제어시스템의 내부자 위협 탐지를 위한 Event Log 타당성 및 중요도 분석에 관한 연구★

김종민*, 김동민**, 이동휘**

요 약

제어시스템은 공공 네트워크와의 통신망 융합에 따라 다양한 루트를 통해 정보유출 및 변조 등의 위협이 제어시스템에서도 그대로 나타날 수 있다. 최근 다양한 보안에 대한 이슈와 새로운 공격기법에 의한 침해 사례가 다변화됨에 따라서, 단순히 차단 및 확인 등의 학습을 통해 정보를 데이터베이스화하는 보안 시스템으로는 새로운 형태의 위협에는 대처하기 힘들어지고 있다. 현재 제어시스템에서는 이처럼 외부에서 내부로의 위협에 치중하여 보안 시스템을 운용하고 있으며, 보안 접근 권한을 가진 내부자에 의한 보안위협 탐지에 대해서는 미비한 실정이다. 이에 따라 본 연구에서는 NSA에서 발표한 “Spotting the Adversary with Windows Event Log Monitoring”의 주요 Event Log 목록을 토대로 중요도 분석을 실시하였다. 그 결과 제어시스템에 내부자 위협탐지를 위한 Event Log의 중요도 여부를 알 수 있었으며, 분석결과를 바탕으로 이 분야의 연구에 기여할 수 있을 것으로 판단된다.

A Study on the Analysis of Validity and Importance of Event Log for the Detection of Insider Threats to Control System

Jongmin Kim*, DongMin Kim**, DongHwi Lee***

ABSTRACT

With the convergence of communications network between control system and public network, such threats like information leakage/falsification could be fully shown in control system through diverse routes. Due to the recent diversification of security issues and violation cases of new attack techniques, the security system based on the information database that simply blocks and identifies, is not good enough to cope with the new types of threat. The current control system operates its security system focusing on the outside threats to the inside, and it is insufficient to detect the security threats by insiders with the authority of security access. Thus, this study conducted the importance analysis based on the main event log list of “Spotting the Adversary with Windows Event Log Monitoring” announced by NSA. In the results, the matter of importance of event log for the detection of insider threats to control system was understood, and the results of this study could be contributing to researches in this area.

Key words : Information Security, Event Log, Log Analysis, Correlation Analysis, Control System

접수일(2018년 09월 6일), 수정일(1차: 2018년 09월 23일), 게재확정일(2018년 09월 29일)

★ 본 연구는 한국전력공사의 2018년 선정 기초연구개발과제 연구비에 의해 지원되었음 (과제번호 : R18XA06-43)

* 경기대학교 융합보안학과

** 동신대학교 에너지융합대학 전기공학부

*** 동신대학교 에너지융합대학 에너지응용학부 (교신저자)

1. 서 론

제어시스템은 일반적으로 독립 폐쇄망으로 구성으로 구축되어 있으나 최근에는 업무상 편의성 및 대외기관과의 협력이 증가됨에 따라 범용 프로토콜과 Windows 기반의 운영체제를 이용한 제어시스템 도입 비율이 높아지고 있다[1][2]. Windows 운영체제의 도입 증가로 인해 해당 운영체제의 보안패치 및 제어시스템 패치를 위해 내부 관리자 계정을 이용해 작업을 하는 사례들이 빈번하게 이루어지면서 제어시스템 내부위협이 새로운 노출요소가 되고 있다.

이렇게 위협에 대한 환경이 변화하고 있지만 제어시스템 보안위협은 방화벽, 백신시스템, IPS, PMS 등을 시설하여 운용하여 외부에서 내부 위협에 치중해 치중하여 Windows OS를 기반으로한 제어시스템에서 필연적으로 해야 하는 보안패치 및 응용프로그램의 업데이트 작업들로 인한 내부 보안위협에 대한 방안은 미비한 실정이다.

따라서 본 연구에서 앞서 신뢰성 있는 분석을 위해 NSA에서 발표한 “Spotting the Adversary with Windows Event Log Monitoring”의 주요 Event Log를 사용하였으며, Windows 운영체제를 기반으로한 제어시스템에서 내부자 보안위협 탐지에 적용 가능한 Event Log를 선정하고, 계층분석방법을 이용해 Event Log별 상대적 중요도를 연구하려한다.

2. 관련 연구

2.1 제어시스템 보안위협 연구

제어시스템의 위협탐지시스템과 관련된 대표적인 연구들을 살펴보면 다음과 같은 것들이 있다.

2006년 발표된 ‘Using Model-based Intrusion Detection for SCADA Networks’논문에서는 다음과 같이 Modbus TCP 네트워크에서의 3가지의 Model-based 이상징후탐지 기법을 제시하고 있는데, 구체적으로 살펴보면 ① Protocol-level Model, ② Communication Pattern Model, ③ Learning-based Model이다. 이들은 미국 SNL(Sandia National Laboratories)의 SCADA Test bed에서 제안된 모델의 기법을 실험하였으며, 그 결과로 Model-based 기법이 SCADA 네트워크에서 효율적임을 밝혔다. 첫째 Protocol-level Model에서는 Modbus 장치 별로 사용 가능한 Function Code 집합을 규정하고, Modbus 프로토콜 specification에 기반 해서 Cross-field 관계를 가지는 규칙을 규정하였다. 둘째로 Communication Pattern Model에서는 IP 주소, TCP 포트 번호에 기반해서 연결 가능한 통신 집합을 규정하였고, 셋째로 Learning-based Model 에서는 Modbus Function Codes를 이용해 Bayesian Network를 구성하고, 조건 확률 관계를 이용해 이상 징후를 탐지하였다[3].

2009년 발표된 “Communication Pattern Anomaly Detection in Process Control Systems”논문에서는 2가지의 이상징후탐지 기법 즉 ① Pattern-based Anomaly Detection과 ② Flow-based Anomaly Detection 기법을 제시하였다. 첫째 Pattern-based Anomaly Detection은 기존의 pattern anomaly detection 기법으로 송・수신 IP 주소, Port 번호를 기반으로 생성된 pattern을 이용하였다. 둘째로 Flow-based Anomaly Detection기법은 Flow 별로 특정시간 간격사이에서 패킷의 평균 바이트 크기와 평균 inter-arrival 시간을 측정한 후, 이미 만들어진 정상 모델과 비교하여 이상징후를 탐지하였다[4].

2012년 발표된 “Bloom Filter Based Intrusion Detection For Smart Grid SCADA” 논문에서는 Modbus Function Codes 및 Data Sequences를 바탕으로 Bloom Filter를 적용해 이상징후를 탐지한 HIDS(Host based Intrusion Detection System)을 제안하였으며, 변전소자동화시스템들의 성능 문제를 고려해 메모리 공간과 탐지 수행 속도를 단축하였다. 이들은 제어시스템 운영 상태에 따라 다른 모델을 적용해야 한다고 주장하였다. 하지만 위 연구에서 Training Set에 존재하지 않는 Test 샘플에 대해서는 탐지가 어려운 단점이 존재한다는 사실을 알아냈는데, 이 단점은 모든 정상행위를 포함하는 ‘화이트리스트’를 규정

하여 사용할 때, 메모리와 속도 측면에서 효율성 확보가 가능해진다는 사실을 연구를 통하여 알게 되었다[5].

2001년 Network Security for Substation Automation 논문에서는 자동화 변전소의 취약성과 위협 공격 가능 시나리오에 대하여 4가지 공격유형을 제시하고 있는데 ①인증된 발신지와 수신지 사이의 제어명령 메시지가 전송과정에서 변조되는 경우인 메시지 위·변조(Message Modification)공격 그 리고 ②공격자에 의해 새로운 제어명령을 내리거나 인증된 발신자로부터 보내진 제어명령을 공격자가 중간에 탈취해 공격하는 Replay attack ③공격자가 패킷을 가로채 의도적으로 누락시킬 수 있는 Message Injection & Replay 공격, 그리고 ④자동화변전소용 스위치, 라우터 등 네트워크 장치를 조작하여 악성 코드로 특정 메시지를 누락(drop)시키거나 메시지를 의도적으로 전송이 불가능하도록 만드는 공격유형을 제시하고 있다. 이러한 전력설비 위협에 대응할 수 있도록 IEC 62351에서는 메시지의 무결성 보장과 암호화 보안 정책을 제시하고 있다. 특히 Goose 메시지는 IEC 61850 통신서비스 일종으로서 각 보호 IED 상호 간에 Trip, Interlocking, Status 등 알람, 상태 및 제어와 관련된 주요 정보 들을 Multicast 방식으로 전달하는 등 전력설비의 보호에 사용되며, 또한 SV(Sampled Value) 메시지는 전류나 전압과 같은 측정값 리포팅 서비스를 위해 사용한다. 하지만 IEC 61850 1st Ed 표준에서는 통신서비스와 데이터에 대한 객체 모델만 제시하고 있을 뿐 네트워크와 지능형 전력설비(IED)에서 제공해야할 보안 대책에 대해서는 다루지 않고 있으며, 최근 발표된 IEC 61850 두 번째 버전인 2nd edition에서는 지능형 전력설비(IED)의 로그 정보를 제 공할 수 있는 LN(Logical Node)인 GSAL, GLOG 기능 정도만 추가 되어져 있다[6].

<표 1> 위협 식별 및 보안 메커니즘

Layer	Attack	Security Mechanisms
Data	Data destruction	Backup procedure
Node	Access to node to gain confidential information	Access Control Encryption Authentication Integrity checking Intrusion detection
	False command	Authentication Integrity checking
	Using a node for a DoS attack	Access control Authentication Integrity checking Intrusion detection
	Dos attack on a critical node	Access control Authentication Integrity checking Intrusion detection Redundancy
	False command	Authentication Integrity checking

2012년 발표된 논문인 Exploiting the GOOSE protocol:A practical attack on cyber-infrastructure에 따르면 IEC 62351에서 권고하는 Goose의 보안 요구사항은 암호화 및 디지털서명을 통한 메시지 인증을 권고하고 있지만, 현재까지는 낮은 사양의 임베디드 IED 시스템으로 인하여 암호화나 메시지 인증을 위한 디지털서명 생성 및 검증 소요시간(tb)이 최소 8.3ms로 앞서 IEC 61850에서 요구한 통신 지연시간(latency, ta+tb+tc) 4ms 를 만족할 수 없음을 검증하였다[7].

지금까지 발표된 제어시스템에서의 위협탐지 방법론에 대한 논문들을 살펴보면 침입탐지 알고리즘과 인덱스 기반의 Function 코드에 대한 가능성을 소개하고 있으며, 내부자에 의한 보안위협 탐지에 대해서는 제시되지 못하고 있다. 따라서 본 연구에서는 제어시스템의 내부자 위협탐지를 위해 NSA에서 발표한 “Spotting the Adversary

with Windows Event Log Monitoring"의 주요 Event Log 목록을 토대로 타당성 분석 및 일관성 분석을 통하여 제어시스템에 적합한 Event Log를 제시하고자 한다.

2.2 Windows Event Log

Windows 시스템은 Application Log, Security Log, System Log와 같이 세 가지 로그를 이벤트에 기록하며, OS 구성에 따라 Directory Service Log, File Replication Service Log, DNS Server Log가 추가될 수가 있다[4]. 주요 이벤트 별 특징은 <표 2>과 같다.

<표 2> 윈도우 시스템 Event Log 종류[8]

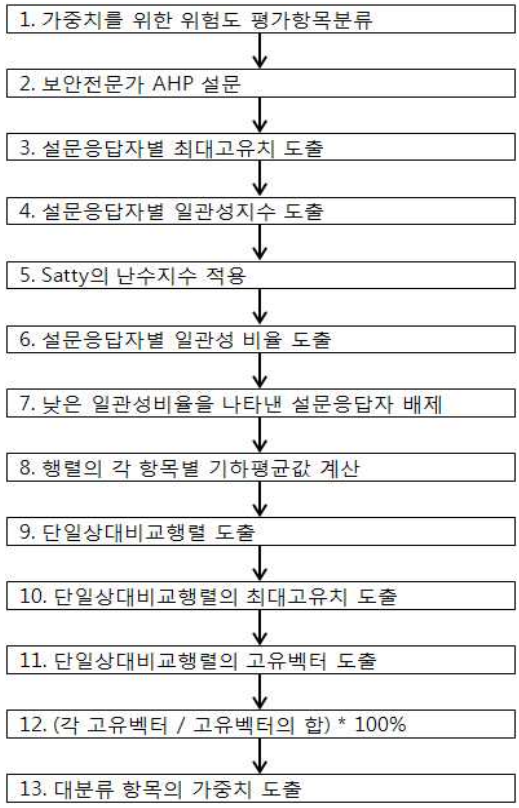
Event Log	설명
Application	응용 프로그램이 기록한 다양한 이벤트가 저장되며, 기록되는 이벤트는 해당 제품의 개발자에 의해 결정된다. ex) 안티바이러스 제품의 경우 악성코드 탐지 및 업데이트를 기록한다. 일반 응용프로그램의 경우 활성화 여부와 성공 여부 등에 대한 정보를 기록한다.
Security	유효하거나 유효하지 않은 로그온 시도 및 파일 생성, 열람, 삭제 등의 리소스 사용에 관련된 이벤트를 기록한다. 감사로그 설정을 통해 다양한 보안 이벤트 저장이 가능하다.
System	Windows 시스템 구성요소가 기록하는 이벤트로 시스템 부팅 시 드라이버가 로드 되지 않는 경우와 같이 구성요소의 오류를 이벤트에 기록한다.

3. 제안하는 방법

본 연구에서 제어시스템의 내부자 위협 탐지를 위한 Event Log 중요도 분석을 하기 위해 NSA의 "Spotting the Adversary with Windows Event Log Monitoring"을 토대로 가치 평가, 선택의 문제의 고민을 해결하기 위한 AHP 방법을 이용하였다. 본 연구를 위해 보안 전문가들을 대상으로 설문하였으며, 설문을 분석하여 평가요소들을 계층화 하였다.

3.1 연구 분석 과정

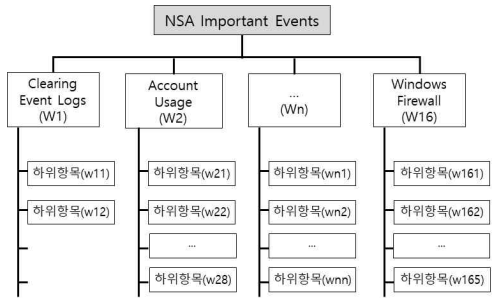
(그림 1)은 본 연구의 검증과정을 나타낸 것이다.



(그림 1) AHP 검증과정

3.2 연구 분석 계층 구조

계층분석(AHP)을 하기 위해서는 항목 설정이 중요하다. (그림2)는 내부자 위협에 대한 Event Log 중요도를 구하기 위한 계층구조도이다. 최상위 단계 평가요소는 NSA 16개의 이벤트 카테고리로 나누어져 있으며, 상위단계 각 요소에 종속된 하위 항목들이 있다.



(그림 1) 분석모형

<표 3>은 NSA의 “Spotting the Adversary with Windows Event Log Monitoring”을 토대로 주요 이벤트를 목록화 하여 16개의 카테고리로 나타낸 것이다.

<표 3> 최상위 항목 요소[9]

카테고리			
Clearing Event Logs	Account Usage	Remote Desktop Logon Detection	Windows Defender Activities
Application Crashes	Software & Service Installation	External Media Detection	Pass the Hash Detection
AppLocker	System or Service Failures	Windows Update Errors	Kernel Driver Signing
Group Policy Errors	Mobile Device Activities	Printing Services	Windows Firewall

<표 4>는 상위 단계의 종속된 하위항목에 대하여 정리한 것이다.

<표 4> 하위항목 요소[9]

General Event Descriptions	General Event IDs
Account and Group Activities	4624, 4625, 4648, 4728, 4732, 4634, 4735, 4740, 4756
Application Crashes and Hangs	1000 and 1002
Windows Error Reporting	1001
Blue Screen of Death (BSOD)	1001
Windows Defender Errors	1005, 1006, 1008, 1010, 2001, 2003, 2004, 3002, 5008
Windows Integrity Errors	3001, 3002, 3003, 3004, 3010 and 3023
EMET Crash Logs	1 and 2
Windows Firewall Logs	2004, 2005, 2006, 2009, 2033
MSI Packages Installed	1022 and 1033
Windows Update Installed	2 and 19
Windows Service Manager Errors	7022, 7023, 7024, 7026, 7031, 7032, 7034
Group Policy Errors	1125, 1127, 1129
AppLocker and SRP Logs	865, 866, 867, 868, 882, 8003, 8004, 8006, 8007
Windows Update Errors	20, 24, 25, 31, 34, 35
Hotpatching Error	1009
Kernel Driver and Kernel Driver Signing Errors	5038, 6281, 219
Log Clearing	104 and 1102
Kernel Filter Driver	6
Windows Service Installed	7045
Program Inventory	800, 903, 904, 905, 906, 907, 908
Wireless Activities	8000, 8001, 8002, 8003, 8011, 10000, 10001, 11000, 11001, 11002, 11004, 11005, 11006, 11010, 12011, 12012, 12013

USB Activities	43, 400, 410
Printing Activities	307

4. 연구 결과

본 장에서는 AHP를 이용하여 NSA 주요 Event Log 요소들에 대해 상대비교 행렬을 이용하여 가중치를 산출하고 산출된 값을 통해 일관성 검정을 하여 일관성 비율과 타당도를 분석하였다.

4.1 일관성 비율

AHP 방법의 장점은 상대비교 행렬을 이용하여 가중치를 산출하는 과정에서 응답자들의 일관성을 검정할 수 있다는 것이다.

상대비교 행렬을 A, 가중치 벡터를 라 하자. 행렬의 차수는 평가요소의 수는 이다. 상대비교 행렬 A의 원소 a_j는 기준요소 i의 평가요소 j에 대한 합리성의 정도 값이다.

$$= \begin{pmatrix} 1 & a_2 & a_{13} \cdots a_{1n} \\ & 1 & 1 \quad a_{23} \cdots a_{2n} \\ & & \cdots \\ & & \backslash 1 \quad a_{n2} a_{n3} \cdots 1 \end{pmatrix}, \underline{w} = [w_1, w_2, \ldots, w_n]' \quad (1)$$

행렬 A에 대해 $| \quad -\lambda I| = 0$을 만족하는 스칼라 λ를 고유치(eigen value)라 하고, 고유치 λ에 대해 $Aw = \lambda \underline{w}$을 만족하는 벡터 $\underline{w}$를 고유벡터(eigen vector)라 한다. 상대비교 행렬 A의 최대 고유치 λ_{max}에 대응하는 고유벡터는 평가요소의 가중치를 얻는데 사용된다. 고유벡터 원소를 원소의 합으로 나누어 합이 1이 되도록 하면 그 값이 가중치가 된다.

상대비교 행렬이 완전한 일관성을 가지고 있다면 $a_{ij} a_{jk} = a_{ik}$이 성립한다. 그러나 실제 응답자가 완전한 일관성을 유지하는 것은 거의 불가능하다. 그럼 응답자의 일관성 정도를 어떻게 측정할 것인가? 완전한 일관성을 유지하지 하는 경우 $\lambda_{max} = n$이 성립하고, 그렇지 못할 경우 $\lambda_{max} > n$이 된다. 이를 이용하여 Saaty(1980)는 일관성지수(consistency index; CI)를 다음과 같이 정의하였다[10][11].

$$\text{일관성지수 :} \quad CI = \frac{\lambda_{max} - n}{n-1} \quad (2)$$

또한, 일관성 지수를 다음 개념으로 유도하였다. 비교 요소 j에 대한 기준 요소 i의 상대적 중요도를 a_{ij}라 하고 불일치 정도를 $\delta_{ij} > -1$라 하면, 상대적 중요도는 $a_{ij} = (1+\delta_{ij}) w_i / w_j$으로 표현할 수 있다. 그러면 다음 式이 성립한다.

$$\lambda_{max} - n = \frac{1}{n} \sum_{1 \quad i<j \quad n} \frac{\delta_{ij}^2}{1+\delta_{ij}} \quad 0 \quad (3)$$

위의 式에서 평가자가 완전한 일관성을 가지면, 즉 δ_{ij}(불일치 정도)가 0이 되면 $\lambda_{max} = n$가 성립하게 된다. 이를 이용하여 일관성 지수 개념을 유도하였다.

일관성이 클수록 λ_{max} 가 n에 가까워진다. 따라서 다음과 같은 CR(일관성 비율)을 사용하여 일관성의 정도를 측정할 수 있다[12].

$$CR(\quad \text{관성비율}) = \frac{CI(\text{일관성지수})}{RI(\text{난수지수})} \quad (4)$$

여기서 CI는 일관성지수로써 일관성이 클수록 0에 가까운 값을 가진다. RI는 Ramdom Index로 1~9사이의 난수를 사용해서 구성한 비교행렬의 CI들의 평균값이다.

<표 5> 설문 응답자의 일관성비율

응답자	최대 고유치 max	일관성 지수 CI	일관성 비율 CR (%)
1	78.429	4.162	2.793
2	69.297	3.553	2.385
3	51.277	2.352	1.578
4	74.161	3.877	2.602
5	43.139	1.809	1.214
6	68.298	3.487	2.340
7	89.796	4.920	3.302
8	80.447	4.296	2.884
9	50.491	2.299	1.543
10	84.652	4.577	3.072

<표 5>는 주요 Event Log에 대한 상대 합리성을 평가한 응답자 10명의 상대비교 행렬로부터 얻어진 최대 고유치와 일관성지수, 일관성 비율(난수 지수=1.12)을 정리한 것이다. 모든 응답자가 일관성 비율이 10% 미만으로 나와 응답자 모두가 평가에 대한 일관성을 나타냈다.

평가 일관성을 유지한 모든 응답자의 평가요소 상대비교 행렬을 이용하여 단일 상대비교 행렬을 계산하면 <표>와 같은 결과를 얻을 수 있다.

4.2 타당도 분석 결과

평가요소에 대한 타당도에 대한 분석결과는 <표 6>과 같으며, <표 6>의 1행 2열의 0.577은 다음 계산 절차에 의해 계산되었다.

응답자 1의 1행 2열 원소 값=0.333
응답자 2의 1행 2열 원소 값=1
응답자 3의 1행 2열 원소 값=1
응답자 4의 1행 2열 원소 값=0.333
응답자 5의 1행 2열 원소 값=1
응답자 6의 1행 2열 원소 값=1
응답자 7의 1행 2열 원소 값=0.333
응답자 8의 1행 2열 원소 값=0.333
응답자 9의 1행 2열 원소 값=0.333
응답자 10의 1행 2열 원소 값=1

그러므로 4개 값의 기하 평균은 ^{0} $.333\times1\times1\times0.333\times1\times1\times0.333\times0.333\times0.333\times1=0.577$이다.

<표 6> 평가요소 타당도 분석 결과

평가요소	Clearing Event Logs	Account Usage	중략	Printing Services	Windows Firewall
Clearing Event Logs	1.000	0.577	…	9.000	3.323
Account Usage	1.732	1.000	…	8.559	5.171
중략	…	…	1.000	…	…
Printing Services	0.111	0.117	…	1.000	8.777
Windows Firewall	0.301	0.193	…	0.114	1.000

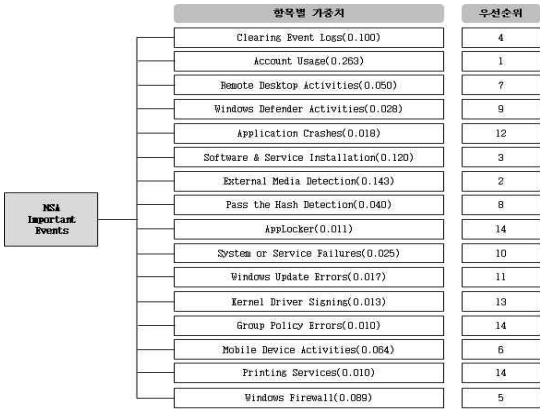
<표 6>의 최대 고유치 $_{max}$는 60.682이다. 이것을 式(2)에 대입하여 일관성 지수를 알아보면 2.991이고 式(4)에 대입하여 일관성 비율을 보면 2.007%(10%미만)로 그룹 전체가 평가의 일관성을 유지하고 있음을 알 수 있다.

4.3 중요도 분석 결과

(그림 2)는 NSA Important Events 평가요소의 중요도 및 우선순위를 분석한 결과이며, Account Usage, External Media Detection, Software & Service Installation 순으로 평가요소의 중요도가 측정되었다.

위의 평가요소가 모두 중요하지만 높은 순으로 보게 되면 Account Usage는 사용자 계정 정보는 수집과 감사 될 수 있는데 로컬 계정 사용을 추적하는 것은 Pass the Hash 활동과 인가되지 않은 다른 계정의 사용을 탐지할 수 있게 도와주며, 원격 데스크톱 로그인이나 권한 그룹에 사용자를 추가하거나, 계정 잠금과 같은 추가적인 정보들에 대해 추적이 가능함에 따른 결과로 볼 수

있고, 다음으로 External Media Detection과 Software & Service Installation은 OS보안 패치나 기존 시스템 패치를 위해 외부 파일을 반입해 작업하는 사례가 증가하면서 이러한 활동에 대해서 관리자들은 새롭게 설치된 소프트웨어나 시스템 서비스에 대한 로그를 통해 확인 및 네트워크에 위험하지 않은지 추가적인 확인을 할 수가 있기 때문에 상대적으로 평가요소 중 Account Usage, External Media Detection, Software & Service Installation의 중요도가 상대적으로 높게 나타났다고 할 수 있다.



(그림 2) 평가요소별 중요도 및 우선순위

5. 결 론

지금까지의 보안위협에 대한 대처는 보안장비를 이용한 방법이 주를 이루었으며, 공격기법에 의한 침해 사례 등이 다변화됨에 따라서, 보안장비에서 새로운 형태 및 내부자로의 위협에 대해 대처하기 힘들어지고 있다. 내부 시스템에서 어떠한 행위를 하게 되면 Event Log에 로그 데이터들이 수집되고 수집된 Event Log들을 분석하여 보안에 문제가 있는지를 판단할 수 있다.

따라서 본 논문에서는 주요 Event Log 들을 목록화 하여 내부자에 의한 위협에 대해 적용 가능성 여부를 타당도 및 중요도 분석을 통해 Account Usage, External Media Detection, Software & Service Installation 순으로 중요도가 나타났음을 알 수 있었다.

이 결과를 토대로 내부자의 보안위협을 감소 및 예방정책에 기여할 수 있으며, 시나리오 개발 및 패턴분석을 통한 보안위협 탐지 시스템 연구가 수행되기를 기대한다.

참고문헌

[1] 이동휘, 최경호, “제어망에서 화이트 리스트 기법을 이용한 이상 징후 탐지에 관한 연구”, 융합보안학회논문지, Vol. 12, No. 4, 2012, pp. 77-84.

[2] 이경문, “발전제어시스템 악성코드 방어를 위한 보안관제 모델 연구”, 석사학위논문, 2017. 02.

[3] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner and Alfonso Valdes, "Using Model-based Intrusion Detection for SCADA Networks", Computer Science Laboratory SRI International, http://www.csl.sri.com/users/cheung/SCADA-IDS-S4-2007.pdf, December 7, 2006.

[4] Alfonso Valdes, Steven Cheung, "Communication Pattern Anomaly Detection in Process Control Systems Technologies for Homeland Security", HST '09. IEEE Conference on, pp. 22-29, May 2009.

[5] Saranya Parthasarathy and Deepa Kundur, "Bloom Filter Based Intrusion Detection For Smart Grid SCADA", Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on, pp.1-6, May 2012.

[6] Martin Naedele, Dacfey Dzung, Michael Stanimirov, "Network Security for Substation Automation Systems", Computer Safety, Reliability and Security, pp.25-34, Sep 2001.

[7] Juan Hoyos, Mark Dehus and Timthy X Brown, "Exploiting the GOOSE protocol:

A practical attack on Cyber-infrastructure", GlobeCom'12 Workshop: Smart Grid Communications: Design for Performance, 2012.

[8] Minasi, Mark, Gibson, Darril, Finn, Aidan, Henry, "Mastering Windows Server 2008 R2", Wiley, 2012. 08, p. 921.

[9] Spotting the Adversary with Windows Event Log Monitoring: An Analysis of NSA Guidance, February 28, 2013.

[10] Ung, S.T., "The Development of Safety and Security Assessment Techniques and Their Application to Port Operations", PhD Thesis, School of Engineering, Liverpool John Moores University, UK, 2007.

[11] S.W. Kim, A. Wall, J. Wang, "Application of AHP to Fire Safety Based Decision Making of a Passenger Ship", OPSEARCH, September 2008, Volume 45, Issue 3, pp 249 - 262.

[12] Saaty, R. L., "The analytic hierarchy process", McGraw Hill, New York, 2008.

[저자소개]

김 종 민 (Jongmin Kim)
2010년 체육학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과 초빙교수

email : dyuo1004@gmail.com

김 동 민 (DongMin Kim)
2011년 한양대학교 대학원 전기공학과 졸업(공박)
2011년~2012년 한양대학교 BK21 사업단 박사 후 연구원
2012년~현재 동신대학교 에너지융합대학 전기공학전공 부교수.

email : dmkim@dsu.ac.kr

이 동 휘(DongHwi Lee)
2007년 경기대학교 정보보호박사
2011년~2012년 University of Colorado Denver, Dept. of Computer Science and Engineering
현 재 동신대학교 에너지융합대학 에너지응용학부 정보보안전공 교수

email : dhclub@dsu.ac.kr