AhnLab CONNECT PLUS

AhnLab TIP

The Most Actionable Threat Intelligence Platform

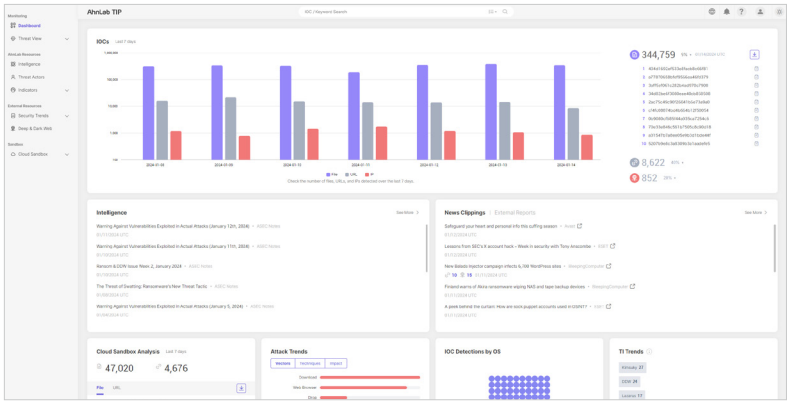
Complete visibility into cyber threats and actionable insights
to help customers make an optimized security decision

Overview

AhnLab TIP(Threat Intelligence Platform) provides the most up-to-date and precise threat intelligence along with comprehensive contextual analysis powered by our threat analysis technology and expertise. Our customers are now able to make an intelligence-driven security decision with an understanding of the background and objective of cyber threats.

“ Threat Intelligence Platform ”

Integration of Our Exceptional Expertise and Security Infrastructure

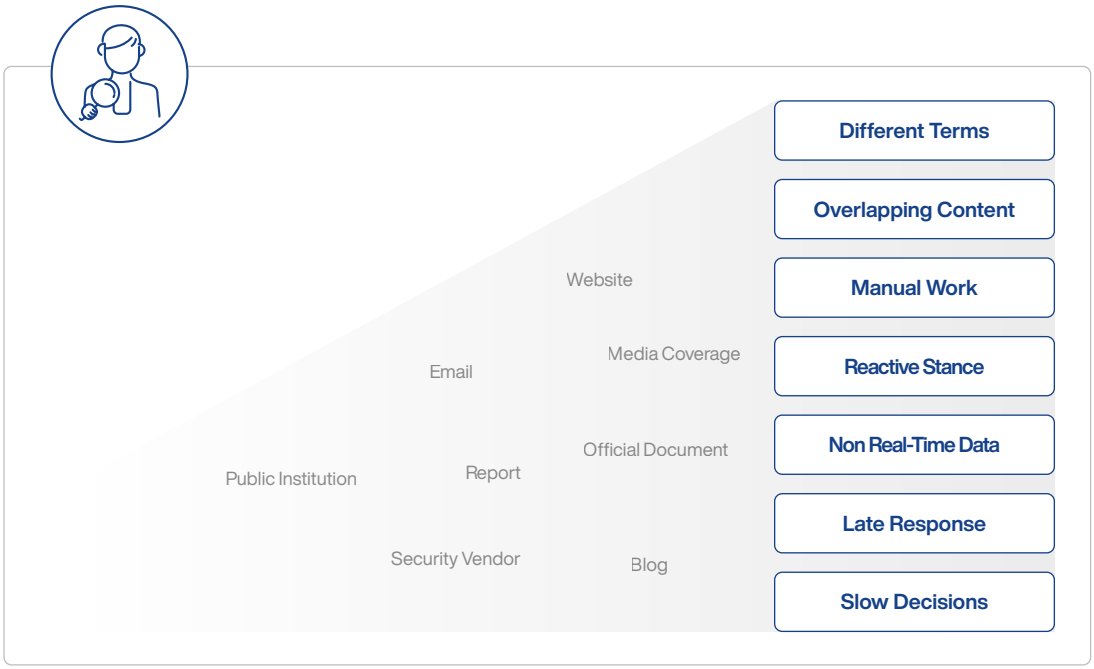


Systematic Process	· Systematically classify and store collected threat data from multiple sources · Conduct a multidimensional analysis using AI and dynamic analysis system · Provide optimized threat intelligence for customers by role
Correlation Analysis	· Deliver actionable insight on multiple threats and their impact · Carry out correlation analysis to close the gap between detection and response · Enable keyword registration to deliver custom threat data and response measure · Reflect the newest threat intelligence in our product and infrastructure
Comprehensive Information	· Execute the closed source monitoring and correlation analysis · Support customers to set the policy considering present and future threats · Enhance customers’ security capabilities by offering response solutions · Perform real-time cyber-attack monitoring

Background

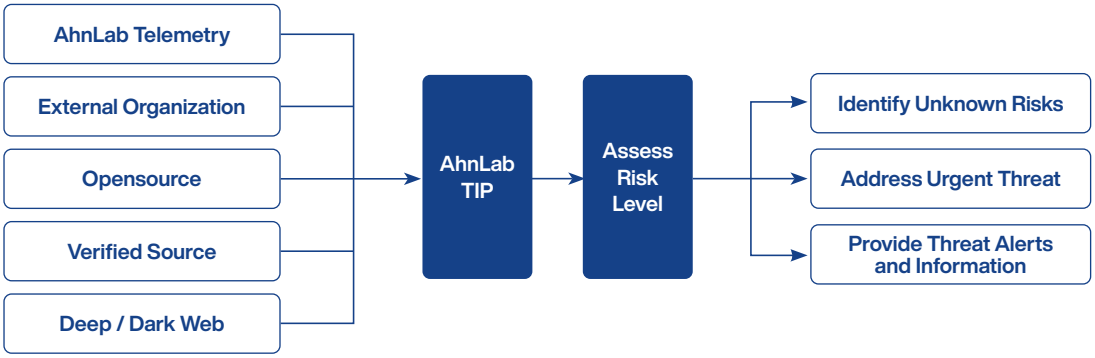
Customers had to incorporate the one-dimensional threat data from various different sources.
It fundamentally undermined the analysis and response efficiency, highly relying on cybersecurity manager's human intelligence in terms of making judgments.

Unable To Monitor Closed Sources Such As Dark Web



Benefits

AhnLab TIP offers comprehensive, yet precise and up-to-date threat intelligence in a single platform. Customers can stay response-ready by gaining complete visibility into cyber threats and understanding the impact on their business.



Enhance Customers' Incident Response Capabilities by Providing Both Quantitative and Qualitative Threat Intelligence

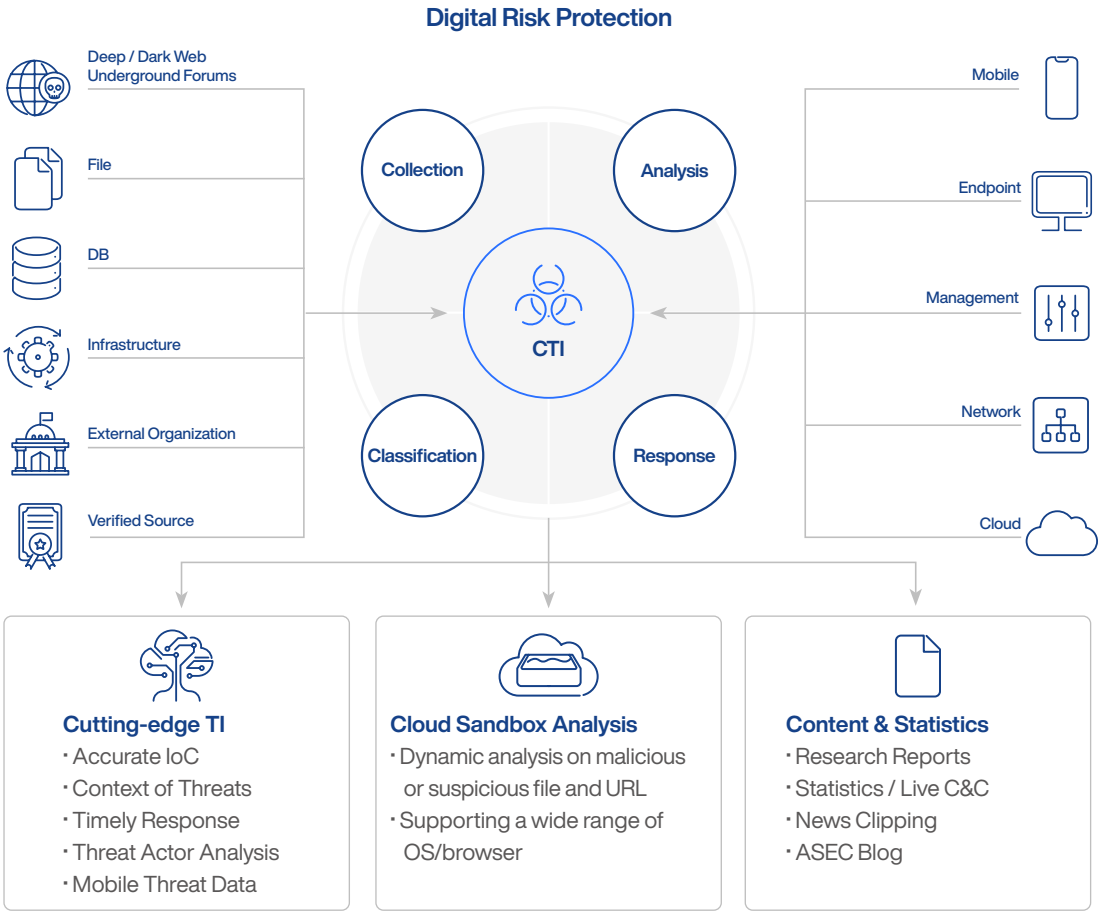
Assessing Impact
Analyze and respond to anomalous behaviors or suspected threats

Minimizing Spread
Design and test various threat scenarios

Improving Policy
Apply new detection policies and patterns in real-time

Features

At the end of the day, the ultimate objective of AhnLab TIP identifying threat information is to provide actionable insights and let customers promptly respond to cyber-attacks. This is why the platform offers in-depth threat intelligence, cloud sandbox analysis, and various TI content.



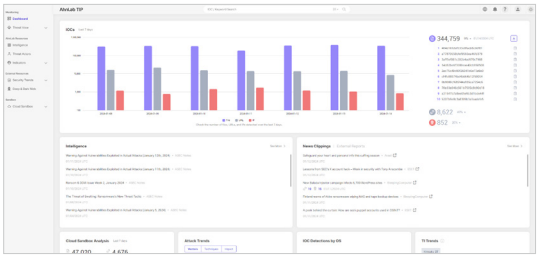
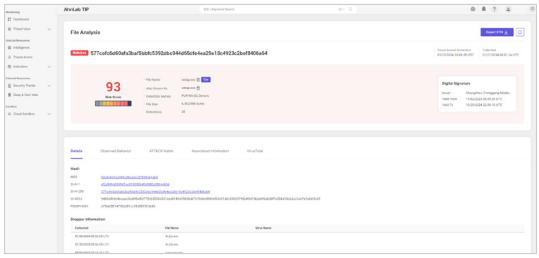
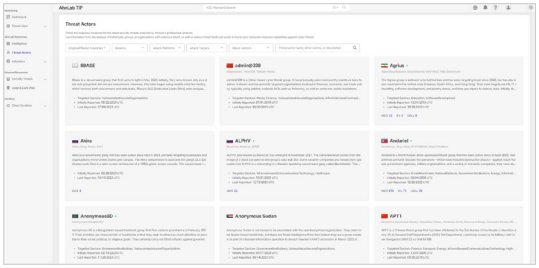
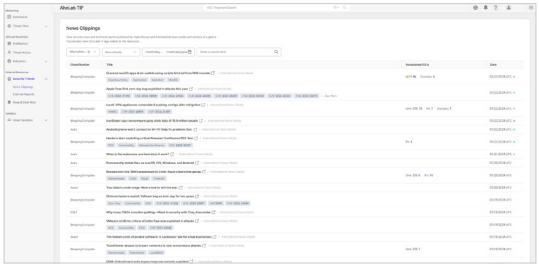
AhnLab TIP provides a broad set of features via a single centralized dashboard, allowing customers to look up and check the entire IoCs. Also, the platform summarizes IoCs by the level of severity and trust of which customers can use them as a source to justify their priority settings.

Cutting-edge TI	· Threat Lookup: URL, IP, domain, hash, threat type, and threat actors · Optimize threat data analysis - IoC feed · Improve response efficiency by identifying the path of malware distribution · Provide threat event in detail and attack flow diagram for better response · Enable product and service integration by providing RESTful API · Conduct correlation analysis on data collected from deep / dark web
Cloud Sandbox Analysis	· Provide the status of threat detection and data collection by path · Conduct analysis by OS, browser and program · Visualize the status of threat and the level of severity per behavior · Analyze files in various format
Content & Statistics	· Deliver in-depth threat analysis report backed by groundbreaking research · Provide the latest threat information from continuous analysis · Visualize cyber threats in multiple types of statistics · Provide C2 information identified by auto analyzing system · Offer a global news clipping
Threat Information from Unofficial Sources	· Tor/IP2 network source · Leaked email and file content · Information on leaked credential and data set

How to make the best use of AhnLab TIP

A. Develop cyber security strategies for a real-time threat response

Customers can learn the right threat intelligence on threat actors, types, vulnerabilities, and so forth at the right time and reflect those in their cyber security strategies.

B. Leverage extensive API integration for better response

AhnLab TIP has become the backbone of preventing and responding to newly emerging threats via a broad set of integrations.

In addition, customers can also maximize the benefit of AhnLab TIP as below.

Designing Strategies for Future	· Make future threat predictions and reflect those in the strategy · Invest in cyber security in accordance with proper priority settings
Addressing Urgent Threat	· Obtain the latest threat intelligence from AhnLab TIP · Assess vulnerabilities and potential impact of urgent threat · Develop countermeasures and minimize the damage
Improving Current Security Posture	· Identify the IP/URL/file severities and blacklist those on IPS, IDS and FW · Conduct a real-time IP/URL/file assessment via integration with SOAR and XDR · Leverage the news clipping to promptly cope with social issues

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

AhnLab