Countermeasure against Insider Threat Regarding Psychological State of Organizational Members and Business Impact of Information Resources

<u>*Yuki Kodaka</u>(y_kodaka@nii.ac.jp), **Hirokazu Hasegawa, **Hiroki Takakura

*The Graduate University for Advanced Studies (SOKENDAI), Japan

**Center for Strategic Cyber Resilience R&D, National Institute of Informatics, Japan

Resume of Presenter

- **Name : Yuki Kodaka**
- Affiliation : The graduate university for advanced studies(SOKENDAI), Japan
- Contact information

  Email address : y_kodaka@nii.ac.jp
- Research interest :

  Insider Threat Countermeasure, Dynamic Access Control.

Research Background

- Insider threat：
  - Former employees, contractors, other business partners
    - **Knowledge of systems and business processes**
    - **Hold legitimate access privileges**

  -> As a result, they can cause widespread damage across organization

- Report on on insider threat

  i. Average annual costs: $8.3 million in 2018, $15.38 million in 2022 [1]

  ii. Over 800 managers and IT professionals, 89% concern about insider threat but only 11% adequately prepared to address these threats [2]

->Countermeasure: Conduct risk assessment and develop a response plan

[1] P. Institute, “2022 cost of insider threats global report”, [retrieved: September, 2024], 2022,
[2] H. Poll, “Vormetric insider threat report”, [retrieved: September, 2024], 2015

Issues and Requirements for Insider Threat Countermeasure

① Difficulty in **identifying malicious activities**

- Hard to determine malicious intent only from outcome of action

-> Strengthen monitoring based on risk assessment

② Difficulty in **managing access records**

- Hard to detect malicious activities in large volumes of access records

-> Define critical operations in advance based on risk assessment

③ Difficulty in **detecting insider threats**

- Hard to detect malicious activities as they are often concealed

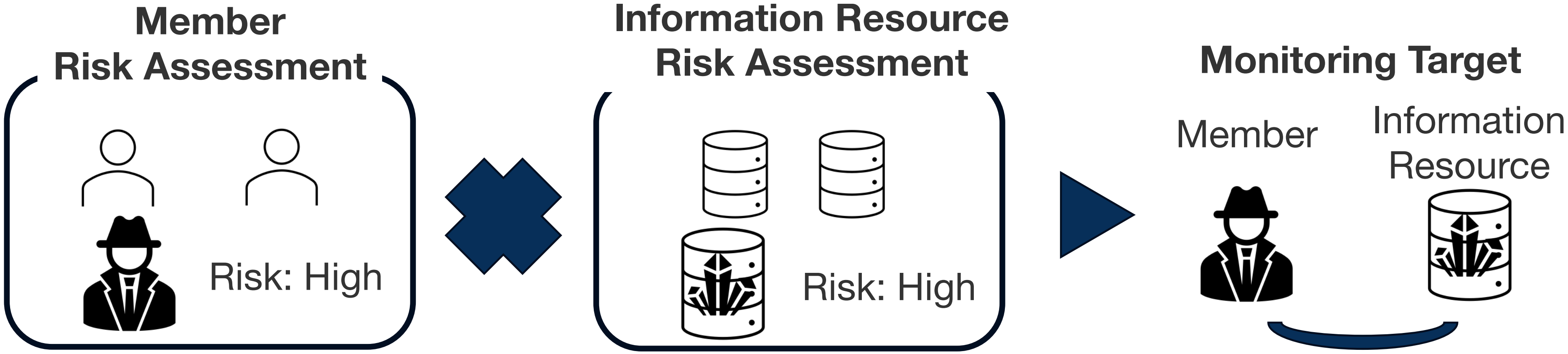
-> Detect signs of attacks early or ensure quick response after attack

Countermeasure against Insider Threat

Regarding Psychological State of Organizational Members

and Business Impact of Information Resources

- Insider threat risk assessment: data or system sabotage



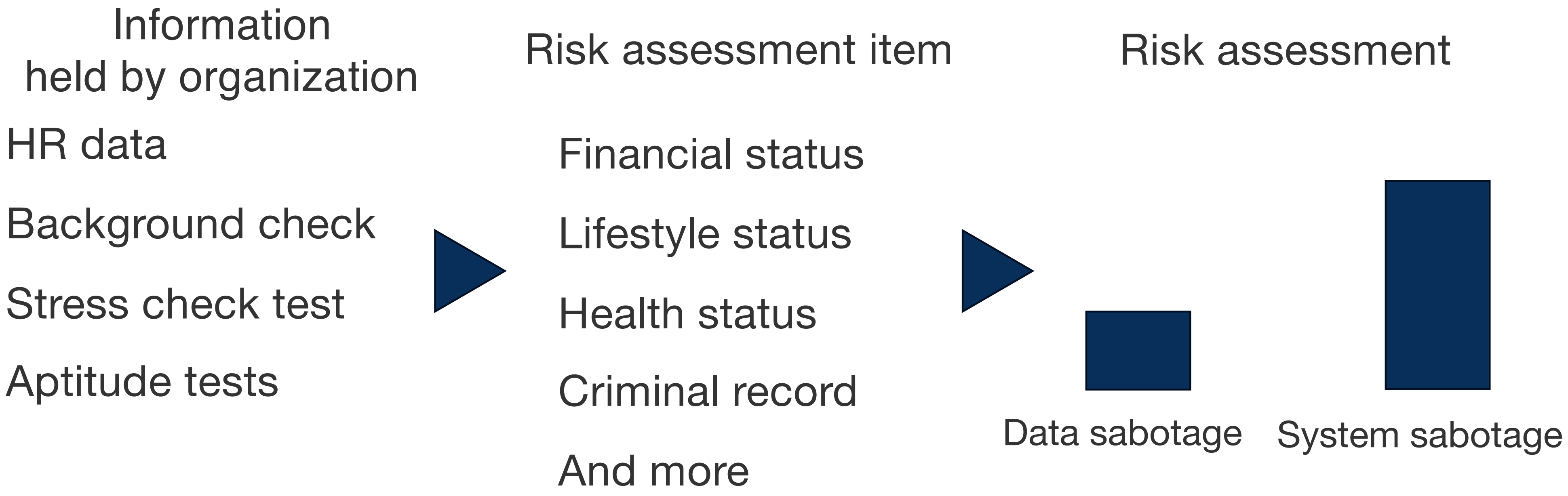
- Countermeasure
  - Prevent step-by-step attack at previous step
  - Roll back from executed attacks quickly using backup data

Member Risk Assessment-1

Member risk assessment：

Two classifications based on **Attribute** information and **Behavior** information

- Member risk assessment based on **Attribute** information



Information held by organization

HR data

Background check

Stress check test

Aptitude tests

Risk assessment item

Financial status

Lifestyle status

Health status

Criminal record

And more

Risk assessment

Member risk assessment item

- Financial status (annual income, debt, credits) [3, 5, 8, 21]
- Lifestyle status (family issues) [3, 14]
- Health status (drug addiction, alcoholism, mental illness) [14]
- Criminal record (arrests) [3, 21]
- Personality characteristics (excitement, neurotic tendency, hostility, lack of co-ordination, lack of conscience, self-love tendency) [3, 5, 21]
- Emotions (stress, lack of job satisfaction, anger, vengeance, lack of organizational belonging) [3, 5, 21]
- Personnel (demotion, termination, job change) [5, 14, 21]
- Job type (technical position) [14]
- Privilege (administrative privileges) [16]

Blue: System, Red: Data, Black: both

Member Risk Assessment-3

Binary conversion

Member	Finance status			Lifestyle status	Health status			…
	Annual income	dept	Credits	Family issue	Drug	Alcoholism	Mental illness	
A	1	1	1	0	0	0	0	
B	0	0	0	0	0	0	0	
…								

Applicable: 1, Otherwise: 0

- Annual income

  Industry, occupation, age group average

  Below:1, Over: 0

- Credits

  Long-term repayment delays

  Presence: 1, Absence: 0

Member risk assessment

Formula：

$$R_{category\_attribute\_member\_i}$$

$$= \frac{1}{n_{category}} \sum_x v_{x,category} \cdot w_{x,category}$$

$$0 \leq R_{category\_attribute\_member\_i} \leq 1$$

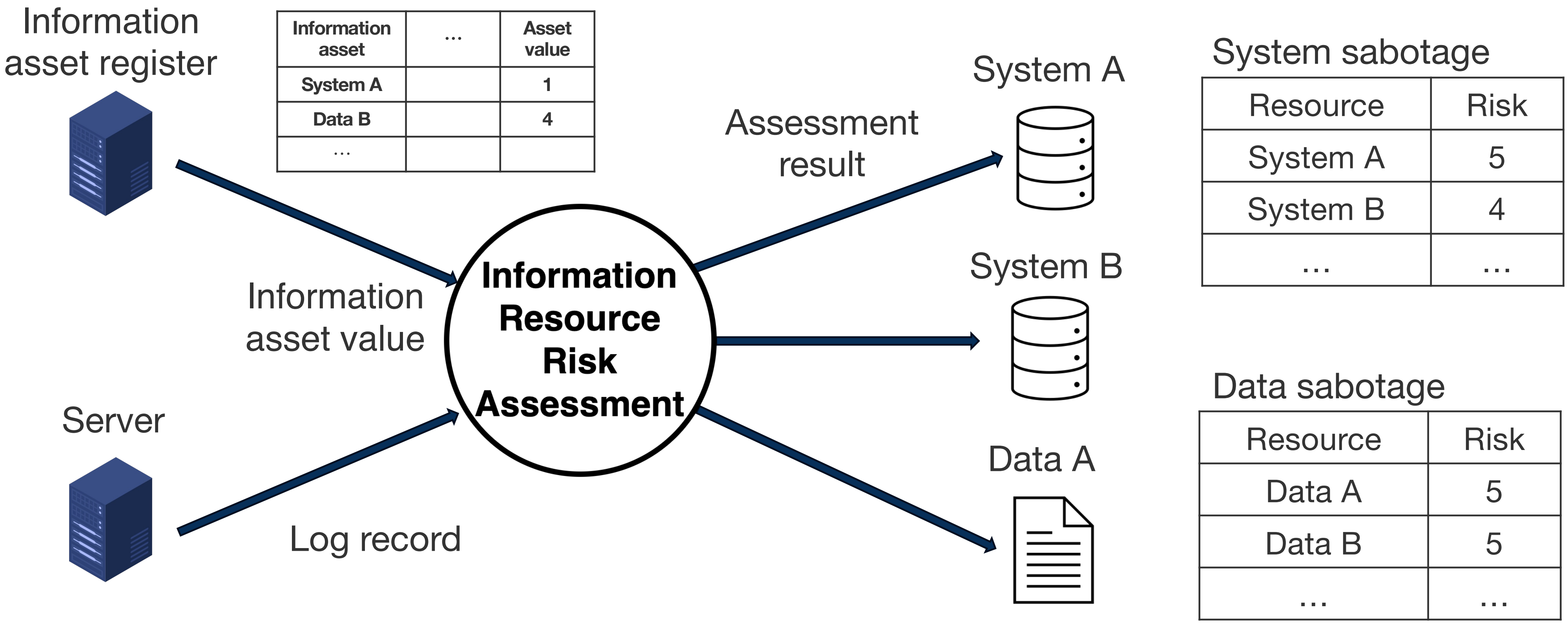
$category$: System or Data

$n_{category}$: Number of assessment items

$v_{x,category}$: Score of assessment item x

$w_{x,category}$: Weight of the assessment item x

Impact when system or data is targeted and destroyed



Information asset	…	Asset value
System A		1
Data B		4
…		

System sabotage

Resource	Risk
System A	5
System B	4
…	…

Data sabotage

Resource	Risk
Data A	5
Data B	5
…	…

Operation Monitoring of high-risk members on information resources

1. Pre-definition of operational path
2. Identification of next operation

   based on access privileges

$z = 1{,}2$ **Monitoring target** for Countermeasure

$z \geq 3$ Risk assessment item

as **Behavior** information

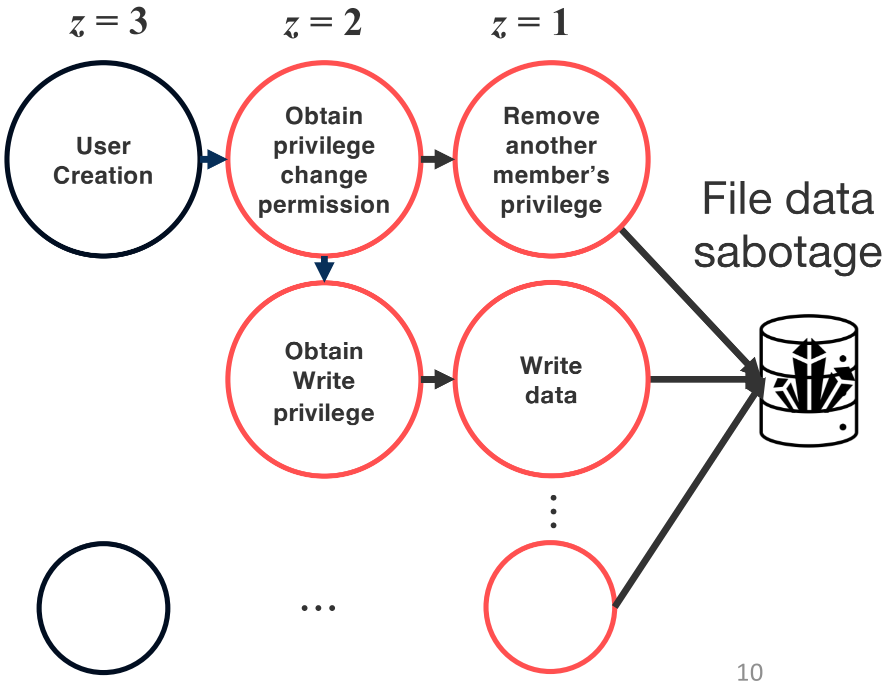
$$v_{y\ operation\_member\_i} = \frac{1}{2}\left(\frac{1}{s} \times D\right)$$

S : Number of steps to achieve sabotage activity

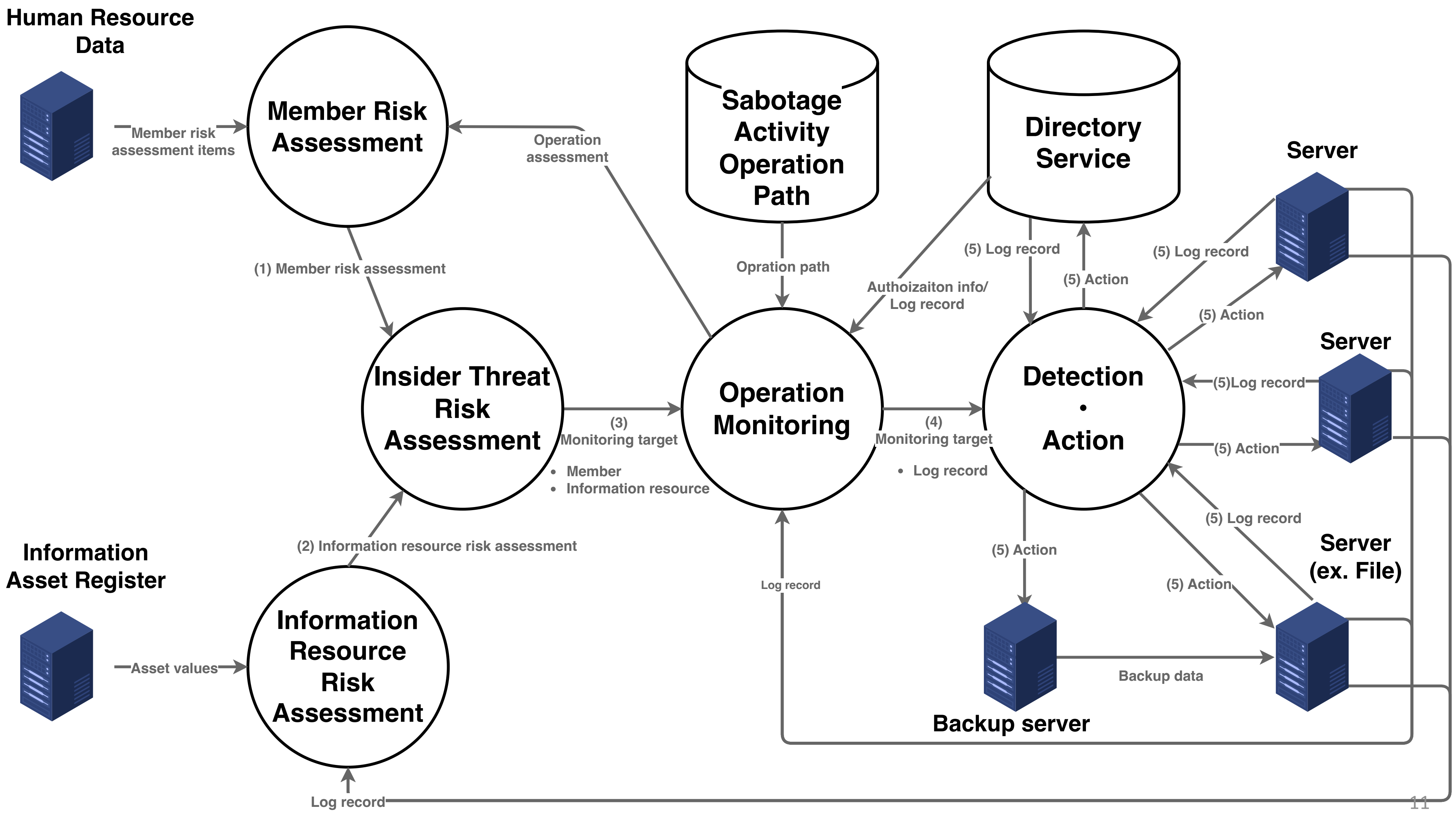
D : Number of connected next step operations

Example of operation path

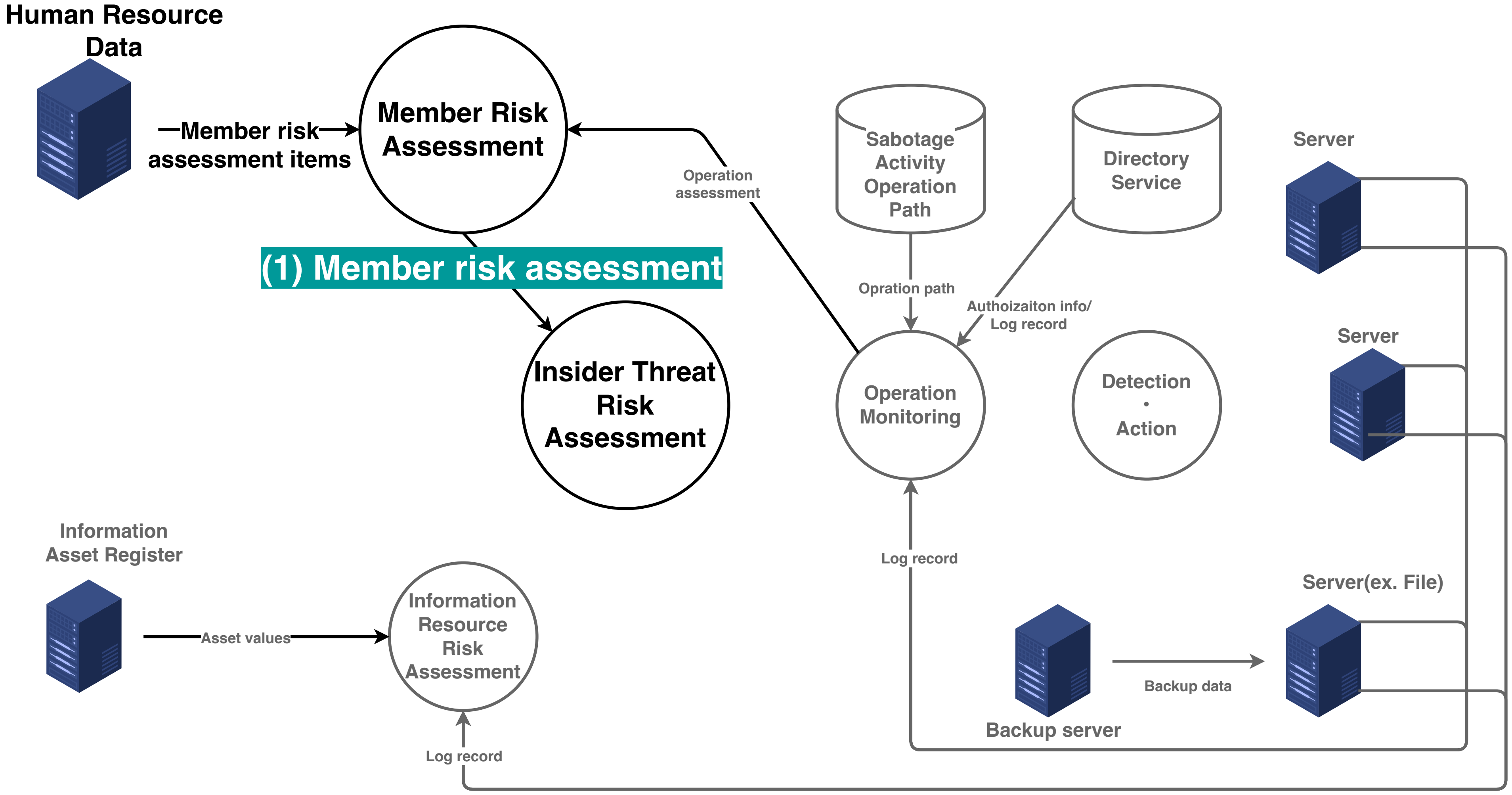
for Achieving Objectives



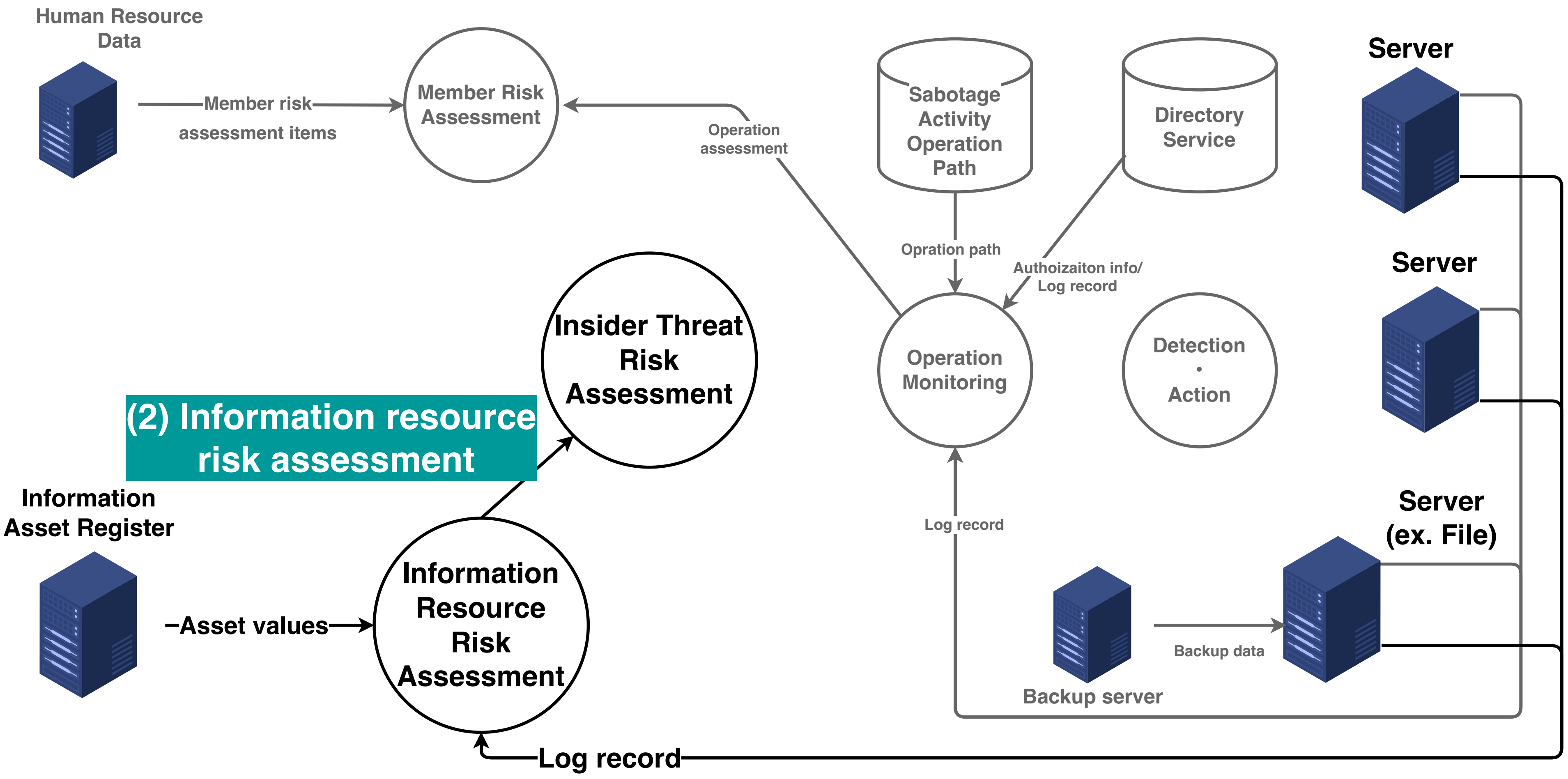
Architecture of Proposed System



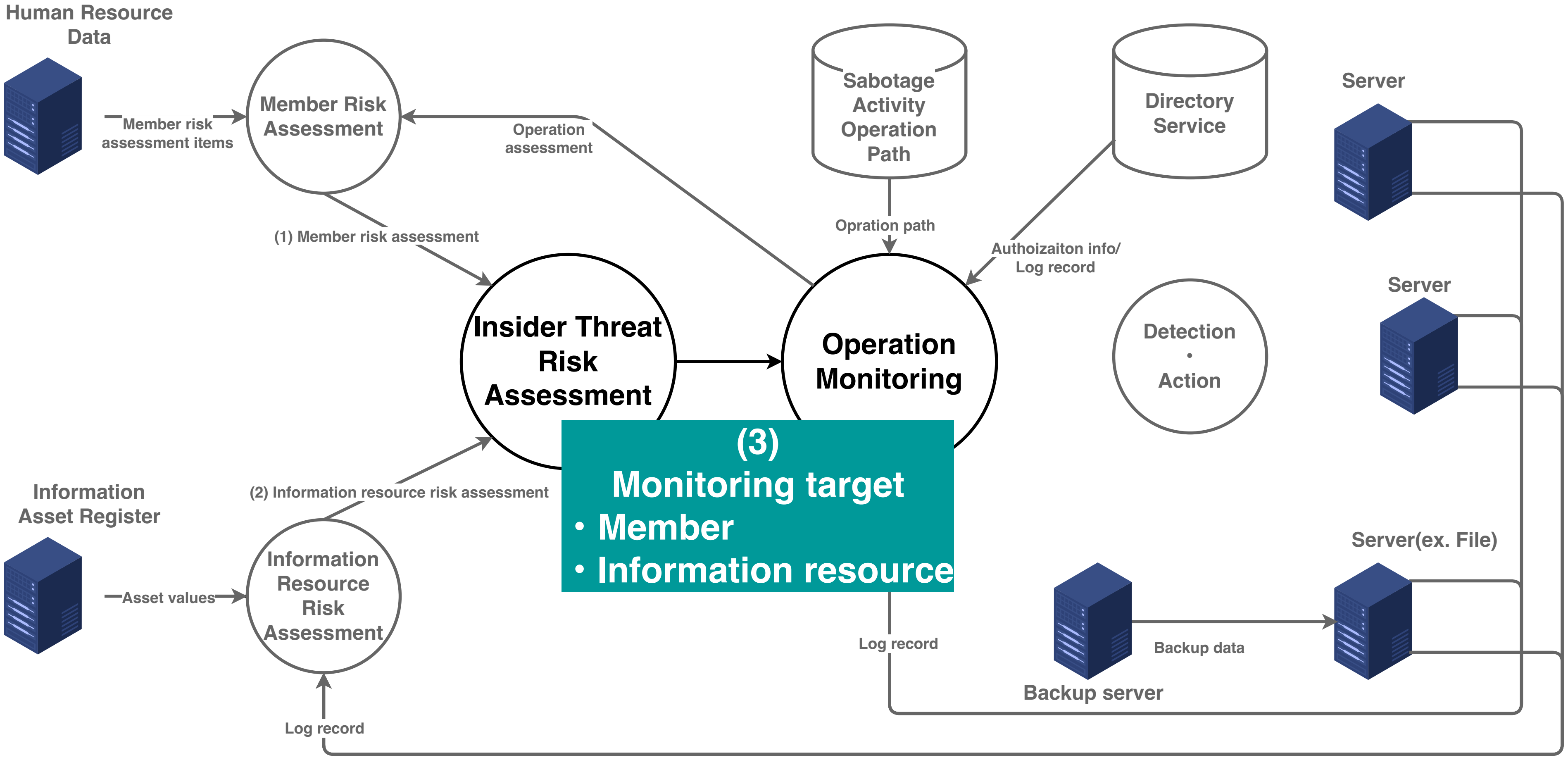
Architecture of Proposed System (Step.1)



Architecture of Proposed System (Step.2)


Human Resource Data
Member risk assessment items
Member Risk Assessment
Operation assessment
Sabotage Activity Operation Path
Directory Service
Server
Opration path
Authoizaiton info/ Log record
Server
Operation Monitoring
Detection • Action
Insider Threat Risk Assessment
(2) Information resource risk assessment
Information Asset Register
Log record
Server (ex. File)
Asset values
Information Resource Risk Assessment
Backup data
Backup server
Log record

Architecture of Proposed System (Step.3)

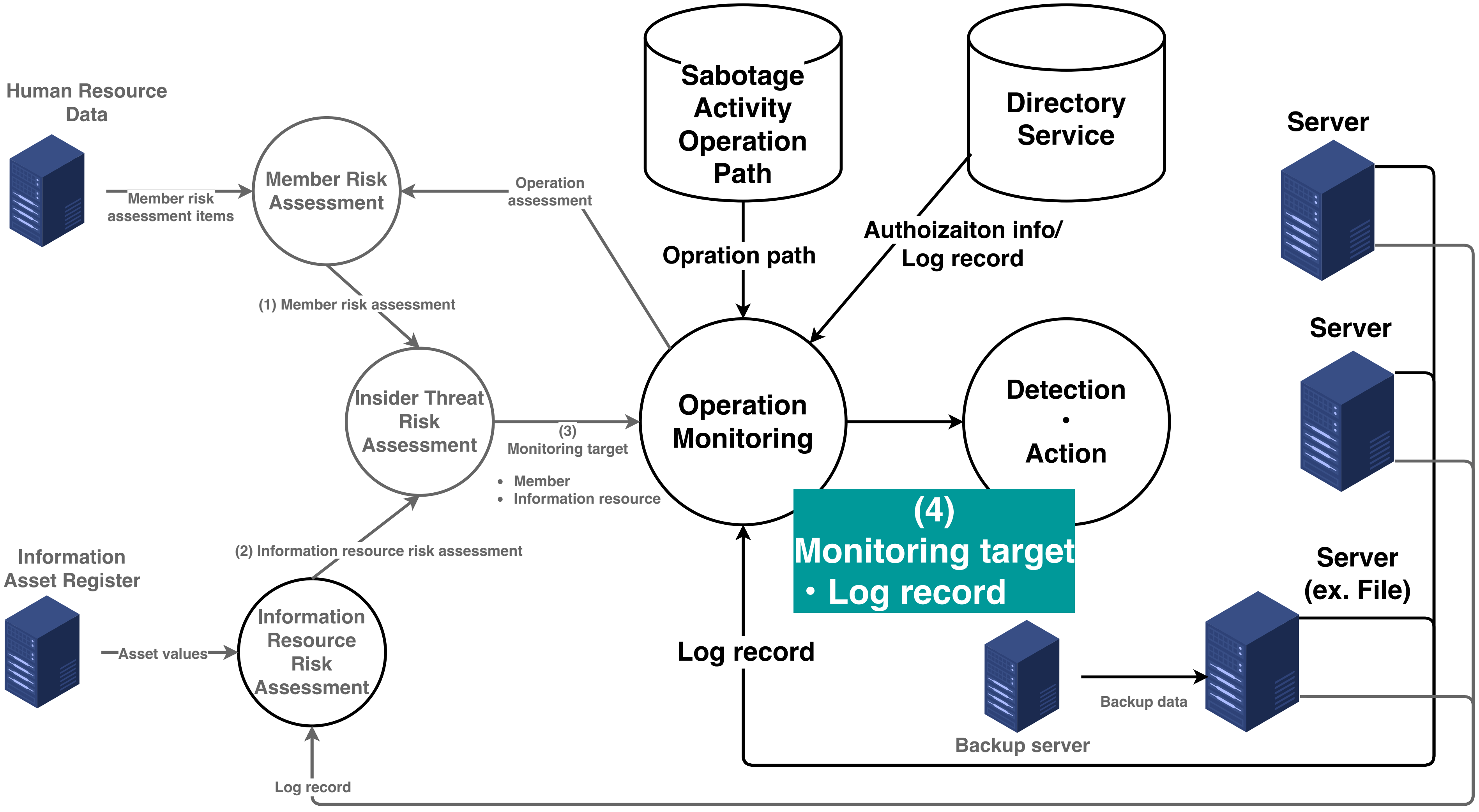


Human Resource Data
Member risk assessment items
Member Risk Assessment
Operation assessment
Sabotage Activity Operation Path
Directory Service
Server
(1) Member risk assessment
Opration path
Authoizaiton info/ Log record
Insider Threat Risk Assessment
Operation Monitoring
Detection • Action
Server
Information Asset Register
(2) Information resource risk assessment
Asset values
Information Resource Risk Assessment
Server(ex. File)
Log record
Backup data
Backup server
Log record

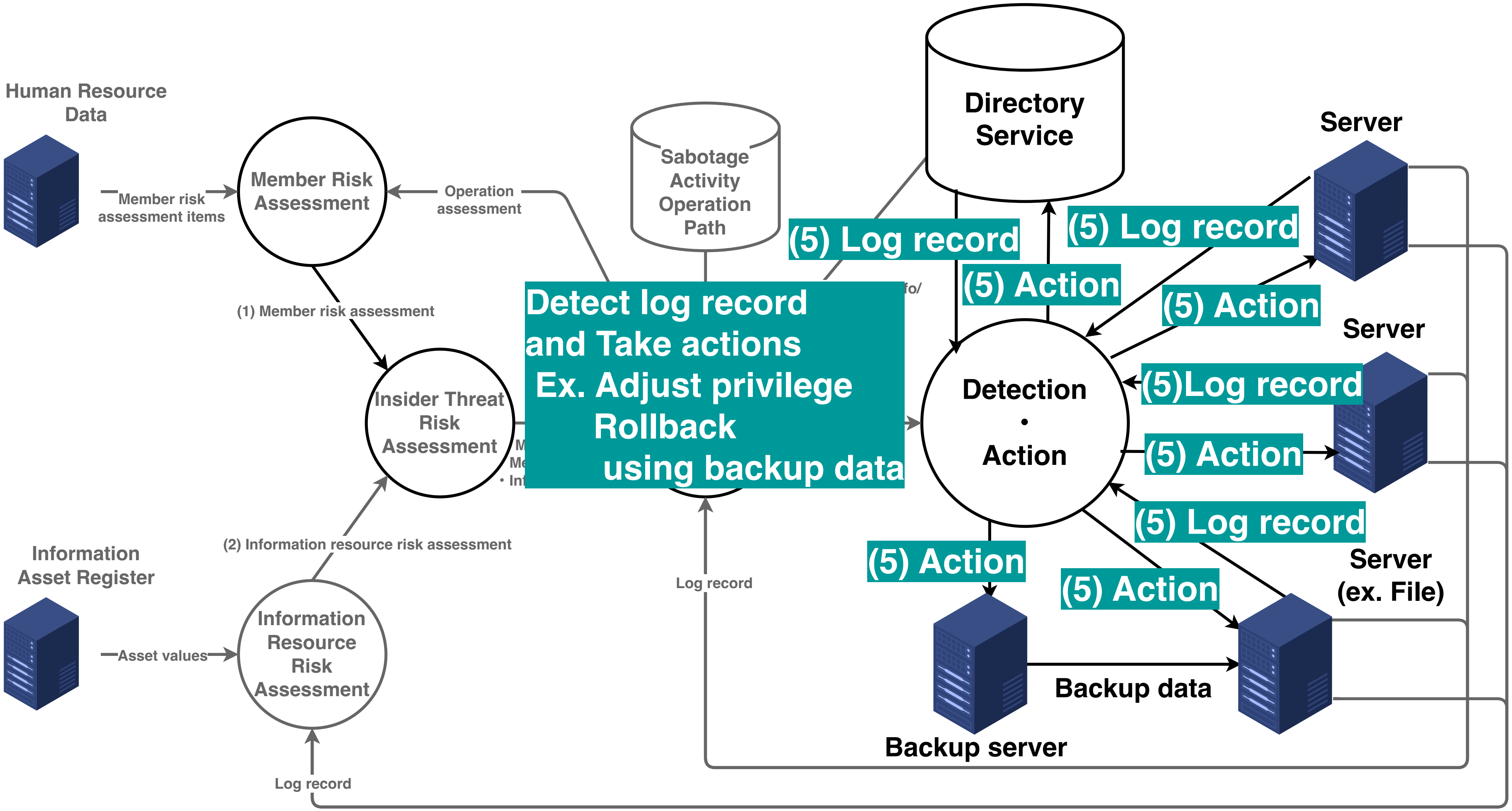
(3)
Monitoring target

- Member
- Information resource

Architecture of Proposed System (Step.4)



Architecture of Proposed System (Step.5)



Detect log record and Take actions
Ex. Adjust privilege
Rollback
using backup data

Challenges in Realizing Implementation

Handling considerations for organizational member information

- Legal issues
  - GDPR in Europe, CCPA in United States, APPI in Japan
- Privacy and ethical concerns

-> Exploring standards and methods that balance security and privacy

Replacement of contaminated data with backup data

- Difficulties in data consistency due to partial data replacement
- Difficulties in data replacement due to unclear scope of contamination

-> Need for reconsideration of the scope and methods of data replacement

Countermeasure against Insider Threat
Regarding Psychological State of Organizational Members
and Business Impact of Information Resources

- Insider threat risk assessment
    - Member risk assessment
    - Information resource risk assessment

-> Countermeasure for high-risk members’ operations on information resource

- Handling considerations for organizational member information
- Replacement of contaminated data with backup data

Reference

[1] P. Institute, “2022 cost of insider threats global report”, [retrieved: September, 2024], 2022, [Online]. Available: https : //www.proofpoint.com/us/resources/threat- reports/cost- ofinsider-threats.

[2] H. Poll, “Vormetric insider threat report”, [retrieved: September, 2024], 2015, [Online]. Available: https : / / enterprise -encryption . vormetric . com / rs / vormetric / images / CW _GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf.

[3] Axelrad et al.., “A Bayesian network model for predictiong insider threats,” Proceeding of the IEEE symposium on Security and Privacy Workshops, pp. 82-89, 2013.

[5] Cappelli et al., “Management and Education of the Risk of Insider Threat(MERIT): system dynamics modeling of computer system sabotage,” Carnegie Mellon University Software Engineering Institute, Tech. Rep. no. CMU/SEI-2006-TN-041, 2008, CERT Technical Note.

[8] Greitzer and Frincke., “Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation,” C. Probst et al. (eds) Insider Threats in Cyber Security. Advances in Information Security,pp. 85-113, 2010.

[14] Moore et al., The “Big Picture” of insider IT sabotage across U. S. critical infrastructure, S. J. Stolfo et al. (eds), Insider Attack and Cyber Secutiry, Advances in Information Security, no. 39, Springer, Boston, , 2008.

[15] Cummings et al., “Insider threat study: illicit cyber activity involving fraud in the U. S. financial sector,” Cert Special Report, no. CMU/SEI-2012-SR-004, 2012.

[16] Homoliak et al.., “Insight into insiders and IT: a survey of insider threat taxonomoies, analysis, modeling, and Countermeasure,” ACM Computing Surveys, vol. 52, issue. 2, no. 30, pp. 1-40, Association for Computing Machinery, Newyork, 2019.

[21] Greitzder et al.., “Insider threats: it’s the HUMAN, stupid!,” Proceeding of the Northwest Cybersecurity Symposium, no. 4 pp. 1-8, 2019.