Monthly Security Report

2021
January

Cover Story

- Vulnerability assessment using Flan Scan
- AI Security monitoring process based on Management Security Methodology
- IGLOO Security's Management Security Methodology
  1) ID.AM Asset Management

IGLOOSECURITY

This report is based on the data collected through the SIEM solution at IGLOO SECURITY's Security Operation Center (SOC). IGLOO SECURITY continuously strives to achieve a 24/7 safe cyber environment throughout the year.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

1. IGLOO Threat Insight

- Summary
- Monthly security threat trend and analysis
- Detailed analysis of attack pattern
- Indicator of compromise(IOC)
- Detection policy

2. Monthly Security Issue

- Security Issue

3. Tech Note

- Vulnerability assessment using Flan Scan

4. Special Column

- AI Security monitoring process
based on Management Security Methodology

5. Focus On IGLOO

- IGLOO Security's Management Security Methodology
  1) ID.AM Asset Management

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 1

IGLOO Threat Insight

1. Summary

2. Monthly security threat trend and analysis

- 01. Monthly attack pattern
- 02. Monthly vulnerability attack TOP 10
- 03. Monthly threat IP address TOP 10

3. Detailed analysis of attack pattern

4. Indicator of compromise(IOC)

5. Detection policy

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Summary

Monthly Hot Issue

The new year of 2021 has passed after 2020, covered with the unprecedented situation of COVID-19, but the world has yet to escape the effects of COVID-19. Not only has the daily life changed, but the overall social and culture has changed. As telecommuting becomes more spreading, ICT and security technologies that support office workers' work from home, such as video conferencing solutions, online education platforms, and VPNs, are taking a new leap beyond re-examination. Various security companies including IGLOO SECURITY In the security outlook for 2021, it can be seen that the security issues of the non-face-to-face era of the COVID-19 era are being dealt with.

However, no matter how the world changes, the traditional security activities that prevent attacks in advance and respond proactively, detect and respond to attacks in a timely manner, should be carried out unchanged. We are doing our best today for the safety of our customers.

Monthly Statistics Analysis

- This month, system vulnerabilities accounted for the highest percentage of attack types.
- In order to prevent authentication bypass attempts on Tomcat admin (administrator) page authentication and system file access detection vulnerability attacks, it is recommended that only authorized users can access the main pages.
- The security administrator must periodically manage the part of applying the latest patch and checking updates to all servers that are internally managed and used.

※ Statistical data used in this report was prepared based on data collected through SIEM at IGLOO SECURITY, INC.'s Security Operation Center.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

2 Monthly security threat trend and analysis

In order to predict cyber threats, the IGLOO SECURITY's Security Operation Center collects and analyzes the monthly attack type, the number and rate of attacks by vulnerability and source IP.

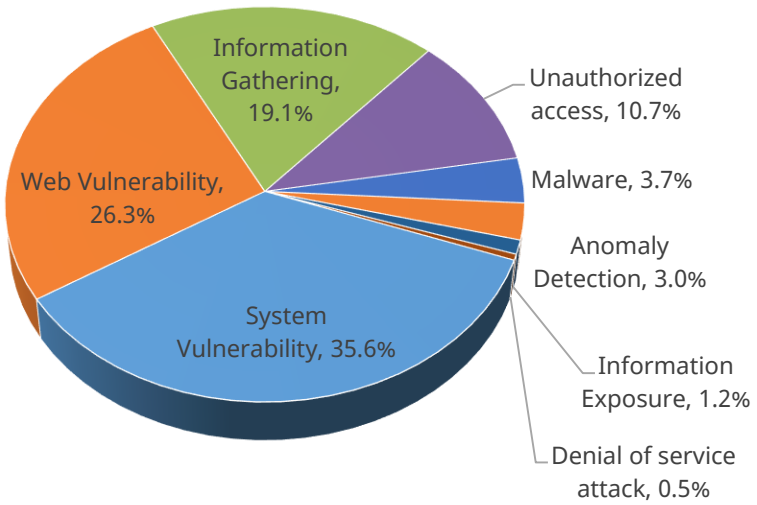
01. Monthly attack pattern

※ Based on the IGLOO Security's SOC report

Pattern	Counts	Ratio(%)	Fluctuation
System Vulnerability	3,620	35.6	-
Web Vulnerability	1,800	26.3	-
Information Gathering	1,305	19.1	-
Unauthorized access	734	10.7	▲1
Malware	253	3.7	▼1
Anomaly Detection	204	3.0	-
Information Exposure	79	1.2	-
Denial of service attack	33	0.5	-
Total	6,841	100	-

[Table1-1] Monthly Attack Patten

As a result of checking monthly attack pattern in January 2021, system vulnerability accounts for the largest percentage of monthly attack patterns, followed by web vulnerabilities and information gathering.
Compared to the previous month, unauthorized access has increased by one level, and malware has decreased by one level. This is judged to be due to the increase in the vulnerability "Tomcat admin (administrator) page authentication bypass attempt" and "system file access detection".



Copyright © IGLOO Security, Inc. 2021. All rights reserved

2 Monthly security threat trend and analysis

02. Monthly vulnerability attack TOP 10

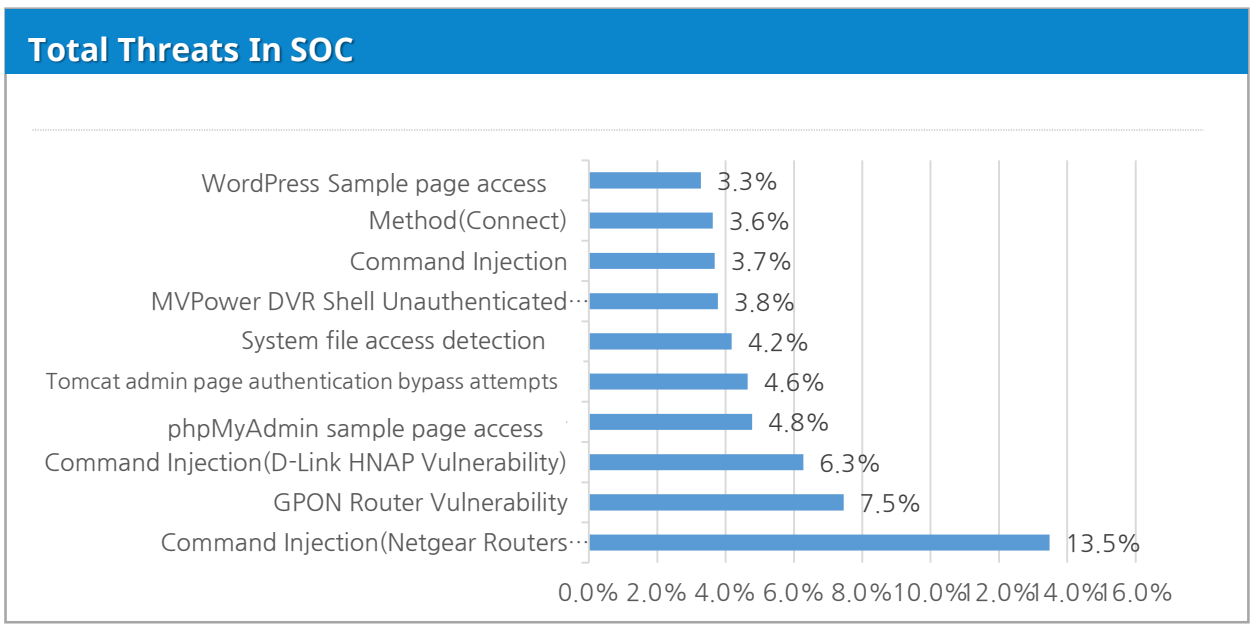
As a result of checking the top 10 monthly vulnerability attacks in January 2021, Tomcat admin (administrator) page authentication bypass attempts, system file access detection, and Method (Connect) vulnerabilities newly entered the Top 10.

In addition, MVPower DVR Shell Unauthenticated Command Execution, Command Injection rankings have risen and WordPress sample page access rankings have plummeted.

※ Based on the IGLOO Security's SOC report

Rank	Detection Name	Counts	Ratio(%)	Fluctuation
1	Command Injection (Netgear Routers Vulnerability)	922	13.5	-
2	GPON Router Vulnerability	510	7.5	-
3	Command Injection(D-Link HNAP Vulnerability)	429	6.3	-
4	phpMyAdmin sample page access	327	4.8	-
5	Tomcat admin(administrator) page authentication bypass attempts	318	4.6	NEW
6	System file access detection	286	4.2	NEW
7	MVPower DVR Shell Unauthenticated Command Execution	258	3.8	▲1
8	Command Injection	252	3.7	▲1
9	Method(Connect)	248	3.6	NEW
10	WordPress sample page access	224	3.3	▼6
	Total	3,774	55.2	-

Top 10 and percentage of vulnerability events that were detected and responded to intrusion reports by the IGLOO Security SOC.



[Table1-2] Monthly vulnerability attack TOP 10

Copyright © IGLOO Security, Inc. 2021. All rights reserved

2 Monthly security threat trend and analysis

03. Monthly threat IP address TOP 10

As of January 2021, as a result of checking the top 10 source IPs, the IP from China occupies the majority. After that, it was identified in the order of the United States, India, Russia, and Korea.
The harmfulness of the source IP is the result of checking in IGLOO_CTI, OSINT information, etc.

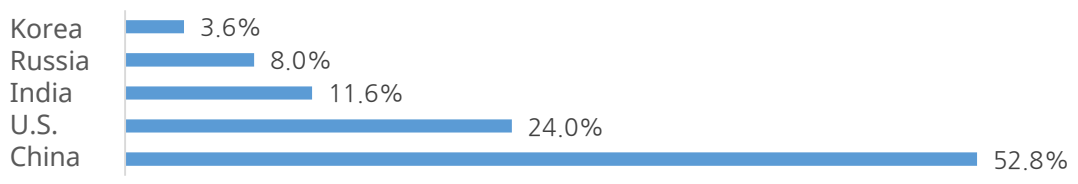
It is recommended to block the firewall or other security devices by referring to the table below.

※ Based on the IGLOO Security's SOC report

Rank	Threat IP	Country	IGLOO_CTI	Attack Information
1	91.241.19.84	RU	4/114	ThinkPHP Remote Code Execution Vulnerability
2	45.155.205.108	RU	14/114	ThinkPHP Remote Code Execution Vulnerability
3	45.146.164.15	RU	7/114	ThinkPHP Remote Code Execution Vulnerability
4	85.214.44.193	DE	8/114	Code Execution(Bash ShellShock)
5	185.234.217.183	IE	12/114	etcpasswd Detect
6	149.129.139.48	SG	8/114	ZeroShell kerbynet RCE (CVE-2009-0545)
7	209.141.50.5	US	9/114	Web Scanner(ZmEu)
8	185.234.219.28	IE	14/114	etcpasswd Detect
9	137.116.133.111	SG	10/114	ZeroShell kerbynet RCE (CVE-2009-0545)
10	208.91.198.220	US	0/114	SQL Injection

Total Countries

This month's attack IP, country ranking detailed Top 10 table and ratio



Rank	Source IP	Country	Rank	Source IP	Country
1	91.241.19.84	RU	6	149.129.139.48	SG
2	45.155.205.108	RU	7	209.141.50.5	US
3	45.146.164.15	RU	8	185.234.219.28	IE
4	85.214.44.193	DE	9	137.116.133.111	SG
5	185.234.217.183	IE	10	208.91.198.220	US

[Table1-3] Monthly source IP address TOP 10

Copyright © IGLOO Security, Inc. 2021. All rights reserved

3 Detailed analysis of attack pattern

We introduce detailed analysis results according to attack patterns, focusing on the TOP 10 of the vulnerability patterns that occurred in January.
By referring to the detailed analysis results for each detection pattern, the vulnerabilities of the system must be taken in advance.

Attack Pattern	Detailed analysis result
Command Injection (Netgear Routers Vulnerability)	A vulnerability that occurs when the web server in the NetGear DGN series router does not authenticate some URLs. You can execute arbitrary commands by using the "syscmd" function of the "setup.cgi" script.
GPON Router Vulnerability	A vulnerability found in Dasan GPON home routers. It is a vulnerability that can pass the authentication process by entering the string '?images' into the URL of the device. By exploiting this vulnerability, an unauthenticated attacker can remotely execute commands on the device and modify DNS settings.
Command Injection (D-Link HNAP Vulnerability)	Due to the vulnerability in the HNAP (Home Network Administration Protocol) related script used when installing D-Link products, it is possible to bypass authentication and execute commands such as service stop and backdoor installation. The attacker inserts a command after the Domain/HNAP1/GetDeviceSettings/ path and tries to execute it using the SOAPAction field.
phpMyAdmin sample page access	phpMyAdmin is an open source tool written in PHP for the purpose of managing MySQL on a web server. It searches for vulnerabilities in the My-SQL server, creates/deletes a database, creates/deletes a table, creates/deletes a field, executes SQL statements, and has permissions. It is an attack that can execute management functions. If this vulnerability exists, it has a vulnerability that can execute system commands by inserting an arbitrary function using the `?` argument in the script/setup.php file of phpMyAdmin.
Tomcat admin (administrator) page authentication bypass attempts	After installing Tomcat, one of WAS, access the administrator page (eg http://localhost:8080/manager, http://localhost:8080/manager/html, etc.) that can be accessed with the default path, and the default ID and PW in the authentication header. If authentication bypass is successful with an attack that accesses by Base64 encoding, it is possible to upload a web shell, obtain server shell authority, and obtain root authority through exploitation.
System file access detection	In order to acquire system information, an attacker attempts to access major system files containing configuration information such as accounts and environment variables such as /etc/passwd or *.conf /.env by using Directory Traversal vulnerability.
MVPower DVR Shell Unauthenticated Command Execution	When processing an HTTP request, validation of the user-supplied input is insufficient, so a remote attacker can execute arbitrary system commands in a query string by using the \'shell\' file in the web interface.
Command Injection	If the input value including the system command does not go through an appropriate verification procedure, the received command may be executed. If a vulnerability exists, an attacker can directly transmit commands to the system, so additional damage may occur through file browsing, downloading, and execution.
Method (Connect)	Try to access the inside through HTTP TLS (Transport Layer Security) tunneling using the Connect Method. For this, the Connect Method is used, and if there is a vulnerability, it may be used as an intermediate stop for an attack.
WordPress Sample page access	This event accesses sensitive sample pages such as wp-login.php, wp-admin.php, and wp-config.php, which are WordPress login pages, and is mainly used to check the existence of the page.

[Table 1-4] Detailed Analysis of the Top 10 Monthly Vulnerability Attacks

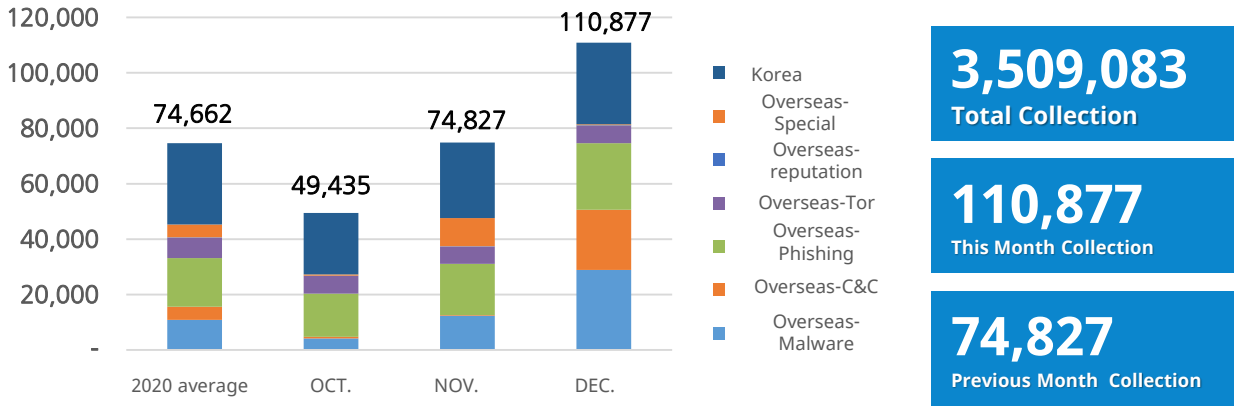
Copyright © IGLOO Security, Inc. 2021. All rights reserved

4 Indicator of compromise(IOC)

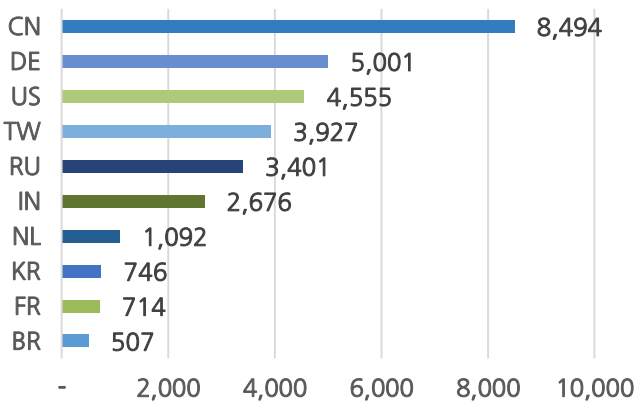
IGLOO Security continues to share security threat information collected by worldwide companies and organizations in order to prevent cyber attacks in advance and to help quickly identify attackers when an attack is detected. It selects and provides detailed information related to the customer company among the collected threat information to enable a preemptive response by detecting the context and purpose of the attack against the security threat that the customer targets the organization.

▶ Monthly threat information collection statistics

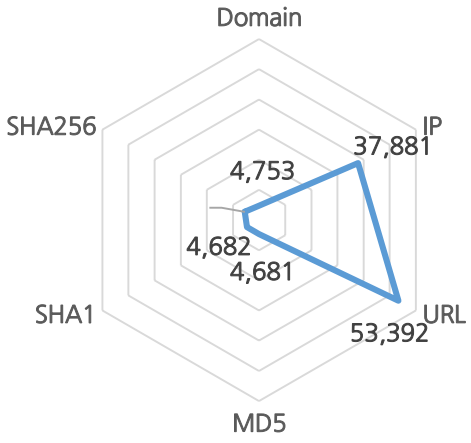
Looking at the data for one month in December 2020, it was confirmed that the collection data increased significantly in the fourth week, especially collection from OSINT data.
URL IoC has increased significantly due to the increase in phishing data.



[Figure 1-1] Counts of threat information collection in the last 3 months



[Figure 1-2] Threat IP Country Status



[Figure 1-3] Collection Status by IoC

* Detailed information is available through IGLOO CTI (Cyber Threat Intelligence).

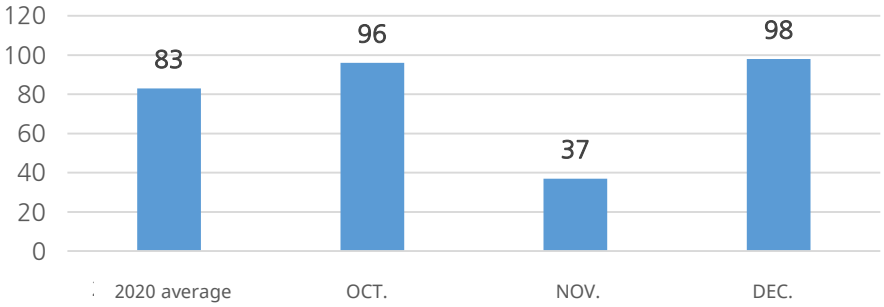
Copyright © IGLOO Security, Inc. 2021. All rights reserved

5 Detection Policy

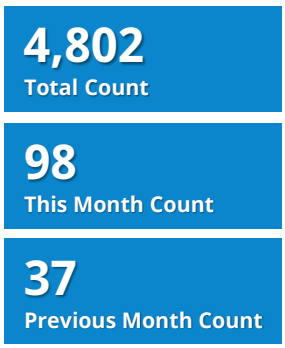
IGLOO Security continues to share cyber threat detection policies collected or self-produced by companies and institutions so that cyber attacks can be quickly identified. The cyber threat detection policy is provided in the form of a Snort Rule so that cyber attacks can be efficiently detected and responded to, and quickly applied to the security operation center, and the security of the organization is kept up to date by applying it to the security device with the provided detection pattern.

▶ Monthly Cyber Threat Detection Policy Statistics

In December 2020, 98 cyber threat detection policies were shared during the month. During the month of December, the Fireeye Red Team Tool, Solarwinds hacking incident detection policy, Apache Struts (CVE-2020-17530), and MS Windows SMB (CVE-2020-17096) vulnerabilities were released.



[Figure 1-4] Counts in the last 3 months



[Figure 1-5] Monthly Counts

Code	Detection Policy	Description	Tag
IGRSI.20.04732	alert tcp any $HTTP_PORTS -> any any (msg:"IGRSI.20.04732 Fireeye, Red team tool, HTTP.BEACON, Large Scale Information Leak"; flow:to_server,established; content:"HTTP/1."; depth:7; content:"Connection: close"; content:"Content-Type: application/json\; charset=utf-8"; content:"Content-Security-Policy: upgrade-insecure-requests"; content:"Strict-Transport-Security: max-age=10890000"; content:"Cache-Control: public, immutable, max-age=315360000"; content:"Accept-Ranges: bytes"; content:"X-Cache: HIT, HIT"; content:"X-Timer: S1593010188.776402,VS0,VE1"; content:"Vary: X-AbVariant, X-AltUrl, Accept-Encoding"; sid:2004732;)	Fireeye Red Team Tool leak-related HTTP.BEACON detection policy	Fireeye, Red team tool, HTTP.BEACON
IGRSI.20.04765	alert tcp $HOME_NET any -> any any (msg:"IGRSI.20.04765 Fireeye, Solarwinds, MSIL.SUNBURST, Large Scale Information Leak"; flow:to_server,established; content:"T "; offset:2; depth:3; content:"/swip/Events HTTP/1"; within:100; content:"Host: "; content:!".solarwinds.com"; within:100; sid:2004765;)	MSIL.SUNBURST detection policy related to Fireeye Solarwinds attack	Fireeye, Solarwinds, MSIL.SUNBURST
IGRSS.2.04818	alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.04818 Apache Struts, CVE-2020-17530, Attempted User Privilege Gain"; flow:to_server,established; content:"${"; http_uri; content:"java.lang.ProcessBuilder"; distance:0; nocase; http_uri; sid:204818;)	A policy that detects attempts to steal user authority that exploit the vulnerability of Apache Struts CVE-2020-17530	Apache Struts, CVE-2020-17530

[Table 1-5] Monthly Major Cyber Threat Detection Policies

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 2

Monthly Security Issue

1. Security issue

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Security Issue

Ransomware advisory utilizing various social issues

- Ahead of the year-end and New Year holidays, cyber threats that induce ransomware infection using various social issues are expected to increase.
- The attacker disguises as an acquaintance who sends a card or a New Year's card to induce clicking on an unknown URL included in the e-mail, or impersonating a public institution to induce the execution of malicious attachments such as 'Notice on changes to the year-end settlement'.
- The following are suggested as major countermeasures to prevent ransomware damage.
- ▲ Use the latest software (SW) and apply security updates
- ▲ Beware of clicking emails and URL links with unclear sources
- ▲ Beware of downloading files from file sharing sites, etc.
- ▲ Back up important data regularly

FireEye, a global cybersecurity company, suffers from cyber attacks

- FireEye Chief Executive Officer Kevin Mandia said in a blog on the 8th that a hacker had stolen the evaluation tools of its Mandiant Red team.
- FireEye Mandiant Red Team is an organization that performs mock hacking to evaluate corporate security capabilities, and is performing mock hacking to diagnose the security level of customers. In other words, a hacker steals the hacking tools possessed by FireEye.
- FireEye did not mention the process of stealing hacking tools, but revealed that none of the stolen tools were related to an unknown "zero-day" vulnerability.
- FireEye said it is difficult to predict whether hackers will exploit the hacking tools they have stolen in the future or will disclose them to the outside world.
- It is presumed that a hacking group sponsored by a specific country was behind the attack, given that a very sophisticated cyber attack was carried out.
- FireEye is investigating the incident in cooperation with the U.S. Federal Bureau of Investigation (FBI) and Microsoft, and said that no cases of exploiting the Red Team's mock hacking tool were found.

Warning on distribution of malicious code using YouTube video

- A YouTube video that induces the installation of malicious code by pretending to be a video explaining the illegal installation of a commercial composition program (Download Crack for Ableton Live Suite for FREE) was found.
- According to AhnLab, the attacker enticed the user to execute the URL by entering the crack download URL and file password in the detailed description of the video.
- When a user accesses the download URL, a compressed file (.zip) containing an executable file (.exe) is downloaded. After that, if you open the executable file after decompressing it by entering the password written in the detailed description of the video, the malicious code is installed.
- Security experts say that attackers are using new methods, such as YouTube videos, to distribute malicious codes, and recommend that they use genuine software and refrain from subscribing to such videos.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Security Issue

Dark web market rapidly grows with the spread of COVID-19

- Research has shown that the popularity of remote desktop protocol (RDP) access authority, payment card information, and DDoS proxy attack services among cybercriminals is rapidly increasing in recent years.
- Flashpoint revealed that with the spread of COVID-19 worldwide, the dark web market is currently enjoying the best heyday of all time.
- First, in 2019, the price of payment card data (card number used for online transactions, expiration date, etc.), which had been priced at an average of $14, rose to about $20.
- In addition, access rights to Microsoft's Remote Desktop Protocol (RDP) were also trading at a higher price than before. This is because if the RDP attack, which is widely used for remote system access, management, and server update, is successful, it can periodically enter and exit the system.
- DDoS proxy attack services have also been on a steady rise. As of 2020, attacks lasting 10 minutes are at $45, and attacks lasting for 4 hours are at $55.
- . It is interpreted that cyber attackers are adopting a segmented subscription-type business model to secure more stable profits.

Warning of malicious attacks targeting telecommuters

- Amid the increasing number of companies and institutions that introduce telecommuting due to COVID-19, it is predicted that cyber attacks aimed at home networks will continue.
- Through the '2021 Cyber Security Forecast Report', Trend Micro selected the following as the major security threats in 2021.
- ▲ Home network threat ▲ COVID-related themes are popular ▲ Reduction of visibility to members of the organization ▲Private data threat ▲N-day vulnerability market activation ▲ Increasing threats through API ▲Remote program threat
- In particular, They stressed that the threat of home network security will increase significantly. It is an analysis that cybercriminals will not directly attack companies and institutions with security policies applied, but will attack by way of personal devices with weak security.
- In addition, They cautioned against cloud security vulnerabilities that arise from transitioning from existing on-premises to public and hybrid clouds. Trend Micro analyzed that there will be cases in which compliance and policies that existed on-premises cannot be applied to the cloud as the digital transformation proceeds rapidly without sufficient preparation.

DDoS attacks aimed at the automobile industry, Ransomware DDoS attacks threatening to do DDoS attacks increase

- In conjunction with the spread of COVID-19, DDoS attacks targeting the automotive industry appear to have surged.
- Imperva released a report that analyzed the changes in DDoS attacks from September last year to March this year and from March this year to 6 months. According to the report (DDoS Attacks in the Time of COVID-19), among the detected DDoS attacks, attacks targeting the automotive industry increased by 108%.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

1 Security Issue

What are the 2021 technology keywords that Amazon CTOs pay attention to? – Edge, machine learning, quantum computing

- Burner Vogels, Amazon.com Vice President and Chief Technology Officer (CTO), at the AWS Annual Conference, introduces technology keywords that the technology industry should focus on in 2021:

1) Edge

✓ The phenomenon of the cloud going beyond the data center and entering the end devices (edges) of the field where actual applications are used will accelerate.

✓ As the cloud expands from a centralized location to the environment where we live and work every day, ultra-low-latency computing experiences are expected to become commonplace in many aspects of life, such as healthcare, transportation, entertainment, and manufacturing.

2) Machine Learning

✓ Through advances in software and semiconductors, machine learning will work anywhere on the edge devices.

✓ Disaster management, manufacturing, and agriculture are the areas where machine learning running at the edge will be actively used. It is expected to be able to detect and intelligently manage current anomalies in real time.

3) Quantum Computing

✓ 2021 will be the first year of quantum computing, and 10 years later, fields that have made innovations with quantum computing will appear.

The United States overturned by the worst supply chain attack ever

- A large-scale cyber attack has been carried out against the US government computer network. Following the Ministry of Finance, the State Department, the Department of Homeland Security, and the National Institute of Health, the Ministry of Energy and the National Nuclear Security Office (NNSA), which are in charge of nuclear weapons, are also known to have been hacked.
- According to the Cyber Security and Infrastructure Security Administration (CISA) under the US Department of Homeland Security (DHS), this attack is believed to be the starting point of a supply chain attack against SolarWinds, a network management software (SW) company. The malware 'SUNBUST', a malware that functions as a backdoor, was installed on the SolarWinds server that performs SW update, and the malware was released in the process of updating 18,000 companies and institutions using SolarWinds solutions. That it was circulated.
- The USCISA issued emergency security instructions to all federal agencies on the 13th to immediately shut down SolarWinds operations, and ordered all computers running SolarWinds to be immediately disabled.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 3

Tech Note

1. Tech Note
   : Vulnerability assessment using Flan Scan

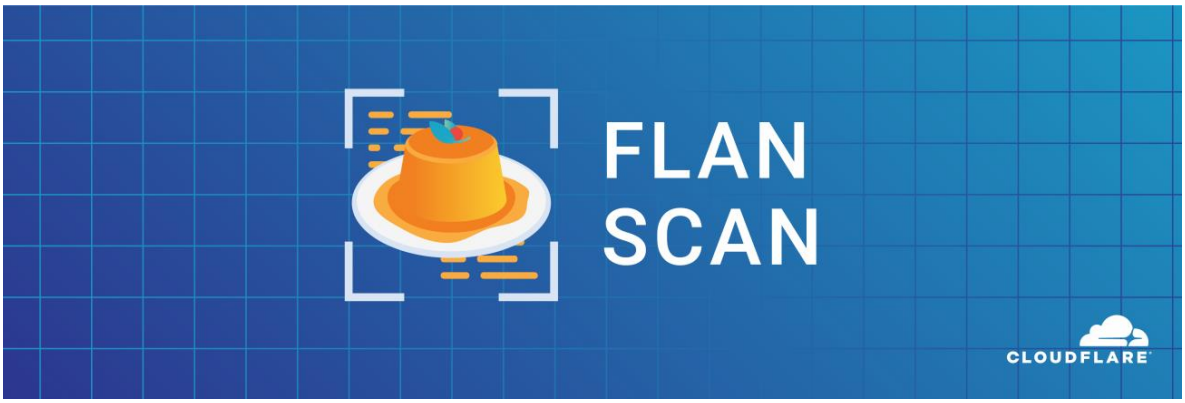
Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Vulnerability assessment using Flan Scan

Government Resource Operation Department
Gwangju Metropolitan City Team

01. Overview

Flan Scan was developed based on the Nmap open source tool from Cloudflare, and is a network vulnerability scanner that detects all services existing in the network and finds vulnerabilities against the CVE database.



Flan Scan has added three features to make it easier to deploy across the entire network and print actionable and valuable results.

Function	Description
Easy to deploy and configure	Configure Flan Scan to run inside a Docker container to make a lightweight scanner with easy configuration.
Save in Cloud	Flan Scan results can be stored in Google Cloud storage or in an S3 bucket.
Report creation	Creates a report that allows you to quickly identify the IP address and port on which the service was found.

[Table 3-1] 3 functions of Flan Scan

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Vulnerability assessment using Flan Scan

02. Docker installation

There are various ways to install Docker, but this article introduces how to install on Kali Linux, and since there is no Docker Repository officially provided for Kali Linux, add and install the Kali Linux-based debian repository.

Docker can be changed depending on the Kali Linux version, so please refer to the site below.

<Installation reference path: https://docs.docker.com/engine/install/debian/>

1) apt package update

```
$ sudo apt-get update
```

2) dependent packages install

```
$ sudo apt-get install apt-transport-https
$ sudo apt-get install ca-certificates
$ sudo apt-get install curl
$ sudo apt-get install gnupg-agent
$ sudo apt-get install software-properties-common
```

Package	Description
apt-transport-https	APT transport via HTTP secure protocol Install to allow use of accessible repositories
ca-certificates	Package for certificate verification
curl	Package requesting URL through command
gnupg-agent	GNU Privacy Guard-Encryption Package
Softwa re-pro perties-common	Provides abstraction of used apt repository and easily manages distribution and independent software sources

[Table 3-2]] docker dependent package install

3) Docker official GPG key add

```
$ curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -
```

Use the curl command to access the web URL (https://download.docker.com/linux/debian/gpg) and install the official key to use for encryption.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Vulnerability assessment using Flan Scan

4) Docker key verification

```
$ sudo apt-key fingerprint 0EBFCD88
```

After adding the GPG key, the verification is completed by comparing the last 8 characters of the key below to see if the key exists.

```
root@kali:~/Tools/flan-master# apt-key fingerprint 0EBFCD88
pub   rsa4096 2017-02-22 [SCEA]
      9DC8 5822 9FC7 DD38 854A  E2D8 8D81 803C 0EBF CD88
uid           [ unknown] Docker Release (CE deb) <docker@docker.com>
sub   rsa4096 2017-02-22 [S]
```

Check

[Figure 3-1] Docker Key check

5) Add Repository

```
$ sudo add-apt-repository "deb [arch=amd64]
  https://download.docker.com/linux/debian $(lsb_release -cs) stable"
```

Since there is no docker Repository officially provided for Kali-Linux, add a repository that operates based on debian to the list.

6) Docker engine install

```
$ sudo apt-get update
$ sudo apt-get install docker-ce docker-ce-cli containerd.io
```

After installing Repository, execute update to get the list of Repository packages.
After getting the package list, install the engine that can run docker.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Vulnerability assessment using Flan Scan

7) Check Docker operation

```
$ sudo docker run hello-world
```

```
root@kali:~/Tools/flan-master# docker run hello-world

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/
```

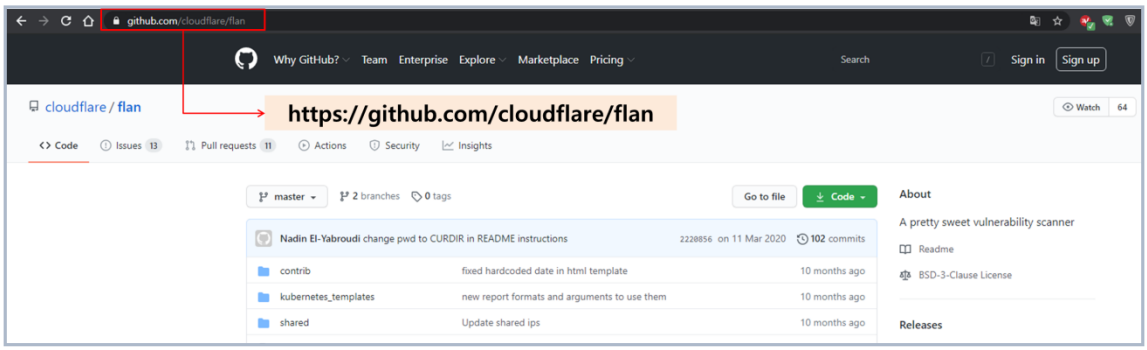
[Figure 3-2] Docker operation check result

03. Flan Scan install

To install Flan Scan, connect to Flan Scan Git Hub Repository and download Clone.
<Installation reference path: https://github.com/cloudflare/flan>

From now on, let's look at the process from downloading Flan Scan to scanning for vulnerabilities after installation.

1) Flan Scan Git Hub Repository access

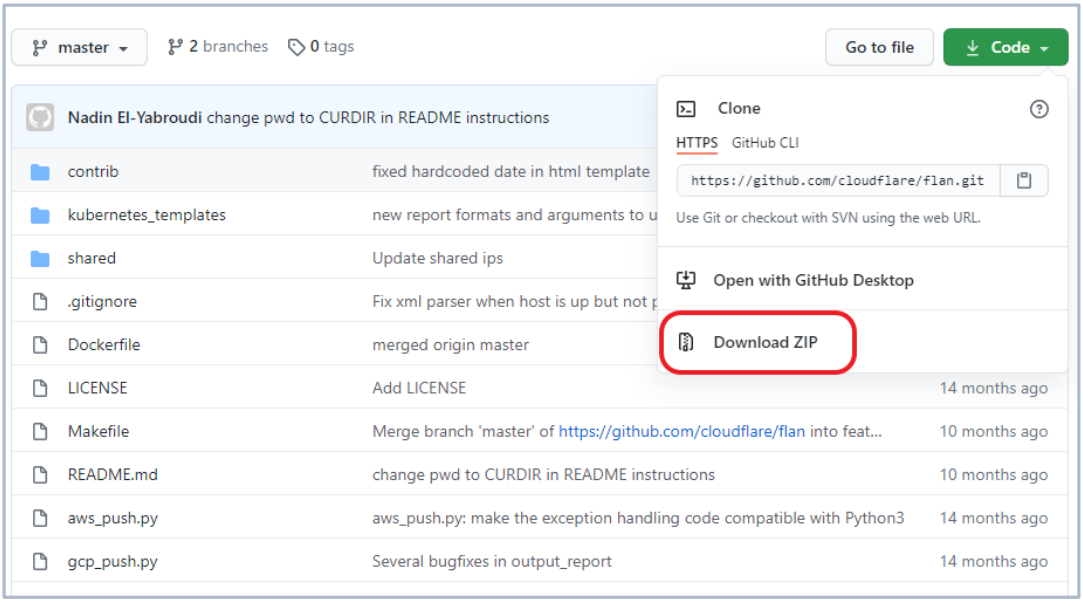


[Figure 3-3] Flan Scan installation web address access

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Vulnerability assessment using Flan Scan

2) Clone download



[Figure 3-4] Clone download screen

3) Flan Scan installation

Flan Scan is downloaded as flan-master.zip file, and after extracting it, you can compile the downloaded Flan Scan using the make build command.

```
root@kali:~/Tools/flan-master# make build
docker build -t flan_scan .
Sending build context to Docker daemon  923.6kB
Step 1/11 : FROM python:3.5-alpine
 ---> 8a92e2ac192e
Step 2/11 : RUN apk add --no-cache nmap nmap-scripts git
 ---> Using cache
 ---> 815a9fd68952
Step 3/11 : COPY requirements.txt /
 ---> Using cache
 ---> cdb217d49f17
Step 4/11 : RUN pip install --no-cache-dir -r requirements.txt
 ---> Using cache
 ---> e3050b014d8b
Step 5/11 : RUN git clone https://github.com/vulnersCom/nmap-vulners /usr/share/nmap/scripts/vulners && nmap --script-updatedb
 ---> Using cache
 ---> 248b452f8b4d
Step 6/11 : RUN mkdir /shared
 ---> Using cache
 ---> c61831ffafae
Step 7/11 : COPY run.sh output_report.py gcp_push.py aws_push.py /
 ---> Using cache
 ---> dd727615e45f
Step 8/11 : COPY contrib /contrib
 ---> Using cache
 ---> 8e9433267f37
Step 9/11 : COPY shared /shared
 ---> 039f7d61173f
Removing intermediate container 4a073a42402d
Step 10/11 : RUN chmod +x /run.sh
 ---> Running in 97954c95e2fc
 ---> 6ee27edf4016
Removing intermediate container 97954c95e2fc
Step 11/11 : ENTRYPOINT /run.sh
 ---> Running in 346fd3fdf27a
 ---> ea396547417b
Removing intermediate container 346fd3fdf27a
Successfully built ea396547417b
Successfully tagged flan_scan:latest
```

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Vulnerability assessment using Flan Scan

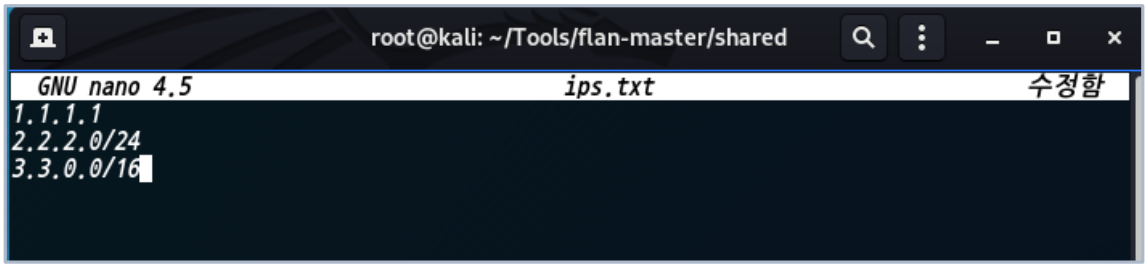
You can set the inspection target by modifying my ips.txt file in the shared directory of flan-master.

```
root@kali:~/Tools/flan-master#
root@kali:~/Tools/flan-master# cd shared/
root@kali:~/Tools/flan-master/shared#
root@kali:~/Tools/flan-master/shared# ls -al
합계 20
drwxr-xr-x 4 root root 4096  1월  6 14:29 .
drwxr-xr-x 5 root root 4096  3월 11  2020 ..
-rw-r--r-- 1 root root   14  1월  6 14:29 ips.txt
drwxr-xr-x 2 root root 4096  1월  6 14:30 reports
drwxr-xr-x 9 root root 4096  1월  6 14:30 xml_files
root@kali:~/Tools/flan-master/shared#
```

[Figure 3-6] Check shared directory after installing Flan Scan

4) Assessment targeting

Flan Scan can be set based on Host or Subnet because it follows CIDR format when designating the IP to be occupied.

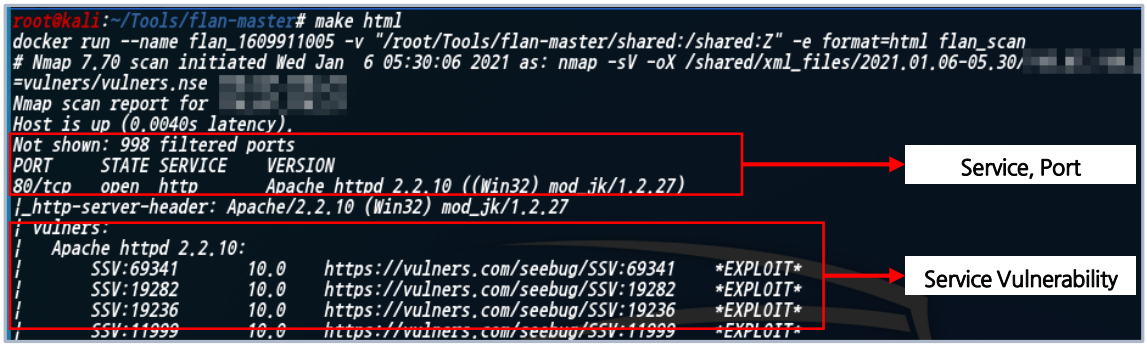


[Figure 3-7] IP setting screen

5) Vulnerability Check

By executing the make html command, you can check for vulnerabilities in the target of the ips.txt file.

If you check the results of the check, you can check the services used and whether the services are vulnerable on the screen.



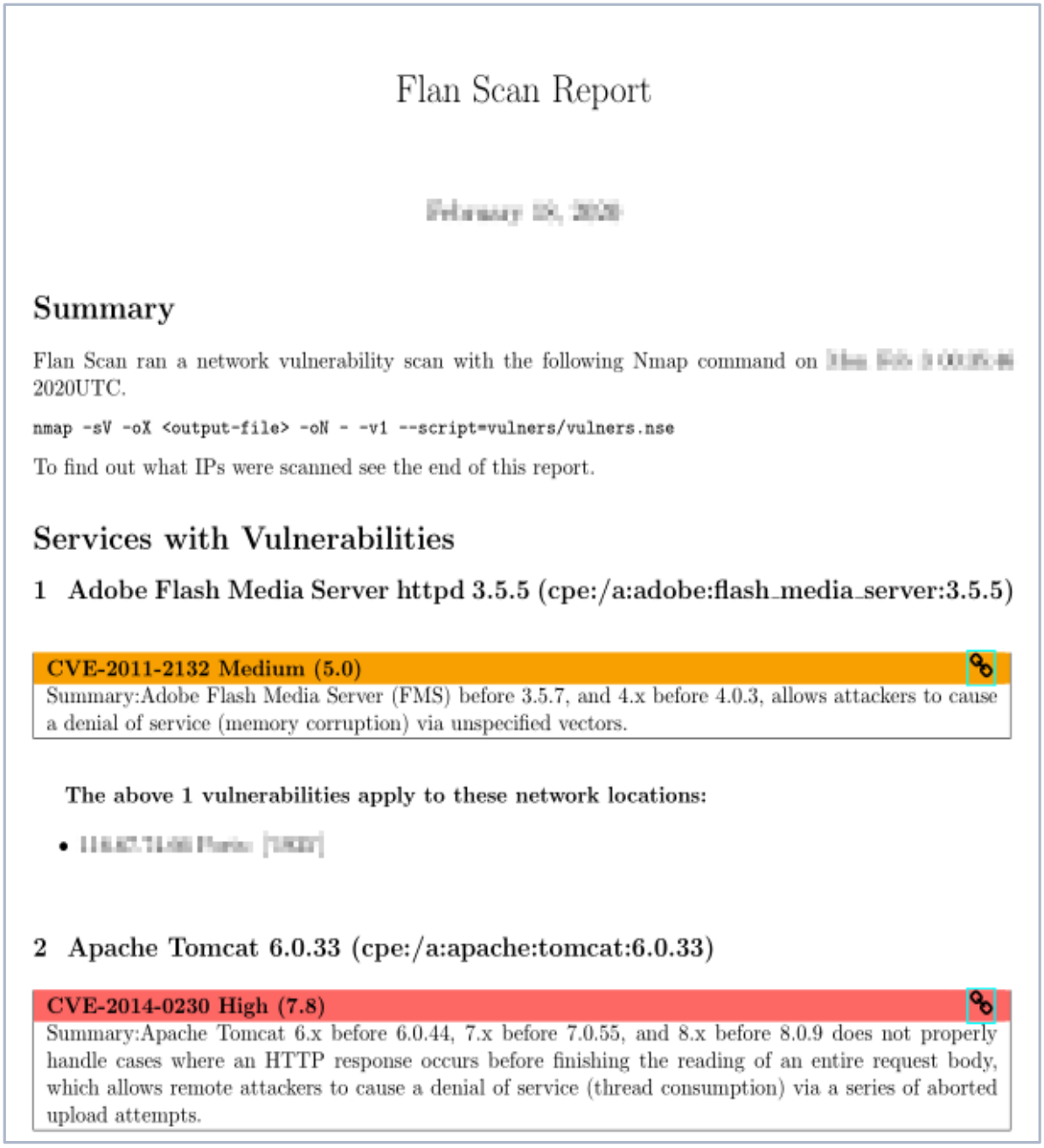
[Figure 3-8] Vulnerability check result screen

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Vulnerability assessment using Flan Scan

6) Report file

The Flan Scan check result can be output as a latex file or html, and as the result content, whether or not the vulnerability of the externally opened service and the vulnerability does not exist, the type of externally opened service can be checked.



Flan Scan Report

[redacted]

Summary

Flan Scan ran a network vulnerability scan with the following Nmap command on [redacted] 2020UTC.

```
nmap -sV -oX <output-file> -oN - -v1 --script=vulners/vulners.nse
```

To find out what IPs were scanned see the end of this report.

Services with Vulnerabilities

1 Adobe Flash Media Server httpd 3.5.5 (cpe:/a:adobe:flash_media_server:3.5.5)

CVE-2011-2132 Medium (5.0)

Summary:Adobe Flash Media Server (FMS) before 3.5.7, and 4.x before 4.0.3, allows attackers to cause a denial of service (memory corruption) via unspecified vectors.

The above 1 vulnerabilities apply to these network locations:

- [redacted]

2 Apache Tomcat 6.0.33 (cpe:/a:apache:tomcat:6.0.33)

CVE-2014-0230 High (7.8)

Summary:Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle cases where an HTTP response occurs before finishing the reading of an entire request body, which allows remote attackers to cause a denial of service (thread consumption) via a series of aborted upload attempts.

[Figure 3-9] Screen for checking whether the service is vulnerable

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Vulnerability assessment using Flan Scan

Services With No Known Vulnerabilities

1 rtsp

- [redacted]

2 smtp

- [redacted] Ports: ['25']
- [redacted] Ports: ['25']
- [redacted] Ports: ['25']
- [redacted] Ports: ['25']

3 Apache httpd (cpe:/a:apache:http_server)

- [redacted]8 Ports: ['80', '443']
- [redacted]9 Ports: ['80', '443']
- [redacted]0 Ports: ['80', '443']
- [redacted]8 Ports: ['80', '443']
- [redacted]3 Ports: ['80', '443']
- [redacted]7 Ports: ['80', '443']
- [redacted] Ports: ['80', '443']
- [redacted] Ports: ['80', '81', '443']
- [redacted]9 Ports: ['80', '443']
- [redacted]5 Ports: ['80', '443']
- [redacted] Ports: ['80', '81', '443']
- [redacted]5 Ports: ['80', '443']
- [redacted] Ports: ['80', '443']
- [redacted] Ports: ['80', '443']
- [redacted]5 Ports: ['80', '443']
- [redacted]4 Ports: ['80', '443']
- [redacted] Ports: ['80', '443']
- [redacted]1 Ports: ['80', '443']
- [redacted] Ports: ['80', '443']
- [redacted]7 Ports: ['80', '443']
- [redacted]5 Ports: ['80', '443']
- [redacted]2 Ports: ['80', '443']
- [redacted] Ports: ['80', '81', '443']

[Figure 3-10] Screen of service type opened to the outside

Copyright © IGLOO Security, Inc. 2021. All rights reserved

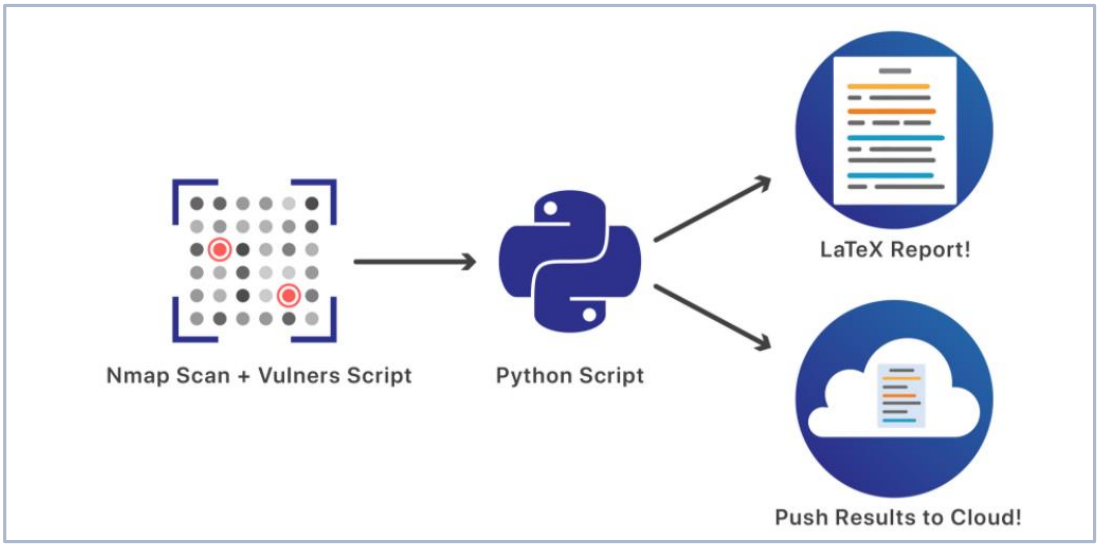
1 Vulnerability assessment using Flan Scan

04. Flan Scan operation method

The first process of Flan Scan is ICMP Ping Scan and SYN Scan, scans the IP address opened to the outside and the open port of the IP address, and then detects services running on the open port.

Flan Scan adds a "vulners" script tag to the default Nmap command to include in the output a list of vulnerabilities applicable to the detected service. Vulnerability scripts work by calling APIs to services operated by vulners.com and returning known vulnerabilities for those services.

The second process uses Python Script to convert the structured XML of the Nmap output into an executable report, and the Flan Scan results are service-centric, with all vulnerable List services.



[Figure 3-11] Flan Scan operation method

05. Conclusion

Flan Scan can be thought of as a very easy and simple inspection tool that can check the vulnerability of information system. Since it is a tool that checks the target system from the outside, if the service port is blocked by a firewall, it is not possible to check whether it is vulnerable. Therefore, if you check from the outside, you must open all ports for the check system IP in the firewall for check.

Since the internal system's vulnerability and all the services in use can be checked in the form of a report, it can be used to remove the vulnerability, and the information system administrator can remove unnecessary services used in the system.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 4

Special Column

AI security monitoring process based on Security Monitoring Methodology

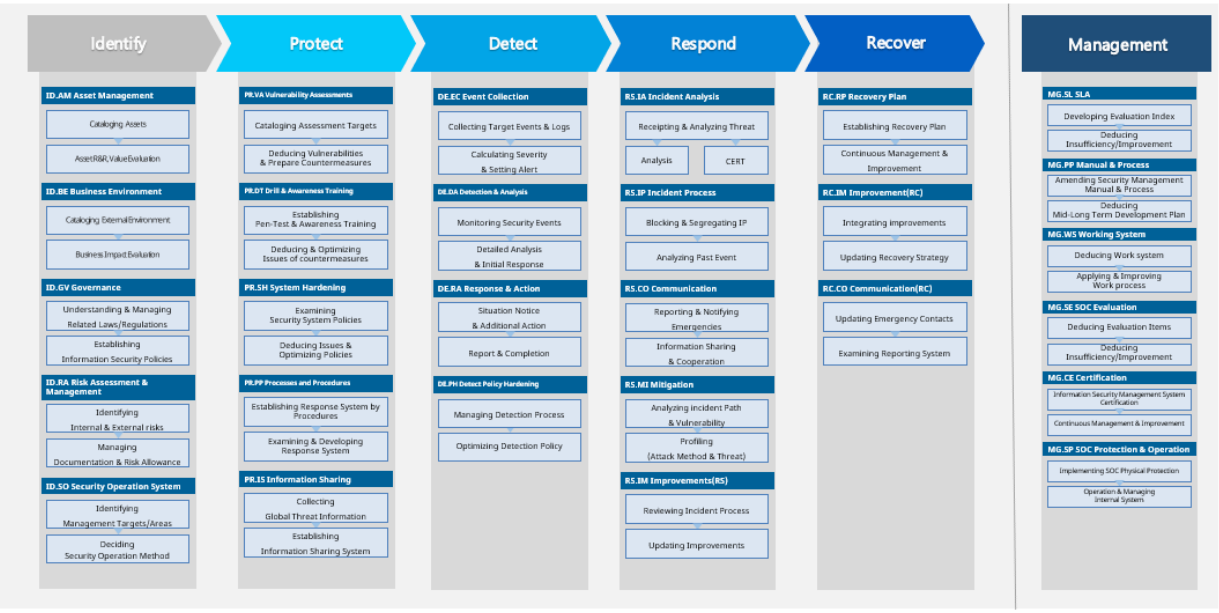
Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on **Management Security Methodology**

Strategic Business Department
Strategic Planning Team

01. Overview

If you look at the overview of IGLOO SECURITY Management Security Methodology (IGMSM), "IGLOO SECURITY's management security methodology is how to operate a security operation center (SOC) based on many years of know-how of security monitoring/operation. The process is defined as 6 functions, 28 sub-activities, and procedures and documents". Each operation site performs security monitoring/operation business through the methodology and procedure optimized for that site, but if it is our site, we refer to our management security methodology as a standard.[1]



[Figure 4-1] IGLOO Security Management Security Methodology (Resource : IGMSM)

The six functions of Identify-Protect-Detect-Respond-Recover-Management expressed in the management security methodology consist of the contents that define the tasks performed by the security operation center (SOC, cyber safety center, etc.). Among these functions, the part that occupies the majority of the duties of security operation/monitoring experts (hereinafter referred to as security monitoring officer) in general security operation centers where the big data-based security operation/monitoring system (hereinafter referred to as SIEM) is introduced is the 'Detect' function.

In general, security officer come to work, take over with shift workers, sit down to review today's security issues, and then check the SIEM for new alerts almost every hour of the day. When an alert occurs, it analyzes the positive/false detection of the alert, and processes and responds according to the result.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on Management Security Methodology

However, if we introduce an artificial intelligence-based security operation/monitoring system (hereinafter referred to as AI security operation/monitoring system) in our peaceful security operation center, can we use the existing security operation/monitoring process as it is? Should the main security operation system be an artificial intelligence security operation/monitoring system, not a SIEM? From the perspective of the security officers, there will be a lot of worries and curiosities. In this article, I would like to explain the artificial intelligence security operation/monitoring process suggested by the IGLOO SECURITY Management Security Methodology to answer these questions. [2]

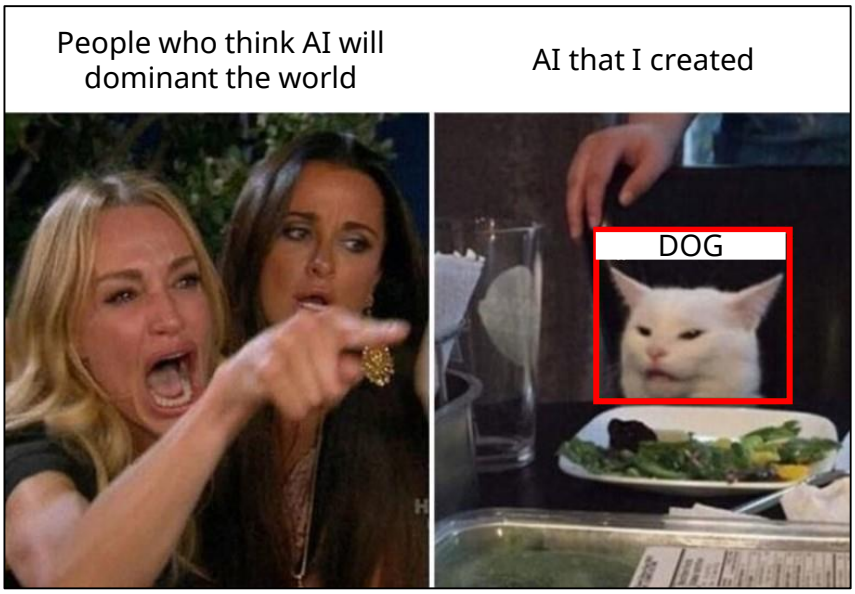
Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on Management Security Methodology

02. Understanding of AI Security Operation/Monitoring

1) Perspective of AI security operation/monitoring

When artificial intelligence technology was first introduced into security operation/monitoring, the reaction was varied. There was also an expectation that it would be possible to operate and monitor security system faster and more accurately than humans by using artificial intelligence, and there was a reaction that it was necessary to reduce the number of security officer because artificial intelligence was introduced. At first, it was a reaction that if artificial intelligence was introduced, everything would be solved, but in conclusion, the reality was not.



[Figure 4-2] An image that satirizes the ideals and reality of artificial intelligence

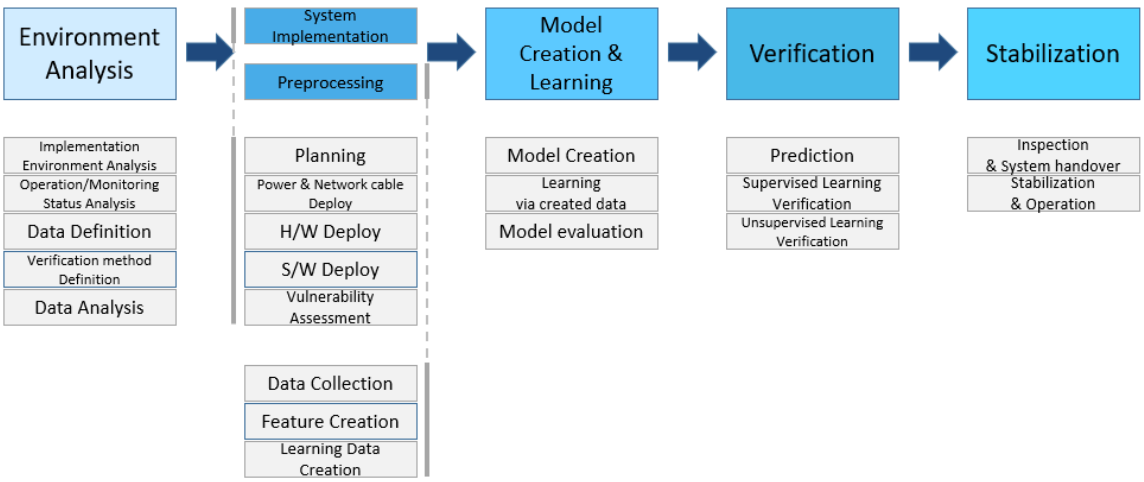
Even if an artificial intelligence security operation/monitoring system is introduced into security operation/monitoring work process, it does not mean that not to use the existing traditional security operation/monitoring system, especially a big data-based security operation/monitoring system (SIEM). Several years have passed since the artificial intelligence security operation/monitoring system was introduced into security operation/monitoring work process, but SIEM, which performs rule-based security operation/monitoring, is still solidifying its position as the core of security operation/monitoring. The artificial intelligence security operation/monitoring system is being used as a complementary relationship rather than replacing the existing SIEM in security operation/monitoring. SIEM is used to detect attacks in the traditional way, and artificial intelligence security operation/monitoring systems are used for attacks that are difficult to confirm with SIEM (too many attacks or attacks cannot be found). [3] Then, let's take a closer look at what makes security operation/monitoring using an artificial intelligence security operation/monitoring system different from the existing SIEM-based security operation/monitoring.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on Management Security Methodology

2) Artificial intelligence security operation/monitoring system implementation process

In order to know the artificial intelligence security operation/monitoring process, it is necessary to first understand the various activities required when implementing an artificial intelligence security operation/monitoring system. The process of building an artificial intelligence security operation/monitoring system is quite different from that of a general SIEM. In the case of SIEM, if it is a process ranging from 'Status Analysis'-'Integration with Collection Targets'-'Policy Setting'-'Operation/Monitoring', then the artificial intelligence security operation/monitoring system will be implemented in the following process. [4]



[Figure 4-3] Artificial Intelligence Security Operation/Monitoring System Implementation Process

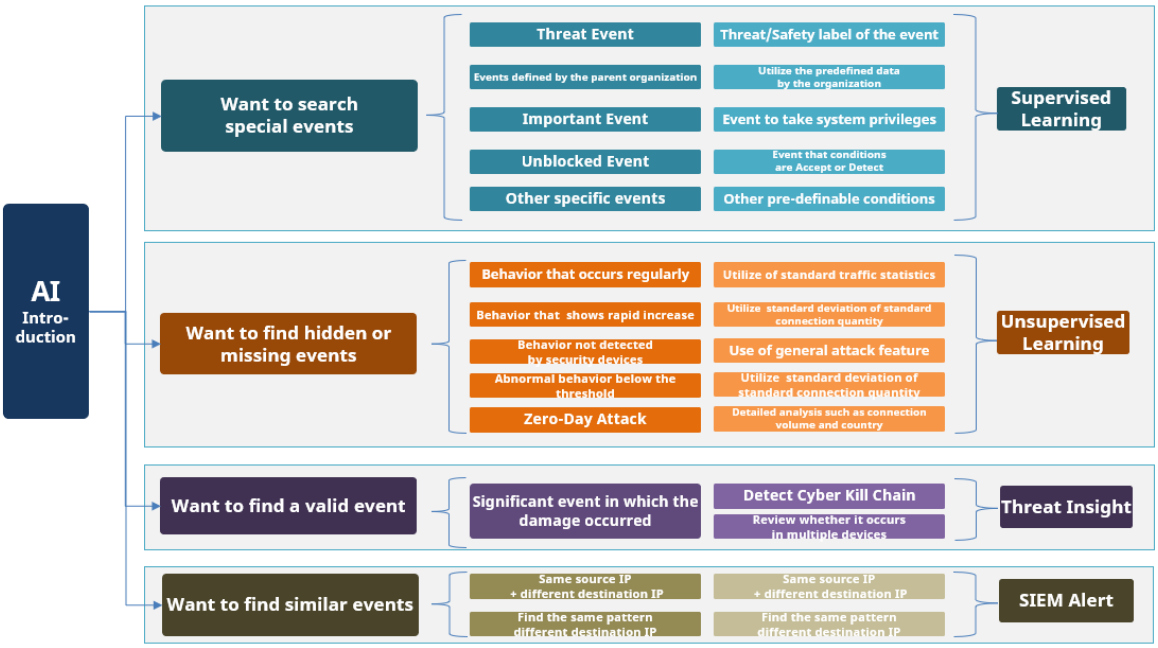
Looking at the Artificial Intelligence Security Operation/Monitoring System Implementation Process, unlike SIEM implementation, there are parts that need to be approached from an expert's point of view rather than an engineer's point of view. It is the 'preprocessing'-'model creation and learning'-'verification' part. In order for the artificial intelligence security operation/monitoring system to perform proper security operation/monitoring, it must first learn with correct data. To this end, data features should be extracted based on an understanding of security and the extraction method should be formalized. And based on this extraction method, training and prediction data are generated, a model is generated from the training data, and model performance is verified through direct labeling on the prediction data. Therefore, in order to perform this series of processes well, active participation of experts with domain knowledge of security is required.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on Management Security Methodology

3) Preparation for establishing artificial intelligence security operation/monitoring process

The most important thing for artificial intelligence security operation/monitoring is to consider how to use 'artificial intelligence' after introducing the artificial intelligence security operation/monitoring system before introducing it. However, in the case of security officer working at the site, the system is implemented first without any time to worry about this. In most cases, they are confused about how to achieve results with the operation/monitoring system. Therefore, I would like to present the following clues to the security officer.



[Figure 4-4] Objective of introducing artificial intelligence security operation/monitoring system [4]

Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on **Management Security Methodology**

You'll want to do all of the above, but there aren't many ways to do it with limited resources (people, systems, etc.). In addition, when introducing an artificial intelligence security operation/monitoring system, it is impossible to select additional personnel in charge, and the workload of existing security operation/monitoring personnel will only increase. The IGLOO Cyber Security Research Lab, which studies AI security operation/monitoring, provides the following advice to relevant personnel who ask questions with such concerns. “If you introduce the artificial intelligence security operation/monitoring system, think that you have recruited a smart security officer. This officer doesn't eat, sleeps, doesn't go home, and helps existing security officers 24 hours a day, 365 days a year.” In other words, instead of thinking that the artificial intelligence security operation/monitoring system has been introduced, do not think that the number of alert that come through SIEM is automated, and the existing security is focused on the high-priority alerts determined by the artificial intelligence security operation/monitoring system. Once you have decided on what target to operate/monitor, it is time to establish a security operation/monitoring process.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

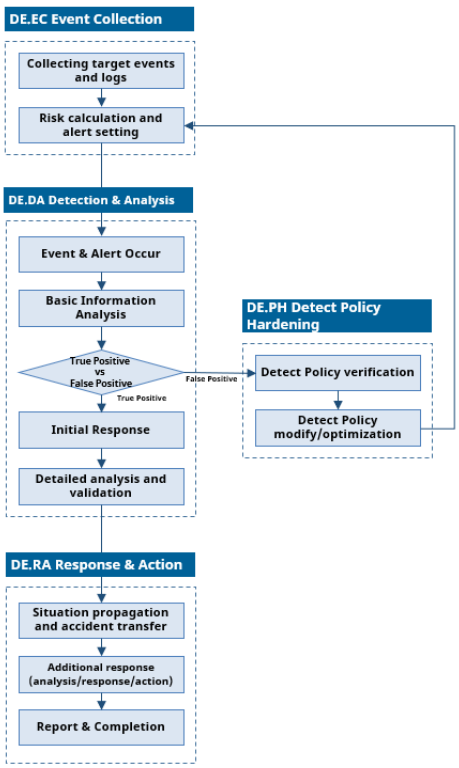
AI security monitoring process based on Management Security Methodology

03. AI Security Operation/Monitoring Process

1) IGLOO SECURITY standard detection process

The standard detection process suggested in the IGLOO SECURITY Management Security Methodology is shown in [Figure 4-5]. [2]

- In the security event collection (DE.EC) stage, security events and logs of the security operation/monitoring target are collected and alerts are set.
- In the detection and analysis (DE.DA) stage expresses the tasks that the security officers should most intensively do, analyzes basic information when events and alerts occur in the operation/monitoring target system, determines whether or not spying, and responds to the initial response and perform detailed analysis.
- In the response and action (DE.RA) stage, the situation is communicated and incidents are transferred, additional responses are carried out if necessary, and when an issue is closed, reporting and closing are performed.
- The detection process management and policy hardening (DE.PH) stage is performed regularly or when false positives occur, and the detection policy is verified, changed, or optimized.



Looking at the standard detection process, there is no difference between the security operation/monitoring process using SIEM and the artificial intelligence security operation/monitoring process, and the security operation/monitoring process seems to be maintaining a certain process regardless of which security operation/monitoring system is used. Then, in what parts is the security operation/monitoring process different when the artificial intelligence security operation/monitoring system is introduced? Let's take a closer look at this part.

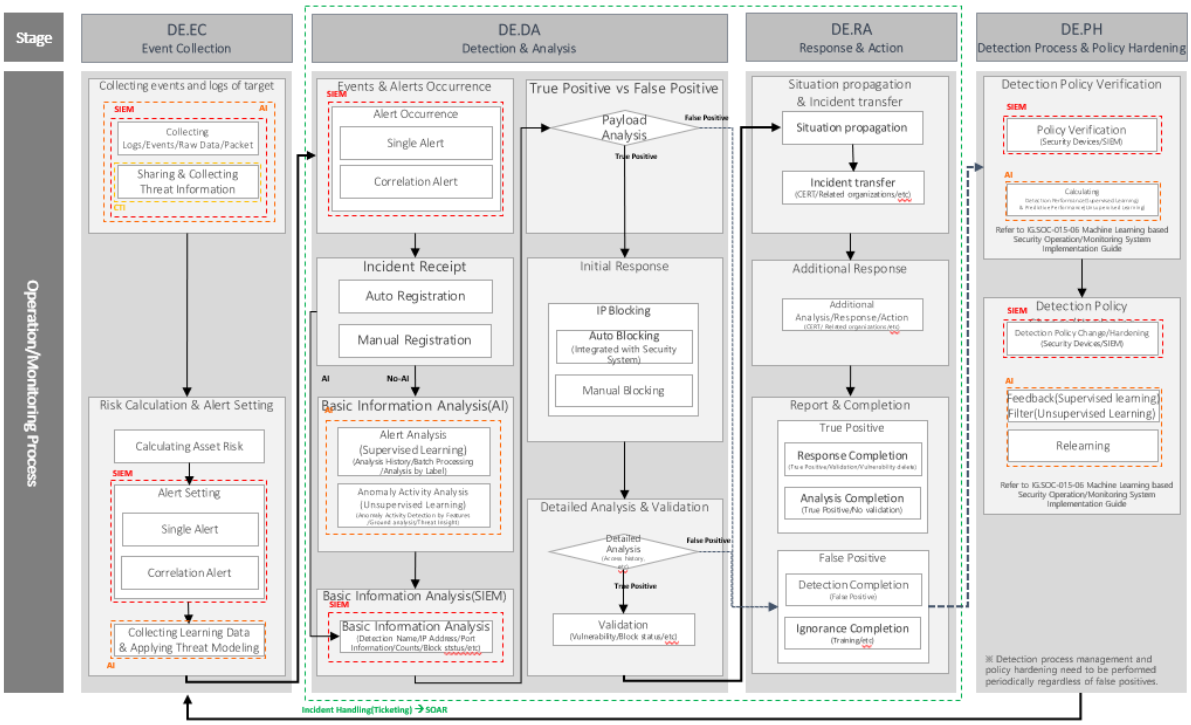
Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on **Management Security Methodology**

2) AI Security operation/monitoring process

The detailed artificial intelligence security operation/monitoring process presented in the IGLOO SECURITY Management Security Methodology is expressed through the detailed detection process in [Figure 4-6].

In the security event collection (DE.EC) stage, there is no significant difference from the big data-based security operation/monitoring process using SIEM. However, for the efficient use of artificial intelligence security operation/monitoring, it is recommended to link various information through Cyber Threat Intelligence. In addition, the artificial intelligence security operation/monitoring system collects learning data and applies threat modeling. This part is a part to be performed in advance when building an artificial intelligence security operation/monitoring system, just like setting standard alerts when building SIEM.

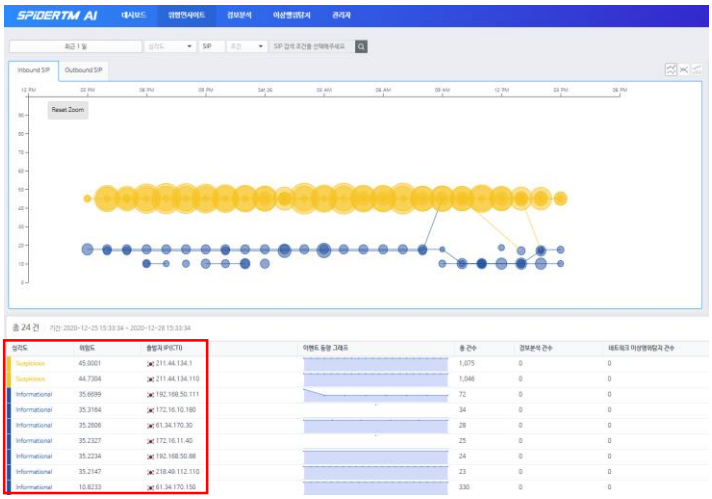


[Figure 4-6] Detailed Detection Process [5]

Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on **Management Security Methodology**

In the detection and analysis (DE.DA) stage, which corresponds to the actual operation/monitoring task, it starts with an alert. Regardless of whether SIEM is the main monitoring or the artificial intelligence security operation/monitoring system is the main monitoring, the starting point of the operation/monitoring depends on the judgment of the security officers. However, when monitoring the artificial intelligence operation/monitoring system as the main, it is recommended to monitor the threat insight screen as much as possible. Operation/Monitoring efficiency is expected to increase by prioritizing analysis based on the level of “risk” displayed in Threat Insight.



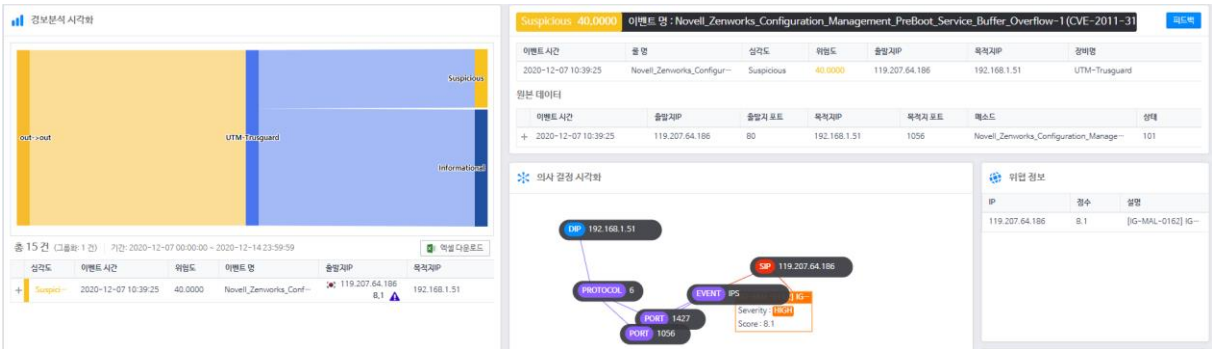
[Figure 4-7] Threat Insight Screen

If there is an artificial intelligence security operation/monitoring system at the stage of basic information analysis after an alert occurs, the contents to be analyzed will be enriched.

In the case of positive and false positive detection, the following contents can be analyzed through the ‘Alert Analysis' screen.

Details that can be analyzed through alert analysis (supervised learning)

: Past analysis history, automatic batch processing, analysis by label, etc.



[Figure 4-8] Alert Analysis(Supervised Learning) Screen

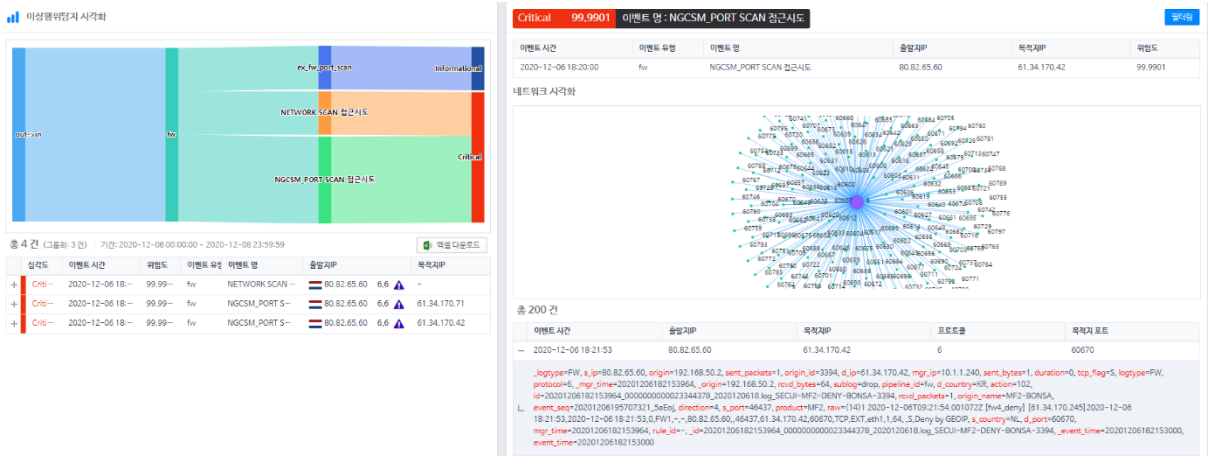
Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on **Management Security Methodology**

In the case of anomaly analysis, the following contents can be analyzed through the ‘Anomaly Analysis' screen.

Details that can be analyzed through anomaly analysis (unsupervised learning)

: anomaly detection by feature, evidence analysis, threat insight analysis, etc.



[Figure 4-9] Anomaly Analysis (Unsupervised Learning) Screen

Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on Management Security Methodology

After basic information analysis, the detection and analysis (DE.DA) process and the response and action (DE.RA) process, which consist of detailed analysis and validation, are conducted using the existing method, but if necessary, artificial intelligence security operation/monitoring could be used additionally.

Examples of detection and analysis using SIEM and artificial intelligence are shown in [Table 4-1].

[Detection Information]

• Detection Model Name : [FW] Information Gathering (PING SCAN) Access Attempts

[Detection Model Information]

• Detection Model Description : A model that identifies abnormal IPs that search multiple IPs using ICMP (Ping)

• Algorithm : Isolation Forest

• Feature : proto_icmp, dstaddr_unique

[How to Analysis]

1) Detection : **[AI Operation/Monitoring System → Anomaly Detection]** Review whether access is attempted to multiple destination IPs with ICMP protocol in AI details

2) Analysis : **[SIEM]** Analysis of whether the source IP attempted to access another destination IP using the ICMP protocol

3) Response : When access attempts with multiple IPs are detected, IP blocking is performed at the firewall, and blacklist IP registration

[Table 4-1] Example of detection and analysis using SIEM and artificial intelligence

If there is a Cyber Threat Information sharing system (CTI) in the security operation center, more clear information could be provided and used for analysis when analyzing basic information in the detection and analysis (DE.DA) process, and SOAR (Security Orchestration, Automation and Response) If there is a product, it is judged that the detection and analysis (DE.DA) and response and action (DE.RA) processes could be automated.

In the process of detection process and policy hardening (DE.PH), the security system and SIEM perform general policy verification and hardening, but the Artificial Intelligence security operation/monitoring system performs detection policy verification and policy hardening through the following additional processes.

• Detection policy verification: detection performance measurement (supervised learning), predictive performance measurement (unsupervised learning)

• Detection policy change/hardening: feedback (supervised learning), filter (unsupervised learning) → Relearning

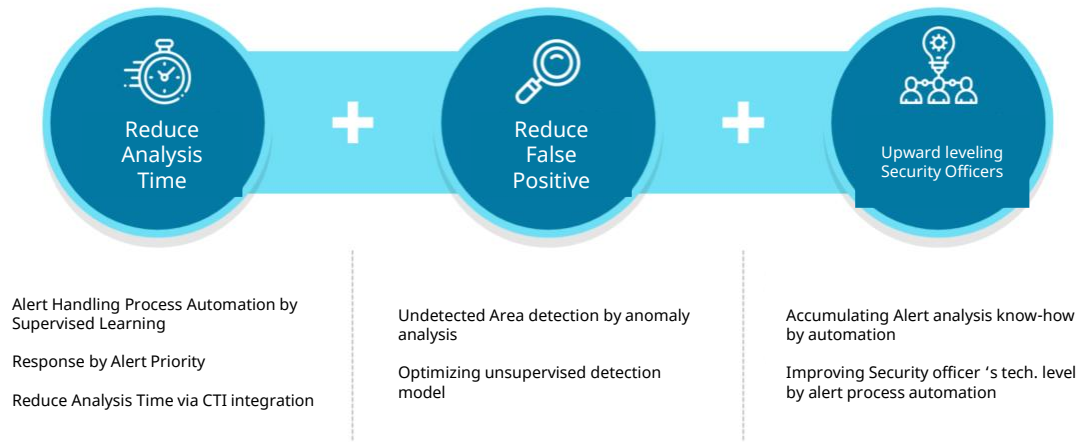
Through this series of processes, we briefly looked at the security operation/monitoring when the Artificial Intelligence was introduced.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

AI security monitoring process based on Management Security Methodology

04. Conclusion

So far, what is artificial intelligence security operation/monitoring, and what is the artificial intelligence security operation/monitoring process suggested by IGLOO SECURITY Management Security Methodology. In conclusion, artificial intelligence is not universal, and even if an artificial intelligence Security Operation/Monitoring system is introduced, the work of security officers is not drastically reduced. However, as mentioned above, if the artificial intelligence recognizes that it is a 'smart security officer' working with security officers, and establishes a security operation/monitoring process optimized for the goal of the site accordingly, in [Figure 4-10] As suggested, it is believed that clear results could be achieved.



[Figure 4-10] Goal of AI Security Operation/Monitoring

05. Resource

[1] IGLOO Security Monthly Security Report, Sep. 2018
[2] IG.SOC-031 Detection Manual (Dec. 2020)
[3] AI Security Operation/Monitoring : Truth and Falsity (IGLOO Security, Sep. 2020)
[4] IG.SOC-015-06 Machine Learning based Security Operation/Monitoring System Implementation Guide
[5] IG.SOC-031-08 Detailed Detection Process

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 5

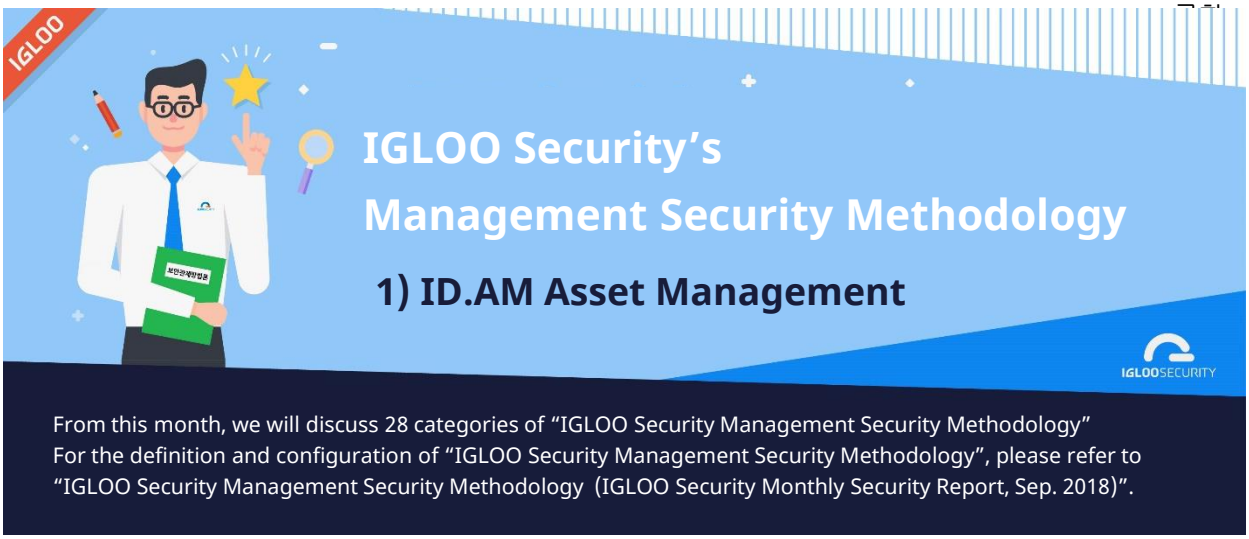
Focus On IGLOO

- IGLOO Security's Management Security Methodology
  1) ID.AM Asset Management

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 IGLOO Security's Management Security Methodology
1) ID.AM Asset Management

Strategic Business Department
Strategic Planning Team



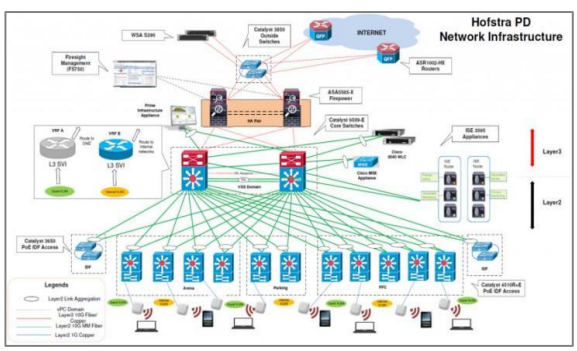
From this month, we will discuss 28 categories of "IGLOO Security Management Security Methodology"
For the definition and configuration of "IGLOO Security Management Security Methodology", please refer to "IGLOO Security Management Security Methodology (IGLOO Security Monthly Security Report, Sep. 2018)".

01. Category : ID.AM Asset Management

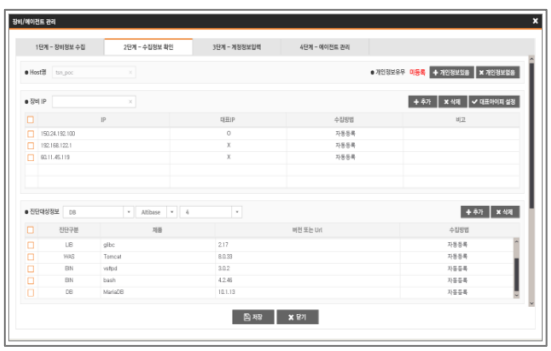
Identify > ID.AM(Asset Management)
: Defining & Categorizing operation/monitoring target data, employees, devices, systems and infrastructures and Managing it by priority.

The first function of "IGLOO Security Management Security Methodology", which contains 20 years of security operation/monitoring know-how of IGLOO SECURITY, is Identify > ID.AM (Asset Management).

Security operation/monitoring could be starting with grasping its target and scope. This is because if the target is not properly identified, it is difficult to respond to attacks from places that are not recognized at all, and it is difficult to grasp them even after the actual attack. For this reason, the Security Operation Center (SOC) performs operation/monitoring tasks after identifying assets through the information and communication network configuration diagram (network configuration diagram) and information asset management list before starting the operation/monitoring. Asset management is the most basic element for grasping the targets and scope.



[Figure5-1]Network Diagram sample(Resource : HP)



[Figure 5-2] Asset MGMT & Vul. Assessment Solution (Resource : IGLOO Security Smart[Guard])

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 IGLOO Security's Security Monitoring Methodology

1) ID.AM Asset Management

In general, the factors to be grasped in the asset management stage are not only the list of assets, but also the importance of each asset. This part not only plays an important role in security operation/monitoring-related tasks such as "risk identification management" and "recovery", which will be described later, and also adjusts the level of alerts according to the importance of assets when performing actual security operation/monitoring.

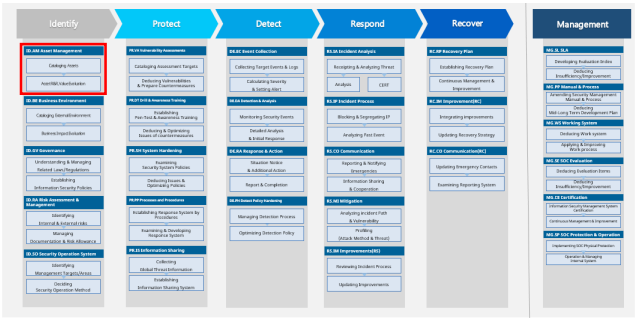
In particular, as "Axonius", which has a cyber security asset management (CSAM) platform, won the award at RSAC Innovation Sandbox Contest 2019, asset management was recognized as more important in cyber security.

[Figure 5-3] RAAC 2019 Innovation Sandbox Contest winning companies (Resource : RSA)

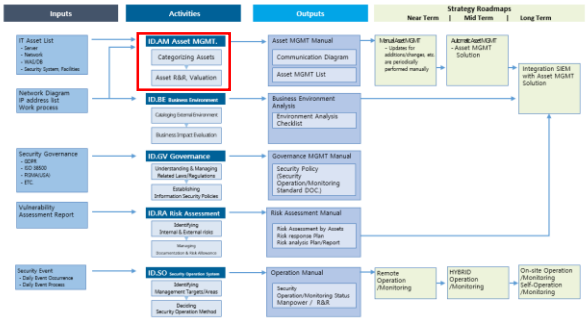
The problem is that the part of identifying assets is not something that security officers can do. There are as many asset managers as the number of assets, and the management method and level are different according to the propensity of the asset manager, so how to organize them and use them for security operation/monitoring seems to remain a task for the security manager.

02. Location of the detailed activity in the IGLOO SECURITY Management Security Methodology

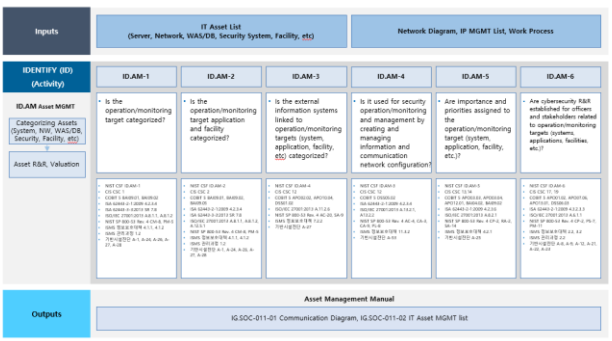
1) Management Security Methodology Process



2) Identify Function Logic Model



3) ID.AM Logic Model



4) Reference

IG.SOC-010 Identify, IG.SOC-011 Asset MGMT Manual,
IG.SOC-011-01 Communication Diagram
IG.SOC-011-02 Asset MGMT List

Copyright © IGLOO Security, Inc. 2021. All rights reserved

We Know SECURITY!

Published by IGLOO SECURITY (www.igloosec.co.kr/en)
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
東京都千代田区岩本町3-4-3 リードシー秋葉原ビル5階
T. +81-3-5829-5801
E-mail. business@ci-corp.jp

Edited by IGLOO SECURITY Marketing Team
Translated by IGLOO SECURITY Overseas Business Team
© 2021 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.