Monthly Security Report

2018 December

Cover Story

How to use TM through Human Resource information integration

2019's Security threats, prospect and potential responses

The alternative to cloud servers, edge computers

IGLOOSECURITY

This report was written, based on the event, analysis, cyber security issues and their trend collected from the SIEM solution installed at IGLOO SECURITY's Security Operation Center. IGLOO SECURITY strives to protect its client from cybersecurity threats through continuous monitoring (24/7, 365days), analysis and response of cybersecurity issues.

Cover Story

1. Monthly Security Issues

- Monthly Security Issues

2. IGLOO Statistics

- Monthly Attack Service Trend and Analysis
- Detailed analysis according to different attack patterns

3. SIEM Guide (SPiDER TM V5.x)

- How to use TM's Human Resource Information Integration

4. Tech Note

- 2019's Security Threats, Prospect and Potential Responses

5. Special Column

- Edge Computing, the Alternative to Cloud Environments

6. Focus On IGLOO SECURITY

- This month's IGLOO SECURITY

01 Monthly Security Issues

'The US President Trump, the hardest decision for North Korea, Will go own way???' … found malicious file disguised as an interview

- Malicious file, disguised as an interview from the US President Trump, has been found. It is inferred that North Korea is liable for phishing attack same as impersonating the Blue house(The Korean presidential residence).
- Attached malicious file titled 'The 2nd North American Summit with Jung-Eun Kim in early next year,' When malicious code is executed, it is likely to be exposed to additional malicious files or infected system information by attempting to connect to a specific host server.
- This malicious file has a style similar to the three North Korean presumed cyber attacks that have occurred in the past. Only some of the code was analyzed as changed variants.

‘It has evolved over 4 years’… Transforming mobile malware with multiple functions

- ‘Rotexy,' mobile malware but originally spyware, was developed over the last four years and turned into a banking Trojan with many features.
- According to Kaspersky, Rotexy was merely malware to steal SMS messages when it first appeared in October 2014, but the latest version of Rotexy has evolved into a banking Trojan horse with ransomware functionality, it also appears to have an operating function.
- Experts are advised to pay attention to mobile security, saying that there is a temporary measure to deal with it, but it is likely that an updated Rotexy will soon be released.

OSI Soft which 65% of Fortune 500 companies are using has been breached

- According to the OSI Software announcement, attackers steal credentials from employees, interns, consultants, and etc. and use them to access OSI soft systems. Approximately 29 computers and 135 accounts were affected at least, and it is analyzed that all of OSI domain accounts were under the influence of the attack.
- Security experts say OSI soft products can be key gateways to reach targets (Fortune 500 companies, etc.) and emphasize that producers-users-partners need to work to increase the security of their associated digital ecosystem.

'Warner Crane Ransomware, I'm not dead yet' ... The importance of a patch is not enough

- Warner Cry 'Ransomware, which first appeared in May of last year and caused huge damage worldwide, still exists. According to recent data released by Kaspersky Lab, 28 percent of the Crypto attacks that occurred during the third quarter of 2018 were Warner Cry, and about 75,000 people were infected.
- Security experts say that despite patches for the vulnerability, many users are not doing. Therefore, Security experts recommend OS patches fix the latest vulnerabilities and update the security solution and vulnerability database.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

Monthly Security Issues

WordPress plug-in which is related GDPR found fatal vulnerability

- A plug-in for WordPress (GDPR compliance) that helps websites and online store managers avoid violating the GDPR is causing problems because of a fatal security flaw that could allow an attacker to control the website
- According to the security vendor Defiant, hackers were able to actually control the site by exploiting vulnerabilities to change settings, register new user accounts, and set the privileges of this new user as an administrator
- Defiant says that attackers were able to take control of the Web site in such a way as to send spam e-mails, attack phishing / watershed halls but did not find a final payload that could play a key role in such attacks. In addition, it is likely that attackers don't tend to reveal their identity in order to collect multiple sites and sell them in packages or to achieve their intended purpose

'If a hacker makes a medical diagnosis?' ... Some healthcare equipment has been found vulnerability to manipulate medical data

- Serious vulnerabilities have been found in Roche products, healthcare companies in Switzerland, that could endanger customers' lives
- According to Medigate which is medical IoT equipment security vendor, there were five high-risk vulnerabilities in Roche that were rated CVSS of 6.5 to 8.3 on three types of products, and if exploited, It appears that protocols for medical equipment and medical data can be easily manipulated.

'What are the next-generation security technologies to lead 2019?' Korea Internet & Security Agency, 9th generation security technology announcement

- Korea Internet & Security Agency(KISA) announced nine next generation security technologies selected with ETRI, KAIST, and Kookmin University in order to create a base for revitalizing the information protection industry. The contents are as follows:

  ① 'Cyber-threat intelligence analysis (CTI) and information sharing technology,' which add expert analysis for threat information,

  ② 'Cloud-based IoT threat self-analysis and response technology' that collects security threat information of IoT devices

  ③ Machine learning cyber-immunization technology, IoT security vulnerability search sharing, and testing technology that remember the normal state of the system. Plus, it identifies the external attack and removes the inherent security vulnerability to return to the normal state

  ④ 'Android-based bio-signal authentication technology'

  ⑤ 'Mobile-based biometric performance testing tool'

  ⑥ The 'cyber self-mutation technology for active proactive security' that responds actively to changes in the subject of protection according to the situation

  ⑦ 'Smart lightweight IoT security technology' to block out unauthorized access by preventing the device from being tampered with by hacking.

  ⑧ 'Binary code analysis technology'

  ⑨ 'Malicious code analysis technology' that detects and classifies a large number of malicious codes based on deep learning,

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

Monthly Security Issues

'I know where you were last summer'…personal information of 500 million clients leaked in Marriott Hotel

- One of the world's largest hotel groups, Marriott International Starwood Hotel's reservation system was hacked, exposing the personal information of 500 million clients. The Starwood Hotel Brands include: Sheraton, Westin, Le Méridien Hotel Etc.
- Marriott realized that they were being hacked last September and conducted an investigation on the issue and discovered that they were being hacked since 2014. it is estimated that 320 million people out of 500 million have had their passport numbers and phone numbers leaked and the rest of the clients seemed to have had their credit card numbers leaked. This is the largest information leak since the Yahoo user information leak from two years ago, where the information of 320 million people was leaked.

'An Embarrassing First Place'…German Chatting platform 'Cuddly' has been fined €20,000 for violating GDPR policy

- The first case of fining GDPR violation has been set in Europe. German chatting platform Cuddly has been fined €20,000 for having the personal information of approximately 8,000 users leaked through a hack last July.
- Cuddly was found guilty of violating GDPR policy by storing user passwords in plain text. However, the fine was minimized due to the fact that Cuddly quickly called in on authorities and cooperated with them after realizing the situation.

'Who are you?...G-mail vulnerability of leaving the 'From' header blank has been exposed

- A vulnerability in Google's G-mail, where the 'from' header can be altered to make it seem as if an unknown user has sent the e-mail, has been discovered This vulnerability is potentially harmful since attackers may disguise themselves as public institutes and send fals alarm mails or false system warning mails.
- According to Tim Cott⊂n, a software developer who discovered this vulnerability and rightly named it the 'ghost email' vulnerability, the ghost email can be made by entering the recipient's email address on the 'from' header and adding long tags such as: *object, script, img* etc. which hides who the email is really from.
- Cotten feared that this vulnerability to lead to an increase in phising, which led him to contact Google to handle the vulnerability.

'I want to know your password~'…Instagram exposes vulnerability of their new function developed to prepare for GDPR

- Ahead of the application of Instagram's 'Data Download' function, a vulnerability of many Users' password appearing on the URL was discovered. The 'Data Download' function was meant for Users to read and download their own user information.
- Several security experts stated that this incident in itself did not affect many Users, however criticized Instagram for handling personal information in a careless manner. Instagram announced that they recognize the severity of the situation and that they will take measures concerning the situation.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

02 IGLOO Statistics

The IGLOO SECURITY SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats become predictable.

Monthly Attack Service Trend and Analysis

Monthly Attack Service(Port) TOP 10

This month's collected data shows that the Unassigned(TCP/9900), Telnet(TCP/23) and MYSQL(TCP/3306) events have risen compared to last month. The Unassigned(TCP/8001) event has newly entered the ranks.

※ Based on IGLOO SECURITY SOC SIEM data collection

Rank	Service (Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	1,634,150,219	42.29%	-
2	DNS(UDP/53)	757,268,920	19.60%	-
3	HTTPS(TCP/443)	566,134,775	14.65%	-
4	Microsoft-DS(TCP/445)	381,407,336	9.87%	-
5	SNMP(UDP/161)	181,547,387	4.70%	-
6	Unassigned(TCP/9900)	153,393,229	3.97%	▲1
7	Telnet(TCP/23)	89,587,160	2.32%	▲2
8	SYSLOG(UDP/514)	43,447,319	1.12%	-
9	MYSQL(TCP/3306)	30,897,701	0.80%	▲1
10	Unassigned(TCP/8001)	26,024,457	0.67%	NEW
Total		3,863,858,503	100.00%	-

[Table2-1] TOP 10 Monthly Attack Ports

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

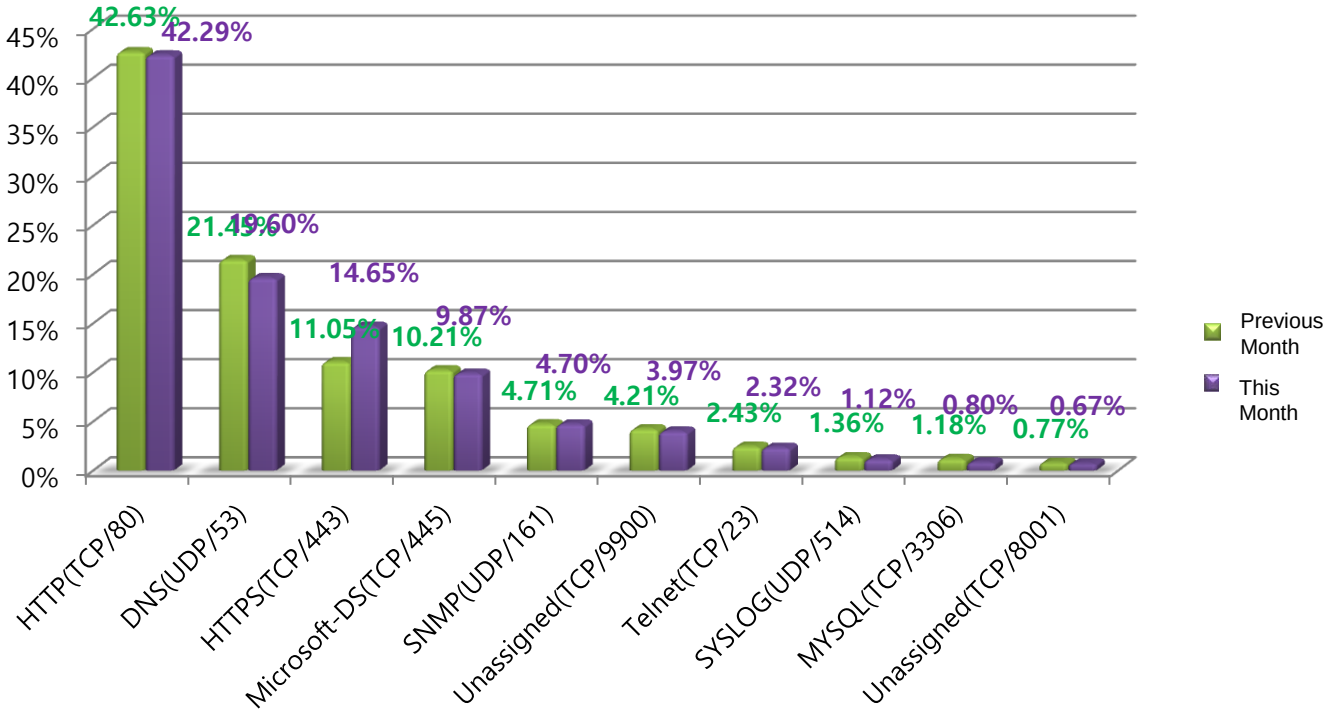
02 IGLOO Statistics

Monthly Attack Service and Trend Analysis

Monthly Attack Service(Port) cases compared to last month

The data collected during the month of December indicated that, compared to last month, there is no noticeable pattern besides a rise in HTTP port detection ratio.

The Unassigned(TCP/8001) case has newly entered the rankings. It is recommended that a firewall policy is established after verifying whether the undefined service port is being used or not. It is also recommended that the User PC's and servers prepare in advance for vulnerabilities through the newest patches.



[Figure2-1] TOP 10 Monthly Attack Ports

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

02 IGLOO Statistics

IGLOO SECURITY is capable of understanding the most recent attack trends through the attack patterns collected in its Security Operation Center (SOC).

Monthly Attack Service Trend and Analysis

Monthly Attack Service Pattern TOP 10

This month's attack event analysis report indicates that the Multi Packet Inspection, Dcom_TCP_Sweep, MS WINS Server Registration Spoofing Vuln-1 and HTTP Connection Limit Exhaustion Attack events have increased compared to last month and the UDP Tear Drop event has dropped in rank. Besides that, the RPC nfsd Overflow and HTTP POST Session Exhaustion Attack (By rudy) have newly entered the ranking.

※ Based on IGLOO SECURITY SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	622,103,040	77.30%	-
2	ACK Port Scan(F/W Scan)	106,147,956	13.19%	-
3	MySQL-Server Login Brute force	29,188,420	3.63%	-
4	Multi Packet Inspection	10,822,040	1.34%	▲3
5	Dcom_TCP_Sweep(MSBlaster Worm Messenger)	9,141,054	1.14%	▲1
6	HTTP POST Session Exhaustion Attack(By rudy)	8,043,986	1.00%	NEW
7	MS WINS Server Registration Spoofing Vuln-1 [Req](UDP-137)	5,634,060	0.70%	▲1
8	HTTP Connection Limit Exhaustion Attack (By Slowloris)	5,315,650	0.66%	▲1
9	RPC nfsd Overflow	4,445,514	0.55%	NEW
10	UDP Tear Drop	3,941,340	0.49%	▼5
Total		804,783,060	100.00%	-

[Table2-2] TOP 10 Monthly Attack Patterns

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

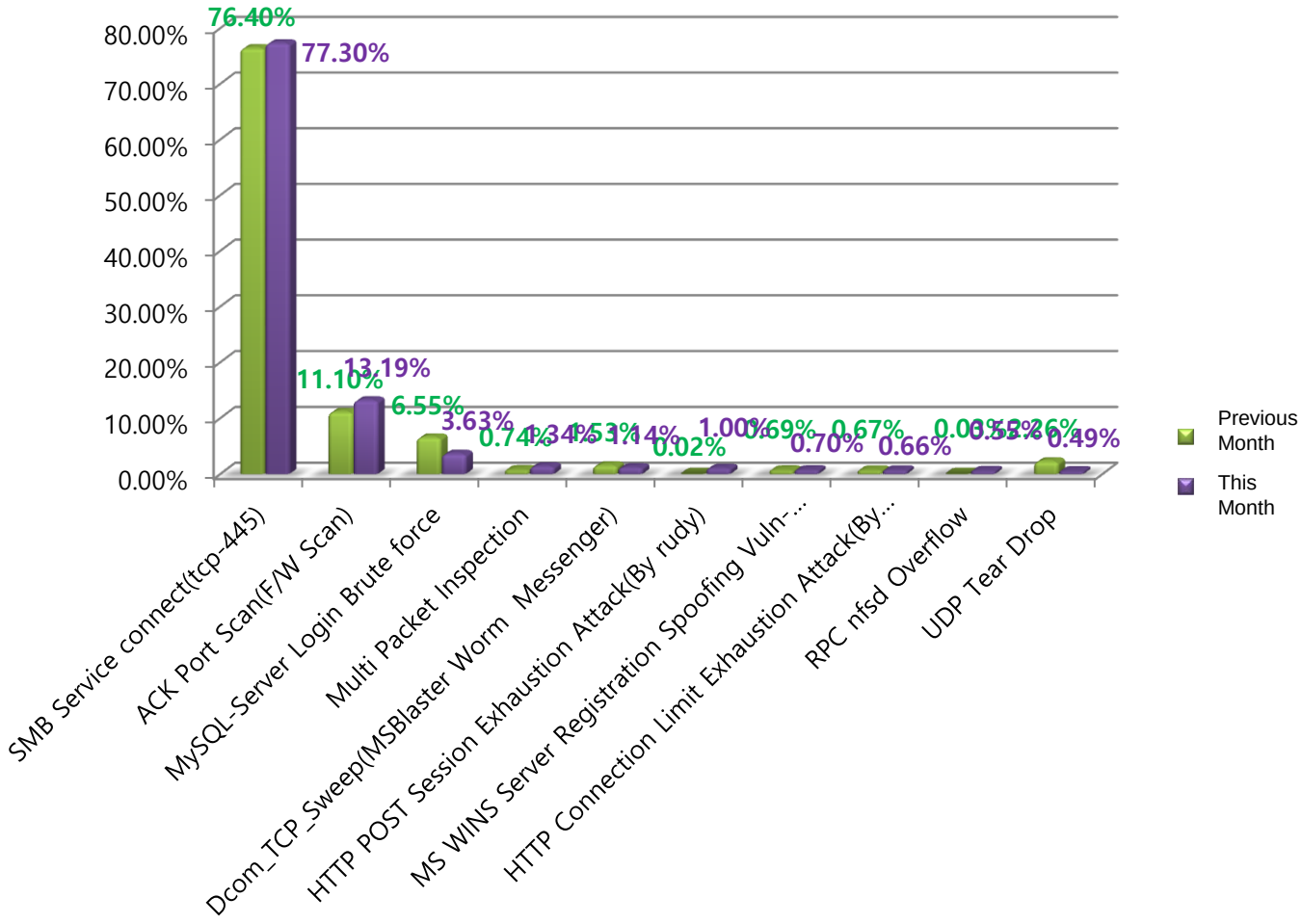
02 IGLOO Statistics

Monthly Attack Service and Trend Analysis

Monthly attack service incident patterns compared to last month

In this month's attack pattern TOP 10, the Multi Packet Inspection, Dcom_TCP_Sweep, MS WINS Server Registration Spoofing Vuln-1 and HTTP Connection Limit Exhaustion Attack events have climbed the ranks. Besides that, resource depleting events and events that extort the admin.'s authority such as the HTTP POST Session Exhaustion Attack(By rudy), RPC nfsd Overflow events have newly appeared in the rankings.

The Multi Packet Inspection event has climbed 3 ranks in the rankings and the attack is a rule which continuously attempts to access the target with a pattern with a specific byte size. The December attack log analysis indicates that the events occurring inside do not seem to be of much threat.



[Figure 2-2] TOP 10 Monthly Attack Patterns

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

02 IGLOO Statistics

Detailed Analysis according to different attack patterns

We are introduced to the TOP10 attack patterns and detailed analysis of November.

The vulnerabilities of the systems must be preemptively processed according to the detailed analysis results of each detection pattern.

Attack Pattern	Detailed Analysis Results
SMB Service Connect (tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
ACK Port Scan (F/W Scan)	ACK Port Scan (F/W Scan) is a type of scanning attack targeting vulnerable ports which are allowed to be accessed by firewall policy. Attackers can collect information on vulnerable ports by analyzing the returned packet as a response to the packet sent in advance. These attacks are not intended to destroy the system but to collect information for planning a scenario for secondary attack.
MySQL-Server Login Brute force	A brute force attack can be launched against an user account in MySQL. MySQL replies with success/error based on supplied credentials and time required for the verification is almost the same in either cases. Hence, an attacker can launch brute force attack against a MySQL user account at a rapid rate and can try many different passwords.
Multi Packet Inspection	A Multi Packet Inspection is a rule that occurs within the IPS of a specified company and detects using the automated pattern learning defense mechanism set-up within the IPS. It denies access for a certain amount of time if a packet, which exceeds the bytes PPS set-up by the IPS, is injected.
Dcom_TCP_Sweep (MSBlaster Worm Messenger)	W32.Blaster.Worm is a type of worm which spreads by exploiting the DCOM RPC Buffer Overflow vulnerability. If TCP/135 port is opened and if it is found to be vulnerable, the worm will infect the system. The infected system activates TCP/4444 port to download malicious file, "mblase.exe“ from the host server using TFTP and registers it to the registry. During this process, network traffic on the infected system may increase.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

02 IGLOO Statistics

Detailed Analysis according to different attack pattern

Attack Pattern	Detailed Analysis Results
HTTP POST Session Exhaustion Attack (By rudy)	A popular low and slow attack tool that is designed to crash a web server by submitting long form fields. The attack is executed via a DoS tool which browses the target website and detects embedded web forms. Once the forms have been identified, R.U.D.Y. sends a legitimate HTTP POST request with an abnormally long 'content-length' header field and then t starts injecting the form with information, one byte-sized packet at a time.
MS WINS Server Registration Spoofing Vuln-1 [Req](UDP-137)	This attack occurs while a name is being registered on the Windows WINS server and the NetBIOS is not inspected thoroughly enough. Through this vulnerability, the attacker is capable of redirecting the victims internet traffic through web proxy spoofing to a specified domain.
HTTP Connection Limit Exhaustion Attack (By Slowloris)	An attack attempt to exploit a spoofing vulnerability in Microsoft windows WINS server. This vulnerability is caused by an error when the vulnerable software is handling a malicious entries in WINS database. It allows a remote attacker to exploit a WINS spoofing via sending a NBNS name registration packet.
RPC nfsd Overflow	A vulnerability which can occur in the *Sun OS*, when a 32bit UID, where 16bits are filled with 0, is sent to the NFS server from the client and obtain access to *Root* authority in the server. Through this vulnerability, the attacker is capable of obtaining more than enough system authority, however this vulnerability can be solved through the latest *Sun OS* patch.
UDP Tear Drop	A common form of denial of service attack, in which the perpetrator overbears a network by exploiting datagram fragmentation mechanisms.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

03 SIEM Guide

The SPiDER TM V5.0 is the integration of IGLOO SECURITY's security management experience and Big Data utilization capability into an integrated security management solution. It is capable of increasing promptness and efficiency in security management process and viewing the network infrastructure as a whole through the unified security management environment from the initial log detection to network, packet analysis.

How to use TM's Human Resource Information Integration

Technical Support Team
Technical Team 2

1. Summary

Companies or organizations use various security equipment in order to respond to outside intrusions. However, a recent issue which has been continuously raised by media outlets is "the threat of an insider" due to the lack of security awareness education or simply a lack of interest in cyber security from the management part of the company.

Preventing inside security breaches are as crucial as blocking attacks from the outside. This months issue will cover how to utilize personnel information to monitor and analyze inside personnel activity.

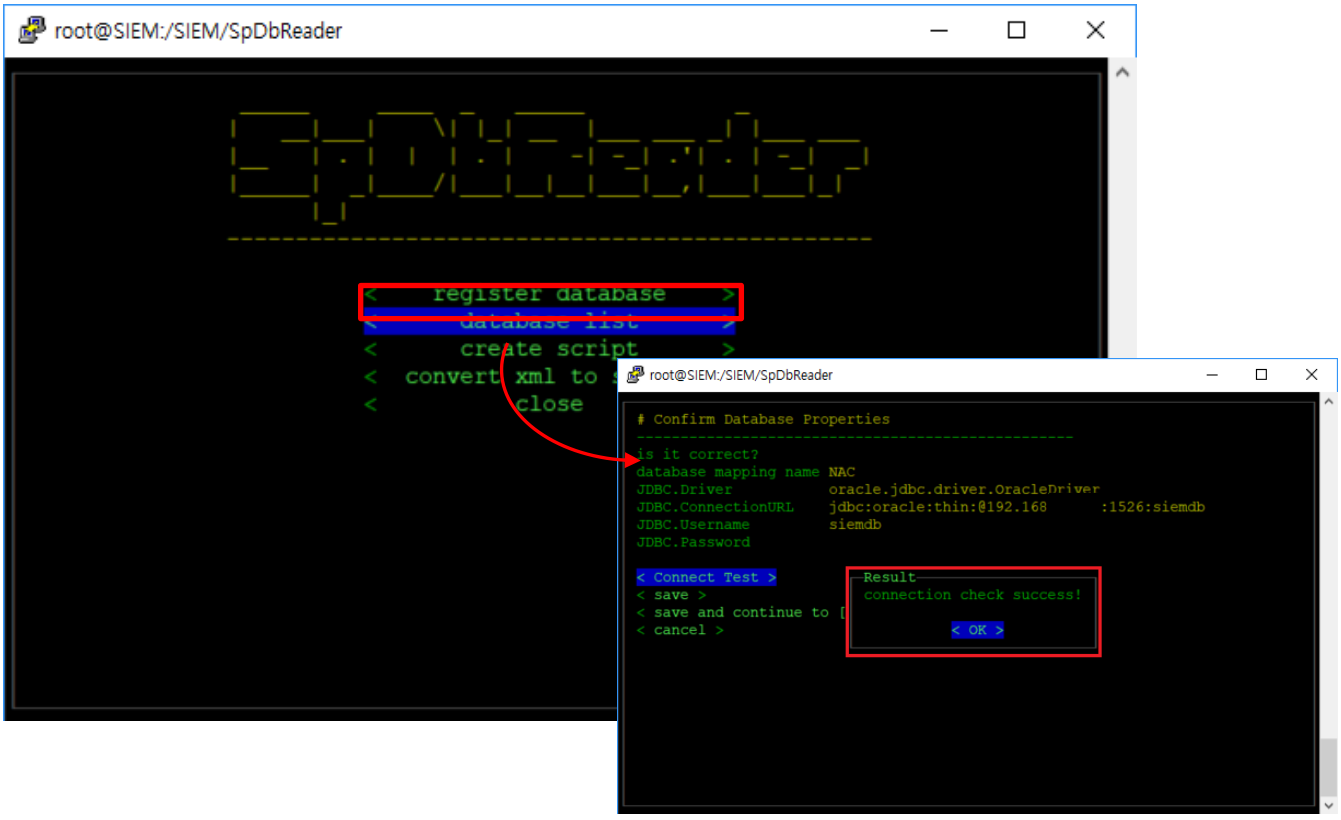
2. Integrating Human Resource Information

1) Human Resource Information extraction through SpDbReader

- SIEM is capable of carrying out a User based monitoring system by gathering a variety and large amount of data and maintaining its original form while adding additional information.
- In order to search personnel information and the original logs, human resource data must be extracted through the SpDbReader.
- The human resource information stored in the Dbsafer, NAC etc. is extracted through the DB Query and saved as a file.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

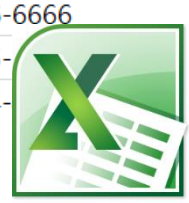
2) Human Resource Information extraction through SpDbReader:
Connection with an equipment containing personnel information



- Select an equipment which contains personnel information and connect with SpDbReader.
- Connect personnel information after confirming equipment access information and equipment table.

3) Results from personnel information extraction

	A	B	C	D	E	F
1	kdk1215	31-DB-4A-5D-15-3A	192.168.100.200	박보검	기술지원	010-999-9999
2	scpmnkc	51-DD-1E-6D-18-2B	192.168.100.210	서강준	기술지원팀	010-999-9999
3	sanghyun	31-DB-4A-5D-15-3A	192.168.100.22	송중기	연극부	010-777-7777
4	hyunwuk	51-DD-1E-6D-18-2C	192.168.100.230	강동원	모델과	010-666-6666
5	sukhyun	99-AD-2C-1D-12-3D	192.168.100.240	안정환	기술지원팀	010-555-
6	itsrain	46-AD-2B-2D-13-2D	192.168.100.250	정지훈	기술지원팀	010-444-

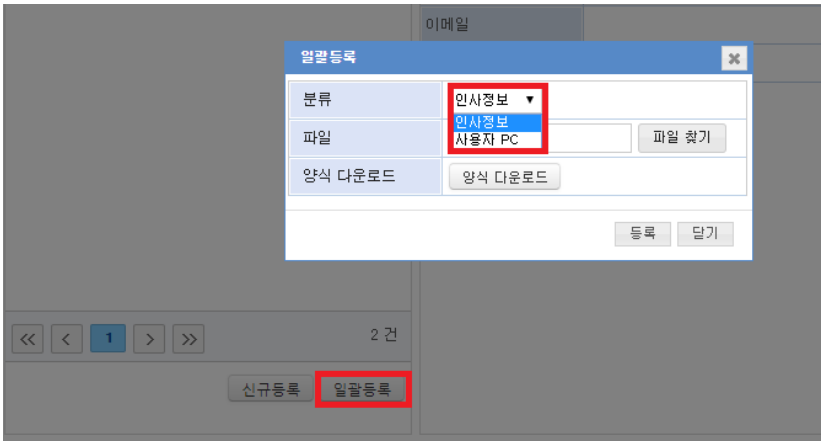


- The extracted data is saved in a csv format or saved in the SIEM DB.
- The extracted data can be connected with the SIEM Human Resource information menu or can have additional information added to the original logs.
- The extracted data can be saved on a specific frequency through a designated route(designated through the SIEM) in a csv format.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

3. Utilizing Human Resources Information

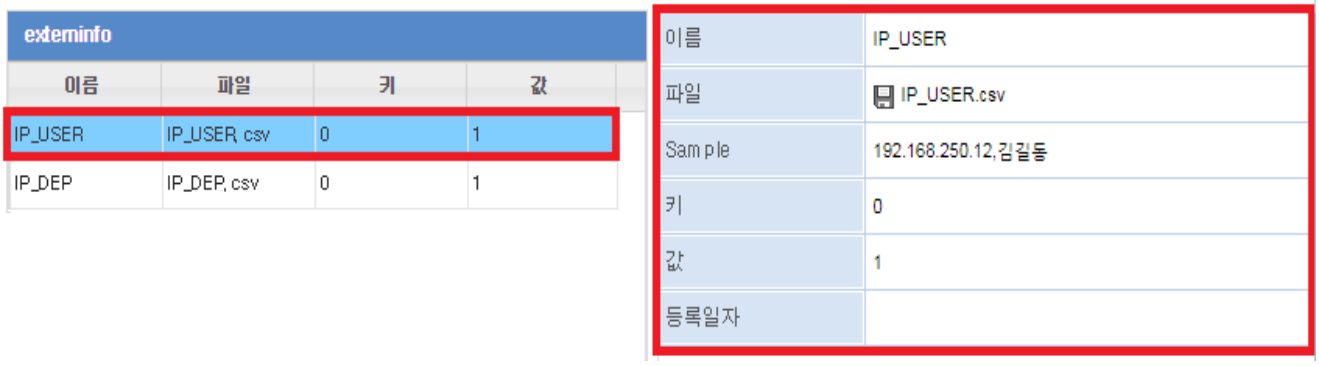
1) Utilizing the Human Resources integration menu



- The extracted information can be collectively registered in the “Operation Management>Human Resource” menu according to whether it belongs under Human Resources or PC User.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

2) EXTERNINFO registration



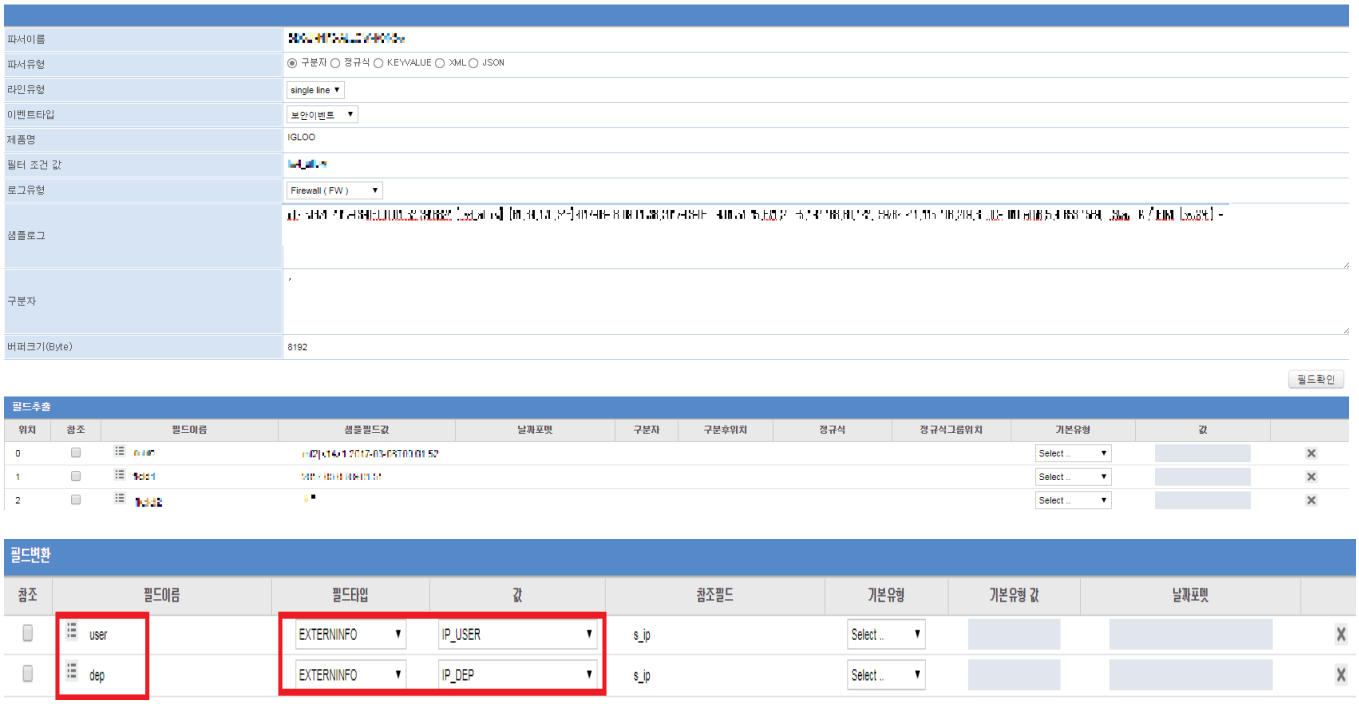
exteminfo

이름	파일	키	값
IP_USER	IP_USER.csv	0	1
IP_DEP	IP_DEP.csv	0	1

이름	IP_USER
파일	IP_USER.csv
Sam ple	192.168.250.12,김길동
키	0
값	1
등록일자	

- The extracted information can be stored through the SIEM **EXTERNINFO** menu.
- Admin>Configuration Management>**EXTERNINFO**(Parser)>Create Parser>select file>Apply
- Additional information can be added to the raw log when registered in **EXTERNINFO**.
  User information can be added based on sourceIP and destinationIP.

2-1) EXTERNINFO registration – Adding Parser fields



파서이름	
파서유형	◉ 구분자 ○ 정규식 ○ KEYVALUE ○ XML ○ JSON
라인유형	single line
이벤트타입	보안이벤트
제품명	IGLOO
필터 조건 값	
로그유형	Firewall (FW)
샘플로그	
구분자	,
버퍼크기(Byte)	8192

필드확인

필드추출

위치	참조	필드이름	샘플필드값	날짜포맷	구분자	구분후위치	정규식	정규식그룹위치	기본유형	값	
0	☐								Select..		✕
1	☐								Select..		✕
2	☐								Select..		✕

필드변환

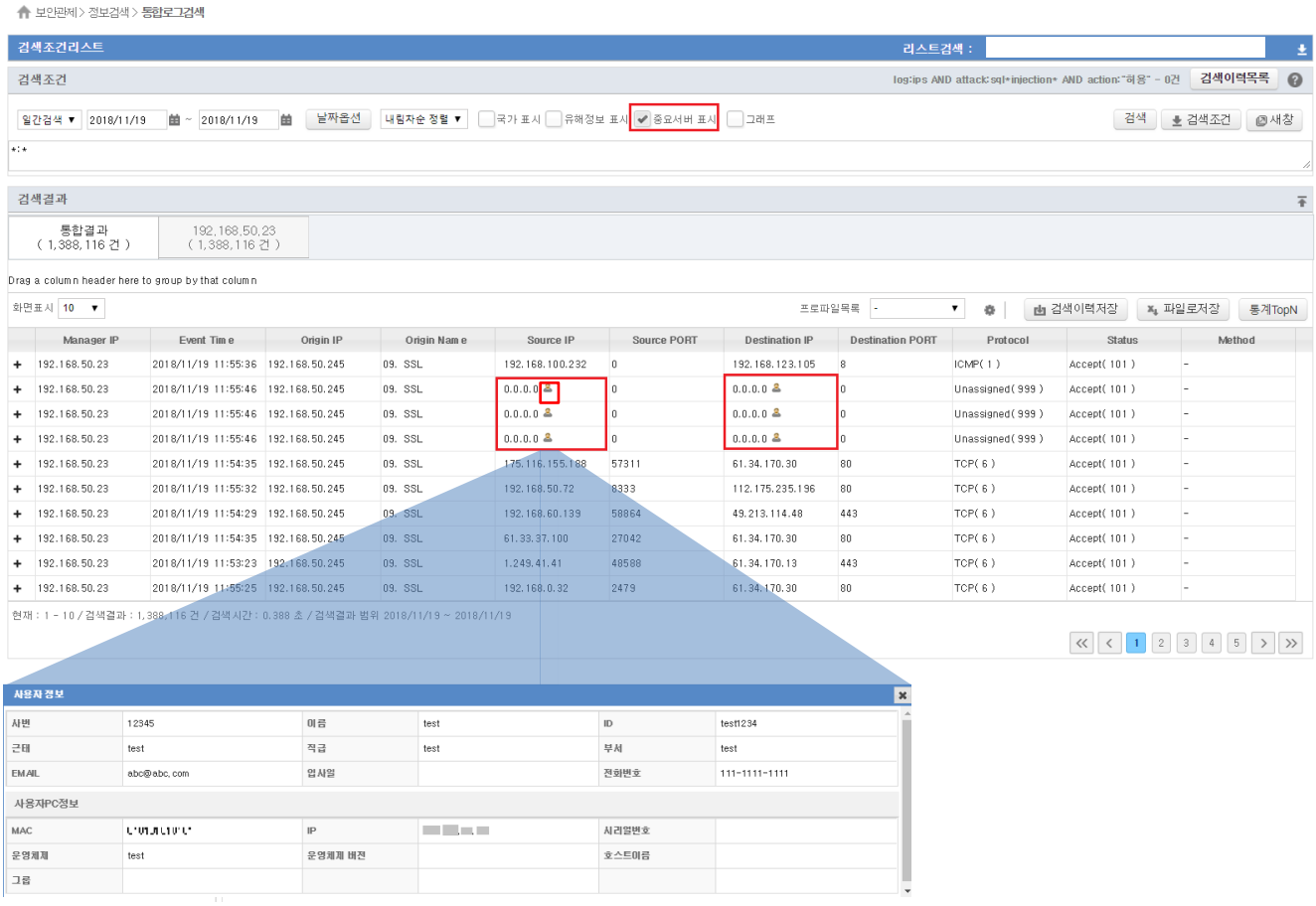
참조	필드이름	필드타입	값	참조필드	기본유형	기본유형 값	날짜포맷	
☐	user	EXTERNINFO	IP_USER	s_ip	Select..			X
☐	dep	EXTERNINFO	IP_DEP	s_ip	Select..			X

- Additional columns such as User, User department, employee number, telephone number etc. can be additionally created.
- In the ‘Default Type Value’ column, select **EXTERNINFO** and insert s_ip and d_ip in the ‘Reference Field Column’.
- It can be checked whether the **EXTERNINFO** has been applied to the field during log search.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

4. Using the Search and Alert functions

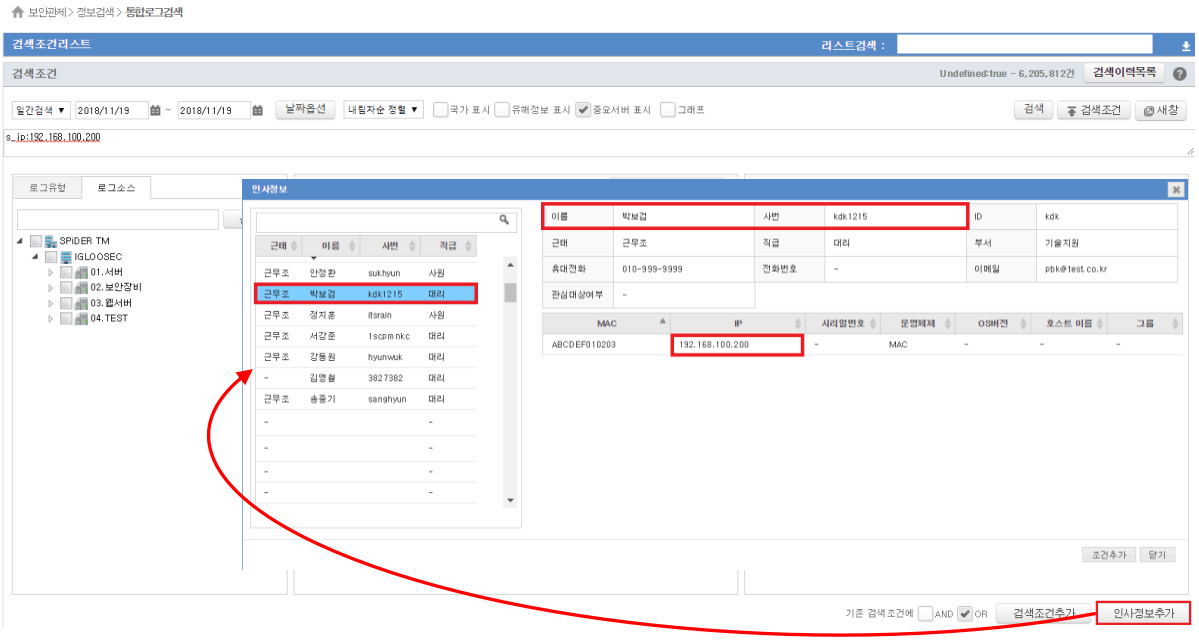
1) Log search : asset (show major servers)



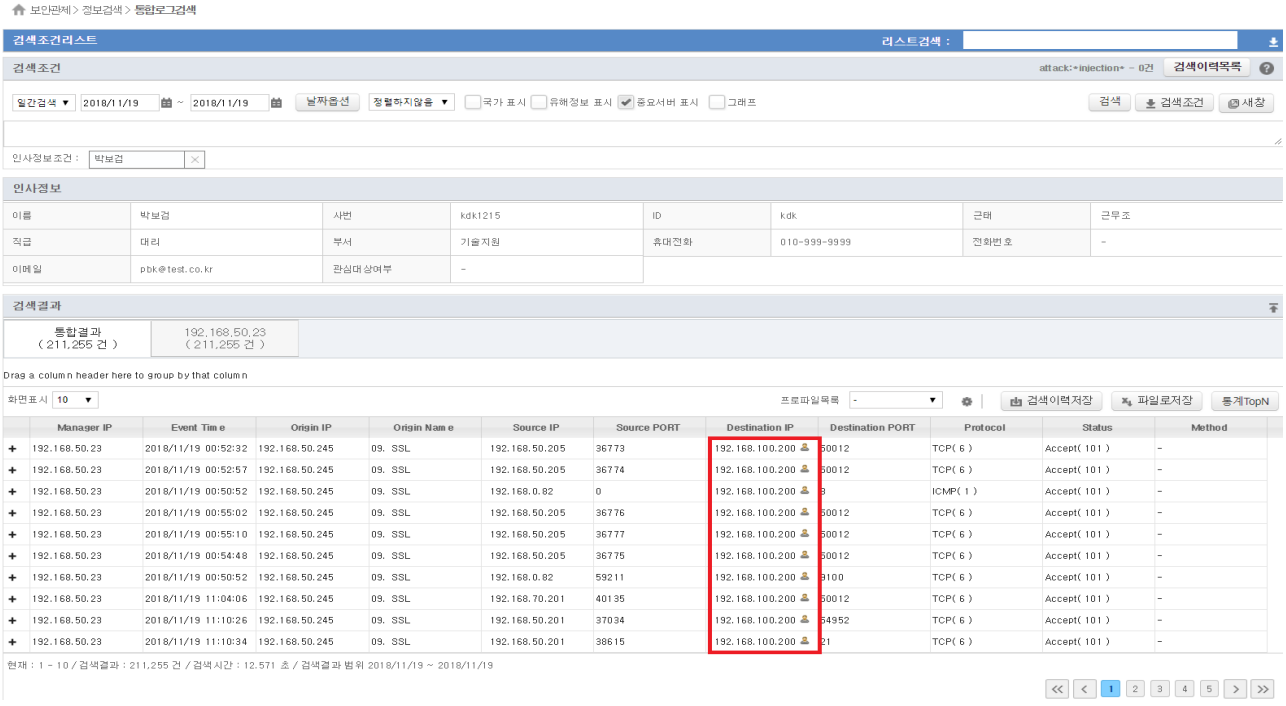
- If the user information has been integrated in the Human Resources menu, a human emoji will appear on the sourceIP and destinationIP of the people who are registered in the Human Resource information when searched under assets of log search and the user information can be viewed in one eye by clicking on the emoji.
- By utilizing the function above, it is possible to check if there was an external access just by a click.
- It also aids in identifying inherent internal threats such as information leaks through internal personnel.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

2) Log search : Human Resources



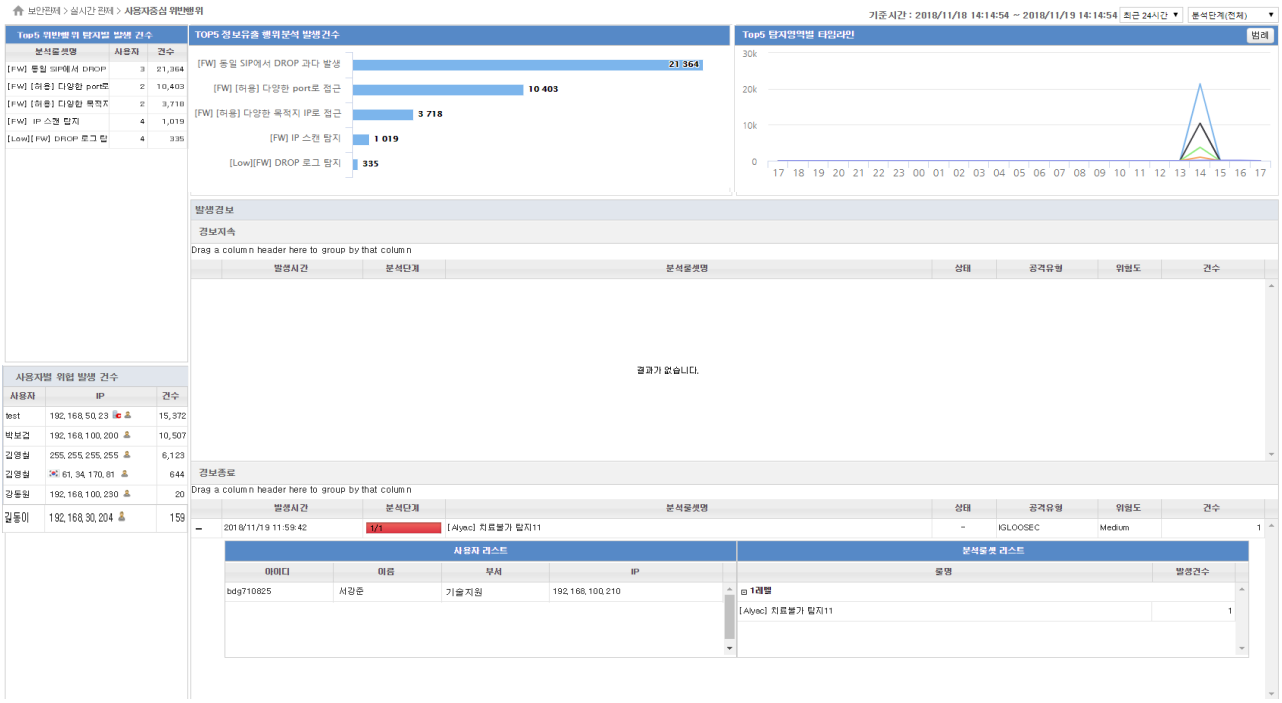
- Through the search condition of the log search menu, specific internal User or asset search conditions can be added.
- A pop-up containing human resource information will appear by clicking on ‘Human Resource’ button. Then, select the user you wish to search and select additional search conditions by using the ‘Add Condition’ button in order to search human resource information.



- Only the events concerning the specified user will appear when searched through the ‘Add Condition’ function.
- It is possible to monitor what the User is up by managing the registered User’s IP.

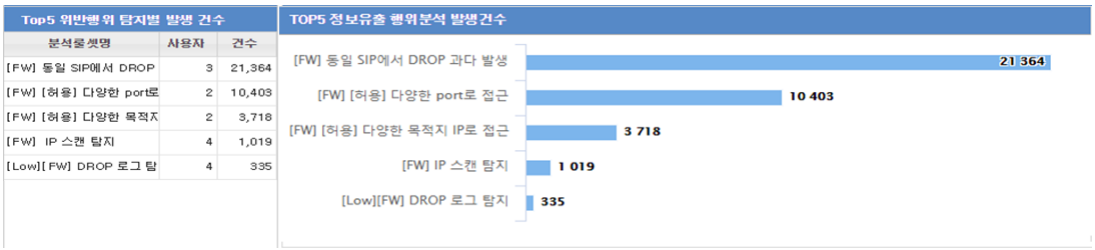
Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

3) User based infringement activity



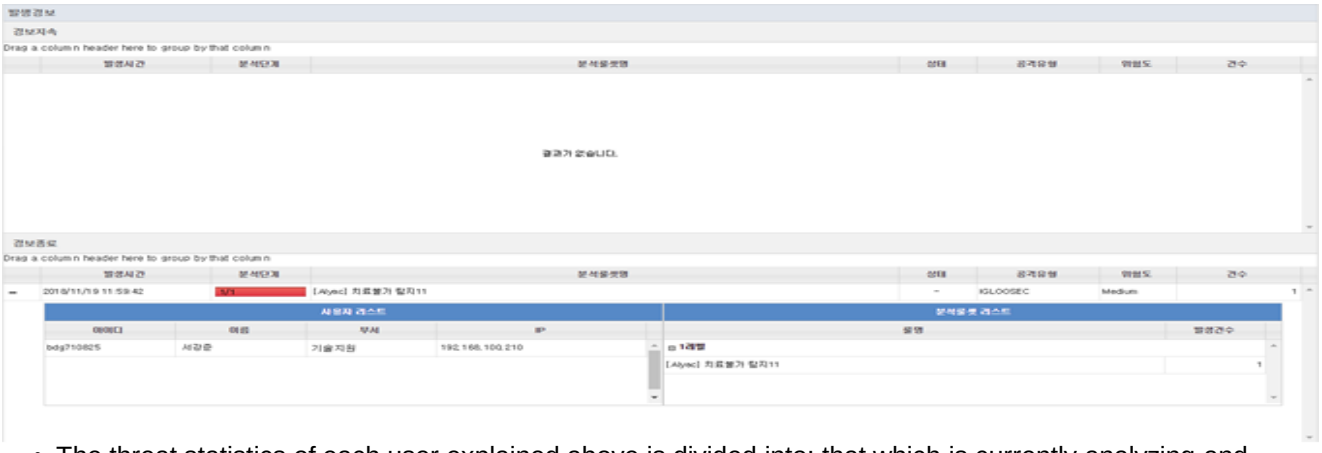
- User information can be checked based on the human resource information of the User based infringement menu.
- When an alert occurs, the User information is shown based on the IP information of the alert.

3-1) User based infringement activity–TOP5 cases based on detection(activity analysis)



- It shows the infringement activity detection analysis rule of each case statistics and displays a simple graph of User infringement activity.

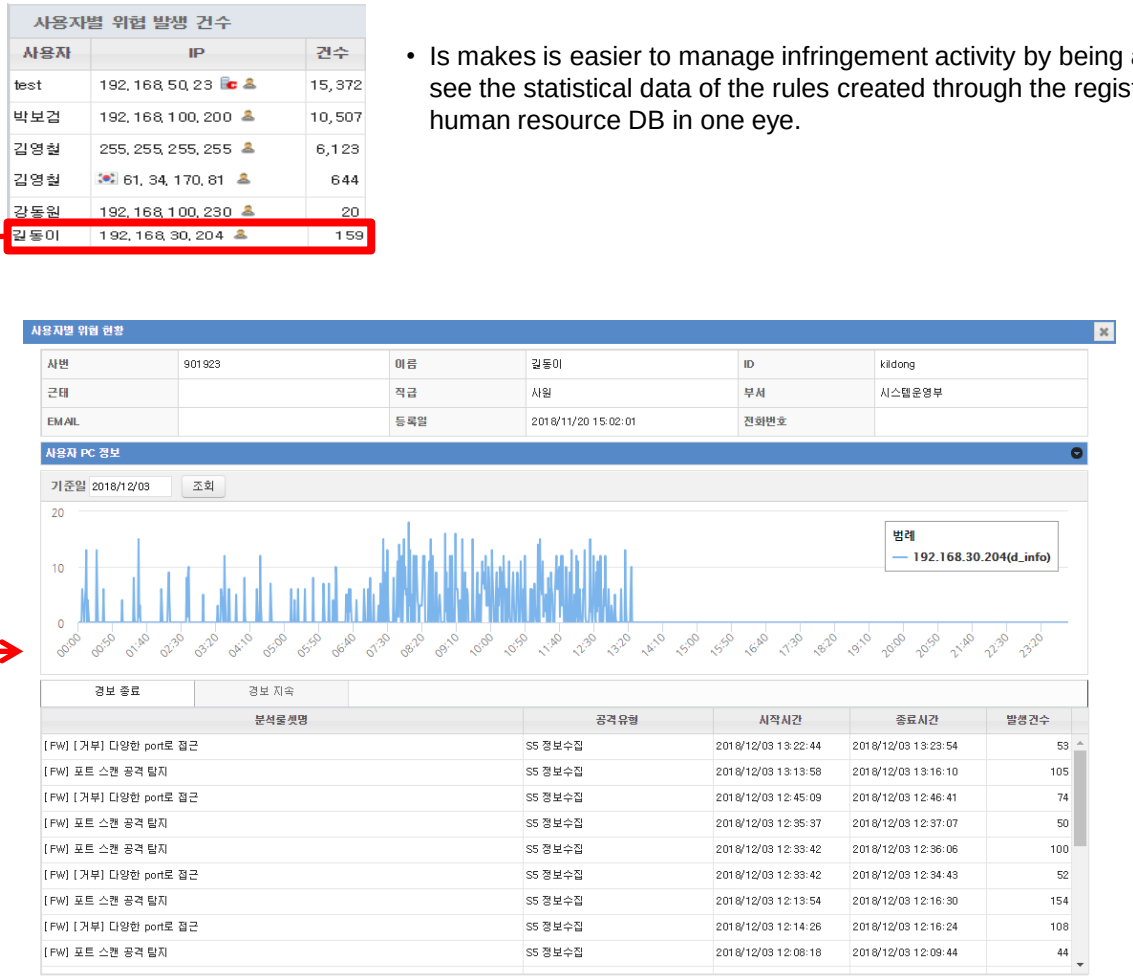
3-2) User based infringement activity – Alert (continuing alert / end of alert)



- The threat statistics of each user explained above is divided into; that which is currently analyzing and that which has finished analyzing.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

3-3) User based infringement activity – number of threat cases and detailed display of each user



사용자별 위협 발생 건수

사용자	IP	건수
test	192.168.50.23	15,372
박보검	192.168.100.200	10,507
김영철	255.255.255.255	6,123
김영철	61.34.170.81	644
강동원	192.168.100.230	20
길동이	192.168.30.204	159

사용자별 위협 현황

사번	901923	이름	길동이	ID	kildong
근태		직급	사원	부서	시스템운영부
EMAIL		등록일	2018/11/20 15:02:01	전화번호	

사용자 PC 정보

기준일 2018/12/03 조회

범례 — 192.168.30.204(d_info)

경보 종료 | 경보 지속

분석룰셋명	공격유형	시작시간	종료시간	발생건수
[FW] [거부] 다양한 port로 접근	S5 정보수집	2018/12/03 13:22:44	2018/12/03 13:23:54	53
[FW] 포트 스캔 공격 탐지	S5 정보수집	2018/12/03 13:13:58	2018/12/03 13:16:10	105
[FW] [거부] 다양한 port로 접근	S5 정보수집	2018/12/03 12:45:09	2018/12/03 12:46:41	74
[FW] 포트 스캔 공격 탐지	S5 정보수집	2018/12/03 12:35:37	2018/12/03 12:37:07	50
[FW] 포트 스캔 공격 탐지	S5 정보수집	2018/12/03 12:33:42	2018/12/03 12:36:06	100
[FW] [거부] 다양한 port로 접근	S5 정보수집	2018/12/03 12:33:42	2018/12/03 12:34:43	52
[FW] 포트 스캔 공격 탐지	S5 정보수집	2018/12/03 12:13:54	2018/12/03 12:16:30	154
[FW] [거부] 다양한 port로 접근	S5 정보수집	2018/12/03 12:14:26	2018/12/03 12:16:24	108
[FW] 포트 스캔 공격 탐지	S5 정보수집	2018/12/03 12:08:18	2018/12/03 12:09:44	44

- Is makes is easier to manage infringement activity by being able to see the statistical data of the rules created through the registered human resource DB in one eye.

- A detailed pop-up screen will appear when the ‘user’ button on the ‘number of threat cases of each user’ screen is clicked on.
- The analysis rule’s progress and detailed screen of a specific scree…can be seen on a detailed screen. This allows monitoring and response of users in violation of internal policy.

5. Conclusion

How to use the Human Resource integration function of SPiDER-TM 5.0

When monitoring attacks, it is a common mistake to focus efforts on external attacks so that internal attacks practically have a bypass through the security monitoring. However, through the SPiDER TM V5.0 Human Resource functions, one is capable of preventing and responding to both external and internal threats from multiple angles.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

04 Tech Note

2019's Security Threats, Prospect and Potential Responses

Service Business Team
Sec. Analytics Team

1. Summary

As always various security threats have been discovered this year. As cyber attacks are being used to cause political damage or gain economic gain through attacks such as; Metlddown(CPU vulnerbility), Spectre, Coinrail and Bitsum hacking incident, Cryptojacking(mining malicious code) and DRDos attakcs utilizing Memcached server, cyber threats are becoming more and more intelligent and thus, more difficult to defend against.

This month's issue will deal with the security threats and major security threats and responses technology within the security technology methodology which IGLOO SECURITY have nominated for 2019.

2. Prospects for 2019 Security Threats

1) Security Threats concerning SmartCity Establishment

A smart city is the term which replaced u-city (Ubiquitous City) in March 2017 as the Smart City Law was reformed. It refers a city which uses technology such as digital devices, various content through communications technology, IoT technology, 5G, block chain etc. in order to improve everyday quality of life.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

Smart Cities are mostly comprised of **3** main categories: Infrastructure, Data and Service. These categories can be divided into **7** sub categories.

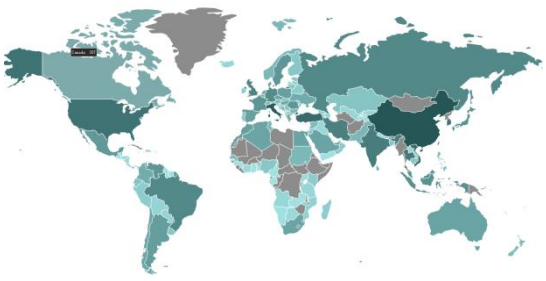
Category		Details
Infrastructure	City Infrastructure	· Smart Cities are mainly focused on software, but also require development in hardware
	ICT Infrastructure	· Citywide wire/wireless connection infrastructure
	Spatial information infrastructure	· The advent of the core of spatial information infrastructure in order to integrate real-space from cyber-space · Spatial information Users shift from people to objects · Map information, 3D map GPS, tracking device infrastructure, satellites
Data	IoT	· Connecting the variety of infrastructure objects within the city through a sensor based network
	Data Sharing	· Smart City platform in a micro-perspective · Unconstrained sharing and utilization support of data · Active roles from the Smart City leaders necessary
Service	Algorithm & Service	· Intelligent service development layer with practical quality and reliability · Data processing analyzing
	City Innovation	· Creating an atmosphere where ideas and services directed at solving issues within the city are possible

[Table 4-1] Smart City components (Reference: Convergence Research Policy Center, The Concept and prospect of Smart Cities)

As seen in the Smart City components (Table 5-1), the whole city in connected through the communication infrastructure and smart devices such as IoT devices allow both wire/wireless connection. If a incident concerning data sharing and IoT were to occur, the Smart City system will be shaken at its core.

Recent security threat cases demonstrate the effect security incidents have on Smart Cities.

There is a case in 2016 where 100,000 IoT devices were gathering information in a network environment. These devices where infested with botnet which caused an large amount of traffic which lead to a DDoS attack. This cyber attack paralyzed the DNS(Domain Name Service), web server and data servers which brought about inconvenience to many company and individual users.



[Figure 5-1] Distribution of IoT roop botnet(Reference:360 Netlab Blog)

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

There is also a case of taking control of devices remotely without directly controlling them. These cases include incidents where the attacker gained access to CCTV devices and microphones which were used to illegally film or record files which would eventually be sold or uploaded to the internet. Another case included an attack where the attack gained access to a Wallpad of the victims house and illegally control the device.

[Figure 4-2] IP CCTV Hacking(Reference : *Security News*)

Besides the attacks mentioned above, information sharing and communication between smart terminals expose vulnerabilities to cyber attacks such as *man in the middle attack*, which intercepts information.

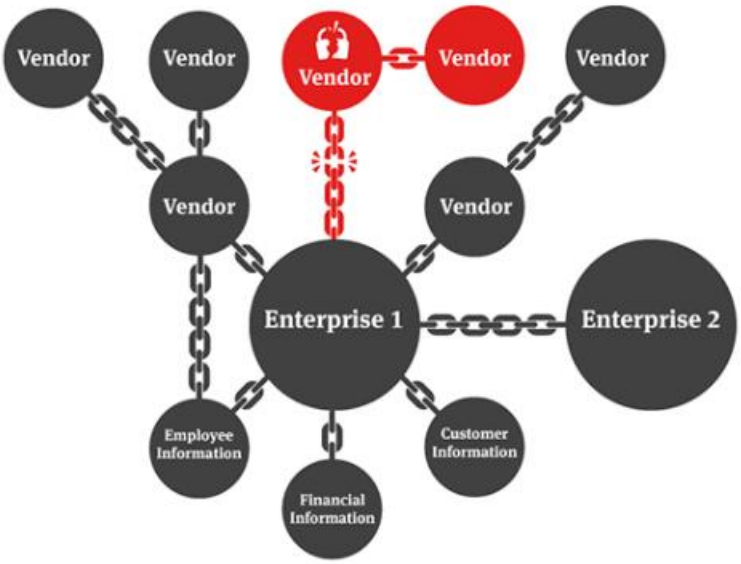
The components of the Smart City, originally designed to solve and improve the standard of living of its members, is exposed to security threats thus exposing the citizens to a larger threat and potential chaos than cyber incidents

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

2) Supply Chain Attack

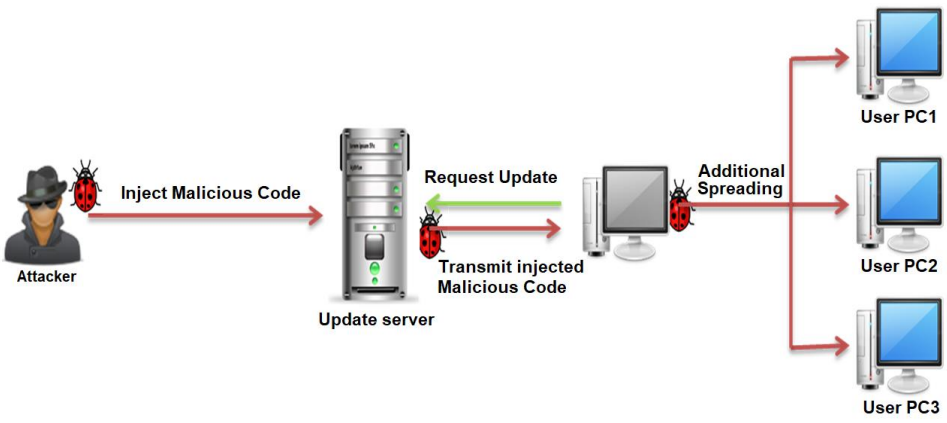
A Supply Chain Attack refers to an attack where the attacker, instead of directly hacking into a company or individual's PC, infests a software and distributes it or intrudes a server and injects a malicious code inside a normal command file. Until now, the attackers have carried out espionage activities such as: spying and wiretapping/radio monitoring, on contractors, systems, companies and suppliers.

Then why do hackers attack product or service suppliers instead of those who are actually part of the company itself?



[Figure 4-3] Supply Chain Attack (Reference : NORTON ROSE FULERIGHT)

The reason why hackers attack software distribution companies instead of the target company itself is because by doing so, the attack is more widespread and difficult to detect thus, increasing the probability of a successful cyber attack. Also, the attack is much easier to carry out since the target already trusts the software supplier



[Figure 4-4] Supply Chain Attack example

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

The target company may be very strict with their security, however if the supplier company or other partner companies are not, then the possibility of an external intrusion is an eventuality. Therefore, instead of directly attacking the target company, which is likely to have enforced security measures, the hackers usually attack the companies which supply the target

If small companies choose convenience over security, attacks targeting vulnerabilities through supply chains will continue to occur in 2019.

3) Evolving malicious codes, attackers learning

In order to efficiently detect or block cyber attacks, security operatives utilize security equipment and anti-virus programs to analyze malicious codes through the development of signature and activity based patterns. With the advent of new forms of malicious codes, security operatives implement AI algorithms with features of past malicious codes by converting them into data and thus carry out security operations automatically.

Through the efforts of security operatives and the implementation of AI, the attacking prowess of the hackers have been minimized, however attackers are always searching for ways to respond to these measures. In the past, attackers would manually check and alter their malicious codes in order to circumvent security equipment or anti-viruses. In order to bypass existing security methods, attackers recently have attempted to utilize AI algorithms with an Adaptive Learning base in order to carry out attacks.

Intelligent Malicious Codes	Advanced	Persistent	Targeted	Vulnerability
	Various high-tech attack methods	Remaining dormant for long periods of time since initial infection	Attack specified target	Spread malicious codes using (newly found)vulnerabilities

[Figure 4-5] Evolving Malicious Codes (Reference : AhnLab)

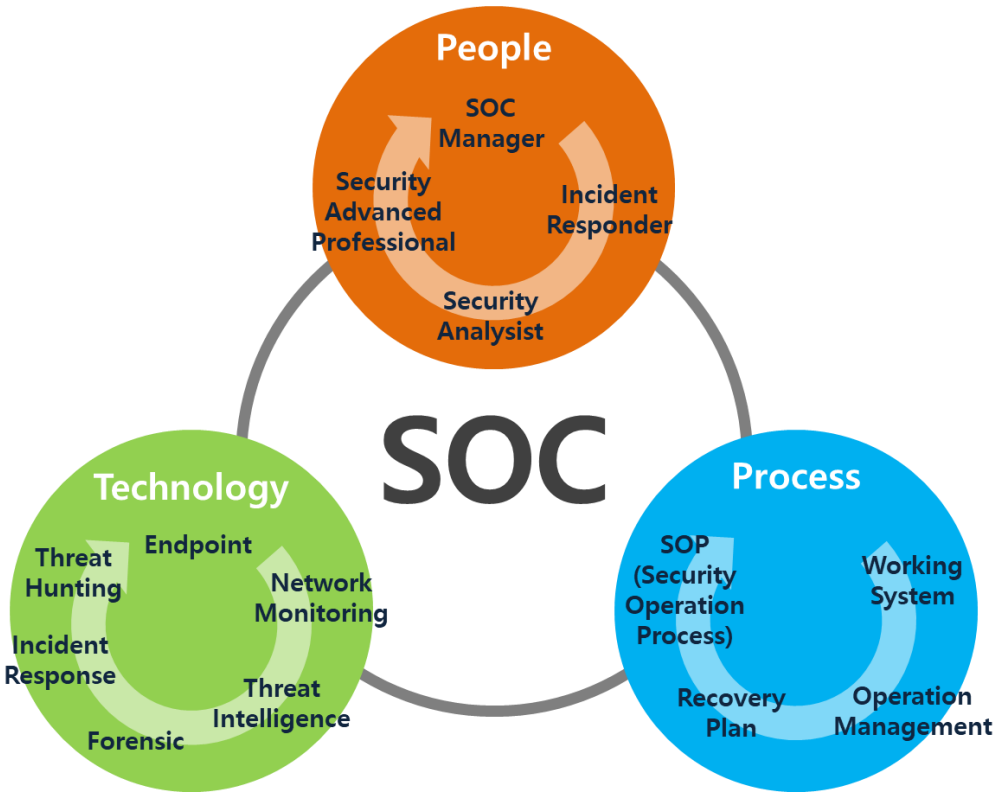
Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

Through the Adaptive Learning system, the malicious codes will continuously discover new ways of attacks by finding and developing new ways of bypassing detection patterns of every time it is detected. Thus, the fight between the security operator using the AI Algorithms and attackers using Adaptive Learning system is most likely to be continued in 2019.

3. 2019 Security Threat Response Measures

As explained in previous paragraphs, cyber attacks are becoming more cunning and high-tech and thus there is a much higher demand of responding to major security incidents through effective measure.

In order to protect company information assets and infrastructure, the role of SOC(Security Operation Center) will increasingly become more important. Until now, SOC's were operated by three components: People, Process and Technology. These component were the basis for defense against cyber attacks with monitoring agents monitoring logs and events as they were detected by security equipment.



[Figure 4-6] # Components of a SOC(Reference : GBM, IGLOO Sec. Security Analytics Team

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

However, with the increase in monitoring subjects, and the different forms of cyber attacks, the security devices detect more events thus, leading to security agents taking longer to process the events manually.

In order to swiftly respond to these security threats in the changing security environment, the Security Orchestration Automation (SOA), a multi-staged, manual and automatic process,is being seen as an alternative.

One of the most important components of applying SOA to security management is *Playbook*. A Playbook is a guide which contains guides and directions on processes and other responses to when a cyber attack occurs. If the attack has the same or similar form to that which is registered in the playbook, the AI Algorithm will respond to it as the playbook dictates. Since the process is not manual anymore, the decrease in manual analysis and response time makes the process more efficient.

With the application of SOA to the SOC, the repetitive process which was carried out by people is now made more efficient, thus allowing security operatives to respond to cyber attacks more swiftly.

4. Reference

- [1] Hackers and Malicious Codes, 'Why·How?' http://www.ciokorea.com/news/37852
- [2] How will AI and Cloud technology integrate into security? https://www.boannews.com/media/view.asp?idx=72999
- [3] Looking into the future of Smart City and Security Industry. https://www.boannews.com/media/view.asp?idx=67401
- [4] Six degrees of separation: cyber risk across global supply chains. http://www.nortonrosefulbright.com/knowledge/publications/155738/six-degrees-of-separation-cyber-risk-across-global-supply-chains
- [5] Can false information penetrate the 'Acupuncture point' of AI and BigData? http://www.asiae.co.kr/news/view.htm?idxno=2018120310532022150
- [6] Korea Internet & Security Agency, Guide Private Information GDPR https://www.kisa.or.kr/business/gdpr/gdpr_tab1.jsp

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

05 Special Column

Edge Computing, the Alternative to Cloud Environments

Service Business Dpt.
Dispatch Security Management Team

1. Summary

Each year, Gatner provides an annual report on IT industries with potential. In both 2018 and 2019, *Edge Computing* has been selected in the top 10 strategic technologies. Edge Computing is receiving much attention in the age of the 4th industrial revolution and 5G. Then, what exactly is Edge Computing? This section will explore the definition, application and future of Edge Computing.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

[Figure 5-1] Gatner's Top 10 Strategic Technology Trends of 2019 – Reference: gantner.com

Field	2017	2018	2019
Intelligent	Applied AI & Advanced Machine Learning	AI Foundations	Autonomous Things
	Intelligent Apps	Intelligent Apps and Analytics	Augmented Analytics
	Intelligent Things	Intelligent Things	AI-Driven Development
Digital	Virtual & Augmented Reality	Digital Twin	Digital Twin
	Digital Twin	**Cloud to the Edge**	**Empowered Edge**
	Blockchains and Distributed Ledgers	Conversational Platform	Immersive Experience
		Immersive Experience	
Mesh	Conversational Systems	Blockchain	Blockchain
	Mesh App and Service Architecture	Event-Driven	Smart Spaces
	Digital Technology Platforms	Continuous Adaptive Risk and Trust	
	Adaptive Security Architecture		
etc			Privacy and Ethics
			Quantum Computing

[Table 5-1] Comparison of Gatner's Top 10 Strategic Technology 2017~2019

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

2. Limits of Cloud Computing and Post Cloud

Cloud Computing refers to the technology which allows electronic devices (computers, mobile devices etc.) to access computing services such as server, storage, software, analysis etc. through the internet. It is currently the hegemony of computing infrastructure.

Due the various advantages of using Cloud Computing such as quick and convenient service provisioning and an efficient use of resources through virtualization, a massive scale distributed processing in the thousands of nods within a data center etc. Cloud Computing has recorded an exponential growth in recent years. However, Cloud Computing still does have some limitations.

First, if the cloud data center(where numerous devices store crucial information) is attacked, a large amount of personal information and invasion of privacy may occur.

Secondly, real-time service is difficult. Processing in the cloud server does not occur in an individual PC, but a request for a process is sent and it may take time for the result to take place. Therefore, it may actually drop the efficiency of some industries which require real-time data processing such as the IoT autonomous vehicle industry.

The third limitation is that Clouds usually process data in one central server, which may increase the possibility of lag or errors if a large amount of data all flow in at once. According to ‘Data Age 2025’, an encyclopedia published by Seagate, by requesting it to the Internet Data Center(IDC), the world wide data creation is said to increase from 16.1ZB(ZettaBytes) in 2015 to 163ZB in 2025, more than a 10 fold increase. Such large amount of data cannot be processed in a Cloud Computing Environment.

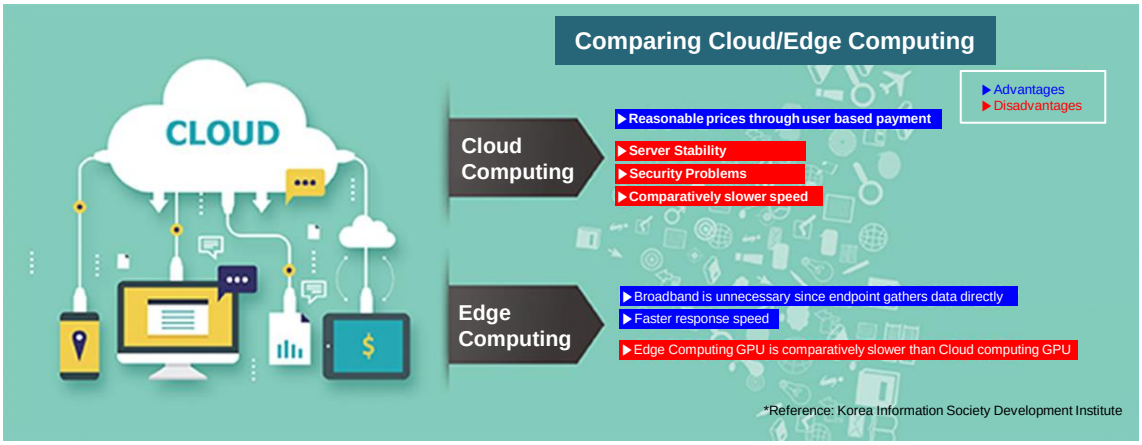
One of the most up and coming alternatives to overcome the short comings of Cloud Computing technology’s limits is ‘Edge Computing.’

3. Edge Computing

1) What is Edge Computing?

Edge computing, as the term states, is where the computing is supported from the different corners of the network. Unlike Could Computing, which is a computing where the data centers are physically far apart are managed centrally, edge computing allows the PC’s from the corners of the network to individually access and analyze data.

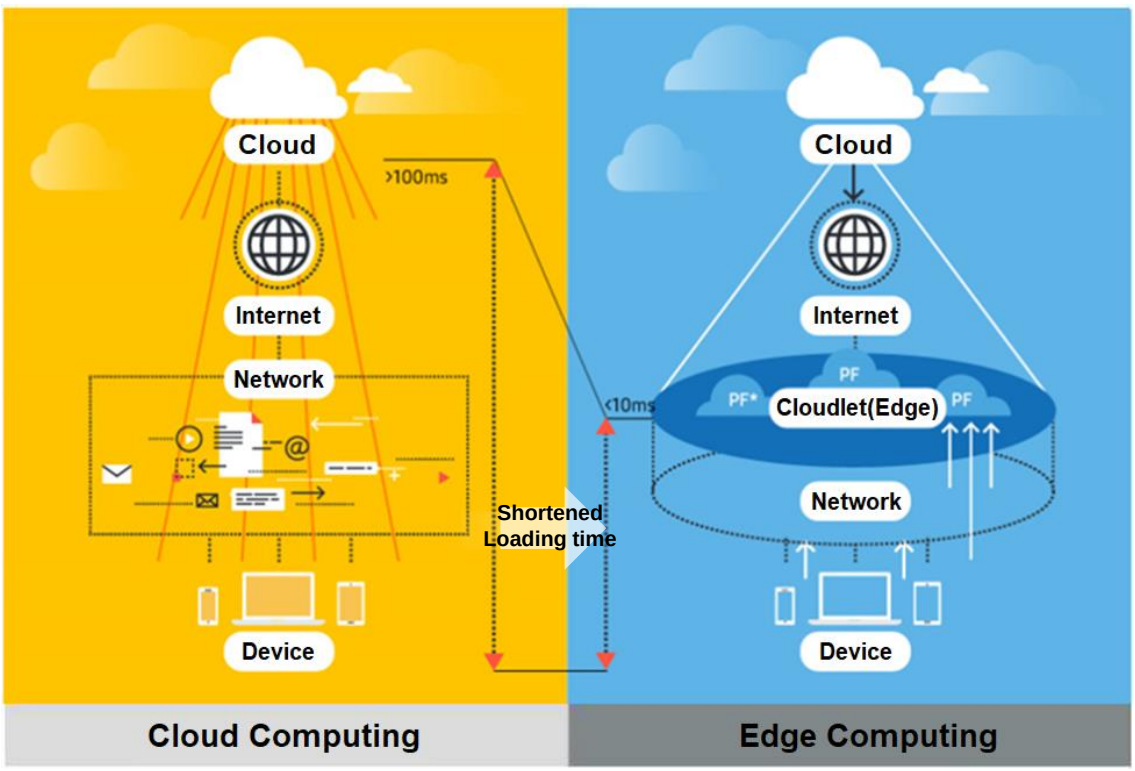
Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.



[Figure 5-2] Comparison between Cloud Computing and Edge Computing – Reference: Koit.co.kr

Compared to Cloud Computing, Edge Computing is capable of processing data faster and safer since the various PC's located on the edges of the network process the collected data independently as soon as it is received.

This method is also referred to as *Fog Computing*. In January 2014, CISCO first suggested Edge Computing as Fog Computing. Roberto Deramora, Chief Director of CISCO's IoT Group, referred to Fog Computing as an expansion of Cloud Computing to the edges, focusing on the edges (individual devices) rather than a centralized system. Currently, Edge Computing is seen as a platform of Cloud Computing and referred to as *Cloudlets*.



[Figure 5-3] Structures of Cloud Computing and Edge Computing – Reference: Samsung News Room

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

Edge Computing has become possible mostly due to the rapid growth in the performances of edge field devices. An easy example would be a smartphone having similar performance capabilities as some PC's. The development of Edge Computing will speed up even more if installation of GPU (Graphic Processing Unit) Processors specialized in parallel transaction is more widespread.

2) Case of Edge Computing Application

Edge computing is seen as the alternative to Cloud Computing as it can cover Cloud Computing's short comings such as: stability, real-time and efficiency.

Effect	Industry	Details
Stability	Autonomous Vehicle	Improve stability by minimizing network delay and data transmission error
Real-Time	Augmented Reality	Realize maximum immersion by minimizing delay time
	Virtual Reality	
Efficiency	Smart Factory	Seek efficient OS by combining Cloud and Edge Computing

[Table 5-2] Edge Computing in Industry

One of the main areas in which Cloud Computing is predicted to have difficulties is in the field of autonomous vehicles. Compared to a normal car which has over 100 central processing units, an autonomous vehicle is most likely to have a far more complex central process. Therefore, even the smallest network delay or data transmission error may lead to critical accidents. Therefore, if the Edges quickly process the data transmitted by the sensors on the car, the vehicle will be able to maintain distance and be aware of its surroundings thus, decreasing the possibility of a car accident.

Next are the highly anticipated augmented reality, virtual reality, biometrics technology etc. With the massive amount of data they produce, they are likely to cause instantaneity issues with only Cloud Computing. If Cloud Computing is replaced with Edge Computing, the data processing time will decrease greatly. This will greatly affect Users of virtual reality technology because of the sensitive nature of a human's visual and auditory senses that may be pulled out of immersion even due to a few milliseconds of delay.

Finally, for the Smart Factory, the data processing based Edge Computing would seem more appropriate than Cloud Computing. Smart Factories sent out massive amounts of data through the sensors within the factory and speed is required within factory. Therefore, instead of sending the highly detailed analysis data to the centralized system and back, it would be more efficient to transmit the data to the Edge Computers. This would also save up storage resources and cost and decrease the chance of data infection during the transmission process.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

4. Edge Computing Security Threats

With the rise of Edge Computing, the importance of Edge Computing Security has been brought up, but since the system models and confidence models have not been identified, the security threat analysis of Edge Computing is still insufficient. Also, not a note of expanding knowledge on Clouds, Cloud Computing will face similar security problems.

1) Authentication Vulnerability

Authentication is the process of determining if the entity is actually the previously identified entity. This is one of the most important prerequisite features in a system. If authentication between Cloud Computing and Edge Computing or between Edge Computing and the various devices do not have an authentication process, it is vulnerable to attacks such as Fake Nodes. Even if there is an authentication process, the attacker is capable of bypassing the process through *Replay Attacks* or *Man-in-the-middle-attacks*.

2) Network Security Threats

An attacker is able to carry out various attacks on Network communication between Cloud and Edge or network communication between Edge and various devices through various means.

⊖ DoS/DDoS Attacks

A Denial of Service(DoS)/Distributed Denial of Serivce(DDoS) is an attack which paralyzes the server by transmitting more data than the network can withstand and in an Edge Environment where quick response is necessary, even the slightest delay may cause problems.

⊜ Routing Threat

The attacker is capable of creating a routing loop or interrupt network transmission through altering the routing information. They are also capable of creating error messages and intentionally creating delay time.

⊛ Wireless network security threat

If the connection between Edge and devices are wireless, they are exposed to various security threats such as Jamming Attacks or Sniffer Attacks.

3) Conspiracy Attack

If a new device is added to a group of devices which are communicating without changing the group key, the newly added device is able to access the other encrypted data made before it was added. Guaranteeing such safety is called forward confidentiality.

On the other hand, if an IoT device leaves the group and the group key is left intact, the said device will continuously have access to the data. Guaranteeing safety from, such vulnerability is called reverse confidentiality.

If the two devices mentioned above share information, without the both types of confidentiality satisfied, the devices have access to all the data.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

4) Attacking the Sub Channel

In a Cloud or Edge environment, there are various virtual objects on a single OS. In this special environment, the attacker is able to extract information of other users through shared memory or cache. The two main forms of attack are *Prime+Probe* and *Flush+Reload*.

5) Malicious Insider

The attacker approaches sensitive data through an insider's mistake or malicious intent and the data can be extracted or destroyed.

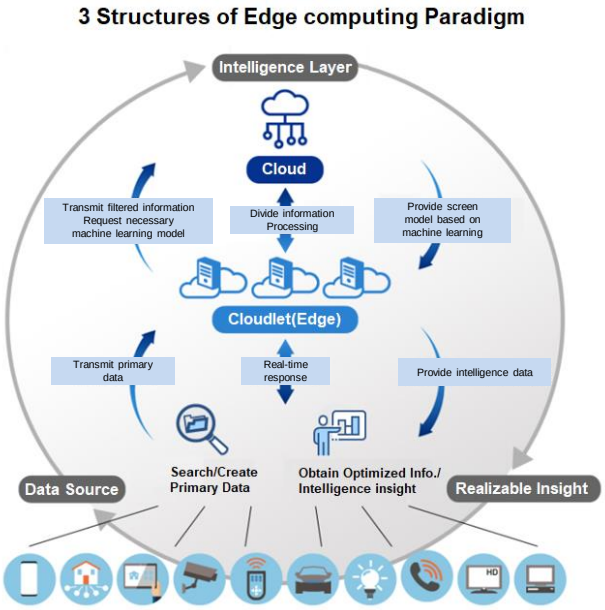
6) Protection of Private Information

Security of personal information such as physical location or address still remains a major issue for both Cloud Computing and wireless network. The personal information problem also applies to Edge Computing since the Edge Computers gathers and processes the sensitive information in real time.

5. Prospects for Edge Computing

Edge Computing and Cloud Computing are two very distinct concepts. Many people believe that Edge Computing will eventually take the place of Cloud Computing. However, there is a large possibility that Cloud Computing and Edge Computing will be able to coexist.

Recently, Gatner announced in their '2019 TOP10 ICT Trends' that "In 2019, as Cloud Computing and Edge Computing are used in a complementary manner, many people will focus on 'an attempt to process large amounts of data as efficiently as possible.'"



[Figure 5-4] Edge-To-Cloud Structure - Reference : Samsung Newsrooms

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

The time has come where IoT devices have become more practical and are required to store and transmit large amount of data efficiently. This makes it more difficult for all the data to be sent to a Cloud based central data center.

Therefore, the mass amount of data is first processed in the sub-Cloud, Edge. Then the Edge filters the data first, before transmitting the data to the upper-Cloud. Through this data, the upper-Cloud develops a machine learning model, and then passes it on to the Edge. Through this process, the Edge of IoT devices processes the data sent by the machine and sets the appropriate commands. This system is called an 'Edge-To-Cloud'

In the Edge-To-Cloud system the privacy policy can be strengthened when data is being sent from the Edge to Cloud. Not only that, the security quality also rises during attacks such as DDos attacks or Web Service attacks when the Cloud is not accessible since the prescriptions of Edge platforms allow the Edge to still function.

6. Conclusion

Edge Computing is allowing a more efficient means of processing massive amount of data in the 5G·AI·IoT·BigData lead 4th revolution with by circulating between dispersing and focusing data.

There are opposing opinions on whether Edge Computing will invade Cloud Computing territory. However, if Cloud Computing is in need of improvements in server overloading and delays due to the IoT data, then it is certain that Edge Computing will surely support Cloud Computing. Therefore, it is necessary to keep an eye on how various industries utilize Edge Computing and build a structure.

7. Reference

[1] http://www.itworld.co.kr/news/107687
[2] http://ryufree.tistory.com/331
[3] http://www.itworld.co.kr/news/111118
[4] https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/
[5] http://etinow.me/246
[6] http://news1.kr/articles/?3365537
[7] https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiOrteServHistIFrame.kci?sereArticleSearchBean.artiId=ART002195348&sereArticleSearchBean.orteFileId=KCI_FI002195348
[8] http://mangastorytelling.tistory.com/attachment/cfile8.uf@99F1B53359DEB0F8320F7A.pdf
[9] http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw65&artId=1382641
[10] http://www.startuptoday.co.kr/news/articleView.html?idxno=210511

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

06 Focus on IGLOO SECURITY

IGLOO SECURITY Inc. '2019 security·threat prospect report'

IGLOO SECURITY

It will require accurate security threat analysis, a security architecture focused on swift incident response and security methodology.

[5th Dec. 2018] IGLOO SECURITY Inc. leader in the field of total security management of the next generation, released its prediction of next years security prospect through its '2019 Security Threat Technology Prospect Report.' This year marks the 7th year of releasing this report and IGLOO SECURITY Analytics team predicts the dangers of major cyber threats and how to respond to these attacks.

IGLOO SECURITY's Security Analytics Team predicts that next gen. technology and changes in the IT infrastructure will allow cyber attacks to become more cunning and will start to influence individuals and society more than ever before through means such as: circumventing new security technologies through hostile learning, intruding smart city vulnerabilities which are exposed due to the immense amount of users, devices and intricately connected network. While on the other side, those who work in the security management industry, are set to counter these movements through active, accurate analysis on security threats, swift security incident response.

Copyright © IGLOO SECURITY, Inc. 2018. All rights reserved.

Published by IGLOO SECURITY (www.igloosec.co.kr)
6 Floor. 7, Jeongui-ro 8-gil, Songpa-gu, Seoul, Korea
T. +82-2-3404-8678
E-mail. overseas@igloosec.com

Distributed by Cyber-Infinity Corp. (www.ci-corp.jp)
株式会社 シーアイシー
東京都千代田区霞ヶ関3-2-5霞ヶ関ビルディング5F
大韓貿易投資振興公社東京IT支援センターS03
T. +81-3-5501-0885
E-mail. bussiness@ci-corp.jp

Edited by IGLOO SECURITY Marketing Team
© 2018 IGLOO SECURITY, Inc. All rights reserved.
The copyright of this publication is held by IGLOO SECURITY. It is not permissible to reproduce, copy, or distribute any or all of the contents of this publication in any form or by any means without the prior written consent of IGLOO SECURITY. All information contained in the publication can be changed without prior notice.