자원 한정적인 조직에서의 사이버보안 성숙도 진단모델 개선에 관한 고찰

이강석[1], 김수현[2], 이임영[3]
[1]순천향대학교 소프트웨어융합학과 박사과정
[2]순천향대학교 컴퓨터소프트웨어공학과 교수
[3]순천향대학교 컴퓨터소프트웨어공학과 교수
gangseok@sch.ac.kr, kimsh@sch.ac.kr, mylee@sch.ac.kr

A Study on the Improvement of the Cybersecurity Maturity Assessment Model for Resource-Constrained Organizations

Gangseok Lee[1], Suhyun Kim[2], Imyeong Lee[3]
[1]Dept. of Software Convergence, Soonchunhyang University
[2]Dept. of Computer Software Engineering, Soonchunhyang University
[3]Dept. of Computer Software Engineering, Soonchunhyang University

요 약

침해사고 대응팀의 성숙도를 진단하는 대표적인 모델인 SIM3와 SOC-CMM는 침해사고 대응팀의 설립 또는 운영 초기단계의 조직에 적용시 제한된 기술과 역량으로 인해 성숙도 진단 및 평가에 오판을 유발한다. 본 연구는 이러한 한계를 보완하는 개선된 성숙도 진단모델을 제시한다.

1. 서론

침해사고 대응팀(CSIRT, Computer Security Incident Response Team)은 사이버보안 위협에 대응하기 위해 침해사고 탐지, 분석, 대응 등 조직의 정보자산을 보호하는 역할을 담당한다. CSIRT의 성공적인 운영은 조직역량, 인적자원, 기술 인프라 등을 체계적으로 평가하고 지속적인 개선활동을 통해 달성된다. CSIRT의 성숙도 평가를 위해 다양한 진단모델이 활용되고 있으며, 대표적으로 SIM3 (Security Incident Management Maturity Model)와 SOC-CMM (Security Operations Center Capability Maturity Model)이 널리 사용되고 있다.

SIM3와 SOC-CMM은 CSIRT와 SOC의 성숙도를 평가하고, 운영능력 향상을 위한 체계적인 평가기법을 제공한다. 그러나 이러한 진단모델은 주로 대규모 조직이나 성숙한 보안환경을 기준으로 설계되어, CSIRT 구축 또는 초기 운영단계 등 자원제약 환경에 있는 조직에 적용시 몇가지 한계점을 드러낸다.

본 연구에서는 기존 성숙도 진단모델의 한계점을 분석하고, 이를 보완하기 위한 개선방안을 제시한다.

2. CSIRT 성숙도 진단모델 분석

CSIRT의 성숙도 진단을 위한 대표적인 모델은 SIM3와 SOC-CMM이 있으며, 이러한 진단모델은 거버넌스, 운영절차, 기술역량, 협력 및 소통 등 다양한 차원에서 CSIRT의 성숙도를 평가한다. 평가결과를 기반으로 CSIRT 구축을 준비 중인 조직은 가장 합리적인 규모의 조직과 서비스를 설계하며, CSIRT를 운영 중인 조직은 강점과 약점분석을 통해 개선분야를 파악할 수 있다.

2.1 SIM3

유럽연합 사이버 보안국(ENISA, European Union Agency for Cybersecurity)은 CSIRT의 실질적 경험을 바탕으로 CSIRT의 역량을 평가하기 위한 CSIRT 프레임워크를 개발[1]하였으며, SIM3는 이 프레임워크에 기반하여 CSIRT의 인적자원, 조직구조, 도구, 절차 등에 관해 평가한다. SIM3는 네 가지 평가영역, 44개의 세부질문으로 구성되며, 완성도에 따라 4단계(0-4)로 평가한다.[2]

1) 조직(Organization)

CSIRT의 운영효율성과 체계성에 관한 항목으로

조직구조, 역할 및 책임, 권한분배 등을 평가한다.

2) 인적 자원 (Human Resources)

보안사고의 효과적 관리를 위한 전문성과 지속적 역량개발을 위한 교육훈련의 존재여부를 평가한다.

3) 도구 (Tools)

침해사고 탐지 및 대응에 필요한 솔루션, 인프라, 통신 시스템 등 기술적 인프라에 대해 평가한다.

4) 절차 (Processes)

침해사고 분석 및 대응, 재발방지 등의 절차와 문서화, 일관성, 지속적 개선 활동을 평가한다.

2.2 SOC-CMM

SOC-CMM은 스웨덴의 룰레오 공과대학(LTU, Luleå University of Technology) 석사 프로그램을 발전시켜, SOC 운영관련 실질적인 경험과 카네기멜론의 CMMi를 기반으로 개발되었다.[3]

SIM3가 CSIRT의 보안사고 대응, 조직구조와 절차에 중점을 두는 반면, SOC-CMM은 SOC의 위협탐지, 대응, 모니터링과 기술적 성숙도 등 기술적 운영능력에 중점을 둔다. 각 평가모델의 특성으로 인해 SIM3는 국가 CSIRT, SOC-CMM은 금융, 에너지, 정부 등의 부문에서 주로 활용되고 있다.

SOC-CMM은 비즈니스, 인력, 절차, 기술, 서비스 등 5가지 영역에서 SOC의 운영 성숙도를 평가한다.

1) 사업(Business)

SOC의 전략적 목표, 거버넌스, 정책, 그리고 고객 요구사항 충족 여부와 조직 비즈니스 목표 및 공동가치 형성 등을 평가한다.

2) 인력(People)

인력의 전문성, 역할과 책임의 명확성, 교육 및 훈련 프로그램의 효과성을 평가한다.

3) 프로세스(Process)

보안위협 탐지 및 대응 프로세스의 일관성, 문서화 수준, 최적화 상태를 점검한다.

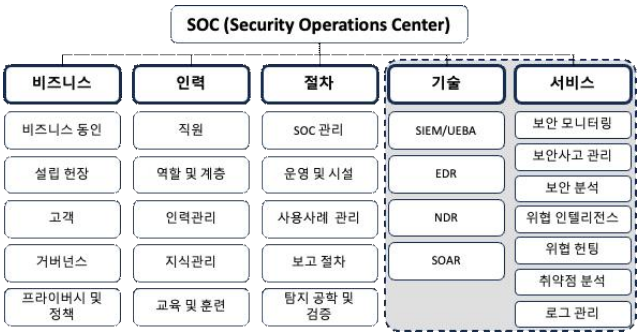
4) 기술(Technology)

SIEM(Security information and event management), NDR(Network Detection and Response), EDR(Endpoint Detection Response), SOAR(Security Orchestration, Automation, and Response), TI(Threat Intelligence), TH(Threat Hunting) 등 보안 모니터링 및 대응 솔루션의 현대화 및 자동화 여부를 평가한다.

5) 서비스(Services)

보안 모니터링, 침해사고 대응, 위협 인텔리전스, 취약점 관리 등 핵심 서비스에 대한 효과성과 성숙도를 평가한다.

(그림 1)은 SOC-CMM의 평가영역과 평가 파라메터를 보여주며, 기술과 서비스 영역에서 세밀한 요구사항을 포함함을 볼 수 있다.



(그림 1) SOC-CMM 평가영역 및 평가 파라메터

3. CSIRT 성숙도 진단모델의 한계

SIM3와 SOC-CMM은 운영중인 CSIRT/SOC의 여러 경험을 통해 개발된 것으로, CSIRT/SOC 구축 또는 운영경험이 많지 않은 초기단계의 조직에게는 다음과 같은 한계가 있다.

3.1 물리적 인프라에 대한 요구사항 미흡

CSIRT는 물리시설로서 모니터룸, 서버룸, 업무공간, 디지털 포렌식 분석실, 비상대책 회의실 등 물리공간과 CCTV, 출입통제 시스템 등 물리보안 시설 등을 갖추고 있다. 물리시설은 운영 효율성, 물리보안, 고객 정보보안 등을 위해 중요한 요소이다.

3.2 CSIRT 내부 보안 인프라 요구사항 부재

CSIRT는 보안서비스 제공을 위한 네트워크 시스템, 업무관리 시스템, 모니터링 시스템, 백업 시스템 등 다양한 시스템과 솔루션을 보유하고 있다. CSIRT는 내부 시스템 보호를 위한 보안 솔루션과 보안체계를 별도로 갖추어야 한다.

3.3 CSIRT 운영을 위한 기술 의존성

성숙도 진단모델은 SIEM, SOAR, TI, TH 등과 같은 기술 인프라 요구사항을 정의하고 있다. 이는 대형 조직에 필요한 구조로 초기 CSIRT를 구축하는 조직에게는 부담이 될 수 있다. 초기 CSIRT 구축단계에서는 고객의 보호자산 특성에 따라, 핵심 서비스를 정의하고 적합한 최적의 보안솔루션을 설계하여 비용 효율성을 극대화할 필요가 있다. 따라서, 초기 설계단계에 적용 가능한 적합한 기술 인프라에 대한 선택적 요구사항을 반영할 필요가 있다.

4. CSIRT 성숙도 진단모델 개선 방안

4.1 개선된 성숙도 진단모델 설계 원칙

3장에서 도출한 문제점을 포함한 CSIRT 성숙도 진단모델 개선을 위한 원칙은 다음과 같다.

1) 거버넌스 체계화 및 가이드 제시

거버넌스는 조직이나 시스템을 운영하면서 이를 효과적으로 관리하기 위한 정책과 체계를 완성해 나가는 과정에서 완성된다. 사이버보안에 대한 경험이 부족한 조직은 거버넌스에 대한 인식부족으로 인해 구체적인 조직체계와 절차를 구상하기 어렵다.

따라서, 국가 사이버보안 체계, CSIRT 보안정책, CSIRT/SOC 운영절차로 구성되는 거버넌스 체계와 합리적인 가이드를 포함한다.

2) 물리적 인프라 요구사항 제시

CSIRT 구축을 위한 물리적 위치와 보안, 물리공간 및 배치, 출입통제, 공급망 관리, 백업센터 및 시스템 등에 대한 요구사항을 포함한다.

3) CSIRT 내부 보안 인프라 요구사항 제시

CSIRT는 내부 시스템 보안을 위한 네트워크 보안, CSIRT/SOC 시스템 보호를 위한 솔루션 및 유지보수 등의 요구사항을 포함한다.

4) 서비스 중심의 설계와 요구사항 제시

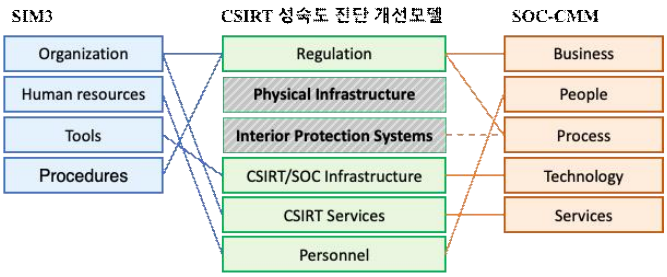
CSIRT 서비스는 다양한 형태의 보안솔루션과 기술로 구현이 가능하므로, 향후 운영 및 개선단계에서 추가적인 기술과 솔루션으로 보완할 수 있다.

따라서, CSIRT의 기술 의존성을 탈피하여, 서비스 설계와 운영을 위한 적합한 기술을 선택할 수 있도록 한다.

4.2 개선된 성숙도 진단모델 구조

개선된 성숙도 진단모델의 설계 원칙에 따라, 기존 성숙도 진단모델에 물리 인프라와 내부 보호 영역을 추가하여 개선된 진단모델을 제시한다.

개선된 진단모델은 법적규제(Regulation), 물리 인프라(Physical Infrastructure), 내부 보호(Internal Protection), CSIRT 기술(Technology), CSIRT 서비스(Service), 인력(Personal) 등 6개의 평가영역으로 구성된다. (그림 2)는 기존 성숙도 진단모델과 평가영역간 차이점을 보여준다.



(그림 2) 기존 CSIRT 성숙도 진단모델과 개선모델간 비교

5. 결론

본 연구에서는 기존의 대표적인 CSIRT 성숙도 진단모델인 SIM3와 SOC-CMM에 대해 살펴보고, 이들 모델이 CSIRT를 구축 또는 초기 운영단계의 조직에 제한적인 요소들을 분석하였다.

이를 기반으로 기존 성숙도 진단모델이 갖는 한계를 보완하는 CSIRT 성숙도 진단 개선모델의 평가영역을 제시하였다.

향후, 각 평가영역별 세부 평가지표를 설계하고, 실제 CSIRT 구축 또는 초기 운영단계의 조직에 적용하여 그 효과성과 타당성을 검증하고자 한다.

참고문헌

[1] Andrea Dufkova 외, “ENISA CSIRT MATURITY FRAMEWORK”, ENISA, 2022.2.
[2] ENISA, “SIM3v2i self-assessment tool”, 2022.
[3] SOC-CMM, “SOC-CMM Assessment Tool”, 2024.