https://doi.org/10.33778/kcsa.2022.22.4.065

사이버 전장인식을 위한 작전상태 요소 식별 및 통합 시계열 분석 연구★

김 선 영*, 권 구 형**, 이 현 진*, 이 재 연*, 고 장 혁**, 오 행 록**

요 약

사이버 작전은 가상의 사이버 전장 환경에서 수행되기 때문에, 지휘관이 사이버작전의 의사결정을 효과적으로 지원하기 위해서는 사이버 환경의 현황을 일관된 형태로 평가하고 가시화할 수 있는 평가지표를 정의하고 이를 측정할 수 있는 기술의 개발이 요구된다. 본 논문에서는 사이버 전장에서 수집할 수 있는 다양한 평가지표를 정의하고 이를 정규화하는 방법과 사이버 현황을 일관된 형태로 평가할 수 있는 기술을 제안한다. 제안하는 사이버 전장 상태 요소들의 통합 시계열 분석 및 도시 기술은 최상위에 정규화된 평가지표가 있으며, 해당 지표는 사이버 자산 관련 지표, 평가 대상망 관련 지표, 사이버 위협 관련 지표로 구성되는 각각의 지표들은 6개의 하위 지표를 가진다. 해당 지표들은 지휘관의 관심 영역에 따라 가중치를 부여하여 활용될 수 있고, 사이버 전장의 전체적인 현황을 파악할 수 있어 사이버 작전을 수행하는데 필요한 상황인식에 활용될 수 있을 것으로 예상된다.

A Study on Operational Element Identification and Integrated Time Series Analysis for Cyber Battlefield Recognition

Son-yong Kim*, Koo-hyung Kwon**, Hyun-jin Lee*, Jang-hyuk Kauh**, Haeng-rok Oh**

ABSTRACT

Since cyber operations are performed in a virtual cyber battlefield, the measurement indicators that can evaluate and visualize the current state of the cyber environment in a consistent form are required for the commander to effectively support the decision-making of cyber operations. In this paper, we propose a method to define various evaluation indicators that can be collected on the cyber battlefield, normalized them, and evaluate the cyber status in a consistent form. The proposed cyber battlefield status element consists of cyber asset-related indicators, target network-related indicators, and cyber threat-related indicators. Each indicator has 6 sub-indicators and can be used by assigning weights according to the commander's interests. The overall status of the cyber battlefield can be easily recognized because the measured indicators are visualized in time series on a single screen. Therefore, the proposed method can be used for the situational awareness required to effectively conduct cyber warfare.

Key words : Operational Element Identification, Integrated Time Series Analysis, Cyber Battlefiled Recognition

접수일(2022년 09월 30일), 수정일(2022년 10월 20일), 게재확정일(2022년 10월 31일)

★이 논문은 2019년 정부(방위사업청)의 재원으로 국방과학연구소의 지원을 받아 수행된 연구임(UC190089ED)

* 사이버전장팀, 한화시스템(주)., 경기도 성남시 분당구 판교역로 188, 13524, 188 Pangyoyeok-Ro Bundang-Gu Seongnam-Si Gyeonggi-Do Korea.

** 국방사이버기술센터, 국방과학연구소., 서울특별시 송파구 거여동 산25, 05744, San25 Songpa-Gu Seoul Korea.

1. 서 론

최근 C4ISR(Command, Control, Computer, Communication, Intelligence, Surveillance, and Reconnaissance)에 사이버보안를 추가한 C5ISR 센터가 미육군 정보기술 및 통합 시스템 센터인 CCDC(Combat Capabilities Development Command)에서 설립되었다[1]. 이는 육·해·공·우주 전장을 중심으로 하는 기존의 물리적인 전장뿐만 아니라, 제5의 전장인 사이버 전장에 대한 중요성이 증가한 결과이다. 국내에서도 '22년에 국방기술진흥연구소에서 발간된 '미래국방 2030 기술전략: 국방 AI 기술로드맵'에서 지능형통합사이버체계에 사이버지휘통제체계를 포함하고 있다[2]. 또한, 사이버 전장에서 발생하는 전투상황을 실시간으로 정보수집하고 외부 인텔리전스 정보와 융합·분석하여 사이버 공격을 판단하고 대응하는 사이버전장관리체계의 개발을 준비하고 있다.

전장관리체계는 각 요소를 유기적으로 통합하여 지휘관에게 부여된 임무 달성을 위해 가용한 자원을 최적의 장소와 시간에 할당하여 전투력 상승효과를 발휘할 수 있도록 지원하는 총제적인 수단과 절차를 말한다[3]. 이를 위해서는 전장공간 가시화 및 전장인식 공유, 자체진단 및 복구, 신속정확한 결심 및 계획 수립 지원, 전장 기능별 운영체계 통합, 수직·수평적 실시간 연동, 정보입력 및 정보유통 자동화와 같은 기능이 요구된다[4]. 사이버 전장관리체계도 이와 유사하게 사이버자산 및 취약점 정보 관리, 위협 인텔리전스 정보 수집 및 분석, 물리전 위협정보 연관분석 및 융합, 사이버 위협 정보 분배 및 공유를 수행할 수 있는 사이버 정보감시정찰 기술, 전장상황 정보 융합, 임무 영향성 및 피해평가, 사이버 작전요소 관리 및 효과도 평가, 사이버 공통작전상황도를 제공하는 사이버 지휘통제 기술, 마지막으로 시스템·네트워크 침입 감내, 기만체계 침입유도, 적 공격 경로 및 원점 분석, 내부자 위협 탐지 기능을 제공하는 사이버 능동대응 기술과 같은 핵심 기술의 개발이 요구된다. 특히, 사이버 작전은 가상의 사이버 환경에서 수행되기 때문에, 지휘관이 사이버작전의 의사결정을 효과적으로 지원하기 위해서는 사이버 환경의 현황을 일관된 형태로 평가할 수 있는 평가지표를 정의하는 것이 필요하며 환경에 따라 유연하게 평가지표를 변경할 수 있어야 한다[4], [5].

본 논문에서는 사이버 작전을 수행하는 네트워크에서 수집할 수 있는 다양한 평가지표를 정의하고 이를 정규화하는 방법과 다양한 평가지표를 분류하여 계층적으로 구성함으로써 사이버 현황을 일관된 형태로 평가할 수 있는 기술을 제안한다. 제안하는 사이버전 평가지표는 사이버자산의 상태정보를 측정하는 지표, 평가 대상 망의 상태정보를 측정하는 지표, 탐지한 위협 또는 자산의 취약점을 기반으로 사이버 위협 상태정보를 측정하는 지표로 구성된다. 자산상태, 네트워크 상태, 위협상태를 측정하는 지표들은 각각 6개의 개별 지표로 구성되며, 개별 지표들은 모두 독립되어 있다. 따라서 개별 지표들은 정규화한 후 가중치를 곱한 후 유클리드 크기(Euclidean Norm)를 계산한다. 계산된 자산 상태, 네트워크 상태, 위협 상태 지표에 가중치에 따라 총괄지표를 계산함으로써 계층구조의 사이버전 평가지표에 활용된다.

제안하는 지표는 지표 자체만으로 자산/망/위협의 상태를 측정하는 데 활용될 수 있을 뿐만 아니라, 지휘관이 사이버전장 상황에 맞는 요소들을 유연하게 조율해 정확한 상황인식(SA; Situational Awareness)과 의사결정을 지원하기 위한 사이버작전의 효과도(MoE; Measure of Effectiveness) 지표 또는 성능 지표(MoP; Measure of Performance)로 활용될 수 있을 것으로 예상된다.

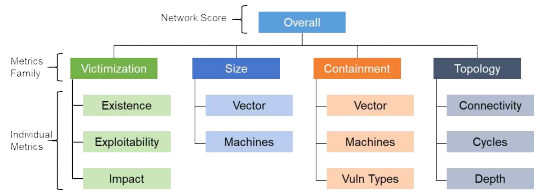
제안하는 논문은 6장으로 구성된다. 2장에서는 사이버 공격에 대한 피해평가 관련된 다양한 연구를 소개한다. 3장에서는 본 논문에서 제시하는 사이버 전장 상태 요소들의 통합 시계열 분석을 위한 시스템 구조를 기술한다. 4장에서는 제안하는 기술에 사용되는 평가지표에 대한 정의 및 측정방안을 기술한다. 5장에서는 제안하는 시계열 분석 기술의 구현 결과를 나타내고 결론에서는 본 논문에서 제안하는 평가지표에 대한 성과와 향후 연구 방향을 기술한다.

2. 관련 연구

사이버 공격의 피해평가 또는 이상탐지를 위한 방안은 활발히 연구되어 다양한 지표들이 상용화 되었다. 그러나, 대부분의 연구는 개별 지표에 집중하고 있어, 사이버 전장 상황을 다각적으로 분석하는 데 한계가 있다. 더불어 다수의 상용화 지표 기반 분석 결과들은 사용자가 직관적으로 이해할 수 있는 가시적 표현을 제공하지 않거나 정량적인 통합 결과를 제공하지 않아 정확한 상황 판단하기에 한계가 있다.

[6]에서는 공격 그래프를 기반으로 SCADA(Supervisory Control and Data Acquisition) 망에서 What-If 시나리오에 따른 사이버 침해 요구 시간에 대한 분석을 10가지 수행 단계로 제안하였다. 그러나, 사이버 공격자가 목적을 달성하기 위해 수행하는 공격의 소요시간을 측정하는 것이 어렵고, 군의 사이버전 무기화(Weaponized)는 사전에 준비된 경우가 많기에 침해 요구 시간이 달라질 수 있다. 본 연구는 [6]에서 공격 그래프 생성을 위해 시스템이 보유하고 있는 취약점 정보를 수집 및 분석 절차를 기반으로 (그림 3) 내 위협 정보 Family Metrics의 일부 요소로 적용하였다.

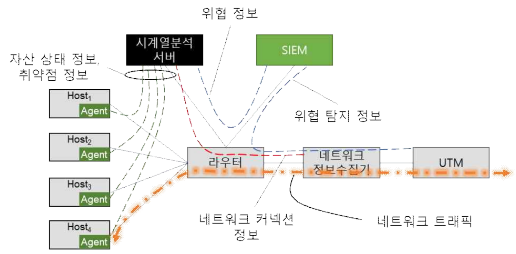
[7]는 공개출처정보로부터 구축된 데이터베이스에서 사이버 위협 평가요소를 선정하고 중요도를 분석하기 위해 계층분석적 의사결정방법(AHP)을 적용하였다. 해당 방안은 사이버 공격 데이터베이스 구조로 사건발생 정보, 사건 정보, 공격 정보, 공격자 정보, 피해자 정보, 피해 정보, 그리고 자료출처 정보 등 7가지 범주 33개 변수로 구성하였다. 더불어 사이버 위협에 직접적으로 영향을 미치는 공격목적, 공격범주, 공격대상, 공격 용이성, 공격 지속성, 공개출처정보의 빈도 등 총 6개 요소를 사이버 위협 평가요소로 선정 후 계층구조를 제시하였다. 그러나 [7]에서는 구축된 사이버 공격 데이터베이스와 제시한 평가요소별 상대적 중요도를 활용하여 사이버 상황을 정량적으로 분석하지 않아, 본 연구에서는 AHP 방법을 활용하여 통합 시계열 분석 요소들을 식별 후 요소들의 중요도를 선정하는 데 활용하였다.



(그림 1) 공격 그래프 매트릭 패밀리[8]

[8]은 MITRE에서 발생 가능한 사이버 공격 경로를 평가하기 위한 도구인 CyGraph에 적용된 기술로 계층구조로 구성된 다수의 정규화된 평가지표를 통해 네트워크의 사이버 공격 취약도를 평가한다. 평가지표는 (그림 1)과 같다. 최상위 Overall Metric은 독립적이고 직교성을 지닌 4개의 Family Metric(Victimization, Size, Containment Topology)으로 구성된다. 해당 논문은 사이버전에서 시계열 기반으로 측정한 지표가 평가대상망의 사이버 위험도를 평가하는데 적용 가능함을 제시한 측면에서 긍정적으로 평가할 수 있으며 본 논문에서 제안하는 기술을 개념화하고 설계하는 데 많이 반영되었다. 그러나, 취약점 중 Privilege Escalation 효과를 야기할 수 있는 취약점을 가진 자산은 해당 취약점을 기반으로 다른 공격들을 수행할 수 있으므로 취약점 및 네트워크 영역 정보를 제외한 나머지 지표는 실제 사이버 공격의 특성을 반영하는 데 한계가 있다. 본 논문에서는 [8]에서 제시한 최상위 Overall Metric부터 내부 Family Metric 및 Individual Metric 구조를 기반으로 정략적으로 분석해 공격 그래프 추출하는 매트릭 패밀리 개념을 사이버 전장 상태 요소 식별 및 통합 시계열 분석에 적용하였다.

따라서, 본 논문에서는 기존 평가지표들이 보유하고 있는 단점들을 극복하고자 사이버 자산에서 측정 가능한 상태 정보, 네트워크 상에서 측정 가능한 상태 정보, 취약점 스캐너 또는 보안 센서 장비를 통해 측정 가능한 취약점 또는 위협에 대한 상태정보를 기반으로 평가지표를 제안한다. 더불어 제시한 평가지표 기반 결과를 직관적으로 도시할 방안도 함께 제안한다.



(그림 2) 사이버 전장 통합 시계열 분석 기술의 시스템 구성도

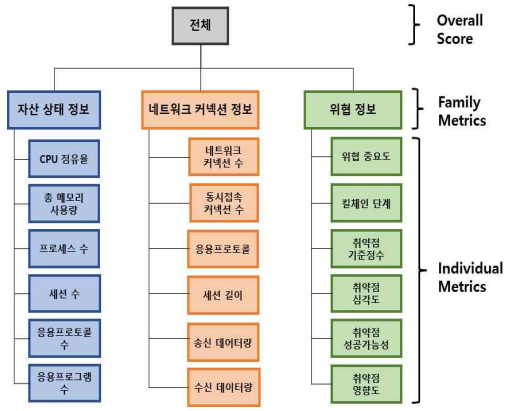
3. 시스템 아키텍처

본 논문에서 제안하는 사이버 전장 통합 시계열 분석 기술의 시스템 구성도는 (그림 2)와 같다. 분석망은 호스트(서버 또는 단말)와 라우터로 구성되어 있으며, 라우터 전단에 분석망으로 유통되는 사이버 위협을 탐지하기 위한 UTM(Unified Threat Management)과 네트워크 사용 상태를 수집하는 네트워크 정보 수집기가 배치된다. SIEM(Security Information and Event Management)은 UTM에서 수집한 위협 로그를 분석하여 탐지한 위협의 중요도, 킬체인 단계 등을 분석한다. 시계열 분석 서버는 주기적으로 SIEM으로부터 수집한 위협 정보, 네트워크 정보 수집기로부터 수집한 네트워크 커넥션 정보, 에이전트를 통해 수집한 자산 상태 정보 및 취약점 정보를 자산 별로 취합한 후 분석하여 통합 시계열 분석 정보를 구성한다.

4. 시계열 분석 설계 및 구현

4.1 사이버 전장 통합 시계열 분석

본 논문에서는 [6], [7], [8]에서 제안한 평가지표들의 운영개념을 기반으로 사이버작전을 위한 사이버 전장 상태 요소들을 총 3가지 종류 및 단계로 구성 후 평가지표에 필요한 세부 요소들을 추가하였다.



(그림 3) 통합 시계열 분석 지표

(그림 3)에서는 통합된 시계열 분석 결과인 OS(Overall Score)를 측정하기 위해 사이버 전장 상태 요소들을 자산 상태 정보, 네트워크 커넥션 정보, 그리고 위협 정보 총 3가지 FM(Family Metrics)으로 구성한다.

4.1.1 자산 상태 정보 Family Metrics

자산 상태 정보 FM는 자산의 상태를 식별하는데 필요한 요소들인 CPU 점유율, 총 메모리 사용량, 프로세스 수, 세션 수, 응용프로토콜 수, 그리

<표 1> 자산 상태 정보 IM 정의

자산 상태 정보 IM	정의
CPU 점유율	분석 시점으로부터 자산이 사용하고 있는 CPU 사용량(%)
총 메모리 사용량	분석 시점으로부터 자산이 사용하고 있는 메모리 사용량(bytes)
프로세스 수	분석 시점으로부터 자산이 백그라운드에서 구동하고 있는 총 프로세스 개수
세션 수	분석 시전으로부터 자산이 타 자산과 맺은 총 세션 개수
응용프로토콜 수	분석 시점으로부터 자산이 맺은 세션 중 발생한 응용프로토콜 개수
응용프로그램 수	분석 시점으로부터 자산에 설치된 응용프로그램 중 활성화인 개수

<표 2> 네트워크 커넥션 정보 IM

네트워크 커넥션 정보 IM	정의
네트워크 커넥션 수	분석 시점으로부터 자산이 타 자산과 맺은 네트워크 커넥션 개수
동시접속 커넥션 수	분석 시점으로부터 1분간 자산이 타 자산과 동시에 맺은 네트워크 커넥션 개수
응용프로토콜	분석 시점으로부터 자산이 맺은 세션 중 발생한 응용프로토콜 종류의 개수
세션 길이	분석 시점으로부터 자산이 맺은 세션의 길이(bytes)
송신 데이터량	분석 시점으로부터 자산이 송신한 데이터량(bytes per second)
수신 데이터량	분석 시점으로부터 자산에 수신된 데이터량(bytes per second)

고 응용프로그램 수 총 6가지 IM(Individual Metrics)으로 구성된다. 각 요소들에 대한 정의는 <표 1>과 같다.

4.1.2 네트워크 커넥션 정보 Family Metrics

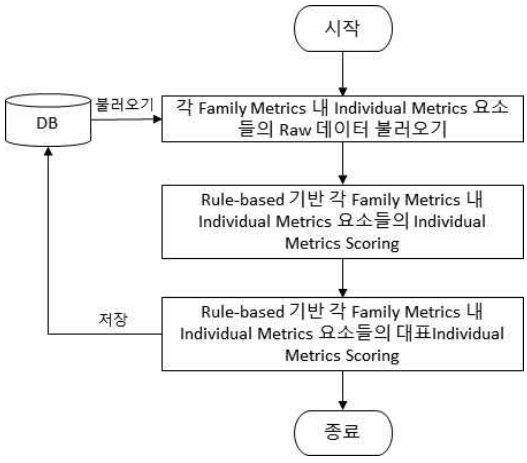
네트워크 커넥션 정보 FM는 자산이 타 자산과 맺은 네트워크 세션 정보를 기반으로 요소들을 구성한다. 이는 네트워크 커넥션 수, 동시접속 커넥션 수, 응용프로토콜, 세션 길이, 송신 데이터량, 그리고 수신 데이터량 총 6가지 IM으로 구분한다. 각 요소들에 대한 정의는 <표 2>와 같다.

4.1.3 위협 정보 Family Metrics

위협 정보 FM는 자산에 발생한 위협 정보 및 보유하고 있는 취약점 정보를 기반으로 요소들을 구성한다. 이는 위협 중요도, 킬체인 단계, 취약점 기준점수, 취약점 심각도, 취약점 성공가능성, 그리고 취약점 영향도 총 6가지 IM으로 구분한다. 각 요소들에 대한 정의는 <표 3>과 같다.

<표 3> 위협 정보 IM

위협 정보 IM	정의
위협 중요도	분석 시점으로부터 자산에 발생한 위협의 중요도 단계 정보
킬체인 단계	분석 시점으로부터 자산에 발생한 위협의 킬체인 단계 정보
취약점 기준점수	분석 시점으로부터 자산이 보유하고 있는 취약점의 CVSS 점수
취약점 심각도	분석 시점으로부터 자산이 보유하고 있는 취약점의 Severity 점수
취약점 성공가능성	분석 시점으로부터 자산이 보유하고 있는 취약점의 Exploitability 점수
취약점 영향도	분석 시점으로부터 자산이 보유하고 있는 취약점의 Impact 점수

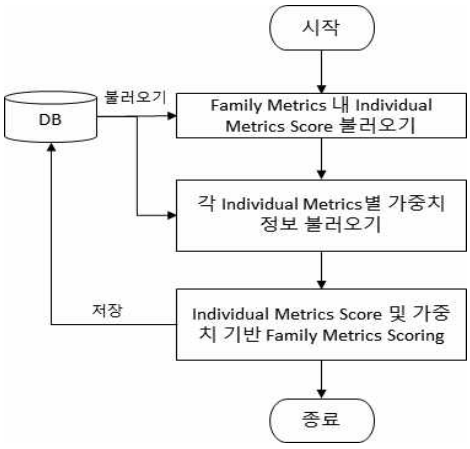


(그림 4) IMS 계산 알고리즘

4.2 시계열 분석 Metrics Scoring

4.2.1 통합 Individual Metrics Scoring

통합 시계열 분석은 (그림 4)와 같이 각 FM 내 IMS(Individual Metrics Scoring)로부터 시작된다. 세 종류의 FM 내 각 IMS를 측정하기 위해서는 DB로부터 이전 분석 시점 이후 5분 동안 발생한 <표 1>, <표 2>, 그리고 <표 3>에 제시된 Raw 데이터를 불러온다. 자산 상태 정보 및 네트워크 커넥션 정보 FM Raw 데이터는 Rule-based를 기준으로 개별 IMS 값으로 반환한다. 제시한



(그림 5) FMS 계산 알고리즘

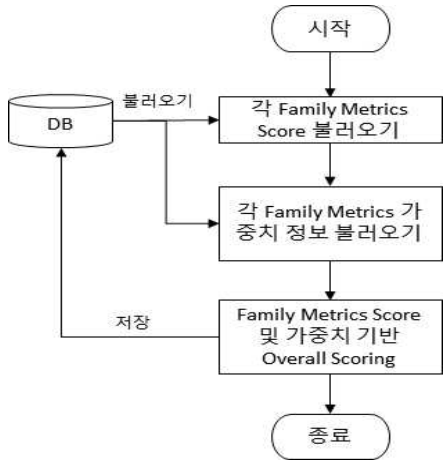
Rule-based는 구축된 군 사이버 영역 모의 환경을 기준으로 평균값을 IMS 3점을 부여 후 표준편차에서 벗어나는 만큼 나머지를 점수화한다. 다만 카테고리 기반 데이터 성격을 지닌 위협 정보 FM Raw 데이터는 식별된 SIEM 장비를 통해 수집 및 분석된 위협 및 취약점 정보를 기반으로 IMS Rule-based를 정의한다. 모의환경 내 다양한 자산별 IMS 대푯값은 식 2를 이용하여 계산한다.

$$IMS_{\text{대푯값}} = \frac{1}{n}\sum_{i=1}^{n} x_i \qquad (2)$$

이때, n은 자산의 수이고, x_i는 i번째 자산의 측정값이다.

4.2.2 통합 Family Metrics Scoring

FMS(Family Metrics Scoring)는 사용자로부터 수행하는 임무 및 근무환경에 맞게 설정된 각 IM에 대한 가중치 정보를 활용해 분석을 진행한다. (그림 5)는 FMS에 대한 흐름도를 도시한다. 더불어 식 3을 이용해 사전에 분석한 IMS(IMS_i)와 각 IM별 가중치 값(w_i)을 DB로부터 불러와 FMS를 측정 후 결과를 다시 DB에 저장한다.



(그림 6) OMS 계산 알고리즘

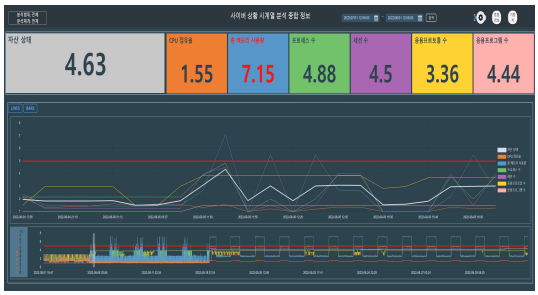
$$FMS = \sqrt{\frac{\sum_{i=1}^{6}(w_i * IMS_i)^2}{\sum_{i=1}^{6}(w_i)^2}} \qquad (3)$$

4.2.3 통합 Overall Scoring

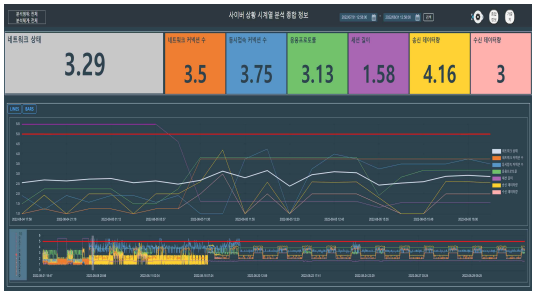
OS(Overall Scoring)는 FMS와 같은 개념을 지닌다. 설정된 각 FMS에 대한 가중치 정보를 활용해 분석을 진행한다. (그림 6)은 OS에 대한 흐름도를 도시한다. 최종 통합 시계열 분석 결과는 식 4를 이용해 분석한 FMS(FMS_i)와 각 FM별 가중치 값(w_i)을 DB로부터 불러와 측정 후 결과를 DB에 저장한다.

$$OS = \sqrt{\frac{\sum_{i=1}^{3}(w_i * FMS_i)^2}{\sum_{i=1}^{3}(w_i)^2}} \qquad (4)$$

(그림 7) 통합 시계열 분석



(그림 8) 자산 상태 정보 FMS



(그림 9) 네트워크 커넥션 정보 FMS

(그림 10) 위협 정보 FMS

(그림 11) 통합 시계열 분석 가중치 설정 화면

5. 사이버 전장 시계열 분석 시각화

통합 시계열 분석 화면은 (그림 7)과 같다. 화면의 상단에는 OS부터 시작해 자산 상태 정보, 네트워크 커넥션 정보, 그리고 위협 정보 FMS에 대한 점수가 각각 도시된다. 화면 하단에는 동일 시점에서 지난 한 달에 대한 분석 추이를 도시한다. 화면 중간부는 화면하단에서 하이라이팅된 기간동안의 측정값을 도시되고, 한다. 상단 각 FMS를 클릭하면 (그림 8), (그림 9), (그림 10)과 같이 개별 FMS와 관련된 IMS들이 도시된다. OS 및 FM에 대한 임계값을 설정할 수 있으며, 설정된 임계값을 초과하는 이벤트가 존재할 경우, 해당 구간을 강조하여 표현한다. 임계값은 각 영역의 하단에서 직접 설정할 수 있어 군 영역에서 지휘

관에게 직관적이면서 빠른 의사결정을 지원할 수 있다. 통합 시계열 분석은 군 환경에서 부대별 분석 요소들의 중요성이 다를 수 있기에 (그림 11)과 같은 가중치 설정 창이 존재한다. 본 기능을 통해 군에서는 소속 부대별 수행하는 작전 및 임무에 따라 적합하면서도 신뢰할 수 있는 분석이 가능해진다.

6. 결 론

본 논문에서는 사이버 작전을 수행하는 네트워크에서 수집할 수 있는 다양한 평가지표를 정의하고 이를 정규화하는 방법과 다양한 평가지표를 분류하여 통합된 사이버 현황을 지휘관이 평가할 수 있는 사이버전 평가지표를 제안했다. 해당 평가지표는 자산 상태 정보 FMS, 네트워크 커넥션 정보 FMS, 그리고 위협 정보 FMS로 구성이 되어 있으며 각각 6개의 개별 IMS 지표들로 추가 구성되어 있다. 더불어 본 논문에서는 분석된 요소들을 시각화하여 특정 기간의 추이를 분석해 사이버 현황을 시각적으로 인지할 방안을 제안했다. 또한 제안하는 지표는 지표 자체만으로 측정하는데 활용될 뿐만 아니라, 사이버전장 상황에 맞는 요소들을 지휘관이 유연하게 조율함으로써 정확한 상황인식과 의사결정을 지원하기 위한 사이버작전의 효과도 지표 또는 성능 지표로 활용될 수 있을 것으로 예상된다.

참고문헌

[1] C5ISR Center Cyber Capabilities, U.S.Army Combat Capabilities Development Comnmand - C5ISR Center, https://www.itea.org/wp-content/uploads/2019/03/Ploskonka_ITEA_26Mar19.pdf.

[2] 국방기술진흥연구소, 미래국방 2030 기술전략, 2022년 1월 26일, https://www.korea.kr/docViewer/skin/doc.html?fn=196698754&rs=/docViewer/result/2022.01/26/196698754.

[3] 박승, “전장관리체계 운용을 위한 전투지휘용 차량의 성능개량 개념,” 한국군사과학기술학회지, 제11권, 제2호, pp.16-22, 2008년 4월.

[4] 김두회, 김용현, 김동화, 신동규, 신동일, “사이버 전투 피해 평가 프레임워크,” In Proc. 한국정보처리학회 추계학술대회, 2017, pp. 178-181.

[5] 홀병진, 김완주, 이수진, & 임재성, “항공무기체계 사이버공격에 대한 작전영향성평가 프레임워크 제안,” 융합보안논문지, 제20권, 제4호, 2020, pp.35-45.

[6] M. A. McQueen, W. F. Boyer, M. A Flynn, and G. A. Beitel, “Quantitative cyber risk reduction estimation methodology for a small SCADA control system,” in Proc. Hawaii International Conference on System Sciences (HICSS'06), Vol. 9. 2006.

[7] 강성록, 문미남, 신규용, & 이종관, “공개출처정보를 활용한 사이버 위협 평가요소의 중요도 분석 연구,” 융합보안논문지, 제20권, 제1호, 2020, pp.49-57.

[8] S. Noel and S. Jajodia, “A Suite of Metrics For Network Attack Graph Analytics,” Network Security Metrics, Nov. 2017.

〔저자소개〕

김 선 영(Son-yong Kim)
한화시스템(주) 재직
고려대학교 전기전자전파공학(공학사)
관심분야 : 인공지능보안,
디지털포렌직, 사이버보안
E-mail : sonyong.kim@hanwha.com

권 구 형(Koo-hyung Kwon)
국방과학연구소 재직
고려대학교 전파공학학과(공학석사)
고려대학교 전기전자전파공학(공학사)
관심분야 : 사이버보안
E-mail : koohyung@add.re.kr

이 현 진(Hyun-jin Lee)
한화시스템(주) 재직
아주대학교 전자공학과(공학박사)
아주대학교 전자공학과 (공학석사)
아주대학교 전자공학과 (공학사)
관심분야 : 사이버보안, 통신프로토콜
분석, 통신시스템 설계, M&S
E-mail : hy.lee79@hanwha.com

이 재 연(Jae-yeon Lee)
한화시스템(주) 재직
광주과학기술원 정보통신(공학석사)
가톨릭대학교 정보통신(공학사)
관심분야 : 사이버보안
E-mail : jaeyeon46.lee@hanwha.com

고 장 혁(Jang-hyuk Kauh)
국방과학연구소 재직
광운대학교 컴퓨터과학과(공학박사)
광운대학교 컴퓨터과학과(공학석사)
광운대학교 컴퓨터과학과(공학사)
관심분야 : 사이버보안
E-mail : jhkauh@add.re.kr

오 행 록(Haeng-rok Oh)
국방과학연구소 재직
고려대학교 컴퓨터학과(수료)
인하대학교 전산학과(공학석사)
인하대학교 전산학과(공학사)
관심분야 : 사이버보안
E-mail : haengrok@add.re.kr