Genians

정부 긴급 보안점검 즉시 대응 가이드

긴급 보안점검 IT 자산 정보의 현행화 및 문서 산출 방안

통합 보안 플랫폼 기업, 지니언스

INDEX 긴급대응

자료 배경

최근 보안 사고와 관련하여 정부는 **4대 필수 점검 항목**에 대한 조사 결과를 제출하도록 요구하고 있으며, 제출 문서에는 **CEO 서명**이 포함되어야 합니다.

이에 지니언스 제품을 사용하는 고객께서는 본 문서를 통해 **제품으로 수집 · 제공 가능한 항목의 범위**를 확인하고, **자산 점검 산출물**을 보다 신속하고 정확하게 준비하실 수 있습니다.

제출 기간

공문발송
2025-09-26

주요 정보 통신 기반 시설, ISMS 인증 기업	상장 기업	중소기업
2025-10-31 제출	2025-11-30 제출	2025-12-31 제출

4대 필수 점검 항목

01	02	03	04
4대 필수 점검 항목	**인터넷 접점 점검**	**인터넷 접점 자산 취약점**	**백업체계 점검**
IT 전체 자산에 대한 현황	인터넷에 노출 통신 가능한 환경 서버/단말	인터넷에 노출되어 있는 서버/단말 취약점	백업의 존재, 무결성, 복구 절차 등 확인 (사이버레질리언스 측면)

지니언스 제품을 통한 긴급 점검 대응 방안

NAC 도입 고객	사내 NAC를 통해 집계한 IT 자산 현황을 Excel 시트로 제공하며, End of Service (EOS) · 단종 플랫폼 등 취약 자산의 존재 여부를 식별 · 통보합니다.
EDR 도입 고객	EDR 데이터를 기반으로 대외 통신 이력을 조회하여 통신 이력이 확인된 단말/서버를 분류하고 Excel 시트로 산출합니다.

Genian NAC 기반 자산 인벤토리 데이터 확보 방안

NAC를 활용한 IT 인벤토리 데이터 확보 방식

Check 01

4p 참조

수집 가능한 IT 자산 범위 식별

* NAC는 네트워크에 연결된 자산만 식별 및 수집 가능
* NAC 센서 미설치 영역 또는 네트워크 미연결 자산은 수집 불가 → 별도 관리 필요

Check 02

5p - 7p 참조

산출 데이터 구성 및 출력 방식 정의

* 자산 정보 화면 구성 방식 선택 (ex: 장비 유형별, 네트워크 인터페이스별)
* 필요한 정보 항목(컬럼)을 선택하여 맞춤형 보고서 포맷을 구성 후 Excel 파일로 산출
* EOS(End of Service), 플랫폼 취약성 여부 등 보안 · 운영에 중요한 상태 정보를 항목에 표기 가능

Option

① **최신 플랫폼 엔진 여부 체크** * 플랫폼DB 업데이트 여부 확인

② **장비 위치 파악을 위한 설정** * 장비 연결 위치를 확인하기 위한 설정 (SNMP등)

상세한 수집 방법은 다음 페이지에서 확인하실 수 있습니다.

NAC 버전별로 수집 및 산출이 가능한 데이터입니다.

Version 6.0

어플리케이션 | 보안 등급 | 위험 등급 | 클라우드 인스턴스 | 원격자 단말현황

Version 5.0

Update 정보 | 열린 Port | CVE | 멀티 부팅 OS | 배터리 여부

공유 폴더 | 무선랜 관리 현황 | 스위치 관리 현황 | IPv6 | USB 정보

Version 4.0

IP/MAC | Platform | 노드 타입 | 사용자 계정 | Tag | On/Off | Agent 상태

등록일자 | 백신 정보 | 시스템 정보 | 패스워드 설정 유/무 | 트래픽 | 호스트 명 | CPU

MEMORY | Motherboard | Network Interface Card | 유/무선 접속(SSID) | 설치 소프트웨어

NAC 기반 인벤토리 데이터 산출 예시

NAC를 통해 산출된 IT 자산 정보 출력 화면

- 관리자 인터페이스(GUI)에 표시되는 정보 [Check 02] 예시

- Excel 형식으로 산출 가능한 자산 정보 [Check 02] 예시

노드목록

출력일 : 2025년 10월 23일 오전 8시 20분 19초 KST

GENIANS 전체 : 391

노드타입	에이전트 동작	동작	IP주소	MAC주소	플랫폼	장비 관리자	접속장치	접속포트
보안장비	설치안됨	UP	.157	91:92	amera	유승훈	o.kr	)/12
PC	설치안됨	UP	.158	BC:43	ws 10 Enterprise x64	정지수		)/24
PC	설치안됨	UP	.160	6:23	ws 10 Professional x64	김학중		1
PC	설치안됨	UP	.173	D5:F6	ws 10 Professional x64	강동현		7
PC	설치안됨	UP	.174	D6:4B	ws 10 Enterprise x64	하금수		5
서버	설치안됨	UP	.181	5:4A	ws XP	문상훈		)
PC	설치안됨	UP	.192	:7:38	ws 10 Enterprise x64	곽중현		5
PC	설치안됨	UP	.195	5:22	ws XP	송정현		1
PC	설치안됨	UP	.196	C:64	ws XP	김이신	kr	11
서버	설치안됨	UP	.203	8:34	ws 7 Professional	김현중		)/15
PC	설치안됨	UP	.204	8:16	ws 10 Professional x64	배승준		7
라우터	설치안됨	UP	.205	8:1B	r	반성군		5
서버	설치안됨	UP	.207	2:1B	ws Server 2008	김전일		)/9
PC	설치안됨	UP	.208	2:5B	ws	임변상		)/9
긴급예외	설치안됨	UP	.209	2:23	ws XP	장이수		)/9
PC	설치안됨	UP	.223	2:08	ws 10 Enterprise x64	오일중		)/24
무선접속장비	설치안됨	UP	.227	7:B4	P	한미녀		1
무선접속장비	설치안됨	UP	.230	6:5A	P	고장남		)/25
네트워킹장비	설치안됨	UP	.231	A:4A	Device	이나영		)/7
무선접속장비	설치안됨	UP	.232	7:90	P	고재필	kr	11
무선접속장비	설치안됨	UP	.233	7:9E	P	김독자		)/10
네트워킹장비	설치안됨	UP	.237	A:C6	Device	강대한		)/8
서버	설치안됨	UP	.249	A:63	ws 7 Professional	김태희	o.kr	)/12
서버	설치안됨	UP	.250	B:77	ws 10 Professional x64	권정우	o.kr	)/12
서버	설치안됨	UP	.251	3:C4	ws 7 Professional	박세중	o.kr	)/12
네트워킹장비	설치안됨	UP	.253	3:2D		강효중		1

NAC 기반 자산 수집 범위 식별

수집 가능한 범위 정의

NAC는 과거 및 현재 네트워크에 연결된 IT 자산의 상태 정보를 자동 수집합니다. 반면, 네트워크에 연결되지 않은 자산에 대해서는 별도로 관리자께서 확인 후 자산 목록을 완성 시키셔야 합니다.

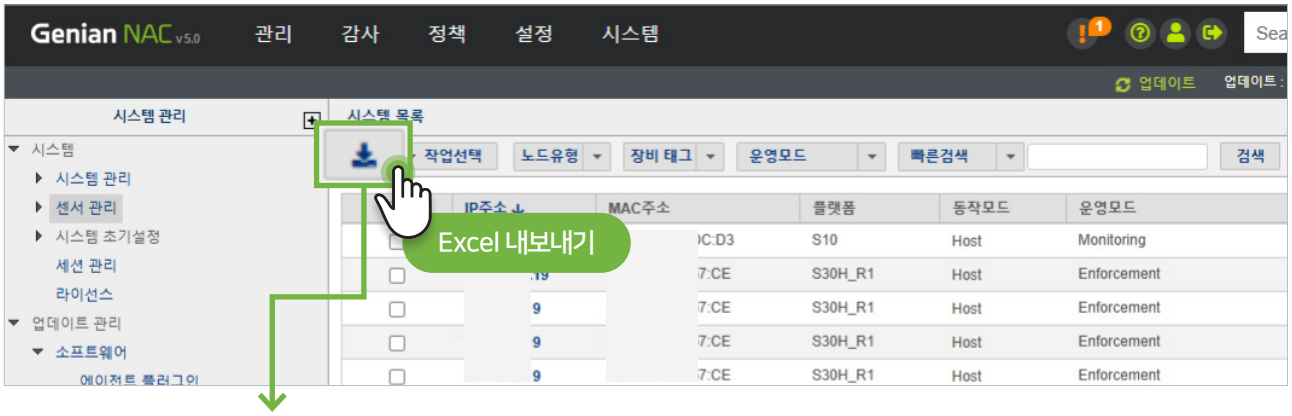
(아래 예시 - NAC 센서가 설치되지 않은 대역을 검출하는 방법입니다.)

왜 해당 과정이 필요한가요?

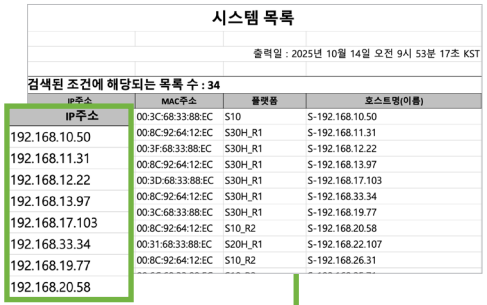
NAC 센서는 대부분의 네트워크 대역에 설치·운영되고 있으나, **비-관리 대역**이 존재할 수 있습니다.
따라서 **NAC 관리대역을 식별**하고, **그 외 대역에 대한 IT 자산 수집 대안**을 마련해야 합니다.

- **접속 경로**

Login > 시스템 > 센서 관리



NAC 센서 설치 범위 관리 대장



관리 중인 네트워크 정보 사내 네트워크 관리 대장

관리 네트워크 대역 비교 분석

관리 네트워크 대역의 비교를 통해 센서 설치 및 미설치 구간을 식별할 수 있음

NAC 기반 Excel 데이터 산출

정보 산출 정의

NAC는 수집한 IP/MAC 기반의 노드 정보를 데이터베이스에 저장합니다.
관리자는 GUI를 통해 표시 컬럼을 자유롭게 구성한 후, 해당 데이터를 Excel 형식으로 산출할 수 있습니다.

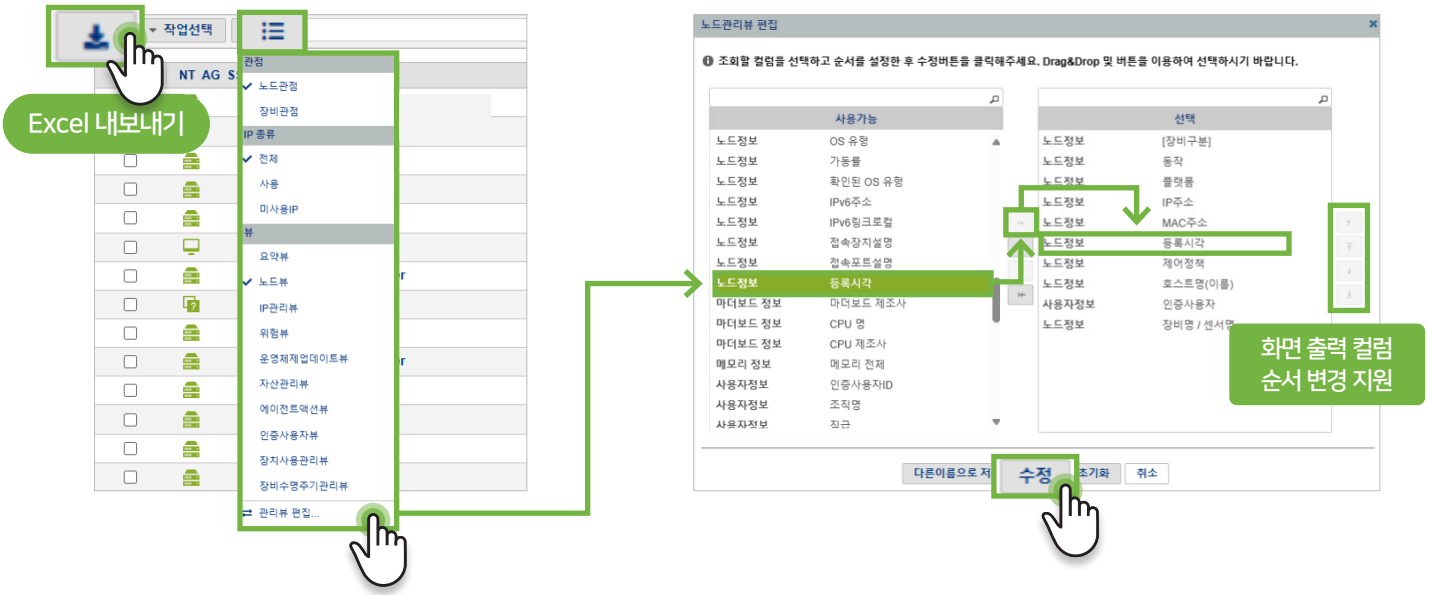
왜 해당 과정이 필요한가요?

NAC가 수집하는 데이터는 "다양한 분류(Category)와 유형(type)"으로 구성되어 있습니다.
관리자 화면(GUI)에는 자주 활용되는 핵심 정보만 제공됩니다.

관리자가 원하는 항목이 기본 화면에 포함되지 않을 경우, 표시 항목(컬럼) 구성을 변경하여 필요한 정보를 포함한 형태로 Excel 파일로 산출할 수 있습니다.

- **접속 경로**

Login > 관리 > 노드



관리뷰 편집을 통한 컬럼 변경 결과 화면

NT AG SS	동작	플랫폼	IP주소 ↑	MAC주소	등록시각
		Cisco Switch	192.168.10.2	00:00:0C:07:AC:0B	2019-10-10 13:01:16
		CheckPoint Gaia Appliance	192.168.10.3	20:67:7C:D8:85:40	2019-12-02 20:19:45
		Cisco Switch	192.168.10.4	00:FD:22:06:0F:7F	2019-10-10 13:01:16
		Cisco Switch	192.168.10.5	00:FD:22:06:2A:7F	2019-10-10 13:01:16
		ICANN, IANA Department	192.168.10.6	00:00:5E:00:01:6B	2019-10-10 13:01:16
		ICANN, IANA Department	192.168.10.7	00:00:5E:00:01:6C	2019-10-10 13:01:16
		Radware Device	192.168.10.8	2C:B6:93:4E:F8:00	2019-10-10 13:01:17
		Radware Device	192.168.10.9	2C:B6:93:4E:F1:00	2019-10-10 13:01:17

장비 혹은 NIC 기반 데이터 산출

관점(노드, 장비) 전환 기반 Excel 산출

NAC는 기본적으로 IP/MAC 기반, 즉 NIC(네트워크 인터페이스 카드) 기반으로 데이터를 수집 · 산출 합니다. 그러나 경우에 따라 자산 기준의 데이터 통합이 필요한 경우, 장비 중심 관점으로 전환하여 정보를 조회하고 Excel 형식으로 산출할 수 있는 기능을 제공합니다.

왜 해당 과정이 필요한가요?

NAC는 기본적으로 NIC(네트워크 인터페이스 카드) 단위로 자산 정보를 구성합니다. 예를 들어 하나의 장비에 다수의 LAN 카드(NIC) 가 탑재된 경우, 하나의 장비가 **여러 개의 노드 항목으로 분리되어 표시** 될 수 있습니다.

긴급 보안점검이나 취약 자산 식별과 같은 상황에서는 장비(H/W) 관점의 통합 정보 산출이 필요합니다.
* 장비 기준 전환 시 대표 NIC 정보만 출력되며, 대표 NIC 외 다른 NIC 정보는 출력되지 않습니다.

- **접속 경로**

Login > 관리 > 노드

노드 관점

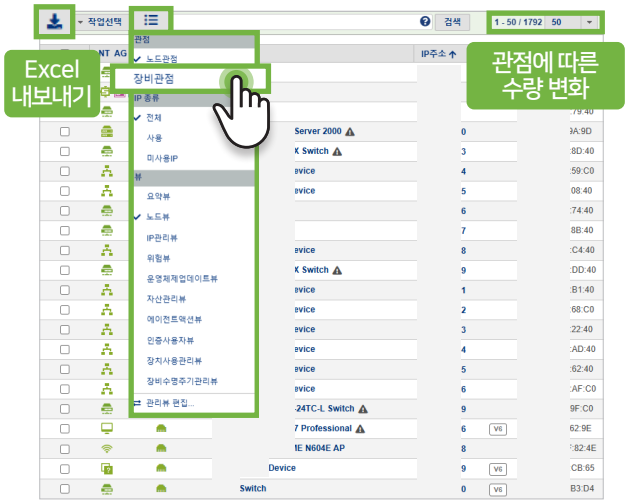
IP와 MAC조합의 기준으로 등록된 데이터

IP사용현황 목적의 자산파악이 필요할 경우장비가 사용하고 있는 NIC별로 나열하여 보여줍니다.

장비 관점

장비 또는 MAC 기준으로 등록된 데이터

※ Agent 설치 단말의 경우 복수의 인터페이스도 하나의 장비로 식별



장비현황 목적의 자산파악이 필요할 경우 장비 한 대당 하나의 노드만 보여집니다.

단종된 플랫폼 현황 식별

지원 종료 및 판매 종료 플랫폼 상태 확인

NAC를 통해 지원이 종료되거나 판매가 중단된 플랫폼을 식별할 수 있으며 이 정보를 기반으로 보안 취약 자산의 현황을 분류 및 분석할 수 있습니다.

왜 해당 과정이 필요한가요?

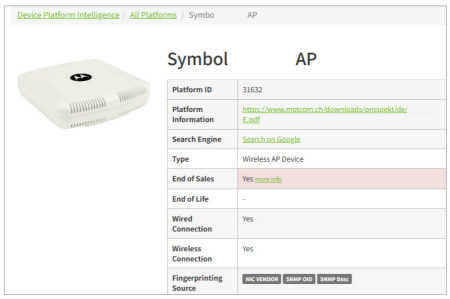
EOS(End of Service) 플랫폼은 제조사로부터 보안 패치와 기술 지원이 중단되기 때문에 공격에 매우 취약하며, 실제 국내외에서 다수의 보안 사고 사례가 확인되었습니다.

따라서 EOS 상태가 식별될 경우, 신속한 교체 또는 별도의 보안 조치가 필요합니다. 불가피하게 운영을 지속해야 하는 경우에는 담당자의 상시 모니터링과 보완 관리 체계 마련이 요구됩니다.

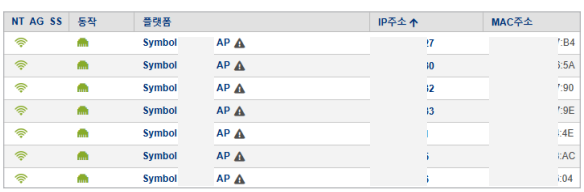
- **접속 경로**

Login > 관리 > 노드 > 현황 & 필터 > 플랫폼 사업 종료, 지원 종료, 판매 종료

Genians Device Platform Intelligence



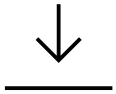
판매종료 list



Genian EDR 기반 외부 통신 이력 확보 방안

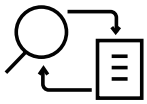
외부 통신 자산 정보 확인 절차

STEP 1



대시보드 다운로드

STEP 2



대시보드를 통한 정보 식별

STEP 3

Excel 파일로 데이터 산출

EDR 대시보드 데이터 산출 확보 방식

Check 01 **EDR 대시보드 다운로드 및 추가**

* EDR 대시보드 다운로드
  (외부 IP 통신 현황.gwj, 원격 관리 툴 접속 현황.gwj)
* EDR 대시보드 추가

Check 02 **대시보드 활용 방법**

* 외부 IP 통신 현황
* 원격 관리 툴 접속 현황

Check 03 **Excel 산출**

* 필요한 데이터를 필터링하여 Excel 포맷으로 산출

상세한 수집 방법은 다음 페이지에서 확인하실 수 있습니다. →

EDR 대시보드 등록 방법

대시보드 다운로드 및 활용

지니언스는 긴급 보안 점검 대응을 지원하기 위해 고객사에 아래와 같은 전용 EDR 대시보드를 제공합니다.

대시보드 링크 : 외부 IP 통신 현황.gwj 원격 관리 툴 접속 현황.gwj

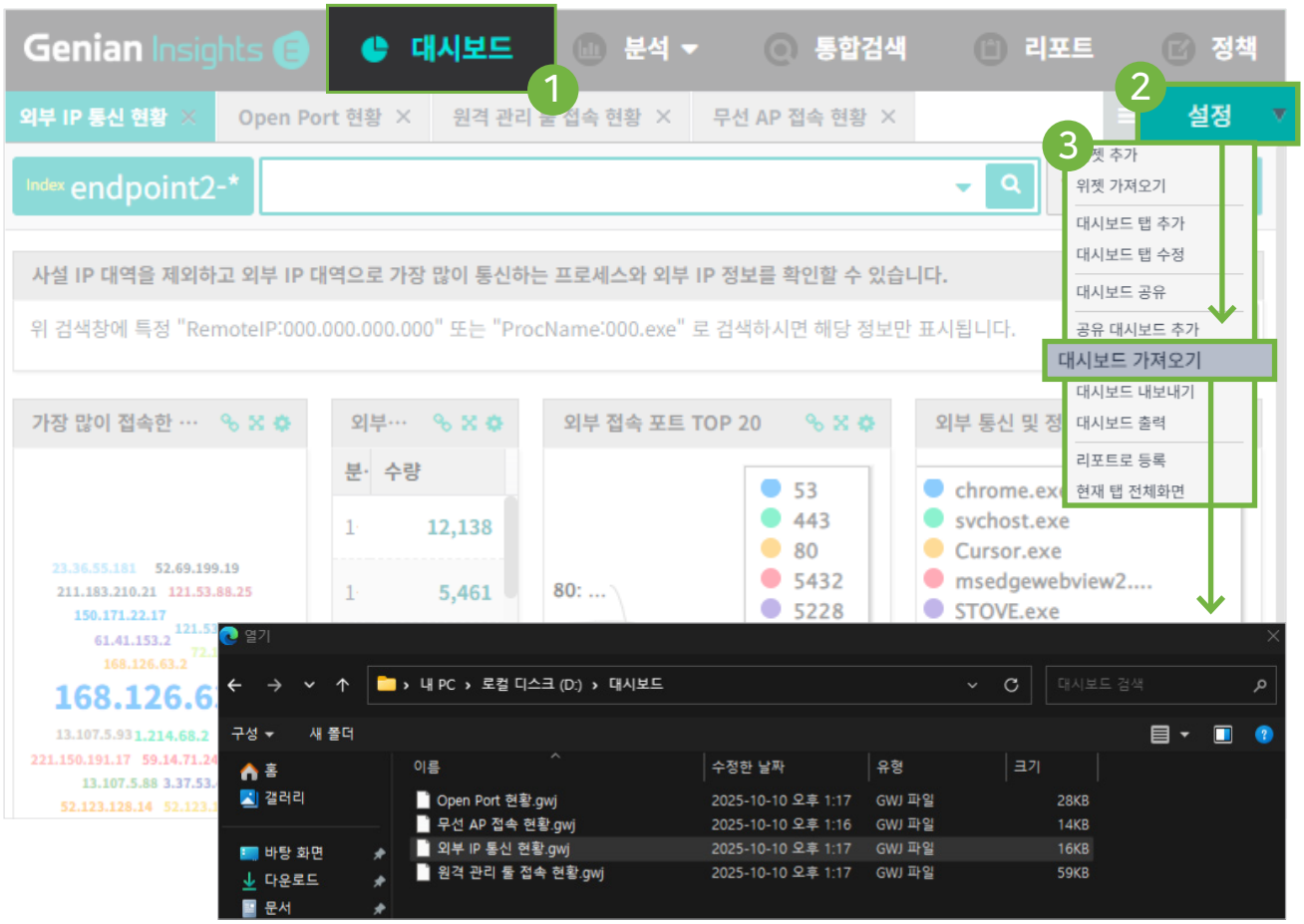
* 위의 링크에서 다운로드 가능합니다.

왜 해당 과정이 필요한가요?

보안 점검 및 대응 효율화를 위해, EDR에 저장된 데이터를 즉시 활용할 수 있는 대시보드 형태로 제공합니다. 관리자는 파일 업로드만으로 주요 정보를 빠르고 직관적으로 확인할 수 있습니다.

- **메뉴 순서**

Login > 대시보드 > 설정 > 대시보드 가져오기



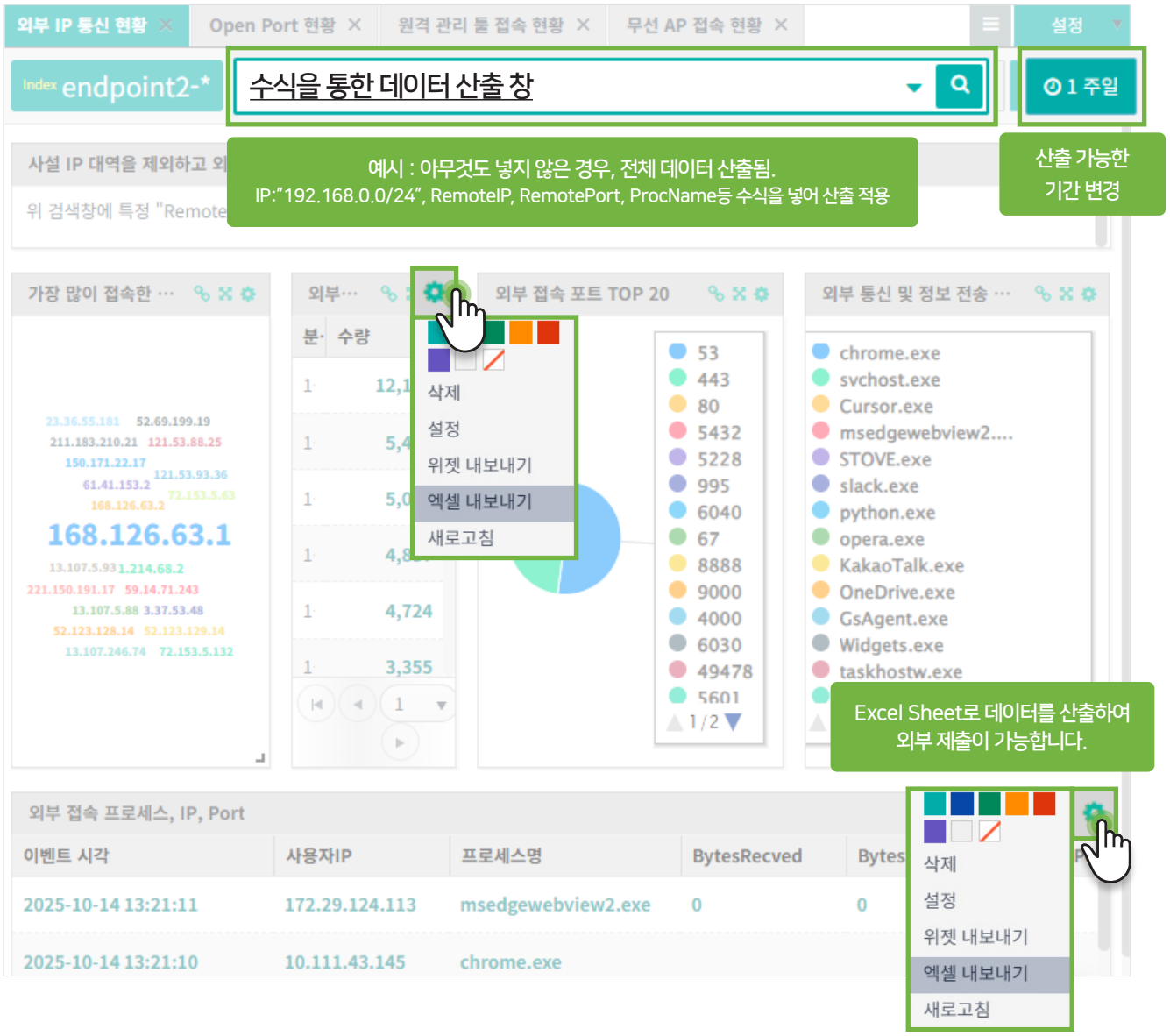
대시보드 활용 방안

외부 IP 통신 현황 확인 방법

EDR 대시보드 활용 시 기본적으로 외부 통신 관련 주요 정보가 자동 표출됩니다.
대시보드 내 검색 수식(Query) 입력을 통해서 특정 IP 대역, 포트, 프로세스명 등의 조건을 지정한 뒤에 필요한 데이터만 선별적으로 산출할 수 있습니다.

왜 해당 과정이 필요한가요?

긴급 보안 점검 대응을 위한 EDR 대시보드는, 사내 EDR이 설치된 단말 또는 서버 중 외부 IP와 통신 이력이 있는 자산을 식별할 수 있도록 구성되어 있습니다. 통신 기록을 기반으로 인터넷 접속이 발생한 IT 자산을 손쉽게 확인할 수 있습니다.



대시보드 활용 방안

원격관리 툴을 통한 접속 이력 보유 자산 확인 방법

EDR 대시보드 활용 시 원격 접속 이력이 있는 단말 정보를 자동으로 표출합니다.
조건 입력을 통해 세부 항목을 확장하거나 특정 기준으로 산출할 수 있습니다.

왜 해당 과정이 필요한가요?

해당 대시보드는 SSH, Telnet, PuTTY 등 알려진 원격 접속 도구(Remote Access Tools)를 통해 외부와 통신한 자산 정보를 산출합니다.

Together.
More Secure.

Genians

14058 경기도 안양시 동안구 벌말로66 하이필드 지식산업센터 A동 12층

대표번호 031-8084-9770 | **기술지원** 1600-9750

FAX 070-4332-1683 | **홈페이지** www.genians.co.kr

* 1:1문의는 svc@genians.com으로 연락주시면 신속히 안내드리겠습니다.