TTA Technical Report

기술보고서

TTAR-xx.xxxx 제정일: 2018년 xx월 xx일

모바일 디바이스에서 전자건강기록의 보안 Part V : 위험 평가 및 결과

Securing Electronic Health Records on Mobile Devices Part V: Risk Assessment and Outcomes

TTA 한국정보통신기술협회 Telecommunications Technology Association

표준초안 검토 위원회 바이오인식 프로젝트그룹(PG505)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	이병기	삼성의료원	교수	-	
표준 초안 작성자	황인정	명지병원	책임연구원	-	
	한태화	연세대학교	교수	-	
	김순석	한라대학교	교수	-	
표준 초안 에디터	이병기	삼성의료원	교수	-	
	최민용	BSI Korea	실장	-	
	한근희	건국대학교	교수	-	
표준 초안 검토	김재성	KISA	수석	PG505 의장	
	전동훈	슈프리마	팀장	PG505 부의장	
	전명근	충북대	교수	PG505 부의장	
	한승진	경인여대	교수	PG505 간사	
	김학일	인하대	교수	PG505 특별위원	
	이필중	포항공대	교수	PG505 특별위원	
	정창신	TTA	팀장	PG505 위원	
사무국 담당	김재웅	TTA	단장	-	
	문서연	TTA	전임	-	

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.xx

서 문

1 기술보고서의 목적

본 기술보고서의 목적은 의료현장에서 전자건강기록이 모바일 디바이스에 저장되고 활용될 때 발생할 수 있는 보안에 관한 것으로서 의료서비스 현장에 적용되고 있는 보안기법과 방식을 참조하여 보안에 관한 접근방식, 보안방법, 표준, 위험관리를 포함한 사이버 보안 실무 가이드 제공을 목적으로 하고 있다.
본 기술보고서는 보안 실무가이드의 Part V 이다.

2 주요 내용 요약

본 기술보고서는 “모바일 디바이스에서 전자건강기록의 보안 (NIST SP 1800-1) 의 마지막 장 5권(V)으로 ‘위험 평가 및 결과 - 위험 평가 방법론을 제공한다.
Part V에서는 참조 설계 시스템 위험 평가를 수행하는 데 사용된 방법론, 해당 위험 평가의 결과, 참조 설계 구현의 의도 된 결과 및 참조 설계 기능 테스트의 결과를 다룬다.
Part V은 10개의 장으로 분류된다.

1장 적용범위
2장 인용표준
3장 용어 정의
4장 약어
5장 요약 - 보안 통제 구현의 워크플로우 및 요약
6장 보안 통제 평가 - 참조 설계의 보안 기능성에 대한 시나리오 기반 평가
7장 위험 평가 방법론 (Risk Assessment Methodology) - 시스템을 수행할 때 우리가 취한 두 가지 접근법. 참고 설계의 위험성 평가
8장 위험 평가 결과 - 우리가 실시한 위험 평가의 상세한 결과
9장 보안 통제 시험 및 평가 - 보안 통제 및 구현의 증거
10장 클라우드 기반 전자의무기록(Electronic Health Record, EHR) 제공자를 선택한 의료 기관을 위한 위험도 설문지

3 인용 기술보고서와의 비교

3.1 인용 기술보고서와의 관련성

이 기술보고서는 미국 국가표준기술연구소(NIST)의 사이버보안센터(National Cybersecurity Center of Excellence, NCCoE)에서 발행한 NIST 특별판 1800-1e Securing Electronic Health Records on Mobile Devices - Risk Assessment and Outcomes 문서를 준용하여 보안 평가와 결과가 어떤 방식으로 이루어지는 보안의 일반적인 시나리오와 방법을 제공한다.

3.2 인용 표준과 본 기술보고서의 비교표

국가표준기술연구소(NIST) 특별판(SP) 1800 시리즈	본 기술보고서	비고
NIST 특별판 1800-1e Securing Electronic Health Records on Mobile Devices Part V: Risk Assessment and Outcomes	Part V	- 기술보고서 형식에 의한 편집

Preface

1 Purpose

The purpose of this technical report is to prevent the potential threat of situation when electronic health records are being stored and utilized in the medical field; accordingly, security requirement in this technical report is specified by referencing security techniques and methods in the medical service.
Part V of the report addresses the methodology used to conduct the reference design system risk assessment, the results of that risk assessment, the intended outcomes of implementing the reference design, and the results of the reference design functional test.

2 Summary

As Part V of “Security of Electronic Health Records on Mobile Devices”, this technical report provides the relevant standards as well as general scenario and test. Part V is divided into six chapters.
Chapter 1 – Coverage
Chapter 2 – Citing Standard
Chapter 3 – Term Definition
Chapter 4 – Abbreviation
Chapter 5 – The workflow and summary of the security control implementation
Chapter 6 – Security Controls Assessment – scenario based evaluation of the security functionality of the reference design
Chapter 7 – Risk Assessment Methodology – the two approaches we took in conducting a system risk assessment of the reference design
Chapter 8 – Risk Assessment Results – detailed results of the risk assessments we conducted

Chapter 9 – Security Controls Test and Evaluation – security controls and the evidence of their implementation
Chapter 10 – Risk Questionnaire for health care organizations selecting a cloud-based EHR provider

3 Relationship to Reference Standards

This technical report applies the “NIST Cybersecurity Practice Guide SP 1800-1 Security Electronic Health Records on Mobile Devices – Risk Assessment and Outcomes” published by National Cybersecurity Center of Excellence (NCCoE) of National Institute of Standards and Technology (NIST) and provides the security standards, the relevant standards as well as general scenario and test under the consideration of current status on mobile device distribution in national hospitals or clinics.

목 차

모바일 디바이스에서 전자건강기록의 보안
Part V 위험 평가 및 결과
Securing Electronic Health Records on Mobile Devices
Part V. Risk Assessment and Outcomes

1 적용 범위

이 기술보고서는 의료서비스 제공기관에서 모바일 디바이스를 이용하여 의료데이터를 저장하고 처리하는 시나리오를 기반으로 의료 데이터 보안에 대해 기술하였다. 이 NIST 사이버 보안 실무 가이드는 표준 기반 참조 디자인에 대해 설명하고 모바일 디바이스 간에 전송되는 전자 건강 기록을 보호하기 위해 이 접근법을 복제하는 데 필요한 정보를 사용자에게 제공한다. Part V 는 참조 설계 시스템 위험 평가를 수행하는 데 사용 된 방법론, 해당 위험 평가의 결과, 참조 설계 구현의 의도 된 결과 및 참조 설계 기능 테스트의 결과를 기술하였다.

2 인용 표준

- NIST SP 1800-1e Securing Electronic Health Records on Mobile Devices – Risk Assessment and Outcomes

3 용어 정의

3.1 전자 건강 기록 (Electronic Health Records, EHR)

모든 의료기관의 전자의무기록(Electronic Medical Records, EMR)을 망으로 통합하여 공유하고 활용할 수 있는 의료정보 시스템. 각 의료기관별로 개별 관리되고 있는 환자의 진료 관련 자료들을 통일 또는 호환성을 향상하고 시스템 및 서비스 표준화를 통해 중복 투자와 낭비를 줄이며 임상 진료의 효과를 향상하는 것이 주목적임

3.2 환자 건강 정보 (Patient Health Information)

환자 건강 정보"란 환자의 임상 진료와 관련된 모든 정보를 의미함. "보호받는 의료 정보"는 HIPAA(Health Insurance Portability and Accountability Act)에 따라 우리의 범위보다 광범위한 특정 정의가 있음. 우리는 "환자 건강 정보"를 사용하고 있고 보호받는 의료 정보를 추가로 정의하거나 처리 방법에 대한 추가 규칙을 설정한다는 의미는 아님.

3.3 논리 연결제어 (Logical Link Control)

OSI 모델의 데이터 링크층의 두 개의 부속 계층의 하나로서 IEEE 802 표준에 의해 정의됨. 이 부속 계층은 네트워크의 매개체를 통해 데이터를 전송한 경우에 두 컴퓨터 사이의 연결을 유지하는 기능을 수행함.

3.4 램파트 논리 연결제어 (Ramparts Logical Link Control)

램파트는 유즈케이스에 대해 방법론 (Ramparts Risk Assessment Methodology)을 만들고 사용함. 이 방법론은 유즈케이스의 보안 기능을 사용하고 NIST 사이버 보안 프레임워크에 매핑함. 또한 NIST SP 800-30, SP 800-53 revision 4, 중요 정보 시스템의 MORDA (Mission Oriented Risk and Design Analysis), 위험 분석 모델 (RAM) 등 지능형 컴퓨터 네트워크 방어를 결합한 것

3.5 모바일 디바이스 보안 관리 (Mobile Device Management)

개인 사용자 단말기에 대해 부분적인 Admin 권한을 가지고 있으면서 사용자 단말기의 분실 등으로 인한 무제가 발생되었을 경우, 이를 원격으로 휴대폰 데이터의 삭제 혹은 잠근설정등의 처리를 도와주기 위해서 OS 단에서 제공해주는 (Google, Apple 등의 OS 제조사) API를 이용한 앱으로 시작한 것이며 최근 들어 모바일 오피스가 활성화 되면서 보안이슈가 대두되었고, 모바일 디바이스 보안은 각 회사의 모바일 보안과 관련하여 중요한 기능으로 자리잡음

3.6 국가사이버보안센터 (NCCoE, National Cybersecurity Center of Excellence)

미국 국가표준기술연구소(NIST, National Institute of Standards and Technology)의 국가 사이버보안센터

3.7 피싱 (Phishing)

블특정 다수의 이메일 사용자에게 신용카드나 은행 계좌정보에 문제가 발생해 수정이 필요하다고 거짓 이메일을 발송해 가짜 웹 사이트로 유인하여 관련 금융 기관의 신용 카드 정보나 계좌정보 등을 빼내는 신종해킹기법. 개인정보(Private Data)와 낚시(Fishing)의 합성어로 낚시하듯이 개인정보를 몰래 빼내는 것을 말함

3.8 트랜잭션 (Transaction)

디지털 교환처리는 다수의 호에 대한 처리를 동시에 병행하는 다중처리 방식이 취해지고 있음. 트랜잭션은 각각의 호에 관한 처리가 간섭하는 경우가 없는 호(呼)에 관한 제어

정보를 저장하기 위하여 호에 대응하여 설계된 메모리 에어리어에서 각 처리간의 제어 정보 접수를 관리함.

3.9 WPA2 (Wi-Fi Protected Access® 2)

WPA2는 와이파이 얼라이언스에서 수행하는 보안프로그램으로, 처음 사용하던 보안 프로토콜인 유선 동등 프라이버시(WEP)의 보안 취약점 때문에 그 대안으로 나온 것임.

3.10 확장 가능 인증 프로토콜 (Extensible Authentication Protocol, EAP)

확장 가능 인증 프로토콜은 무선 네트워크와 점대점 연결에 자주 사용되는 인증 프레임워크임. RFC 2284가 쓸모없게 되어 이를 대신하여 RFC 3748에 정의되어 있으며, RFC 5247을 통해 업데이트되었음. EAP는 EAP 방식들이 만들어내는 키 요소와 매개변수의 전송 및 이용을 제공하기 위한 인증 프레임워크임.
RFC가 정의하는 방식들의 수는 많으며 수많은 업체에 특화된 방식들과 새로운 제안들이 존재함. EAP는 유선 프로토콜이 아니며 단지 메시지 포맷을 정의함. EAP를 사용하는 개별 프로토콜은 프로토콜의 메시지 내의 EAP 메시지들을 캡슐화하는 방법을 정의함.

3.11 침입 탐지 시스템(Intrusion Detection System, IDS)

컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템. 침입 차단 시스템만으로 내부 사용자의 불법적인 행동(기밀 유출 등)과 외부 해킹에 대처할 수 없으므로 모든 내, 외부 정보의 흐름을 실시간으로 차단하기 위해 해커 침입 패턴에 대한 추적과 유해 정보감시가 필요함.

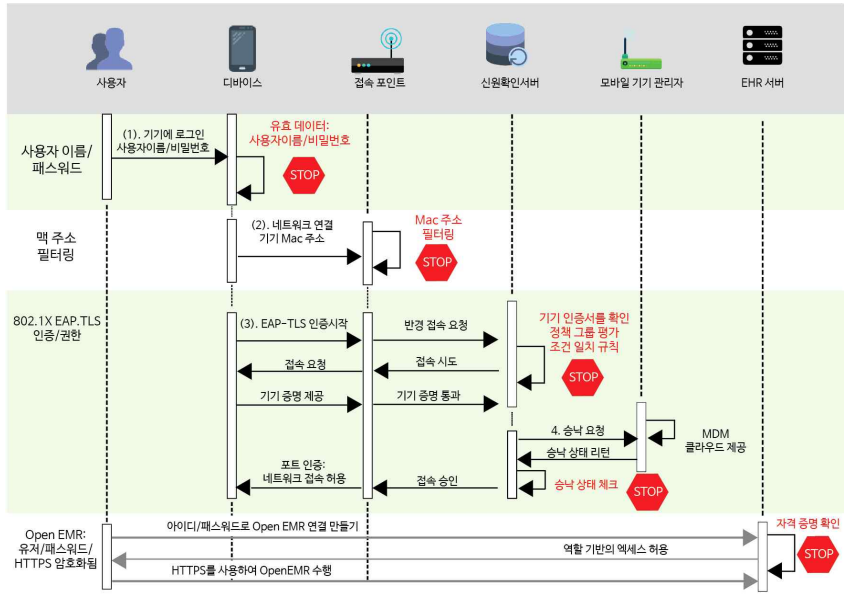
4 약어

- HIPAA : Health Insurance Portability and Accountability Act
- MORDA : Mission Oriented Risk and Design Analysis
- RAM: Risk Analysis Model
- LLC: Logical Link Control
- MDM : Mobile Device Management
- CSF : Cyber Security Framework

5 요약

5.1 보안 통제 구현의 워크플로우 및 요약

본 참조 디자인의 기능은 적(adversary)이 무단접속을 통해 환자 건강 정보 획득을 어렵게 한다. 동시에 인증된 사용자는 쉽게 접근 권한을 제공받는다. 참조 디자인은 환자 정보 보호를 강화하고 시스템 사용 변경을 최소화하도록 설계되었다. 참조 디자인의 모든 구성 요소와 마찬가지로, 모든 조직은 환자정보 보호와 시스템 변경을 최소화하는 기능과 방법에 대해 자체 위험 기반 결정을 해야 한다. 참조 디자인의 보안 기능은 전자건강기록(Electronic Health Records, EHR)에 접근하는 일반 사용자의 비즈니스 워크플로우를 이용한다. 이 워크플로우와 관련 보안 검사는 그림 5-1에서 보여준다.



(그림 5-1) 사용자 및 디바이스 전자 건강 기록 서버 통신 단계

EHR에 대한 접근 권한을 부여 받기 전에 사용자는 다음 5단계를 수행해야 한다. 그러나 실제 환경에서는 사용의 용이성이 가장 중요하기 때문에 1단계(디바이스에 로그인)와 5단계 (EHR에 로그인)를 제외한 모든 단계는 사용자에게 제공된다. 즉, 투명성이 보장된다.

1단계. 사용자가 본인의 이름과 암호를 디바이스에 입력한다.

2단계. 각 조직에 있는 모바일 디바이스에서 통신이 시작된다. 각 조직은 데이터 센터에

있는 전자 건강 기록 서버와의 통신을 용이하게 하는 AP들을 최소한으로 제공한다. AP에 대한 각각의 연결은 우선 적절한 MAC (media access control) 주소로 디바이스에 의해 접근되고 응답되어야 한다.
MAC 주소는 물리적 디바이스에서 변경할 수 없지만 운영 체제에서는 변경할 수 있다. 따라서 낮은 수준의 공격자도 보안 우회를 간단하게 수행할 수 있다. MAC 필터링은 ID 및 접근 제어를 위한 첫 번째 방어 계층이다.

3단계. 디바이스는 올바르게 서명되고 신뢰할 수 있는 인증서를 AP(Access Point)에 요청한다. 사용자가 디바이스에 이 인증서를 갖고 있지 않으면 웹 기반 OpenEMR에 대한 접속 시도를 로컬 네트워크로 접근할 수 없다. 이 시뮬레이션에서 AP와 OpenEMR 에 동일한 인증기관이 사용되었다.
하드웨어 인증은 IT 부서에서 제공하는 스마트카드 또는 다른 토큰이 될 수 있다. 두 가지 모두에 대해 별도로 신뢰할 수 있는 CA(certificate authority;인증기관)를 설정하고 두 서비스에 대한 접근을 위한 하드웨어 인증을 요구함으로써 이 트랜잭션에 보안을 추가할 수 있다. 이 방법은 분실하거나 도난당한 디바이스에 대한 접근 권한을 얻은 내부자 또는 공격자를 약화시킨다. AP에 접근할 수는 있지만 OpenEMR에는 접근할 수 없다.

4단계. 모바일 디바이스 보안 관리(Mobile Device Managemt)는 할당된 정책에 따라 디바이스에 대한 적합성 검사를 수행한다.

5단계. 사용자가 적절한 MAC 및 인증서 자격 증명을 사용하여 디바이스에 대한 접근을 우회하거나 얻은 경우 디바이스에 문제가 발생한다. OpenEMR은 암호화 및 PKI 기반 인증서를 사용하여 추가 클라이언트 인증을 수행한다.
트랜잭션은 웹 응용 프로그램에 기록되며, 이 빌드에 사용된 모바일 보안 디바이스 보안관리(MDM)는 로그가 열려있는 동안 디바이스의 특정 위치를 추적할 수 있다.
그 후 사용자는 적절한 사용자 이름 및 암호 자격 증명을 얻기 위해 OpenEMR에 의해 요청된다. 공격자가 OpenEMR 도구에 접근하기 위해 무차별 대입 공격을 시도하면 웹 서버 응용 프로그램이 모든 시도를 기록하기 때문에 관리자가 추적할 수 있는 가능성이 더 높다. OpenEMR은 몇 번의 로그인 공격 시도 후에는 사용자를 잠궈 접근을 하지 못하도록 한다.

마지막 단계에서 올바른 로그인 자격 증명을 가진 사용자는 OpenEMR 시스템에 로그인한다.

6 보안 기능 평가

보안 기능구현이 비즈니스과제를 충족한다는 사실을 입증하기 위해서 랩바트(Ramparts)는 참조 디자인에 대한 객관적인 평가를 실시했다.

평가 결과에 따르면 아키텍처 및 구현은 전자건강기록 및 환자 건강 정보에 대한 읽기 및 쓰기 접근권한이 부여 된 사용자에게만 국한되므로 보안이 강화되었다.

이 평가는 아키텍처 또는 구현 기능 및 보안에 대해 모든 측면을 완벽하게 테스트하기 위한 것이 아니다. 모든 측면의 테스트는 비실용적이며 어려울 것이다.
참조 디자인의 원칙 및 구현 세부 사항을 조직의 기업 인프라에 적용하려면 예상 할 수 없는 위협 사용자 지정이 필요하다.
이런 형태로 테스트를 시행하면 유사한 조직의 테스트 결과와 다를 수 있다.
이 참조 디자인을 채택한 조직은 여기에 제시된 내용을 토대로 자체 시스템 보안 계획을 업데이트하고 자체 구현의 보안을 검증하는 데 이용해야 할 것이다.

평가는 세 부분으로 구성된다 :
1. 보안 시나리오 평가 - 참조 디자인이 여러 가지 공격 시나리오의 맥락에서 환자 건강 정보를 보호한다는 증거를 제공한다.

2. 기능성 평가 - NCCoE 사용 사례 문서에 설명 된 주요 기능, 원래 이 과제를 설명한 "전자 건강 정보의 안전한 교환"이 빌드에서 올바르게 구현되었다는 증거를 제공한다

3. 보안성 평가 - 유즈케이스에 명시된 보안 기능이 빌드에서 올바르게 구현되었다는 증거를 제공한다.

6.1 보안 시나리오 평가

평가자는 시나리오에 따라 예상되는 공격에도 건강 정보의 보안을 유지할 수 있다는 증거를 제공하기 위해서 참조 디자인에 대한 시나리오 기반 보안 테스트를 수행했다.
공격 기반 시나리오 테스트에서 NCCoE 건강 IT 설계자와 엔지니어는 시스템 관리자의 역할을 수행했다.
다양한 공격 시나리오에서 수비수는 네트워크를 가동하여 탐지 된 모든 위협을 모니터링하고 대응할 수 있는 리소스로 대규모 의료기관의 운영을 모방했다.

테스트가 새로운 공격자 시나리오로 전환되면 시스템 관리자는 적절한 완화 조치를 재설정한다. 암호 재설정과 같은 완화 조치가 포함되었지만 VPN 접근 차단이나 공격자의 초기 발판은 포함되지 않았다. 테스트 절차에서는 침입자가 내부 Windows 데스크톱 컴퓨터를 손상시킬 수 있다고 추정했다.

평가자는 유즈케이스 아키텍처 및 구현은 인가된 사용자만 전자 건강 기록 시스템 및 환자 건강 정보에 대한 읽기 및 쓰기 접근 권한을 얻을 수 있음을 보장한다는 목표와 관련하여 향상된 보안을 제공함을 입증했다.

6.1.1 분실된 모바일 디바이스 시나리오

이 시나리오에서 공격자는 탈취 또는 분실된 모바일 디바이스를 획득하였다. 디바이스는 어떤 시점에 전자 건강 기록 시스템에 접근할 수 있었다.
디바이스에 저장된 환자 건강 정보가 없다. 디바이스가 망가지지 않는 조건 하에 환자 건강 정보에 접근 이력을 디바이스를 통해 검사했다. 다시 말해, 디바이스의 디스크 및 메모리에 대한 포렌식 이미지를 얻기 위한 것이다.
유실된 디바이스를 발견하면 디바이스가 Health ISP 네트워크의 모든 리소스에 접근 할 수 없도록 차단되어야 한다. 유실된 디바이스임이 파악되는 즉시 방어자(관리자)는 침입에 대한 블록을 구현했다. 민감한 정보가 들어있는 파일이나 이력은 디바이스에 저장되어 있을 수 있으므로 방어자(관리자)는 원격으로 파일 지우기를 시작했다. 민감한 정보가 삭제되고 분실된 디바이스가 침입할 수 없도록 로그인 정보가 삭제되었음을 확인했다.

6.1.2 내부 네트워크 접근 시나리오

이 시나리오에서 공격자는 내부 Health ISP 네트워크에 접근했다.
공격자는 피싱(Phishing)을 통해 네트워크에 접근하고 윈도우(Windows) 화면을 지속적으로 유지했다. 이 지속적인 존재는 낮은 레벨의 캡처된 윈도우(Windows) 도메인 자격 증명을 사용하여 데스크톱에 원격 접근 할 수 있는 능력으로 나타난다. 실제 시나리오에서는 일반적으로 네트워크 트래픽 재설정이 있는 백도어의 형태를 취한다. 이 발판을 통해 공격자는 Health ISP의 네트워크 다이어그램을 얻었다. 공격자가 접근 권한을 얻는 동안 시스템 관리자 자격 증명은 얻지 못했다.
테스트를 통해 심층 방어 전략을 확인하고 접근 통제와 같은 아키텍처의 보안 기능으로 인해 발견 된 많은 약점이 피해를 제한하는 데 도움이 되었음을 입증했다.

6.1.3 OpenEMR 접근 시나리오

이 시나리오에서 공격자는 일반적인 사용자 자격증명(예:안내원,회계사)이 있는 OpenEMR 웹 응용 프로그램에 접근했다. 공격자는 시스템에 일상적으로 접근 할 수 있는 악의적인 내부자이거나 사용자 자격 증명을 캡처한 외부인이었다. 공격자는 네트워크 내 접근할 수 있는 권한을 확보하고 환자 건강 정보의 보안규정을 위반하며 접근을 시도했다. 내부 네트워크 접근 시나리오에서와 마찬가지로 테스트를 통한 접근 시 환자 건강정보의 양을 줄인다면 좀 더 안전한 관리가 유지된다.

6.1.4 물리적 접근 시나리오

이 시나리오에서 공격자는 데이터 센터에 직접 접근 할 수 있다. 우리는 공격자가 장기간 감시되지 않는 데이터 센터에 접근을 할 수 있다고 가정했다. 공격자는 전자 디바이스와 다른 디바이스를 가져올 수 있었다. 이런 경우 우리는 공격자가 접근 포인트에 연결하고

기록 및 모니터링 된 네트워크 트래픽 및 테스트 결과 등을 사용할 수 없도록 모든 트래픽을 암호화한다. 그 결과로 공격자가 모든 트래픽을 사용할 수 없게 만든다.

6.2 기능성 평가

개별 기능 테스트를 통해 빌드가 유즈케이스에 설명 된 주요 기능을 제공함을 보증한다. 모바일 디바이스를 사용하는 1차 진료 의사가 안전하게 보낼 수 있다.

• 처음 한 명의 의사가 두 번째 의사에게 진료의뢰하기 위해 전자건강기록 저장소에서 검색하여 정보를 전달하고 의뢰함
• 처방전 정보를 약국으로 전달함. 아래의 하위 섹션에서는 각 기능의 의도를 간략하게 설명하고 유효성 검사 및 결과를 설명한다.

6.2.1 진료의뢰 보내기

이 테스트는 전자 건강 기록을 전자문서로 작성하여 다른 의사에게 진료의뢰서를 전달하는 기능을 평가한다. 이 시나리오에서 진료의뢰서를 작성하여 전달하는 의사와 수신 의사는 동일한 전자 건강 기록 솔루션을 사용하고 응용 프로그램에 의해 접근 할 수 있다. 진료의뢰를 받은 의사는 모바일 디바이스를 통해 환자 기록에 접근했다. 환자 치료 시 의뢰받은 의사는 환자 기록을 EHR 어플리케이션으로 업데이트한다. 초기 진료의뢰를 요청한 의사는 처치 내역을 전달 받고 업데이트된 환자 기록에 접근할 수 있다.
국내의 경우, 진료의뢰서는 대부분 1차 의료기관에서 대형병원으로 오프라인으로 보내는 경우가 많지만 온라인 진료의뢰를 위한 시스템이 구축되고 있다. 진료의뢰서, 요청서, 되의뢰의 3종류의 서식을 온라인으로 보내고자 하며 현재 상급종합병원을 중심으로 관련된 협력기관 (1차 및 2차 의료기관) 과의 연동을 진행하고 있다.

6.2.2 처방전 보내기

이 테스트는 전자 건강 기록 솔루션의 처방전 발송 기능 테스트이다. 이 테스트는 모바일 디바이스 및 전자 건강 기록 솔루션을 사용하여 의사가 처방전을 약국으로 보내는 것을 시뮬레이션 했다.

• 전자 건강 기록 신청서를 통해 직접 약국에 전송
• 이메일 또는 팩스를 통해 처방전을 서비스 업체로 전송
이러한 작업이 성공적으로 완료되었다.

국내의 경우, 처방전은 이메일이나 팩스로 보내는 경우는 없고(의료법 상) 환자가 병원에서 병원비 정산 후 키오스크를 통해 가까운 약국으로 처방전을 전달 할 수 있다. 온라인으로 전달되지 않는 경우, 환자가 키오스크 또는 원무과에서 프린트 된 처방전을 약국으로 직접 가져간다.

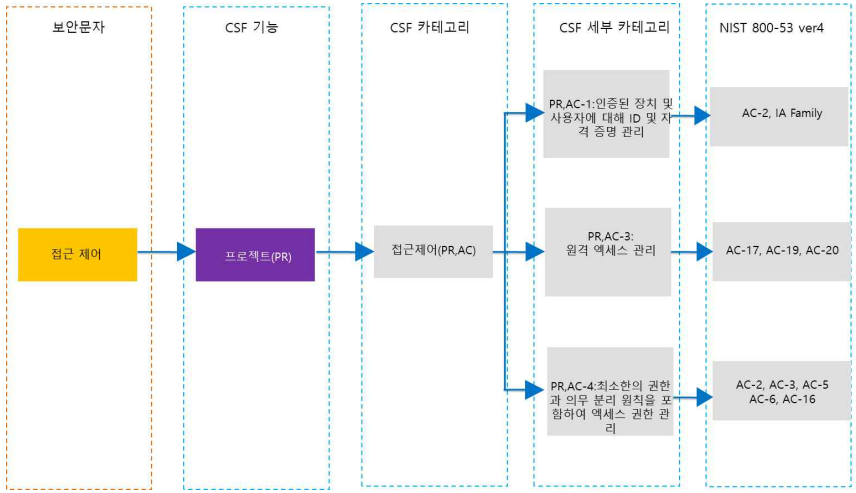
` 6.3 보안성 평가

보안 평가는 아키텍처의 일반적인 보안 기능을 평가했다. 포함할 테스트를 결정하기 위해 표 1 : NIST SP 1800-1d : 표준 및 컨트롤 매핑의 관련 표준 및 컨트롤을 참조하면 된다. 다섯 가지 보안 기능은 아래와 같이 나열된다.

1. 접근 통제
2. 감사 통제 / 모니터링
3. 디바이스 무결성
4. 개인 인증 또는 엔티티 인증
5. 전송 보안

각 기능은 사이버 보안 프레임워크 범주와 하위 범주로 분류된다.

사이버 보안 프레임워크 하위 범주는 하위 범주와 관련되어 인용된 각 표준의 특정 섹션을 참조하여 보안 평가 테스트를 결정하는 데 사용되었다.
프로세스의 예제는 그림 6-1에서 보여준다.



(그림 6-1) 보안 평가에 포함할 테스트를 결정하는 프로세스의 예

프레임워크 하위 범주에 매핑된 보안 표준은 추가 유효성 검사 항목을 제공한다.
프레임워크 하위 범주를 기반으로 테스트를 체계적으로 개발함으로써 우리는 보안 기능 요구에 대해 합리적이고 포괄적인 테스트 세트를 만들었다.
이 보안기능에 대한 모든 테스트가 예제 빌드에서 실행되는 것은 아니다. 모든 보안 평가

테스트는 사용자가 아키텍처의 자체 운영 구현을 평가하고 정책, 절차 및 구성 요소 테스트 및 운영 환경과 관련된 기타 보안 측면에 대한 지침을 제공하는 데 도움을 준다.

7. 위험 평가 방법론

조직은 NIST SP 800-30에 명시된 바와 같이 다음 작업을 수행하여 위험 평가를 수행한다.

- 위협 원인 및 이벤트 식별
- 취약성 파악 및 조건의 파악
- 발생 가능성을 결정
- 영향의 크기 결정
- 위험 결정

위험 평가를 수행하는 두 가지 방법을 제공한다.
(1) 표에 의한 수행 방법 : NIST SP 800-30의 3.2장 "위험 평가 실시"및 NIST SP 800-30의 부록 D-1의 작업 목록 및 모범사례 표를 참조하면 된다. 이는 테스트를 위한 아키텍처 설계 및 빌드사례에 대한 초기 위험 평가 방법이다.
(2) 공격/결함 트리에 의한 평가 방법 : NIST SP 800-30에서 언급한대로 공격/결함 트리 방법론은 사용 사례에 맞게 사용자가 정의되었다. 이것은 유즈케이스의 아키텍처를 분해함으로써 수행되었다. 두 방법 모두 위험 평가와 분석을 수행했다.

두 가지 방법 모두 위험 요인에 대해 위험 평가와 사용 사례에 대해 분석을 수행 한 후 다음과 같은 위험을 결정했다.

- 기밀성 상실 – 중요한 정보의 무단 공개로 인한 영향
- 무결성 손실 – 데이터 또는 시스템의 무단 변경으로 시스템 또는 데이터 무결성이 손실될 때 미치는 영향
- 가용성 손실 – 시스템 기능 및 운영 효율성에 미치는 영향

테이블 기반 방법은 소프트웨어 도구를 사용하지 않고 위험을 평가하는 기술을 제공한다. 반면에 프로그래밍 언어 지원도구(Decision Programing Language, DPL) 도구를 사용하여 폴트 트리 기법을 사용하면 그래프 기반 분석을 수행하고 특정 위협 이벤트를 사용하여 위협 시나리오를 생성할 수 있다. 모델링과 시뮬레이션은 많은 수의 위협 시나리오를 생성하여 집중된 하위 세트에 대한 분석을 직접 수행하지 않도록 한다.

위험 평가는 위험 목록과 위험 수준을 결정한다. 확인된 위험은 보안 기능을 검증하기 위한 자료로 사용된다.
중요한 인프라 사이버 보안 개선을 위한 NIST 프레임워크 (사이버 보안 프레임워크 또는 CSF라고도 함) 및 보안 기능에 연결하면 필요 모든 구성 요소를 갖춘 기업 인프라를 구

축함으로써 대책을 마련할 수 있다. 조직은 이러한 위험을 처리하고 건강 정보를 보호하기 위한 조치를 취할 수 있다. 이 섹션에서는 두 가지 평가 방법을 모두 사용는 적용 사례를 제공한다.

7.1 테이블 기반 위험 평가 적용사례

이 섹션에서는 평가 및 확인을 위한 사례를 제공한다.

- 적대적 위험의 예
- 비적대적 위험의 예

위험 평가 과정에서 3.2장 "위험 평가 실시"에서 설명한 작업을 수행하고 NIST SP 800-30의 부록 D-1에 요약 된 참조 표, 템플리트 및 평가 척도 표를 사용한다.
요약하면 다음 작업 6가지를 수행했다.

- 과제 1 : 우려의 위협 원인을 확인하고 기능화한다.
- 작업 2 : 잠재적 위협 이벤트를 식별한다.
- 작업 3 : 취약성 및 취약성을 식별한다.
- 작업 4 : 가능성을 결정한다.
- 작업 5 : 영향을 결정한다.
- 작업 6 : 위험을 결정한다.

*위협(Threat): 손실이나 손상의 원인이 될 가능이 제공되는 환경 예)취약점, 해커의 존재
각 작업에 대해 우리는 최종 작업 6에서 사용 된 결과를 사용하여 여러 가지 중간 표를 작성하여 위험을 판별했다. 중간 테이블은 출력이 최종 테이블로 집계되기 때문에 이 문서에서 생략된다. 우리의 평가 결과는 위험 수준을 높음에서 낮음으로 분류하여 다음 그룹에 포착된다.

- 적대적 위험 (기밀성 상실)
- 적대적 위험 (무결성 손실)
- 적대적 위험 (가용성 상실)
- 비적대적 위험 (기밀성 상실)
- 비적대적 위험 (무결성 손실)
- 비적대적 위험(가용성 손실)

*위험(Risk): 위험에 따라 생길수 있는 손실에 대한 가능성 예)정보유출, 공격, 탈취
아래의 적대적 위험 템플릿 테이블과 비적대적 위험 템플릿 테이블은 각 위험 요소에 대한 평가 결과를 보여준다.

<표 7-1> 적대적 위험 템플릿

1	2	3	4	5	6	7	8	9	10	11	12	13
위협 사건	위협 원인	위협원 기능			관련성	공격 개시 확률	취약성 및 사전 발생 조건	심각성 및 확대 가능성	공격 가능성에 대한 성공률	전반적인 가능성	영향 수준	위험
		능력 (capability)	의도 (intent)	목표 (targeting)								
모바일 시스템 및 디바이스 (예 : 랩탑, PDA, 스마트 폰)의 알려진 취약점을 악용	적 / 해커	보통	높음	낮음	가능함	보통	멀웨어 - 기술 / 아키텍처 및 기능성	보통	보통	보통	낮음	보통

<표 7-2> 적대적 위험 샘플 워크쓰루

번호 (Column)	사건 (Heading)	콘텐츠(Content)	사례 (Example walkthrough/Explanation)
1	위협 사건	위협 이벤트 식별	유즈케이스를 기반으로, 위협 이벤트 중 하나를 선택함 "모바일 시스템 및 디바이스 (예: 랩탑, PDA, 스마트 폰)의 알려진 취약점 악용
2	위협 원인	위협 이벤트를 일으킬 수 있는 위협 원인을 식별	"적/해커"가 공격을 시작할 수 있음
3	능력	위협 원인 영향 평가	공격자는 여러 가지 성공적인 공격을 지원할 수 있는 적절한 자원, 전문 지식 및 기회를 가지고 있음
4	의도	위협 원인 의도 평가	적들은 조직의 사이버 자원을 혼란 시키려하므로 소스 원인은 "보통"임
5	목표	위협 원인 타겟 평가	위협 원인 타겟팅은 공격자가 공개적으로 사용할 수 있는 정보만 사용하여 타겟팅 할 수 있음
6	관련성	위협 이벤트의 관련성을 결정함 위협 이벤트 관련성은 위협이 진행되기 위해 고려해야 할 사항 중 충족하지 못한 것이 있으면 발생하지 않음	이 위협 이벤트의 관련성은 "가능"임
7	공격 개시 확률	기능, 의도 및 대상을 고려하여 하나 이상의 위협 원인에 의해 위협 이벤트가 시작될 가능성에 대한 것임	보통의 기능과 의도 및 낮은 위협의 소스 타겟팅을 사용하면 공격자가 치료 이벤트를 시작할 가능성이 높으므로 "보통"이 여기에 사용됨
8	취약성 및 사전 발생조건	위협 이벤트를 시작하는 위협 원인이 될 수 있는 취약성과 악영향의 가능성을 높이는 취약성을 식별함	IT 시스템 및 취약성 평가와 관련된 취약점을 기반으로 특정 제품이나 제품군을 사용하여 해커가 악용 할 수 있는 취약점 (악성 소프트웨어)은 악영향을 미칠 수 있음

9	심각성 및 확대가능성	위협 취약의 심각성과 확산을 평가함	이 취약점은 취약점의 노출과 탈취 용이성 및 / 또는 악용으로 인해 발생할 수 있는 영향의 정도에 의하며 “보통”임 관련 보안 통제 또는 기타 개선 조치가 부분적으로 구현되어 어느정도 효과적임
10	공격가능성에 대한 성공률	위협 이벤트가 일단 시작되면 위협 원인, 취약성 및 악영향을 미칠 가능성을 판단함	적절한 치료 소스 기능과 취약성의 확대를 기반으로 위협 이벤트가 시작되거나 발생하는 경우 악영향을 미칠 가능성이 다소 적으면 "보통"으로 평가함
11	전반적인 가능성	위협 이벤트가 시작되어 악영향을 미칠 가능성을 결정함(예 : 공격 개시 확률과 개시된 공격이 성공할 확률의 조합).	전반적인 가능성은 공격 개시 확률 (7 번, 보통)과 개시된 공격의 성공 확률 (10 번, 보통)의 조합임 표 5 : 평가 척도 – 전체 가능성 (Overall Likelihood)를 확인하면 전반적인 가능성이 보통임
12	영향 수준	위협 이벤트로부터 악영향 (즉, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 잠재적 인 손해)을 결정함	이 위협 이벤트로 인해 조직 운영에 잠재적으로 해를 끼칠 수 있음. 이 위협 이벤트는 모바일 시스템 및 / 또는 모바일 디바이스가 가용성을 상실 할 수 있으므로 조직 운영에 심각한 악영향을 미칠 것으로 예상됨. 영향의 정도는 보통임.
13	위험	위험도를 가능성과 영향의 조합으로 결정함	위험도는 가능성 (열 11, 보통)과 영향 (열 12, 보통)의 조합임 표 7-5와 6 평가기준 – 위험 수준 (가능성과 영향의 조합)을 확인하면 위험 수준이 보통임

<표 7-3> 비적대적 위험 템플릿

1	2	3	4	5	6	7	8	9	10	11
위협 이벤트	위협 원인	효과 범위	관련성	위협 이벤트 발생 가능성	취약성 및 사전조건	심각도 및 확산율	우회적 사건으로 인한 부정적인 영향	전반적인 가능성	위협수준	위험
잘못된 권한 설정	우연성 (사용자 , 관리자)	보통	예측됨	보통	정보 관련 / 특별 접근 프로그램	보통	높음	보통	보통	낮음

<표 7-4> 비적대적 위험 샘플 워크쓰루

번호 (Column)	사건 (Heading)	콘텐츠 (Content)	사례 (Example walkthrough/Explanation)
1	위협 이벤트	위협 이벤트 식별	유스 케이스를 기반으로, 위협 이벤트 중 하나가 선택됨 "잘못된 권한 설정"
2	위협 원인	위협 이벤트를 일으킬 수 있는 위협 원인을 식별	"우발적인 (사용자, 관리자 사용자)" 에 의해 위험이 시작될 수 있음
3	효과 범위	위협 원인으로부터의 영향 범위를 확인	사고의 영향은 광범위하며 일부 중요한 자원을 포함하여 정보 시스템의 사이버

			자원의 상당 부분을 차지함. 따라서 "보통"이 여기에 사용됨
4	관련성	위협 이벤트의 관련성을 결정함 위협 이벤트 관련성은 위협이 진행되기 위해 고려해야 할 사항 중 충족하지 못한 것이 있으면 발생하지 않음	이 위협 이벤트의 관련성은 "예측 됨"임
5	위협 이벤트 발생 가능성	위협 이벤트가 발생할 확률을 결정함	사고가 발생할 가능성이 다소 높음. 그래서 "보통"이 여기에 사용됨
6	취약성 및 사전 조건	위협 이벤트를 시작하는 위협 원이 악용 할 수 있는 취약성과 악영향의 가능성을 높일 수 있는 취약성을 식별함	IT 시스템 및 취약성 평가와 관련된 취약점을 기반으로(잘못된 권한 설정과 관련된) 취약성은 사용자에 의해 우연히 악용 될 수 있으며 이로 인해 악영향을 미칠 수 있음
7	심각도 및 확산율	취약성의 심각성과 취약성의 확산을 평가함	이 취약점은 취약점의 노출과 착취의 용이성 및 악용으로 인해 발생할 수 있는 영향의 정도에 따라 결정됨. 관련 보안 통제 또는 기타 개선 조치가 부분적으로 구현됨
8	우회적 사건으로 인한 부정적인 영향	위협 이벤트가 일단 시작되면 취약성 및 취약성을 고려하여 악영향을 미칠 가능성을 판단함	중간정도의 위협 치료를 기반으로 할 때, 부작용이 있을 가능성이 높으며, 부작용은 "높음"으로 평가해야함
9	전반적인 가능성	위협 이벤트가 발생할 가능성을 결정하고 악영향 (즉, 위협이 발생할 가능성과 위협 이벤트가 악영향을 미칠 가능성)의 조합을 초래할 가능성을 결정함	위협 이벤트가 발생하여 악영향을 미칠 가능성은 위협 발생 가능성 (5번, 보통)과 위협 이벤트가 악영향을 미칠 가능성 (8번, 높음)의 조합임 표 5 : 평가 척도 – 전체 우도 (Overall Likelihood)를 확인하면 전반적인 가능성이 보통임
10	위협 수준	위협 이벤트로부터 악영향 (즉, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 잠재적 인 손해)을 결정함	이러한 위협 이벤트로 인해 조직 운영 및 정보 관련 특별 접근 프로그램에 잠재적으로 해를 끼칠 수 있음 이 위협 이벤트는 모바일 시스템 및 모바일 디바이스가 가용성을 상실 할 수 있으므로 조직 운영에 심각한 악영향을 미칠 것으로 예상 될 수 있음 영향의 정도는 보통임
13	위험	위험도를 가능성과 영향의 조합으로 결정함	위험도는 영향 (9번, 보통)와 위험수준 (10번, 보통)의 조합임. 표 7-5와 6의 : 평가 기준 – 위험 수준 (가능성과 영향의 조합)을 확인하면 위험 수준이 보통이다.

<표 7-5> 평가 기준 – 전체 발생률 (overall likelihood)

위협 이벤트 개시 또는 발생 가능성	가능성이 있는 위협 이벤트로 인해 악영향				
	매우 낮음	낮음	보통	높음	매우 높음
매우 높음	낮음	보통	높음	매우 높음	매우 높음
높음	낮음	보통	보통	높음	매우 높음
보통	낮음	낮음	보통	보통	높음
낮음	매우 낮음	낮음	낮음	보통	보통
매우 낮음	매우 낮음	매우 낮음	낮음	낮음	낮음

<표 7-6> 평가 기준 – 위험 수준 (발생률 및 영향도의 조합)

가능성 (위협 이벤트가 발생하고 악영향을 미침)	가능성이 있는 위협 이벤트로 인해 악영향				
	매우 낮음	낮음	보통	높음	매우 높음
매우 높음	매우 낮음	낮음	보통	높음	매우 높음
높음	매우 낮음	낮음	보통	높음	매우 높음
보통	매우 낮음	낮음	보통	보통	높음
낮음	매우 낮음	낮음	낮음	낮음	보통
매우 낮음	매우 낮음	매우 낮음	매우 낮음	낮음	낮음

7.2 램 파트의 공격 / 결함 트리 구동 위험 평가 적용사례

NIST는 램파트 논리제어(Ramparts LLC)와 협력하여 공격/결함 트리를 사용하여 위험 평가를 수행했다. 이 방법론을 사용하여 공격 이벤트의 영향을 식별하고 우선순위를 지정할 수 있었다. 공격 이벤트의 영향을 우선 순위화하여 공격 기반 시나리오 테스트, 대응책 구현 및 대응책 개발에 중점을 두었다. 분석 접근 방식을 선택할 때 그래프 기반 분석은 다음과 같은 다 대다 관계를 설명하는 효과적인 방법을 제공한다.

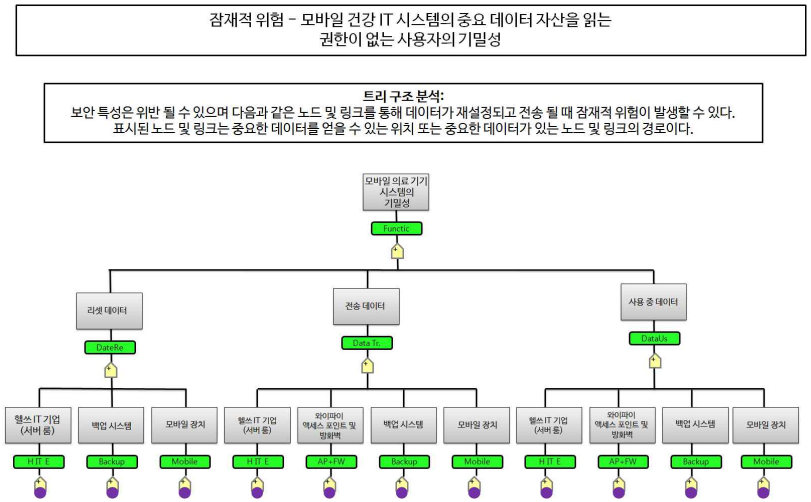
- 위협 원인 및 위협 사건,
- 위협 이벤트 및 취약점,
- 위협 사건 및 영향 / 자산.

단계

램파트의 공격 / 결함 트리 위험 평가 방법론에 관련된 단계는 다음과 같다.

(1) 위험 평가의 범위 (잠재적인 위험, 보안 기능, 중요 데이터 자산을 정의하고 NIST 사이버 보안 프레임워크에 매핑)

(2) 보안 기능 및 중요 데이터 자산을 대상으로 하는 공격 이벤트 트리 생성 (위협 시나리오)
(3) 대책 / 보호 디바이스 지정
(4) 업계의 주요 적을 기반으로 보안 기능이 손상될 가능성을 할당
(5) 분석 및 현재 결과 (시스템에 대한 가장 큰 상대 위험이 어디에 있는지, 그리고 위험을 최소화하기 위하여 향후에 어느곳을 신경 쓸 것인지 확인한다.)



(그림 7-1) 기밀성 공격트리 모형

1단계 : 위험 평가 범위 지정

CSF는 이 위해성 평가의 범위를 알리는 데 사용된다. 잠재적인 위험은 환자 건강 정보의 기밀성, 무결성 및 가용성에 대한 위험으로 정의된다. 표2 에 정의 된 보안 기능은 CSF 및 기타 표준에 매핑된다.

2단계 : 대책 및 안전 디바이스가 포함된 공격 이벤트 트리 만들기 (공격 시나리오)

잠재적인 공격 이벤트는 이벤트 트리를 사용하여 개발된다. 하위 레벨 이벤트에 발생 가능성을 부여 할 수 있는 논리 구조를 정의한다. 논리 구조는 또한 다른 전문 분야의 보안 전문가가 평가를 보다 쉽게 검토하고 기여할 수 있도록 한다. 이벤트 노드는 발생 가능성을 지정할 수 있는 수준으로 분해되었다. 성공하기 위해 병행하여 발생해야하는 공격 시나리오의 이벤트는 함께 AND 연산된다. 병렬로 발생할 수 있는 이벤트는 함께 OR연산으로 되어 나타난다.

이 사용 사례를 위해 선택된 공격 이벤트 트리의 논리적 구조는 다음과 같다.
(1) 기밀성, 무결성 및 가용성에 대한 세 가지 잠재적 위험에 대해 별도의 공격 트리가 만들어졌다.

(2) 각 트리의 맨 위에 잠재적 위험이 모델링되고 측정되는 위험으로 정의 되었다
(3) 트리의 두 번째 계층은 휴지 상태의 데이터, 전송중인 데이터 및 사용 중인 데이터로 모델링되었다.
(4) 세 번째 계층에서는 시스템의 디바이스 및 데이터 노드를 모델링했다. 아래의 그림 7-1은 기밀성 공격 트리를 보여준다.

3단계 : 대책 / 보호 디바이스 지정

NIST SP 1800-1b (기술보고서 PART II) : 접근 방식, 아키텍처 및 보안 기능 중 보안 대책 /안전한 디바이스는 낮은 수준의 공격 사건에 할당되었다.

예를 들어 "Install File Copying Malware" 이벤트를 모델링 할 때 모바일 디바이스에서 실행되는 최신 바이러스 백신 소프트웨어가 할당되었다. 이런 대책은 발생 가능성을 지정하는 데 고려 사항의 일부이다 (4 단계).

4단계 : 업계의 주요 적을 기반으로 보안 기능이 손상 될 수 있는 가장 낮은 수준의 공격 이벤트 발생 가능성을 할당

발생 가능성은 Very High, High, Medium-High, Medium, Low-Medium, Low 및 Very Low로 지정된다. 전문가 의견을 입력 할 때 이 세분화 수준이 너무 세밀 할 수 있으므로 그 대신 높음, 중간 및 낮음의 질적 척도가 사용될 수 있다.

다음과 같은 '발생률(likelihoods)'이 사용되었다.

<표 7-7> 위험 발생률

값(Value)	정성적 값(Qualitative Numeric Value)
낮음(Low)	.01
보통보다 낮음(Medium Low)	.1
보통(Medium)	.5
보통보다 높음(Medium High)	.75
높음(High)	.9

정성적 수치 값은 이벤트 트리 내에서 상위 레벨의 확률을 계산하는 데 사용된다.
이것은 특정 공격 시나리오가 발생할 가능성이 있는지 평가하는 데 사용되었다.
공격 트리의 하위 레벨 이벤트에 발생 값의 가능성을 지정할 때 다음 기준이 사용된다.

1. 공격 성공 가능성
이 성공 기준은 시스템에 배포 된 보호 대책, 이벤트의 복잡성 및 알려진 악용의 가용성을 고려한다.

2. 공격자가 발견되지 않을 가능성
모든 탐지가 동일하게 생성되는 것은 아니다. 적절한 경우 킬 체인(Kill Chain) 모델의 7단계가 고려된다. 정찰 단계 (공격 초기)의 탐지는 (공격 후반) 목표 행동 단계에서 탐지하는 것보다 훨씬 유리할 수 있다. 공격자가 몇 달 또는 몇 년 동안 중요한 데이터를 내보낼 수 있었고 시스템에 다른 접근을 설정했을 수 있는 경우 분명히 그 피해가 훨씬 클 수 있다. 시스템에 배치 된 탐지 대책은 탐지 기준으로 간주된다.

3. 공격자의 자원 요구
시간과 돈에 대한 공격의 비용은 사건에 대한 질적 가치를 부여받는다. MORDA에서 차용 하여 다음의 표와 같은 규모가 산정되었다

<표 7-8> 규모 산정

값(Value)	비용 범위(Range)
무료(Free)	0 - $1,000
매우 낮음(Very Low)	$1,000~$10,000
낮음(Low)	$10,000~$100,000
보통(Medium)	$100,000~$1 Million
높음(High)	$1 Million~ $10 Million
Very High	> %10 Million

이 평가에 사용한 가정은 잠재적인 적들이 사용하게 될 공격이 매우 낮고 부족한 리소스 수준에 있다는 것이다.

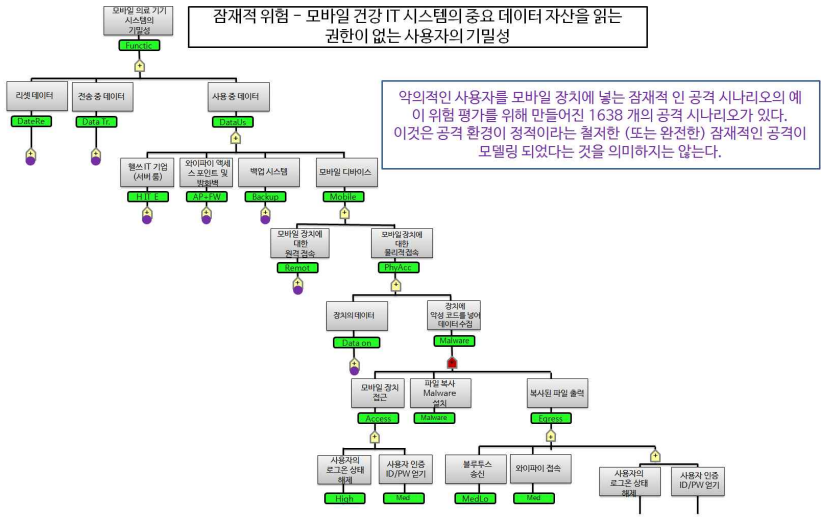
4. 공격 트리 이벤트에 할당 할 단일 질적인 값을 생각해 내면 성공 가능성, 탐지 가능성, 공격자의 자원이 필요하다.
낮은 확률이지만, 적의 성공으로 이벤트가 득점되면 공격자가 발견되지 않을 가능성을 고려해야 한다.
탐지 대응책은 제로 데이 공격 (알려지지 않은 /보고되지 않은 / 패치되지 않은 공격)으로부터 중요 데이터를 보호하고 중요한 데이터에 대한 모든 성공적인 공격으로 인한 잠재적 손상을 최소화하는 데 도움이 될 수 있다.

이 평가는 적의 성공 확률에 동등한 비중을 부여하고 있으며 발견되지 않다.
좋은 보안을 제공하는 조직의 한 가지 목표는 비용이 많이 드는 목표를 달성하기 위해 상대방이 필요로 하는 자원을 만드는 것이다. 이 평가를 위해 모든 공격 시나리오에 대해 동일하게 낮은 수준의 리소스를 사용했다.

아래 표는 세 가지 유형의 "적대적인 가능성"을 조합하여 할당된 가능성(Assigned Likelihood of Occurrence)에 대한 단일 값을 산출하기 위해 결합될 수 있다.

<표 7-9> 사건발생 가능성에 대한 값

사건	공격 성공 가능성	공격이 탐지되지 않을 가능성	공격 필수 자원	공격 발생 가능성
A	매우 낮음	매우 낮음	자유/매우 낮음	매우 낮음
B	매우 낮음	낮음	자유/매우 낮음	낮음
C	매우 낮음	중간	자유/매우 낮음	낮음-보통
D	매우 낮음	높음	자유/매우 낮음	보통
E	매우 낮음	매우높음	자유/매우 낮음	보통-높음
F	낮음	매우 낮음	자유/매우 낮음	낮음
G	낮음	낮음	자유/매우 낮음	낮음
H	낮음	중간	자유/매우 낮음	낮음-보통
I	낮음	높음	자유/매우 낮음	보통
J	낮음	매우높음	자유/매우 낮음	보통-높음
K	중간	매우 낮음	자유/매우 낮음	낮음-보통
L	중간	낮음	자유/매우 낮음	낮음-보통
M	중간	중간	자유/매우 낮음	보통
N	중간	높음	자유/매우 낮음	보통-높음
O	중간	매우높음	자유/매우 낮음	보통-높음
P	높음	매우 낮음	자유/매우 낮음	보통
Q	높음	낮음	자유/매우 낮음	보통
R	높음	중간	자유/매우 낮음	보통-높음
S	높음	높음	자유/매우 낮음	높음
T	높음	매우높음	자유/매우 낮음	매우 높음
U	매우높음	매우 낮음	자유/매우 낮음	보통
V	매우높음	낮음	자유/매우 낮음	보통
W	매우높음	중간	자유/매우 낮음	보통-높음
X	매우높음	높음	자유/매우 낮음	높음
Y	매우높음	매우높음	자유/매우 낮음	매우 높음



(그림 7-2) 악성코드 사용에 대한 사례

완벽한 공격 지점 (시나리오)을 보려면 아래의 그림 7-2를 참조하면 된다. 이 지점은 모바일 디바이스에 대한 실제 사용의 예로서 물리적 디바이스 접근 및 디바이스에 악성 코드 유포 공격에 대한 데이터 공격을 보여준다.

5단계 : 분석 및 현재 결과

확립된 신뢰성 확률 이론을 사용하여, OR 결합 된 트리 구조의 이벤트 (병렬로 발생할 수 있는 이벤트)는 P = 1- (1-p2) (1-p3)로 표시되는 확률을 가질 수 있다. 1에서 이벤트 2와 이벤트 30이 모두 적의 목표에 도달 한 확률을 뺀 것이다.
함께 And 된 이벤트 (순차적 인 이벤트)는 P = p4 * p5로 나타낼 수 있다.
이는 이벤트4 또는 이벤트5가 수행되지 않았을 가능성이 높다. 모델링 된 복잡한 공격트리 구조에서 다음 분석을 실행하고 결과를 사용했다.

모델링 된 복잡한 공격 트리 구조에서 분석이 실행되고 다음과 같은 결과가 사용되었다.

1) 낮은 수준의 공격 이벤트에 대한 변경이 가장 큰 영향을 미칠 부분을 표시하기 위해 부분 파생물이 사용되었다.

2) 계산된 최소 절단 세트는 모델링된 총 공격 수를 나타냅니다.
사용 된 분석에 대한 심층적인 토론은 "위험 분석 모델 (RAM)"에서 찾아 볼 수 있다.
이곳에 사용된 위험 평가 방법은 일반적으로 시스템 구현자와 대응책 개발자가 사용하는 증거 기반 취약성 테스트를 효과적이고 효율적으로 집중하는 데 사용되며 아래에 표시된 것처럼 위험 관리 시스템 / 프레임워크에 입력된다.

8 위험 평가 결과

8.1 테이블 기반 평가 적용사례

아래의 표들은 적대적 위험 테스트에서 테이블을 이용한 결과들을 보여준다.

<표 8-1> 테이블 이용 결과 – 기밀성 기반 적대적 위험

1	2	3	4	5	6	7	8	9	10	11	12	13	
위협 사건	위협 근원	위협원 기능			관련성	공격개시확률	취약성 및 사전조건	심각도 및 확산률	공격성공가능성	위험가능성	위험수준	위험	위험요소
		수용성	공격의지	타겟팅									
시스템 침입 및 무단 시스템 접근	적 / 해커	보통	높음	높음	가능	보통	암호 복잡성 통제 부족으로 인한 약한 암호	높음	높음	높음	매우높음	매우높음	10
외부 네트워크의 네트워크 스니핑을 통해 중요 정보획득	적 / 해커	낮음	보토	보통	예측	보통	아키텍처와 디자인에 보안을 부적절하게 통합	중간	높음	높음	매우높음	매우높음	9
도난된 휴대폰	적 / 해커	높음	높음	높음	확정	높음	사용자 교육 및 물리적 보안 부족	높음	높음	높음	높음	높음	8
통신 차단 공격 수행	적 / 해커	낮음	높음	보통	가능	보통	암호화되지 않은 데이터를 가로 채기위한 전송 암호화 부족	높음	높음	높음	높음	높음	8
공개적으로 접근가능한 정보시스템의 데이터 생성, 삭제	적 / 해커	보통	보통	보통	예측	보통	부적절한 접근 통제 및 집행 부적절한 데이터	보통	보통	높음	높음	높음	8

및 수정으로 인한 무결성 손상 (예: 웹손상)							보존, 백업 및 복구						
모바일 시스템의 알려진 취약점을 악용 (예 : 랩톱, PDA, 스마트폰)	적 / 해커	보통	높음	높음	가능	높음	멀웨어 – 기술적 / 아키텍처적 및 기능적	보통	보통	보통	높음	보통	5
악의적인 기능 제공 / 삽입 / 설치	적 / 해커	보통	높음	보통	에상	보통	아키텍처와 디자인에 보안을 부적절하게 통합	보통	보통	보통	높음	보통	5
공격수행 (즉 공격 도구 또는 활동을 직접 /조정)	적 / 해커	보통	보통	보통	에상	보통	아키텍처와 디자인에 보안을 부적절하게 통합	보통	보통	보통	보통	보통	5

<표 8-2> 테이블 이용 결과 – 무결성 기반 적대적 위험

1	2	3	4	5	6	7	8	9	10	11	12	13	
위협 사건	위협 근원	위협원 기능			관련성	공격개시확률	취약성 및 사전조건	심각도 및 확산률	공격성공가능성	위험가능성	위험수준	위험	위험요소
		수용성	공격의지	타겟팅									
공개적으로 접근할 수 있는 정보시스템 (예 : 웹 손상)의 데이터를 생성, 삭제 및 수정하여 무결성 손실 유발	적 / 해커	보통	타겟팅	보통	예측	보통	부적절한 접근 통제 및 / 시행 부적절한 데이터 보존, 백업 및 복구	보통	보통	높음	매우높음	매우높음	10

도난된 휴대폰	적 / 해커	높음	높음	높음	확정	높음	사용자 교육 및 물리적 보안 부족	높음	높음	높음	높음	높음	8
모바일 시스템의 알려진 취약점을 악용 (예 : 랩톱, PDA, 스마트폰)	적 / 해커	보통	높음	높음	가능	높음	멀웨어 - 기술적 / 아키텍처	보통	보통	보통	높음	높음	8
시스템 침입 및 무단 시스템 접근	적 / 해커	보통	높음	높음	가능	보통	암호 복잡성 통제 부족으로 인한 약한 암호	높음	높음	높음	보통	보통	8
통신 차단 공격 수행	적 / 해커	낮음	높음	보통	가능	보통	암호화되지 않은 데이터를 가로 채기위한 전송, 암호화 부족	보통	높음	높음	높음	높음	8
악의적인 기능 제공 / 삽입 / 설치	적 / 해커	보통	높음	보통	에상	보통	아키텍처와 디자인에 보안을 부적절하게 통합	보통	보통	보통	높음	보통	5
외부 네트워크의 네트워크 스니핑을 통해 민감 정보획득	적 / 해커	낮음	보통	보통	예측	보통	아키텍처와 디자인에 보안을 부적절하게 통합	중간	높음	높음	높음	높음	8
악의적인 기능 제공 / 삽입 / 설치	적 / 해커	보통	높음	보통	에상	보통	아키텍처와 디자인에 보안을 부적절하게 통합	보통	보통	보통	높음	보통	5

<표 8-3> 테이블 이용 결과 - 가용성 기반 적대적 위험

1	2	3	4	5	6	7	8	9	10	11	12	13	
위협 사건	위협 근원	위협원 기능			관련성	공격 개시 확률	취약성 및 사전조건	심각도 및 확산률	공격성공 가능성	위험 가능성	위험 수준	위험	위험 요소
		수용성	공격의지	타겟팅									
도난된 휴대폰	공격 / 해커	높음	타겟팅	높음	확정	높음	사용자 교육 및 물리적 보안 부족	보통	보통	높음	높음	높음	8
모바일 시스템의 알려진 취약점을 악용 (예 : 랩톱, PDA, 스마트폰)	공격 / 해커	보통	높음	높음	가능	높음	멀웨어 - 기술적 / 아키텍처	보통	보통	보통	높음	높음	8
공개적으로 접근가능한 정보시스템의 데이터 생성, 삭제 및 수정으로 인한 무결성 손상 (예: 웹손상)	공격 / 해커	보통	보통	보통	예측	보통	부적절한 접근 통제 및 집행 부적절한 데이터 보존, 백업 및 복구	보통	보통	높음	높음	높음	8
시스템 침입 및 무단 시스템 접근	공격 / 해커	보통	높음	높음	가능	보통	암호 복잡성 통제 부족으로 인한 약한 암호	보통	보통	보통	높음	보통	5
통신 차단 공격 수행	적 / 해커	낮음	높음	보통	가능	보통	암호화되지 않은 데이터를 가로 채기위한 전송	보통	보통	보통	높음	보통	5

							암호화 부족						
악의적인 기능 제공 / 삽입 / 설치	적 / 해커	보통	높음	보통	예상	보통	아키텍처에 의한 보안을 부적절하게 통합	보통	보통	보통	높음	보통	5
외부 네트워크의 네트워크 스니핑을 통해 민감 정보획득	적 / 해커	낮음	보통	보통	예측	보통	아키텍처에 의한 보안을 부적절하게 통합	보통	낮음	보통	보통	보통	5
공격수행 (즉 공격 도구 또는 활동을 직접 /조정)	적 / 해커	보통	보통	보통	예상	보통	아키텍처에 의한 보안을 부적절하게 통합	보통	낮음	낮음	보통	낮음	2

<표 8-4> 테이블 이용 결과 – 기밀성 기반 비적대적 위험

1	2	3	4	5	6	7	8	9	10	11	
		위협원 기능									
위협 사건	위협 근원	수용성	공격의지	타겟팅	관련성	공격개시확률	취약성 및 사전조건	심각도 및 확산률	공격성공가능성	위험가능성	위험수준
유출된 민감 정보	의도하지 않은 (사용자, 관리자)	보통	예측	낮음	부적절한 사용자 교육 추적 할 수 없는 사용자 작업	보통	매우 높음	매우 높음	매우 높음	매우 높음	10
휴대 디바이스 분실	의도하지 않은 (사용자)	매우 낮음	확정	보통	정보 관련 / 특별 접근 프로그램	보통	높음	높음	높음	높음	8
잘못된 권한 설정	의도하지 않은 (사용자, 관리자)	높음	예측	보통	정보 관련 / 특별 접근 프로그램	보통	높음	보통	높음	높음	8
권한있는 사용자의	의도하지 않은	높음	예측	낮음	부적절한 사용자 교육	보통	매우 높음	보통	높음	높음	8

중요하고 민감한 정보의 잘못된 취급	(사용자, 관리자)				추적 할 수 없는 사용자 작업						
로그온 한 디바이스에서 이탈한 거리	의도하지 않은 (사용자)	낮음	확정	보통	부적절한 사용자 교육	보통	높음	보통	보통	보통	5
바이러스 또는 기타 멀웨어 다운로드	의도하지 않은 (사용자)	낮음	확정	보통	부적절한 사용자 교육, 정책 집행 부족, 부적절한 구성 관리	보통	보통	보통	보통	보통	5
보안되지 않은 Wi-Fi 네트워크 사용	의도하지 않은 (사용자)	매우 낮음	확정	높음	부적절한 사용자 교육	낮음	보통	보통	보통	보통	5
소프트웨어 제품에 취약점 유입	구조적 취약 (소프트웨어)	높음	예상	보통	부적절한 변경 관리 또는 구성 관리	높음	보통	보통	보통	보통	5
약한 접근 통제	의도하지 않은 (사용자, 관리자)	높음	예측	보통	부적절한 접근 통제 및 시행	높음	보통	보통	보통	보통	5
디스크 에러	구조적 취약 (IT 장비)	높음	예상	보통	환경 규제 부족	보통	낮음	낮음	보통	낮음	2

<표 8-5> 테이블 이용 결과 – 무결성 기반 비적대적 위험

1	2	3	4	5	6	7	8	9	10	11	
		위협원 기능									
위협 사건	위협 근원	수용성	공격의지	타겟팅	관련성	공격개시확률	취약성 및 사전조건	심각도 및 확산률	공격성공가능성	위험가능성	위험수준

권한있는 사용자의 중요&민감 정보의 잘못된 취급	의도하지 않은 (사용자, 관리자)	높음	예측	낮음	부적절한 사용자 교육 추적 할 수 없는 사용자 작업	보통	매우 높음	매우 높음	매우 높음	매우 높음	10
유출된 민감 정보	의도하지 않은 (사용자, 관리자)	보통	예측	낮음	부적절한 사용자 교육 추적 할 수없는 사용자 작업	보통	매우 높음	높음	높음	높음	8
휴대 디바이스 분실	의도하지 않은 (사용자)	매우 낮음	확정	보통	정보 관련 / 특별 접근 프로그램	보통	높음	높음	높음	높음	8
잘못된 권한 설정	의도하지 않은 (사용자, 관리자)	높음	예측	보통	정보 관련 / 특별 접근 프로그램	보통	높음	보통	높음	높음	8
로그온 한 디바이스에서 벗어난 거리	의도하지 않은 (사용자)	낮음	확정	보통	부적절한 사용자 교육	보통	높음	보통	보통	보통	5
바이러스 또는 기타 멀웨어 다운로드	의도하지 않은 (사용자)	낮음	확정	보통	부적절한 사용자 교육, 정책 집행 부족, 부적절한 구성 관리	보통	보통	보통	보통	보통	5
보안되지 않은 Wi-Fi 네트워크 사용	구조적 취약 (소프트웨어)	매우 낮음	확정	높음	부적절한 변경 관리 또는 구성 관리	낮음	보통	보통	보통	보통	5
소프트웨어 제품에 취약점 유입	구조의 (소프트웨어)	높음	예측	보통	부적절한 변경 관리 또는 구성 관리	높음	보통	보통	보통	보통	5
약한 접근 통제	의도하지 않은 (사용자, 관리자)	높음	예측	보통	부적절한 접근 통제 및 시행	높음	보통	보통	보통	보통	6
디스크 에러	구조적 취약 (IT 장비)	높음	예측	보통	환경 규제 부족	보통	낮음	낮음	보통	낮음	2

<표 8-6> 테이블 이용 결과 – 가용성 기반 비적대적 위험

1	2	3	4	5	6	7	8	9	10	11	
위협 사건	위협 근원	위협원 기능			관련성	공격 개시 확률	취약성 및 사전 조건	심각도 및 확산률	공격성 공가능성	위험 가능성	위험 수준
		수용성	공격의지	타겟팅							
휴대 디바이스 분실	의도하지 않은 (사용자)	매우 낮음	확정	보통	정보 관련 / 특별 접근 프로그램	보통	매우 높음	매우 높음	매우 높음	매우 높음	10
권한있는 사용자의 중요하고 민감한 정보의 잘못된 취급	의도하지 않은 (사용자, 관리자)	높음	예측	낮음	부적절한 사용자 교육 추적 할 수 없는 사용자 작업	보통	높음	높음	높음	높음	8
유출된 민감 정보	의도하지 않은 (사용자, 관리자)	보통	예측	낮음	부적절한 사용자 교육 추적 할 수없는 사용자 작업	보통	매우 높음	높음	높음	높음	8
바이러스 또는 기타 멀웨어 다운로드	의도하지 않은 (사용자)	낮음	확정	보통	부적절한 사용자 교육, 정책 집행 부족, 부적절한 구성 관리	보통	보통	높음	높음	높음	8
소프트웨어 제품에 취약점 유입	구조적 취약 (소프트웨어)	높음	예상	보통	부적절한 변경 관리 또는 구성 관리	높음	보통	높음	높음	높음	8
디스크 에러	구조적 취약 (IT 장비)	높음	예상	보통	환경 규제 부족	보통	낮음	높음	높음	높음	8
잘못된 권한 설정	의도하지 않은 (사용자, 관리자)	높음	예측	보통	정보 관련 / 특별 접근 프로그램	보통	높음	보통	보통	보통	5

로그온 한 디바이스에서 이탈한 거리	의도하지 않은 (사용자)	낮음	확정	보통	부적절한 사용자 교육	보통	높음	보통	보통	보통	5
보안되지 않은 Wi-Fi 네트워크 사용	구조적 취약 (소프트웨어)	매우 낮음	확정	높음	부적절한 변경 관리 또는 구성 관리	낮음	보통	보통	보통	보통	5
약한 접근 통제	의도하지 않은 (사용자, 관리자)	높음	예측	보통	부적절한 접근 통제 및 시행	높음	보통	보통	보통	보통	5

8.2 결함 트리 기반 평가 적용사례

부록 II 결함트리 기반 평가 적용사례에 첨부함

9 보안 기능 평가에서 수행된 시험 항목

<표 9-1> 보안기능평가에서 수행된 시험항목

시험항목	CSF 하위 카테고리	NIST 800-53 관련	평가 목표	평가 단계	적합성의 증거
1	PR.AC-1 인증 된 디바이스 및 사용자에 대해 ID 및 자격 증명 관리	AC-2	아키텍처는 각 역할에 할당 된 접근 권한을 여러 사용자 역할에 대해 설명	OpenEMR에 관리자로 로그인하여 사용자가 작업 기능을 수행하는 데 필요한 최소 권한의 접근을 허용하는 지정된 계정 유형을 확인	여러 권한과 역할 수준을 허용할 수 있음
2	PR.AC-1 인증 된 디바이스 및 사용자에 대해 ID 및 자격 증명 관리	AC-2	현재 허가 된 사용자만 EHR 데이터에 접근 가능	시스템이 접근통제를 적용하는지 테스트한다. OpenEMR에서 역할을 확인한 후 두 명의 사용자와 두 개의 디바이스에 대한 자격 증명을 입력한다. 세 번째 디바이스에는 사용자가 없다. b) 사용자가 승인 된 디바이스에 접근할 수 있지만 세 번째 디바이스에는 접근 할 수 없음. c) 한 사용자의 자격 증명을 삭제. d) 사용자가 더 이상 로그인 할 수 없음	인증 된 자격 증명을 사용하지 않으면 EHR 정보에 접근권한이 있는 사용자가 접근을 추가 / 수정 / 제거 할 수 있음
3	PRAR-1 원격 접근 관리	IA-3	알 수없는 디바이스를 연결 할 때 / 알 수없는 디바이스가 EHR 시스템에 연결할 경우 문제발생	테스트 : a) 유효한 인증서가 없는 디바이스를 사용하여 OpenEMR에 접근을 시도함	EHR 시스템은 디바이스를 알 수없는 것으로 인식하고 연결을 설정하기 전에 접근을 완전히 거부하거나 추가 인증을 할수 있음
4	PRAR-1 원격 접근 관리	AC-17	EHR 시스템에 대한 연결은 특정 보안 프로토콜을 통해서만 허용됨	테스트 : a) 모바일 디바이스를 사용하여 EHR 응용 프로그램에 연결을 시도함. 1) FTP 포트 21; 2) HTTP 포트 80;	EHR 시스템은 연결이 안전하지 않은 연결을 통한 접근을 허용하지 않도록함. 보안되고 적절한 연결 프로토콜 만 사용할 수 있음

5	PR.AC-4 최소 권한 및 업무 분리 원칙을 포함하여 접근 권한이 관리됨	AC-17 AC-6	시스템 구성 요소는 인증된 정보 접근 만 허용하도록 구성함	구성 요소 설정 (네트워크 ACL, 방화벽 규칙, OS 권한, 응용 프로그램 설정)을 검사하여 인증된 사용자 및 서비스에만 접근을 제한하는 메커니즘이 있는지 확인함. 제한된 설정이 적용되었음을 확인함 서비스가 기능을 수행하고 기본 거부 접근법을 사용하는 데 필요한 최소 권한 설정을 가지고 있음을 확인함	설정은 명시적으로 허용 된 시스템 및 사용자에 대한 접근을 제한함
6	PR.AC-4 최소 권한 및 업무 분리 원칙을 포함하여 접근 권한이 관리됨	AC-6	시스템은 할당 된 역할보다 더 큰 접근 권한을 사용자에게 허용하지 않음	시스템이 접근 통제를 적용하는지 테스트하면 된다. a) 권한이 있는 사용자로 로그인하면 된다. 로그아웃. b) 특별한 권한이 없는 사용자로 로그인하여 권한 있는 접근을 시도함	권한이 없는 사용자는 추가 권한을 얻지 못함
7	PR.AC-4 최소 권한 및 업무 분리 원칙을 포함하여 접근 권한이 관리됨	IA-5	응용 프로그램 및 시스템 구성 요소에는 권한이 부여 된 기능을 감사 할 수 있는 메커니즘이 포함됨	응용 프로그램 내에서 설정을 검토하여 솔루션에서 사용되는 구성 요소가 권한 사용이 사용 된 시기를 나타내는 감사 기능을 제공하는지 확인함	감사 기능이 존재하며 프로덕션 환경에서 구현 될 때 사용할 수 있음
8	DE.CM-4 : 악성 코드 발견	SI-3	모바일 디바이스에는 악성 코드 (안티 바이러스 소프트웨어) 보호 기능이 설치되어 있음	1) 모바일 디바이스를 검사하여 악의적인 코드 보호가 설치되어 있는지 확인한다. 2) 서명 파일을 검사하여 코드 보호 소프트웨어가 최신인지 확인함	악성 코드 / 바이러스 백신 소프트웨어가 설치됨
9	DE.CM-4 : 악성 코드 발견	SI-35	EHR 응용 프로그램은 악의적인 코드가 업로드되는 것을 허용하지	1) OS를 검사하여 악의적 인 코드 보호가 설치되어 있는지 확인하면 된다. 2) 테스트 : EICAR (European Antivirus Research Institute) 표준 안티 바이러스 테스트 파일을 응용 프로그램 내에 업로드하려고 시도함. 바이러스	응용 프로그램은 악의적 인 파일을 업로드하려는 모든 시도를 탐지하거나

			않음	스캐너가 유해한 바이러스를 발견한 것처럼 반응하는지 확인함. 3) 압축 된 EICAR 테스트 파일을 업로드하려고 시도함. 4) 보관 된 EICAR 테스트 파일을 업로드하려고 시도함	격리함
10	DE.CM-5 승인되지 않은 모바일 코드가 감지	SC-18	테스트에 적합한 내용만 응용 프로그램 내에 업로드 할 수 있는지 확인함	테스트 : 1) OpenEMR 응용 프로그램에 로그인함. 2) 사용자 입력이 필요한 응용 프로그램 내 필드를 식별함. 3) 스크립트 코드가 포함 된 HTML 및 JavaScript가 포함 된 여러 파일 형식을 업로드하려고 시도함	애플리케이션은 작업에 명시적으로 필요한 파일 형식 (예 : TIFF, JPEG 및 PDF)으로 파일 형식 업로드를 제한하는 기능을 사용함
11	PR.DS-1 : 휴면 상태의 데이터가 보호 됨	SC-28	EHR 내 데이터는 인증된 사용자 및 서비스만 접근 할 수 있음	검사 : 1) 설치된 암호화 도구 또는 소프트웨어가 작동하는지 확인하기 위해 구성 설정이나 사용 가능한 로그 또는 레코드를 검토하여 암호화 도구가 사용되는지 확인한다. EHR 데이터가 어떻게 구현되는지 문서화함. 2) 사용 중인 암호화 유형과 EHR 제품에 내장 된 암호화 유형 또는 별도의 메커니즘을 표시함. 3) 데이터를 보호하기 위해 사용되는 비 암호화 메커니즘 (파일 공유 검색 및 무결성 보호)을 식별함	데이터는 저장 및 처리 중에 보호됨
12	PR.AC-3 원격 접근 관리	AC-17 (1)	EHR에 대한 원격 접근은 접근 유형별로 모니터링 및 통제함으로써 비인가 접속을 차단함	테스트 : 1) 인터넷을 통해 사용자 A (위)에 로그인 인 로그아웃함 2) 사용자 A가 전화 접속을 통해 로그인하도록 하면 됨 권한없을시 실패함 3) 사용자 B가 인터넷을 통해 로그인하며 권한없을시 실패함 4) 사용자 B가 인증 된 출처에서 전화 접속을 통해 로그인 및 로그아웃하도록 함 5) 사용자 B가 권한이 없는 소스 위치에서 전화 접속을 통해 로그인하면 실패함 6) 위의 사용자 A와 C가 인터넷을 통해 로그인시 권한이 없으면 실패함, 권한이 있는 사용자 C만 성공함 7) 권한이 부여 된 출처에서 전화 접속을 통해 B 및 C 사용자가 로그인함. 두 사용자 모두 권한	시도한 로그인과 권한이 부여 된 함수의 사용은 앞에서 설명한대로 성공하거나 실패한다. 이것은 원격 접근 유형을 기반으로 접근을 제한하기위한 메커니즘이 EHR 서버에 의해 올바르게 시행됨

				있는 기능을 수행하려고 시도하며 사용자 D 만 성공함 8) 인증되지 않은 사용자 X가 인증된 위치 (위의 사용자 B가 전화 접속 권한이 있는 위치)에서 전화 접속을 통해 원격으로 EHR 서버에 접근하려고 시도시 실패함	
13	PR.AC-3 원격 접근 관리	AC-17	인증 된 MAC 주소를 가진 디바이스 만 네트워크 접근 권한이 부여됨	1) 인증 된 모바일 디바이스를 사용하여 인증 된 사용자는 EHR에 로그인함. 2) 그렇지 않은 경우 인증된 모바일 디바이스를 가지고 접근권한이 없는 MAC주소를 이용하여 로그인을 시도함. 3) 로그인 시도가 실패하는지 확인함.	MAC 주소 확인이 수행됨
14	PR.AC-5 네트워크 무결성을 보호하고 적절한 경우 네트워크 분리함	AC-4	정보 흐름 통제 정책은 지정된 모바일 디바이스와 EHR 서버 간의 정보 흐름을 통제함	테스트 : 1) EHR 어플리케이션을 통해 하나의 모바일 디바이스에서 직접 다른 디바이스로 EHR 정보를 보냄 2) 서버 OS에서 IP 스푸핑을 시도함 Linux에서 평가할 명령 : ls / proc / sys / net / ipv4 / conf / * / rp_filter cat / proc / sys / net / ipv4 / conf / * / rp_filter grep rp_filter /etc/sysctl.conf	1) EHR 정보는 디바이스에서 디바이스로 직접 접근 할 수 없음 2) 시스템은 가상 서버 (masquerading server)에서 전송 된 패킷으로부터 보호됨
15	PR.DS-2 : 전송 중 데이터가 보호	SC-8 SC-13	EHR 정보의 기밀성과 무결성은 전송 중에 (SC-8) 암호 메커니즘을 사용하여 보호됨	데이터를 전송할 때 현재위치에서 암호화 메커니즘을 확인하기 위해 전송 설정을 검사함 테스트 : 1) Wireshark를 설정하여 모바일 디바이스와 EHR 서버 간의 링크를 도청하고 패킷 수집을 시작함 (허브는 무선 접근 지점과 유선 네트워크 사이에 배치 할 수 있으며 Wireshark는 허브에 연결된 컴퓨터에서 실행될 수 있음). 2) 모바일 디바이스에서 EHR 서버로 EHR 정보 전송 3) 패킷 캡처 끄기 4) 패킷 캡처를 검사하여 전송 된 EHR 정보와 함께 디지털 서명이 전송되었는지 확인함 5) EHR에 대한 전자 서명이 무엇인지 계산하고 전자 서명이 전송 된 값과 동일한 지 확인함 6) 암호화 알고리즘과 알고리즘에 의해 변경된 정보를 확인함 . 동일하게 암호화되었는지 확인함	FIPS 140-2 준수 메커니즘은 전송중인 데이터를 보호하는 데 사용됨

16	PR.PT-4 : 통신 및 통제 네트워크가 보호됨	SC-7	시스템의 모든 Wi-Fi 관련 제품은 IEEE 802.11i 및 IEEE 802.1X 표준을 준수함	Wi-Fi 인증 제품의 WiFi Alliance 온라인 목록을 참조하여 시스템에 사용되는 모든 모바일 디바이스 및 접근 지점이 1) WPA2 ™ (Wi-Fi Protected Access® 2) EAP (확장 가능 인증 프로토콜) 및 3) 보호 된 관리 프레임	사용중인 디바이스는 Wi-Fi 인증을 받음
17	PR.PT-4 : 통신 및 통제 네트워크가 보호됨	SC-7	유선 네트워크가 강화되었다. (EHR 서버는 침입차단, 바이러스 백신 소프트웨어 및 IDS로 보호되며 모든 패치는 최신 버전임)	유선 네트워크를 검사하여 방화벽, 바이러스 백신 소프트웨어 및 IDS가 있는지 확인함 모든 패치가 최신인지 확인함	유선 네트워크에 나열된 보안 구성 요소가 나열되어 있음
18	PR.PT-4 : 통신 및 통제 네트워크가 보호됨	SC-7	모바일 디바이스 (무선 클라이언트)는 일반적으로 강화되어 있음	모바일 디바이스에는 방화벽, 바이러스 백신 소프트웨어 및 IDS가 설치되어 있으며 패치가 최신 상태이며 802.11 ad hoc 모드가 비활성화되어 있으며 블루투스(Bluetooth)는 기본적으로 해제되어 있음	모바일 디바이스에 나열된 보안 구성 요소가 나열되어 있음
19	PR.PT-4 : 통신 및 통제 네트워크가 보호됨	SC-7	응용 프로그램은 보안 정책에 따라 강화된 디바이스의 연결 만 허용함	1. 모바일 디바이스를 사용하여 OpenEMR에 성공적으로 로그인/로그아웃하면 됨 2) 해당 휴대 디바이스에서 블루투스를 켜고 EHR에 로그인함. 3) 모바일 디바이스가 더 이상 EHR 서버에 로그인 할 수 없는지 확인함	호환되지 않는 모바일 디바이스는 OpenEMR 응용 프로그램에 접근 할 수 없음
20	PR.PT-4 : 통신 및 통제 네트워크가 보호됨	SC-7	로그인하는 동안 모바일 디바이스의 구성이 규격을 벗어남	1) 모바일 디바이스를 사용하여 OpenEMR에 성공적으로 로그인함 2) OpenEMR에 로그인 한 상태에서 해당 모바일 디바이스의 Bluetooth를 킴. 3) 휴대 디바이스가 다른 디바이스에 표시되지 않는지 확인함	EHR은 OpenEMR에 접근하는 모바일 디바이스에 연결할 수 없음

10 클라우드 기반 EHR 솔루션 선정을 위한 보안 체크 리스트

10.1 개요

제한된 자원과 자본을 갖춘 의료기관은 개별 기업 위험 평가를 기반으로 임상의와 관리자에게 헬스케어 IT를 제공하기 위해 클라우드 기반 서비스를 선택할 수 있다.
클라우드 컴퓨팅 리소스는 종종 여러 거주자가 공유하고 의료기관의 외부에서 호스팅되며 공용 인터넷을 통해 데이터가 전송되기 때문에 의료기관은 헬스케어 IT의 클라우드 사용에 따른 잠재적 위험에 대해 교육을 받아야한다.

제공되는 기능과 서비스 수준 및 법률, 규정 및 보안 관련 표준 및 요구 사항을 준수 할 수 있는 능력은 클라우드 컴퓨팅 공급 업체마다 크게 다를 수 있다. 보건 정보 기술 국가 코디네이터 (National Coordinator for Health Information Technology)의 사무국은 의료 기관이 의료 정보 및 개인 정보 보호에 대한 보안을 제공하고 기술 및 법규 준수를 지원하는 클라우드 공급 업체를 선택하는 데 도움이 되는 설문 조사를 제공한다.

설문 조사는 클라우드 제공자를 선택할 때 철저한 보안 중재자로 보아서는 안된다.
오히려 조직이 초기 단계에서 보안 문제를 해결할 수 있도록 지원하여 향후 잠재적 위협 및 취약점을 완화하고 최소화할 수 있다. 각 조직에서는 클라우드 기반 의료 IT 서비스로 전환하기 전에 철저한 위험 평가를 수행하고 조직의 재무, 업무 운영 및 법률 및 규정 요구 사항을 기반으로 전략적 결정을 내릴 것을 필수적으로 권장한다. 또한 조직의 환경이 크게 변경되면 정기적인 재평가를 권장한다.

10.2 보안 체크리스트

10.2.1 공급 업체 계약

(1) EHR 시스템 공급 업체가 포괄적인 비즈니스 서비스 계약에 기꺼이 서명하는가?
(2) EHR 시스템 공급 업체가 HIPAA 개인 정보 보호 및 보안 규칙을 준수하는지 확인하려고 하며 요청이 있을 경우 감사 받을 의향이 있는가?

10.2.2 타사 응용 프로그램 통합

(1) 보건 의료기관은 클라우드 기반 EHR 시스템을 실습 관리 소프트웨어, 청구 시스템 및 전자 메일 시스템과 같은 다른 사내 제품과 통합해야 하는가?
(2) 클라우드 기반 EHR 시스템을 사내 애플리케이션에 통합해야하는 경우, 구현 절차 및 기술은 무엇이 사용되는가? 서로 다른 시스템 간에 통신되는 데이터를 보호하는 보안 기능은 무엇인가?

10.2.3 개인 또는 디바이스 인증 및 권한 부여

(1) EHR 시스템 공급 업체가 시스템에 접근 할 수 있는 모바일 디바이스 유형을 제한하는가?
(2) 모바일 디바이스는 디바이스 보안 준수를 위해 모바일 디바이스 관리 통제를 받는가?
(3) 클라이언트 자체 디바이스를 사용하여 클라우드 기반 EHR 시스템에 접근하기위한 보안 컴플라이언스 정책이 있는가?
(4) 디바이스를 분실, 도난당했거나 해킹당한 것으로 밝혀지면 보호 된 데이터가 손상되지 않도록 조치가 취해져 있는가?
(5) 클라우드 기반 EHR 시스템은 환자의 건강 정보에 접근하기 전에 사용자를 인증해야하는가?
  1) 시스템에 접근하는 데 사용되는 인증 메커니즘은 무엇인가?
  2) 사용자 ID는 고유하게 식별 할 수 있는가?
  3) 다중 요소 인증이 사용된다면 어떤것인가?
  4) 암호를 사용하는 경우 공급 업체는 강력한 암호를 적용하고 암호의 유효기간을 지정하는가?
  5) 시스템은 인증 된 사용자에게 시스템 접근시 데이터 접근을 제한하기 위해 역할 기반 통제 접근법을 사용하는가?
  6) 최소 권한 정책이 사용되는가? 시스템의 사용자에게는 시스템 내에서 승인 된 작업을 수행 할 수 있는 충분한 권한이 있으며 그 외 정책에 따른 다른 권한은 기본적으로 거부되는가?

10.2.4 데이터 보호

(1) 클라우드에 저장된 데이터를 보호하는데 어떤 방법을 사용되는가?
(2) 손실, 도난 및 해킹으로부터 데이터를 보호하기 위해 사용되는 방법은 무엇인가?
(3) 시스템은 보호되어야 할 데이터의 정확한 사본을 백업하는가? 이 백업 파일은 다른 위치에 보관되며 적절히 보호되고 쉽게 복원되는가?
(4) 시스템이 정지 된 상태에서 보호 된 데이터를 암호화하는가?
(5) EHR 시스템 공급 업체가 사업을 중단하면 어떻게 되는가? 모든 임상 데이터 및 정보를 검색 할 수 있는가?
(6) EHR 시스템 공급 업체는 민감한 정보를 포함하거나 사용한 IT 장비 및 저장 디바이스를 폐기하기 위한 보안 절차와 정책을 갖고 있는가?

10.2.5 전송중인 데이터의 보안

(1) 네트워크는 전송중인 데이터를 어떻게 보호하는가?

(2) 한 지점에서 다른 지점으로 전송되는 건강 정보를 암호화하는 데 사용할 수 있는 기능은 무엇인가?
(3) 전자적으로 환자의 건강 정보를 가로 채거나 수정할 수 있는 위험을 줄이기 위해 합리적이고 적절한 방법은 무엇인가?

10.2.6 모니터링 및 감사

(1) 보안 이벤트를 위해 시스템과 네트워크를 지속적으로 모니터링 하는가?
(2) EHR 공급 업체가 모든 승인된 접근 세션과 승인되지 않은 접근 세션을 기록하는 감사 기능을 제공하는가?
(3) 시스템에는 환자 건강 정보를 생성, 저장, 수정 및 전송하는 정보 시스템 활동을 모니터링, 기록 및 검토 할 수 있는 감사 통제 메커니즘이 있는가?
(4) 시스템이 감사 / 접근 레코드의 사본을 보유하고 있는가?
(5) EHR 시스템 공급 업체는 어떻게 운영되는가?

10.2.7 비상 사태

(1) EHR 시스템 공급 업체는 재해 발생시 정보 시스템에 대한 비상 접근을 활성화 할 수 있는 기능을 제공하는가?
(2) EHR 시스템 공급 업체는 필요한 경우 비상 접근 설정을 하고 활성화하는 책임이 있는 개인의 역할을 식별하는 정책과 절차를 갖고 있는가?
(3) EHR 시스템은 응급시 복구를 제공하고 정상 작동을 재개하며 재난 발생 시 환자의 건강 정보에 접근하도록 설계되어 있는가?

10.2.8 고객 및 기술 지원

(1) 고객 지원 / IT 지원 계약 및 관련 서비스 수준 계약에는 무엇이 포함되어 있는가?
(2) EHR 시스템 공급 업체는 보안 및 개인 정보 보호 정책 및 절차 (재해 복구 포함)의 서면 사본을 제공 할 수 있는가?
(3) 새로운 기능은 얼마나 자주 출시되는가? 배포 방법은 무엇인가?

부 록 Ⅰ-1

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

지식재산권 확약서 정보

해당사항 없음

Ⅰ-1.1 지식재산권 확약서(1) (스타일 적용-대항목/소항목)

- 발명의 명칭
- 권리자의 성명
- 등록(출원) 번호
- 등록(출원) 연월일
- 실시조건
- 확약서 접수일

Ⅰ-1.2 지식재산권 확약서(2) (스타일 적용-대항목/소항목)

- 발명의 명칭
- 권리자의 성명
- 등록(출원) 번호
- 등록(출원) 연월일
- 실시조건
- 확약서 접수일

※ 상기 기재된 지식재산권 확약서 이외에도 본 기술보고서가 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2 *(스타일 적용-본문상단제목)*

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

시험인증 관련 사항 *(굴림, 15포인트, 굵게, 가운데정렬)*

해당사항 없음

부 록 Ⅰ-3

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

본 기술보고서의 연계(family) 표준

본 기술보고서	국가표준기술연구소(NIST) 특별판(SP) 1800 시리즈
PART Ⅰ	NIST 특별판 1800-1a PART Ⅰ 요약 (NIST SP 1800-1a: Executive Summary)
PART Ⅱ	NIST 특별판 1800-1b PART Ⅱ 개인정보 보호 체계 (NIST SP 1800-1b: Approach, Architecture, and Security Characteristics – what we built and why)
PART Ⅲ	NIST 특별판 1800-1c PART Ⅲ 보안실무자들을 위한 지침 (NIST SP 1800-1c: How To Guides – instructions to build the reference design)
PART Ⅳ	NIST 특별판 1800-1d PART Ⅳ 보안 표준과 보안 기능 (NIST SP 1800-1d: Standards and Controls Mapping – listing of standards, best practices, and technologies used in the creation of this practice guide)
PART Ⅴ	NIST 특별판 1800-1e PART Ⅴ 위험 평가 및 결과 (NIST SP 1800-1e: Risk Assessment and Outcomes – risk assessment methodology, results, test, and evaluation)

부 록 Ⅰ-4

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

참고 문헌

[1] NIST SP 800-30의 부록 D-1

[2] NIST SP 800-53 revision 4

부 록 Ⅰ-5 *(스타일 적용-본문상단제목)*

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문기술보고서 해설서 *(굴림, 15포인트, 굵게, 가운데정렬)*

해당사항 없음

부 록 Ⅰ-6

기술보고서의 이력

판수	채택일	기술보고서번호	내용	담당 위원회
제1판	2018.09.	제정 TTAx.xx-xx.xxxx	모바일 디바이스에서 전자건강기록의 보안 Part Ⅴ : 위험 평가 및 결과	PG505

부 록 Ⅱ-1
결함트리 기반 평가 적용 사례

본문 8.2 결함 트리 기반 평가 적용사례

편도함수	확률	최대 충격값	사건
0.0715	0.9	0.0644	User_walks_away_from_logged_on_Mobile_Device1
0.0715	0.9	0.0644	User_walks_away_from_logged_on_Mobile_Device54
0.00732	0.1	0.000732	Install_File_Copying_Malware
0.00732	0.1	0.000732	Install_File_Copying_Malware551
0.000385	0.9	0.000347	User_walks_away_from_logged_on_Mobile_Device443
0.000385	0.9	0.000347	User_walks_away_from_logged_on_Mobile_Device554
0.000604	0.5	0.000302	Mobile_Device_User_Does_Not_Notice
0.00302	0.1	0.000302	Connect_as_OpenEMR2
0.000335	0.9	0.000302	Ask_Receives_Critical_Data_from_the_User1
0.000335	0.9	0.000302	Disconnect_OpenEMR
0.000169	0.9	0.000152	User_walks_away_from_logged_on_Mobile_Device442
0.000169	0.9	0.000152	User_walks_away_from_logged_on_Mobile_Device555
7.22E-05	0.9	6.50E-05	Steal_Media2
0.0065	0.01	6.50E-05	Decrypt_Critical_Data11
7.22E-05	0.9	6.50E-05	Steal_Media40
0.0065	0.01	6.50E-05	Decrypt_Critical_Data440
0.0065	0.01	6.50E-05	Decrypt_Critical_Data554
7.22E-05	0.9	6.50E-05	Steal_Media54
6.51E-05	0.9	5.86E-05	PluginHub
0.00586	0.01	5.86E-05	Decrypt_Critical_Data443
6.51E-05	0.9	5.86E-05	PluginHub54
0.00586	0.01	5.86E-05	Decrypt_Critical_Data534
6.33E-05	0.9	5.70E-05	Laptop_Wireshark2
6.33E-05	0.9	5.70E-05	Laptop_Wireshark54
0.00396	0.01	3.96E-05	Decrypt_Backup_Data_at_Rest25
0.00396	0.01	3.96E-05	Decrypt_Backup_Data_at_Rest544
7.71E-05	0.5	3.85E-05	Obtain_OS_Athenication443

7.71E-05	0.5	3.85E-05	Obtain_OS_Athenication555
0.00359	0.01	3.59E-05	Decrypt_the_Back_up4
0.00359	0.01	3.59E-05	Decrypt_the_Back_up54
7.19E-05	0.5	3.59E-05	During_Phyiscal_Transfer_Obtain_Copy54
7.19E-05	0.5	3.59E-05	During_Phyiscal_Transfer_Obtain_Copy1
6.47E-05	0.5	3.24E-05	Obtain_a_copy_of_the_backup
6.47E-05	0.5	3.24E-05	Obtain_a_copy_of_the_backup54
3.37E-05	0.5	1.69E-05	WiFi_Egress442
3.37E-05	0.5	1.69E-05	WiFi_Egress54
3.37E-05	0.5	1.69E-05	Obtain_OS_Athenication442
3.37E-05	0.5	1.69E-05	Obtain_OS_Athenication55
3.23E-05	0.5	1.61E-05	Send_Data_to_New_GW
3.23E-05	0.5	1.61E-05	Acquire_Password2
0.00161	0.01	1.61E-05	Decrypt_Critical_Data16
3.23E-05	0.5	1.61E-05	Acquire_Password54
1.79E-05	0.9	1.61E-05	Capture_Critical_Data2
3.23E-05	0.5	1.61E-05	Send_Data_to_New_GW54
0.00161	0.01	1.61E-05	Decrypt_Critical_Data1554
1.79E-05	0.9	1.61E-05	Capture_Critical_Data554
0.000135	0.1	1.35E-05	Critical_Data_is_Resident_on_the_Mobile_Device
0.000135	0.1	1.35E-05	Critical_Data_is_Resident_on_the_Mobile_Device54
0.00114	0.01	1.14E-05	Decrypt_Critical_Data338
0.00114	0.01	1.14E-05	Decrypt_Critical_Data339
0.00114	0.01	1.14E-05	Decrypt_Critical_Data7
0.00114	0.01	1.14E-05	Decrypt_Critical_Data5
0.00114	0.01	1.14E-05	Decrypt_Critical_Data552
0.00114	0.01	1.14E-05	Decrypt_Critical_Data53
0.00088	0.01	8.80E-06	Decrypt_Critical_Data35
0.00088	0.01	8.80E-06	Decrypt_Critical_Data40
0.00088	0.01	8.80E-06	Decrypt_Critical_Data54
1.02E-05	0.75	7.67E-06	Thumb_Drive40
1.02E-05	0.75	7.67E-06	Thumb_Drive
1.02E-05	0.75	7.67E-06	Thumb_Drive54
0.000716	0.01	7.16E-06	Blue_Tooth_Access
7.16E-05	0.1	7.16E-06	Critical_Data_residue_on_Mobile_device2
7.16E-05	0.1	7.16E-06	Gain_Access_to_the_Backup_System1
0.000716	0.01	7.16E-06	Decrypt_Backup_Data_at_Rest21

0.000716	0.01	7.16E-06	Blue_Tooth_Access454
7.16E-05	0.1	7.16E-06	Backup_data_Captured1
7.16E-05	0.1	7.16E-06	Critical_Data_residue_on_Mobile_device454
7.16E-05	0.1	7.16E-06	Gain_Access_to_the_Backup_System54
0.000716	0.01	7.16E-06	Decrypt_Data20
7.16E-05	0.1	7.16E-06	Backup_data_Captured54
0.000716	0.01	7.16E-06	Decrypt_Data54
0.000716	0.01	7.16E-06	Decrypt_Backup_Data_at_Rest54
0.000674	0.01	6.74E-06	Remote_Access_to_the_MDM1
0.000674	0.01	6.74E-06	Phyisical_Access_to_the_MDM1
0.000674	0.01	6.74E-06	Remote_Access_to_the_MDM54
0.000674	0.01	6.74E-06	Phyisical_Access_to_the_MDM54
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR339
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR38
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR53
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR52
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR5
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR9
7.16E-06	0.9	6.44E-06	WiFi_Data_Capture2
6.44E-05	0.1	6.44E-06	Decrypt_WiFi_Data_Transfer3
0.000644	0.01	6.44E-06	Decrypt_Critical_Data14
0.000644	0.01	6.44E-06	Decrypt_Critical_Data544
6.44E-05	0.1	6.44E-06	Decrypt_WiFi_Data_Transfer54
7.16E-06	0.9	6.44E-06	WiFi_Data_Capture54
7.13E-06	0.9	6.42E-06	Image_Disk_with_Forensic_Tool1
7.13E-06	0.9	6.42E-06	Image_Disk_with_Forensic_Tool54
0.000625	0.01	6.25E-06	Decrypt_Critical_Data31
0.000625	0.01	6.25E-06	Decrypt_Critical_Data51
0.000625	0.01	6.25E-06	Decrypt_Critical_Data37
5.19E-05	0.1	5.19E-06	Access_to_Health_IT_OpenEMR40
5.19E-05	0.1	5.19E-06	Access_to_Health_IT_OpenEMR45
5.19E-05	0.1	5.19E-06	Access_to_Health_IT_OpenEMR54
1.02E-05	0.5	5.11E-06	Buying_Malware
1.02E-05	0.5	5.11E-06	Buying_Malware37
1.02E-05	0.5	5.11E-06	Buying_Malware51
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR7
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR11

4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR39
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR338
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR552
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR553
3.68E-05	0.1	3.68E-06	Access_to_Health_IT_OpenEMR2
3.68E-05	0.1	3.68E-06	Access_to_Health_IT_OpenEMR337
3.68E-05	0.1	3.68E-06	Access_to_Health_IT_OpenEMR51
3.60E-05	0.1	3.60E-06	Access_the_Backup_system_on_site1
3.60E-05	0.1	3.60E-06	Access_the_Backup_system_on_site54
3.25E-05	0.1	3.25E-06	Access_to_Health_IT_OpenEMR35
3.25E-05	0.1	3.25E-06	Access_to_Health_IT_OpenEMR440
3.25E-05	0.1	3.25E-06	Access_to_Health_IT_OpenEMR554
5.80E-06	0.5	2.90E-06	Mobile_Device_User_Does_Not_Notice38
0.00029	0.01	2.90E-06	Decrypt_Critical_Data52
0.00029	0.01	2.90E-06	Decrypt_Critical_Data38
2.90E-05	0.1	2.90E-06	Connect_as_OpenEMR38
5.80E-06	0.5	2.90E-06	Mobile_Device_User_Does_Not_Notice52
3.22E-06	0.9	2.90E-06	Ask_Receives_Critical_Data_from_the_User38
3.22E-06	0.9	2.90E-06	Disconnect_OpenEMR38
3.22E-06	0.9	2.90E-06	Disconnect_OpenEMR52
2.90E-05	0.1	2.90E-06	Connect_as_OpenEMR52
3.22E-06	0.9	2.90E-06	Ask_Receives_Critical_Data_from_the_User52
3.58E-06	0.75	2.68E-06	Malicious_Access_Point1
2.68E-05	0.1	2.68E-06	Critical_data_is_resident_on_Mobile_device1
0.000268	0.01	2.68E-06	Access_from_AP_to_Mobile_Device1
5.37E-06	0.5	2.68E-06	Mobile_Device_Attaches_to_Malicious_Access_Point1
0.000268	0.01	2.68E-06	Access_from_AP_to_Mobile_Device54
3.58E-06	0.75	2.68E-06	Malicious_Access_Point54
2.68E-05	0.1	2.68E-06	Critical_data_is_resident_on_Mobile_device54
5.37E-06	0.5	2.68E-06	Mobile_Device_Attaches_to_Malicious_Access_Point54
2.31E-05	0.1	2.31E-06	Access_to_Health_IT_OpenEMR4
2.31E-05	0.1	2.31E-06	Access_to_Health_IT_OpenEMR37
2.31E-05	0.1	2.31E-06	Access_to_Health_IT_OpenEMR551
1.87E-05	0.1	1.87E-06	Blue_Tooth_Egress442
1.87E-05	0.1	1.87E-06	Blue_Tooth_Egress54

0.000148	0.01	1.48E-06	Access_from_AP_to_Mobile_Device443
1.97E-06	0.75	1.48E-06	Malicious_Access_Point443
2.95E-06	0.5	1.48E-06	Mobile_Device_Attaches_to_Malicious_Access_Point443
1.48E-05	0.1	1.48E-06	Install_File_Copying_Malware443
2.41E-06	0.5	1.21E-06	WiFi_Egress443
1.13E-05	0.1	1.13E-06	Access_thru_HIT_Server_Room_Firewall
0.000113	0.01	1.13E-06	Decrypt_Critical_Data
1.13E-05	0.1	1.13E-06	Access_thru_HIT_Server_Room_Firewall50
0.000113	0.01	1.13E-06	Decrypt_Critical_Data36
1.13E-05	0.1	1.13E-06	Access_thru_HIT_Server_Room_Firewall36
0.000113	0.01	1.13E-06	Decrypt_Critical_Data50
1.43E-06	0.5	7.13E-07	Obtain_OS_Athenication1
1.43E-06	0.5	7.13E-07	Obtain_OS_Athenication54
6.69E-06	0.1	6.69E-07	Access_to_Health_IT_OpenEMR
6.69E-06	0.1	6.69E-07	Access_to_Health_IT_OpenEMR36
6.69E-06	0.1	6.69E-07	Access_to_Health_IT_OpenEMR50
7.15E-07	0.9	6.44E-07	Capture_Critical_Data54
6.44E-05	0.01	6.44E-07	Breach_Firewall54
6.44E-05	0.01	6.44E-07	Decrypt_Critical_Data154
5.68E-06	0.1	5.68E-07	Coding_Malware
5.68E-06	0.1	5.68E-07	Coding_Malware37
5.68E-06	0.1	5.68E-07	Coding_Malware51
4.19E-06	0.1	4.19E-07	Access_to_Health_IT_OpenEMR30
4.19E-06	0.1	4.19E-07	Access_to_Health_IT_OpenEMR366
4.19E-06	0.1	4.19E-07	Access_to_Health_IT_OpenEMR550
7.15E-07	0.5	3.58E-07	Capture_Critical_Data3
3.58E-05	0.01	3.58E-07	Breach_Firewall
3.58E-05	0.01	3.58E-07	Decrypt_Critical_Data15
2.84E-06	0.1	2.84E-07	Egress_Data_Thru_Firewall40
2.84E-06	0.1	2.84E-07	Egress_Data_Thru_Firewall2
2.84E-06	0.1	2.84E-07	Egress_Data_Thru_Firewall54
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management34
2.50E-06	0.1	2.50E-07	VPN_Server32
2.50E-06	0.1	2.50E-07	Risk_Manager32
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners32
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root2

2.50E-06	0.1	2.50E-07	DNS_Server_Ext34
2.50E-06	0.1	2.50E-07	Health_IT_DNS34
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_34
2.50E-06	0.1	2.50E-07	Health_IT_DNS32
2.50E-06	0.1	2.50E-07	DNS_Server_Ext32
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root32
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_32
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management32
2.50E-06	0.1	2.50E-07	Virus_Malware32
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_32
2.50E-06	0.1	2.50E-07	Risk_Manager34
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners34
2.50E-06	0.1	2.50E-07	Virus_Malware34
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_34
2.50E-06	0.1	2.50E-07	VPN_Server34
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_38
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_38
2.50E-06	0.1	2.50E-07	Virus_Malware38
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management38
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners38
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root38
2.50E-06	0.1	2.50E-07	DNS_Server_Ext38
2.50E-06	0.1	2.50E-07	Health_IT_DNS38
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_39
2.50E-06	0.1	2.50E-07	VPN_Server38
2.50E-06	0.1	2.50E-07	VPN_Server39
2.50E-06	0.1	2.50E-07	Risk_Manager39
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners39
2.50E-06	0.1	2.50E-07	Virus_Malware39
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_39
2.50E-06	0.1	2.50E-07	Risk_Manager38
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management39
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root39
2.50E-06	0.1	2.50E-07	Health_IT_DNS39
2.50E-06	0.1	2.50E-07	DNS_Server_Ext39
2.50E-06	0.1	2.50E-07	VPN_Server53
2.50E-06	0.1	2.50E-07	Risk_Manager53

2.50E-06	0.1	2.50E-07	Vulnerability_Scanners53
2.50E-06	0.1	2.50E-07	Virus_Malware53
2.50E-06	0.1	2.50E-07	Health_IT_DNS53
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_53
2.50E-06	0.1	2.50E-07	VPN_Server52
2.50E-06	0.1	2.50E-07	DNS_Server_Ext53
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners52
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management53
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root53
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_53
2.50E-06	0.1	2.50E-07	Risk_Manager52
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root52
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_52
2.50E-06	0.1	2.50E-07	DNS_Server_Ext52
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management52
2.50E-06	0.1	2.50E-07	Virus_Malware52
2.50E-06	0.1	2.50E-07	Health_IT_DNS52
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_52
1.94E-06	0.1	1.94E-07	Health_IT_CA_Root40
1.94E-06	0.1	1.94E-07	Intrusion_Detection_System__IDS_40
1.94E-06	0.1	1.94E-07	DNS_Server_Ext40
1.94E-06	0.1	1.94E-07	Mobile_Network_Access_Control__NAC_40
1.94E-06	0.1	1.94E-07	Vulnerability_Scanners40
1.94E-06	0.1	1.94E-07	Health_IT_Configuration_Management40
1.94E-06	0.1	1.94E-07	Health_IT_DNS40
1.94E-06	0.1	1.94E-07	VPN_Server40
1.94E-06	0.1	1.94E-07	Virus_Malware40
1.94E-06	0.1	1.94E-07	Risk_Manager40
1.94E-06	0.1	1.94E-07	Health_IT_Configuration_Management54
1.94E-06	0.1	1.94E-07	Health_IT_CA_Root54
1.94E-06	0.1	1.94E-07	Vulnerability_Scanners54
1.94E-06	0.1	1.94E-07	Intrusion_Detection_System__IDS_54
1.94E-06	0.1	1.94E-07	Health_IT_DNS54
1.94E-06	0.1	1.94E-07	DNS_Server_Ext54
1.94E-06	0.1	1.94E-07	Health_IT_CA_Root35
1.94E-06	0.1	1.94E-07	Mobile_Network_Access_Control__NAC_54
1.94E-06	0.1	1.94E-07	DNS_Server_Ext35

1.94E-06	0.1	1.94E-07	Health_IT_Configuration_Management35
1.94E-06	0.1	1.94E-07	Health_IT_DNS35
1.94E-06	0.1	1.94E-07	Intrusion_Detection_System__IDS_35
1.94E-06	0.1	1.94E-07	Risk_Manager54
1.94E-06	0.1	1.94E-07	Virus_Malware54
1.94E-06	0.1	1.94E-07	Vulnerability_Scanners35
1.94E-06	0.1	1.94E-07	Risk_Manager35
1.94E-06	0.1	1.94E-07	VPN_Server35
1.94E-06	0.1	1.94E-07	VPN_Server54
1.94E-06	0.1	1.94E-07	Mobile_Network_Access_Control__NAC_35
1.94E-06	0.1	1.94E-07	Virus_Malware35
3.25E-07	0.5	1.62E-07	Mobile_Device_User_Does_Not_Notice443
3.25E-07	0.5	1.62E-07	Ask_Receives_Critical_Data_from_the_User443
1.62E-06	0.1	1.62E-07	Connect_as_OpenEMR443
1.62E-06	0.1	1.62E-07	Connect_as_OpenEMR54
3.25E-07	0.5	1.62E-07	Ask_Receives_Critical_Data_from_the_User54
3.25E-07	0.5	1.62E-07	Mobile_Device_User_Does_Not_Notice54
1.37E-06	0.1	1.37E-07	Virus_Malware37
1.37E-06	0.1	1.37E-07	Health_IT_CA_Root37
1.37E-06	0.1	1.37E-07	Mobile_Network_Access_Control__NAC_37
1.37E-06	0.1	1.37E-07	Health_IT_Configuration_Management37
1.37E-06	0.1	1.37E-07	Vulnerability_Scanners37
1.37E-06	0.1	1.37E-07	Risk_Manager37
1.37E-06	0.1	1.37E-07	VPN_Server37
1.37E-06	0.1	1.37E-07	Health_IT_DNS37
1.37E-06	0.1	1.37E-07	Intrusion_Detection_System__IDS_37
1.37E-06	0.1	1.37E-07	Risk_Manager12
1.37E-06	0.1	1.37E-07	Health_IT_CA_Root3
1.37E-06	0.1	1.37E-07	DNS_Server_Ext11
1.37E-06	0.1	1.37E-07	DNS_Server_Ext37
1.37E-06	0.1	1.37E-07	Health_IT_DNS5
1.37E-06	0.1	1.37E-07	Intrusion_Detection_System__IDS_6
1.37E-06	0.1	1.37E-07	VPN_Server13
1.37E-06	0.1	1.37E-07	Virus_Malware9
1.37E-06	0.1	1.37E-07	Vulnerability_Scanners8
1.37E-06	0.1	1.37E-07	Health_IT_Configuration_Management4
1.37E-06	0.1	1.37E-07	Mobile_Network_Access_Control__NAC_7

1.37E-06	0.1	1.37E-07	Health_IT_Configuration_Management51
1.37E-06	0.1	1.37E-07	Health_IT_DNS51
1.37E-06	0.1	1.37E-07	Intrusion_Detection_System__IDS_51
1.37E-06	0.1	1.37E-07	DNS_Server_Ext51
1.37E-06	0.1	1.37E-07	Vulnerability_Scanners51
1.37E-06	0.1	1.37E-07	Risk_Manager51
1.37E-06	0.1	1.37E-07	VPN_Server51
1.37E-06	0.1	1.37E-07	Health_IT_CA_Root51
1.37E-06	0.1	1.37E-07	Mobile_Network_Access_Control__NAC_51
1.37E-06	0.1	1.37E-07	Virus_Malware51
1.34E-06	0.1	1.34E-07	Blue_Tooth_Egress443
2.49E-07	0.1	2.49E-08	Health_IT_Configuration_Management
2.49E-07	0.1	2.49E-08	Health_IT_CA_Root
2.49E-07	0.1	2.49E-08	VPN_Server
2.49E-07	0.1	2.49E-08	Vulnerability_Scanners
2.49E-07	0.1	2.49E-08	Virus_Malware
2.49E-07	0.1	2.49E-08	Risk_Manager
2.49E-07	0.1	2.49E-08	DNS_Server_Ext
2.49E-07	0.1	2.49E-08	Health_IT_DNS
2.49E-07	0.1	2.49E-08	Intrusion_Detection_System__IDS_
2.49E-07	0.1	2.49E-08	Mobile_Network_Access_Control__NAC_
2.49E-07	0.1	2.49E-08	Health_IT_DNS36
2.49E-07	0.1	2.49E-08	DNS_Server_Ext36
2.49E-07	0.1	2.49E-08	Health_IT_CA_Root36
2.49E-07	0.1	2.49E-08	Health_IT_Configuration_Management36
2.49E-07	0.1	2.49E-08	Intrusion_Detection_System__IDS_36
2.49E-07	0.1	2.49E-08	Vulnerability_Scanners36
2.49E-07	0.1	2.49E-08	Virus_Malware36
2.49E-07	0.1	2.49E-08	Risk_Manager36
2.49E-07	0.1	2.49E-08	VPN_Server36
2.49E-07	0.1	2.49E-08	Mobile_Network_Access_Control__NAC_36
2.49E-07	0.1	2.49E-08	Vulnerability_Scanners50
2.49E-07	0.1	2.49E-08	Virus_Malware50
2.49E-07	0.1	2.49E-08	DNS_Server_Ext50
2.49E-07	0.1	2.49E-08	Risk_Manager50
2.49E-07	0.1	2.49E-08	Health_IT_Configuration_Management50
2.49E-07	0.1	2.49E-08	Health_IT_DNS50

2.49E-07	0.1	2.49E-08	Intrusion_Detection_System__IDS_50
2.49E-07	0.1	2.49E-08	VPN_Server50
2.49E-07	0.1	2.49E-08	Mobile_Network_Access_Control__NAC_50
2.49E-07	0.1	2.49E-08	Health_IT_CA_Root50
1.97E-08	0.75	1.48E-08	Malicious_Access_Point554
2.95E-08	0.5	1.48E-08	Mobile_Device_Attaches_to_Malicious_Access_Point554
1.48E-06	0.01	1.48E-08	Access_from_AP_to_Mobile_Device554
1.48E-06	0.01	1.48E-08	Blue_Tooth_Access554
1.48E-07	0.1	1.48E-08	Install_File_Copying_Malware554
2.41E-08	0.5	1.21E-08	WiFi_Egress554
1.34E-08	0.1	1.34E-09	Blue_Tooth_Egress554
0.815	0.9	0.733	Physical_Access___User_walks_away_from_logged_on_Mobile_Device1
0.0855	0.1	0.00855	Install_File_Modifying_Malware
0.0855	0.1	0.00855	Install_File_Modifying_Malware123
0.0045	0.9	0.00405	User_walks_away_from_logged_on_Mobile_Device4433
0.0045	0.9	0.00405	User_walks_away_from_logged_on_Mobile_Device443
0.0009	0.5	0.00045	Obtain_OS_Athenication4433
0.0009	0.5	0.00045	Obtain_OS_Athenication443
0.0307	0.01	0.000307	Access_from_AP_to_Mobile_Device1
0.000613	0.5	0.000307	Mobile_Device_Attaches_to_Malicious_Access_Point1
0.000409	0.75	0.000307	Malicious_Access_Point1
0.0033	0.01	3.30E-05	Changing_Crtical_Data4122
0.0033	0.01	3.30E-05	Changing_Crtical_Data4
6.60E-05	0.5	3.30E-05	Mobile_Device_User_Does_Not_Notice
3.67E-05	0.9	3.30E-05	Ask_Receives_Critical_Data_from_the_User1
0.00033	0.1	3.30E-05	Connect_as_OpenEMR2
6.60E-05	0.5	3.30E-05	Mobile_Device_User_Does_Not_Notice1221
3.67E-05	0.9	3.30E-05	Ask_Receives_Critical_Data_from_the_User1211
3.67E-05	0.9	3.30E-05	Disconnect_OpenEMR1222
3.67E-05	0.9	3.30E-05	Disconnect_OpenEMR
0.00033	0.1	3.30E-05	Connect_as_OpenEMR2122
0.00306	0.01	3.06E-05	Access_from_AP_to_Mobile_Device554

0.00306	0.01	3.06E-05	Access_from_AP_to_Mobile_Device443
4.07E-05	0.75	3.06E-05	Malicious_Access_Point554
4.07E-05	0.75	3.06E-05	Malicious_Access_Point443
0.000306	0.1	3.06E-05	Install_File_Modifyying_Malware554
6.11E-05	0.5	3.06E-05	Mobile_Device_Attaches_to_Malicious_Access_Point554
6.11E-05	0.5	3.06E-05	Mobile_Device_Attaches_to_Malicious_Access_Point443
0.000306	0.1	3.06E-05	Install_File_Modifying_Malware443
0.000204	0.01	2.04E-06	Force_Backup_Online__Critical_System_Failure274
0.000204	0.01	2.04E-06	Decrypt_the_Back_up54
0.000204	0.01	2.04E-06	Force_Backup_Online__Critical_System_Failure27
4.07E-06	0.5	2.04E-06	Replace_with_Modified_Backup1
0.000204	0.01	2.04E-06	Decrypt_the_Back_up4
4.07E-06	0.5	2.04E-06	During_Phyiscal_Transfer_Obtain_Copy1
4.07E-06	0.5	2.04E-06	During_Phyiscal_Transfer_Obtain_Copy54
4.07E-06	0.5	2.04E-06	Replace_with_Modified_Backup14
6.60E-07	0.5	3.30E-07	Mobile_Device_User_Does_Not_Notice32
3.30E-05	0.01	3.30E-07	Changing_Crtical_Data3212
3.30E-05	0.01	3.30E-07	Decrypt_Critical_Data52
3.30E-06	0.1	3.30E-07	Connect_as_OpenEMR52
3.67E-07	0.9	3.30E-07	Disconnect_OpenEMR52
3.67E-07	0.9	3.30E-07	Ask_Receives_Critical_Data_from_the_User52
6.62E-06	0.01	6.62E-08	Re_Encrypt_Modified_Critical_Data2644
6.62E-06	0.01	6.62E-08	Decrypt_Critical_Data534
6.62E-06	0.01	6.62E-08	Changing_Crtical_Data2644
7.35E-08	0.9	6.62E-08	PluginHub
7.35E-08	0.9	6.62E-08	PluginHub54
6.62E-06	0.01	6.62E-08	Decrypt_Critical_Data443
6.62E-06	0.01	6.62E-08	Changing_Crtical_Data264
6.62E-06	0.01	6.62E-08	Re_Encrypt_Modified_Critical_Data264
7.15E-08	0.9	6.43E-08	Laptop_Wireshark54
7.15E-08	0.9	6.43E-08	Laptop_Wireshark2
2.04E-08	0.9	1.83E-08	Capture_Critical_Data554
3.67E-08	0.5	1.83E-08	Acquire_Password54
3.67E-08	0.5	1.83E-08	Send_Data_to_New_GW54

1.83E-06	0.01	1.83E-08	Re_Encrypt_Modified_Critical_Data2654
2.04E-08	0.9	1.83E-08	Capture_Critical_Data2
1.83E-06	0.01	1.83E-08	Changing_Crtical_Data2654
1.83E-06	0.01	1.83E-08	Decrypt_Critical_Data1554
3.67E-08	0.5	1.83E-08	Acquire_Password2
3.67E-08	0.5	1.83E-08	Send_Data_to_New_GW
1.83E-06	0.01	1.83E-08	Changing_Crtical_Data265
1.83E-06	0.01	1.83E-08	Decrypt_Critical_Data16
1.83E-06	0.01	1.83E-08	Re_Encrypt_Modified_Critical_Data265
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data6
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data35
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data6
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data53
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data552
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data233
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data323
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data323
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data233
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data333
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data7
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data3
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data31
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data333
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data5
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data338
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data23
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data339
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data32
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data23
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data32
1.00E-06	0.01	1.00E-08	Re_Encrypt_Modified_Critical_Data2633
1.00E-06	0.01	1.00E-08	Changing_Crtical_Data26
1.00E-06	0.01	1.00E-08	Re_Encrypt_Modified_Critical_Data26
1.00E-06	0.01	1.00E-08	Decrypt_Critical_Data54
1.00E-06	0.01	1.00E-08	Changing_Crtical_Data2633
1.00E-06	0.01	1.00E-08	Decrypt_Critical_Data40
1.16E-08	0.75	8.72E-09	Thumb_Drive40

1.16E-08	0.75	8.72E-09	Thumb_Drive54
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR339
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR53
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR52
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR45
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR38
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR9
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR5
7.33E-07	0.01	7.33E-09	Re_Encrypt_Modified_Critical_Data2623
7.33E-07	0.01	7.33E-09	Changing_Crtical_Data2623
7.33E-07	0.01	7.33E-09	Decrypt_Critical_Data544
7.33E-08	0.1	7.33E-09	Decrypt_WiFi_Data_Transfer3
8.15E-09	0.9	7.33E-09	WiFi_Data_Capture54
7.33E-08	0.1	7.33E-09	Decrypt_WiFi_Data_Transfer54
8.15E-09	0.9	7.33E-09	WiFi_Data_Capture2
7.33E-07	0.01	7.33E-09	Decrypt_Critical_Data14
7.33E-07	0.01	7.33E-09	Re_Encrypt_Modified_Critical_Data262
7.33E-07	0.01	7.33E-09	Changing_Crtical_Data262
7.11E-07	0.01	7.11E-09	Decrypt_Critical_Data31
7.11E-07	0.01	7.11E-09	Decrypt_Critical_Data51
7.11E-07	0.01	7.11E-09	Re_Encrypt_Modified_Critical_Data223
7.11E-07	0.01	7.11E-09	Re_Encrypt_Modified_Critical_Data2
7.11E-07	0.01	7.11E-09	Changing_Crtical_Data223
7.11E-07	0.01	7.11E-09	Changing_Crtical_Data2
7.11E-07	0.01	7.11E-09	Decrypt_Critical_Data37
7.11E-07	0.01	7.11E-09	Re_Encrypt_Modified_Critical_Data22
7.11E-07	0.01	7.11E-09	Changing_Crtical_Data22
5.90E-08	0.1	5.90E-09	Access_to_Health_IT_OpenEMR40
5.90E-08	0.1	5.90E-09	Access_to_Health_IT_OpenEMR54
1.16E-08	0.5	5.81E-09	Buying_Malware
1.16E-08	0.5	5.81E-09	Buying_Malware51
1.16E-08	0.5	5.81E-09	Buying_Malware37
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR35
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR7
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR11
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR338
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR39

4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR552
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR553
4.19E-08	0.1	4.19E-09	Access_to_Health_IT_OpenEMR337
4.19E-08	0.1	4.19E-09	Access_to_Health_IT_OpenEMR2
4.19E-08	0.1	4.19E-09	Access_to_Health_IT_OpenEMR51
3.70E-08	0.1	3.70E-09	Access_to_Health_IT_OpenEMR554
3.70E-08	0.1	3.70E-09	Access_to_Health_IT_OpenEMR440
2.63E-08	0.1	2.63E-09	Access_to_Health_IT_OpenEMR37
2.63E-08	0.1	2.63E-09	Access_to_Health_IT_OpenEMR551
2.63E-08	0.1	2.63E-09	Access_to_Health_IT_OpenEMR4
1.29E-08	0.1	1.29E-09	Access_thru_HIT_Server_Room_Firewall
1.29E-08	0.1	1.29E-09	Access_thru_HIT_Server_Room_Firewall36
1.29E-08	0.1	1.29E-09	Access_thru_HIT_Server_Room_Firewall50
1.29E-07	0.01	1.29E-09	Decrypt_Critical_Data50
1.29E-07	0.01	1.29E-09	Re_Encrypt_Modified_Critical_Data3
1.29E-07	0.01	1.29E-09	Changing_Crtical_Data1
1.29E-07	0.01	1.29E-09	Changing_Crtical_Data2211
1.29E-07	0.01	1.29E-09	Re_Encrypt_Modified_Critical_Data2211
1.29E-07	0.01	1.29E-09	Decrypt_Critical_Data36
1.29E-07	0.01	1.29E-09	Changing_Crtical_Data221
1.29E-07	0.01	1.29E-09	Re_Encrypt_Modified_Critical_Data221
1.29E-07	0.01	1.29E-09	Decrypt_Critical_Data
7.62E-09	0.1	7.62E-10	Access_to_Health_IT_OpenEMR
7.62E-09	0.1	7.62E-10	Access_to_Health_IT_OpenEMR50
7.62E-09	0.1	7.62E-10	Access_to_Health_IT_OpenEMR36
8.15E-10	0.9	7.33E-10	Capture_Critical_Data54
7.33E-08	0.01	7.33E-10	Changing_Crtical_Data2634
7.33E-08	0.01	7.33E-10	Re_Encrypt_Modified_Critical_Data2634
7.33E-08	0.01	7.33E-10	Breach_Firewall54
7.33E-08	0.01	7.33E-10	Decrypt_Critical_Data154
6.46E-09	0.1	6.46E-10	Coding_Malware
6.46E-09	0.1	6.46E-10	Coding_Malware51
6.46E-09	0.1	6.46E-10	Coding_Malware37
4.78E-09	0.1	4.78E-10	Access_to_Health_IT_OpenEMR30
4.78E-09	0.1	4.78E-10	Access_to_Health_IT_OpenEMR550
4.78E-09	0.1	4.78E-10	Access_to_Health_IT_OpenEMR366
4.07E-08	0.01	4.07E-10	Changing_Crtical_Data263
4.07E-08	0.01	4.07E-10	Re_Encrypt_Modified_Critical_Data263

4.07E-08	0.01	4.07E-10	Breach_Firewall
4.07E-08	0.01	4.07E-10	Decrypt_Critical_Data15
8.15E-10	0.5	4.07E-10	Capture_Critical_Data3
3.23E-09	0.1	3.23E-10	Egress_Data_Thru_Firewall54
3.23E-09	0.1	3.23E-10	Egress_Data_Thru_Firewall40
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management35
2.84E-09	0.1	2.84E-10	DNS_Server_Ext35
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_52
2.84E-09	0.1	2.84E-10	Health_IT_DNS52
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root38
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management53
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_52
2.84E-09	0.1	2.84E-10	VPN_Server34
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners52
2.84E-09	0.1	2.84E-10	DNS_Server_Ext53
2.84E-09	0.1	2.84E-10	Risk_Manager52
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root35
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root53
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_32
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management52
2.84E-09	0.1	2.84E-10	VPN_Server52
2.84E-09	0.1	2.84E-10	Virus_Malware52
2.84E-09	0.1	2.84E-10	Health_IT_DNS53
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management38
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_35
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root32
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners53
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management32
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_32
2.84E-09	0.1	2.84E-10	Risk_Manager53
2.84E-09	0.1	2.84E-10	DNS_Server_Ext32
2.84E-09	0.1	2.84E-10	Health_IT_DNS32
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_53
2.84E-09	0.1	2.84E-10	Health_IT_DNS35
2.84E-09	0.1	2.84E-10	DNS_Server_Ext38
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_35
2.84E-09	0.1	2.84E-10	Virus_Malware53
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners35
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_53
2.84E-09	0.1	2.84E-10	VPN_Server35
2.84E-09	0.1	2.84E-10	Virus_Malware35
2.84E-09	0.1	2.84E-10	Risk_Manager35

2.84E-09	0.1	2.84E-10	Vulnerability_Scanners38
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_38
2.84E-09	0.1	2.84E-10	VPN_Server39
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_34
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners39
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_39
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_39
2.84E-09	0.1	2.84E-10	Risk_Manager39
2.84E-09	0.1	2.84E-10	Virus_Malware39
2.84E-09	0.1	2.84E-10	Health_IT_DNS39
2.84E-09	0.1	2.84E-10	DNS_Server_Ext34
2.84E-09	0.1	2.84E-10	Virus_Malware32
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_34
2.84E-09	0.1	2.84E-10	Risk_Manager32
2.84E-09	0.1	2.84E-10	Health_IT_DNS34
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root2
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners32
2.84E-09	0.1	2.84E-10	VPN_Server32
2.84E-09	0.1	2.84E-10	Health_IT_DNS38
2.84E-09	0.1	2.84E-10	Risk_Manager34
2.84E-09	0.1	2.84E-10	DNS_Server_Ext52
2.84E-09	0.1	2.84E-10	Risk_Manager38
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root52
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management34
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners34
2.84E-09	0.1	2.84E-10	VPN_Server38
2.84E-09	0.1	2.84E-10	Virus_Malware34
2.84E-09	0.1	2.84E-10	DNS_Server_Ext39
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management39
2.84E-09	0.1	2.84E-10	VPN_Server53
2.84E-09	0.1	2.84E-10	Virus_Malware38
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_38
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root39
2.20E-09	0.1	2.20E-10	Vulnerability_Scanners54
2.20E-09	0.1	2.20E-10	DNS_Server_Ext54
2.20E-09	0.1	2.20E-10	VPN_Server54
2.20E-09	0.1	2.20E-10	Health_IT_Configuration_Management54

2.20E-09	0.1	2.20E-10	Risk_Manager54
2.20E-09	0.1	2.20E-10	Health_IT_DNS54
2.20E-09	0.1	2.20E-10	Intrusion_Detection_System__IDS_54
2.20E-09	0.1	2.20E-10	Mobile_Network_Access_Control__NAC_54
2.20E-09	0.1	2.20E-10	Virus_Malware54
2.20E-09	0.1	2.20E-10	Health_IT_CA_Root54
2.20E-09	0.1	2.20E-10	Health_IT_DNS40
2.20E-09	0.1	2.20E-10	DNS_Server_Ext40
2.20E-09	0.1	2.20E-10	Health_IT_Configuration_Management40
2.20E-09	0.1	2.20E-10	Intrusion_Detection_System__IDS_40
2.20E-09	0.1	2.20E-10	Vulnerability_Scanners40
2.20E-09	0.1	2.20E-10	Mobile_Network_Access_Control__NAC_40
2.20E-09	0.1	2.20E-10	VPN_Server40
2.20E-09	0.1	2.20E-10	Virus_Malware40
2.20E-09	0.1	2.20E-10	Risk_Manager40
2.20E-09	0.1	2.20E-10	Health_IT_CA_Root40
1.83E-09	0.1	1.83E-10	Connect_as_OpenEMR54
3.67E-10	0.5	1.83E-10	Ask_Receives_Critical_Data_from_the_User54
1.83E-09	0.1	1.83E-10	Connect_as_OpenEMR443
3.67E-10	0.5	1.83E-10	Mobile_Device_User_Does_Not_Notice54
3.67E-10	0.5	1.83E-10	Mobile_Device_User_Does_Not_Notice443
3.67E-10	0.5	1.83E-10	Ask_Receives_Critical_Data_from_the_User443
1.56E-09	0.1	1.56E-10	VPN_Server37
1.56E-09	0.1	1.56E-10	Risk_Manager37
1.56E-09	0.1	1.56E-10	Mobile_Network_Access_Control__NAC_37
1.56E-09	0.1	1.56E-10	Virus_Malware37
1.56E-09	0.1	1.56E-10	Intrusion_Detection_System__IDS_37
1.56E-09	0.1	1.56E-10	DNS_Server_Ext11
1.56E-09	0.1	1.56E-10	Health_IT_DNS37
1.56E-09	0.1	1.56E-10	Health_IT_DNS5
1.56E-09	0.1	1.56E-10	Health_IT_Configuration_Management4
1.56E-09	0.1	1.56E-10	Vulnerability_Scanners37
1.56E-09	0.1	1.56E-10	Intrusion_Detection_System__IDS_6
1.56E-09	0.1	1.56E-10	Health_IT_CA_Root3
1.56E-09	0.1	1.56E-10	DNS_Server_Ext37
1.56E-09	0.1	1.56E-10	VPN_Server13
1.56E-09	0.1	1.56E-10	Risk_Manager12

1.56E-09	0.1	1.56E-10	Vulnerability_Scanners8
1.56E-09	0.1	1.56E-10	Health_IT_Configuration_Management37
1.56E-09	0.1	1.56E-10	Virus_Malware9
1.56E-09	0.1	1.56E-10	Health_IT_CA_Root37
1.56E-09	0.1	1.56E-10	Mobile_Network_Access_Control__NAC_7
1.56E-09	0.1	1.56E-10	Health_IT_CA_Root51
1.56E-09	0.1	1.56E-10	DNS_Server_Ext51
1.56E-09	0.1	1.56E-10	Intrusion_Detection_System__IDS_51
1.56E-09	0.1	1.56E-10	Health_IT_DNS51
1.56E-09	0.1	1.56E-10	VPN_Server51
1.56E-09	0.1	1.56E-10	Mobile_Network_Access_Control__NAC_51
1.56E-09	0.1	1.56E-10	Virus_Malware51
1.56E-09	0.1	1.56E-10	Risk_Manager51
1.56E-09	0.1	1.56E-10	Health_IT_Configuration_Management51
1.56E-09	0.1	1.56E-10	Vulnerability_Scanners51
8.15E-09	0.01	8.15E-11	Force_Backup_Online__Critical_System_Failure264
8.15E-10	0.1	8.15E-11	Backup_data_Captured1
8.15E-09	0.01	8.15E-11	Re_Encrypt_Modified_Critical_Data284
8.15E-09	0.01	8.15E-11	Decrypt_Data54
8.15E-09	0.01	8.15E-11	Changing_Crtical_Data284
8.15E-10	0.1	8.15E-11	Backup_data_Captured54
8.15E-09	0.01	8.15E-11	Decrypt_Data20
8.15E-09	0.01	8.15E-11	Changing_Crtical_Data28
8.15E-10	0.1	8.15E-11	Gain_Access_to_the_Backup_System1
8.15E-09	0.01	8.15E-11	Re_Encrypt_Modified_Critical_Data28
8.15E-09	0.01	8.15E-11	Force_Backup_Online__Critical_System_Failure26
8.15E-10	0.1	8.15E-11	Access_the_Backup_system_on_site1
8.15E-09	0.01	8.15E-11	Force_Backup_Online__Critical_System_Failure25
8.15E-09	0.01	8.15E-11	Re_Encrypt_Modified_Critical_Data25
8.15E-09	0.01	8.15E-11	Changing_Crtical_Data25
8.15E-09	0.01	8.15E-11	Decrypt_Backup_Data_at_Rest21
8.15E-09	0.01	8.15E-11	Force_Backup_Online__Critical_System_Failure1
8.15E-09	0.01	8.15E-11	Changing_Crtical_Data8
8.15E-09	0.01	8.15E-11	Re_Encrypt_Modified_Critical_Data8
8.15E-09	0.01	8.15E-11	Decrypt_Backup_Data_at_Rest25
2.84E-10	0.1	2.84E-11	Health_IT_DNS36
2.84E-10	0.1	2.84E-11	VPN_Server

2.84E-10	0.1	2.84E-11	Risk_Manager
2.84E-10	0.1	2.84E-11	Vulnerability_Scanners
2.84E-10	0.1	2.84E-11	Virus_Malware
2.84E-10	0.1	2.84E-11	Health_IT_CA_Root36
2.84E-10	0.1	2.84E-11	DNS_Server_Ext36
2.84E-10	0.1	2.84E-11	Health_IT_DNS
2.84E-10	0.1	2.84E-11	Health_IT_Configuration_Management
2.84E-10	0.1	2.84E-11	DNS_Server_Ext
2.84E-10	0.1	2.84E-11	Health_IT_CA_Root
2.84E-10	0.1	2.84E-11	Mobile_Network_Access_Control__NAC_
2.84E-10	0.1	2.84E-11	Intrusion_Detection_System__IDS_
2.84E-10	0.1	2.84E-11	Health_IT_Configuration_Management36
2.84E-10	0.1	2.84E-11	Risk_Manager36
2.84E-10	0.1	2.84E-11	Mobile_Network_Access_Control__NAC_36
2.84E-10	0.1	2.84E-11	Virus_Malware36
2.84E-10	0.1	2.84E-11	Vulnerability_Scanners36
2.84E-10	0.1	2.84E-11	VPN_Server36
2.84E-10	0.1	2.84E-11	Intrusion_Detection_System__IDS_36
2.84E-10	0.1	2.84E-11	Health_IT_CA_Root50
2.84E-10	0.1	2.84E-11	DNS_Server_Ext50
2.84E-10	0.1	2.84E-11	Virus_Malware50
2.84E-10	0.1	2.84E-11	Vulnerability_Scanners50
2.84E-10	0.1	2.84E-11	Mobile_Network_Access_Control__NAC_50
2.84E-10	0.1	2.84E-11	Intrusion_Detection_System__IDS_50
2.84E-10	0.1	2.84E-11	Health_IT_DNS50
2.84E-10	0.1	2.84E-11	Health_IT_Configuration_Management50
2.84E-10	0.1	2.84E-11	VPN_Server50
2.84E-10	0.1	2.84E-11	Risk_Manager50
0.377	0.9	0.339	Degrade_the_Back_up4
0.678	0.5	0.339	During_Phyiscal_Transfer_Obtain_Copy1
0.0455	0.9	0.041	Degrade_the_Back_Up_Media
0.0455	0.9	0.041	Degrade_Back_Up2
0.41	0.1	0.041	Gain_Access_to_the_Backup_System1
0.41	0.1	0.041	Backup_data_Accessed1
0.41	0.1	0.041	Access_the_Backup_system_on_site1
0.0455	0.9	0.041	Degrade_Back_Up
1.56E-12	0.9	1.40E-12	Unplug_Ethernet_Cables_from_Access_Points3
1.56E-12	0.9	1.40E-12	Unplug_Ethernet_Cables_from_Access_Points1

1.56E-12	0.9	1.40E-12	Traffic___High_Volumes_Sent177
1.56E-12	0.9	1.40E-12	Traffic___High_Volumes_Sent111
1.56E-12	0.9	1.40E-12	Physically_Destroy_Any_Critically_Functional_Devices3
1.56E-12	0.9	1.40E-12	Physically_Destroy_Any_Critically_Functional_Devices1
1.56E-12	0.9	1.40E-12	Traffic___High_Volumes_Sent1
1.56E-12	0.9	1.40E-12	Physically_Destroy_Any_Critically_Functional_Devices66
1.02E-12	0.9	9.17E-13	Install_Device_Degrading_Malware411
1.02E-12	0.9	9.17E-13	Install_Device_Degrading_Malware413
4.83E-13	0.9	4.34E-13	User_walks_away_from_logged_on_Mobile_Device4431
4.83E-13	0.9	4.34E-13	User_walks_away_from_logged_on_Mobile_Device4433
3.11E-13	0.5	1.56E-13	WiFI_RF_Jamming_Device_Data_Transfer1
3.11E-13	0.5	1.56E-13	WiFI_RF_Jamming_Device_Data_Transfer3
2.12E-13	0.5	1.06E-13	Acquire_Password21
1.18E-13	0.9	1.06E-13	PluginHub1
1.18E-13	0.9	1.06E-13	Send_Data_to_New_GW_or_Reconfigure1
1.18E-13	0.9	1.06E-13	PluginHub3
2.12E-13	0.5	1.06E-13	Acquire_Password23
1.18E-13	0.9	1.06E-13	Send_Data_to_New_GW_or_Reconfigure3
9.66E-14	0.5	4.83E-14	Obtain_OS_Athenication4433
9.66E-14	0.5	4.83E-14	Obtain_OS_Athenication4431
8.03E-14	0.5	4.01E-14	Buying_Malware22
8.03E-14	0.5	4.01E-14	Buying_Malware9
8.03E-14	0.5	4.01E-14	Buying_Malware
1.73E-13	0.1	1.73E-14	Access_to_HIT_Server_Room_Firewall77
1.73E-13	0.1	1.73E-14	Access_to_HIT_Server_Room_Firewall11
1.73E-13	0.1	1.73E-14	Access_to_HIT_Server_Room_Firewall
1.73E-13	0.1	1.73E-14	Login_3
1.73E-13	0.1	1.73E-14	Connect_as_New_Device0
1.73E-13	0.1	1.73E-14	Login11
1.73E-13	0.1	1.73E-14	Connect_as_New_Device3
1.73E-13	0.1	1.73E-14	Login_66
1.73E-13	0.1	1.73E-14	Connect_as_New_Device55
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall777
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall677
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall277
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall477

1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall377
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall311
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall411
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall611
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall711
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall811
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall877
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall211
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall8
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall7
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall2
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall3
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall6
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall4
1.71E-14	0.9	1.54E-14	Degrade_Access_Point11
1.71E-14	0.9	1.54E-14	Degrade_Access_Point3
1.54E-13	0.1	1.54E-14	Gain_Access_to_Access_Point13
1.54E-13	0.1	1.54E-14	Gain_Access_to_Access_Point11
1.71E-14	0.9	1.54E-14	DisconnectDevice00
1.71E-14	0.9	1.54E-14	Disconnect_OpenEMR3333
1.71E-14	0.9	1.54E-14	Disconnect_OpenEMR000
1.71E-14	0.9	1.54E-14	DisconnectDevice3333
1.54E-13	0.1	1.54E-14	Connect_as_OpenEMR23333
1.54E-13	0.1	1.54E-14	Connect_as_Device00
1.54E-13	0.1	1.54E-14	Connect_as_OpenEMR2000
1.54E-13	0.1	1.54E-14	Connect_as_Device3333
1.54E-13	0.1	1.54E-14	Connect_as_OpenEMR2
1.54E-13	0.1	1.54E-14	Connect_as_Device
1.71E-14	0.9	1.54E-14	Disconnect_OpenEMR
1.71E-14	0.9	1.54E-14	DisconnectDevice
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent311
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent777
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent877
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent711
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent477
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent377
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent677

1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent611
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent411
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent811
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent211
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent277
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent3
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent7
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent6
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent4
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent8
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent2
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall79
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall822
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall39
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall722
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall322
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall89
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall422
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall69
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall622
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall49
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall29
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall222
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall72
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall62
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall82
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall42
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall32
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall22
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent422
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent322
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent622
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent89
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent29
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent39
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent222
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent69

6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent822
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent79
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent49
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent722
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent62
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent82
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent72
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent32
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent42
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent22
4.46E-14	0.1	4.46E-15	Coding_Malware9
4.46E-14	0.1	4.46E-15	Coding_Malware22
4.46E-14	0.1	4.46E-15	Coding_Malware
5.27E-14	0.01	5.27E-16	Access_from_AP_to_Mobile_Device4433
5.27E-14	0.01	5.27E-16	Access_from_AP_to_Mobile_Device4431
7.02E-16	0.75	5.27E-16	Malicious_Access_Point4431
5.85E-16	0.9	5.27E-16	Install_Device_Degrading_Malware4433
5.85E-16	0.9	5.27E-16	Install_Device_Degrading_Malware4431
7.02E-16	0.75	5.27E-16	Malicious_Access_Point4433
1.05E-15	0.5	5.27E-16	Mobile_Device_Attaches_to_Malicious_Access_Point4433
1.05E-15	0.5	5.27E-16	Mobile_Device_Attaches_to_Malicious_Access_Point4431
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR411
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR877
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR777
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR811
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR611
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR711
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR111
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR477
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR377
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR311
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR677
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR177
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR3
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR1
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR8

1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR4
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR7
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR6
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR622
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR822
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR69
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR422
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR322
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR79
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR89
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR39
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR49
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR722
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR19
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR122
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR32
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR82
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR62
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR72
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR42
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR12
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent833
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent81
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent30
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent40
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent60
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent61
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent80
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent333
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent73
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent41
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent83
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent70
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent31
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent71
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent63
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent43

9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent433
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent33
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent733
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent633
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent766
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent46
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent355
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent66
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent866
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent655
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent855
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent36
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent755
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent455
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent21
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent233
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent20
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent23
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent26
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent255
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent63333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent43333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent83333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent4000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent3333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent73333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent4333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent33333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent700
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent8333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent8000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent800
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent600
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent300
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent3000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent7333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent7000

8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent6000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent400
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent6333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent8444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent6444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent7444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent3111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent8111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent4444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent6111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent7111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent3444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent4111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent200
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent2000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent2333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent23333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent2222
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent2444
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR63
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR833
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR43
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR71
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR733
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR61
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR83
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR41
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR31
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR80
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR81
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR60
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR33
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR30
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR73
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR333
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR433
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR633

1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR70
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR40
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR355
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR46
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR855
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR655
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR66
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR455
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR866
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR36
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR766
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR755
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR133
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR11
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR10
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR13
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR16
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR155
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR6000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR7000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR83333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR4333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR4000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR6333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR8000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR700
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR63333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR800
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR600
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR73333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR400
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR7333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR43333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR300
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR8333

9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR33333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR8111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR7111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR4444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR4111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR6444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR7444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR8444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR6111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR13333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR1000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR1333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR100
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR1444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3222