https://doi.org/10.33778/kcsa.2021.21.3.039

봉쇄-탐지-대응 기반 보안관제 대시보드 설계

한 충 희*

요 약

효율적인 보안관제센터 운영을 위해서는 보안관제 대시보드의 표준화가 반드시 필요하다. 보안관제 대시보드는 24시간 365일 내내 함께 생활해야 하는 보안관제근무자들에게 많이 활용되도록 구성해야 한다. 또한 보안관제센터의 업무활동을 종합적으로 표출할 수 있어야 한다. 추가적으로 보안관제센터의 업무활동들을 쉽게 설명할 수 있어야 할 것이다. 이에 본 논문에서 사례기관에 실제 적용한 봉쇄·탐지·대응 기반의 보안관제 대시보드 디자인을 설명하고자 한다. 이를 통해 불필요한 귀빈 맞춤형 대시보드 구성작업에 대한 노력과 시간을 줄이고 보안관제센터의 효율적인 운영에 이바지하고자 한다.

Security Operation Dashboard Design by Blockade-Detection-Response

Han Choong-Hee*

ABSTRACT

Standardization of the security operation dashboard is essential for efficient operation of security operation center. The security operation dashboard should be configured so that it is widely used by security operation workers who have to liv e together 24 hours a day, 365 days a year. In addition, it must be able to comprehensively express the business activities of the security operation center. In addition, it should be possible to easily explain the business activities of the security o peration center. Therefore, in this paper, we would like to explain the design of a security control dashboard based on bloc kade, detection, and response that is actually applied to case organizations in the power sector. Through this, it is intended to reduce the effort and time required for configuring a custom dashboard for VIPs, and contribute to the efficient operatio n of the security operation center.

Key words : Security operation center, Dashboard, Blockade-Detection-Response

접수일(2021년 08월 31일), 수정일(2021년 09월 23일), 게재확정일(2021년 9월 27일)

* 전력거래소 안전관리실/정보보안팀(주저자/교신저자)

1. 서 론

보안관제 업무란 정보자산들을 사이버공격으로부터 보호하는 활동이다. 이를 위해 보안 이벤트 및 로그 등을 실시간으로 감시, 대응하는 활동을 수행한다. 정보자산에 대한 보안은 전문집단이 수행하고, 관제대상기관은 기관의 핵심역량에 집중할 수 있도록 하는 것이다. 정보공유분석센터(ISAC, Information Sharing & Analysis Center)와 같은 의미를 갖고 있다. ISAC은 사이버테러와 정보 침해사고에 대해 효과적으로 공동 대응하기 위한 서비스 체계이다. 취약점과 침해요인, 대응방안에 관한 정보를 제공하고 침해사고가 발생하지 않도록 실시간 경보와 분석업무를 수행하게 된다.

보안관제센터의 대시보드는 효율적인 사이버 위협 탐지 대응활동을 위한 가장 기본적인 수단이다. 그러나 현재까지 이루어진 보안관제 대시보드에 대한 연구는 다양한 보안장비들의 연동에 초점을 맞추어 왔다. 빅데이터 기반의 통합보안관제시스템의 도입에 따라 빅데이터 처리된 보안로그에 대한 빠른 검색을 지원하기 위한 보안관제 대시보드의 연구에 집중하였다.

이에 본 논문에서는 보안관제센터의 대시보드에 어떤 정보를 표출시키는 것이 가장 효율적인가에 대하여 연구하였다. 이를 위해 현재 사용되는 기존의 보안관제 대시보드의 표출정보들이 무엇인가를 분석하였다. 또한 24시간 365일 매일매일 보안관제 대시보드를 사용하는 보안관제센터 근무자들을 대상으로 어떤 화면들을 주요 사용하고 있는지를 분석하였다. 이러한 분석들을 기반으로 BDR(Blockade Detection Response)기반의 보안관제 대시보드를 구축하였다.

2. 선행 연구

2.1 보안관제

보안관제라는 용어는 사이버공간의 안전성을 보장하고 위협과 침해사고들을 분석하며, 침해사고들에 능동적으로 대응한다는 의미이다[1]. 보안관제의 역할은 내·외부로부터의 불법해킹, 위협요소로부터 정보시스템, 데이터 등의 손상을 막고, 피해 발생시 재발방지를 위한 총체적인 운영관리를 말한다[2]. 많은 수의 서버 및 네트워크를 모니터링, 분석하여 조치사항에 대하여 실시간으로 분석 처리하는 업무이다[3]. 보안관제센터는 정보통신시스템 보호를 위한 핵심으로 조직의 사이버 방어 체계의 기본 인프라이다. 보안관제센터의 근본 목적은 침해사고를 식별하여 침해대응을 신속하게 하는 것이며 조직의 경영활동과 서비스가 안전하게 지속될 수 있도록 보장하는 것이다. Cyril은 보안관제센터를 ‘Security Operation Centre’라고 표현한다. 보안관제센터는 침해사고에 대한 탐지와 대응을 하기 위한 플랫폼들을 의미한다고 설명한다. 보안관제센터는 분석가, 운영자, 관리자 등의 요원들이 정보시스템, 인프라, 서비스들을 모니터하는 곳이다[4].

Natalia는 보안관제센터를 ‘Security Intelligence Center’로 설명한다. 보안관제센터를 운영하기 위한 기술적 요소들로 데이터 수집능력, 식별, 추적, 복구 능력들이 필요하다고 설명한다. 취약점을 점검하고 침해사고 대응과 복구 능력도 필수적인 기술적 요소들로 정의하였다. 또한 SIC를 NOC(Network Operation Center)와 통합하여 NSIC(Network Security Intelligence Center)라는 새로운 용어를 제안하였다[5].

Rasim은 IoT, Big Data, 스마트기기, Cloud 컴퓨팅의 등장에 따라 4차 산업시대의 보안관제의 개념으로 ‘CPS(Cyber-Phisical System, 사이버 물리시스템) 보안’이라는 용어를 소개하였다. CPS 보안은 수많은 IoT기기 보안 위협, 스마트그리드 보안 등을 포괄적으로 해결하기 위한 연구 노력의 일환으로 설명하고 있다[6].

보안관제는 영어로는 ‘Security Monitoring’ 또는 ‘Security Monitoring & Control’ 등으로 사용된다. Monitoring의 사전적 의미는 ‘컴퓨터 프로그램 수행 중 일어날 수 있는 여러 가지 오류에 대비하기 위한 감시활동’으로 설명된다. 관제는

‘국가나 공항 따위에서 강제적으로 관리하여 통제하는 일’을 말한다. 보안관제는 대상기관의 정보시스템 및 다양한 IT자원을 해킹, 바이러스 등과 같은 여러 사이버 공격으로부터 보호하기 위해 각종 보안 이벤트 및 시스템 로그들을 모니터링하고 분석하여 문제점에 대응하는 보안 업무라고 설명한다[7].

2.2 보안관제시스템

보안관제시스템은 방화벽(Firewall), 침입차단시스템(IPS), Anti-DDoS장비 등의 보안 이벤트를 하나로 통합하여 관리할 수 있게 해주는 시스템이다. 이기종 장비들에서 생산되는 보안이벤트를 한 곳에서 확인할 수 있도록 해주는 것이 주요 기능이다. 보안이벤트를 위험 등급 구분 방법론, 정규화·규칙 기반 이벤트 수집, 비정상 감지 및 대응, 통합정책 관리와 같은 기술을 활용하여 매 순간 발생한 보안이벤트에 대한 즉시적인 대응을 가능하게 해준다[8]. 고도화 되는 보안 위협에 대응하기 위해 인공지능 기술을 활용하는 방향으로 변화하고 있다. 사람이 직접 패턴을 만들고 대응하는 전통적인 보안관제에서 인공지능을 접목시킨 MDR(Managed Detection & Response)로 변화하고 있다. 실제 발생한 사건을 인공지능이 걸러내고 그 결과를 보안 전문가의 심층분석을 통해 대응하도록 한다[9]. 보안관제를 개선하기 위해 SIEM(Security Information and Event Management)이 도입되었다. SIEM장비를 이용하여 보안이벤트들을 실제로 악의적인지 아닌지를 조사하여 업무 편의성이 대폭 증가하였다[10].

2.3 보안관제 시각화 연구

기존의 보안관제 솔루션은 RDBMS(Relational Database Management) 기반으로 구축되지만 대량의 데이터 처리가 어려웠다. 이를 개선하기 위해 빅데이터 솔루션이 등장하여 비정형 데이터에 대해서도 빠른 검색 속도를 구현하였다[11, 12].

전상준은 빅데이터 보안관제 솔루션을 이용하여 보안관제 체계를 구현하는 방법을 연구하였다. 보안업계에서 사용되는 상용솔루션 중 하나인 Splunk와 Elastic Stack이라는 검색엔진을 활용해 보안로그를 단계별로 수집, 분석, 시각화 하는 대시보드를 구현하는 방안을 비교하였다[13].

현석우는 기존 보안관제의 한계점을 개선하기 위해 정보보호 장비, 취약점 DB, 탐지 로그와의 연동 결과들을 시각화하는 방안 연구하였다. 자산이 가지는 보안 취약점에 특화된 공격 위협에 신속히 대응하기 위해 취약점 DB와 연동시키고자 노력하였다[14]. 조우진은 보안관제의 빠른 대처를 위해 오픈소스 Elastic Stack을 이용하여 보안 로그를 시각화 하는 방법을 연구하였다[15].

이와 같이, 지금까지의 보안관제 시각화 연구들은 보안 장비들의 연동에 초점을 맞추어 각 장비들의 기능을 시각적으로 표출하려는 시도가 주를 이루어 왔다.

3. 보안관제 대시보드 표준화 연구

보안관제 대시보드 표준화를 위해 사례기관에서 사용하고 있는 기존의 대시보드의 표출항목들을 조사하였다. 그 다음으로 사례기관의 보안관제 전문요원들을 대상으로 자주 보는 화면들을 조사분석하였다.

3.1 사례기관의 기존 대시보드 분석

사례기관의 개선 전 보안관제 대시보드 표출내용은 12개의 주요 내용을 전체 상황반에 배치를 한 상황이다. 12개의 표출내용은 다음과 같다.

첫째, 금일 IPS 탐지 차단 발생 현황 그래프이다. 오늘 00시부터 현재시간까지의 각 시간대별 IPS에서 탐지한 누적 위협탐지 이벤트 발생 현황을 그래프로 일반 그래프 형식으로 표시하였다.

둘째, 금일/전일 IPS 탐지 차단 발생량 수치 현황이다. 오늘 00시부터 현재시간까지의 각 시간대

별 IPS에서 탐지한 누적 위협탐지 이벤트 발생 현황을 텍스트 형식으로 표시하였다.

셋째, 금일 출발지 IP Top 5 현황이다. 오늘 00시부터 현재시간까지 IPS에서 탐지 또는 차단한 출발지 IP Top 5 현황을 텍스트 형식으로 표시하였다.

넷째, 금일 목적지 IP Top 5 현황이다. 오늘 00시부터 현재시간까지 IPS에서 탐지 또는 차단한 목적지 IP Top 5 현황을 텍스트 형식으로 표시하였다.

다섯째, 금일 출발지 국가 Top 5 현황이다. 오늘 00시부터 현재시간까지 IPS에서 탐지 또는 차단한 출발지 국가 Top 5 현황을 Pie 그래프 형식으로 표시하였다.

여섯째, 금일 출발지 포트 Top 5 현황이다. 오늘 00시부터 현재시간까지 IPS에서 탐지 또는 차단한 출발지 포트 Top 5 현황을 일반 그래프 형식으로 표시하였다.

일곱째, 금일 목적지 포트 Top 5 현황이다. 오늘 00시부터 현재시간까지 IPS에서 탐지 또는 차단한 목적지 포트 Top 5 현황을 일반 그래프 형식으로 표시하였다.

여덟째, 금일 이벤트 발생장비 Top 5 현황이다. 오늘 00시부터 현재시간까지 각 IPS에서 탐지 또는 차단한 장비중 이벤트 발생이 가장 많은 IPS 장비 Top 5 현황을 일반 그래프 형식으로 표시하였다.

아홉째, 금일 IPS 장비별 허용 이벤트 발생장비 Top 5 현황이다. 오늘 00시부터 현재시간까지 각 IPS에서 탐지 또는 차단한 장비중 허용 이벤트 발생이 가장 많은 IPS 장비 Top 5 현황을 텍스트 형식으로 표시하였다.

열번째, 금일 IPS 장비별 차단 이벤트 발생장비 Top 5 현황이다. 오늘 00시부터 현재시간까지 각 IPS에서 탐지 또는 차단한 장비 중 차단 이벤트 발생이 가장 많은 IPS 장비 Top 5 현황을 텍스트 형식으로 표시하였다.

열한번째, 금일 IPS 탐지명 Top 5 현황이다. 오늘 00시부터 현재시간까지 각 IPS에서 탐지 또는 차단한 이벤트 중 Top 5 현황을 텍스트 형식으로 표시하였다.

열두번째, 금일 IPS 탐지명 최근 Top 30 현황이다. 각 IPS에서 탐지 또는 차단한 최근 이벤트 30건에 대한 상세 탐지현황을 텍스트 형식으로 표시하였다.

기존 대시보드의 표출항목은 1개 화면으로 구성되어 역동성이 결여되어 있다. 표출하는 내용도 웹서비스에 대한 위협에 한정되어 보안관제의 모든 활동들을 표현하기에 부족한 것으로 분석된다.

3.2 보안관제 주요 업무 화면 분석

실제 보안관제 근무자들이 많이 보는 화면들과 평균적인 업무활용 비율을 조사하였다. 사례기관의 보안관제센터에 실제 근무하는 보안관제 근무요원들을 대상으로 진행하였다. 보안관제 근무요원들에게 실제 근무시 주로 이용하는 화면 명칭과 평균적인 이용비율을 조사하였다. 조사결과 총 12개의 화면을 주로 이용하고 있는 것으로 분석되었다. 12개의 화면을 상세히 살펴보면 다음과 같다.

첫째, 통합보안관제시스템[ESM] 실시간 이벤트 분석화면이다. 평균적인 이용율은 30%로 분석되었다. 각종 보안장비(IPS, DDoS, FW 등)에서 발생되는 이벤트들을 ESM에서 수집하는데 웹서비스들을 대상으로 유입되는 사이버 위협들을 실시간으로 분석하는 경우에 이용한다.

둘째, 악성메일 분석화면이다. 평균적인 이용율은 13%로 분석되었다. 외부로부터 유입되는 모든 메일에 대한 악성 메일 여부를 확인하고 악성 첨부파일이 있는 경우 악성 IP/URL 등의 위협정보를 분석한다. 악성메일에 의해 유입되는 사이버 위협을 탐지 차단하는 장비이다.

셋째, Spam메일 대응 화면이다. 평균적인 이용율은 12%로 분석되었다. 외부로부터 유입되는 메일을 사전에 정해진 패턴으로 검사하여 스팸메일을 차단하는 화면이다. 악성메일에 의해 유입되는

사이버 위협들을 탐지하는 장비이다.

넷째, IPS장비 화면이다. 평균적인 이용율은 11%로 분석되었다. 내부 또는 외부에서 발생 또는 유입되는 트래픽들을 사전에 정해진 패턴 룰을 이용하여 탐지 차단하는 장비이다. 웹서비스 위협에 대응하는 장비이다.

다섯째, IDS장비 화면이다. 평균적인 이용율은 10%로 분석되었다. 내부 또는 외부에서 발생 또는 유입되는 트래픽들을 사전에 정해진 패턴 룰로 공격 여부를 판단 및 탐지하는 화면이다.

여섯째, 통합보안관제시스템[ESM] 검색 화면이다. 평균적인 이용율은 7%로 분석되었다. 각종 보안장비(IPS, DDoS, FW)로부터 수집된 이벤트들을 통합적으로 검색하는 화면이다. 웹서비스들을 대상으로 유입되는 사이버 위협들을 탐지하기 위한 화면으로 구분할 수 있다.

일곱째, IPS종합화면이다. 평균적인 이용율은 5%로 분석되었다. 개별 IPS장비에서 발생되는 IPS 탐지·차단 이벤트들을 종합 분석하는 경우에 사용하는 화면이다. 웹서비스들을 대상으로 유입되는 사이버 위협들을 탐지하기 위한 화면이다.

여덟째, 웹페이지 장애여부 탐지화면이다. 평균적인 이용율은 3%로 분석되었다. 사이버 위협에 의한 위조, 변조 등의 행위여부에 대한 모니터링이 필요한 홈페이지들을 사전에 등록한 후 서비스의 장애 여부, 위변조 여부 등을 확인하기 위해 사용하는 화면이다. 웹페이지의 장애 여부를 확인하는 화면으로 구분할 수 있다.

아홉째, 방화벽 장비 화면이다. 평균적인 이용율은 4%로 분석되었다. 내·외부에서 유입되는 트래픽에 대하여 사전에 정해진 룰에 의해 허용·차단 등을 설정하고 확인하기 위한 화면이다. 사이버 위협을 발생시키는 악성 IP를 등록하는 화면으로 구분할 수 있다.

열 번째, 유해사이트 대응화면이다. 평균적인 이용율은 2%로 분석되었다. 악성 페이지에 의한 위협을 차단하기 위해 유해한 것으로 식별된 URL을 등록하여 차단하는 경우에 사용하는 화면이다. 악성 페이지에 의해 유입되는 사이버 위협을 차단하는 화면으로 구분할 수 있다.

열한번째, 바이러스 대응 화면이다. 평균적인 이용율은 1%로 분석되었다. 바이러스, 랜섬웨어 감염 등 악성코드 감염에 대한 이력을 확인하고 유사시 PC에 대한 원격 지원을 위한 화면이다. 내부로 유입된 사이버 위협들을 탐지 대응하기 위한 화면으로 구분할 수 있다.

열두번째, 통합보안관제시스템(ESM) 상관분석 화면이다. 평균적인 이용율은 2%로 분석되었다. 시스템 리소스, 보안장비 로그 미수집 등 연결된 모든 장비에 대한 정보를 분석하여 상세한 경보를 생성할 수 있는 화면이다.

<표 1>과 같이 보안관제 근무자들이 자주 보는 화면에 대한 조사를 통해 보안관제센터의 업무처리를 위해 다양한 보안장비화면들이 활용되고 있음을 확인할 수 있다.

<표 1> Security equipment usage

No	Item	Details
1	ESM real time monitor	30%
2	Anti_Email APT	13%
3	Anti_SPAM Email	12%
4	Intrusion Prevention System	11%
5	Intrusion Detection System	10%
6	ESM log Serch system	7%
7	Intrusion Prevention System Analysis	5%
8	Web Page monitoring System	3%
9	Firewall System	4%
10	Anti-Bad website System	2%
11	Anti-Virus System	1%
12	ESM log High level Serch system	2%

4. BDR 기반 보안관제 대시보드 구축

4.1 BDR(Blockade-Detection-Response)

사이버보안 활동의 핵심은 봉쇄(Blockade)이다. 봉쇄는 '사이버 위협의 유입경로 구간에서 사이버 위협의 유입을 제한하기 위한 활동'이다. 정보보안 활동은 수많은 보안장비들에 봉쇄정책을 등록하는 것으로부터 시작된다. 사이버 위협이 유입되는 경로에는 이미 사이버 위협을 차단하기 위해 방화

벽, IPS, Anti-DDoS 등 수 많은 봉쇄를 위한 보안장비들이 운영되고 있다.

탐지(Detection)는 '사이버 위협을 직접적으로 색출하는 활동'을 의미한다. 봉쇄는 차단 정책에 의해 진행되는 기계적인 과정인 반면, 탐지는 보안관제 분석요원, 바이러스 전문가 등 숙련된 전문가가 수행하는 과정이다. 고위험도의 이벤트인지, 저위험도의 이벤트인지 등을 판단하고 악성행위를 발생시키는 악성 IP를 추출하는 과정 등이 탐지 활동에 해당된다. 이 밖에 전 직원들의 PC에 Antivirus, EDR 등의 제품을 설치하여 운영하는 것도 탐지 활동에 해당된다.

대응(Response)은 '발생된 사이버 위협에 대한 대응활동'이다. 대응 활동에는 사이버 위협이 다시 발생되지 않도록 악성IP 보안장비 등록, 바이러스 치료, 삭제, 악성행위 시도의 제한 등의 활동이 포함된다. 또한 조직내의 구성원들이 정보보안의 목표와 정책들을 충분히 이해할 수 있도록 사이버 위협 사례 등을 교육하는 활동들도 포함된다. 사이버 보안은 완벽할 수 없기 때문에 구성원들의 적극적인 동참이 반드시 필요하다.

4.2 BDR 기반 보안관제 대시보드

BDR기반 보안관제 대시보드는 사이버 위협의 유입경로별 봉쇄, 탐지, 대응에 대한 종합적인 현황파악과 관리를 용이하게 한다. 다양한 보안장비들로부터 탐지되는 다량의 보안로그들을 분석하여 각각의 보안장비들이 기계적으로 탐지 차단하고 추가적으로 보안관제 요원에 의한 보안관제 경험 기반의 악성 IP, URL 등에 대한 수동 차단까지 시각적으로 파악할 수 있도록 한다. BDR 기반 보안관제 대시보드는 3개의 화면으로 구성한다: BDR 종합화면, Detection 현황, Response 현황.

4.2.1 BDR 주요 현황

BDR 주요 현황화면에서는 5개의 분석내용을 표출한다: Blockade ratios by Threat Gates, Blockade status by security systems, SIEM security events detection by hours, Total Response Status, Response by Frontier Systems.

Blockade ratios by Threat Gates는 유입경로별 봉쇄 비율을 나타내며 사이버 위협이 유입경로별로 어느 정도 수준으로 봉쇄되고 있는지 표출한다. 오픈된 웹서비스에 의한 위협으로 발생하는 위험을 봉쇄하는 봉쇄율은 기관의 웹서비스 중 해외로부터의 접근을 허용하고 있는 웹서비스의 비율이 어느 정도인가로 결정할 수 있다. 악성메일에 의한 위협으로 발생하는 위험을 봉쇄하는 봉쇄율은 기관의 악성 메일 모의훈련 중 모의 악성메일 열람자의 비율이 어느 정도인가로 결정할 수 있다. 악성 웹페이지에 의한 위협으로 발생하는 위험을 봉쇄하는 봉쇄율은 기관의 악성 웹페이지 위협 감염자의 비율이 어느 정도인가로 결정할 수 있다. 악성 저장매체에 의한 위협으로 발생하는 위험을 봉쇄하는 봉쇄율은 기관의 외부저장매체 허용 비율이 어느 정도인가로 결정할 수 있다[16].

Blockade status by security systems는 보안장비들에 의한 봉쇄현황을 나타내며 각 보안장비들에 의한 기계적 봉쇄현황을 표현한다. 각 보안장비들에 의한 대응현황을 각 유입경로별로 구분하여 어느 유입경로에서 얼마나 많은 대응을 하고 있는지 파악할 수 있도록 한다.

SIEM(Security Information and Event Management) security events detection by hours는 SIEM장비가 분석하는 위협 이벤트들의 탐지 현황을 시간대별로 표출한다. SIEM장비는 각 보안장비들이 발생시키는 원본 로그 이벤트들을 종합적으로 분석하여 관제요원들의 업무활동을 지원하게 된다.

Total Response Status는 종합 대응현황을 표시하며 각 보안장비들의 기계적인 대응과 관제요원들에 의한 대응을 모두 종합하여 표출한다. 종합 대응현황을 통해 보안장비들이 탐지하는 위협이벤트들을 어떻게 대응하고 있는지 종합적으로 파악할 수 있다.

Response by Frontier Systems는 경계선 보안장비 위협 대응 현황을 나타내며 경계선에 배치되어

있는 Anti-DDoS장비와 Firewall 2개 장비에 의한 대응현황을 세부적으로 표출한다. 이 화면을 통해 각 경계선 보안장비들이 어느 방향에서 어느 수준으로 대응을 하고 있는지 파악할 수 있다. 각 장비별로 6개 방향의 대응현황을 표출한다: Out-In Detection, Out-In Blocking, In-Out Detection, In-Out Blocking, In-In Detection, In-In Blocking.

4.2.2 Detection 현황

Detection 현황 화면에서는 6개의 내용을 표출한다: Top 5 Nations, Top 5 cyber attack patterns, Top 5 attacked Ports, Types of attack events, attack flow from nations to web systems, Risk ratios by web systems.

Top 5 Nations은 공격국가 순위 Top5를 나타내며 가장 공격량이 많은 5개 국가의 공격량과 최근 추이를 공격국가 Top 5라는 항목으로 표출한다. 이 화면을 통해 어떤 국가로부터의 공격이 얼마만큼 유입되고 있는지 파악할 수 있다.

Top 5 cyber attack patterns은 사이버 공격 패턴 Top 5를 나타내며, 가장 공격량이 많은 공격 유형 5개를 최근 추세와 함께 표출한다. 유입되는 공격이벤트 중 가장 많은 건수의 공격유형을 파악할 수 있도록 한다.

Top 5 attacked Ports는 공격 발생 Top 5를 나타내며 가장 공격이 많이 발생하는 포트 5개를 보여준다.

Types of attack events는 공격이벤트 유형현황을 나타내며 모든 위협이벤트들의 유형을 크게 information gathering, web vulnerability and denial of service로 구분하여 각 유형의 비율을 표출한다. 이 화면을 통해 저 위험도 위협 이벤트인 information gathering 이벤트들을 제외한 고위험도 위협 이벤트들의 비율을 파악할 수 있다.

Attack flow from nations to web systems는 공격 흐름도를 나타내며 어느 국가로부터 어떤 형태의 위협 이벤트들이 발생되어 어떤 정보시스템으로 유입을 시도하는지를 파악할 수 있도록 도와준다.

Risk ratios by web systems는 웹기반 정보시스템별 위험 노출비율을 나타내며 각 정보시스템별로 사이버 위협에 노출되어 있는 수준을 표출한다. 정보시스템별로 위협이벤트들이 어느 정도 유입되는지에 대해 파악하므로서 효율적인 보안관제 활동을 가능하게 한다.

4.2.3 Response 현황

Response 현황은 8개의 내용을 표출한다: Total Threat events, Alert events by SIEM, Response by Experts, Bad IP nation analysis, Security system connection link, IPS blocking by network, Response status by networks, Real time Top 5 SIEM Security events analysis.

Total Threat events는 위협 이벤트 종합현황을 나타내며 4개의 분석정보를 표출한다: 모든 보안장비들이 대응하고 있는 위협 이벤트들의 총 발생량과 발생건수, SIEM장비에서 빅데이터 분석한 총 데이터량, SIEM장비가 분석한 BigData 건수, 외부기관으로부터 수집한 외부 위협정보를 표출한다. 이 화면을 통해 보안관제센터가 대응해야 하는 모든 이벤트들이 어느 정도 규모에 해당되는지를 파악할 수 있다.

Alert events by SIEM는 SIEM장비 경보 이벤트를 나타내며 4개의 분석정보를 표출한다. 4개는 분석정보는 SIEM장비에 의해 경보되는 시간대별 위협이벤트 총 발생건수, 주요 위협이벤트 1위와 2위의 발생건수와 나머지 위협이벤트의 발생건수로 구분하여 표출한다. 이러한 정보를 통해 SIEM장비가 대응하는 시간대별 보안이벤트들의 주요 이벤트 내용을 쉽게 파악할 수 있다.

Response by Experts는 관제요원 대응현황을 나타내며 각 유입경로별로 관제요원이 보안장비에 각 위협정보를 등록하므로서 추가적인 사이버 위협의 발생을 봉쇄하는 현황을 표시한다. 관제요원들에 의한 봉쇄는 보안장비들에 의해서 기계적으로 대응하기 어려운 위협들에 대한 경험기반의 사

이버 위협 봉쇄라고 표현할 수 있다.

Bad IP nation analysis는 악성 IP 발생국가 현황을 나타내며 악성 IP를 발생시키는 국가를 발생건수와 비율로 표출한다. 어느 국가에서의 공격이 가장 많이 유입되는지를 분석하는데 유용하게 활용될 수 있다.

Security system connection link는 보안장비 연결링크를 나타내며 신속한 위협이벤트 대응을 위해 각 네트워크별로 운영하고 있는 보안장비들로 이동할 수 있는 연결링크를 모아 놓은 화면이다. 이러한 연결링크를 통해 각 보안장비로 신속히 이동하여 대응할 수 있다.

IPS blocking by networks는 네트워크별 IPS 장비 봉쇄현황을 나타내며 IPS가 룰기반으로 대응하고 있는 보안이벤트들의 총 발생량을 월별로 표출한다. 이 화면을 통해 월별 IPS 대응량의 변화를 파악할 수 있다.

Response status by networks는 네트워크별 대응현황을 나타내며, 네트워크별로 대응하고 있는 위협이벤트 발생량을 탐지와 차단 기준으로 표출한다. 각 기관이 운영하고 있는 네트워크 중 어느 네트워크로 사이버 위협 이벤트가 유입되는지 판단할 수 있다.

Real time Top 5 SIEM Security events analysis는 실시간 Top 5 SIEM 보안 이벤트 분석을 나타내며 SIEM장비에서 발생되는 실시간 위협이벤트들 중 Top 5를 상세히 표출한다. 각 이벤트 내용을 클릭하면 더욱 상세한 분석화면으로 이동하여 세밀한 대응활동을 가능하게 한다.

5. 결 론

기존에 통합보안관제솔루션에 기본적으로 탑재되어 운영되는 대시보드 화면들은 보안관제센터가 수행하는 모든 업무활동들을 포함하지 못하고 있다. 대부분의 보안관제 대시보드 화면들은 웹서비스를 통해 유입되는 사이버 위협에 대한 탐지와 분석에 초점이 맞추어져 있다.

그러나, 실제 보안관제센터에서는 웹서비스로 유입되는 사이버 위협 이외에도 악성메일에 의해 유입되는 사이버 위협, 악성페이지에 의해 유입되는 사이버 위협, 악성 매체에 의해 유입되는 사이버 위협과 같은 모든 유형의 사이버 위협을 탐지하고 대응하고 있다. 실제 수행하는 업무활동과 대시보드의 표출항목이 서로 간에 상당한 차이가 존재하는 것이다.

보안관제센터의 대시보드가 진정한 의미에서 사이버 위협 탐지 대응활동의 관문역할을 수행하기 위해서는 현재의 대시보드 표출항목들은 상당한 부분에서 개선되어야 한다. 대시보드 표준모델은 보안관제센터의 사이버 위협 탐지 대응활동을 효과적으로 지원하기 위하여 크게 3가지 방향으로 개선되어야 한다.

첫째, 종합성이다. 보안관제센터에서 수행하는 업무활동들을 모두 표출하는 방향으로 보안관제센터의 대시보드가 구성되어야 한다는 것이다. 현재의 대시보드는 웹서비스로 유입되는 사이버 위협에 초점을 맞추어 구성되어 있다. 그러나 현재의 보안관제센터는 악성메일에 의한 위협, 악성페이지에 의한 위협, 악성 매체에 의한 위협에 대해서도 사이버 위협 대응활동을 수행하고 있는 상황이다. 따라서 보안관제센터의 대시보드는 이러한 모든 대응활동들을 종합적으로 표출시켜서 체계적으로 구성해야 할 것이다.

둘째, 활용성이다. 현재의 대시보드는 24시간 365일 중 몇 시간 정도 밖에 방문하지 않는 귀빈들을 위해 전시용으로 구성되어 있다. 당연하게도 전시용으로 구성되어 있는 대시보드에 대한 활용성은 거의 전무한 실정이다. 대시보드의 주인은 보안관제센터 근무자들이어야 한다. 보안관제센터 근무자들이 가장 많이 보는 화면들이 표출되어 있어야 한다.

셋째, 용이성이다. 보안관제센터 근무자를 처음 시작하게 되더라도 보안관제센터의 표준 대시보드 화면 구성들을 따라 가다 보면 무엇을 중점적으로 봐야 하는지 쉽게 확인할 수 있어야 한다. 보안관제센터가 어떤 위협으로부터 어떻게 탐지하고 어

떻게 대응하는지에 대해서 쉽게 파악할 수 있어야 할 것이다.

이러한 관점에서, 본 논문에서 제안하는 BDR 기반 보안관제 대시보드 설계방향은 보안관제센터의 대시보드 표준으로 활용될 수 있을 것이다. BDR 기반 보안관제 대시보드를 통해 보안관제센터의 업무들을 종합적으로 표출하고, 활용성과 용이성이 극대화 될 수 있을 것이다.

참고문헌

[1] Sitaram Kowtha, Laura A. Nolan, Rosemary A. Daley, 'Cyber Security Operation Center Characterization Model and Analysis', Johns Hopkins University, Applied Physics Laboratory, 978-1-4673-2709-1/12, IEEE, 2012.

[2] Eui-yeon Jung , 'A Study on the Integrated Security Monitoring &Control in Financial Investment Industry Computer Networks', Korea Information Processing Society, 19-2, Feb, 2012.

[3] Gil Sun, Yu, 'A Study on the Cyber Security monitoring Detection and Response', Department of Digital Forensics, The Graduate School of Hanseo University, August, 2018.

[4] Cyril Onwobiko, 'CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process', Intelligence & Security Assurance, E-Security Group, London, UK. 2018.

[5] Natalia Miloslavskaya, 'Network Security Intelligence Center as a combination of SIC and NOC', National Research Nuclear University MEPhI, 1877-0509/2018 Elsevier.

[6] Rasim Alguliyev, Yadigar Imamverdiyev, Lyudmila sukhostat, 'Cyber-physical systems and their security issues', Institute of Information Technology, Azerbaijan National Academy of Sciences, 0166-3615/2018 Elsevier.

[7] Tae-Woong Seo, 'An Analysis of Vulnerabilities and Performance on the CCTV Security Monitoring and Control', Journal of Multimedia, 15(1), Jan, 2012.

[8] Kim, MinJun, 'A study on the implementation of white-list intrusion detection system on control networks', Department of Industry Security, Graduate School, Kyonggi Univ, Jun, 2011.

[9] Jin_Young Jung, 'Security Management Automation Method Using Artificial Intelligence in Financial Sector', KonKuk Univ, Master's Thesis, Feb, 2018.

[10] Charles Feng, Shuning Wu, Ningwei Liw, 'A User- Centric Machine Learning Framework for Cyber Security Operation Center', ZhonDu Tecnologies, Symantec Corporation, 978-1-5090-6727/17, IEEE, 2017.

[11] Hanbitmedia, "Network security system construction and security control",2016, pp. 38-42

[12] Infothebooks, "Security Control Practice Guide for Nurturing Next-Generation Information Security Talents", 2017, pp. 45-48.

[13] Jeon Sang June, "Design and Evaluation Security Control Iconology for Big Data Processing", JOURNAL OF PLATFORM TECHNOLOGY, 2020.12, pp. 38-46.

[14] Suk-woo Hyun, "A Study of Effectiveness of the Improved Security Operation Model Based on Vulnerability Database", Korea Institute Of Information Security And Cryptology, 2019.10, 1167-1177(11 pages)

[15] Woo-Jin Jo, "A log visualization method for network security monitoring", Korean Institute Of Smart Media, 2018, 70 - 78 (9 pages)

[16] Han ChoongHee, 'A study for Information Security Risk Assessment Methodology Improvement by blockade and security system level assessment ', Korea Information Assurance Society, vol 20-4, pp.187-196, Oct, 2020.

[저 자 소 개]

한 충 희 (Han Choong-Hee)
1996년 2월 동국대 컴퓨터공학 학사
2002년 2월 동국대 정보보호학 석사
2019년 8월 전남대 정보보호학 박사
email : justicehan@kpx.or.kr