pago

PAGO THREAT INTELLIGENCE REPORT 2026

The Leader in Business Technology Media
NETWORK TIMES | DATANET IT·정·보·마·당

PAGO THREAT INTELLIGENCE REPORT 2026

Table of Contents

EXECUTIVE SUMMARY

The series of large scale cyber threats that occurred throughout 2025 show that organizations must reassess their entire operating model. Attackers leverage legitimate credentials, publicly disclosed vulnerabilities and PoCs, and use AI and automation to penetrate environments at speed. In the Asia Pacific region in particular, supply chain attacks, exposed asset discovery, and reputation attacks using disinformation are emerging, forming a new axis of threat that existing defensive frameworks cannot address. As a result, organizations have reached a point where a full review of their operating model is required.

24/7 Operation and Proactive Response

As corporate IT environments become more complex, security responses have become increasingly challenging. The simultaneous expansion and interconnection of IT, OT, IoT, SaaS, cloud, and AI has blurred the boundaries between internal and external organizations, broadening the attack surface. Security Operations Centers (SOCs), tasked with responding nimbly to these changes, are struggling to overcome the limitations of event monitoring.

Security operations in the AI era must begin from scratch. AI detects initial events and assesses risk priorities. Experts analyze the context, intent, and business impact to make a final decision. The results are then automatically executed according to a playbook. Humans can verify AI analysis and feed it back into policies and playbooks, improving detection quality and response speed. In particular, 24/7 continuous operation is essential for real-time detection without security gaps, and proactive response must be strengthened through continuous threat exposure management (CTEM).

Security strategies beyond 2026 should focus on ① reducing risk before an attack and ② designing structures to quickly recover from an attack.

Security Operations Model Beyond 2026

This report addresses fundamental questions and answers about how security should function from a management, operational, and technical perspective. Based on a comprehensive analysis that cross validates real world detection and response cases handled by the PAGO MDR Center between 2023 and 2025 with global threat reports, it presents recommendations on how organizations should design their security operating models beyond 2026..

This report will help companies answer three questions:

Q1. What is the “Critical Moment” in a real world attack sequence?

Q2. From a management perspective, where should security operations focus?

Q3.What should the security operating model look like after 2026?

Through this report, we aim to establish a critical reference point for shaping security strategy beyond 2026 and to help organizations design an optimal operating model capable of effectively managing threats that are evolving at an unprecedented speed and scale due to AI.

CEO of PAGO Networks Paul Kwon

2025 GLOBAL THREAT ENVIRONMENT

The global threat landscape in 2025 was a continuation of change that couldn't be simply described as "increased attacks" or "increased threat sophistication." New attack patterns emerged, and the attack surface expanded to unexpected areas.

The most important changes are speed and cost. Cybercrime organizations are using AI and automation technologies to quickly and accurately launch targeted, customized attacks across a wide range of areas.

In particular, 2025 marks the beginning of large-scale automation of attacks, with attackers leveraging the following automation tools and techniques to enhance the effectiveness of their attacks.

- Automated large-scale authentication attempt tool
- Sophisticated scanning and PoC application automation tools
- Automatic collection of asset composition of the target company
- Detecting abnormal keys in GitHub, SaaS, and CI/CD environments
- Automatically generate disinformation and botnet-based threatening messages

Attack tools and changes in tactics and strategies

Analysis of a breach incident responded to by PAGO MDR Center in 2025 revealed that it took only 48 hours from the time an attacker gained access via a valid VPN account to the company-wide deployment of ransomware.

A global research report also warns of rapidly unfolding attacks. The CrowdStrike Global Threat Report (GTR) 2025 Analysis found that after gaining initial access, attackers took an average of 48 minutes to infiltrate and expand, with the fastest time being 51 seconds. To quickly reach target systems while easily bypassing security detection, attackers use the following methods.

▪ Unkown Threat

In 2025 threat patterns saw the emergence of new attack techniques disguised as legitimate activity. These include unusual behaviors performed under legitimate user accounts, lateral movement within the scope of normal user behavior but with rapid escalation, and unauthorized automated scripts exploiting exposed assets. These threats, which are undetectable by existing security technologies, are becoming increasingly common. Because these actions cannot be simply dismissed as attacks and blocked, a new security approach is needed that assesses risk based on the situation and context and implements appropriate measures.

▪ Theft of legitimate credentials

Theft of legitimate credentials is becoming the primary route of compromise. This is because in the cloud era where clear physical security perimeters have disappeared, identity is becoming the 'new security perimeter.' The 'Verizon Data Breach Investigations Report (DBIR) 2025' analyzes that 75-86% of breach incidents start with 'stolen accounts,' and the attack success rate on accounts not using MFA has increased 2.3 times compared to 2023.

With valid credentials, advanced intrusion techniques are unnecessary, abnormal logs are rarely generated, and rapid internal spread becomes possible early in the attack. In particular, the theft of a single cloud access key can cascade into a full compromise of SaaS, IaaS, and CI slash CD environments. This trend is also confirmed in the PAGO DeepACT Weekly Threat Intelligence Reports published throughout 2025. Attackers are focusing on gathering credentials in the early stages. More than 70% of threats detected and blocked in PAGO Networks customer environments were information stealers and remote access Trojans (RATs) used for information theft.

In particular, AgentTesla, FormBook, and Remcos RAT, which are widely distributed in the Malware-as-a-Service (MaaS) manner, were the main ones. Rather than precisely hitting specific targets, these malware spread indiscriminately through large-scale spam and phishing, and steal credentials stored in the infected system's web browser, email client, and VPN software and send them to the C2 server.

▪ Abuse of legal tools

Attackers use the **Living off the Land (LotL)** tactics to evade advanced detection technologies such as EDR This involves abusing legitimate tools, including built in system utilities, native functions, and commercial remote management software. By doing so, attackers can infiltrate environments without additional cost while avoiding security detection. As a result, organizations must invest more heavily in advanced security capabilities to identify subtle abnormal behavior originating from legitimate tools and to further mature detection and analysis.

Looking at the most damaging security incident PAGO MDR Center responded to in 2025, the attacker used legitimate administrative tools and activities commonly accepted as normal in Windows environments, such as VPN, RDP, net.exe, and PsExec. In addition, many cases were identified in which attackers installed commercial remote management tools such as AnyDesk, Chrome Remote Desktop, and TeamViewer on compromised systems, then used them as C2 channels and persistent backdoors.

Among the incidents detected by PAGO MDR Center, there were also cases that exploited vulnerabilities in the legitimate Microsoft signed driver PROCEXP152. sys. Because the activity originates from a properly signed driver, existing security solutions fail to detect the anomalous behavior.

The attacker's objective was to directly access kernel memory, remove the user mode API hooking that is essential for EDR operation at the kernel level, and forcibly terminate EDR protected processes. Through threat hunting conducted by PAGO experts, abnormal driver loading and kernel level activity were detected, allowing these advanced evasion techniques to be blocked in advance.

PAGO DeepACT 2025 Top 10 Threat TTPs

The following table shows the most frequent and highest risk behavior based TTPs detected by PAGO MDR Center in 2025 through real breach incidents and threat hunting.

Ranking	TTP	Description
1	vT1505.003: Web Shell	Remote command execution via IIS w3wp.exe or Exchange OWA processes
2	T1059.001: PowerShell	Execution of malicious scripts such as Invoke WebRequest and evasion of defensive policies
3	T1078: Valid Accounts	Legitimate system logins using stolen VPN, RDP, or Active Directory credentials
4	T1003.001: LSASS Memory	LSASS memory dumping and credential extraction using tools such as Mimikatz and NLBrute
5	T1490: Inhibit System Recovery	Deletion of volume shadow copies using tools like vssadmin which is a common ransomware precursor
6	T1548.002: UAC Bypass	Disabling UAC through registry modification of ConsentPromptBehaviorAdmin
7	T1053.005: Scheduled Task	Establishing persistence through malicious scripts or programs via Task Scheduler
8	T1021.001: Remote Desktop Protocol	Internal lateral movement using RDP
9	T1059.003 / T1087: Command Shell	sqlservr.exe launching cmd.exe to execute reconnaissance commands such as net group
10	T1218: System Binary Proxy Execution	C2 payload download using legitimate system binaries (LOLbins) such as certutil

Preemptive RDP Exposed Assets of Manufacturing Companies

From 2023 to 2025, one of the most critical exposure risks detected by PAGO MDR Center across the IT and OT environments of manufacturing, energy, and food and beverage companies was externally exposed RDP ports. PAGO MDR Center's preemptive threat response process scanned enterprise environments to identify unauthorized exposed RDP services and mitigated them before damage occurred. At Manufacturing Company A, externally exposed RDP assets were being repeatedly probed by automated scanners, but these events were classified as simple scanning and assessed as low risk. PAGO MDR Center determined that the activity was not benign scanning, blocked the RDP ports, and prevented a potential incident.

PAGO DeepACT MDR Response Process

1. Identification of exposed assets through EASM
   - Access to RDP ports from external sources at unusual times
   - Dozens of login attempts originating from the same IP range
2. Analysis of attacker intent through threat hunting
   - User agent analysis confirmed automated tool bot patterns
   - Verification that the same attacker group was active across other industries
3. Risk reclassification during the validation phase
   - Determined to be credential based initial intrusion attempts rather than simple scanning
   - Priority elevated
4. Automated blocking and rule based isolation
   - Temporary blocking of RDP ports
   - Redefinition of access based on whitelisting
   - Firewall policy updates

Through PAGO MDR's preemptive response, the attacker was prevented from reaching the authentication stage, and the threat was contained without any impact on the company's production facilities or manufacturing systems.

▪ Shadow AI·Shadow IT

As AI usage surges, the threat of shadow AI, including unauthorized AI tools, automation scripts, and personal AI apps, is growing significantly. AI bots that integrate with external SaaS platforms are also prone to management blind spots.

Potential threats from Shadow AI include: ▲external API key leaks ▲exposure of sensitive information contained in training data ▲misuse of LLM-based automation scripts ▲elevation of account privileges through unauthorized connections between SaaS. In particular, when AI scripts automatically connect to SaaS and transmit sensitive data while disguising it as a normal workflow, it is difficult to detect because it appears as legitimate activity in logs.

Shadow IT is expanding significantly as various digital assets, including shadow AI, are being used without the approval of the management organization. Vulnerabilities, incorrect configurations, and data and credentials left in shadow IT become useful tools for easy infiltration.

▪ Expanding attack surface

Shadow IT, misconfigurations, unpatched vulnerabilities, and abandoned account information and credentials create attack surfaces for attackers. As businesses expand, various types of IT resources are used, and remote and hybrid work environments are introduced, management blind spots increase and the attack surface expands. Attackers can easily a single scan can compromise a target system. PAGO MDR Center response cases also demonstrate numerous instances where threats originated from attack surfaces that could have been effectivelymanaged.

Key exposure points revealed in PAGO incident response data include:

- RDP ports directly exposed to the Internet are targets

for brute force attacks

- Unpatched MS Exchange servers or insecure web applications are exploited as launch pads for webshell uploads and internal reconnaissance

- Weak, easily guessed database passwords grant attackers immediate remote code execution (RCE) privileges

▪ Vulnerable supply chain

In 2025, supply chain risk expanded globally across all industries. Rather than precisely targeting vulnerabilities in a specific system, attackers are now infiltrating weak points within the supply chain and then spreading through the entire ecosystem, causing far broader damage.

According to the IBM 2025 Cost of a Data Breach report, the average cost of secondary damage caused through supply chain attacks is about 30% higher than the initial breach. In practice, between 2024 and 2025, the APAC region saw a sharp increase in secondary propagation attacks leveraging exposed SaaS accounts, stolen tokens, and abuse of cloud IAM privileges. The supply chain threat is particularly severe in APAC due to two key factors.:

- High reliance on small and mid sized **MSPs, MSIs, and SaaS resellers.**

- Complex environments where **IT and OT**, headquarters and branch offices, and internal and external systems are tightly intertwined.

Increasing attacker yield

Cybercrime organizations seek to invest time and money efficiently to achieve high profits, so they look for organizations that are easier to infiltrate and achieve their goals. The manufacturing industry in the APAC region is a favorite target for attackers, and its security measures are weak compared to the IT and OT levels. It is relatively easy to penetrate and yields high profits.

▪ Attacks targeting profitable manufacturing industries

While the manufacturing industry is actively adopting cutting-edge technologies and achieving AI and cloud innovation, it still operates decades-old legacy equipment. This older equipment is highly vulnerable to security breaches due to inadequate security patches and firmware updates. Furthermore, the adoption of AI and cloud computing without additional security measures is significantly expanding the attack surface by increasing external connectivity.

The APAC region, including South Korea, is home to a concentration of cutting-edge semiconductor and automobile manufacturers. Their AI and cloud innovations are being pursued without sufficient security considerations, creating an environment highly vulnerable to attacks. Furthermore, the rapid adoption of cloud computing in the APAC region is leading to a growing frequency of attacks exploiting vulnerabilities in the cloud, such as security misconfigurations, configuration errors, and poorly managed assets. According to PAGO MDR Center data, the combined cost of cloud breaches stemming from misconfigurations in APAC companies is significantly higher than in the United States.

▪ APAC region with high supply chain damage

Because the APAC region lies at the heart of the global supply chain ecosystem, attacking manufacturers in this region could jeopardize the entire global supply chain. For example, when manufacturing plants in China shut down during COVID-19, supply chains across all industries worldwide ground to a halt.

Attackers, aware of this reality, are shifting their attack targets from the US to the APAC region. While the APAC manufacturing industry is experiencing rapid growth in IT-OT convergence, its security maturity remains low, and even simple attack techniques can cause widespread supply chain damage. Small and medium-sized supply chain operators, in particular, face insufficient security, and significant differences in security quality across countries make them even more vulnerable to attacks. In fact, 60% of the targeted attacks detected by the PAGO MDR Center were aimed at this sector, highlighting the urgent need for security measures for manufacturers in the APAC region.

▪ Exploitation of complex regulations and misinformation

As cyberattacks threaten industry and national security, many countries around the world are responding by strengthening cybersecurity regulations.

In the case of serious incidents, massive fines and penalties may be imposed. Under the European Union General Data Protection Regulation (GDPR), fines can reach 4% of annual global revenue, while the NIS2 Directive imposes penalties of 2%. Korea's Personal Information Protection Act allows administrative fines of up to 3%.

In the United States, if a publicly listed company fails to report a breach to the Securities and Exchange Commission (SEC) after becoming aware of it, it may even face delisting. As a result, attackers are earning higher profits through a new method known as regulation extortion. After a successful intrusion, attackers threaten victim organizations by stating that failure to properly report the breach to relevant authorities will result in massive fines, and demand payment to cover up the incident.

Not only companies with low awareness of regulations, but even those with relatively strong regulatory response capabilities are being drawn into such threats. In particular, some companies operating overseas comply with attacker demands because they do not accurately understand the regulations of the countries in which they operate.

Attacks that damage reputation by using false information are also becoming more frequent. Using social media and the internet, attackers falsely disclose large scale theft of confidential or customer information or spread other false claims to undermine corporate trust. As AI has removed language and cultural barriers, Asian countries that use distinct languages and scripts are also suffering damage from disinformation.

Evolving the Attack Ecosystem to Maximize Profits

Attackers are constantly improving their attack tactics, strategies, tools, and ecosystems to maximize profits. They employ even rudimentary techniques, employing sophisticated methods to evade security detection and exploiting victim psychology to maximize profits.

Before encrypting the data, they first leak it, threaten to make it public, and delete cloud backups, giving the victim organization no time to respond and forcing them to negotiate. They also inform the victimized organization of its sales, whether it has cyber insurance, and the amount of damage it will incur in case of regulations and lawsuits, and then offer to cover up the damage for a lower cost.

However, complying with the attacker's demands does not guarantee complete recovery, and the rate of re-attack is very high. According to a Cybereason survey, 78% of organizations that paid a ransom were attacked a second time, and 63% of those organizations received a higher ransom the second time. In 36% of these second attacks, the attackers were the same. Analysis also showed that only 47% of organizations that paid were able to recover without damage.

These attack methods render the traditional response strategy of "maintaining strong backup systems for ransomware recovery" ineffective. Affected organizations must bear not only the direct damage caused by ransomware, but also customer attrition, reputational harm, regulatory risk, and potential class action lawsuits from customers.

Changes in attack patterns, not attack techniques

2025 marked the beginning of a fundamental shift in cyber threat patterns. Attack speeds accelerated dramatically, while both large scale mass attacks and highly sophisticated targeted attacks emerged simultaneously across the threat landscape. Based on PAGO MDR Center detections and global threat reports, the key messages are as follows:

▪ Attacks are not only more intelligent, they are also faster. ▪ The attack surface is expanding explosively in areas we did not previously recognize.

▪ Credential theft is becoming the primary vector for all attacks.

▪ Supply chains target smaller organizations first, then spread to larger ones.

▪ Shadow AI has emerged as a new attack surface.

▪ Ransomware is shifting from encryption focused attacks to reputation focused extortion.

▪ The gap between automated attacks and manual response continues to widen.

3 YEARS OF INSIGHT (2023-2025)

The global pandemic, which lasted 3 years and 4 months from January 2020 to May 2023, cfundamentally reshaped the cyber threat environment. As security perimeters extended into the cloud, the notion of a clearly defined internal network largely disappeared. With corporate assets increasingly connected to cloud platforms, MSPs, and other third parties, attack exposure grew, and the risk of breaches driven by authorization and configuration errors rose sharply within complex hybrid environments.

AI innovation accelerated after the pandemic, driving rapid changes in the threat environment. As Agentic-AI and AI-powered applications spread, the number of AI assets operating outside an organization's direct control has increased sharply. At the same time, security teams face a dual burden. They must maintain legacy security systems while adapting to an evolving risk environment. Despite the deep interconnection between IT, OT, and cloud systems, security operations remain fragmented across separate tools and processes. This fragmentation limits visibility and makes it difficult to effectively manage the full attack chain, from initial intrusion to lateral expansion.

Limitations of traditional detection techniques

An analysis of the threat trends detected through PAGO MDR Center over the past 3 years and the research reports of global experts leads to the conclusion that the focus should be on 'methods, not technology.'

However, current SOCs are limited to simple event analysis and notification processing, which limits their ability to block attacks that bypass security and unfold at high speed. The limitations of the current SOC are:

▪ Identity-based attacks that bypass EDR detection

Identity-based attacks go beyond simple account takeovers and encompass all attacks that exploit identity, including unauthorized privilege escalation, session hijacking, token reuse, and SaaS login exploits. Attacks are increasingly focused on identity, which has become the new security perimeter. The evolution of identity-related attacks from 2023 to 2025 is as follows:

- Approximately 2.8x increase in identity-based attack-related events.
- Attempts to exploit cloud and SaaS access rights increased 2.5 times.
- Internal movement attempts disguised as legitimate accounts increased 70%.

Identity abuse attacks are a common method of bypassing EDR. While EDR excels at detecting endpoint threats, it fails to prevent access using legitimate accounts. Therefore, by 2026, **Identity Threat Detection and Response (ITDR)**, permission-based risk scoring, and SaaS access pattern analysis will become essential operational elements.

▪ Limitations of signature- and pattern-based detection

Signature and pattern-based detection detects unknown threats. Examples of unknown threats most frequently detected are:

- Events that appear to be normal behavior but have a

Unknown threat exploiting a normal user account

In the first half of 2025, PAGO MDR Center detected abnormal behavior in a normal user account at a financial service company. This behavior proceeded in a different situation from the work pattern that the user has been performing, but it was not detected with a signature-based security solution.

DeepACT MDR Response Process

1. Context-Driven Detection
- Detect specific file access attempts that were logged in to a normal location but did not appear in existing business patterns
- Detect 'out of normal working hours activity' on the account

2. Validation of past behavior of normal users
- Analysis of behavior patterns for 30 days
- Abnormal File Download Path Found

3. Threat Hunting Starts
- Sample file hash analysis
- Investigate associations with other user accounts
- Navigating the trace of remote command execution

4. Initial Automatic Quarantine → Security Team Collaboration → Final Cleanup
- Blocking access to suspicious files
- Lock account temporarily
- Joint response from SecOps and IR team

As a result of the analysis, it was confirmed that the attacker attempted to access important internal data by stealing a normal user account. The attacker could not access the data because the PAGO DeepACT MDR blocked abnormal behavior in the initial stage.
This unknown threat cannot be identified only by detection technology. It can be successfully acted on through MDR, which combines context + hunting + immediate response.

different **context;**

- Unusual login attempts performed with a legitimate user account;
- Attacks with unsophisticated but fast internal movement;
- Unauthorized automated scripts exploiting exposed assets

Combining data collected by PAGO Networks and CrowdStrike's investigation, the reasons for the increase in unknown threats can be summarized as follows.

- **Automated attack proliferation**: PoC(Proof of Concept)-based attack scripts are distributed in large quantities, individual attack patterns are not consistent and show 'atypical behavior'.
- **Shadow AI and unmanaged automation spread:** AI-based scripts and SaaS-to-automated connection tools disguise themselves as normal behavior, making detection based on file hashing and pattern matching difficult.
- **Increase in identity-based threats:** Attacks using legitimate accounts evade signature- and pattern-based detection.

▪ Shortened TTE (Time-to-Exploit)

All systems and applications have vulnerabilities. Therefore, security researchers and white hat hackers search for unknown vulnerabilities, test their exploitability, and publish **Proofs of Concept** (PoC) of their processes and results to the community. This is a vital activity that helps other researchers and developers verify and quickly distribute security patches and advisories.

The problem is that PoCs significantly reduce the cost and time required for attackers to develop exploits. Once a PoC is published, attackers immediately begin attempting to exploit it.

According to a recent analysis of infringement cases by domestic and foreign security industries and major security companies, the time taken from the release of PoC to attempting to exploit is clearly reduced to weeks, days, or hours. Cloudflare also disclosed an accident that took only 22 minutes to launch an attack after the release of PoC.

Shorter TTEs allow attackers to exploit vulnerabilities before security teams can even understand patch announcements, increasing the frequency and success rate of zero-day exploits.

To quickly respond to vulnerabilities, security organizations are leveraging AI-based real-time vulnerability scanners. However, identifying vulnerable elements within massive IT systems can be challenging. Furthermore, vulnerable elements are often compressed or fragmented within the system, often undetected.

Patching can introduce additional issues, so it's crucial to thoroughly review and test it before applying patches. For example, WAN-facing services often require near-real-time patching, but administrators concerned about service continuity may be reluctant to implement real-time patching.

Security, which must consider business continuity, clearly faces limitations in speeding up vulnerability response. However, criminals can use automated vulnerability detection tools to identify and attack vulnerable systems in near real-time. Commercial penetration testing tools like Metasploit allow for effective attacks without the need to develop separate vulnerability scanning tools.

To address these issues, patch management needs to be elevated from an "operational task" to a "risk reduction strategy". Organizations need to assess the exploitability of newly disclosed vulnerabilities and remediate them based on priority, while continuously reducing risk by identifying and eliminating unresolved vulnerabilities and exposed attack surfaces through an ongoing CTEM approach.

Incident-to-Breach Ratio (IB Ratio)

When we synthesize global threat intelligence and actual incident response cases of PAGO MDR Center, there are continuous reports of cases where damage is caused due to delayed response even though detection has occurred. This is called the **'Incident-to-Breach Ratio (IB Ratio)'**, and it is calculated as ▲detection but response is late or ▲ insufficient context of detected information.

In fact, many incidents detected by PAGO MDR Center resulted in actual breaches due to operational gaps, procedural delays, and approval process issues, despite initial alerts being issued. This stems from the following limitations of traditional SOCs:

- **Event-Centric Architecture:** Difficulty in detecting unknown threats and identity-based attacks due to reliance on rules and signatures;
- **Alert Handling Process:** Alert → ticket creation → analysis → customer notification → follow up actions, resulting in a response that lags far behind the speed of the attack
- **Partial Operation:** Even with 24/7 monitoring in place, continuous decision making, isolation, and response are often not possible.
- **Separate functional organizations:** Monitoring, breach response, and threat intelligence are separated, resulting in delays between decision-making and execution.

Therefore, simply 'detecting' threats is not enough; a system that verifies and responds to detected threats in real time must be in place.

Efficiency of security investments

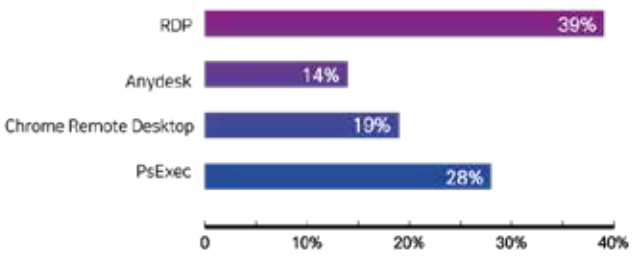
While corporate investments to combat cyber threats continue to increase, they are failing to reduce the costs of breaches. Forrester projects that global cybersecurity spending will increase 13.1%, from $154.6 billion in 2024 to $174.8 billion in 2025, and that it will continue to grow at double-digit rates each year, reaching $302.5 billion in 2029.

These investments are not resulting in lower costs of breach. The average cost of a breach, as analyzed by IBM CODB, is expected to be $4.44 million in 2025, a 9% decrease from $4.88 million in 2024, but similar to the $4.45 million in 2023.

In the APAC region in particular, the cost of a breach is 22% higher than in the US due to a combination of issues such as supply chain disruption, regulatory risks, and cloud configuration errors. PAGO Networks analyzes the reasons why it cannot lower the cost of infringement:.

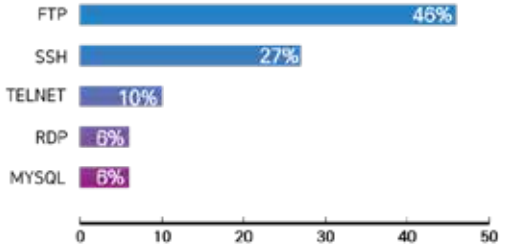
-The response delay incurs a higher cost than the initial detection failure.

Figure 1 Legitimate remote access tools used in attacks



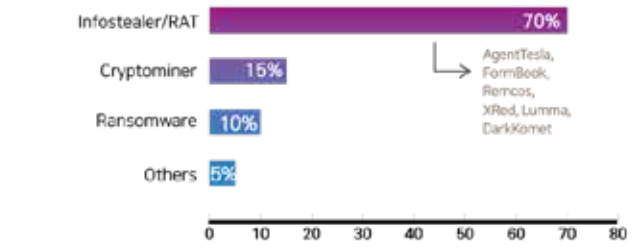
(Source: PAGO DeepACT Threat Intelligence)

Figure 2 Targeted attack surface



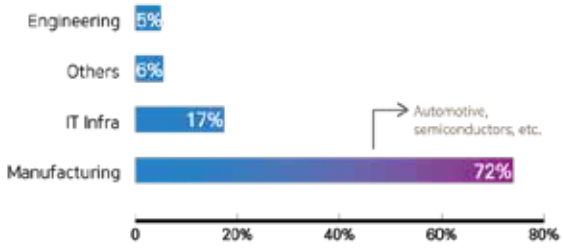
(Source: PAGO DeepACT CTEM Database)

Figure 3 Types of detected malicious tools



(Source: PAGO DeepACT Threat Intelligence)

Figure 4 Distribution of security incidents by industry



(Source: PAGO DeepACT Compromise Report)

Revitalizing the Underground Economy through the Division of Labor

The underground market is becoming increasingly specialized, streamlining the overall ecosystem and increasing profitability. An analysis of 2025 threat intelligence data from PAGO Networks shows that attacks are no longer executed end to end by a single group. In real world cases, PAGO Networks identified a strong causal relationship between large scale infostealer activity and the use of "Valid Accounts" observed during incident response in 2025. This serves as clear evidence of a highly specialized underground ecosystem. Within this structure, attack groups are further professionalizing and scaling ransomware operations.

Today's underground market consists of multiple collaborating groups, including those specializing in credential theft through "Infostealers," those focused on initial intrusion and access resale as "Initial Access Brokers," and those dedicated to ransomware deployment through "RaaS (Ransomware as a Service)." Together, these groups form a highly organized, profit sharing ecosystem built on division of labor.

A highly specialized attack ecosystem

The specialized attack ecosystem operates through 4 stages:

- **Credential Harvesting:** Infostealers such as AgentTesla and Lumma Stealer distribute these credentials to unspecified numbers of people through mass phishing emails.
- **Access Brokerage:** Countless stolen RDP, VPN, and AD credentials are commercialized and sold on dark web marketplaces by 'Initial Access Brokers.'
- **Access Acquisition:** RaaS operators such as LockBit purchase valid internal access rights to specific companies (e.g., manufacturing, IT infrastructure).
- **Intrusion & Monetization:** RaaS groups use the purchased valid accounts to log into the target company normally. This completely bypasses traditional firewalls and intrusion detection systems (IDS), making it appear as normal activity from internal users. They then carry out the final attack, such as deleting shadow copies and deploying ransomware.

- The spread of damage is fast in cloud and SaaS environments.
- Reputation and legal dispute costs account for an increasing proportion of the total cost.
- After the data is leaked, the customer dropout rate **(Attrition Rate)** increases repeatedly.

To reduce the cost of breaches, one thing that must be improved is **"operational speed"**. Operational speed varies depending on the degree of integration of the following three elements.

1. **Detection Speed:** Improved detection speed through automation using AI-based correlation analysis and normalization.
2. **Decision Speed:** Improve decision speed by combining intelligence that can verify the level of detected threats with the capabilities of expert analysts.
3. **Containment Speed:** Rapid containment of certain threats through 24/7 operating systems and automated operating procedures.

Changing the Security Operations Model

In 2026, organizations will face challenges not only from increasingly sophisticated attack techniques, but also from complex operating environments and the inability to keep pace with accelerating attack speeds. As the time from initial intrusion to lateral expansion continues to shrink, the concept of a security **"Golden Time"** is disappearing, and identifying the **"Critical Moment"** to stop an attack is becoming increasingly difficult. As a result, security operations are evolving beyond the detection and removal of individual events and are being elevated as a core component of **"Business Resilience Metrics"**.

To position security as a management metric, organizations must establish KPIs that directly contribute to improving business sustainability. The security KPIs that can serve as management metrics are as follows:

▪ **MTTD(Mean Time to Detect):** The time it takes to detect the initial threat signal and maintain the security operating system in a detectable state. This is an indicator showing whether the MTTD is being achieved. Recently, AI-based correlation analysis and abnormal behavior detection technologies have significantly shortened the MTTD.

▪ **MTTA(Mean Time to Acknowledge):** This refers to the time it takes for an alert to be recognized as a real threat. MTTA is determined by 24/7 operations, the maturity of the alert prioritization system, and the verification process. A structure that enables real-time assessment within the operating system can shorten MTTA.

▪ **MTTR(Mean Time to Respond):** The time it takes from detection to response and isolation, it's an indicator of resilience. MTTR can be shortened by establishing an operational system that integrates the detection, assessment, and isolation processes into a single structure, rather than separating them. Furthermore, mature operational practices, such as a 24/7 response organization, a high level of automation, and systems that enable immediate assessment and decision-making, can shorten MTTR, rather than relying solely on technology and performance.

▪ **Containment Ratio:** The percentage of initial penetration attempts that are successfully blocked. A high Containment Ratio indicates that the organization has automated defenses in place throughout the attack process.

▪ **Exposure Reduction Index:** This indicator shows how much the attack surface has been reduced through Continuous Threat Exposure Management (CTEM)-based operations. It demonstrates whether threats are managed proactively, rather than reactively, and reflects the security operations philosophy and process maturity.

Prerequisites for Mature Security Operations

For over a decade, SOCs have been considered "operational security organizations", continuously evolving through the addition of advanced defense technologies. However, SOCs employ a linear detection and response model that involves alert monitoring, standardized event analysis, ticketing, and follow-up requests. This limits their

Attempted breach based on leaked credentials - quarantined within 24 minutes.

PAGO MDR Center detected that in late 2024, an attacker attempted to access the cloud console of a domestic SaaS company using a leaked account. If detected by a general security control service, the average response time would be several hours because it would have to go through the process of log-based detection, ticket issuance, customer notification, approval, and response.
However, PAGO MDR Center completed the process from login attempt detection to containment within 24 minutes. This significantly shortened the global mean time to response (MTTR) of 3-6 hours, completely blocking account privilege escalation and lateral movement attempts and preventing damage.

PAGO DeepACT MDR Response Process

1. Detecting abnormal patterns in login events
   - Log in from a region other than the normal user's country;
   - Explore console features independent of account permissions;
   - Repeat session token validation;
2. Eliminate false positives in the validation phase
   - Comparison of normal automation scripts and patterns;
   - Verification of inconsistencies with the user's work pattern;
3. Analyst's immediate judgment
   - Judging by credential stuffing;
   - Quick approval after assessing the risk of account hijacking;
4. Automatic quarantine
   - Force terminate account session;
   - Forced MFA re-registration;
   - Automatically block dangerous IPs;
   - API Key Invalidation;

What this case demonstrates is that credential attacks are not prevented by technology, but by "speed of judgment." The combination of MDR verification, automated response, and expert judgment allowed for the early containment of the attack.

ability to block recent attacks, which utilize a wide range of battlefields and simultaneously engage in multiple intrusion activities. A defense strategy that takes the entire attack lifecycle into account is necessary. Gartner analyzes that **"we have reached a critical turning point in the speed of defense operations"**, meaning that the entire structure of security operations, including security operations processes, the speed of human intervention, the level of automation, and the risk decision-making system, must be redesigned.

▪ Automation and 24/7 security operations

After 2025, security strategies are increasingly focused on "how to design a structural balance between operational costs and loss costs." In particular, ensuring that security investment leads to minimized breach impact requires "highly mature, automated 24/7 security operations". According to research by IBM and Gartner, organizations that have matured their automated 24/7 security operations save an average of $2.2 million. This is the sum of:

- Reduced downtime
- Reduce productivity loss
- Reduced regulatory fines
- Preventing cloud resource overflow
- Minimize customer churn
- Reduced accident investigation costs
- Reduce legal response costs

▪ The misconception about '24/7'

Attackers are using automation to rapidly and widely infiltrate vast areas, but defenders are unable to keep up with the attackers' speed and scope, and are largely relying on manual responses. This structure, no matter how much security investment is made, will not mitigate the damage.

Security control services can only respond to detected events by notifying security personnel. Event analysis, impact assessment, and rapid response must be directly performed by the security organization. Even a 24-hour SOC cannot immediately respond to high-risk events outside of security personnel's working hours.

Problem 1: Mistaking notification monitoring for 24/7

Most 'alert monitoring' is 24 hours a day, but judgment, quarantine, and action are taken during working hours from 9:00 to 18:00.

Problem 2: Ticket-based operating structure

In a structure where a ticket is created, approved by the customer, and then decided again by the internal security team, MTTR will never be reduced.

Problem 3: Limitations of the Event-Driven SOC Model

Event-driven SOCs only detect 'events that violate established rules,' making it difficult to detect unknown threats and identity-based attacks.

Problem 4: Misinterpreting labor shortages as lack of automation.

Many organizations understand automation as "detection automation," but true automation is "isolation and blocking automation.

▪ Meaning of MTTR reduction

Because many attacks complete lateral movement and data theft within one hour of initial intrusion, security teams must detect, assess, and isolate threats within that window. As seen in attack cases detected by CrowdStrike, where intrusion to expansion occurs in under a minute, critical decisions must be made in "seconds".

Reducing MTTR is not only a technical metric from a CISO perspective. From the CEO and CFO viewpoint, it is a key indicator directly tied to reducing financial loss. According to research by IBM, a 30% reduction in MTTR leads to an average 49% reduction in breach costs.

Breach costs include not only direct damages, but also losses that can be avoided through rapid response.

✓ Direct costs resulting from a security breach

- Costs incurred due to delayed response
- Damage caused by data leaks
- System isolation downtime
- OT and manufacturing disruption costs
- Legal response costs
- Customer churn and reputational damage

✓ Costs that can be reduced through rapid response

- Early containment of breach scope
- Minimize recovery costs
- Reduced regulatory reporting burden
- Limited revenue loss

This shows that a SOC must not only reduce MTTR itself, but also raise the maturity of its response processes, capabilities, and operating model. In practice, incident response cases handled by PAGO MDR Center show that organizations that consistently reduce MTTR share the following common characteristics:

- Detection, decision making, and isolation integrated into a single continuous flow;
- Fully operational 24/7 response model
- High level of automation in initial analysis and isolation
- Built in processes for alert validation and prioritization

▪ Resilience-centered security operations

An analysis of CEO focused cyber threat surveys conducted by security firms and institutions between 2023 and 2025 reveals a common conclusion: the more critical issue was not failing to stop the attack, but failing to recover quickly. PAGO MDR incident response cases similarly show that organizations that shortened detection and response times significantly reduced breach costs.

Security is no longer a challenge confined to technical teams. It has become a core factor in strengthening overall business resilience. From an executive perspective, "resilience" goes beyond rapidly identifying and stopping an attack. It also includes minimizing system downtime during incidents, restoring operations quickly, protecting customer experience and brand trust, and reducing recovery costs and legal risk. All of these elements must now be reflected in security operations.

REDESIGNING SECURITY OPERATIONS

Threat data from the past 3 years and analyses of domestic and global threat trends clearly show that the center of security strategy is shifting from SOC to MDR. This reflects changes in attack patterns, operating environments, and executive decision making, and indicates the need to redesign security strategies around MDR, taking into account total breach costs, cyber risk, and operational speed.

MDR is structurally superior to traditional SOC in the following ways:

▪ **'Operational unification' from detection, judgment, response, and isolation:** Traditional SOCs have separate detection, judgment, response, and isolation functions, but MDR integrates them to enable quick and accurate decision-making and action.

▪ **24/7 response:** While traditional SOCs focus on simple monitoring, MDR can respond to real threats, enabling uninterrupted security measures.

▪ **Incorporate threat hunting into your core processes:** Traditional SOCs are limited to event-driven, limited responses. In contrast, MDR can identify ongoing attacks and even unknown threats through threat hunting, enabling precise action based on solid evidence and signals.

▪ **Respond before a breach occurs by utilizing CTEM:** While traditional SOCs respond after a breach, MDR can proactively respond by leveraging CTEM to identify all potential points of compromise.

Fake MDR flood

Even among global companies that have invested heavily in security, a series of large-scale security incidents have led to a growing awareness of the need for fundamental improvements to existing security operations. In particular, with the proven effectiveness of MDR in improving security operations, full-scale adoption began in 2025.

However, some services promote themselves as "MDR" when their primary function is merely monitoring and rerouting notifications, creating market confusion. These services rely on a small number of point security solutions to relay events, undermining the value of true MDR. Fake MDRs exhibit the following characteristics:

- Delivers detection events only, leaving risk assessment to the customer;
- Relies on unvalidated, ticket based processes;
- Does not provide threat hunting;
- Does not offer automated response or isolation services;
- Lacks sufficient 24/7 detection and response personnel;

A true MDR requires a foundation for rapid and accurate threat detection and immediate action across the entire enterprise. Based on internal threat intelligence and external intelligence sources, validated experts must analyze detected threats, respond based on the business context and impact, and be held accountable for the consequences.

MDR Requirements

A mature MDR possesses the expertise, accountability, and reliability to act on behalf of a customer's SOC. Leveraging a mature MDR allows security organizations to focus on "essential security"-developing and implementing a business-focused security strategy - while mitigating and improving overall management risks.

The capabilities that a mature MDR must possess are as follows:

▪ Threat hunting and verification

Threat hunting is an essential activity for preventing damage. Expert hunters directly identify and analyze breaches undetected by existing security solutions in customer environments. They assess their impact on actual business and potential exploits, enabling early response to even unknown threats.

Looking at the core TTPs that PAGO MDR Center determined to be 'real threats' and reported to customers, most incidents were not low-risk file-based alerts, but rather high-risk breaches that occurred when an attacker had already infiltrated the system.

This clearly demonstrates the need for threat hunting, which is not an optional 'advanced feature' in MDR, but rather an essential strategy for 'securing golden time.'

Not all evidence identified through threat hunting leads to actual impact, which makes a validation process essential. By combining the full attack context with threat intelligence data, organizations can accurately assess real exploitability and threat severity. This information is provided as data for "Decision by Signal," enabling "precise" response decisions..

Improvements achieved through PAGO MDR Center's verification based threat hunting include the following.:

- Validation based filtering reduced false positives by 31% to 46%.
- Threat hunting based detection proactively blocked 20% to 30% of initial intrusions.
- Integrating validation and hunting shortened MTTR by 38%.
- Probability of blocking lateral movement increased by 1.7×

▪ Collaboration between experts and AI

As cyberattacks leverage AI to accelerate and scale, current security operations are embedding AI in SIEMs to improve detection accuracy and speed. Furthermore, advanced MDR systems take automation to the next level with advanced AI SIEMs.

The role of AI-SIEM in MDR is as follows:

- Automated analysis of log context.
- Reclassification of unknown threat signals.
- Integration of SaaS, cloud, and identity events
- Containment Automation triggers.
- Threat intelligence based risk scoring.

While AI-SIEM can automate the process of event normalization, classification, and risk assessment, not all threats can be addressed by AI. In particular, AI alone cannot address previously undetected, unknown threats, identity-based attacks leveraging legitimate credentials, shadow AI, and emerging AI-driven threats.

Therefore, Augmented AI, where experts and AI collaborate, becomes a prerequisite for MDR. Augmented AI serves as the operational backbone that supports the enterprise security operating model and becomes the fundamental operational engine of MDR.

▪ Managing ongoing threat exposure

Continuous Threat Exposure Management (CTEM) is a proactive security strategy that identifies, verifies, prioritizes, and remediates attack surfaces across an organization. Attack surfaces include vulnerabilities, misconfigurations, and management mismanagement across assets, environments, applications, and identities that attackers can exploit.

The CTEM model defined by Gartner includes the following stages: ▲Scope definition (Scoping), ▲Exposure assessment (Discovery), ▲Exposure prioritization (Prioritization), ▲Validation-based risk assessment (Validation), and ▲Risk mitigation (Remediation). Integrating the CTEM process into MDR will shift security operations from being centered on 'detection' to 'preemptive response'.

It's crucial to include ITDR here. ITDR is a technology that detects and responds to identity-related threats such as account takeover, credential stuffing, and privilege escalation. It's a key element in transitioning from endpoint-centric detection to identity-centric detection and response strategies.

▪ Threat Intelligence

Threat intelligence is a service that provides real-time insight into the latest attack strategies, patterns, and tools. It detects threats that existing tools may miss, prioritizes potential vulnerabilities, and enables proactive hunting to minimize damage. Combining threat intelligence with expert insights in MDR allows organizations to identify potential threats and reduce false positives.

A mature MDR possesses the analytical capabilities to issue regular threat intelligence reports based on actual operational data. By providing the latest threat trends and essential threat information for customers and industries, it contributes to improving the overall security of society.

▪ 24/7 Operation and Proactive Response

Recently, attackers have been launching attacks at night and on weekends, when security personnel have difficulty responding immediately. In an actual case that occurred at a customer site, a brute-force attack was launched at 8:43 PM on Saturday, and an internal account was successfully hijacked at 9:06 PM. At 3:45 AM on Sunday, an RCE attack was launched via sqlservr.exe, and at 11:35 AM on Sunday, a UAC bypass and backdoor account were created. Finally, at 10:51 PM on Sunday, internal reconnaissance via a web shell was initiated. Even though these threats occurred throughout the weekend, security personnel were only able to recognize and respond after arriving at work on Monday morning because it was a non-working day.

In another case, the breach was only discovered when the attacker shut down the system or sent a threatening

LotL Detection: The Core of Threat Hunting

PAGO Networks' threat hunting experts focus on identifying "suspicious behavior" within a system, rather than hunting for known malicious files based on indicators of compromise (IoCs). In fact, most of the breach attempts detected and responded to by PAGO MDR Center involved identifying and addressing attackers active on the system. The most frequently detected incident involved the LotL technique, which exploits legitimate, built-in tools such as PowerShell, cmd.exe, w3wp.exe (IIS), and sqlservr.exe (MS-SQL). This technique appears to be becoming a standard attack model for attackers.
PAGO MDR Center uses specialized process relationship analysis techniques to detect LotL attacks. Each individual process is normal, but the execution relationships between them are abnormal, identifying patterns.

· Case 1: Web shell execution detection

- Abnormal process relationship: w3wp.exe (IIS web server process) runs cmd.exe (command prompt) as a child process - Digging data: This abnormal process relationship was detected in many customers.
- Analysis for decision-making: Classify and respond to strong IoCs indicating that an attacker is executing remote commands through a malicious web shell uploaded to a website.

· Case 2: RCE detection through SQL Server

- Abnormal process relationship: sqlservr.exe (MS-SQL Server process) runs cmd.exe as a child process.
- Data breach: Detecting abnormal processes in breach incidents that occurred at some customers.
- Analysis for decision-making: An attacker has taken control of the database server and is executing operating system (OS) commands through a SQL injection vulnerability attack or exploitation of the xp_cmdshell stored procedure.

Attacks like Cases 1 and 2 cannot be resolved with existing detection and response technologies that block individual files or IPs. Instead, context-based behavioral analysis can be used to transform events into events of interest, which can then be converted into incidents requiring response.

email after completing all threat activities over the weekend. To prevent such threats, 24/7 **Always-On** MDR services and **Preemptive Response**, which can even make decisions for threat response, are essential. By identifying threats through 24/7 real-time detection and responding on behalf of the security organization, the spread of threats is blocked early.

The breach data from incidents responded to by PAGO MDR Center demonstrates the necessity of 24/7 operations and preemptive response.

- Successful isolation within 24 to 40 minutes after detecting credential theft attacks.
- Early stage blocking of intrusion attempts based on exposed RDP and SSH ports.
- Proactive blocking of PoC based attack scans at the awareness stage.
- Eliminate false positives with context-based redefinition after classifying unknown threats
- An operational structure that combines automatic isolation and human judgment, reducing MTTR by an average of 38%.

PAGO MDR Center rapidly detects breaches and immediately proposes countermeasures through "Validation-Automation-Hunting." In situations where customers find it difficult to respond directly, PAGO Networks experts make strategic decisions and take action.

PAGO MDR Center's 24/7 proactive response ensures that any breach is preventing damage before it occurs and minimizing the business impact is not only a strong security strategy, but also a financial decision that reduces company-wide losses.

Detecting nation-state attacks based on threat intelligence

Threat intelligence is a service that provides crucial data that reveals attacker tactics, techniques, and procedures (TTPs). PAGO DeepACT MDR accumulates intelligence based on real-world cases and combines it with publicly available, open-source intelligence (OSINT) data to enable more accurate threat detection.

1. Hafnium attack detection

PAGO MDR Center detected unusual activity on a customer's Exchange server. The key indicator was that the IIS application process w3wp.exe (specifically MSExchangeOWAAppPool or MSExchangeECPAppPool) was launching cmd.exe as a child process.

· **TTP:** The threat actor installed malicious web shells, such as proxy.aspx and page.aspx, in the /owa/auth/ or /ecp/auth/ paths of the Exchange server. Then, it executed cmd.exe and performed internal network reconnaissance commands (e.g., net group Domain computers /domain, ipconfig).
· **Threat Intelligence Analysis:** This behavior is consistent with the typical attack chain used by the Chinese threat group HAFNIUM when exploiting ProxyLogon and ProxyShell vulnerabilities. Through analysis of fileless attacks with no file signatures and abnormal process relationships, PAGO MDR Center detected and blocked early reconnaissance activity by a nation state APT group in real time..

2. x0wolf attack detection

PAGO MDR Center detected a sophisticated multi-stage attack introduced via a web shell (modify.aspx) in a customer breach incident.

· **TTP:** The threat actor exploited a vulnerability in the Microsoft Sysinternals driver PROCEXP152.sys, which has a legitimate signature, to disable EDR solutions and then execute the CobaltStrike payload (0302.exe). The C2 IP identified by PAGO MDR Center was 104[.]21[.]80[.]1, and the C2 tunneled to a file named lcx5qm.jpg. Additional malicious files disguised as unknown files were downloaded.
· **Threat Intelligence Analysis:** The lcx5qm.jpg file is a unique custom hacking tool used by the Chinese threat group x0wolf for SOCKS5 proxy C2 tunneling. The attackers combined the widely known CobaltStrike with the x0wolf group's own tools to create a dual C2 channel that is difficult to detect. PAGO MDR Center identified the attacker by linking the activities of the two tools and provided additional information along with the IoC block.

Security strategy centered on "MDR"

Security technologies are becoming increasingly standardized, and SOCs continue to respond to incidents by adopting advanced security tools. However, since real world breaches can still be carried out using relatively basic techniques, the urgent challenge is not technology itself but the redesign of operating models.

As a result, the core of security strategy in 2026 is not the adoption of stronger solutions, but the establishment of an MDR operating model that actually works. When true MDR is adopted as a foundational operating infrastructure, organizations can move beyond "Post Breach IR" toward "Preemptive MDR".

MDR should also be viewed not as an additional cost for the SOC, but as a financial decision strategy. By accurately detecting and responding to fast moving, multi stage attacks, MDR helps prevent breaches and improve the efficiency of security operations. Ultimately, this reduces overall organizational costs and enables companies to focus more on their core business, strengthening long term competitiveness.

Case Study: Preventing ransomware with proactive response

Ransom notes displayed by ransomware attackers typically state that "your data has been encrypted and confidential information has been exfiltrated," and demand payment by holding "service disruption and business paralysis" hostage. Attackers deliberately apply pressure to maximize their profits, emphasizing that damage increases as the victim's downtime grows longer.

To minimize such damage, 24/7 security operations capable of preemptive response are essential. PAGO MDR Center's preemptive response services have multiple proven cases of successfully blocking ransomware damage even during hours when security staff are not on duty.

· **Detect:** At 11:35 a.m. on Sunday, threat hunting detected in real time an attempt to bypass UAC (T1548.002, modification of the ConsentPromptBehaviorAdmin registry setting) on a specific corporate server, along with the creation of a new administrator account named "default" (T1136.001).

Analyze: The 24/7 security experts at the PAGO MDR Center immediately determined that this action was an attempt to 'secure system control and persistence through the creation of a backdoor account' and converted the situation into a high-risk (critical) breach incident.

· **Respond:** PAGO security experts immediately activated the client's emergency contact network, but as it was Sunday morning, they were unable to reach the customer immediately. However, judging that the situation required rapid containment, they remotely implemented "preemptive network isolation" measures according to a predefined and agreed-upon response policy (playbook).

BOARD RECOMMENDATIONS TO SECURE BUSINESS VALUE

Security decision making authority should no longer remain confined to traditional CISO or CIO organizations. Cyberattacks are not merely IT incidents, but compound risks that affect finance, operations, reputation, and customer trust. Accordingly, security strategy in 2026 must be redefined not as a technology driven function, but as a "Business Risk" that executive leadership must manage directly.

Redefining the Management Value of Security

Companies have traditionally categorized security investments into IT operating expenses (OPEX), regulatory compliance costs, and technology investments. However, they must now broaden their focus to encompass issues of resilience and survivability. This means security budgets have shifted from "technology costs" to "risk-adjusted costs". Management must shift its focus from the size of security investments to "how security protects the enterprise."

When making decisions about security operations from a recovery and survival perspective, the board should consider the following indicators:

- MTTD (Mean Time to Detect)
- MTTA (Mean Time to Acknowledge)
- MTTR (Mean Time to Respond)
- Containment Ratio
- Exposure Reduction
- IB Ratio(Incident-to-Breach Ratio)

This metric is important to prevent confusion caused by fake MDRs. These fake MDRs lack adequate or nonexistent response personnel, lack 24/7 continuous operation, and lack a detection structure based on verification and threat hunting. Because they fail to respond effectively in real-world attack situations, they easily fall into the trap of believing MDR is useless. This can lead to management failures that go beyond security failures.

A true MDR has 24/7 security analysis and response experts and organizations, threat hunting and validation processes, automated quarantine, embedded CTEM processes, extensive threat intelligence, and advanced response capabilities powered by augmented AI. A true MDR provides an "Operation Standard" for management and is adopted as part of a business risk management strategy.

Questions Boards Should Ask in 2026

As security has moved beyond technical execution to board level strategic decision making, executive questions must also change. The following questions are not about "performance reporting," but about assessing the organization's "ability to survive".

CEO's Question

- How quickly are attacks detected?
- Is response made immediately after detection?
- Doesn't the response depend on the person's working hours?
- Can it detect unknown threats?
- Are strategies to reduce the attack surface actually being implemented?

CFO's Question

- How much actual risk reduction is achieved compared to cyber investment?
- How did improving MTTR impact the financial statements?
- Is the security organization's response speed leading to cost-saving structures?

Board of Directors Questions

- How long is the recovery time when a breach occurs?
- Are response plans for each attack scenario documented and tested?
- Is MDR operational capability verifiable both internally and externally?

APPENDIX: RESEARCH METHODS AND DATA SOURCES

This report was produced by the IT magazine <Network Times> at the request of Pago Networks.
The report was prepared based on multi-layered threat intelligence accumulated by the PAGO MDR Center from 2023 to 2025, actual MDR service breach response cases, and annual reports officially announced by reliable global security companies and organizations.
Because reports from different organizations and companies view the same threats from different perspectives, the PAGO MDR Center identified and cross-validated overlapping sections of PAGO MDR service case studies, intelligence, and global reports to extract and analyze only the most reliable areas. Furthermore, the PAGO MDR Center's specialized security insights aimed to provide immediately actionable intelligence for corporate security organizations, and suggested essential considerations for executives and boards of directors when developing security strategies as part of their business strategy.

The official annual reports of the global threat intelligence agencies referenced in this report are as follows:

- Verizon Data Breach Investigations Report (DBIR) 2023–2025: Breach vectors, supply chain attacks, credential theft attack patterns, and regional breach trends
- CrowdStrike Global Threat Report (GTR) 2024–2025: Breakout time, attacker tactics (TTPs), and domain movement speed
- IBM Cost of Breach Report (CODB) 2023–2025: Breach cost structure, effects of automation and AI adoption, and the scale of losses due to delays in recognition and response
- Mandiant M-Trends 2023–2025: Initial breach detection paths, shifts in dwell time, and attacker operating models
- Gartner CTEM & SOC Modernization Framework (2023–2025): Attack Surface Management, Operating Model Transformation (Prevention → Exposure → Resilience) Insights

THE LEADER IN BUSINESS TECHNOLOGY MEDIA
NETWORK TIMES | DATANET IT·정·보·마·당

Founded in 1993, Network Times, an IT magazine, provides in-depth analysis of the IT industry and accurate information to help readers develop advanced IT strategies. Led by reporters specializing in IT infrastructure and solutions, cyber/physical security, Network Times publishes the Monthly Network Times and the IT Internet media outlet Datanet, covering a wide range of topics.We are producing industry analysis reports and technical white papers.

www.datanet.co.kr | 02-6397-3100

pago

PAGO Networks, a Managed Detection and Response (MDR) specialist, protects customers across a wide range of industries, including energy, chemicals, semiconductors, power, manufacturing, finance, healthcare, government, and research, in Korea and the APAC region. PAGO's MDR platform, DeepACT, serves as a virtual, dedicated CERT, IR, or SOC team for customers of all sizes and in diverse environments, including OT/ICS, IT, cloud, and data centers.
PAGO MDR Center offers comprehensive services including Managed-EPP, Managed-EDR, Managed-NDR, and Managed-XDR, along with expanded, customized solutions for incident response, threat hunting, attack surface management, breach assessment, and threat intelligence (TI) sharing.

www.pagonetworks.com/
65 Hoenamu-ro, Yongsan-gu, Seoul
Representative number 080-077-5171