Playbook

Securing the Post-Breach Golden Hour Is Critical

AhnLab EDR Response Playbook for Reducing Dwell Time

AhnLab

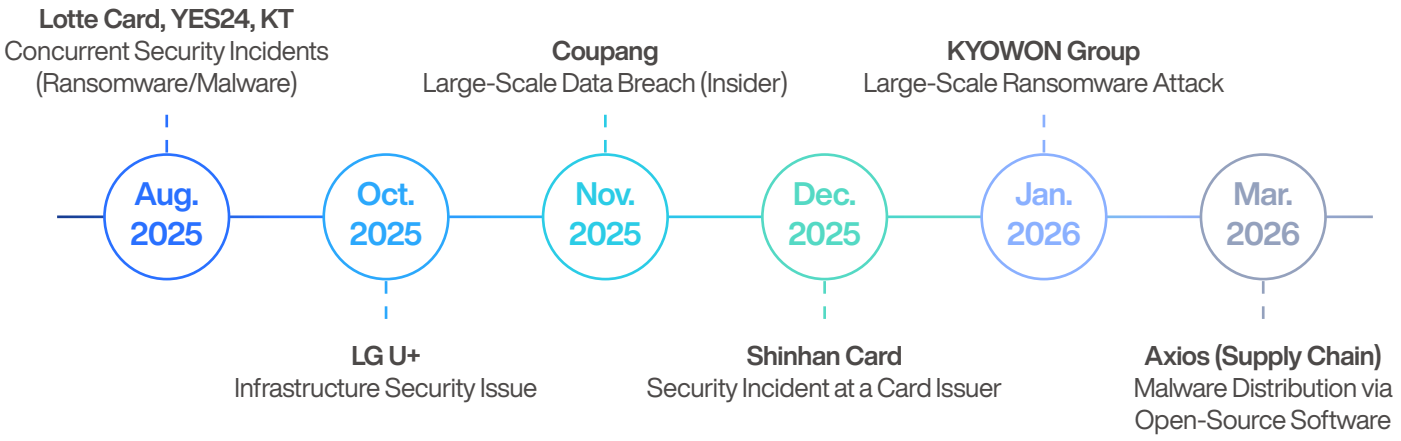
Table of Contents

Insights from Major Security Incidents in 2025–2026

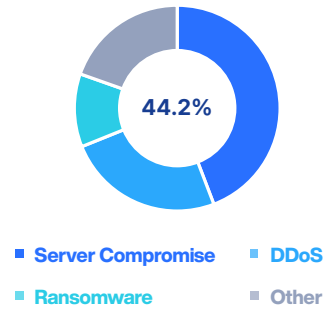
Security incidents in South Korea increased significantly in 2025, while attack methods also became more complex and diverse. A total of 2,383 incidents were reported in 2025, up 26.3% year over year. Server compromises accounted for the largest share at 44.2%, while distributed denial-of-service (DDoS) attacks and ransomware also remained major threats.

These figures indicate that organizations continue to face multi-layered attacks targeting a wide range of infrastructure. Looking at major incidents, multiple ransomware- and malware-based security incidents affected Lotte Card, YES24, and KT in August 2025. These were followed by security issues involving LG U+ infrastructure, a large-scale data breach at Coupang, a ransomware attack against KYOWON Group, and the Axios supply chain attack. Together, these incidents show that attackers are exploiting a wide range of attack vectors, including servers, accounts, legitimate software, and open-source packages.

Attack Trends and Response Implications from Major Incidents

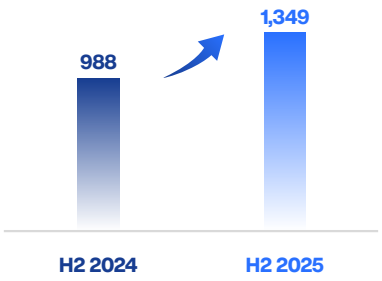


Server Compromise Ranks No. 1



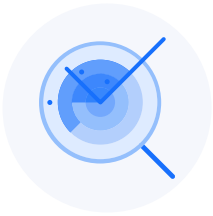
Largest share of all security incidents in 2025

Accelerating Growth in Security Incidents



1,349 incidents in H2 2025
+36.5% YoY

Increase in Attacks Targeting Large Enterprises



5.8%

Focus on ransomware & supply chain attacks Increasingly sophisticated targeted threats

Threat Highlights

- Security incidents are not only increasing in number, but also becoming more sophisticated in both their targets and methods.
- Attackers are using a range of vectors, including server compromise, ransomware, and supply chain attacks, to target organizations' critical assets and operational environments with increasing precision.
- As targeted attacks against large enterprises and critical service infrastructure continue to grow, security incidents are increasingly likely to result in prolonged persistence, data exfiltration, and service disruption.
- Organizations need to respond faster and strengthen EDR-based response capabilities that can identify and disrupt attack activity early.

Ultimately, incident response is about more than preventing an initial compromise. What matters most is reducing the time attackers remain in the environment and disrupting the attack chain before it leads to data exfiltration or mass encryption. The key metric for measuring this is Dwell Time, or the length of time an attacker remains within a compromised environment.

Based on major security incidents from 2025 to 2026, this guide outlines post-compromise detection and response strategies from an EDR perspective. It organizes major attack scenarios into four playbooks covering ransomware and server compromise, abuse of legitimate tools, package supply chain attacks, and trust-based impersonation attacks, with each playbook examining the attack flow, key EDR detection points, and response measures centered on blocking and isolation. Together, they show where attacks need to be detected and blocked to reduce Dwell Time.

How to Use This Guide

- **Understand Recent Incident Trends and Key Threat Types**
  Review the rise in security incidents in 2025 and major attack types such as server compromise, DDoS, and ransomware, along with how major incidents in South Korea have unfolded.

- **Understand Why Reducing Dwell Time Matters**
  The longer an attacker remains inside a compromised environment, the greater the risk of data exfiltration, internal propagation, and mass encryption. This guide treats Dwell Time as a key incident response metric and explains how AhnLab EDR can help reduce it.

- **Identify EDR Detection Points for Major Incident Scenarios**
  Use the four playbooks covering ransomware and server compromise, abuse of legitimate tools, package supply chain attacks, and trust-based impersonation attacks to review attack flows and key detection points.

- **Review Immediate Post-Compromise Response Actions**
  Examine response measures for each incident type, including terminating suspicious processes, isolating compromised hosts, blocking C2 communication, removing malicious files, and revoking code-signing certificates and re-signing affected software/packages.

- **Define Operational Priorities After Deploying AhnLab EDR**
  Use the 30/60/90-day roadmap to define operational tasks at each stage, including identifying protected assets, configuring detection policies, tuning rules, automating response actions, and conducting incident response exercises.

Why Traditional Security Is No Longer Enough

Recent security incidents are increasingly difficult to detect through traditional malware detection alone. Attacks no longer end with the execution of a single malicious file. Instead, they unfold as a sequence of connected activities after the initial compromise, including privilege escalation, lateral movement, C2 communication, data collection, and mass encryption. Incident response must therefore expand to correlate endpoint activity such as process execution, file creation, registry changes, and external communications, enabling organizations to identify and disrupt attack chains at an early stage.

Limitations of Signature- and Reputation-Based Detection	Traditional anti-malware solutions and Endpoint Protection Platforms (EPPs) are effective at blocking known malware and detecting threats through signatures and reputation data, but they have limitations when dealing with new or variant threats and ransomware designed to bypass conventional detection.
Abuse of Trusted Tools, Signatures, and Packages	Attackers exploit elements that organizations trust to bypass security controls. Legitimate remote access tools such as AnyDesk can be abused to maintain persistent remote control, while stolen code-signing certificates can be used to make malware appear legitimate. Compromised open-source packages can further extend the attack path into development environments and CI/CD pipelines.
Attack Chains Rather Than Isolated Eveants	An attack may begin with vulnerability exploitation or web shell-based intrusion, then progress through privilege escalation → internal reconnaissance → lateral movement → C2 communication → data collection → mass encryption. Individual events may appear legitimate in isolation, but when correlated across a timeline, they can reveal the broader attack chain.

Recent attack patterns require the following shift in detection approach.

Limitations of Traditional Detection	Recent Attack Methods	Required Detection Approach
Focus on known malware	Novel, variant, and fileless attacks	Behavior-based detection
Trust in legitimate programs	Abuse of legitimate tools such as AnyDesk	Execution context analysis
Trust in digitally signed files	Leaked code-signing certificates	Verify signature status and behavior
Trust in packages	Open-source supply chain attacks such as Axios	Track processes and network activity after installation
Analysis focused on individual events	Long-term persistence, reconnaissance, and C2 communication	Attack timeline visibility

> The limitations of traditional detection go beyond simply failing to catch malicious files. The real challenge is how quickly organizations can identify attack chains that emerge when seemingly legitimate executions, configuration changes, and external communications are linked together. AhnLab EDR correlates these activities and reconstructs them as an attack timeline, helping organizations respond before the attack progresses to data exfiltration or mass encryption.

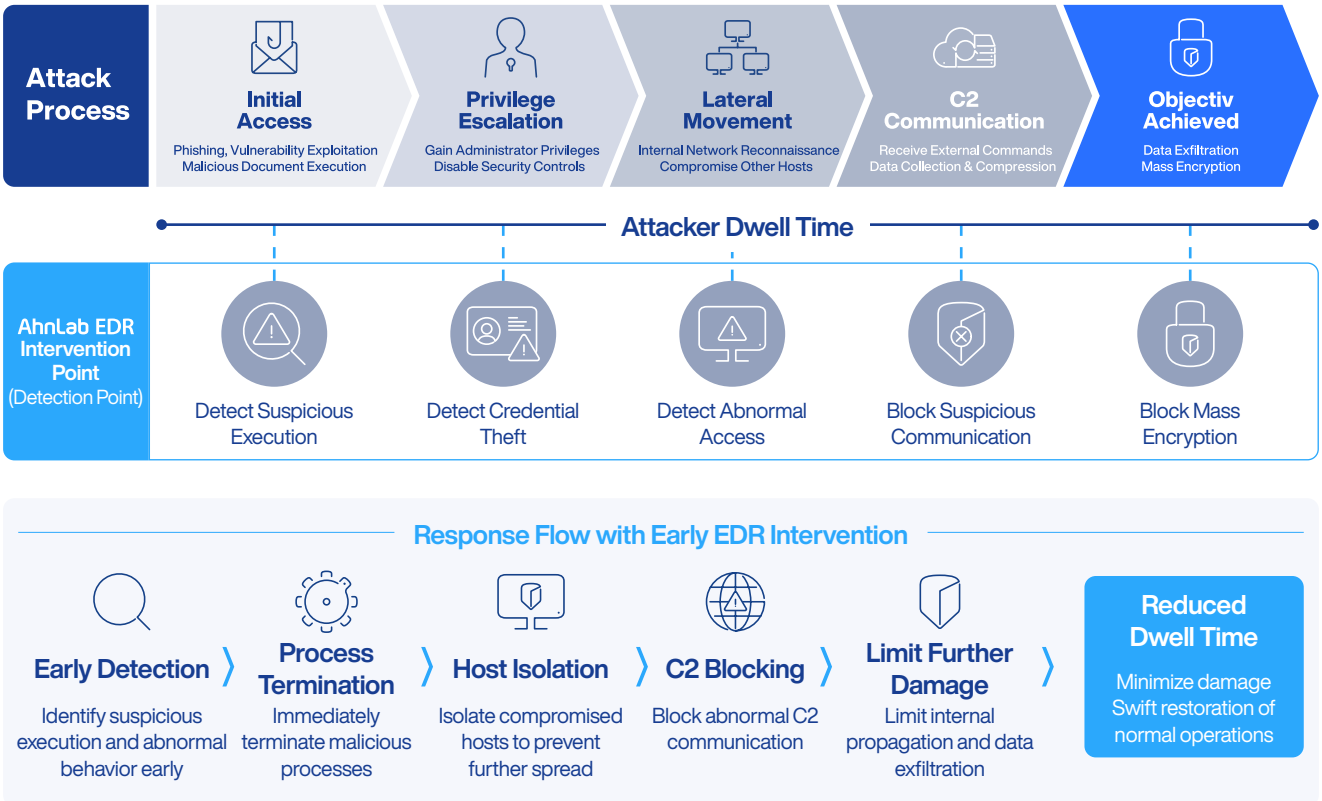
Why Reducing Dwell Time Matters: The Role of AhnLab EDR

Dwell Time refers to the length of time an attacker remains in an environment from the initial intrusion until the attack is detected and remediated. The longer this period lasts, the more opportunities the attacker has to expand the scope of the attack through repeated internal reconnaissance, privilege escalation, data collection, C2 communication, and lateral movement. The damage from ransomware attacks can escalate through mass encryption and double extortion, while data breaches can cause greater harm through the prolonged collection and exfiltration of customer data.

The key to effective incident response is reducing MTTD and MTTR before an attacker can achieve their objective. MTTD measures the time from the onset of a threat to detection, while MTTR measures the time from detection through containment, removal, and recovery. Reducing both metrics shortens Dwell Time.

AhnLab EDR detects suspicious activity in real time throughout each stage of the attack cycle and enables response actions such as terminating malicious processes, isolating infected hosts, and blocking C2 communication. This helps disrupt the attack flow before it progresses to data exfiltration or mass encryption.

AhnLab EDR Intervention Points Across Attack Stages and Dwell Time Reduction



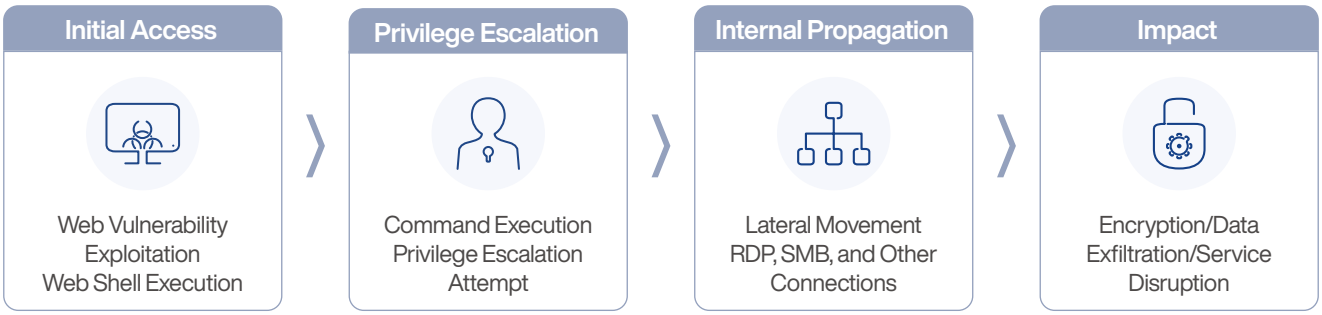
Seemingly legitimate executions, configuration changes, and external communications can form a broader attack sequence when they are linked together. AhnLab EDR identifies these attack patterns early, reducing detection delays and enabling organizations to respond before the attacker achieves their intended objective.
The key is to reduce both MTTD, the time it takes to detect a threat, and MTTR, the time from detection to response. Shortening both helps reduce attacker Dwell Time and limit the potential spread and impact of an attack.

Playbook 1. Ransomware and Server Compromise

Response to Mass Encryption, Service Disruption, and Data Exfiltration

Ransomware and server compromises can begin with intrusion into the internal network through vulnerable servers or web shells, then progress through internal reconnaissance, lateral movement, and C2 communication before culminating in mass encryption, data exfiltration, or service disruption. If the attack also involves attempts to delete backups or exfiltrate data, the impact can escalate to business disruption, exposure of personal data, and double extortion, while also directly damaging the organization's reputation.
The key to effective response is not waiting until the damage becomes visible and then focusing on recovery. Organizations need to identify and block early warning signs after the initial intrusion, including suspicious process execution, long-term persistence, internal propagation, and large-scale file modifications.

Ransomware and Server Compromise Flow



AhnLab EDR-Based Detection Points

When responding to ransomware and server compromises, the focus should be on the sequence of post-intrusion activity rather than the malicious file itself. Suspicious commands executed through web shells or vulnerable servers, internal reconnaissance and lateral movement, C2 communication, and large-scale file modifications are all key indicators that need to be detected before the attack progresses to encryption or data exfiltration.

Detection Range	EDR Detection Point
Post-Intrusion Execution Activity	Detect abnormal command/script execution by web server child processes following web shell execution
Internal Propagation/ Communication Activity	Correlation analysis of internal reconnaissance, lateral movement, remote access, C2 communication, and data collection and exfiltration activities
Pre-Impact Activity	Detect large-scale file modifications, encryption patterns, deletion of volume shadow copies, and attempts to damage backup files

Post-Detection Response Procedure

Once these indicators are identified, immediately disrupting the attack flow is the first priority. Isolate servers suspected of compromise to prevent further spread, terminate active malicious processes and block external communications, then determine the extent of encryption, data exfiltration, and backup damage before moving on to recovery and recurrence-prevention measures.

No.	Response Stage	Action	EDR Usage Point
1	Isolate Compromised Servers	Disconnect suspected compromised servers and hosts from the network	Apply host isolation policies
2	Block Execution	Terminate suspicious processes and remove web shells and malicious scripts	Terminate processes based on process-tree analysis
3	Block Communication	Block C2 communication and additional remote access	Block suspicious network connections
4	Assess Scope of Impact	Check for mass file modifications, backup deletion, and data access/exfiltration	Analyze file and network event timelines
5	Recovery and Recurrence Prevention	Verify backup integrity and search across the organization for the same IoCs and behaviors	Hunt based on IoCs and behavioral patterns

Golden Hour: Early stages of web shell intrusion and internal propagation

AhnLab EDR correlates suspicious execution, internal propagation, C2 communication, and large-scale file modification activity into an attack timeline, allowing organizations to intervene earlier before the attack progresses to encryption or data exfiltration. This can reduce Dwell Time to a matter of hours or even minutes, minimizing the impact of widespread compromise, service disruption, and data exfiltration.

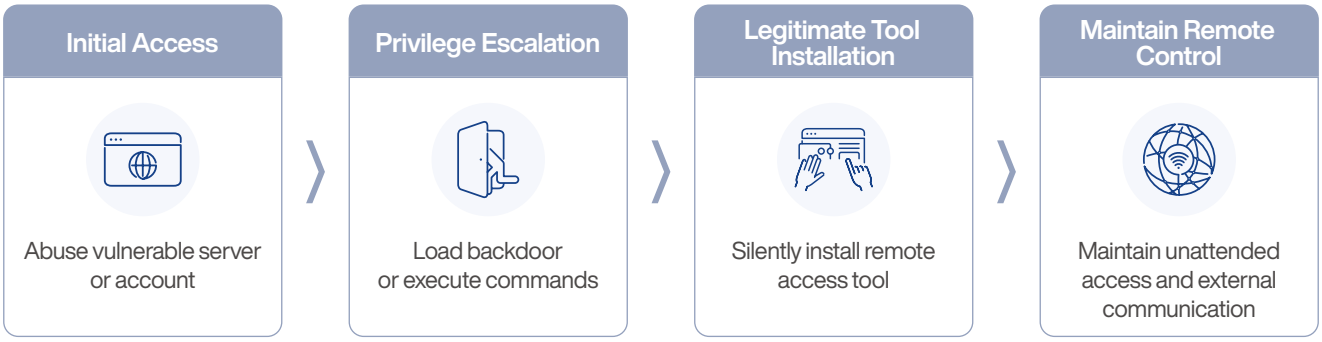
Playbook 2. Abuse of Legitimate Tools

Response to Persistent Control Through Legitimate Tools Such as AnyDesk

Legitimate remote access tools such as AnyDesk are commonly used for IT support and remote work, but within an attack chain they can be abused to maintain control of an internal network and evade detection. After gaining initial access through a vulnerable server or account, an attacker may deploy a backdoor and use PowerShell scripts or similar methods to install remote access tools silently in the background or enable unattended access.

In this type of attack, the key is not simply whether a remote access tool is running, but the context in which it was installed, what process or user initiated it, any configuration changes, and its external communications. Even a seemingly legitimate tool can become a means of persistent attacker control when it appears within an abnormal execution flow.

Abuse of Legitimate Tools Flow



AhnLab EDR-Based Detection Points

Abuse of legitimate tools may look like normal operational activity when each action is viewed in isolation. AhnLab EDR analyzes the relationships between process execution, file creation, configuration changes, and external connections to distinguish legitimate remote support activity from persistent attacker control.

Detection Range	EDR Detection Point
Abnormal Execution Flow	Detect execution chains where a remote access tool is installed or commands/scripts are executed under server/business application processes, followed by backdoor execution
Abuse of Legitimate Tools	Detect abnormal installation/configuration changes, including file creation in unauthorized paths, silent installation, unattended access configuration, and service/registry registration
Persistent Control/External Communication	Determine whether external control activity persists through remote access sessions, C2 communication, connections over nonstandard ports, or data exfiltration traffic

Post-Detection Response Procedure

When responding to attacks that abuse legitimate tools, the first priority is to disrupt the attacker's control before a remote access session becomes prolonged. Isolate suspected compromised hosts, terminate any running remote access tools, scripts, and backdoor processes, then remove unauthorized configurations and traces of persistence to prevent the attacker from reconnecting.

No.	Response Stage	Action	EDR Usage Point
1	Block Execution	Force-terminate remote access tools, PowerShell scripts, backdoors, and their associated parent process trees	Terminate process trees when high-risk patterns are detected
2	Host Isolation	Disconnect servers and endpoints showing signs of compromise from the network	Apply network isolation policies to block internal lateral movement
3	Block Communication	Block C2 communication, unauthorized external access, and remote access connection attempts	Block suspicious network connections and alternate ports used to bypass controls
4	Restore Configuration	Remove unauthorized changes such as unattended access settings, service registrations, and registry modifications	Analyze file and registry change events and restore systems to a known-good state
5	Prevent Reconnection	Delete unauthorized remote access files, review account access policies, and check for recurrence of the same activity	Conduct organization-wide hunting based on matching IoCs and behavioral patterns

> **Golden Hour: Immediately after legitimate tool installation and unattended access configuration**
> AhnLab EDR performs correlation analysis across the execution context of remote access tools, configuration changes, and external communication activity to identify abnormal use. This allows organizations to disrupt the attacker's control before a remote access session can be maintained for an extended period, reducing Dwell Time.

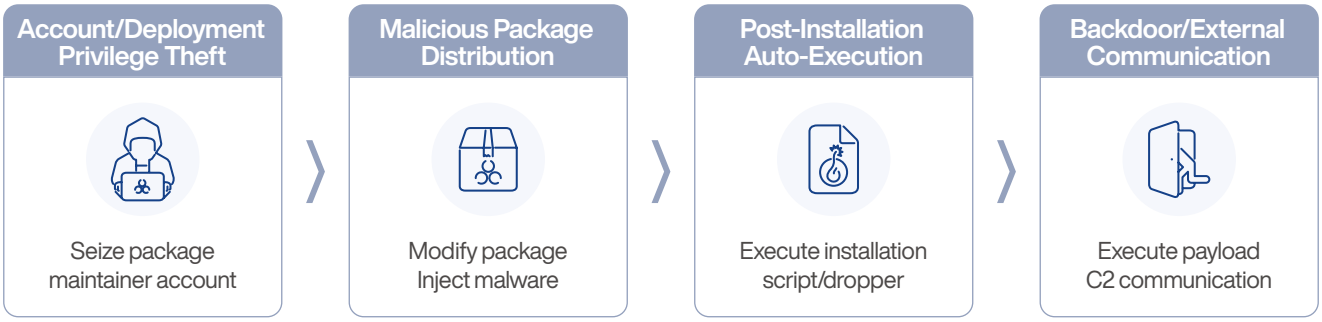
Playbook 3. Package Supply Chain Attacks

Response to Malicious Execution Following Open-Source Package Installation

Package supply chain attacks abuse trusted open-source packages and their installation processes as a channel for malware distribution. In the Axios supply chain attack, a maintainer account was compromised and a malicious version was subsequently published to npm. The attack flow then continued through automatically executed installation scripts, which launched a dropper and backdoor.

The key point to monitor in a package supply chain attack is what happens after installation. Even if the installation itself appears legitimate, suspicious process execution and external communication immediately afterward may indicate that a trusted package is being used as an attack vector to compromise the development environment.

Package Supply Chain Attack Flow



AhnLab EDR-Based Detection Points

Package supply chain attacks begin within a legitimate installation process, making it difficult to identify a threat based solely on the package name or whether it was downloaded. AhnLab EDR correlates process execution, file creation, persistence activity, and external communications immediately after installation to distinguish legitimate installation activity from a malicious execution flow.

Detection Range	EDR Detection Point
Post-Installation Execution Flow	Detect flows in which suspicious child processes are spawned by Node.js immediately after package installation, followed by script or command execution
Payload/Persistence Activity	Detect persistence activity such as downloading OS-specific payloads, creating files in hidden paths, and registering registry Run keys
C2 Communication/ Information Collection	Correlate backdoor behaviors such as periodic beaconing, external C2 communication, system reconnaissance, file enumeration, and command execution

Post-Detection Response Procedure

Responding to a package supply chain attack does not end with remediating the infected endpoint alone. Organizations must identify the malicious package version and review installation history, isolate developer PCs and CI/CD environments, and assess potential exposure across the development environment, including caches, tokens, and API keys.

No.	Response Stage	Action	EDR Usage Point
1	Assess Scope of Impact	Check malicious package version, installation history, and dependency inclusion	Perform correlation analysis between package installation times and process execution events
2	Isolate Environment	Isolate developer PCs and CI/CD environments suspected of infection	Isolate developer workstations showing suspicious activity and block further execution
3	Block Execution	Terminate suspicious child processes under Node.js, droppers, and backdoor processes	Block malicious script/backdoor execution based on process-tree analysis
4	Block Communication	Block external communication to C2 domains, IP addresses, and ports	Block suspicious network connections and outbound traffic to malicious domains
5	Prevent Recurrence	Clear package caches, pin package versions, rotate tokens and API keys, and review components based on the SBOM	Continuously monitor child processes under Node.js and external communication activity

Golden Hour: When a malicious script executes immediately after package installation

AhnLab EDR identifies process execution, payload downloads, and external communication activity early after package installation, providing an opportunity to intervene before the attack spreads to development environments and CI/CD pipelines. This reduces Dwell Time following malicious package installation and lowers the risk of cascading infections.

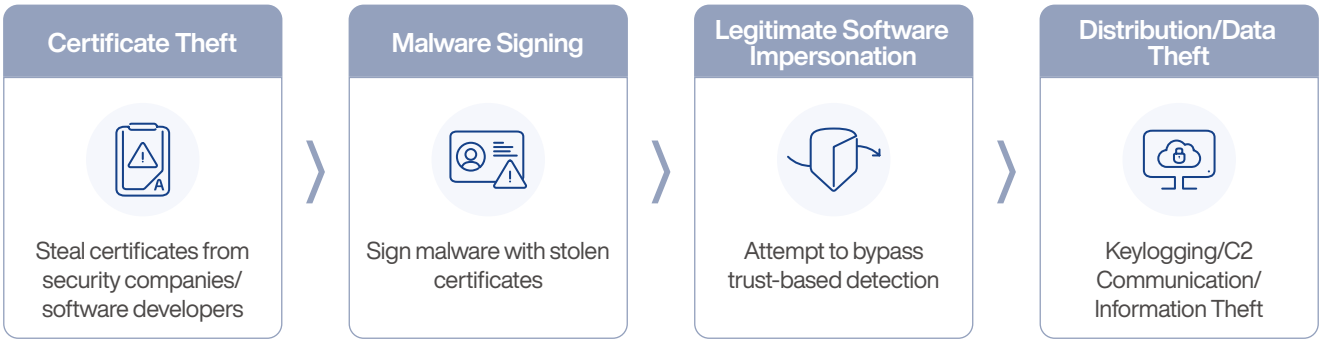
Playbook 4. Trust-Based Impersonation Attacks

Response to Detection Evasion Through Code-Signing Certificate Abuse and Legitimate Software Impersonation

Trust-based impersonation attacks abuse the trust associated with code-signing certificates, legitimate software, certificate authorities, and security companies to make malicious activity appear legitimate. As seen in cases involving leaked code-signing certificates and malware disguised as legitimate software, signed files and legitimate modules can be abused to conceal malicious activity.

If a code-signing certificate is compromised or a legitimate module is tampered with, the attack may progress to keylogging, C2 communication, and data theft. Organizations should therefore assess threats based on post-execution behavior rather than assuming that a file or program is safe simply because it is "signed" or appears "legitimate."

Trust-Based Impersonation Attack Flow (Code-Signing Certificate Compromise and Legitimate Software Impersonation)



AhnLab EDR-Based Detection Points

From an EDR perspective, post-execution behavioral events should take priority over a file's signature status. The starting point for detection is to correlate behaviors that may be concealed by the apparent trustworthiness of a valid signature, such as web shell creation, malicious modules masquerading as legitimate ones, keystroke theft, and external C2 communication.

Detection Range	EDR Detection Point
Execution of Impersonating Signed Files	Detect execution of malicious files signed to appear as legitimate programs, as well as the replacement of legitimate plugins or executables with malicious modules impersonating them
Web Shell and File Tampering Activity	Detect web shell insertion into web root directories, abnormal command execution by web server child processes, and file integrity violations
Data Theft and External Communication	Detect memory injection, API hooking for keylogging, abnormal outbound connections, C2 communication, and attempted data transmission

Post-Detection Response Procedure

A code-signing certificate compromise cannot be resolved simply by deleting malicious files. Organizations must block malicious activity involving signed files and external communications while also restoring the trust framework by revoking the compromised certificate, issuing a new certificate, and re-signing affected packages.

No.	Response Stage	Action	EDR Usage Point
1	Block Malicious Behavior	Terminate signed malicious files and related processes	Detect/Terminate malicious processes
2	Block Communication	Block C2 communication and abnormal external connections	Block suspicious network connections
3	Restore Tampered Components	Remove or restore tampered files/registry settings	Analyze file/registry change events
4	Certificate Remediation	Revoke leaked certificates, issue new certificates, and re-sign packages	Behavior-based monitoring of signed programs
5	Block Further Distribution	Prevent further malware distribution and track suspicious files and communications	Hunt based on IoCs and behavioral patterns

Golden Hour: Initial execution of a signed malicious file and the start of C2 communication

AhnLab EDR identifies threats by analyzing post-execution activity, including memory access, keylogging, persistence activity, and external communications, regardless of whether the file is signed. This reduces how long malicious activity disguised as legitimate software can remain hidden and helps contain its spread through the supply chain before the attacker can establish prolonged Dwell Time.

Roadmap for Deploying and Operating AhnLab EDR

Deploying the solution alone is not enough to maximize the benefits of EDR. Organizations need to establish a phased operational framework covering protected asset identification, policy configuration, rule tuning, automated response, threat hunting, and operational KPI management. The AhnLab EDR operations roadmap defines the specific tasks organizations should complete during the first 90 days after deployment, organized into 30-, 60-, and 90-day stages.

AhnLab EDR Deployment/Operations Roadmap

Build the Foundation

30 Days

- Identify and classify protected assets
- Deploy pilot agents
- Set baseline detection policies
- Draft an isolation playbook

Optimization and Integration

60 Days

- Tune high-risk behavior rules
- Reduce false positives
- Start proactive threat hunting
- Integrate with SOAR and existing infrastructure

Enhancement and Operationalization

90 Days

- Expand agent deployment organization-wide
- Build an operational KPI dashboard
- Implement automated response processes
- Conduct regular tabletop incident response exercises

AhnLab EDR Operational Performance Review Items

Key Performance Indicators	Governance and Operational Maturity Management
▪ **MTTD:** Reduce time from threat occurrence to detection ▪ **MTTR:** Reduce time from detection through containment, isolation, and recovery ▪ **Average Dwell Time:** Reduce attacker Dwell Time within the compromised environment (Target: within a few hours) ▪ **Automated Isolation Rate/False Positive Rate:** Manage automated response quality	▪ Reduce incident investigation (IR) reporting time ▪ Enable threat hunting ▪ Ensure regulatory compliance and maintain audit evidence ▪ Conduct regular incident response exercises

The key to effective EDR operations is not deployment itself, but embedding EDR into day-to-day operations. By following the 30/60/90-day roadmap to progressively establish processes, tune detection rules, and strengthen monitoring capabilities, organizations can continuously reduce MTTD, MTTR, and Dwell Time while lowering incident response costs and the risk of business disruption.