RidgeSecurity

취약점 분석 및 모의 침투 테스트

RidgeBot 제안서

RidgeSecurity의 지능형 보안 검증 로봇인 RidgeBot(릿지봇)은 위협, 취약성 및 악용에 대한 종합적인 지식을 바탕으로 모델링 되었으며, 최첨단 해킹 기술이 탑재되어 있습니다.
실제 공격자처럼 행동하여 끊임없이 익스플로잇을 찾아내고 그 결과를 문서화합니다.

CONTENTS

CONTENTS

04

도입 효과

05

모의 침투 테스트 및
취약점 진단 가이드

1-1 침해 사고 사례

'K-사이버방역'에서 소개한 공급망 보안위협 사례

관련 링크

1-2 기존 보안 테스트의 문제점

취약점 스캐너
VULNERABILITY SCANNER

- 높은 오탐률
- 실제 공격 가능성과 관계 없는 패치 우선 순위 경고
- 취약성에 대한 검증이 없음
- 실제 PoC 침투 시험이 없음

&

수동 침투 테스트 서비스
MANUAL PENETRATION TEST SERVICE

- 시험 당 3-6억원의 고비용
- 많은 시간과 숙련된 시험자 필요
- 일관되지 않는 결과물
- 회사 데이터가 시험자에게 노출

1-3 기존 보안 테스트의 문제점

RidgeBot – 자동 모의 침투 테스트

RIDGEBOT – AUTOMATIC SIMULATED PENETRATION TEST

자동 모의 침투 테스트

→ 사람은 보조만 하는 자동화 시스템

자동 모의 침투 테스트

→ 사람은 보조만 하는 자동화 시스템

RidgeBot(릿지봇)

RIDGEBOT

최초의 자동 모의 침투 테스트 로봇

최초의 자동 모의 침투 테스트 로봇

해커의 관점에서 공격 경로 제시

7*24 끊임없는 보안 검증 서비스

실시간 학습에 기반한 반복 공격

1-4 취약점 진단의 유형

→ 취약점 진단 유형은 크게 CCE, CVE, CWE 등이 있으며, 설정 변경 및 개선이 가능한 진단 항목으로 구성되어 있습니다.

CCE 취약점
(Common Configuration Enumeration)

사용자에게 허용된 권한 이상의 동작을 허용하거나, 범위 이상의 정보 열람, 변조 및 유출을 가능하게 하는 시스템 설정 상의 취약점으로 운용자가 설정 변경을 통해 개선이 가능합니다.

(포트 차단, 불필요한 서비스 비활성화 등)

IT Infra Configuration 진단
(OS, Networks, DBMS 등)

CVE 취약점
(Common Vulnerabilities and Exposures)

하드웨어 또는 소프트웨어의 결함, 체계, 설계상의 오류(허점)으로 해당 제조사의 공식 패치를 통해서 개선이 가능합니다.

(OS, 애플리케이션 보안 업데이트 설치)

APPlication 진단
(MS, Adobe, Linux, php 등)

CWE 취약점
(Common Weakness Enumeration)

소프트웨어 언어(C, JAVA 등) 및 아키텍처, 디자인 설계, 코딩 등의 개발 단계에서 발생하는 취약점으로 개발자의 소스 코드 수정을 통해서만 개선이 가능합니다.

(웹 페이지 소스 코드 수정)

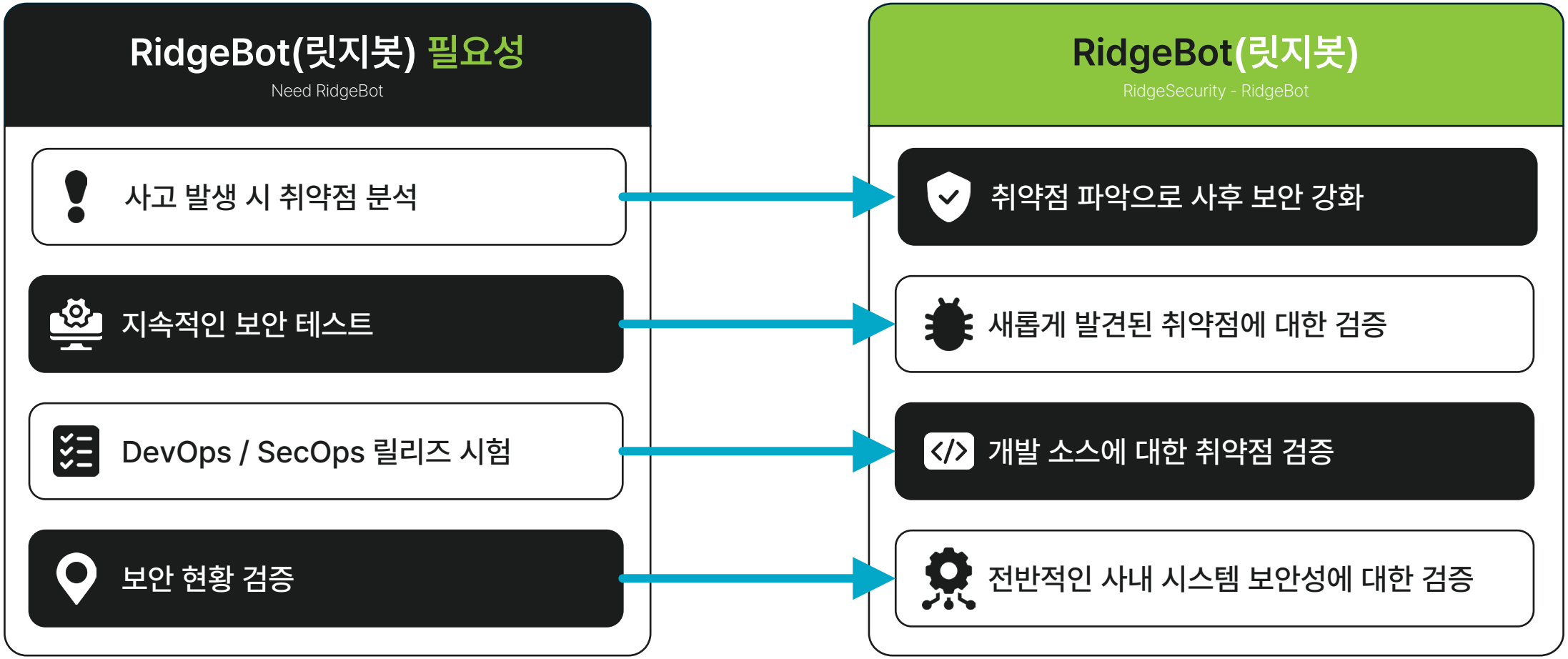
Web Server 소스 진단
(HTML, ASP, JSP 등)

1-5 RidgeBot – 스캐너 / VMS가 아님

→ RidgeBot(릿지봇)은 유일하게 완전 자동화된 침투 테스트 시스템입니다.

취약성 스캔 (Nessus, Nexpoise, Openvas)	취약성 관리 시스템 (Tenable.sc, InsightVM, Qualys)	침해 공격 시뮬레이션 (Picus, Attack IQ, XM Cyber)	침투 테스트 (RidgeBot, BurpSuite, Metasploit Pro, Core Impact)
-	(VMS)	(BAS)	PT
취약성 DB에 기반한 잠재적 문제 식별 실제 페이로드 사용 없음 OS / 소프트웨어 취약점	문제를 DB에 기록 주기적 자산 상태 모니터링 패치 상태 감사 보고서	대부분 Mitre-Att&ck 프레임워크 기반 공격 기술을 취합하여 공격 시나리오 작성 보안 장치의 사용자 정책을 미세 조정하는데 사용	실제 익스플로잇으로 문제점을 공격 증거 제시 : 공격 경로, 쉘, 권한, 민감한 자료 측면 이동, 공격 지속, 다중 벡터 공격 소프트웨어 취약성, 잘못된 구성 식별과 정책 튜닝 등

2-1 Why RidgeBot??

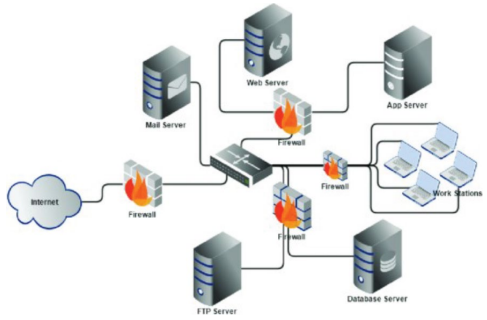


RidgeBot 서비스만이 답!!

3-1 RidgeBot – 자동 모의해킹 테스트 로봇

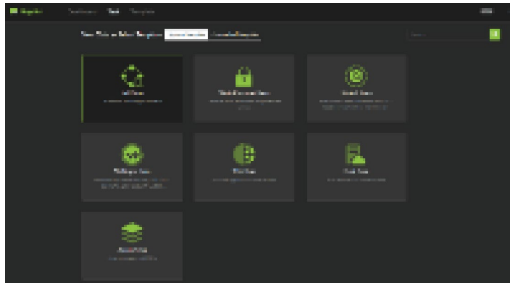
RidgeBot 수분 / 시간 소요 VS **수동으로 수일 / 수주 소요**

설치
(Download)



어플라이언스나 VM에 RidgeBot 설치

테스크 스케쥴
(Tesk Schedule)

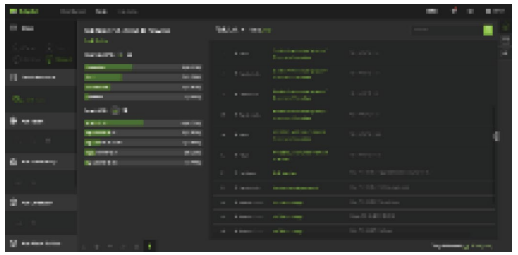


테스크 시작 또는 스케쥴

자동화 침투
(Automation Penetration)

자동 침투 테스트

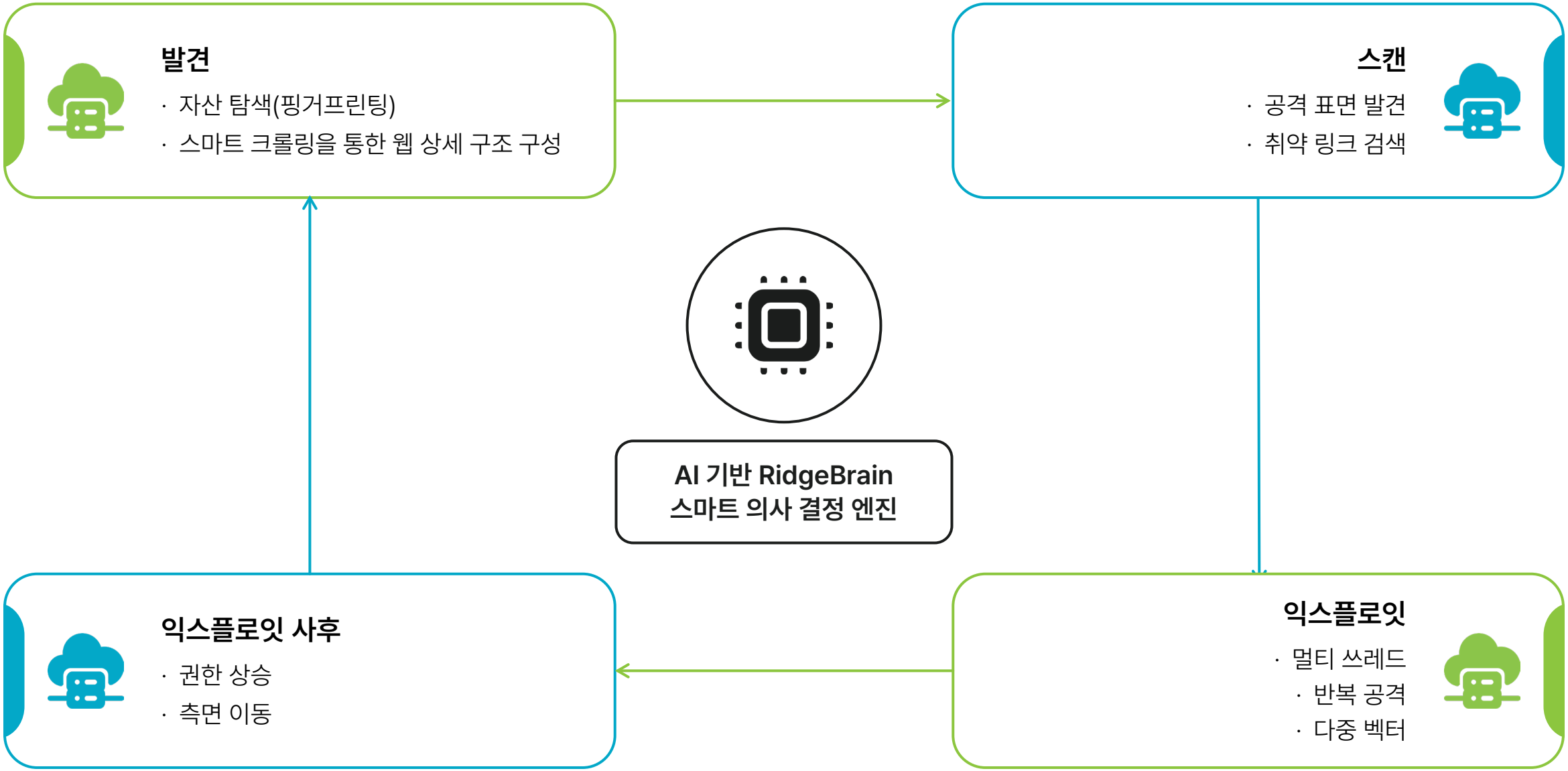
보고서 검토 / 다운로드
(Review / Download Report)



보고서 검토 및 다운로드

RidgeBot(릿지봇) — 위협, 취약성 및 악용에 대한 종합적인 지식으로 모델링 되고 최첨단 모의 침투 기술을 갖춘 지능형 보안 검증 로봇으로 지속적인 보안 검증 서비스를 제공합니다.

3-2 핵심 기술


발견
· 자산 탐색(핑거프린팅)
· 스마트 크롤링을 통한 웹 상세 구조 구성
스캔
· 공격 표면 발견
· 취약 링크 검색
AI 기반 RidgeBrain
스마트 의사 결정 엔진
익스플로잇
· 멀티 쓰레드
· 반복 공격
· 다중 벡터
익스플로잇 사후
· 권한 상승
· 측면 이동

3-3 AI 기반 자동화

→ RidgeBot의 AI 기술을 광범위하게 사용하며 증거를 수집 및 분석하고 위험을 식별, 진단 및 수정하여 인간 컨설턴트와 유사하게 행동합니다.
대상에서 수집된 실시간 데이터를 기반으로 RidgeBot은 자동으로 지능적인 결정을 내리고 작업에 적합한 AI 모델을 선택합니다.

위협 인텔리전스

20억

공격이벤트

1억

취약점

10만

타사 취약점

만2천

POC 익스플로잇

6000

핑거프린트 규칙

3500

권한 상승 취약점

1000

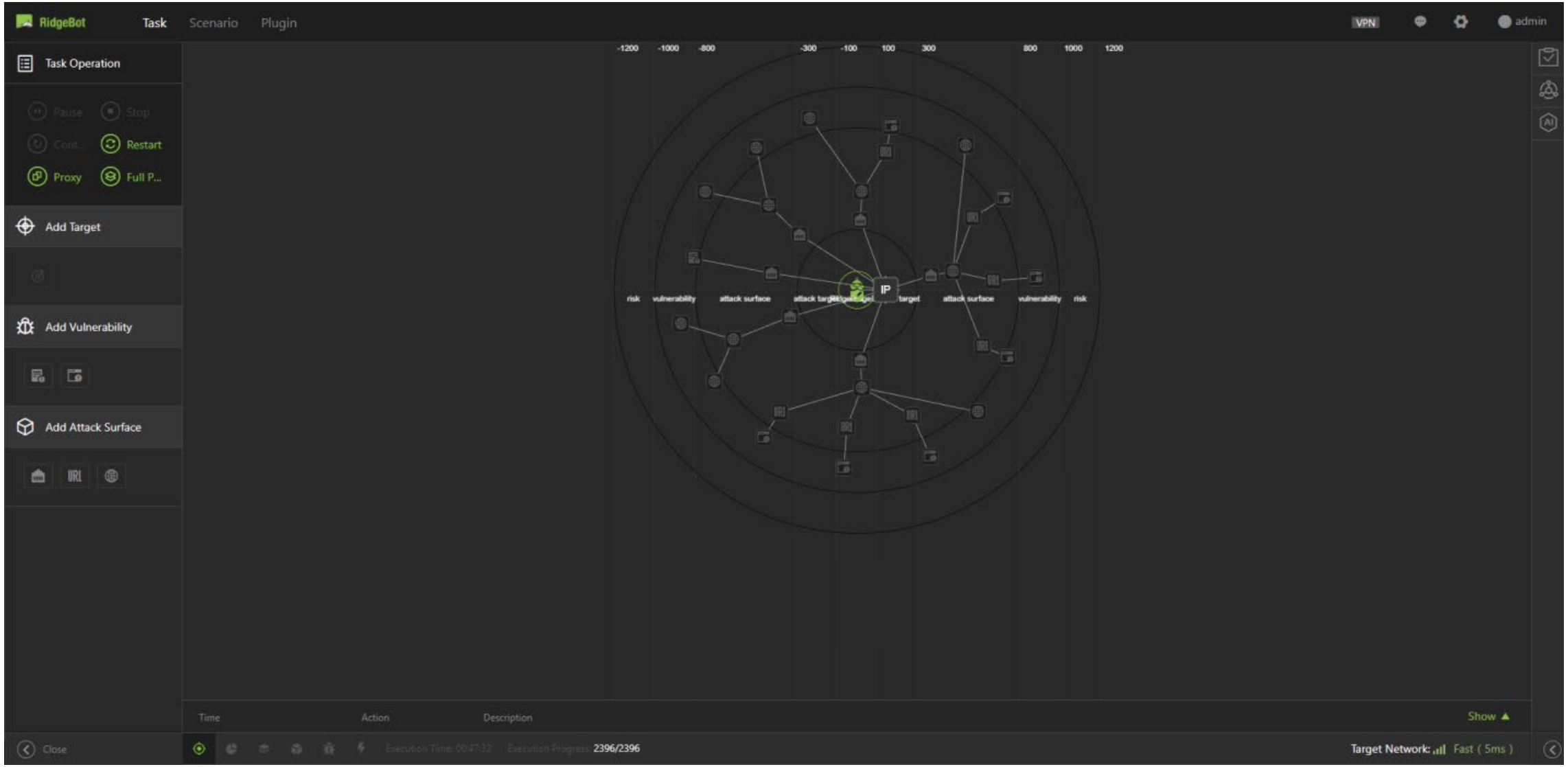
DNS

데이터베이스

글로벌 URL

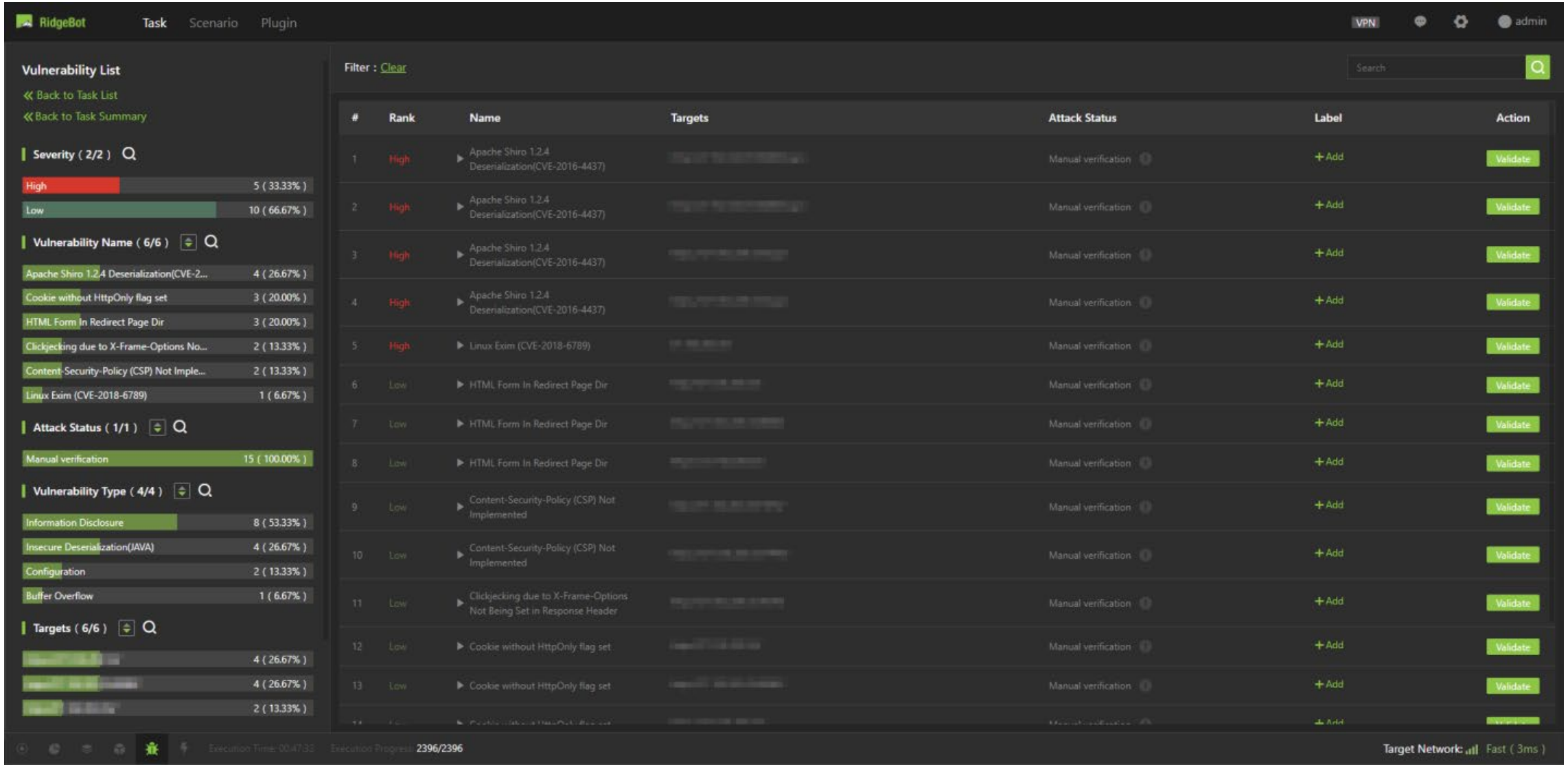
데이터베이스

3-3 RidgeBot 테스트 – 취약점 분석(결과)



3-3 RidgeBot 테스트 – 취약점 분석(결과)

3-3 RidgeBot 테스트 – 취약점 분석(결과)



4-1 RidgeBot Sales 전략

모의 침투 테스트 및 취약점 분석 서비스

✓ 대기업, 금융권, 관공서 등만 받을 수 있는 서비스가 아닙니다.
✓ 사이버 보안 점검은 모든 고객사에 필수입니다.
✓ 모의 침투 테스트 및 취약점 분석 서비스 대중화를 통하여 보다 안전한 세상을 만드는데 앞장 서겠습니다.

대상 : 모든 기업이 대상

✓ 랜섬웨어(보안사고) 이슈 고객사
✓ 외부 침입이 의심되는 고객사
✓ 보안 감사 대상 사업자
✓ 교육 / 공공 입찰사업 시 추가 제안(SI 사업)

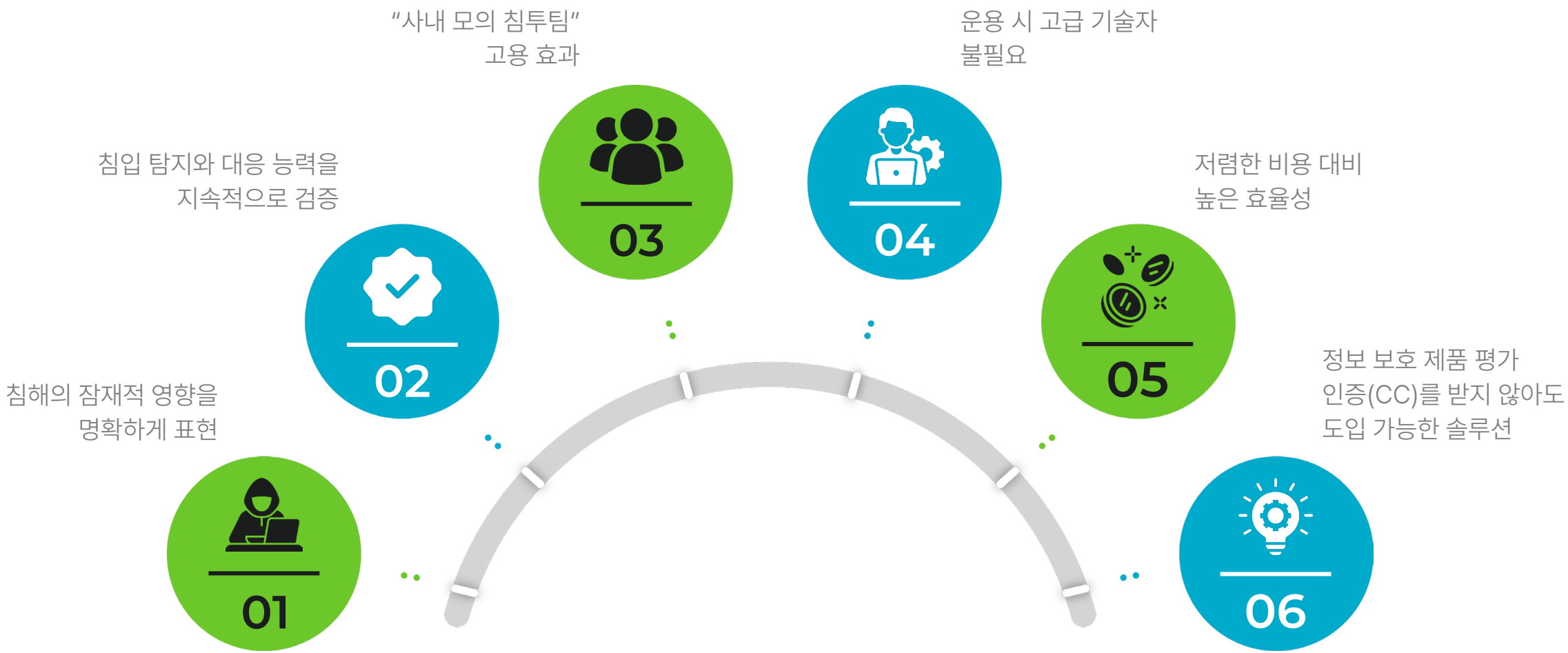
Web Server (Domain / IP)

✓ 대 / 내외 웹 서버 운영 고객사(그룹웨어, Web, 쇼핑몰 등)

제안 방법

✓ IP 호스트는 서버(Windows, Linux OS) 위주로 제안
✓ Client는 필요시 서버 진단(침투) 테스트 후 결과 값으로 Client도 모의 침투 테스트 제안

4-2 RidgeBot 도입 효과



4-3 RidgeBot 테스트 사례 1

Executive Summary

System Version: **V3.2.0-20210119** Plugin Library Version: **V1.1.7**

TASK NAME	START TIME	END TIME	TOTAL TIME	STATUS
ransomewarecheck	Jan 22, 2021 at 03:27	Jan 22, 2021 at 05:32	2 hours and 5 minutes	Success

Total Health Score

Policy: Minimum Score 60

In this task, we have tested 2 IPs and 10 web servers, the Total Health Score of the target system is 24, this score is based on 100 scale.It is a comprehensive evaluation based on multiple factors such as percentage of vulnerability, attack surface, encrypted traffic etc. This test system is considered as in a "Risky"(Risky<60; 60<=normal<85; good>=85) condition with the score of 24. The vulnerability found on each asset can be found in "Asset Detail".

The platform successfully performed 6 exploits. These 6 exploited risks are critical and require immediate attention. It means a real hacker can easily achieve the same result. In the "Exploit Details", we provided information on how it attacked - path, techniques and actions etc for security team to replicate and fix the issue.

Among 6 exploits, 67.0% remote command execution, 33.0% credential disclosure.

Risk Weighted Assessment

Total number of targets:	2
Number of active assets:	2
Number of active Domains:	0
Number of attack surface(s):	1544

고객사 침투 테스트 필요성

- ✓ 웹 서버에 대한 취약점 점검
- ✓ 방화벽을 운용하더라도 대외 서비스를 위해 외부에 오픈되어 있는 포트를 통한 공격 발생 가능성
- ✓ OS : Windows Server
- ✓ 테스트 장비 : 대외 서비스를 위한 웹 서버 1ea

테스트 결과 및 위협 예상

- ✓ 외부에 오픈된 RDP 포트 및 취약한 계정 / 암호 사용 발견
- ✓ 랜섬웨어 감염 Exploting 및 다수의 높은 취약성 발견
- ✓ 해커의 서버 장악 가능성
  → 사내 망에 접근하여 모든 정보 탈취 및 시스템 손상, 랜섬웨어 유포 등 심각한 손실 초래 가능성

4-4 RidgeBot 테스트 사례 2

고객사 침투 테스트 필요성

- ✓ 웹 서버에 대한 취약점 점검
- ✓ 외주 개발한 시스템으로 취약점 의심
- ✓ OS : Linux Server
- ✓ 테스트 장비 : 대외 서비스를 위한 웹 서버 1ea

테스트 결과 및 위협 예상

- ✓ SQL Injection 공격으로 원격 코드 실행 가능성
  → 외부 공격자가 고객 정보, 개인 데이터, 영업 비밀, 지적 재산권 등 중요한 데이터에 무단으로 액세스
- ✓ Cross-Site Scripting(XSS) 공격으로 악성 스크립트가 웹 사이트에 인젝션 될 가능성
  → 해커가 웹 애플리케이션을 사용하여 브라우저 스크립트의 형태로 다른 정상적인 사용자에게 맬웨어를 배포

핵심 요약

시스템 버전: 20210518I3.4.0 플러그인 라이브러리 버전: V2.0.5

태스크 이름	시작 시간	종료 시간	전체 시간	상태
dwcts web (https://www.computer.co.kr/)	2021년 7월 17일 12:00	2021년 7월 17일 13:54	53분	성공

전체 상태 점수

정책: 최소 점수 60점

위험 60 매우 좋음

30

이 태스크에서는 1개의 IP와 1개의 웹 서버를 테스트하였고 대상 시스템의 전체 상태 점수는 30점이며 이 점수는 100 척도에 기반합니다. 이는 취약성 백분율, 공격 표면, 암호화된 트래픽 등의 다중 인자에 기반한 포괄적 평가입니다. 이 테스트 시스템은 '위험함'(위험함<60, 60<=보통<85, 좋음>=85) 상태인 것으로 간주되며 점수는 30점입니다. 각 자산에서 발견된 취약성은 '자산 세부정보'에서 확인할 수 있습니다.

플랫폼이 악용 가능한 위험을 발견하지 못했습니다. 이는 이 대상의 취약성을 악용하기 어려워 위험 발생 빈도가 매우 낮거나 해킹이 발생하지 않도록 방지할 수 있을 정도로 우수한 보안 방어를 갖추었음을 의미합니다.

위험 가중 평가

중요 비즈니스 위험

성공적인 0 익스플로잇 개수

취약성

높음 51

중간 63

낮음 20

정보 0

전체 대상 개수 :	2
활성 자산 개수 :	1
활성 도메인 개수 :	1
공격 표면 개수 :	244

4-5 글로벌 공격 트렌드

1. 약한 자격 증명, 즉 악성 공격자가 **알아내기 쉬운 패스워드(Weak credential)**
2. **원격 명령 실행**(Remote Command Execution – 취약성을 악용하여 원격으로 명령을 실행하고 이를 통해 트로이목마 등 악성코드를 유포)
3. **SQL 인젝션**(SQL Injection – DB에 임의의 Query문을 주입하고 실행해서 DB가 비정상적인 동작을 하도록 조작하는 행위)
4. **크로스 사이트 스크립팅**(XSS – 웹 페이지, 게시판, 웹 메일 등에 악성 스크립트 코드를 삽입해서 공격자가 원하는 각종 악성 기능이 작동하도록 하는 공격

릿지봇을 통해서 찾아낸 해결 방법

1. 강력한 비밀번호를 사용

2. 외부에 노출되어서는 안 되는 포트를 차단

3. OS, DB, 각종 웹 애플리케이션의 최신 보안 업데이트 적용

5-1 모의 침투 테스트 및 취약점 진단 가이드

→ 릿지봇 모의 침투 테스트 및 취약점 진단 진행 시 아래 내용을 참고해주시기 바랍니다.

내부망

✓ 내부에서만 접근 가능한 호스트에 대한 침투 테스트로 방문이 필요합니다.

✓ 내부 호스트에 대해 테스트할 경우 해당 호스트에 대해 모든 포트로 접근이 가능해야 합니다.

✓ 내부망에서의 방화벽 설정은 끄고 침투 테스트를 합니다.

외부망

✓ 웹 서버(도메인 주소), 그룹웨어 서버(공인 IP) 등에 대한 침투 테스트입니다.

✓ 외부에 열려 있는 웹 서버의 경우 IP 주소는 의미가 없습니다. 무조건 도메인 주소(예 : www.estc.co.kr)로 타겟 설정을 하고 침투 테스트를 합니다.

5-2 모의 침투 테스트 및 취약점 진단 가이드

→ IP 호스트 : 침투 테스트 시 대상을 IP로 지정합니다.

→ 웹 서버 : 침투 테스트 시 대상을 도메인 주소로 지정합니다.

웹 서버 예시

A 도메인 주소의 A레코드(또는 CNAME)이 여러 개일 경우에는 라이선스도 도메인 수만큼 각각 구매를 해야 합니다.
www.estc.co.kr / shop.estc.co.kr / epc.estc.co.kr = 3ea 웹 서버 라이선스

B 도메인 주소 하위의 서브 디렉토리는 1개 라이선스만 있으면 됩니다.
www.estc.co.kr/company / www.estc.co.kr/product = 1ea 웹 서버 라이선스

5-3 IP 호스트와 웹 서버 라이선스 비교표

구분	구축형(1년)	OneTime 서비스형
최소 구매 수량	IP 20ea / Web Server 1ea	IP 5ea / Web Server 1ea
라이선스 사용 횟수	지정 IP 대상 1년 무제한 (90일 이후 IP 변경 가능)	IP당 1회
라이선스 사용 기간	1년	구매 시 1회
컨설팅	별도 비용 발생	구매 시 1회
관리	고객사에서 운영	관리 불필요

RidgeSecurity

취약점 분석 및 모의 침투 테스트

감사합니다.

RidgeSecurity의 지능형 보안 검증 로봇인 RidgeBot(릿지봇)은 위협, 취약성 및 악용에 대한 종합적인 지식을 바탕으로 모델링 되었으며, 최첨단 해킹 기술이 탑재되어 있습니다.
실제 공격자처럼 행동하여 끊임없이 익스플로잇을 찾아내고 그 결과를 문서화합니다.