Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 5 pp. 487-493, 2024

https://doi.org/10.5762/KAIS.2024.25.5.487
ISSN 1975-4701 / eISSN 2288-4688

효과적인 사이버보안 관리를 위한 통합 솔루션: Cisco 2024 사이버보안 준비 지수 분석을 통한 전략적 통찰 및 도전 과제 해결

유도진[1], 김제원[2*]
[1]극동대학교 해킹보안학과, [2]강원대학교 디지털밀리터리학과

Integrated Solutions for Effective Cybersecurity Management: Strategic Insights and Challenges Resolution through Cisco's 2024 Cybersecurity Readiness Index Analysis

Do Jin Yoo[1], Ze One Kim[2*]
[1]Department of Hacking & Security Far East University
[2]Department of Digital Military, Kangwon University

요 약 본 연구는 Cisco의 2024 사이버보안 준비 지수 보고서를 기반으로, 글로벌 기업들이 사이버보안 위협에 대응하기 위한 통합 보안 솔루션의 중요성을 강조한다. 분석을 통해 통합 사이버보안 솔루션의 적용이 관리 효율성을 증대시키고, 보안 커버리지의 명확성을 향상시키며, 보안 운영을 단순화하는 구체적인 방법을 탐구하였다. 이 연구는 다양한 포인트 솔루션의 사용이 초래할 수 있는 문제점들을 심도 있게 분석하고, 이를 해결할 수 있는 통합 솔루션의 효과를 실제 사례를 통해 조명하였다. 이를 통해, Cisco와 같은 통합 사이버보안 솔루션이 기업들이 신속하게 변화하는 사이버보안 위협 환경에 효과적으로 대응하도록 지원하는 방식을 밝히고자 하였다. 본 연구는 기업과 정부 기관이 강화된 사이버보안 전략을 수립하고 실행하는 데 필요한 실질적인 권장 사항을 제공하며, 통합 솔루션을 통해 사이버보안 준비도를 구체적으로 개선하는 방안을 제시한다. 또한, 조직의 규모에 따른 준비도 차이를 해소하기 위한 통합 접근 방식의 중요성을 강조하고, 이 접근을 통해 모든 조직이 지속 가능한 보안 자세를 개발하고 유지할 수 있도록 실질적인 방법을 제공한다.

Abstract This paper is based on Cisco's 2024 Cybersecurity Readiness Index Report, highlighting the importance of integrated security solutions for global enterprises facing cybersecurity threats. Through the analysis, this study explores how the application of integrated cybersecurity solutions enhances management efficiency, improves the clarity of security coverage, and simplifies security operations. This study analyzes the problems caused by using various point solutions and illuminates the effectiveness of integrated solutions through actual case studies. This demonstrates how integrated cybersecurity solutions like Cisco support enterprises effectively respond to rapidly changing cybersecurity threat environments. This paper provides practical recommendations for enterprises and government agencies to establish and implement enhanced cybersecurity strategies and presents concrete methods to improve cybersecurity readiness through integrated solutions. In addition, it emphasizes the importance of an integrated approach to address the differences in readiness levels according to the organizational size, offering practical methods to help all organizations develop and maintain a sustainable security posture.

Keywords : Integrated Cybersecurity Solution, Cybersecurity Readiness, Management Efficiency, Security Coverage, Cybersecurity Threat Response, Sustainable Security Strategy

본 논문은 강원대학교 학술연구비에 의하여 연구되었음.
*Corresponding Author : Ze One Kim(Kangwon Univ.)
email: Kimsbae2010@naver.com
Received April 1, 2024 Revised April 22, 2024
Accepted May 3, 2024 Published May 31, 2024

1. 서론

현재의 디지털 경제에서 기업과 정부 기관은 클라우드 컴퓨팅, 빅데이터, 인공지능(AI), 사물인터넷(IoT)과 같은 정보 기술의 혁신적 발전을 비즈니스 모델 재정의와 운영 효율성 극대화의 기회로 활용하고 있다[1]. 그러나 이러한 기술들의 발전은 복잡하고 지능적인 사이버보안 위협의 출현을 촉진시켜, 조직의 사이버보안 준비도가 어느 때보다 중요해지게 하였다. 사이버 공격의 성공은 데이터 유출, 금융 손실, 그리고 조직의 명성에 대한 중대한 손상을 초래하며, 이는 전 세계적으로 기업과 정부에 중대한 도전 과제를 제기한다[1]. 이러한 배경 하에 Cisco의 "2024 사이버보안 준비 지수" 보고서는 전 세계 8,000명 이상의 사이버보안 전문가와 비즈니스 리더를 대상으로 한 설문조사를 기반으로, 현재의 사이버보안 위협과 대응 전략에 대해 분석하였다[2]. 본 연구는 이 보고서를 바탕으로 사이버보안 위협의 진화에 대응하기 위한 전략적 접근의 필요성을 강조하고, 조직이 사이버보안 준비도를 어떻게 강화할 수 있는지를 제안한다. 연구의 목적은 기술 발전이 사이버보안에 미치는 영향을 이해하고, 조직들이 보다 효과적인 보안 전략을 수립하여 위협에 대응할 수 있는 방법을 모색하는 것이다.

본 논문은 포인트 솔루션의 과도한 사용과 그로 인해 발생할 수 있는 문제점들, 특히 관리 복잡성, 보안 커버리지의 모호성, 그리고 관제 대시보드의 분산이 조직의 보안 운영 효율성을 어떻게 저하시키는지를 깊이 있게 분석한다[3]. 또한, 통합 사이버보안 솔루션의 중요성과 이러한 시스템이 조직에 어떻게 도움을 줄 수 있는지를 탐구한다. 이를 통해 Cisco와 같은 통합 사이버보안 솔루션을 사용함으로써 조직이 변화하는 사이버보안 위협 환경에 어떻게 보다 효과적으로 대응할 수 있는지를 강조하고자 한다.

2. 연구방법

본 연구는 Cisco의 "2024 사이버보안 준비 지수" 보고서와 관련된 심층적인 분석을 통해, 통합 사이버보안 솔루션의 중요성과 포인트 솔루션의 사용으로 인한 문제점을 조명하였다. 이 연구는 특히, 다양한 보안 솔루션의 관리 복잡성 및 보안 커버리지 모호성 문제를 해결하기 위한 전략적 접근을 탐구한다.

2.1 연구설계

본 연구는 Cisco의 "2024 사이버보안 준비 지수" 보고서에 기반하여, 전 세계 30개 시장에서 8,136명의 비즈니스 및 사이버보안 리더들을 대상으로 한 설문조사 결과를 분석한다. 이 분석을 통해, 현재 사이버보안 위협 환경에 대한 기업들의 준비 상태와 대응 전략을 평가하며, 포인트 솔루션의 과다 사용이 초래할 수 있는 문제점과 통합 솔루션의 이점에 주목한다[4].

2.2 문헌연구

사이버보안 위협의 진화, 사이버보안 인력 부족, 기술 변화가 사이버보안 준비도에 미치는 영향[4] 등에 관한 연구를 포함하여, 다양한 문헌을 검토하였다[5-8]. 등의 연구를 통해, 포인트 솔루션의 사용 문제와 통합 솔루션의 필요성에 대한 근거를 제공한다. 이러한 문헌 검토를 통해, 본 연구는 포인트 솔루션 사용이 초래할 수 있는 관리 복잡성, 보안 커버리지의 모호성, 관제 대시보드 분산 등의 문제를 심층적으로 탐구한다. 또한, 통합 사이버보안 솔루션을 통한 효과적인 보안 관리의 중요성을 강조하며, 이러한 접근 방식이 조직의 사이버보안 자세를 어떻게 강화할 수 있는지에 대한 이론적 근거와 실질적 권장 사항을 제시한다.

2.3 Case Study

본 연구는 Cisco의 "2024 사이버보안 준비 지수" 보고서를 중심으로 한 Case Study를 수행하여, 조직들이 사이버보안 위협에 어떻게 대응하고 있는지, 그리고 통합 솔루션을 통한 보안 관리의 효율성을 어떻게 향상시킬 수 있는지에 대해 평가한다. 이 과정에서 다음 네 가지 주요 영역에 초점을 맞춘다:

- **조직의 사이버보안 준비 상태**: Cisco 보고서는 전 세계 30개국 이상에서 8,000명의 사이버보안 전문가와 비즈니스 리더를 대상으로 한 설문조사 결과를 제공한다[9,10]. 이 데이터는 조직의 사이버보안 준비도, 위협 인식, 그리고 대응 전략에 관한 귀중한 통찰을 제공한다.
- **사이버보안 위협에 대한 대응 전략**: 본 Case Study는 조직들이 어떻게 사이버보안 위협을 인식하고 대응하는지에 대한 실질적인 전략을 심층 분석한다. 여기에는 포인트 솔루션의 사용이 초래할 수 있는 관리의 복잡성과 통합 사이버보안 솔루션을 통한 보안 관리의 효율성에 대한 통찰도 포함된다.

- **도전 과제 및 대응 방안**: 이 섹션에서는 조직들이 직면한 주요 사이버보안 도전 과제를 식별하고, 이에 대응하기 위해 채택한 전략 및 접근 방식을 분석한다. 특히, 포인트 솔루션의 과도한 사용으로 인해 발생하는 보안 커버리지의 모호성과 관제 대시보드의 분산이 초래하는 관리 문제를 다룬다[11].
- **Best Practice 및 권장 사항**: 본 Case Study는 통합 사이버보안 솔루션의 사용이 갖는 잠재적 이점과, 조직들이 신속하게 변화하는 사이버보안 위협 환경에 보다 효과적으로 대응하기 위한 베스트 프랙티스를 제시한다[12,13]. 이를 통해 다른 조직들이 사이버보안 준비도를 강화하고, 효과적인 보안 전략을 수립하는 데 필요한 실질적인 가이드라인을 제공한다.

이 Case Study는 조직의 사이버보안 준비 상태와 통합 사이버보안 솔루션의 중요성을 심층적으로 탐구하며, 현대 사이버보안 환경에서의 복잡성에 효과적으로 대응하기 위한 전략적인 접근 방법을 모색한다. Cisco 보고서와 관련 연구의 결합을 통해, 본 연구는 조직들이 보다 효율적이고 강화된 사이버보안 전략을 개발하고 실행할 수 있도록 지원하는 데 목적을 둔다. 위 Case Study 방법을 표로 정리하면 아래와 같다.

Table 1. Summary of the Case Study on Cisco's 2024 Cybersecurity Readiness

Area	Description
Organizational Cybersecurity Readiness	-**Survey Scope:** Conducted by Cisco, encompassing over 8,000 cybersecurity professionals and leaders from more than 30 countries. -**Insights Provided:** Delivers a comprehensive understanding of how organizations gauge their cybersecurity preparedness, perceive potential threats, and plan their response strategies.
Cybersecurity Threat Response Strategies	-**Organizational Perception and Response:** Explores the depth of organizational strategies to identify and counteract cybersecurity threats. -**Management Insights:** Addresses the challenges of managing isolated (point) security solutions versus the advantages of adopting cohesive (integrated) cybersecurity management systems.
Challenges and Response Measures	-**Main Challenges:** Outlines the primary cybersecurity challenges encountered by organizations. -**Specific Issues:** Highlights the ambiguity in security coverage and operational difficulties stemming from the excessive use of point solutions and dispersed management dashboards.
All Best Practices and Recommendations	-**Integrated Solutions Benefits:** Emphasizes the advantages of utilizing integrated cybersecurity frameworks over isolated solutions. -**Guidelines for Enhancement:** Provides actionable recommendations for organizations to bolster their cybersecurity readiness and formulate effective security strategies, tailored to navigate the evolving cybersecurity threat landscape efficiently.

3. 결과 및 논의

3장은 상기 2장에서 명시한 내용을 바탕으로 한 결과들을 구체적으로 연결하였다. 이는 Cisco 2024 사이버보안 준비 지수 보고서의 분석, 문헌 연구, 그리고 설문조사 결과를 포함하여, 각 연구 방법론에서 도출된 데이터를 사용하여 주요 발견과 논의를 제시한다.

3.1 주요 발견

Cisco의 "2024 사이버보안 준비 지수" 분석을 통해 얻은 주요 발견은, 많은 조직들이 사이버보안 준비 상태의 중요성을 인식하고 있음에도 불구하고, 현재의 사이버보안 위협 환경에 충분히 대응할 준비가 되어 있지 않다는 것이다. 단지 소수의 응답 조직만이 '숙련된(Mature)' 카테고리에 분류되었으며, 대다수가 '형성중(Formative)' 또는 '초보자(Beginner)' 단계에 머무르고 있었다. 특히, 포인트 솔루션의 과다 사용으로 인한 문제점과 통합 솔루션의 필요성이 강조되었다. 포인트 솔루션들의 사용은 종종 보안 커버리지의 모호성, 관리의 복잡성 증가, 그리고 관제 대시보드의 분산으로 이어질 수 있으며, 이는 전반적인 보안의 효율성을 저하시킬 수 있다.

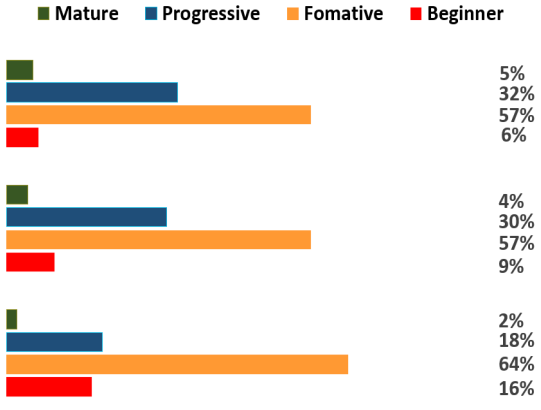

Fig. 1. Overall Readliness by Company Size

3.2 논의

3.2.1 사이버보안 프레임워크의 적용

Safitra et al의 연구는 조직이 변화하는 위협에 적응적으로 대응할 수 있도록 하는 미래 지향적인 사이버보안 프레임워크의 중요성을 강조한다[12]. 이러한 프레임워크는 특히, 다양한 포인트 솔루션을 사용함으로써 발생하는 보안 커버리지의 모호성과 관리의 복잡성 문제를 해결하는 데 중요할 수 있다. 조직은 이 프레임워크를 통해 각 솔루션의 커버리지를 명확하게 정의하고, 책임 영역을 분명히 할 수 있어야 한다.

3.2.2 통합 사이버보안 솔루션의 배치

Ahmad et al의 연구는 조직이 진화하는 위협 환경에 적극적이고 신속하게 적응하며 조직 학습을 가능하게 하는 사이버보안 관리와 사고 대응의 통합의 중요성을 강조한다[14]. 이러한 통합은 수십 개의 포인트 솔루션을 사용하는 대신에 통합된 관제 시스템을 적용하여 관리의 복잡도를 감소시키고, 효율적인 모니터링과 신속한 대응을 가능하게 한다. 조사 결과는 조직들이 파편화된 보안 조치에서 통합 사이버보안 솔루션으로 전환할 필요성을 강조하므로, 다수의 포인트 솔루션 사용은 효과적인 위협 탐지 및 대응에 주요한 장애물로 식별되었으며, 64%의 조직이 이로 인해 보안 운영 내 복잡성이 증가한다고 인정하였다. 이에 대응하여, 다양한 보안 Tool들을 일체형 시스템으로 통합할 수 있는 플랫폼 접근 방식을 채택하는 것이 필수적으로 보여진다. 이 접근 방식은 보안 관리 과정을 단순화할 뿐만 아니라 조직이 복잡한 사이버 위협에 효과적으로 대응할 수 있게 강화한다. 추가적으로, 현재 AI를 도입한 기업은 전체의 7%에 불과하며, 이 중에서 숙련된 상태에 있는 회사는 10% 미만이다. 이는 AI 기술의 활용을 높이고 사이버보안에 보다 효과적으로 통합할 필요가 있음을 나타낸다. AI 기술을 통합하면 보안 데이터 분석의 정확성과 위협 대응의 신속성을 높일 수 있으며, 이는 조직이 복잡한 사이버 위협에 더욱 효과적으로 대응할 수 있게 돕는다.

3.2.3 사이버보안 문화 및 교육의 강화

Georgiadou et al.의 연구는 조직의 사이버보안 문화 프레임워크를 평가하고, 조직이 사이버보안 위협에 대응하기 위한 준비도를 강화할 수 있는 방법을 제시한다[15]. 이는 조직 내에서 사이버보안 문화를 강화하고, 직원들에게 지속적인 교육과 인식 제고 활동을 실시함으로써, 인간의 약점을 공격하는 사이버위협으로부터 조직을 보호하는 데 중요하다. 특히, 직원들이 다양한 보안 솔루션과 통합된 관제 시스템의 사용 방법을 이해하고, 보안 커버리지가 겹치지 않도록 하며, 보안 관리의 복잡성을 최소화하는 방법을 교육하는 것이 필요하다. 또 다른 중요한 도전 과제는 사이버보안 전문가 부족으로, 조직의 절반 가까이가 10개 이상의 사이버보안 관련 직위를 채우지 못하고 있다고 보고하였다. 이 인력 격차는 조직이 견고한 사이버보안 조치를 유지하는 데 중대한 장애가 된다. 따라서 사이버보안 인력의 채용 및 지속적인 교육에 투자하는 것은 사이버보안 인력을 강화하는 데 전략적 필요성이 된다.

3.2.4 클라우드 보안과 AI 통합 강화

클라우드 보안 강화와 AI 및 머신러닝의 우선순위화는 현재 사이버보안 분야에서 중점을 두어야 할 두 가지 핵심 영역이다. 클라우드 강화 준비도에서 '초보자'나 '형성 중' 단계에 있는 조직이 54%에 달함을 감안할 때, 클라우드 보안을 강화하는 것은 필수적이다. 클라우드 기반 운영으로의 전환은 제3자 클라우드 서비스에 의해 도입된 독특한 취약점들을 고려하여 더욱 견고한 보안 프레임워크를 요구하며, 고급 암호화 및 동적 취약점 보호와 같은 클라우드 중심의 보안 조치들을 우선적으로 배치해야 한다. 동시에, AI와 머신러닝은 사이버보안 방어를 강화하는 데 점점 더 중요해지고 있다. 위협 탐지와 대응을 혁신할 잠재력에도 불구하고 AI 강화에서 '숙련된' 상태에 도달한 회사가 단 10%에도 못 미치는 것으로 나타나, 많은 조직들이 이 기술들을 충분히 활용하지 못하고 있다. 이는 조직들에게 AI 기반 솔루션을 보다 포괄적으로 통합할 명확한 기회를 제공한다.

상기 논의한 내용들을 표로 요약하면 아래 Table 2와 같다.

Table 2. Strategic Enhancements in Cybersecurity

Section	Key Insights
Cybersecurity Framework Application	-Importance of adaptive frameworks to evolving threats. -Reduces complexity and ambiguity from point solutions.
Recognizing multi-cultural families	-Integration crucial for rapid threat response. -Reduces management complexity; 67% report operational challenges.

Cybersecurity Culture and Education	-Emphasizes continuous education and awareness. -Nearly half of organizations face a cybersecurity professional shortage.
Cloud Security and AI Integration	-54% of organizations at beginner or intermediate cloud security levels. -Only 7% advanced in AI for cybersecurity.

3.2.5 개선된 대응 전략 제안

또한 조직의 사이버보안 체계를 강화하고 관리 복잡도를 줄이기 위해, 혁신적이고 창의적인 접근 방식을 도입하는 것이 필수적이다. 이러한 맥락에서, 아래의 인터랙티브 사이버보안 시뮬레이션 랩과 사이버보안 피드백 루프를 활용한 개선안을 제시한다.

3.2.5.1 인터랙티브 사이버보안 시뮬레이션 랩

사이버보안 시뮬레이션 랩은 직원들에게 다양한 사이버보안 위협 시나리오를 가상 환경에서 경험하게 함으로써, 실제 상황에서의 대응 전략을 실습하고 검증할 수 있는 기회를 제공한다. 클라우드 기반 플랫폼을 통한 구현은 조직이 기존의 IT 인프라에 큰 변화 없이 이 시뮬레이션 랩을 효율적으로 도입할 수 있도록 한다.

- **목표 설정과 맞춤형 시나리오 개발**: 조직의 특정 사이버보안 목표와 위험 평가를 바탕으로, 핵심 위협 시나리오를 선정하고, 조직의 IT 인프라와 업무 프로세스를 반영하는 맞춤형 시나리오를 개발한다. 이러한 접근은 직원들이 조직에 특히 중요한 사이버보안 위협 벡터에 집중할 수 있게 하며, 실제 업무 환경에서 발생할 수 있는 위협에 대한 현실감 있는 경험을 제공한다.
- **실시간 대응 및 피드백 메커니즘**: 시뮬레이션 중 발생하는 사이버보안 이벤트에 대해 실시간으로 대응하고, 직원들의 대응 방식에 대한 즉각적인 피드백을 제공하여, 직원들이 자신의 대응 방식을 개선하고 학습 효과를 극대화할 수 있도록 한다.
- **성과 추적 및 분석**: 시뮬레이션 랩에서의 직원들의 행동, 의사결정, 그리고 대응 성과를 추적하고 분석하여, 조직은 사이버보안 교육 프로그램을 지속적으로 개선하는 데 필요한 데이터를 확보할 수 있다.

3.2.5.2 사이버보안 피드백 루프

사이버보안 피드백 루프는 조직 내에서 직원들의 사이버보안 관련 활동에 대한 실시간 피드백을 제공하여, 사이버보안 의식과 행동의 지속적인 개선을 촉진한다. 이는 직원들이 자신의 행동이 조직의 사이버보안 상태에 어떤 영향을 미치는지 실시간으로 이해하고, 적극 개선할 수 있는 동기를 부여한다.

- **피드백의 자동화 및 맞춤화**: 자동화된 피드백 시스템을 통해, 직원별로 맞춤화된 피드백을 제공하며, 이는 각 직원의 사이버보안 학습 경로와 개선 필요 영역에 대한 명확한 가이드라인을 제시한다.
- **통합 보안 대시보드의 활용**: 통합 보안 대시보드를 통해, 관리자는 조직 전체의 보안태세와 직원들의 교육 진행 상황을 한눈에 파악하고, 전략적인 사이버보안 의사결정을 지원할 수 있다.
- **정기적인 리뷰 및 개선 회의**: 사이버보안 리뷰 및 개선 회의를 정기적으로 개최하여, 사이버보안 피드백 루프를 통해 수집된 데이터와 피드백을 기반으로 조직 내 사이버보안 문화를 강화하고 지속적인 개선을 촉진한다.

상기 내용들을 정리하면 아래 Table 3와 같다.

Table 3. Cybersecurity Simulation Labs & Feedback Loop Detailed Summary

Strategy	Purpose & Benefit	Key Implementation Aspects
Interactive Cybersecurity Simulation Labs	Equip employees with practical experience in handling cyber threats, enhancing their preparedness for real-life incidents.	-Develop scenarios based on actual risk assessments -Provide real-time feedback for immediate learning -Analyze performance to fine-tune training
Cybersecurity Feedback Loop	Foster a proactive cybersecurity culture through continuous feedback, promoting awareness and adaptive behaviors.	-Automate personalized feedback to guide improvement -Use a dashboard for a clear view of cybersecurity status and training progress -Conduct regular meetings to discuss feedback and strategize improvements

이렇듯 인터랙티브 사이버보안 시뮬레이션 랩과 사이버보안 피드백 루프의 결합은 조직의 사이버보안 역량 강화를 위한 혁신적인 접근법을 제시한다. 이 통합된 접근법은 사이버보안 위협에 대한 실질적이고 심층적인 대응 능력 개발, 직원들의 지속적인 학습과 개선을 촉진하며, 조직 내 사이버보안 문화의 강화를 목표로 하며, 이러한 통합된 접근 방식은 조직의 사이버보안 위협에 대

한 효과적인 대응 능력을 갖추는 것뿐만 아니라, 사이버 보안 관리의 복잡성을 해결하고, 조직 전반에 걸쳐 강력한 사이버보안 문화를 구축하는 데 기여할 것이다. 조직은 이를 통해, 사이버보안이 단순히 기술적인 문제가 아니라 조직 전략과 문화의 핵심 부분임을 인식하고, 이에 따라 행동할 수 있다.

4. 결론

본 연구는 Cisco의 2024 사이버보안 준비 지수 분석을 통해, 글로벌 조직들이 직면한 사이버보안 도전 과제에 대응하기 위해 통합 보안 솔루션의 중요성을 강조하였다. 연구 결과, 사이버보안 위협의 복잡성 증가 속에서 통합 솔루션을 채택함으로써 관리의 효율성을 향상시키고, 보안 커버리지의 명확성을 높이며, 보안 운영을 단순화할 수 있음이 밝혀졌다. 본 논문은 다양한 포인트 솔루션의 사용으로 인해 발생하는 문제점들을 심도 있게 분석하고, 이러한 문제를 해결할 수 있는 통합 솔루션의 효과를 조명하였다.

이 연구의 목적은 Cisco와 같은 통합 사이버보안 솔루션이 조직을 어떻게 지원하여 신속하게 변화하는 사이버보안 위협 환경에 효과적으로 대응할 수 있는지를 제시하는 것이다. 연구 결과는 조직들이 자신의 보안 전략을 강화하는 데 필요한 구체적이고 실질적인 권장 사항을 제공하며, 이는 사이버보안이 단순한 기술적 문제를 넘어 조직 전략과 문화의 핵심 부분임을 강조한다.

한편 이 연구는 Cisco의 보고서 데이터를 중심으로 진행되었으므로, 특정 지역이나 산업에 대한 더 세밀한 분석을 추가적으로 포함시킬 수 있는 여지가 있다. 따라서 향후 연구는 다양한 전략과 솔루션의 적용 가능성을 더 넓은 범위에서 탐구할 필요가 있다. 이는 클라우드 보안, 인공지능 및 머신러닝 기술의 통합, 그리고 조직 내 사이버보안 문화와 인력 교육 프로그램의 발전을 포함하여, 조직이 사이버보안 도전 과제를 보다 효과적으로 극복하고 지속 가능한 보안 전략을 수립할 수 있도록 지원할 것이다.

References

[1] Fadziso, T., Rao Thaduri, U., Dekkati, S., Ballamudi, V.K.R., & Desamsetti, H. (2023). "Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat." *figshare. Journal contribution.* DOI: https://doi.org/10.6084/m9.figshare.24189921.v1

[2] Frumento, E. (2019). "Cybersecurity and the evolutions of healthcare: challenges and threats behind its evolution." *M_Health current and future applications*, Springer. DOI: https://doi.org/10.1007/978-3-030-02182-5_4

[3] An, A. (2022). "The Evolution of Cybersecurity Threats in the Digital Age." *International Journal of Business Management and Ventures.* DOI: https://doi.org/10.1016/j.jisa.2020.102726

[4] Hasan, S., Ali, M., Kurnia, S., Thurasamy, R. (2021). "Evaluating the cyber security readiness of organizations and its influence on performance." *Journal of Information Security and Applications*, Vol. 58, 102726, ISSN 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2020.102726

[5] Zhou, L., Yan, W.Q., Shu, Y., Yu, J. "CVSS: A Cloud-Based Visual Surveillance System." *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications*, pp. 14, 2019. DOI: https://doi.org/10.4018/978-1-5225-7113-1.ch002

[6] Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H., Baskerville, R.L. (2019). "How integration of cyber security management and incident response enables organizational learning." *Journal of the Association for Information Science and Technology*, Vol. 71, No. 8, pp. 939-953. DOI: https://doi.org/10.1002/asi.24311

[7] Furnell, S. "The cybersecurity workforce and skills." *Computers & Security*, Vol. 100, 102080, January 2021. DOI: https://doi.org/10.1016/j.cose.2020.102080

[8] Quezada-Sarmiento, P.A., Enciso, L., Mayorga-Diaz, M.P., Mengual-Ándres, S., Hernandez, W., Vivanco-Ochoa, J.V., Vicente-Torres Carrión, P. "Promoting innovation and entrepreneurship skills in professionals in software engineering training: An approach to the academy and bodies of knowledge context." 2018 *IEEE Global Engineering Education Conference (EDUCON)*, Santa Cruz de Tenerife, Spain, 17-20 April 2018. DOI: https://doi.org/10.1109/EDUCON.2018.8363312

[9] Bartsch, M., Frey, S. (Eds.), *Cybersecurity Best Practices: Solutions for Increasing Cyber Resilience in Companies and Authorities*, 1st ed., Springer Vieweg, Wiesbaden, 2018, pp. LXVII, 644. DOI: https://doi.org/10.1007/978-3-658-21655-9

[10] Stallings, W., *Effective Cybersecurity: A Guide to Using Best Practices and Standards*, Addison-Wesley Professional, 2018, pp. LXVII, 644. DOI: https://doi.org/10.1007/978-3-658-21655-9

[11] Berlilana, T., Noparumpa, A., Ruangkanjanases… (2021). "Cybersecurity hygiene in the era of Internet of Things (IoT): Best practices and challenges." *Sustainability*, 13(24), 13761. DOI: https://doi.org/10.3390/su132413761

[12] Safitra, M.F., Lubis, M., Fakhrurroja, H. (2023). "Cybersecurity in the digital age: Tools, techniques, &

best practices." *Sustainability*, 15(18), 13369.
DOI: https://doi.org/10.3390/su151813369

[13] Szumski, O. "Cybersecurity best practices among Polish students." *Procedia Computer Science*, Vol. 126, 2018, pp. 1271-1280.
DOI: https://doi.org/10.1016/j.procs.2018.08.070

[14] Ahmad, A., Desouza, K.C., Maynard, S.B., Ahmad, A. (2020). "How integration of cyber security management and incident response enables organizational learning." *Journal of the Association for Information Science and Technology*.
DOI: https://doi.org/10.1002/asi.24311

[15] Georgiadou, A., Mouzakitis, S., Bounas, K., Vozikis, A. (2022). "A cyber-security culture framework for assessing organization readiness." *Journal of Computer Information Systems*.
DOI: https://doi.org/10.1080/08874417.2020.1845583

유 도 진(Do Jin Yoo) [정회원]

- 2014년 2월 : 강원대학교 중어중문학과 (문학사)
- 2018년 8월 : 명지대학교 대학원 융합보안학과 (공학석사)
- 2021년 8월 : 명지대학교 대학원 보안경영공학과 (공학박사)
- 2022년 9월 ~ 현재 : 극동대학교 해킹보안학과 조교수

〈관심분야〉
보안경영, 사이버보안, K-RMF

김 제 원(Ze One Kim) [정회원]

- 1990년 2월 : 강원대학교 체육교육학과 (교육학사)
- 1997년 3월 : 후쿠오카교육대 교육학과 (교육학석사)
- 2000년 3월 : 큐슈예술공과대 생활환경예술공학 (공학박사)
- 1990년 3월 ~ 2017년 2월 : 코오롱 총괄이사
- 2017년 3월 ~ 2019년 2월 : 강원대학교 산학협력중점교수
- 2019년 3월 ~ 현재 : 강원대 디지털밀리터리 학과 부교수
- 2022년 3월 ~ 2022년 10월 : 강원대학교 대외협력본부장

〈관심분야〉
군사체육, 사이버보안, K-RMF