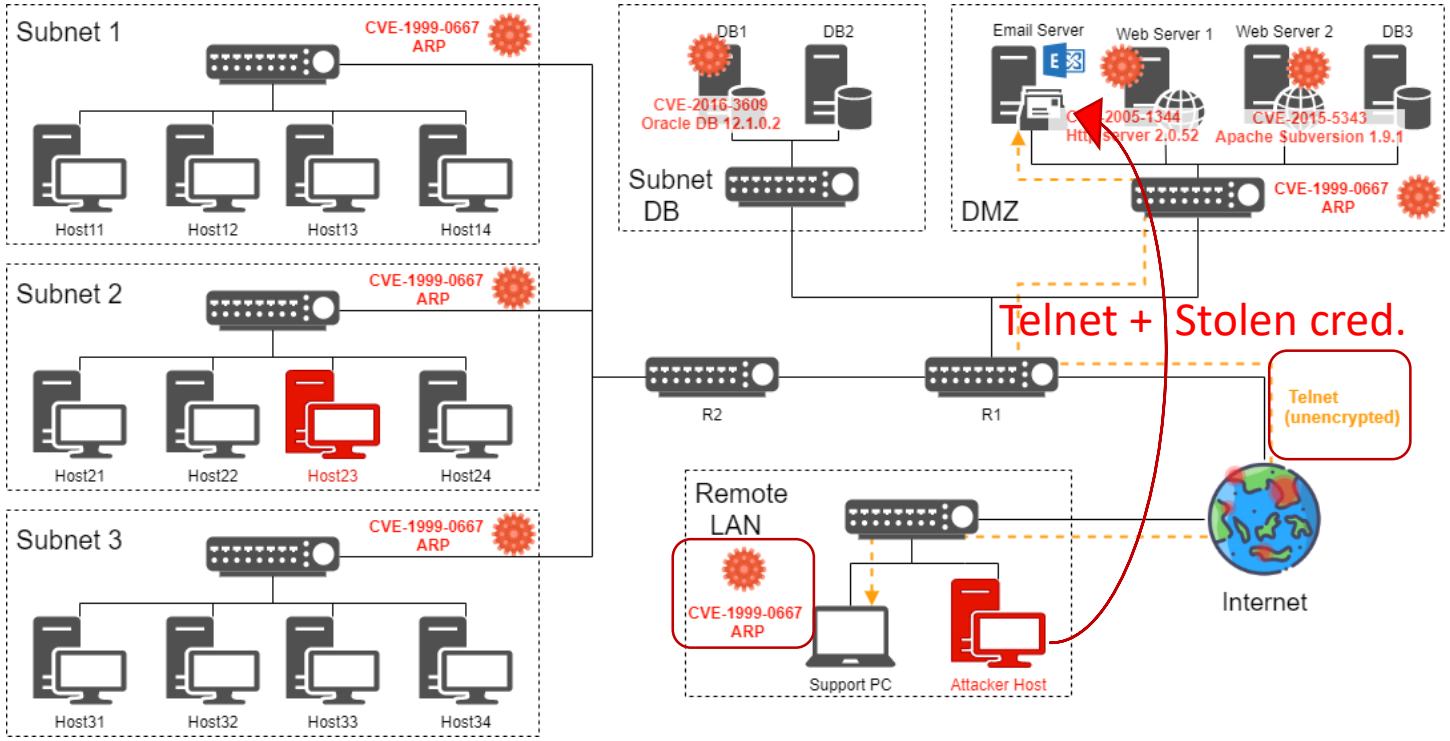
# Evaluation Environment – Attacks

1. Access sensitive information on DB1
2. Spoof Host12-Host22 communication



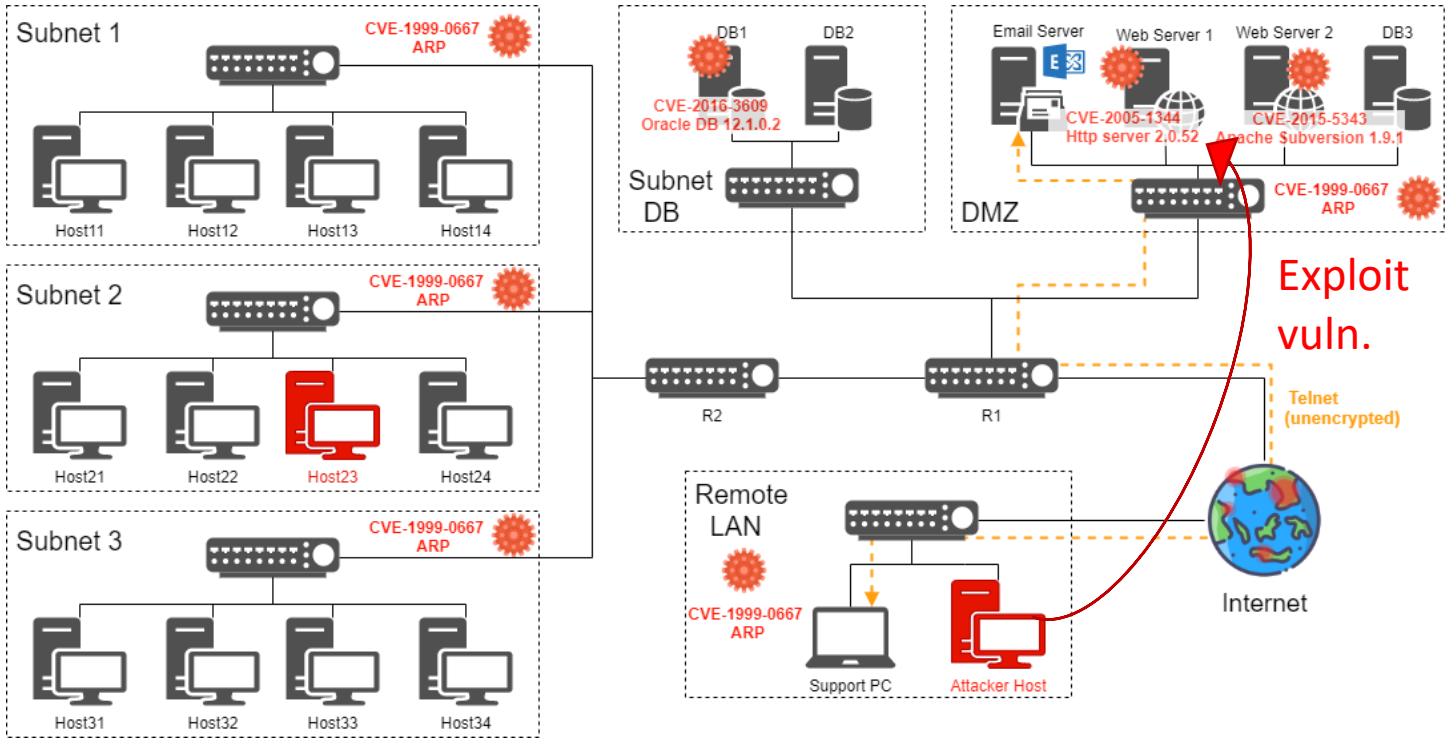
# Evaluation Environment – Attacks

1. Access sensitive data on DB1
2. Spoof Host12-Host22 communication
3. Access sensitive data on Email Server



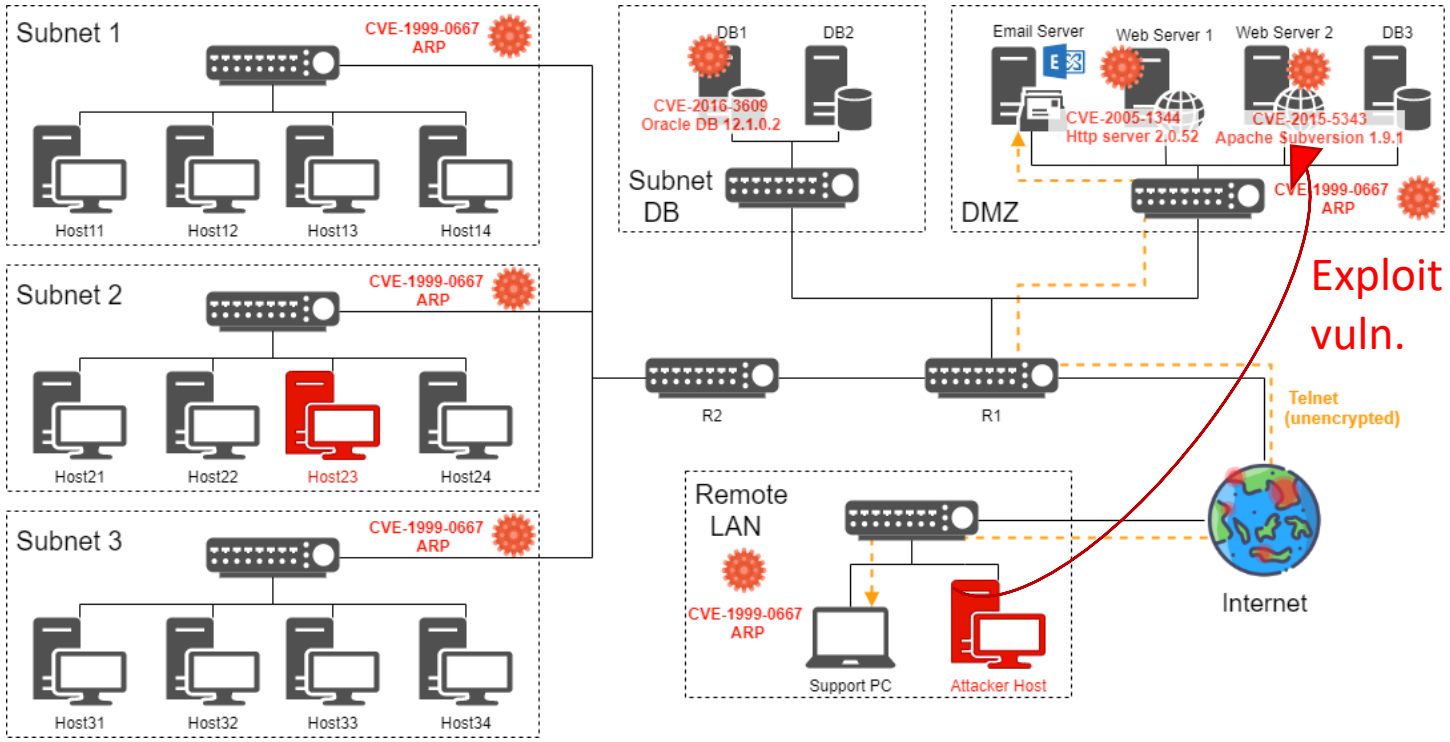
# Evaluation Environment – Attacks

1. Access sensitive data on DB1
2. Spoof Host12-Host22 communication
3. Access sensitive data on Email Server
4. Run code on Web Server 1



# Evaluation Environment – Attacks

1. Access sensitive data on DB1
2. Spoof Host12-Host22 communication
3. Access sensitive data on Email Server
4. Run code on Web Server 1
5. Denial of service to Web Server 2

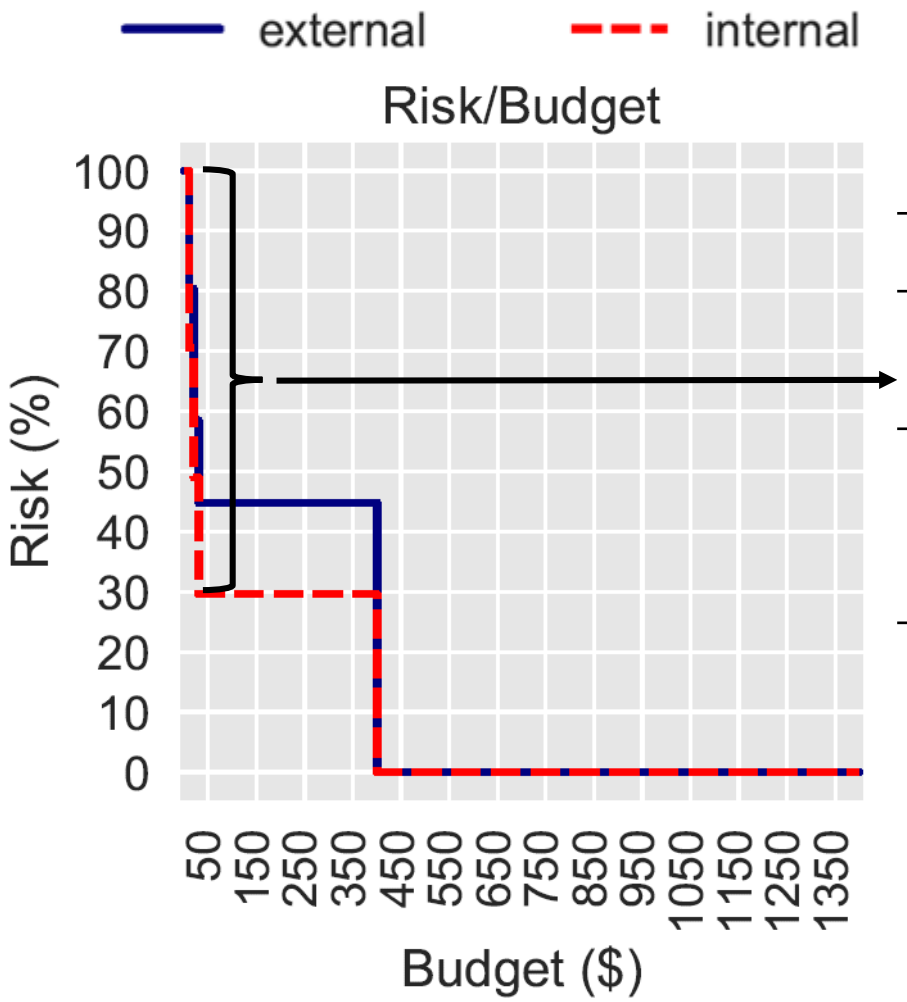


# Evaluation Environment

- Possible countermeasures:

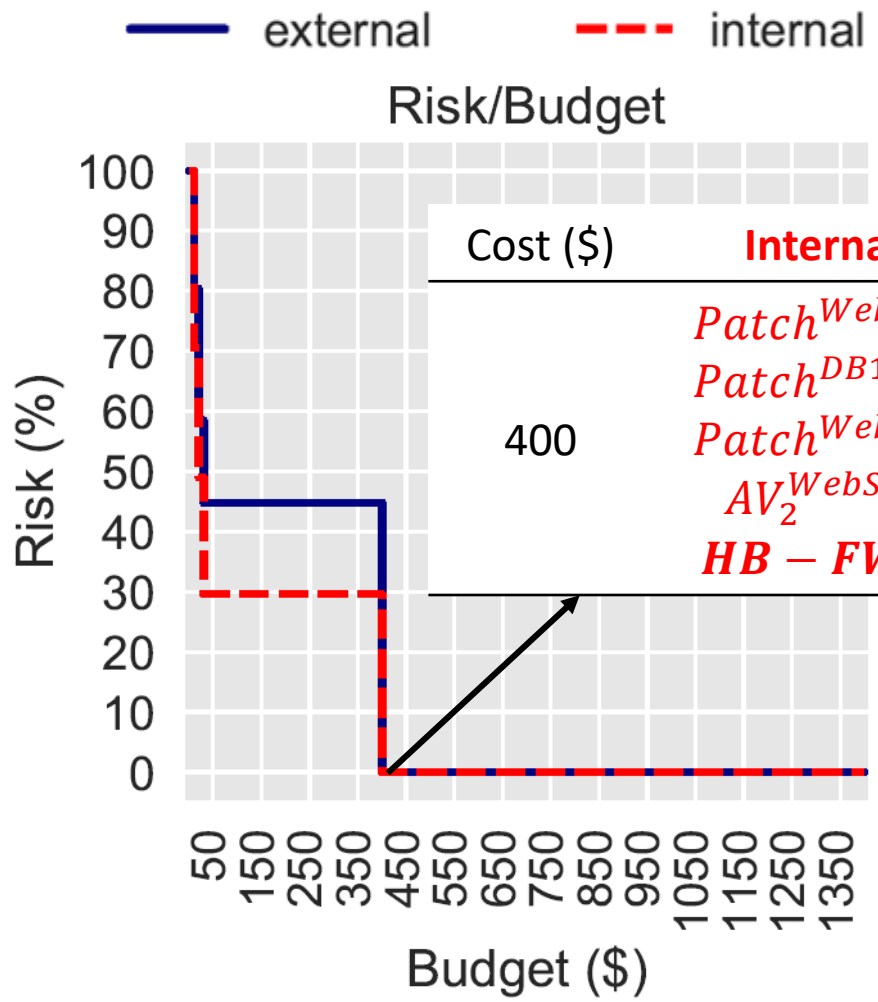
| Product | Type | Cost ($)<br>Deploy / Update |
|---|---|---|
| Cisco Next-Gen Firewall | Network-based firewall | 1000 / 10 |
| ZoneAlarm | Host-based firewall | 300 / 10 |
| Snort | Network-based IPS | 1000 / 10 |
| Wazuh | Host-based IPS | 300 / 10 |
| McAfee EDR | EDR | 50 / – |
| Kaspersky EDR | | |
| Various | Patch | – / 10 |

# Evaluation Results



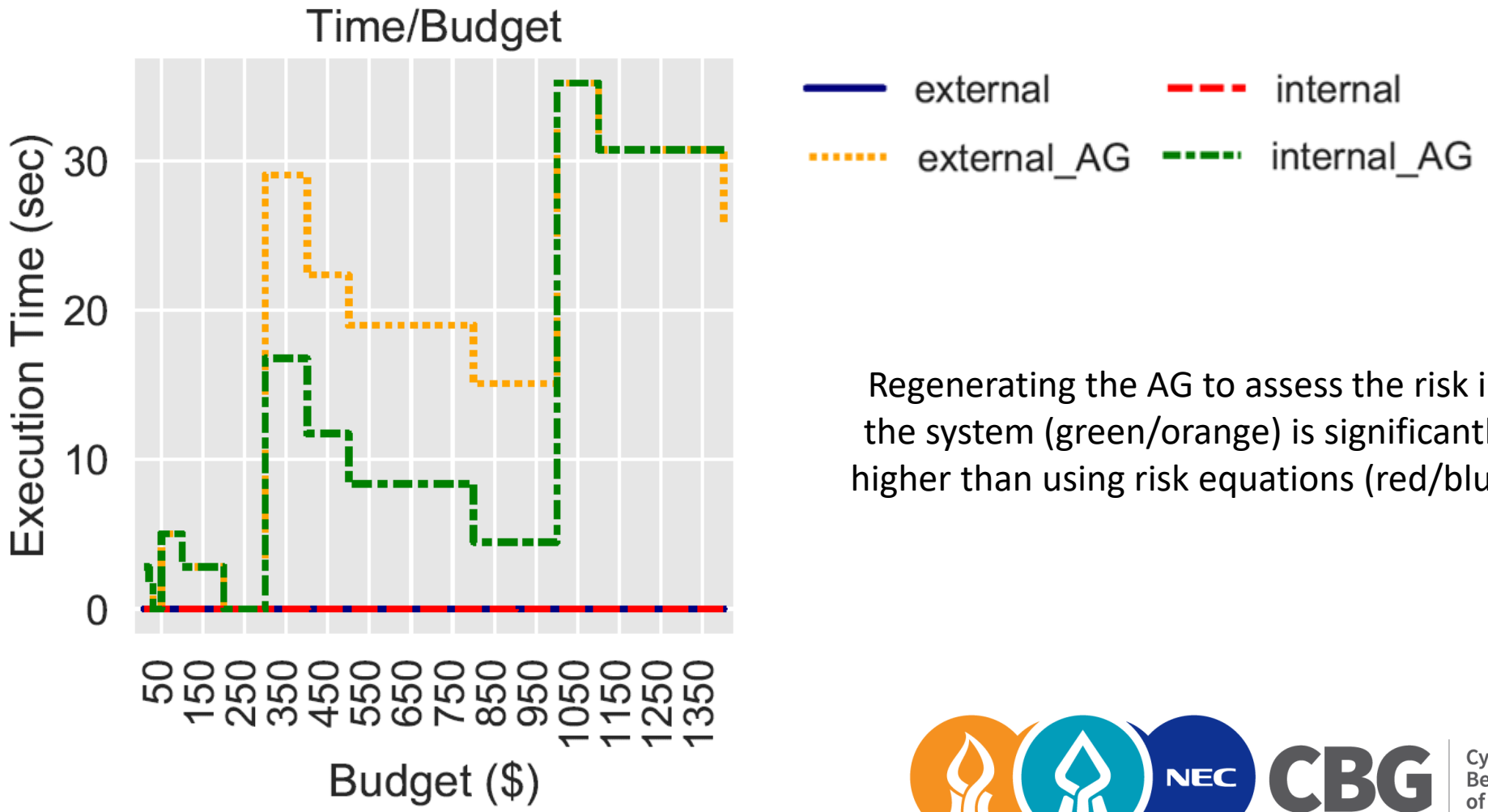

| Cost ($) | Internal Plan | External Plan |
|---|---|---|
| 10 | $Patch^{WebServer1}$ | $Patch^{WebServer1}$ |
| 20 | $Patch^{WebServer1}$, $\boldsymbol{Patch^{DB1}}$ | $Patch^{WebServer1}$, $\boldsymbol{Patch^{WebServer2}}$ |
| 30 | $Patch^{WebServer1}$, $Patch^{DB1}$, $Patch^{WebServer2}$ | $Patch^{WebServer1}$, $Patch^{WebServer2}$, $Patch^{DB1}$ |

# Evaluation Results




| Cost ($) | Internal Plan | External Plan |
|---|---|---|
| 400 | $Patch^{WebServer1}$, $Patch^{DB1}$, $Patch^{WebServer2}$, $AV_2^{WebServer1}$, $\boldsymbol{HB-FW^{Host11}}$ | $Patch^{WebServer1}$, $Patch^{WebServer2}$, $Patch^{DB1}$, $AV_2^{WebServer1}$, $\boldsymbol{HB-IPS^{EmailServer}}$ |

# Evaluation Results




Regenerating the AG to assess the risk in the system (green/orange) is significantly higher than using risk equations (red/blue)

# Conclusions

- We suggest a heuristic approach for the countermeasure selection problem that considers the system's topology, vulnerabilities, and the interactions between them.
- Experiments show that our method provides cost-effective plans
- Comparison with other methods shows that our approach provides optimal plans (in terms of risk)

# Thank you


CBG

Cyber@
Ben-Gurion University
of the Negev

NEC