AhnLab

Case Study

AhnLab XDR Utilization Strategy in the Golfzon Ransomware Case

Industry

Sports simulation software

Benefits

- Rapid deployment of AhnLab XDR in a SaaS model
- Enhanced event visibility across security solutions and proactive threat response
- Expert-driven event analysis and reporting through AhnLab MDR integration
- Enhanced productivity for security teams
- Reduced overall organizational risk through enhanced detection accuracy
- Full utilization of the technical and operational network established with AhnLab

Solutions

- AhnLab V3
- AhnLab EDR
- AhnLab EPP
- AhnLab MDR
- AhnLab XDR

Overview

Golfzon is a leading company specializing in golf simulators (GS), integrating its core information technology (IT) with golf to provide innovative and immersive golf services.

Golfzon adopted AhnLab's security solutions to strengthen its organizational security and provide safe and reliable services to its customers. By implementing AhnLab's endpoint and integrated security solutions, the company has reduced threat risks and ensured service stability.

Following a ransomware incident in 2023, Golfzon deployed AhnLab EDR and EPP solutions across its internet network, IDC, AWS, and electronic financial networks. Additionally, the company introduced AhnLab MDR, a managed detection and response service, enabling AhnLab's threat experts to actively analyze detected threats and provide response strategies. To further optimize security risk management, Golfzon expanded its deployment by adding AhnLab XDR alongside AhnLab EDR. With AhnLab V3, AhnLab EDR, and AhnLab EPP already deployed, Golfzon was able to smoothly implement AhnLab XDR. These solutions empower Golfzon with real-time threat detection and response capabilities, ensuring ransomware recovery and service continuity.

By continuously launching and operating security-enhanced golf products and services, Golfzon is committed to delivering the best golf experience to its customers.

> With AhnLab's support, Golfzon was able to swiftly recover from the ransomware incident and identify and address the attacker lurking in the internal network. We also greatly benefited from actively leveraging the technical and operational network built together with AhnLab through existing managed security service. Moving forward, Golfzon will continue to collaborate with AhnLab to develop secure and reliable golf services and products.
>
> ***- Jeong-hoon Kim, Information Security Team, Golfzon***

Challenges

- Ransomware incident caused by BlackSuit
- Insufficient framework for managing and responding to multiple events
- Need for more effective operation of AhnLab EDR
- Need to adopt an approach for determining event priority and importance

Challenges

On November 23rd, 2023, Golfzon experienced a service disruption due to an attack by the ransomware group "BlackSuit." The stolen information was subsequently exposed on the dark web.

During the incident analysis, Golfzon discovered that the threat actor had exploited authorized user privileges to carry out various malicious activities. Additionally, the threat actor continued launching attacks using Golfzon's internal information even after the ransomware incident. Recognizing the severity of the situation, Golfzon deployed AhnLab EDR to analyze all endpoint activities and prevent further attacks. In addition, the company installed the endpoint protection platform "AhnLab EPP" on its servers and endpoints with AhnLab's support.

As Golfzon had been operating over 20 different security solutions, manually handling and responding to individual events from them proved to be challenging. It was difficult to determine whether each alert was a false positive, an actual attack that is relevant for further investigation. The lack of sufficient resources, personnel, and tools further complicated the process of thoroughly reviewing these events.

As a result, Golfzon collaborated with AhnLab to deploy AhnLab XDR, enabling the identification of relevant threats among the millions of daily alerts and allowing proactive measures to be taken. This also enhanced the efficiency of their existing AhnLab EDR operations.

Solutions

Golfzon had already deployed AhnLab EDR and AhnLab EPP, while also leveraging AhnLab MDR to effectively manage a wide range of endpoint threats. Following the ransomware incident, AhnLab's threat intelligence analysis team, A-FIRST, conducted an in-depth investigation of the breach, diagnosing vulnerabilities and providing tailored remediations.

To address the challenge of manually responding to individual events generated by multiple security solutions, Golfzon deployed AhnLab XDR. Implemented as a SaaS-based solution, AhnLab XDR eliminated concerns related to hardware expansion and performance limitations caused by data volume, enabling rapid deployment. Additionally, it ensured seamless operations without compromising the availability of servers and endpoints.

Golfzon integrated asset data of more than 1,500 PCs and over 700 servers with AhnLab XDR, combining logs from security systems and key operational solutions. Based on detection scenarios, it configured the system to send threat notifications via email, Telegram, and other communication platforms. Through this, Golfzon aimed to expand AhnLab XDR's capabilities beyond individual security solution management to enterprise-wide risk management and response.

Solutions

- Deployed AhnLab EDR and EPP, and leveraged AhnLab MDR support for in-depth breach analysis
- Implemented AhnLab XDR in a SaaS model to resolve hardware expansion and performance issues
- Deployed AhnLab XDR and integrated it with key asset information

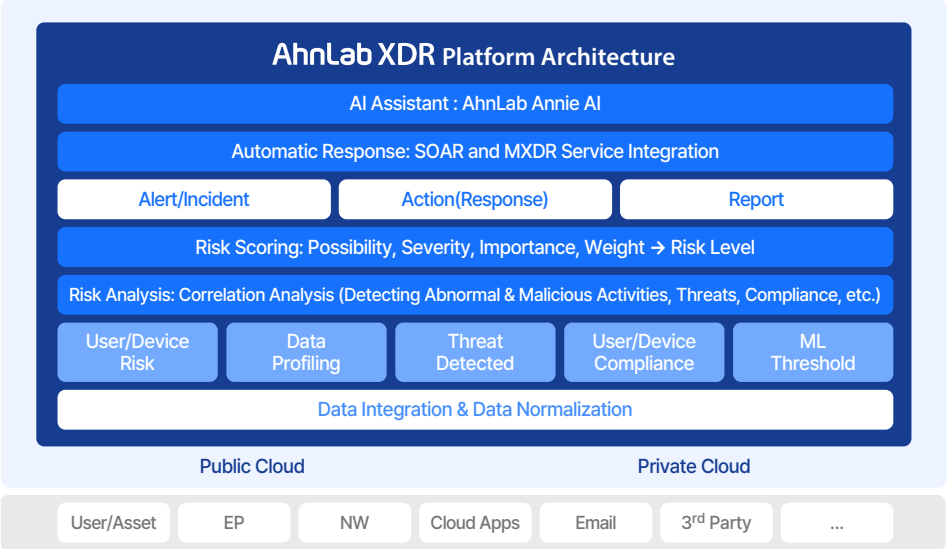

Figure 1. AhnLab XDR Platform Architecture

Benefits

After introducing AhnLab XDR following AhnLab EDR/MDR and EPP, Golfzon's overall security posture has improved. The company can now carry out analysis and processes that are both intuitive and meaningful through correlation analysis of various security solution logs centered around AhnLab XDR.

Golfzon was able to reduce false positives and minimize resource waste on low-priority threats generated by the security systems. At the same time, it implemented an effective security framework for pinpointing incident histories that could not be detected or responded to by the security team. As a result, Golfzon has achieved improvements in blocking suspicious malicious IP access, abnormal VPN logins, and brute force attacks, as well as enhancing unmanaged firewall policies. This has led to a significant reduction in overall security events.

In fact, the number of security risks decreased from 3,046 in May 2024 to 1,691 in August 2024, marking a 56% reduction within 3 months. Among them, the risks identified in the endpoint domain dropped from 1,840 to 264, showing an 86% decrease.

Figure 2. Reduction in Golfzon's Internal Risks After Implementing AhnLab XDR

Benefits

- Intuitive security management through log correlation analysis
- Reduction in overall security events
- Improved detection accuracy and increased productivity of security personnel
- Maximized efficiency in data collection and integration

The detection accuracy rate was improved and security personnel's productivity increased. Also, the Data Hub allowed the company to enhance its security while also making data collection and integration more efficient.

Future Plans

Golfzon aims to actively utilize AhnLab's security solutions as part of its continuous investment and efforts to enhance security. In particular, the company will establish a stronger security framework based on AhnLab XDR to proactively address the increasingly complex threat landscape. By using AhnLab XDR, Golfzon will conduct advanced correlation analysis between events from various security solutions. This will strengthen company-wide risk management and response, and enhance real-time threat monitoring, detection, and analysis capabilities.

Golfzon is currently considering implementing AhnLab's MXDR service. AhnLab MXDR is a dedicated XDR management service that is separate from MDR, where AhnLab's security experts identify internal threats, conduct in-depth analysis, eliminate them, and send real-time alerts. AhnLab is currently working to strengthen Golfzon's security by providing real-time updates via email on risk detection reports, unusual findings, and malware detection recommendations through its MDR services.

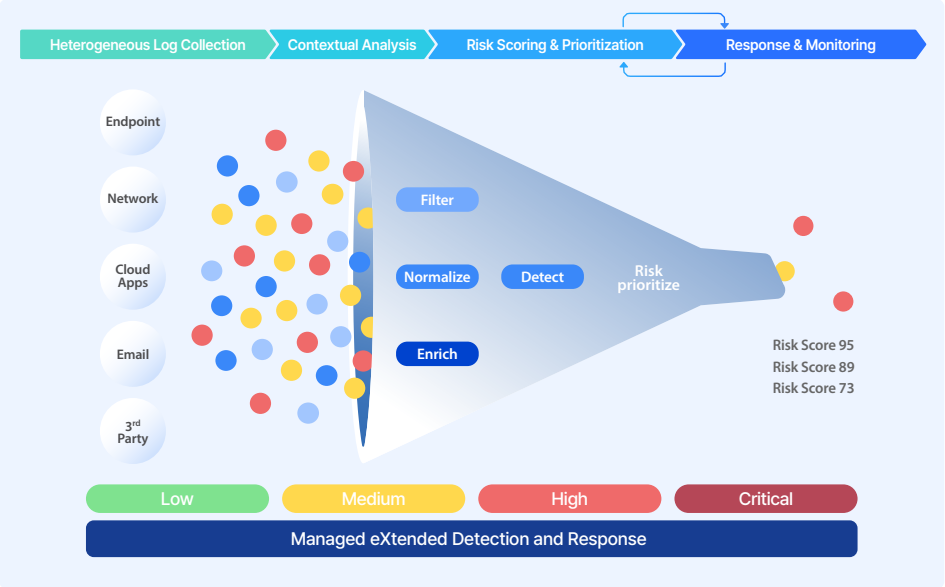

Figure 3. AhnLab MXDR Threat Detection/Response Process

In the future, Golfzon will continue collaborating with AhnLab to enhance security assessments and monitoring for not only endpoints but also cloud environments and external systems, ensuring that threat actors do not target Golfzon's infrastructure. Through the collaboration, Golfzon aims to provide stable services to its customers and solidify its leading position within the industry.

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com/en | global.sales@ahnlab.com