AhnLab

eBook

MITRE ATT&CK 第 7 轮评测 实现 100% 拦截率！

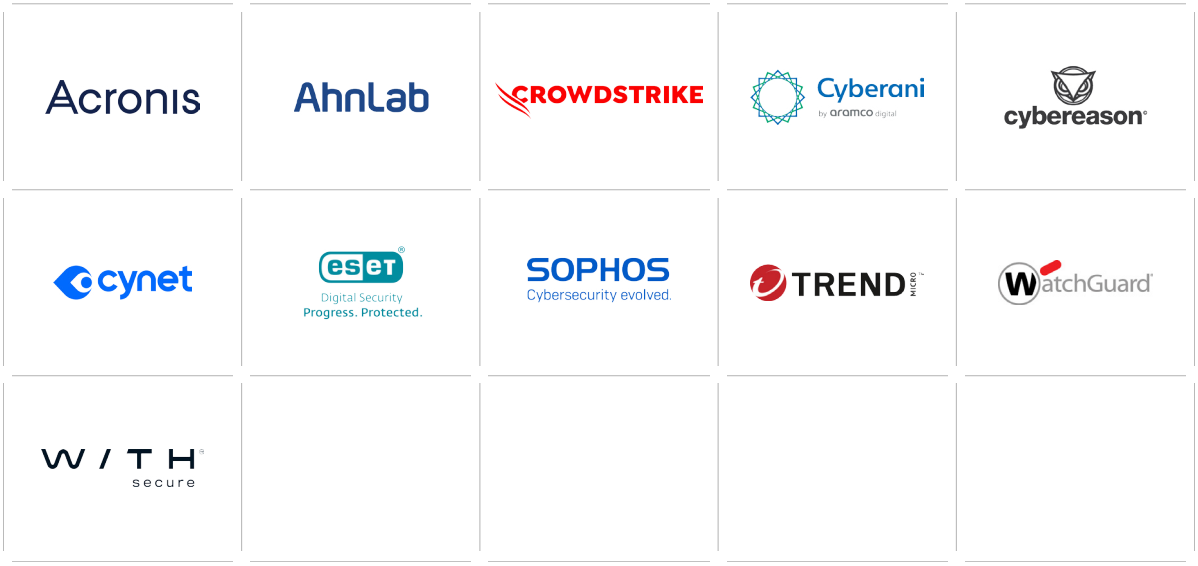
AhnLab 参与由非营利研发机构 MITRE 举办的 MITRE ATT&CK® 企业版第 7 轮评测，在防护（Protections） 领域实现 100% 拦截率。
这一成绩充分证明了 AhnLab 拥有全球领先的安全防护能力。

关于 MITRE ATT&CK 评测

MITRE 是一家在美国政府支持下开展国家安全相关研究的非营利组织，长期与政府、企业及学术机构合作，推动具有公共价值的研发（R&D）项目。
在网络安全领域，MITRE 以 MITRE ATT&CK® 框架闻名，该框架系统性地研究并定义攻击者的战术（Tactics）、技术（Techniques）与流程（Procedures，TTPs）。

MITRE ATT&CK 评测是 MITRE 实施的全球性安全产品测试，重点评估安全解决方案对已知攻击组织行为的应对能力与技术能力方面的表现。评测通过模拟主要攻击组织使用的最新攻击技术，在攻击的各个阶段测试安全解决方案的检测能力、检测证据及上下文呈现能力，以及是否具备阻断能力。该评测并非针对排名或竞争，而是基于 MITRE ATT&CK® 知识库，展示各安全厂商在威胁检测上的技术方法。

今年迎来第 7 轮评测，因其与真实攻击组织技术的高度相似性及威胁场景的完整性，被公认为全球最具权威性的安全产品测试之一。本次第 7 轮评测共有 11 家全球安全厂商参与。AhnLab 作为唯一参评的韩国厂商，自第 3 轮起已连续 5 次参与 MITRE ATT&CK 评测。



[图 1] MITRE ATT&CK 评测第 7 轮参评厂商

评测场景设计

MITRE ATT&CK 评测采用分层式场景设计结构，由威胁场景阶段（Step）及其对应的子步骤（Substep）组成。MITRE 基于该结构对威胁场景进行模拟执行，从而系统性地评测参评厂商安全解决方案的整体防御能力。

与以往轮次相比，本次评测的最大变化在于：在传统本地环境（Windows / Linux）基础上，新增了云环境评测场景。这一变化充分反映了当前攻击者在本地与云环境之间横向移动、实施复合攻击的现实趋势，使评测更加贴近真实攻击场景。

从整体架构来看，MITRE ATT&CK 评测主要包括以下两大模块：
▲检测（Detections）▲防护（Protections）

1.检测（Detections）

检测（Detections）模块用于评测安全解决方案对网络威胁的发现、分析及关联能力。MITRE 会综合各子步骤中收集到的恶意事件证据及其上下文信息，并按照以下等级体系对检测效果进行评定。检测等级从 None → General → Tactic → Technique 依次递进，等级越高，表示解决方案对攻击行为的识别越精准，对攻击阶段与技术的刻画越完整。

类别	说明
N/A	不纳入评测范围的情况
None	未提供对应子步骤的有效证据，或不符合评测要求
General	可说明存在恶意、可疑或异常行为的基础证据
Tactic	提供特定行为的背景及潜在意图等战术（Tactic）层面的上下文信息
Technique	不仅识别战术（Tactic），还提供行为方法、细节等技术（Technique）层面的完整上下文信息

[表 1] MITRE ATT&CK 评测 · 检测模块等级（恶意事件）

同时，评测还会重点验证解决方案对误报（False Positives）的控制能力。评测场景中同时包含恶意事件与正常事件，以确认解决方案是否能够准确区分攻击行为与正常业务行为。

类别	说明
N/A	不纳入评测范围的情况
Reported	对正常行为误判为恶意行为并触发告警
Not Reported	正确识别为正常行为，未触发告警

[表 2] MITRE ATT&CK 评测 · 检测模块等级（误报）

2.防护（Protections）

防护（Protections）模块用于评测安全解决方案是否能够在攻击对系统造成实质性影响之前进行有效阻断。测试结果以通过 / 未通过（Pass / Fail）的方式呈现，用于判断系统是否在关键阶段成功完成防御。

类别	说明
N/A	不纳入评测范围的情况
Protected	在恶意行为实际发生前成功完成阻断
Not Blocked	允许恶意行为发生，未能完成阻断

[表 3] MITRE ATT&CK 评测 · 防护模块评测标准

攻击组织说明

MITRE ATT&CK 第 7 轮评测延续第 6 轮的方式，通过组合多种攻击组织的攻击技术来构建整体威胁场景。本次模拟执行的攻击组织主要包括以下两大类型：▲以经济利益为目的的网络攻击组织（Financially-Motivated Cybercriminal Collective）▲以中国为背景的网络间谍组织（People’ s Republic of China，PRC Cyber Espionage Group）

各攻击组织说明如下。

1.Scattered Spider：以经济利益为目的的网络攻击组织

MITRE 在本次评测中模拟了以社会工程攻击、远程访问工具部署以及多因素认证（MFA）绕过能力著称的攻击组织 Scattered Spider。攻击者持续针对受害者的云资源展开攻击，在建立初始立足点后，进行网络与目录服务侦察，并逐步访问敏感系统及数据存储库。该组织的攻击特点是攻击节奏极快，能够在短时间内获取大量数据并迅速实施数据窃取，对企业构成严重威胁。

2.Mustang Panda：以中国为背景的网络间谍组织

此外，MITRE 还模拟了持续演进攻击能力与工具体系的中国背景网络间谍组织 Mustang Panda。该组织通常结合社会工程手段，并滥用合法工具与服务来投放定制化恶意代码。其已知的多种攻击行为与工具在中国网络攻击生态中被广泛使用，例如：LOTL（Living off the Land）攻击技术、定制化恶意代码、基于云基础设施的攻击方式。

拦截率 100%！AhnLab 领先行业的评测成果

AhnLab 以以下解决方案参与了本次 MITRE ATT&CK 评测：△下一代终端检测与响应解决方案 AhnLab EDR △终端安全平台 AhnLab EPP △SaaS 型安全威胁分析平台 AhnLab XDR在防护（Protections）评测模块中实现 100% 拦截率的同时，AhnLab 在覆盖本地环境与云环境的一体化威胁可视性及检测准确性方面也取得了备受瞩目的成果。

从用户角度来看，AhnLab 本次评测结果在以下方面值得关注：

1.100% 威胁阻断！验证行业领先的安全实力

AhnLab 在防护（Protections）模块中成功阻断了 100% 的恶意行为，确保评测环境中的系统在攻击发生前即得到有效保护，再次验证了其在 MITRE ATT&CK 评测、全球认证及真实客户环境中持续获得验证的行业领先安全能力。

值得一提的是，本次防护评测中还包含仅由正常行为构成的测试场景。AhnLab 能够准确识别这些正常行为，并未进行误阻断，充分证明了其在阻断能力之外，同样具备极高的判断准确性。

换言之，AhnLab 能做到只阻断应被阻断的恶意行为，同时放行正常业务活动，在真实用户环境中同时实现强安全性与高可用性的平衡。

2.覆盖本地环境与云环境的全面威胁可视性

如前所述，MITRE ATT&CK 第 7 轮评测采用了融合本地环境（Windows / Linux）与云环境的混合攻击场景。在该场景下，AhnLab 各项解决方案针对跨操作系统的高级攻击技术，提供了详细的事件证据与分析信息。通过这些证据，用户能够从攻击行为的“上下文（Context）”出发，全面理解威胁的发生过程与影响范围。

在今年新引入的云场景中，AhnLab 将旗下 XDR 解决方案 AhnLab XDR 与评测环境中的云资源进行联动，构建威胁检测体系。AhnLab XDR 以“开放式 XDR（Open XDR）”为理念，能够有效检测攻击者在本地环境与云环境之间横向移动时实施的恶意行为，并持续提供上下文信息。通过本次评测，AhnLab 不仅在传统本地环境中验证了自身实力，也进一步证明了其在云环境下同样具备卓越的威胁检测能力。

3.精准检测率（False Positives）达 90%，实现“零延迟检测”

针对用于评估检测准确性与质量而构建的正常事件场景，AhnLab 取得了约 90% 的正确识别率。这意味着，解决方案在面对正常业务行为时，未触发不必要的威胁告警，有效降低了误报问题。该结果表明，AhnLab 的解决方案能够基于精准检测能力，切实缓解客户在日常安全运营中普遍面临的过度告警（误报）困扰。

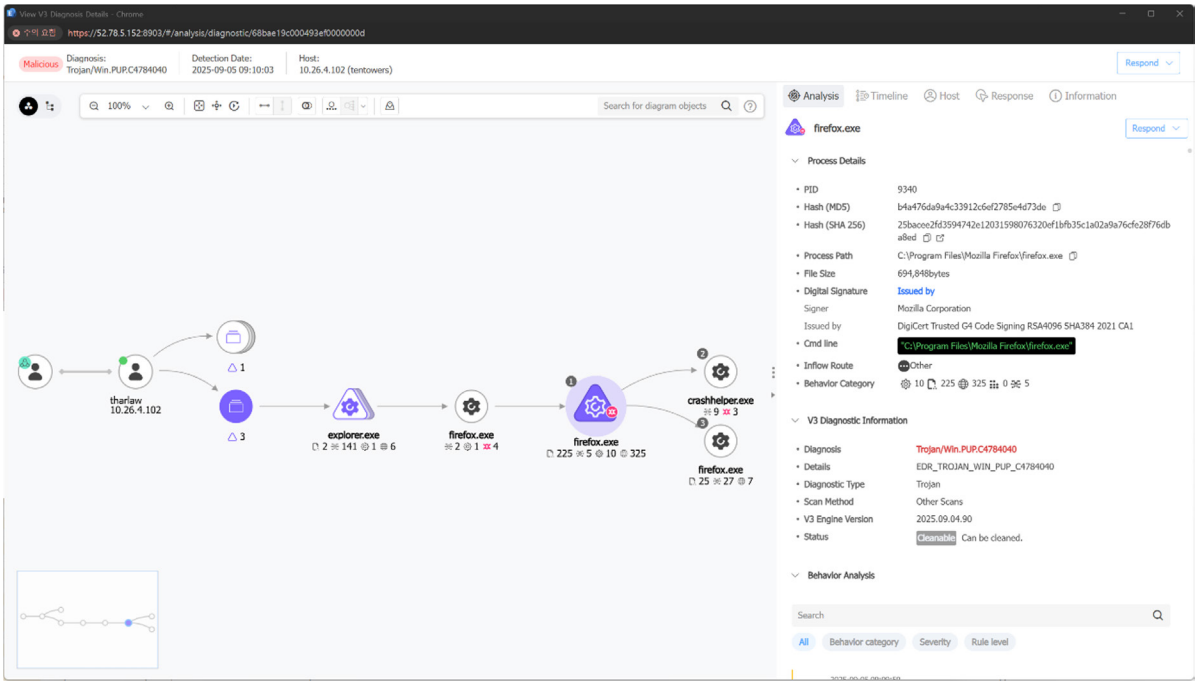
此外，MITRE ATT&CK 评测还同时验证了检测告警是否存在延迟（Delay）。这是因为在真实环境中，用户需要第一时间获取检测结果并快速展开威胁响应。在本次评测中，AhnLab 的各项解决方案均以实时方式提供检测结果，成功实现了“零延迟检测（Zero Delay）”。

实际评测中的威胁检测实例

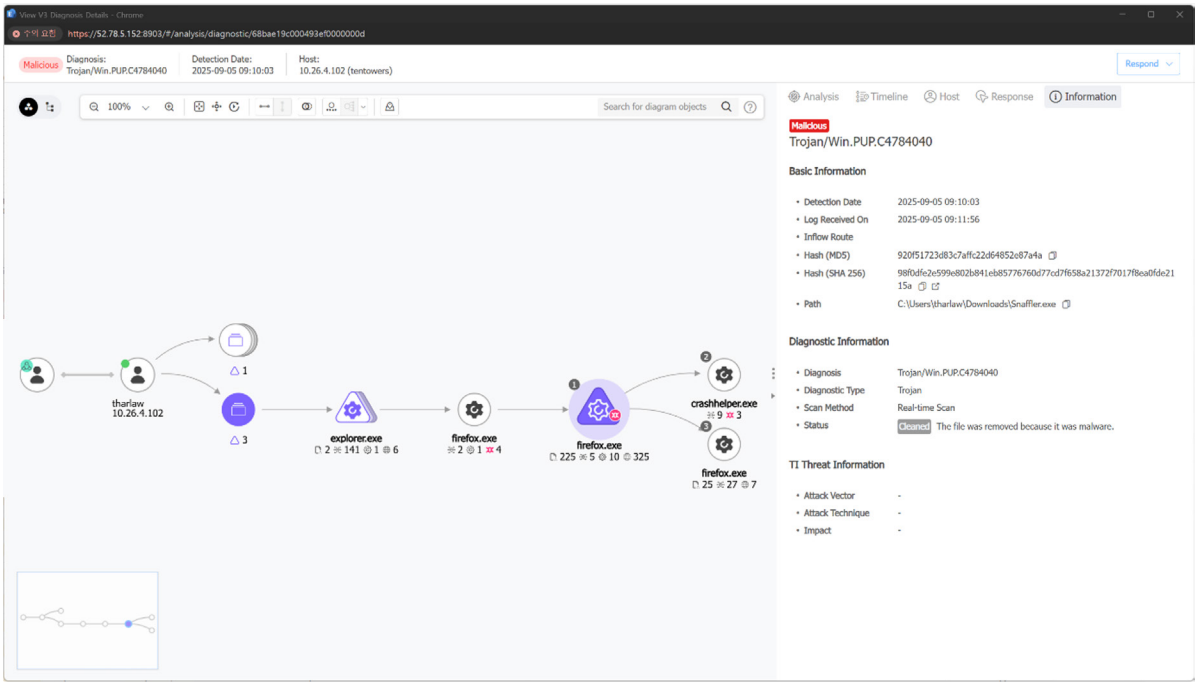
在 MITRE ATT&CK 第 7 轮评测中，AhnLab 的各项解决方案在 Windows、Linux 以及云环境中全面展现了卓越的威胁检测与阻断能力。下面将通过具体实例，说明 AhnLab 是如何在实际评测场景中实现检测与防护的。

1.防护（Protections）：Test 1

攻击者成功侵入受害者环境后，使用用户账户 tharlaw 从文件服务器下载了名为 Snaffler.exe 的可执行文件。在下载文件的同时，攻击者还触发了对本地磁盘与网络共享状态的扫描行为。



[图 2] Protections：Test 1 – 文件下载证据

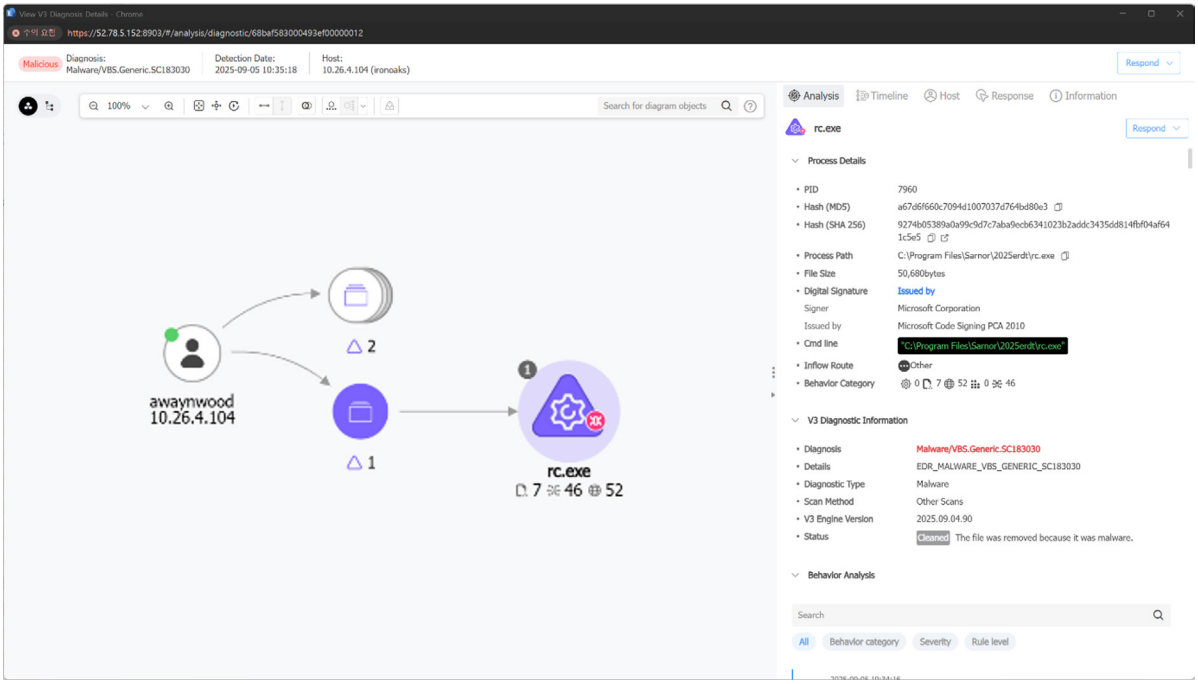


[图 3] Protections：Test 1 – 文件拦截证据

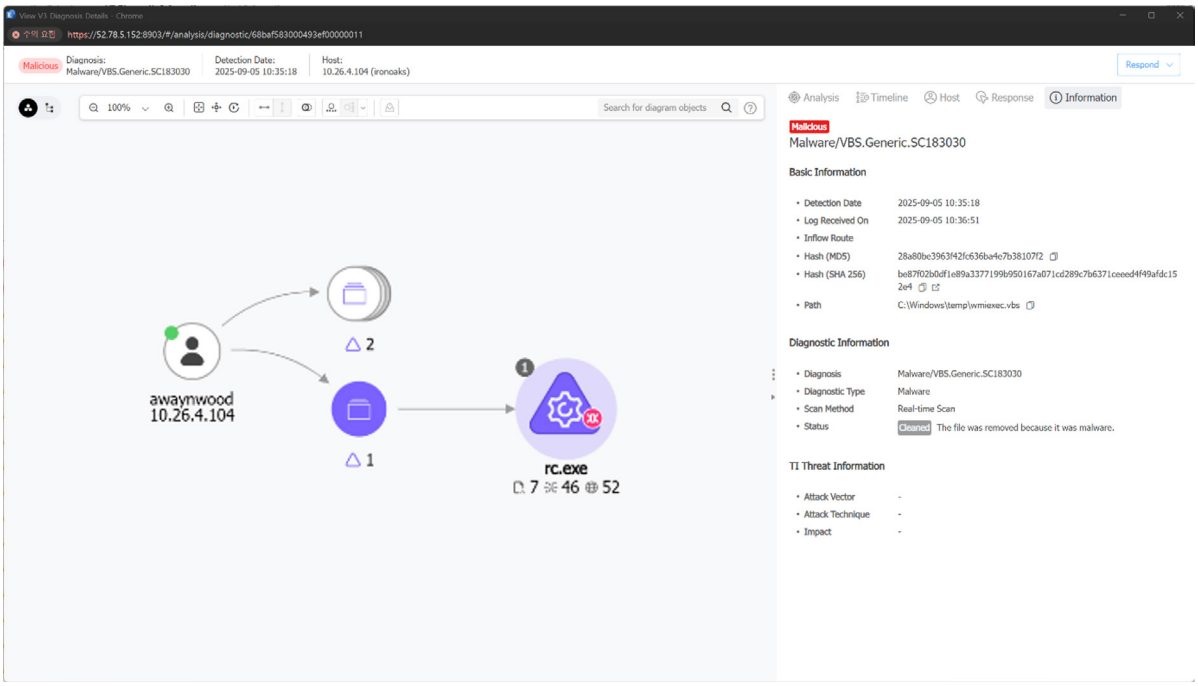
AhnLab EDR 检测到从外部下载的可执行文件 Snaffler.exe 含有恶意特征码。随后，通过与 AhnLab 的防病毒解决方案 AhnLab V3 联动，将其诊断为 Trojan/Win.PUP.C4784040 并成功拦截，从而在恶意行为实际发生前完成阻断。不仅实现了对恶意文件的拦截，还通过 EDR 与防病毒解决方案的协同分析，向用户呈现了拦截发生的具体背景与上下文，意义重大。

2.防护（Protections）：Test 5

在另一受感染环境中，攻击者使用用户账户 awaynwood，通过远程命令执行工具将 wmiexec.vbs 下载至 C:\Windows\Temp 路径。随后，攻击者利用该脚本在文件服务器 heartshome（10.26.3.106）上创建了网络共享。



[图 4] Protections：Test 5 – 文件下载证据

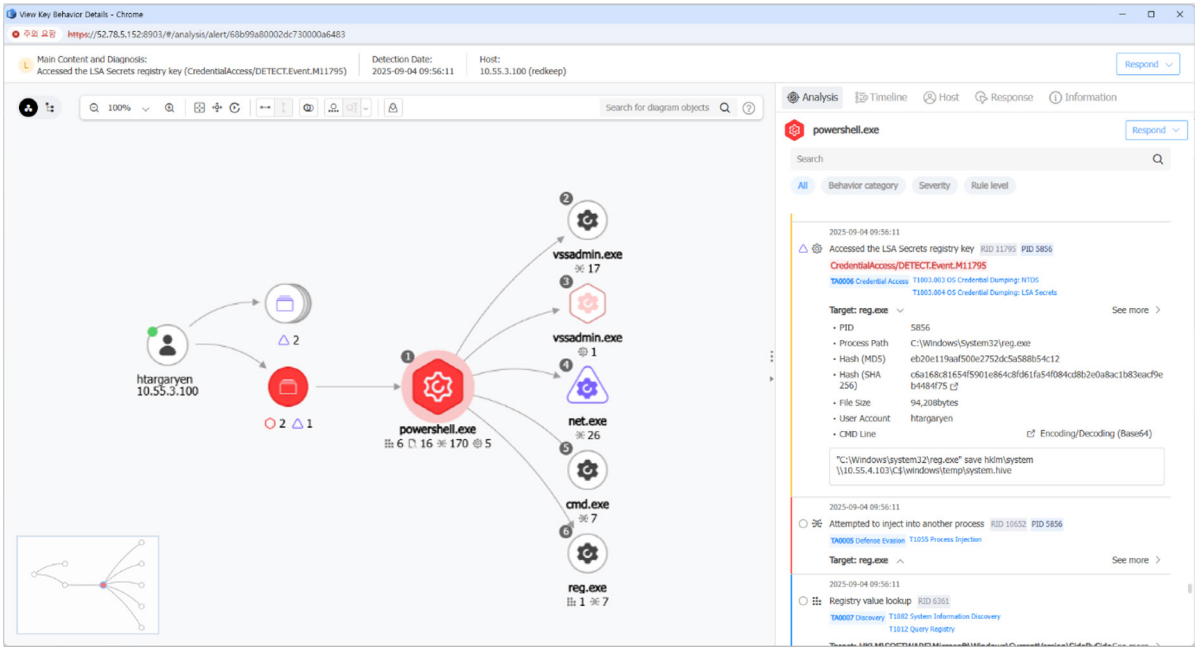


[图 5] Protections：Test 5 – 文件拦截证据

与 Test 1 类似，AhnLab EDR 检测到下载至 C:\Windows\Temp 路径下的 wmiexec.vbs 含有恶意特征码。AhnLab 随即通过 AhnLab V3 将其诊断为 Malware/VBS.Generic.SC183030 并完成阻断，防止攻击进一步扩散。

3.检测（Detections）：Substep 7.5 – 本地环境（On-Premise）

攻击者使用用户账户 htargaryen，在域控制器 redkeep（10.55.3.100）上利用 NTDS 凭据转储方式提取 NTDS 文件，并尝试进行离线破解。作为该攻击链的一部分，攻击者在 redkeep 上执行 reg.exe，试图将系统注册表 Hive 远程保存至 \\10.55.4.103\C$\Windows\Temp\system.hive（目标主机：harrenhal）。



[图 6] Detections：Substep 7.5 – 系统 Hive 外泄行为检测

AhnLab EDR 通过行为关联图，清晰展示了攻击者使用未签名的 reg.exe 远程导出系统 Hive、以实施域凭据窃取的攻击流程。系统准确识别并标注了关键路径，包括：

- 注册表 Hive 路径：HKLM\SYSTEM
- 远程 UNC 存储位置：\\10.55.4.103\C$\Windows\Temp\system.hive

同时，AhnLab 提供了与该行为高度匹配的 TID：

- TA0006 Credential Access
- T1003.002 OS Credential Dumping: Security Account Manager

由此，用户能够对攻击者的凭据窃取意图与执行过程形成清晰、完整的理解。

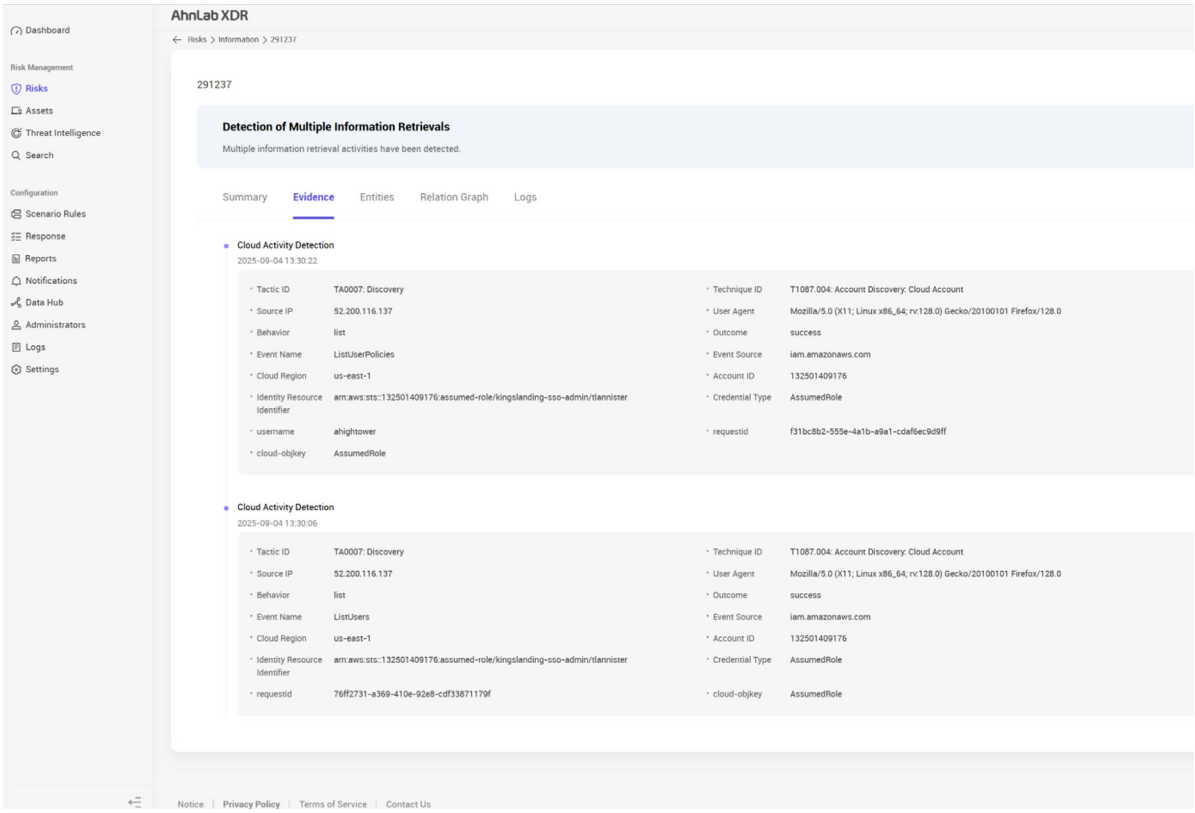
4.检测（Detections）：Substep 7.2 – 云环境（Cloud）

在云环境中，攻击者使用用户账户 tlannister 创建了一个新的 AWS 账户 ahightower。在创建账户前，攻击者先查询了受害环境中已有的命名规则，以便伪装成正常用户。

AhnLab XDR 发现，攻击者在创建账户前，通过获取用户列表来分析命名体系。该命名规则以《权力的游戏》中家族名称为基础，并在前方添加一个字母，例如：

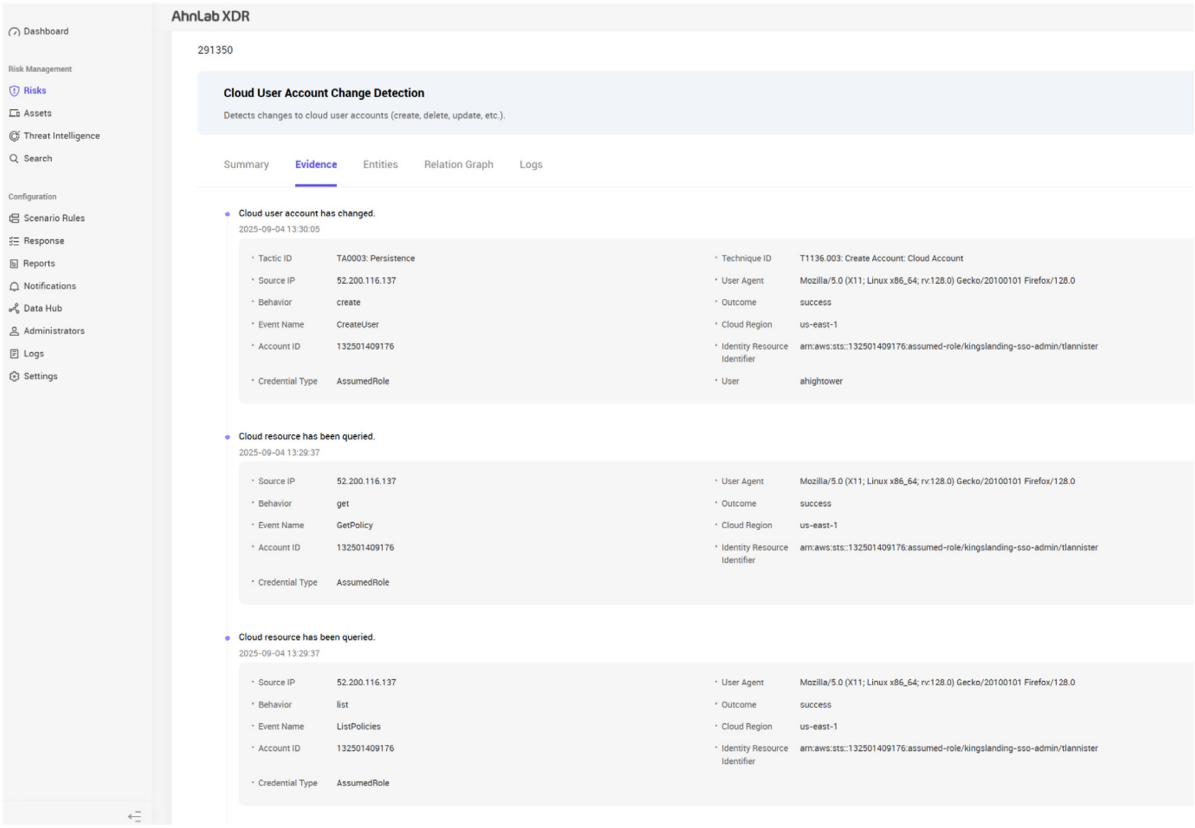
- a + targaryen
- t + lannister
- j + mormont
- a + hightower

首先，AhnLab XDR 检测到 tlannister（攻击者） 通过 ListUserPolicies 与 ListUsers 事件获取用户列表与相关策略。



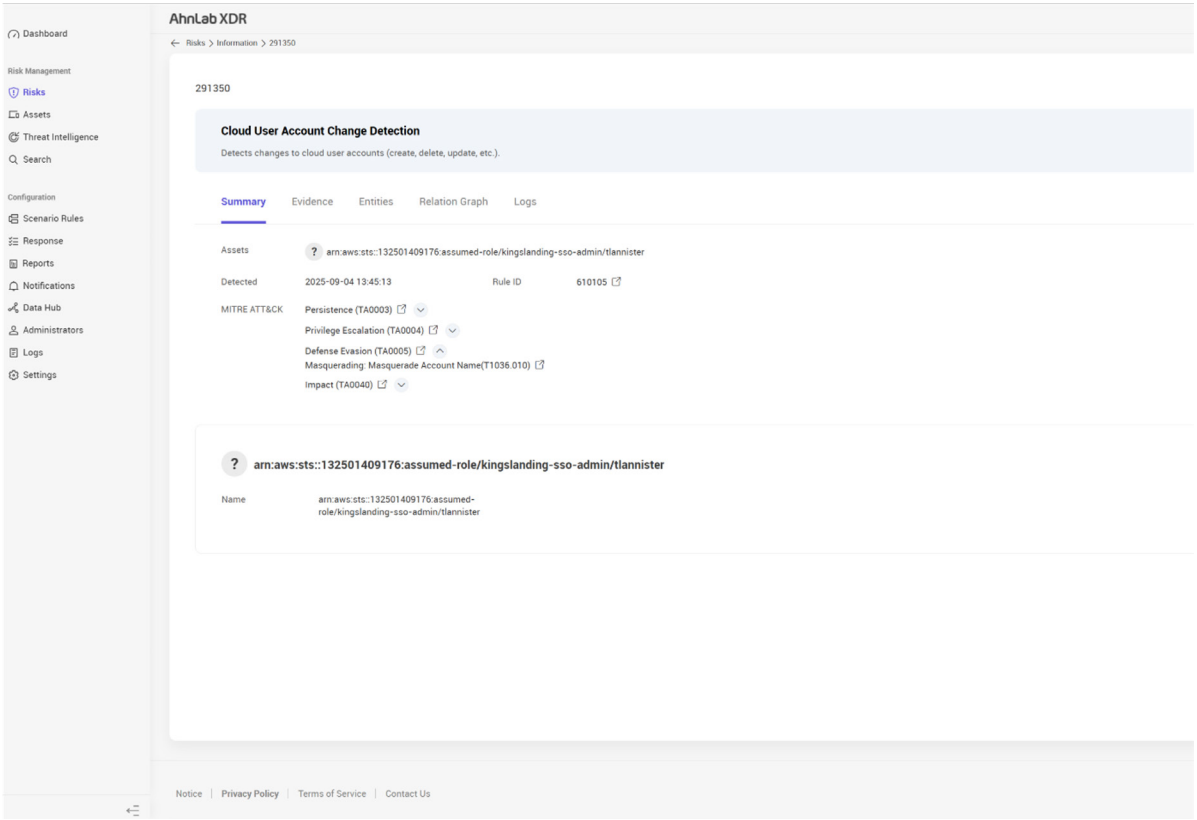
[图 7] Detections：Substep 7.2 – 获取用户列表与策略

随后，系统检测到攻击者通过 CreateUser 事件创建了账户 ahightower。



[图 8] Detections：Substep 7.2 – 创建 ahightower 账户

针对上述行为，AhnLab XDR 提供了准确匹配的 MITRE ATT&CK 技术映射（TID），包括：
- Defense Evasion（TA0005）
- Masquerading：Masquerade Account Name（T1036.010）



[图 9] Detections：Substep 7.2 – 提供匹配的 TID

通过完整的行为链与上下文分析，AhnLab XDR 使用户能够清晰理解：
攻击者通过伪装账户命名方式，试图规避检测并冒充正常用户的攻击意图与手法。

结论：以经过验证的技术实力，守护客户安全

MITRE ATT&CK 评测被公认为全球最具权威性的测试，采用与真实威胁高度相似的精细技术场景。AhnLab 在本次评测中，全面展示了覆盖本地与云环境的强大拦截能力、全面威胁可视化及精准检测实力。尤为值得一提的是，AhnLab 已连续 5 年参与 MITRE ATT&CK 评测，不仅通过持续、客观的第三方验证来证明自身技术实力，还通过不断推进解决方案的迭代与升级，持续增强客户信任，具有重要意义。

MITRE ATT&CK 第 7 轮评测详细结果可在 MITRE 官方网站查看。参与本次评测的 AhnLab 产品的更多信息，也可通过 AhnLab 官方网站进行了解。
▶了解更多 AhnLab EDR
▶了解更多 AhnLab XDR
▶了解更多 AhnLab EPP

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区新镇路1699弄E栋303室
https://www.ahnlab.com/cn | cn.sales@ahnlab.com
电话： +86 10 8260 0932（北京）| +86 21 6095 6780（上海）