SWIMLANE

로우코드(Low-code) 보안 자동화

현재와 미래를 위한 타협 없는 보안 자동화

이영옥 이사

솔루션 엔지니어 APJ

가장 크고 빠르게 성장하는 보안 자동화 전문 회사

고객들은 우리의 비전을 함께합니다!

Homeland Security
AMERICAN EXPRESS
Square
LUMEN
Booking.com
TOSHIBA
Bloomberg
Deloitte.
BMW
U.S. AIR FORCE
COMCAST
ADP

업계에서 인정받는 솔루션

Gartner peerinsights
Gartner
FORRESTER
AWARDS
500 Technology Fast 500 2022 North America Deloitte.
Tech Cares 2022

고객들의 운영결과

95%
경고 볼륨 감소

50%
MTTR 감소

20배
실행 가능성 증가

$160k
평균 월간 절감액

가장 크고 빠르게 성장하는 보안 자동화 전문 회사

모든 팀을 위한 막대한 가치

사이버 보안 책임자

완전한 감독 및 모든 보안 작업에 대한 제어

- 운영 활동, 메트릭 및 KPI의 통합 보기
- 임직원 업무 안정화, 생산성 향상 및 이직률 감소
- 기존 보안 도구 및 기술 투자의 활용도 향상

보안 오케스트레이터

사용하기 쉬운 보안 자동화 및 구성 가능한 보안 워크플로

- 자동화, 사례 관리 및 보고를 위한 단일 플랫폼
- 플레이북 및 앱 개발을 위한 로우(low)코드 스튜디오
- 모든 사이버 보안, IT 및 인프라 도구 통합

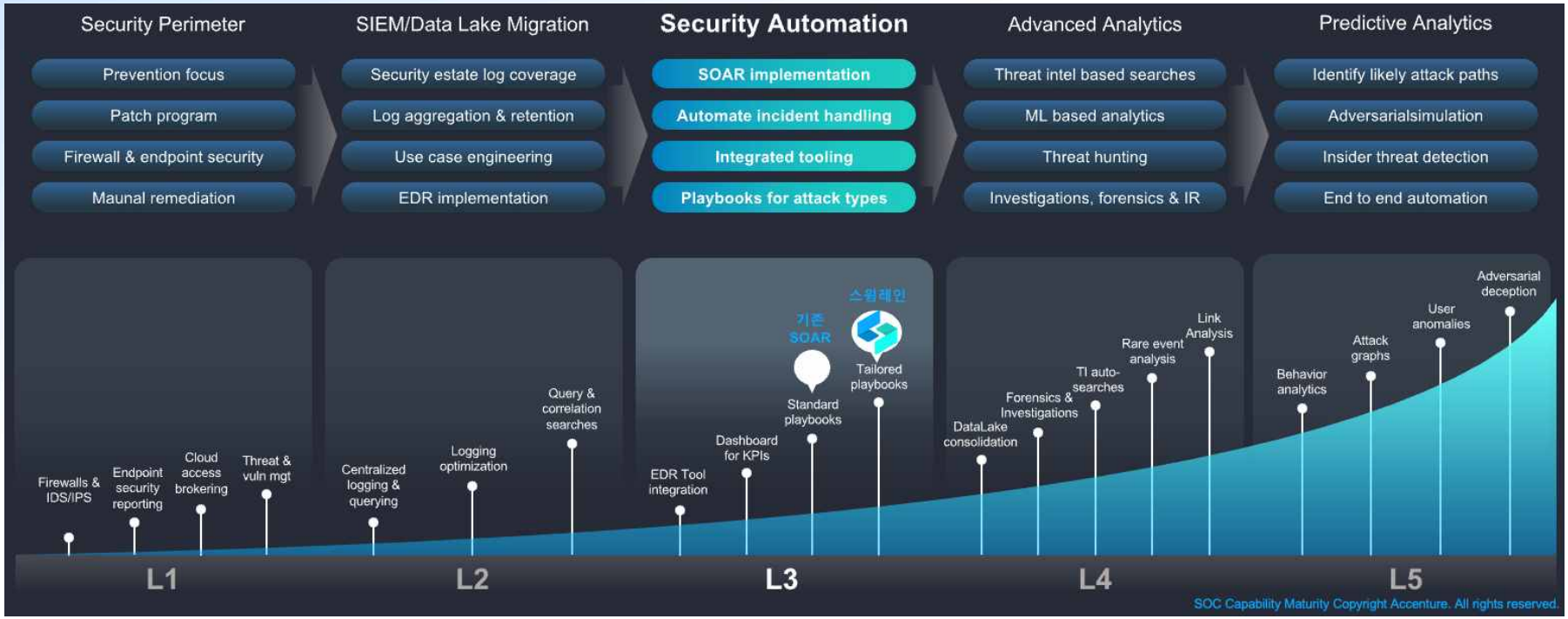
보안 분석가

반복 작업의 중앙화된 가시성 및 자동화

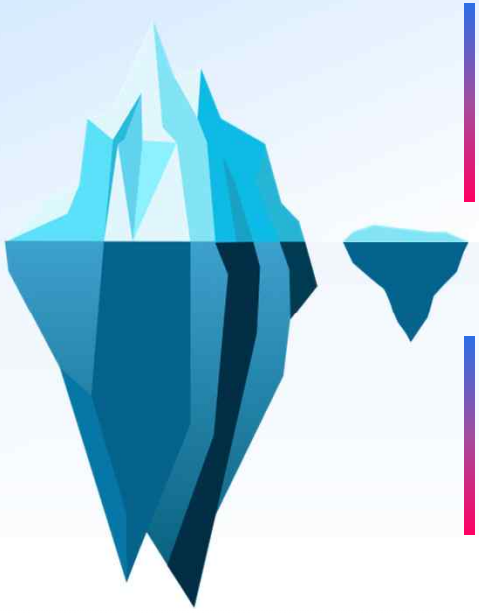
- 수동으로 분석 및 관리되는 보안 경고 감소
- 사례, 알림 및 인텔리전스에 대한 향상된 평균 응답 시간
- 24시간 운영을 지원하는 상시 가상 분석가

보안 성숙도 모델

우리는 현재 L3 (Security Automation)에 진입하고 있음!



빙산의 표면 위와 아래



비즈니스 가치 입증

- ROI 측정의 어려움
- 프로그램 효율성에 대한 제한된 가시성
- CISO 이사회 책임

인재 부족

- 숙련된 노동력 부족
- 경고 피로
- 직원 만족도

위협에 보조를 맞춤

- 증가하는 공격 대상
- 고도로 발전된 위협 행위자
- 무분별한 도구 확산으로 대규모 원격지 이벤트 생성

기술 변화

- 지속적으로 진화하는 솔루션
- 새로운 보안 기술로의 마이그레이션
- 끊임없이 변화하는 벤더 믹스

지속적인 프로세스 개선

- 지속적으로 변화하는 "모범 사례"
- 지속적인 프로세스 변경 추진
- 변화의 속도와 정확성이 중요해짐

이해 관계자 및 사용자 이동

- 보안에 인접한 팀에는 자동화 앱이 필요
- 보안은 사기나 IT 및 인프라에 집중됨
- 사용 사례는 SOC 외부로 확장 필요

스윔레인만이 수면 위와 아래에 기능을 제공

플레이북

벤더 정의 플레이북 및 편집기

- 코드 없는 자동화 플레이북 만들기
- 자동화 논리를 관리하는 시각적 방법
- 플레이북 실행 및 기록 모니터링 기능
- 플레이북 구축 및 테스트를 위한 스튜디오

케이스 관리

사례 관리 및 보고

- 동적 사례 관리, 할당, 에스컬레이션
- 증거 보관함 및 보관
- 보안 및 대역 외 통신
- NIST, MITRE ATT&CK 및 D3FEND 매핑 및 시각화

미리 준비된 연동

표준 보안 연동

- 모든 상용 도구에 대한 새로운 연동 비용 없음
- 공통 보안 도구에 사전 구축된 연동
- 연동을 추가, 수정 및 확장하는 기능

쉬운 연동

모든 도구 및 시스템에 즉각 연동

- Rest API에 실시간으로 연결하는 기능
- 새로운 데이터에 액세스하거나 새로운 조치를 취하는데 대기 시간이 없음
- IT 및 DevOps에 대한 자동화의 광범위한 적용 가능성

설정 가능한 사용자 경험

마켓플레이스가 있는 로우 코드 어플리케이션 스튜디오

- 사기, 감사 등과 같은 비 SOC 사용자를 위한 랜딩 페이지
- 학습 및 승인을 위한 사용자 루프 자동화
- 클릭 한 번으로 배포하여 UI 및 UX 사용자 지정, 개선 및 조정
- 단순한 사용 사례와 복잡한 사용 사례를 모두 빠르게 배포

활성 감지 패브릭

이벤트 소스에 대한 가시성 확보

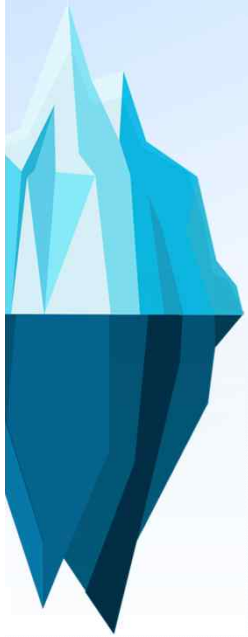
- 그룹, 팀, 임원 및 개인을 위한 대시보드
- 내보내기 및 엑셀 없이 실시간 보고 작성
- 정보를 빠르게 드릴다운, 필터링 및 얻을 수 있는 기능
- 원터치로 생성되는 드래그 앤 드롭 대시보드

셀프 서비스 비즈니스 인텔

설정 가능한 대시보드 및 보고서

- 대규모 원시 원격 이벤트를 수집 및 분석하고 즉각적인 대응을 수행
- 멀티 및 하이브리드 클라우드 원격 측정 가시성
- 풀 리퀘스트, 게시/구독 및 웹후크와 같은 소스에 연결

스윔레인 터바인과 경쟁 솔루션 비교



기본 자동화

고도의 적응력

플랫폼 기능		SWIMLANE	레거시 SOAR Google paloalto splunk>	노코드 torq tines
플레이북	벤더 정의 플레이북 및 편집기	●	●	●
케이스 관리	사례 관리 및 보고	●	●	◔
미리 준비된 연동	표준 보안 통합	●	●	●
쉬운 연동	모든 도구와 시스템에 즉시 연결	◔	◔	◔
구성 가능한 사용자 경험	마켓플레이스가 있는 로우코드 어플리케이션 스튜디오	●	◔	◔
셀프 서비스 비즈니스 인텔	설정 가능한 대시보드 및 보고서	●	●	◔
활성 감지 패브릭	이벤트 소스에 대한 가시성 확보	◔	◔	◔

차별화가 기업과 조직에 제공하는 것

피싱

인텔 조회

경고 관리

인텔 관리

관리형 탐지 및 대응

Deloitte.

취약점 관리

TOSHIBA

컴플라이언스 지원

U.S. Citizenship and Immigration Services

클라우드 보안

Booking.com

위협 사냥

Bitdefender

OT위협 대응

OG&E

감사 자동화

incomm payments

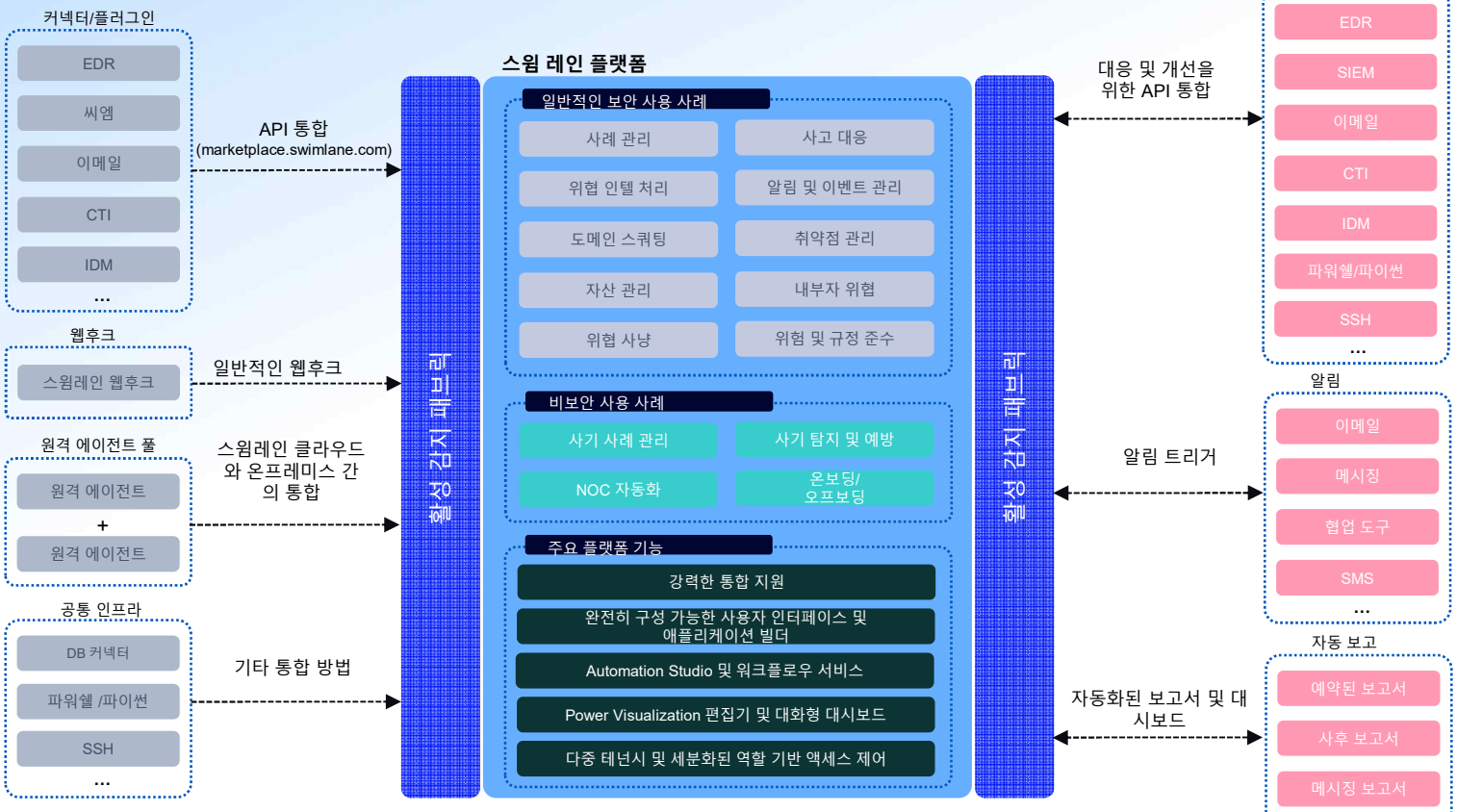
사기 방지

ADP

ID 프로비저닝

Booz | Allen | Hamilton

스윔레인 플랫폼 프레임워크



스윔레인 배포 모델

스윔 레인 클라우드 (SaaS)

- ☑ 미국, 영국 및 EU, 싱가포르 및 호주
- ☑ 데이터 복원력을 통한 고가용성
- ☑ 관리형 인프라 및 소프트웨어 업데이트

하이브리드

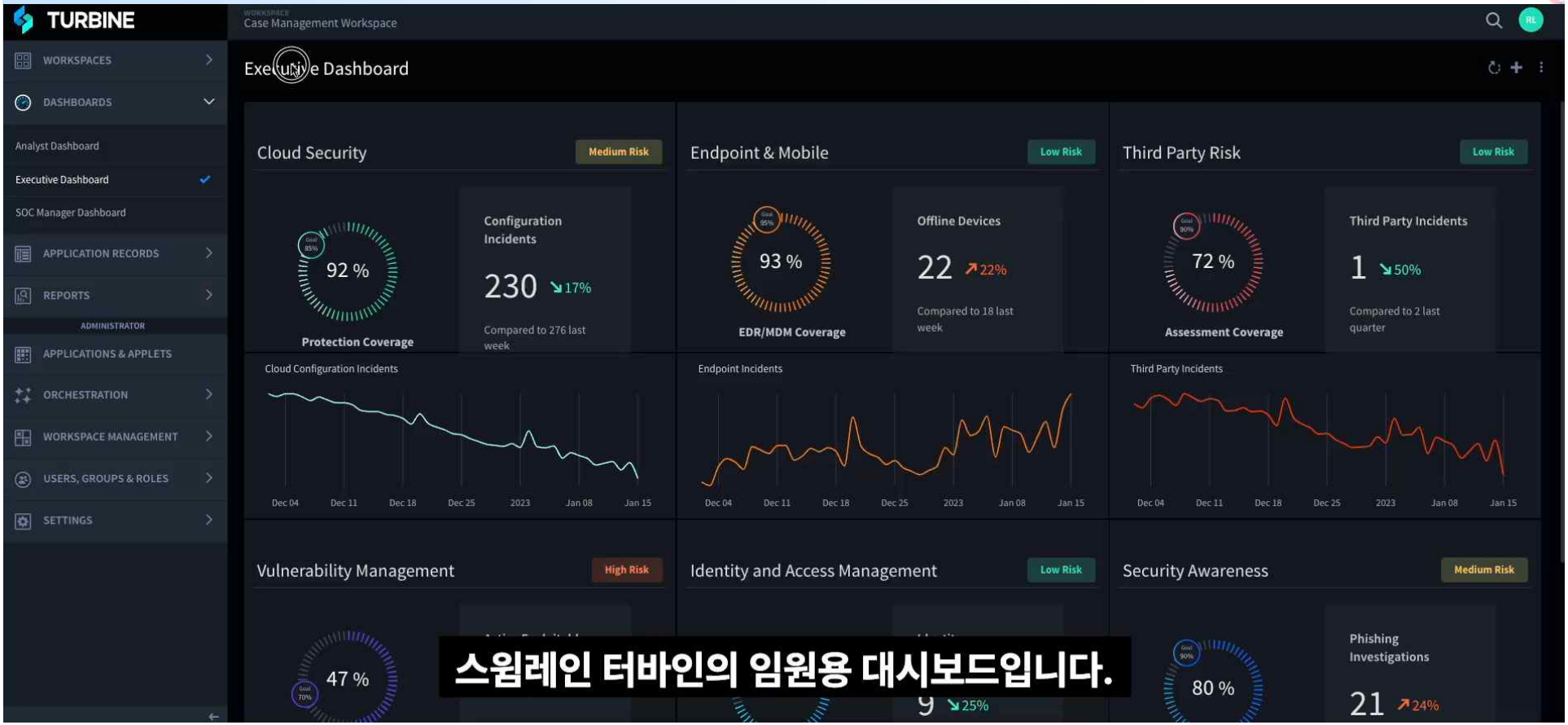
- ☑ 유연한 인프라 설정
- ☑ 클라우드, 프라이빗 클라우드 또는 온프레미스 환경 통합
- ☑ 원격 에이전트를 사용하여 자동화된 대응 작업 확장

온프레미스

- ☑ 권장 사이징이 포함된 간단한 설치 패키지
- ☑ 선호하는 Linux OS를 선택
- ☑ "에어갭(오프라인)" 환경 지원

AWS Marketplace를 통해 직접 거래 가능

스윔레인의 터바인 데모


TURBINE
WORKSPACE
Case Management Workspace
WORKSPACES
DASHBOARDS
Analyst Dashboard
Executive Dashboard
SOC Manager Dashboard
APPLICATION RECORDS
REPORTS
ADMINISTRATOR
APPLICATIONS & APPLETS
ORCHESTRATION
WORKSPACE MANAGEMENT
USERS, GROUPS & ROLES
SETTINGS
Executive Dashboard
Cloud Security
Medium Risk
92 %
Protection Coverage
Configuration Incidents
230 ↘17%
Compared to 276 last week
Endpoint & Mobile
Low Risk
93 %
EDR/MDM Coverage
Offline Devices
22 ↗22%
Compared to 18 last week
Third Party Risk
Low Risk
72 %
Assessment Coverage
Third Party Incidents
1 ↘50%
Compared to 2 last quarter
Cloud Configuration Incidents
Endpoint Incidents
Third Party Incidents
Dec 04
Dec 11
Dec 18
Dec 25
2023
Jan 08
Jan 15
Vulnerability Management
High Risk
47 %
Identity and Access Management
Low Risk
↘25%
Security Awareness
Medium Risk
80 %
Phishing Investigations
21 ↗24%
스윔레인 터바인의 임원용 대시보드입니다.

고객 성공을 보장하기 위한 검증된 방법론

가치 증명 프로세스

고객의 환경에서 스윔레인의 가치를 신속하게 입증하기 위한 오랜 시간 동안 입증된 테스트 프로세스 및 방법론

ROI 계산자

비즈니스 운영, 효율성 및 응답 시간에 대한 스윔레인의 영향을 자동으로 정량화

우선 순위 고객 성공

스윔레인의 모든 전문 지식, 고객 성공, Pro Serv, 기술 지원, 교육 등

오토메이션 성숙도 모델

통찰력 기반 권장 사항은 비즈니스에 대한 고가치 사용 사례를 식별하는 데 도움이 됨

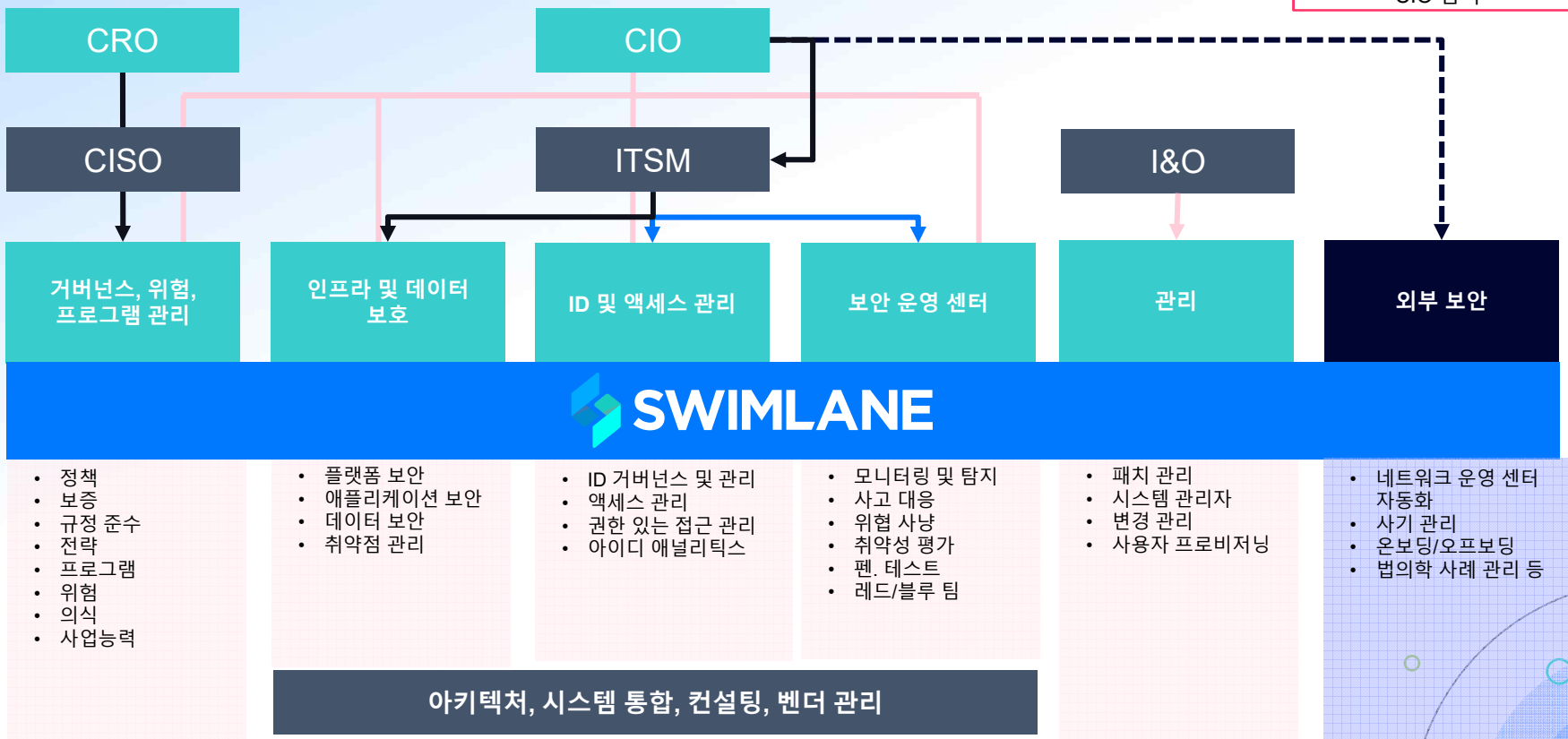
빠른 시작 마이그레이션 서비스

사전 번들 자동화 솔루션으로 가치 실현 시간 단축

교육 및 인증

자기주도 교육 프로그램은 자동화 기술과 전문성을 최대화하는 데 도움이 됨

보안 조직 모델 참조 및 그 이상



Gartner의 중앙 집중식 보안 조직 모델에서 채택 | ID:381600

지속적인 프로세스 - 스윔레인의 고객 자동화 고도화 모델

자동화 준비 상태 평가

- ✓ SAMM(스윔레인 자동화 성숙도 모델)에 대해 잠재 고객을 매핑하고 성숙 과정의 기준선을 설정하기 위한 주요 입력을 캡처하기 위한 예비 평가
- ✓ 규모, 회전율, 보안팀이 설정한 목표 프로필을 충족하는 고객/잠재 고객을 매핑하고 우선 순위를 지정할 수 있음
- ✓ 준비성 평가 결과와 가장 잘 일치하는 SAMM의 모든 필수 요소를 달성하기 위해 고객/잠재 고객을 지원/활성화하는 데 필요한 주요 초점 영역을 조기에 식별

- ➢ SAMM은 SAMM 인덱스와 비교하여 고객의 현재 성숙도를 평가하기 위한 명확한 개요와 주요 지침을 통해 성숙도의 4가지 핵심 요소에 중점을 둡니다.
- ➢ 평가 결과를 통해 스윔레인은 고객 조직 에 대해 의도한 비즈니스 결과를 달성하기 위해 자동화 로드맵을 상향 조정하기 위한 적절한 수준의 지침/지원을 제공할 수 있습니다.

- ➢ Use Case Map은 목표 결과 및 고객 가치 창출 시간에 따라 특정 사용 사례에 대한 성숙도 수준을 기반으로 특정 고객에게 무엇을 포지셔닝할지 영업팀을 안내하는 주요 기준을 설명합니다.
- ➢ 이것은 차례로 고객의 사용 사례가 성장함에 따라 오른쪽으로 이동하는 고객의 성숙도 수준에 영향을 미칩니다.

1 자동화 준비 상태 평가

잠재 고객 대상

01

기술/도구

기존 SOC 기능의 도구 및 기술 평가

02

사람

리소스의 스킬셋 및 기능에 대한 이해

03

프로세스

문서화된 프로세스 및 제어의 가용성

04

자동화 검토

현재 구현되어 있는 자동화 수준

2 스윔레인 자동화 성숙도 모델

	레벨 1	레벨 2	레벨 3	레벨 4	레벨 5
	기본 가시성 *학습*	**풍부한 가시성** *맥락화*	**자동화된 대응** *신속한 반응*	**자동화된 예방** *사전 예방적인*	**고급 자동화 운영** *확장*
사업 목표 *운영 결과*	• 경고에 대한 가시성 통합 • 케이스 및 알림 볼륨과 추세에 대한 통찰력 향상 • 사례 및 경고의 기록 추적 및 감사 기능 추가 • 가시성 격차 및 피드백 루프에 대한 이해 제공	• 사례 및 경고에 대한 컨텍스트 개선 • 자동화된 응답을 위한 모델에 대한 신뢰 구축 • 조직별 위협 패턴 및 인텔 선별 • 반복적인 개선 피드백 루프 구축	• MTTR 감소 • 부서 간 협업 확대 • 경고 및 사례당 노력 감소 • 반복 피드백 루프 강화 및 가속화	• 보안 원격 측정 가시성 및 실행 가능성 확장 • 인프라에 남겨진 가시성 및 대응 능력 전환 • 위협 수명 주기의 초기 단계로 탐지 및 대응 이동	• 자동화 기능을 인접한 보안 기능으로 확장 • 자가 치유/적응형 방어에 접근하기 위해 피드백 루프에 가속화
기술 *일반적인 사용 사례 및 도구*	• 자동화된 사례 생성, 알림 및 에스컬레이션을 통한 경고 추적 • 이메일/피싱, SIEM, EDR, NDR, CWP 및 기타 충실도가 높은 경고 소스	• 경보 강화 및 기본 조정 피드백, 경보 및 사례 상관 관계 포함 • 위협 인텔 플랫폼, 위협 인텔 피드, 디렉터리 서비스, CMDB, 샌드박스, DLP	• 강력한 튜닝 피드백을 통한 부분적으로 자동화된 사례 및 경고 응답 • IDP, FW/IDS 관리자, Slack/Teams, Jira	• 강력한 자동 사례 및 경보 응답, 최적화된 튜닝 피드백, 향상된 선제적 위협 감지 • 웹후크, 챗봇, Git, IaaS, APM	• SecOps를 넘어 보안 자동화의 확장된 사용 • 사기 탐지, 애플리케이션 보안
사람들 *자동화 기술 개발*	• SecOps 자동화 플랫폼 및 해당 기능에 대한 기본적인 이해	• 일반적인 사용 사례와 관련된 애플리케이션 아키텍처에 대한 충분한 이해와 함께 SecOps 자동화 플랫폼에 대한 중간 이해	• 공통 사용 사례와 관련된 SecOps 자동화 플랫폼, 아키텍처 및 기능에 대한 강력한 이해	• 일반적인 사용 사례를 넘어 확장할 수 있는 SecOps 자동화 플랫폼, 아키텍처 및 기능에 대한 강력한 이해	• SecOps 자동화 플랫폼, 아키텍처 및 처음부터 사용 사례를 구축할 수 있는 기능에 대한 강력한 이해
프로세스 *거버넌스 프레임워크*	• 최소한의 구조화된 제어가 포함된 기본 프로세스 및 절차	• 기본 거버넌스 및 위험 관리 정책 및 절차	• 조직 전체의 프로세스 및 정책이지만 최소한의 검증	• 명확한 검증 및 측정 프로세스를 갖춘 강력한 조직 전반의 프로세스 및 정책	• 예방 및 예측 프로세스를 갖춘 성숙한 조직 전체 프로세스 및 정책

3 사용 사례 맵

제안된 구조 – 개발을 위해 PS 조직의 지원 필요

사업 가치
사용 사례의 예상 결과는 무엇입니까 ?

스윔레인 SSP
사용 가능한 협회 OOB SSP는 무엇입니까?

플러그인/커넥터 가용성
현재 지원되는 기술 및 버전?

구현 노력 수준
스윔레인을 구현하려면 어떤 유형의 패키지를 제공해야 합니까?

보안 도구
구현과 관련된 보안 도구는 무엇입니까?

필수 스킬셋
구현하려면 어떤 수준의 기술이 필요합니까?

가치 창출 시간
사용 사례를 구현하는데 걸리는 시간

자동화 대상
자동화의 예상 %는 달성될 것입니까?

4 자동화 성숙도 모델 적용 (기본 단계)

안녕하세요, 방금 자동화를 탐구하기 시작했습니다. SOAR 솔루션을 사용할 준비가 되었는지 어떻게 알 수 있습니까?

1

자동화 준비 상태 평가

점수: 1.55

기술/도구: 1.50
사람: 1.67
프로세스: 1.55

+

고객의 요구 사항 평가

2

준비 점수를 SAMM에 매핑하고 성숙도 기준을 충족하기 위한 요구 사항 식별

Level 1

Base Visibility

레벨 1을 달성하기 위해 식별된 요구 사항

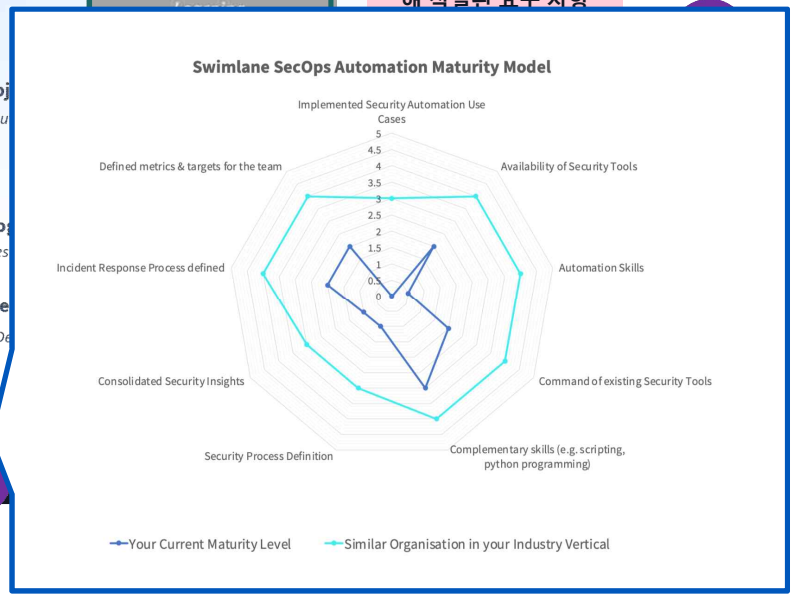
Business Obj
Operational Ou

Technolog
Typical Use Cases

People
Automation Skills De

Proce
Governance F

3



대상 비즈니스 가치에 따른 활용 사례 매핑

- ☑ 확인된 사용 사례
- ☑ 사용 가능한 SSP/커넥터
- ☑ 관련 기술
- ☑ 필수 스킬셋
- ☑ 노력 수준
- ☑ 가치 창출 시간
- ☑ 자동화 대상

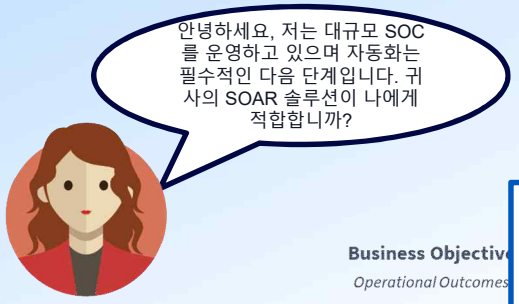
적절한 활용사례 제안

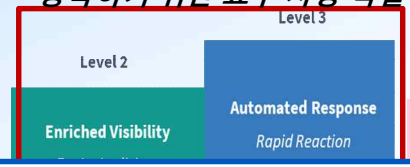
반복 프로세스

구현 > 성숙도 매핑 > 성장을 위한 경로 제안(사람/프로세스/기술/ 활용사례)

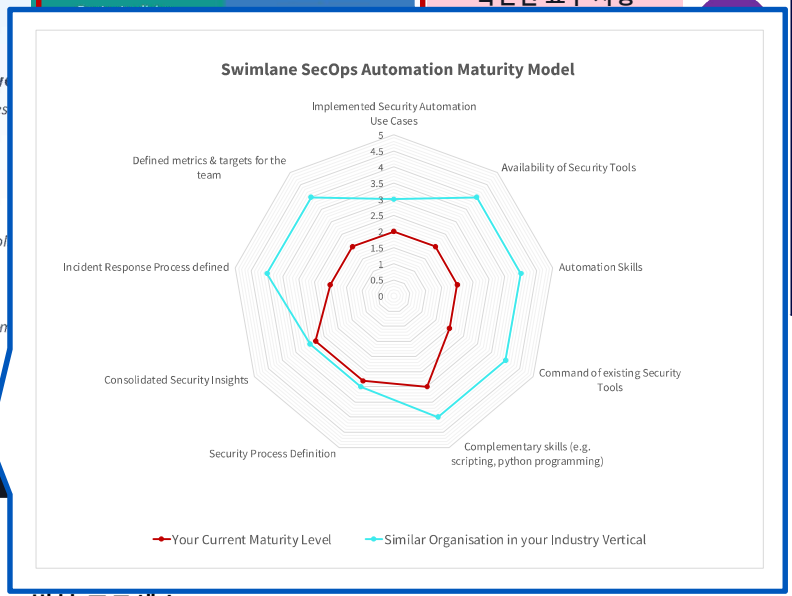
4 자동화 성숙도 모델 적용 (중간 단계)

준비 점수를 SAMM에 매핑하고 성숙도 기준을 충족하기 위한 요구 사항 식별





레벨 3 달성을 위한 확인된 요구 사항



대상 비즈니스 가치에 따른 활용 사례 매핑

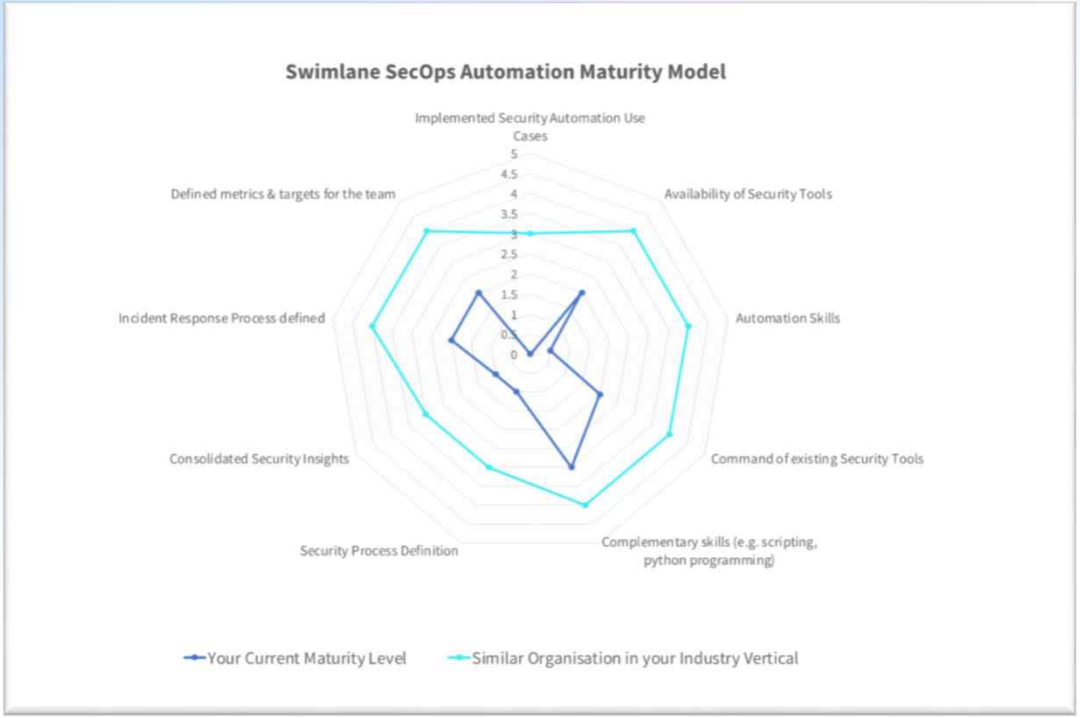
- ☑ 확인된 사용 사례
- ☑ 사용 가능한 SSP/커넥터
- ☑ 관련 기술
- ☑ 필수 스킬셋
- ☑ 노력 수준
- ☑ 가치 창출 시간
- ☑ 자동화 대상

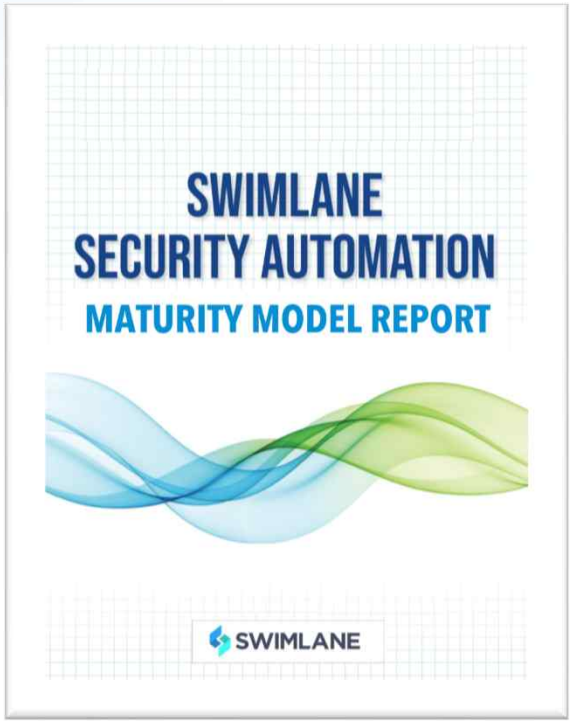
적절한 활용사례 제안

반복 프로세스

구현 > 성숙도 매핑 > 성장을 위한 경로 제안(사람/프로세스/기술/ 활용사례)

5 스윔레인 자동화 성숙도 모델 참여





Open Cybersecurity Schema Framework

https://schema.ocsf.io/

THANK YOU

https://tubine-demo.pov.us-east-1.swimlane.io/