

보안, 프레임워크 그리고 머신러닝

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

splunk® > turn data into doing™



Agenda

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

보안 운영 (SecOps)

보안 운영 워크플로우

로그, 모니터링, 탐지, 대응, 자동화, AI까지 필요

보안/비보안
솔루션
로그/모니터링



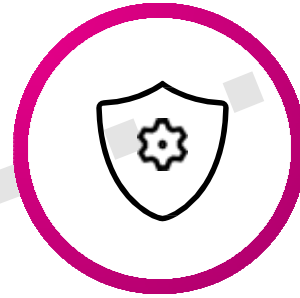
로그/패킷
데이터 수집

인시던트
탐지/분석



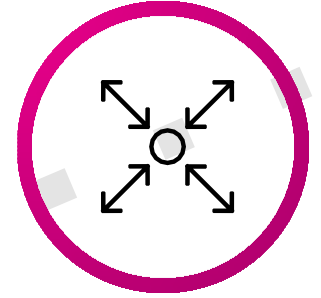
임계치 분석/아노말리
분석(통계)/머신러닝
시나리오를 이용한
이상징후 탐지

대응/복구



선제적 분석을 통한
보안 이상징후 대응

AI SecOps



머신러닝을 이용한
자율적 탐지/ 자동화된
대응 및 복구

선제적

보안 이상징후

반응

보안 운영 워크플로우



다양한 데이터 소스부터 복잡한 탐지 운영 절차

데이터 소스

-  방화벽
-  IDS / IPS
-  엔드포인트 보안
-  웹방화벽
-  지능형 멀웨어
-  포렌식
-  멀웨어 디토네이션

수집

모니터링/탐지/경고/조사

-  SIEM
-  위협 인텔리전스 플랫폼

분석

-  Tier 1
-  Tier 2
-  Tier 3




자동화/대응

-  방화벽
-  IDS / IPS
-  엔드포인트 보안
-  웹방화벽
-  지능형 멀웨어
-  포렌식
-  멀웨어 디토네이션

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

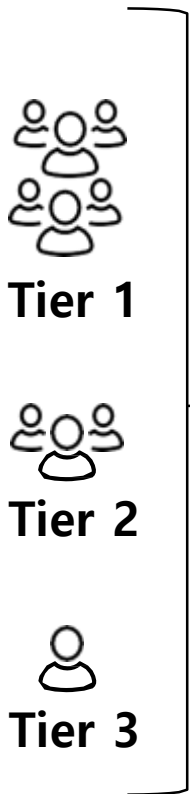


CISO

-  팀 운영 성능
-  프로세스 & 운영
-  메트릭 & 리포팅

보안 운영 워크플로우

많은 보안 경험 요구 - 하드웨어 스킬 & 소프트웨어 스킬



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

보안 운영이 어려운 이유?

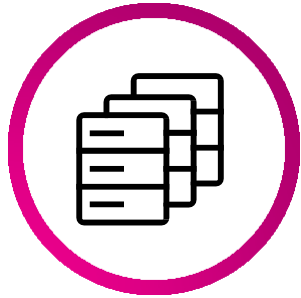
보안 인력, 프로세스, 도구, 비용, 법규 등의 어려움

리소스



보안 인시던트 대응 업무 담당 인력의 부족

솔루션



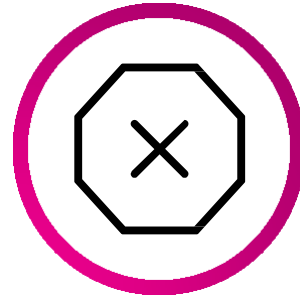
인시던트 대응 처리를 위해 다양한 제품 오케스트레이션 필요

경고



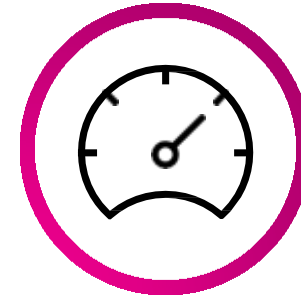
인시던트& 경고는 지속적으로 증가

정적



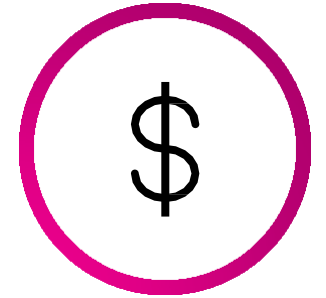
증량의 관리 및 협업 없이 정적, 독립적으로 수행

속도



탐지, 분류, 대응 위한 시간은 빠를 수록 좋음

비용



사이버범죄로 인한 비용은 지속적으로 증가

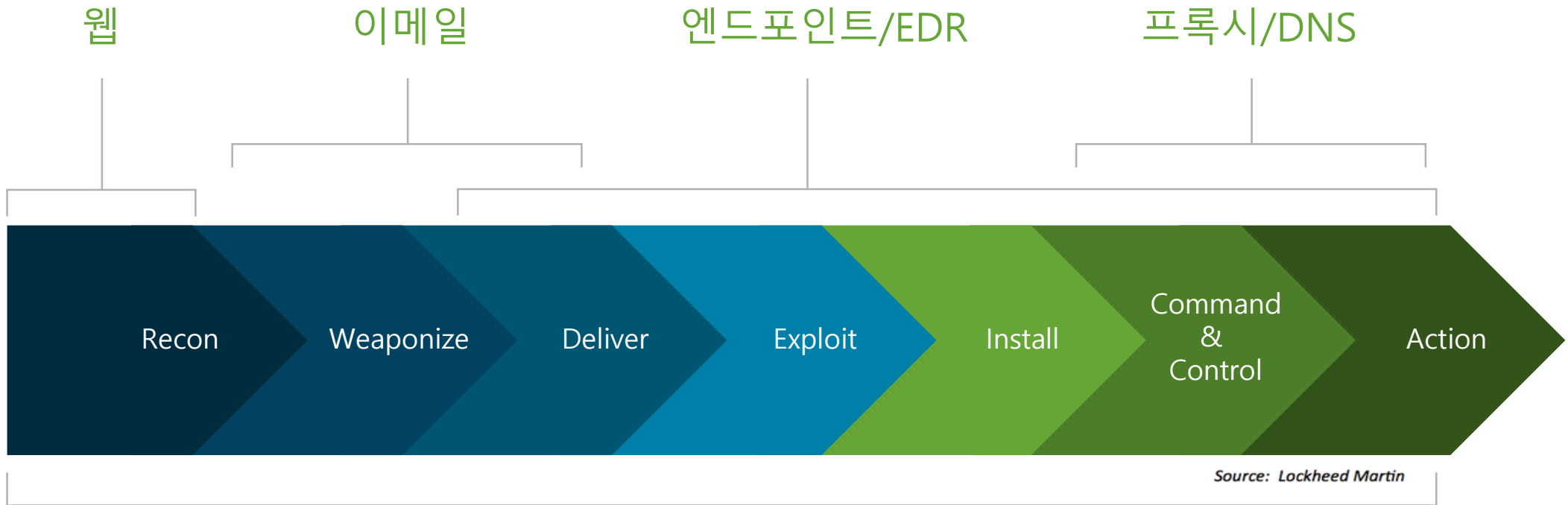
보안 프레임워크

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

보안 프레임워크

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

Cyber Kill Chain (Lockheed Martin)



ATT&CK , CIS Top 20, Threat Intelligence

보안 프레임워크

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

Cyber Kill Chain (Lockheed Martin)



Detect(탐지), Deny(거부), Disrupt(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

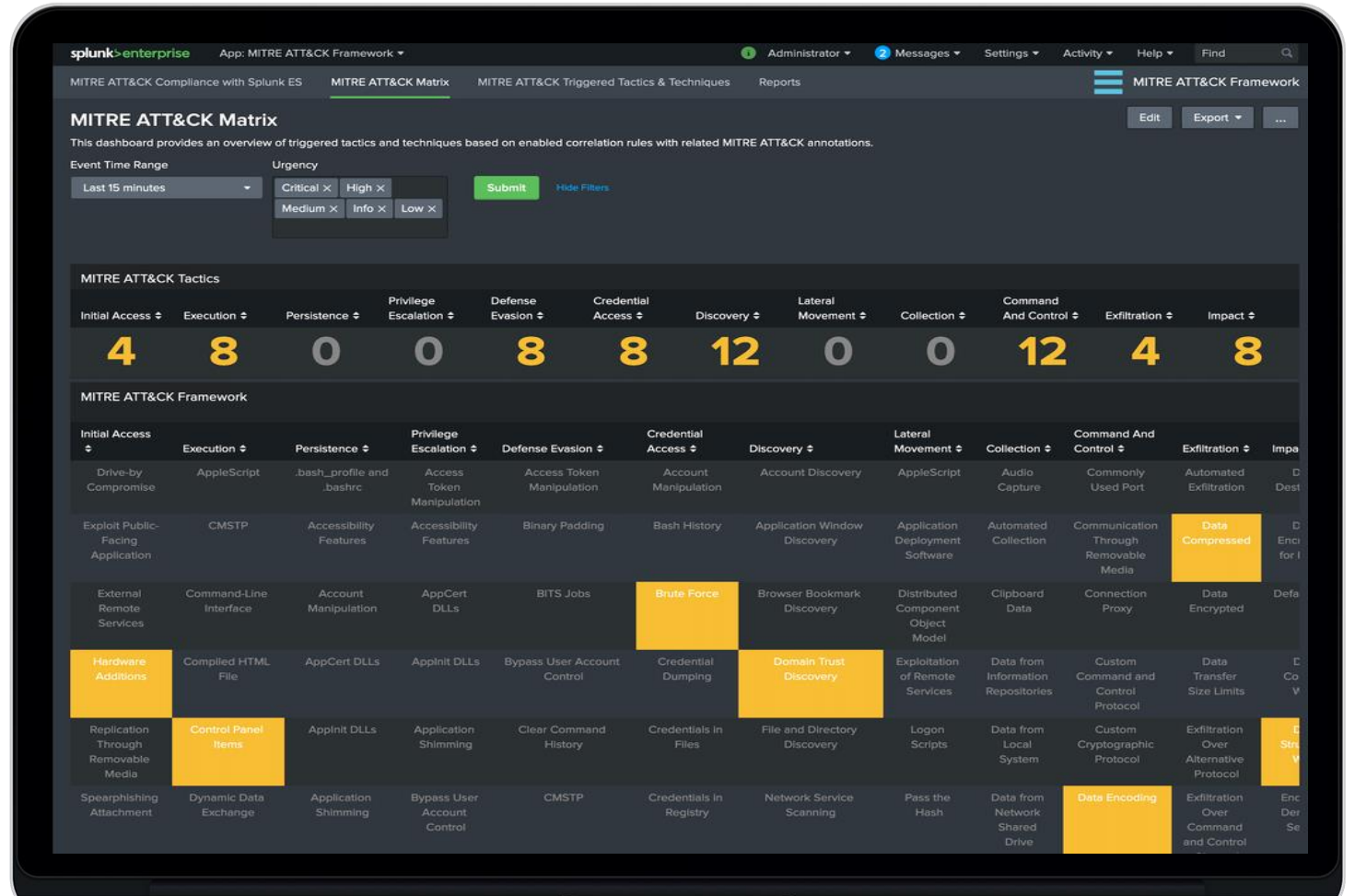
보안 프레임워크

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 기반으로 하여 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)

Tactics	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise		Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application		Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services		Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions		Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
	Spearphishing Attachment	Scheduled Task/Job (5)	Browser Extensions	Event Triggered Execution (15)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over C2 Channel	Defacement (2)
Phishing (3)	Spearphishing Link	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
	Spearphishing via Service	Software Deployment Tools	Event Triggered Execution (15)	Group Policy Modification	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Replication Through Removable Media		System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption
Supply Chain Compromise (3)		User Execution (2)	Create or Modify System Process (4)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Trusted Relationship		Windows Management Instrumentation	Event Triggered Execution (15)	Hijack Execution Flow (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol	Exfiltration Over Web Service (2)	Network Denial of Service (2)
			External Remote Services	Impair Defenses (6)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Data Staged (2)	Non-Standard Port	Scheduled Transfer	Resource Hijacking
Valid Accounts (4)	Default Accounts		Hijack Execution Flow (11)	Indicator Removal on Host (6)	Process Injection (11)	Steal Web Session Cookie	Peripheral Device Discovery		Email Collection (3)	Protocol Tunneling	Transfer Data to Cloud Account	Service Stop
	Domain Accounts		Implant Container Image	Indirect Command Execution	Scheduled Task/Job (5)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
	Local Accounts		Office Application Startup (6)	Masquerading (6)	Valid Accounts (4)	Unsecured Credentials (6)	Process Discovery		Man in the Browser	Remote Access Software		
	Cloud Accounts		Pre-OS Boot (3)	Modify Authentication Process (3)			Query Registry		Man-in-the-Middle (1)	Traffic Signaling (1)		
			Scheduled Task/Job (5)	Modify Cloud Compute Infrastructure (4)			Remote System Discovery		Screen Capture	Web Service (3)		
			Server Software Component (3)	Modify Registry			Software Discovery (1)		Video Capture			
			Traffic Signaling (1)	Obfuscated Files or Information (5)			System Information Discovery					
				Pre-OS Boot (3)			System Network Configuration Discovery					
							System Network Connections Discovery					

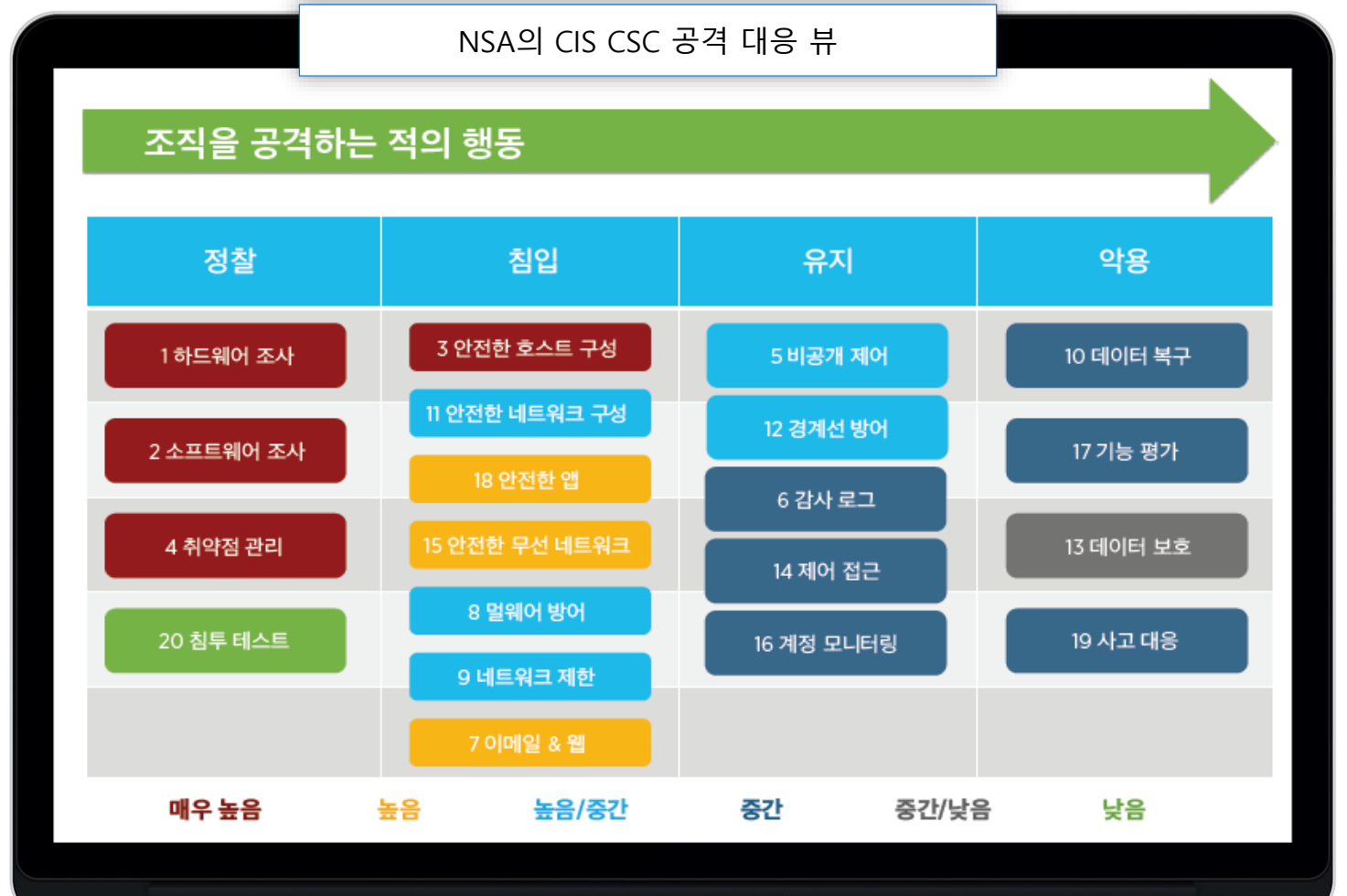
보안 프레임워크

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



보안 프레임워크

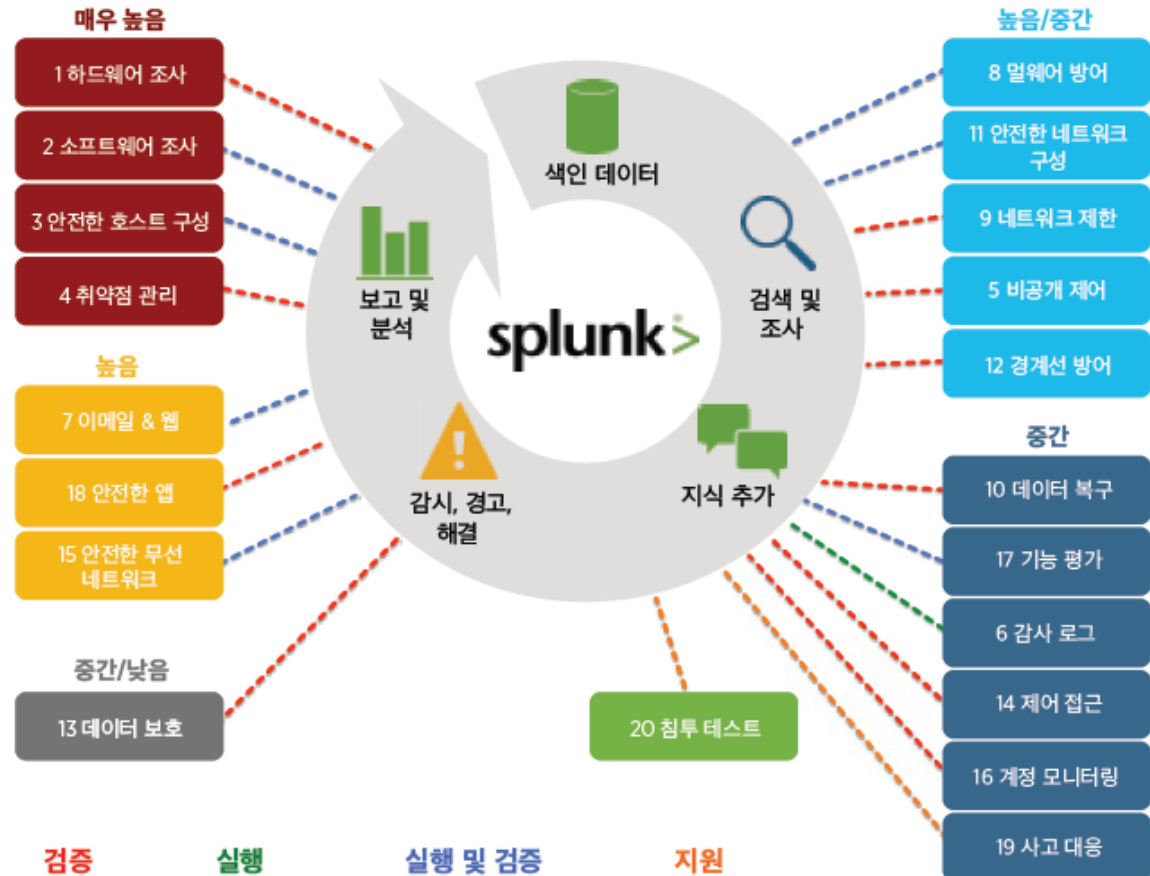
보안 프레임워크(LM Cyber Kill Chain, MITRE ATT&CK, CIS Critical Security Controls)

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 카테고리과 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	✓		✓	✓	✓
CSC6: 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: Wireless access control			✓		✓
CSC16: Account monitoring and control			✓	✓	✓
CSC17: Security skills assessment and appropriate training to fill gaps	✓		✓	✓	
CSC18: Application software security			✓		✓
CSC19: Incident response and management	✓	✓	✓	✓	✓
CSC20: 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



The screenshot displays the Splunk ES Content Updates interface. At the top, the navigation bar includes 'Content Library', 'Analytic Story Detail', 'Keyword Search', 'Feedback Center', '검색', 'Usage Details', 'Docs', and 'Take a Tour'. The main content area is titled 'Content Library' and shows 'Total Analytic Stories' as 73 and 'ESCU App Version' as 3.0.6. Below this, there are two charts: 'Story Categories' (a horizontal bar chart) and 'Analytic Stories by CIS Critical Security Control' (a vertical bar chart). A prominent red-bordered arrow graphic shows the 'Kill Chain 단계' (Kill Chain Phases) with counts: Reconnaissance (4), Weaponization (0), Delivery (13), Exploitation (8), Installation (10), Command & Control (21), and Actions on Objectives (50). Below the arrow, there are filter dropdowns for '범주' (Category), 'Kill Chain 단계' (Kill Chain Phases), '데이터 모델' (Data Models), and 'CIS Critical Security Controls'. The 'CIS Critical Security Controls' dropdown is highlighted with a red box. At the bottom, a table lists analytic stories with columns for 'Category', 'Kill Chain Phases', 'CIS', 'Data Models', 'Created', and 'Last Updated'. The table contains two rows of data.

Category	Kill Chain Phases	CIS	Data Models	Created	Last Updated
Best Practices	-	16	Change	2017-09-06	2017-09-06
Vulnerability	Actions on Objectives Delivery Exploitation	12 18 3 4	Endpoint	2018-12-06	2018-12-06

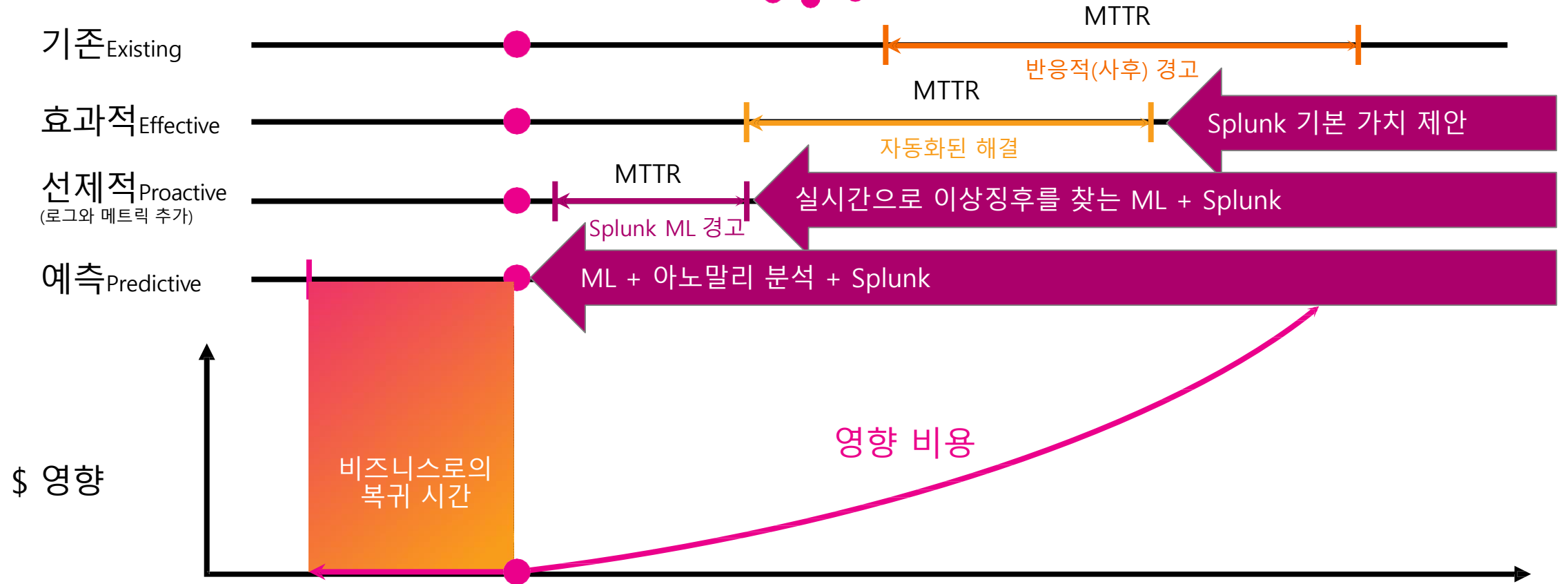
AI SecOps 적용하기

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`

2 프리미엄 앱

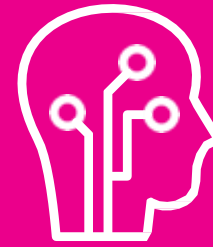
3 MLTK



코어 플랫폼
검색 + 스마트하게 사용



패키지된 프리미엄 앱
(ES, UBA, ITSI 등)



ML TOOLKIT

splunk> 운영 인텔리전스를 위한 플랫폼

AI SecOps 적용하기

Splunk ES에 ML 룰 추가

splunk > enterprise 앱: Enterprise Security Administrator

보안 포스터 | 인사면접 검토 | 조사 케이스 수 | 글래스 테이블 | 보안 인텔리전스 | 보안 도메인 | Operational Technology | 감사(audit) | 검색 | 설정

콘텐츠 관리

Knowledge object와 상관(correlation) 검색, 특업, 조사 케이스, 핵심 지표, 글래스 테이블 및 보고서 같은 Splunk Enterprise Security 고유 콘텐츠를 관리합니다.

[< ES 설정으로 돌아가기](#)


14 개체 유형: 모두 앱: 모두 상태: 모두 MLTK X 필터 지우기

<input type="checkbox"/>	i	이름 ^	유형 ↕	앱 ↕	다음 예약 시간	⚡	작업
<input type="checkbox"/>	>	Audit - MLTK Errors - Last 7 days	저장된 검색	SA-Utills			
<input type="checkbox"/>	>	Audit - MLTK Models	저장된 검색	SA-Utills			
<input type="checkbox"/>	>	Audit - Searches using an MLTK Model	저장된 검색	SA-Utills			
<input type="checkbox"/>	>	ESCU - Abnormally High AWS Instances Launched by User - MLTK - Rule	상관(correlation) 검색	ES Content Updates	Oct 28, 2020 1:00 AM UTC		사용 가능 비활성화
<input type="checkbox"/>	>	ESCU - Abnormally High AWS Instances Terminated by User - MLTK - Rule	상관(correlation) 검색	ES Content Updates	Oct 28, 2020 1:00 AM UTC		사용 가능 비활성화
<input type="checkbox"/>	>	ESCU - Baseline of Command Line Length - MLTK	저장된 검색	ES Content Updates			
<input type="checkbox"/>	>	ESCU - Baseline of DNS Query Length - MLTK	저장된 검색	ES Content Updates			
<input type="checkbox"/>	>	ESCU - Baseline of Excessive AWS Instances Launched by User - MLTK	저장된 검색	ES Content Updates			
<input type="checkbox"/>	>	ESCU - Baseline of Excessive AWS Instances Terminated by User - MLTK	저장된 검색	ES Content Updates			
<input type="checkbox"/>	>	ESCU - Baseline of SMB Traffic - MLTK	저장된 검색	ES Content Updates			
<input type="checkbox"/>	>	ESCU - DNS Query Length Outliers - MLTK - Rule	상관(correlation) 검색	ES Content Updates	Oct 28, 2020 1:00 AM UTC		사용 가능 비활성화
<input type="checkbox"/>	>	ESCU - SMB Traffic Spike - MLTK - Rule	상관(correlation) 검색	ES Content Updates	Oct 28, 2020 1:00 AM UTC		사용 가능 비활성화
<input type="checkbox"/>	>	ESCU - Unusually Long Command Line - MLTK - Rule	상관(correlation) 검색	ES Content Updates	Oct 28, 2020 1:00 AM UTC		사용 가능 비활성화
<input type="checkbox"/>		Machine Learning Audit	보기	SA-Utills			







AI SecOps 적용하기

Splunk ES + 행위분석(UBA)을 추가하여 성능강화

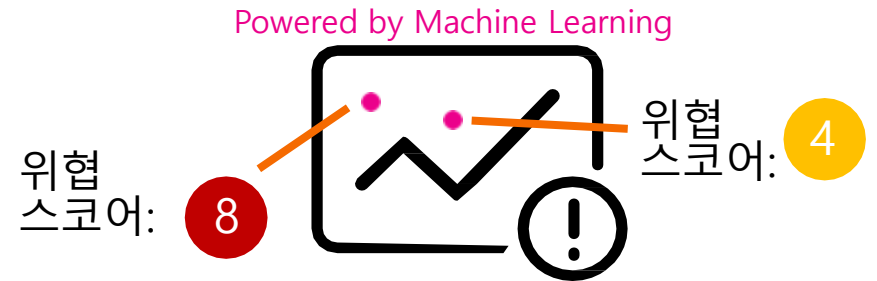
0010
01010
0101 분석된 데이터

>  기준선 설정

>  상관분석 & 탐지

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

-  사용자 행위
-  부서 행위
-  지역 행위
-  회사 행위

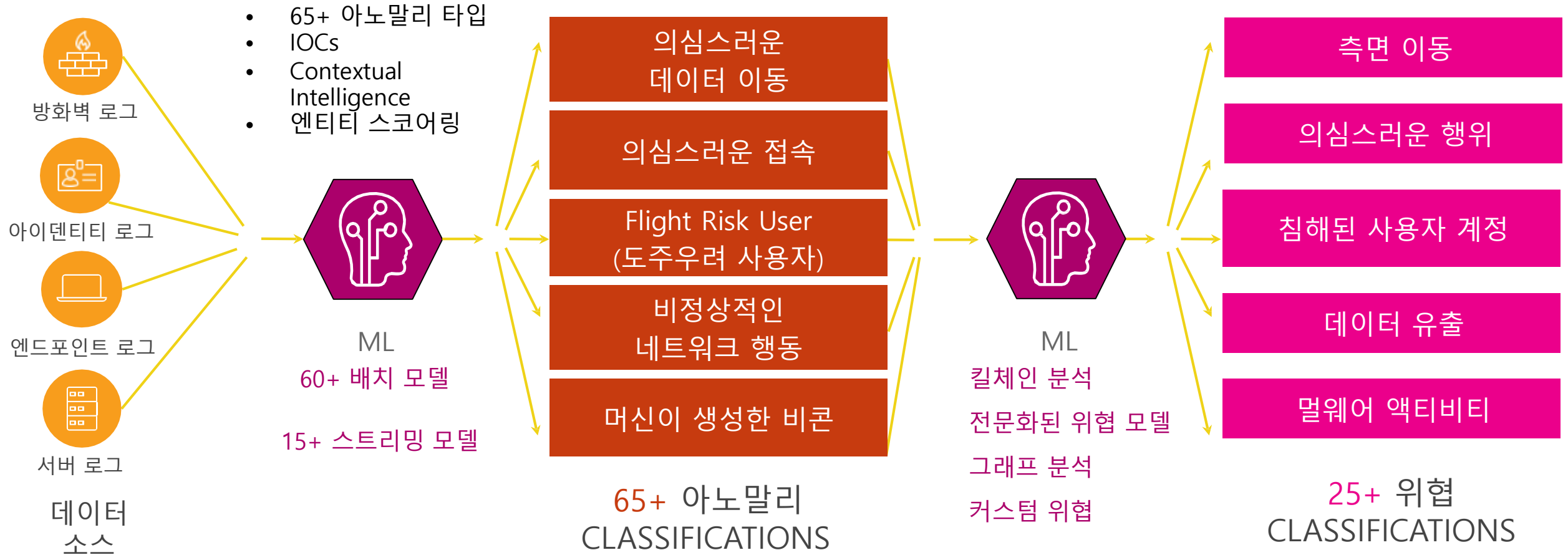


예:

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

AI SecOps 적용하기

Splunk ES + 행위분석(UBA)을 추가하여 성능강화



AI SecOps 적용하기

MLTK를 이용한 알려지지 않은 위협 탐지

머신러닝 워크플로우

단계 1

▶ 데이터 접근 및 불러오기

단계 2

▶ 데이터 전처리 작업

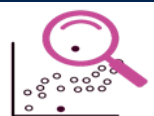

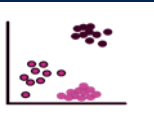
단계 3

▶ 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

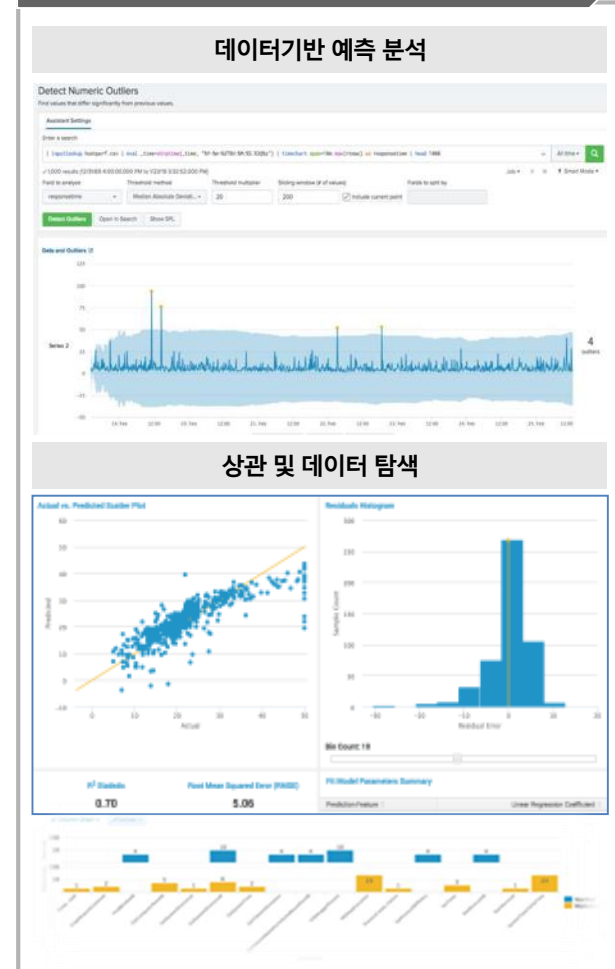
▶ 추출된 특징을 이용해 학습 & 최적의 모델 개발을 위해 반복 작업

Anomaly detection	Predictive Analytics	Clustering
 <ul style="list-style-type: none"> ▶ 과거 행위와의 편차 ▶ (aka 다변량 AD or 응집성 AD) 	 <ul style="list-style-type: none"> ▶ 사용자 이탈 예측 ▶ 이벤트/트렌드 예측 ▶ 실패의 조기 경고 	 <ul style="list-style-type: none"> ▶ 동료 그룹 식별 ▶ 이벤트 상관분석 ▶ 경고 노이즈 감소

단계 5

▶ 최적의 학습된 모델을 통합 시스템에 반영

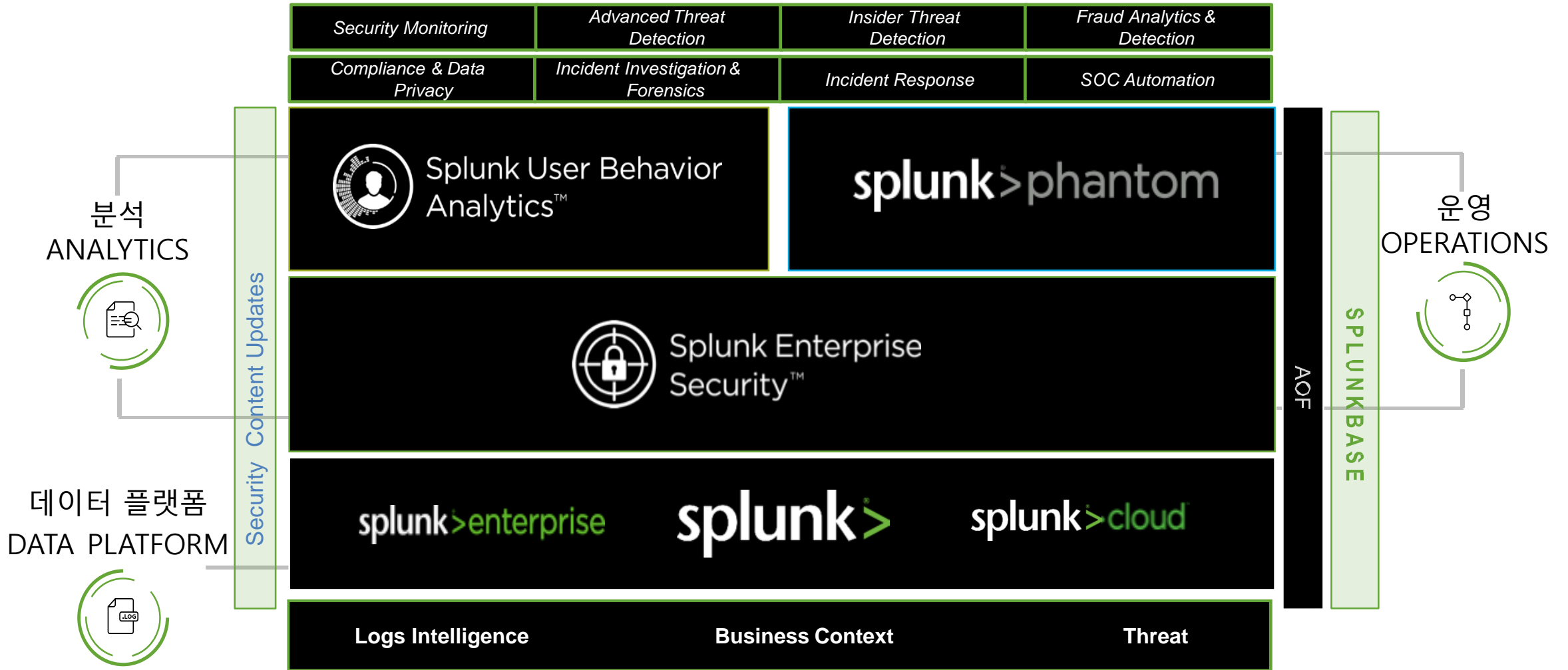
머신러닝 알고리즘(300+)



Splunk 보안 포트폴리오

splunk® > turn data into doing™

Splunk 보안 포트폴리오

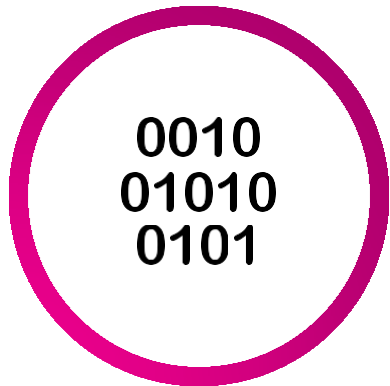


AOF(Adaptive Operations Framework) : 보안 아키텍처는 유기적으로 작동하도록 설계되지 않은 여러 계층의 도구와 제품을 포함하므로 보안팀은 여러 도메인을 연결하여 방어를 코디네이션하는 방법에 차이가 있습니다. AOF는 고객사의 보안 제품 및 기술을 Splunk Enterprise Security 및 Splunk Phantom을 포함한 Splunk 보안 솔루션과 연결하여 이러한 격차를 해결합니다.

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

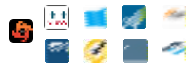
Splunk 보안 포트폴리오

데이터



splunk>cloud
splunk>enterprise

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



분석



Splunk Enterprise Security™

ES 콘텐츠 업데이트

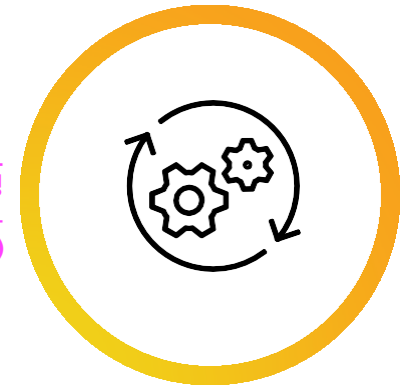


Splunk User Behavior Analytics™



Machine Learning Toolkit (MLTK)

운영



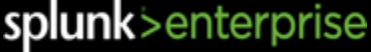


어댑티브 운영 프레임워크 (AOF)



Splunk Enterprise Security™

어댑티브 응답(Adaptive Response)

Splunk 보안 포트폴리오

	 Splunk Enterprise Security™	 Splunk User Behavior Analytics™	
<ul style="list-style-type: none"> • 데이터 수집 및 색인 • 검색 / 조사 / 상관 분석 • 시각화 및 레포트 • 모니터링 및 경고 • 어디서나 저장/액세스(빅데이터 플랫폼) • 애드혹 검색 • 유니버설 저장(형태/크기/속도에 관계없이 빠르게 저장 가능) • 스트림(와이어,네트워크 패킷) 데이터 수집 • 1,000+ 앱 에코시스템 	<ul style="list-style-type: none"> • 이벤트 상관분석 & 노트블(Notble) 프레임워크 • 위험 스코어링 프레임워크 • 인시던트 조사 워크플로우 • 자산 및 ID 프레임워크 • 워크플로우 액션 커스텀정의 • 클래스 테이블(KPI 분석) • 250+ 보안 상관 시나리오/ 대시보드/유즈케이스 • 시퀀스 템플릿 • 어댑티브 대응 액션 • OOTB - 보안 메트릭, 대시보드, 유즈케이스, 분석 스토리 	<ul style="list-style-type: none"> • 딥러닝기반 엔드포인트 행위 분석 • 아노말리 / 알려지지 않은 위협 발견 • 즉시 사용 가능한 분석 • 사용자 위험 평가 및 모니터링 • 통합 위험 시각화 • 킬 체인 뷰 • 커스텀 시나리오 정의 	<ul style="list-style-type: none"> • 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™