# 시스코 머신러닝 기반의 보안 관제 서비스

## - Cisco ATA(Active Threat Analytics)


시스코 시스템즈 코리아

컨설팅 사업부

장주수 수석부장(juschang@cisco.com)

# 사이버보안 현실

Sources:
- The Global State of Information Security Survey 2015 (PWC)
- Global Megratrends in Cybersecurity 2015 (Ponemon)
- Data Breach Investigations Report 2014 (Verizon)

## 비즈니스 모델의 변화

IoT

**25%**
IoT에 의한 사이버 공격 위험 증가

클라우드

**x5-10**
IT에 알려져 있는 않은 Shadow IT/ Shadow Cloud 서비스 이용

## 고도화되는 보안 위협

60% 데이터는 몇시간 만에 유출

54% 의 정보유출은 수개월 동안 눈치채지 못함

## 보안 기법의 복잡화 및 단편화

**12x** 보안 전문가의 필요성 증대

**45** 한 고객이 사용하고 있는 평균 보안 장비 제조사의 수

# 보안의 복잡성 증가

## SIEM과 분석관련 툴에 대한 투자


- 구축, 운영 및 유지보수 등의 복잡성
- 심층 분석 부족
- 보안 운영의 낮은 SIEM 이해도 및 분석의 어려움

## 보안 운영

- 24x7 SOC 운영 인력
- 보안 인력의 지속적 교육 및 훈련
- 보안 전문 인력 확보

## 보안 파트너/ 에코시스템

- 다양한 보안 솔루션의 통합 운영의 어려움
- 비즈니스와 기술의 접목

## 위협 인텔리전스

- 즉각적이고 적합한 보안 위협 인텔리전스의 확보의 어려움
- 상대적으로 높은 비용이 요구되는 신뢰도 높은 위협 인텔리전스 정보

# 보안 위협 조사에 소요되는 막대한 시간과 비용

**70,000 이벤트/주**
평균적인 보안 이벤트[1]

**395 시간/주**
False Positive 조사에 소요되는 시간[2]

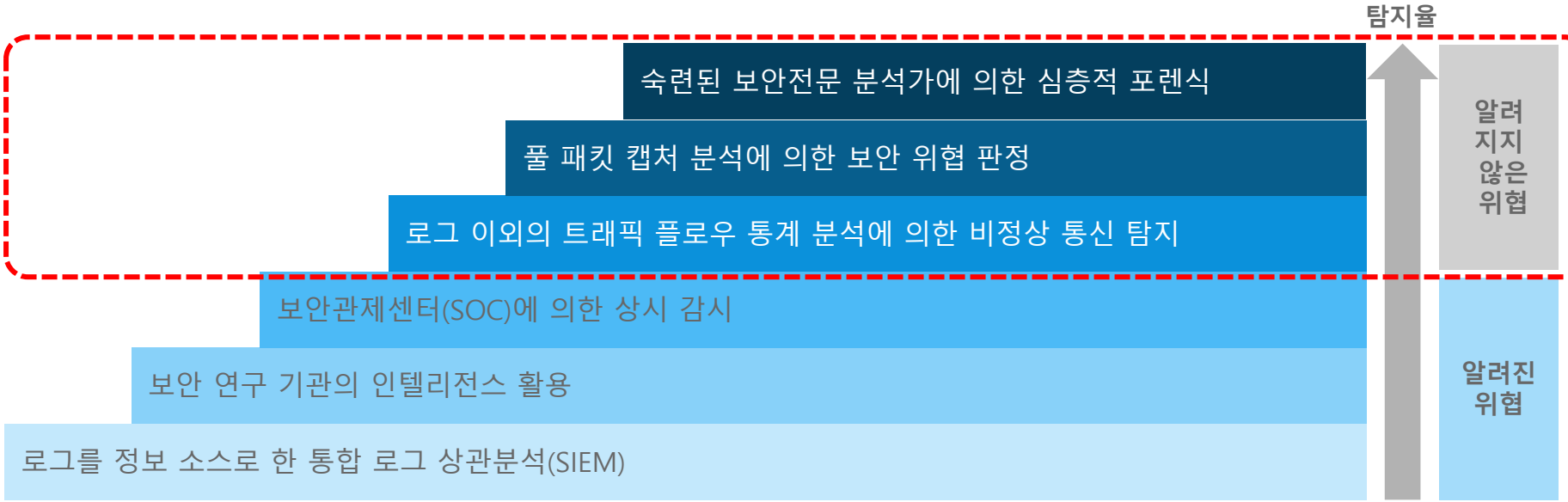
**$1.3M**
False Positive 조사에 소요되는 비용[2]

*Derived from Ponemon Institute Cost of Cyber Crime Study 2015

1. 2014 State of Infections Report. Damballa. May 2014. https://www.damballa.com/downloads/r_pubs/Damballa_Q114_State_of_Infections_Report.pdf
2. The Cost of Malware Containment. Ponemon Institute. January 2015. http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf

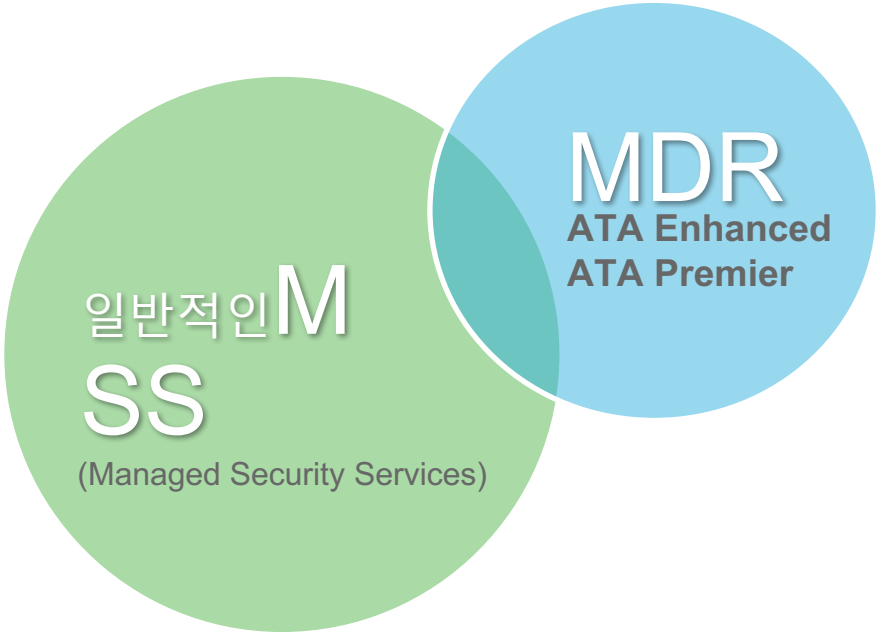
# 보안 위협 탐지 및 대응 수준의 확장 필요성

- 기존 통합 로그 상관 분석만으로는 불충분하며 로그만으로 찾아낼 수 없는 사이버 공격 징후를 구체적 증거자료를 기반으로 다면 분석 필요
- 로그 외 넷플로우/풀 패킷캡쳐/전문 보안툴 활용 극대화 및 숙련된 전문분석가의 심층 분석 필요
- 비정상적인 행위 및 통신 탐지 기술 적용 필요



# 머신러닝 기반의 새로운 보안관제 트렌드 : MDR

Gartner : Managed Detection and Response(MDR)



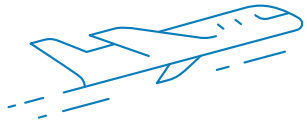

## MDR이란?

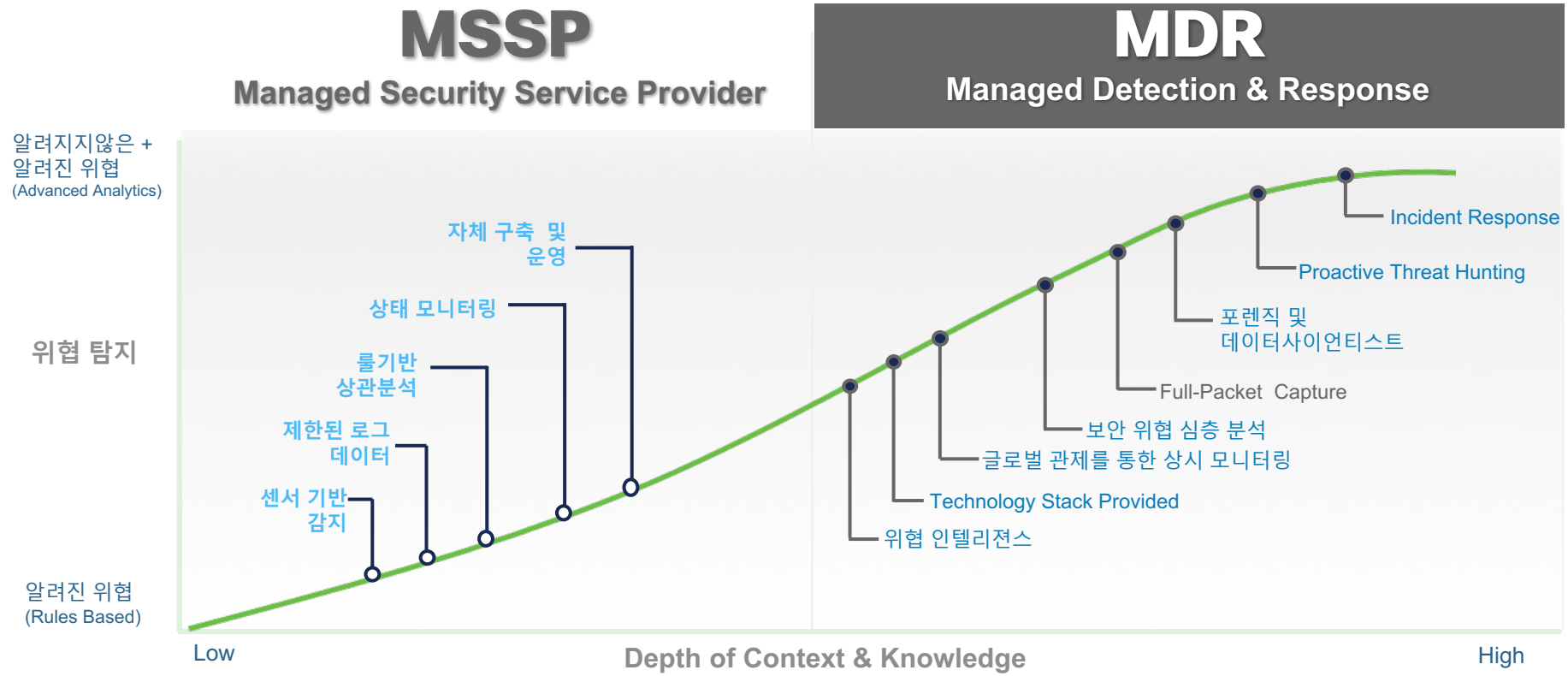
**위협 탐지 및 높은 수준의 사고 대응에 초점을 맞춘 새로운 보안 서비스 영역**

위협 인텔리전스, 선진적인 분석 기술, 빅데이터를 활용한 새로운 탐지 기술 등을 기반한 서비스

- **MDR 시장 전망 :**
  가트너(GARTNER)는
  2020년까지 **15%** 기업/조직에서 MDR 이용
  **50%** MSS사업자에서 MDR서비스 제공

# 보안관제 서비스의 진화





# MDR 서비스와 기존 MSS의 비교

## Managed Security Services

- **방화벽, IDS/IPS 위주의 보안 이벤트 원격 모니터링**
- **보안시스템 정책관리 및 업데이트**

- 서비스 사업자가 관리하는 인터넷 경계 장비의 모니터링에 초점을 둔 대응

- 제한된 Context 정보 수집
- 주요 이벤트에 대한 탐지 및 추정된 대응안 통보 서비스

## Managed Detection and Response

- **제로데이 위협에 대한 Monitoring 및 Investigation**
- **잠재된 내부 위협에 대한 Proactive Threat Hunting**

- 인터넷경계, 내부네트워크 및 주요 시스템 등 전반적인 IT 인프라에 대한 1차적인 모니터링 및 분석 자동화
- 전문가에 의한 심층 조사 및 대응

- 자동분석 및 요청에 대한 주요 사건 중심
- 주요 사건 조사를 위한 Full Context 활용
- 대응프로세스를 시스템화 전반적인 분석 및 대응 과정 자동 로깅 및 투명성 제공

**시스코 Active Threat Analytic 서비스**

# 시스코 보안 관제 서비스 : Active Threat Analytics

## 조직/사람

- 조직적인 운영
- 숙련된 전문가
- 고객사의 보안역량강화
- 고객사 보안 전문인력의 효율적인 운영 지원

## 인텔리전스

- 실제적 보안 인텔리전스 제공
- 광범위한 시스코 독자적 보안 인텔리전스 텔레메터리 활용
- 고객 전용 보안인텔리전스화
- 산업군별로 특화된 보안 인텔리전스 제공

Cisco ATA

## 기술

- 최신의 보안 기술 통합
- 유연성을 갖춘 모듈화된 아키텍처
- 새로운 요구의 수용 및 진화를 위한 확장형 플랫폼

## 분석

- 실시간성 분석
- 비정상 행위 탐지
- 제로데이 위협에 포커스
- 평균 대응시간 최소화

# 시스코 선별적 보안 인텔리전스 : 탈로스(Talos)

인텔리전스

시스코 탈로스

101 1110011 0110011 101000 0110 00 1001 1101 1110011 0110011 101000 0110 00
1000 0110 00 0111000 111010011 101 1100001 110 101000 0110 00 0111000
001110 1001 1101 1110011 0110011 101000 0110 00 1100001110001110 1001

Cisco Collective Security Intelligence

이메일 단말 웹서비스 네트워크 방화벽/IPS 시스템

**1.6M**
글로벌 센서

**100TB**
일간 수집 데이터량

**150M+**
엔드포인트

**300+**
엔지니어, 분석가, 조사관

**35%**
전세계 이메일 트래픽

**13B**
웹 리퀘스트

**24x7x365**
운영

**40+**
언어

180,000+ 일간 파일 샘플 분석
FireAMP Community

Advanced Microsoft
and Industry Disclosures

Snort 및 ClamAV 오픈소스
커뮤니티

허니팟

AEGIS 프로그램

자체 및 공용 위협 피드

동적 분석

# ATA 플로우 프레임워크

기술

- 풀 패킷 캡처
- 프로토콜 메타데이터
- 어플리케이션/솔루션 로그
- 머신 이벤트 및 로그
- 불특정 텔레메트리
- 기타 스트리밍 텔레메트리

위협
인텔리전스
피드

분석
+
정형화

집적화

경보

데이터 집적

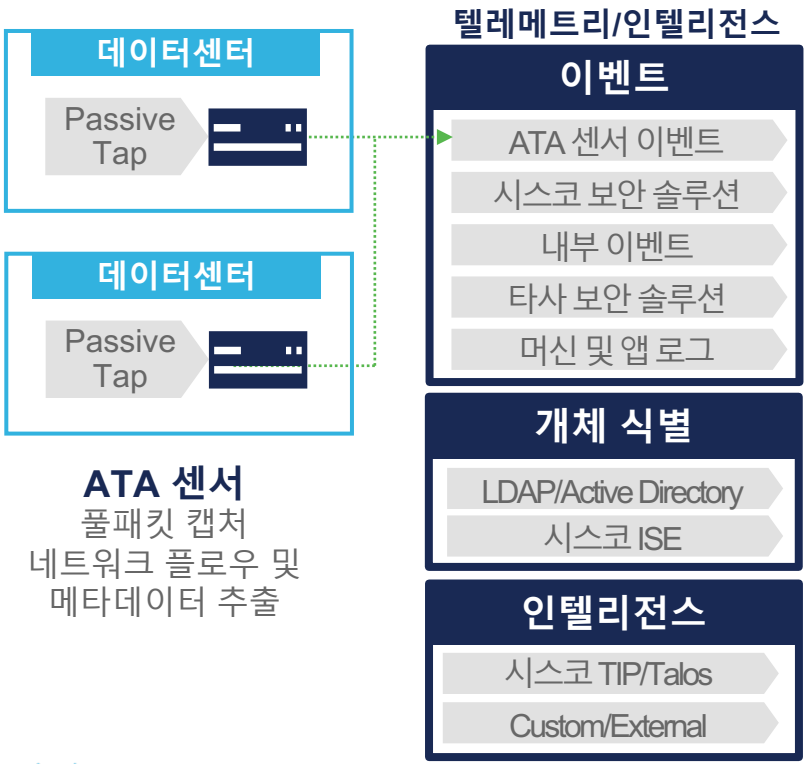
## 어플리케이션 + 분석 도구 + 전문가

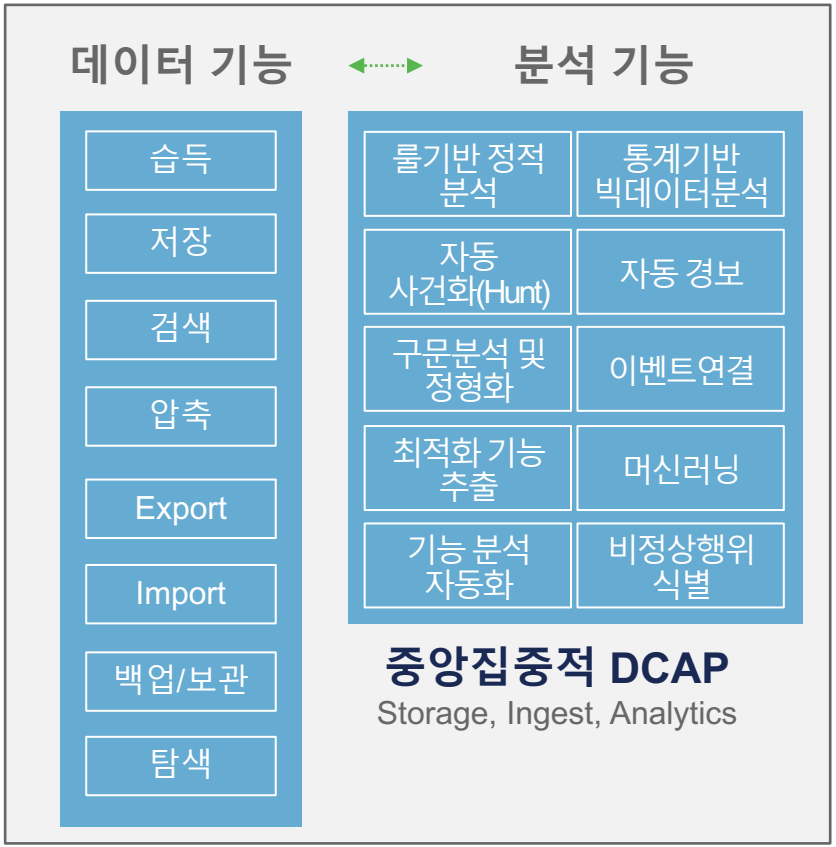
| 로그 마이닝과 분석 | 네트워크 패킷 마이닝 과 PCAP 재건 | 빅데이터 분석 및 탐색, 예측모델링 |
|---|---|---|

# 머신러닝기반 빅데이터 분석플랫폼 : DCAP

기술

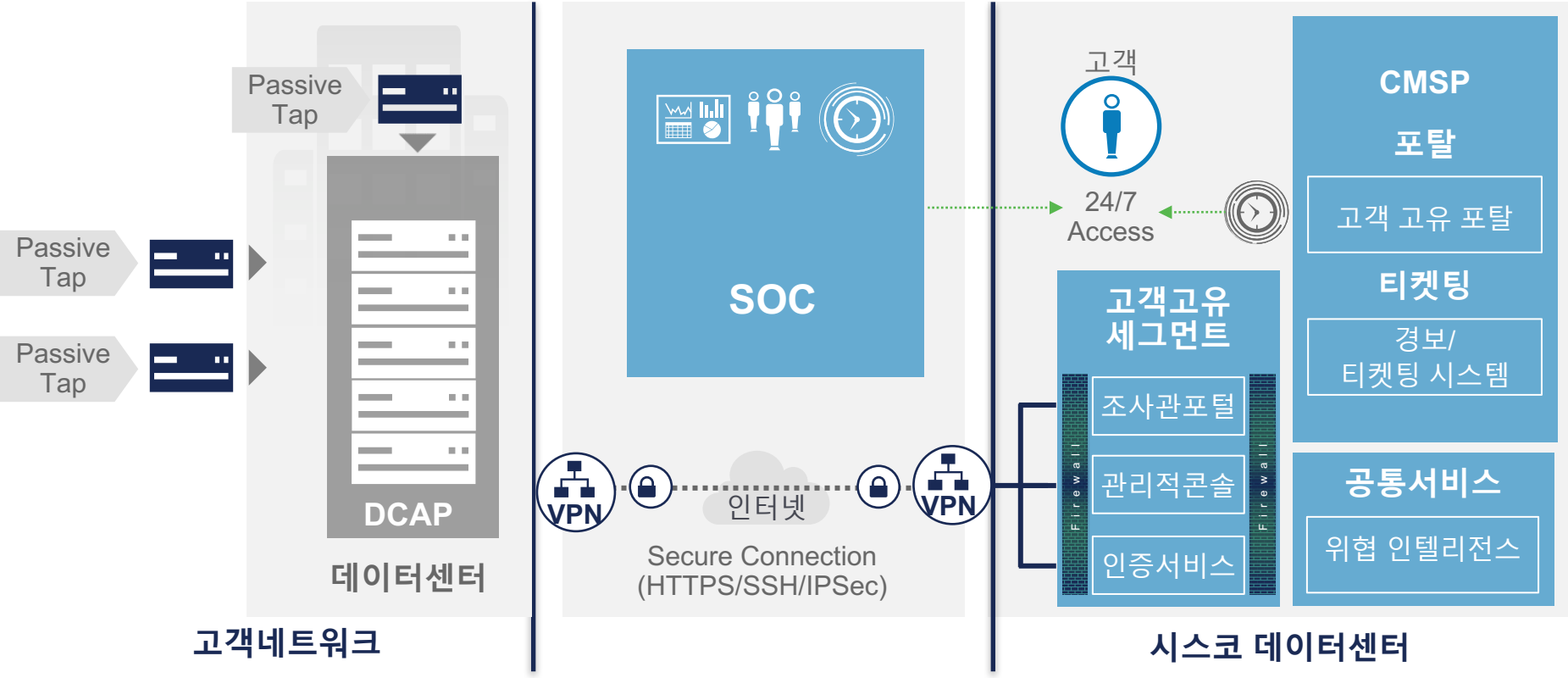
- **DCAP** : **D**ata **C**ollection and **A**nalysis **P**latform



# ATA SOC 구성

기술



# ATA 위협 탐지 및 인시던트 분석

분석

## ATA DCAP 분석 엔진(자동 분석)

| 분석엔진 | 분석 방법 |
|---|---|
| 확정적 룰기반 분석 (DRB) | • 시그니처, 임계치, 알려진 C2 도메인 및 IP 에 대한 탐지<br>• 알려진 위협에 대한 빠른 분석<br>• 지속적인 업데이트 및 관리/튜닝 |
| 통계적 룰기반 분석 (SRB) | • 데이터유출, 관리자의 비정상로그인등, 비정상적 행위에 대한 분석<br>• 지속적인 학습에 의한 임계치 동적 조정<br>• 환경변수등을 고려한 통계적모델 |
| 데이터 과학 중심 분석(DSC) | • 데이터, 자산 등의 자동화된 분류와 함께 종합분석된 위험모델링 적용<br>• 발생된 이벤트로 부터의 학습 및 자동화된 튜닝<br>• 머신러닝 기반의 빅데이터 분석기법 적용 |

## ATA SOC 요원(인적분석 )

| 요원 | 분석 방법 |
|---|---|
| 애널리스트 (1차 분석) | • 이벤트 모니터링 및 인시던트 발생 시, 1차 특정화<br>• 로그와 패킷의 상관 분석을 통한 오탐 경감<br>• 비정상 행위 및 플로우로 알려지지 않은 위협을 탐지 |
| 인베스티게이터 (2차 분석) | • 감염 단말, 피해 상황을 특정<br>• 원인, 침입 경로, 정보 유출의 유무, 추천 대응책 검토 및 보고<br>• 알려지지 않은 위협을 탐지하기 위한 Hunting용 스크립트 작성<br>• 대응 후, 방어력을 향상시키기 위한 탐지 룰을 조율 |
| 데이터 사이언티스트 | • 통계 분석/빅데이터 분석 룰 수립 및 최적화 |

- 오탐/불필요 이벤트 경감
- 알려지지 않은 위협 탐지
- 정확한 분석 결과 보고
- 인시던트 대응 차단 범위 최소화

# 네트워크 데이터 기반 분석 중요성

분석

**보안 장비**

- 미리 정의된 규칙/룰 기반 차단
- 탐지 규칙/룰 우회 공격 대응 불가

**로그 분석/SIEM**

- 특정 지점/시스템 기반 탐지 공격 정보 확보만 가능
- 공격 전체 가시성 확보 불가

## 네트워크 포렌식 분석

❖네트워크의 모든 데이터의 저장 및 분석

❖다양한 데이터와 연관 분석

- 지능화/표적형 공격 대응
- 침해흔적/공격 추적 조사
- 공격 전반 내용 파악
- 공격 대응 명확한 증적 확보
- 정확한 대응 방안 제시

**전체 패킷 데이터 (Full Packet)**

- 모든 전송 패킷 수집
- 포렌식 분석 용도
- 분석 및 데이터 추출

**세션데이터 (Netflow)**

- 출발/목적지 IP, 포트번호, 프로토콜종류, 전송패킷/바이트수 정보
- 이상징후 탐지

**추출데이터**

- 네트워크 기반 전송 파일/파일 해시값 추출
- 가상머신 동적 분석
- 악성 코드 탐지 등

# Full Packet Capture

분석

- 캡처된 패킷상의 메타데이터 수집 및 머신러닝 기반의 비정상 행위 도출 자동화
- 비정상적 행위 및 알려지지 않은 위협 행위 등에 대해 캡처된 패킷을 활용 Replay 등 수행
- 공격 징후에 대한 추정성 보고가 아닌 확정적 증적 기반의 능동적 대응

## 기존 통합로그 수집 및 분석

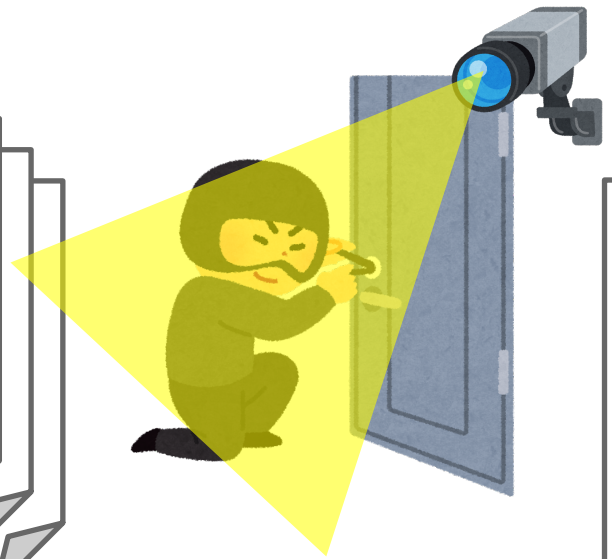
- 각종 장비로부터 받는 로그만 분석

## Full Packet Capture

- 설제 네트워크상의 모든 통신데이터 분석

***보고***
2017.11.11 20:30에
문 앞에 사람이 계속 머물렀던 것 같습니다.

***대응***
문제가 없는지 확인해 보세요
-이상-



***보고***
2017.11.11 20:30에 현재
도둑이 문을 열려고 합니다.

***대응***
문앞으로 경비를 보내
당장 잡으세요
-이상-

# 사이버킬체인 대응 차별점

분석

## 표적형 공격의 킬 체인


## 로그로만 분석


## 로그와 패킷의 통계 분석

# Proactive Threat Hunting

분석

- 진화하는 위협의 수동적 감시 외, 능동적 위협 감지의 Proactive Threat Hunting 실시
- 수집된 데이터 활용한 서비스 이용률, 프로토콜 등 다양한 관점의 분석
- 비정상 통신 발생 여부나 외부 발생 보안위협의 감염 로그나 트래픽을 상세 지속적 분석 및 조사

## 고객 환경 트래픽 분석

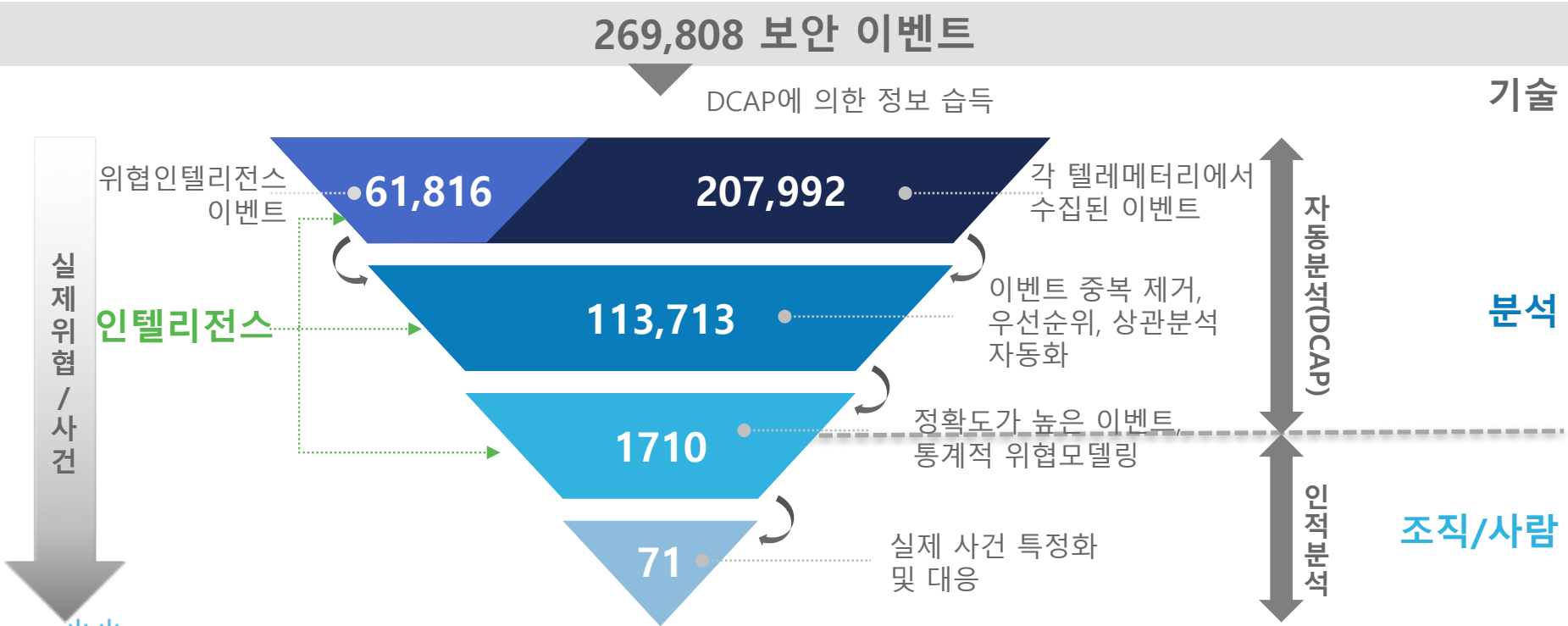
- ATA DCAP의 수집된 고객 풀 패킷 데이터 분석
- 하기 특성의 잠재적 비정상 통신의 능동적 조사
  - 각 프로토콜별 이용률
  - 서버 상에서 제공되어 있는 각 서비스의 이용률
  - 클라이언트 PC의 요청 서비스 이용률
  - 서버 및 클라이언트PC의 트래픽(패킷수/바이트수)
  - 통신 시설(국가나 조직)의 통계
  - HTTP나 DNS에 의한 수상한 도메인과의 통신 상황
  - Email에 의한 수상한(알 수 없는) 첨부 파일

## 외부 발생 이벤트의 내부 감염 여부 감시

- 로그 및 트래픽 분석 기반 외부 발생한 영향력 큰 위협의 고객사 영향 발생 유무 등 조사
- 사전 대책(Signature 업데이트 등) 필요시 대응책 제시
  - 예1 : HeartBleed의 OpenSSL 취약성 검색 활동 수신 상황
  - 예2 : 외부의 확인된 알려지지 않은 Malware 침 여부 확인 등

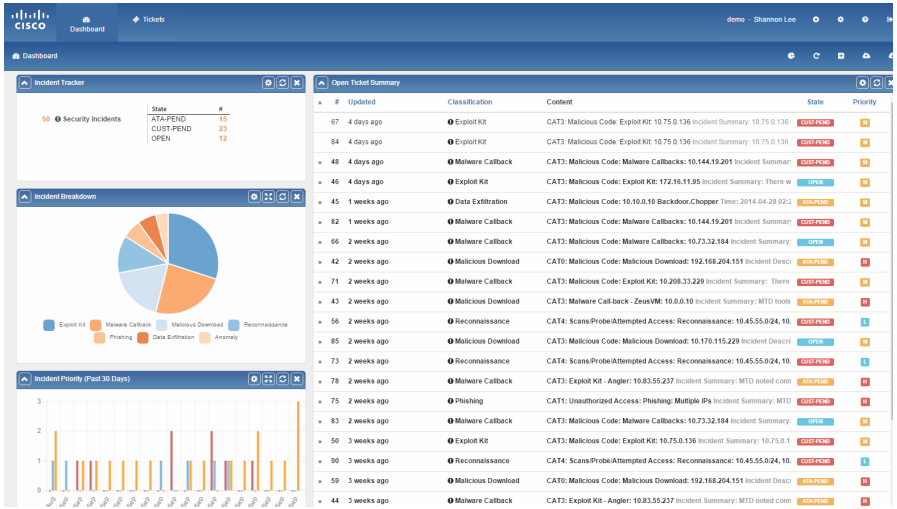
# ATA 위협 탐지 및 인시던트 최적화 고객 사례

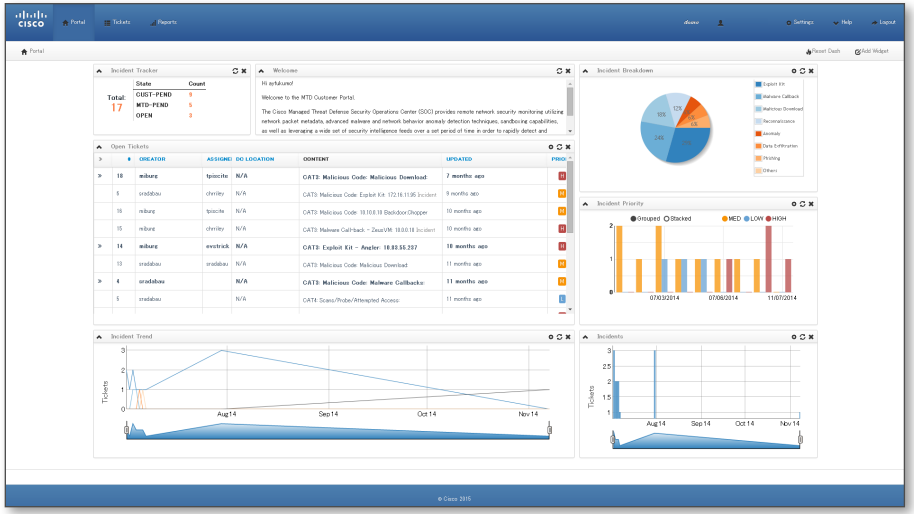
## ATA Premier Service 사용 고객의 2주간 실제 데이터 분석사례



# ATA 커스터머 포털(Customer Portal)

- 티켓 ID번호
- 티켓 오픈 일시
- 티켓 개요
- 인시던트의 요인
- 티켓에 관한 상황, 상세 정보



# ATA 보고서

## 인시던트 발생시 보고 내용

| 항목 | | 게시 정보 |
|---|---|---|
| 인시던트 정보 | | • 감염 단말의 IP주소<br>• 접속한 곳의 IP주소 및 포트 번호 |
| 애널리스트 분석 결과 | | • 인시던트의 개요 설명<br>( 비정상 침입, 악성 코드, 공격 상황 ) |
| 추천 대응 | | • 대응 내용<br>• 감염 단말 IP주소 정보<br>• 차단 URL, IP주소, 파일 해시값(Hash value) |
| 공격 상황 | 비정상 침입 | • 메일 송/수신자의 주소<br>• 접속한 곳의 URL<br>• 비정상으로 침입한 단말의 IP주소 |
| | 악성 코드 다운로드 | • 악성 코드의 명칭, 해시값<br>• 악성 코드의 다운로드 유무<br>• 다운로드한 단말의 IP주소 |
| | 콜 백 (Call back) | • 콜 백 통신의 시도, 성공 유무<br>• 콜 백 통신한 단말의 IP주소 |
| | 정보 유출 | • 정보 유출의 시도, 성공 유무<br>• 정보 유출 단말의 IP주소<br>• 정보 유출 파일 정보, 해시값 |

## 보고서 샘플

**Incident Summary:** YYYY-MM-DD HH:MM:SS UTC에 Nemucod라고 식별된 악성 ZIP파일이 첨부된 전자 메일을 감지했습니다.
**Time:** YYYY-MM-DD HH:MM:SS UTC
**Source IP:** 203.0.113.1、**Source Ports:** Ephemeral / tcp
**Destination IP:** 198.51.100.1、**Destination Port:** 25 / tcp
**Location:** ○○데이터 센터
**Indicators of Compromise:**
악성 파일이 첨부된 피싱 메일
파일명: aaaaa.zip, 파일 사이즈: X.X KB
SHA256 Hash 해시값: abc123xyzabc123xyzabc123xyzabc123xyzabc123xyzabc123xyzabc123xyzabc123xyz
**Incident Analysis:**
YYYY-MM-DD HH:MM:SS UTC에 Nemucod라고 식별된 악성 ZIP파일이 첨부된 전자 메일을 감지했습니다.
이 Nemucod의 아종(Subspecies)은 실행 시에 Teslacrypt를 다운로드합니다. 이 메일에 근거한 총 8개의 커넥션이 회선 상에서 확인되었습니다. 다양한 발신자와 메일명이 사용되었지만, 첨부파일의 제목과 내용은 동일한 것이었습니다.
**귀사의 환경에서 관측한 정보:**
**전자 메일의 상세 정보:**
Subject: test mail、Recipient: admin[@]example.co.jp、Senders: test[@]abc.example
첨부 파일(파일명/SHA256해시값/파일 크기):
aaaaa.zip / abc123xyzabc123xyzabc123xyzabc123xyzabc123xyzabc123xyzabc123xyz / X.X KB
**추가 조사에 의한 정보:**
ZIP파일의 내용물: bbbbbbbbbb.js
SHA256해시값: 456def789456def789456def789456def789456def789456def789456def789
TeslaCrypt를 다운로드한 곳: hxxp://example[.]invalid/system/logs/ccccccccc.exe (198.51.100[.]1)
TeslaCrypt를 콜 아웃 통신한 곳: hxxp://198.51.100[.]2/main.php
조사 시에 감염과 합치되는 콜 아웃은 감지되지 않았습니다.
**Next Steps:**
메일 서버를 조사하고 이들 전자 메일이 차단되었는지 여부, 혹은 첨부파일이 삭제되었는지의 여부를 확인하는 것을 추천합니다. 만일 전자 메일이 사용자의 메일상자로 송신된 첨부파일을 연 경우, 네트워크를 통해 감염이 확대되는 위험을 최소한으로 하기 위해 이 시스템을 복원하는 것을 추천합니다. 인시던트 리스펀스(Incident Response)의 프로세스를 시작하여, 시스템의 악성코드 스캔, 로그 확인, 악성코드 감염이 확인된 경우에는 시스템을 초기화하는 것을 추천합니다.
**Mitigation Actions:**

-하기의 도메인과 IP주소를 차단하는 것을 검토해 주십시오.
example[.]invalid/ (198.51.100[.]1)
198.51.100[.]2

-하기의 해시값을 가진 파일을 차단하는 것을 검토해 주십시오.
abc123xyzabc123xyzabc123xyzabc123xyzabc123xyzabc123xyzabc123xyz
456def789456def789456def789456def789456def789456def789456def789

# ATA 서비스 종류 및 제공 내용

## Enhanced

+통계적 이상 분석
+ NetFlow정보 분석
+ 프로토콜 메타데이터 추출
+ 데이터의 보강 (Data Enrichment )

Speed
Accuracy
Focus

## Premier

+ 머신러닝, 빅데이터 분석
+ 풀 패킷 캡처 기능
+ Proactive Threat Hunting (원인 특정)

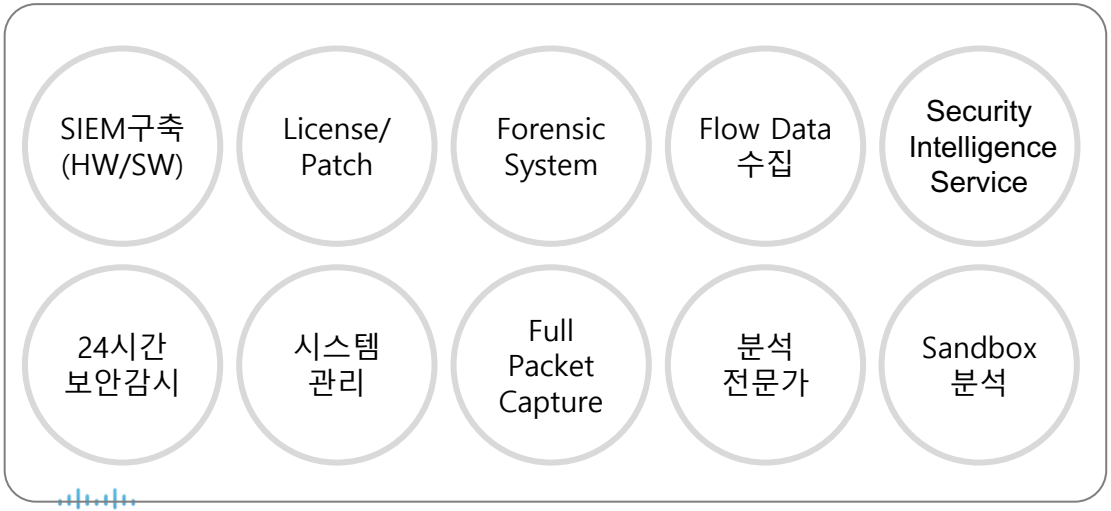
Speed
Accuracy
Focus

| 서비스 | | Enhanced | Premier |
|---|---|---|---|
| 서비스 | 24시간 시스템으로 감시/분석 | ✔ | ✔ |
| | 원인 특정, 대책 제시 | ✔ | ✔ |
| | 분석 장치 관리 서비스 | ✔ | ✔ |
| | 고객 문의 대응 | ✔ | ✔ |
| | 정기 보고 | **분기별** | **매월** |
| | 고객 포털 | ✔ | ✔ |
| | Proactive Threat Hunting (비정상 통신의 능동적인 조사) | | ✔ |
| 감시 대상 | 시스코 장비 로그(Syslog) | ✔ | ✔ |
| | 3rd Party 장비 로그 (Syslog) | ✔ | ✔ |
| | Netflow | ✔ | ✔ |
| | 풀 패킷 | | ✔ |
| 분석 방법 | 룰 기반 해석(인텔리전스) | ✔ | ✔ |
| | 통계 분석(Netflow) | ✔ | ✔ |
| | 빅 데이터 분석(풀 패킷) | | ✔ |

# Why Cisco ATA?

## 자체 구축 대비 ATA의 효율적 투자, 그리고 단계적 내재화를 통한 효율적 관리

- 자체 운용 시  각 보안 장비 유지 보수 (최신 보안 패치, 시그니처 업데이트, 검증 작업 등의 변경 관리) 비용
- 인재 고용, 전문가 확보, 교육 비용 발생
- 조직 설립에 소요되는 기간(통상 2~3년)이 필요
- 보안 인텔리전스의 독자 취득 및 ATA의 분석 방법, 능력(노하우)




VS

**ATA**

(People/Technology/ Intelligence/Analytics)