의료장비 보안 취약점 분석을 위한 POC 사례

(2023년 5월 23일)

한기태(kthan@kuh.ac.kr)

[목 차]

1. POC 배경

◆ 네트워크 범위 : 건국대학교 병원 전체 네트워크

◆ 대상 : 의료장비를 포함하는 각종 자산

◆ 분석 목적 : 자산의 가시화 및 통신 현황 분석

1. POC 배경

POC 목 적

1. 자산 식별 및 가시화

- 건국대병원 전체 네트워크 자산 식별 및 가시화
- 각종 의료장비, 관리 PC등 유형별 정리
- VLAN or IP 대역별 그래프 정리
- 보안 취약점 가시화

2. 통신 현황 분석

- 악성코드/바이러스 탐지
- 네트워크 품질을 저하시킬 수 있는 요소 분석
- 이상징후 탐지

2. 방화벽을 이용한 POC

2-1) POC 개요

① 방화벽 제품 : Paloalto IoMT Security (라이센스)

② 기간 : 2023년 3월 6일 ~ 3월 29일 (약 23일간)

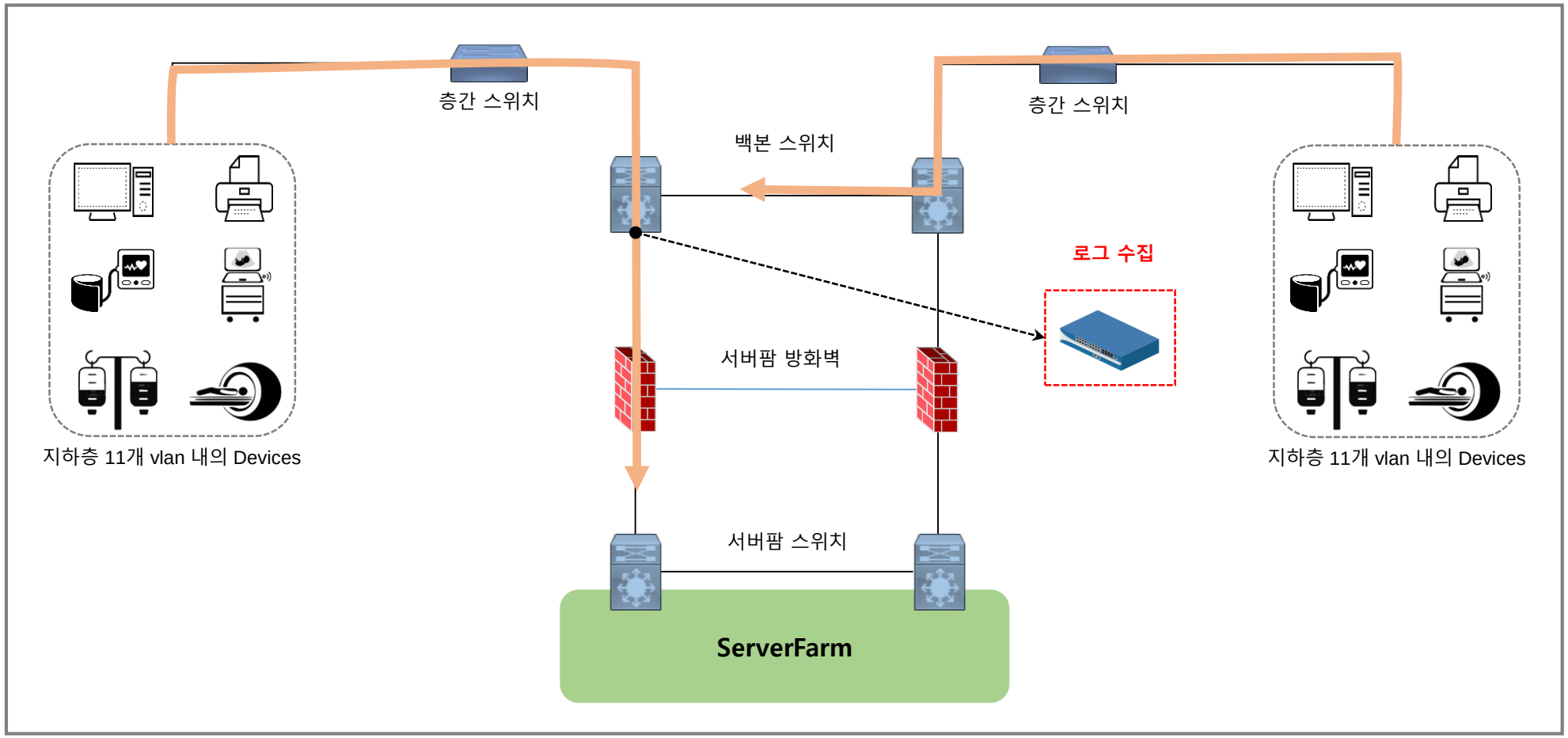
③ 대상 : 지하층 약 11개 대역에 대한 IoT, Non-IoT Device

④ 목적 : 관리되지 않던 IoMT 기기들의 확인(IP관리, 자산관리) 및 해당 기기들의 Alert, 취약점 확인

⑤ 구성 : Device들이 서버팜 아래의 시스템들과의 통신시에 해당 경로상의 트래픽을 미러링 받아 Device 확인

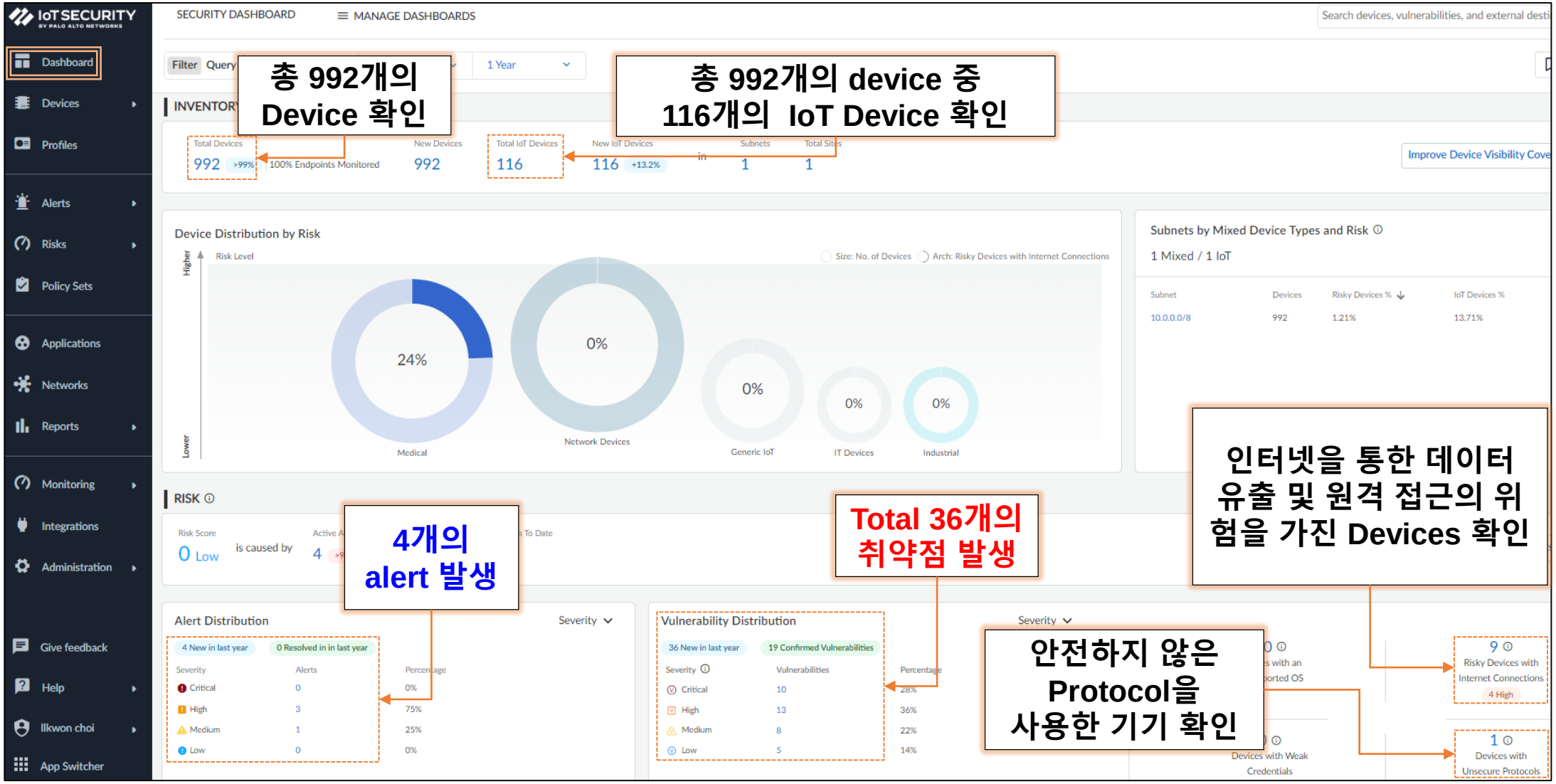
2. 방화벽을 이용한 POC

2-2) POC 구성



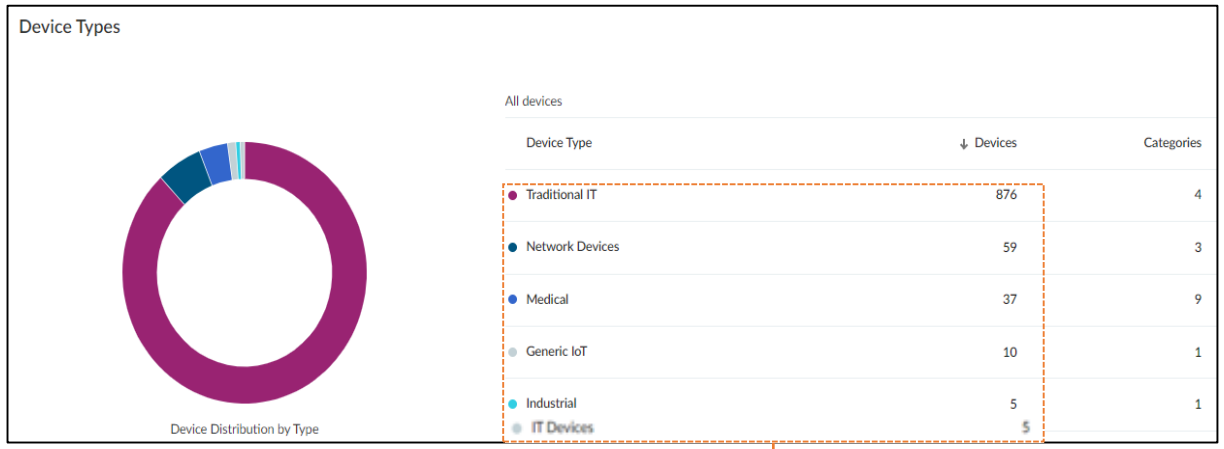
2. 방화벽을 이용한 POC

2-3) Dashboard : 장비목록(Inventory), Alert, 취약점(Vulerability) 확인



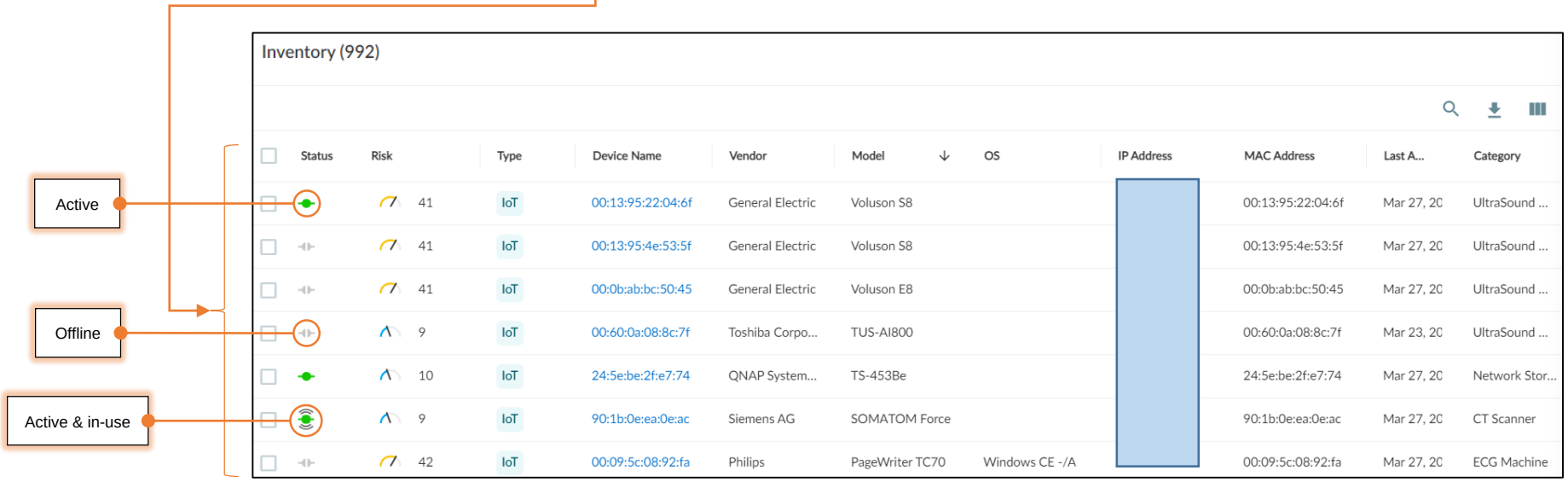
2. 방화벽을 이용한 POC

2-3) Dashboard : Total Devices 확인



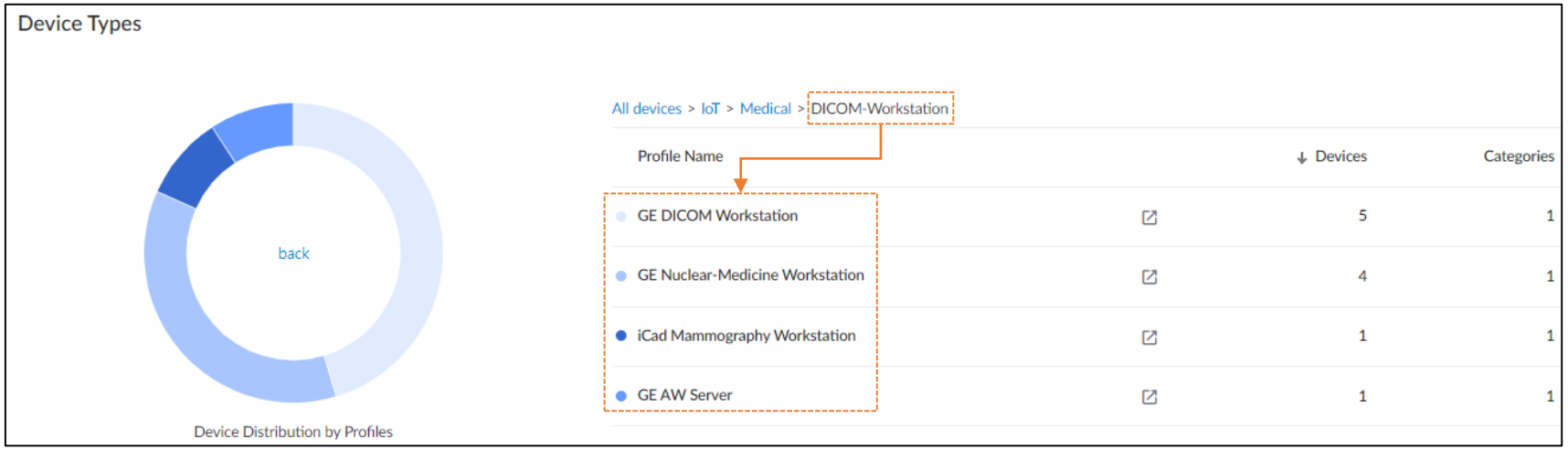
총992개의 기기들이
6개의 Device type으로 분류됨

Device Type	Device
Traditional IT	876
Network Device	59
Medical	37
Generic Iot	10
Industrial	5
IT Device	5



2. 방화벽을 이용한 POC

2-3) Dashboard : Medical 확인 (DICOM-Workstation : 의료영상 디스플레이 기기)



[X-Ray, CT, MRI 같은 의료영상 이미지를 DICOM 형식으로 디스플레이 해 주는 기기]

Device Name	Profile	Vendor	OUI Vendor	OS	IP Address	MAC Address	Last Activity	Applications
98:f2:b3:1d:50:74	GE AW Server	General Electric	Hewlett Packard Enterprise			98:f2:b3:1d:50:74	Mar 29, 2023, 10:00	ssl and 2 more
68:05:ca:e2:8c:64	GE DICOM Workstation	General Electric	Intel Corporation			68:05:ca:e2:8c:64	Mar 29, 2023, 09:58	netbios-ns and 1 more
00:00:f0:94:98:e4	GE DICOM Workstation	General Electric	Samsung Electronics Co.,Ltd	Windows		00:00:f0:94:98:e4	Mar 29, 2023, 10:06	websocket and 43 more
00:12:3f:36:25:d5	GE DICOM Workstation	General Electric	Dell Inc.	Windows		00:12:3f:36:25:d5	Mar 29, 2023, 10:06	websocket and 44 more
00:14:22:49:e4:cb	GE DICOM Workstation	General Electric	Dell Inc.	Windows		00:14:22:49:e4:cb	Mar 29, 2023, 10:06	soap and 20 more
00:01:03:3d:32:c3	GE DICOM Workstation	General Electric	3Com Corporation	Windows		00:01:03:3d:32:c3	Mar 29, 2023, 10:06	facebook-base and 37 more
00:68:eb:cb:1d:5a	GE Nuclear-Medicine Workstation	General Electric	HP Inc.			00:68:eb:cb:1d:5a	Mar 29, 2023, 08:47	dicom and 2 more
00:68:eb:cb:1b:05	GE Nuclear-Medicine Workstation	General Electric	HP Inc.			00:68:eb:cb:1b:05	Mar 29, 2023, 09:49	dicom and 2 more
00:68:eb:c1:8a:cc	GE Nuclear-Medicine Workstation	General Electric	HP Inc.			00:68:eb:c1:8a:cc	Mar 29, 2023, 06:09	dicom and 1 more
00:68:eb:c1:8a:c0	GE Nuclear-Medicine Workstation	General Electric	HP Inc.			00:68:eb:c1:8a:c0	Mar 29, 2023, 09:57	dicom and 5 more
d0:50:99:7e:d8:83	iCad Mammography Workstation	iCAD Inc.	ASRock Incorporation			d0:50:99:7e:d8:83	Mar 29, 2023, 10:00	unknown-udp and 10 more

2. 방화벽을 이용한 POC

2-3) Dashboard : Medical 확인 (DICOM-Workstation : 의료영상 디스플레이 기기)

[Devices] Medical 확인 (UltraSound Machine : 의료 초음파 기기)

[Devices] Medical 확인 (HealthCare : 혈압계)

[Devices] Medical 확인 (ECG Machine : 심전도기)

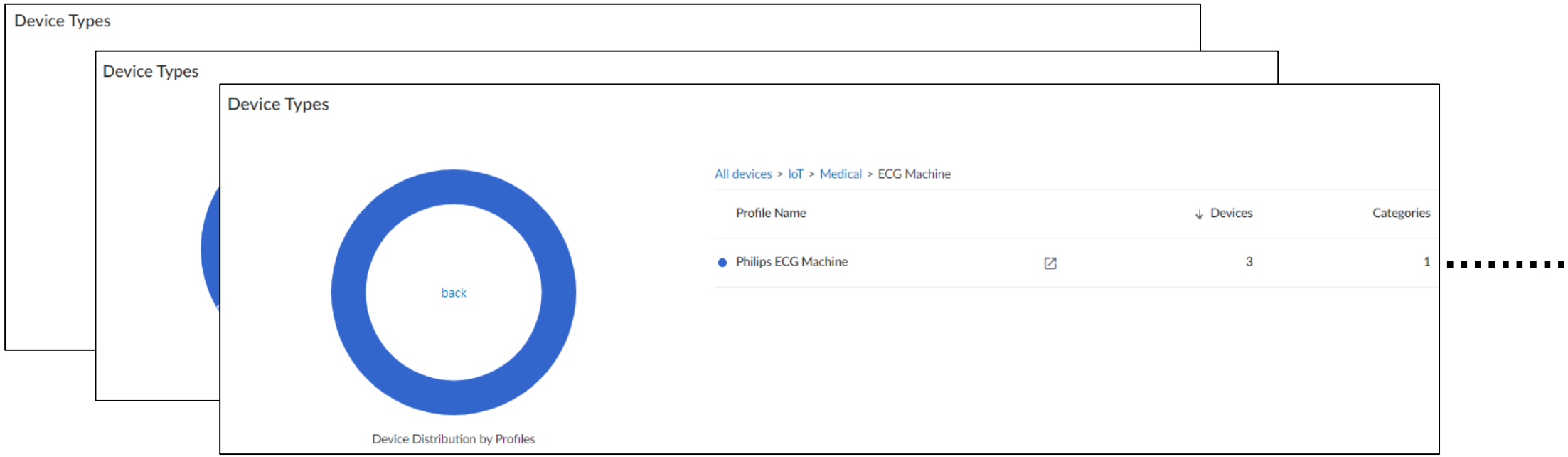
[Devices] Medical 확인 (MRI Machine : MRI 기기)

[Devices] Medical 확인 (Point of Care Analyzer : 혈액분석기)

[Devices] Medical 확인 (Clinical Analyzer) 혈액검사/체외진단 기기

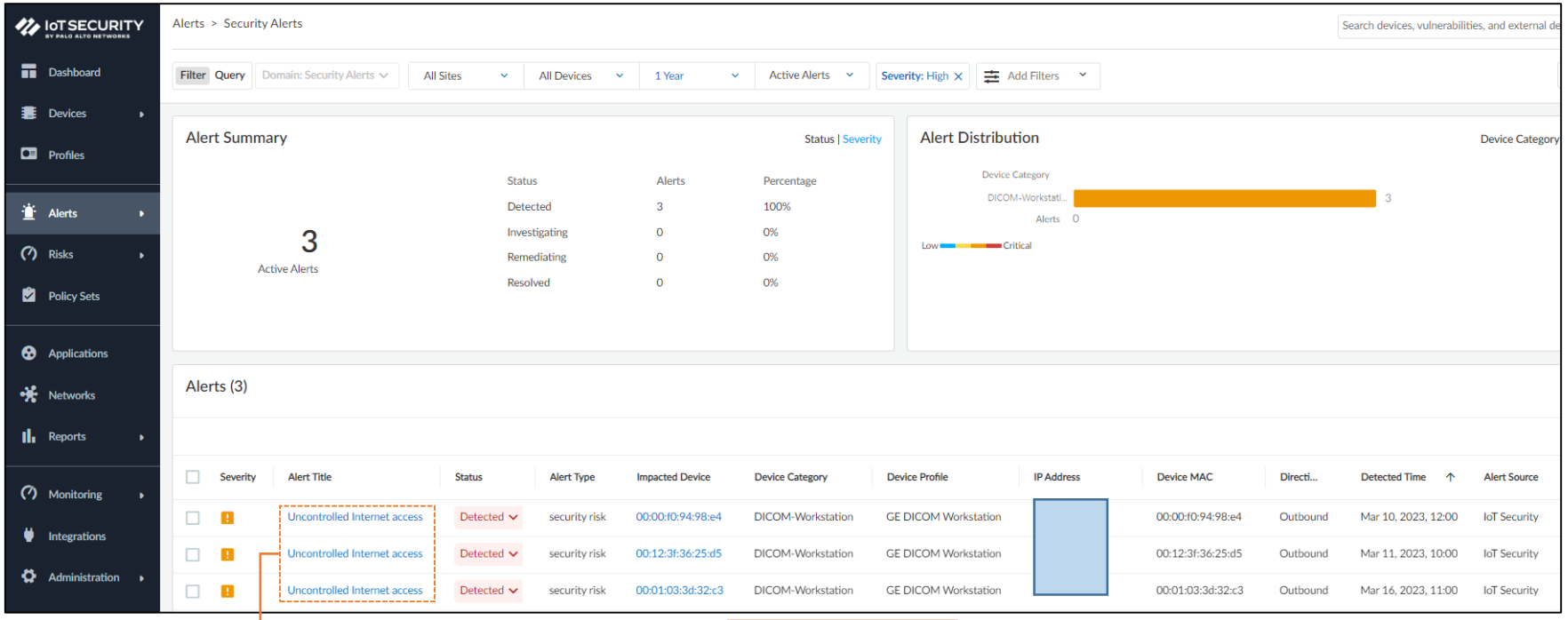
[Devices] Medical 확인 (Radiography System : 방사선 촬영기기)

[Devices] Medical 확인 (CT Scanner : 단층 촬영기기)



2. 방화벽을 이용한 POC

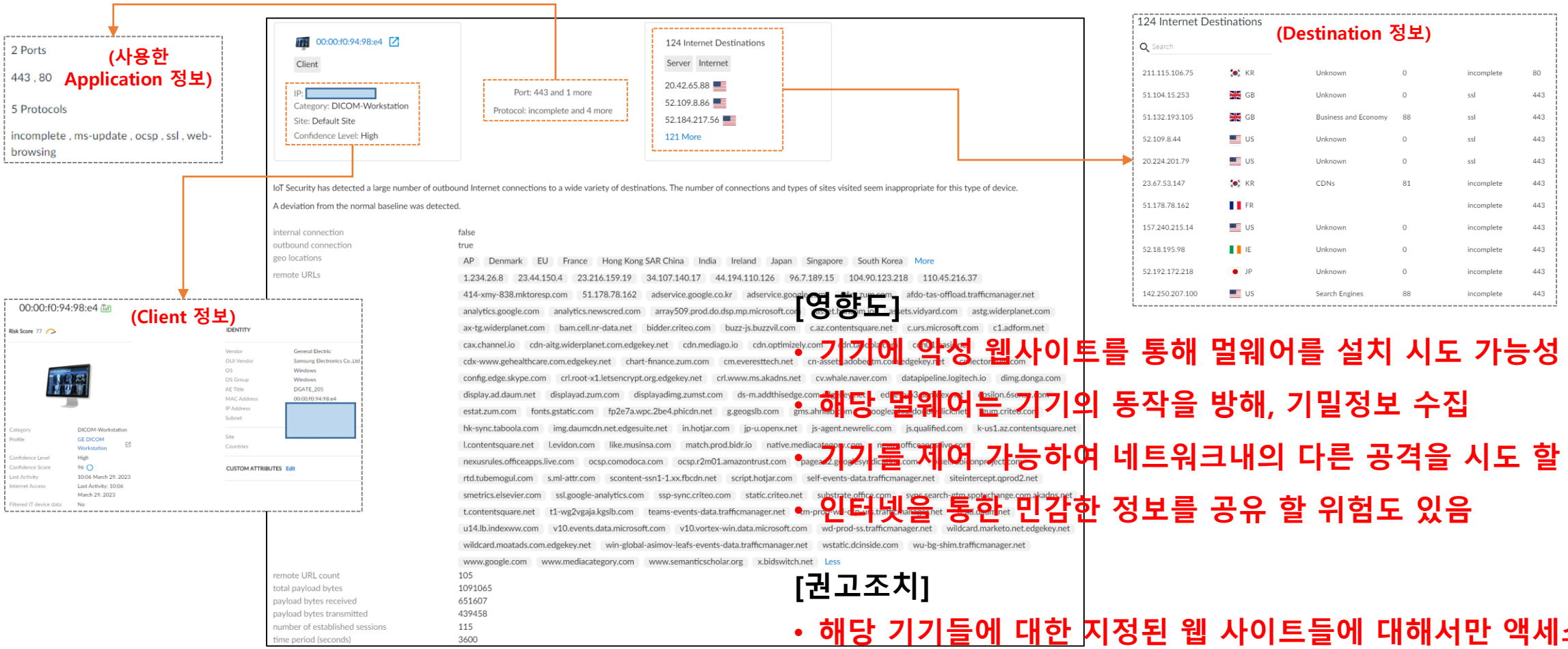
2-3) Dashboard : [Alert] Severity : High 발생



통제되지 않은 인터넷 접속 발생
(다수의 목적지로 인터넷 connection이 발생,
방문했던 사이트의 type과 connection이 부적절한 것으로 탐지됨)

2. 방화벽을 이용한 POC

2-3) Dashboard : [Alert] Severity : High 발생



[영향도]

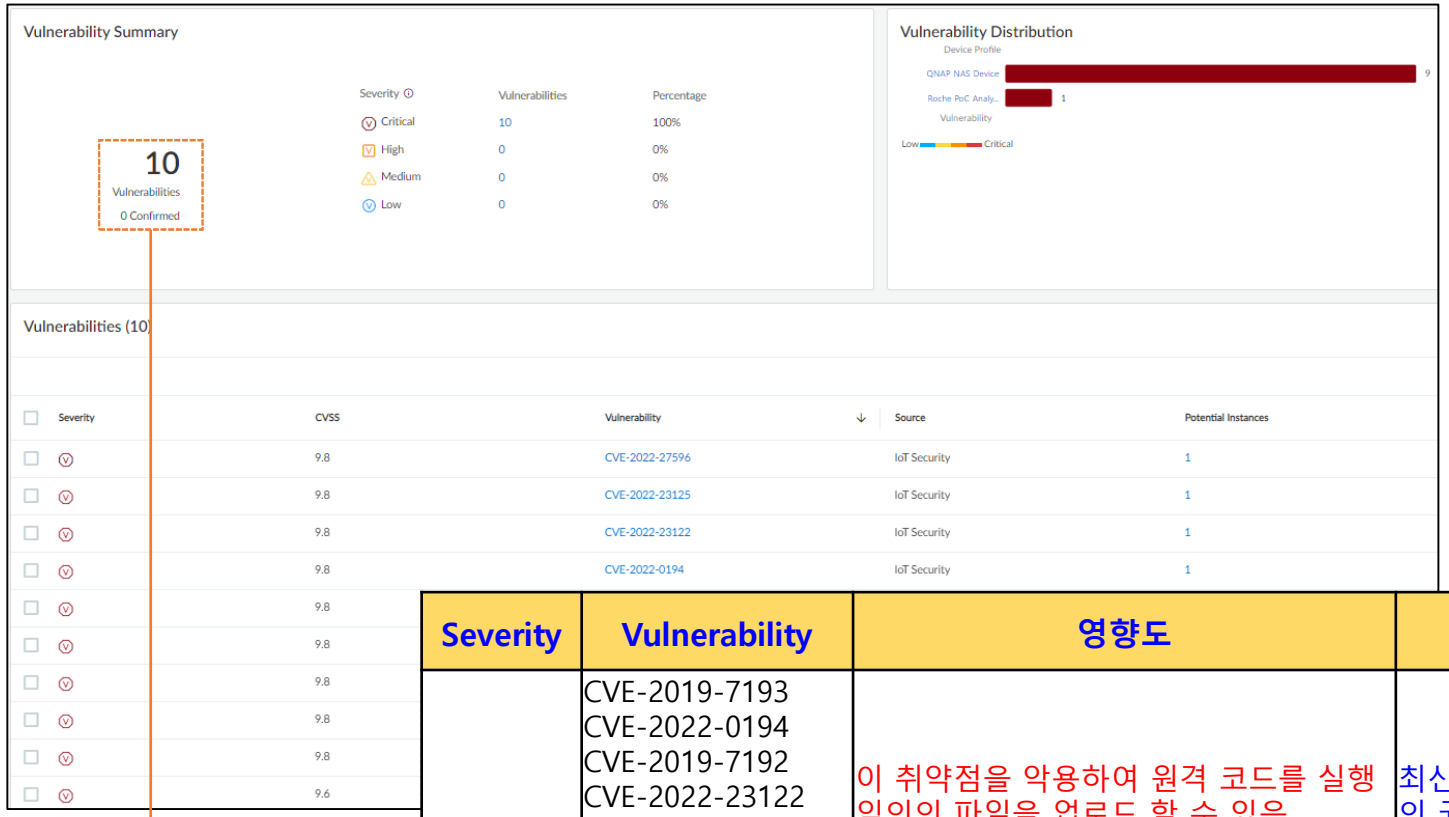
- 기기에 악성 웹사이트를 통해 멀웨어를 설치 시도 가능성
- 해당 멀웨어는 기기외 동작을 방해, 기밀정보 수집
- 기기를 제어 가능하여 네트워크내의 다른 공격을 시도 할 수 있음
- 인터넷을 통한 민감한 정보를 공유 할 위험도 있음

[권고조치]

- 해당 기기들에 대한 지정된 웹 사이트들에 대해서만 액세스 할 수 있도록 방화벽 정책을 업데이트 해야함

2. 방화벽을 이용한 POC

2-3) Dashboard : [Vulnerability(취약점)] Critical 발생 (영향도 및 권고조치)



Severity	Vulnerability	영향도	권고조치	Device	모델
Critical	CVE-2019-7193 CVE-2022-0194 CVE-2019-7192 CVE-2022-23122 CVE-2022-23125 CVE-2022-27596 CVE-2019-7195 CVE-2019-11043 CVE-2019-7194	이 취약점을 악용하여 원격 코드를 실행 임의의 파일을 업로드 할 수 있음 장치에 대한 무단 액세스 권한을 얻고 시스템 파일을 수정	최신 버전으로 업데이트 및 벤더에 문의 권장 (인터넷에 액세스 할 수 없도록 하고 사용하지 않는 포트는 차단)	10.30.X.X	TS-453Be (파일서버)
	CVE-2018-18563	공격자가 시스템 설정을 수정하거나 임의 코드를 실행하기 위한 무단 액세스 권한 획득	사용 가능한 패치와 취약성을 완화하는 지원을 받을 것을 권장	10.10.X.X 10.10.X.X	CoaguCheck Pro II (혈액분석기)

3. 통신현황 분석 솔루션을 이용한 POC

3-1) POC 개요

① POC 제품 : Nozomi Guardian

② 기간 : 2023.01.10 ~ 2023.02.24 (약 45일간)

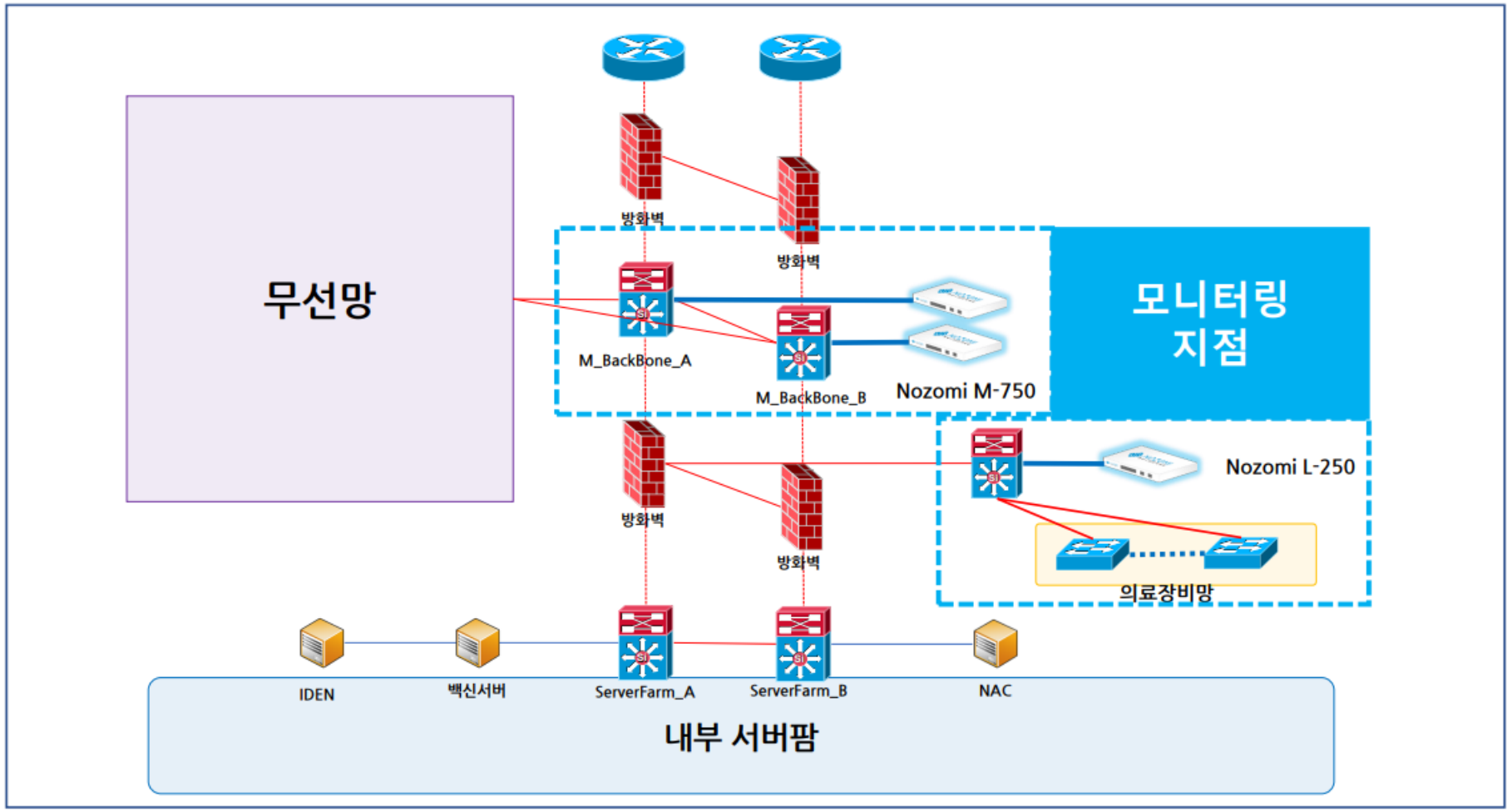
③ 대상 : 지하층 1층, 지상 2층

④ 목적 : 관리되지 않던 IoMT 기기들의 확인(IP관리, 자산관리) 및 해당 기기들의 Alert, 취약점 확인

⑤ 구성 : 지하1층과 지상2층 구역과 의료장비 망 구간의 트래픽 조사

3. 통신현황 분석 솔루션을 이용한 POC

3-2) POC 구성



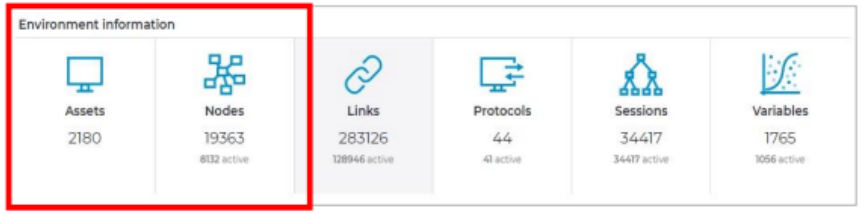
3. 통신현황 분석 솔루션을 이용한 POC

3-3) 장비별 식별 자산

장비별 자산 탐지 내역

- 백본 Active 1

- 백본 Actvie 2



- 의료장비망

이슈 내용

1. 자산 숫자에 대비 높은 비율의 링크/세션
   - 병원 네트워크의 특성으로 인한 통신 구조
2. 백본 네트워크 장비에서 의료장비가 탐지됨
3. 라우팅 등 다양한 네트워크적 요소로 인하여 가시화가 어려운 자산들이 다수 분포하고 있음

탐지 총합

1. 총 3대 장비에서 탐지된 건국대학교 병원 자산 총합
   - 중복 자산 제거 (CMC 기본 기능)

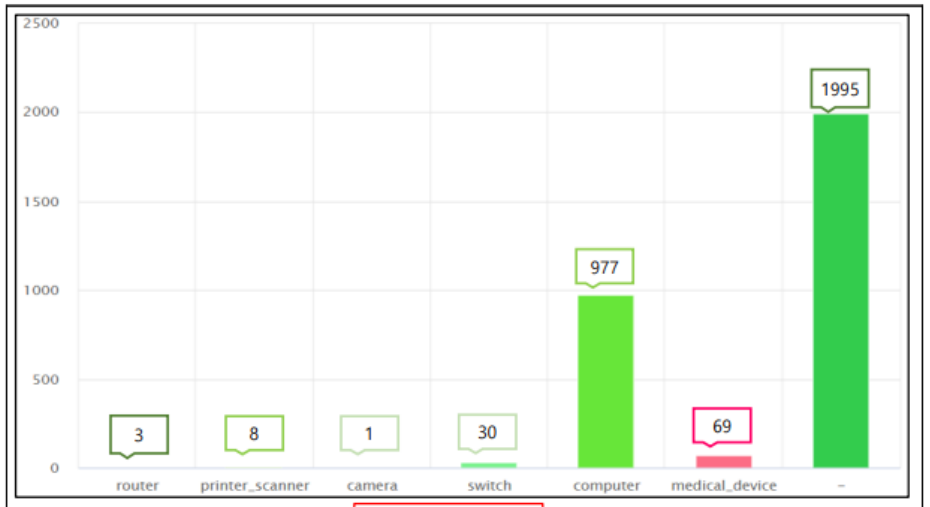
자산	노드
3083	15911

- 병원 네트워크 특성 상 자산 및 통신 내역이 매우 유동적임

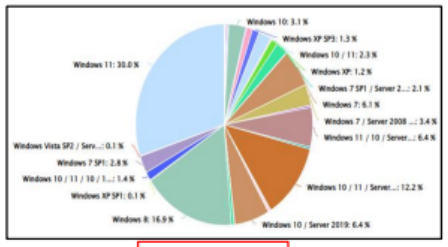
3. 통신현황 분석 솔루션을 이용한 POC

3-4) 자산 현황

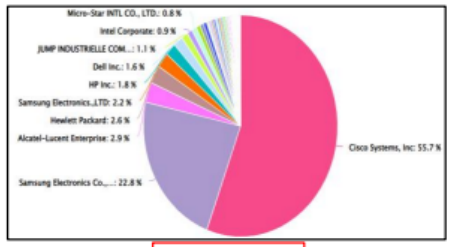
자산 유형별 탐지 내역



자산 유형 분포도



OS 유형 분포



벤더 유형 분포

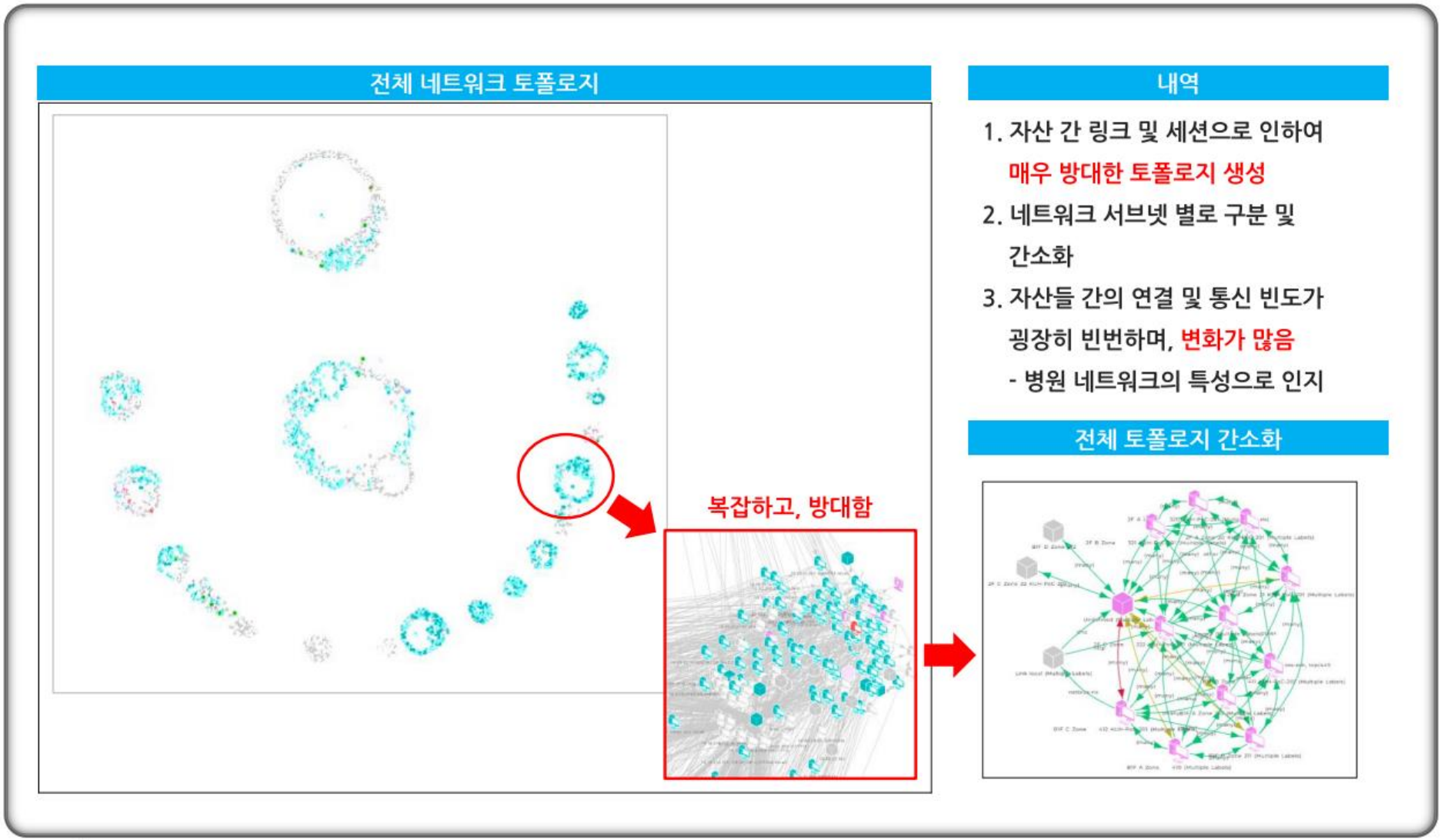
자산 유형별 탐지 내역

위치	VLAN	IP대역	descrption	전체	의료 장비
2층	20	1	2F A-Zone	69	0
	21	1	2F B-Zone	179	7
	22	1	2F C-Zone	6	0
지하1층	210	1(	4 [B1F A-Zone]	133	0
	211	1(	4 [B1F B-Zone]	80	0
	212	1(	4 [B1F D-Zone]	7	0
2층	320	1	[2F_A존 장비용]	17	0
	321	1	[2F_B존 장비용]	46	0
	322	1	[2F_C존 장비용]	127	0
지하1층	410	1(	4 [B1F_A존 장비용]	122	19
	411	1(	4 [B1F_B존 장비용]	21	0
	412	1(	4 [B1F_C존 장비용]	149	14
기타 대역	-		미제공 대역	2127	29
합계				3083	69

※ 자산 목록 별도 제공

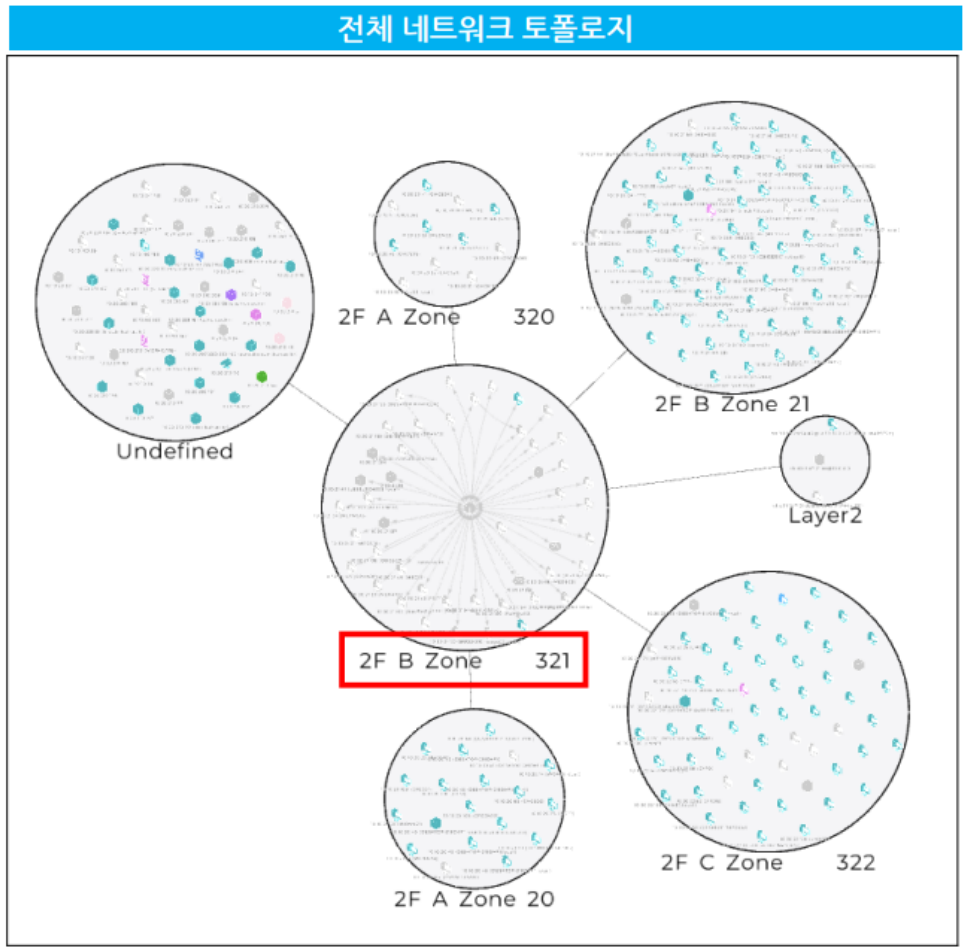
3. 통신현황 분석 솔루션을 이용한 POC

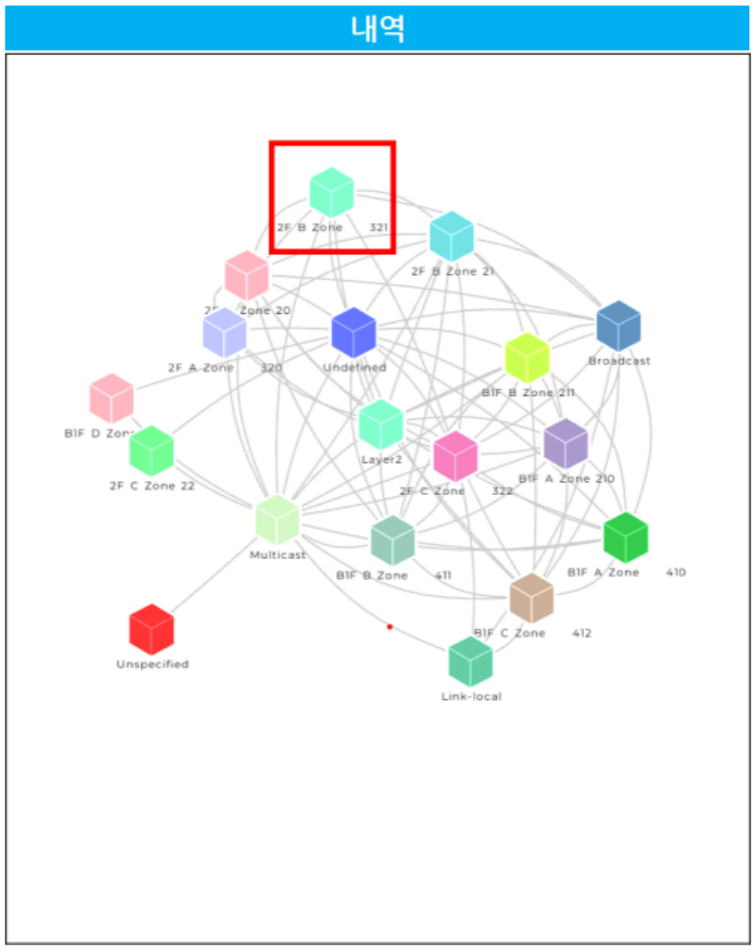
3-4) 전체 네트워크 토폴로지



3. 통신현황 분석 솔루션을 이용한 POC

3-5) VLAN별 가시화





※ 타 VLAN 영역 별도 참조 [별첨 #1]

3. 통신현황 분석 솔루션을 이용한 POC

3-6) 현황 분석 : ① 탐지 내역 요약

시그니쳐 및 임계치 기반 알람이 발생하였으며, 랜섬웨어 및 의료장비 이상징후가 탐지 되었음

탐지된 Alerts (위협/이상징후 탐지 알람) 내역

항목	구분	알람 종류	수량			종류별 (합계)	합계
			백본(A)	백본(S)	의료망		
위협 탐지 (13종)	1	SIGN:CLEARTEXT-PASSWORD		1	1	2	2,678
	2	SIGN:DDOS	775	9		784	
	3	SIGN:MALICIOUS-DOMAIN	11			11	
	4	SIGN:MULTIPLE-ACCESS-DENIED	23	1		24	
	5	SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS	1			1	
	6	SIGN:NETWORK-MALFORMED	5	1		6	
	7	SIGN:NETWORK-SCAN		6		6	
	8	SIGN:OUTBOUND-CONNECTIONS	137	39		176	
	9	SIGN:PACKET-RULE	45			45	
	10	SIGN:PASSWORD:WEAK		90		90	
	11	SIGN:SUSP-TIME		4		4	
	12	SIGN:TCP-SYN-FLOOD	929	170		1,099	
	13	SIGN:WEAK-ENCRYPTION	305	124	1	430	
이상 징후 (12종)	1	VI:NEW-ARP	1	1	2	4	1,509,014
	2	VI:NEW-FUNC-CODE	127	1,835	18	1,980	
	3	VI:NEW-LINK	166,062	524,957	90,059	781,078	
	4	VI:NEW-MAC		3	1	4	
	5	VI:NEW-NODE	2,400	971	108	3,479	
	6	VI:NEW-NODE:MALICIOUS-IP	1			1	
	7	VI:NEW-NODE:TARGET	150,798	486,851	37,306	674,955	
	8	VI:NEW-PROTOCOL	602	4,986	1,899	7,487	
	9	VI:NEW-PROTOCOL:APPLICATION	4,715	23,591	145	28,451	
	10	VI:NEW-PROTOCOL:CONFIRMED	6,557	4,821	50	11,428	
	11	VI:PROC:NEW-VALUE		6	31	37	
	12	VI:PROC:NEW-VAR		108	2	110	
총계							1,511,692

이슈 내역

1. 위협 탐지(13종 탐지)
   - DDoS / 랜섬웨어
   - 암호화되지 않은 비밀번호
   - 네트워크 스캔 등
2. 이상 징후 (12종 탐지)
   - 새로운 자산/통신/프로토콜 등
   - 기존에 사용하지 않았던 명령어
   - 의료장비를 대상으로 하는 이상징후

분석 내역

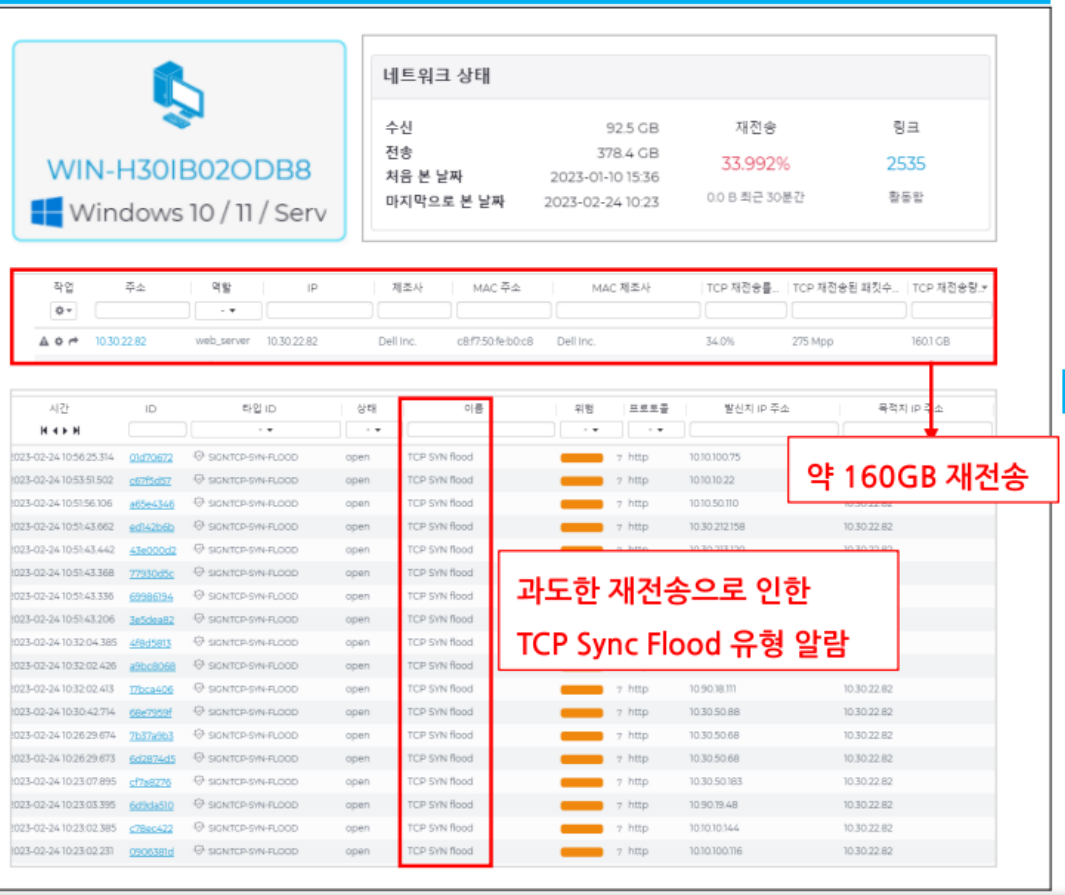
1. 자산들의 통신 변동성이 큰 네트워크 특성 상 두가지 유형의 알람이 굉장히 많이 발생하고 있음
   - NEW-LINK 및 NEW-NODE
2. 불필요한 알람을 제외처리, 유의미한 두가지 유형의 알람을 분석
   - 랜섬웨어 및 의료장비 이상징후

3. 통신현황 분석 솔루션을 이용한 POC

3-6) 현황 분석 : ② 네트워크 품질 (TCP 재전송)

네트워크 내 높은 TCP 재전송률을 보이는 노드들이 포함되어 있으며, 그중 특별히 높은 수치를 보이는 노드의 경우 TCP Sync Flood 공격 유형의 알람을 발생시키고 있음, 이러한 TCP 재전송과 관련된 내역은 네트워크 품질을 저하시키는 요소로 작용할 수 있음

TCP Sync Flood 유형 알람 발생



이슈 내용

1. 특정 노드(IP 10.30.22.82)에서 특히 높은 TCP 재전송률을 보임
   - 재전송률 30% 이상, 재전송량 160GB 이상
2. TCP SYNC Flood 유형의 알람 발생
3. 네트워크 병목 또는 대상 시스템의 부하로 인하여 발생할 수 있음

분석 내역

1. 네트워크 지연으로 인한 서비스 중단
2. 대상 시스템의 리소스 부족의 전조 증상
3. 정보 전송 지연으로 인한 서비스 품질 저하
4. 해당 노드의 시스템 점검 필요

3. 통신현황 분석 솔루션을 이용한 POC

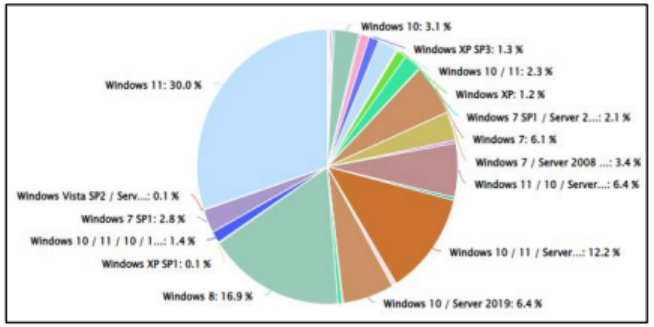
3-6) 현황 분석 : ③ 오래된 OS & 보안취약점 현황

일부 자산들이 Window XP, 7과 같은 오래된 OS를 사용 중에 있는 것으로 확인되었으며, OS 버전의 업그레이드를 권장함. 그렇지 못할 경우 최대한의 보안 패치를 적용하여 병원 네트워크 공격에 악용될 수 있는 보안 취약점을 최소화 시켜야 함

오래된 OS 현황 (Window XP, 7, etc...)

작업	캡처 장치...	주소	역할	IP	운영체제
					XP
	port8	10.10.21.212	other	10.10.21.212	Windows XP SP3
	port1	10.80.30.91	consume	10.80.30.91	Windows XP SP3
	port8	10.30.210.114	consume	10.30.210.114	Windows XP SP3
	port1	10.80.30.36	producer	10.80.30.36	Windows XP SP3
	port8	10.10.210.234	other	10.10.210.234	Windows XP SP3
	port8	10.10.211.214	other	10.10.211.214	Windows XP SP3
	port8	10.30.210.59	other	10.30.210.59	Windows XP SP3
	port8	10.10.20.33	other	10.10.20.33	Windows XP SP3
	port1	10.80.30.67	other	10.80.30.67	Windows XP SP1
	port8	00:1a:a0:aa:a9:e6@10	other	-	Windows XP
	port1	10.80.30.73	other	10.80.30.73	Windows XP
	port8	10.10.20.91	other	10.10.20.91	Windows XP
	port8	10.30.210.64	other	10.30.210.64	Windows XP
	port8	10.30.212.213	other	10.30.212.213	Windows XP

- Window XP
- Window 7
- Window 8 등
- 더이상 보안 업데이트를 지원하지 않는 유형의 OS 다수 식별



- 전체 자산 OS 비율

이슈 내용

1. Window XP, 7 같은 오래된 OS 사용
2. 누락된 보안 패치로 인한 취약점 발생 가능

분석 내역

1. 서비스 지원이 중단된 OS의 경우 더이상의 보안 패치가 어려우며, 이미 많은 취약점을 포함하고 있음

2. 최신 버전의 OS 사용을 권장
   - OS 업그레이드가 어려울 경우 가능한 모든 보안 패치를 적용해야 하며, 해당 자산에 대한 지속적인 모니터링이 필요함

3. 통신현황 분석 솔루션을 이용한 POC

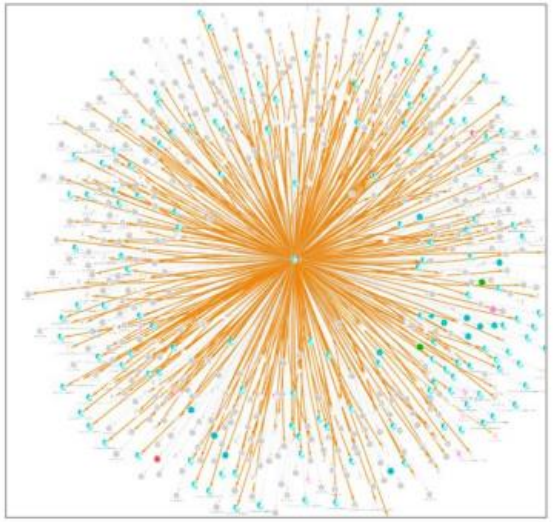
3-6) 현황 분석 : ④ 위협 탐지 -> Wannacry 랜섬웨어

내부 자산(10.30.211.11)의 Wannacry 랜섬웨어가 탐지되었음

내부 자산 악성코드 탐지 (Wannacry 랜섬웨어)

대상 자산의 통신 현황

(SMB를 통한 악성 파일 전송)



주요 Alert

(악성 도메인 접근 & 패킷 룰 탐지)

타입 ID	위험	프로토콜
SIGN:PACKET-RULE	7	smb
SIGN:PACKET-RULE	7	smb
SIGN:PACKET-RULE	7	smb
SIGN:PACKET-RULE	7	smb

타입 ID	위험	프로토콜
SIGN:MALICIOUS-DOMAIN	5	http
SIGN:MALICIOUS-DOMAIN	5	http
SIGN:MALICIOUS-DOMAIN	5	dns
SIGN:MALICIOUS-DOMAIN	5	http

이슈 내용

1. 23-01-11(08:12) 경 내부 자산의 악성 도메인 접근 탐지 (Wannacry 관련 사이트)
2. 23-01-11(08:12) 경 랜섬웨어 감염 의심
3. 23-01-16(16:04) 시점에서 내부 자산을 향하여 SMB 유형의 프로토콜을 사용하여 랜섬웨어 파일 전송 시작
4. 23-01-31(10:51) 마지막 파일 전송 알람 발생

예상되는 위협 또는 피해

1. 랜섬웨어 감염시 PC/시스템 내 파일 암호화 피해 발생으로 병원 진료 및 업무 차질 발생
2. 감염 확대로 인해 피해확산

권고 사항

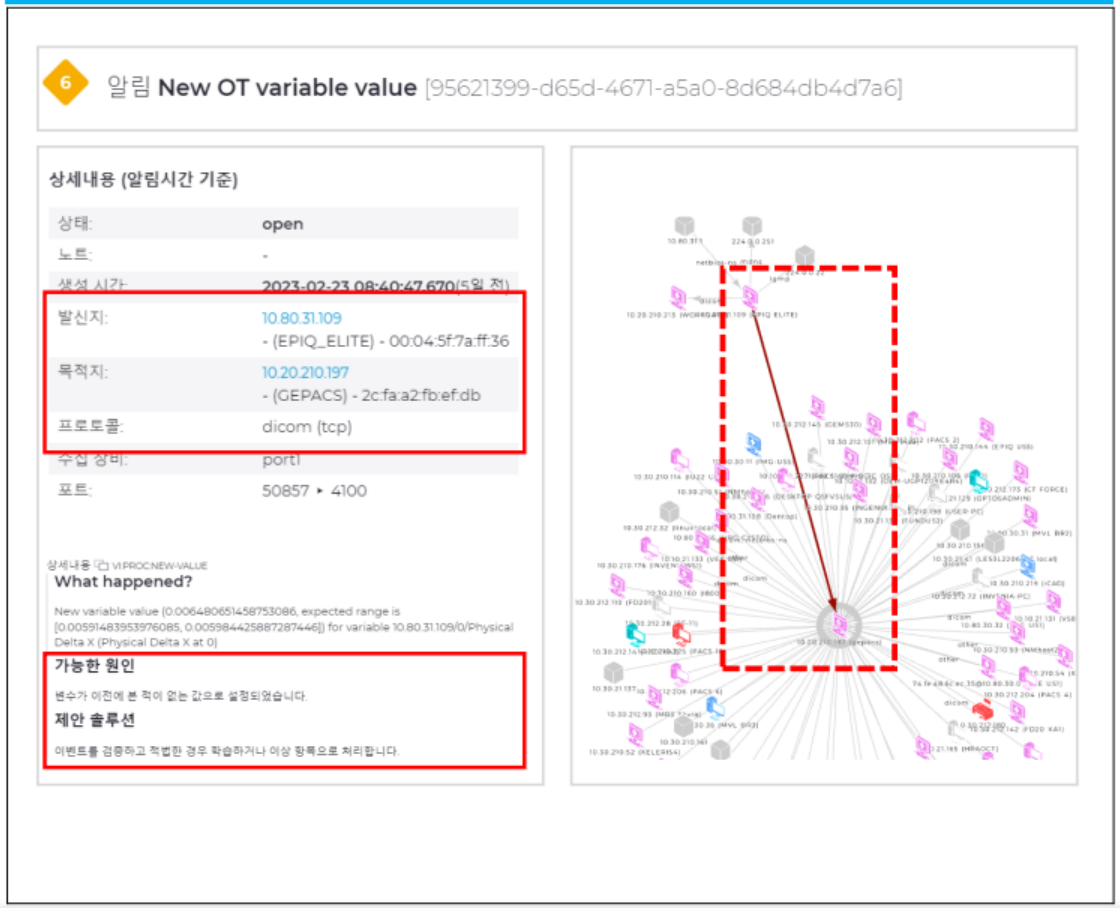
1. 감염PC 격리 및 백신 검사

3. 통신현황 분석 솔루션을 이용한 POC

3-6) 현황 분석 : ⑤ 이상징후 탐지 > 의료장비 이상징후

의료장비 대상 이상징후 탐지, 이러한 유형의 이상징후는 의료장비의 오작동 또는 바이러스 감염 징후일 수 있음

의료기기 이상징후 탐지



이슈 내용

1. 두 노드 EPIQ_ELITE 및 GEPACS 간 DICOM 프로토콜을 이용한 통신 시작
2. 양측 모두 헬스케어 관련 장비
3. 장비 간 기존에 사용하지 않던 변수(설정값)을 통해 통신, 이상징후로 탐지

분석 내역

1. 의료장비를 대상으로 하는 이상징후는 다른 유형의 알람에 비해 치명적일 수 있음
   - 의료기기 오작동
   - 랜섬웨어 등 바이러스 감염으로 인한 중단
2. 지속적인 모니터링 및 양성 여부 판단 필요

3. 통신현황 분석 솔루션을 이용한 POC

3-7) POC 결론

건대병원 전체 네트워크를 대상으로 자산 식별 및 가시화를 진행하였으며
보안 취약점 및 위협/이상징후를 탐지하였습니다.

중점 사항	주요 권고 사항
자산 식별 및 가시화	솔루션 설치 위치 변경
오래된 OS	최신 OS 업그레이드
보안 취약점	최신 보안 패치 적용
위협 및 이상징후	대상 자산 점검

"전체적인 OS 업그레이드 및 위협 대상 자산 점검 필요"

4. 의료장비 보안 취약점 분석을 위한 POC 결론

- ✓ 자산 식별이 필요하다. (수량, OS, 제조사 등)
- ✓ 통신 토폴로지의 주기적 모니터링 필요하다.
- ✓ 솔루션에 식별된 의료장비 자산과 병원정보시스템(HIS)에 등록된 장비코드와의 연계가 필요하다.
- ✓ 솔루션과 보안장비의 연계가 필요 하다.
- ✓ 병원내 정보보안 관제 시스템 및 조직이 필요하다. (비용에 관한 현실적인 문제 있음)

감 사 합 니 다.