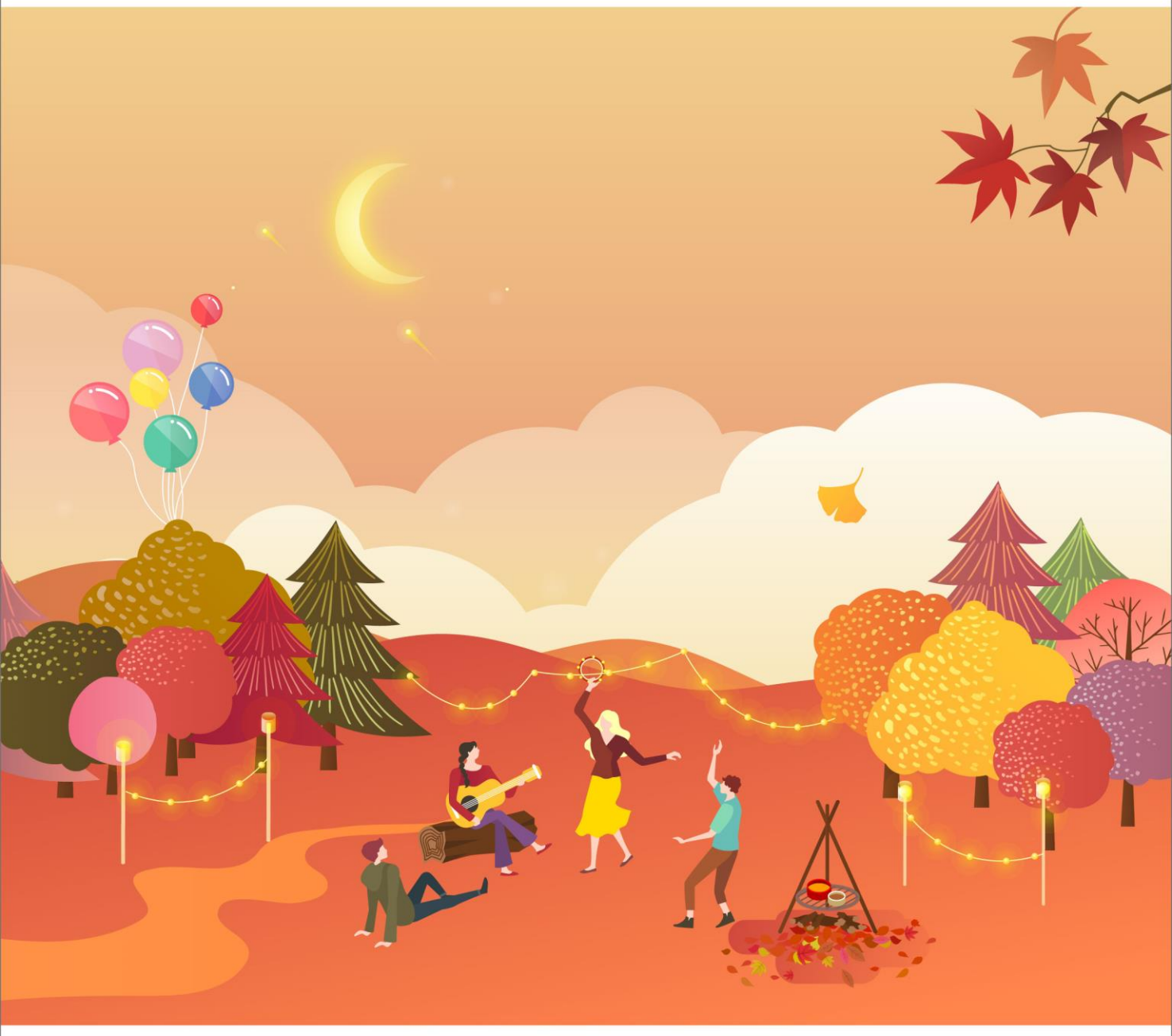
Monthly Security Report

2020
October



Cover Story

- “Zero Trust” security model that can respond to changes in the business environment of the untact era
- Digital New Deal Policy and Information Security

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. 2020. All rights reserved

Cover Story

1. Monthly Security Issue

- Security Issue

2. IGLOO Statistics

- Monthly attack service and trend analysis
- Detailed analysis according to different patterns

3. Tech Note

- A “Zero Trust” security model that can respond to changes in the business environment in the untact era

4. Special Column

- Digital New Deal Policy and Information Security

5. Focus On IGLOO Security

- This month’s IGLOO Security

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 1

Monthly Security Issue

1. Security issue

Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Security Issue

In the first half of 2020, cyber attackers aimed at telecommuters

- In the first half of 2020, it appears that cyber attackers focused on attacks targeting home and remote workers.
- According to Fortinet's “Global Threat Prospect Report for the First Half of 2020,” cybercriminals are using the uncertainty and fear arising from the global pandemic as opportunities to launch massive cyber attacks. They were exploiting a situation where the digital attack surface expanded as the number of remote workers working outside the corporate network increased.
- In addition, attacks and ransomware targeting IoT devices and OT (operation technology) were also evolving more precisely. It seems that it was aimed at increasing remote access as the movement of employees was restricted due to COVID-19.
- Security experts stressed to devise measures to protect the devices and home networks used by remote workers.

Security threats targeting students taking online classes

- With the spread of COVID-19, Online class is active worldwide, and related security threats are also increasing, such as the number of malicious domains related to online classes. Security experts suggest security measures to counter this.
  - ➢ At the end of class, physically hide the PC's web camera and turn off the microphone. In particular, important information, including personal information, must be hidden from the camera's view.
  - ➢ Click only the link sent by the online class coordinator and log in directly through the school portal site.
  - ➢ Use complex passwords and do not share important information on cloud storage platforms.
  - ➢ Schools should install anti-virus software on all devices, including student PCs, and install security devices such as network firewalls and Internet gateways to continuously monitor them.
  - ➢ Education accounts of students and teachers must be secured with two-factor authentication.

Ransomware death incident in German hospital

- A ransomware attack paralyzes the IT system of a general hospital operated by the University of Dusseldorf, Germany, and one patient who needs urgent medical treatment dies. The patient was taken to a hospital 32 kilometers away, but eventually died as a result of delayed treatment for an hour.
- Düsseldorf police said, "A letter was found threatening a message asking the hacker to contact you, but there was no request for the cost of decryption, and the recipient was a university, not a hospital.“
- When police contacted the attacker and explained that the hospital, not the university, was paralyzed, the attacker provided a digital key to decrypt the data. In other words, it was presumed that it was not aimed at the hospital from the beginning and accidentally encrypted the hospital server instead of the university.
- The police are currently pursuing the attacker for negligence and fatality.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Security Issue

Cyber threat advisory targeting COVID-19 vaccine and treatment technology

- At the national level, cyber attacks to preempt COVID-19 vaccine and treatment technologies are occurring, and there is a growing voice that efforts should be made not only to prevent COVID-19 but also to prevent cyber attacks.
- The U.S. Department of Justice officially prosecuted two Chinese people who stole information related to the development of the COVID-19 vaccine in July on 11 charges, including hacking. They are from Chengdu Electronics Science and Technology University in China, and are suspected of having conducted extensive hacking over the past 10 years in connection with the Ministry of State Security (MSS) of China.
- In Russia, suspicions have been raised that hackers attempted to intercept the results of COVID-19 vaccine research in countries around the world. The US National Security Agency (NSA), the UK National Cyber Security Center (NCSC), and the Canadian Federal Communications Agency (CSE) announced that in July, the Russian hacker group'APT29' conducted COVID-19 research achievements in the UK, Canada, US academia and pharmaceutical industry Claimed to have tried to hack
- According to the U.S. Federal Bureau of Investigation's Cyber Security Administration, Iran has also attempted to hack data on the U.S. COVID-19 vaccine research since January.
- Security experts predict that as the COVID-19 outbreak is prolonged globally, more attempts to 'weapon resource' for COVID-19 vaccines and treatments will increase, and accordingly, hacking attempts to lead the competition for technology development will increase rapidly.

Warning of malicious app intercepting financial counseling phone

- Amidst increasingly sophisticated financial fraud, malicious apps that intercept financial counseling calls have been discovered, requiring user attention.
- According to AhnLab, a “Kaishi” mobile malware was discovered that pretended to be a financial application to steal information from infected smartphones, intercept financial consultation calls, and reconnect to attackers.
- The attacker uses voice phishing or smishing to allow users to access a phishing site that is designed very similar to a real famous financial company's website. Prompted to download the malicious installation file of Kaishi by popping up a message.
- During the installation process, the attacker requests excessive privileges such as calling functions, address books, text messages, etc., stealing them, and monitoring the user's phone status, so that even if the user makes a financial advisory call to the correct number, the call is directed to the attacker's number It was reconnecting (redirecting).
- As security experts say that as untact financial transactions using smartphones are becoming more and more sophisticated, attacks aimed at them are becoming more and more sophisticated.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Security Issue

97% of companies have difficulty maintaining network security due to increased telecommuting

- With the recent expansion of the telecommuting system, a survey result was announced that the majority of corporate IT networking and security officers are having difficulty maintaining the organization's network security.
- According to a survey by Juniper Networks of over 1,000 corporate IT and security officers in various industries in nine countries, including the United States and the United Kingdom, 97% of respondents said they had difficulty maintaining organizational network security. In particular, it is analyzed that the work burden of the IT team is increasing in the context of large-scale telecommuting.
- In addition, 87% of respondents say they need a security solution that increases visibility of applications in use, reduces false positives, and supports rapid threat response.
- Security experts emphasized the need to secure visibility of all network elements and prepare a security strategy that can respond immediately when necessary, saying that the work burden of IT and security managers is increasing as the organizational manpower is distributed.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 2

IGLOO Statistics

1. Monthly attack service and trend analysis
   - 01. Top 10 monthly vulnerability attacks
   - 02. Event by vulnerability compared to previous month
   - 03. Top 10 monthly attack service(port)
   - 04. Monthly attack service(port) cases compared to previous month
   - 05. Top 10 monthly attack service patterns
   - 06. Monthly attack service incident patterns compared to previous month
2. Detailed analysis according to different patterns

Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the vulnerability and analyzes the attack. Through this process, future cyber threats can be predicted.

01. Top 10 monthly vulnerability attacks

In the top 10 vulnerability attacks collected for one month in October 2020, attacks using the MVPower DVR Shell Unauthenticated Command Execution, Command Injection (D-Link HNAP Vulnerability), and Netlink GPON Router Remote Code Execution vulnerabilities entered the ranking. In addition, the attack patterns of Command Injection (Netgear Routers Vulnerability) and GPON Router Vulnerability entered the top rankings with a rate increase compared to the previous month.

※ Based on the Incident response report data of IGLOO Security SOC

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	Command Injection (Netgear Routers Vulnerability)	847	20.40%	▲6
2	GPON Router Vulnerability	667	16.06%	▲8
3	MVPower DVR Shell Unauthenticated Command Execution	543	13.08%	NEW
4	Command Injection(D-Link HNAP Vulnerability)	488	11.75%	NEW
5	phpMyAdmin sample page access	339	8.16%	▼2
6	URL extension access control	329	7.92%	-
7	WordPress sample page access	284	6.84%	▼6
8	Netlink GPON Router Remote Code Execution	217	5.23%	NEW
9	Cross Site Script(XSS)	258	6.21%	-
10	ZeroShell kerbynet RCE (CVE-2009-0545)	180	4.34%	▼6
Total		4,152	100.00%	-

[Table2-1] TOP 10 monthly vulnerability attacks

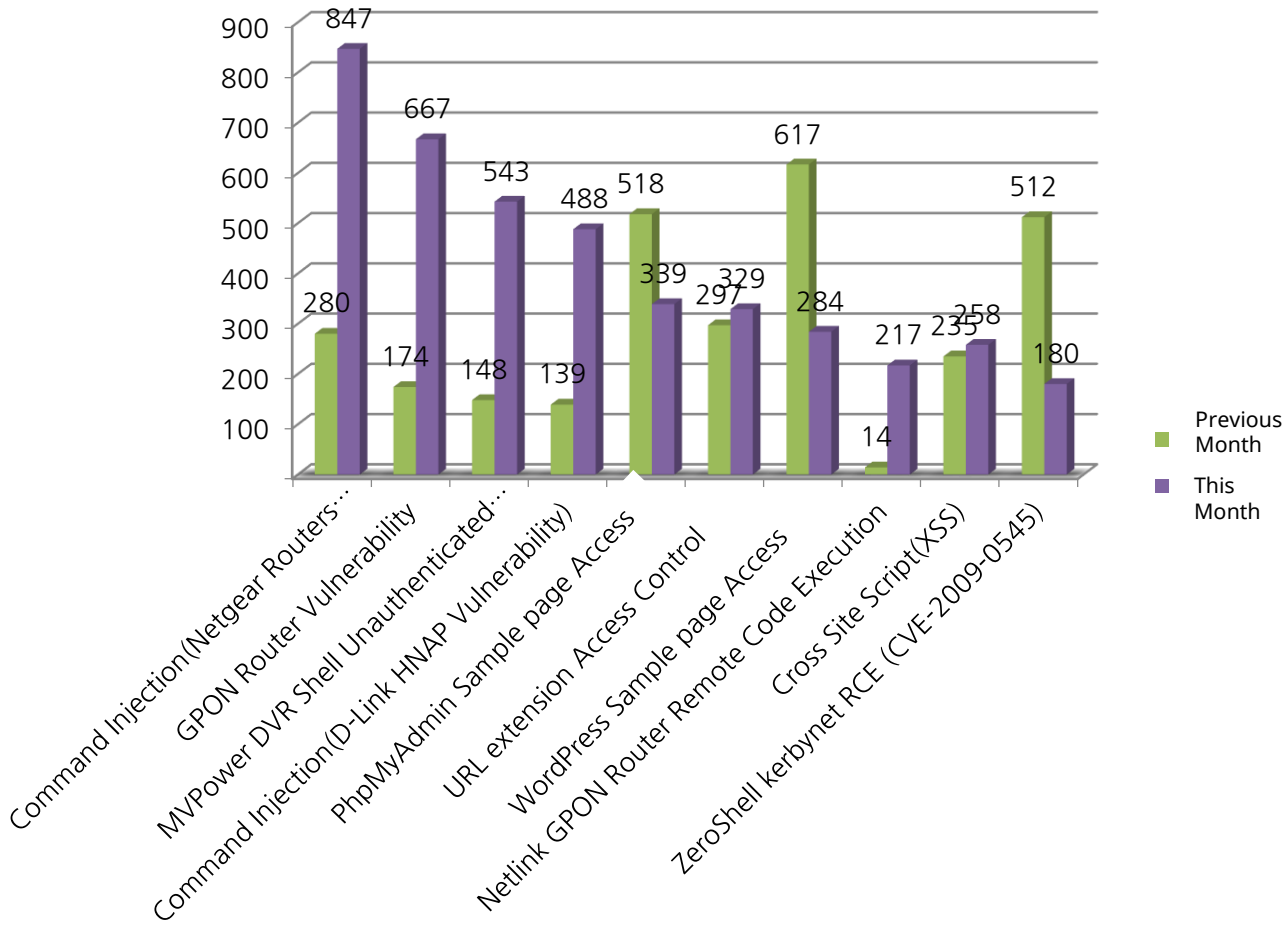
Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the vulnerability and analyzes the attack. Through this process, future cyber threats can be predicted.

02. Event by vulnerability compared to previous month

As a result of the analysis of vulnerability events collected for one month in October 2020, 6 RCE (Remote Code Execution) attacks were among the top 10, and the number of RCE attacks increased significantly compared to the previous month. It is judged as an RCE attack caused by a number of BotNet attacks, and the security officer needs to check whether the assets corresponding to the RCE vulnerability attack included in the Top 10 are included in the asset and whether the latest security firmware is updated.



[Figure 2-1] Comparison of previous month by vulnerability

Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats can be predicted.

03. Top 10 monthly attack service(port)

As a result of analysis of events collected for one month in October 2020, the number of events using the HTTPS (TCP/443) port significantly decreased by about 3.3 billion compared to the previous month. (TCP/7178) Events using ports slightly increased compared to the previous month.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of cases	Ratio(%)	Fluctuation
1	DNS(UDP/53)	845,743,791	45.16%	▲1
2	HTTPS(TCP/443)	354,617,751	18.94%	▼1
3	Microsoft-DS(TCP/445)	233,407,780	12.46%	▲1
4	HTTP(TCP/80)	130,141,151	6.95%	▼1
5	SNMP(UDP/161)	89,707,207	4.79%	-
6	ICMP(0/ICMP)	83,073,866	4.44%	-
7	MSSQL(TCP/1433)	36,596,593	1.95%	▲1
8	Unsigned(TCP/7178)	33,949,082	1.81%	▲2
9	Telnet(TCP/23)	33,145,745	1.77%	-
10	Unsigned(UDP/14218)	32,281,523	1.72%	NEW
	Total	1,872,664,489	100.00%	-

[Table 2-2] Monthly attack service (port) TOP 10

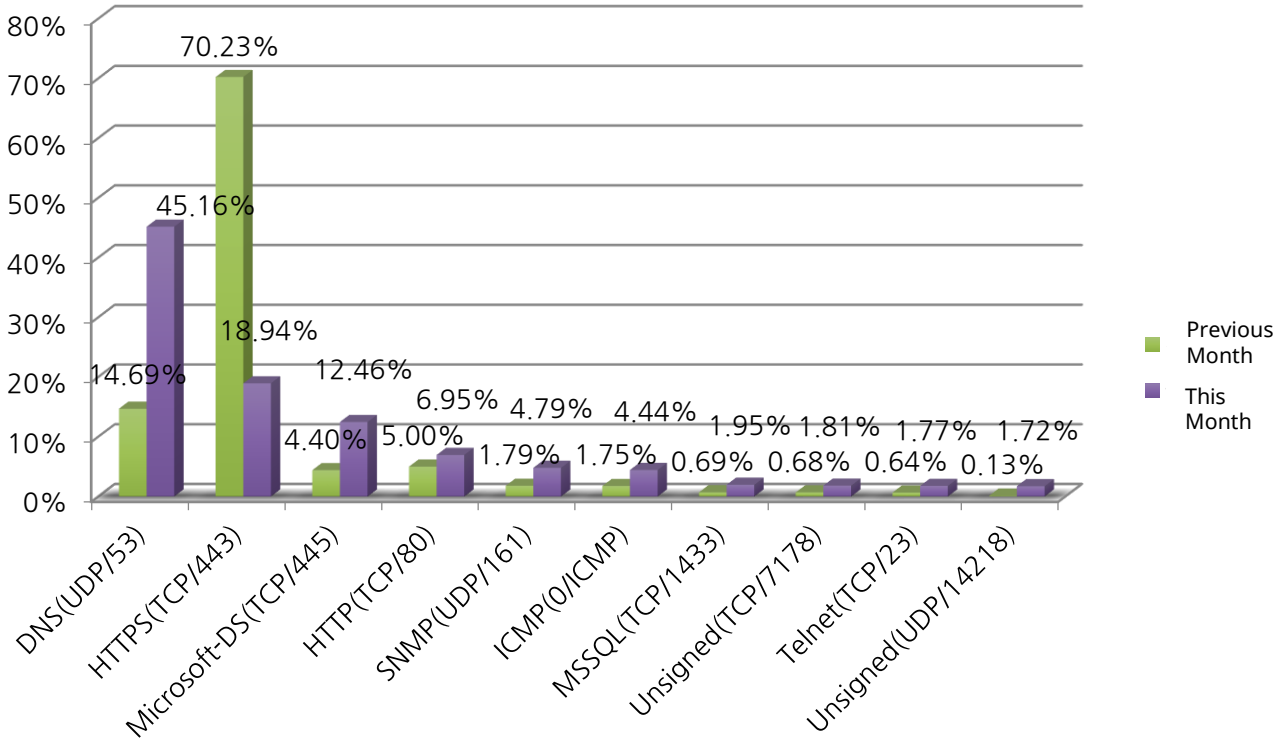
Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats can be predicted.

04. Monthly attack service(port) cases compared to previous month

As a result of analysis of events collected for one month in October 2020, Unsigned(UDP/14218) port is newly confirmed in the TOP10 ranking. Recently, the number of history of service ports not specified in Well-Known Ports has been continuously increasing. Among the unclear service ports, there is a service port actually used by each company. It is recommended to control access through firewall policy establishment after checking whether undefined service ports are actually used.



[Figure2-2] TOP10 monthly attack port

Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The trend of attack patterns detected by IGLOO SECURITY SOC can be used to identify the trend of the latest attacks.

05. Top 10 monthly attack service patterns

In the attack pattern TOP10 in October 2020, the ranking of the HTTP Login Brute Force event slightly increased, and other HTTP Connection Limit Exhaustion Attack (By Slowloris), javascript: (Common XSS Injection -7), and FIN Port Scan events newly entered the ranking.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	718,555,112	93.92%	-
2	Ack Storm	16,994,754	2.22%	-
3	ACK Port Scan(F/W Scan)	9,463,348	1.24%	-
4	HTTP Connection Limit Exhaustion Attack(By Slowloris)	6,025,366	0.79%	NEW
5	Dcom_TCP_Sweep(MSBlaster Worm Messenger...)	5,766,050	0.75%	▼1
6	HTTP Login Brute Force	2,910,880	0.38%	▲1
7	Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	1,886,796	0.25%	▼2
8	javascript: (Common XSS Injection -7)	1,463,808	0.19%	NEW
9	TLS Malformed Handshake DoS	1,156,610	0.15%	▼3
10	FIN Port Scan	877,354	0.11%	NEW
	Total	765,100,078	100.00%	-

[Table 2-3] TOP10 monthly attack pattern

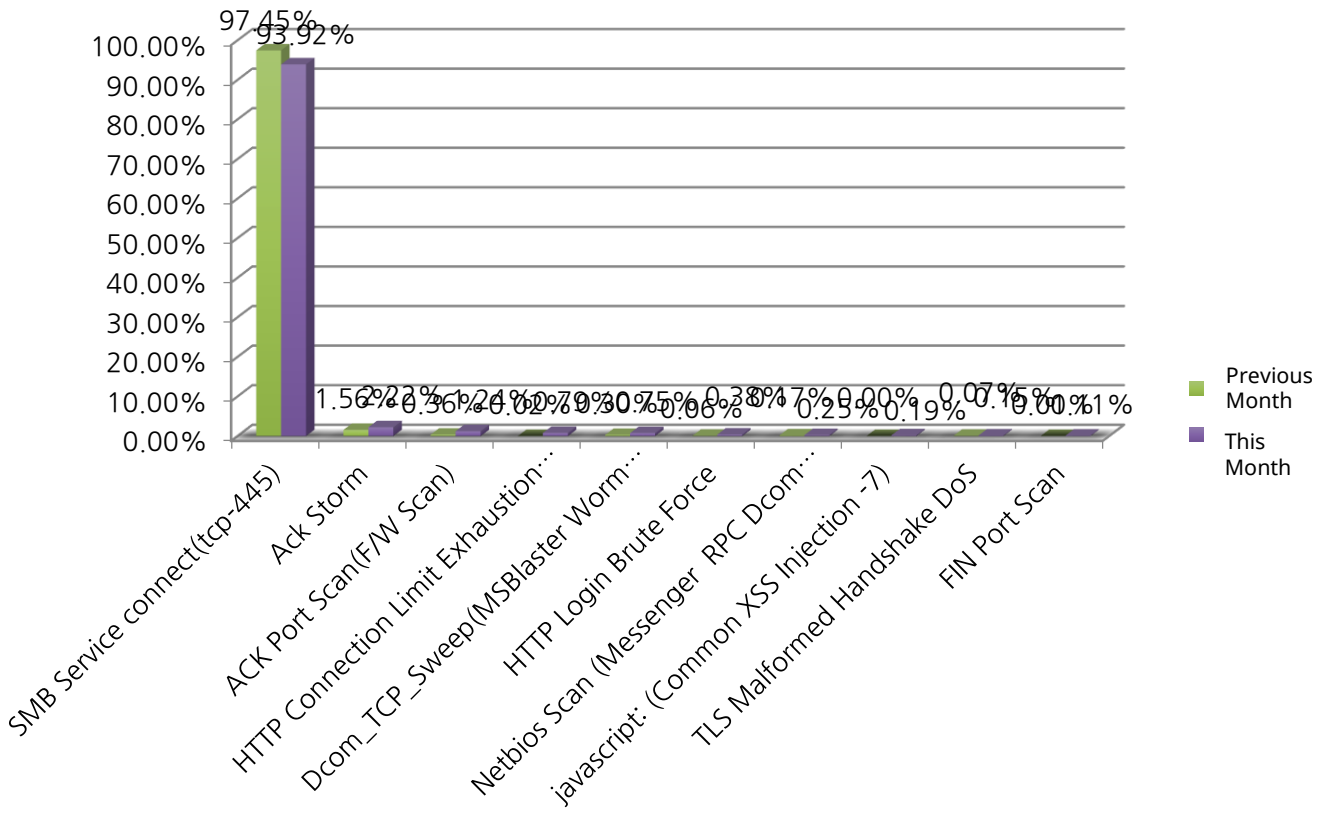
Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The attack pattern rankings detected by IGLOO SECURITY SOC can be used to identify the latest trends of attacks.

06. Monthly attack service incident patterns compared to previous month

In the top 10 attack events in October 2020, scanning attempts for open service ports as a whole are dominated, and attempts to access SMB service ports account for more than 90% of the same as last month. Recently, the latest vulnerabilities for SMB have occurred, such as CVE-2020-1301, a remote code execution vulnerability in SMBv1, and CVE-2020-1206, a client/server information disclosure vulnerability in SMBv3. All of them are provided with emergency patches from MicroSoft, so if you are not using the latest Windows Update or SMB port, you need to disable it.



[Figure 2-3] Monthly event comparison by Attack(Pattern)

Copyright © IGLOO Security, Inc. 2020. All rights reserved

2 Detailed analysis according to different patterns

We introduce detailed analysis results according to attack patterns, focusing on the TOP 10 among attack patterns that occurred in October.
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 Results
SMB Service connect(tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
Ack Storm	Attacker sends a large amount of TCP / IP Ack signal to the target server, and the target server is an attack method that creates unnecessary load and delays normal service. This attack is also used to Hijacking the packet in which the Session is made.
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.
HTTP Connection Limit Exhaustion Attack (By Slowloris)	Slowloris is an attack tool that maintains a TCP connection by sending an abnormal HTTP Request to a web server, unlike the existing DoS attack type that transmits a large number of packets. The attack target web server may run out of connection resources, and after the connection resources are exhausted, it is in a denial of service state that cannot respond to user requests.
Dcom_TCP_ Sweep (MSBlaster Worm Messenger...)	W32.Blaster.Worm is a worm that spreads by using the DCOM RPC Buffer Overflow vulnerability. The worm checks whether the TCP / 135 port is enabled and infects the system when it is found. The infected system activates TCP / 4444 port, downloads malicious files from the host server, registers them in the registry, and in this process, traffic from the infected system may increase.
HTTP Login Brute Force	This attack accesses the HTTP WEB service port(80) and repetitively inserts random strings through a Tool-Kit in order to find out the password for a specific ID(root, guest etc). Passwords which are easy to guess or are in an alphabetic/symbolic order are more prone to this attack. This attack can be prevented by using IDs and passwords over 6 letters and by Filtering data from the HTTP port(80/TCP).
Netbios Scan (Messenger RPC Dcom MyDoom ...) (UDP-137)	NetBios checks each other's information through UDP port 137, establishes a session with TCP 139, and exchanges data through TCP 138. An attacker can use this UDP port 137 to establish a session with the target system and scan information about the folders and networks shared on the target system.
javascript: (Common XSS Injection -7)	The javascript: (Common XSS Injection -7) vulnerability occurs when an attacker uses a web application to send malicious data such as JavaScript to other end users. End users can change user preferences by simply clicking links on websites containing malicious code, reading content contained in emails, or clicking posts posted on BBS, or changing cookies (cook-ie) or intercept and post false advertisements, etc.
TLS Malformed Handshake DoS	TLS Malformed Hadnshake DOS attack is a type of DOS attack using a maliciously manipulated TLS packet. It occurs during the handshake of a maliciously manipulated TLS client. It is an attack that a remote attacker can cause a load on the victim system by sending a maliciously crafted TLS packet to the affected system.
FIN PORT SCAN	This method can be used as a faster alternative to the normal TCP port scan. It scans by observing the host responding to the TCP FIN packet to find the TCP port to listen on. The target host uses the property of sending a response only when there is no response when the FIN is transmitted to the Listening port, and the port is checked without actually initializing the TCP connection.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 3

Tech Note

"Zero Trust" security model that can respond to changes
in the business environment of the untact era

Copyright © IGLOO Security, Inc. 2020. All rights reserved

"Zero Trust" security model that can respond to changes in the business environment of the untact era

Security Operation Team

01. Overview

1) Change to the Untact Era

The recent COVID-19 outbreak has expanded to a second outbreak, and the worldwide pandemic continues. As a result, the needs and changes for untact services are accelerating in various industries such as business work environment, education environment, medical service environment, and finance.

Recently, companies are changing their work environment to smart work environment such as telecommuting environment and remote video conference for non-face-to-face work. For this reason, the information security environment for ICT assets is also required to change according to the trend of the times.

Social Change

- Pandemic due to COVID-19
- Continued social distancing
- Increasing demand for untact service
- Changes in the environment across society, such as non-face-to-face education (online classes) and video conferences

Business Change

- Telecommuting, Video Conference
- Smart work environment
- Untact business increase (service industry, medical care, education, etc.)

Technical Change

- Increasing cloud services that enable home work environments
- Increase in remote access environments such as VPN
- Increasing BYOD-based work environment such as mobile devices
- Untact environment security model required

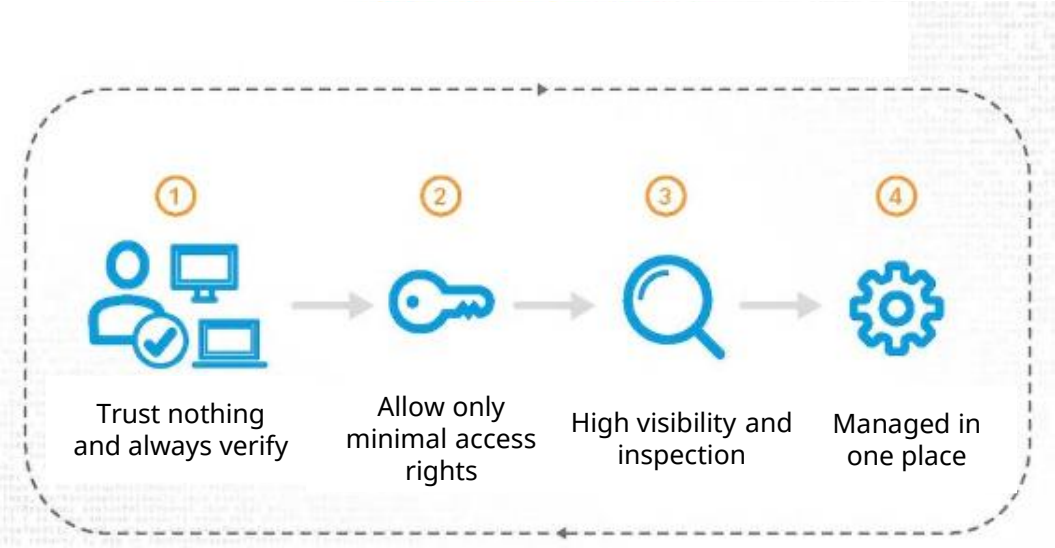
2) Background of interest in the zero trust security model

Background of interest	Description
Increasing data breaches	Over 500 million user accounts leaked from major portal sites such as Yahoo Politicians' email disclosure scandal during 2016 U.S. presidential election
Suspicion of all actions	Starting with the idea that all systems have already been compromised, Start with the philosophy that all actions should be suspicious
Data-focused security	Existing network security model limitations, applied to the outer perimeter (microperimeter) of each data
Increasing cloud service environment	The existing on-premises environment is changed to a cloud-based environment, and a new philosophy and paradigm shift for security is required.
Blacklist-based security limits	Security incidents by internal users are constantly increasing, Accordingly, it is necessary to worry about the reliability of the blacklist-based security model.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

3) Definition of the zero trust model

The concept of the zero trust security model implies the attitude of 'trust nobody'.
In other words, it is a security model that no one should trust anyone, both inside and outside the organization, without proper authentication procedures, and that an identity verification process must be performed before granting access rights to everything that wants to access the system.
Instead of assuming that all services in the Firewall are secure, they should assume violations and treat each service request as if it originated from the public network. Regardless of where the service request originated or the resource to be accessed, the zero trust model requires 'do not trust, always check.'



[Figure 3-1] Basic Concept of Zero Trust Security (Source: akamai.com)

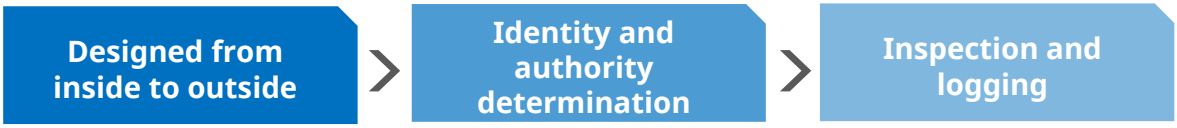
4) Principles of the Zero Trust Model

Principles	Description
Make it clear	Based on all data points provided, content including user ID, location, device status, service or workload, data classification and anomalies must always be authenticated and approved.
Access setting by permission	Limit user access and gain data and productivity at the same time with Just-In-Time/Just-Enough-Access (JIT/JEA), risk-based adaptive policies and data protection
Assuming Violation	Access is segmented by network, user, device, and app awareness to minimize the impact of violations and prevent horizontal movement Leverage analytics, enable threat detection, and improve defense to gain visibility and verification end-to-end encryption across all sessions

Copyright © IGLOO Security, Inc. 2020. All rights reserved

02. Zero trust concept diagram and security model establishment stage

1) Conceptual diagram of zero trust



1) Design from inside to outside: Identification of information assets (information systems, electronic documents, paper documents, etc.) and data that need protection
2) Identity and authority determination: To determine the identity and authority of internal and external users to access information assets and data
3) Inspection and logging: Inspection and logging under the premise that all users and traffic are not trusted

- The zero trust model is a highly secure method that monitors all data under the premise that all files are a potential risk, ensures that all data is accessed through a safe path, and allows data access only when absolutely necessary.
- When designing the system, it is designed from inside to outside, not from outside to inside, always distrust in principle, check identity, inspect all traffic and review logs

Copyright © IGLOO Security, Inc. 2020. All rights reserved

2) Zero Trust security model establishment stage

Establishment Stage		Description
1	Zero trust definition	• It is a step to set goals in terms of policy and create a roadmap to achieve the goals. Do not be constrained by technical issues, define what 'Zero Trust' is, and decide on how to implement Zero Trust and related technologies.
2	Understanding the user experience	• In the process of planning a zero trust model, you should consider the impact on the user experience. • Because no user is trusted without authentication and verification procedures, the user's experience of using systems and data is significantly different.
3	Select the Suitable Architecture	• In implementing the Zero Trust model, three methods are used to identify the strengths and weaknesses of each and select the method that suits the purpose. • Designed through three architectures: microsegmentation, software-defined perimeter (SDP), and zero trust proxy
4	Introducing strict and accurate authentication procedures	• Security mechanisms do not focus on the perimeter of the network, but on the target systems and applications themselves. • Enhance password through user multi-factor authentication (MFA) and grant access through additional authentication procedures • Requires a system that allows authenticated users to register their devices and receive verification
5	Prepare for problems	• All applications that allow access to sensitive data must be identified, and all privileges granted to users must be temporary, time-limited, and managed to be automatically expunged. • Calculate the scope and scale of work required to implement the zero trust model and prepare for problems.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

03. Plan and technical elements for implementing a zero trust security model

1) Zero Trust Security Model Implementation Plan

Implementation plan	Description
Microsegmentation	• Classify and manage all networks, assets, users, applications, data stores, etc., divided into logical groups • Advantages: Enhance security, control of process units • Disadvantages: Difficulty in implementation and deployment, poor scalability
SDP : Software Defined Perimeter	• A method of crossing the network boundary by verifying and confirming authentication and authorization for users through an application • Advantages: Enhanced security through tunneling, encrypted communication • Disadvantages: Need control measures after tunneling, lack of group classification policy standards
Zero trust proxy	• A method of acquiring authentication and authorization based on network traffic by setting an OnDemand Perimeter between an authenticated user and an application. • Advantages: Combining the advantages of the above two technologies • SPOF can occur

2) Technical elements of the zero trust security model

Technology element	Description	Detailed Technology
Network	Traffic control and monitoring between East-West by segmenting the network in micro units	Default Deny setting
Workload	Workload protection by subdividing into virtual machine, container, and function units	Agent-based VM control
Data	Data protection shared across all devices and applications	Private permission setting
User	Thorough control of personal identification	MFA setting, DID applied
Device	Vulnerability protection and intrusion prevention of internet-connected devices	Medium control, IP/MAC
Visibility and Analysis	Monitoring and analysis of all traffic activities on the internal network of the organization	Network Traffic Analysis
Automation and Orchestration	Build a system that can respond more agilely and accurately to large-scale network analysis	Incident Response, SOAR

Copyright © IGLOO Security, Inc. 2020. All rights reserved

04. 10 Ways to Successful Zero Trust Security

1) ID reorganization

- ID is the best way to start a zero trust.
- Although many organizations are focusing on micro-segmentation as an approach to implementing zero trust, this approach is subject to significant limitations.
- The micro-segmentation approach reduces the attack surface and is useful in on-premise, legacy application environments, but it is not effective in cloud environments.
- The zero trust model represents the transition from network-based controls to identity-based policies and processes. Identity-based security should coordinate silos between teams of experts and lay the groundwork for a zero trust model.

2) Implement conditional access control

- Hackers typically compromise login information, then use it to access systems and move horizontally across the network.
- Therefore, Zero Trust does not determine whether a particular user or device is inside or outside the corporate network.
- Access control decisions for zero trust must be made dynamically, risk assessment and understanding of all incoming resource requests from multiple dimensions, and then grant conditional access based on them.
- This conditional access method takes into account the importance of user identities and access rights, device health, application and network safety, and data being accessed.
- The fine-grained policy-guided enforcement engine then determines whether to allow, restrict, or block access to resource requests.
- Using a zero-trust network model that enforces the correct conditional access policies for users and devices, you can prevent hackers from moving horizontally across your network using stolen login information.

3) Strengthen user's credentials

- Weak passwords weaken the security of ID-based systems, and the network can be easily compromised through password spray attacks by hackers or attacks using login information.
- Setting up multi-factor authentication in conditional access control can improve the way users authenticate and restrict hackers from using stolen credentials.
- Multi-factor authentication provides an additional layer of user authentication, especially when accessing critical applications and data.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

4) Establish a plan for a double boundary strategy

- To avoid business disruption and risk, it adds new identity-based controls to the enterprise environment while maintaining existing network-based protection.
- In Zero Trust, applications are considered assets in the cloud or legacy environment.
- Cloud-native applications support identity-based control and conditional access rules can be layered relatively easily.
- Another category includes applications deployed behind network firewalls in legacy environments.
- One option to do this at scale is to manage access through a secure authentication gateway or application proxy, which can also reduce your risk by eliminating VPNs.

5) Intelligence and behavior analysis integration

- By inferring unusual user or object behavior and easily identifying threats, telemetry can be used to enforce conditional access control.
- The ability to make the right access control decisions depends on the quality, quantity, and variety of signals that are incorporated into those decisions.
- Incorporating a source of threat intelligence, for example the IP address of a bot or malware, will keep attackers trying to acquire new resources. By incorporating details about logon (time, location, etc.) and ensuring that it matches the user's daily routine, it is difficult for an attacker to imitate, while minimizing user discomfort.

6) Reduce attack surface area

- To strengthen the security of your identity infrastructure, it is important to minimize the attack surface.
- For example, implementing Privileged Identity Management functionality minimizes the chances of compromised accounts being used by administrators or other privileged roles.
- It's also a good idea to block apps using legacy authentication protocols.
- This is important because these protocols do not support conditional access or multi-factor authentication, allowing attackers to bypass them.
- You can also reduce the impact of compromised credentials by restricting authentication access entry points to control how users access your apps and resources.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

7) Increased awareness of security

- Generates large volumes of security events and alerts from user identities and endpoint infrastructure.
- Using a SIEM system to aggregate and correlate data to detect suspicious activity and patterns can lead to potential network intrusions and events such as leaked credentials, invalid IP addresses, and access from infected devices are displayed.
- SIEM systems can be used to audit user activities, document compliance with regulatory requirements, and support forensic analysis.
- Improve monitoring of least-privileged access and manage users to access only the resources they really need.

8) End user self-diagnosis

- Users are far less reluctant to Zero Trust than many other security initiatives.
- The reason is that users are already familiar with the identity-based access used by personal devices and apps, and they want the same experience at work.
- Using the zero trust model, security organizations can use modern productivity scenarios such as mobile devices, personal devices (BYOD), and SaaS applications to satisfy users without compromising security capabilities.
- It balances security and productivity by monitoring abuse or misuse, while allowing users to reset or unlock account passwords without administrator intervention.
- Similarly, implementing self-service group management allows owners to create and manage groups themselves, eliminating the need for administrators to take action.

9) Excessive trust is dangerous

- Zero Trust is not a "big bang" initiative like implementing multifactor authentication.
- Zero Trust is completely different from the traditional network-based access model and requires the implementation of next-generation security controls to the final stage over the long term.
- It takes time to achieve your vision through small, ongoing projects.
- In the process, it is important to properly set and manage expectations. Secure support from key stakeholders and create effective communication plans throughout the project lifecycle.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

10) Proof of value in every process

- The most effective way to build a Zero Trust initiative over the long term is to demonstrate the added value of each investment.
- According to IDG's security survey, 51% of respondents said that a zero trust access model could improve the ability to protect customer data, and 46% helped provide a good and secure end-user experience.
- The ability to make the right access control decisions depends on the quality, quantity, and variety of signals that are incorporated into those decisions.
- Incorporating a source of threat intelligence, for example the IP address of a bot or malware, will keep attackers trying to acquire new resources. By incorporating details about logons (time, location, etc.) and ensuring that they match the user's daily routine, it is difficult for an attacker to imitate, while minimizing user discomfort.

05. Conclusion

The existing security model has been systematized in a form that focuses on protecting internal information assets from external intruders and security threats.

However, the recent information system environment communicates information through various points of contact such as mobile, cloud, IoT, remote work, and communication between companies. To understand the basic idea of the Zero Trust security model, you need to be aware that security threats can penetrate any device's touchpoints and in a variety of ways.

It is necessary to consider the organization's security model from the philosophy that "anyone" can become a party to security threats beyond the past blacklist-based control.

Zero Trust is not aimed at innovative improvements to the security model. Rather, it is important to gradually improve the current security system. To this end, introducing a high-cost security solution right away does not implement a zero-trust security model.

What should precede the introduction of technology is to embrace the basic concept and strategy of the zero trust security model within the organization, and the introduction of technology must be accompanied in the subsequent realization process.

Most organizational IT experts trusted the internal environmental elements and security systems. However, the zero trust security model does not guarantee reliability based on the boundary standards inside and outside the firewall. In order for the Zero Trust security model to be successfully settled, it is necessary to establish a culture within the organization that can doubt not only internal members but also environmental factors that have been trusted so far.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 4

Special Column

Digital New Deal Policy and Information Security

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

Security Consulting Team

01. Overview

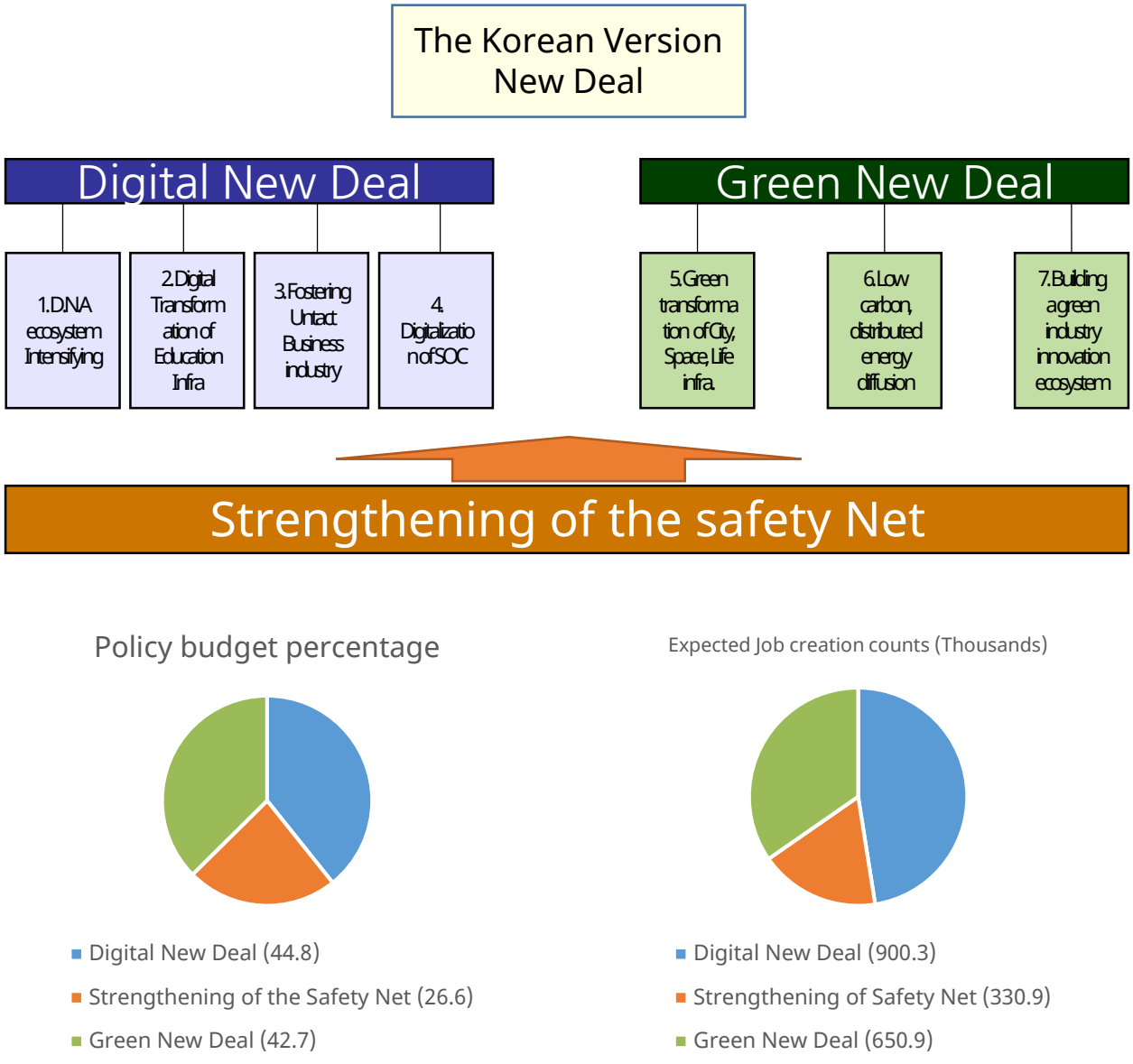
On July 14, 2020, South Korea President Moon Jae-in declared, “The Korean version of the New Deal is a 'Korea's Great Transformation' declaration to become a leading country.” “The 4th Industrial Revolution and Digital Civilization are the future of humanity that has already begun” and emphasized that “the Korean version of the New Deal is the national development strategy to lead in the current.”

The Korean version of the New Deal is composed of three pillars: the Digital New Deal, the Green New Deal, and the strengthening of the safety. Among them, the Digital New Deal is a declaration that the core of the national industry will be transformed from civil engineering to IT in accordance with the global trend of converting all industries to digital center. It is a task that must be successful for Korea, which is experiencing a recession crisis due to the impact of COVID-19, in that it is responsible for job creation and future industries through the digital new deal policy. The government aims to create approximately 1.9 million jobs by investing 160 trillion won in the Korean version of the New Deal by 2025, of which 58.2 trillion won will be invested in the Digital New Deal and create 90.3 million jobs.

The big picture of the Digital New Deal begins with data. Data generated in the public and private sectors are collected in a huge facility called 'Data Dam' based on cloud computing technology through a channel called 5G. The platform is set up. The collected data is used to create new digital businesses in the public and private sectors under the supervision of relevant ministries. This is the 'digital infrastructure' of the Korean version of the New Deal.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security



[Figure 4-1] Korea's New Deal Focus Area

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

02. Digital New Deal Goals and Tasks

The Digital New Deal is planned to be carried out in 12 tasks in four areas. The four areas are strengthening the DNA ecosystem, digital transformation of educational infrastructure, fostering untact industries, and digitalizing SOC.

1) Strengthening the DNA ecosystem

It aims to accelerate the use and convergence of data, 5G and AI across all industries to create digital new products and services and improve the productivity of our economy.

Classification	Goals and Details
① Data construction, opening, and utilization	Big data platform expansion (10 → 15 fields), public data (140,000) sequential development, AI learning data establishment '700 types (150 additional types) by 2020'
② 5G national network and cloud	Implementation of 5 5G national network pilot projects , transition to cloud-based public sector, 5 core services and industry joint cloud platform establishment, etc.
③ 5G·AI convergence	7 Mega size AI-X projects, vouchers for small and medium-sized enterprises AI solutions (14→200 cases), development of leading 5G convergence models (5 every year), KRW 1 trillion in smart Korea funds, etc.
④ K-Cyber Prevention System	Security consulting support for 2,500 small and medium-sized enterprises (300 additional), security inspection of 150 safety-related information systems such as railroad and aviation, etc.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

2) Digital transformation of education infrastructure

It aims to establish a digital infrastructure base and expand educational contents to create an on-offline convergence learning environment for elementary, middle, high school, university, and vocational training centers nationwide.

Classification	Goals and Details
⑤ Digital-based education	Established WiFi network in 200,000 classrooms nationwide, replaced 200,000 laptops exceeding the service life, and distributed 240,000 tablets (additional 80,000) for digital textbooks in pilot schools.
⑥ Strengthening online education in universities, etc.	Complete replacement of old servers and networks in 39 national universities, and installation of future education centers and remote education support centers in 10 regions

3) Fostering untact industries

It aims to lay the foundation for the growth of the related untact industry by establishing a untact infrastructure in areas close to people's lives, such as healthcare, work, and business.

Classification	Goals and Details
⑦ Digitalization of infectious diseases and care	Installation of 1,000 dedicated respiratory clinics (500 additional locations), utilizing mobile and wearable devices, and customized health care services for 300,000 people (80,000 additional people), etc.
⑧ Spreading remote work for small and medium-sized enterprises	160,000 SMEs (additional 80,000) support vouchers for remote work systems, and 1,562 video conferencing infrastructure for joint use, etc.
⑨ online business support for small business owner	Support for online exhibitions, shopping malls, and live commerce stores for 320,000 small business owners and promote subscription economy pilot projects (5,000 cases per year) Established 100,000 5G-AI-based smart stores and 10,000 smart workshops

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

4) SOC digitalization

It aims to enhance the competitiveness of related industries by digitizing the core infrastructure of SOC for safe and convenient people's life, and smartening cities and industrial complexes.

Classification	Goals and Details
⑩ Four digital safety management systems	Digitalization of major arterial roads, railways and ports, national river remote water control system, etc.
⑪ Digital innovation of urban and industrial spaces	· Establishment of CCTV-linked integrated platforms (108), spreading smart city solutions and creating pilot cities (2 locations) · Real-time safety, traffic, crime prevention management integrated monitoring center (10 locations), remote monitoring of hazardous chemicals leakage from old industrial complexes (15 locations)
⑫ Build a smart logistics system	· Small and medium-sized smart joint logistics centers (11 locations), large E-Commerce logistics complexes, and smart logistics center certification · Establishment of a smart joint logistics center (2 locations) in the harbor hinterland, an integrated platform for trading and management of public food products such as agricultural products, and an online auction platform for livestock products · Development of logistics technology such as cutting-edge delivery using robots, IoT, and big data

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

03. IT industry outlook through details of digital new deal

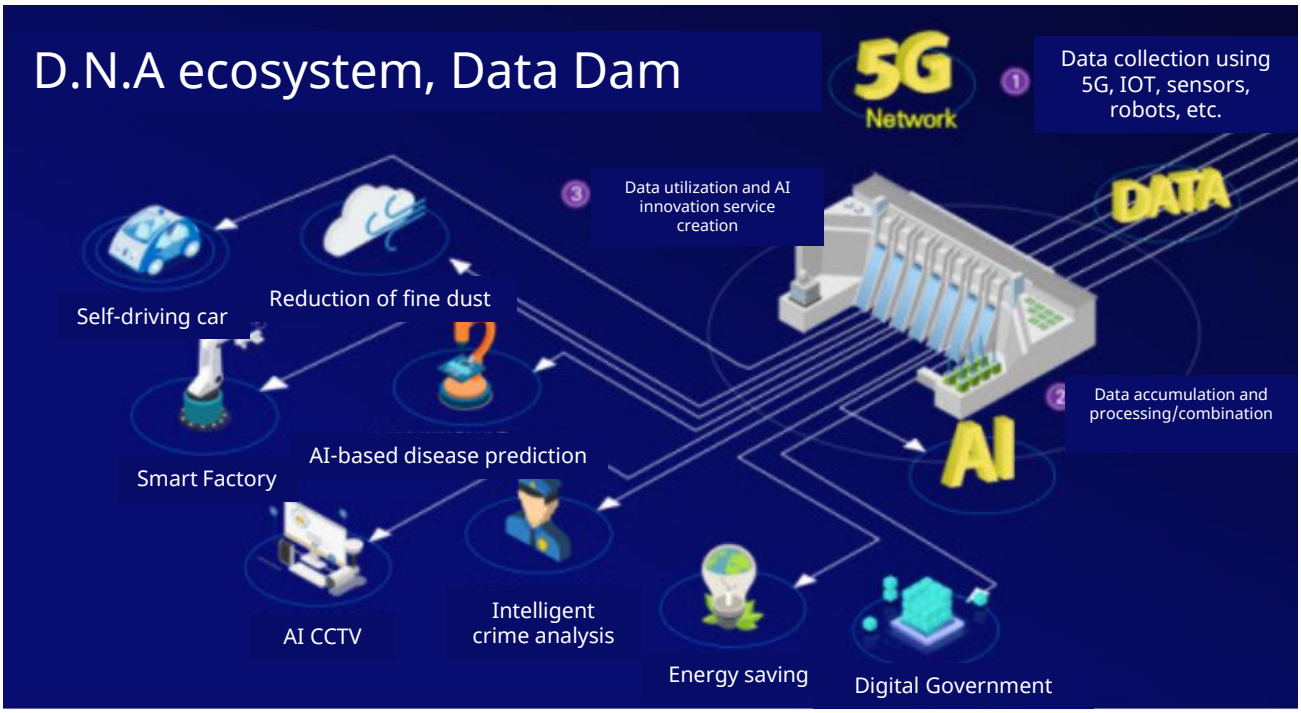
Out of the 35.1 trillion won of the 3rd additional revised budget decided at the National Assembly plenary meeting on July 3, 2020, 4.8 trillion won was confirmed for the Korean version of the New Deal, and 2.6 trillion won for the Digital New Deal.
Half of the digital New Deal project, 1.3 trillion won, will be invested in strengthening the DNA ecosystem, 0.75 trillion won for fostering non-face-to-face services and industries, and 0.45 trillion won for SOC digitization.
In the digital New Deal, the task that the assumption is to focus on is to build a “data dam” to make the most of the data that is the basis of the digital economy. Data dam refers to a system in which a public institution or private enterprise collects data, processes it, and reconstructs it into useful information.It accelerates the digital economy by reinforcing the basis for the use of big data collection, processing, and transactions, and through 5G nationwide network. This is the goal of'Data Dam' to confirm the convergence of 5G and AI across all industries.

The Digital New Deal is also significant in that the government is actively promoting digital transformation, which has been promoted mainly by private companies. The government will lead the expansion and construction of major infrastructures that are the basis of the digital economy, and a virtuous cycle structure is created in which private companies and individuals conduct creative development and research activities based on this.

This digital new deal is expected to provide a driving force to support the wave of digitalization of society, industry, and individuals accelerated by COVID-19. From the IT industry perspective, collaboration solutions such as data management and analysis such as data and AI, network technologies such as 5G and high-speed Internet, cloud services for digital-based operational efficiency, and video conferencing technologies that support untact culture and home work, And it is expected that the IT industry such as cyber security will grow.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security



[Figure 4-2] Digital New Deal-Data Dam (Source: Ministry of Science and ICT)

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

04. Security issues for digital new deal

Since Corona 19, the speed of digital conversion of companies has been very fast, and Korea also started a digital new deal project in line with this trend. For the digital New Deal policy to be successful, security must be supported above all else. This is because if a data dam is built and the dam is strong or there are gaps, the foundation of the digital new deal could be destroyed.

1) Available data and protection policy need to be supplemented

A policy to protect unidentified pseudonym data must be in place. This is because even pseudonym data that is currently unidentifiable due to poor de-identification processing or advanced analysis technology can become identifiable data depending on how the data is combined.
Benefits and data protection must be considered when using personal data. In particular, there is a lack of experts in the protection of non-identifying data in Korea, and the ability to use pseudonymous data is not high, so it is not known what security problems will occur.

There are also various opinions on the use of data with consent for the use of personal information. It is not clear to what extent it will be used when'consent to personal information activities'. There is a debate over Google's “comprehensive consent,” and the French National Commission on Freedom of Information (CNIL) levied a fine of 50 million euros (about 64 billion won) for violating the GDPR.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

2) Indiscriminate collection, sharing, and analysis environment'risk'

Companies that provide innovative services such as fintech collect customer information through various smart devices and data exchanges, analyze them in the cloud, and develop and provide personalized services. There are not many customers who can rest assured that the collected personal information is encrypted and distributed, securely de-identified, and that attackers or illegal users will not steal. There are high concerns that a large number of personal information will be collected indiscriminately, shared and neglected without encryption or equivalent protection measures.

According to the Ministry of Public Administration and Security, there were 25 reports of personal information leakage in Korea in the first half of 2019, and the scale of personal information leakage reached 5.27 million.
Once a data breach incident, companies are repeatedly targeted by attackers. Thales explains that “no company is immune to data breaches,” 37% of US distribution companies suffered from data breaches in the previous year, and 62% of companies suffered from accidents in the past.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

3) Difficulty protecting cloud IoT personal information

In the cloud/IoT environment, privacy protection issues become much more complex and difficult. Smart city applications such as e-healthcare and connected cars will collect information on daily life, and data leakage and stealing will increase in the process.

New services called fintech is provided based on various personal information. In the case of a combination of vehicle navigation and insurance companies, their driving habits, location information, and driving records collected through vehicle navigation are provided to the insurance company to calculate their insurance premiums. This means that a lot of sensitive information is shared among several companies.

In addition, the creation of data exchanges and personalization services using advanced analytics can compete, which can lead to neglect of personal information protection. While using personalization services a lot, it may not react sensitively to personal information leakage accidents.

05. Conclusion and Implications

So far, we have divided the IT environment into a safe and reliable inside and a dangerous and unreliable outside. The basic of security was a defense-oriented strategy to block threats from outside to inside, but now we have reached the limit. This is because IT infrastructure and data don't just stay inside.

Physical boundaries are meaningless, and time constraints have disappeared. It is rapidly changing into the era of Anytime, Anywhere, AnyDevice, where neither user, device nor data can guarantee absolute trust and safety. Amid these changes, the past IP-based (area-based) security model is losing its strength. It may still be meaningful in some areas, but it is bound to be inadequate as a security model for the entire IT environment.

Major countries in the world have been promoting digital economy transformation policies for 3-4 years, and the trend is accelerating further with the corona 19 as an opportunity. It is time for Korea to change too. As the Digital New Deal project includes personal information, cloud, and IoT fields, IoT and cloud-based service-type support should be strengthened, away from infrastructure construction or hardware-oriented system implementation.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

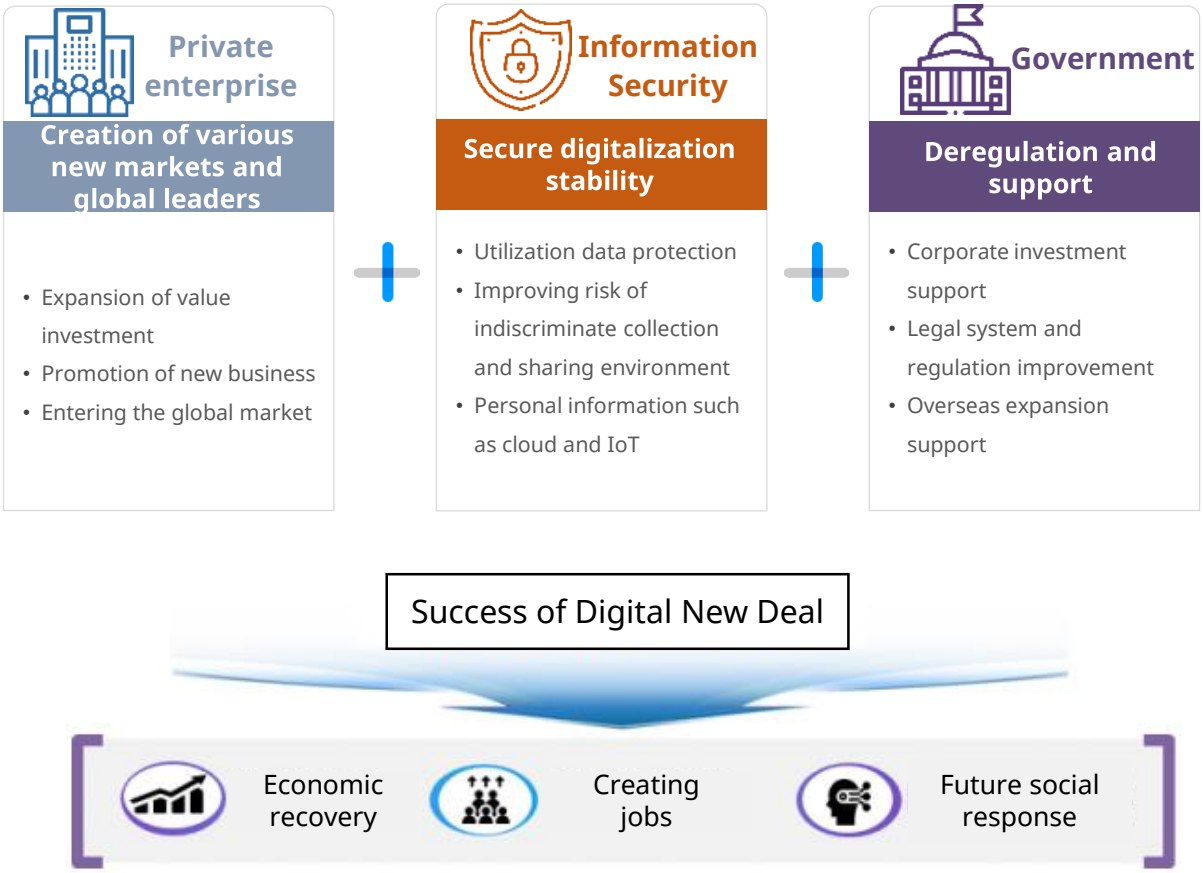
Security is essential for the success of the Digital New Deal, but investment in security is insufficient in terms of the Digital New Deal policy itself. Considering that security is inevitably applied to all of the detailed tasks of the digital new deal, such as building a digital infrastructure, fostering a untact industry, and digitizing SOC, it remains regrettable.

However, even if it is not a direct investment, policies for fostering related industries such as creating a foundation for spreading untact services and strengthening cloud and cyber safety nets are expected to have a positive effect on the security industry. In the future, the information protection market is expected to grow centering on the digital security through wired and wireless network connections and the indirect market with information protection embedded throughout the industry.

Creating a new market for information protection following digital transformation, expanding investment to secure cyber resilience led by the private sector, and creating a sustainable information protection ecosystem are the conditions for the success of the Digital New Deal.

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security



[Figure 4-3] Success of Digital New Deal (Source: Ministry of Science and ICT)

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Digital New Deal Policy and Information Security

06. Reference

[1] The 7th Emergency Economic Conference of the Korean New Deal Comprehensive Plan

[2] Focus on Korean New Deal 'Untact Digital SOC'

https://mk.co.kr/news/economy/view/2020/05/463700

[3] Digital New Deal, leading the digital transformation after COVID-19!

https://www.gov.kr/portal/ntnadmNews/2208307

[4] The Korean version of the New Deal, revitalizing the digital economy koscom

[5] Digital New Deal and Security Paradigm

http://www.cctvnews.co.kr/news/articleView.html?idxno=209753

[6] “One month to enter into force of the 3rd Data Act, companies using personal information should pay attention to huge fines”

https://weekly.donga.com/3/all/11/2178007/1

[7] 2020 National Information Protection White Paper

[8] Korea Internet & Security Agency Archives https://www.kisa.or.kr/public/laws/laws2.jsp

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 5

Focus On IGLOO Security

IGLOO SECURITY, INC. acquired 5 patents related to SIEM·Vulnerability assessment

Copyright © IGLOO Security, Inc. 2020. All rights reserved

Focus on IGLOO Security

IGLOO SECURITY, INC. acquired 5 patents related to SIEM·Vulnerability assessment

- IGLOO Security strengthens security technology competitiveness by securing intellectual property rights

[24th September 2020] IGLOO SECURITY, INC. (CEO Lee Deuk-choon, www.igloosec.com/en) announced that two SIEM (Integrated Security Control) patents that intuitively recognizes meaningful security information and three vulnerability assessments patents are acquired.

The two SIEM patents focus on implementing a visualization function to easily identify the status and location of security alerts. Through this, you can check changes in security events in the current and past times over time with a simple button click. In addition, by applying 3D simulation, it is possible to clearly recognize the location of events occurring in various information and physical security devices.

The three vulnerability assessment patents aim to increase the accuracy and efficiency of security vulnerability assessment. It is a method of transmitting and executing a compiled binary file, and assessment can be performed even when command execution is impossible. In addition, by integrating multiple security assessment criteria and determining whether a command is operating normally prior to assessment, the difficulty of applying multiple criteria can be eliminated and the occurrence of assessment errors can be prevented.

IGLOO SECURITY, INC. plans to apply the acquired patented technology to the AI (artificial intelligence) security monitoring solution SPiDER TM AI Edition (Spider TM AI Edition) and the security assessment automation solution Smart[Guard] (Smart Guard). Security personnel will be able to respond in a timely manner to breaches that may affect key IT systems and gain visibility into rapidly changing corporate security environments and attack flows.

Lee Deuk-choon, CEO of IGLOO SECURITY, said, “As the speed of untact digital conversion has accelerated, the number of attacks that cyber attackers can target has expanded. Accordingly, the importance of security technology that can quickly and accurately identify high-risk events and security vulnerabilities is expected to increase. It is expected that the ability to respond to advanced cyber infringement attempts can be enhanced through the acquired patented technology.”

Copyright ⓒ IGLOO Security, Inc. 2020. 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
© 2020 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.