EQST insight

보안위협의 변화와 효과적인 보안 취약점 대응 방안

■ 보안위협 변화와 위험 관리

최근 대부분의 기업들은 내부정보 유출을 막고 외부에서 접근해 오는 사이버 공격에 대응하기 위해 다양한 보안 솔루션을 도입해서 운영하고 있으며, 별도의 전문적인 보안담당자를 지정하여 보안 솔루션 관리 및 모니터링을 진행하고 있다.

과거에는 보안 인프라가 견고하지 않아 한 번의 공격으로도 공격자가 목적을 달성할 수 있었던 탓에 공격 빈도가 높고, 불특정 다수를 겨냥하는 공격 시도도 많았다. 그럼에도 보안담당자는 단일성 공격을 백신, IPS 등 보안장비의 업데이트만으로도 상당 부분 대응할 수 있었기에 다양한 보안 솔루션들의 관계성은 고려할 필요가 없었다. 이러한 흐름이 지속되면서 공격자들의 악의적인 공격은 성공 확률이 낮아졌고, 성공률을 높이기 위해 점점 더 복잡한 공격 형태로 진화하게 됐다.

이렇듯 보안 솔루션 간 상호 연계가 제대로 이뤄지지 않으면서, 최근 각 보안 솔루션에서 발생하는 대용량 로그가 보안담당자들이 탐지해 분석할 수 있는 가용 범위를 넘어섰다. 이를 해결하기 위해 다양한 보안 솔루션을 통합적으로 연계해 외부 침해 및 내부정보 유출을 방지하기 위한 통합관제(SIEM) 솔루션이 등장했으며, 고도화되고 지능화된 침입을 탐지 및 차단하기 위해 지속적으로 개선되고 있는 상황이다.

특히 최근 금융회사를 타깃으로 하는 공격이 늘고 있다. 금융 사이버 공간은 개인의 중요 금융 정보가 집약되고 관리되는 공간으로 실시간으로 악의적인 공격자들의 APT[1] 공격 침투 시도가 빈번히 발생하고 있는 상황이다. APT 공격은 보안 솔루션 탐지를 우회하기 위해 알려지지 않은 취약점을 악용하거나 샌드박스에서는 작동하지 않도록 설계됐기 때문에 하나의 보안 솔루션으로는 100% 탐지 및 차단할 수 없다. 하지만 금융보안 담당자는 이러한 위협에 선제적으로 대응해야 하며, 사이버위협 발생 시 중요 자산을 신속하고 안전하게 보호할 수 있도록 공격자를 식별하고 대처할 수 있어야 한다.

이에 금융회사들은 금융 관련 법규에 따라 운영리스크, 시장리스크, 신용리스크 등을 체계적이고 정량적으로 관리하고 있다. 하지만 아직 정보보호 리스크를 관리하기 위한 체계가 제대로 마련되지 않은 탓에 IT 보안 리스크를 정량화하여 관리하는 기업은 많지 않은 상황이다.

정보보호에 있어 위험관리는 기술적 데이터로 구성된 위협 및 취약점 정보를 관리적 측면의 정보로 나타낼 수 있는 방안이므로, 정보보호의 중요성을 토대로 이를 운영하기 위한 관리 체계가 반드시 수립되어야 한다. 일반적으로 정보보호 예방 활동에는 취약점 관리 업무와 별도로 정보보호 위험관리 업무가 있는데, 두 업무 간의 기술적, 관리적 측면에서 실시간 연결성을 가져가는 것이 매우 어렵다는 점에서 이러한 관리 체계의 필요성은 더욱 커진다.

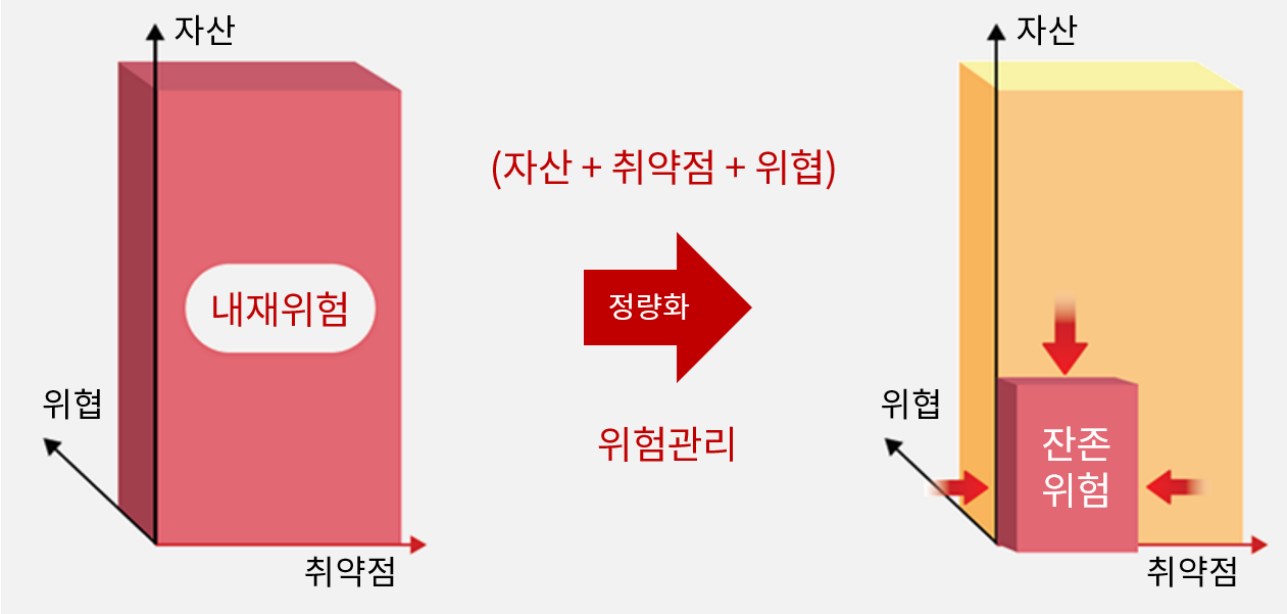
BNK 부산은행에서는 2016 년부터 위와 같은 보안위협의 변화와 위험관리의 필요성을 고려하여 정보보호 통합 플랫폼을 구축하고 있다. 본 기고문은 금융정보보호 컨퍼런스 'FISCON 2022'에서 발표된 '정량적 위험관리를 통한 통합 보안관제 구축 사례' 내용을 중점적으로 소개한다.

[1] APT(Advanced Persistent Threat, 지능형 지속 공격 위협) : 특정한 타깃을 대상으로 한 지속적으로 사이버 공격을 의미함.

■ 정보보호 위험관리

정보보호 위험관리 대상은 “자산의 가치, 자산이 가지고 있는 취약점, 외부의 위협”으로 구분할 수 있다.

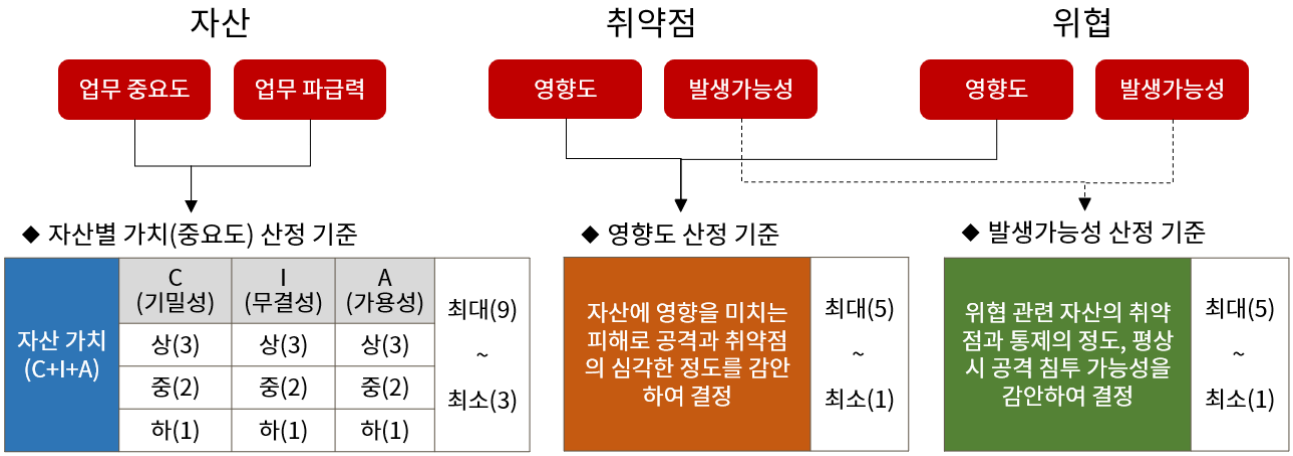
위협하는 자의 위협 행위와 정보를 취급하는 대상 자산의 취약성을 결합하여 위험 측정하고, 측정된 값이 높다는 것은 위험이 사고로 이어질 가능성이 높다는 것을 의미한다. 따라서 정보보호 위험관리라는 것은 “자산과 취약점, 위협을 종합하여 정량화된 수치가 나오고, 이것을 관리” 하는 것이며, “자산, 취약점, 위협”에 대한 내재 위험을 줄임으로써 잔존 위험을 최소화” 하는 것이 목적이다.



위험관리 체계 구축의 핵심은 위험관리의 중요 지표인 위험도를 기 보유한 보안 솔루션을 활용하여 어떻게 정량화하여 평가할 것인가에 대한 방안을 수립하는 것이다. 효율적인 위험관리 활동을 위해서는 모든 정보보호 활동이 위험관리를 중심으로 수행되어야 한다. 일반적인 위험도 평가 산식은 다음과 같으며, ‘자산 가치, 영향도, 발생가능성’을 결합하여 계산된다.

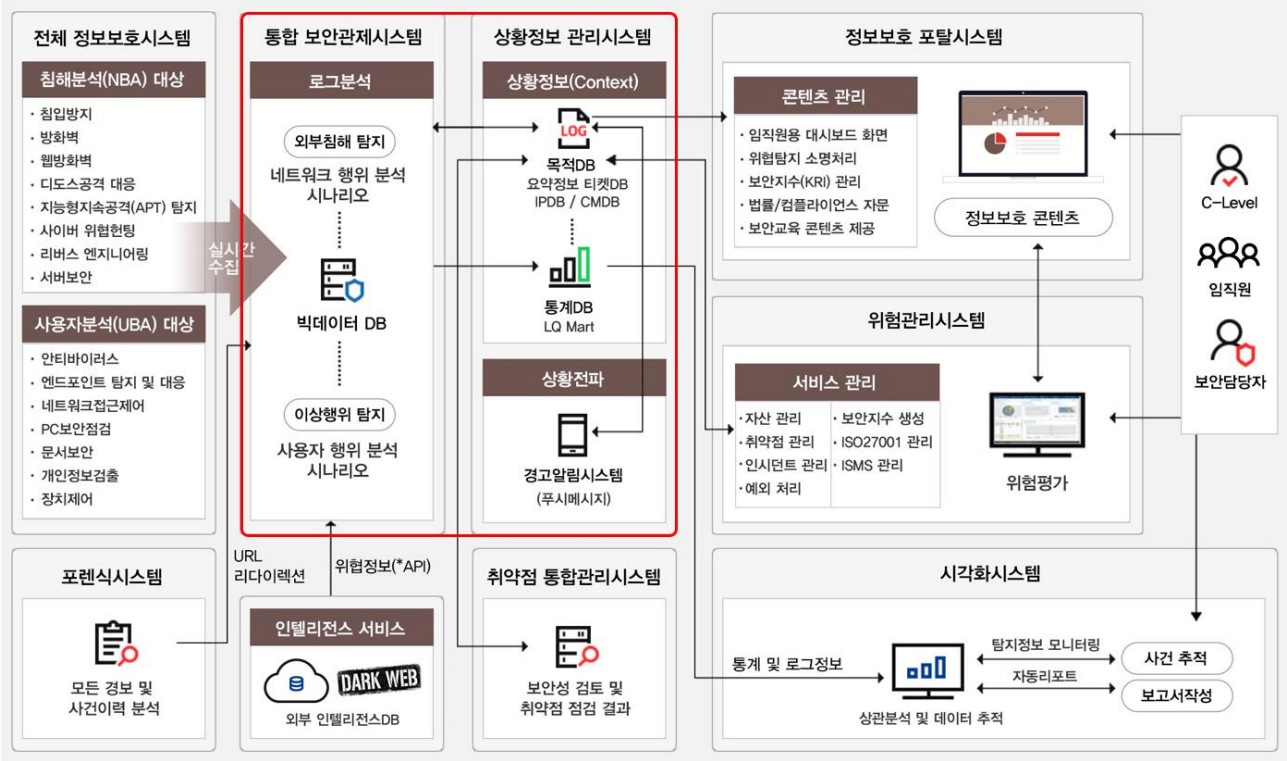
위험도(Risk Value) = 자산 가치(Asset Value) + 2 × 영향도(Impact) × 발생가능성(Likelihood)

자산 가치는 자산의 기밀성, 무결성 및 가용성 기준에 따라 자산 담당자가 정보보호 가이드 기준에 따라 산정한다. 영향도는 자산에 영향을 미치는 피해로써 공격과 취약점의 심각한 정도를 감안하여 결정된다. 발생가능성은 위협 관련 자산의 취약점과 통제의 정도, 평상 시 공격 침투 가능성을 감안하여 결정된다. 위험도를 계산하기 위한 3 대 요소에서 영향도와 발생가능성은 실시간 발생하는 위협에 영향을 받기 때문에 실시간으로 계산되어야 한다. 이를 위해 BNK 부산은행에서는 자산의 취약점과 실시간 수집되는 보안 솔루션의 로그를 결합하여 영향도와 발생가능성을 측정하도록 구성했다.

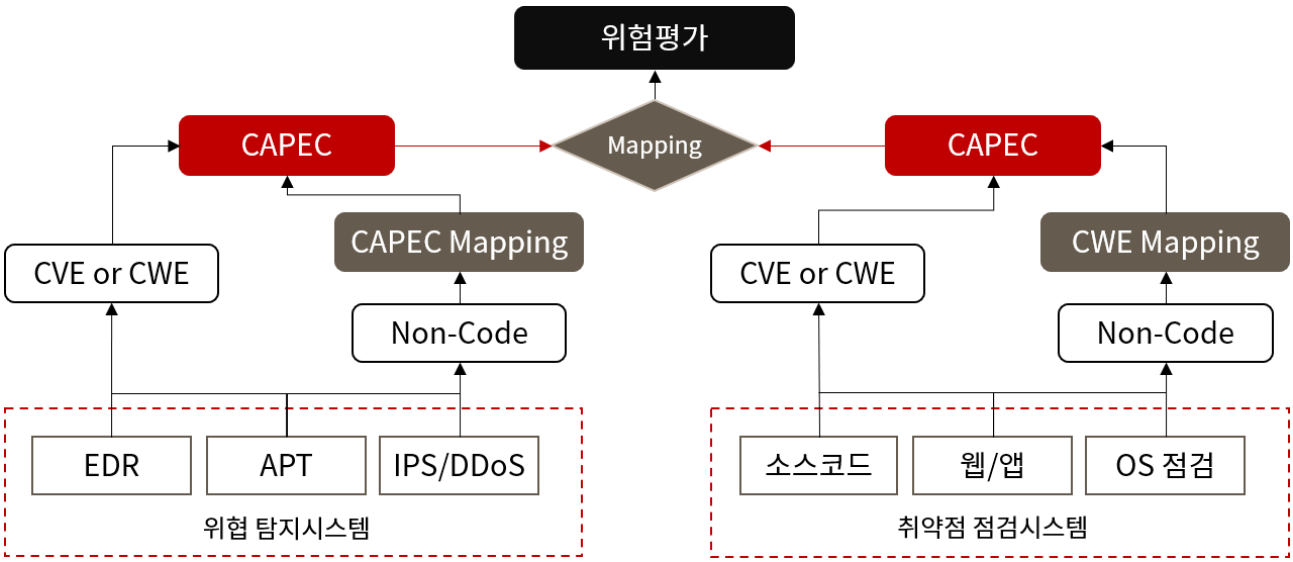


■ 정보보호 통합 플랫폼 구성

BNK 부산은행의 정보보호 통합 플랫폼 구성 현황은 다음과 같으며, 타 기관과 차별화된 통합 보안관제시스템 및 상황정보 관리시스템을 구축하고 있다. 특히 상황정보(Context)는 상황에 대한 올바른 판단과 활동을 위해서 행위 구성요소(대상자, 행위, 행위자)에 대한 현재 상태를 사람이 직관적으로 이해할 수 있도록 구성해야 한다.



통합 보안관제시스템에서는 행위를 기반으로 해킹 공격을 분석 및 평가하기 위해, 국제 표준인 CAPEC(Common Attack Pattern Enumeration and Classification, 사이버 공격 패턴 및 목록) 정보에 기반하여 취약점과 위협 간 관련성을 설계했다. 위협 탐지 시스템은 각자 가지고 있는 정책에 따라 위협을 탐지하게 되고, 시스템에 따라 CVE[2]나 CWE[3] 코드 등 탐지된 취약점을 매핑하여 나타내어 준다. 다음 그림과 같이 CVE 나 CWE 코드가 있으면 자동으로 CAPEC 으로 매핑되도록 구축하였고, 코드가 매핑되지 않으면 직원들이 수기로 CAPEC 코드를 매핑한다.



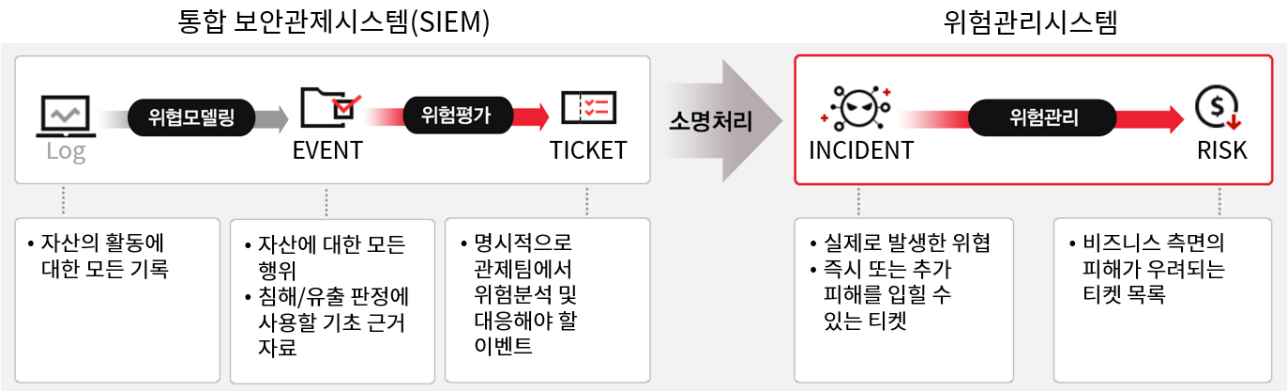
위협 탐지시스템과 유사하게 취약점에 대한 CVE 나 CWE 코드를 매핑하여 출력해 주는 취약점 점검 시스템도 있으며, 코드가 매핑되지 않으면 수기로 CWE 코드를 매핑한다. 이를 통해 탐지된 위협과 자산의 취약점을 연결시킬 수 있으며, 탐지된 위협이 자산의 취약점과 일치한다면 해당 위협에 대한 위험 평가를 높게 평가할 수 있다.

[2] CVE(Common Vulnerabilities and Exposures) : 공개적으로 알려진 컴퓨터 보안 결함 목록

[3] CWE(Common Weakness Enumeration) : 소프트웨어 및 하드웨어의 약점들을 찾아 분류해 놓은 목록

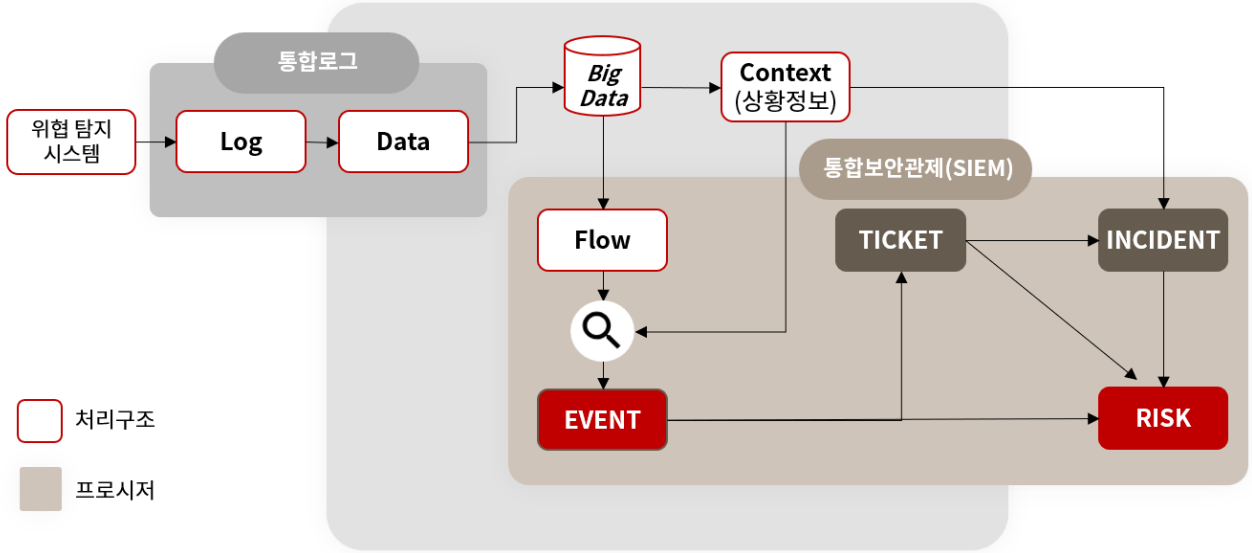
■ ETIR 모델 정의

통합 보안관제시스템과 위험관리시스템을 하나의 프로세스로 연동하여 관리하기 위해, BNK 부산은행은 데이터 흐름관점에서 ETIR 모델[4]을 정의했다. ETIR 모델에서는 예측 가능한 공격자의 위협 행위로부터 피해 정도를 예측하고, 인지된 사고에 대한 사실관계를 파악해 비즈니스적 위험 기준에서 위험 완화 전략을 수립한다.



위협 탐지 시스템에서 수집한 통합로그는 통합 보안관제시스템에서 ETIR 모델 관점으로 다음 그림과 같이 처리된다. 일반적인 기업과 동일하게 위협 탐지 시스템에서 생성된 로그는 파싱 및 정규화를 통해서 데이터화하고, 빅데이터 시스템에 저장하는 순으로 처리된다. 이후 대부분의 기업은 빅데이터를 역할에 기반하여(Role-based) 이벤트와 티켓으로 처리하지만, BNK 부산은행은 '상황 정보와 플로우'라는 개념을 통해서 이벤트를 생성한다.

[4] ETIR 모델(Event, Ticket, Incident, Risk) : 위협 정보로부터의 위험관리 과정을 일원화한 모델

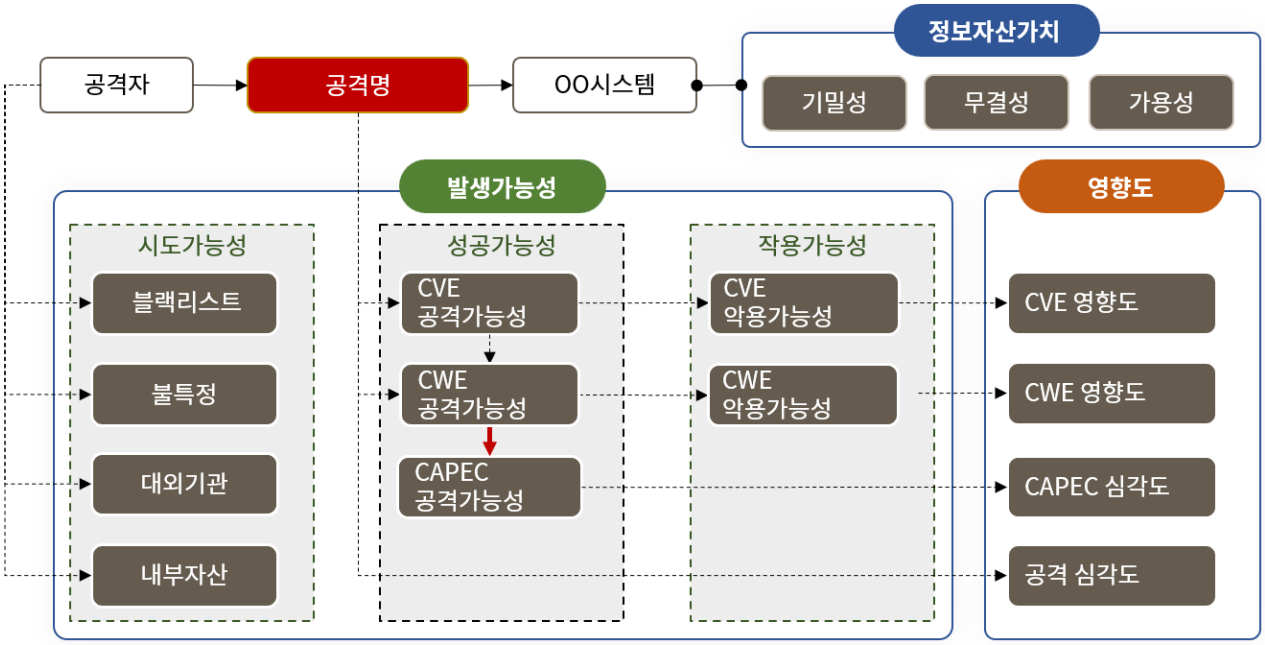


위험도는 정보자산가치와 발생가능성, 영향도를 합쳐서 계산된다. 정보자산가치는 일반적인 CIA[5](기밀성, 무결성, 가용성) 평가에 따르고, 발생가능성과 영향도는 위협과 자산 취약점 정보를 결합하여 계산한다. 발생가능성은 시도가능성과 성공가능성, 적용가능성을 결합하여 계산된다.

- 시도 가능성 : 공격자가 어떤 그룹에 속해 있는지에 따라 점수를 평가함
- 성공 가능성 : 탐지된 CAPEC 의 공격가능성 값을 활용하여 평가함
- 작용 가능성 : CVE 또는 CWE 의 악용가능성을 활용하여 평가함

[5] CIA(Confidentiality, Integrity, Availability) : 기밀성, 무결성, 가용성으로 정보의 보안 위험성을 측정하고 적절한 보안 정책을 수립하는 기준이 되는 보안의 기본 요소임

마지막으로 영향도는 CWE 영향도, CAPEC 심각도, 공격 심각도를 참고하여 평가한다. 이처럼 다양한 관점으로 발생가능성과 영향도를 측정하며, BNK 부산은행의 위험도 계산 주요 요소는 아래 그림과 같다.



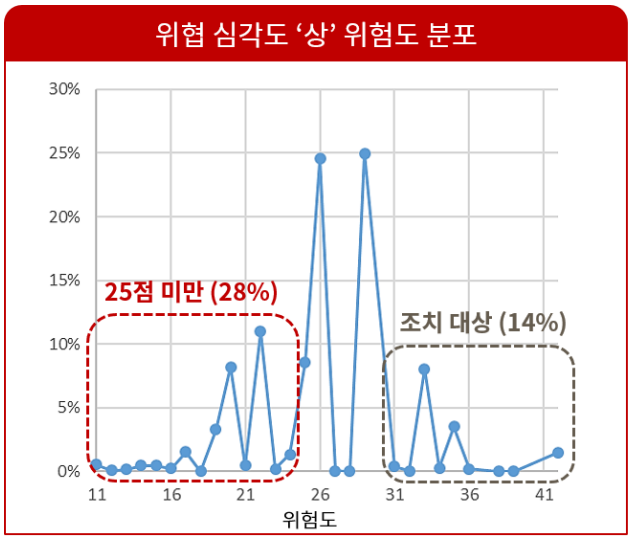
이후 이벤트에서 계산된 위험도가 수용 가능한 위험수준(DoA, Degree of Assurance)을 초과하면 티켓을 발행하며, 위험도가 DoA 미만인 경우에도 티켓과 연관된 이벤트는 분석 처리한다.

발생된 티켓은 보안 관제 직원이 소명 처리를 통해 사고 및 위험 유무를 식별하고, 이러한 소명 처리 내용은 위험관리 시스템에 축적된다. 위험관리 시스템에는 티켓뿐만 아니라 이벤트와 인시던트도 같이 저장하여 관리된다.

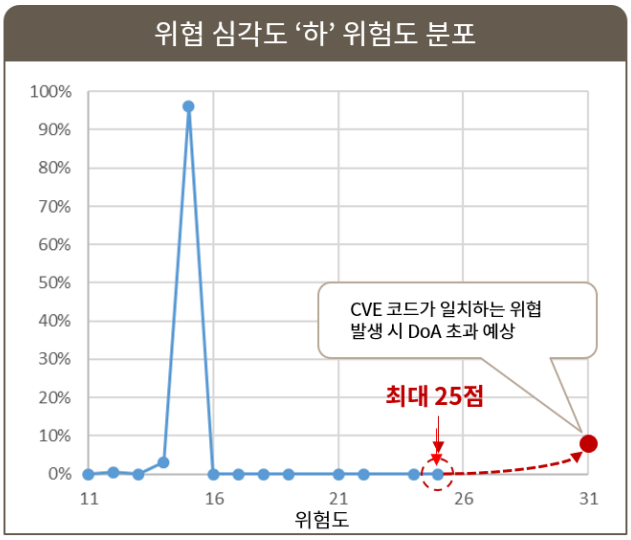
저장된 사고 및 위험 목록은 향후 사고로 발생할 가능성이 있는 경우(잔존위험) 위험 목록에 등록하고, 자산의 가치를 훼손하는 위험의 우선순위화를 통해 높은 순위부터 대응한다.

■ ETIR 티켓 효과

ETIR 모델에서는 실제 발생가능성이 높은 위협에 대한 티켓을 생성한다. 따라서 심각도 '상' 위협에서 위험도가 DoA 이상인 이벤트 14%에 대해서는 우선 조치한다. 또한 심각도 '하' 위협에서 가장 높은 위험도 점수는 25 점이였으며, 이는 심각도 '상' 위협 하위 28%에 해당한다. 즉, 위협의 심각도가 낮더라도 CVE 코드가 일치하는 위협이 발생하면 티켓이 생성될 수 있으므로, 위협 탐지 정확도가 증가하는 효과가 있다.

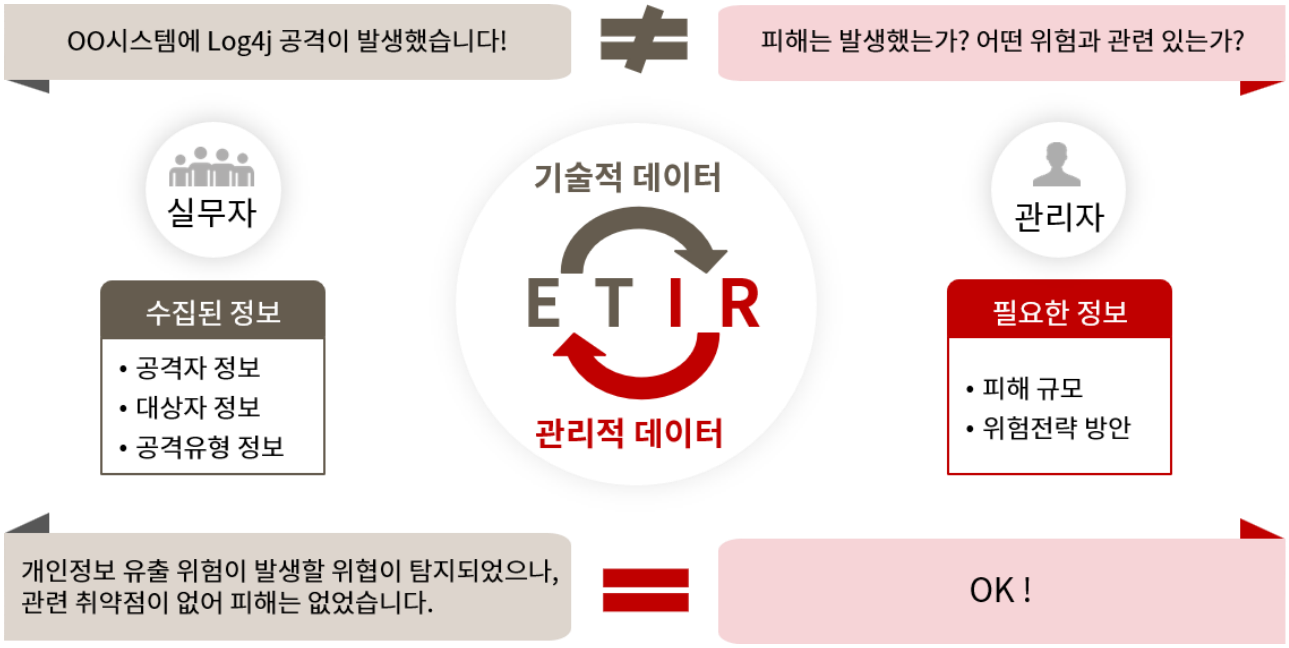


위험도 20~33 구간에서 88% 이벤트가 분포하며,
고른 분포로 인해 **정밀한 DoA 조정이 필요**함



위험도 14~15 구간에서 99% 이벤트가 분포하며,
DoA 25 이상에서는 **심각도 '중' 이상 중점 분석**이 필요함

한편 실무자와 관리자는 바라보는 관점이 다르기 때문에, 서로 의사소통을 쉽게 할 수 있는 방안을 마련하는 것이 중요하다. 즉 아래 그림과 같이 실무자는 수집된 기술적 데이터(공격자, 공격 유형 등)를 관리자에게 보고하지만, 관리자 관점에서는 관리적 데이터(피해 규모, 위험 전략 방안 등)를 필요로 한다. 이러한 소통을 원활히 제공할 수 있는 방안으로 ETIR 모델이 적합할 것으로 기대된다.



> 취약점을 찾는 것도 중요하지만, 식별된 취약점에 대한 활용방안 또한 중요하다. 취약점을 보안관제 및 컨설팅 영역에서 적합하게 활용할 수 있는 방안 가이드도 보안전문가에게 필요한 역량이라 할 수 있다.