



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2023년10월16일

(11) 등록번호 10-2589096

(24) 등록일자 2023년10월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) G06N 20/00 (2019.01)(52) CPC특허분류
H04L 63/1433 (2013.01)
G06N 20/00 (2021.08)

(21) 출원번호 10-2023-0051272

(22) 출원일자 2023년04월19일

심사청구일자 2023년04월19일

(56) 선행기술조사문헌

KR100935861 B1*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

한화시스템(주)

경북 구미시 1공단로 244, (공단동)

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

이경호

서울특별시 성북구 안암로 145 (안암동5가)

김유경

서울특별시 성북구

(뒷면에 계속)

(74) 대리인

특허법인세원

전체 청구항 수 : 총 14 항

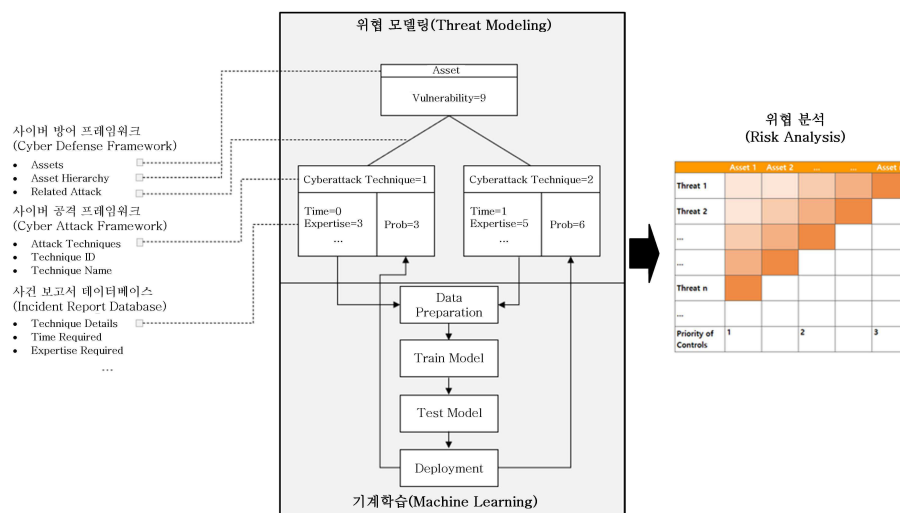
심사관 : 문형섭

(54) 발명의 명칭 사이버 지휘통제 의사결정 지원 장치 및 방법

(57) 요약

본 발명에 따른 사이버 지휘통제 의사결정 지원 장치는 사이버 공격 프레임워크와 사이버 방어 프레임워크를 확률형 공격 트리 기반의 사이버 위협 모델링 방법으로 맵핑하는 사이버 위협 맵핑부 및 소정의 공공 데이터베이스에서 제공되는 공격기술의 실행 난이도 및 실행 소요시간을 포함하는 입력요소를 소정의 인공지능 알고리즘에 적용하여 공격발생확률을 산출하고, 상기 공격발생확률에 상응하는 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성을 위험 분석 정보로 제공하는 정보 제공부를 포함한다.

대표도 - 도3



(52) CPC특허분류

H04L 63/1441 (2013.01)

(72) 발명자

이현민

서울특별시 성북구 안암로 145 (안암동5가)

성동은

서울특별시 성북구 안암로 145 (안암동5가)

김병욱

경상북도 구미시 1공단로 244(공단동)

김선영

경상북도 구미시 1공단로 244(공단동)

명세서

청구범위

청구항 1

사이버 지휘통제 의사결정 지원 장치에 의해 수행되는 방법에 있어서,
 사이버 공격 프레임워크와 사이버 방어 프레임워크를 확률형 공격 트리 기반의 사이버 위협 모델링 방법으로 맵핑하는 단계와,
 소정의 공공 데이터베이스에서 제공되는 공격기술의 실행 난이도 및 실행 소요시간을 포함하는 입력요소를 소정의 인공지능 알고리즘에 적용하여 공격발생확률을 산출하는 단계와,
 상기 공격발생확률에 상응하는 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성을 위험 분석 정보로 제공하는 단계를 포함하고,
 상기 공격발생확률을 산출하는 단계는,
 상기 인공지능 알고리즘에서 상기 공격기술의 실행 난이도 및 실행 소요시간의 가중치로 초기에 랜덤한 가중치를 설정하는 단계; 및
 상기 인공지능 알고리즘에서 입력값과 출력값 사이의 차이가 최소화되도록 상기 초기에 설정된 랜덤한 가중치를 조정하도록 학습하는 단계를 포함하는 것인, 사이버 지휘통제 의사결정 지원 방법.

청구항 2

제1항에 있어서,
 상기 사이버 공격 프레임워크와 사이버 방어 프레임워크를 위협 맵핑하는 단계는,
 위협정보언어로 STIX(Structure Threat Information eXpression) 기반의 공통언어를 사용하여 상기 사이버 공격 프레임워크의 공격기술과 상기 사이버 방어 프레임워크의 자산을 맵핑하는 것인, 사이버 지휘통제 의사결정 지원 방법.

청구항 3

제2항에 있어서,
 상기 STIX 기반의 공통언어는 TTP(Tactics, Techniques, and Procedures)의 유형(Title), 일시(Timestamp), 자원(Resources), 목표 희생자(Victim_Targeting)를 분류하는 것인, 사이버 지휘통제 의사결정 지원 방법.

청구항 4

제2항에 있어서,
 상기 맵핑된 공격기술 및 자산을 확률형 공격트리 형식 기반의 위협 모델로 시각화하여 출력하는 단계; 및
 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성에 대한 위험 분석 정보를 계층별로 표시하여 시각화하는 단계를 더 포함하는, 사이버 지휘통제 의사결정 지원 방법.

청구항 5

제1항에 있어서,

상기 사이버 공격 프레임워크와 사이버 방어 프레임워크를 위협 맵핑하는 단계는,

상기 사이버 공격 프레임워크의 공격기술은 MITRE ATT&ACK 프레임워크의 기술 ID 및 기술명을 요소로 적용하여 맵핑하고, 상기 사이버 방어 프레임워크의 자산은 MITRE D3FEND의 아티팩트를 자산으로 맵핑하는 것인, 사이버 지휘통제 의사결정 지원 방법.

청구항 6

제1항에 있어서,

상기 소정의 공공 데이터베이스는 NVD(National Vulnerability Database) 및 VERIS(Vocabulary for Event Recording and Incident Sharing) 중 적어도 하나인 것인, 사이버 지휘통제 의사결정 지원 방법.

청구항 7

삭제

청구항 8

제6항에 있어서,

상기 위협 분석 정보가 제공된 이후, 상기 공격기술의 실행 난이도 및 실행 소요시간의 입력요소를 통해 상기 인공지능 알고리즘에 적용된 가중치의 미분값 및 학습률을 산출하는 단계; 및

상기 미분값 및 학습률을 이용하여 상기 가중치를 최적화하고 가중치 조정량의 크기를 제어하는 단계를 더 포함하는, 사이버 지휘통제 의사결정 지원 방법.

청구항 9

사이버 지휘통제 의사결정 지원 장치에 있어서,

사이버 공격 프레임워크와 사이버 방어 프레임워크를 확률형 공격 트리 기반의 사이버 위협 모델링 방법으로 맵핑하는 사이버 위협 맵핑부 및

소정의 공공 데이터베이스에서 제공되는 공격기술의 실행 난이도 및 실행 소요시간을 포함하는 입력요소를 소정의 인공지능 알고리즘에 적용하여 공격발생확률을 산출하고, 상기 공격발생확률에 상응하는 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성을 위협 분석 정보로 제공하는 정보 제공부를 포함하고,

상기 정보 제공부는 상기 인공지능 알고리즘에서 상기 공격기술의 실행 난이도 및 실행 소요시간의 가중치로 초기에 랜덤한 가중치를 설정하고, 상기 인공지능 알고리즘에서 입력값과 출력값 사이의 차이가 최소화되도록 상기 초기에 설정된 랜덤한 가중치를 조정하도록 학습하는 것인, 사이버 지휘통제 의사결정 지원 장치.

청구항 10

제9항에 있어서,

상기 사이버 위협 맵핑부는 위협정보언어로 STIX(Structure Threat Information eXpression) 기반의 공통언어를 사용하여 상기 사이버 공격 프레임워크의 공격기술과 상기 사이버 방어 프레임워크의 자산을 맵핑하는 것인, 사이버 지휘통제 의사결정 지원 장치.

청구항 11

제10항에 있어서,

상기 STIX 기반의 공통언어는 TTP(Tactics, Techniques, and Procedures)의 유형(Title), 일시(Timestamp), 자원(Resources), 목표 희생자(Victim_Targeting)를 분류하는 것인, 사이버 지휘통제 의사결정 지원 장치.

청구항 12

제11항에 있어서,

상기 사이버 위협 맵핑부는 상기 맵핑된 공격기술 및 자산을 확률형 공격트리 형식 기반의 위협 모델로 시각화하여 출력하고,

상기 정보 제공부는 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성에 대한 위협 분석 정보를 계층별로 표시하여 시각화하는 것인, 사이버 지휘통제 의사결정 지원 장치.

청구항 13

제9항에 있어서,

상기 사이버 위협 맵핑부는 상기 사이버 공격 프레임워크의 공격기술은 MITRE ATT&ACK 프레임워크의 기술 ID 및 기술명을 요소로 적용하여 맵핑하고, 상기 사이버 방어 프레임워크의 자산은 MITRE D3FEND의 아티팩트를 자산으로 맵핑하는 것인, 사이버 지휘통제 의사결정 지원 장치.

청구항 14

제9항에 있어서,

상기 소정의 공공 데이터베이스는 NVD(National Vulnerability Database) 및 VERIS(Vocabulary for Event Recording and Incident Sharing) 중 적어도 하나인 것인, 사이버 지휘통제 의사결정 지원 장치.

청구항 15

삭제

청구항 16

제11항에 있어서,

상기 정보 제공부는 상기 위협 분석 정보가 제공된 이후, 상기 공격기술의 실행 난이도 및 실행 소요시간의 입력요소를 통해 상기 인공지능 알고리즘에 적용된 가중치의 미분값 및 학습률을 산출하고, 상기 미분값 및 학습률을 이용하여 상기 가중치를 최적화하고 가중치 조정량의 크기를 제어하는 것인, 사이버 지휘통제 의사결정 지원 장치.

발명의 설명

기술 분야

[0001] 본 발명은 사이버 지휘통제 의사결정 지원 장치 및 방법에 관한 것으로서, 특히 사이버 자산에 대한 실시간 위협 분석을 통해 구체적인 방어 기술을 의사결정권자에게 제공할 수 있으며, 더 나아가 기존 위협 표준들과 더불어 정량적인 사이버 자산의 위협 분석 결과를 도출할 수 있는, 사이버 지휘통제 의사결정 지원 장치 및 방법에 관한 것이다.

배경 기술

[0003] 현재의 전장이 5차원(지상, 공중, 해상, 우주, 사이버) 전장으로 확장되어 감에 따라 사이버 지휘통제의 중요성이 부각되고 있다. 또한, 사이버 공간 전장 정보가 물리적 공간의 전장 정보와 연계될 수 있다는 관점이 생기면

서 사이버 전장에서도 사이버 자산의 위험 분석에 대한 중요성이 증가하였다.

- [0004] 사이버 공간에서 국가 또는 비국가 행위자(advanced Persistent Threat)들이 지속적으로 새로운 기술을 활용하여 사이버 공간뿐만 아니라 물리적 공간에도 영향을 주는 제로데이 공격(Zero-day Attack) 등과 같은 다양한 공격을 시도하고 있기 때문에, 사이버 자산의 위험 분석이 신속하게 수행될 필요가 있다.
- [0005] 한편, 위험관리 표준의 경우 ISO 2700x, National Institute of Standards and Technology (NIST) Special Publication 800-37 등이 존재한다. 이때, ISO 2700x는 국제표준화기구(ISO, International Organization for Standardization) 및 국제전기기술위원회(IEC, International Electrotechnical Commission)에서 제정한 정보 보호 관리체계에 대한 국제 표준이다. 그리고, NIST 800-37은 보안 정보 시스템의 위험 관리를 위한 미국 연방 정부 지침, 표준 및 프로세스이다. NIST 800-37의 위험 관리 프레임워크(RMF, Risk Management Framework)는 정보 보안, 개인 정보 보호 및 위험 관리 프레임워크를 제공한다.
- [0006] 하지만, 해당 위험관리 표준들의 경우, 해당 표준 적용은 전문가 분석이 요구되며 구체적인 방어 기술을 제공하지 않는다는 한계점들이 존재한다.

발명의 내용

해결하려는 과제

- [0008] 본 발명이 해결하고자 하는 과제는 사이버 자산에 대한 실시간 위험 분석을 통해 구체적인 방어 기술을 의사결정권자에게 제공할 수 있으며, 더 나아가 기존 위험 표준들과 더불어 정량적인 사이버 자산의 위험 분석 결과를 도출할 수 있는, 사이버 지휘통제 의사결정 지원 장치 및 방법에 관한 것이다.
- [0009] 다만, 본 발명이 해결하고자 하는 과제는 상기된 바와 같은 과제로 한정되지 않으며, 또다른 과제들이 존재할 수 있다.

과제의 해결 수단

- [0011] 상술한 과제를 해결하기 위한 본 발명의 제1 측면에 따른 사이버 지휘통제 의사결정 지원 방법은 사이버 공격 프레임워크와 사이버 방어 프레임워크를 확률형 공격 트리 기반의 사이버 위협 모델링 방법으로 맵핑하는 단계와, 소정의 공공 데이터베이스에서 제공되는 공격기술의 실행 난이도 및 실행 소요시간을 포함하는 입력요소를 소정의 인공지능 알고리즘에 적용하여 공격발생확률을 산출하는 단계와, 상기 공격발생확률에 상응하는 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성을 위험 분석 정보로 제공하는 단계를 포함한다.
- [0012] 본 발명의 일부 실시예에 있어서, 상기 사이버 공격 프레임워크와 사이버 방어 프레임워크를 위협 맵핑하는 단계는, 위협정보언어로 STIX(Structure Threat Information eXpression) 기반의 공통언어를 사용하여 상기 사이버 공격 프레임워크의 공격기술과 상기 사이버 방어 프레임워크의 자산을 맵핑할 수 있다.
- [0013] 본 발명의 일부 실시예에 있어서, 상기 STIX 기반의 공통언어는 TTP(Tactics, Techniques, and Procedures)의 유형(Title), 일시(Timestamp), 자원(Resources), 목표 희생자(Victim_Targeting)를 분류할 수 있다.
- [0014] 본 발명의 일부 실시예는, 상기 맵핑된 공격기술 및 자산을 확률형 공격트리 형식 기반의 위협 모델로 시각화하여 출력하는 단계; 및 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성에 대한 위험 분석 정보를 계층별로 표시하여 시각화하는 단계를 더 포함할 수 있다.
- [0015] 본 발명의 일부 실시예에 있어서, 상기 사이버 공격 프레임워크와 사이버 방어 프레임워크를 위협 맵핑하는 단계는, 상기 사이버 공격 프레임워크의 공격기술은 MITRE ATT&ACK 프레임워크의 기술 ID 및 기술명을 요소로 적용하여 맵핑하고, 상기 사이버 방어 프레임워크의 자산은 MITRE D3FEND의 아티팩트를 자산으로 맵핑할 수 있다.
- [0016] 본 발명의 일부 실시예에 있어서, 상기 소정의 공공 데이터베이스는 NVD(National Vulnerability Database) 및 VERIS(Vocabulary for Event Recording and Incident Sharing) 중 적어도 하나일 수 있다.
- [0017] 본 발명의 일부 실시예에 있어서, 상기 공격발생확률을 산출하는 단계는, 상기 인공지능 알고리즘에서 상기 공격기술의 실행 난이도 및 실행 소요시간의 가중치로 초기에 랜덤한 가중치를 설정하는 단계; 및 상기 인공지능 알고리즘에서 입력값과 출력값 사이의 차이가 최소화되도록 상기 초기에 설정된 랜덤한 가중치를 조정하도록 학습하는 단계를 포함할 수 있다.
- [0018] 본 발명의 일부 실시예는, 상기 위험 분석 정보가 제공된 이후, 상기 공격기술의 실행 난이도 및 실행 소요시간

의 입력요소를 통해 상기 인공지능 알고리즘에 적용된 가중치의 미분값 및 학습률을 산출하는 단계; 및 상기 미분값 및 학습률을 이용하여 상기 가중치를 최적화하고 가중치 조정량의 크기를 제어하는 단계를 더 포함할 수 있다.

- [0020] 또한, 본 발명의 제2 측면에 따른 사이버 지휘통제 의사결정 지원 장치는 사이버 공격 프레임워크와 사이버 방어 프레임워크를 확률형 공격 트리 기반의 사이버 위협 모델링 방법으로 맵핑하는 사이버 위협 맵핑부 및 소정의 공공 데이터베이스에서 제공되는 공격기술의 실행 난이도 및 실행 소요시간을 포함하는 입력요소를 소정의 인공지능 알고리즘에 적용하여 공격발생확률을 산출하고, 상기 공격발생확률에 상응하는 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성을 위험 분석 정보로 제공하는 정보 제공부를 포함한다.
- [0021] 본 발명의 일부 실시예에 있어서, 상기 사이버 위협 맵핑부는 위협정보언어로 STIX(Structure Threat Information eXpression) 기반의 공통언어를 사용하여 상기 사이버 공격 프레임워크의 공격기술과 상기 사이버 방어 프레임워크의 자산을 맵핑할 수 있다.
- [0022] 본 발명의 일부 실시예에 있어서, 상기 STIX 기반의 공통언어는 TTP(Tactics, Techniques, and Procedures)의 유형(Title), 일시(Timestamp), 자원(Resources), 목표 희생자(Victim_Targeting)를 분류할 수 있다.
- [0023] 본 발명의 일부 실시예에 있어서, 상기 사이버 위협 맵핑부는 상기 맵핑된 공격기술 및 자산을 확률형 공격트리 형식 기반의 위협 모델로 시각화하여 출력하고, 상기 정보 제공부는 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성에 대한 위험 분석 정보를 계층별로 표시하여 시각화할 수 있다.
- [0024] 본 발명의 일부 실시예에 있어서, 상기 사이버 위협 맵핑부는 상기 사이버 공격 프레임워크의 공격기술은 MITRE ATT&ACK 프레임워크의 기술 ID 및 기술명을 요소로 적용하여 맵핑하고, 상기 사이버 방어 프레임워크의 자산은 MITRE D3FEND의 아티팩트를 자산으로 맵핑할 수 있다.
- [0025] 본 발명의 일부 실시예에 있어서, 상기 소정의 공공 데이터베이스는 NVD(National Vulnerability Database) 및 VERIS(Vocabulary for Event Recording and Incident Sharing) 중 적어도 하나일 수 있다.
- [0026] 본 발명의 일부 실시예에 있어서, 상기 정보 제공부는 상기 인공지능 알고리즘에서 상기 공격기술의 실행 난이도 및 실행 소요시간의 가중치로 초기에 랜덤한 가중치를 설정하고, 상기 인공지능 알고리즘에서 입력값과 출력값 사이의 차이가 최소화되도록 상기 초기에 설정된 랜덤한 가중치를 조정하도록 학습할 수 있다.
- [0027] 본 발명의 일부 실시예에 있어서, 상기 정보 제공부는 상기 위험 분석 정보가 제공된 이후, 상기 공격기술의 실행 난이도 및 실행 소요시간의 입력요소를 통해 상기 인공지능 알고리즘에 적용된 가중치의 미분값 및 학습률을 산출하고, 상기 미분값 및 학습률을 이용하여 상기 가중치를 최적화하고 가중치 조정량의 크기를 제어할 수 있다.
- [0028] 상술한 과제를 해결하기 위한 본 발명의 다른 면에 따른 컴퓨터 프로그램은, 하드웨어인 컴퓨터와 결합되어 상기 사이버 지휘통제 의사결정 지원 방법을 실행하며, 컴퓨터 판독가능 기록매체에 저장된다.
- [0029] 본 발명의 기타 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

- [0031] 전술한 본 발명의 일 실시예에 의하면, 각 사이버 위협 자산에 해당되는 위험 분석 정보를 제공함으로써 사이버 지휘통제를 위한 의사결정의 오류를 최소화시킬 수 있다. 특히, 위험 분석 정보를 인공지능 알고리즘을 활용함으로써 넓은 범위의 요소들을 보다 정확하게 분석할 수 있다.
- [0032] 더욱이, 자산의 취약점을 보완하기 위해 필요한 시간, 인력 및 자본 등을 포함하는 취약점 보완 소요 자원을 반영하여, 최종 제공되는 위험도에 대한 정보의 신뢰성을 향상시킬 수 있다.
- [0033] 이러한 본 발명의 일 실시예에 따르면, 사이버 지휘통제를 위한 의사결정 오류를 더욱 줄어든게 하는 효과를 기대할 수 있다.
- [0034] 본 발명의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [0036] 이하에 첨부되는 도면들은 본 실시예에 관한 이해를 돕기 위한 것으로, 상세한 설명과 함께 실시예들을 제공

한다. 다만, 본 실시 예의 기술적 특징이 특정 도면에 한정되는 것은 아니며, 각 도면에서 개시하는 특징들은 서로 조합되어 새로운 실시 예로 구성될 수 있다.

도 1은 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치의 블록도이다.

도 2는 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치의 기능을 설명하기 위한 블록도이다.

도 3은 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치의 기능을 설명하기 위한 블록도이다.

도 4는 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0037] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 제한되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야의 통상의 기술자에게 본 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.
- [0038] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다. 명세서 전체에 걸쳐 동일한 도면 부호는 동일한 구성 요소를 지칭하며, "및/또는"은 언급된 구성요소들의 각각 및 하나 이상의 모든 조합을 포함한다. 비록 "제1", "제2" 등이 다양한 구성요소들을 서술하기 위해서 사용되나, 이들 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 구성요소를 다른 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 구성요소는 본 발명의 기술적 사상 내에서 제2 구성요소일 수도 있음은 물론이다.
- [0039] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야의 통상의 기술자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [0041] 이하 첨부된 도면을 참조하여 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치(100) 및 방법에 대해 보다 상세히 설명하도록 한다.
- [0042] 도 1은 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치(100)의 블록도이다.
- [0043] 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치(100)는 입력부(110), 통신부(120), 표시부(130), 메모리(140) 및 프로세서(150)를 포함한다.
- [0044] 입력부(110)는 사이버 지휘통제 의사결정 지원 장치(100)의 사용자 입력에 대응하여 입력데이터를 발생시킨다. 일 예로, 사용자 입력은 네트워크 로그, 보안 이벤트 로그, 인터넷 트래픽, 취약성 스캔 결과 등일 수 있다. 입력부(110)는 적어도 하나의 입력수단을 포함한다. 입력부(110)는 키보드(key board), 키패드(key pad), 돔 스위치(dome switch), 터치패널(touch panel), 터치 키(touch key), 마우스(mouse), 메뉴 버튼(menu button) 등을 포함할 수 있다.
- [0045] 통신부(120)는 보안 이벤트나 알람 등을 타 시스템에 전달하거나, 다른 시스템으로부터 정보나 명령을 수신할 수 있다. 이와 같은 통신부(120)는 유선 통신 모듈 및 무선 통신 모듈을 모두 포함할 수 있다. 유선 통신 모듈은 전력선 통신 장치, 전화선 통신 장치, 케이블 홈(MoCA), 이더넷(Ethernet), IEEE1294, 통합 유선 홈 네트워크 및 RS-485 제어 장치로 구현될 수 있다. 또한, 무선 통신 모듈은 WLAN(wireless LAN), Bluetooth, HDR WPAN, UWB, ZigBee, Impulse Radio, 60GHz WPAN, Binary-CDMA, 무선 USB 기술 및 무선 HDMI 기술, 그밖에 5G(5th generation communication), LTE-A(long term evolution-advanced), LTE(long term evolution), Wi-Fi(wireless fidelity) 등의 기능을 구현하기 위한 모듈로 구성될 수 있다.
- [0046] 표시부(130)는 사이버 지휘통제 의사결정 지원 장치(100)의 동작에 따른 데이터, 즉 맵핑 결과, 공격발생확률, 위험 분석 정보 등을 표시한다. 표시부(130)는 액정 디스플레이(LCD; liquid crystal display), 발광 다이오드(LED; light emitting diode) 디스플레이, 유기 발광 다이오드(OLED; organic LED) 디스플레이, 마이크로 전자 기계 시스템(MEMS; micro electro mechanical systems) 디스플레이 및 전자 종이(electronic paper) 디스플레이

이를 포함한다. 표시부(130)는 입력부(110)와 결합되어 터치 스크린(touch screen)으로 구현될 수 있다.

- [0047] 메모리(140)는 사이버 지휘통제 의사결정 지원 장치(100)의 동작 프로그램들을 저장한다. 여기에서, 메모리(140)는 전원이 공급되지 않아도 저장된 정보를 계속 유지하는 비휘발성 저장장치 및 휘발성 저장장치를 통칭하는 것이다. 예를 들어, 메모리(140)는 콤팩트 플래시(compact flash; CF) 카드, SD(secure digital) 카드, 메모리 스틱(memory stick), 솔리드 스테이트 드라이브(solid-state drive; SSD) 및 마이크로(micro) SD 카드 등과 같은 낸드 플래시 메모리(NAND flash memory), 하드 디스크 드라이브(hard disk drive; HDD) 등과 같은 마그네틱 컴퓨터 기억 장치 및 CD-ROM, DVD-ROM 등과 같은 광학 디스크 드라이브(optical disc drive) 등을 포함할 수 있다.
- [0048] 프로세서(150)는 프로그램 등 소프트웨어를 실행하여 사이버 지휘통제 의사결정 지원 장치(100)의 적어도 하나의 다른 구성요소(예: 하드웨어 또는 소프트웨어 구성요소)를 제어할 수 있고, 다양한 데이터 처리 또는 연산을 수행할 수 있다.
- [0049] 프로세서(150)는 사이버 공격 프레임워크 및 사이버 방어 프레임워크의 맵핑을 수행하며, 맵핑 결과를 토대로 소정의 인공지능 알고리즘을 통해 위험 분석 정보를 제공할 수 있다.
- [0050] 한편, 본 발명의 일 실시예에서, 프로세서(150)는 인공지능(Artificial Intelligence) 알고리즘으로서 SVM(Support Machine Vector), K-Nearest Neighbor, Decision tree, Random forest, na*?ve bayes 등의 분류형 인공지능 알고리즘을 이용할 수 있다.
- [0051] 그밖에 프로세서(150)는 데이터 전처리, 기계학습, 신경망 네트워크(neural network), 또는 딥러닝 알고리즘 중 적어도 하나를 이용할 수 있다. 일 예로, 인공지능(Artificial Intelligence) 알고리즘으로서 기계학습, 신경망 네트워크(neural network), 또는 딥러닝 알고리즘 중 적어도 하나를 이용할 수 있으며, 신경망 네트워크의 예로는, CNN (Convolutional Neural Network), DNN (Deep Neural Network), RNN (Recurrent Neural Network)과 같은 모델을 포함할 수 있다. 이러한 인공지능 알고리즘에는 사용자 GUI가 포함될 수 있으며, 학습모델을 관리하기 위한 프로그램 등이 포함될 수 있다.
- [0053] 도 2는 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치(100)의 기능을 설명하기 위한 블록도이다. 도 3은 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치(100)의 기능을 설명하기 위한 블록도이다.
- [0054] 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치(100)는 사이버 위협 맵핑부(210) 및 정보 제공부(220)를 포함한다. 이때, 사이버 위협 맵핑부(210) 및 정보 제공부(220)는 프로세서(150)에 의해 수행되는 것으로 이해될 수 있다.
- [0055] 사이버 위협 맵핑부(210)는 사이버 공격 프레임워크와 사이버 방어 프레임워크를 확률형 공격 트리(Attack Probability Tree)와 같은 사이버 위협 모델링 방법으로 맵핑시킨다. 즉, 사이버 지휘통제 의사결정 지원 장치(100)는 사이버 공격에 대한 대응 전략을 수립하고 관리하기 위하여 사이버 공격 프레임워크와 사이버 방어 프레임워크를 맵핑함으로써 효율적인 대응 전략 수립을 가능하게 할 수 있다.
- [0056] 여기에서, 사이버 공격 프레임워크는 해커나 사이버 공격자가 사용하는 기술, 절차, 전략 등을 나타내는 프레임워크이다. 이와 반대로, 사이버 방어 프레임워크는 조직이나 기관 등에서 적용하는 보안 방어 전략 및 대응 방안을 나타내는 프레임워크이다.
- [0057] 위협 맵핑은 사이버 공격 프레임워크와 사이버 방어 프레임워크를 맵핑하여, 조직이나 기관에서 어떤 보안 위협에 노출되었는지를 파악하고, 이를 대응 전략 수립에 반영할 수 있도록 하는 과정을 의미한다. 이때, 위협 맵핑을 위해서 본 발명의 일 실시예는 확률형 공격 트리와 같은 사이버 위협 모델링 방법을 적용할 수 있다. 확률형 공격 트리는 공격자가 실행할 수 있는 다양한 공격 기술을 표현하고, 각 공격 기술의 실행 가능성과 효과 등을 고려하여 전체적인 공격 가능성을 계산하는 모델이다.
- [0058] 사이버 위협 맵핑부(210)는 위협정보 언어로 STIX(Structure Threat Information eXpression) 기반의 공통언어를 사용하여 사이버 공격 프레임워크의 공격기술과 상기 사이버 방어 프레임워크의 자산을 맵핑할 수 있다. 위협정보 언어는 보안 전문가들이 악성 코드, 사이버 공격, 해킹 등의 위협 정보를 수집, 분석 및 공유하기 위한 언어이며, 일반적으로 STIX(Structure Threat Information eXpression)라는 형식으로 표현될 수 있다.
- [0059] 이때, STIX는 위협정보를 구조화하고 공유하기 위한 국제 표준이며, STIX를 이용하여 위협 정보를 기술할 수 있다. 즉, STIX 기반의 공통언어는 위협에 대한 정보를 표현하는 다양한 요소들을 정의하고 있으며, 이를 통해

TTP(Tactics, Techniques, and Procedures)의 유형(Title), 일시(Timestamp), 자원(Resources), 목표 희생자(Victim_Targeting)를 분류할 수 있다.

- [0060] 이때, TTP는 해커나 사이버 공격자가 사용하는 기술, 절차, 전술을 의미하며, TTP의 분류를 통해 위협 정보 수집 및 분석을 보다 효율적으로 수행할 수 있다. 일시는 위협 정보의 발생 일시를 나타내며, 자원은 공격 대상이나 사용된 도구, 기술 등을 의미한다. 그리고, 목표 희생자는 공격 대상 그룹 등을 의미한다.
- [0061] 본 발명의 일 실시예는 STIX 기반의 공통언어를 적용함으로써, 위협 정보를 표현하는 요소들을 정의하여 공유하기 쉽도록 구조화하고, 정보 공유를 통해 보안 전문가들이 위협에 대한 정보를 보다 빠르고 정확하게 파악할 수 있도록 지원할 수 있으며, 이를 통해 사이버 보안에 대한 대응 및 대처 능력을 향상시킬 수 있다.
- [0062] 보다 상세하게, 사이버 위협 맵핑부(210)는 사이버 공격 프레임워크의 공격기술은 MITRE ATT&ACK 프레임워크의 기술 ID(Technique ID) 및 기술명(Technique Name)을 요소로 적용하여 맵핑하고, 사이버 방어 프레임워크의 자산은 MITRE D3FEND의 아티팩트(Artifact)를 자산으로 맵핑할 수 있다.
- [0063] 다음으로, 정보 제공부(220)는 소정의 공공 데이터베이스에서 제공되는 공격기술의 실행 난이도(Attack Difficulty) 및 실행 소요시간(Time Required)을 포함하는 입력요소를 소정의 인공지능 알고리즘에 적용하여 공격발생확률(Attack Probability)을 산출한다. 여기에서, 공격 실행 난이도는 공격자가 공격을 성공적으로 수행하기 위해 필요한 기술, 도구, 지식 등의 난이도를 의미하며, 실행 소요시간은 공격자가 공격을 성공적으로 수행하는 데 소요되는 시간을 의미한다. 그리고 정보 제공부(220)는 공격발생확률에 상응하는 맵핑된 사이버 방어 프레임워크의 자산 취약성을 위험 분석 정보로 제공한다.
- [0064] 일 실시예로, 소정의 공공 데이터베이스는 위협 정보 공유 체제인 NVD(National Vulnerability Database) 및 VERIS(Vocabulary for Event Recording and Incident Sharing) 중 적어도 하나일 수 있다.
- [0065] 이때, 정보 제공부(220)는 VERIS 등의 공공 데이터베이스에서 제공되는 action.malware, impact.loss 등과 같은 변수에 상응하는 기술명을 요소로 이용하여 공격발생확률을 산출할 수 있으며, 공격발생확률을 기반으로 해당되는 자산의 취약성을 산출할 수 있다. 이때, action.malware 변수는 공격자가 사용한 악성 코드의 유형을 나타내며, impact.loss 변수는 해당 공격으로 인해 발생한 손실의 정도를 나타낸다. 이러한 변수들은 공격 사례를 분석하여 보안 전략을 수립하고, 취약성을 분석 및 개선하는 등의 목적으로 사용될 수 있다.
- [0066] 또한, 본 발명의 일 실시예에서 정보 제공부(220)는 공격기술의 실행 난이도 요소 및 실행 소요시간 요소를 인공지능을 통해 분석하여 적정 가중치를 산출할 수 있다.
- [0067] 즉, 정보 제공부(220)는 인공지능 알고리즘에서 공격기술의 실행 난이도 및 실행 소요시간의 가중치로 초기에 랜덤한 가중치를 설정하고, 인공지능 알고리즘에서 입력값과 출력값 사이의 차이가 최소화되도록 초기에 설정된 랜덤한 가중치를 조정하도록 학습할 수 있다. 이 과정에서, 정보 제공부(220)는 손실함수를 이용하여 예측값과 실제값의 차이를 측정할 수 있다.
- [0068] 또한, 추가적으로 정보 제공부(220)는 위험 분석 정보가 제공된 이후, 공격기술의 실행 난이도 및 실행 소요시간의 입력요소를 통해 인공지능 알고리즘에 적용된 가중치의 미분값 및 학습률(learning rate)을 산출하고, 미분값 및 학습률을 이용하여 가중치를 최적화하고 가중치 조정량의 크기를 제어할 수 있다. 일 예로, 정보 제공부(220)는 현재 가중치에서 미분값과 학습률을 곱한 값을 현재 가중치에서 차감하여 새로운 가중치를 계산할 수 있다. 이렇게 계산된 가중치는 기존 가중치와 비교하여 얼마나 크게 조정할지를 결정하는 가중치 조정량의 크기를 제어하면서 업데이트될 수 있으며, 이 과정은 일반적으로 손실함수가 최소화되는 방향으로 가중치가 업데이트될 수 있다.
- [0069] 본 발명의 일 실시예는 이러한 가중치 최적화 과정을 추가적으로 수행함으로써, 새로운 입력값이 주어졌을 때 더욱 정확한 결과를 도출할 수 있도록 인공지능 알고리즘의 성능을 향상시킬 수 있다.
- [0070] 결과적으로 본 발명의 일 실시예는 인공지능 알고리즘을 통해 산출된 공격발생확률을 확률형 공격트리 형태로 맵핑했을 때, 각 공격기술에 해당하는 자산이 확인되며 자산의 취약성이 도출된다. 그리고 취약성이 평가된 자산들을 순서대로 나열하고, 이를 통해 MITRE D3FEND와 같은 사이버 방어 프레임워크를 이용하여 각 자산의 취약성 우선순위와 migration을 제공함으로써 사이버 지휘통제 의사결정을 지원할 수 있다.
- [0071] 한편, 본 발명의 일 실시예에서, 사이버 위협 맵핑부(210)는 맵핑된 공격기술 및 자산을 확률형 공격트리 형식 기반의 위협 모델로 시각화하여 출력할 수 있다. 일 예로, 시각화된 위협 모델은 공격기술과 취약 자산들의 상관관계를 보여줄 수 있으며, 이때 각각의 노드는 해당 공격기술 또는 취약 자산을 나타낼 수 있다. 일 예로, 각

노드는 일정한 형태, 색상으로 표시될 수 있으며, 크기, 색상 등의 속성은 해당 자산의 위험성에 따라 달리 표현될 수 있다.

[0072] 또한, 정보 제공부(220)는 맵핑된 사이버 방어 프레임워크의 자산 취약성에 대한 위험 분석 정보를 계층별로 표시하여 시각화하여 출력할 수 있다. 정보 제공부(220)는 시각화된 정보를 제공함으로써 사이버 보안 담당자들의 사이버 위협에 대한 전반적인 이해를 돕고 대응 전략 수립에 큰 도움을 줄 수 있다.

[0074] 이하에서는 도 4를 참조하여 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 장치(100)에 의해 수행되는 방법을 설명하도록 한다.

[0075] 도 4는 본 발명의 일 실시예에 사이버 지휘통제 의사결정 지원 방법의 순서도이다.

[0076] 먼저, 사이버 공격 프레임워크와 사이버 방어 프레임워크를 확률형 공격 트리 기반의 사이버 위협 모델링 방법으로 맵핑한다(S110).

[0077] 다음으로, 소정의 공공 데이터베이스에서 제공되는 공격기술의 실행 난이도 및 실행 소요시간을 포함하는 입력 요소를 소정의 인공지능 알고리즘에 적용하여 공격발생확률을 산출한다(S120).

[0078] 다음으로, 공격발생확률에 상응하는 상기 맵핑된 사이버 방어 프레임워크의 자산 취약성을 위험 분석 정보로 제공한다(S130).

[0079] 한편, 상술한 설명에서, 단계 S110 내지 S130은 본 발명의 구현예에 따라서, 추가적인 단계들로 더 분할되거나, 더 적은 단계들로 조합될 수 있다. 또한, 일부 단계는 필요에 따라 생략될 수도 있고, 단계 간의 순서가 변경될 수도 있다. 아울러, 기타 생략된 내용이라 하더라도 도 1 내지 도 3에 기술된 내용과 도 4에 기술된 내용은 상호 적용될 수 있다.

[0081] 이상에서 전술한 본 발명의 일 실시예에 따른 사이버 지휘통제 의사결정 지원 방법은, 하드웨어인 컴퓨터와 결합되어 실행되기 위해 프로그램(또는 어플리케이션)으로 구현되어 매체에 저장될 수 있다.

[0082] 상기 전술한 프로그램은, 상기 컴퓨터가 프로그램을 읽어 들여 프로그램으로 구현된 상기 방법들을 실행시키기 위하여, 상기 컴퓨터의 프로세서(CPU)가 상기 컴퓨터의 장치 인터페이스를 통해 읽힐 수 있는 C, C++, JAVA, Ruby, 기계어 등의 컴퓨터 언어로 코드화된 코드(Code)를 포함할 수 있다. 이러한 코드는 상기 방법들을 실행하는 필요한 기능들을 정의한 함수 등과 관련된 기능적인 코드(Functional Code)를 포함할 수 있고, 상기 기능들을 상기 컴퓨터의 프로세서가 소정의 절차대로 실행시키는데 필요한 실행 절차 관련 제어 코드를 포함할 수 있다. 또한, 이러한 코드는 상기 기능들을 상기 컴퓨터의 프로세서가 실행시키는데 필요한 추가 정보나 미디어가 상기 컴퓨터의 내부 또는 외부 메모리의 어느 위치(주소 번지)에서 참조되어야 하는지에 대한 메모리 참조관련 코드를 더 포함할 수 있다. 또한, 상기 컴퓨터의 프로세서가 상기 기능들을 실행시키기 위하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 통신이 필요한 경우, 코드는 상기 컴퓨터의 통신 모듈을 이용하여 원격에 있는 어떠한 다른 컴퓨터나 서버 등과 어떻게 통신해야 하는지, 통신 시 어떠한 정보나 미디어를 송수신해야 하는지 등에 대한 통신 관련 코드를 더 포함할 수 있다.

[0083] 상기 저장되는 매체는, 레지스터, 캐쉬, 메모리 등과 같이 짧은 순간 동안 데이터를 저장하는 매체가 아니라 반영구적으로 데이터를 저장하며, 기기에 의해 판독(reading)이 가능한 매체를 의미한다. 구체적으로는, 상기 저장되는 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있지만, 이에 제한되지 않는다. 즉, 상기 프로그램은 상기 컴퓨터가 접속할 수 있는 다양한 서버 상의 다양한 기록매체 또는 사용자의 상기 컴퓨터상의 다양한 기록매체에 저장될 수 있다. 또한, 상기 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장될 수 있다.

[0084] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0085] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

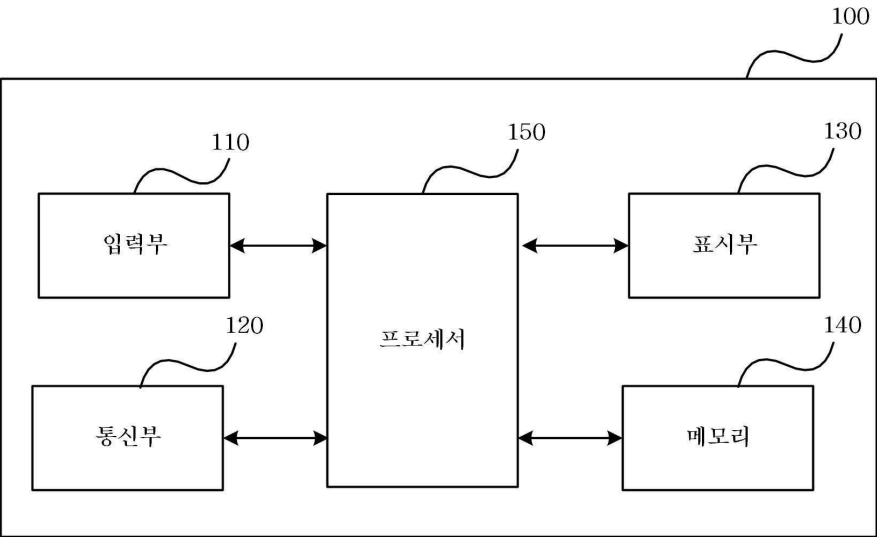
부호의 설명

[0087]

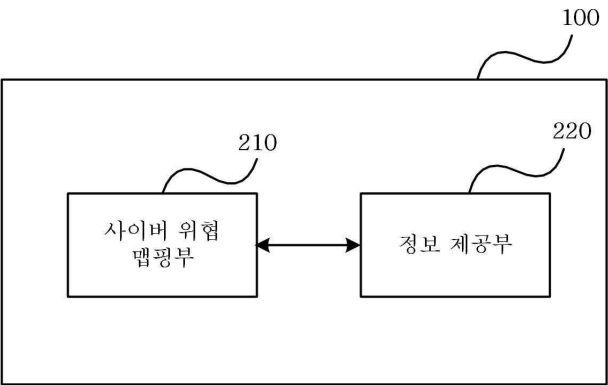
- 100: 사이버 지휘통제 의사결정 지원 장치
- 110: 입력부
- 120: 통신부
- 130: 표시부
- 140: 메모리
- 150: 프로세서
- 210: 사이버 위협 맵핑부
- 220: 정보 제공부

도면

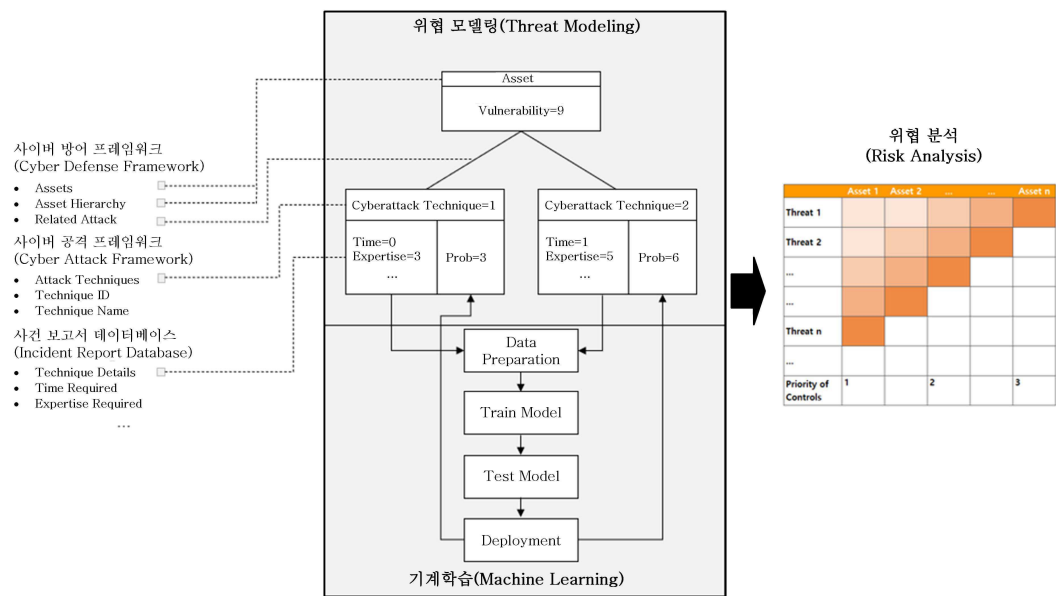
도면1



도면2



도면3



도면4

