2025 월간 위협 분석 보고서

침해사고 대응과 인텔리전스의 필요성

PLAINBIT 사이버위협대응센터
인텔리전스팀

※ 본 보고서는 2025년 11월 국가사이버안보센터(NCSC) 합동분석협의체를 통해 발간되었습니다.

2025 월간 위협 분석 보고서

침해사고 대응과 인텔리전스의 필요성

Contents

01 개요 #1

02 침해사고 대응 프레임워크의 이해 #3

03 사이버 위협 인텔리전스의 개념과 역할 #6

04 위협 행위자 식별을 통한 인텔리전스 방안 #9

05 결론 #12

01 서론

최근 사이버 공격은 단순 악성코드 감염이나 시스템 침입을 넘어 지속적이고 정교한 위협 형태로 발전하고 있다. 이러한 공격은 장기간에 걸쳐 특정 조직의 자산이나 정보를 목표로 하며, 공격자는 조직 내부의 취약점을 체계적으로 탐색하고 분석한 뒤 탐지를 회피할 수 있는 다양한 기법을 활용한다. 특히 이메일 피싱, 공급망 공격, 클라우드 환경 침해 등은 조직 내부의 방어를 우회하거나 신뢰 관계를 악용하는 방식으로 수행되어 단순한 보안 솔루션을 운영하는 것만으로는 탐지가 어려운 경우가 많다.

이러한 위협 환경 속에서 사고 대응(Incident Response, IR)은 단순한 기술적 복구 행위를 넘어 조직의 사이버 리스크 관리 체계 내에서 수행되어야 하는 핵심 기능으로 인식되고 있다. 즉, 침해사고 대응은 탐지된 이벤트를 단순히 처리하는 데 그치지 않고, 원인 분석, 영향 평가, 재발 방지 대책 수립 등 일련의 과정을 통해 조직의 보안 역량을 강화하는 지속적인 개선 활동으로 이어져야 한다.

미국 국립표준기술연구소(NIST)는 '사이버보안 위험 관리를 위한 침해사고 대응 가이드라인(SP 800-61r3)[1]'을 통해 기존의 4단계 대응 절차 대신, NIST 사이버보안 프레임워크(CSF 2.0)에 기반한 여섯 가지 기능을 중심으로 사고 대응을 재정의했다. 새로운 체계는 사고 대응을 단순한 기술적 절차에서 벗어나 조직 전체의 리스크 관리 활동으로 확장시킨 것이 특징이다.

최근 개정된 지침에서는 조직이 변화하는 위협 환경을 지속적으로 관찰하고, 조직 전반의 보안 상태를 주기적으로 평가하고 위협 동향을 반영해야 한다고 강조한다. 또한, 국내외 인텔리전스 네트워크를 확보해 사이버 위협 관련 정보를 수집하고 이를 분석에 활용함으로써, 침해사고 탐지 및 대응 능력을 향상시킬 것을 권고하고 있다. 이러한 내용은 수집된 사이버 위협 정보가 단순한 데이터 수집을 넘어 실시간 탐지, 우선순위 결정, 대응 정책 수립 등 실제 사고 대응 활동에 직접 활용되어야 한다는 것을 의미한다.

그러나 국내 기관 및 기업의 대응 체계는 여전히 사후적 성격이 강하며, 사이버 위협 인텔리전스의 활용 수준도 침해지표(IOC) 중심의 탐지에 머무르는 경우가 많다. 공격 그룹의 전술·기술·절차(TTPs)나 공격 인프라, 캠페인 패턴 등 고차원적인 분석 결과가 대응 프로세스에 충분히 반영되지 못함에 따라 동일 유형의 공격이 반복적으로 발생하고 대응 효율성 또한 제한되고 있다. 이러한 문제는 사고 대응과 사이버 위협 인텔리전스가 분리된 채 운영되는 구조적 한계에서 비롯된다.

---

[1] Alexander Nelson (NIST), Sanjay Rekhi (NIST), Murugiah Souppaya (NIST), Karen Scarfone (Scarfone Cybersecurity), "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile", NIST SP 800-61 Rev. 3, 2025-04-03, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

이에 본 보고서는 NIST SP 800-61r3 프레임워크를 기반으로 각 단계별 인텔리전스 활용 방안을 분석하고, 팔로알토네트웍스社의 연구를 참고해 공격자 행위 분석 결과를 인텔리전스 체계에 통합하여 대응 역량을 고도화하는 방안을 제안한다. 이러한 접근을 바탕으로, 보고서는 사이버 위협 인텔리전스가 제공할 수 있는 가치와 적용 지점을 명확히 정의하고, 공공기관을 포함한 보안 조직이 인텔리전스 기반 대응 체계를 설계할 때 고려해야 할 기술적 및 운영적 요소를 제시하고자 한다.

02 침해사고 대응 프레임워크의 이해

미국 국립표준기술연구소(NIST)가 발표한 Spection Publication 800-61 Revision 3 문서에서는 사이버보안 사고 대응에 대한 접근 방식을 새롭게 정의하고 있다. 이전까지 침해사고 대응은 주로 보안 담당 부서가 기술적으로 문제를 해결하는 절차로 인식되었지만, 이번 개정에서는 이를 조직 전체의 리스크 관리 프로세스와 연계된 지속적인 관리 체계로 확장했다. 특히 Rev.3 문서는 NIST 사이버보안 프레임워크(CSF 2.0)와 연동되도록 구성해 사고대응을 준비(Preparation)와 대응(Response)로 구분하고, 여기에 인텔리전스를 체계적으로 결합하는 방식을 제시하고 있다.

1. NIST SP 800-61r3 문서의 주요 개정 방향

NIST SP 800-61r3 문서의 개정 사항의 핵심 내용은 다음과 같이 크게 세 가지로 요약된다.

첫째, 기존의 4단계로 구성된 침해사고 대응 생애주기 모델인 ① 준비(Preparation), ② 탐지 및 분석(Detection & Analysis), ③ 격리와 제거 및 복구(Containment, Eradication & Recovery), ④ 사후 활동 (Post-Incident Activity) 단계를 폐지하고, 이를 NIST 사이버보안 프레임워크 2.0에서 제시하는 6가지 기능인 ① 거버넌스 수립(Govern), ② 위험 식별(Identify), ③ 보호 체계 구축(Protect), ④ 탐지(Detect), ⑤ 대응(Respond), ⑥ 복구(Recover)와 체계적으로 연결하였다. 이렇게 함으로써 사고 대응은 개별 부서나 기술 중심의 절차가 아니라, 조직 전체의 관리와 위험 통제를 포괄하는 통합 프로세스로 발전하게 되었다.

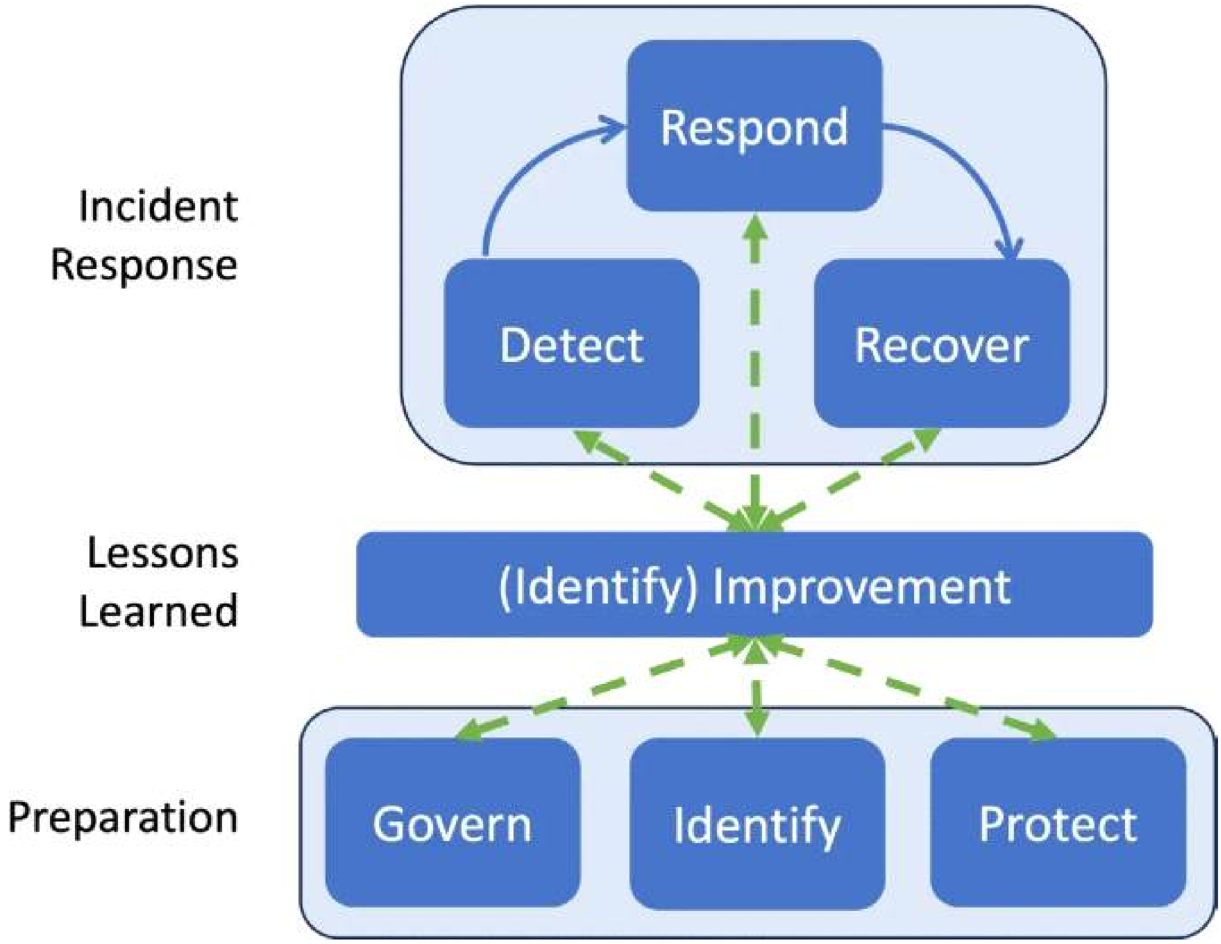
구분	주요 내용
NIST SP 800-61r2	• 4단계의 침해사고 대응 생애주기 모델 적용 : ① 준비(Preparation), ② 탐지 및 분석(Detection & Analysis), ③ 격리와 제거 및 복구(Containment, Eradication & Recovery), ④ 사후 활동 (Post-Incident Activity)
NIST SP 800-61r3	• NIST 사이버 보안 프레임워크 2.0에서 제시하는 6가지 기능과 연결 : ① 거버넌스 수립(Govern), ② 위험 식별(Identify), ③ 보호 체계 구축(Protect), ④ 탐지(Detect), ⑤ 대응(Respond), ⑥ 복구(Recover)

둘째, 인텔리전스는 더 이상 사고 대응의 보조 도구가 아닌 핵심적인 운영의 요소로 자리 잡았다. NIST는 인텔리전스를 통해 공격자의 목적과 전술을 사전에 파악하고, 사고 발생 시 신속하게 분석하며 복구 이후에는 그 결과를 정책과 절차에 다시 반영하는 순환 구조를 강조하고 있다. 이러한 구조를 통해 대응 활동은 단순한 사후 조치가 아닌 데이터 기반의 의사결정 과정으로 전환된다.

셋째, 지속적 개선 개념의 비중이 크게 강화되었다. 각 단계에서 얻은 교훈과 데이터는 다음 주기의 전략 수립과 정책 보완에 직접 반영되며, 침해사고 대응은 반복적인 사건 관리가 아니라 조직이 경험을 통해 점진적으로 성숙해지는 과정으로 자리 잡았다.

2. 인텔리전스가 반영된 6대 기능 구조

이번 절에서는 NIST가 제시한 여섯 가지 기능, 즉 거버넌스 수립(Govern), 위험 식별(Identify), 보호 체계 구축(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)가 인텔리전스와 어떻게 연계되는지를 구체적으로 살펴본다. 이때, Govern–Identify–Protect'를 사고 대응 이전의 준비 단계로, 'Detect–Respond–Recover'를 실제 사고 발생 이후의 대응 단계로 구분하여 여섯 가지 기능은 단순히 기술적 절차의 나열이 아니라, 조직이 위협 환경을 이해하고 대응 역량을 지속적으로 향상시키기 위한 관리 체계로 구성되어 있다.


Incident
Response
Respond
Detect
Recover
Lessons
Learned
(Identify) Improvement
Preparation
Govern
Identify
Protect

▲ 사이버 보안 프레임워크 2.0에 기반한 침해사고 대응 생명주기 모델
(출처 : NIST, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile", NIST SP 800-61 Rev. 3)

(1) Govern, Identify, Protect: 사전 대비와 방어 강화 단계

이 단계들은 조직이 인텔리전스를 기반으로 위협을 예측하고, 위험을 사전에 통제하기 위한 정책과 체계를 마련하는 과정이다. 단순히 보안 장비를 설치하거나 규정을 만드는 수준이 아니라, 인텔리전스를 통해 조직의 리스크를 정량적으로 파악하고, 이를 경영 의사결정에 반영하는 수준으로 발전시키는 것이 목표이다.

먼저 ‘거버넌스 수립(Govern)’ 단계에서는 인텔리전스를 통해 산업 전반의 위협 동향과 공격 패턴을 분석한다. 이렇게 도출된 정보는 경영진이 조직의 위험 허용 한계를 정하고, 보안 정책과 대응 전략의 우선순위를 결정하는 근거로 활용된다.

다음으로 ‘위험 식별(Identify)’ 단계에서는 내부의 주요 자산과 서비스, 그리고 그에 내재된 취약점을 외부 인텔리전스 정보와 비교하여 분석한다. 이를 통해 공격자가 실제로 이용할 가능성이 높은 공격 경로를 예측하고, 중요 자산을 중심으로 보호 대상을 선정한다.

마지막으로 ‘보호 체계 구축(Protect)’ 단계에서는 식별된 위험을 완화하기 위한 구체적인 보안 조치를 마련한다. 예를 들어, 인텔리전스 기반 공격 시나리오를 참고하여 접근 제어 정책을 세분화하거나, 사용자 인증 절차를 강화하고, 정기적인 보안 인식 교육을 실시한다. 또한 최신 위협 정보를 지속적으로 반영해 정책이 현실적인 대응력을 유지하도록 관리한다.

(2) Detect, Respond, Recover: 사고 탐지, 대응 및 복구 단계

이 단계는 실제 사고 발생 이후 조직이 인텔리전스를 활용해 탐지 정확도를 높이고, 대응 속도를 향상시키며, 복구를 통해 체계를 개선하는 과정을 의미한다. 인텔리전스는 기술적 도구를 지원하는 부가적 데이터가 아니라, 모든 의사결정의 중심이 된다.

먼저 ‘탐지(Detect)’ 단계에서는 인텔리전스에서 제공하는 침해 지표(Indicators of Compromise), 공격자의 행위 패턴, 위협 데이터베이스 정보를 실시간으로 분석한다. 이를 SIEM이나 EDR 같은 탐지 시스템에 적용해 공격 징후를 조기에 식별하고, 위협 탐지의 정확도를 높인다.

다음으로 ‘대응(Respond)’ 단계에서는 공격자의 인프라 정보, 명령·제어 서버 주소, 관련된 공격 캠페인 정보를 활용해 대응 절차를 자동화한다. 보안 운영팀은 인텔리전스 데이터를 기반으로 대응 우선순위를 결정하고, SOAR 시스템을 통해 차단 및 경보 조치를 즉시 실행할 수 있다.

마지막으로 ‘복구 및 개선(Recover)’ 단계에서는 사고 처리 과정에서 얻은 교훈과 데이터를 다시 인텔리전스 체계에 반영한다. 복구 과정에서 발견된 새로운 공격 지표나 전술은 사이버 위협 인텔리전스 플랫폼에 등록되고, 이를 바탕으로 향후 탐지 정책이 업데이트된다. 이러한 과정을 반복함으로써 조직은 점차 인텔리전스 중심의 자율적 대응 체계로 발전할 수 있다.

03 사이버 위협 인텔리전스의 개념과 역할

1. 사이버 위협 인텔리전스의 개념

사이버 위협 인텔리전스(Cyber Threat Intelligence, CTI)는 단순히 침해 지표(Indicators of Compromise, IOC)를 수집하는 기술적 활동을 넘어, 위협 행위자의 전략, 전술, 기법을 분석하고 이를 바탕으로 조직의 대응 전략을 고도화하는 지식 체계이다. 인텔리전스는 침해사고 대응의 각 단계에서 핵심적인 의사결정 요소로 작용하며, 특히 NIST SP 800-61r3에서 제시한 새로운 프레임워크 안에서는 사고 대응을 지속적으로 개선하고 자동화하는 기반이 된다.

인텔리전스는 그 활용 목적과 범위에 따라 '전략적 인텔리전스(Strategic Intelligence)', '전술적 인텔리전스(Tactical Intelligence)', '운영적 인텔리전스(Operational Intelligence')의 세 가지 수준으로 구분된다.

3 WAYS
TO DELIVER THREAT INTELLIGENCE
01
Strategic Threat Intelligence
02
Tactical Threat Intelligence
03
Operational Threat Intelligence

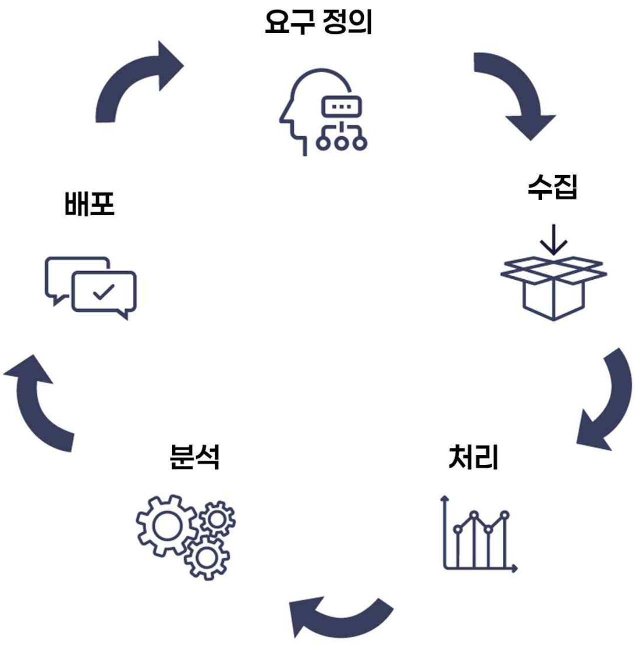
▲ 사이버 위협 인텔리전스의 목적 및 범위에 따른 구분
(출처 : Fortinet, "Cyber Threat Intelligence: Defending Against Evolving Cyber Threats")

'전략적 인텔리전스'는 국가나 산업 전반의 위협 동향과 장기적 보안 전략 수립을 지원하는 고수준의 정보로, 경영진이나 정책 결정자가 조직의 방향성을 설정할 때 활용된다. '전술적 인텔리전스'는 공격자의 전술·기술·절차(TTPs)를 세부적으로 식별하고 이를 탐지 규칙과 방어 체계에 직접 반영하는 역할을 한다. '운영적 인텔리전스'는 특정 공격 캠페인이나 위협 행위자의 활동 패턴을 중심으로 분석되어, 보안 운영팀이 실질적인 대응 전략을 설계할 때 근거로 사용된다.

이러한 세 단계는 서로 유기적으로 연결되어 있으며, 전략적 인사이트는 전술 및 운영적 대응으로 이어지고, 하위 수준의 분석 결과는 다시 상위 수준의 의사결정에 반영되는 순환 구조를 형성한다.

2. 사이버 위협 인텔리전스의 수집과 분석 과정

인텔리전스는 다양한 출처에서 데이터를 수집하고, 이를 구조화된 분석 과정을 통해 위협 정보를 도출한다. 일반적으로 다음과 같은 '5단계 생애주기(Lifecycle)'를 따른다. 인텔리전스는 다양한 출처에서 데이터를 수집하고 이를 정제·분석해 위협 정보를 도출하는 과정을 거친다. 이 과정은 단순한 데이터 수집이 아니라 정보를 체계적으로 관리하고 활용하기 위한 반복적 순환 구조로 구성되며, 각 단계는 서로 긴밀히 연결되어 지속적인 개선이 이루어진다.



▲ 사이버 위협 인텔리전스의 5단계 생애 주기(Lifecycle)

첫 번째 단계는 '요구 정의' 단계로, 조직은 보호해야 할 핵심 자산과 보안 목표, 예상되는 위협 요소를 식별한다. 이 단계에서 인텔리전스 수집의 범위와 우선순위를 명확히 설정함으로써, 이후의 분석이 조직의 실질적 위험에 초점을 맞출 수 있도록 한다.

두 번째는 '수집' 단계이다. 이 단계에서는 공개 정보(OSINT), ISAC, CERT 간 정보 공유 등과 같은 폐쇄형 위협 정보 네트워크, 내부 시스템 로그, 악성코드 분석 결과 등 다양한 출처에서 데이터를 확보한다. 수집된 데이터는 양보다 질이 중요하며, 신뢰할 수 있는 출처와 최신의 데이터 확보가 핵심이다.

세 번째는 '처리' 단계로, 수집된 데이터를 정제하고 표준화하여 분석 가능한 형태로 변환한다.

중복된 침해 지표를 제거하고, 위협 수준이나 신뢰도를 평가하는 과정이 포함된다. 예를 들어, 각 데이터는 민감도나 공유 가능 범위를 명시하는 TLP[2] 기준에 따라 분류된다.

네 번째는 '분석' 단계로, 수집된 데이터 간의 상관관계를 파악해 공격자의 전술·기술·절차를 식별한다. 이 단계에서는 MITRE ATT&CK 프레임워크, 다이아몬드 모델 등과 같은 분석 프레임워크가 활용되어 공격 행위의 맥락을 체계적으로 이해할 수 있다.

마지막으로 '배포' 단계에서는 분석 결과를 관련 이해 관계자에게 전달하고, 탐지 규칙이나 보안 정책을 업데이트한다. 이 과정에서 인텔리전스는 단순한 보고서 형태가 아니라, 자동화된 시스템과 연동되어 실시간으로 활용될 수 있도록 설계된다.

이 다섯 단계는 일회성으로 끝나는 절차가 아니라, 새로운 위협이 발생할 때마다 갱신되는 순환적 구조이다. NIST SP 800-61r3 문서에서 강조하는 '지속적인 개선' 개념은 바로 이 인텔리전스 생애주기의 반복적 순환을 의미하며, 조직이 경험을 통해 대응 능력을 지속적으로 향상시키는 기반이 된다. 지속적 개선 개념은 바로 이 인텔리전스 생애주기의 순환 구조와 맞닿아 있다.

3. 침해사고 대응에서의 인텔리전스 역할

본 절에서는 인텔리전스가 이러한 각 단계를 유기적으로 연결하고 전체 프로세스의 효율성을 높이는 방식에 초점을 맞춘다. 인텔리전스는 개별 단계의 보조적 수단이 아니라, 모든 절차를 통합적으로 관리하고 최적화하는 핵심 축으로 작용한다.

예를 들어, 인텔리전스는 준비 단계에서 수집된 위협 정보가 탐지 정책에 반영되도록 하고, 탐지 단계에서 새롭게 확인된 공격 행위가 대응 전략 수립에 즉시 활용되도록 한다. 또한 대응 과정에서 생성된 데이터와 교훈은 복구 단계뿐만 아니라 이후의 전략적 보안 의사결정에도 영향을 미친다. 즉, 인텔리전스는 각 단계 간의 정보 흐름을 매개하여, 사고 대응이 일회성 조치가 아니라 지속적으로 발전하는 순환 구조로 작동하도록 만든다.

이러한 인텔리전스 중심의 접근 방식은 NIST SP 800-61r3 문서에서 제시하는 '지속적인 개선' 개념과 일맥상통하며, MITRE ATT&CK 프레임워크와 다이아몬드 모델에서 강조하는 '위협 행위자 중심 분석'의 철학과도 맞닿아 있다. 결국 인텔리전스는 개별 대응 단계를 조율하고 학습 가능한 구조로 진화시키는 지식 기반 자산으로서, 조직의 사고 대응 체계를 전사적 수준에서 고도화하는 역할을 수행한다. 즉, 인텔리전스는 침해사고 대응의 각 단계를 개별적인 절차가 아닌 하나의 통합된 지식 체계로 연결하는 매개체라고 할 수 있다.

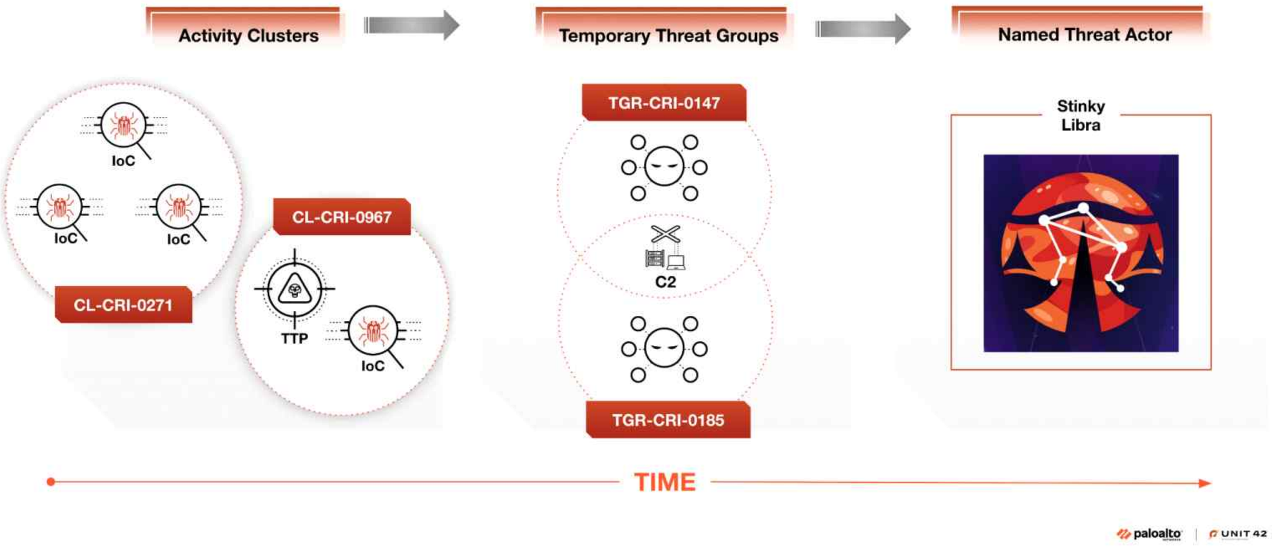
---

2) Traffic Light Protocol

04 위협 행위자 식별을 통한 인텔리전스 적용 방안

사이버 위협 인텔리전스의 고도화는 단순히 공격 징후를 식별하는 수준을 넘어 공격의 배후에 있는 행위자와 그들의 동기, 목적, 수단을 분석하는 단계로 발전하고 있다. 이러한 분석 과정을 'Attribution'이라고 표현하며, 이는 위협 행위자를 식별하거나 특정 국가, 조직, 혹은 그룹과의 연관성을 도출하는 것을 의미한다. 위협 행위자를 식별하는 과정은 단순한 기술적 탐지 정보를 넘어 공격자의 전술적, 전략적 의도를 이해하고 장기적인 방어 전략을 수립하는데 필수적인 인텔리전스 활동이다.

위협 행위자 식별을 기반으로 한 인텔리전스 방안은 팔로알토네트웍스社의 사이버 위협 인텔리전스 및 사고 대응 조직인 Unit42의 Attribution 프레임워크에서 방향성을 찾을 수 있다. 이 프레임워크는 사이버 위협을 '행위(Activity)', '임시 위협 그룹(Temporary Threat Group)', '명명된 위협 그룹(Named Threat Actor)'의 3단계로 구분하여 개별 공격이 발생하면서 생기는 이벤트를 점진적으로 더 큰 위협 맥락으로 통합한다.


Activity Clusters
Temporary Threat Groups
Named Threat Actor
IoC
IoC
IoC
CL-CRI-0271
CL-CRI-0967
TTP
IoC
TGR-CRI-0147
C2
TGR-CRI-0185
Stinky Libra
TIME
paloalto | UNIT 42

▲ Unit42 Attribution 프레임워크의 3단계 구성
(출처 : PaloaltoNetworks Unit42, "Introducing Unit 42's Attribution Framework")

1. Unit42 Attribution 프레임워크의 구조와 특징

Unit42의 Attribution 프레임워크 모델은 위협 인텔리전스의 분석 체계를 계층적으로 수립한 대표적인 사례이다. 가장 하위 단계인 '행위(Activity)'는 단일한 공격 사건이나 캠페인을 의미한다. 예를 들어, 특정 피싱 이메일 캠페인이나 악성코드 유포 사건이 이에 해당한다. 이 단계에서는 공격에 사용된 도메인, 해시, 인프라, 악성 파일 등의 기술적 지표가 수집된다.

이러한 다수의 행위가 일정한 유사성을 보일 경우, 이를 묶어 '임시 위협 그룹(Temporary Threat Group)'으로 분류한다. 이 그룹은 공격 기법, 인프라 재사용, 피해 대상, 언어·시간대 등의 공통점을 기준으로 구성된다. 임시 위협 그룹은 위협 행위자의 활동 패턴을 중간 수준에서 파악할 수 있게 하며, 장기적인 행위자 식별을 위한 기초 데이터를 제공한다.

마지막으로 충분한 증거가 확보되고 공격의 지속성과 일관성이 입증될 경우, 해당 위협 그룹은 명명된 위협 행위자(Named Threat Actor)로 분류된다. 예를 들어, Kimsuky, Lazarus, APT37 등과 같은 명칭이 여기에 해당한다. 이 단계에서는 기술적 지표뿐 아니라 정치적 동기, 목표 산업군, 협력 관계 등과 같은 전략적 요인까지 분석 대상에 포함된다.

2. Unit42의 위협 행위자 식별 기준과 접근 방식

Unit42는 위협 행위자를 식별할 때 명확하고 재현 가능한 기준을 통해 일관된 판단을 유지하고 있다. 이들은 공격 활동을 세 단계로 구분해 각 단계별로 필요한 최소한의 근거를 명확하게 제시한다. 이러한 기준은 분석의 객관성을 높이고, 위협 행위자에 대한 신뢰성 있는 결론을 도출하기 위한 최소 요건으로 활용된다.

첫째, 전술·기술·절차(TTPs)에 대한 분석이다. Unit42는 공격의 행위가 일정한 일관성을 보일 때만 위협 행위자 식별이 가능하다고 본다. 초기 단계에서는 악성코드나 인프라의 유사성이 주요 근거가 되며, 중간 단계에서는 커스텀한 도구의 재사용이나 동일한 공격 패턴이 확인되어야 한다. 최종적으로 명명된 위협 그룹으로 판단하기 위해서는 공격자가 고유한 도구 체계와 공격 방식을 지속적으로 유지하고 있어야 한다.

둘째, 인프라와 도구 분석이다. Unit42는 단순히 동일한 인프라를 사용하는지 여부가 아니라, 인프라의 운영과 관리 방식, 도메인 등록 패턴, 명령제어 서버의 구성, 빌드 환경의 일관성 등을 종합적으로 검토한다. 특히 장기간에 걸쳐 일관된 인프라 사용이 확인될 경우, 위협 행위자 식별의 신뢰도는 높게 평가된다.

셋째, 타겟과 피해자 분석이다. 기술적 유사성만으로는 충분하지 않기 때문에, 공격자가 반복적으로 특정 산업이나 지역을 대상으로 삼았는지, 피해 조직의 특성이 일정한지 등을 함께 고려한다. 공격 대상의 일관성은 행위자의 전략적 의도와 목적을 추정할 수 있는 중요한 단서로 활용된다.

마지막으로, 시간적 지속성과 운영상의 습관이 평가된다. Unit42는 일정 기간 이상 동일한 패턴으로 활동이 이어진 경우에만 높은 신뢰도를 부여한다. 또한 공격자의 언어 흔적, 코드 작성 습관, 시간대 패턴 등 비기술적 특성 역시 분석 대상이 된다. 이러한 요소들은 행위자의 고유한 행동 특성을 파악하고, 지속적으로 관찰되는 행위 패턴을 통해 식별의 정확도를 높인다.

이러한 기준들은 절차가 아닌 원칙으로서 상호 보완적으로 작용한다. Unit42는 이를 바탕으로

신뢰도를 낮음, 중간, 높음의 세 수준으로 구분하여 평가하며, 각 수준은 증거의 양과 질, 일관성에 따라 결정된다. 이러한 접근은 단순히 공격자를 특정하는 것을 넘어, 왜 공격이 발생했는지와 어떤 방식으로 수행되었는지를 이해하는 데 중점을 둔다.

구분	**초기 단계** (Activity Cluster)	**중간 단계** (Temporary Threat Group)	**최종 단계** (Named Threat Actor)
TTPs 분석	• 동일한 악성코드 계열, 인프라, 코드 서명 등 기초적 유사성 확인	• 커스텀 툴·스크립트 재사용, 일관된 공격 시점 및 패턴 식별	• 독자적인 TTP 집합 보유, 고유한 공격 생애주기 및 도구 체인 유지
인프라 및 도구 분석	• 도메인/IP 등 인프라 지표의 유사성 확인	• 인프라 구성·운영 방식 • 빌드 환경의 지속성 분석	• 장기적 인프라 사용 일관성 및 독자적 툴셋 유지 여부 평가
표적 및 피해자	• 동일 산업/지역 대상 반복적 공격 식별	• 피해 조직의 기술 스택 • 의도(금전·정보·파괴) 분석	• 공격 동기 • 전략적 목적 • 지역적 특성 명확화
시간적 일관성	• 단기적 활동 유사성 확인	• 최소 6개월 이상 지속된 활동 확인	• 장기적 활동 패턴의 일관성 및 반복된 캠페인 수행 평가
운영보안(OPSEC) 및 기타 요소	• 언어 흔적·코드 서명 등 기초적 단서 식별	• OPSEC 습관, 코드 주석, 시간대 등 비기술적 지표 평가	• 고유한 운영 습관·언어 패턴·전술적 의사결정 구조 분석

05 결론

본 보고서는 NIST SP 800-61r3 문서에서 제시하는 침해사고 대응 프레임워크와 팔로알토네트웍스社의 Unit42가 정의한 위협 행위자 식별 방안을 중심으로 인텔리전스 기반 사고 대응 체계의 방향성을 제시하였다. 이를 통해 사이버 위협 인텔리전스는 단순히 사고 발생 후의 분석 도구가 아닌 사고 대응의 전 과정을 지탱하는 핵심 축으로 작용함을 확인할 수 있었다.

NIST SP 800-61r3 문서는 사고 대응을 기술적 절차의 연속으로 보는 기존 관점에서 탈피하여 거버넌스와 리스크 관리의 연장선에서 지속적으로 개선되는 관리 체계로 재정의하였다. 특히 인텔리전스를 탐지, 대응, 복구뿐 아니라 거버넌스와 보호 체계 구축 단계까지 통합함으로써, 보안 운영의 전 주기를 데이터 기반으로 전환할 수 있는 토대를 마련하였다. 이는 조직이 '사고를 처리하는 것'에서 '위험을 관리하는 것'으로 패러다임을 전환하는 중요한 이정표라 할 수 있다.

한편 Unit42의 위협 행위자 식별 방안은 위협 인텔리전스의 분석 신뢰도를 정량화하고 표준화한 사례로 평가된다. 전술·기술·절차 분석, 인프라 및 도구 운영 방식, 표적의 일관성, 시간적 지속성, 운영 습관 등 다층적인 기준을 통해 위협 행위자의 정체를 식별함으로써, 단순한 IOC 중심의 탐지 체계에서 벗어나 보다 고도화된 인사이트를 제공한다. 이를 통해 조직은 공격의 기술적 특성 뿐 아니라 전략적 배경과 동기를 함께 파악할 수 있으며, 이는 향후 대응 전략 수립에 실질적인 도움을 제공한다.

따라서 인텔리전스 기반 사고 대응의 핵심은 '정보의 수집'이 아니라 '맥락의 이해'에 있다. 조직은 다양한 출처에서 수집된 인텔리전스를 통합·분석하여, 이를 경영적 의사결정과 기술적 대응에 모두 활용할 수 있는 체계를 구축해야 한다. 또한, Unit42가 제시한 기준처럼 위협 행위자 식별의 신뢰 수준을 명확히 구분함으로써, 인텔리전스 활용의 객관성과 투명성을 확보해야 한다.

향후에는 이러한 프레임워크를 기반으로 한 자동화와 협업 체계가 더욱 중요해질 것이다. 위협 인텔리전스 플랫폼(TIP), 보안 오케스트레이션(SOAR), 머신러닝 기반 위협 예측 기술이 결합될 경우, 조직은 실시간으로 인텔리전스를 생성·활용하는 자율적 방어 체계를 구현할 수 있다. 나아가 정부 기관, 산업별 ISAC, 민간 보안업체 간의 협력을 통해 인텔리전스의 품질과 활용도를 극대화하는 것이 필요하다.

결국 인텔리전스는 단순한 보조 도구가 아니라, 사고 대응의 출발점이자 중심축으로 기능해야 한다. 본 보고서에서 제시한 방향성을 바탕으로, 공공기관과 민간 기업이 인텔리전스 중심의 사고 대응 문화를 정착시킨다면, 향후 사이버 위협에 대한 국가적 대응 역량 또한 한층 강화될 것으로 기대된다.

참고자료

[1] Alexander Nelson (NIST), Sanjay Rekhi (NIST), Murugiah Souppaya (NIST), Karen Scarfone (Scarfone Cybersecurity), "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile", NIST SP 800-61 Rev. 3, 2025-04-03, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[2] PaloaltoNetworks Unit42, "Introducing Unit 42's Attribution Framework", 2025-07-31, https://unit42.paloaltonetworks.com/unit-42-attribution-framework/

[3] Fortinet, "Cyber Threat Intelligence: Defending Against Evolving Cyber Threats", https://www.fortinet.com/resources/cyberglossary/cyber-threat-intelligence