Journal of the Korea Convergence Society
Vol. 9. No. 7, pp. 55-62, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.7.055

A Study on the Real-time Cyber Attack Intrusion Detection Method

Jae-Hyun Choi, Hoo-Jin Lee*
Department of Smart Convergency Consulting, Hansung University

실시간 사이버 공격 침해사고 탐지방법에 관한 연구

최재현, 이후진*
한성대학교 스마트융합컨설팅학과

Abstract Recently, as the threat of cyber crime increases, the importance of security control to cope with cyber attacks on the information systems in the first place such as real-time detection is increasing. In the name of security control center, cyber terror response center and infringement response center, institutional control personnel are making efforts to prevent cyber attacks. Especially, we are detecting infringement accident by using network security equipment or utilizing control system, but it's not enough to prevent infringement accident by just controlling based on device-driven simple patterns. Therefore, the security control system is continuously being upgraded, and the development and research on the detection method are being actively carried out by the prevention activity against the threat of infringement. In this paper, we have defined the method of detecting infringement of major component module in order to improve the problem of existing infringement detection method. Through the performance tests for each module, we propose measures for effective security control and study effective infringement threat detection method by upgrading the control system using Security Information Event Management (SIEM).

Key Words : Security Control Center, ESM, SIEM, Correlation Analysis, Cyber Crime

요 약 최근 다양한 사이버 범죄 위협이 증가하는 추세로 정보시스템을 대상으로 공격하는 사이버 공격에 대해 실시간 탐지 등 최전선에서 초동 대응을 해야 하는 보안관제의 중요성이 높아지고 있다. 보안관제센터, 사이버테러 대응센터, 침해대응센터 등의 이름으로 기관의 관제인원들은 사이버 공격 예방을 위해 많은 노력을 하고 있다. 특히 침해사고 탐지를 위한 방법으로 네트워크 보안장비를 이용하거나 관제시스템을 활용하여 탐지를 하고 있지만 장비 위주의 단순한 패턴기반으로 관제를 하는 방법으로는 침해사고의 예방을 위한 방법으로는 부족하다. 그러므로 보안관제시스템은 지속적으로 고도화 되고 있으며 침해위협에 대한 예방활동으로 탐지방법에 대한 개발과 연구가 활발히 진행되고 있다. 이에 본 논문에서는 기존 침해사고 탐지 방법에 대한 문제점 개선을 위해 주요 구성 모듈의 침해사고 탐지 방법을 정의하고, 성능테스트를 통해 효율적인 보안 관제를 위한 방안을 제시하고 SIEM(Security Information Event Management)을 활용한 관제시스템 고도화를 통하여 효과적인 침해위협 탐지 방법을 연구하고자 한다.

주제어 : 보안관제센터, 통합보안관리시스템, 보안정보 및 이벤트 관리시스템, 상관분석, 사이버범죄

1. Introduction

Even a few years ago, the security control system just checked the availability of various systems (CPU, Memory, Disk, etc.). Since then, the control systems have evolved into enterprise security management

*Corresponding Author : Hoo-Jin Lee (hjiee@hansung.ac.kr)
Received May 29, 2018 Revised July 3, 2018
Accepted July 20, 2018 Published July 28, 2018

(ESM) and have evolved into a system that integrates and manages the actual logs of security devices.

Currently, researches in the domestic and foreign security market are actively progressing and ESM is gradually being developed as a security information & event management (SIEM) integrated control system. The evolution from ESM to SIEM has given rise to many impacts and changes in security management. Since ESM is a control system that integrates and manages the logs of security equipment and SIEM can independently parse the data fields in the logs of security equipment, SIEM equipment gives opportunity to expand the scope of control. The evolution to SIEM enabled us to create a correlation analysis policy for scenarios that use big data and created an environment for sophisticated analysis with independent parsing function[1,2].

In this paper, we propose an effective method to detect intrusion threats through scenarios for prevention of infringement accidents by measuring the effectiveness of control system using SIEM, we will study the efficient control system using analytic policy and propose verification of correlation analysis policy[3].

2. Necessity of Improving Detection Methods for Invasive Accidents

It is necessary to improve the detection method of infringement to realize the safe cyber space for infringement accident by increasing the necessity of improvement of core functions due to various environmental changes and strengthening cyber infringement response system[4].

Security management technologies include ESM and SIEM. ESM provides modularized functions for each security function and solution product and is developed to perform consistent monitoring by integrating collected data[8]. Through the introduction of ESM, data that is poured from various security equipments can be gathered consistently on a single screen, enabling effective security control[5].

The ESM consists of three components: agent, manager, console and event logs are collected through the agents installed in each security solution and transmitted to the manager. The security officer processes various events through the console provided by the manager.

As the log data generated by the increasing security equipment grows exponentially and the cyber attack type becomes complex over a long period of time, big data based SIEM is needed[7].

Table 1. Comparison of ESM and SIEM

Item	Difference between ESM and SIEM
Justice	Operational and in-depth analysis from the perspective of disability management, expanding into compliance concerns
Management / Analysis target	Extend management and analysis
Core uses	Latest security threat trend response (APT attack, long-term attack, etc.)
Threat detection characteristics	Support in-depth analysis and association analysis
Collection/ Save	Overcome the RDBMS-based processing delay
Visualization	Various report support
User	Provide a variety of reports from a user perspective (dashboards, reports, etc.)
Detection error	High detection accuracy

3. Intrusion Response System Introduction

3.1 Summary

The infringement incident response system is a system for ensuring the security of the information system from intelligent cyber security threats by collecting repeated and regular log data generated during IT security control[2].

3.2 Main configuration module

As shown in Table 2, the main modules of the infringement response system are a security information management module, security information integration module, correlation analysis module, real-time security control module, cyber security support module, threat information detection module. In addition, there are various modules but major modules are presented in Table 2.

Table 2. Major module

Classification	Explanation
Security information management module	◦ Security information and traffic collection in the information protection of network and network resources ◦ Transmission of information for analyzing information system infringement attacks such as normalization, filtering, and shortening
Security information integrated module	◦ Integrate and manage the security information generated by the linking organization ◦ Analysis and processing of infringing attack information by the primary control policy ◦ Transmit normalized real-time alarm to correlation module
Correlation analysis module	◦ Correlation analysis between heterogeneous security information based on normalized real-time alarm ◦ Provide security control function based on risk index and risk index
Real time security control module	◦ Support real-time monitoring by visualizing infringing attack information ◦ Provides management and management functions based on security control such as linkage institution management and statistical information provision
Cyber safety support module	◦ Provides statistical information such as network traffic status and invasion attack information by network ◦ Notification of direct infringement at a linked organization. Providing information on the reception function and providing information on major information protection trends.
Threat information detection module	◦ Providing real-time intrusion threat information from the network ◦ Detection and analysis of infringement threat information by detection rules

3.2.1 Security information management module

The security information management module is a module that collects various security information generated in the interworking network and the information protection system in real time and generates and transmits basic information for analyzing the invasion attack.

Table 3. Security information management module function

Function	Explanation
Manage logs	◦ Designed based on encryption communication between security information management module and collection module
	◦ Guaranteed retransmission when missing data transmission between security information management module and integration module
	◦ It provides the indication of the cause of not receiving log through its own security check on the log collection per connected security device - Provides self-checking function of information protection system log transmission, log format inconsistency, network failure, log loss due to system load and various faults - Tracking and responding functions by creating function-specific log file for security information management module
	◦ Software patching and configuration management must be possible through updated files and "integrity" verification function is provided.
Installation management	◦ Providing user interface for security information management module installation and security equipment interworking - Agency code, organization name, security equipment name, interlock key value User input - Querying and analyzing your own log files - Rollbacks to software patches and automatic backups when settings are changed

The configuration of the security information management module is divided into the collection and management functions and the configuration diagram is shown in Fig 1.

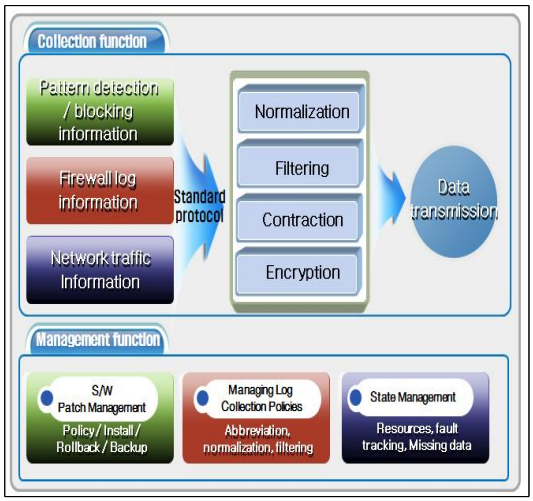


Fig. 1. Security information management module configuration diagram

3.2.2 Security information integration module

The security information integration module integrates and manages the security information generated by the interworking organization and generates and transmits the normalized real-time alarm through the primary security control policy and the institution profiling threshold.

Existing ESM have the ability to simply collect and transmit security events.

The security information management integration module provides normalization and filtering function according to the basic control policy of collected security events, and provides correlation analysis and integrated control basis through linking of alarm data and TMS data of ECSC internal security system[6[9]].

The functions of the security information integration module are shown in Table 4, and the integration module process is shown in Fig 2.

Table 4. Security information integration module function

Function	Explanation
Security information integration	◦ Security log description collected from individual interworking organizations
	◦ Threat of infringement by the primary control policy, normalization of security information
	◦ Attack type and type of attack data by organization security information filtering for collected thresholds
	◦ Network information filtering on thresholds of collected data by organization
	◦ Alert message transmission using correlation analysis module (over-threshold and pattern-matching security information)
	◦ Store and manage all security information that is consistent with and inconsistent with the control policy
	◦ Normalize the alarm data of the security control system that is being constructed and operated to the specified form and send it to the correlation analysis module - Normalization and transmission of alarm data in the infringement threat management system - Normalization and transmission of alarm data of integrated security control system
	◦ Integration analysis of infringement threat system through linkage of integrated threat analysis system - Send security information collected based on infringement threat system including payload value - Integrated threat analysis system analysis result is integrated into correlation analysis module,
Configuring security information	◦ "Security information integration module" should support parallel configuration in consideration of scalability in the future. In addition, it supports integration and management of physical and logical data

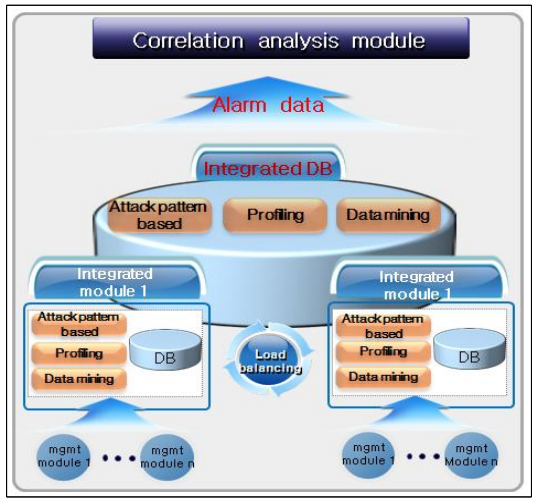


Fig. 2. Integrated module process

3.2.3 Security information correlation analysis module

The security information correlation module is a module that performs correlation analysis between information security systems against various security event occurrences between these models based on real-time alarm, derives the final risk, and supports security control tasks.

The functions of the security information correlation analysis module are shown in Table 5, and the correlation analysis module configuration diagram is shown in Fig 3.

Table 5. Security information correlation analysis module function

Function	Explanation
Correlation analysis	◦ Correlation analysis between alarm data generated by security control policy by type of invasion attack - Correlation analysis through classification system (attacker's IP, Port, string, keyword, etc.) that defined the information generated from various security devices - Correlation analysis between security information based on stepwise correlation analysis policy - Load adjustment by correlation analysis application standard (semi-automatic / automatic) - History management of correlation analysis provides past history of the same situation - Backtracking of attacks
	◦ Calculate and visualize the risk index and risk based on the correlation analysis result data - Evaluate the risk for alarm data based on the policy-specific risk for correlation analysis and calculate final risk - Visualization of final risk and monitoring support - Management of initial risk and risk index calculation criteria
	◦ Risk index = initial risk index × weight by attack type + (Σ correlation analysis risk index) - The risk index is adjusted according to the National Cyber Safety Center (NIS) cyber crisis alarm rating - Weights adjustment through correlation analysis by attack type through security control policy

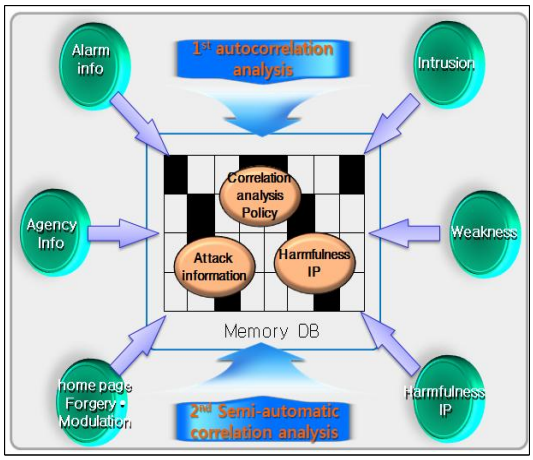


Fig. 3. Structure of correlation analysis module

3.3 System configuration diagram

The information security data of the linking organization is collected and normalized by the threat detection module based on the detection rule created in the security control center, and the correlation analysis is performed. Figure 6 shows the structure of the system for responding to infringement incidents in order to build and operate a preventive-based security control system based on the statistical-based security control system by strengthening continuous information security control ability as a result of the analysis and the result.

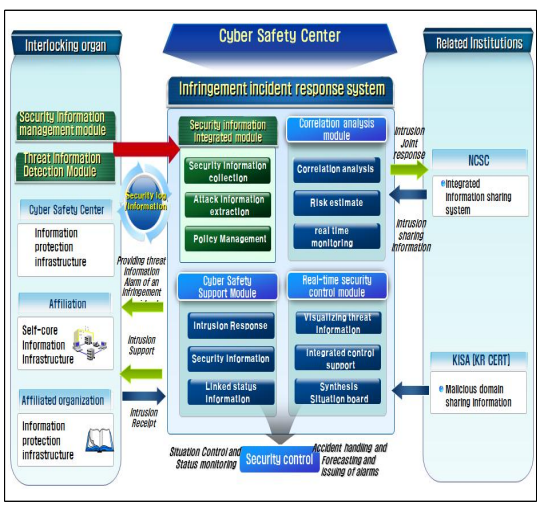


Fig. 4. Correlation analysis module process

3.3.1 Hardware specifications

Table 6. Hardware specifications module function

Hardware	Recommended specification	EA
Analysis and integration server	UNIX OS family recommended	3
	CPU 8 core	
	Memory 8GB	
	HDD 300GB X 2 EA	
DB / File server	Oracle	1
	CPU 16 core	
	Memory 16GB	
	HDD 300GB X 4 EA (1TB)	

4. System performance testing

4.1 Management module performance test

Table 7. Management module scenarios and performance requirements

Management module scenarios and performance requirements	
Scenario	◦ Load 256 random attack types using Packet Generator ◦ Syslog generates 40,000, 50,000, and 60,000 packets per second three times. ◦ Normalize and filter string-based syslogs at 960,000 events per minute, targeting 16,000 events per second. ◦ The processed event is converted into raw data and transmitted to the security information integration module
Performance requirements	◦ It should be possible to process more than 16,000 cases per second (960,000 cases per minute) as a performance test standard.

The performance of the security information management module was tested three times. The test scenarios and performance requirements are shown in Table 7 and the test results are shown in Table 8. In addition, the average time of 3,000 raw data was found to satisfy the reference time (within 10 minutes) and the average processing time was 559 seconds.

Table 8. Management module performance test results

No	Load per second	Number of transaction	Average number	Time
1	40,000	1,056,000	16,123	65 sec
2	50,000	1,056,000	18,206	58 sec
3	60,000	1,056,000	20,308	52 sec

4.2 Integration module performance test

Table 9. Integration module scenarios and performance requirements

Integration module scenarios and performance requirements	
Scenario	◦ From the security information management module, receive 10,000 raw logs per minute (600,000 per minute). ◦ The control policy for strings is applied through the primary control policy and stored in the original data database at the same time. ◦ Send alarm data to correlation analysis module
Performance requirements	◦ It should be possible to process 10,000 or more per second (600,000 per minute) as a performance test standard

As a result of performing the performance test of the security information integration module three times, the performance satisfying the performance requirement of an average of 10,000 per second was achieved.

Table 10. Integration module performance test results

No	Load per second	Throughput	Average number	Time
1	1,000	600,000	10,000	60 sec
2	1,000	600,000	10,000	61 sec
3	1,000	600,000	10,000	59 sec

4.3 Correlation analysis module performance test

As a result of performing the performance test of the correlation analysis module three times, the average processing time of 559 seconds (9.32 minutes) was obtained from 3000 raw data average times, and the performance satisfies the performance requirements.

Table 11. Correlation analysis module scenario and performance requirements

Correlation analysis module scenario and performance requirements	
Scenario	◦ Send a string packet to the packet generator. ◦ Generate raw data after normalization and filtering processing through management module. ◦ The generated raw data generates alarm data after processing through the primary module policy of the integration module.

	◦ The generated alarm data is transmitted to the correlation analysis module and displayed on the real-time control screen.
Performance requirements	◦ The standard time for visualization in a form that a single security information is generated and can finally be checked through the collection and analysis steps is set to 10 minutes or less. ◦ Calculation method: Calculate the time (date of completion of automatic correlation analysis - management module collection date and time) and apply the average value of 3,000 security information

Table 12. Correlation analysis module performance test result

No	Load per second	Collection time	Display time	Processing time (Within 10 minutes)
1	3,000	456	120 sec	576 second (9.6minute)
2	3,000	431	120 sec	551 second (9.18minute)
3	3,000	432	120 sec	522 second (9.2minute)

4. Conclusion

So far, we have examined the efficiency of cyber threat analysis and response capability and the effectiveness of detecting and responding to infringement accidents through the correlation analysis of the security information of the connected organizations and providing effective information protection services for the interworking organizations.

In this paper, we propose an effective method to detect threat of intrusion by measuring the effectiveness of each module of SIEM proposed in this paper. An efficient control system was studied using the existing control method and correlation analysis policy with new modules. We could get satisfactory results through system performance test for correlation analysis policy, and we could get better results as test progressed.

In order to respond to evolving IT infringement accidents in the future, it is necessary to establish a roadmap for continuous improvement in order to strengthen cyber infringement response system, which is indispensable to changes in the IT technology paradigm such as the cloud and the Internet of things.

REFERENCES

[1] J. G. Um & H. Y. Kwon, (2016). Model proposal of detection method of cyber attack using SIEM, Journal of *IIBC, 16(6),* 43-54.

[2] J. H. Sim, S. H. Kim & T. M. Chung, (2014). *A Survey of Solutions using Security Information Event Management.* Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 390-391.

[3] S. B. Kang, (2011). *(A) study on the effective countermeasures for preventing computer security incident.* Doctoral dissertation Korea University, Seoul.

[4] S. M. Park, (2011). *An Empirical Study of Cyber Security Center Model in Public Sector.* Doctoral dissertation Soongsil University, Seoul

[5] H. H. Kang, (2014). *(A) study on the improvement of alert function in ESM for effective attack detection, Master dissertation,* Sungkyunkwan University, Seoul.

[6] Y. Lee, (2017). *A study on effective attack detection using threat scoring function through ESM.* Master dissertation, Sungkyunkwan University, Seoul.

[7] H. Kim, (2010). *A study on malicious code detecting by ESM correlation. M.S. dissertation,* Korea University, Seoul.

[8] G. W. Lee, (2017). *Design of integrated security system for intelligent continuous threat detection and active response.* Master dissertation Korea University, Seoul.

[9] D. J. Jeon & D. G. Park, (2014). Analysis Model for Prediction of Cyber Threats by Utilizing Big Data Technology, *Journal of the Korea Information Science Society,* 81-100.

[10] B. J. Jeon, D. B. Yoon & S. S. Shin. (2017). Improved Integrated Monitoring System Design and Construction, *Journal of Convergence for Information Technology,* 25-33.

[11] S. S. Nam & C. H. Seo, (2015), Context cognition technology through integrated cyber security context analysis, *Journal of digital convergence,* 313-319.

[12] B. J. Jeon, D. B. Yoon & S. S. Shin. (2017). Integrated Monitoring System using Log Data, *Journal of Convergence for Information Technology,* 35-42.

[13] Y. H. Kim & H. H. Nam, (2014). Log Analysis

Supporting System based on Log Data for Efficient Big Data Analysis, *Journal of Korea Information Science Society*, 936-938.

[14] NIS, MSIP, KCC, MOSPA, KISA, NSRI, (2013). *2013 National Information Security White Paper*.

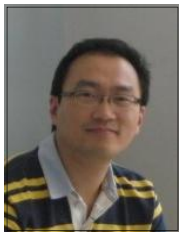
[15] I. S. Jeon, K. H. Han, D. W. Kim & J. Y. Choi, (2015). Using the SIEM Software vulnerability detection model proposed, *Journal of the Korea Institute of Information Security and Cryptology, 25(4)*, 961-974.

[16] C. J. Park, (2014), Present Status and Analysis of Domestic Security Control System, *Korea Electronics and Telecommunications Society, 9(2)*, 261-266.

최 재 현(Choi, Jaehyun) [정회원]

- 2011년 2월 : 한국방송통신대학교 컴퓨터과학과(이학사)
- 2013년 8월 : 한국방송통신대학교 정보과학과(이학석사)
- 2017년 2월 ~ 현재 : 한성대학교 스마트융합컨설팅학과 박사 재학
- 2016년 7월 ~ 현재 : (주)싸이버원 수석컨설턴트
- 관심분야 : 정보보안, 인공지능, 빅데이터
- E-Mail : jaehyun.choi@hansung.ac.kr

이 후 진(Lee, Hoojin) [정회원]



- 2007년 12월 : The University of Texas at Austin, Electrical & Computer Engineering(공학박사)
- 2008년 1월 ~ 2009년 6월 : Freescale Semiconductor, Inc., System & Architecture Engineer
- 2009년 9월 ~ 현재 : 한성대학교 스마트융합컨설팅학과 교수
- 관심분야 : 통신 및 네트워크 시스템, 멀티미디어 신호처리, 정보보안
- E-Mail : hjlee@hansung.ac.kr