보안, 프레임워크 그리고 머신러닝

스플렁크 총판 SCK
박용 Splunk Consultant
andy.park@sckcorp.co.kr

splunk> turn data into doing™

Agenda

1. 보안 운영(SecOps)
2. 보안 프레임워크
3. AISecOps 적용하기
4. Splunk 보안 포트폴리오

보안 운영(SecOps)

splunk> turn data into doing™

보안 운영 워크플로우

로깅, 모니터링, 탐지, 대응, 자동화, AI까지 필요

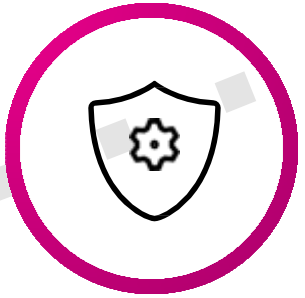
보안/비보안 솔루션 로깅/모니터링

로그/패킷 데이터 수집

인시던트 탐지/분석

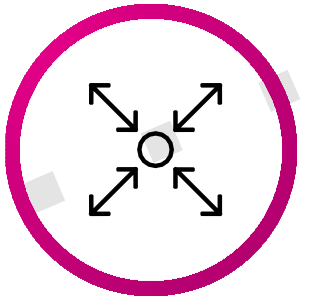
임계치 분석/아노말리 분석(통계)/머신러닝 시나리오를 이용한 이상징후 탐지

대응/복구



선제적 분석을 통한 보안 이상징후 대응

AISecOps



머신러닝을 이용한 자율적 탐지/ 자동화된 대응 및 복구

선제적

보안 성숙도

반응적

splunk> turn data into doing

보안 운영 워크플로우

다양한 데이터 소스부터 복잡한 탐지 운영 절차

운영(Operation)

Tier 1
보안 분석

- 피싱 조사
- 위협 인텔리전스(TI)
- 이벤트 분류

Tier 2
위협 대응

- 위협 헌팅
- 멀웨어 조사
- 내부자 위협 조사

Tier 3
위협 대응

관리(Management)

SOC Director

CISO

- 팀 운영 성능
- 프로세스 & 운영
- 메트릭 & 리포팅

splunk> turn data into doing

보안 운영 워크플로우

많은 보안 경험 요구 – 하드웨어 스킬 & 소프트웨어 스킬

Tier 1

Tier 2

Tier 3

- 보안 지식
- 네트워크 & 장비
- 응용 계층 프로토콜
- DB & 질의어
- OS(윈도우즈, 리눅스, 유닉스)
- 기본적인 파싱
- 커맨드 라인 친숙성
- 보안 모니터링 툴
- 보안 프레임워크
- 보안 위협 연구

- 코딩/스크리팅
- 규정 준수(컴플라이언스)
- 취약점 & 스캐닝
- 조사 방법
- 트러블 슈팅
- 커뮤니케이션 & 문서 작성
- 비판적 사고
- 창의력 & 호기심

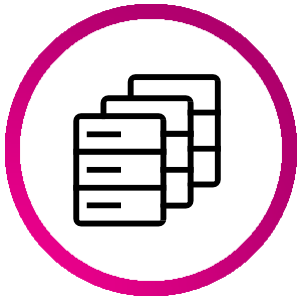
보안 운영이 어려운 이유?

보안 인력, 프로세스, 도구, 비용, 법규 등의 어려움

리소스

보안 인시던트 대응 업무 **담당 인력의 부족**

솔루션

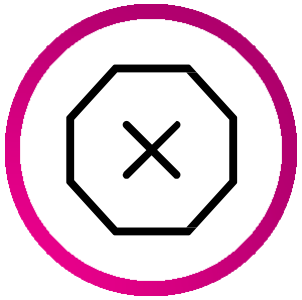


인시던트 대응 처리를 위해 다양한 제품 **오케스트레이션 필요**

경고

인시던트& 경고는 **지속적으로 증가**

정적

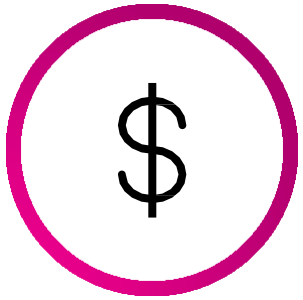


중앙의 관리 및 **협업** 없이 **정적, 독립적으로 수행**

속도

탐지, 분류, 대응 위한 **시간은 빠를 수록 좋음**

비용



사이버범죄로 인한 **비용은 지속적으로 증가**

보안 프레임워크

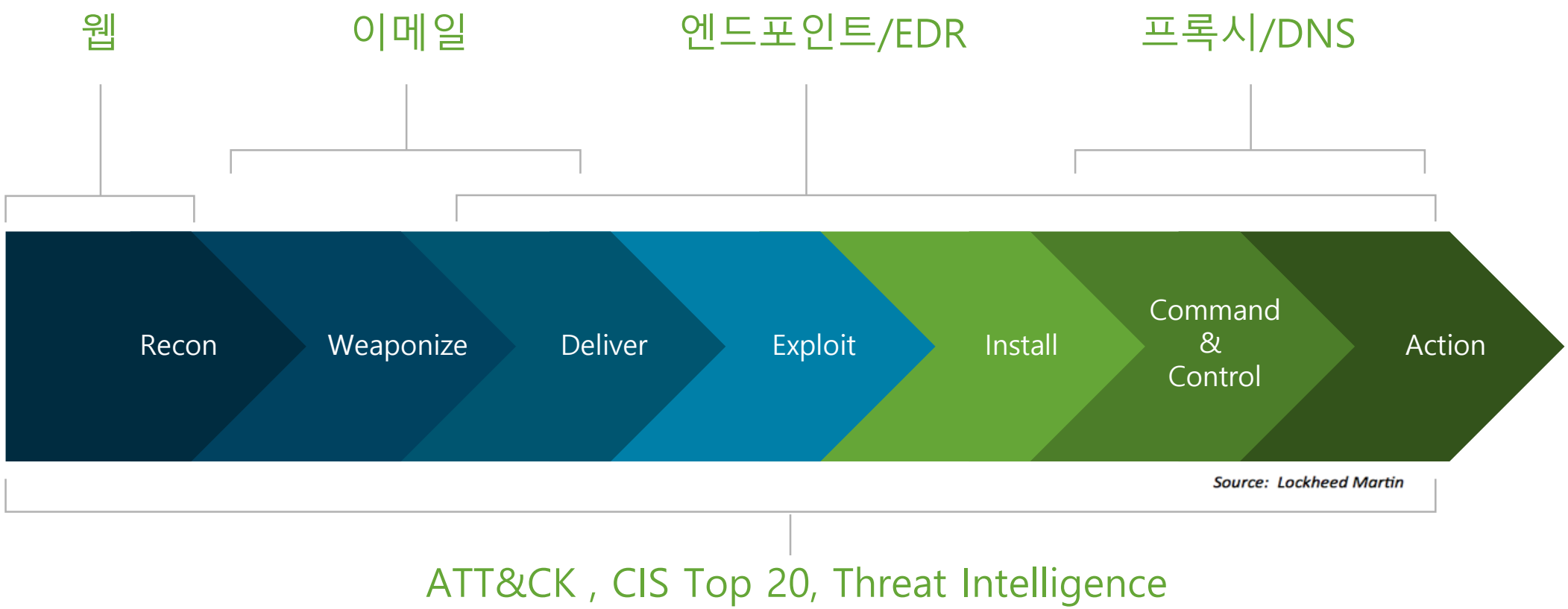
- Lockheed Martin Cyber Kill Chain
- MITRE ATT&CK
- CIS Critical Security Controls

splunk> turn data into doing

보안 프레임워크

보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

Cyber Kill Chain (Lockheed Martin)



보안 프레임워크

보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

Cyber Kill Chain (Lockheed Martin)

Detect(탐지), Deny(거부), Disturb(교란), Degrade(저하), Deceive(기만), Contain(억제)

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Threat Intelligence NIDS D/B Security	Information Sharing Policy				
Weaponization	Threat Intelligence NIDS					
Delivery	Context-Aware Endpoint Malware Protection	Change Management File Integrity Application Whitelisting NIPS	Inline AV	Queuing		Router ACLs App-Aware Firewall Trust Zones Inter-Zone NIPS
Exploitation	Endpoint Malware Protection	Secure Password	DEP			App-Aware Firewall Trust Zones Inter-Zone NIPS
Persistence / Lateral Movement	Log Monitoring	Privilege Separation Secure Password Two- Factor	Router ACLs AV			App-Aware Firewall Trust Zones Inter-Zone NIPS
Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust Zones DNS Sinkholes
Actions on Targets	Endpoint Malware Protection	Encryption	Endpoint Malware Protection	Quality of Service	Honeypot	Incident Response
Exfiltration	DLP	Egress Filtering	DLP			Firewall ACLs

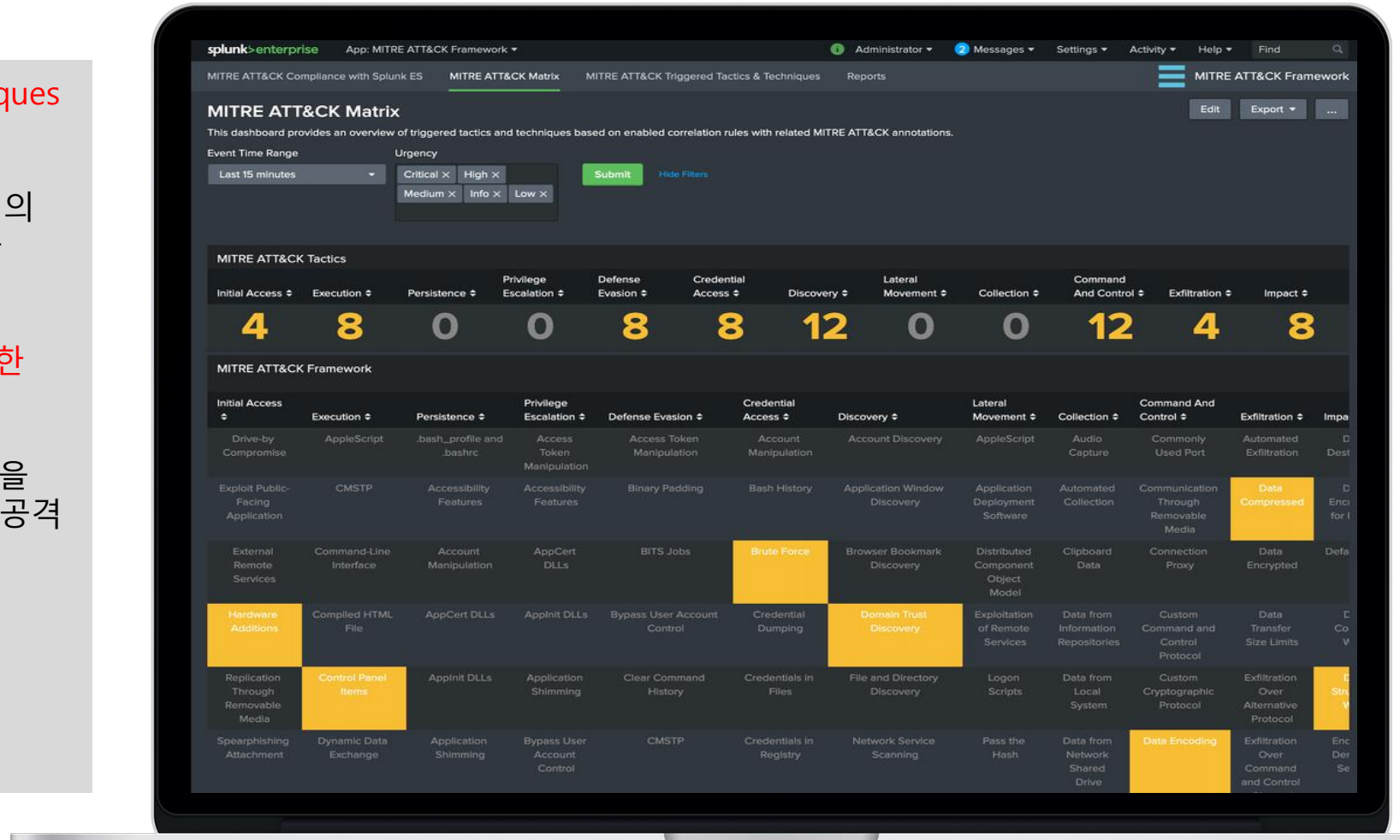
Source: https://nigesecurityguy.wordpress.com/tag/cyber-kill-chain/

보안 프레임워크

보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

MITRE ATT&CK 매트릭스

- ATT&CK은 Adversarial Tactics, Techniques and Common Knowledge의 약어
- 실제 관찰된 내용을 기반으로하여 해커의 전술과 기술에 대한 전세계적으로 접근 가능한 지식 기반입니다
- 해커의 침투 이전 또는 이후 활동에 대한 사례 분석을 통해 공격자의 공격 전술(tactics, 단기적 목적), 침투기술(techniques,단기적 목적-전술을 달성하기 위한 방법), 침투기술을 실제 공격 그룹(APT5)이 침투 기술을 활용하는 절차(Procedure)를 프레임워크로 제안



보안 프레임워크

보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

MITRE ATT&CK 매트릭스(12개 Tactics, 184 개 Techniques)

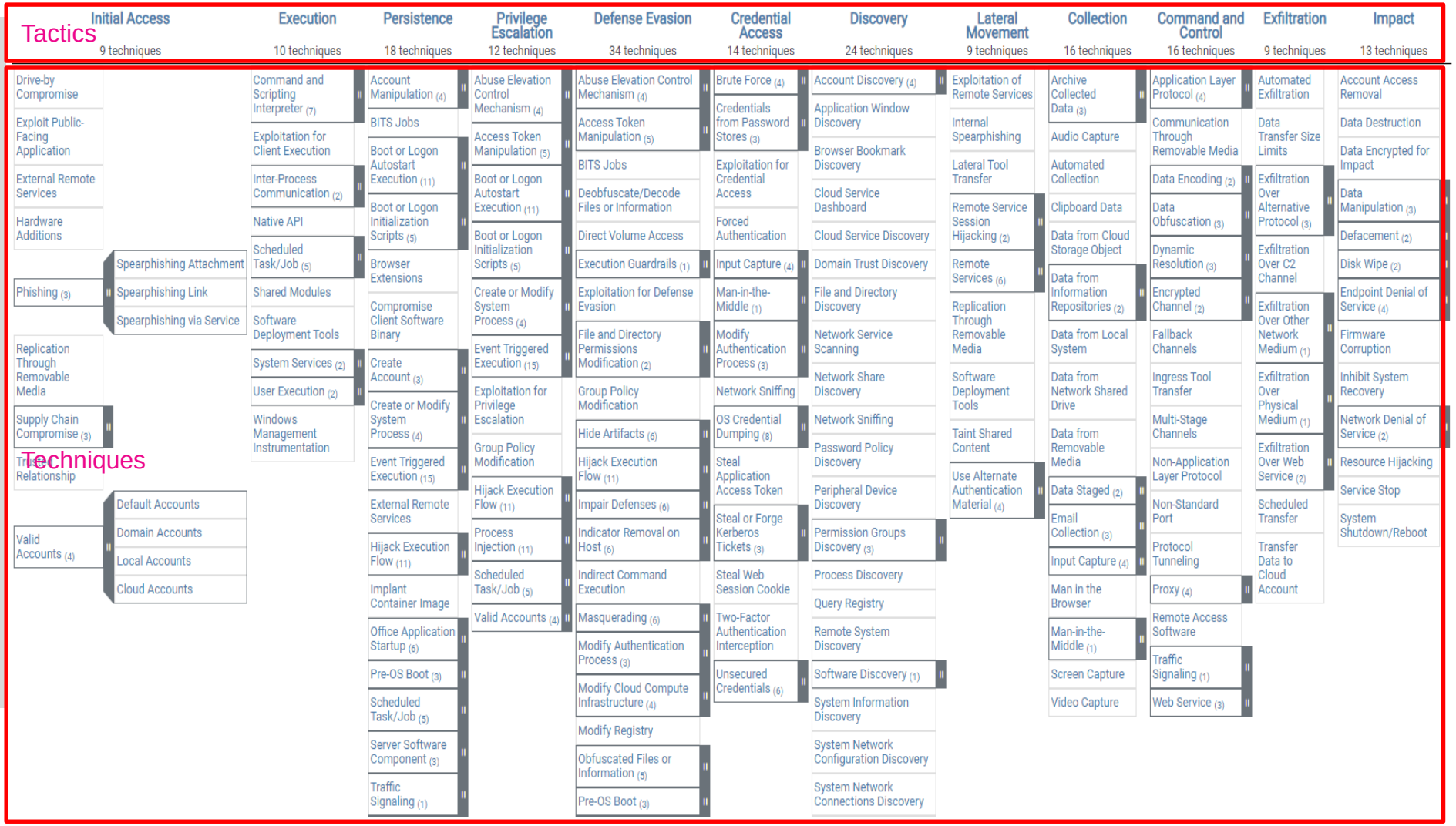
활용방안

1)공격자 그룹이 활용한 공격패턴과 침해사고와 관련된 침해지표(IoC)간의 연관분석을 통한 공격자 그룹 프로파일링.

2)공격자 그룹이 사용할 수 있는 기술들을 매트릭스화 하여 현재 우리 조직 내에 방어 능력이 어느 정도 커버되는지 식별

3)모의 침투 테스트 시에 공격자들이 사용할 수 있는 기술들을 선택적으로 취합하여 공격 시나리오 재구성(red teaming)

Source : https://attack.mitre.org/



보안 프레임워크

보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

CIS 핵심 보안 통제항목

- CIS 핵심 보안 통제항목 (Critical Security Controls, CSC) 는 오랜 시간에 걸쳐 입증되고 우선 순위가 매겨진 20가지의 "검증된" 보안 통제 목록
- 기업 시스템의 보안 위협을 최소화하고 자사의 중요한 데이터를 유지관리하는데 활용
- 2008년 미국 국가안보부 (NSA) 에 의해 처음 작성되었으며, 이전에 SANS와 사이버 보안 이사회에서 관리
- 현재는 Center for Internet Security (CIS) 에서 관리하고 있으며 "기업 보안 프로그램을 측정할 수 있는 실제 척도"로 간주됨

NSA의 CIS CSC 공격 대응 뷰

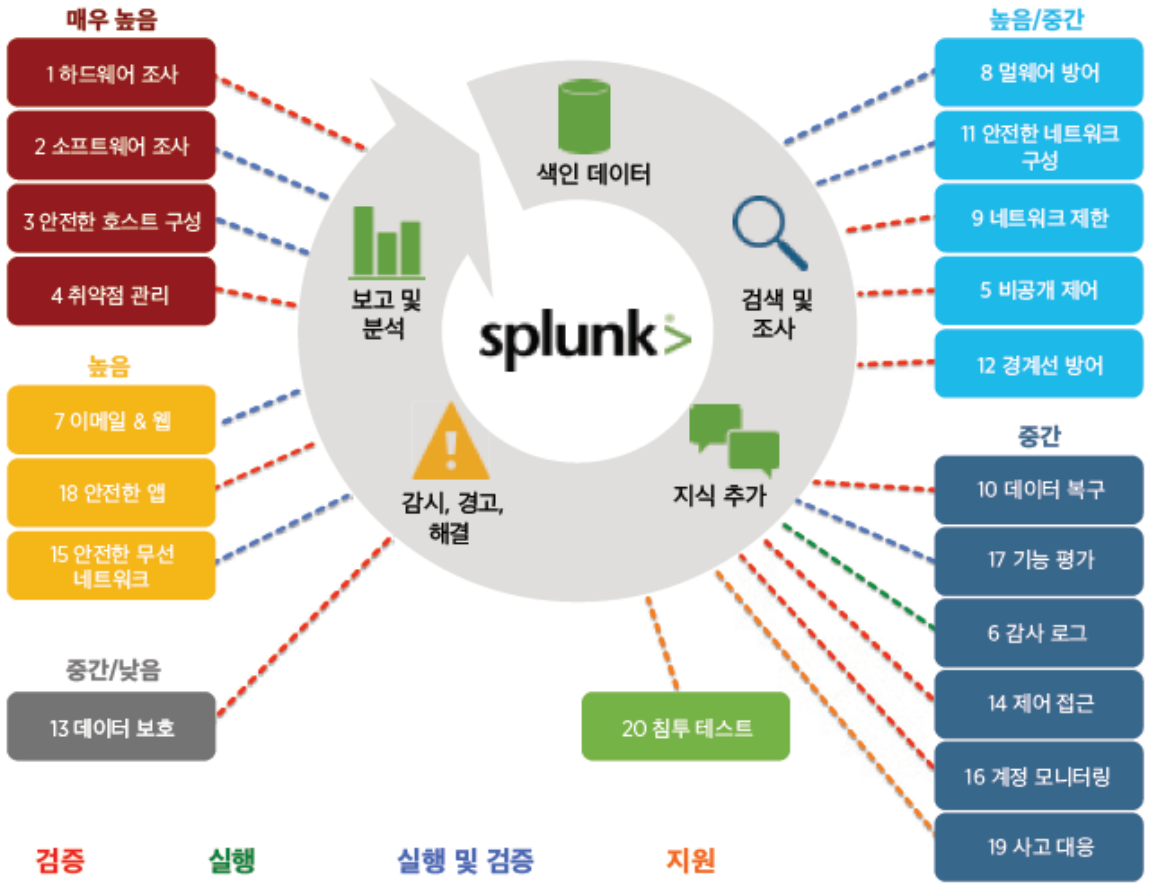
보안 프레임워크

보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

CIS 핵심 보안 통제항목

- 통제 항목들을 적용하면 이미 알려져 있는 높은 우선 순위의 공격뿐만 아니라 가까운 미래에 발생할 가능성이 있는 공격에 대한 위협까지도 줄일 수 있습니다. 또한 위협 탐지 및 방어를 위한 고품질 데이터를 제공합니다.
- 통제 항목들은 연방 정부 및 민간 업계 전문가 모두의 의견을 수렴하여 작성되었습니다.
- 공격 상황에서 NSA 가 취하는 조치에 대해 CIS CSC 가 어떻게 적용되는지를 보여주는 예입니다. 각 통제 항목들은 정찰(Reconnaissance), 침투(Get In), 잠복(Stay In), 익스플로잇 (Exploit)의 4 가지 카테고리와 하나 이상 대응됩니다

CIS CSC 각 통제 항목으로 매핑되는 Splunk 소프트웨어



보안 프레임워크

보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

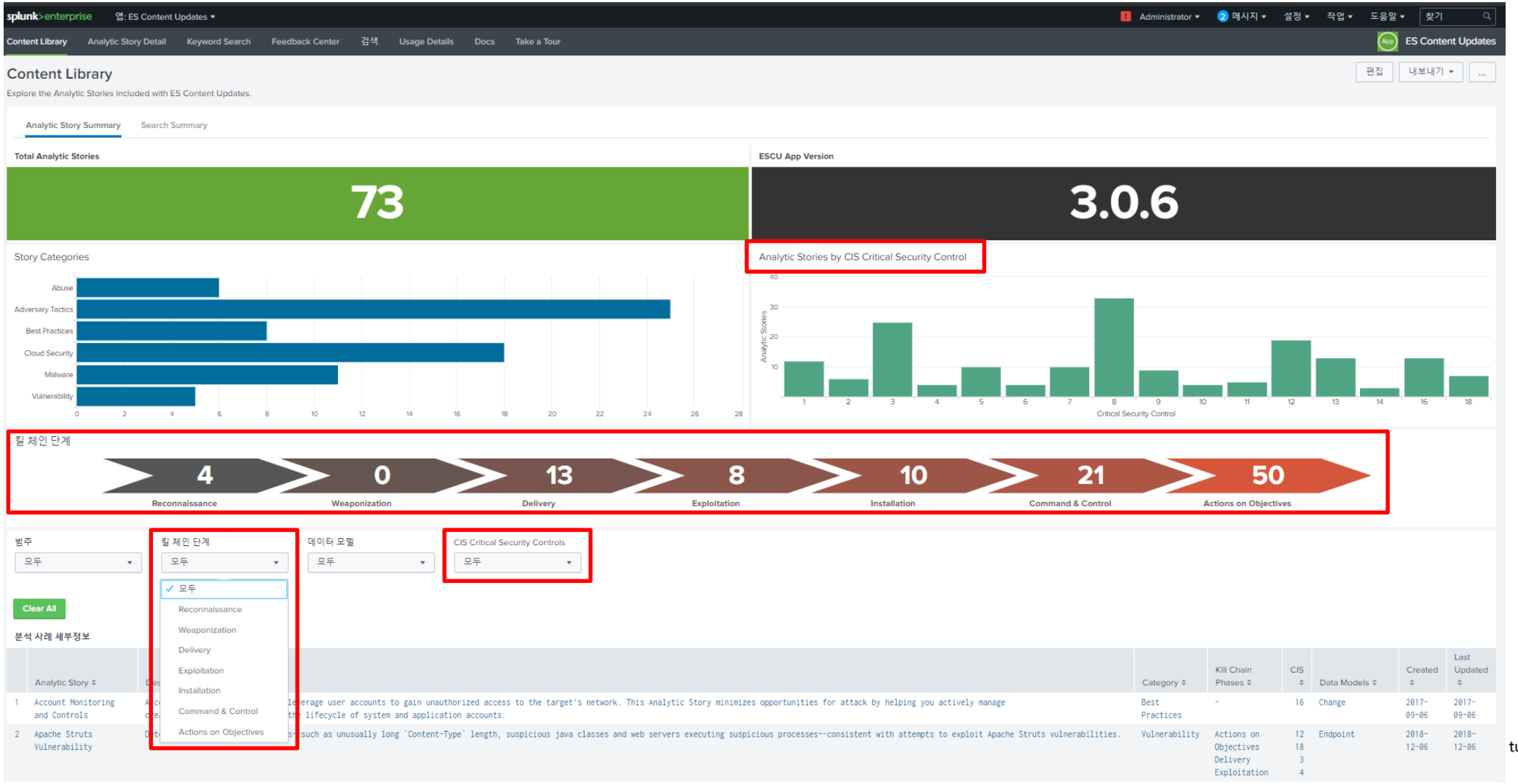
CIS 핵심 보안 통제항목

	Ransomware	DDoS	Malicious Insiders	Phishing	Vulnerability Exploits
CSC1: Inventory of authorized and unauthorized devices	✓		✓		✓
CSC2: Inventory of authorized and unauthorized software	✓		✓	✓	✓
CSC3: Secure configurations for hardware and software	✓	✓	✓	✓	✓
CSC4: Continuous vulnerability assessment and remediation	✓		✓	✓	✓
CSC5: Controlled use of administrative privileges	✓		✓	✓	✓
CSS6: Maintenance, monitoring and analysis of audit logs	✓	✓	✓	✓	✓
CSC7: Email and browser protections	✓			✓	✓
CSC8: Malware defenses	✓			✓	✓
CSC9: Limitation and control of network ports	✓	✓	✓		✓
CSC10: Data recovery capability	✓		✓		
CSC11: Secure configurations for network devices		✓	✓		✓
CSC12: Boundary defense		✓			✓
CSC13: Data protection			✓		
CSC14: Controlled access based on the need to know	✓		✓		
CSC15: Wirelss access control			✓		✓
CSC16: Account monitoring and control			✓	✓	✓
CSC17: Security skills assessment and appropriate training to fill gaps	✓		✓	✓	
CSC 18: Application software security			✓		✓
CSC 19: Incident response and management	✓	✓	✓	✓	✓
CSC 20: Penetration Tests and Red Team Exercises			✓		✓

보안 프레임워크

보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

Splunk에서 보안 프레임워크 사용



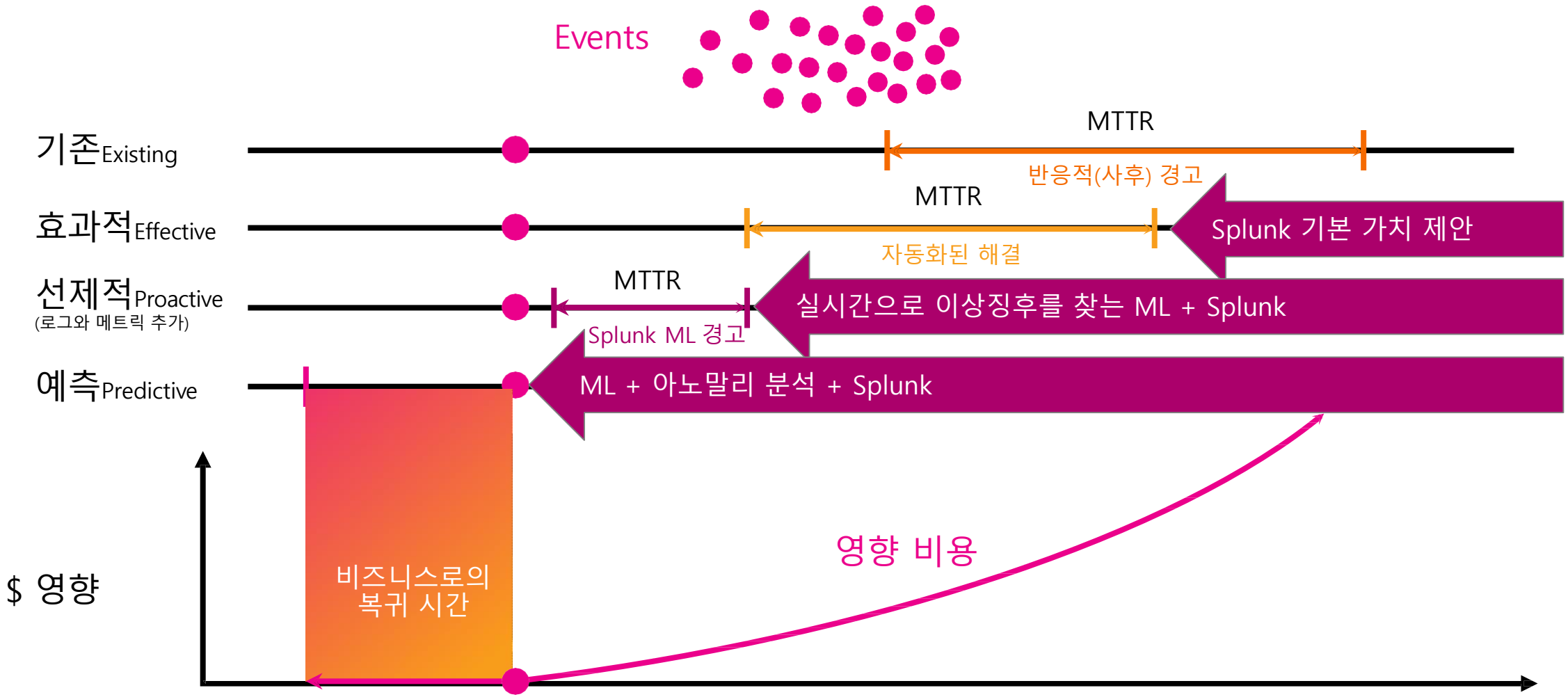
AISecOps 적용하기

Splunk ES + Splunk UBA + MLTK

splunk> turn data into doing™

머신러닝(ML)

알려지지 않은 위협 탐지



MTTR(Mean Time To Repair) : 평균적으로 장애극복을 위해 소요되는 수리시간

Splunk에서 ML 사용하기

1 splunk>enterprise

코어 플랫폼
검색 + 스마트하게 사용

2 프리미엄 앱

패키지된 프리미엄 앱
(ES, UBA, ITSI 등)

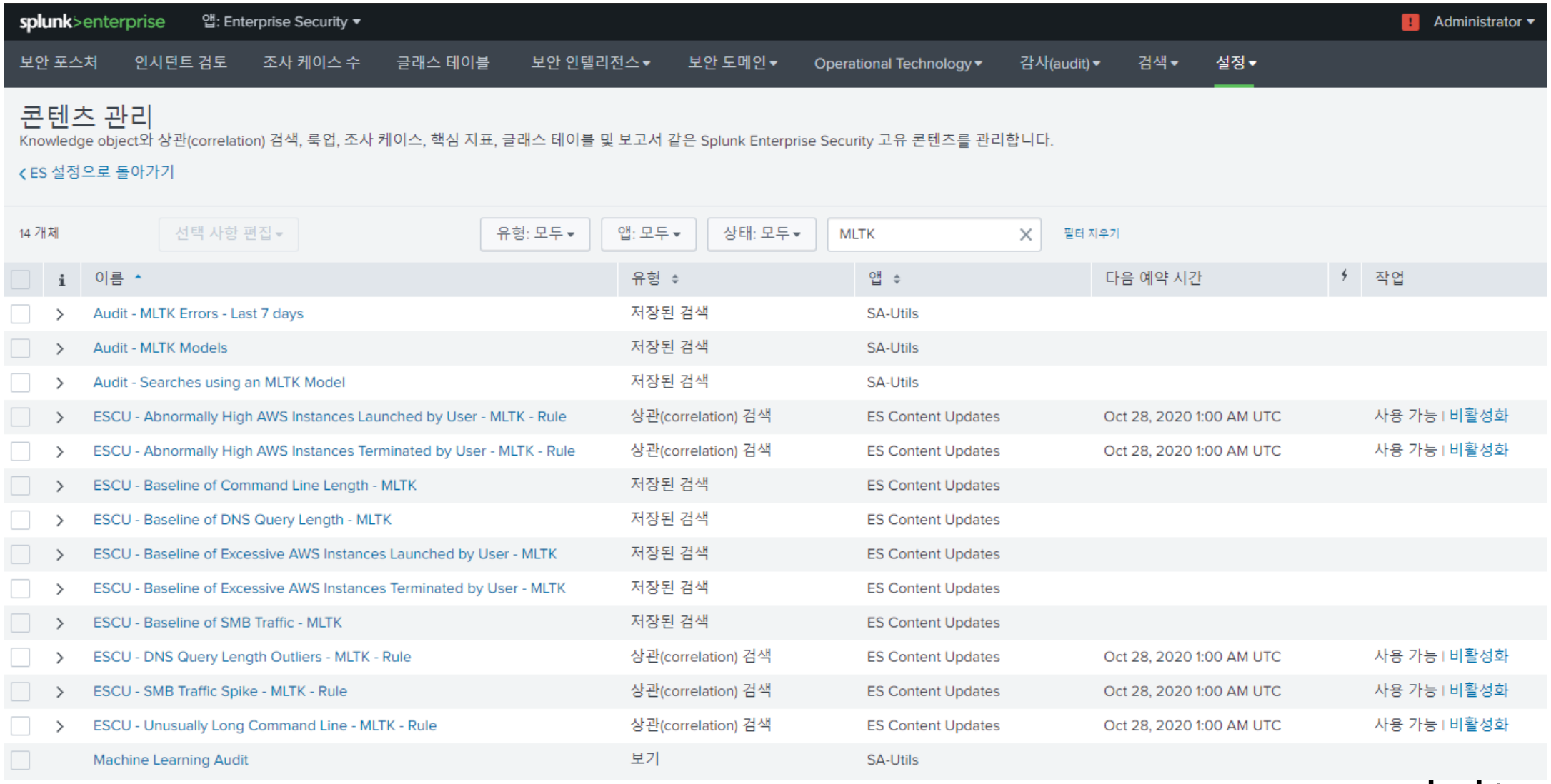
3 MLTK

ML TOOLKIT

splunk> 운영 인텔리전스를 위한 플랫폼

AISecOps 적용하기

Splunk ES에 ML 룰 추가



AISecOps 적용하기

Splunk ES + 행위분석(UBA)을 추가하여 성능강화

0010 01010 0101 분석된 데이터

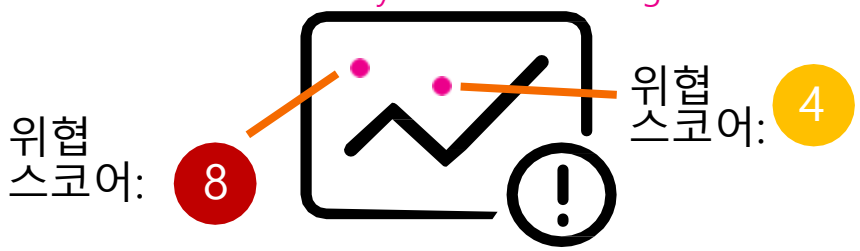
- 네트워크 행위
- 애플리케이션 행위
- 로그인 시도 행위
- 이동식 미디어
- 출입증 스캔
- 프린터 행위

> 기준선 설정

- 사용자 행위
- 부서 행위
- 지역 행위
- 회사 행위

> 상관분석 & 탐지

Powered by Machine Learning

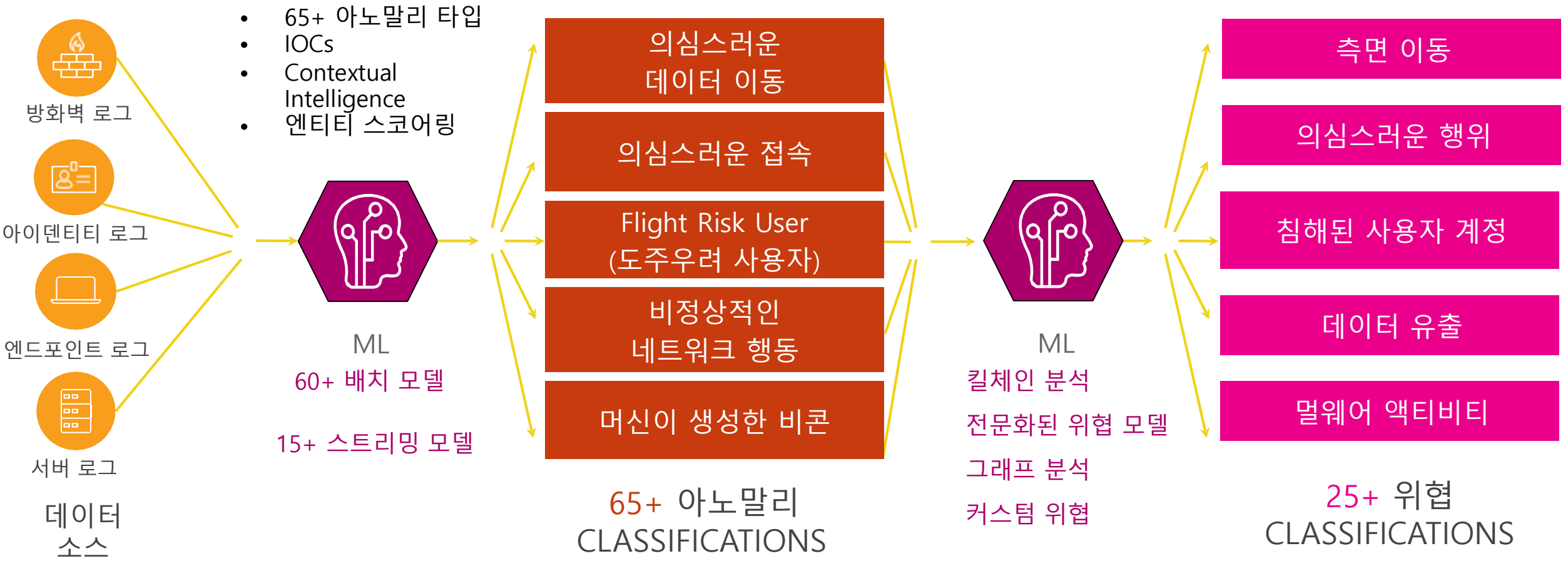


예:

- 의심스러운 사용자 또는 장치에서 데이터 유출
- 비정상적인 횟수로 연결된 데이터 스토리지
- 비정상적인 방법으로 프린터 사용
- 권한 에스컬레이션
- 여러 번 실패한 로그인 시도
- 멀웨어
- 블랙리스트 IP 주소
- 침해된 계정

AISecOps 적용하기

Splunk ES + 행위분석(UBA)을 추가하여 성능강화



splunk> turn data into doing

AISecOps 적용하기

MLTK를 이용한 알려지지 않은 위협 탐지

머신러닝 워크플로우

단계 1

- 데이터 접근 및 불러오기

단계 2

- 데이터 전처리 작업

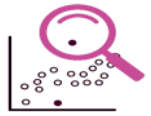
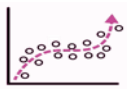
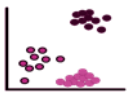
단계 3

- 전처리 가공된 데이터를 통해 특징 추출(Search & Visualize)

데이터 유형	특징 선택 작업	기법
센서 데이터	원시 센서 데이터에서 신호 속성을 추출하여 하이 레벨 정보 생성	펄스 및 전환 메트릭 – 상승 시간, 하강 시간, 정착 시간 등의 신호 특성 도출 스펙트럼 측정 – 신호 출력, 대역폭, 중심 주파수, 중간 주파수 플로팅
트랜잭션 데이터	데이터에서 정보를 개선하는 도출된 값 계산	타임스탬프 분해 – 타임스탬프를 일, 월 등의 성분으로 분해 집계 가치 계산 – 특정 이벤트가 발생한 총 횟수 등의 상위 특징 작성

단계 4

- 추출된 특징을 이용해 학습 & 최적의 모델 개발을 위해 반복 작업

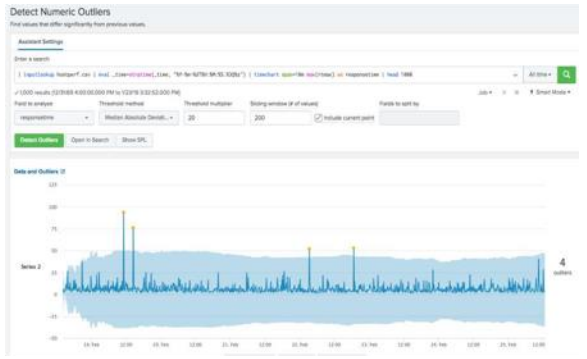
Anomaly detection	Predictive Analytics	Clustering
		
▸ 과거 행위와의 편차 ▸ (aka 다변량 AD or 응집성 AD)	▸ 사용자 이탈 예측 ▸ 이벤트/트랜드 예측 ▸ 실패의 조기 경고	▸ 동료 그룹 식별 ▸ 이벤트 상관분석 ▸ 경고 노이즈 감소

단계 5

- 최적의 학습된 모델을 통합 시스템에 반영

머신러닝 알고리즘(300+)

데이터기반 예측 분석

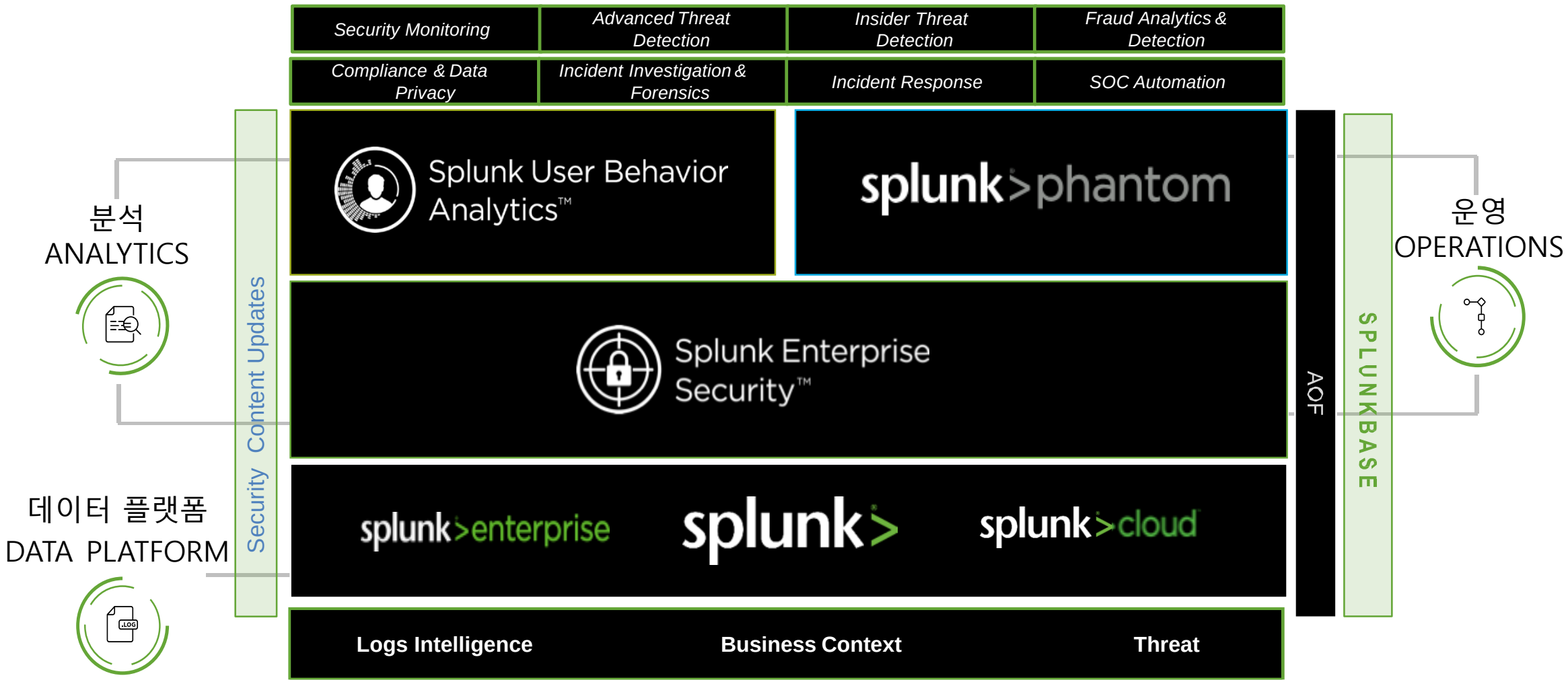


상관 및 데이터 탐색

Splunk 보안 포트폴리오

splunk> turn data into doing™

Splunk 보안 포트폴리오

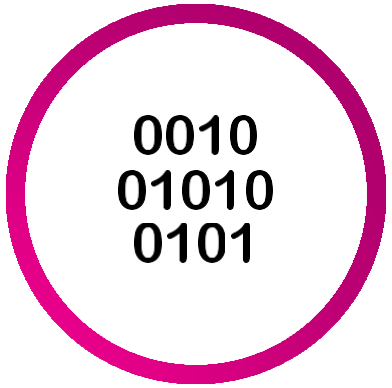


AOF(Adaptive Operations Framework) : 보안 아키텍처는 유기적으로 작동하도록 설계되지 않은 여러 계층의 도구와 제품을 포함하므로 보안팀은 여러 도메인을 연결하여 방어를 코디네이션하는 방법에 차이가 있습니다. AOF는 고객사의 보안 제품 및 기술을 Splunk Enterprise Security 및 Splunk Phantom을 포함한 Splunk 보안 솔루션과 연결하여 이러한 격차를 해결합니다.

•모든 소스에서 정형 또는 비정형 데이터 수집 / 풍부한 분석으로 지원되는 협업 의사 결정 추진 / SOC의 포괄적인 기술 범위에 대해 오케스트레이션된 작업 수행

Splunk 보안 포트폴리오

데이터



splunk>cloud
splunk>enterprise

- 유니버셜 인덱싱
- Petabyte 스케일
- 검색, 경고, 리포트, 시각화
- DFS(Data Fabric Search)
- DSP(Data Stream Processor)

분석

splunk> Security Essentials

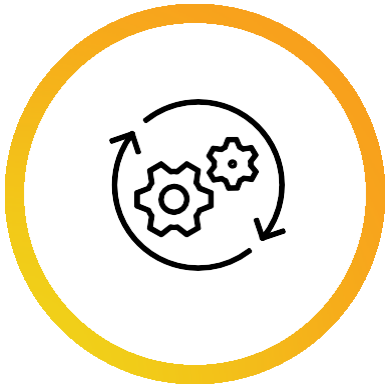
Splunk Enterprise Security™ — ES 컨텐츠 업데이트

Splunk User Behavior Analytics™

Machine Learning Toolkit (MLTK)

운영

어댑티브 운영 프레임워크 (AOF)



Phantom

Splunk Enterprise Security™

어댑티브 응답(Adaptive Response)

Splunk 보안 포트폴리오

splunk>enterprise	Splunk Enterprise Security™	Splunk User Behavior Analytics™	splunk> phantom
• 데이터 수집 및 색인 • 검색 / 조사 / 상관 분석 • 시각화 및 레포트 • 모니터링 및 경고 • 어디서나 저장/액세스(빅데이터 플랫폼) • 애드혹 검색 • 유니버셜 저장(형태/크기/속도에 관계없이 빠르게 저장 가능) • 스트림(와이어,네트워크 패킷) 데이터 수집 • 1,000+ 앱 에코시스템	• 이벤트 상관분석 & 노터블(Notble) 프레임워크 • 위험 스코어링 프레임워크 • 인시던트 조사 워크플로우 • 자산 및 ID 프레임워크 • 워크플로우 액션 커스텀정의 • 글래스 테이블(KPI 분석) • 250+ 보안 상관 시나리오/ 대시보드/유즈케이스 • 시퀀스 템플릿 • 어댑티브 대응 액션 • OOTB - 보안 메트릭, 대시보드, 유즈케이스, 분석 스토리	• 딥러닝기반 엔드포인트 행위 분석 • 아노말리 / 알려지지 않은 위협 발견 • 즉시 사용 가능한 분석 • 사용자 위험 평가 및 모니터링 • 통합 위협 시각화 • 킬 체인 뷰 • 커스텀 시나리오 정의	• 보안 오케스트레이션, 자동화 및 대응 엔진(SOAR) • 플레이북을 Drag&Drop 방법으로 쉽게 생성(Visual Playbook Editor로 코딩없이 플레이북 생성) • 경고 및 주요 이벤트를위한 워크플로우 자동화 • 사례 관리, 컨텍스트 강화 • 200+ 앱 및 1,900+ API와 통합하는 에코시스템
빅데이터 분석 플랫폼	분석기반 SIEM	엔드포인트 행위 분석	보안 운영 오케스트레이션/자동화/대응

Thank You!

splunk> turn data into doing™