보안 모니터링 및 대응의 진화, Threat Hunting 을 위한 고려사항

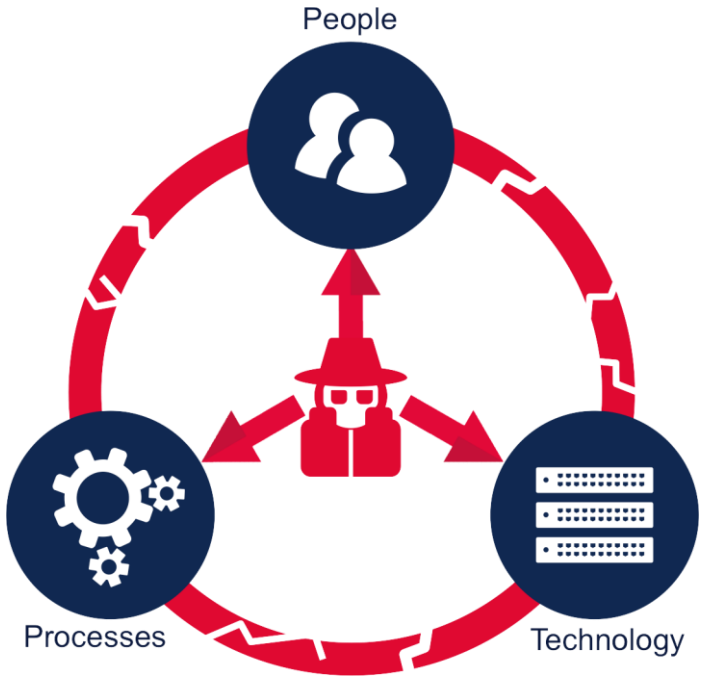
김용호 부장(yonghkim@cisco.com)
보안컨설턴트, 시스코 보안컨설팅 서비스팀

보안 위협의 새로운 트렌드 : 탄력성 vs. 협력성

효과적인 공격을 위한 빠르고 지속적인 변화

공격에 대한 즉각적인 대응의 불확실성

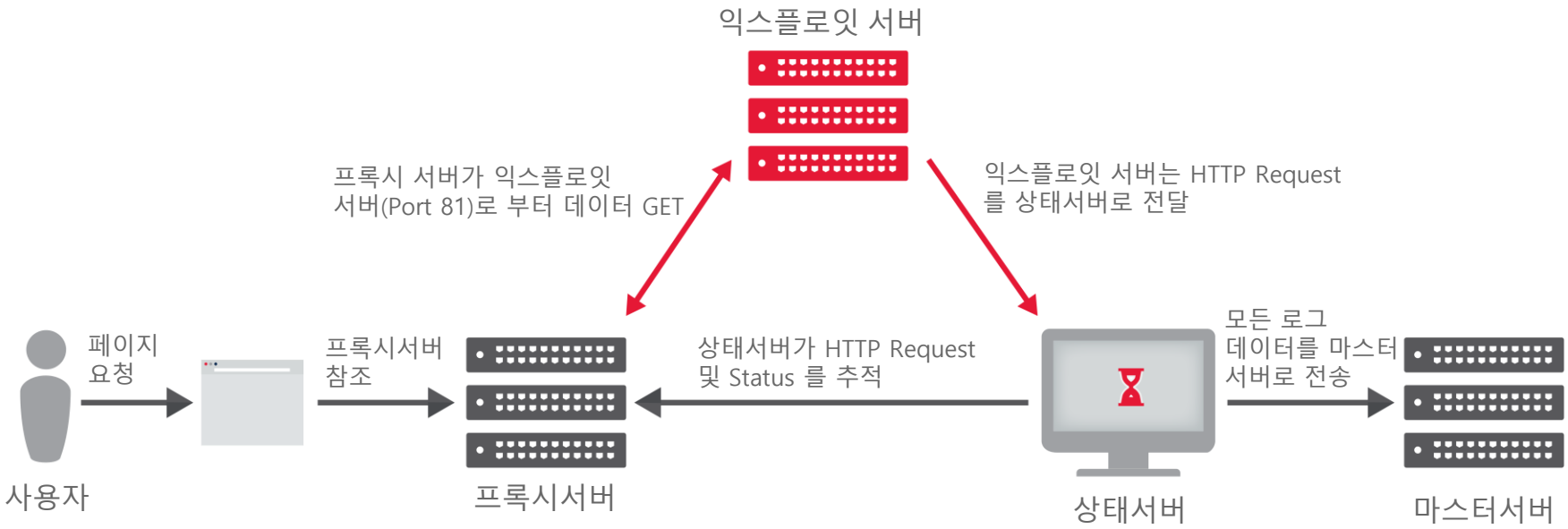
조각화된 대응으로 인한 효과적인 대응 불가



참고자료 : 시스코 연례 보안 보고서 2016

탄력적 구조의 공격 인프라 확대

- 우회 및 신속한 재구성 목적의 설계



참고자료 : 시스코 연례 보안 보고서 2016

사이버 보안 인프라 및 체계에 대한 확신 감소

59%

최근 기술에 대한 신뢰도

-5%

51%

보안 취약점의 지능적인 탐지 능력에 대한 확신

0%

54%

방어 능력에 대한 확신

-4%

45%

공격 억제 범위의 산정 및 식별 능력에 대한 확신

-1%

54%

공격 검증 능력에 대한 확신

+0%

56%

정기적인 보안 정책에 대한 리뷰

+0%

참고자료 : 시스코 연례 보안 보고서 2016

복잡성과 조각화된 대응

사일로화 된 보안체계로는 신속한 보안 대응 및 보호 불가

54

특정 고객이 사용하고 있는 전체 보안 관련 제품 제조사 수

1208

$7.3B

지난 5년간 벤처캐피탈로부터 투자를 받은 스타트업 회사 및 투자금 규모

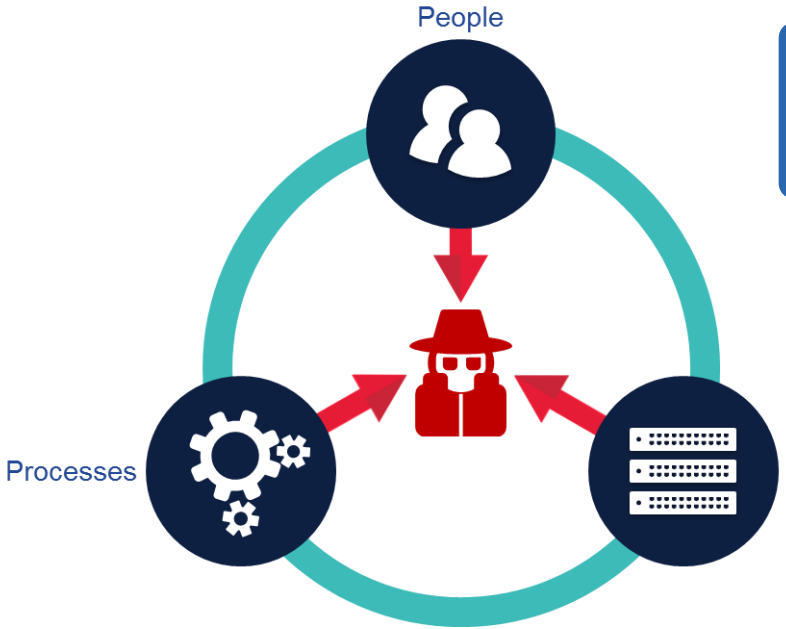
12x

보안 전문 운영 능력, 팀, 인력에 대한 요구

참고자료 : 시스코 연례 보안 보고서 2016

The beginning of Threat Hunting

실행력을 갖춘 협력 기반의 위협 색출, 그리고 선제적 제압



Actionable Collaboration

- 조직(People), 프로세스(Process) 및 기술(Technology) 전반에 걸친 실행력있는 협력

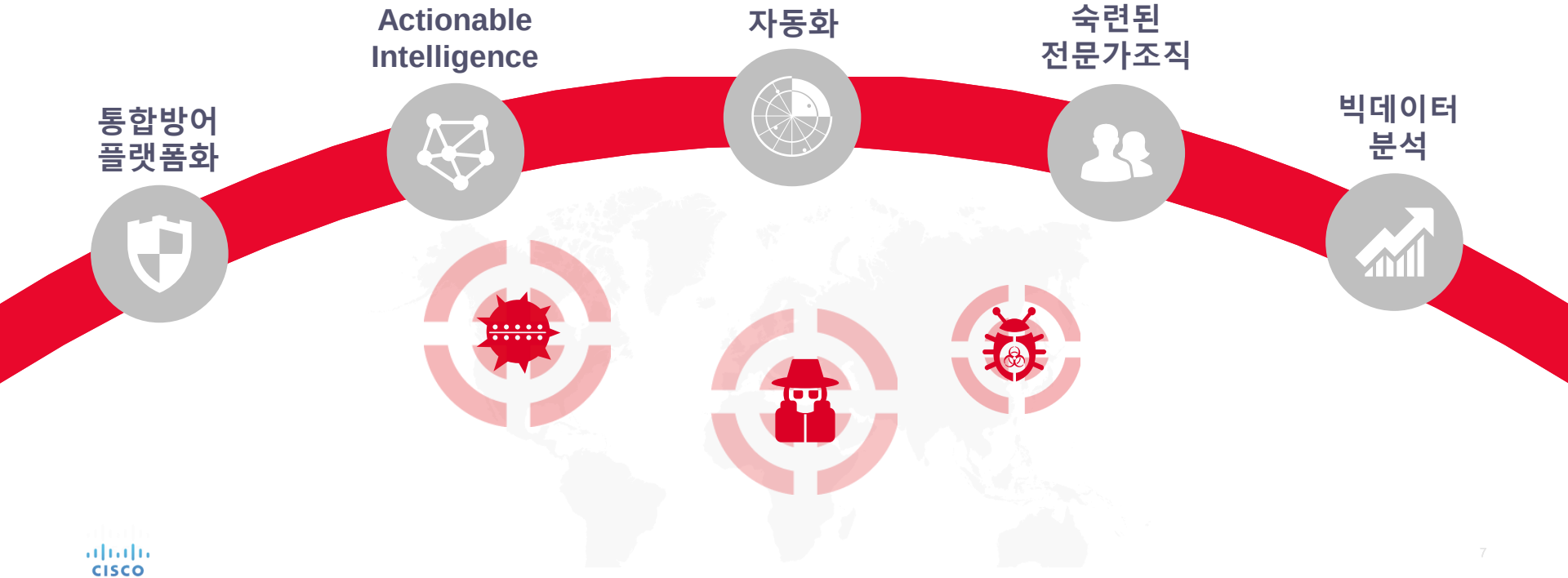
Threat Hunting

- 스트림기반 빅데이터 분석, 머신 및 딥러닝과 전문가 조직을 통한 잠재적 위협 색출

Pre-emptive Control

- 공격자들이 사용하는 인프라스트럭처 및 통신을 선제적으로 제압

Threat Hunting을 위한 고려 사항



통합방어
플랫폼화

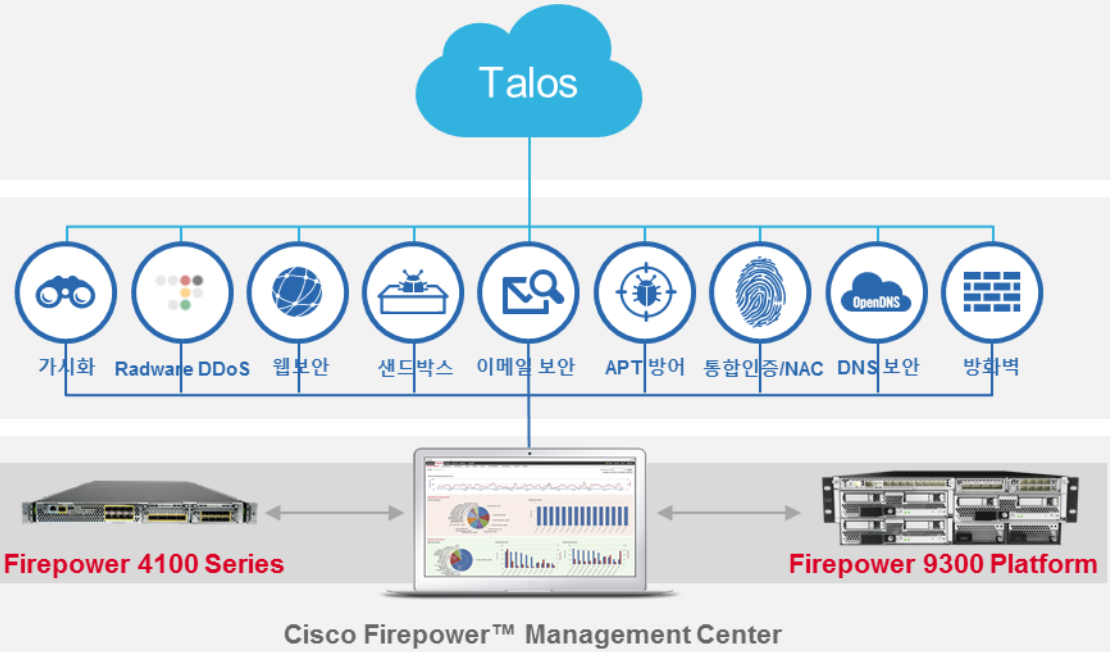
통합 방어를 통한 효과적인 협력 및 통제

시스코 차세대 통합 보안 플랫폼 Firepower 9300/4100

Shared Actionable Intelligence

Shared Contextual Awareness

Consistent Policy Enforcement



Actionable Intelligence

Actionable Intelligence

시스코 탈로스그룹에 의해 선별된 위협 인텔리전스의 적용

위협 인텔리전스

이메일 엔드포인트 웹 네트워크 IPS 디마이스

천 6백만
글로벌 센서

100 TB
하루 분석 데이터량

1억 5천만이상
단말을 통한 정보 수집

600명 이상
전문 엔지니어, 아키텍트 및 연구원

35%
전세계 이메일 분석량

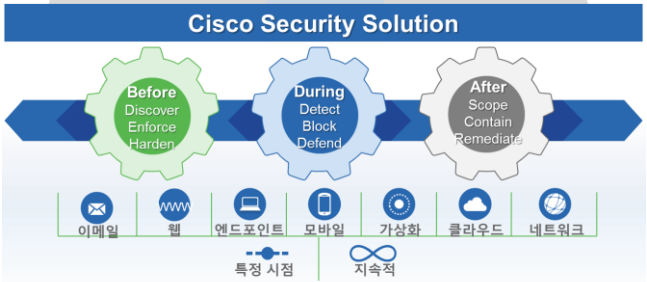
13 billion
웹접속 요청 스캔

24x7x365
상시 운영

40+
다양한 언어 정보

cisco

시스코® TALOS

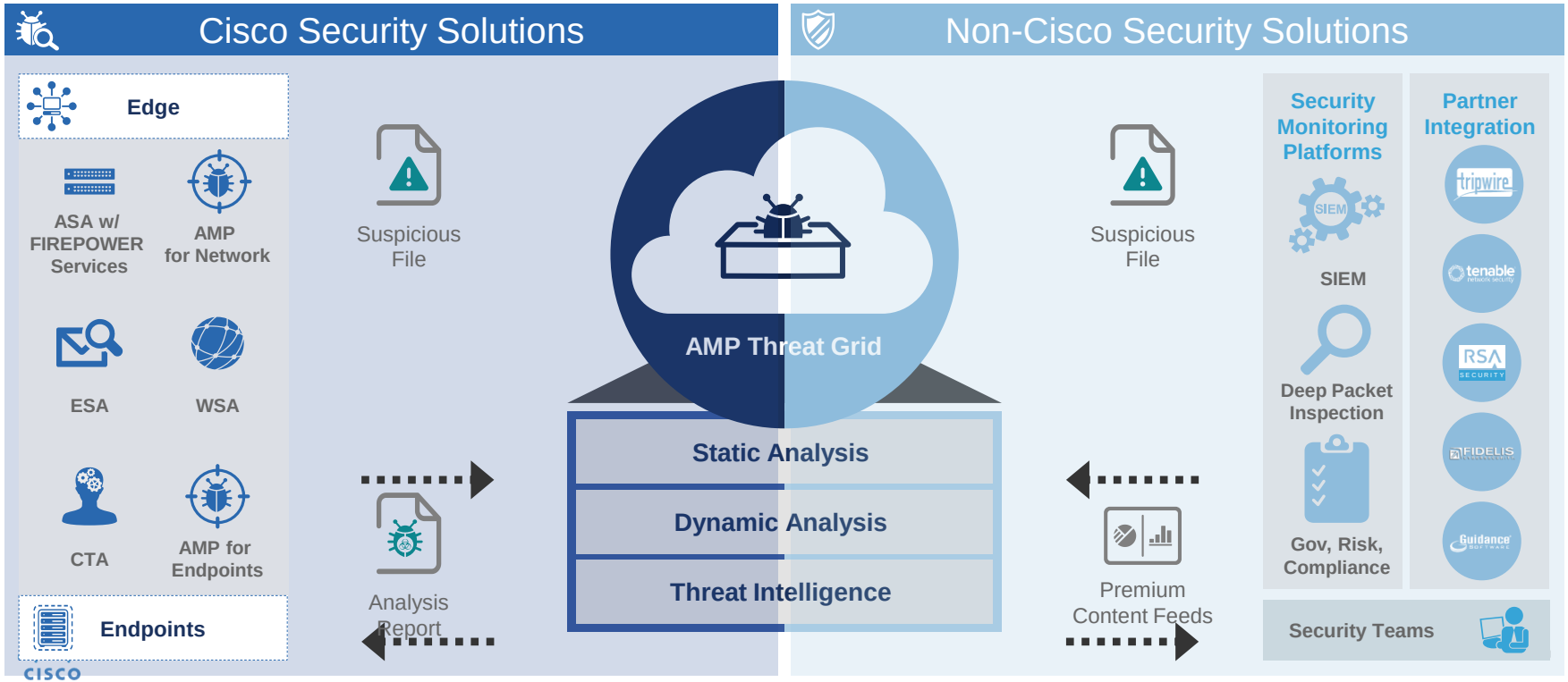


실제적 위협선별 및 대응방안연구

- AMP Threat Grid 클라우드의 월간 10M이사의 파일 분석 결과 러닝
- 상시 운영되는 허니팟을 통한 샘플 수집 및 분석
- AEGIS™ 프로그램을 통한 조정 및 전파
- 사설 및 공인 위협 정보 피드 반영
- 상시 다양한 취약점 및 익스플로잇 조사/분석
- Snort 및 ClamAV 오픈소스 커뮤니티를 통한 공유

엔드 투 엔드의 자동화된 분석 체계 적용

시스코 AMP Threat Grid Everywhere 전략



자동화

숙련된
전문가조직

不聞不若聞之, 聞之不若見之,

見之不若知之, 知之不若行之;

Cyber Range Service

A delivery platform to experience the intelligent Cyber Security for the real world

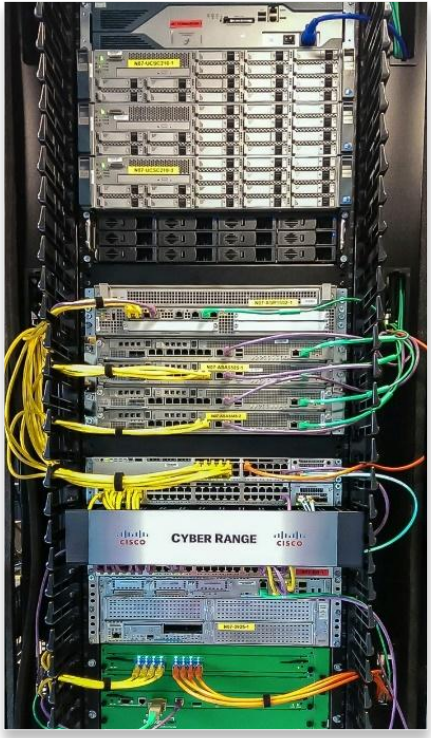
숙련된
전문가조직

숙련된 전문가 육성을 위한 실전학습

시스코 사이버레인지 서비스 및 딜리버리 플랫폼

플랫폼 및 서비스 효과

- Day 1 실제 침해 대응 훈련 환경 제공
- 선도적 관제 및 침해대응 기술, 보안 운영 및 절차에 대한 심도 깊은 실전 학습 효과
- 현재의 보안 이슈 및 익스플로잇에 대한 침해전 시뮬레이션 및 예방 학습 효과
- 현 운영 보안 인프라 및 도입 검토 중인 보안 인프라의 효과성에 대한 실전 검토



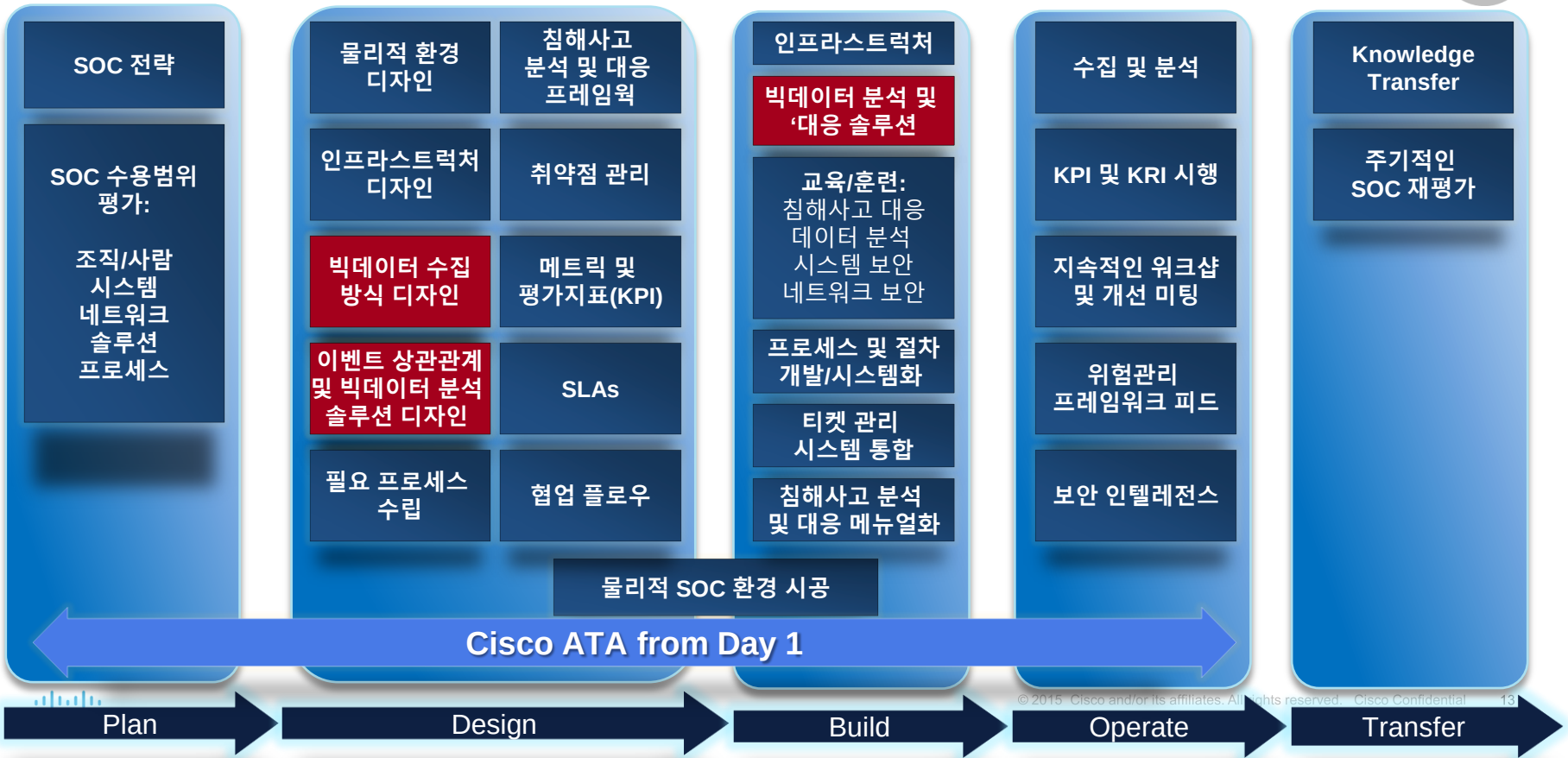
실전 학습 환경

- 12개 IT 기술 및 솔루션에 대한 60개 이상의 최신 공격 사례 재현
- 200– 500 개 이상의 다양한 악성코드를 100개 이상의 어플리케이션에 병합 재현
- 최신 보안 기술 및 솔루션 설치, 실제 보안 인프라 제공

PEOPLE PROCESS DATA THINGS

숙련된
전문가조직

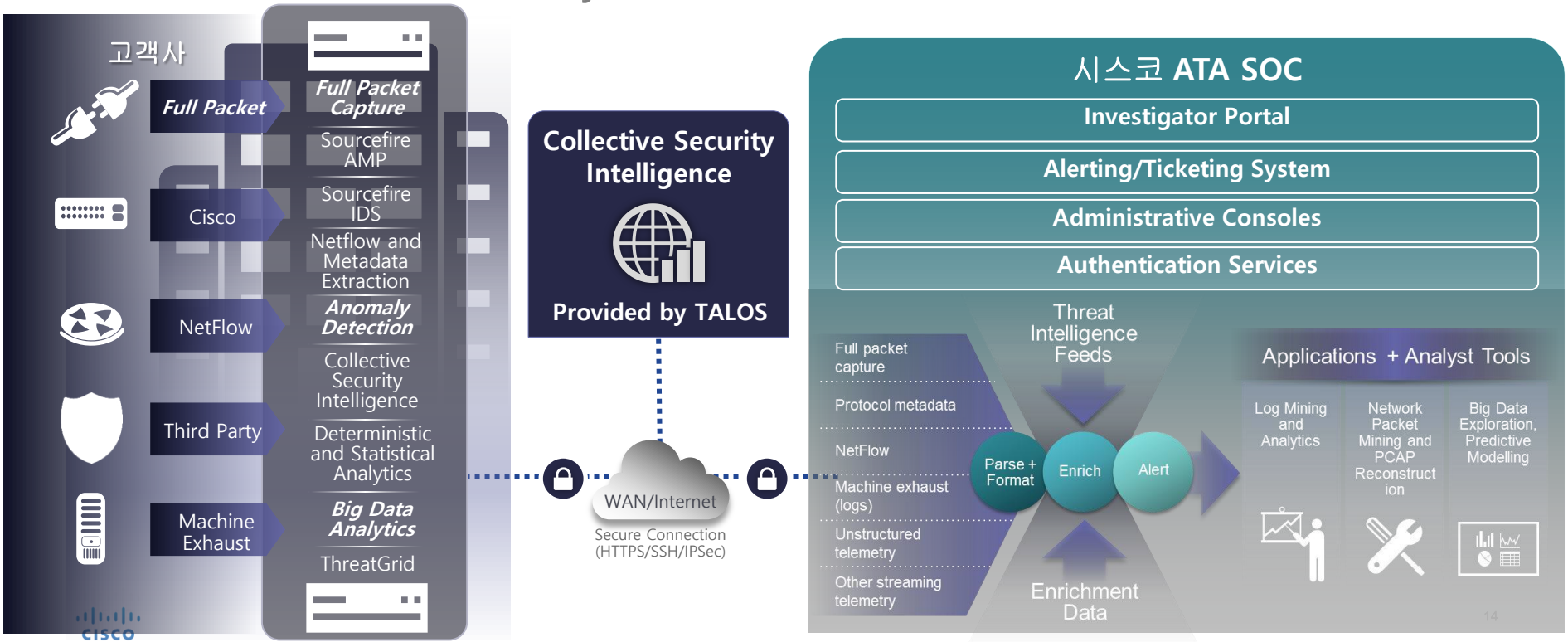
차세대 SOC 구축을 위한 단계적 어프로치



숙련된
전문가조직

전문가에 의한 Threat Hunting 서비스

시스코 Active Threat Analytic 관제 서비스

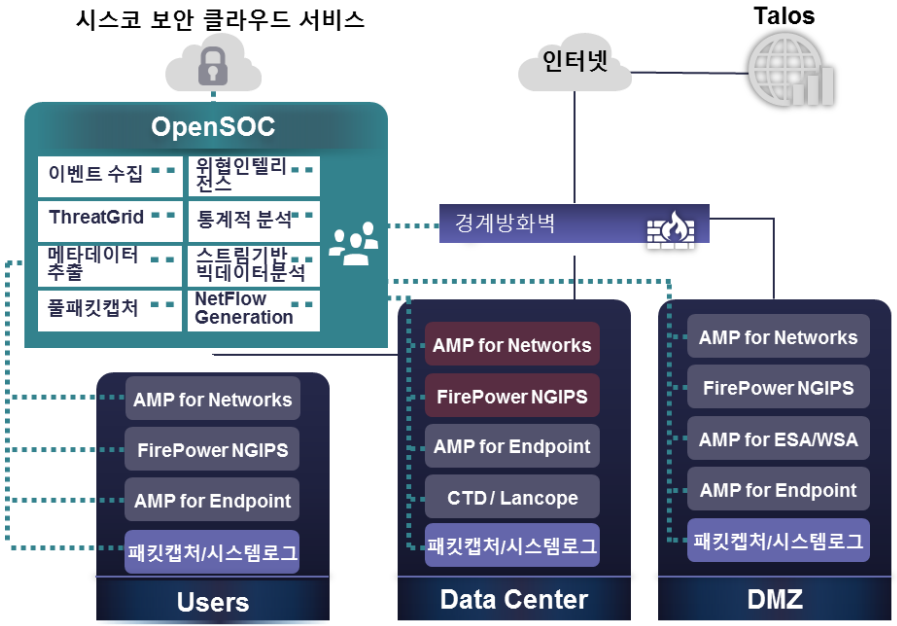


숙련된
전문가조직

전문가에 의한 Threat Hunting 서비스

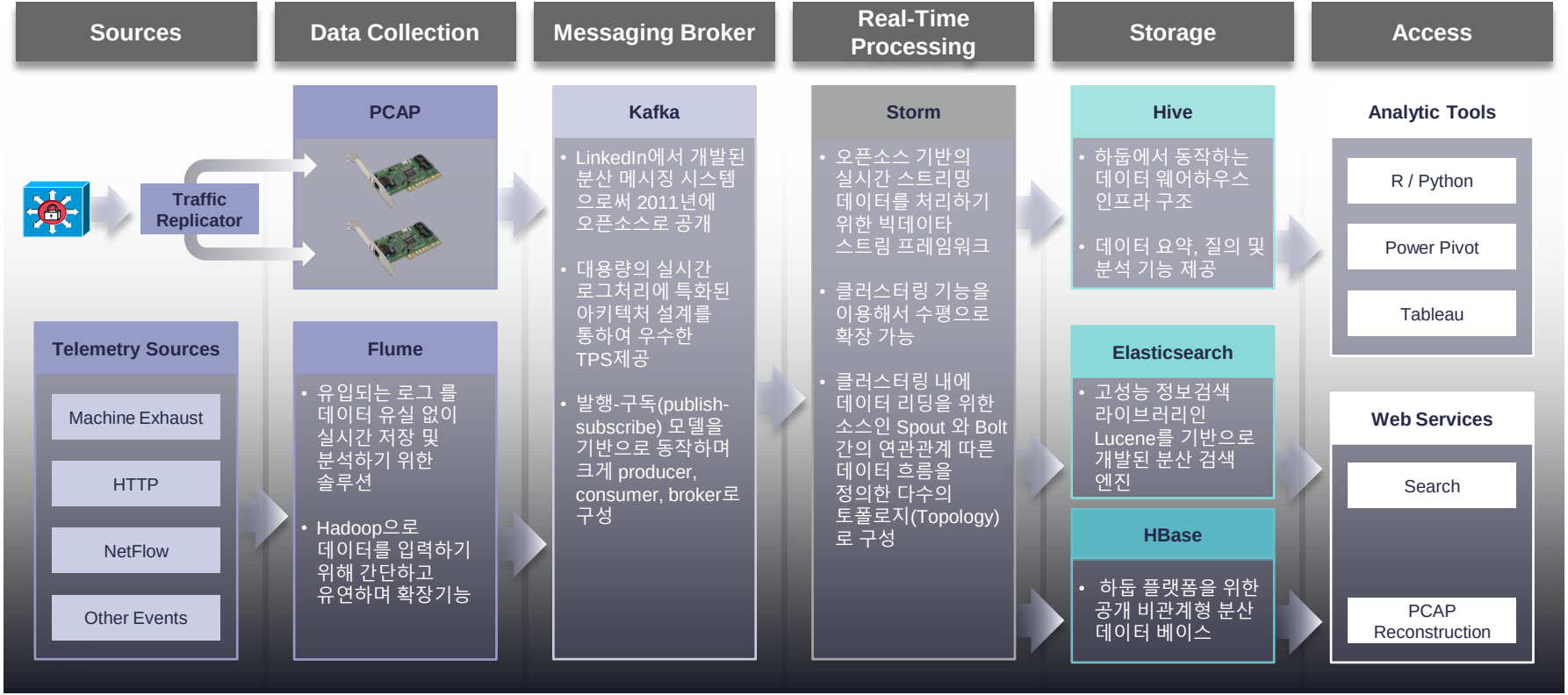
시스코 Active Threat Analytic 관제 서비스

- 다양한 보안 이벤트 경보에 대한 전문화된 분석적 대응
- 사고/사건화 되기 이전에 사전 위협 분석 및 감지, 대응체계화 ➔ Threat Hunting
- 하둡기반의 특화된 풀패킷 수집 플랫폼 구축
- 빅데이터 기반 분석 및 심층적인 포렌식의 전문가 서비스 제공



스트림 기반 빅데이터 분석 프레임웍

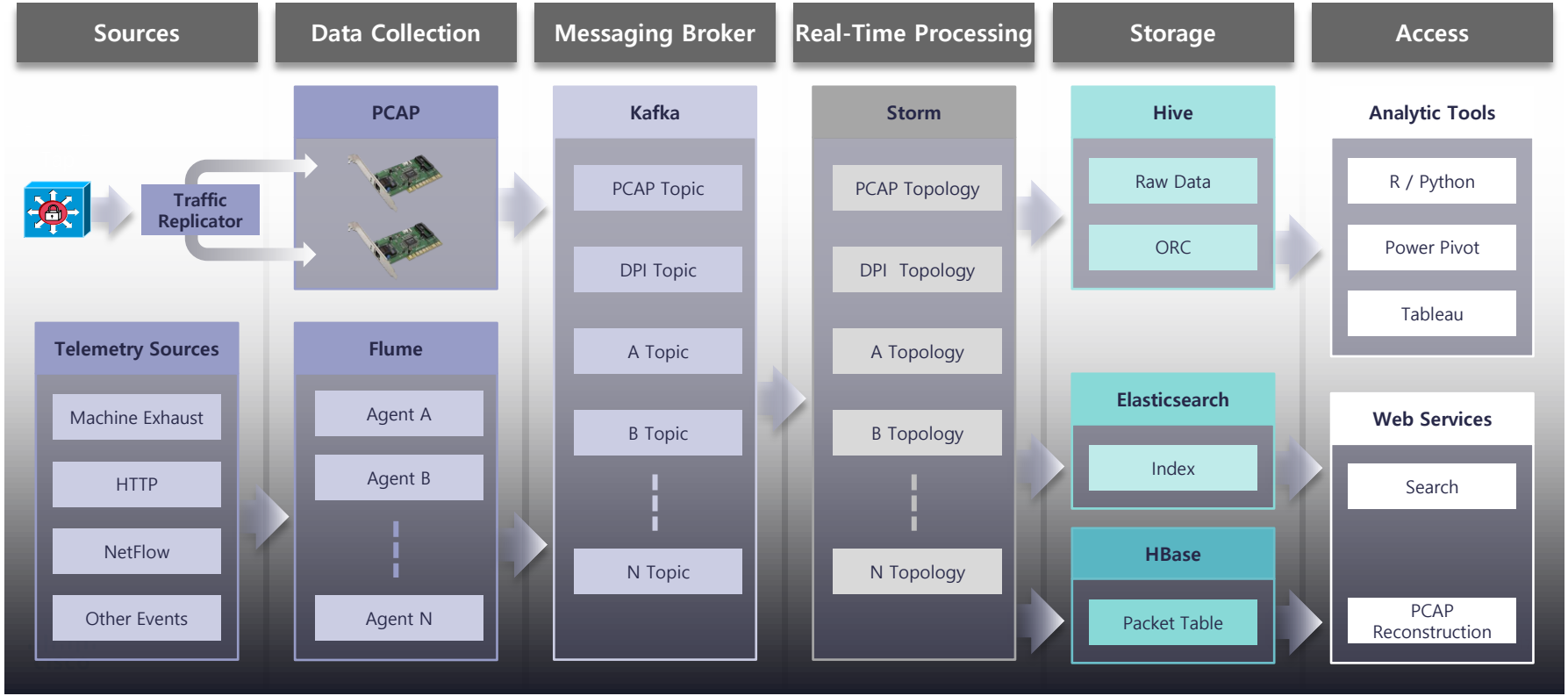
시스코 OpenSOC 프레임워크의 활용



빅데이터 분석

스트림 기반 빅데이터 분석 프레임웍

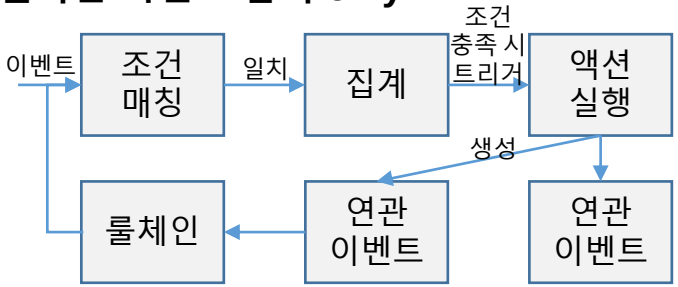
시스코 OpenSOC 프레임워크의 활용



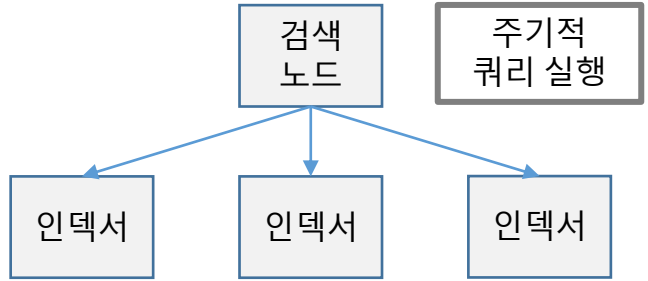
스트림 기반 빅데이터 분석의 차별성

기존 SIEM 아키텍처

1) 실시간 이벤트 탐지 only

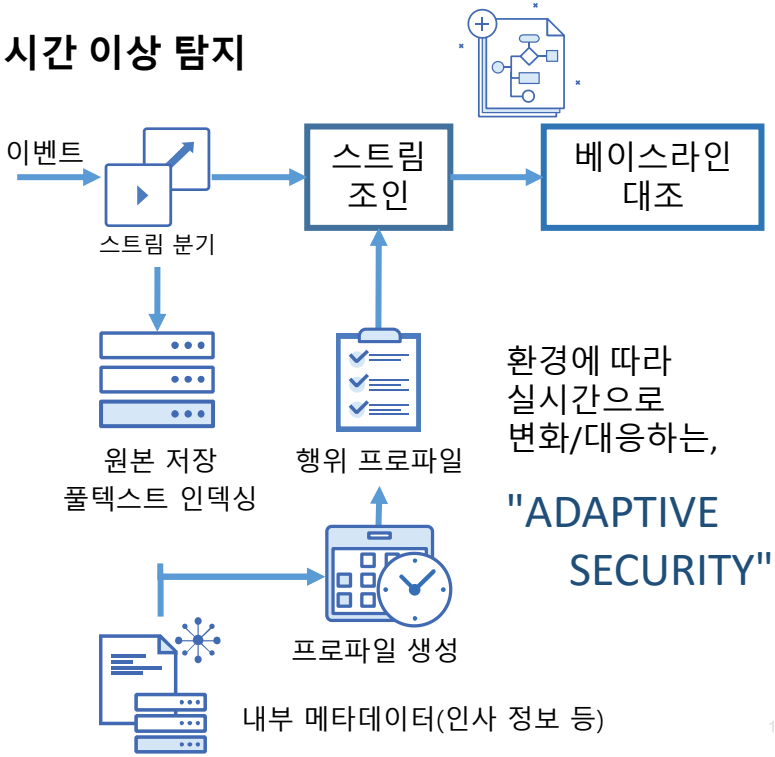


2) 배치 이상 탐지 ONLY

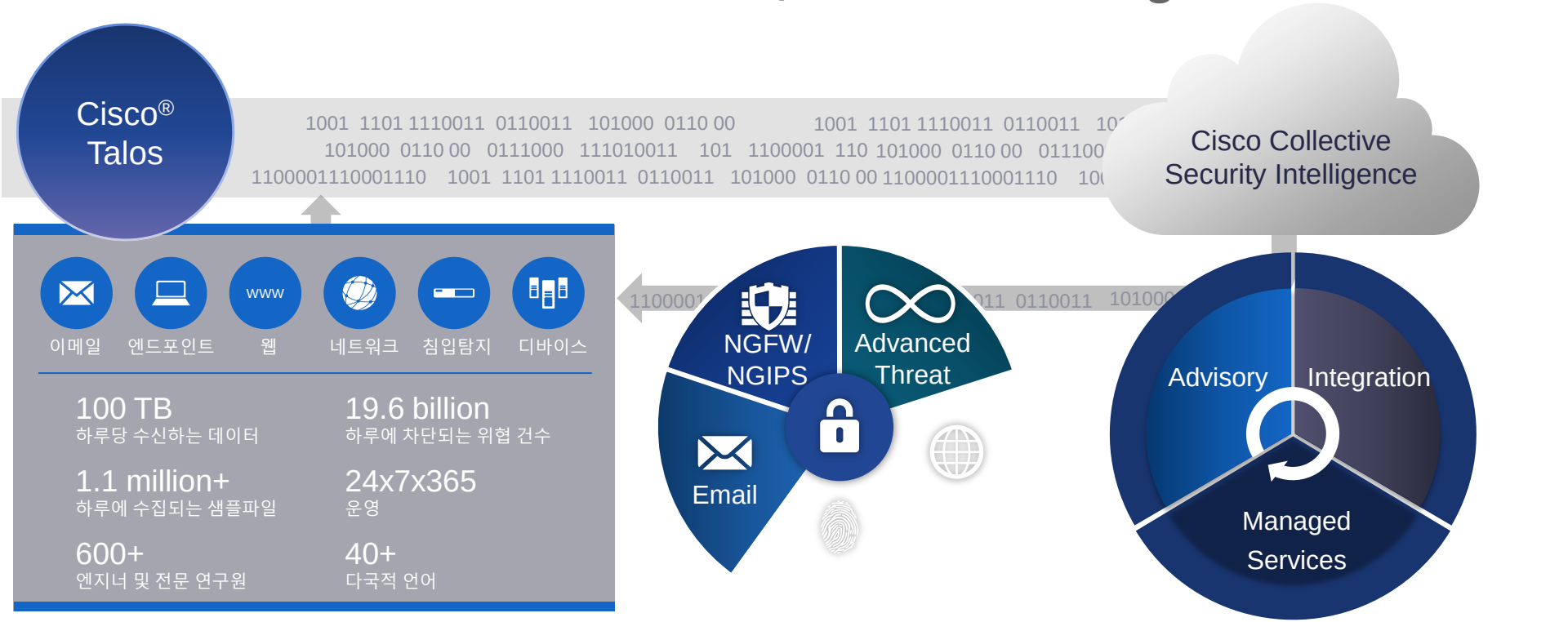


NG SIEM 아키텍처

실시간 이상 탐지



보안 모니터링 및 대응의 진화, Threat Hunting 위한 선택



Cisco Breadth, Collaboration and Methodology


CISCO