Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.2, Apr. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.2.353

융합보안관제환경을 위한 아키텍처 구축 및 활용 방안에 대한 연구

황 동 욱,†‡ 이 상 훈
딜로이트안진회계법인

Study of Conversions Security Management System, Co-Relation Rule-Set scenario and architecture for incidence detection

Donguk Hwang,†‡ Sanghun Lee
Deloitte Anjin LLC

요 약

정보보호를 위해 다양한 종류의 시스템을 구축하고 운영하는 시대는 지나가고 이제는 구축한 시스템을 얼마나 잘 연동하고 활용하느냐가 중요한 시대가 되었다. 기업과 기관은 지속적이고 능동적인 APT 공격에 노출되어 있으며, 시그니처 기반의 보안시스템을 우회하고 회피하는 기술이 발달하여 침입 사실을 인지하지 못하고 침해사고를 당하는 일이 발생되고 있다. 과거 백신과 IPS, IDS 등을 이용하여 단순 보안관제를 통해 침입 대응이 가능하였다면 이제는 수십여 종의 보안 솔루션과 시스템을 모니터링하고 관제하여야 한다. 이러한 시점에서 본 논문은 수십여 종에 달하는 단위 보안시스템을 융합하고 상호 연관분석에 필요한 기반환경에 대하여 알아보고 시그니처 기반의 공격탐지 기법에서 벗어나 APT 공격을 인지할 수 있는 기법과 방법 그리고 날로 늘어가는 정보자산의 정보와 보안이벤트를 통합하고 모니터링 할 수 있는 방법을 연구해 보고자 한다. 또한 통합자원정보 수집과 네트워크 정보 등의 정보를 상호 융합하여 어떠한 효과를 얻을 수 있는지에 대하여 실 사례 통해 알아보고 향 후 발전해 나가야 할 방향에 대하여 논 하고자 한다.

ABSTRACT

We already have seen many studies and articles about the methodology responding the security risks and threats. But we still have some controversial subjects to be settled. Now, we are living in the era that we should focus on how to use the security systems instead of how to make it. In this point of view, a company need to find out the answer for these questions, which security risks have to be handled in a corporate, which system is better for responding the security threats, and how we can build necessary security architecture in case of developing systems. In this article, we'd like to study on-site scenarios threatening the corporate assets, the limit on dealing with these threats, and how to consolidate the security events and information from enormous assets. Also, we'd like to search for the direction form the actual cases which have shown the desired effect from converging the assets and network informations.

Keywords: *Conversions Security Managment System(CSMS), ESM(Enterprise Security Management System), Co-Relation Rule-Set, Incident Detection Scenario, SIEM(Security Information and Event Management), Combined Aseet Management*

접수일(2014년 1월 7일), 수정일(2014년 2월 26일), 게재확정일(2014년 4월 3일)

† 주저자, tomnjery@gmail.com
‡ 교신저자, tomnjery@gmail.com (Corresponding author)

I. 서 론

1.1 연구의 목적

최근 정보보호에 대한 중요성이 대두되면서 과거 침입차단시스템(Firewall)과 침입탐지시스템(Intrusion Detect System), 백신 등으로 구성된 단순한 침입탐지환경에서 벗어나 지금은 자동으로 침입을 탐지하고 방어하는 침입방지시스템(Intrusion Protection System)과 서비스 보호를 위한 웹 쉘 탐지, 사용자 보호를 위한 유해사이트 차단 등 다양한 종류의 정보보호시스템이 출시되어 운영되고 있다.

기업은 이러한 이기종간의 보안시스템에서 발생되는 로그를 중앙에서 관리하기 위해 통합보안관제 시스템(Enterprise Security Management)을 도입하여 관리하기 위한 노력을 기울이고 있으나 그 용도는 로그 수집기 기능과 관제 대상 시스템의 성능모니터링 용도로 사용되고 있어 통합보안관제시스템이라는 용도로 활용이 어려운 상황이다. 기업은 이제 보다 개선된 보안관제환경과 중앙관리시스템 활용방안을 요구하고 있는 추세로서 대규모 전산망 환경에서의 보안시스템 관리와 시스템에서 발생되는 대량의 로그를 관리할 수 있는 로그 통합 수준을 뛰어넘어 서버, 네트워크, 보안장비, 사용자활동 등 분야의 구분 없이 이벤트를 수집, 분석, 조회가 가능한 융합보안관제 환경을 요구하고 있다. 이러한 시점에서 본 논문은 시장의 다양한 요구사항에 발맞추어 증가되고 있는 정보보호시스템을 영역과 종류별로 구분해 각 정보보호 시스템이 대응 가능한 공격 기술에 대하여 알아보고, 중앙으로 수집되는 로그를 활용하여 새로운 결과를 얻어낼 수 있는 방안에 대하여 연구하고자 한다. 또한 실제 예시를 통해 대량로그관리시스템, 통합정보자원 및 융합보안관제환경을 이용한 연관성 분석 시나리오와 아키텍처 개발, 그리고 연관성분석 방법론을 개발하고 그 효과를 알아보고자 한다.

1.2 연구의 배경

기업이 제공하는 서비스가 늘어감에 따라 같이 증가하고 있는 보안시스템의 종류를 알아보기 위해 아래 [Table 1]과 같이 각 시스템의 종류에 대한 자료를 조사하였다.[1] 조사 결과 침임을 탐지/차단하는 탐지/방어시스템과 정보시스템에 접근한 이력과 행위를 기록하는 원격접속통제시스템, 산재된 시스템에서 발생되는 보안 이벤트를 중앙 집중화하고 경보를 발령하는 분석/관리시스템 그리고 취약점을 분석하고 침해사고 대응지원 및 예방을 위한 예방/지원시스템으로, 16개의 탐지/방어시스템 群, 2개의 원격접속통제시스템 群, 5개 분석/관리시스템 群, 11개 예방/지원시스템 群으로 분류되었다.

Table 3. Category of Information Security System

Div.	Information security system
Detection /Prevention	Anti-Denial of Service(Anti-DDoS)
	Web Application Firewall
	IPS, IDS
	Firewall
	Webshell Finder/Detection
	Anti Virus
	PC/USB media access control
	Connect to Harmful website filter
	United Threat Management
	Wireless Intrusion Prevent System
	Virtual Private Network
	Voice over TCP/IP IPS
	Private Information Protection/Filter
	Anti-Advanced Persistent Threat
	Spam/Virus mail filter
	Secure OS
access control	Remote Access Control
	DBMS Remote Access Control
Analysis /Management	Enterprise Security Management
	Security Information & Event Management
	Threat Management System
	Risk Management System
	DB Transaction Logging System
Support	System Vulnerability Scanner
	Network Vulnerability Scanner
	Database Vulnerability Scanner
	Web Management System
	Patch Management System
	Network Access Control
	Source Code Vulnerability Scanner
	System Forensic

	Network Forensic
	Digital Rights Management
	Database Encryption

조사결과 총 4개 영역에 대하여 34종의 보안시스템이 조사되었으며 2000년도 초반을 기준으로 백신, 침입차단시스템(FW), 침입탐지시스템(IDS) 등 3~4가지 종으로 구축되던 기존 보안 인프라에 비해 지금은 약 10배 가량 증가 되었다는 사실을 알 수 있다. 이와 같이 늘어난 보안시스템에서 발생되는 침입탐지 로그와 경보 이벤트는 수백 메가바이트를 넘어서 수십 기가바이트 수준으로 생산되고 있으며 이에 대한 로그 수집 및 분석 기능에 대한 처리 속도와 용량 증가에 대한 요구가 늘어남에 따라 빅-데이터 처리기술이 나타나게 되었다. 기존 R-DBMS 환경에서 벗어나 nonSQL[(2)] 환경으로 발전함에 따라 대량의 데이터를 관리할 수 있게 되었으며, 기존 ESM(Enterprise Security Management) 환경에서 단위 보안시스템이 생산하는 RAW DATA를 저장할 수 없었다는 점과 보안 벤더에서 제공하는 Co-Relation Rule-Set에 한하여 보안관제가 가능했다는 점, 유연성과 확장성이 부족하여 보안 관리자가 원하는 정보를 단위보안시스템에서 다시 찾아봐야 한다는 점, 단순 로그 수집 기능으로 사용하여 사건 발생 시 로그 검색 기로만 사용했다는 한계점을 극복할 수 있게 되었다. 이제는 이렇게 개선된 기반 기술을 활용하여 기업보안 담당자들이 수집/분석하고자 하는 목적과 용도에 맞게 활용할 수 있는 방안에 대하여 알아보고자 한다.

1.3 연구의 방법

본 연구는 실제 기관의 정보보호 환경을 토대로 수행되었으며 실 사례를 통해 공개되는 IP정보 및 시스템 구성은 연구자료 발표에 맞게 각색되었다. 연구의 대상 기관은 1일 4만여 건의 침입시도 이벤트가 발생되고 있으며 〔Table 2〕와 같이 대부분의 정보보호 시스템이 구축된 기관으로서 대량의 로그를 수집, 관리할 수 있는 기반환경은 구성되어 있으나 수집된 대량의 로그를 어떻게 상호 연관분석하고 활용할 수 있는 방안은 없는 상태이다. 이와 같은 환경에서 대량의 시스템 정보 및 로그를 활용할 수 있는 방안에 대하여 알아보고 보안 이벤트 정보와 시스템 자원정보를 융합한 침입탐지 및 침해사고탐지 시나리오의 개발 및 구현에 대한 연구 결과를 기술 하도록 한다. 금 번 연구는 실제 예시를 통해 기관의 자산을 위협하는 사례와 그에 따른 대응 방안을 연구하고 정보보호의 최종 목표를 위한 대량 데이터 수집/분석, Co-Relation 정책 개발, 인프라적 다이어그램 제안 그리고 정책 및 관리환경을 수립하기 위한 사례를 분석하고 해결 방안을 제시하여 최종적인 아키텍처 모델을 제안하고자 한다. 그리고 기존 사용되고 있는 용어와의 혼선을 피하기 위해 본 논문에서는 아래 〔Table 2〕와 같이 용어를 정의하고 기술하도록 한다.

Table 4. Definition of terms in this paper

Term	Substance
CSMS	Heterogeneous devices and correlating information collected through analysis / management systems, CSMS(Conversions Security Management System)
SIEM	Between disparate systems to centralize and manage the system log, SIEM(Security & Information Event Management)
ESM	Centralized security system and manage the system log, ESM(Enterprise Security Management)

II. 본론

2.1 통합보안관제환경과 융합보안관제환경

융합보안관제환경(CSMS)은 통합자원정보(ITAM)와 서버, 네트워크, 보안 등 이기종 시스템으로부터 발생되는 모든 로그를 수집 관리할 수 있는 대량로그관리시스템(SIEM)을 통해 구성되며 전사 보안시스템 통합 및 모니터링 창구를 단일화하여 보안관제 프로세스 처리 시간을 단축하고 위협을 탐지/방어할 수 있는 시스템을 근간으로 한다. 상호 연관성 분석 정보를 수집하기 위해 대량로그관리시스템을 이용하여 어떠한 보안 이벤트를 수집하여야 하는지에 대하여 아래 〔Fig 1〕과 같이 제시하였다.

Fig.1.Structure of information gathering

위 〔Fig 1〕에서는 크게 네트워크기반, 정보유출감시/사후감사시스템, 호스트기반 보안시스템, 자산정보관리시스템 3개 영역으로 구분되어 있으며 각 영역별 단위보안 시스템 및 관리시스템은 아래 〔Table 3〕과 같이 분류하였다.

Table 5. Domain of security system

Div.	System	note
Network base	Anti-DDoS, IPS, F/W, IDS, WEB-F/W, Spam/Virus Filter, WIPS, ETC..	7 ea
Audit	Remote Access Control, Private filter, DB Access control, Network forensic, DB Transaction Logging, Hamful website Filter, ETC..	6 ea
Host base	Webshell Detection, SSL Server, ESM Agent, Anti-Virus for server, Secure O/S, Anti-Virus for PC, PC media control, DRM, Secure USB, Mobie Anti-Virus, Private Finder, MDM, and User activity ETC..	13 ea

위 〔Table 3〕과 같이 26종의 단위보안 시스템으로부터 수집되는 로그는 대량로그관리시스템(SIEM)으로 집중화 되며 실시간 보안관제가 가능한 환경으로 구축되어 있다. 기존 통합보안관제 환경에서는 공격목표 PC 또는 서버, 네트워크장비, DBMS등 고유하게 발생되는 로그를 수집할 수 없어 통합보안관제시스템으로 수집된 정보만으로는 실제 공격 대상이 되는 서버나 PC에 어떠한 영향력을 미쳤는지는 알 수가 없다는 단점이 있었다. 이러한 단점을 보완하기 위해서는 보안시스템 이외에 서버 및 PC에서 발생되는 시스템 자원정보를 수집하여야 하며 정상작업에 의핸 상태변화 여부를 판단하기 위한 원격접속통제 감사 로그, 개인정보유출 차단로그, DB접근통제 감사로그, DB 트랜잭션 감사로그와 부가적 정보 분석을 위한 네트워크 포렌식 로그, 유해사이트 차단로그, 사용자활동 정보로그(웹 접속이력, 네트워크 연결 상태정보 등)의 정보를 추가로 수집 하여야 한다. 이러한 여러 종류의 정보를 상호연관 분석하기 위해서는 이벤트가 발생된 시간이 매우 중요하므로 시각동기화 서버(NTP)를 이용하여 동기화 하여야 한다. 대상을 식별하기 위해 사용되는 정보(IP, MAC, 사용자계정명 등)또한 DB화 되어 주기적으로 변경, 관리 되어야 하며, 대량로그관리(SIEM)시스템 또한 상기 로그와 자산정보를 실시간으로 상호 비교하여 서버, 네트워크, PC 등의 상태변화를 모니터링 하여야 하므로 정확한 자원 정보를 최신으로 유지하고 있어야 한다. 본 논문은 각 각의 이벤트와 자원정보가 실시간으로 변화하는 모습을 모니터링 하는 것으로 시스템의 상태변이 모니터링이 중요하다. 이러한 상태변화 모니터링 기법은 독일 C.A.Petri 가 고안한 Petri Net모델[3]을 근간으로 하며 어떠한 사건이 발생하면 반드시 상태의 변화가 발생하다는 것에 기초하고 있으며 아래 〔Fig 2〕와 같이 표현되고 있다.

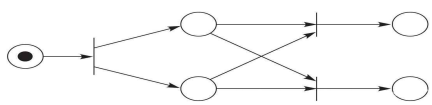


Fig.2. Petri Net representation

그러나 상태변화 탐지 기법을 통해 모든 변화를 탐지할 수 있다는 점은 장점이자 단점으로서 시시각각 변화하는 값이 범위가 커 오탐이 매우 많다는[4] 연구가 있으므로 이를 보완하기 위해 본 논문에서는 지식관리DB를 이용하여 이를 해결하고자 한다. 지식관리DB는 한번이라도 발생된 사건에 대한 이력을 기록한 후 다시 발생된 상태변화를 이전 사건과 비교해 나가며 과거 사례와 일치하는 이벤트를 제거해 나가는 방식으로서 실제 본 방식을 이용하여 본 연구 대상 기관에 적용해 보았다. 이 기관은 최근 12개월 동안 발생한 침입탐지 횟수를 기준으로 상위 10개의 공격에 대하여 확인한 결과 총 28종의 공격이 발생되었으며, 이 중 19건이 중복으로 발생하는 것으로 확인되었다. 또한 이 28종 중 상위 10개의 공격유형이 전체 이벤트 중 82.%로서 공격의 대부분을 차지하고 있는 것으로

나타났으며 아래 〔Fig 3〕과 같은 분포로 나타났다.

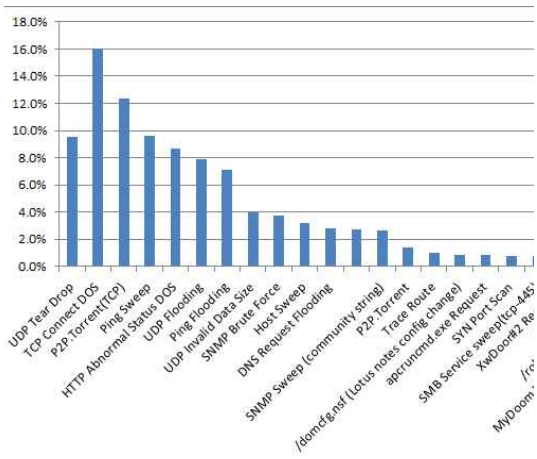


Fig.3.The distribution ratio of the attack

특히 28종의 공격유형에 대한 총 침입탐지 수는 9,868,615 건으로 이중 중복으로 발생된 공격이 9,542,950건으로 96.7%의 비율로 나타났다. 신규로 발생된 9개의 공격유형은 325,664 건으로 3.3%의 비율을 나타내어 중복 발생이벤트가 많다는 것을 확인할 수 있다. 이는 곧 관제요원이 처리해야할 대부분의 침입탐지 이벤트는 한번이라도 발생되었던 과거 이벤트와 동일한 사건으로서 그 처리결과를 지식관리DB화하고 실시간으로 발생되는 이벤트와 자동으로 이력을 비교하여 96.7%의 이벤트를 자동으로 처리할 수가 있다는 점을 시사한다. 실제 이러한 환경에서 분석에 필요한 시간을 알기위해서는 알려지지 않은 사건의 수(n), 알려진 사건의 수(k), 분석소요시간(t)로 총 처리시간(T)으로 아래 〔수식 1〕과 같은 수식으로 도출이 가능하다.

$$\text{Total process time(T)} = (\text{Number of Unknown case(n)} - \text{Number of Known case(k)}) * \text{Process time(t)}$$

〔수식 1〕

실 환경에서 알려진 사건을 관리하는 지식관리DB가 없는 경우 총 처리시간(T)은 알려지지 않은 사건의 수(100) * 분석소요시간(30분) = 3,000분(50시간) 의 시간이 소요되었지만 지식관리DB를 이용하여 97.6%의 알려진 사건의 수(k)를 제외하면 총 처리시간(T) = (알려지지 않은 사건의 수(100) - 알려진 사건의 수(97.6%)) * 분석소요시간(30) = 3,000분(50시간) = 99분으로서 기존 대비 30% 수준 정도로 단축이 가능하였다. 최근 도입되어 있는 위험관리시스템(Risk Management System)이 취약점분석평가결과와 자산 가치평가결과만 사용하여 자산의 위험을 관리하는 것이라면 융합보안관리(CSMS)시스템은 위 위험관리시스템(RMS)에 시스템 서비스 정보(Port open)를 추가로 대조하고 실시간으로 발생되는 시스템 상태변화를 감지, 취약성정보와 자산의 서비스운용 현황을 상호연관관계를 자동으로 분석함으로서 실시간으로 분석/대응이 가능하다는 장점이 있다. 또한 네트워크 포렌식[5] 시스템과 융합하여 공격이 발생된 실제 RAW DATA를 확인이 가능하므로 침입시도 기법분석과 동시에 조치까지 가능한 환경이라는 점이 가장 큰 차이점이라 할 수 있다. 다음 절에서는 실제 네트워크 포렌식 시스템이 융합된 사례를 통해 기존 통합보안관제환경에서 얻을 수 없는 효과를 알아보도록 한다.

2.2 융합보안관제 환경의 구축

아래 〔Fig 4〕은 융합보안환경을 구축하기 위한 기본 구성을 표현한 것으로 이 기종간의 시스템 연동을 도식화 한 것이다.

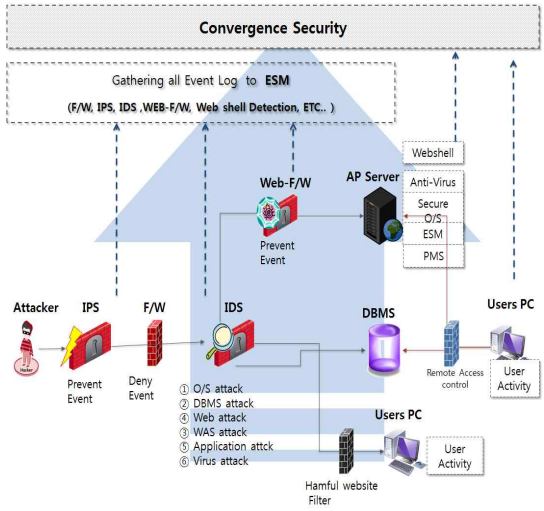


Fig.4. Architecture of Interlock system on CSMS

연동 분야는 네트워크, 원격접속통제, 데이터베이스보안, 호스트보안, 보안감사, 서버 및 사용자 활동정보, 시스템이벤트 로그, 로그관리시스템으로서 전사

에서 발생되는 모든 로그를 수집하고 관리하는 환경이며[6] 아래 [Fig 5]는 각 시스템에서 수집되는 정보의 예시로서 시스템, 네트워크, 보안, 원격접속, 어플리케이션으로부터 수집되어야 하는 정보의 예시를 나타낸 것이다.

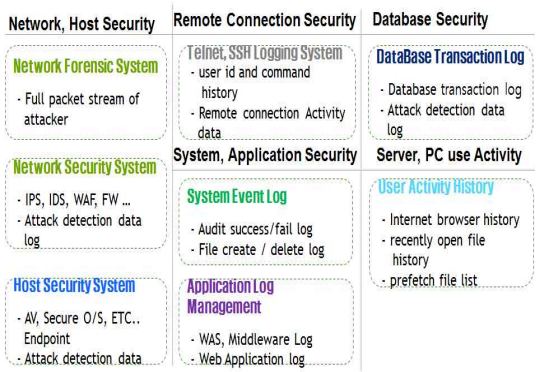


Fig.5. Categories of system information and event log

아래 [Table 4]는 서버, 네트워크, 보안시스템, PC 등에서 수집하여야 할 예시 정보와 금 번 연구에 필요한 수집정보 일부를 정리한 표로서 보안관제 목적에 따라 보다 더 많은 종류의 정보를 수집해야 할 수도 있다. 이번 연구 사례의 기본 개념은 침입을 탐지하거나 발생된 경우에는 반드시 시스템 상태변화가 발생된다는 점을 근간으로 하므로 process 별 port 목록과 같은 시스템 자원정보에 대한 수집이 중요하다.

Table 6. Example of Combined asset of information gathering

Div.		Substance
Server	OS	Interface info. (IP, gateway, DNS)
		Crontab, Auturun list
		Account List
		Host.allow, host.deny List
		F/W status (windows FW, iptable)
		message.log, secure log, su log
		iptable log, ssh log
		process, port list
		netstat status
		ARP table status
		Route table status
		Share folder
		Command history
		File list and permission
	DBMS	DBMS ver.
		Account list
		Transaction log
		Audit log
	application	App name ver, install date,
		Account list
		mail log, web log, DNS log, FTP log
PC	OS	Interface info.(IP, gateway, DNS IP)
		activeX
		Auturun list
		process, port list
		netstat status
		ARP table status
		route table status
		Share folder
Security Device	F.W	event date, time, sec.
		Allow/Deny status
		Source IP, Destination IP
		Source , Destination Port
		Protocol(TCP/UDP)
		send / receive byte
		session time
		NAT Log
		Real time session status
	IPS/ IDS/ WAF	event date, time, sec.
		Source IP, Destination IP
		Source , Destination Port
		Event name/ID
		Attack detection Count
		Attack try Count
		Detection/Prevention
		Threat level
		Raw data
	Webshell finder	event date, time, sec.
		target hostname
		target IP
		Detected file name and directory
		Detection name
		Result
		Raw data
	VMS	target IP
		Detected file name and directory
		Detection name
		Result
	Secure USB	User name
		device name
		Connection status
		Connect/Disconnect Log
	Spam/ Virus Filter	event date, time, sec.
		Event name/ID

지금부터는 이러한 통합자원정보와 융합보안관제 환경을 활용하여 탐지할 수 있는 케이스를 아래 〔Table 5〕과 같이 연관성 분석 시나리오를 정의하고 대응 방안에 대하여 알아보도록 한다.

Table 7. Co-Relation rule-set for combined asset information and Conversions Security Management environment

Div. name	gathering info.	Case.	Co-Relation	Detail
System changed Port, process name, and the status of the network connection information is collected compared with the previous acquisition of the anomaly detection system	**⑳ lsof info.** -Open Port by Process Info. -Status the opened PORT of connection (SYN_Sent, Listen, ESTABLISHED)	①A new process is created and generated PORT Listen ②SYN_SENT new process generation ①Generating TCP ESTABLISHED with IP not existing before	**〔lsof info.〕** The connection info. of new generated process name, S_IP, S_ PORT, D_IP, D_PORT, network **〔Co-Relation〕** ①ID, IP, user name, Div. name, contact info., logging info(command) ②log info. at that time	Whether A command of telnet, nc, netcat, *.sh, and etc. changing a connection of network exists in co-relation system log or not.
Gathering info. of ARP table for L2 communication which is the same LAN region and detecting abnormal activity of network compared with the previous collected info.	**㉑ arp info.** -arp table information.	①Registering MAC address and IP not existing before at arp table ②Generating a change of MAC address assigned to existing IP	**〔arp table〕** IP, MAC, HostName info. of generated system **〔Co-Relation〕** ①Info of applicant name, Div. name, IP, MAC ②ID, IP, user name, Div. name, contact info., logging info(command) ③, log info. at that time	Whether a detection IP and MAC address exist in co-relation log.
Detecting an abnormal state comparing info of new generated	**firewall info.** - Allow, Deny, Session info.	① Generating new connection for installing	**〔Connection info.〕** New generated S_IP, S_ PORT, D_IP, D_PORT info.	Whether a new connecting trial is found existing IP to IP
Connection, Allow, Deny log through log analysis of firewall Allow, Deny		disapproved PC or server, network, security device ②Allow or Deny is trying to connect to IP and PORT of log	**〔Accept, Deny info.〕** New generated S_IP, S_ PORT, D_IP, D_PORT, block/pass result info.	connection info., in Allow, Deny log.
Collecting info. of modified process in system and detecting a abnormal state of system compared with the prior info.	**㉒ps info.** -process info.	①Alerting when a new process is generated ②Deleting the existing process	**〔Basic Analysis〕** New generated process name, PID, percentage of memory usage, path, exe file **〔Co-Relation〕** ①Logged ID, IP, user name, Div. name, contact info., logging info(command) ③log info. at that time	Whether a command operating process like start, *.sh, etc. exists. Whether a command stopping process such as stop, kill, *.sh, etc. exists.
Gathering indefective info. about system file and detecting a abnormal state compared with the prior info.	**㉓ tripwire result** -File list in monitoring object folder(Bin, Var, Dev) -HASH info. of each existing file in monitoring object folder(bin, var, dev, corelogic)	①Alerting when a process not existing before is generated ②Changing HASH value of object file	**〔Basic Analysis〕** Directory of new generated file, file name, owner, own authority, size, generated date, modified date, access date **〔Co-Relation〕** ①Logged ID, IP, user name, Div. name, contact info., logging info(command) ③log info. at that time	Whether a command generating file like mk, cp, mv, rm, make, install, etc. exists. Whether a command changing contents of file like vi, put, update, etc. exists.
Gathering generated, deleted, modified info. about user account info. and detecting a abnormal	**Gathering etc/password file** info. -ID, group, owner, shell script, home directory,	①Generating and deleting a new account ①Generating a change of UID, GID, HOME	**〔Basic Analysis〕** Logged ID, IP, login time info. **〔Co-Relation〕** ①Logged ID, IP, user name, Div. name, contact info., logging info(command) ③log info. at that	Whether it is confirmed that a new account is added in co-relation object system and a command

state compared with the prior info.	password	DIR, login shell of an existing account	time	about account modification exists.
Gathering the info. of logged user and detecting a login abnormal behavior when changes is occurred.	**last info.** -ID, terminal, activating time, version, login state	①Generating when a new user logs on	**〔Basic Analysis〕** Logged ID, IP, login time info. **〔Co-Relation〕** ①Logged ID, IP, user name, Div. name, contact info., logging info(command) ③log info. at that time	Whether a new user exists in co-relation object system, and a change command and access log of the same ID exist in log at the same time.
An attacker detects an abnormal behavior perceiving a change of a network card for invading the other system or network sniffing.	**ifconfig info** -IP address, Eth info, Promiscuous info	①Activating Promiscuous Mode for eavesdropping on adjacent system traffic	**〔Basic Analysis〕** network Promiscuous Mode **〔Co-Relation〕** ①Applicant name, Div. name, IP, MAC info. ②ID, IP, user name, Div. name, contact info, logging info(command) ③log info. at that time	Whether a command changing connection of network such as LibPcap, etc. exists in co-relation object system.
Detecting an abnormal behavior approaching a port that malware uses.	**firewall info.** - Allow, Deny, Session info.	①A destination is in the outside, and access log exists in port such as 4444, 6666, 7777, 3774	**〔Basic Analysis〕** firewall ALLOW, DENY log **〔Co-Relation〕** process name, path, file name, info. of task history	to drive the process start, *. sh Reverse Connect command or commands such exist?
Detecting a behavior of acquiring common user's	**su log** ID, terminal, access location IP, login time	①Acquiring login-limited ROOT authorit	**〔Basic Analysis〕** SU Log log	Confirming a trace of executing a command of server

administrator authority		y.		History Log, and whether a logged user executes a command after logging in through the right process.
Detecting connection of new device	**mount log** -Check /var/log/dmesg, device name	①Installing USB, CD-ROM in server newly	**〔Basic Analysis〕** User login log, executing command log, log of a device trying mount	Whether it is to generate connection of a new device by a normal operation.
Detecting a change of automatic start list	**schedule log** - Crontab, Schedule, execution cycle, an executive command	①An automatic start command is added when starting system	**〔Basic Analysis〕** User login log, executing command log, info. of Crontab, Schedule before changed	Whether it is to change an automatic start command by a normal operation.
Detecting an abnormal behavior of anti-virus software by infected malware	**〔Anti-Virus Mgt.〕** Agent Down state log	①A user ends anti-virus on purpose ②Anti-virus is ended by Anti-AV malware	**〔Anti-Virus Mgt.〕** check te malware infected list and check the server or PC 〔IDS/IPS〕 IDS log to IP which the behavior occurred	①check terminate server of Anti-Virus or stop the service with IPS/IDS log
Detecting whether malware is spreaded in large quantities	**〔Anti-Virus Mgt.〕** Detection log **〔IDS/IPS〕** Detection log	①Detecting an attack by a tool such as JEUS, MIRANDA spreading a large quantity malware.	**〔Anti-Virus Mgt.〕** when malware is detected	①Checking whether there is an attack in IDS/IPS when malware is detected as new one
Detecting a hacking trial of opened server	**〔IDS/IPS, Web firewall, Anti-DDoS〕**	①An outside attacker is detected	**〔Diagnosing weakness DB〕** The result of diagnosed vulnerabilityes	①Confirming object IP, PORT, and detected

outside, and alerting after comparing the info. with the result of diagnosed vulnerability.	**Detection alarming log**	by security system after attacking inside assets	about IP and PORT of object of an attack system	attack name, and checking whether vulnerability exists in the assets.
Detecting an behavior that 주의관제IP executes after approaching inside	**〔IPS〕** Allow/Deny log of each IP **〔network IDS system〕** All security event log of IDS/IPS working based on network 〔Host IDS system〕 All security event log of IDS/IPS working installed in Host	①Blacklist IP tries to approach to assets	**〔⑤⑦⑫invasion and blocking system info.〕** Detection time, starting point IP, starting point PORT, destination IP, destination PORT, Accept/Deny info. **〔⑧⑨⑪netwrok IDS system info.〕** Detection time, starting point IP, starting point PORT, destination IP, destination PORT, name of attack detection, detection RAW, detection/defense result info. **〔⑬⑭server web, WAS info.〕** Detection time, starting point IP, starting point PORT, destination IP, destination PORT, Method, Parameter, response code **〔⑥ server Secure Log info.〕** Starting point IP, result of access trial **〔⑩⑰ Host IDS info.〕** Host IP, file name, path, detection/blocking result	①Arranging all log in order of time, and grasping the destination and the path that object IP approaches ②Is it blocked in the middle firewall? ③Is there any info. that IDS information detected as an attack? ④Do the final server and PC firewall log allow to approach to the final service? ⑤What is the access-allowed service?
When an attack is detected, grasping the influence of the attack automatically and then alerting	**〔network IDS system〕** All security event log of IDS/IPS working based on network **〔Host IDS system〕** All security event log of IDS/IPS working installed in Host **〔integrated 〕** opened port info. **〔result of diagnosing vulnerability〕** IP, name of existing vulnerability for each port	①Occurring an event detecting an attack like prevention from invasion, IDS, Anti-DDoS, detecting webshell in IDS system	Checking the same IP, PORT, detection history in all log of related security system when occurring IDS event, and alerting whether there is the same attack name in the diagnosed vulnerability list	Whether there is service destination IP and PORT where an attacker accesses. Whether the result of vulnerability diagnosis corresponds with a name of an occurred attack.
Detecting an abnormal behavior about DB approached by a developer and operator	**〔DB access control system〕** Query log that occurs by accessing personal info. DB of SQL Query	①Generating other schema and table access after compared with Query log about accessible system for each user ID	There is no existing history among generated Query or DML command like select * from is generated.	
Detecting unusual transaction between AP-DB and DB-DB	〔Transaction logging system〕 Starting point IP, PORT, destinatio	①New type transaction on which is not profiled before is	Alerting whether there is no existing history among generated transaction or DML command	

server	n IP, PORT, transactio n query	generate d.	checking table info. like select Tables from USER_TABLES is generated.	

위 〔Table 5〕에서 기술된 관제 가능 영역은 크게 19가지 영역으로 구분하였으며, 이상 징후 조기경보와 위험관리영역 그리고 비정상행위조기경보 영역으로 구분하였다. 이상 징후 조기경보영역은 네트워크와 시스템 이상 징후로 구분하였다. 위험관리영역은 악성코드관리, 해킹대응, 주의관제IP관리, 유효공격 판단자동화로 구분, 비정상행위조기경보영역은 비정상 트랜잭션 발생탐지로 구분하였다. 이와 같이 융합보완관제환경은 이기종간의 시스템 정보 융합뿐만 아니라 사용자의 활동정보와 서버의 네트워크 연결 및 파일의 상태변화라는 통합자원 정보에 대한 정보도 수집하는 것이 기존 보안환경과의 차이점이라 할 수 있다. 이와 같이 다양한 정보를 수집/분석할 때에는 수집된 정보에 대한 정확한 판단이 중요하다. 수집 정보 중 벤더의 탐지정책에 의해 발생되는 탐지 이벤트를 기준으로 분석을 수행할 경우 오판 문제점에 대한 연구 결과가 있으며[7] 이를 해결하기 위해 앞 절에서 기술한 지식관리DB를 이용해 해결하도록 한다. 각각의 사건에 대한 프로파일 및 유사도 측정 기법은 N-gram 기법을 활용하여 수집하며 N-gram 기법은 아래 〔Fig 6〕과 같이 표현되고 있다.[8]

$$a[i,j] = \max \begin{cases} a[i,j-1] + gap \\ a[i-1,j-1] + p(i,j) \\ a[i-1,j] + gap \end{cases}$$

Fig.6.Similarity measure formula

N-gram 기법의 전제는 이상 행위가 정상적인 사용과는 다르다는 데 두고 있다. 정상행위를 추출하고 정의하기 위한 대표적인 기법은 뉴멕시코 대학의 Forest 연구팀에서 개발한 기법이 있으나 오탐이 많다는 단점을 보유하고 있다. 위 기법은 전역정렬 기법으로서 유사도 측정 시 유사도가 100%인 경우와 아닌 경우로 나뉘어 프로파일링을 하지만 본 관제환경에서는 100% 일치가 아닌 경우에는 별개의 사건으로서 분류하여 신규 사건으로 처리 하여야 한다. 침입탐지 유사도 측정은 해당 공격이 침입시도인지 아닌지를 구분하여 사건의 가능성 분석하는 것이라면 본 논문에서 사용하는 기법은 침입시도에 대한 유사도 측정보다 실제 발생된 상태 변화 이벤트를 활용하고 있으므로 100% 일치 할 경우에만 지식관리DB를 이용하여 과거사례를 분석하여야 한다. 또한 정보보호에서는 탐지율과 오탐율은 trade off 관계로서 반드시 하나를 포기하여야 균형을 이룰 수 있다는 단점이 존재하지만 아래 〔Fig 7〕과 같이 현재 발생하고 있는 사건과 과거에 발생한 한 번이라도 발생한 사건을 상호 비교하여 오탐을 제거하는 지식관리DB형태를 이용한다면 발생되는 이 문제를 해결할 수 있다.

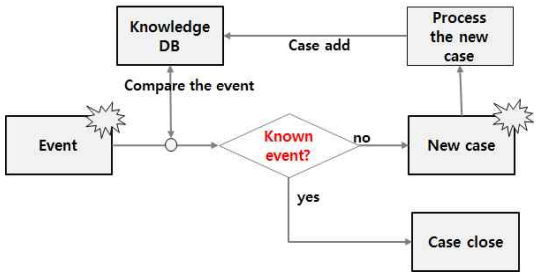


Fig.7.False positives avoid methodology using the Analysis of past cases

위 〔Fig 7〕에서 중요한 점은 한번이라도 발생된 사건은 「지식관리DB」에 모두 저장되어 있다는 점이다. 지금부터 네트워크 융합과 위 〔Table 5〕에서 기술한 내용에 대한 세부방법에 대하여 기술하도록 한다. 기존 침입탐지/방지시스템, 웹 방화벽 등 단위보안 시스템들은 공격으로 탐지된 1개의 Packet만을 저장하고 있어 일반적 관제환경에서는 공격의 원인과 공격의 영향력을 분석하기가 어렵다. 이는 공격 영향도 파악을 위해서는 실제 공격 대상이 되는 서버나 PC에 직접 접근하여 조사하여야하나 네트워크를 통한 공격에 대한 로그는 분석이 어려워 조사를 중단하는 경우가 많이 있다. 이러한 문제점을 도식화 하면아래 〔Fig 8〕과 같이 표현할 수 있다.

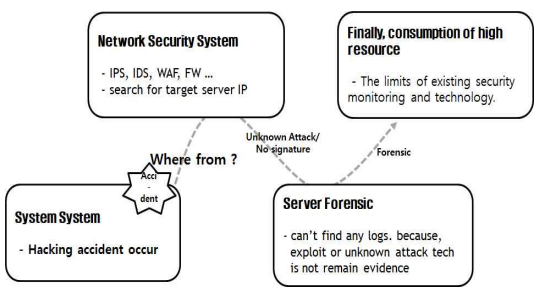


Fig.8. Problems of past security environmental

위 〔Fig 8〕에서는 나타내는 문제점은 침입시도가 인지된 시점으로부터 공격 기법 파악 및 영향도 파악을 위해서는 공격 대상 시스템에 접근하여 로그를 분석해야하는 환경으로 수백 건 씩 발생되는 침입탐지 이벤트를 모두 분석한다는 것은 사실상 불가능하다. 서론에서 살펴본 바와 같이 일일 4만 건의 침입탐지 이벤트가 발생되는 입장에서는 이를 자동으로 처리해 주는 자동화 시스템이 필요하다. 자동화를 위해 네트워크 포렌식 시스템과의 서버로그정보 또는 사용자 활동정보 수집이 필요하며 해당 정보를 이용한 개념은 아래 〔Fig 9〕과 같이 표현할 수 있다.

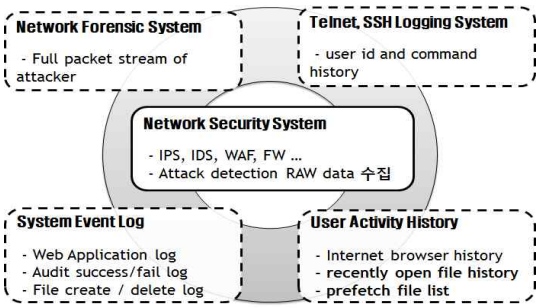


Fig.9.Concept of Interlock system with other system

위 〔Fig 9〕에서는 기존 보안시스템 간의 연동이 아닌 서버의 네트워크 포렌식 시스템이외에도 Telnet, SSH, Web log, Audit log, File Create/Delete 정보 등이 융합되어 있다. 이런 정보를 활용하면 기존 단순 보안시스템 수준의 관제에서 벗어나 시스템로그, 원격접속통제, 사용자활동정보 분석 등을 활용하여 보안시스템에만 치중된 보안관제가 아닌 사건의 원인, 결과, 시스템 영향 등 다양한 관점에서의 보안관제 서비스가 가능해지며 이를 이용하기 위한 정보는 아래 〔Fig 10〕 예시와 같다.

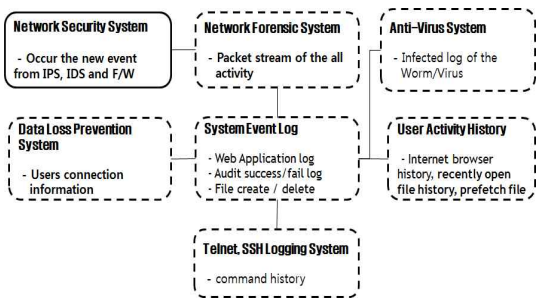


Fig.10. Reference point of multifaceted

2.2.1 융합정보를 이용한 공격 분석 예시

지금부터 예시를 통해 이전 보안관제 모델과 신규 융합보안관제 모델과의 차이점에 대하여 기술하도록 한다. 본 예시는 보안관제 요원이 통합보안관제시스템(ESM)을 이용하여 모니터링 하는 도중 Black List IP로부터의 접근을 탐지한 상황으로서 아래 〔Fig 11〕과 같이 이벤트를 확인 한 상황의 예시이다.

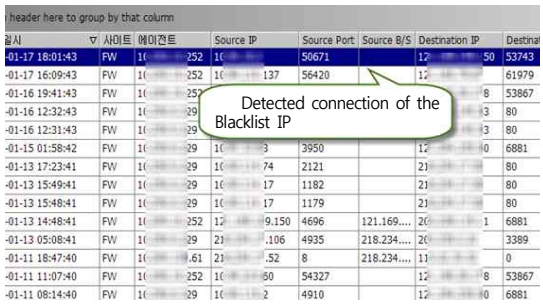


Fig.11. Attack detection with a ESM

ESM을 통해 해당 이벤트의 탐지된 시간 정보를 기준으로 타 보안시스템에서 발생된 공격탐지 이벤트가 있는지 검색을 하는 과정으로 아래 〔Fig 12〕과 같이 연동된 장비에 대한 조회가 가능하다.

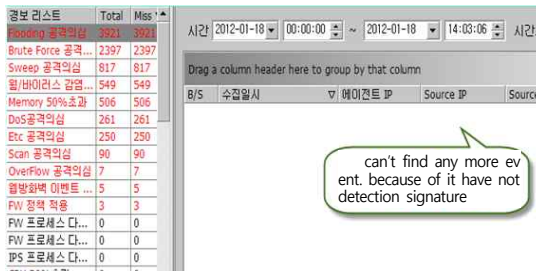


Fig.12.Security event search using the ESM

그러나 위 〔Fig 12〕과 같이 통합보안관제시스템에서는 침입탐지/방지시스템이나 웹 어플리케이션 방화벽 이 탐지하지 못한 이벤트는 조회가 불가하다. 이는 알려진 공격에 대하여 시그니처 기반 보안 시스템의 한계로서 기존 보안시스템만 연동된 ESM 환경에서는 금 번 예시처럼 알려지지 않은 공격에 대한 탐지 불가하다는 것을 알 수 있다. 이와 같은 경우 분석요원은 더 이상 공격에 대한 분석이 불가능하며 사건을 종료하거나 실제 대상 서버에 접근하여 공격 영향도를

분석하여야 한다. 이것이 기존 통합보안관제환경(ESM)의 한계점으로 이를 극복하기 위해서는 앞 절에서 제시한 융합보안관제 환경이 필요하며 네트워크 포렌식 시스템을 융합함으로서 이와 같은 문제를 해결할 수 있다. Black List IP로 부터 접속이 탐지된 시간을 기준으로 네트워크 포렌식 시스템에 저장된 패킷 스트리밍 정보를 조사하게 되면 공격자가 시도한 모든 공격을 복원하고 분석할 수 있다. 아래 〔Fig 13〕는 해당 사건이 발생된 탐지시간을 기준으로 추출한 패킷 스트림 정보이다.

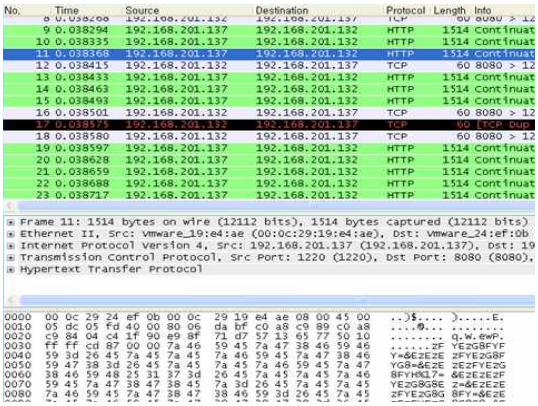


Fig.13.Confirmation of network packet stream flow

위 〔Fig 13〕과 같이 네트워크 포렌식 시스템이 연동 되어 있을 경우 관제요원은 모든 공격 행위를 복원하고 분석할 수 있으므로 정확한 상황판단이 가능해진다. 본 예시에서 분석된 정보는 아래 〔Fig 14〕와 같이 대량의 변수를 발송하는 공격이며 공격 영향도 또한 즉시 파악이 가능하다.

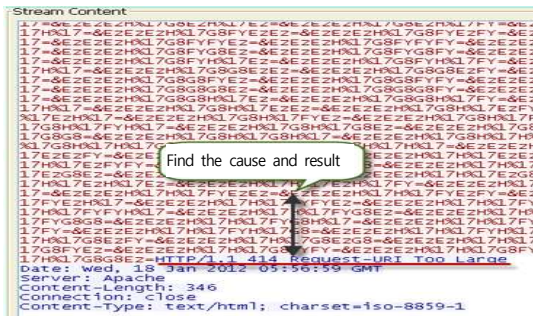


Fig.14. Perceive the attack method and Impact, using the network forensic system

위 〔Fig 14〕과 같이 확인한 결과 수 백 여개의 파라미터가 연속적으로 삽입 되어있는 패킷을 확인 할 수 있었으며, 아래 웹 서버의 응답코드가 414 Request-URI Too Large 이라는 값을 확인할 수 있어 실제 서버에는 공격 피해가 발생되지 않았다는 점을 알 수 있다. 웹서버의 접근 로그는 ESM을 통해 수집이 가능하지만 이번 공격은 웹 서버가 상세한 로그를 기록할 수 없는 POST Method를 이용하여 전송되었기 때문에 해당 시스템이 ESM과 연동되어 있다 하더라도 공격 기법이나 영향도를 파악할 수 없다. 그러나 융합보안환경에서는 단위보안시스템에서는 탐지 및 확인이 불가능했던 RAW Data와 네트워크 스트림에 대한 확인이 가능하므로 공격에 대한 추가 분석이 가능해 진다. 본 예시에서 나타나 있는 Payload를 검색해보면 아래 〔Fig 15〕와 같은 HASH 충돌 공격 기법임을 알 수 있다.

Fig.15.Confirmation of attacker's method

해당 공격은 CVE-2011-4885 HASH Table Collision DoS 공격으로서 한 번에 대량의 변수와 변수 값을 웹 서버에 전달하는 공격임을 알 수 있다. 이 공격은 웹 서버가 사용자로부터 전달 받은 변수 데이터를 관리할 때 발생되는 취약점을 이용한 것으로 서버가 관리하는 변수 HASH Table이 충돌을 발생시켜 서비스를 중단시키는 공격이다. 이에 대한 자세한 기법은 아래 〔Fig 16〕와 같다.

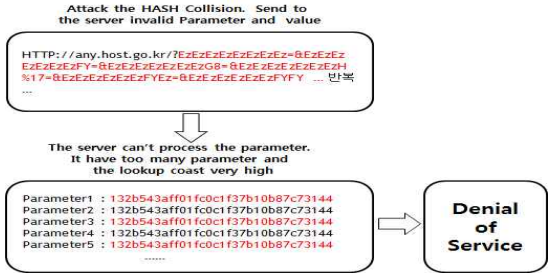


Fig.16. HASH Table Collision DoS

2.2.2 융합정보를 이용한 신규서비스 탐지 예시

아래 〔Fig 17〕은 서버 내부에서 신규서비스가 발생되었을 경우의 다이어그램과 상호연관분석관계도를 나타낸 것이며 지금부터 각 사례에 대한 세부사항을 알아보도록 한다.

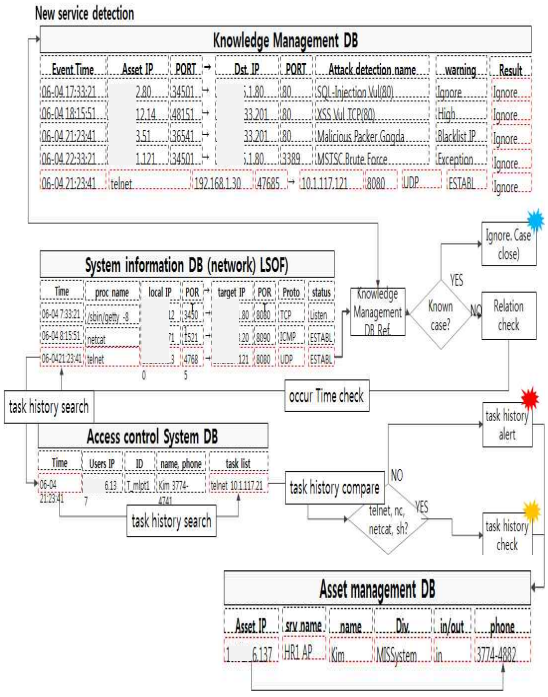


Fig.17.Case of new local service detection

위 〔Fig 17〕은 신규 서비스발생 사례의 경우로 시스템 자원정보DB에는 시스템의 실시간 네트워크 연결현황 정보가 핵심정보로 사용된다. 또한 프로세스명, 로컬IP, 로컬 Port 정보와 대상지 IP, 포트, 프로토콜정보, 상태정보의 변화를 모니터링하는 원리로 신규 서비스발생을 탐지하게 된다. 관리자에 의한 신규서비스 오픈 및 해킹이나 웜 바이러스를 통해 악성 프로세스가 활동하는 경우 공격자는 원격 또는 외부에 위치한 자신의 서버(C&C)서버에 연결되어 추가 명령 및 악성코드를 다운로드를 받아야 하므로, 시스템에서는 반드시 네트워크 소켓을 생성하고 연결하는 활동이 발생된다는 점에서 착안한 것이다. 정상 네트워크 연결 발생 시에는 1차적으로 과거에 유사한 사례가 있었는지를 판단하기 위해 기존 지식 관리 DB를 참조하여 과거에 처리된 이력이 있는지 확인한다. 이때 사용되는 지식관리DB는 아래 〔Fig 18〕과 같이 구성되어 있어 과거 사례에 대한 모든 정보를 포함하고 있어야 한다.

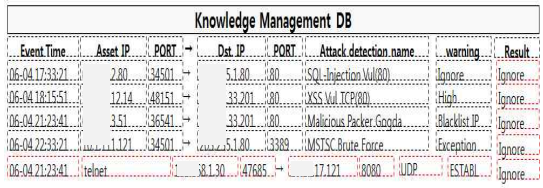


Fig.18 . Knowledge Database Structure

현재 발생된 이벤트가 예전 무시 처리가 된 이벤트인지를 비교하고 기존 지식관리DB에 존재하지 않는 경우 해당 이벤트는 2차적으로 작업관리DB에 접속하여 사전에 등록된 정기작업에 의한 변경사항인지 비교하고 정상 작업에 의한 시스템 상태변화인지를 판단한다. 만약 지식관리DB와 작업관리DB에서 어떠한 비교 데이터도 찾지 못하게 되면 해당 이벤트는 3차적으로 원격접속통제시스템통합DB에서 해당 프로세스명, 프로세스 실행시간 정보를 토대로 운영자 또는 담당자가 해당 상태변화를 유도한 것이 맞는지 비교하게 된다. 이 3단계 과정에서도 유사성을 찾지 못하게 되면 해당 이벤트는 자산관리 시스템에 등록된 시스템 담당자에게 문자메시지나 이메일을 통해 시스템 상태변화 정보를 전송하게 된다. 이와 같은 4단계의 과정을 통해 이벤트는 자동으로 정교화 되고 오탐이 제거되게 된다. 여기서 중요한 점은 원격접속통제시스템통합DB의 정보이다. 시스템 상태변화는 사용자에 의한 상태변화로서, 이중 정상 사용자, 비정상 접근자에 의한 변화를 감지하는 단계이다. 해커와 같은 공격자의 비정상적인 접근과 Exploit을 이용한 비정상적인 시스템 접근은 원격접속통제시스템을 통과하지 않고 시스템에 직접 접근한 경우이므로 어떠한 로그도 원격접속통제시스템통합DB에 등록되지 않는다는 점에서 착안한 것으로서 공격자가 비정상적인 경로를 통해 시스템 권한 획득 시 즉시 탐지가 가능하게 된다. 또한 보안관제 대상 시스템은 반드시 원격접속통제시스템을 통과하여 접근하여야 하므로 반드시 모든 시스템은 직접 접속이 가능한 네트워크 연결을 제거되어야 한다. 경보를 받은 담당자는 발생된 이벤트의 프로세스 명, 실행한 사용자, 시작된 시간, 출발지 IP, 포트, 목적지 IP, 포트 등 네트워크 연결 상태를 확인하고 해당 상태변화에 대한 평가를 수행한다. 담당자 수동 확인결과 정상 작업으로 확인된 경우 담당자는 이벤트에 대하여

승인 플래그를 적용하고 해당 사유를 기재하고 제출한다. 제출 된 작업은 프로세스 정보, IP 정보 등을 기준으로 지식관리DB에 저장되고 다음 이벤트 발생 시 비교 자료로 활용되며 시스템은 해당 정보를 매번 비교하여 불필요한 경보를 발령하지 않고 자동으로 최초 발생한 상태변화 정보와 위험 경보만을 담당자에게 발령하게 된다. 해당 원리에 대한 개념은 아래 [Fig 19]과 같이 구현이 가능하며 해당 코드의 설명은 다음과 같다.

```
:START_Stats
REM #### Record current netstat talbe
    netstat -ano > Before_netstat_Table.tbl

    echo Checking New Service....
REM #### sleep 5 second
    timeout 5


REM #### Record the netstat table 1 minute after.
    netstat -ano > after_netstat_Table.tbl


REM #### diff before and after
    diff.exe before_netstat_Table.tbl after_netstat_Table.tbl > new_changed_netstat_Table.info

REM #### File empty check
    for /f %%i in ("new_changed_netstat_Table.info") do set size=%%~zi

REM if file is empty then have any changed
REM #### Is Not empty file then
    if %size% gtr 0 (
REM #### Send to Server
REM     type new_changed_netstat_Table.info | nc.exe -w 5 1[redacted]16.137 8087
        echo ========== %date% %time% ========== >> alert_list.txt
        type new_changed_netstat_Table.info >> alert_list.txt
    )

GOTO :START_Stats
```

Fig.19.Agent code of new service detection case

New_System_Agent는 자신의 Netstat -an 정보를 5초 단위로 수집하여 5초 전의 시스템 상태와 현재의 시스템 상태를 비교한 후 시스템 상태에 변동이 탐지되면 아래 [Fig 20]와 같이 해당 변경 사항을 수집서버인 10.9*.**.137 서버로 전송하도록 구현되어 있다.

```
  TCP    0.0.0.0:8087           0.0.0.0:0              LISTENING
9d89
  TCP    1[redacted]16.137:47572   1[redacted]16.137:8087     TIME_WAIT
):₩Desktop₩융합보안관제환경을 위한 아키텍처 구축 및 활용 방안에 대한
17a18
  TCP    0.0.0.0:8087           0.0.0.0:0              LISTENING
8d88
  TCP    1[redacted]16.137:47573   1[redacted]16.137:8087     TIME_WAIT
0d89
  TCP    1[redacted]16.137:47575   1[redacted]4.127.240:80    TIME_WAIT
):₩Desktop₩융합보안관제환경을 위한 아키텍처 구축 및 활용 방안에 대한
17a18
  TCP    0.0.0.0:8087           0.0.0.0:0              LISTENING
4d84
  TCP    1[redacted]16.137:47549   [redacted].131.111:80      TIME_WAIT
6c86
  TCP    1[redacted]16.137:47569   1[redacted]9.222.15:80     ESTABLISHED
```

Fig.20.Gathering the changed information

해당 서버는 클라이언트로부터 수신된 변경 정보를 자산정보를 이용하여 클라이언트의 신분을 확인하고 출발지 IP/포트, 목적지 IP/포트 정보를 자신이 보유한 과거 지식관리DB와 비교하여 해당 변동 사항이 정상인지 비정상인지를 판단하게 된다. 실제 실험기간(2013-12-18 5:49:52.25)동안 위 그림과 같이 내부 사용자(1*.9*.8.14:9574)PC에서 접속이 인가되지 않은 IP(1**.**.*.*:80)로의 접근이 발견되어 원인파악 및 조치가 가능 하였다.

2.2.3 융합정보를 이용한 신규인접 시스템 탐지 예시

세 번째로 신규인접 시스템 발생 경보이다. 해당 상태변화 탐지는 인접한 시스템 간 ARP* 정보 교환이 발생될 경우 ARP Table의 상태변화가 발생한다는 점에 착안하여 탐지되게 되며 그 절차는 [Fig 21]과 같다.

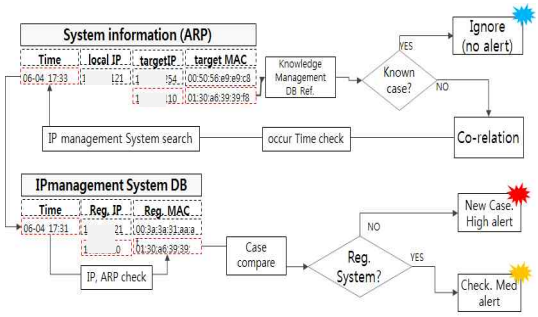


Fig.21. Case of new system detection

시스템 대부분은 평소 자신이 통신하는 시스템의 ARP 정보를 Table에 등록되어 있지만 공격이나 무단으로 설치된 신규 시스템이 발생될 경우 신규 ARP 정보가 갱신될 경우 시스템은 상태변화를 감지하고 이벤트를 발생시킨다. 발생된 이벤트는 정상적인 작업에 의해여 시스템이 추가되었는지 확인하기 위해 1단계로 자신이 발견한 신규 생성 MAC 정보를 IP관리시스템DB와 비교하게 된다. 만약 IP관리시스템DB에 해당 정보가 없다면 시스템은 지식관리DB 참조 단계인 2단계로 넘어가게 되며 기존 지식관리DB에서 동일하거나 유사한 이력이 있는지 검사하게 된다. 이 단계에서도 확인되지 않으면 해당 이벤트는 자산관리DB에 등록된 담당자에게 SMS 또는 이메일을 발송하여 경보발생을 알리게 된다. 해당 시스템의 개념증명 코드는 아래 [Fig 22]와 같이 구현이 가능하며 시스템의 상태변화를 5초 단위로 수집하고 차이점을 비교하게 된다.

* 로컬주소결정 프로토콜로서 인접한 시스템 간 통신에 사용

```
:START_Stats
REM #### Record current arp talbe
    arp -a > before_arp_Table.tbl

    echo Checking new system...
REM #### sleep 5 second
    timeout 5


REM #### Record the arp table 1 minute after.
    arp -a > after_arp_Table.tbl


REM #### diff before and after
    diff.exe before_arp_Table.tbl after_arp_Table.tbl > new_changed_arp_Table.info

REM #### File empty check
    for /f %%i in ("new_changed_arp_Table.info") do set size=%%~zi

REM If file is empty then have any changed
REM #### Is Not empty file then
    if %size% gtr 0 (
REM #### Send to Server
        type new_changed_arp_Table.info | nc.exe -w 5 10.9[illegible]37 8087
        echo ========== %date% %time% ========== >> alert_list.txt
        type new_changed_arp_Table.info >> alert_list.txt
    )

GOTO :START_Stats
```

Fig.22.Agent code of new system detection case

위 〔Fig 22〕 Agent는 자신의 시스템 상태변화를 탐지하고 탐지가 발생될 경우 서버로 변동된 정보를 아래 〔Fig 23〕같이 송신하게 되며, 서버는 지식관리 DB를 조회하여 해당 상태변화가 정상인지 비정상인지를 판단하게 된다.

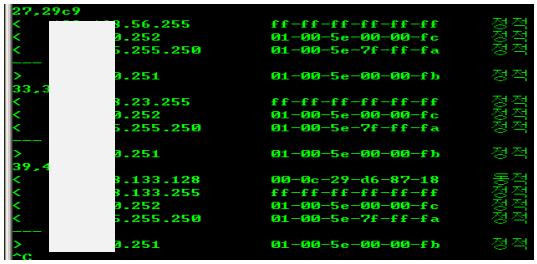


Fig.23.Gathering the changed information

위 실험을 통해 실험 기간인 2013-12-18 1:24:30.24에 1*.9*.**.203 IP를 가진 WIPS_senser#3 센서가 00-11-74-40-9b-35 MAC 주소로 등록된 것이 확인되었으며, 당일 야간 해당 장비의 장애가 발생하여 WIPS 센서가 재시작된 것을 확인할 수 있었다. 위 실험과 같이 정보를 수집하고 자산관리DB와 작업관리DB 등 상호 연계된 시스템들 간 상호 참조를 통해 각종 상태변화를 탐지할 수 있었다.

2.2.4 융합정보를 이용한 이상 징후 탐지 예시

네 번째 해킹시도 탐지의 경우 각 단위보안시스템으로부터 수집되는 보안탐지 이벤트를 근간으로 하며 상호연관분석관계도는 아래 〔Fig 24〕 과 같으며 이는 이상트래픽 발생 시 상호연관성 분석시나리오는 방화벽의 통신 상태에 대한 프로파일링을 근간으로 한다.

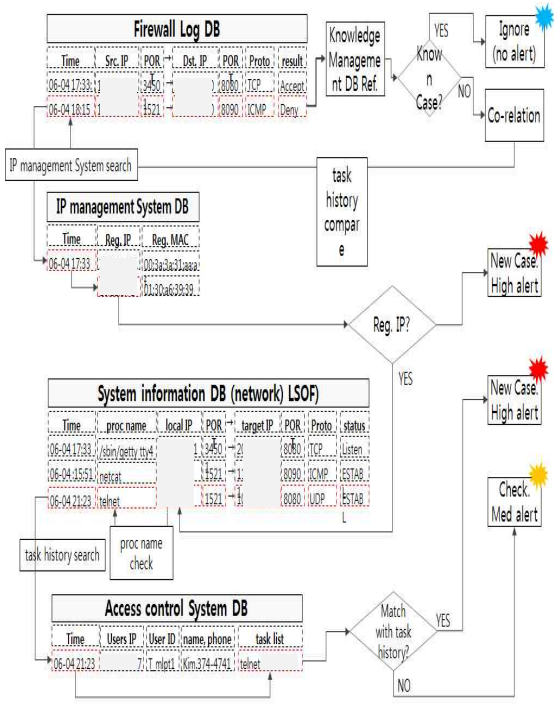


Fig.24.Case of anomaly traffic detection

방화벽에서 실시간으로 생성되는 세션정보와 서버와 서버 간 통신, 서버와 PC간 통신 등 모든 통신이력이 방화벽의 Access와 Deny 로그에 저장되고 관리된다는 원리에 착안한 부분이다. 구간과 구간을 연결하는 방화벽은 평소 동일한 시스템 간의 통신이 발생된다. 주기적으로 방화벽 로그파일의 상태변화를 점검하기 위해 아래 〔Fig 25〕 같이 주기적으로 비교한다.

```
:START_Stats
REM #### file diff before and after
diff.exe before_stats_firewall_log.tbl after_stats_firewall_log.tbl > new_changed_stats_Table.info

REM #### File empty check
for /f %%i in ("new_changed_stats_Table.info") do set size=%%~zi

REM If file is empty then have any changed
REM if %size% gtr 0 (echo Not empty ) else (type new_changed_stats_Table.info | nc.exe -w 5 [illegible].137 8087)
REM if %size% gtr 0 (type new_changed_stats_Table.info | nc.exe -w 5 10.91.16.137 8087)
if %size% gtr 0 (type new_changed_stats_Table.info >> alert_list.txt )

GOTO :START_Stats
```

Fig.25. Difference check in firewall access log

만약 공격자나 해킹, 악성코드에 감염된 시스템이 동일한 네트워크 대역에 대한 포트스캔을 수행하거나 동일 내부망을 목표로 텔넷이나 윈도우 터미널 서비스 포트에 접근한 이벤트가 탐지될 경우 시스템은 IP관

리시스템DB와 비교하여 정상 시스템여부를 1차적으로 검사하게 된다. 그 다음 2차적으로 시스템자원정보DB에 접근하여 방화벽에서 발견된 출발지, 목적지 IP와 포트를 기준으로 어떠한 프로세스가 해당 통신을 발생시켰는지 비교하게 된다. 프로세스 정보 중 해당 이벤트를 발생시킨 정보가 확인된 경우 3차적으로 원격접속통제시스템DB를 조회하여 정상적인 작업에 의한 신규 프로세스 발생여부를 판단하게 되며 4차적으로 작업이력DB를 검사하여 신뢰성 있는 작업에 의한 상태변화가 발생되었는지 검사하게 된다. 시스템은 이 단계에서도 신뢰성을 찾을 수 없게 되면 자산관리DB에 등록된 담당자에게 경보를 발생하게 되고 관리자는 경보발생 원인을 분석하여 침해사고 대응팀을 가동하거나 발생된 원인에 대한 결과를 지식관리DB에 등록하고 케이스를 종료하게 된다.

2.2.5 융합정보를 이용한 해킹징후 예시

네 번째 해킹징후 탐지 예시는 공격 목적지와 목적지 포트 그리고 공격 탐지명을 기준으로 목적지 IP가 보유한 자산이 취약점을 보유하고 있는지 확인하는 과정을 통해 자동으로 처리된다. 먼저 공격이 발생된 출발지, 목적지 IP, 목적지 포트, 탐지명을 하나의 이벤트로 만들고 그 결과를 지식관리DB에 조회하여 과거 발생된 이력 중 동일한 이벤트발생 여부를 확인하게 된다. 지식관리DB에서 확인되지 않는 경우에는 그다음 취약점관리DB를 참조하여 대상IP와 포트에서 서비스 중인 서비스가 해당 취약점을 보유하고 있는지 비교하게 된다. 해당 과정은 아래 〔Fig 26〕와 같은 다이어그램으로 표현할 수 있다.

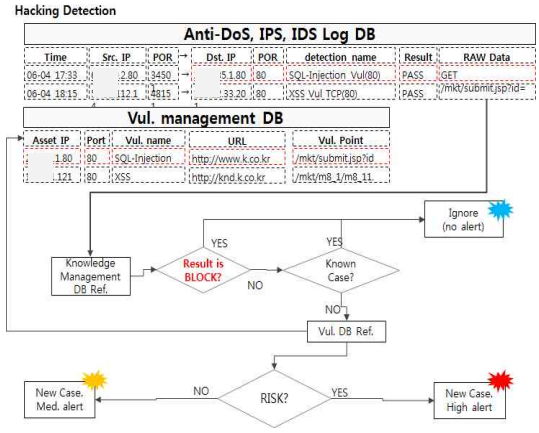


Fig.26. Sample database structure and diagram

예를 들어 탐지된 공격명에 SQL 이라는 문자열을 가지고 있고 취약점관리DB에서도 해당 문자열을 가지고 있다면 공격 대상서버는 해당 공격으로부터 위험하다는 결과를 얻게 되며 시스템은 해당 이벤트를 보안관제요원이나 분석요원에게 경보를 발생하게 된다. 발생된 경보는 반드시 확인하여야 하며 침입시도 분석결과를 관제요원은 확인하여 지식관리DB와 침해사고대응관리시스템에 재입력함으로서 아래 〔Fig 27〕과 같은 절차를 통해 과거 데이터를 비교대상 정보로 재활용하거나 과거사례 분석결과로 사용할 수 있다.

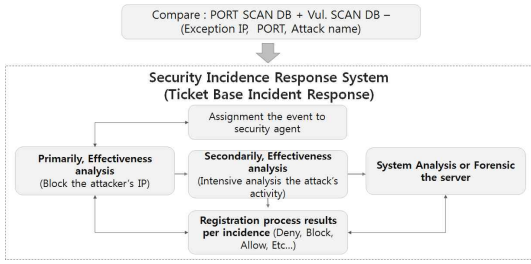
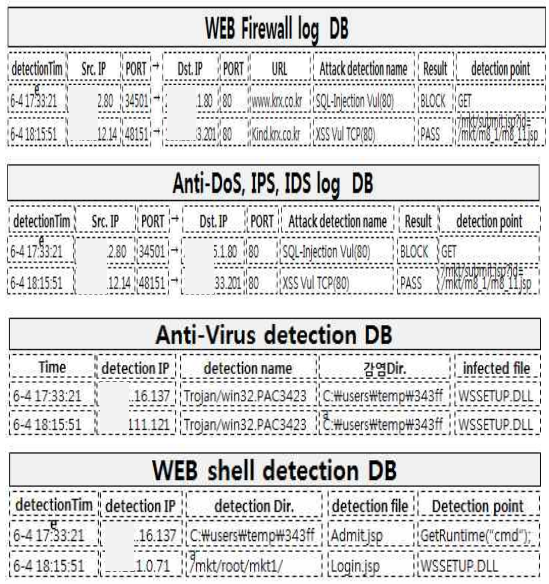


Fig.27.Incidence response and management system

위와 같이 시스템, 네트워크, 단위보안시스템, 취약점점검결과 등의 정보를 융합함으로서 위협에 대한 경보가 아닌 실제 위험한 정보를 확인할 수 있는 기반환경을 만들 수 있으며 위와 같은 융합보안관제 시나리오 분석을 위해서 아래 〔Fig 28〕의 데이터베이스 항목이 필요하다.



Firewall log DB

Time	Src. IP	PORT	→	Dst. IP	PORT	Proto	Result
6-4 17:33:21	1 .11.121	34501	→	5.1.80	8080	TCP	Accept
6-4 18:15:51	1 1.0.71	1521	→	.33.201	8090	ICMP	Deny

System information DB (network)

Time	proc name	local IP	PORT	→	target IP	PORT	Proto	status
6-4 17:33:21	/sbin/getty -8 tty2	.1.121	34501	→	5.1.80	8080	TCP	Listen
6-4 18:15:51	netcat	.0.71	1521	→	.33.201	8090	ICMP	ESTABL
6-4 21:23:41	telnet	8.1.30	47685	→	17.121	8080	UDP	CLOSE

System information DB (process)

Time	COMMND	UID	PID	SIZE	Node NAME
6-4 17:33:21	ssh	ROOT	908	4096	/sbin/getty -8 38400 tty4
6-4 18:15:51	daemon	daemon	1379	108204	/usr/sbin/console-kit--no-daemon
6-4 21:23:41	telnet	postgres	4514	113964	postgres: writer process

WEB, WAS log DB

Time	Src. IP	Meth.	Request URL	Result
6-4 17:33:21	0.2.81	GET	/m8_1/JHM094.jsp?	200
6-4 18:15:51	12.15.1	POST	/Login.jsp	500

Port scan result DB

수집Time	Target IP	포트
6-4 17:33:21	2.80	135, 445, 80
6-4 18:15:51	1.121	80, 8080
6-4 21:23:41	1.121	4447, 8090

System information DB (file)

Time	file Dir.	file name	Mod. Time
6-4 17:33:21	/lib/tls/i686/	Apt-get	6-4 17:33:21
6-4 18:15:51	/sbin/	Prc.statd	6-4 17:33:21
6-4 21:23:41	/proc/776/exe	rsyslogd	6-4 17:33:21

System Account information DB

Time	name	Pass	UID	GID	HOME DIR	Login shell
6-4 17:33:21	games	x	sys	root	/usr/sbin	/bin/sh
6-4 18:15:51	root	x	root	root	/usr/sbin	/bin/sh
6-4 21:23:41	news	x	sys	root	rsyslogd	/bin/sh

IP management System DB

Time	local IP	MAC
6-4 17:33:21	1.121	00:3a:3a:31:aa:af
6-4 17:33:21	1.125	11:31:a3:a3:ff:ff

System information (ARP)

Time	local IP	targetIP	target MAC
6-4 17:33:21	1.121	1.254	00:50:56:e9:e9:c8
6-4 17:33:21	1 121	1 110	01:30:a6:39:39:f8

Vul. management DB

Asset IP	Por	Vul. name	URL	Vul. Point
1.121	80	SQL-Injection	http:// x.co.kr	ibmit.jsp?id=%
1.121	80	XSS	http:// c.co.kr	8_1/m8_11.jsp
1.121	80	File Upload	http:// x.co.kr	5_1_m5_up.jsp
1.121	80	CSRF	http:// c.co.kr	_1/m8_11.jsp

Asset management DB

Asset IP	Srv name	ame	Div.	in/out	phone
1.121	Srv AP	Kim	MISSystem	in	4882
.0.71	srv2 AP	Lee	MISSystem	Out	4902
8.1.30	srv3 AP	Hwang	AP1System	in	7756
.0.71	srv4 AP	park	System	in	4511

Knowledge Management DB

Event Time	Src. IP	PORT	→	Dst. IP	PORT	Attack detection name	warning
6-4 17:33:21	80	34501	→	.80	80	SQL-Injection Vul(80)	Ignore
6-4 18:15:51	.14	48151	→	.201	80	XSS Vul TCP(80)	High
6-4 21:23:41	51	36541	→	.201	80	Malicious Packer Gogda	Blacklist IP
6-4 22:33:21	121	34501	→	.80	3389	MSTSC Brute Force	Exception

Fig.28.Sample Database structure and data

위 살펴본 바와 같이 시스템 상태변화를 모니터링 함으로서 해킹이나 침해사고 탐지가 가능한 환경을 구성해 보았으며 기존 통합보안 관리환경에서는 탐지하지 못하는 이벤트를 감지할 수 있다는 점에 대하여 알아보았다. 또한 이와 같은 데이터베이스를 활용하여 아래 [Fig 29]과 같이 현재 발생된 경보, 시스템상태, 과거 발생이력, 네트워크 연결 상태 등의 정보를 한눈에 볼 수 있도록 관제화면을 구성하면 보안관제요원은 즉시 현재 상태와 과거 상태를 비교하고 발생된 이벤트를 분석하고 대응이 가능하다.

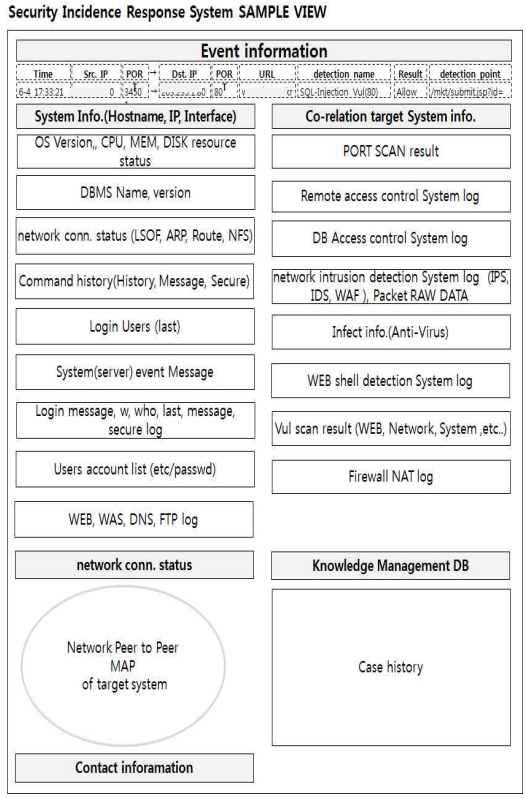


Fig.28.Sample monitoring view

III. 결론 및 제언

서론에서는 자산을 위협하는 기술과 그에 상응하는 대응방안에 대해 알아보았으며 늘어나는 정보보안시스템의 종류와 대량로그관리시스템을 이용한 융합보안관제기술에 대하여 알아보았다. 또한 본론에서는 융합보완관제기술에 대한 방법론과 아키텍처를 실 예시와 사례를 통해 대응 방안을 알아보았으며 실제 공격기술과 대응 방법에 대한 연구 자료를 기술하였다. 융합이라는 것은 서로 상관관계가 모호한 정보를 통합함으로서 새로운 가치를 이끌어내는 것이며 보안 전략/계획, 자산식별/평가, 위험관리 그리고 법률과 사람과 서로 빠짐없이 융합되어야만 진정한 정보보호가 가능해 진다는 점을 강조하고 싶다. 금 번 연구를 통해 어느 한 분야에 치중한 기술은 기업이나 기관의 보안담당자가 보고자 하는 정보를 제공해 주기에는 부족하다는 점을 알 수 있으며 특정 분야에 치우진 정보가 아닌 시스템, 네트워크, 데이터베이스, 어플리케이션, 사용자활동정보, 네트워크 포렌식 등 다양한 정보 수집하고 융합하여 상호연관 분석하여야 한다는 점을 알 수 있었다. 본 논문에서는 크게 4가지 사례에 대하여 상세히 알아보았으나 지금까지 구성된 보안시스템을 뛰어넘어 CCTV 정보와 출입통제 시스템 그리고 시스템원격접속통제시스템을 연동하여 누가, 언제, 어떤 사무실, 어느 PC에서 어떤 계정을 이용하여, 어떤 네트워크 경로를 통해 어떤 정보에 접근하였는지를 실시간으로 감지하는 방법 등 실세계에서 일어나는 정보를 가상의 세계에서 실세계까지 연동할 수 있는 기반을 만들기 위한 노력이 더욱 필요하므로 시나리오 개발과 그에 따른 검증작업을 통해 증명해 나가야 할 것이다. 또한, 이러한 대량의 데이터를 수집하는 과정에 있어서 서버나 네트워크, 보안시스템 등의 시스템상태정보와 이벤트 로그정보를 활용함에 있어서 문제는 없겠으나 APT공격 대응을 위해서는 일반 사용자의 네트워크, 디스크, 시스템 상태변화(사용자가 접근한 URL 및 IP정보, DNS Query 정보 등) 정보 등 사용자 활동정보를 수집하게 된다. 이러한 정보는 기업의 생산성에 기여하는 서버는 사용자의 개인적 Activity가 존재하지 않으므로 개인정보보호관점의 문제가 발생하지 않겠으나 사용자 PC의 활동정보가 모니터링 될 경우 사적 용도의 웹 페이지 접근기록이나 생산된 문서 등에서 개인정보[9]가 수집될 수 있다. 이러한 관점에서 수집되는 정보가 개인의 사생활 침해의 요소는 없는지 또한 법률적 관점에서의 고찰이 필요할 것으로 사료된다.

References

[1] YongDal-Jung, "IT Security Guide for Enterprise v.6," HawSing Media, Seoul-Ganam-YeoksamDong, pp.39, Feb. 2011

[2] Microsoft, "Querying nonSQL data stores with a SQL-style language", US-0039442, pp.1, Apr. 2012

[3] TADAO MURATA, "Petri Nets:Properties, Analysis and Applications," Proceedings of the IEEE, Vol. 77, pp.541-580, APR. 1989

[4] YangHa-Chun, "Hacking Detection Mechanism of Cyber Attacks Modeling," The Journal of the Korean institute of electronic communication sciences v.8 no.9, pp.1313-1318, Jan. 2013

[5] Sangik-Lee, "A study on integrity of the gathering log data in network forensic," DDC : 005.8 22, Aug. 2009

[6] DongHee-Lee, "A study on Improved Convergence Security Monitoring System model," Journal of information and security v.11 no.5, pp.3-12 , 1598-7329, Jan. 2011

[7] OkHyun-Ha, "A Study on Conversion Security Control System for Industrial Security," Journal of information and security v.9 no.4, pp.1-6, Dec. 2009

[8] ByongRae-Cha, "Normal Behavior Profiling based on Bayesian Network for Anomaly Intrusion Detection," Journal of the Korea society of computer and information v.8, no.1, pp.103-113, Mar. 2003

[9] DaeSun-Choi, "Risk analysis for Private information," Journal of information and security, v.23 no.3, pp.56-60, Jun. 2013

〈저자소개〉

황 동 욱 (Donguk Hwang) 정회원
2014년 02월: 숭실사이버대학교 정보보안학사
2005년 11월~2007년 11월 : 한국정보보호진흥원 침해사고대응지원센터
2008년 10월~2010년 01월 : (주)나우콤 보안사업부 침해사고분석팀
2010년 02월~현재 : 딜로이트안진회계법인 리업리스크자문본부
〈관심분야〉 SCADA, 모의해킹, 디지털포렌식

이 상 훈 (Sanghun Lee) 정회원
2012년 02월: 한국외국어대학교 경영정보대학원 경영학(MIS) 석사
2003년 10월~2005년 06월 : ㈜에이쓰리시큐리티컨설팅 보안컨설팅팀
2005년 07월~2009년 02월 : ㈜오픈타이드코리아 컨설팅 본부
2009년 02월~현재 : 딜로이트안진회계법인 리업리스크자문본부
〈관심분야〉 정보보호관리체계(ISMS), 보안관제, 리스크 분석 등