AhnLab

eBook

Achieving 100% Protections in MITRE ATT&CK Evaluations Round 7

Once again, AhnLab has demonstrated our industry-leading cybersecurity capabilities in the independent MITRE ATT&CK Evaluations Enterprise Round 7, achieving 100% Protections. Our rock-solid defense, powered by contextualized and accurate cross-domain detection, indicates that our rigorously tested solutions are ready to safeguard our customers from ever-evolving cyber attacks in the real world.

About MITRE ATT&CK Evaluations

MITRE, the host of MITRE ATT&CK Evaluations, was established to advance national security in new ways and serve the public interest as an independent adviser. Through public-private partnerships and federally funded R&D centers, MITRE works across government and in partnership with industry and academia to tackle challenges. In the cybersecurity industry, MITRE is well-known for creating and developing the MITRE ATT&CK Framework, a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

MITRE ATT&CK Evaluations is built on the backbone of MITRE's objective insight and conflict-free perspective. Cybersecurity vendors participate in the evaluation to improve their offerings and to provide defenders with insights into their product's capabilities and performance. The evaluation enables defenders to make better informed decisions on how to leverage the products that secure their environments.

The evaluation, which is just completing its seventh round, is recognized worldwide as one of the most trusted security product tests, due to its similarity to real-world threats and the completeness of its attack scenarios. A total of 11 cybersecurity companies participated in round 7. AhnLab was the only South Korean company to participate in the evaluation for five consecutive rounds, starting from round 3.

Figure 1. Participants of MITRE ATT&CK Evaluations Round 7

How the Evaluation Is Shaped

The MITRE ATT&CK Evaluation consists of scenarios, which are composed of steps and substeps that comprise each step. Based on this structure, MITRE tests participants' defense ability against emulated cyber threats.

The most notable difference from previous rounds is that MITRE has newly added the "Cloud" to existing "On-Premises" environments as of this round. Considering that today's adversaries traverse on-premises and cloud domains to compromise victims, MITRE has further advanced its scenarios to evaluate participants in more real-world-like environments.

As for scenarios, there are two types in this evaluation: Detections and Protections.

1. Detections

The Detections evaluation measures how precisely a solution can identify potential threats in both on-premises (Windows and Linux) and cloud environments without using containment, blocking, or prevention techniques. With adversary behaviors executing uninterrupted, solutions demonstrate their visibility into the entire attack lifecycle, from initial access to action on objectives.

During the actual evaluation, the vendor and MITRE jointly collected evidence from the vendor's products, and MITRE calibrated the evidence of malicious events based on the five detection categories outlined below. Detection categories, in order from None to General, Tactic, and Technique, represent more accurate and contextualized threat detection.

Categories	Description
N/A	Evaluation for the (sub) step was not performed.
None	The vendor's evidence does not meet the detection criteria, or no evidence is provided.
General	The evidence satisfies the detection criteria but does not provide details on why (tactic) or how (technique) the action was performed.
Tactic	The evidence satisfies the detection criteria for General and provides details on why the action was performed (tactic).
Technique	The evidence satisfies the detection criteria for Tactic and provides details as to how the action was performed (technique).

Table 1. Detection categories of MITRE ATT&CK Evaluation – Malicious Events

In addition to malicious events, MITRE also tests the accuracy of detections with false positive substeps. By measuring specific non-malicious events that were incorrectly flagged as threats, MITRE tested participants to ensure that they can pinpoint normal behaviors and improve detection qualities.

Categories	Description
N/A	Evaluation for the (sub) step was not performed.
Reported	A solution generated an alert that meets the documented Detection Criteria and identifies benign activity under test as malicious.
Not Reported	A solution did not alert the benign activity under test as malicious.

Table 2. Detection categories of MITRE ATT&CK Evaluation – False Positives

2. Protections

The Protections evaluation assesses the effectiveness of blocking and preventing adversary attack sequences from causing a significant impact. The test follows a pass/fail methodology, where either a solution blocks an attack at a critical juncture or fails to stop it before the adversary has an impact.

Categories	Description
N/A	Evaluation for the (sub) step was not performed.
Protected	The activity under test was blocked from occurring.
Not Blocked	The activity under test was not blocked.

Table 3. Protection categories of MITRE ATT&CK Evaluation

Adversary Emulation in Round 7

In this round, MITRE incorporated and emulated the real-world techniques and tactics of Scattered Spider and Mustang Panda.

1. Scattered Spider: Financially-Motivated Cybercriminal Collective

MITRE emulated “Scattered Spider”, a threat actor linked to a number of high-profile attacks, and known for their expertise in social engineering, installing remote access tools, and bypassing multi-factor authentication (MFA). Emulated adversaries conduct creative and persistent targeting of victims' cloud resources to establish footholds, perform network and directory reconnaissance, and access sensitive systems and data stores. They operate at a high tempo, quickly accessing and exfiltrating large volumes of data.

2. Mustang Panda: People’s Republic of China (PRC) Cyber Espionage Group

MITRE also emulated “Mustang Panda”, one of the most active PRC state-sponsored cyberespionage groups that consistently refines its capabilities and toolsets to exploit victims around the world. The group employs well-planned social engineering tactics and exploits legitimate tools and services to deploy custom malware. Many of this adversary’s known behaviors and tools are widely used across the PRC offensive cyber ecosystem, such as their reliance on living off the land techniques, custom malware, and cloud-hosted infrastructure.

Highlights of Our Results on Top of Flawless Protections

In round 7, the detection and protection capabilities of AhnLab EDR, AhnLab EPP, and AhnLab XDR were rigorously assessed. Our products achieved 100% protection in testing, and there are additional highlights to be noted from the real-world user perspective.

1. 100% Protections – Proving Industry-Leading Defense Capabilities

We blocked 100% of malicious activities in the Protections testing, successfully keeping the evaluation environment and systems secure. The result once again demonstrates our industry-leading defense capabilities, which have been continuously verified through previous MITRE ATT&CK evaluations, other global cybersecurity assessments, and real-world customer environments.

Notably, the protection included tests composed solely of normal events, in addition to those comprised of malicious behaviors. Our solutions precisely identified these non-malicious events as normal and did not block them, thereby proving the accuracy of blocking capabilities. In simple terms, we stopped what needed to be stopped and allowed what needed to be allowed, delivering both robust security and practicality for real-world customers.

2. Cross-Domain Threat Visibility Across On-Premises and Cloud

As explained earlier, MITRE incorporated on-premises (Windows/Linux) and cloud scenarios in round 7. Our solutions provided detailed evidence and analysis of sophisticated techniques that span across operating systems, delivering comprehensive visibility and context of threat activities.

In the newly introduced cloud scenario this year, we integrated AhnLab XDR with the cloud resources in the testing environment to establish an architecture for behavioral detections. Embracing the concept of "open XDR" with seamless integration, AhnLab XDR effectively detected malicious activities carried out by attackers across cloud environments and provided contextual analysis. Consequently, we were able to demonstrate our exceptional cross-domain detection capabilities not only in on-premises environments but also in the cloud.

3. About 90% Accuracy in False Positives along with Zero Delays

For non-malicious substeps designed to assess detection accuracy and quality, we achieved about 90% accuracy. This result indicates that no threat alerts were generated for normal activities, demonstrating that our solutions can effectively address the false positive issue that many customers encounter when operating security systems.

Additionally, the evaluation assesses whether there was any delay in detections, as real-world users need to leverage detection evidence immediately for threat response. Our solutions provided all detection results in real-time, achieving zero-delay detections.

How We Specifically Countered Emulated Threat Behaviors

In this round, our solutions demonstrated outstanding detection and protection capabilities across Windows, Linux, and cloud environments. Let's take a closer look at how this was achieved through real examples.

1. Protections: Test 1

An attacker, using the username tharlaw, who infiltrated the victim's environment, downloaded an executable file named Snaffler.exe from the file server. Along with downloading Snaffler.exe, an adversary also scanned the local drive and network shares.

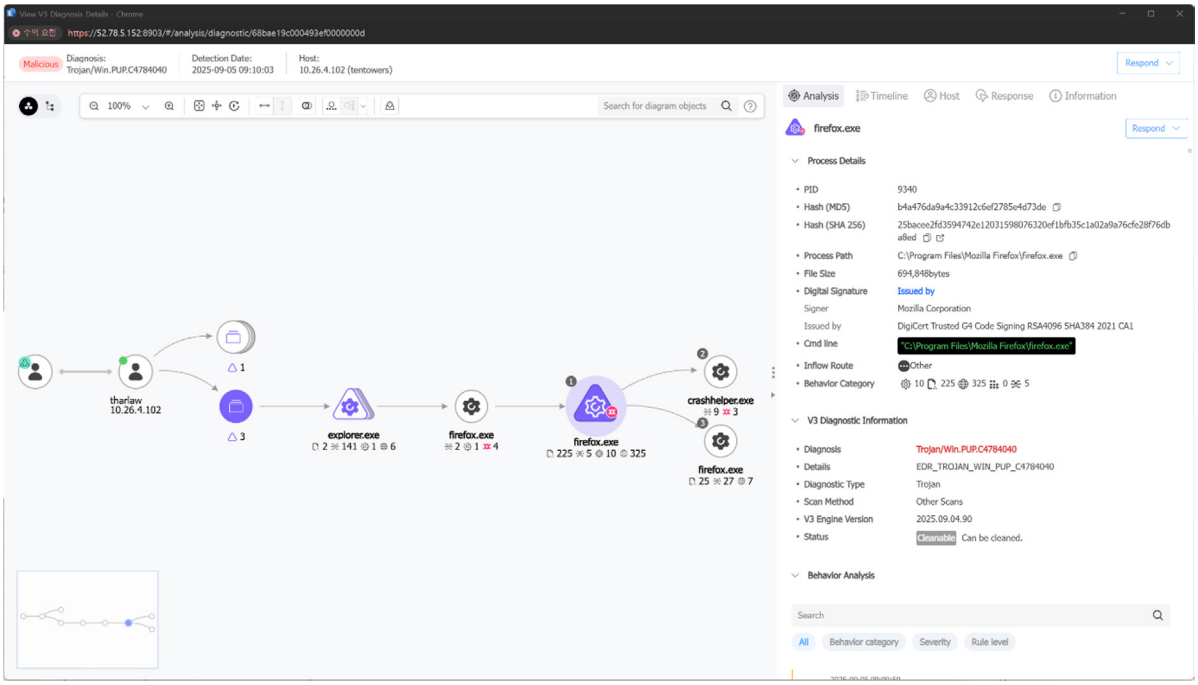

Figure 2. Protections: Test 1 – File Download

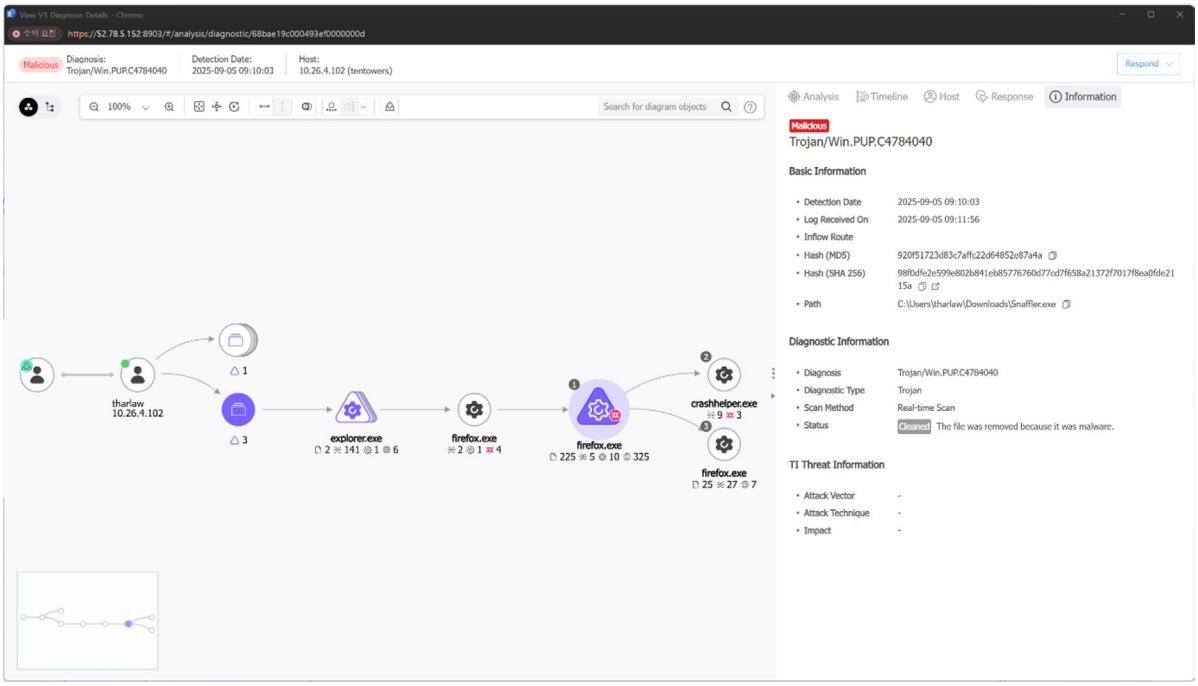

Figure 3. Protections: Test 1 – File Prevention

AhnLab EDR detected that the externally downloaded executable file Snaffler.exe contained a malicious signature. By interacting with our antivirus solution, AhnLab V3, AhnLab EDR detected the file as Trojan/Win.PUP.C4784040 and blocked it, preventing the malicious behavior from being executed in the victim's environment. This is significant not only because the malicious file was blocked, but also because the integration between EDR and antivirus allowed users to understand the context in which the blocking occurred.

2. Protections: Test 5

The attacker, using a username called awaynwood, infiltrated the victim's environment and downloaded wmiexec.vbs to the C:\Windows\Temp directory via a remote command execution tool. The attacker used this script to create a network share on the file server heartshome (10.26.3.106).

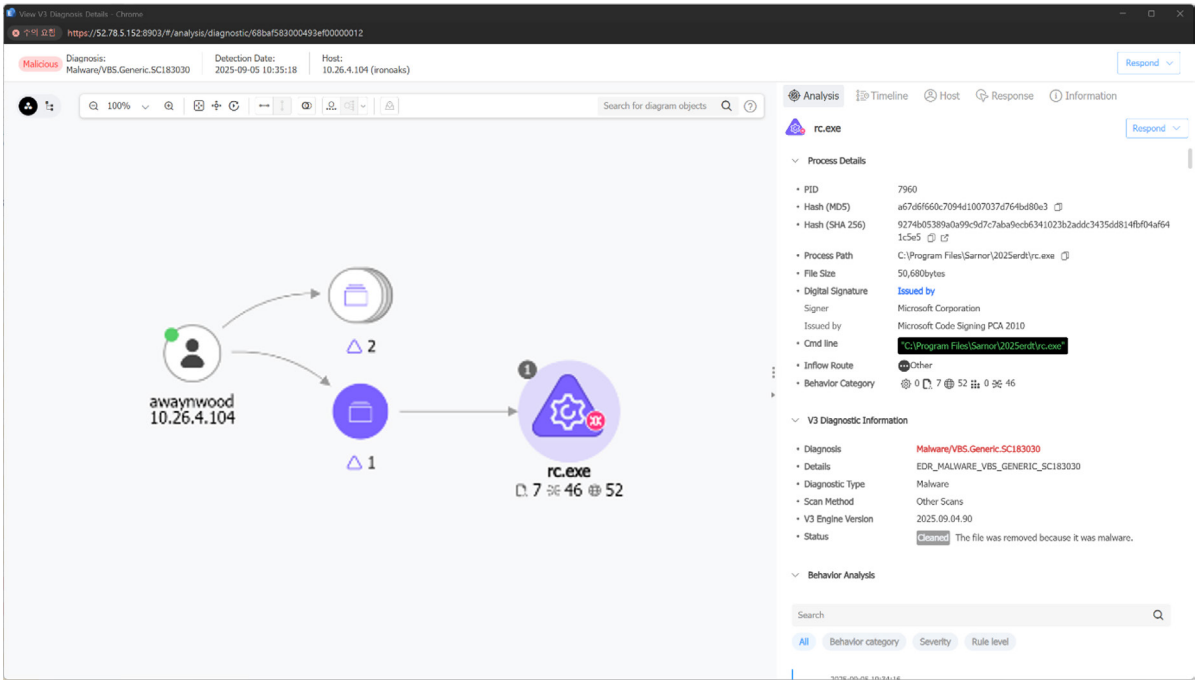

Figure 4. Protections: Test 5 – File Download

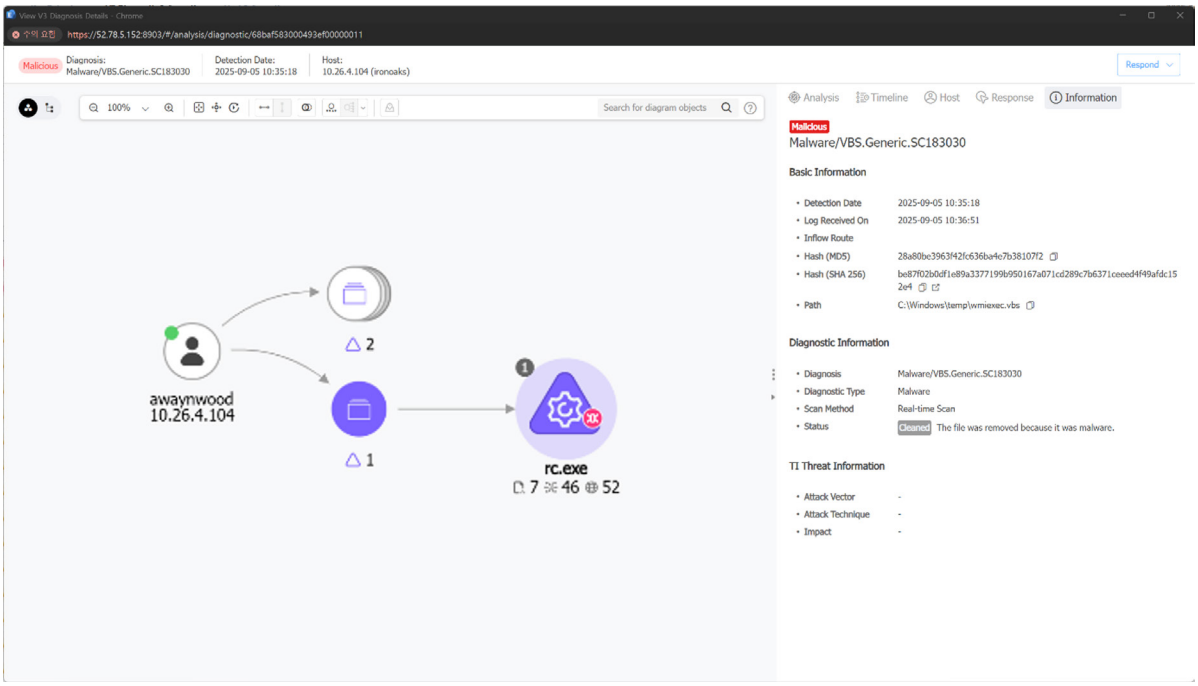

Figure 5. Protections: Test 5 – File Prevention

Similar to Test 1, AhnLab EDR detected that the executable file wmiexec.vbs, downloaded externally to the C:\Windows\Temp path, contained a malicious signature. It leveraged AhnLab V3 to block the file by detecting it as Malware/VBS.Generic.SC183030.

3. Detections: Substep 7.5 (On-premises)

The attacker, using a username htargaryen, extracted the NTDS file through credential dumping on the domain controller redkeep (10.55.3.100) and performed offline cracking. As part of this process, the attacker attempted to execute reg.exe on redkeep (10.55.3.100) to save the system hive remotely to Windows\Temp\system.hive on harrenhal (10.55.4.103).

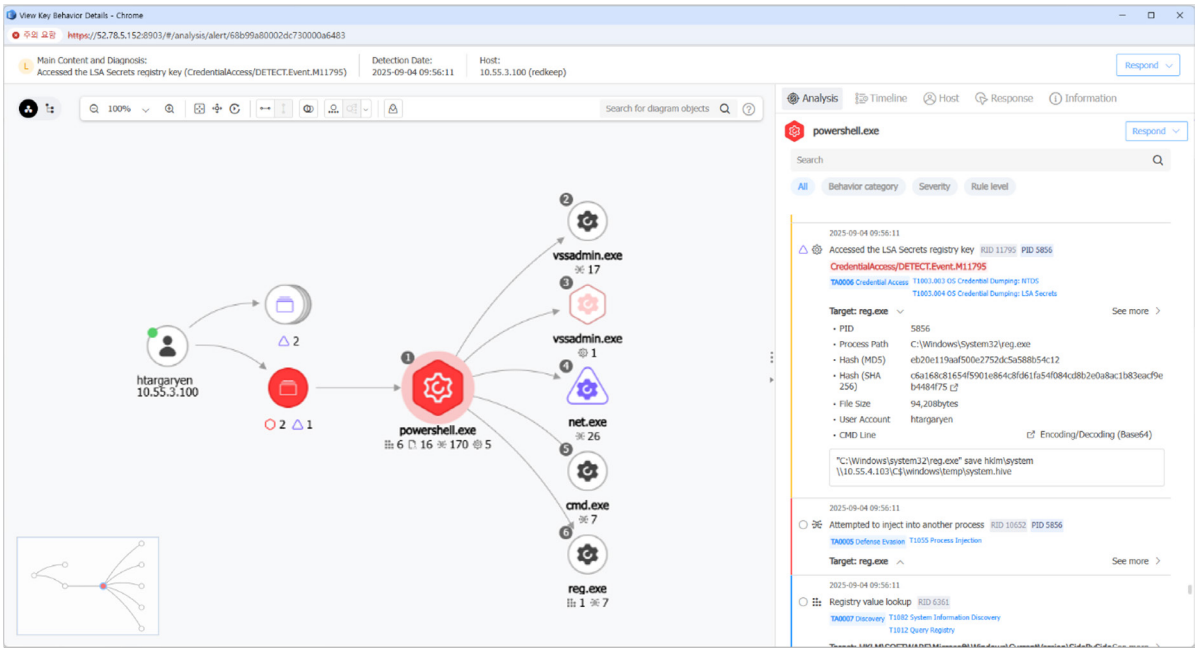

Figure 6. Detections: Substep 7.5 – System Hive Exfiltration

AhnLab EDR presented a behavioral diagram showing how an attacker attempted to use an unsigned reg.exe to store the system hive remotely for domain credential theft. Our EDR accurately detected the registry hive path (HKLM\SYSTEM) and the remote UNC storage location (\\10.55.4.103\C$\Windows\Temp\system.hive), and provided the corresponding TID (TA0006 Credential Access & T1003.002 OS Credential Dumping: Security Account Manager). This allowed users to gain a detailed understanding of the attacker's system hive exfiltration activity for credential theft.

4. Detections: Substep 7.2 (Cloud)

Finally, in the cloud scenario, the attacker used a username tlannister to create an AWS account called ahightower. To masquerade as a legitimate user, the attacker checked the existing naming convention in the victim's environment and created the account (ahightower) accordingly.

AhnLab XDR identified that the attacker retrieved the user list to check the naming convention and then created the account. The naming convention followed a pattern of adding a single letter to family names from Game of Thrones:

- a + targaryen
- t + lannister
- j + mormont
- a + hightower

In detail, AhnLab XDR first detected that tlannister (the attacker) retrieved existing user lists and policies through the ListUserPolicies and ListUsers events.

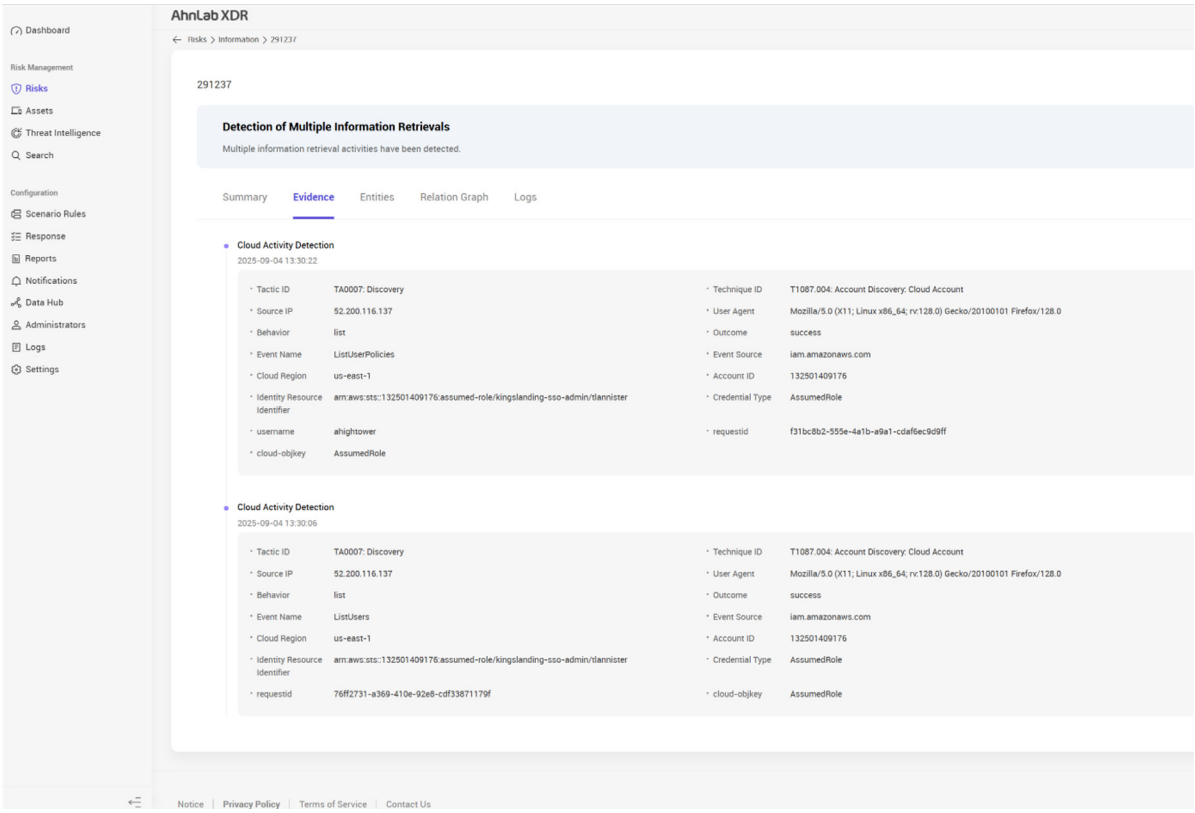

Figure 7. Detections: Substep 7.2 – Retrieving User List and Policies

Then, AhnLab XDR detected the attacker creating ahightower via the CreateUser event.

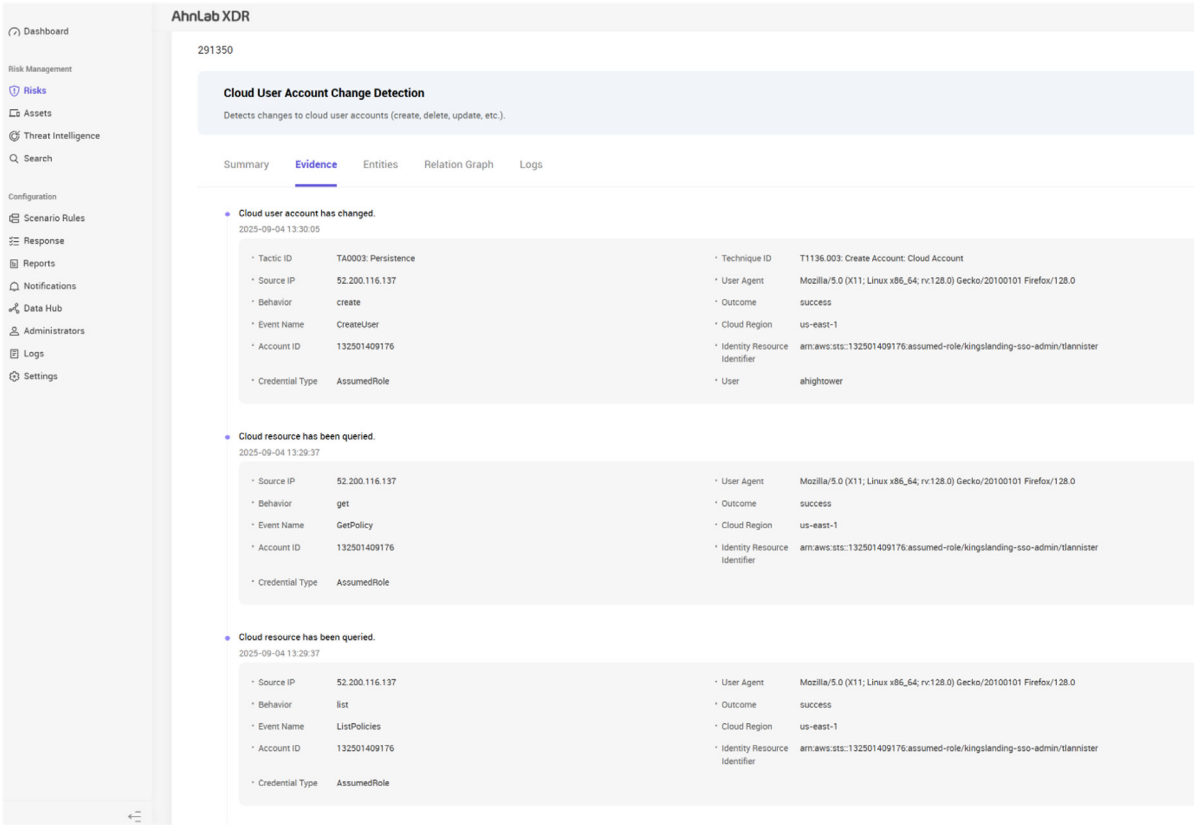

Figure 8. Detections: Substep 7.2 – Creating ahightower

For this behavior, AhnLab XDR provided the appropriate TIDs and descriptions: Defense Evasion (TA0005) and Masquerading: Masquerade Account Name (T1036.010).

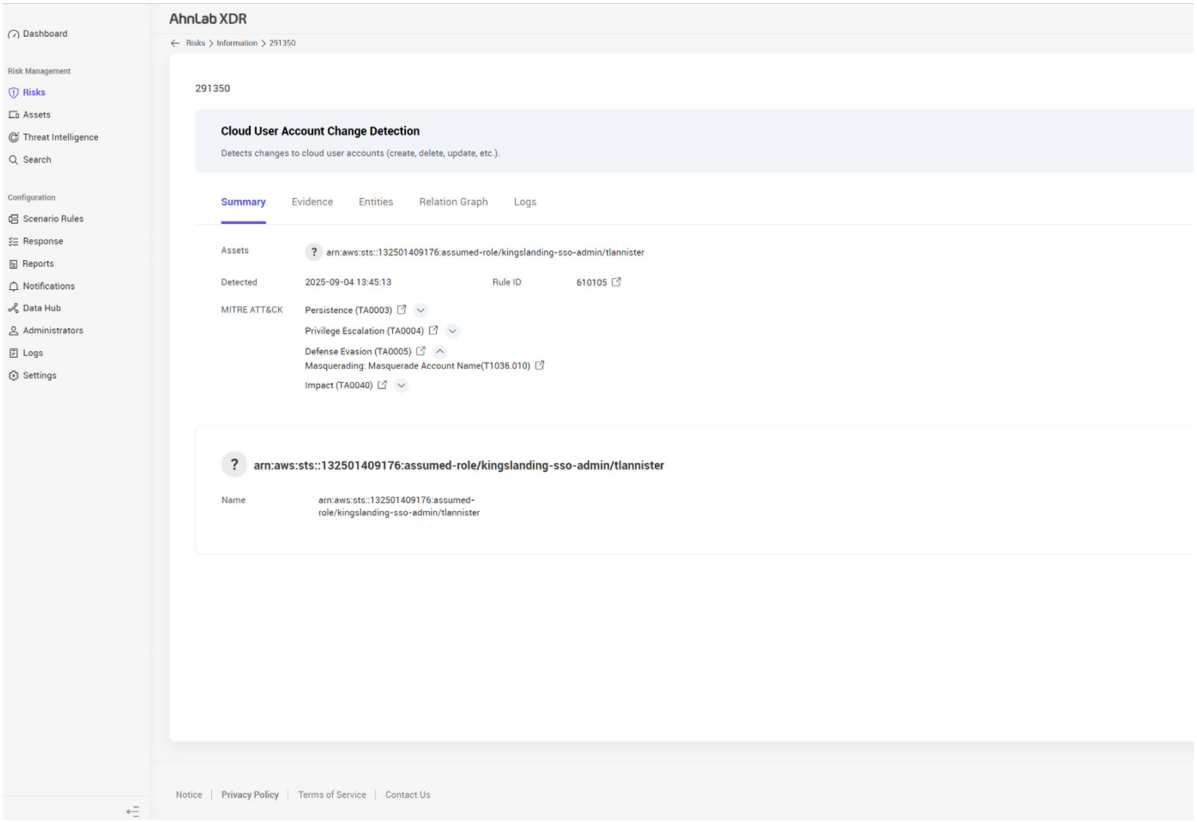

Figure 9. Detections: Substep 7.2 – Providing Corresponding TIDs and Descriptions

In summary, our evidence clearly uncovered that the attacker attempted to create cloud accounts and evade detection by disguising account names to appear legitimate.

Conclusion: Continuously Proven, Relentlessly Evolving

The MITRE ATT&CK evaluation is globally recognized for its credibility and comprises sophisticated techniques that closely resemble real-world cyber threats. In this evaluation, we successfully demonstrated our strong protection capabilities, comprehensive threat visibility, and accurate cross-domain detection across on-premises and cloud environments.

Most importantly, by participating in this evaluation for five consecutive years, we continue to ensure that our solutions are objectively assessed while relentlessly enhancing core technologies to strengthen customer trust in the long-term.

Visit the MITRE ATT&CK Evaluation website to find the results of Round 7. Also, learn more about our solutions assessed in the evaluation.

▶AhnLab EDR

▶AhnLab XDR

▶AhnLab EPP

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com / global.sales@ahnlab.com
© 2026 AhnLab, Inc. All rights reserved.