

정부 긴급 보안점검 즉시 대응 가이드

긴급 보안점검 IT 자산 정보의 현행화 및 문서 산출 방안

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



4대 필수 점검 항목

01

4대 필수 점검 항목

IT 전체 자산에
대한 현황

02

인터넷 접점 점검

인터넷에 노출 통신
가능한 환경 서버/단말

03

인터넷 접점 자산
취약점

인터넷에 노출되어 있는
서버/단말 취약점

04

백업체계 점검

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 조화하여 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

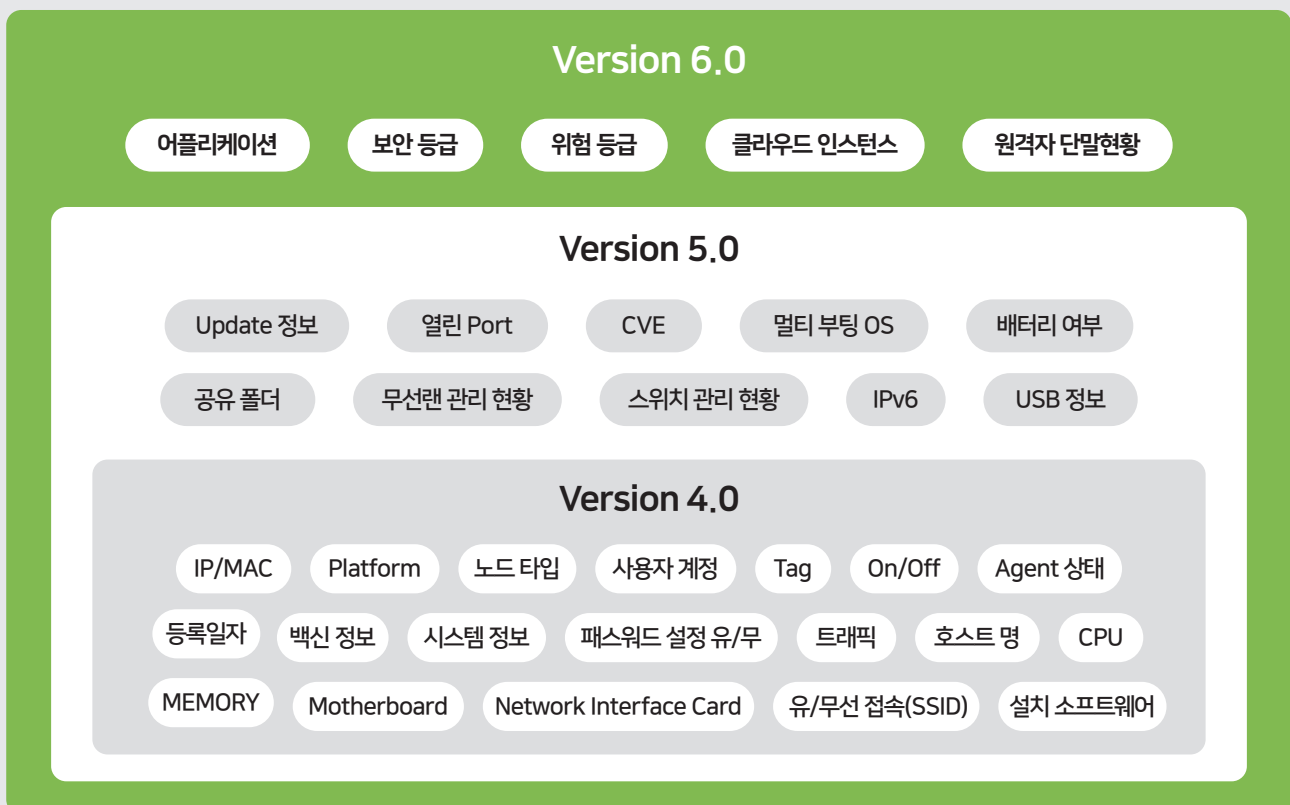
- * 자산 정보 화면 구성 방식 선택 (ex: 장비 유형별, 네트워크 인터페이스별)
- * 필요한 정보 항목(컬럼)을 선택하여 맞춤형 보고서 포맷을 구성 후 Excel 파일로 산출
- * EOS(End of Service), 플랫폼 취약성 여부 등 보안 · 운영에 중요한 상태 정보를 항목에 표기 가능

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.



NAC 기반 인벤토리 데이터 산출 예시

NAC를 통해 산출된 IT 자산 정보 출력 화면

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

작업선택

Excel 내보내기

NT	AG	SS	동작	IP주소 ↑	MAC주소	플랫폼	장비 관리자	접속장치	접속포트
				157	:91:92	nera	유승훈	.o.kr	/12
				158	:BC:43	ws 10 Enter	정지수		/24
				160	A6:23	ws 10 Profe	김학중		
				173	:D5:F6	ws 10 Profe	강동현		
				174	:D6:4B	ws 10 Enter	하금수		
				181	D5:4A	ws XP	문상훈		
				192	:C7:38	ws 10 Enter	곽중현		
				195	15:22	ws XP	송정현		
				196	AC:64	ws XP	김이신	.o.kr	1
				203	78:34	ws 7 Profes	김현중		/15
				204	38:16	ws 10 Profe	배승준		
				205	18:1B	ws Server 2	반성균		
				207	:2:1B	ws	김전일		/9
				208	:2:5B	ws	임변상		/9
				209	:2:23	ws XP	장이수		/9
				223	:2:08	ws 10 Enter	오일중		/24
				227	A7:B4	ws	한미녀		
				230	A6:5A	ws	고장남	.kr	/25

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

노드 목록

출력일 : 2025년 10월 23일 오전 8시 20분 19초 KST

GENIANS 전체 : 391

노드타입	레이아웃	동작	동작	IP주소	MAC주소	플랫폼	장비 관리자	접속장치	접속포트
보안장치	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	:5:F6	ws 10 Professional x64	강동현		7
PC	설치안됨	UP		.174	:6:4B	ws 10 Enterprise x64	하금수		3
서버	설치안됨	UP		.181	5:4A	ws XP	문상훈		3
PC	설치안됨	UP		.192	:7:38	ws 10 Enterprise x64	곽중현		3
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	ws	반성균		3
서버	설치안됨	UP		.207	2:1B	ws Server 2008	김전일		/9
PC	설치안됨	UP		.208	2:5B	ws	임변상		/9
간접예외	설치안됨	UP		.209	2:23	ws XP	장이수		/9
PC	설치안됨	UP		.223	:2:08	ws 10 Enterprise x64	오일중		/24
무선접속장치	설치안됨	UP		.227	7:B4	ws	한미녀		1
무선접속장치	설치안됨	UP		.230	6:5A	ws	고장남		/25
네트워크장치	설치안됨	UP		.231	:A:4A	ws Device	이나영		/7
무선접속장치	설치안됨	UP		.232	7:90	ws	고재필	kr	11
무선접속장치	설치안됨	UP		.233	7:9E	ws	김득자		/10
네트워크장치	설치안됨	UP		.237	:A:C6	ws 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
네트워크장치	설치안됨	UP		.253	3:2D	ws	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 대역이 존재할 수 있습니다. 따라서 NAC 관리대역을 식별하고, 그 외 대역에 대한 IT 자산 수집 대안을 마련해야 합니다.

접속 경로

Login

>

시스템

>

센서 관리

Genian NAC v5.0 관리 감사 정책 설정 시스템

시스템 관리 시스템 목록

시스템 목록

작업선택 노드유형 장비 태그 운영모드 빠른검색 검색

시스템	IP주소	MAC주소	플랫폼	동작모드	운영모드
IC-D3	S10	Host	Monitoring		
7:CE	S30H_R1	Host	Enforcement		
7:CE	S30H_R1	Host	Enforcement		
7:CE	S30H_R1	Host	Enforcement		
7:CE	S30H_R1	Host	Enforcement		

NAC 센서 설치 범위 관리 대장

시스템 목록				
출력일 : 2025년 10월 14일 오전 9시 53분 17초 KST				
검색된 조건에 해당되는 목록 수 : 34				
IP주소	MAC주소	플랫폼	호스트명(이름)	
192.168.10.50	00:3C:68:33:88:EC	S10	S-192.168.10.50	
192.168.11.31	00:8C:92:64:12:EC	S30H_R1	S-192.168.11.31	
192.168.12.22	00:3F:68:33:88:EC	S30H_R1	S-192.168.12.22	
192.168.13.97	00:8C:92:64:12:EC	S30H_R1	S-192.168.13.97	
192.168.17.103	00:3D:68:33:88:EC	S30H_R1	S-192.168.17.103	
192.168.13.97	00:8C:92:64:12:EC	S30H_R1	S-192.168.33.34	
192.168.17.103	00:3C:68:33:88:EC	S30H_R1	S-192.168.19.77	
192.168.33.34	00:8C:92:64:12:EC	S10_R2	S-192.168.20.58	
192.168.19.77	00:31:68:33:88:EC	S20H_R1	S-192.168.22.107	
192.168.20.58	00:8C:92:64:12:EC	S10_R2	S-192.168.26.31	

관리 중인 네트워크 정보 사내 네트워크 관리 대장

사내 네트워크 관리 대장			
2025년 관리 대장			
IP주소	위치정보	층수	비고
192.168.10.50	본점	4F_5	
192.168.11.31	본점	6F_3	
192.168.12.22	용인 지점	2F_6	
192.168.13.97	이수 지점	1F_4	
192.168.17.103	김포 지점	1F_2	
192.168.13.97	망원 지점	2F_5	
192.168.17.103	한남 지점	1F_4	
192.168.20.58	한티 지점	3F_12	
192.168.61.100	선릉 지점	2F_8	
192.168.103.50			

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 표시될 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

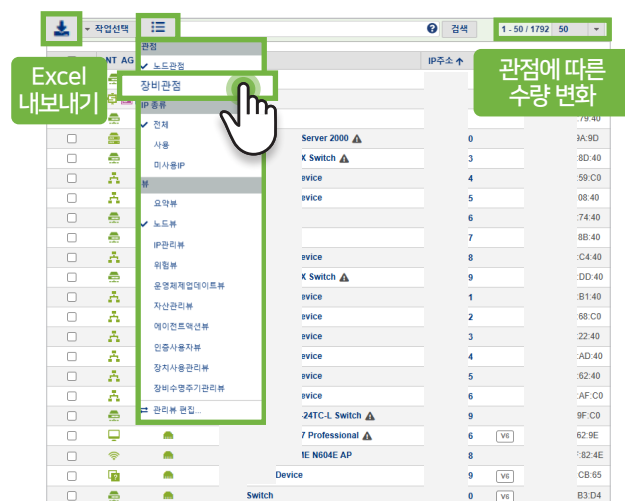


IP사용현황 목적의 자산파악이 필요할 경우장비가 사용하고 있는 NIC별로 나열하여 보여줍니다.

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

Excel 내보내기

Geniens Device Platform Intelligence

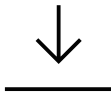
판매종료 list

NT	AG	SS	동작	플랫폼	IP주소	MAC주소
				Symbol AP	17	1B4
				Symbol AP	10	15A
				Symbol AP	12	190
				Symbol AP	13	19E
				Symbol AP		14E
				Symbol AP		1AC
				Symbol AP		104

Genian EDR 기반 외부 통신 이력 확보 방안

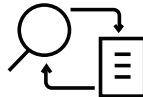
외부 통신 자산 정보 확인 절차

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 톨 접속 현황.gwj)
- * EDR 대시보드 추가

Check 02

대시보드 활용 방법

- * 외부 IP 통신 현황
- * 원격 관리 톨 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

The screenshot displays the Genian Insights EDR interface. The top navigation bar includes 'Genian Insights', '대시보드' (Dashboard), '분석' (Analysis), '통합검색' (Integrated Search), '리포트' (Report), and '정책' (Policy). The '대시보드' menu is highlighted with a green box and a circled '1'. Below the navigation bar, there are tabs for '외부 IP 통신 현황', 'Open Port 현황', '원격 관리 툴 접속 현황', and '무선 AP 접속 현황'. The '설정' (Settings) menu is highlighted with a green box and a circled '2'. A dropdown menu from '설정' shows options like '대시보드 가져오기' (Import Dashboard), which is highlighted with a green box and a circled '3'. A file explorer window is open, showing the downloaded dashboard files: 'Open Port 현황.gwj', '무선 AP 접속 현황.gwj', '외부 IP 통신 현황.gwj', and '원격 관리 툴 접속 현황.gwj'.

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.

수식을 통한 데이터 산출 창

예시 : 아무것도 넣지 않은 경우, 전체 데이터 산출됨.
IP:"192.168.0.0/24", RemoteIP, RemotePort, ProcName 등 수식을 넣어 산출 적용

산출 가능한 기간 변경

Excel Sheet로 데이터를 산출하여 외부 제출이 가능합니다.

이벤트 시각	사용자IP	프로세스명	BytesRecv	Bytes
2025-10-14 13:21:11	172.29.124.113	msedgewebview2.exe	0	0
2025-10-14 13:21:10	10.111.43.145	chrome.exe		

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.

The screenshot displays the Genian Insights dashboard interface. At the top, there's a navigation bar with tabs like '대시보드', '분석', '통합검색', '리포트', and '정책'. Below this, a search bar contains the text '수식을 통한 데이터 산출 창' (Data output window using formulas). A green box highlights the search bar and a '1주일' (1 week) filter button. Below the search bar, a green box contains the text '예시 : IP:"192.168.0.0/24", RemoteIP, RemotePort, ProcName 등 수식을 넣어 산출 적용' (Example: IP:"192.168.0.0/24", RemoteIP, RemotePort, ProcName etc. use formulas to apply output). Another green box on the right says '산출 가능한 기간 변경' (Change outputable period). The main area shows several widgets. The '네트워크 사용 현황' (Network usage status) widget has a dropdown menu open with options: '삭제' (Delete), '설정' (Settings), '위젯 내보내기' (Export widget), '엑셀 내보내기' (Export to Excel), and '새로고침' (Refresh). The '네트워크 접속 현황' (Network connection status) widget shows a pie chart and a list of IP addresses. The '네트워크 접속 결과' (Network connection result) widget shows a success rate of 98.1% (60,495) and a failure rate of 1.9%. The 'powershell 을 통한 ssh 접속 현황' (SSH connection status via powershell) widget shows a success rate of 100.0% (22) and a failure rate of 0.0% (0). The 'powershell 을 통한 ss...' widget shows a success rate of 100.0% (22) and a failure rate of 0.0% (0).

Together. More Secure.

Genians

14058 경기도 안양시 동안구 별말로66 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.