AhnLab XDR

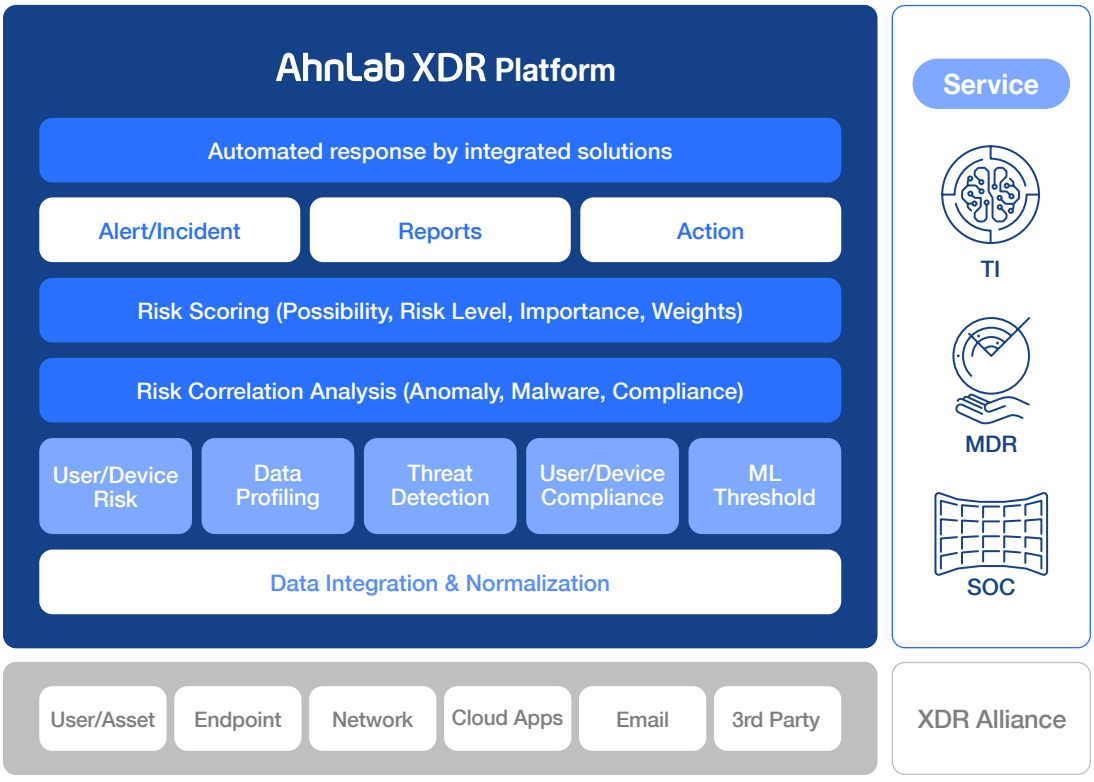
The Evolution of Threat Detection & Response

AhnLab XDR enables our customers to effectively cope with cyber threats across all security domains by delivering precise threat detection, correlation analysis, and risk scoring capabilities.

Overview

As cyber threats become sophisticated in the digital transformation era, organizations are adopting more security products to defend against modern attacks. The increasing number of point products makes cybersecurity staff struggle with addressing a massive amount of security events and prioritizing cyber risks. Businesses are now expecting a holistic security approach, and this is where XDR(eXtended Detection and Response) comes in.

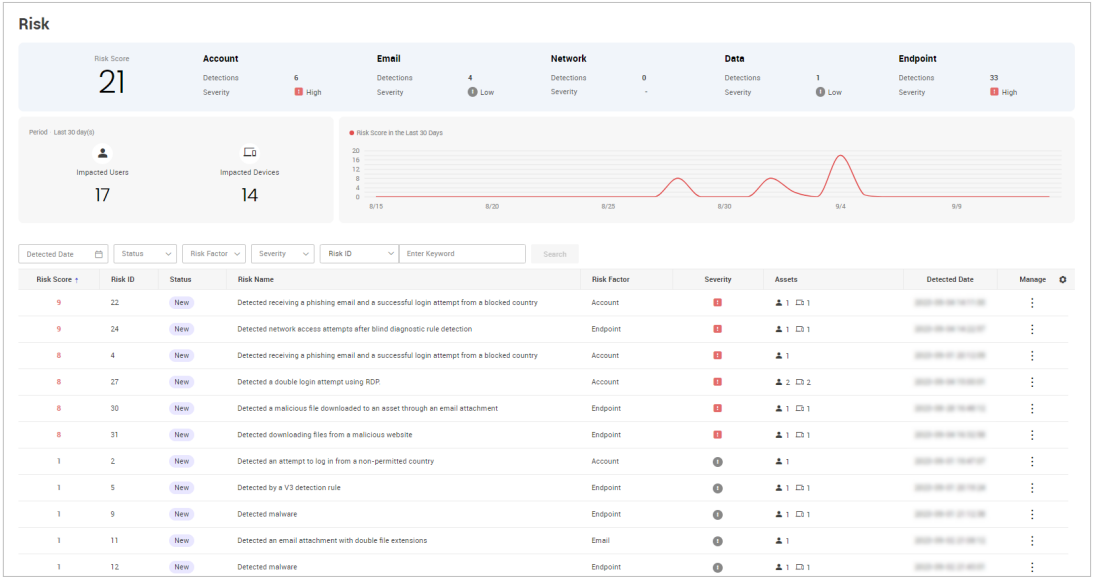
AhnLab XDR is a cloud-based, SaaS-delivered platform that collects and analyzes logs from various systems and helps customers prioritize and manage cyber risks. Powered by artificial intelligence and machine learning technology, AhnLab XDR integrates and normalizes logs from heterogeneous products and performs user/asset-based risk analysis, ultimately allowing customers to upgrade their security with an optimal response capability.



Key Features

Risk Scoring

AhnLab XDR normalizes and enriches the initially collected data and conducts a correlation analysis. Then, it generates a risk score based on the analysis that ultimately enables customers to build a threat response strategy with a thorough understanding of the priority and impact of cyber threats.



Up-to-date Scenario Rules

AhnLab XDR is equipped with pre-defined scenarios of existing and prevalent cyber risks. By continuously updating the scenario rules, AhnLab XDR ensures users always stay ahead of the latest threats.

* **Scenario Example: An insider attempts to leak the critical file**

Set threshold by analyzing the user behavior pattern for a month

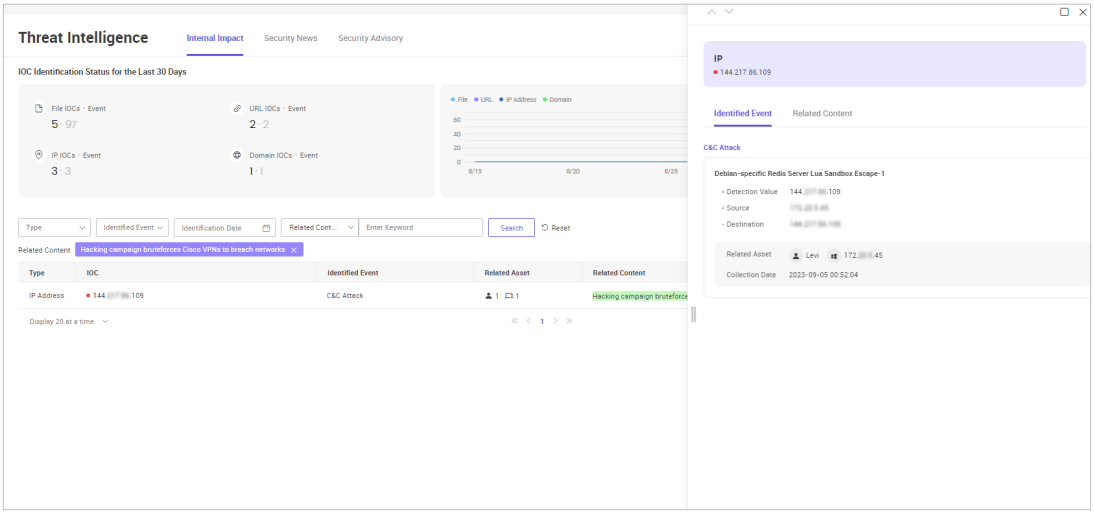
- ✓ Working from 9am to 7pm
- ✓ Downloading less than ten files per hour
- ✓ Uploading files to the internal server – less than 300mb per month
- ✓ Not using an external email account
- ✓ Merely sending files to external email – less than 10mb per month

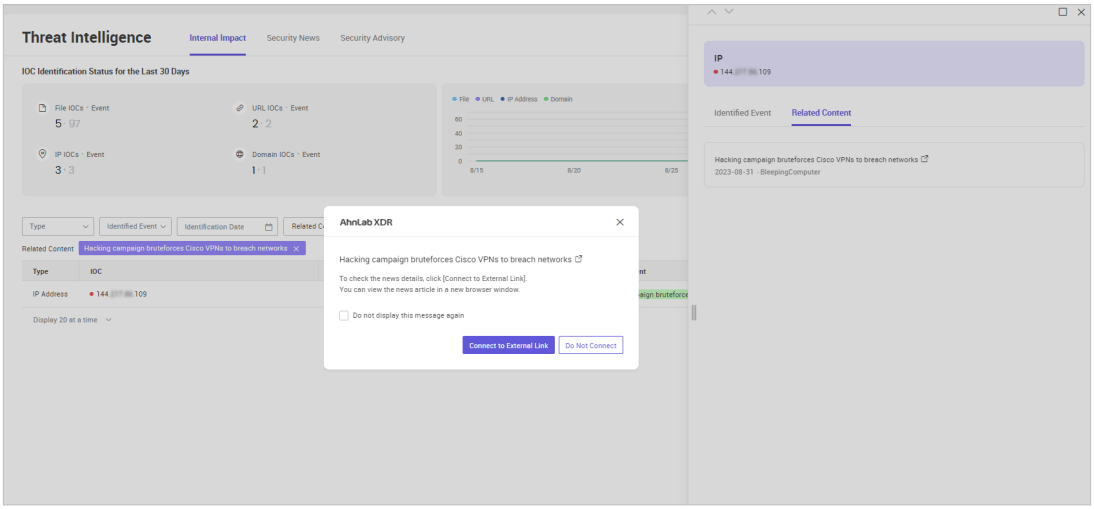
Information	Behavior	Timeline
Account	Logging in to the proper user account	9:00pm
Time/Location	Working at 9pm (office)	
System Access	Accessing the internal document management system	9:00pm
	File size increased	
Download History	Downloading 200 project files	9:01pm - 9:30pm
File Compression History	Compressing multiple project files	9:31pm
	Accessing individual email account	
External System Access	Logging in to external email	9:35pm
	Attachment size increased / Off-business hours	
File Attachment History	Attaching large file to the email	9:36pm
None	AhnLab XDR detects and blocks suspicious behavior of data leakage	9:37pm
None	Security team checks AhnLab XDR dashboard	10:00am (next day)

Key Features

Threat Intelligence based Monitoring

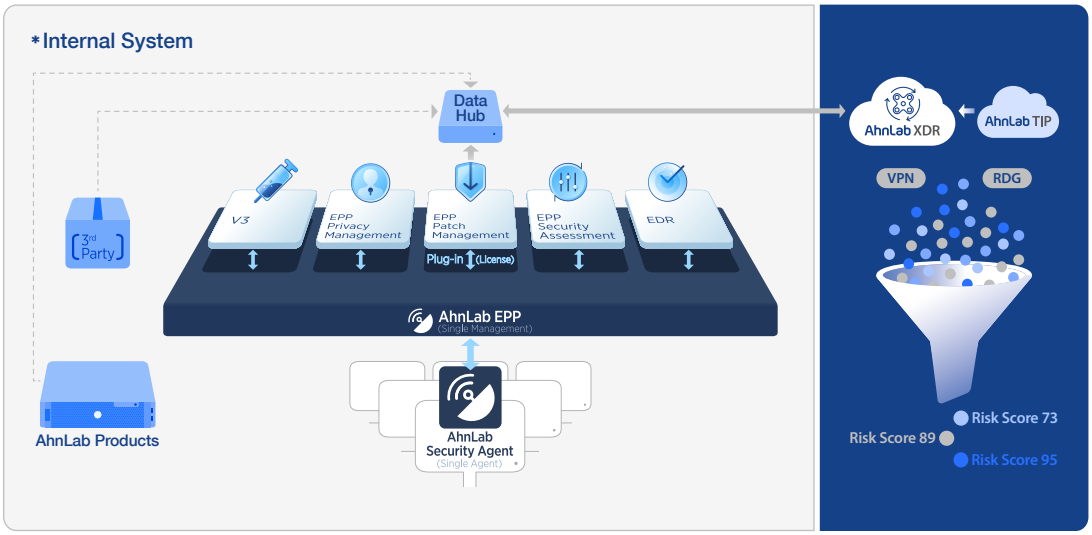
AhnLab XDR offers a threat intelligence-based monitoring feature that allows customers to check how much their assets are related to IOCs confirmed by AhnLab TIP and carry out an immediate response measure. Also, the integration with AhnLab TIP provides richer content for customers, such as news clipping and security advisory.





Log Collection and Integrated Threat Response

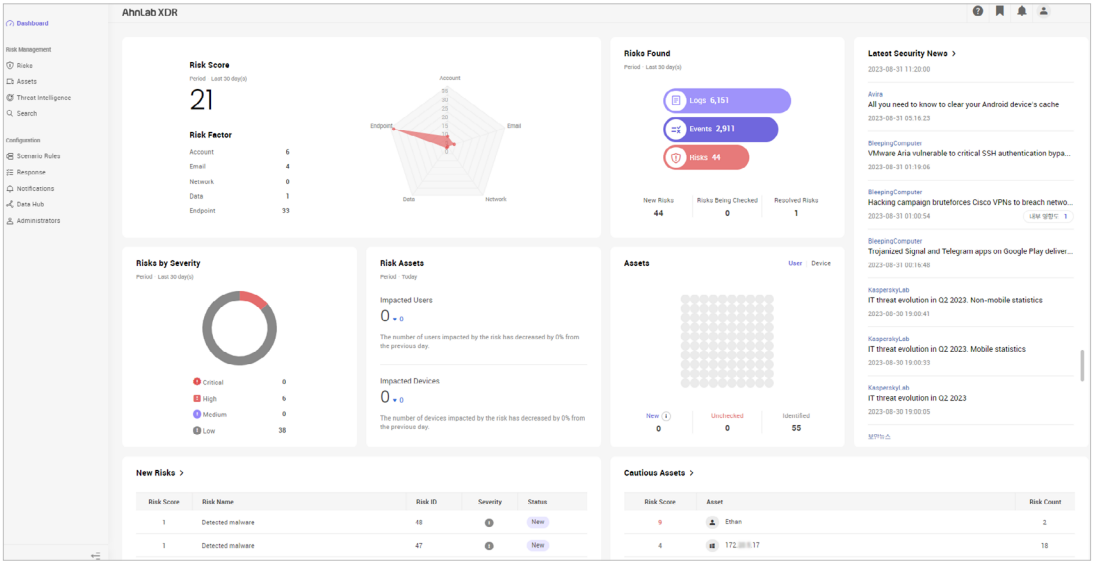
Interoperating with our EPP and EDR, AhnLab XDR can collect additional data from users/assets and leverage them for an optimal response. The data acquisition process does not require the agent as the data can be collected from AhnLab Data Hub, where all the security product data reside.



Dashboard

AhnLab XDR dashboard displays the current risk level of the organization in the form of “Risk Score” and allows an intuitive view of related users and assets. Risks of users and assets are categorized into the five risk factors, and detection details for each factor can be found in 'Risk Details.'

The dashboard also visualizes the risk severity of logs and events collected over the last 30 days as well as the status of “top 5 risks”, “newly identified risks”, “risks being addressed”, “resolved risks”, “newly identified or unidentified users”, and “risky assets”. Moreover, by integrating with AhnLab TIP, our XDR delivers rich content including the latest news and IOC information via the dashboard.



Benefits

With AhnLab XDR, customers can precisely identify the risks and prioritize them based on the risk score. For the risk that needs to be addressed, seamlessly integrated security products offer optimized response measures. All in all, the benefits of AhnLab XDR truly matter as it essentially improves an organization’s level of security as well as operational efficiency.

Precise Risk Identification

AhnLab XDR monitors assets (device ID, host name, IP, Mac, etc.) of users (ID, company name, department name, employee name, email address, etc.) and precisely identifies the risk by conducting correlation analysis on “entity status”, and “user/device behavior”.

Seamless Interoperation, Systematic Response

AhnLab XDR collects logs from heterogeneous products and performs data correlation analysis, allowing customers to systematically respond to the confirmed incident by leveraging features of different products.

Advanced Security with Better Efficiency

Our SaaS-delivered XDR offers continuous updates as well as better operational efficiency. The integration of AhnLab XDR with our threat intelligence platform allows customers to check the latest cyber threats and level of impact on their assets. Moreover, it can collect logs from different products without the agent, minimizing performance impact.

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

AhnLab