GENIANS WHITEPAPER

NAC의 눈, DPI

Device Platform Intelligence

GENIANS, INC.
Next-Gen Network Access Control for the IoT era
mkt@genians.com

Genians

Introduction *

최근 CCTV 해킹 사고가 심심치 않게 보도되고 있습니다. 단순히 가정집 엿보기의 수준을 넘어 기업의 정보유출 등 심각한 부작용을 낳고 있습니다. 다수의 사례는 해외 등 원격 네트워크를 통하여 패스워드 설정 오류를 이용하거나 CCTV 단말의 취약성을 이용하는 것으로 알려지고 있습니다. 많은 기업(관)에서 안전과 보안을 목적으로 CCTV를 사용하고 있습니다. 귀사의 CCTV는 안전합니까? 혹시 누군가가 우리 사무실을 24시간 들여다 보고 있는 것은 아닐까요?

네트워크는 더 넓어지고 복잡해지고 있습니다. 네트워킹이 필요한 새로운 단말들이 지속적으로 연결되고 있습니다. 기업의 네트워크는 더 이상 데스크톱과 스마트폰의 전유물이 아닙니다. 업무용 패드, 바코드스캐너, AP(Access Point), Video Surveillance(IPTV 등), 디지털 도어, 방범장치, 기타 IoT(사물인터넷) 장비 등 종류를 헤아릴 수 없이 빠르게 증가하고 있습니다. 이에 따라 보안위협 역시 증가하고 있습니다.

급변하는 상황 속에서 네트워크에 접속하는 다양한 기기를 실시간으로 인지하고 정확히 파악하는 것이 날로 어려워 지고 있습니다. 네트워크에 연결되는 사물인터넷(IoT)과 관련된 단말은 얼마나 될까요? 사물인터넷의 범주를 명확히 정의하기는 어렵지만 시스코(Cisco)는 그 수가 2014년 144억개에서 2020년 501억개로 약3.5배 증가할 것이라고 예측하였고, Machina Research는 M2M(Machine to Machine) 시장에서 2014년 45억개에서 2024년 290억개로 증가할 것이다라고 전망하고 있습니다. 'Gartner 보고서'와 'Forbes Developing The Connected World Of 2018 And Beyond' 역시 2020년에는 약 200억개 이상의 단말이 네트워크에 연결될 것으로 전망하고 있습니다. 더불어 보안위협 역시 증가할 것으로 예상하고 있습니다.

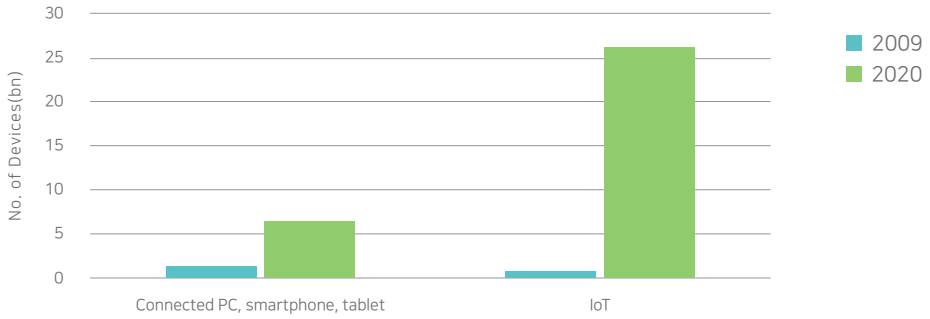


Figure 1. Total of Connected IoT Devices
* Gartner (November 2013)

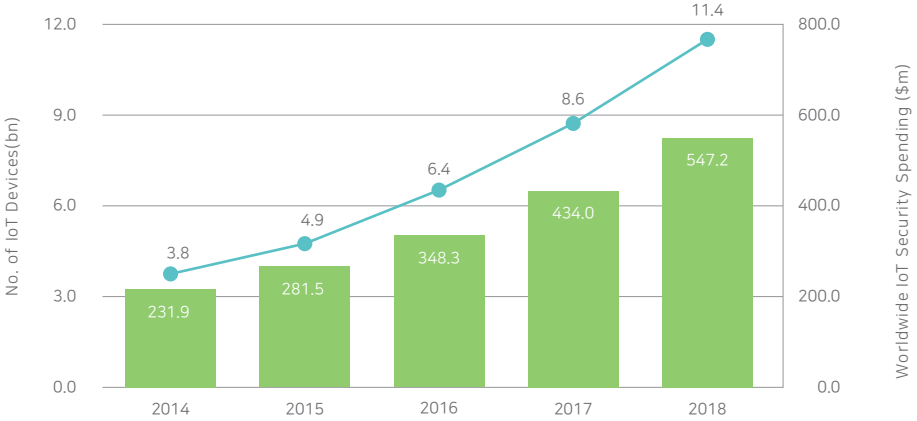


Figure 2. IoT Security Spending

사물인터넷(IoT) 과 보안위협의 증가

컴퓨터, 스마트폰, 태블릿 PC를 비롯하여 사물인터넷(IoT) 기기들의 연결은 불과 몇 년 사이에 큰 폭으로 증가되고 있습니다. 단말 증가에 따른 관리의 어려움과 동시에 관리되지 않은 단말의 잠재적인 보안위협 역시 크게 증가하고 있습니다.

최근 국내 인터넷전문가협회가 인터넷 분야 분야 전문가를 대상으로 한 설문 조사에 의하면 사물인터넷 상용화를 위해 가장 필요한 조건으로 '철저한 보안'이 꼽혔으며, 사물인터넷 보급의 가장 큰 우려는 '해킹위험'으로 조사되었습니다. 지금까지는 해킹 등으로 인한 피해가 개인정보 유출, 금전상 손해 정도에 국한되었으나, 사물인터넷 환경에서의 보안 사고는 사고적 재해나 인명사고로 이어진다는 데 문제의 심각성이 있습니다. 또한 사물인터넷은 아래와 같은 특징으로 기존 IT 보안 환경을 더욱 복잡하게 만들 수 있으며 잘 운용되고 있는 기존의 정보보안 체계에 누수(Security Hole)를 발생시킬 수 있습니다.

1) 노출영역(Attack Surface)의 확대
   - 네트워크 연결이 증가함에 따라 노출영역이 함께 확대됨

2) 자원제약(Resource Limitation)
   - 다수의 IoT 기기는 저 사양으로 별도의(임베디드 보안 기술 등)기술이 요구됨

3) 개방형 플랫폼(Open Platform)
   - 리눅스 등, 개방형 플랫폼 소스는 취약점 발견 및 이를 이용한 공격이 용이함

4) 낮은 보안 수준
   - 다수의 기 출시된 상용 IoT 기기의 보안 수준이 매우 낮음.
     (2015년 시만텍 자료에 따르면 스마트홈 기기의
     패스워드 강도, 상호인증 등 보안 기능이 부족한 것으로 나타났으며 인텔(McAfee)의 연구에서도 유사한 결과가 도출됨)

5) 피해 심각성 및 범위
   - 헬스케어, 자율주행, 교통 시스템 해킹 등은 기계적 장치를 넘어 사람의 생명까지 위협

이제 IoT에 대한 보안까지 고려해야 합니다. 보안 관리 환경은 더욱 복잡해 지고 더욱 어려워지고 있습니다. 우리는 어떻게 대응해야 할까요? 시만텍(Symantec)의 "An Internet of Things Reference Architecture" 보고서는 IoT 보안을 위한 주요 토대(Cornerstone) 4가지를 언급하고 있습니다. 그것은 바로 Protecting Communication, Protecting Device, Managing Device and Understand your System 입니다. 가장 중요한 것은 IoT 기기에 대한 가시성(Visibility)을 확보하는 것 입니다. 나머지 모든 것은 그 이후 입니다.

단말의 가시성(Visibility) 확보

지니언스는 가시성 확보의 중요성을 잘 알고 있습니다. 이미 2012년에 발간된 "Preparing BYOD Invasion by Genian NAC Suite (v4.0)"에서 BYOD(Bring Your Own Device) 환경에서의 모바일 기기의 인식(Awareness) 비율을 언급하였습니다.

기기를 완전히 인식하고 있는 비율은 고작 9% 였습니다. 또한 많은 관리자들이 이러한 기기의 인식 문제를 가장 심각한 위협이라고 언급하였으며 이는 기기에 대한 포괄적인 보안정책(Comprehensive Security Baseline)의 수립과 이행에 큰 걸림돌이라고 지적하였습니다.

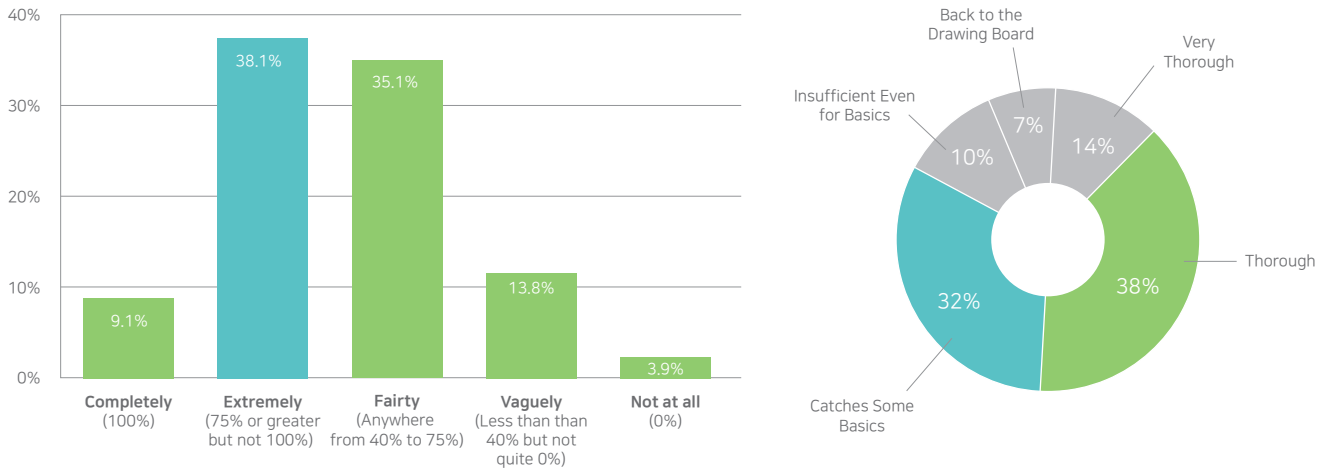


Figure 3. State of Mobile Device Awareness, SANS Mobile/BYOD Security Survey 2012

10년 가까이 지난 지금, 변화된 IoT 환경에서 우리의 인식에 대한 역량은 얼마나 개선되었을까요? 트렌드마이크로(TrendMicro)는 2018년 조사보고서를 통하여 IoT 보안 위협에 대해 인식하고 있는 비율이 14% 이며, IoT 솔루션을 도입 / 운영하기 전에 보안요구사항을 정의할 수 있는 비율은 37%라고 언급하고 있습니다. 또한 기업에서 이루어지는 IoT 관련 공격의 절반이상(54%)이 사무실 기기를 대상으로 하고 있음을 말해주고 있습니다.

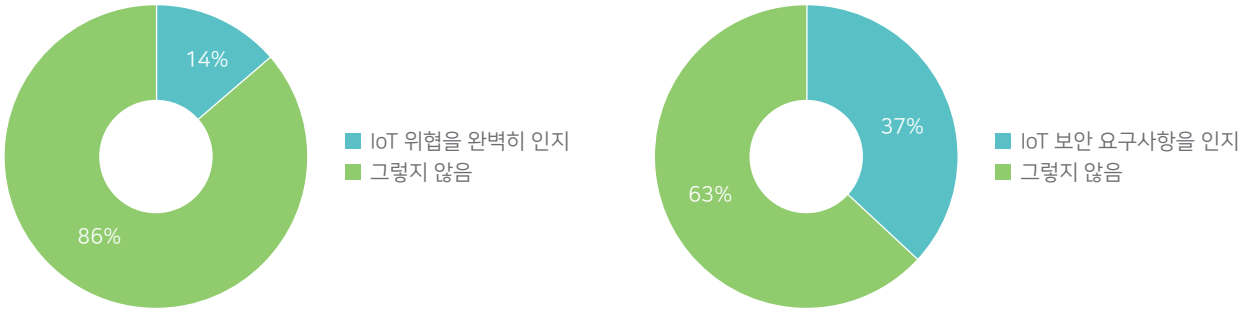


Figure 4. Trendmicro Research Finds Major Lack of IoT Security Awareness, Nov. 2018

불행히도 여전히 우리는 환경변화에 따른 보안 위협을 인식하고 대응방안을 찾는데 어려움을 겪고 있는 것 같습니다. 그리고 이러한 어려움은 단기간에 해소될 것 같지 않습니다.

Our Approach

Genian NAC는 단말의 가시성 확보에서 출발합니다. NAC를 통하여 네트워크에 연결된 모든 유/무선 단말을 탐지하고 정확히 분류할 수 있습니다. 단말의 IP/MAC 주소뿐 아니라 단말의 종류(PC/모바일/서버/라우터/스위치/보안장비 등)와 단말의 이름, 플랫폼의 상세정보(Canon iR ADV C5535 Printer)를 포함한 다양한 정보를 확인할 수 있습니다. 사용자 인증과 접근통제 등의 많은 보안기능은 그 이후 입니다.

NT AG SS	위험	동작	동작상태차트	IP주소	MAC주소	정책	제어정책	호스트명(이름)	플랫폼
				172.29.20.1	60:12:8B:D0:6C:BB		Default Policy	CANOND06CBB	Canon iR ADV C5535 Printer
				172.29.20.3	84:BA:3B:15:47:6B		Default Policy	CANON15476B	Canon iR ADV C3530 Printer
				~~172.29.20.4~~ V6	44:8A:5B:6A:A2:95		Default Policy		
				172.29.20.5	AC:E2:D3:C1:42:17		Default Policy	HPC14217	HP HP OfficeJet Pro 8210
				172.29.20.6	~~98:E7:F4:44:FE:6D~~		Default Policy	SA44FE6D	Samsung SL-J3520W Series
				172.29.20.6	98:E7:F4:FB:9A:0D		Default Policy		Samsung SL-J3520W Series

Figure 5. Genian NAC v5.0 노드 현황

지니언스㈜는 단말의 가시성을 확보하는 것이 보안관리의 첫 걸음 이라는 것을 잘 알고 있습니다. 그리고 이를 위해 오랜 기간 많은 준비를 진행하였습니다. GPDB(Genian Platform DataBase)는 그 결과 중 하나 입니다. 이미 모든 Genain NAC에 탑재되어 관리자도 미처 인식하지 못한 단말을 찾아 확인시켜 주고 보안정책 수립 및 운영을 위한 토대를 제공하고 있습니다. 이미 3만 여 종의 단말을 탐지/식별할 수 있으며 스마트폰 등 새로운 단말의 출시와 거의 동시에 GPDB도 업데이트 됩니다.

아래 내용은 2019년 4월 현재 출시 예정인 삼성전자의 최신 스마트폰 '갤럭시 폴드(Galaxy Fold)' 가 탐지되어 GPDB에 반영된 내용을 보여줍니다. GPDB는 이제 단말 탐지의 범위와 업데이트 속도, 정보제공의 양 등을 고려할 때 Genian NAC의 핵심 인프라로 확고히 자리매김 하고 있습니다.

Node Type	Manufacturer	Platform Name	OS	Connection ...	CPEs	CVEs	Mat...	DRs	DR ID	Rev
Mobile Device	SAMSUNG ELECTRONICS CO., LTD.	Samsung Galaxy Fold Phone	Android	Wireless	0	0	4	6		
									BDR-27830	kkui
									BDR-29195	ente
									BDR-27832	ejgir
									BDR-29196	ente
									BDR-27831	kkui
									BDR-29387	ejgir

Figure 6. GPDB에서 Samsung Galaxy Fold Phone의 탐지

하지만 지니언스㈜는 IoT(사물인터넷) 시대에 GPDB로는 충분하지 않다고 생각합니다. 단말에 취약점이 존재하지는 않을까요? 단종이 되었거나 제조사가 사라져 유지보수의 문제가 있지는 않을까요? 더 많은 정보가 필요하지 않을까요?
이러한 질문에 대한 해답, Genian DPI를 소개 합니다.

Genian DPI
(Device Platform Intelligence)

DPI는 GPDB의 업그레이드 버전을 의미합니다. 이전의 GPDB 보다 더 다양한 단말을 더 정확하게 탐지할 수 있고 더 많은 유용한 정보를 직관적으로 제공합니다. 기존의 GPDB가 단말을 탐지하여 분류하고 인지하는데 초점을 맞추었다면 DPI는 보안관리 및 운영을 위한 확장정보와 위협(취약성)정보를 추가로 제공합니다. 이를 통해 단말 또는 단말을 통해 발생할 수 있는 사이버 위협뿐만 아니라 비즈니스 위협에도 대응할 수 있게 됩니다. 이제 가시성의 확대를 통하여 단말로부터 야기될 수 있는 종합적인 위험(Risk)을 효과적으로 관리할 수 있게 됩니다.

	GPDB(Genian Policy DataBase)	DPI(Device Platform Intelligence)
Device Identity	디바이스 식별 정보	디바이스 식별 정보
Device Context	N/A	디바이스 확장 정보
Device Risk	N/A	디바이스 위협 정보

Table 1. GPDB 와 DPI 비교

실제 DPI가 제공하는 정보의 목록은 아래와 같습니다. (2019년 4월 현재)

구분	세부 정보
디바이스 식별 정보 (Device Identity)	- 디바이스 제조사, 이름, 모델번호 - 디바이스 사진 - 네트워크 연결 방식(Wired/Wireless) - 디바이스 상세 정보 URL
디바이스 확장 정보 (Device Context)	- 제조사 명칭 - 제조사 홈페이지 URL - 본사의 위치와 현재 사업 진행 여부 - 제품 판매 종료(End of Sales) 여부 - 제품 지원 종료(End of Support) 여부 - 검색엔진 연결 URL
디바이스 위협 정보 (Device Risk)	- 디바이스에 보고된 CVE 정보 (CVE No. / Severity / Description 등) - 제조사에 보고된 CVE 정보 (CVE No. / Severity / Description 등)

Table 2. DPI가 제공하는 디바이스 관련 정보

이러한 정보는 매우 유용합니다. 이제 관리자는 자신의 네트워크에 존재하는 단말 중에 CVE를 통하여 취약성이 보고된 단말 만을 빠르게 찾아 조치할 수 있게 됩니다. 또는 판매가 중단되었거나(End Of Sales) 지원이 중단된(End Of Support) 단말 만을 빠르게 찾아 업그레이드 및 교체 계획을 수립할 수 있습니다. CCTV 와 같이 외형이 비슷하거나 제조사가 다양한 단말에 대하여 사진을 통해 정확히 대상을 인식할 수 있습니다. 제조사의 사업진행 계속 여부나 폐업 등의 정보를 확인하여 구매계획을 수립하는데 도움을 줄 수 있습니다.

Genian NAC v5.0 사용자는 DPI 기능을 제한 없이 사용할 수 있습니다. 예를 들어 GPDB를 통하여 아래와 같이 'D-Link DIR-400 Wireless Router' 을 탐지하는 것이 가능했습니다.

동작상태차트	IP주소	MAC주소	정책	제어정책	호스트명(이름)	NIC벤더	플랫폼
	~~172.29.20.108~~	C4:12:F5:5B:94:FF		Default Policy	DIR-400	D-Link	D-Link DIR-400 Wireless Router
	172.29.20.149	C4:12:F5:4C:83:FA		Default Policy		D-Link	D-Link DIR-400 Wireless Router
	~~172.29.20.224~~	C4:12:F5:4C:83:FA	DHCP	Default Policy		D-Link	D-Link DIR-400 Wireless Router

Figure 7. GPDB를 이용한 'D-Link'디바이스 확인

그러나 DPI를 이용하면 아래와 같은 추가적인 정보의 확인이 가능합니다.

D-Link DIR-400 Wireless Router

Platform Information	http://www.dlink.ru/mn/products/5/760_b.html
Search Engine	Search on Google
End of Sales	Yes more info
End of Support	Yes more info
Wired Connection	Yes
Wireless Connection	Yes
Fingerprinting Source	HTTP NIC VENDOR
Added at	Apr 30, 2019
Manufacturer Name	D-Link Systems, Inc.
Homepage	http://www.dlink.com
Headquarters	Taiwan
Business Status	Ongoing

Suggest Update

Platform's Common Vulnerabilities and Exposures (CVE)

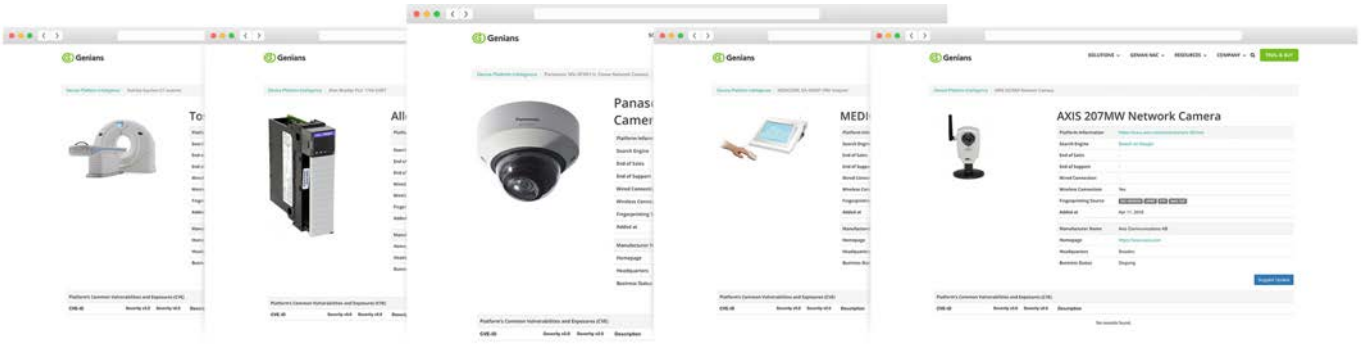
CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2009-3347 09/24/2009		HIGH	Buffer overflow on the D-Link DIR-400 wireless router allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.10 through 8.11. NOTE: as of 20090917, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.

Manufacturer's Common Vulnerabilities and Exposures (CVE)

CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2018-19300 04/11/2019	CRITICAL	HIGH	On D-Link DAP-1530 (A1) before firmware version 1.06b01, DAP-1610 (A1) before firmware version 1.06b01, DWR-111 (A1) before firmware version 1.02v02, DWR-116 (A1) before firmware version 1.06b03, DWR-512 (B1) before firmware version 2.02b01, DWR-711 (A1) through firmware version 1.11, DWR-712 (B1) before firmware version 2.04b01, DWR-921 (A1) before firmware version 1.02b01, and DWR-921 (B1) before firmware version 2.03b01, there exists an EXCU_SHELL file in the web directory. By sending a GET request with specially crafted headers to the /EXCU_SHELL URI, an attacker could execute arbitrary shell commands in the root context on the affected device. Other devices might be affected as well.
CVE-2019-9126 02/25/2019	HIGH	MEDIUM	An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. There is an information disclosure vulnerability via requests for the router_info.xml document. This will reveal the PIN code, MAC address, routing table, firmware version, update time, QOS information, LAN information, and WLAN information of the device.

Figure 8. DPI를 이용한 'D-Link' 디바이스 확인

이제 단말 식별의 한계는 사라졌습니다. 사무용기기는 물론이고 CCTV 와 프린터, 스캐너, 게임기, 무선접속 장치(AP), 산업용제어장치(PLC 등) 심지어 의료기기와 작곡용 MIDI까지 네트워크에 연결된 모든 장비를 새로운 방법으로 확인하고 관리할 수 있습니다.



단말 탐지와 정확성

DPI는 단말 관리를 위한 유용한 정보를 제공합니다. 이를 위해 무엇보다 정확한 단말의 탐지가 필요합니다. Genian NAC는 어떠한 네트워크 환경에서도 정확한 단말을 탐지하기 위한 기술과 인프라를 보유하고 있습니다. 아래와 같은 단계를 반복적으로 수행함으로써 더욱 정확하고 정교한 단말의 탐지가 이루어 집니다.

✕ 정보수집 단계

단말이 네트워크에 연결되면 정보수집이 시작됩니다. 정보수집은 크게 능동적 수집(Active Scan) 과 수동적 수집(Passive Scan) 방식으로 구분할 수 있습니다.

A. 능동적 수집(Active Scan)
- HTTP User-Agent, TCP Fingerprinting 등 10가지 이상의 방법이 사용됩니다.
- 단말을 대상으로 특정한 정보를 전송하고 회신되는 정보를 수집합니다.
- 일반적인 사무실 환경 등에서 운영이 가능합니다.

B. 수동적 수집(Passive Scan)
- DHCP, SMTP 등 5가지 이상의 방법이 사용됩니다.
- 단말을 대상으로 아무 정보를 전송하지 않고 오직 전달되는 정보만을 수집합니다.
- 설비, 제조, 라인 등의 제한적 환경에서 운영이 가능합니다.

✕ 정보분석 단계

수집된 내용을 분석하여 유의미한 정보를 확인합니다. 특정 값(Value)의 유무, 기술(description)정보, 약속된 행동 및 정의된 표준 등이 단말을 식별하고 특징을 구별 짓게 하는 구분자(Identifier)로 활용됩니다.

✕ 패턴생성 단계

분석된 정보의 묶음(세트)으로 특정 단말을 탐지 및 정의(Define)할 수 있는 패턴을 생성합니다.

✕ 매칭 단계

정보 수집과 동시에 매칭이 시도 됩니다. 만약 단말 탐지를 위한 패턴과 일치하는 경우 즉시 해당 단말로 식별됩니다. 만약 패턴이 존재하지 않는 경우 재처리 과정을 거쳐 단말 탐지를 위한 패턴생성 단계를 거치게 됩니다.

위의 4단계를 통해 단말은 완전히 식별될 수 있습니다. 이후 DPI 에는 단말을 대상으로 부가적인 정보(디바이스 확장 정보)가 추가 됩니다. 제조사 및 사업에 관한 정보는 물론이고 취약점 정보(CVE, Common Vulnerability & Exposure) 와 공통 플랫폼 목록(CPE, Common Platform Enumeration) 등이 추가되어 저장 됩니다. 이것은 향후 더욱 더 많은 관련 정보를 제공할 수 있는 기반이 됩니다.

Conclusion *

가트너 보고서에 따르면 2020년 전세계 PC 등을 포함하는 IoT 기기의 수가 200억대에 이를 것이라 전망하고 있습니다. 국내의 상황은 이보다 더 급격하게 성장하고 있습니다. 국내 IoT 기술은 다른 나라보다 상대적으로 높게 평가되고 있습니다. 2019년 IDC 보고서에 따르면 우리나라의 IoT 시장 규모는 세계 5위로 추산되었습니다. 2019년 과학기술정보통신부 보도자료에 따르면, 2018년 IoT 산업의 사업체 수는 2천여개사이며, 매출액은 8조 6천억원 규모로 전년대비 18.6%의 증가세를 보이고 있다고 합니다. 이 같은 추세라면 향후 얼마나 다양한 단말이, 얼마나 많이 출시될까요? 어떻게 가시성을 확보할 수 있을까요? 단말관리와 보안관리의 두 마리 토끼를 잡기가 점점 더 어려워 지고 있습니다. 이것이 디바이스 플랫폼 인텔리전스, DPI가 필요한 이유 입니다.
명심하십시오. DPI는 단순히 단말의 정보 분석만을 위한 솔루션이 아닙니다. 안전한 네트워크 환경의 구축을 위한 출발점이며 누수 없는 가시성의 완성은 보안관리의 완성 입니다.

참조 URL
https://www.genians.com/device-platform-intelligence/
https://www.genians.com/cybersecurity-solutions/#Device_Platform_Intelligence

CONTACT US
본 자료 및 내용문의 : mkt@genians.com

Genians

Next-Gen Network Access Control for the IoT era

2005년 설립된 지니언스㈜는 국내 NAC(Network Access Control) 시장을 선도하며 글로벌 비즈니스 확장을 통해 보안 소프트웨어 전문기업으로 성장하고 있습니다. 네트워크 보안 및 단말 분석 분야 특화기술을 기반으로 내부 보안에 특화된 제품 라인업을 보유 중입니다. 네트워크에 접속하는 단말의 가시성을 확보하여 제어하는 네트워크 접근 제어 솔루션 '지니안 NAC (Genian NAC)'를 통해 국내 시장을 선도하고 있습니다. 2017년 단말 기반 지능형 위협 탐지 및 대응 솔루션 '지니안 인사이츠 E (Genian Insights E)'를 출시하며 EDR (Endpoint Detection & Response) 시장에 진출했습니다. 2016년 1월 해외사업 시작과 함께 미국 보스턴에 현지법인을 설립한 바 있으며 2017년 8월 코스닥에 상장했습니다.

Doc. v 1.0-KO