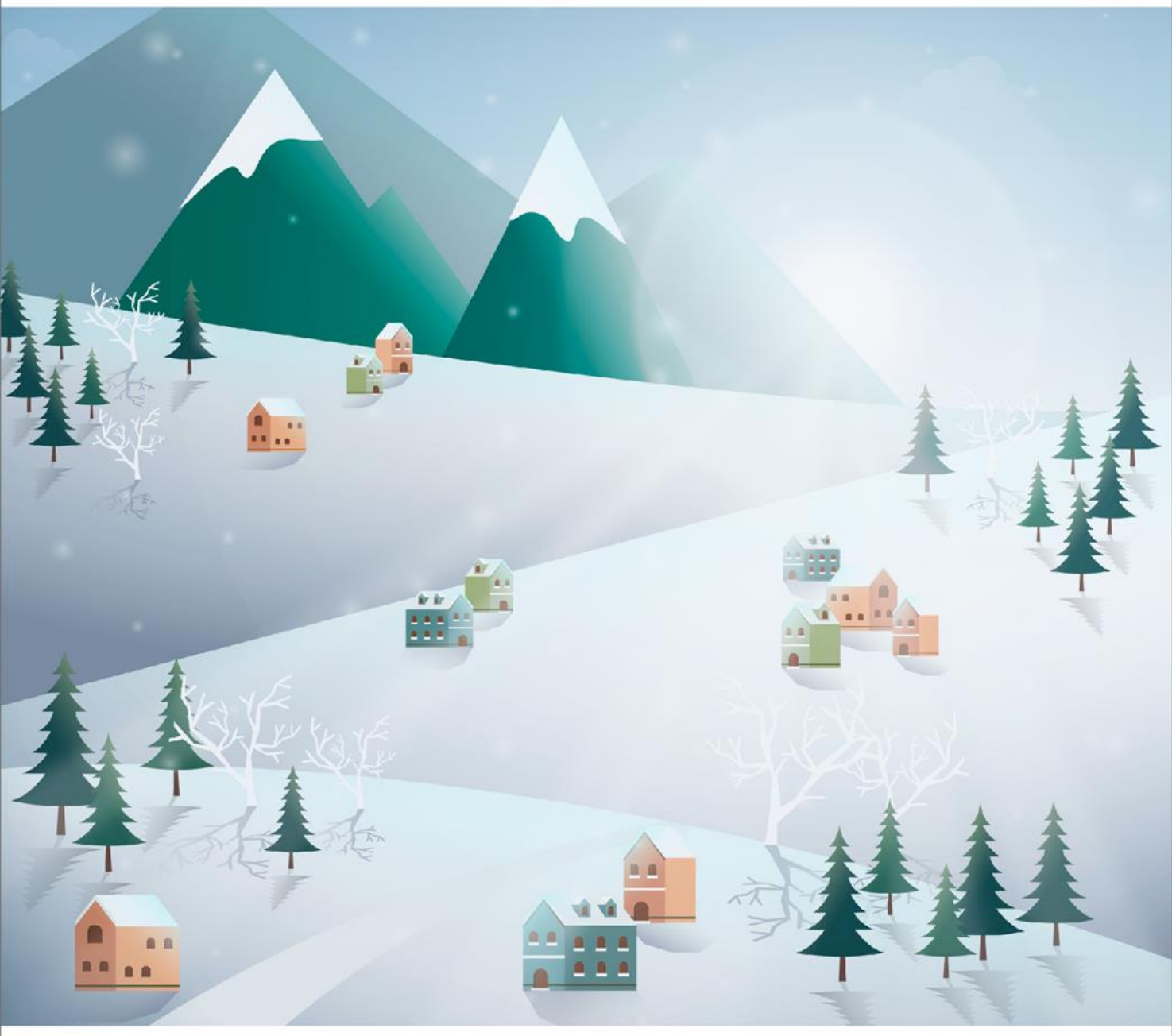
Monthly Security Report

2019
February



Cover Story

Guide to server monitoring and malfunction management through SPiDER-TM V5.0

How to efficiently use Threat Intelligence for security monitoring

IGLOOSECURITY

This report was written based on the event status, 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 clients from cybersecurity threat through continuous monitoring (24/7, 365 days), analysis, and response of cybersecurity issue.

Cover Story

1. Monthly Security Issues

- Monthly Security Issues

2. IGLOO Statistics

- Monthly Attack Service Trends and Analysis
- Detailed Analysis Results of each Attack Pattern

3. SIEM Guide (SPiDER TM V5.x)

- Guide to server monitoring and malfunction management through SPiDER-TM V5.0

4. Special Column

- How to efficiently utilize Threat Intelligence for security monitoring

5. Focus On IGLOO Security

- This Month’s IGLOO SECURITY

01 Monthly Security Issue

Monthly Security Issues

‘Strangers are watching’…Warning for Digital door lock hacking

- The possibility of cyber attacks on security vulnerabilities of 'wireless communication based devices' such as 'Wall pad' and 'Digital door lock' which can control home ICT equipment has been discovered.
- Norma co., a wireless network security company, gave a demonstration on the process of opening a digital door lock through the ‘Signal Replay Attack’ which catches wireless signals generated by the pad in a separate transceiver when the door is opened which then copies and amplifies the wireless signals and transmits the amplified signal back to the door lock. If someone has a wireless signal transmitting and signal receiving device which they can easily get online or offline for only 200$~300$, everybody can open a door lock regardless of the complexity of the password and how often the password is changed.
- Security experts advise that many wireless devices used in everyday life are left vulnerable to basic signal retransmission attacks and that they should choose security-enhanced products at the manufacturing stage.

‘An M&A you say? Don’t forget security measures~’…The Marriott Hotel hacking case demonstrates the importance of security

- In late 2018, the Marriott Hotel Hacking case occurred, where information valued at approximately $450,000 thousand was leaked. This incident has garnered the attention of the security industry. This was because it had a different aspect from other security issues in general. This was because the attack originated from Starwood Hotel's system where the incident occurred. Starwood Hotel merged with Marriott Hotel in 2016.
- According to surveys conducted by Checkmarx, a security company, the attack on the Starwood POS system occurred two weeks after the M&A deal was signed, and if only Marriot had inspected Starwood Hotel’s security system, it would have been more than enough to prevent the attack.
- Security experts claim that even though an incident originates from the subsidiary, the responsibility can only be directed at the parent company and that security risks should be as carefully inspected as information such as budget, market share etc.

‘Still there’…Cryptocurrency exchange markets, still vulnerable to attacks

- Despite the numerous hacking risks that still exist, the security level of cryptocurrency exchange markets still maintain a low standard.
- According to an MSIT(Ministry of Science and Technology) and KISA (Korea Internet Development Agency) survey conducted on 21 cryptocurrency exchange markets from September to December of 2018, 7 exchange markets satisfied all 85 inspection criteria, but the remaining 14 only satisfied 61 criteria showing a low standard of security and raising concerns over vulnerabilities against attacks.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Monthly Security Issues

‘I only go after one target’…A malware family which uninstalls cloud security products has been detected. Its goal is to mine cryptocurrency.

- A malware family which intrudes a targeted system and uninstalls cloud security products has been discovered.
- According to Palo Alto Networks, attackers, known as 'Rocke', use this malware to gain administrator authority and then delete security products developed by Tencent Cloud and Alibaba Cloud in order to inject Monero mining malware.
- Security experts predict there will be more attempts to attack agent-based cloud security solutions, and advise public cloud companies to thoroughly prepare for these attacks.

‘Can you send my salary to a new account?’…The New type of ‘BEC(Business Email Compromise)’ attack is detected

- As the BEC pattern changes, a spear phishing attack that encourages enterprises to send large amounts of money to the wrong bank account, more attention and awareness is required.
- In the past, attackers disguised themselves as either a CEO or a CFO and asked victims to send large amounts of money to a specified account. However recently, attackers tend to disguise themselves as one of the many employees at the company and attempt to intercept the salary of the employee they are disguised as.
- They would send an email to HR and say that they have “recently changed their bank account so please transfer ‘my’ salary to he new account.” and if by any chance the salary is not deposited in the their account, the attacker will persuade HR that by not using the new account, they might have to request various documents from the company.
- Security experts explained that hackers are currently heavily scanning the payroll system of the company as well as carrying out attacks. They also advise that HR representatives should thoroughly look through emails and contact security if they notice any thing suspicious.

‘Don’t be bedazzled’…Beware of the 'Vidar' malicious code which seizes user information through a ransomware injected through a website advertisement.

- Users should be aware of the spread of Vidar, a malicious code which seizes user information through a ransomware injected through website advertisements.
- In order to spread Vidar, hackers use the malvertising technique, an attack which uploads malicious advertisements on websites with vulnerable security levels and wait for users to click on the advertisement.
- When a user enters the website containing the malicious code, the 'fallout' exploit kit analyzes the users access environment and if the user has not updated the Internet Explorer(IE) browser vulnerability patch, then the 'Vidar' malicious code will be installed.
- The 'Vidar' Malicious code collects data concerning the users PC system (OS, network connection, HW etc.) and sends it to the hacker. After the information theft process is complete, the 'Gandcrab' ransomware is downloaded and critical files within the PC are encrypted.
- Security Experts advise users to maintain the OS, web browser, application programs etc. to the latest versions and refrain from visiting illegal adult sites, torrent sites and any other sites with low security levels.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Monthly Security Issues

Japanese Government begins to monitor IoT Devices as a means to enhance security ahead of the 2020 Tokyo Olympics...public resentment rises within the Japan

- The Japanese Government has come under scrutiny after passing a bill which would allow them to monitor IoT devices under the rationale of increasing public safety. According to ZDNet, a US based IT news website, the Japan NICT (National Institute of Information and Communications Technology) will provide internet service providers with information concerning a list of IoT devices that have vulnerabilities. The goal is to notify the public on which devices are vulnerable, thus protecting them from security threats.
- Due to concerns over hackers attacking the Tokyo Olympic IT infrastructure through vulnerable IoT devices, the Japanese Government is planning on investigating 200 million passwords of various routers, webcams and other devices.

Will the EU and US officially implement GDPR fines aimed at IT companies?...Googles imposed with a fine of about €50 million

- Recently the EU has implemented a GDPR (General Data Protection Regulation) fine of about €50 million on Google. This case has garnered the attention of the international community as it awaits to see if this will trigger a wave of GDPR fines within the EU.
- On the 21st of January, French Data protection agency CNIL (Commission Nationale de L'informatique) fined Google € 50 million under the pretext that Google had violated transparency laws concerning personal information processing and agreement clauses. The CNIL claimed that Google had dispersed the information(data processing, storage period and other information concerning data processing) so that it could not be seen in one glance. They added that this prevented consumers from verifying how their information was being used and that this was against transparency regulations.
- Google announced that they are planning an appeal the decision. Google claims that they have invested large amounts of time and resources in developing a personalized advertisement system which does not violate the GDPR and that they are concerned about the effect this case will have not only in Europe but to all the publishers, content creators and technology companies around the world.

US Department of Justice, indict Huawei and Mengwang Huawei CFO... 13 charges including technology theft and violating sanctions imposed on Iran

- According the Reuters and other media sources, the prosecution of Huawei and its CFO Mangwang before the high-level trade negotiations, planning to be held in Washington DC, has gained much attention.
- Hwawei is currently under the charge of violating sanctions imposed on Iran and supplying Iran telecommunications company with device parts. Huawei is also being accused of having stolen a smart phone technology named 'Tafi' from US telecommunications company T-Mobile.
- Under the request of US Authorities, the US Federal Police are attempting to gain custody of CFO Mang Wan Zhou, who was arrested in Vancouver, by Canadian Authorities.
- After the news was revealed, Geng Shuang, spokesperson for China's foreign ministry claimed that the US was targeting Chinese businesses and urged the US to stop pressuring Chinese companies from carrying out legitimate businesses.

Copyright © IGLOO Security, Inc. 2019. 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 and Trend Analysis

Monthly Attack Service(Port) TOP 10

As a result of the event analysis collected in February 2019, Telnet (TCP/23), SNMP (UDP/161) related events were decreased compared to the previous month. ICMP (0/UDP), Unassigned (TCP/8001) server events were increased. NetBIOS (UDP/137) event has newly entered the rankings.

※ Based on Igloo Security SOC SIEM data collection

Rank	Server (Port)	Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	1,768,886,549	45.42%	-
2	DNS(UDP/53)	681,071,733	17.49%	-
3	Microsoft-DS(TCP/445)	466,277,818	11.97%	-
4	HTTPS(TCP/443)	382,108,240	9.81%	-
5	ICMP(0/ICMP)	181,751,205	4.67%	▲1
6	SNMP(UDP/161)	171,712,327	4.41%	▼1
7	IUA(TCP/9900)	110,121,466	2.83%	-
8	Unassigned(TCP/8001)	51,879,331	1.33%	▲2
9	Telnet(TCP/23)	47,585,109	1.22%	▼1
10	NetBIOS(UDP/137)	33,471,478	0.86%	NEW
Total		3,894,865,256	100.00%	-

[Table 2-1] TOP 10 Attack ports throughout the month

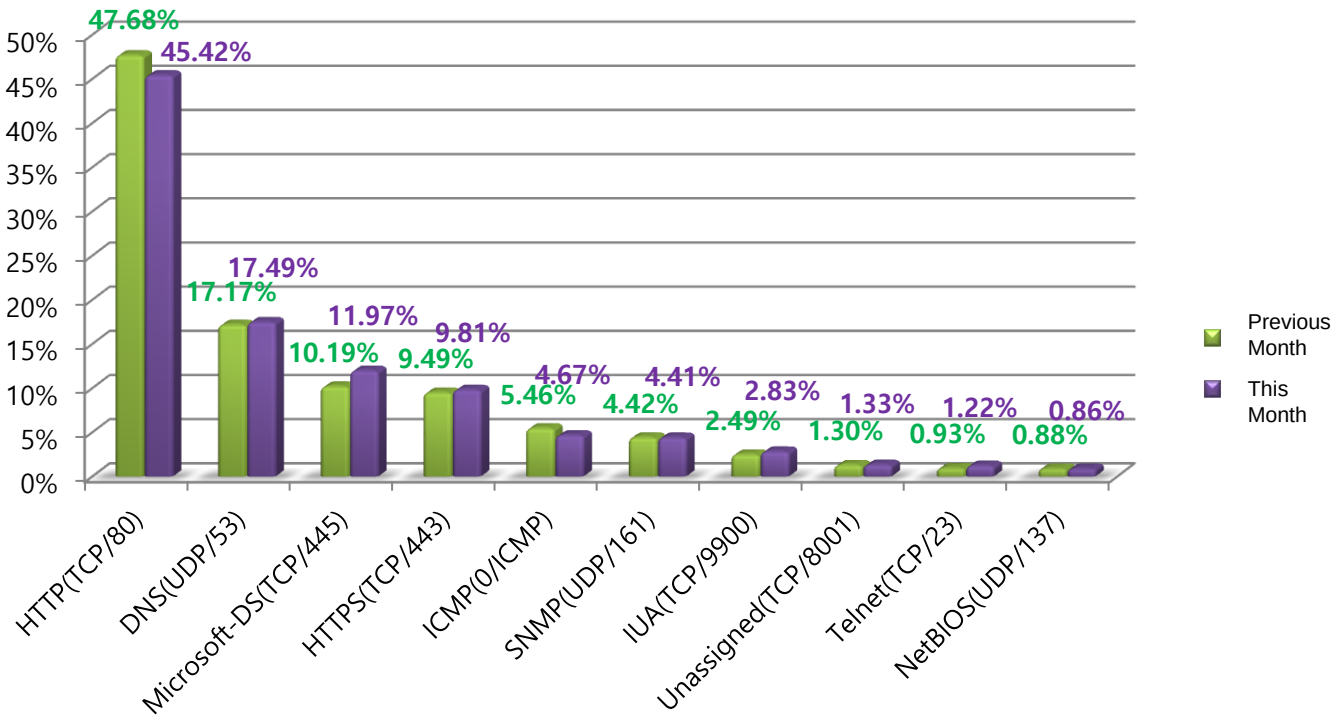
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

02 IGLOO Statistics

Monthly Attack Service and Trend Analysis

Monthly Attack Service(Port) cases compared to last month

Among the events collected in February 2019, events using ICMP and Unassigned (TCP / 8001) ports have increased compared to January. SNMP and Telnet events have decreased. NetBIOS(UDP/137) events has newly entered the ranks. Netbios is one of the MS programs that enables communication within a local area network. It is commonly used when sharing files and printers over a network. Recent, attempts to infect malicious code using a file sharing service such as NetBios have been continuously occurring, if you do not use the service, disabling it is recommended.



[Figure 2-1] TOP 10 Attack ports throughout the month

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

02 IGLOO Statistics

Igloo Security has ranked the latest attack patterns through the SOC and this will help understand security trends.

Monthly Attack Service and Trend Analysis

Monthly Attack Service Pattern TOP 10

According to results of the February 2019 incident analysis, SYN Port Scan, HTTP POST Session Exhaustion Attack(By rudy) events have occurred. Dcom_TCP_Sweep and 2 other patterns dropped in rank. However, There is no significant change in the number of detections compared to the previous month.

※ Based on Igloo Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	635,197,654	75.73%	-
2	ACK Port Scan(F/W Scan)	123,587,002	14.73%	-
3	MySQL-Server Login Brute force	23,814,994	2.84%	-
4	SYN Port Scan	20,521,740	2.45%	NEW
5	Dcom_TCP_Sweep(MSBlaster Worm Messenger)	8,475,014	1.01%	▼1
6	HTTP Connection Limit Exhaustion Attack (By Slowloris)	8,433,764	1.01%	-
7	Multi Packet Inspection	6,170,762	0.74%	▼2
8	MS WINS Server Registration Spoofing Vuln-1 [Req](UDP-137)	5,426,260	0.65%	▼1
9	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	3,738,954	0.45%	-
10	HTTP POST Session Exhaustion Attack(By rudy)	3,418,492	0.41%	NEW
Total		838,784,636	100.00%	-

[Table 2-2] TOP 10 Attack patterns throughout the month

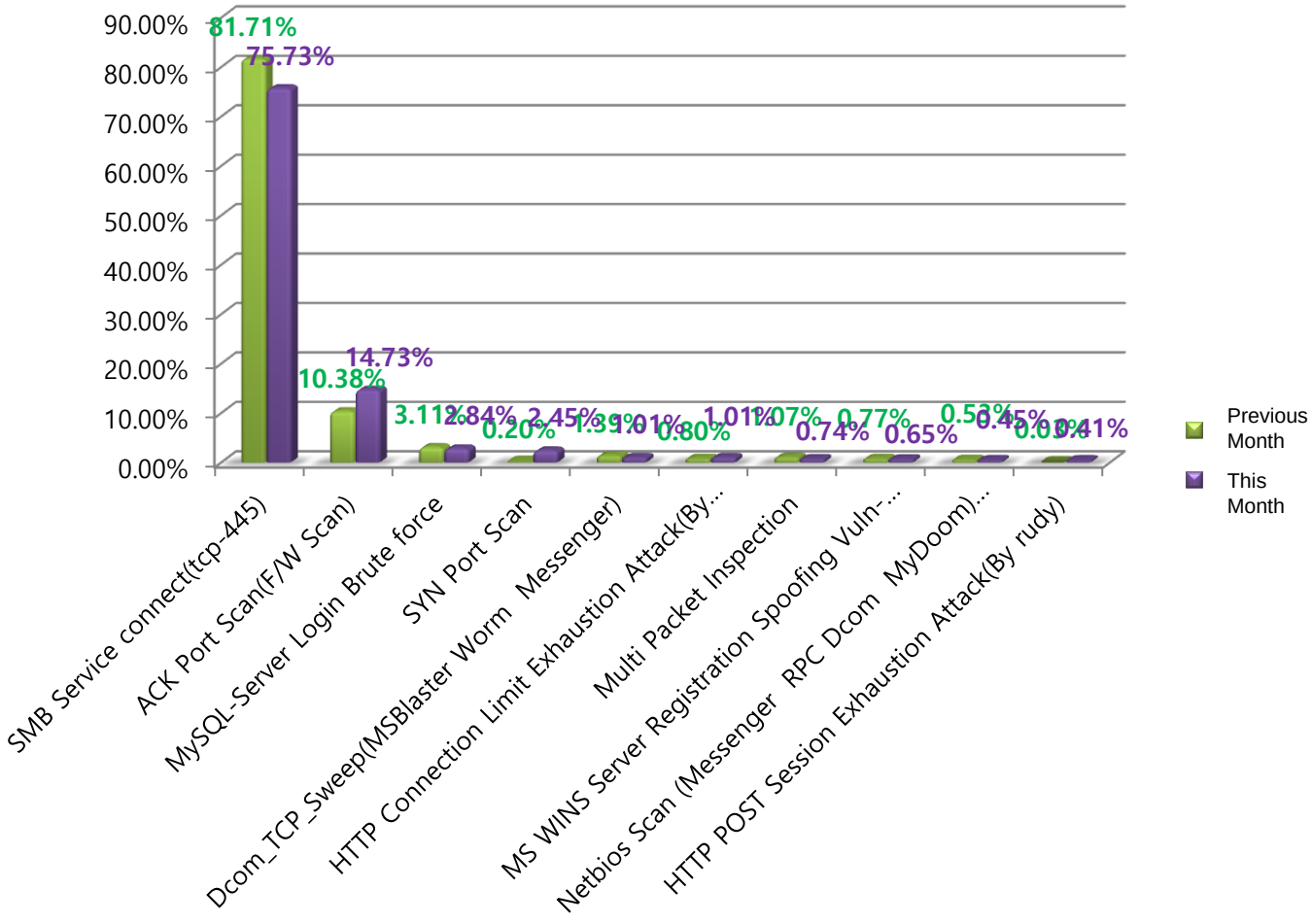
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

02 IGLOO Statistics

Monthly Attack Service and Trend Analysis

Monthly attack service incident patterns compared to last month

As a result of the attack event analysis of February 2019, the ratio of SMB service connect (tcp-445) event increased by 5% compared to the previous month, but the number of detections have slightly increased. The number of TOP 3 attacks have increased overall, and other attacks show minimal changes (below 3,000,000 cases). The Top 3 attacks, which account for about 90% of all attacks, are closely related to internal information breaches (service port scan, user account information, and SMB service scan), so it is necessary to establish access control lists (ACLs) and prohibit the use of simple passwords for user accounts.



[Figure 2-2] TOP 10 Attack patterns throughout the month

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

02 IGLOO Statistics

Detailed Analysis Results of each Attack Pattern

A detailed introduction on the attack pattern is carried out based on the January TOP 10 Attack Patterns. The vulnerabilities of the system are prepared in advanced for an attack based on the data collected and analyzed.

Attack Pattern	Results from Detailed Analysis
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.
SYN Port Scan	SYN Port Scan sends SYN signal to all ports from port 0 to port 65,535 either sequentially or randomly to find out if certain TCP/IP ports are opened to provide service in the targeted computer
Dcom_TCP_Sweep (MSBlaster Worm Messenger)	The W32.Blaster.Worm worm is a type of worm that spreads by exploiting the DCOM RPC Buffer Overflow Vulnerability. The worm activates the TCP / 135 port and infects the system if a vulnerability is detected. The infected system activates the TCP / 4444 port to download a malicious file from the host server and register it in the registry. In this process, the traffic of the infected system may rise.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

02 IGLOO Statistics

Detailed Analysis Results of each Attack Pattern

Attack Pattern	Results from Detailed Analysis
HTTP Connection Limit Exhaustion Attack (By Slowloris)	Slowloris is an attack tool that maintains TCP connection by transmitting an abnormal HTTP request to a web server unlike a DoS attack type that transmits a large amount of packets. The target web server may be exhausted from the connection resource, and after the connection resource is exhausted, the web server falls into a service denied state of being unable respond to user's request.
Multi Packet Inspection	A rule that can occur in a specific company IPS is detected by the automatic pattern learning defense function set in the IPS. If a packet that has the same pattern more than Bytes set in the IPS is repeatedly inputted, the access is blocked for the set time in the IPS.
MS WINS Server Registration Spoofing Vuln-1 [Req](UDP-137)	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.
Netbios Scan (Messenger RPC D com MyDoom) (UDP-137)	NetBios checks each other's information with UDP port 137, establishes a session with TCP 139, and exchanges data via TCP 138. An attacker can use this UDP port 137 to establish a session with an attack target system and scan information about the folder and network shared by the target system.
HTTP POST Session Exhaustion Attack(By rudy)	R.U.D.Y is an abbreviation of "R-U-Dead-Yet" and is a connection resource-depleted denial of service tool using the POST method of HTTP. It generates a large number of connections that are not normally terminated by using an incomplete HTTP header and divided data, and exhausts the connection resources of the target system.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

03 SIEM Guide

SPiDER TM V5.0 is the manifestation of Igloo Security's security management experience and ability apply big data into an Integrated Cyber Security Management Solution. It's capacity ranges from the initial threat detection to log/network packet analysis through a single security management environment. This allows its users to have ensure both efficiency and an overall view on the infrastructure

Guide to Server monitoring and malfunction management through SPiDER TM V5.0

Tech Support Center
Tech. Support Team 1

1. Synopsis

The SPiDER TM V5.0 is a prime example of a SIEM (Security Intelligence Event Management) solution. It installs Agents on the designated server and gathers various information concerning the server it is installed in.

Although the SMS (Server Integrated Monitoring System) also contains similar functions, the SIEM supports additional functions such as managing the system through monitoring, having the Agents deployed onto the SIEM, manufacturing the collected information and applying this information as alarms on the SIEM. Thus, the SIEM monitors crucial system files besides collecting important server information (Messages, secure, last, cron). The SIEM is also capable of collecting and manufacturing a server's crucial system resource information (CPU, Memory, Process, Disk Using) and applying it to meet its purpose.

Recently, due to the implementation of the access control solution, designed to control access to the server, it is possible to manage the 'Login' process but it is difficult to verify access from another system's backdoor or server access through a vulnerable section.

However, the SIEM can detect unauthorized activity within the server through the 'secure' and 'last' logs. The SIEM's ability to monitor server malfunctions through the server's system resource information and other PING CHECK functions.

Therefore, let us check if the SIEM can perform monitoring duties on server systems and malfunctions.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

2. Attack scenario

Let's summarize the main server system files collected by the SIEM Agent (Unix / Windows).

Log Type	Linux	AIX	HPUX	Solaris
messages	○	○	○	○
wtmp/utmp	○	○	○	○
wtmpx/utmpx				○
btmp	○		○	
Pacct	○	○	○	○
lastlog	○	○	○	○
sulog		○	○	○
errlog		○		
Xfertog(FTP Log)	○	○	○	○
audit.log	○			
secure	○			
syslog		○	○	○
history	○	○	○	○
authlog				○

[Table 3-1]Logs from Unix

Log Type	Windows
Application	○
System	○
Security	○
Active Directory Service	○
DNS Service	○

[Table 3-2] Logs from Windows

SIEM can collect and utilize the above logs to detect unauthorized activity within the server.

For example, there is a server history log and a secure log. We can find a log of what commands the user has left in the history log and we can find records of user credentials for telnet and ssh connections in the secure log. The log can be checked in more detail than the utmp log being collected above. So, it should be set up in superior level to be collected when the SIEM Agent is integrated. In addition, it can collect additional important log file from the server and apply the corresponding SIEM policy.

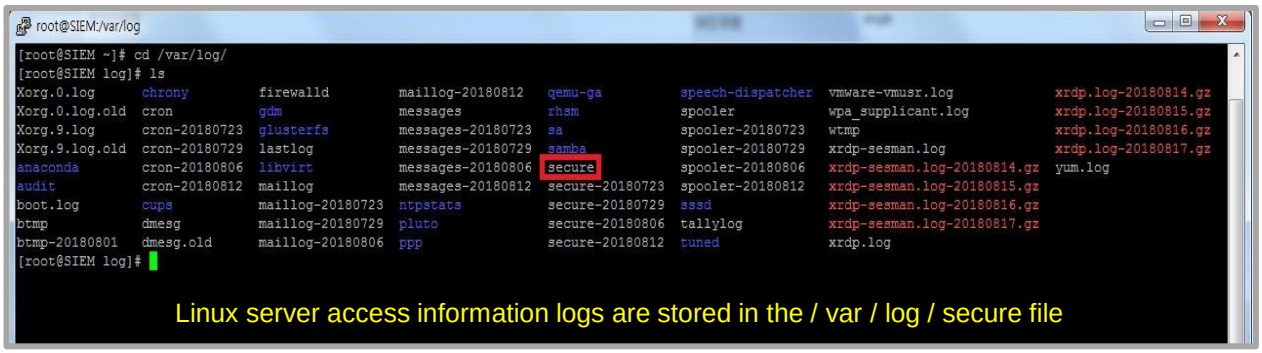
It is possible to collect such logs as shown above due to the function which allows files to be collected within the SIEM Agent thus, allowing the process of security monitoring to become more fluid. Therefore, the next chapter will be a guide on monitoring methods of monitoring unauthorized activity in the server through the SIEM logs shown above.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

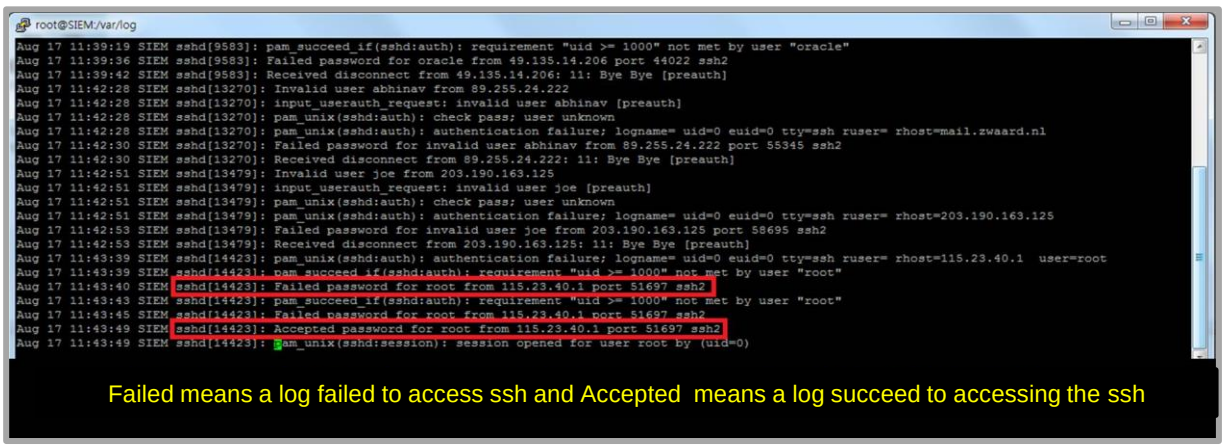
1) Unauthorized access detection through SIEM

To help users understand SIEM we provide tests and examples focused on the Linux system. Please refer to the following example. You can apply the following detection methods depending on your situation by setting the OS and environment configuration.

▶ Server log information concerning 'Server System Log in' Detection Monitoring



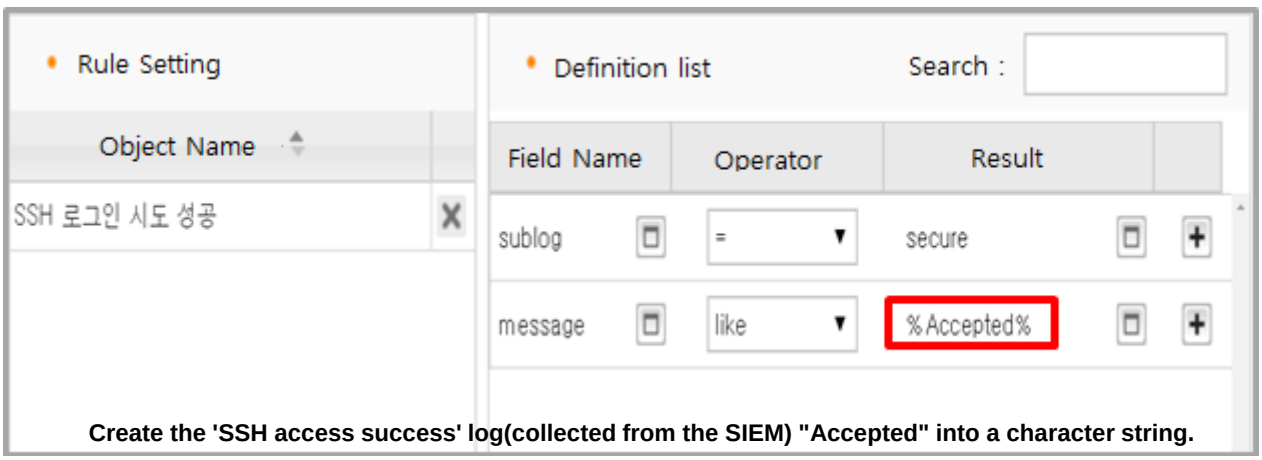
[Picture 3-1] Secure log check



[Picture 3-2] Detailed secure log check

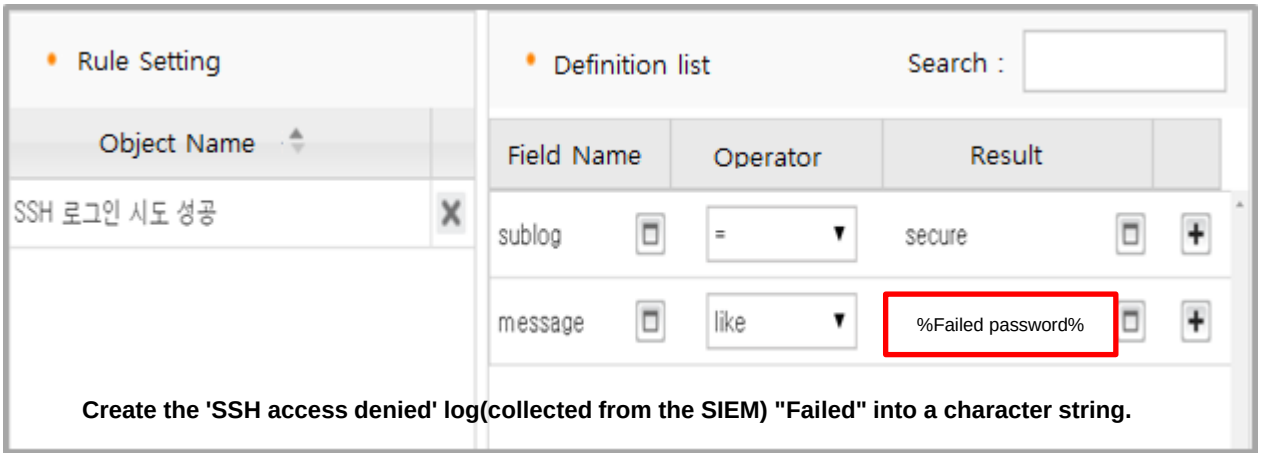
▶ How to apply SIEM in order to monitor server information

Managing the Menu application order of SIEM → creating the Object shown below in the Object Management menu



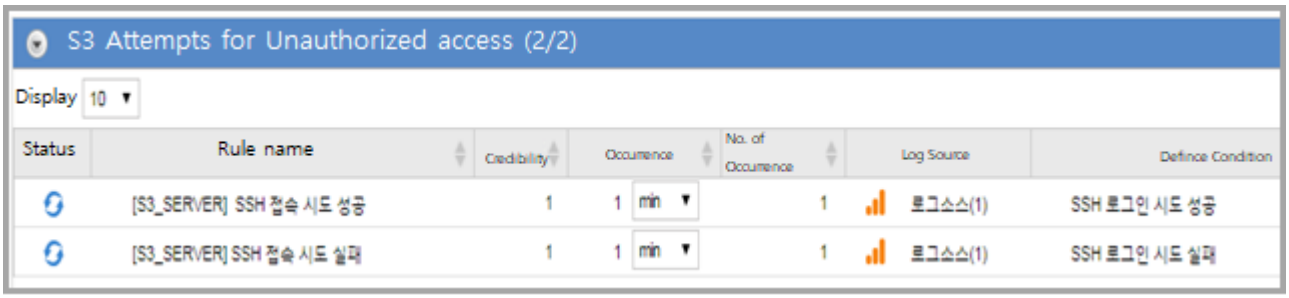
[Picture 3-3] Success message for Object registration

Copyright © IGLOO Security, Inc. 2019. All rights reserved.



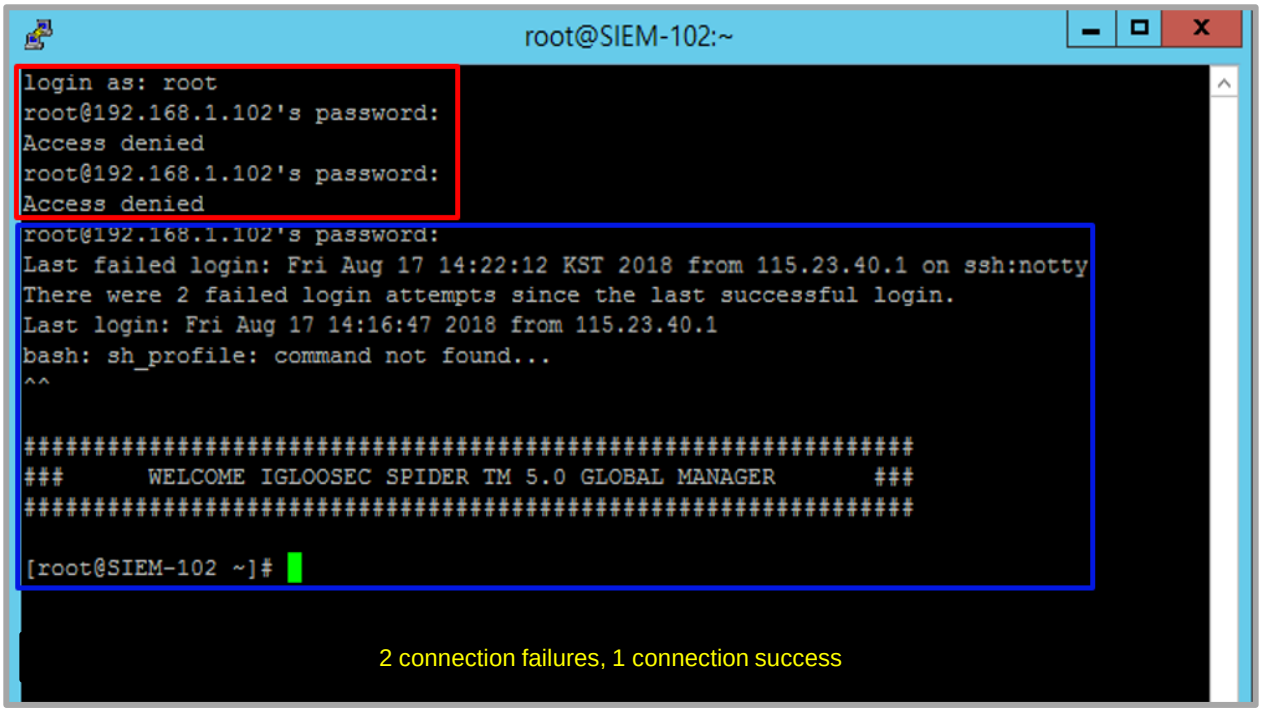
[Picture 3-4] Registration of Fail message as Object

Managing the Menu application order of SIEM → creating the Object shown below in the Object Management menu



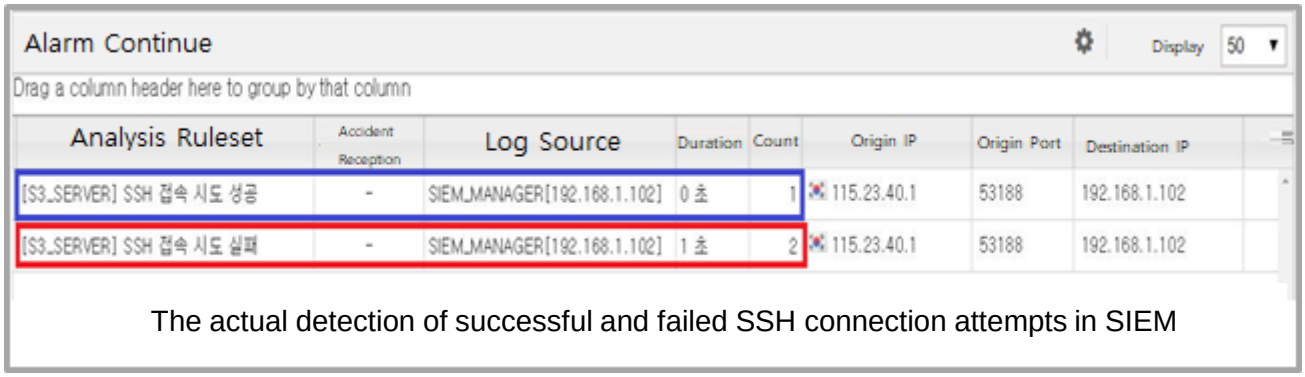
[Picture 3-5] Example of single alarm application

Test procedure to check whether SIEM alarm operates normally



[Picture 3-6] Server login test

Copyright © IGLOO Security, Inc. 2019. All rights reserved.



[Picture 3-7] SIEM alarm activated

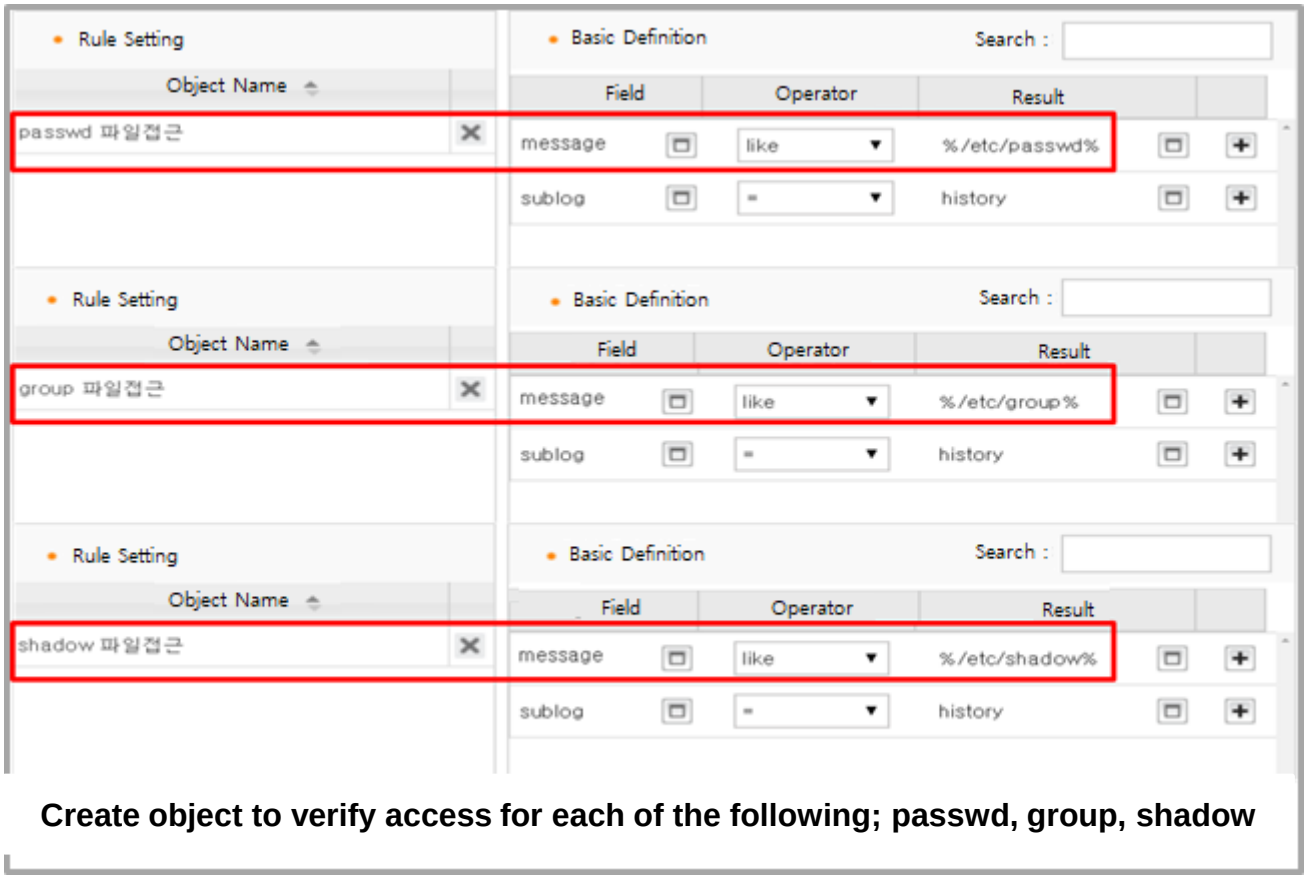
It is possible to verify and respond to unauthorized detection in real-time as shown above. Additional security monitoring is possible on servers which contain access controls by integrating the access control aspect with the SIEM.

▶ How to apply monitoring through the Linux History Log detection

This section will introduce users on how to detect attempts at accessing crucial files through the Linux .bash_history command.

※ This process is only possible through the support of an engineer and a request in advance for .bash_history logs.

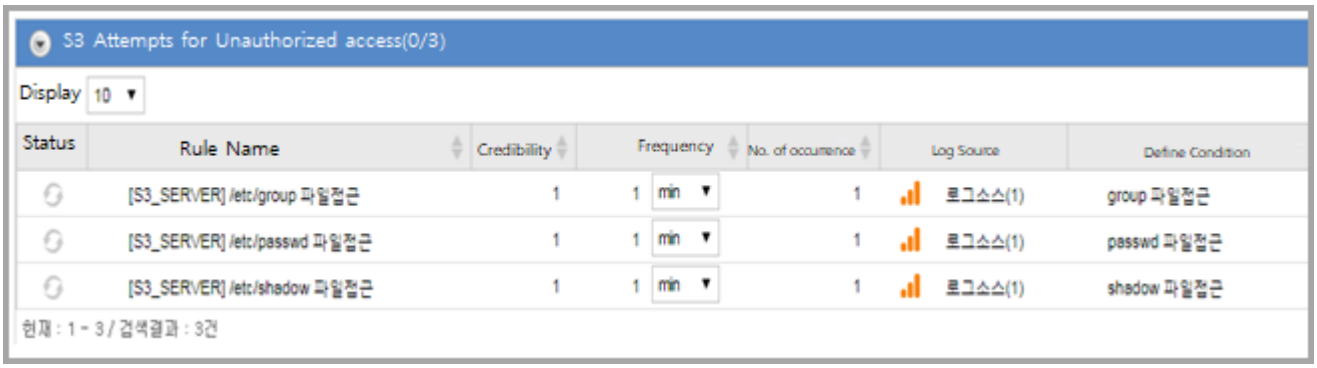
Managing the Menu application order of SIEM → creating the Object shown below in the Object Management menu



[Picture 3-8] How to apply objects

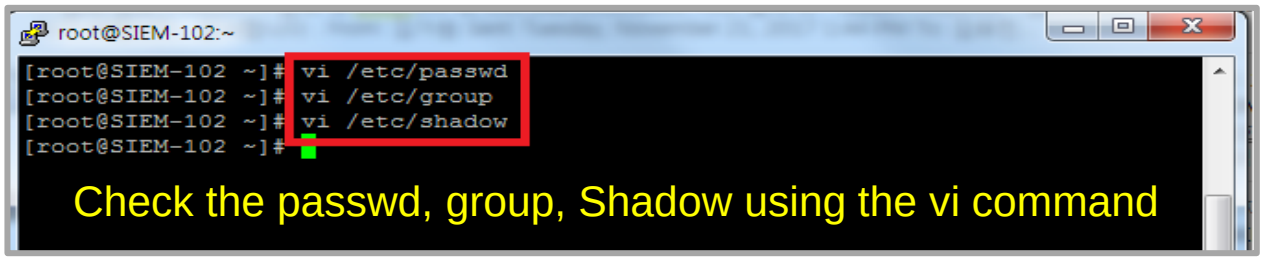
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Managing the Menu application order of SIEM → creating the Object shown below in the Object Management menu



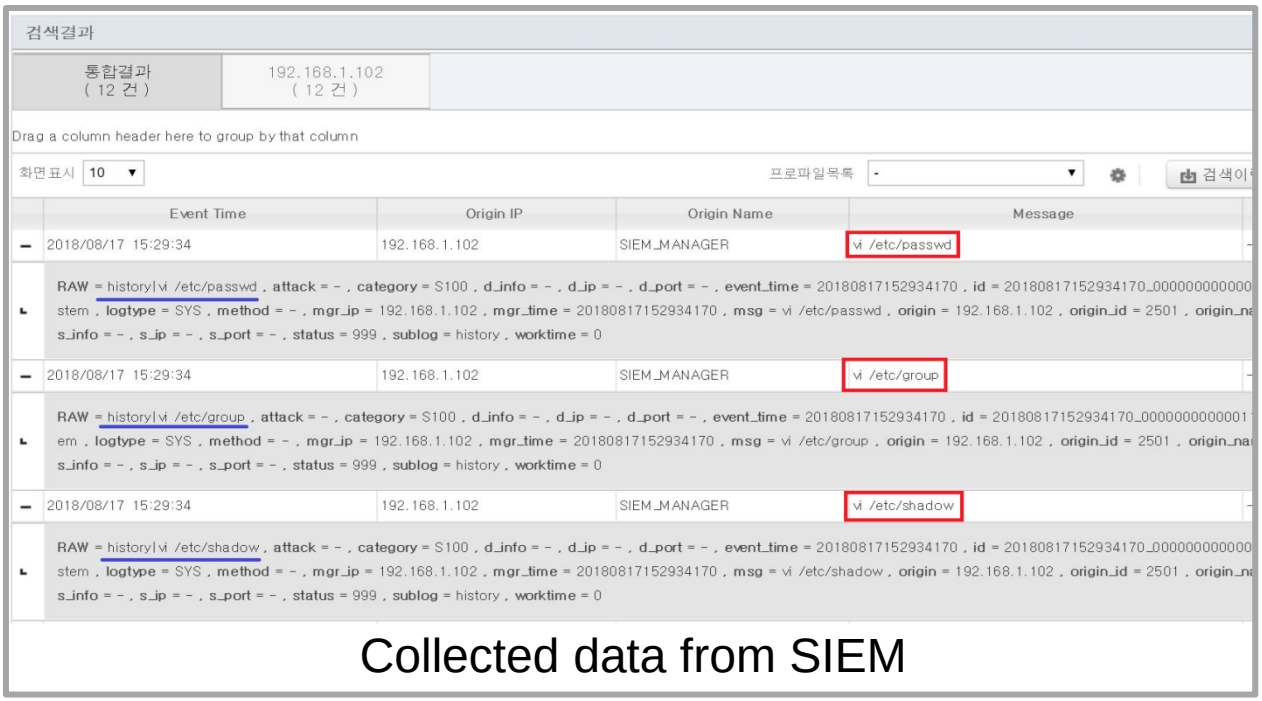
[Picture 3-9] Example of single alert application

On the actual server, we can checked the corresponding files using the “vi” command shown below.



[Picture 3-10] Actual server test

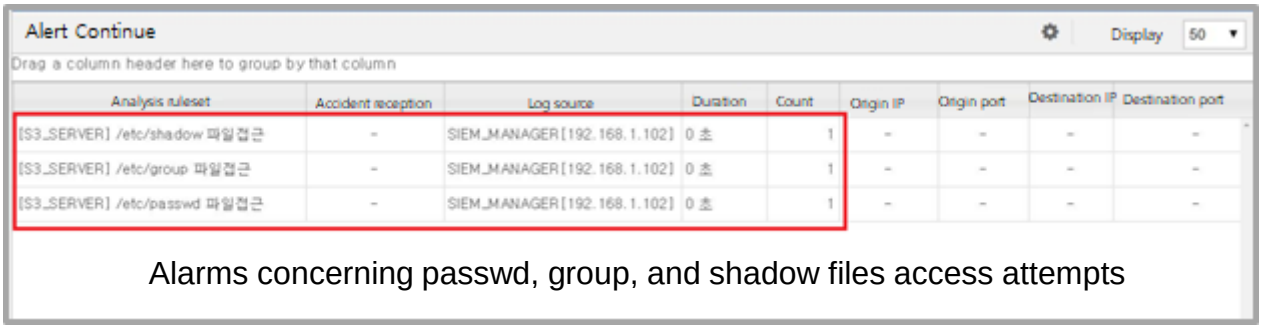
The actual logs are searched in the SIEM as follows.



[Picture 3-11] Log search screen

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

We can check that the following alarm occurred in the SIEM



[Picture 3-12] Alert screen

3. Methods for monitoring malfunctions through the SIEM

Server malfunction monitoring is made possible through the basic functions provided by the SIEM such as collecting information on basic CPUs, Memory, DISK storage, processes, Ping Check and Ports of the servers. Users can set a threshold value to the CPU, Memory, DISK storage and set an alert if there is an anomaly to the threshold value. Ping Check also monitors critical ports or processes and is an effective way to check if they is a problem

In addition, SIEM determines whether an event is collected while integrated with a security equipment to support intuitive decision making which might occur during an event in integrated alert.

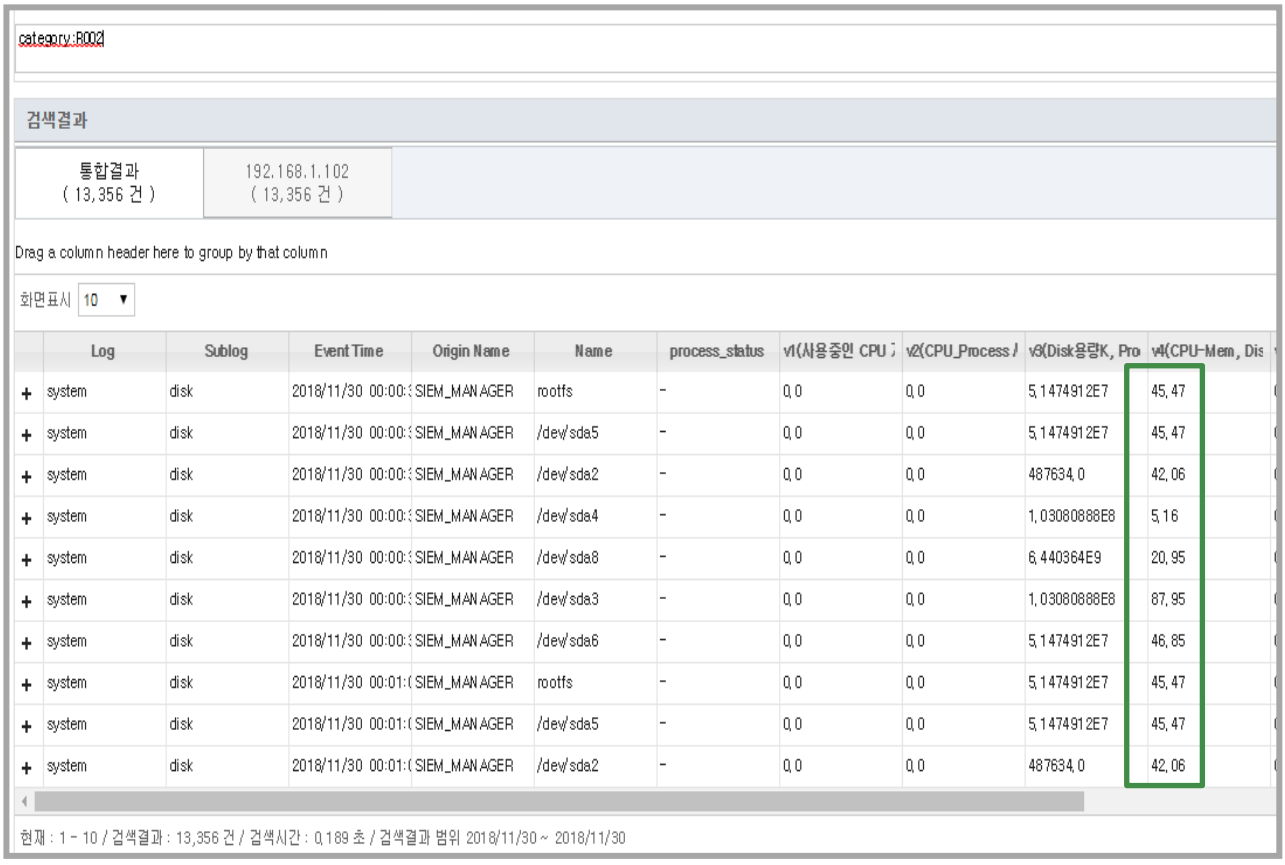
1) How to monitor malfunctions through SIEM

▶ Malfunction managing through configuration of DISK threshold

Example) set the disk threshold of the / dev / sda3 partition to 80, and set the alarm to go off when the usage of it's rate is over the 80.

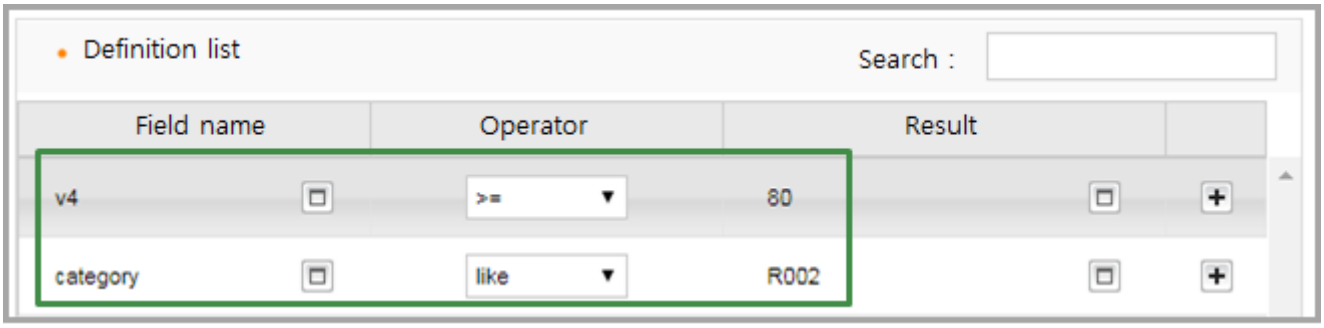
Detailed log information about the use of DISK in SIEM is R002 and v4 is DISK usage rate.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.



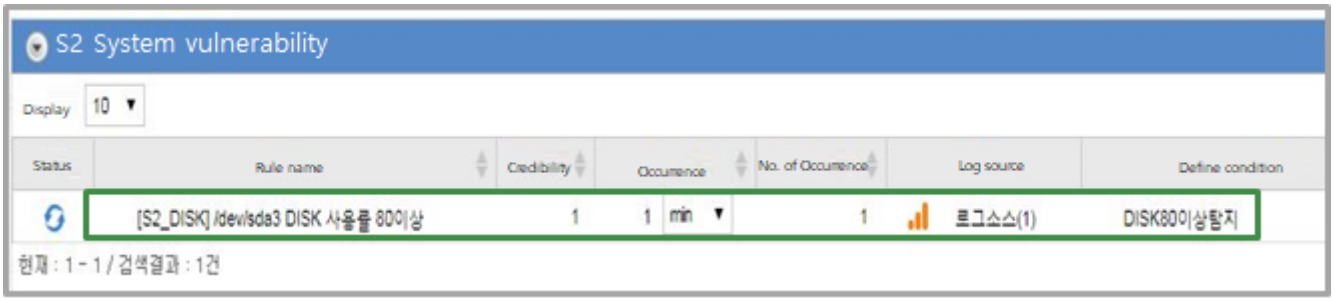
[Picture 3-13] DISK use rate screen through log search

Managing by Menu application order in SIEM -> Create Object management menu as shown below



[Picture 3-14] Register DISK object

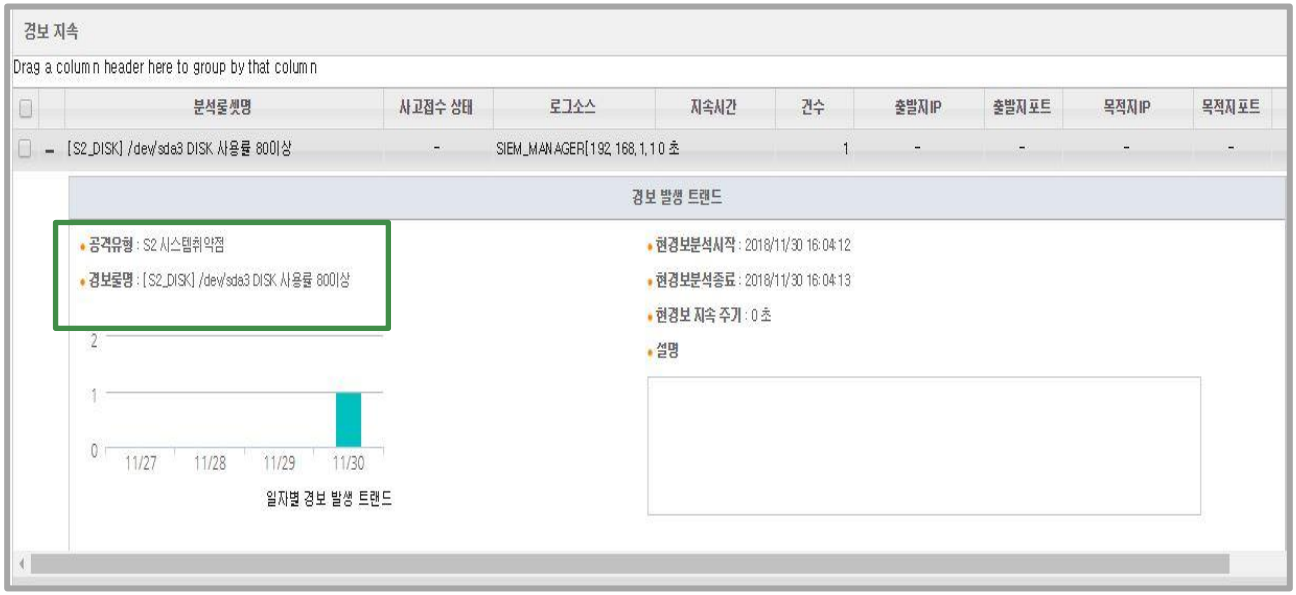
Managing the Menu application order of SIEM → creating the Object shown below in the Object Management menu



[Picture 3-15] DISK single alarm register

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Below is a screen of an alert going off in the SIEM.



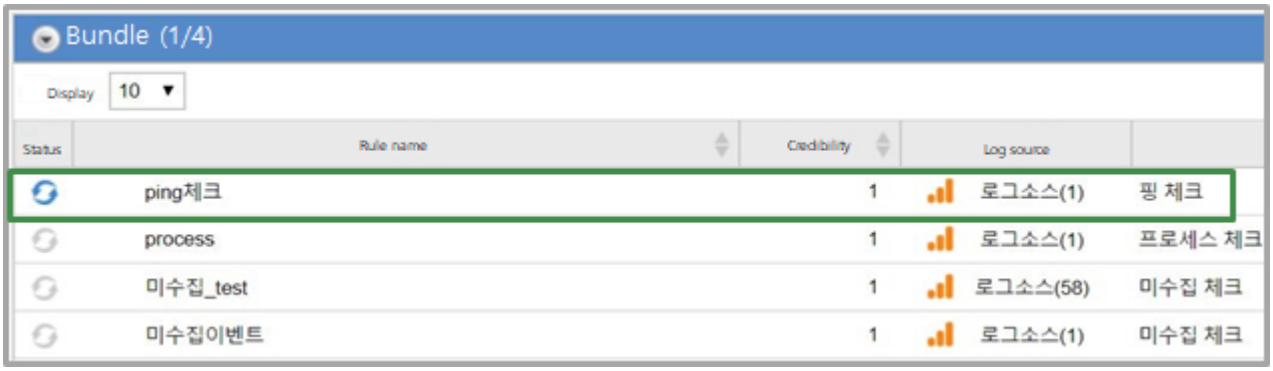
[Picture 3-16] DISK alert of correlation analysis

It is possible to manage the DISK effectively by applying the pre-alarm to prevent the Disk from becoming Full.

▶ Server malfunction managing through the Ping Check function setting

Example) 192.168.100.100 is the IP address for the critical server and the function test will be carried out under the assumption that communication has been severed due to an anomaly in the server network.

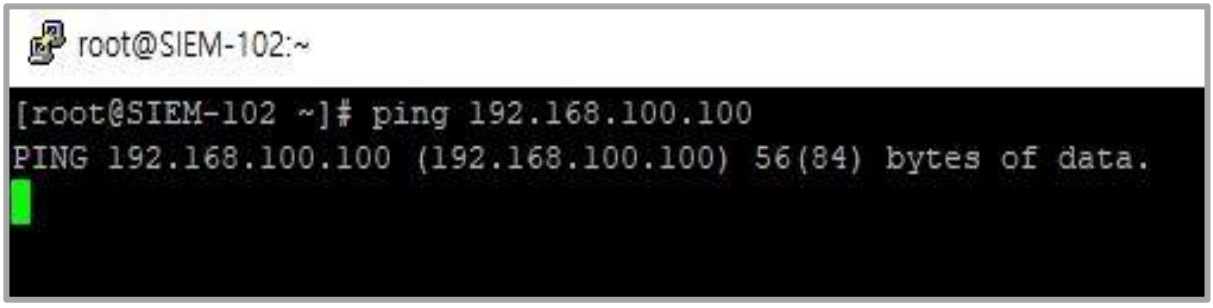
Managing the Menu application order of SIEM → creating the Object shown below in the Object Management menu



[Picture 3-17] Ping check function from bundle rule is activated

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

A Ping from an actual server was transmitted to 192.168.100.100, however the Ping did not reach its designated destination.



[Picture 3-18] Screen of attempting to send ping from server

[Picture 3-19] Correlation analysis ping alarm is activated

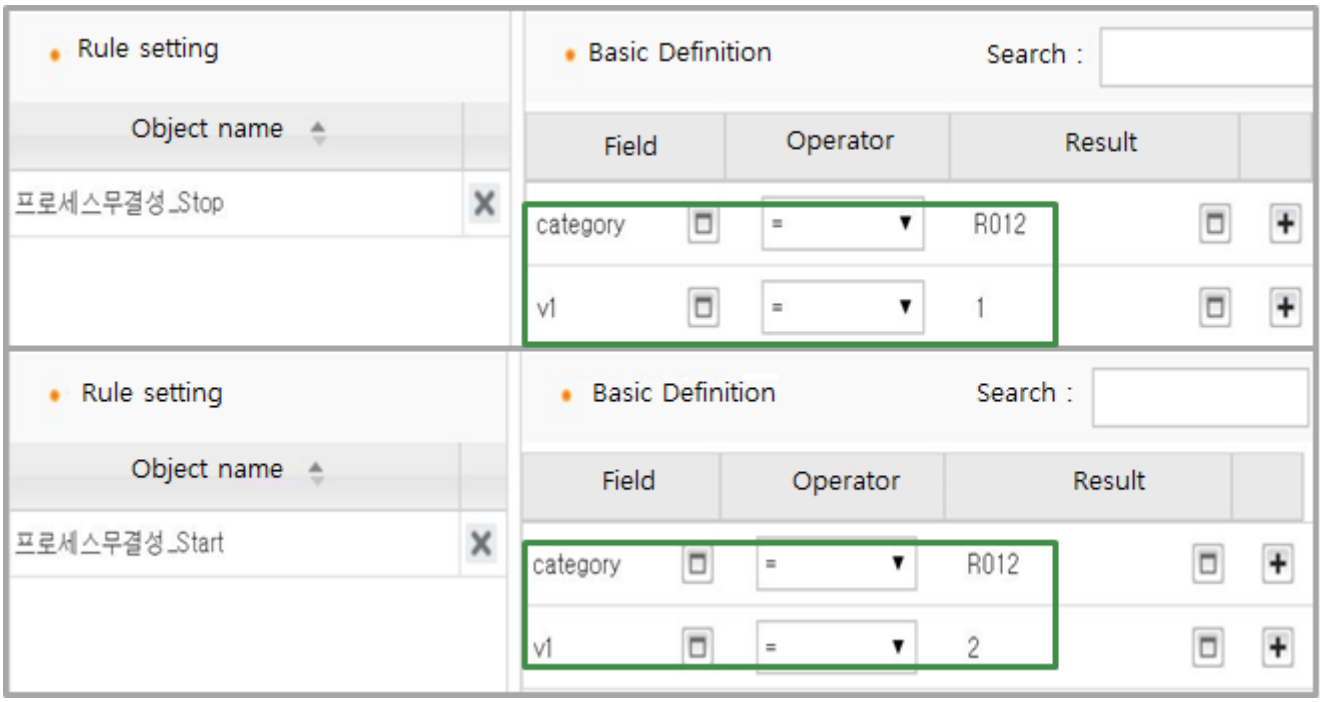
If there is a malfunction with crucial equipment and network the Ping Check function can easily be used to perform malfunction monitoring.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

▶ Detecting important process through the detection of the 'process' function

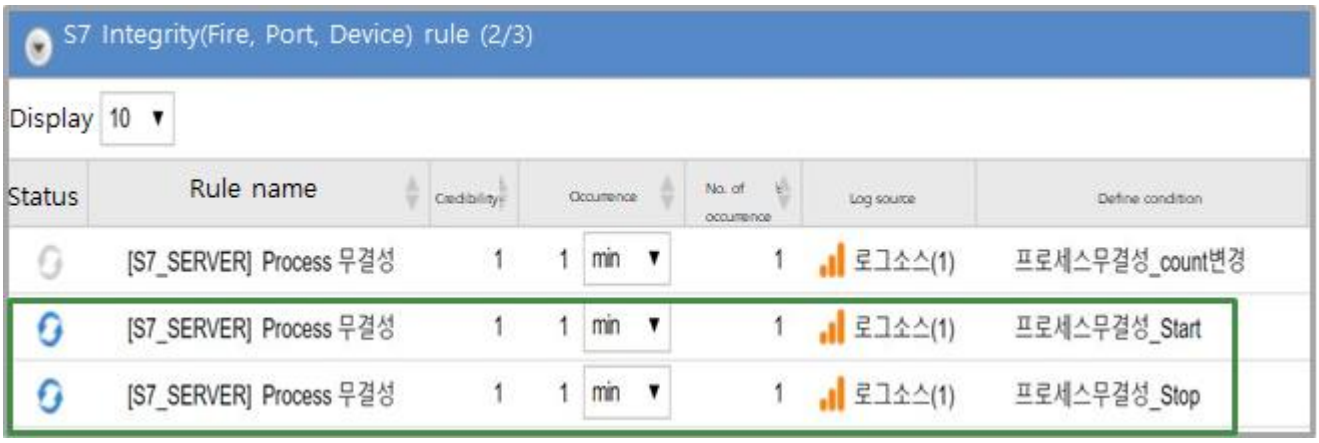
Example) How to detect a crucial Process called spcollect when it is either Down or active

Managing the Menu application order of SIEM → creating the Object shown below in the Object Management menu



[Picture 3-20] Registering process as Object

Managing the Menu application order of SIEM → creating the Object shown below in the Object Management menu



[Picture 3-21] Registering process as single alert

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

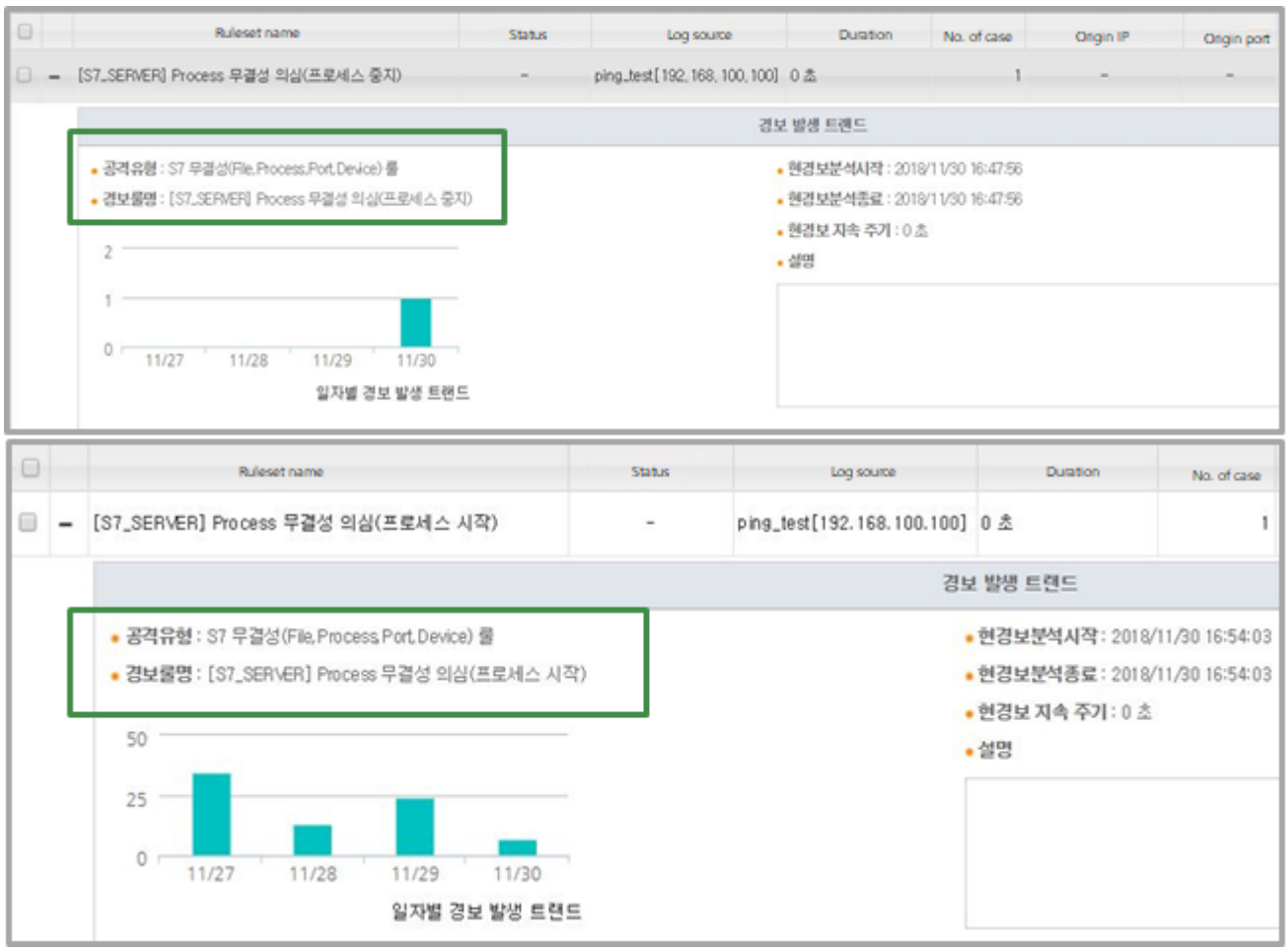
Below is an attempt at activating / deactivating the process of an actual server.

```
[root@SIEM-102 spcollect]# ./xcollect stop
killed 27933
27940
killed
[root@SIEM-102 spcollect]# ps -ef|grep spcollect | grep -v grep
[root@SIEM-102 spcollect]#
[root@SIEM-107 spcollect]# ./xcollect start
[root@SIEM-107 spcollect]# spcollect start !!

[root@SIEM-107 spcollect]# ps -ef|grep spcollect | grep -v grep
root     148847      1  0 16:54 pts/5    00:00:00 /bin/sh /SIEM/spcollect/SpcollectCheck.sh
root     148859      1 48 16:54 ?        00:00:08 /SIEM/spcollect/spcollect /SIEM/spcollect
```

[Picture 3-22] Actual activation and deactivation process of a server

We can see that the following alarm activates in the SIEM



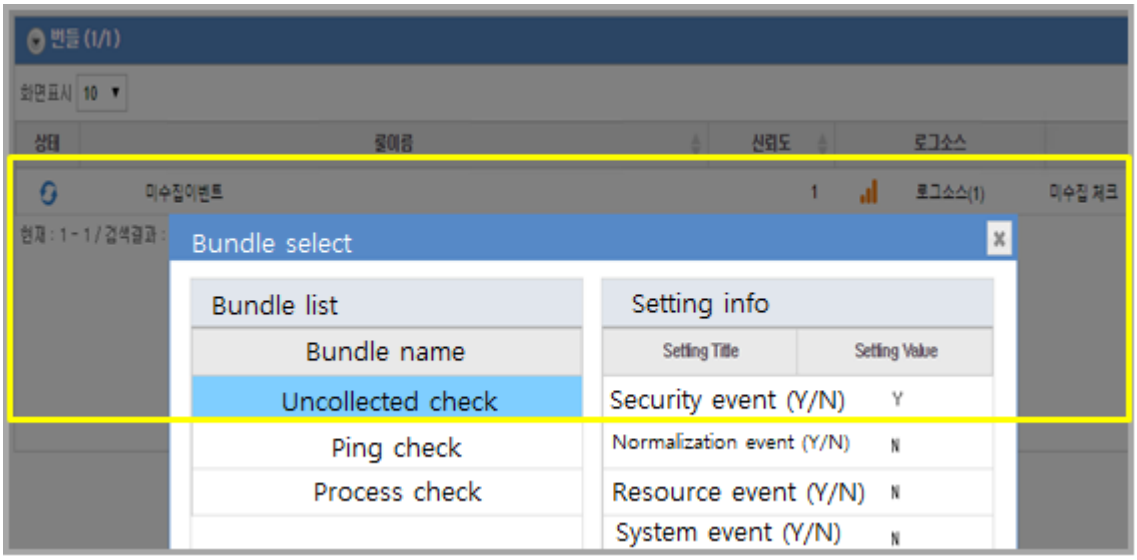
[Picture 3-23] Alerts concerning deactivation/activation of correlation analysis

If there is an impotent process as shown above, anomalies within the server can be detected by mainly applying either a deactivation related log or an activation related log and monitoring the process.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

▶ Malfunction point management through uncollected logs of devices

Managing the Menu application order of SIEM → Single alert management → Bundle Rule



[Picture 3-24] How to process uncollected events by registering bundle rules

An alert has been activated in the SIEM as shown below.

[Picture 3-25] Alert notifying user of an uncollected event

As shown above, if the main equipment do not collect logs, alerts as shown above can be used to identify the problem with the device more efficiently.

4. Conclusion

As described in the previous outline, we examined how to monitor servers and malfunctions.

In order to successfully monitor servers and server malfunctions, one must be aware in advanced of the servers' vulnerabilities and a list of the main processes.

In addition, as explained above, the server and malfunction monitoring can be carried out with more accuracy by collecting logs of management processes such as port integrity (Open.Close) and Oracle.

It is advised that each site consult with the engineers to activate such function which can be used to monitor one's major assets.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

04 Special Column

How to efficiently utilize Threat Intelligence For Security Monitoring

Service Business Department
Security Analysis Team

1. Synopsis

According to CISCO's "2018 Asia Pacific Security Competency Benchmark Report," 55% of organizations receive more than 10,000 security alerts each day. The operators in Security Operation Center(SOC) classify more than 10,000 cases of true positives and false positives on a one by one process, and then they further investigate to see if there have been any additional damage to the servers or systems. No matter how well-trained the security operators are, analyzing more than 10,000 security alarms and events every day is not an easy task.

These environmental factors have raised the issue concerning the limitations of how much 1 person can analyze and how to deal with the overwhelming amount of alerts in a more efficient way. The rise of such issues have given birth to organizations such as CTA (Cyber Threat Intelligence) for outside of Korea and C-TAS(Cyber Threats Analysis System) from KISA for the South Korean domestic scene. This kind of system shares information on attacks such as; malicious code sample, phishing, SMS phasing/smishing and other IoCs (Indicators of Compromise) can be shared. This report will deal with how intelligence is gathered and how it is utilized.

2. What is going to be shared?

Information shared in the domestic and foreign information security fields generally include IP addresses used by attackers, domain addresses and URLs used as malicious code distribution, Command and Control (C & C) servers, and malicious code HASH information. They also share Snort / YARA rules to detect these attacks and TTPs (Tactics, Techniques and Procedures) to identify attackers' actions.
We can utilize the information from the SOC for blocking and detecting attacks that may occur in the future by reflecting the information shared by the firewall, the IDS / IPS (Intrusion Detection / Blocking System), and the Advanced Persistent Threat (APT) solution. In additional security-related news, new vulnerability information and malicious code and attack tool analysis reports are shared. National cyber security related organizations and companies are trying to reduce hacking incidents by analyzing these incidents and sharing related content. The following is an example of such shared information.

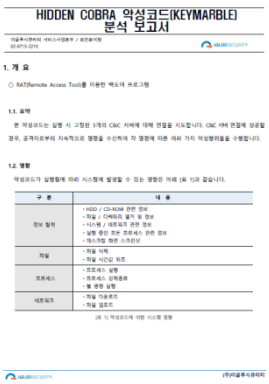
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Information Classification	Description
News clipping	Security related News
Security Notice	Ways to respond to well-known attacks and countermeasures
Security related event	Security related events
Security related column	Columns on recent issues or technologies
New Vulnerabilities and Exploits	List of newly released CVE, Exploit, PoC Code
Analysis report	Security Technology Analysis Report Malicious Code Analysis Report New Vulnerability, Exploit, and PoC Code Analysis Report Hacking Case Analysis Report
Detection policy	Snort, YARA detection policy
IoC	Black List IP, URL, HASH, etc.
Malicious Mail information	Malicious e-mail addresses, content, attachments, etc.
Security alert statistics	Statistics of attack patterns / ports

[Table 4-1] Example of security related information being shared

Such cyber security related information is shared with various channels such as a daily report, analysis report, CTI (Cyber Threat Intelligence) system etc.

Security related news, security bulletins, events, and vulnerability lists are shared in the form of daily reports such as Daily Security NEWS and the CTI is used to share information on social issues, analysis reports which report on responses or countermeasures of an attack method, large amounts of IP, HASH, URL informatin and vulnerability information.

Daily Security NEWS	Analysis Report	IGLOO CTI
		

[Table 4-2] Various ways to share information

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

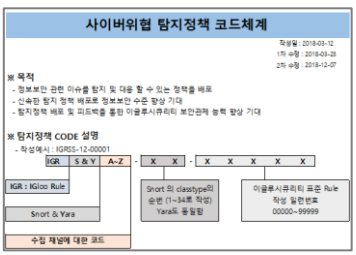
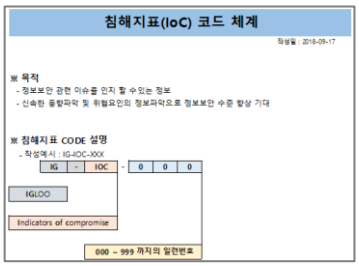
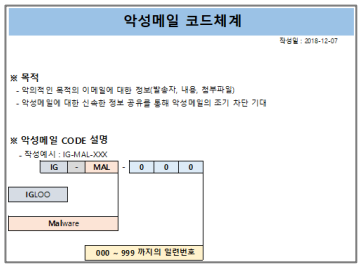
3. How will the information be collected and distributed

Cyber threat intelligence from various sources, each in their own way.

In the form of information, agency A may refer to URLs as HXXP: // instead of HTTP: // to avoid hyperlinks, and include dot (.) in square brackets [.]. Agency B distributes the malicious code HASH information to SHA256, but Agency C distributes it as MD5 or SHA1. In terms of information distribution methods, they are distributed through 'e-mail', 'SMS', 'information sharing systems' or by 'posting on the homepage'.

Collection and standardization can be troublesome for users who want to use information shared by various forms and distribution methods.

Although it is difficult to collect and standardize all information in the same form, it is helpful to apply standardized codes by dividing them into types and classification of information (detection policy, intrusion index, malicious code information, etc.) The following figure is an example of a detection policy, intrusion index, and code system of the malicious code information.

Cyber threat detection policy code system		Form : IGRSS.01.00001
IoC code system		Form : IG-IOC-001
Malicious mail code system		Form : IG-MAL-001

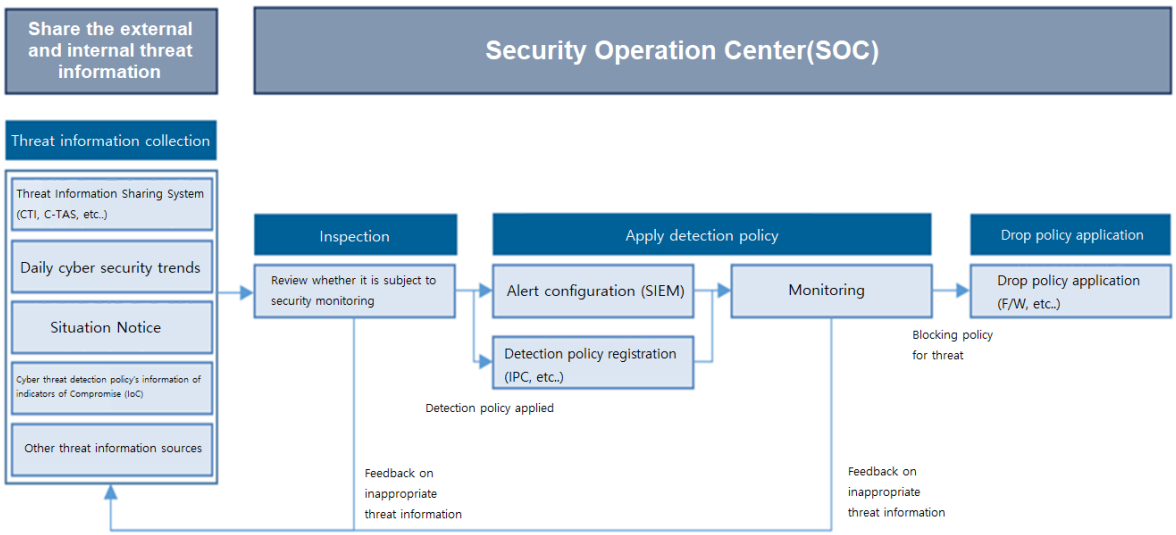
[Table 4-3] Example of cyber threat information code system

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

4. How will the collected information be utilized

It can be utilized in the SOC(Security Operation Center) as evidence when analyzing security alerts collected from internal and external threat intelligence (threat URL/IP, vulnerability information, intrusion index, detection policy, malicious code etc.) For example, a DDoS(Distributed Denial of Service) attack has been discovered and has spread from the media to other institutes. Then, the attackes IP can be registered in the drop policy so it cannot enter the internal network. In addition, an analysis of the possible infection due to the malicious code and damage can take place followed by a swift response by searching the IP or a comminucation history if the IP has been shared by the C&C.

After the threat information is shared, the following procedure is carried out. First, when threat information is collected, determine whether the information has any connections to the target of security monitoring. Even though information has been acquired from reliable OSINT (Open Source Intelligence) or government institutions, the initial analytic or information processors later on may have misinterpreted the information. Therefore, instead of trusting the information 100%, it is important to distinguish important information from unnecessary information.
Secondly, if the threat information seems to be a real threat to subject of security monitoring, appply a detection policy which can identify the attack to the threat detection system. On the SIEM (Security Information and Event Management), Set the alert to continuously monitor or search for related security alerts.
Third, if an actual threat occurs, set the firewall or APT solution to block the threat through a drop policy in order to preemptively stop the threat.
Unnecessary information should be sorted on each phase through a feedback process in order to refine the threat information.



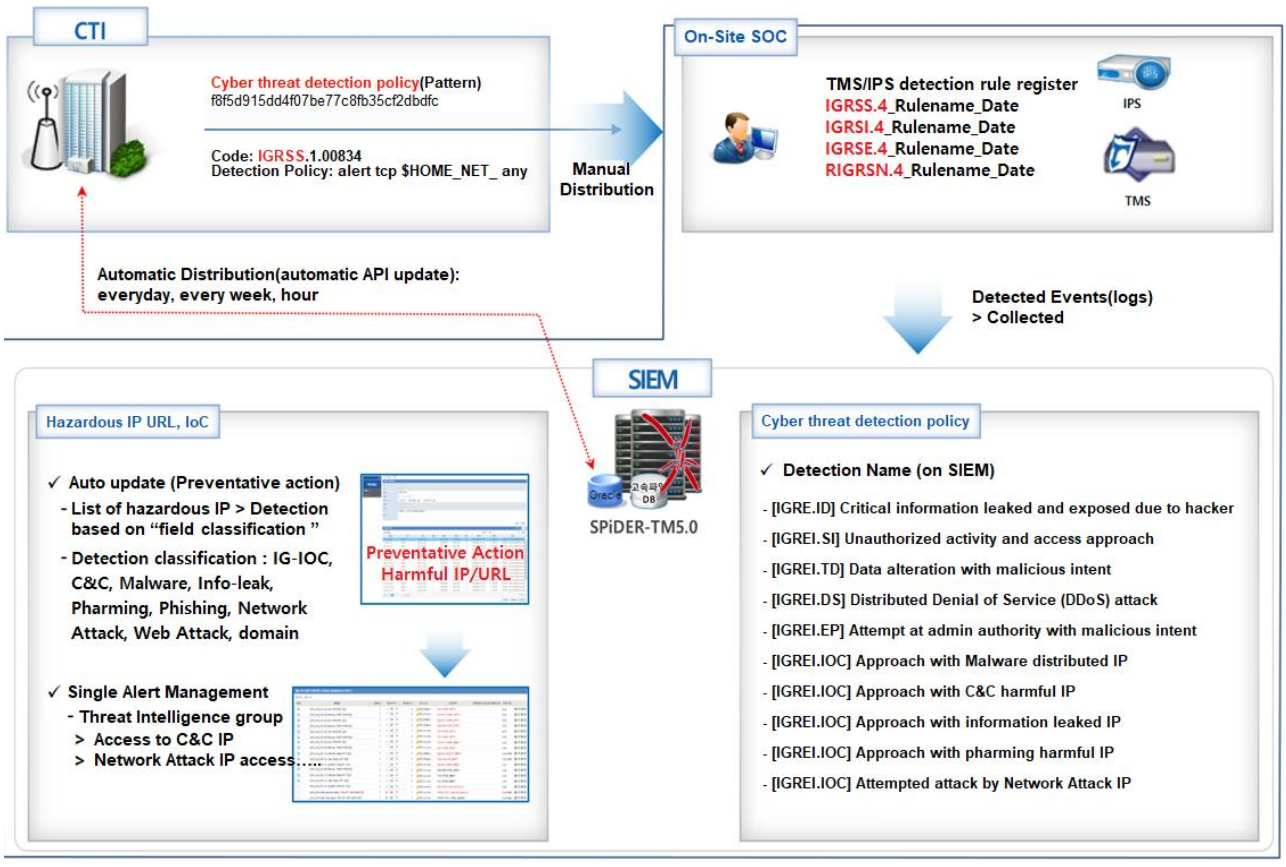
[Picture 4-1] Threat information application and processing

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

5. Example : Utilize thread intelligence using SIEM

Each organization has access to different information and also has different ways of responding to hacks. For example, if there is a case of 10 thousand alerts, as stated above, it is more efficient to utilize a SIEM, instead of a single security device (firewall, IDS/IPS, vaccine etc.) to identify all the information. The picture below shows a diagram of each SOC receiving cyber threat intelligence and applying it to IPS/TMS, then shows how the SIEM efficiently processes the events. it functions as a "conceptual diagram of the utilization of cyber threat intelligence on the SIEM."

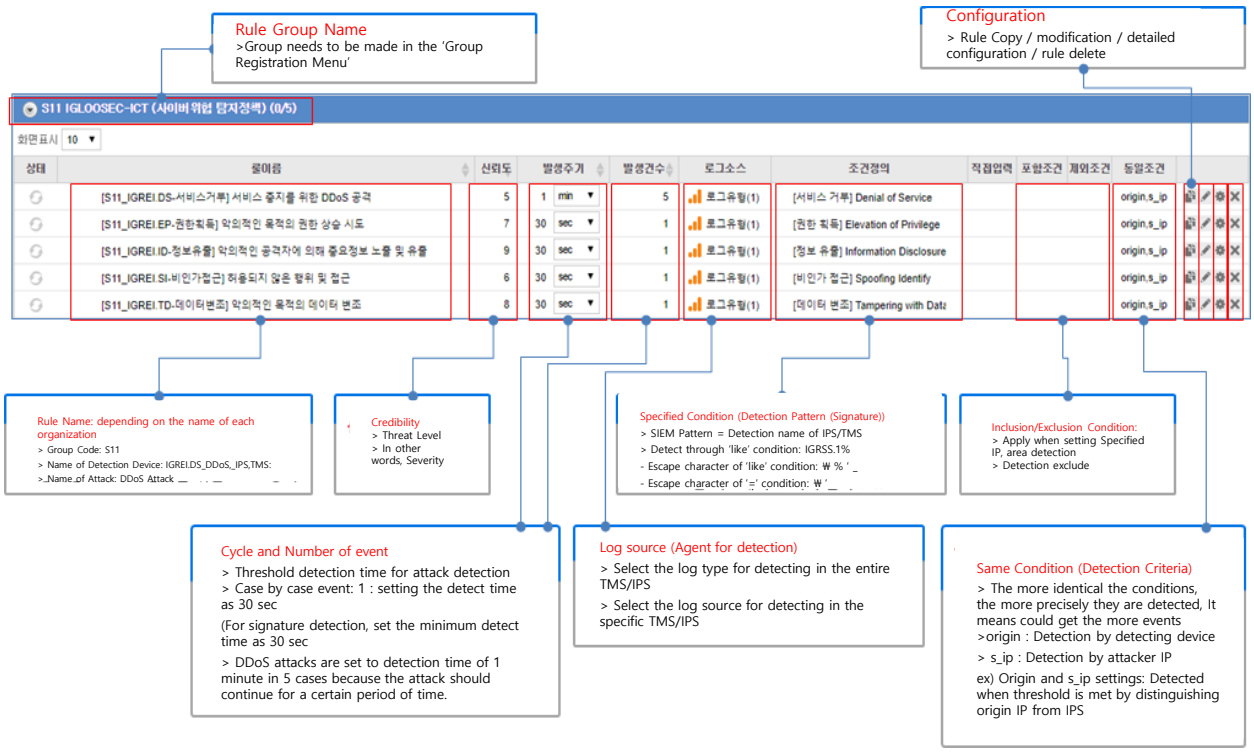
First of all, the detection policies are organized by week, day and hour through the CTI. These policies have a unique code number. Through these code numbers, operators in the SOC register an appropriate detection and drop policy on a single security device (firewall, IDS/IPS, APT solution etc.). Finally, when an alert activates on one of the detection policies or intrusion index (from the single security devices), the user can understand the situation in one eye through the SIEM.



[Picture 4-2] Conceptual Diagram of utilizing cyber threat information on the SIEM

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

In the SIEM, each cyber threat information is classified according to information, a policy is generated and alarms are generated according to the frequency of the alert. The picture below shows how it is displayed.



[Picture 4-3] Setting and utilizing threat intelligence through the SIEM

6. Conclusion

It does not matter how valuable the information is, if it cannot be analyzed and utilized properly, it is of no use. Therefore, in order to increase the value of the information, instead of having large amounts of information, it is more important to analyze the collected information and utilizing it through feedback.

The information collected from OSINT, the media, analysis reports, information sharing channels between institutes through the alerts activated in the fast network and various devices can be used to help identify new/altered malicious codes or abnormal activities and can be utilized to decrease false positives and supplement the limitations of a signature-base detection system. If a traditional signature-based detection system is used alongside an activity based detection system, the asset can be safety protected from the hacker by identifying the attackers malicious intent in advance.

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

05 Focus on IGLOO Security

IGLOO SECURITY Co., LTD, Volunteer activity in Cambodia

"We support the dreams of children in Cambodia"

- **Held the '氷庫, Bingo' pavilion completion ceremony which will provide educational opportunities for more students.**
- **Through the talent donation of the employees, the children had a chance to befriend music and art.**
- **As a leading security company, IGLOO SECURITY plans to continue volunteer activities to support the dreams of Cambodian children.**

[February 18, 2019] IGLOO SECURITY (CEO : Lee Deuk Choon, www.igloosec.co.kr) announced that they have carried out volunteer services in a Cambodian children's educational facility known as 'Our School' from the 11th to the 15th of February. This year marked the 7th anniversary of IGLOO Securities volunteer work in Our School. This year, the CEO of IGLOO Security, Lee Deuk Choon with other employees participated in the completion ceremony of the 'Bingo Building' and carried out arts and crafts classes.

Mr. Lee(The CEO of IGLOO SECURITY) and the employees held a ceremony to celebrate the opening of the Bingo Building ('氷庫, Bingo'), which will be used as a classroom and also provide offices for teachers. The Bingo hall will allow it to be possible to eliminate the difficulty of lacking the learning space and will provide customized curriculums suitable for each grade, which can accommodate students of various ages from kindergarten to elementary school.

In addition, the employees of Igloo Security began to donate talents in the field of art, which is not a common class for Cambodian children to come by. They conducted music lessons using a digital piano, made paper fans, and eco-bag paintings. Through these activities, they focused on creating opportunities for children to be acquainted with music and art and to enhance their sense of accomplishment.

On the other hand, IGLOO SECURITY conducted an in-house event called 'Igloo Lotto' for 5 weeks at the end of last year to select volunteers. Employees were asked to select five out of the 30 numbers with their own words associated with the company, such as ' Lee Deuk-Choon', and five numbers were added each week to provide employees with the most number of opportunities to visit the school. Every week they shared the lottery process and new of the selected employee, and got a warm response from our employees back home.

Under the goal of 'safeguarding the dreams of children', IGLOO SECURITY has been conducting annual overseas volunteer activities focusing on youth education support at 'Our School' located in Cambodia since 2013.

IGLOO Security CEO, Mr. Lee Deuk-Choon stated that "Education can give anyone the courage and strength to overcome any difficulty. 'Bingo' the name of the IGLOO Security Head Quarters library was named as a tribute to the collective knowledge and wisdom of the employees of IGLOO Security and since the Our School in Cambodia was also named Bingo (Building), I truly support the children and the opportunity for an education which will allow them to dream and take steps toward that dream."

Copyright © IGLOO Security, Inc. 2019. 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.