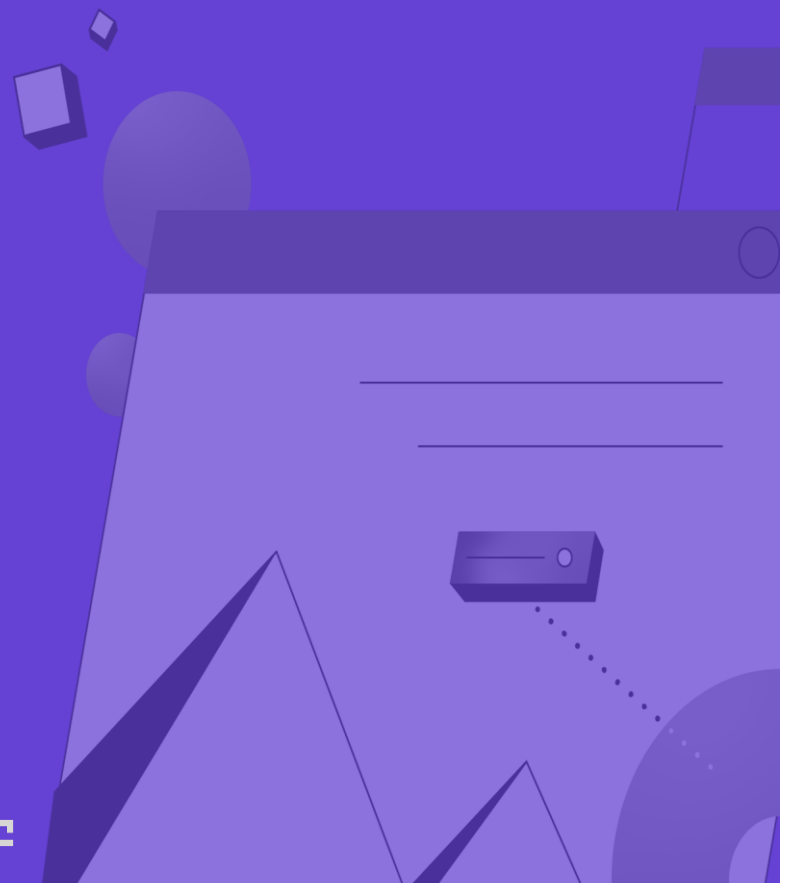
ATTACKIQ

AttackIQ Flex

BAS(Breach & Attack Simulation) test-as-a-service

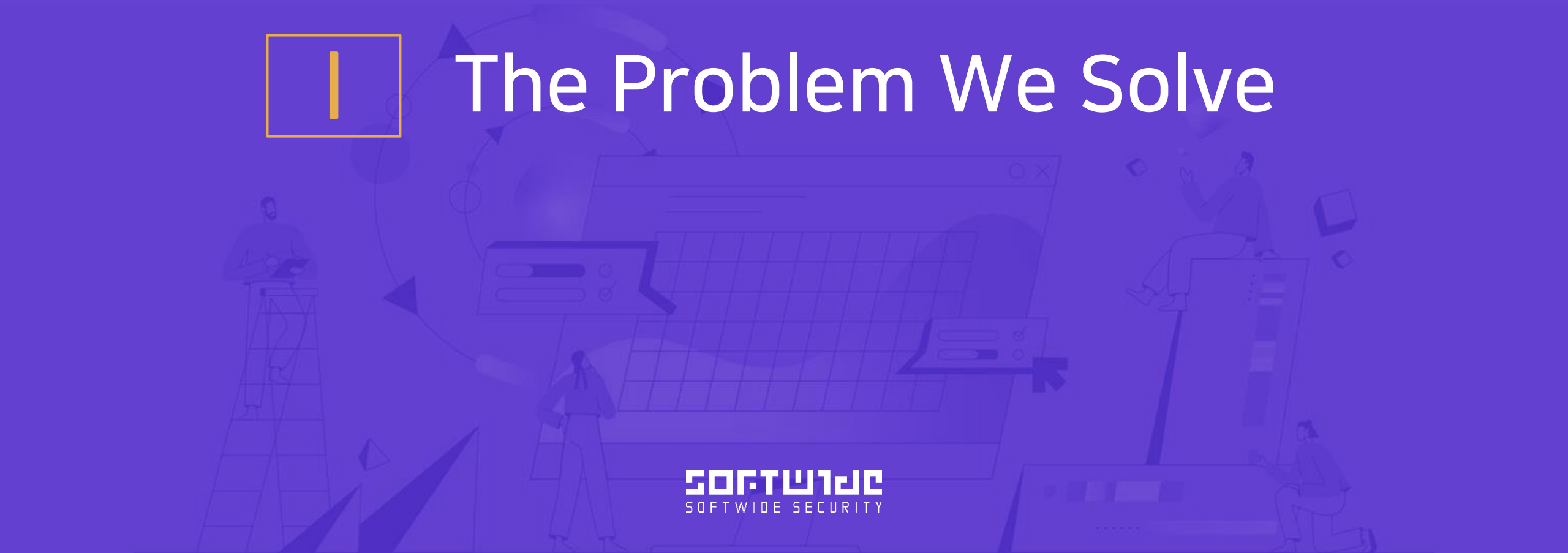
SOFTWIDE SECURITY

Index



ATTACKIQ

I The Problem We Solve



SOFTWIDE SECURITY

Here's What We Know

보안 프로그램의 유효성을
어떻게 측정할 수 있을까요?

You can do it.
or
The adversary can do it.

Be *Ready!*
Get *Flexed!*

1. 보안 제어는 오직 평균 39%의 시간 동안 최고의 공격 기술만을 차단합니다.
2. 82%의 침해에서, 위협을 막기 위한 보안 제어가 마련되어 있었지만 실패했습니다.
3. 모든 데이터 침해의 85%는 인적 오류의 일부 요소와 관련이 있습니다.
4. 최근 설문 조사에 따르면 70% 이상의 고객이 최소 25% 이상의 제어 기능이 제대로 작동하지 않는다고 응답했습니다.

진화하는 보안 시장

진화하는 보안 시장은 …

1. 보안 구매자는 단순히 "최고의" 보안 제어를 구입하고 구현하는 것에서 벗어나 기존 보안 제어의 효율성을 평가하는 패러다임으로 나아갈 준비가 되어 있습니다.

2. 광범위하게 분산된 기업 환경에서 보안 제어의 효율성을 테스트하려면 확장성이 뛰어난 개방형 플랫폼이 필요합니다.

3. 보안 프로그램에서 결과 최적화 및 테스트 자동화의 필요성을 인식하고 있음에도 불구하고 일부 고객은 공격 에뮬레이션 및 제어 테스트 프로그램을 독립적으로 채택할 수 없습니다.

… 큰 기회를 창출했습니다

보안 실무자들은 단순히 시간을 투자한다고 위협 환경(특히 예산이 제한된 환경)에서 벗어날 수 있는 것이 아니라는 것을 알고 있습니다.

AttackIQ는 경량 에이전트 아키텍처부터 API 우선 접근 방식까지 보안 제어 효율성을 평가하기 위한 유일하게 확장 가능한 개방형 플랫폼을 구축했습니다.

AttackIQ는 특히 중견 시장의 기술 부족과 리소스 제약을 해결하기 위해 소프트웨어를 활용하는 관리형 BAS 제품을 통해 플랫폼을 서비스 중심으로 조정했습니다.

보안 테스트의 어려움

비용

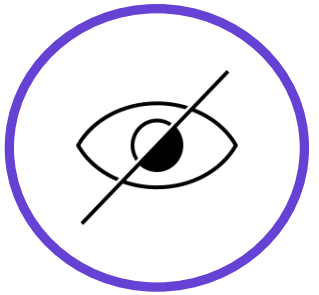
많은 조직에서는 전체 BAS 솔루션을 위한 예산이 없지만 소규모로 엔터프라이즈급 혜택을 원합니다.[1]

빠른 처리 요구 사항

조직은 평가를 수행하는 데 몇 주가 걸리지 않고 특정 자산이나 공격 표면이 취약한지 즉시 파악하기를 원합니다.[2]

복잡성 및 기술 격차 테스트

조직에는 테스트를 실행할 전문 지식이 부족하며, 동시에 레드 팀 구성은 고통스러울 정도로 침해적이고 과잉이며 집중적인 온보딩이 필요합니다.



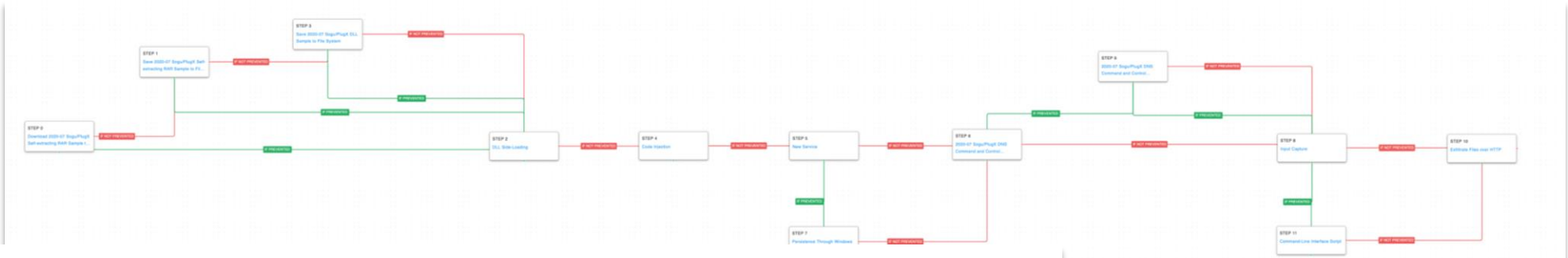
가시성 부족

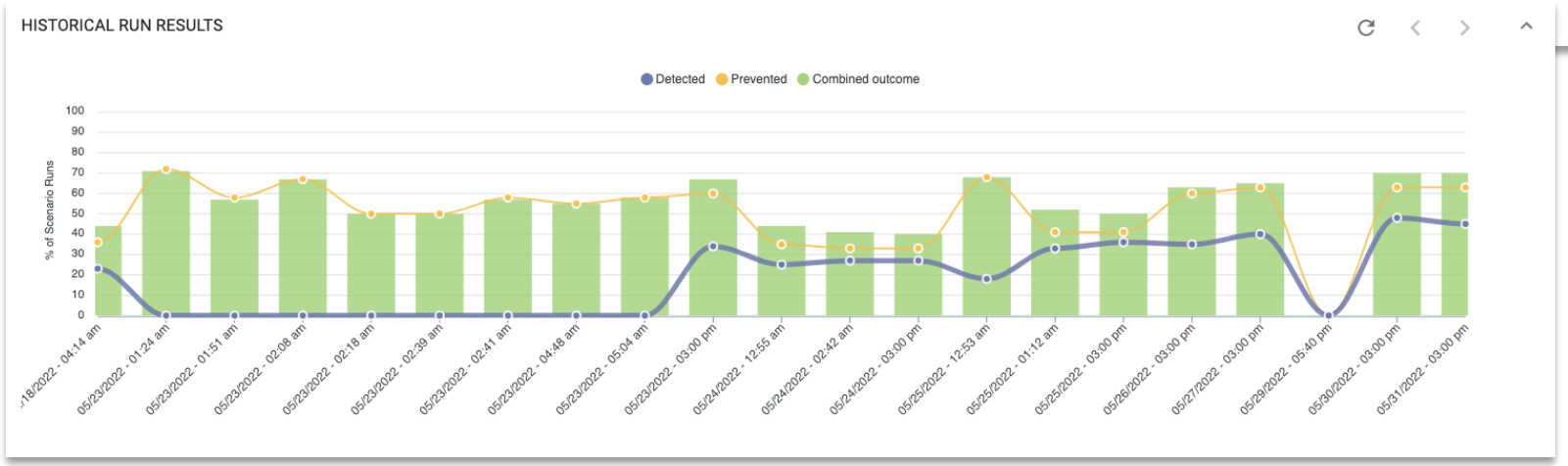
Air-Gapped 네트워크, M&A 활동 중 또는 네트워킹 자산이 제3자에 의해 관리되어 발견되지 않은 제어 오류가 있는 경우와 같이 에이전트를 배포하기 어려운 경우 테스트는 비실용적일 수 있습니다.

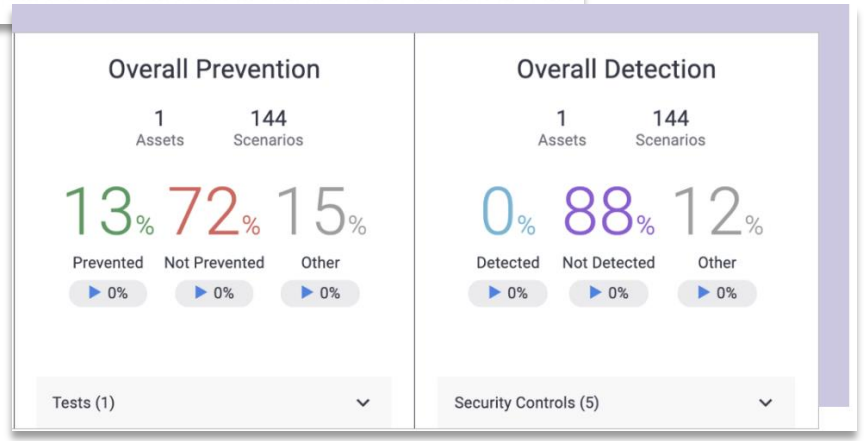
[1] 레드팀의 평균 비용은 단일 소규모 범위 계약의 경우 25,000달러부터 단일 테스트의 경우 40,000달러에서 120,000달러까지 다양합니다. Mandiant와 Palo Alto Networks의 데이터를 기반으로 합니다.
[2] 고객의 일화적(Anecdotal)인 증거

위협 정보 기반 방어 사고방식 채택

보안 팀은 규정 준수 목록의 측면에서 생각하는 대신,
실제 보안 결과(그래프 및 지표) **측면에서 생각해야 합니다.**



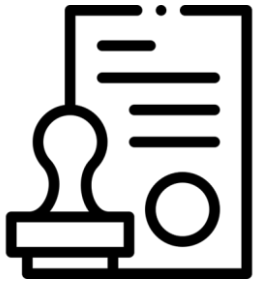




효과적인 엔터프라이즈 보안의 미래

Cyber-Insurance

- 사이버 보험 시장의 **가치는 100억 달러로** 2022년부터 2029년까지 **연평균 성장률(CAGR)이 26%로 예측됩니다.** (1)
- 고객은 BAS를 사용하여 보안 제어를 검증하고 공급자에 대한 위험을 완화하여, **궁극적으로 사이버 보험의 보험료를 절감하고 있습니다.**
- 보험사에서는 **제어 테스트를 요구할 것으로 예상됩니다**.



Regulatory Requirements

- EU가 새로 비준한 DORA(Digital Operational Resilience Act)는 **기업이** 2025년 1월까지 **디지털 운영 탄력성 테스트에 참여하도록 규정하고 있습니다**.
- **미국 정부는 MITRE ATT&CK 프레임워크를 사용하여 위협 테스트를 자동화할 것을 강력히 권장하며** 앞으로도 유사한 명령을 구현할 것으로 예상됩니다.

Optimization & Automation

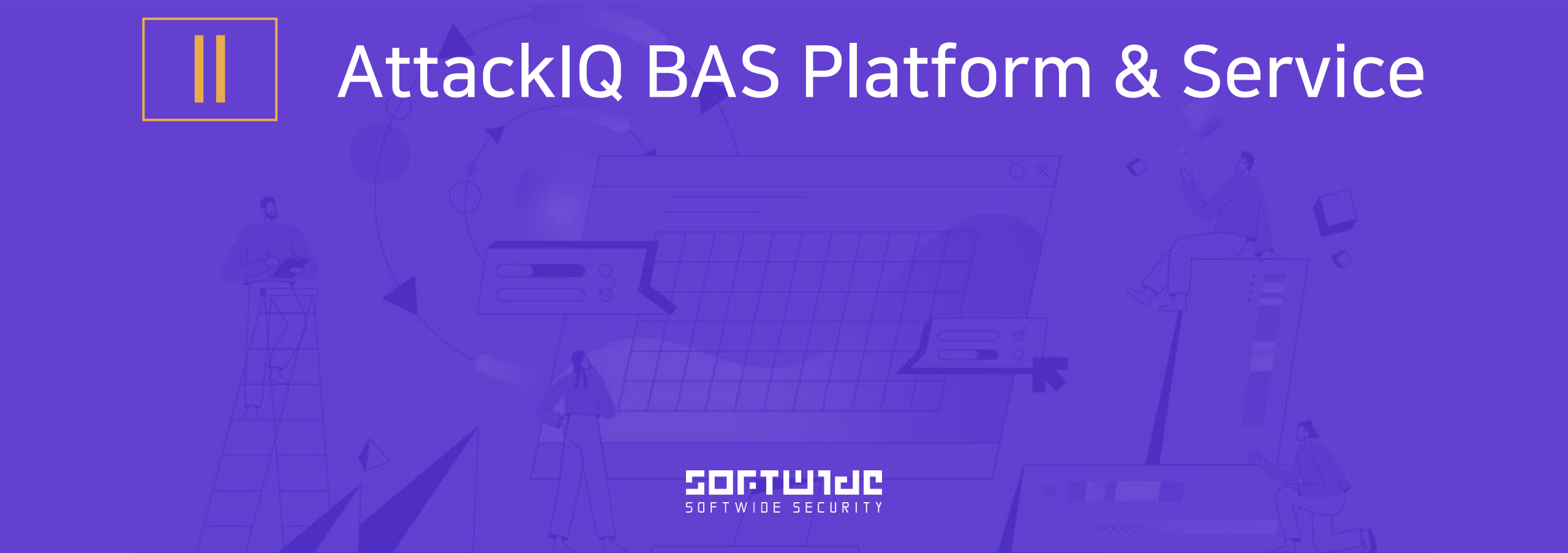
- BAS는 **보안 제어 지출에서 보안 결과 입증으로** 예상되는 패러다임 전환을 가능하게 합니다.
- 보안 예산이 압박을 받고 있는 상황에서 CISO는 BAS 평가를 활용하여 경영진에게 **기존 제어** 및 신규 조달**에 대한 책임을 보여주고 효율성을 입증**할 수 있습니다.

(1) Fortune Business Insights, 사이버 보험 시장

ATTACKIQ

II

AttackIQ BAS Platform & Service



SOFTWIDE SECURITY

BAS(Breach & Attack Simulation)

Gartner

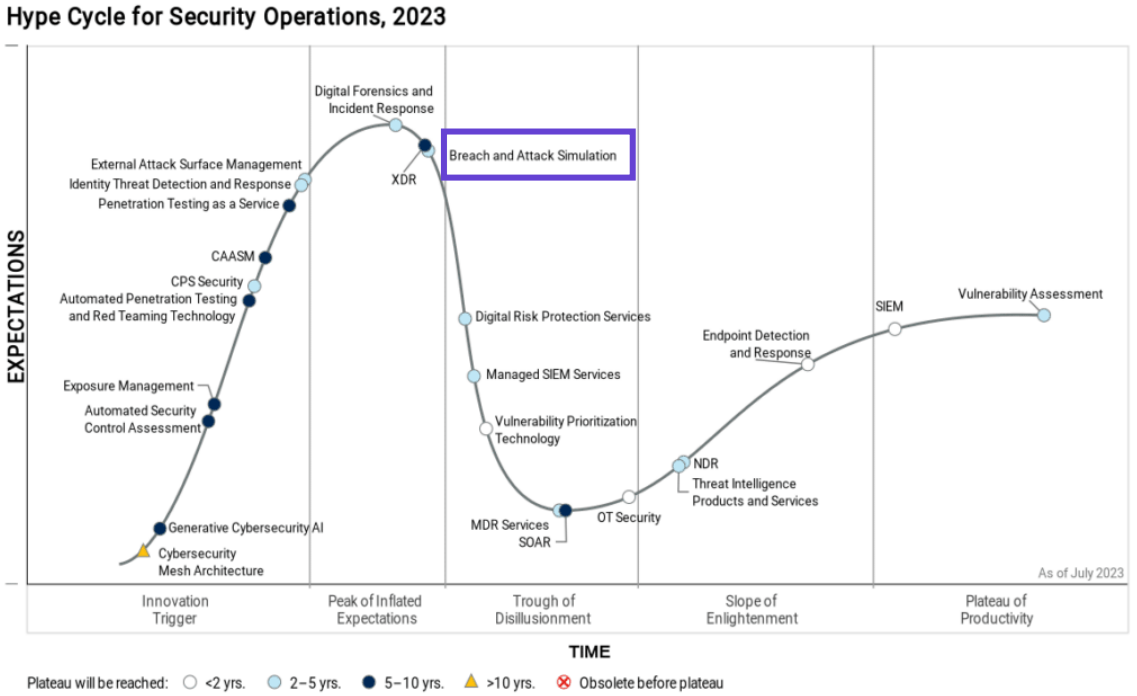
BAS(breach & attack simulation)란?

소프트웨어 에이전트, 가상 머신 및 기타 수단을 사용하여 엔터프라이즈 인프라에 대한 전체 공격주기(내부 위협, 측면 이동 및 데이터 유출 포함)를 지속적이고 일관되게 시뮬레이션 할 수 있는 툴

- BAS(Breach & Attack Simulation) - 사이버 방어가 의도한대로 작동하는지 테스트하고 검증하기 위해 적의 행동 에뮬레이션

Gartner calls BAS a
"Top Security and Risk Management Trend"

- 2022-23년 Gartner Hype Cycle for Security Operations - peak of inflated expectations
- 2021년 Gartner Top Security and Risk Management Trends 포함
- 2017년 Gartner Hype Cycle Threat-Facing Technologies - Innovation Trigger



AttackIQ BAS 플랫폼

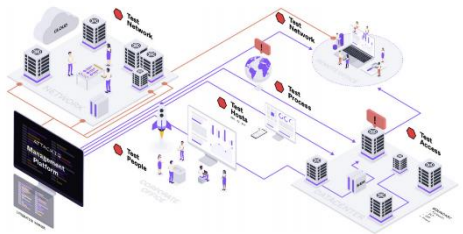
- MITRE ATT&CK Matrix 기반의 BAS(Breach & Attack Simulation) 플랫폼

#1

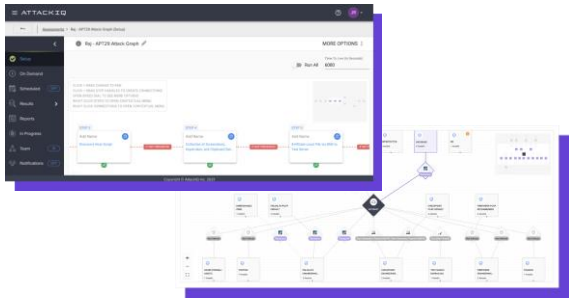
in Breach & Attack Simulation

ATTACKIQ

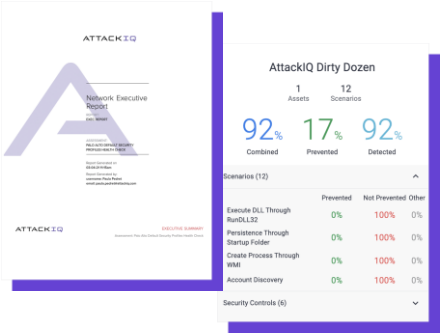
MITRE ATT&CK 기반으로 정의된 공격자 시나리오를 통하여 보안 솔루션의 효율성과 공격 형태에 따른 전술을 시뮬레이션 하여 실제로 공격이 발생하기 이전에 문제점을 스스로 진단하고 대응할 수 있도록 해주는 플랫폼



Deploy Test Point



Run Scenarios



Review Results

AttackIQ BAS 서비스

- 조직의 규모, 예산, 필수 요건에 따라 선택할 수 있는 BAS(Breach & Attack Simulation) 서비스

AttackIQ Flex

직접 신속한 테스트가 필요한 조직을
위한 온디맨드, 에이전트리스
서비스형 테스트

Self Service
Validation you run on your own

AttackIQ Ready!

보안 검증 수행 인력이 부족하거나
정기적인 테스트가 필요한 조직을 위한
BAS 서비스

Full Service
Validation we run for you

AttackIQ Enterprise

언제든지 보안 제어를 테스트하고
AttackIQ의 전체 기능 활용이 가능한
고객 관리형 BAS 서비스

Customer Managed
Validation we run with you

AttackIQ BAS 서비스

Continuous Security Validation

보안 제어의 효율성을 정기적으로 테스트하고 검증하여 원하는 수준의 보호를 제공하는지 확인합니다. 여기에는 위험을 사전에 완화하고 사이버 보안 탄력성을 강화하기 위해 취약성을 모니터링, 평가 및 해결하는 작업이 포함됩니다.

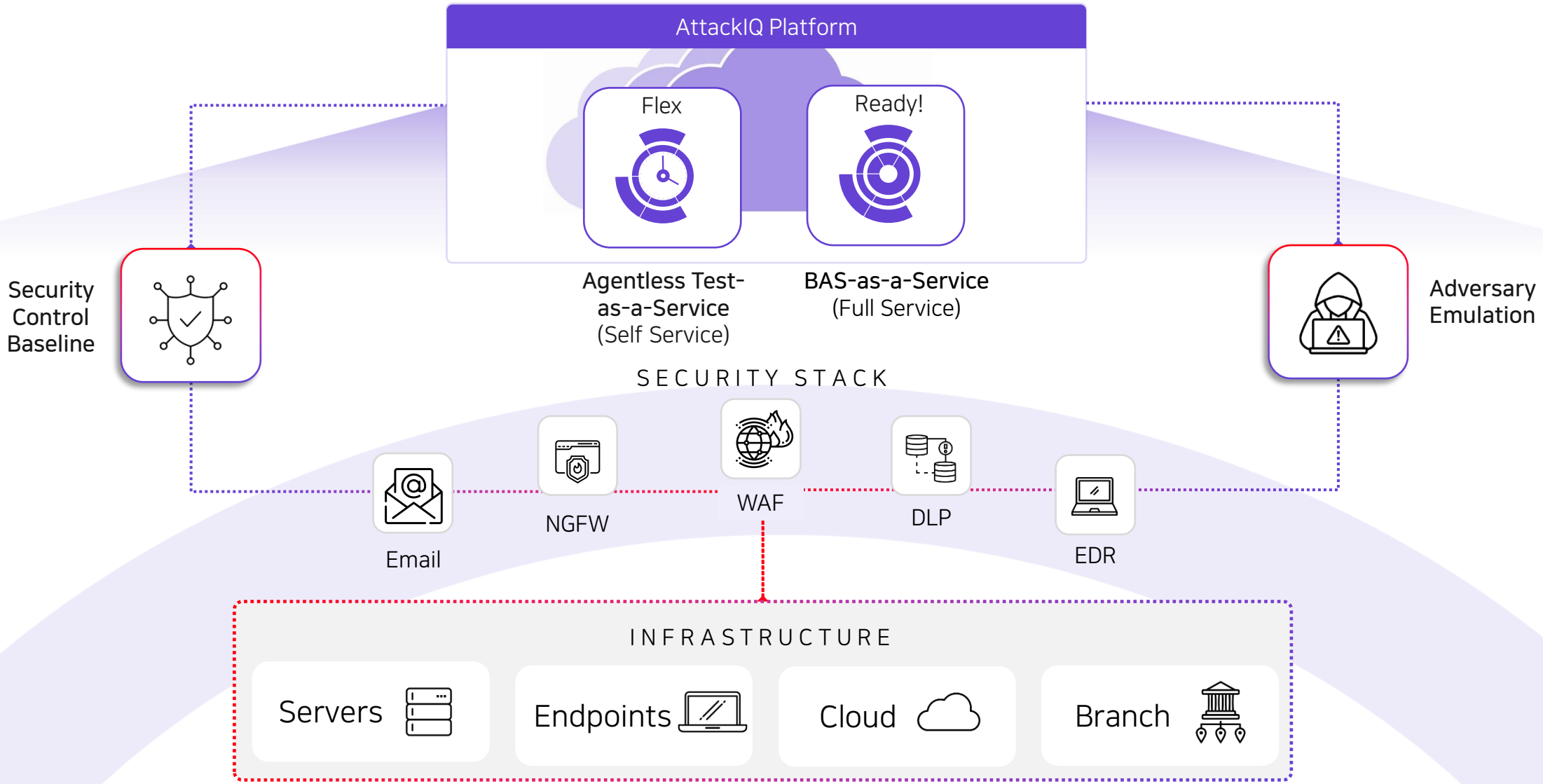
Threat Modelling

시스템의 잠재적인 위협과 취약성을 식별, 분석, 매핑합니다. 이는 조직이 잠재적인 공격 벡터를 고려하고 전체 적 캠페인과 전술, 기술 및 절차에 대한 적절한 보안 조치를 설계함으로써 위험을 완화하고 데이터를 보호하기 위한 전략을 적극적으로 고안하는 데 도움이 됩니다.

MITRE ATT&CK & Threat-Informed Defense

조직에 영향을 미칠 가능성이 가장 높은 위협에 대한 지식을 사용하여 MITRE ATT&CK® 프레임워크에 설명된 것과 같은 적대적인 행동에 대한 보안 제어를 테스트하고 조정하는 데 중점을 둡니다.

AttackIQ BAS 서비스



AttackIQ BAS 서비스 비교

	AttackIQ Flex	AttackIQ Ready!	AttackIQ Enterprise
Security Control Baseline Validation	Point in Time	Weekly and Monthly	all the Time
Threat Emulation	Self-Contained Test Package	Customizable Test	Customizable Test
Reporting	✓	✓	✓
Remediation Guidance	✓	✓	✓
Boundary Posture Management	✗	✓	✓
Adversary Library Access	✗	Partial	Full
Curated Adversary Research Team Content	✓	✓	✓
Testing in Production and at Scale	✗	Up to 5 Test Points	Up to 500 Test Points
AttackIQ Notebooks	✗	✗	Add-on
Customizable Dashboards	✗	✗	✓

ATTACKIQ

AttackIQ Flex

BAS(Breach & Attack Simulation) test-as-a-service

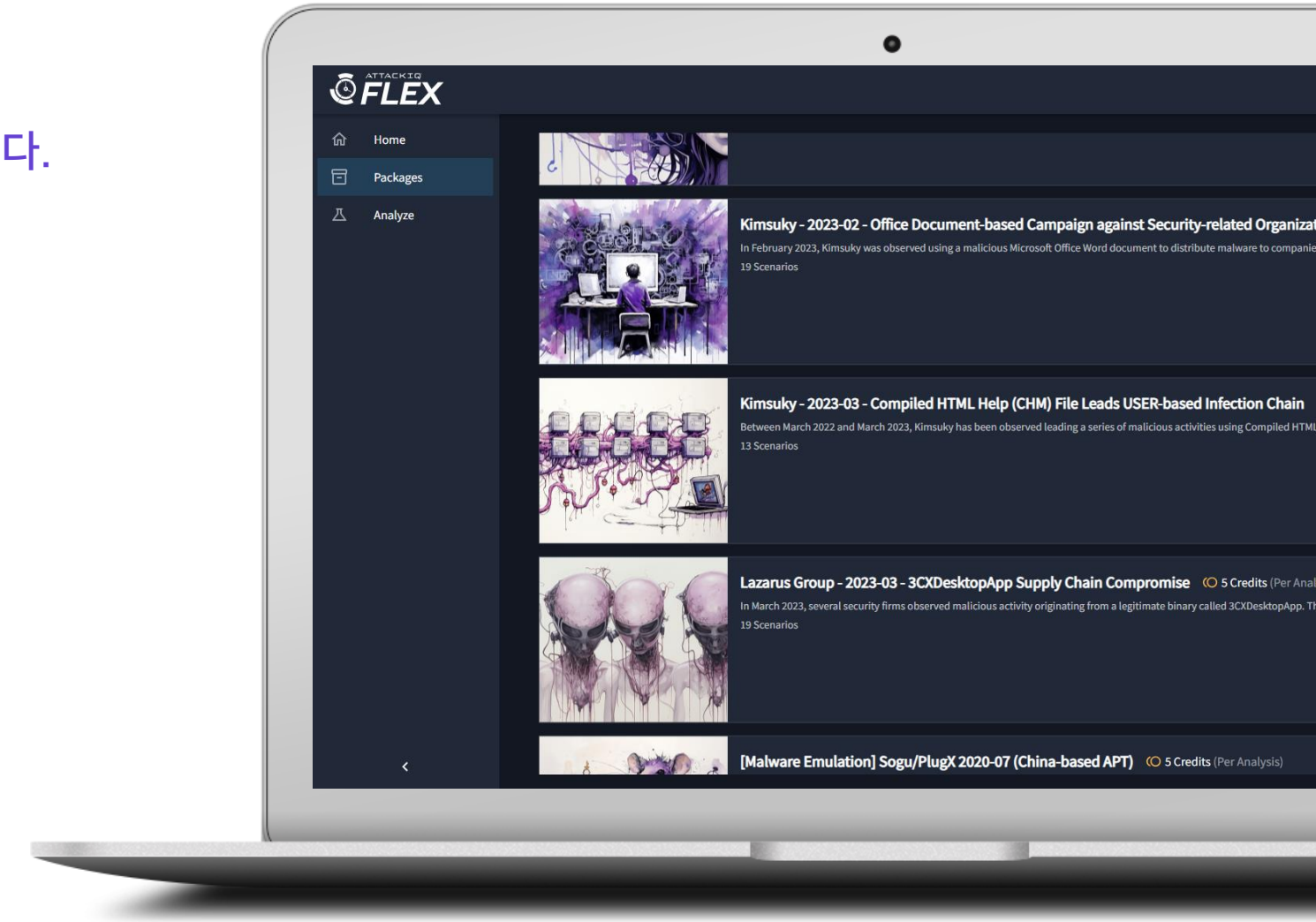
SOFTWIDE SECURITY

AttackIQ Flex 개요

AttackIQ Flex는 누구나 버튼 클릭만으로
몇 분 안에 사이버 공격을 시뮬레이션 할 수 있는
BAS(Breach & Attack Simulation) 서비스입니다.

간단한 테스트 환경을 통해 신속하게 적대적인 행동을
에뮬레이션하고 제어 기능을 테스트할 수 있습니다.

- 버튼 클릭만으로 업계 최고의 적 에뮬레이션
- 직관적이고 단순화된 테스트 경험
- 수동 레드팀 평가 대비 극히 일부 비용으로
  자동화된 보안 테스트 수행



AttackIQ Flex 특징

AttackIQ Flex를 사용하면 조직에서 온디맨드(on-demand) 방식으로 보안 제어를 신속하게 테스트할 수 있습니다.

모두를 위한 테스트

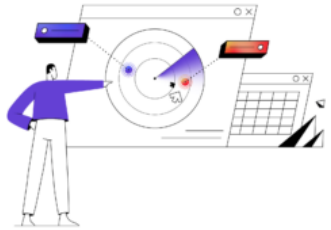
테스트한만큼 지불하는 방식으로 고가의 BAS 플랫폼 도입이 어려운 조직도 BAS 테스트를 수행할 수 있습니다.

가장 빠른 결과 확인

에이전트 없는 테스트를 통해 조직은 Flex를 배포하고 몇 주가 아닌 몇 분 만에 보안 검증 질문에 대한 답변을 얻을 수 있습니다.

단순화된 테스트

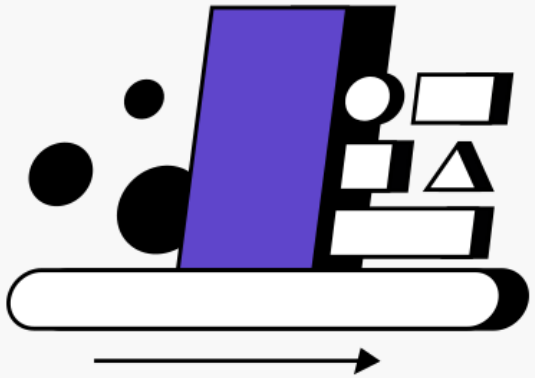
AttackIQ Flex의 자체 테스트 패키지는 설계 및 실행을 간소화하고 보안 제어 검증과 관련된 복잡성을 줄입니다.



향상된 가시성

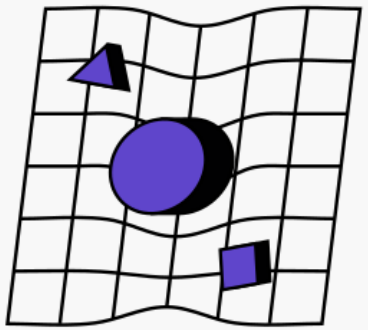
자체 테스트 패키지를 사용하면 조직은 관리·인터넷 연결 여부에 관계없이 모든 네트워크에서 신속한 테스트를 수행할 수 있습니다.

AttackIQ Flex 테스트 방식



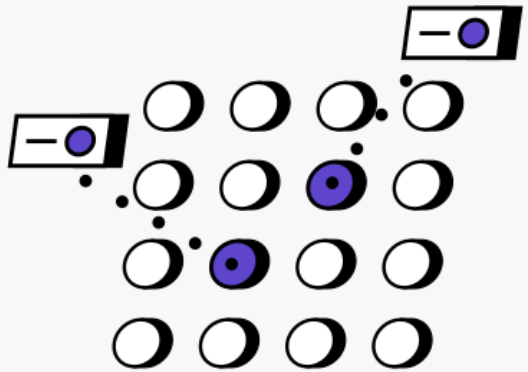
Attack Flow

실제 공격자 행동 시뮬레이션



Atomic Testing

필수 탐지 기능 시뮬레이션



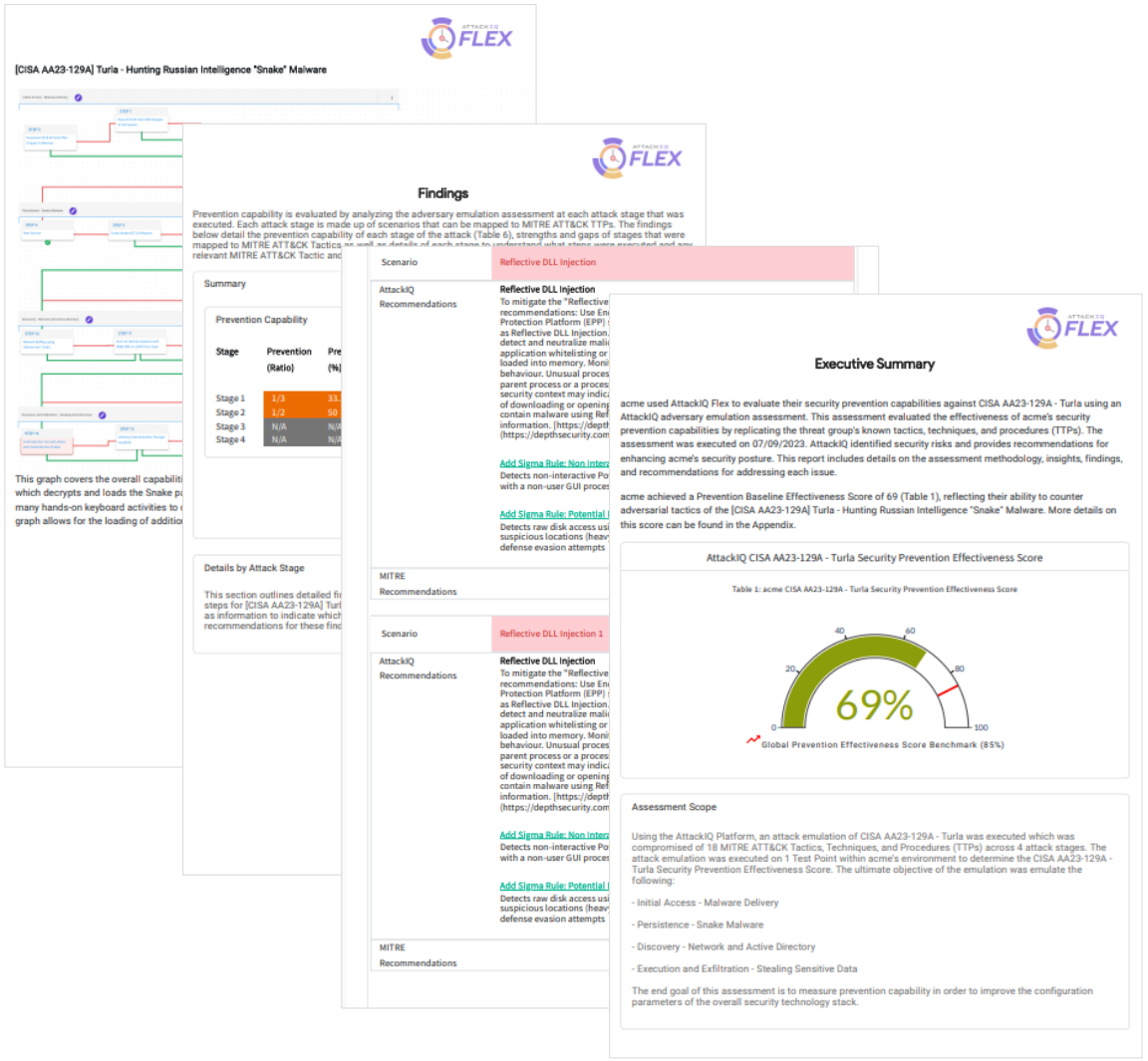
Packet Capture Replay

경계 방어 테스트를 위한
네트워크 트래픽 시뮬레이션

- Adversary Campaigns
- One-Click and Done Security Control
- Baseline Tests
- CISA Alerts

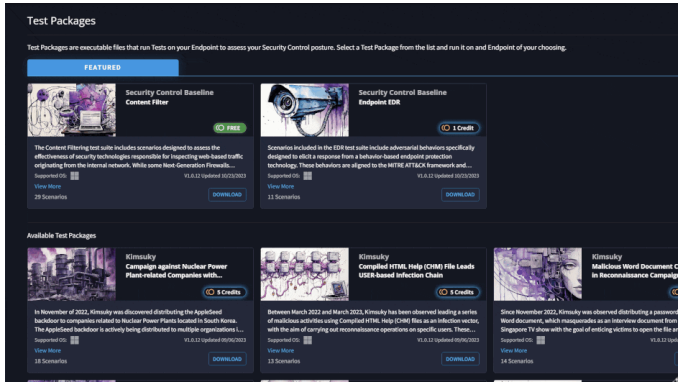
AttackIQ Flex 인터페이스 & 보고서

Capabilities			
Flex Interface	엄선된 적대 연구 및 CTI		
	보고 대시보드		
Reporting		Security Baseline	Adversary Emulation
	보안 상태 개선을 위한 권장 조치 과정이 포함된 CISO 경영진 요약	✓	✓
	상세한 적 배경을 갖춘 공격 흐름		✓
	테스트 성능 점수 및 글로벌 비교	✓	✓
	단계별, 기법별 상세 예방 결과		✓
	자세한 MITRE ATT&CK 및 AttackIQ 관련 완화	✓	✓
	공격 방법론 및 에뮬레이션 세부 정보, 실행 단계	✓	✓



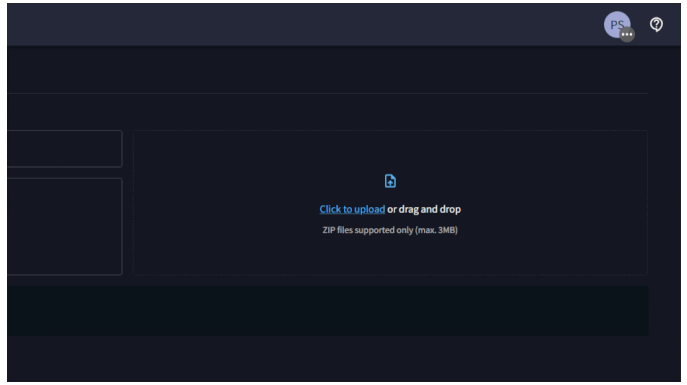
AttackIQ Flex 테스트 절차

AttackIQ Flex는 공격 시뮬레이션을 통해 보안 조치를 평가할 수 있는 안전하고 간단한 방법을 제공합니다.
광범위한 사전 구성된 테스트 라이브러리에서 패키지를 선택하고 몇 분 안에 테스트 결과를 확인할 수 있습니다.



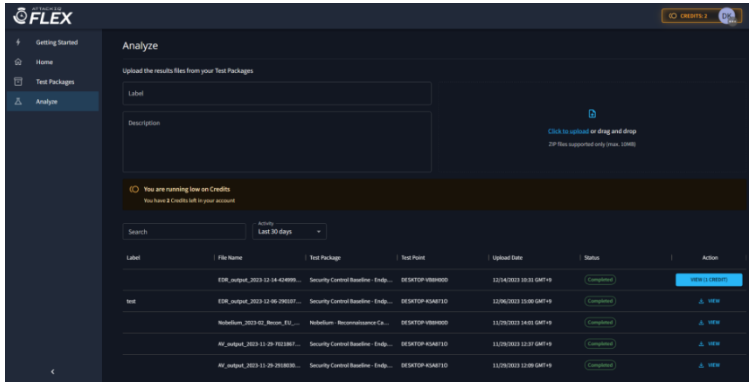
1. 테스트 패키지 다운로드

'테스트 패키지' 탭으로 이동하여 실행하려는 Flex 테스트 패키지를 다운로드하세요.



2. 결과 업로드

테스트가 완료되면 테스트를 실행한 위치에 간단한 결과 파일이 생성됩니다. 이 파일을 가져와 암호화된 결과를 Flex Portal의 분석 탭 아래에 업로드 하세요.



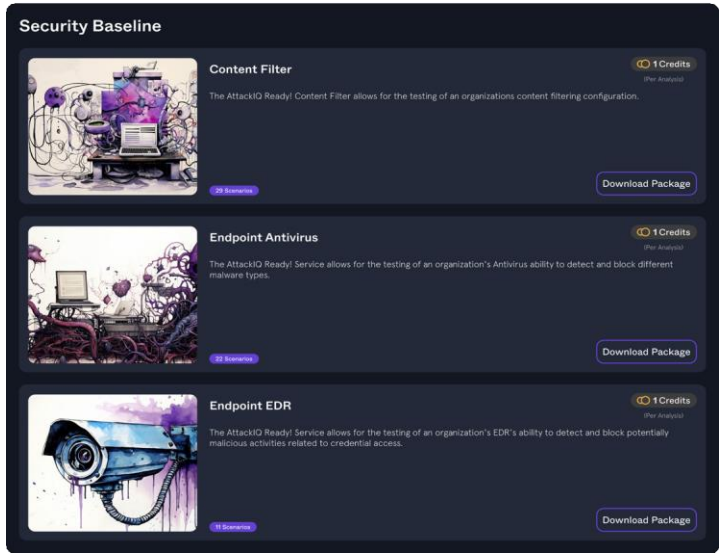
3. 보고서 보기

몇 초 내 계정의 크레딧을 활용하여 '분석' 탭에서 보고서를 볼 수 있는 옵션에 제공됩니다.

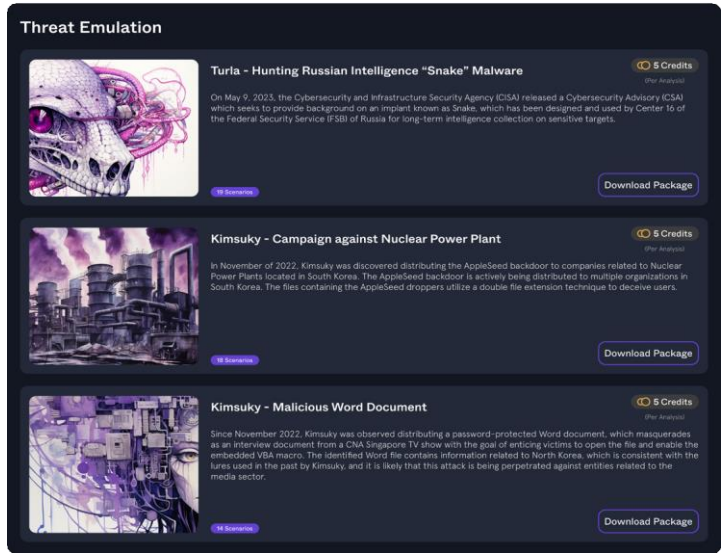
AttackIQ Flex 테스트 패키지

테스트 패키지는 보안 제어 상태를 평가하기 위해 엔드포인트에서 테스트를 실행하는 실행 파일입니다.
기본적으로 실시하고 실행할 수 있는 다양한 테스트 요구사항을 충족하고 전술, 기술 및 절차(TTPs)를 포함하는
포괄적인 번들로 '보안 제어 베이스라인'과 '위협 에뮬레이션' 두 가지 유형으로 제공되며, 지속적으로 업데이트 됩니다.

Security Control Baseline



Threat Emulation



AttackIQ Flex 테스트 패키지 - Security Control Baseline

보안 제어 베이스라인은 엔드포인트 EDR, AV, 차세대 방화벽 등 핵심 보안 제어의 효율성을 테스트합니다.

기준일 : 2024년 1월 30일

Security Control Baseline		Scenarios (개수)
엔드포인트 안티바이러스 (Endpoint Antivirus)	다양한 실시간 악성코드 샘플로 일반적인 공격 패턴을 에뮬레이션하여 엔드포인트 안티바이러스 기능을 검증	22
차세대 방화벽 (Nextgen Firewall)	위협을 방지하고 지능형 위협을 감지하고, 포괄적인 네트워크 가시성과 상황 인식을 제공하고, 보안 네트워킹 및 융합을 지원하는 차세대 방화벽(NGFW)의 능력을 평가	18
엔드포인트 EDR (Endpoint EDR)	자격 증명 수집, 실행, 검색 및 지속성을 포함한 다양한 적대적 전술, 기술 및 절차(TTPs)를 통해 EDR 탐지 기능을 검증	11
콘텐츠 필터 (Content Filter)	내부 네트워크에서 악성 콘텐츠를 다운로드하는 등 네트워크 검사 기능을 검증	29
C2C 웹 커뮤니케이션 (Command and control Web Communication)	C2 통신에 대한 회사의 보안 상태를 평가하고 현재 방어의 잠재적인 위험과 격차를 식별	10

AttackIQ Flex 테스트 패키지 - Threat Emulation

위협 에뮬레이션은 알려진 공격자 캠페인의 TTPs를 테스트하여 새로운 위협에 대한 제어 기능을 검증합니다.

기준일 : 2024년 1월 30일

Threat Emulation		Scenarios (개수)
CISA AA23-074A	다수의 행위자가 Telerik 취약점을 악용하여 웹셸 및 백도어 배포	17
CISA AA23-339A	위협 행위자들의 정부 서버에 대한 초기 액세스를 위한 Adobe ColdFusion CVE-2023-26360 익스플로잇	10
CISA AA23-347A	러시아 해외 정보국(SVR)의 전 세계적인 JetBrains TeamCity CVE 활용	29
갈륨 (Gallium)	오염된 사랑 작전	15
구트로더 (Gootloader)	감염부터 BokBot을 통한 다양한 엔드게임 페이로드까지	19
김수키 (Kimsuky)	AppleSeed를 활용한 원자력 발전소 관련 기업 반대 캠페인	18
김수키 (Kimsuky)	컴파일된 HTML 도움말(CHM) 파일로 사용자 기반 감염 사슬 리드	13
김수키 (Kimsuky)	정찰 캠페인에 정점을 이루는 악성 Word 문서	14
김수키 (Kimsuky)	보안 관련 기관을 대상으로 한 Office 문서 기반 캠페인	19
라자루스 그룹 (Lazarus Group)	3CXDesktopApp 공급망 손상	19
라자루스 그룹 (Lazarus Group)	Dream Job 작전(ClearSky)	11
무스탕 판다 (Mustang Panda)	정부를 대상으로 한 글로벌 피싱 캠페인	13
노벨륨 (Nobelium)	유럽 정부에 대한 정찰 캠페인	16
오일리그 (OilRig)	탐색, 수집 및 유출 루틴으로 이어지는 VBA 매크로	27
칵봇 (QakBot)	LotL(Living-off-the-Land) 기법을 사용한 감염 사슬	16
칵봇 (QakBot)	ISO 이미지 배포로 인한 Brute Ratel, Cobalt Strike 및 SharpHound 발생	24
리시다 랜섬웨어 (Rhysida Ransomware)	다양한 부문 및 지역에 대한 글로벌 캠페인 [Cobalt Strike 버전]	21
소구/플러그X (Sogu/PlugX)	멀웨어 에뮬레이션	13
툴라 (Turla)	러시아 정보국의 "Snake" 멀웨어 헌팅	19

AttackIQ Flex 테스트 패키지 - Endpoint Antivirus

엔드포인트 안티바이러스

다양한 실시간 악성코드 샘플로 일반적인 공격 패턴을 에뮬레이션하여 안티바이러스 기능 검증

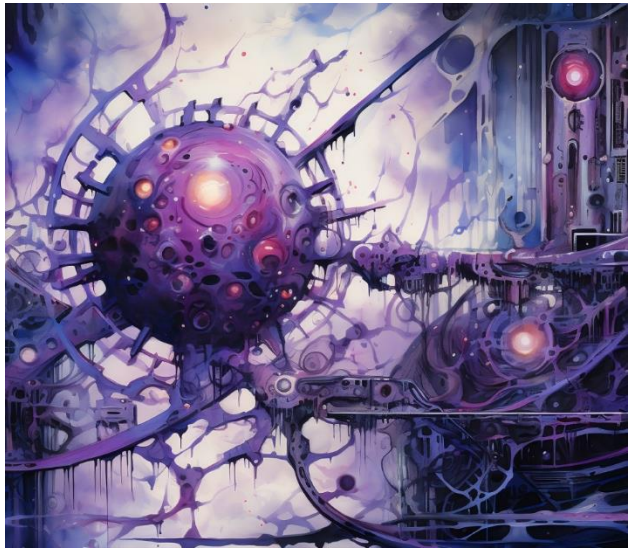
이 평가 패키지에는 일반적인 랜섬웨어, 멀웨어 및 EICAR 샘플을 사용하여 AV 효율성을 테스트하도록 설계된 다양한 시나리오가 포함되어 있습니다. 또한 일반적으로 AV 탐지를 회피하는 "해커 도구"도 포함됩니다.
AttackIQ는 실행 없이 로컬 파일 시스템에 저장되고 기록되는 라이브 악성코드 샘플을 활용합니다.
각 시나리오는 암호화된 형식으로 다운로드 되고 나중에 해독된 디스크에 저장되며 최종적으로 복사본이 만들어집니다. 보안 제어가 대응할 시간을 주기 위해 각 작업 사이에 3초의 지연이 적용됩니다.
Flex는 해시 비교를 사용하여 어떤 샘플이 엔드포인트에 성공적으로 심어졌는지 확인합니다. 파일을 저장하고 파일 시스템에 복사할 수 있고 결과 해시가 예상 해시와 일치하면 결과는 방지되지 않음이 됩니다. 그렇지 않으면 시나리오 실행이 방지됨으로 표시됩니다.
테스트가 끝나면 정리 프로세스의 일부로 준비된 모든 파일이 즉시 제거됩니다.

[포함된 22개 시나리오]

- MiniDuke 악성 코드 샘플을 파일 시스템에 저장
- Etumbot 악성 코드 샘플을 파일 시스템에 저장
- 2020-04 라자루스 그룹 운영 드림잡 악성 오피스 문서를 파일 시스템에 저장
- 2022-05 Emotet 악성 XLS 전달 문서를 파일 시스템에 저장
- Emotet(epoch5) 2022-09 DLL 파일을 파일 시스템에 저장
- Locky 샘플을 파일 시스템에 저장
- WannaCry 웜 샘플을 파일 시스템에 저장
- Petya 랜섬웨어를 파일 시스템에 저장
- Conti 랜섬웨어 2021-08을 파일 시스템에 저장
- BlackMatter 랜섬웨어 2021-10을 파일 시스템에 저장
- TeslaCrypt 랜섬웨어를 파일 시스템에 저장
- CryptoWall 랜섬웨어를 파일 시스템에 저장
- CryptoLocker 랜섬웨어를 파일 시스템에 저장
- 2023-01 Lockbit 3.0 랜섬웨어 샘플을 파일 시스템에 저장
- Httptunnel Hacktool을 파일 시스템에 저장
- 2020-12 ZeroLogon Hacktool을 파일 시스템에 저장
- Hacktool Netcat을 파일 시스템에 저장
- Hacktool Mimikatz를 파일 시스템에 저장
- EICAR 파일을 파일 시스템에 저장
- Zip EICAR 파일을 파일 시스템에 저장
- TXT EICAR 파일을 파일 시스템에 저장
- 이중 압축된 EICAR 파일을 파일 시스템에 저장

AttackIQ Flex 테스트 패키지 - Rhysida Ransomware

리시다 랜섬웨어



여러 부문 및 지역을 대상으로 한 글로벌 캠페인 [코발트 공격 버전] 검증

2023년 8월 9일 Trend Micro는 의료 부문을 표적으로 삼는 새로운 Rhysida 랜섬웨어 활동에 대한 세부 정보를 보고했습니다. Rhysida의 운영자는 최근 8월 초 캘리포니아에 기반을 둔 의료 시스템인 Prospect Medical Holdings를 상대로 발생한 사건에 연루되어 미국 전역의 17개 병원과 166개 진료소에 영향을 미쳤습니다. 식별된 활동 동안 Rhysida는 피싱 미끼를 통해 피해자의 시스템에 도달한 후 시스템과 네트워크 내에서 검색 및 측면 이동 활동을 지원하기 위해 Cobalt Strike가 배포 및 실행되었습니다. 이 공격 그래프는 공격자가 사용하는 ZIP 파일을 다운로드하고 저장하는 것으로 시작하여 파일 내에 포함된 Cobalt Strike 샘플의 배포로 계속되며, 이는 나중에 프로세스 인젝션 또는 반사 DLL 인젝션을 통해 실행됩니다. 이후 Cobalt Strike는 운영 체제 정보, 활성 프로세스, CPU 속성, 설치된 보안 소프트웨어 및 관리자 계정과 같은 시스템 정보를 획득합니다. Rhysida를 배포하기 전에 가해자는 SILENTKILL이라는 PowerShell 스크립트를 사용하여 보안 소프트웨어를 식별하고 비활성화하거나 이를 우회하기 위한 제외 규칙을 만들었습니다. 또한 스크립트는 로컬 계정 암호 변경, 로컬 방화벽 수정, 시스템 백업 삭제 등을 수행하여 복구 작업을 지연시킬 수 있습니다.
Rhysida 운영자는 PsExec을 활용하여 PowerShell 스크립트와 Rhysida 랜섬웨어 페이로드 자체를 배포하는 것이 관찰되었습니다. 배포 시 Rhysida는 손상된 시스템의 모든 로컬 드라이브에 있는 모든 파일을 식별하고 나열하려고 합니다. 완료되면 4096비트 RSA 키와 ChaCha20을 사용하여 파일을 암호화하고 확장자 ".rhysida"를 추가하는 작업을 수행합니다.

[포함된 21개 시나리오]

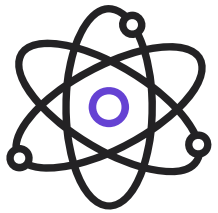
- 2023-05 Rhysida 악성 ZIP 샘플을 파일 시스템에 저장
- wevtutil.exe를 통해 Windows 이벤트 로그 지우기
- 2023-05 Rhysida 랜섬웨어 샘플을 파일 시스템에 저장
- “vssadmin.exe"를 사용하여 생성된 볼륨 섀도 복사본 삭제
- PowerShell을 사용하여 레지스트리 키를 통해 Windows Defender 비활성화
- 시스템 정보 검색 스크립트
- 라이브러리 로드 및 원격 스레드 생성을 통한 코드 주입
- WMI 명령을 사용하여 보안 소프트웨어(AntiVirusProduct) 검색
- 예약된 작업 실행
- 2022-09 코발트 스트라이크 비콘 샘플을 파일 시스템에 저장
- “reg.exe"를 사용하여 레지스트리를 통해 Rhysida 사용자 배경 화면 설정
- 반사 DLL 인젝션(Reflected DLL injection)
- 파일 삭제 시나리오
- 작업 목록을 통한 프로세스 검색
- Net 명령 스크립트를 통한 도메인 관리자 계정 검색
- 파일 및 디렉터리 검색 스크립트
- 2023-05 Rhysida 악성 ZIP 샘플을 메모리에 다운로드
- 콘티 파일 암호화
- 2023-08 SILENTKILL 샘플을 파일 시스템에 저장
- WMI를 사용하여 CPU 속성 가져오기
- "New-NetFirewallRule" PowerShell 명령을 통해 Rhysida 방화벽 제외 추가

AttackIQ Flex 기대효과

AttackIQ Flex는 비용과 시간이 많이 소요되는 수동 테스트 없이 보안 제어를 검증 할 수 있습니다.
원하는 만큼 비즈니스 요소 전반에 걸쳐 테스트를 수행하고 조직의 방어 역량을 강화할 수 있습니다.

방어 역량 강화

Flex는 AttackIQ의 Advanced Adversary Emulation SW를 활용하여 현실 세계의 적들과 그들의 캠페인에서 사용된 전술, 기술 및 절차를 복제합니다. 공격자가 목표를 달성하기 전에 공격을 차단할 수 있도록 방어 역량을 강화할 수 있습니다.



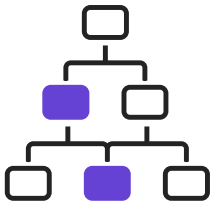
ATOMIC TESTING

비용 절감 & 효율 상승

Flex는 비용이 많이 들고 시간이 많이 소요되는 수동 테스트 없이도 보안 제어를 검증할 수 있는 경제적인 수단을 제공합니다. 테스트가 필요한 패키지를 선택해 서로 다른 요소에서 원하는 만큼 많이 또는 적게 테스트할 수 있습니다.

신속한 결정 및 조치 가능

에이전트리스 테스트를 통해, 조직은 Flex를 구축하고 몇 분 만에 보안 검증 질문에 대한 답변을 받게 됩니다. 이러한 가속화된 프로세스는 신속한 의사 결정과 효과 향상을 위한 사전 조치를 가능하게 합니다.



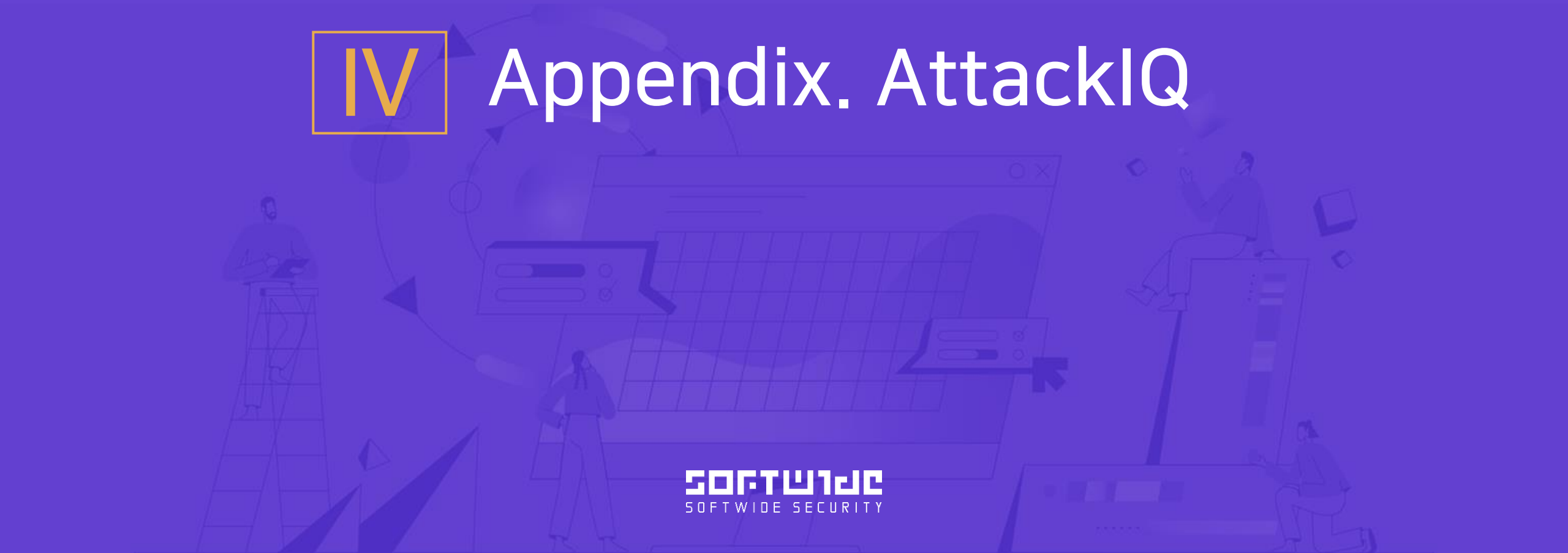
ATTACK GRAPHS

빠른 위협 대응

Adversary Research Team은 새로 발생한 위협으로부터 48시간 이내에 공격 그래프를 생성하여 실제 사용자에 대한 제어를 검증할 수 있습니다.

ATTACKIQ

IV Appendix. AttackIQ



SOFTWIDE SECURITY

AttackIQ MITRE ATT&CK

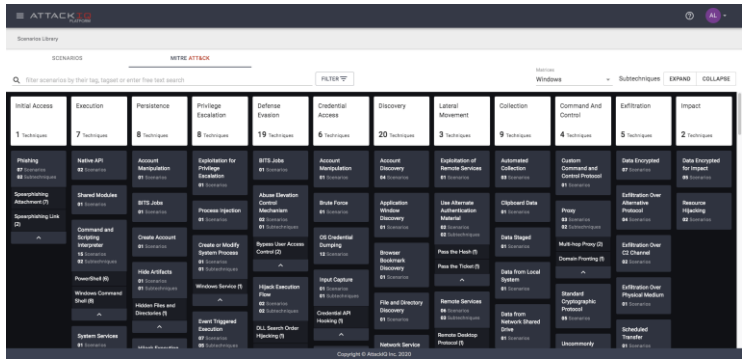
MITRE ATT&CK 전문성

- MITRE Engenuity CTID(Center for Threat-Informed Defense) 창립 멤버로 사이버 방어 개선을 위한 공동 연구 및 개발 수행

MITRE ENGENUITY | Center for Threat Informed Defense

Center for Threat-Informed Defense
RESEARCH PARTNER
FOUNDER

- AttackIQ 플랫폼 - MITRE ATT&CK 프레임워크 운영



2022년 업계 최고의 BAS 솔루션 선정

- eSecurity Planet 2022 사이버보안제품 어워드 최고의 BAS 솔루션 선정

Best Breach and Attack Simulation (BAS) Solution: AttackIQ

Winner: AttackIQ

Finalists: Cymulate, Picus Security

The top solution in the emerging breach and attack simulation (BAS) sector belongs to San Diego-based AttackIQ. Competing with upstart BAS vendors like Cymulate and Picus Security, AttackIQ's platform, capabilities, and user reviews impressed us the most. The AttackIQ Security Optimization Platform offers a friendly user interface, MITRE-informed threat intelligence, and real-time testing of an organization's defensive posture.

See our full list of the Top BAS Solutions.

eSecurity Planet's BEST BAS VENDORS 2022

AttackIQ Awards

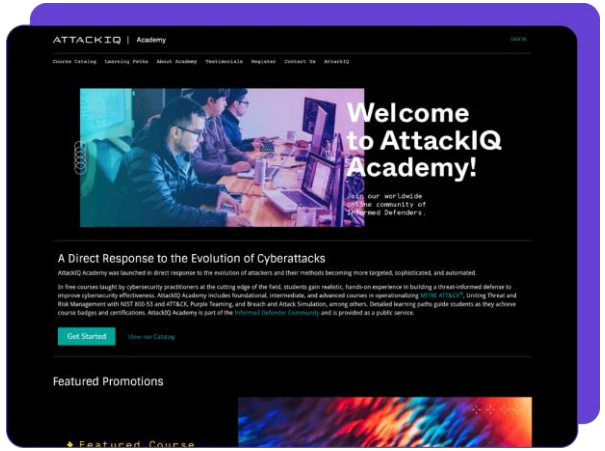
AttackIQ Customers

금융, 의료, 기술, 정부, 군 등 전 세계 유수의 기업과 기관이 AttackIQ와 함께 하고 있습니다.

AttackIQ Community

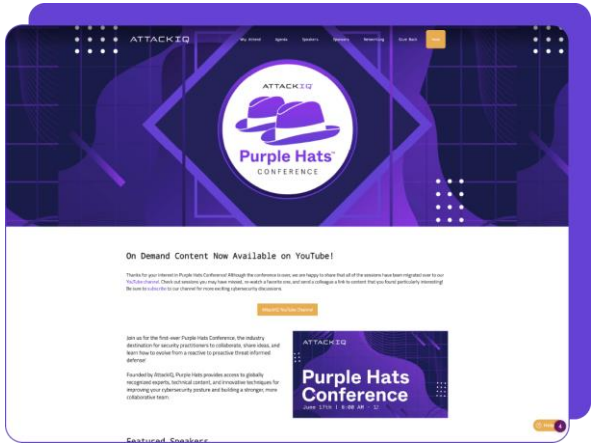
AttackIQ Academy

MITRE ATT&CK부터 퍼플 팀 구성, 클라우드 보안 등에 이르기까지 다양한 심층적인 사이버 보안 주제에 대한 온라인 강의 무료 제공



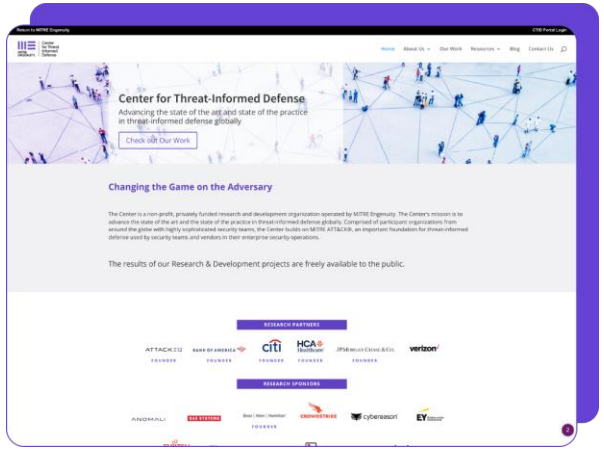
Purple Hats

사이버 보안 실무자들이 협업하고 아이디어를 공유하며 대응적 위협 정보 방어에서 사전 예방적 위협 정보 방어로 발전하는 방법을 배울 수 있는 Purple Hats 컨퍼런스



Center for Threat-Informed Defense

MITRE Engenuity가 운영하는 비영리 연구 개발 조직인 위협 정보 방어 센터(Center for Threat-Informed Defense)의 창립 멤버로, MITRE ATT&CK®를 기반으로 실무자가 사이버 보안 태세를 강화할 수 있도록 지원



Informed Defenders Council

혁신적인 기술, 조직적 기술, 방어 모범 사례를 공유한다는 목표로 설립된 Informed Defenders Council은 산업과 대륙 전반에 걸쳐 사이버 보안 및 기술 리더로 구성되어 사이버 보안 미래 형성에 도움을 주기 위해 노력

THANKS FOR YOUR ATTENTION

Contact us:

서울시 서초구 마방로 10길 5, 태석빌딩 7층 **(주)소프트와이드시큐리티**

02-6052-5701

pr@softwidesec.com

www.softwidesec.com