AhnLab

Case Study

EDR Architecture and Implementation Strategies for Shipbuilding and Marine Industry

A shipbuilding and marine company in Korea, referred to as Company A, has implemented AhnLab EDR on its internal and external networks to establish a stable endpoint threat detection and response system.

Overview

With advancements in information and communication technology, the shipbuilding and marine industry is not immune to cyber threats like hacking and ransomware. New and variant malware is being introduced in large numbers, and threats are becoming increasingly sophisticated, requiring an advanced incident response system optimized for the industry's specific operational environment. AhnLab's endpoint threat detection and response solution, AhnLab EDR, contributes to creating a secure business environment by providing excellent threat detection and response capabilities in complex network and operational environments. By integrating AhnLab EDR with anti-malware solution AhnLab V3, and sandbox-based intelligent threat response solution AhnLab MDS, a comprehensive security coordination system can be established, which can enable real-time detection, monitoring, analysis, and response to not only known threats but also unknown threats and abnormal behaviors.

Challenges

(1) Lack of an Effective Endpoint Incident Management System

Need to resolve inefficiencies caused by a response centered on individual solutions, and address difficulties in proactively detecting and responding to increasingly sophisticated threats.

(2) Emerging Need for Integrated Response to Internal and External APT Threat Intelligence

With the continuous spread of various threats, such as advancements in malware self-protection technology and malware using stolen digital signatures, a comprehensive response system is needed.

(3) Absence of an Operating System Optimized for the Service Environment

Many security personnel face difficulties in conducting preliminary investigations, analysis management, and monitoring during security incidents. Therefore, a systematic operational process is needed, covering everything from incident prevention to detection, analysis, response, and advanced analysis.

Challenges

- Gain visibility into known and unknown threats with an integrated agent-based approach
- Need for an integrated threat detection and response process for successful incident response
- Enhance proactive response and business continuity through the establishment of a preemptive defense system

EDR Implementation Method

Company A has installed EDR systems separately on its internal and external networks. With the goals of 1) detecting and responding to threats through endpoint anomaly detection and response, 2) enabling proactive incident detection and response, and 3) establishing control systems to prevent internal spread during threat occurrences, as well as analyzing endpoint anomalies, threat causes, and penetration paths, they set up a centralized log storage and analysis server. Additionally, AhnLab MDS was integrated to detect and respond to unknown threats.

Before fully implementing EDR at Company A, the existing EMS (Enterprise Management System) was migrated to an EPP (Endpoint Protection Platform) on the external network, and the EPP Agent was patched. Then, MDS Agents were automatically distributed through EPP servers on both the internal and external networks, and PC cleansing was performed. The purpose of PC cleansing is to preemptively remove hidden security threats, and it was conducted in three stages as follows.

First, suspicious PCs and servers were selected through the collection, detection, and analysis of known or unknown malware. Suspicious files within PCs and servers were extracted using the MDS Agent, and unknown executable files were classified by risk level as 'High' or 'Medium'. The MDS Agent uses machine learning (ML) to extract suspicious files and can automatically or manually collect these files from entire or specific systems. Additionally, connections to Command and Control (C&C) and malicious sites were detected, and suspicious files were either deleted or quarantined. The EPP server analyzed logs for known malware diagnoses.

Second, AhnLab's malware experts conducted detailed analysis, extracted AhnReport logs, and performed system analysis on PCs where malicious activities and files were detected, focusing on suspicious files identified in the first stage. Furthermore, support for responding to new and variant threats was provided by offering AhnLab V3 pattern updates or creating and applying a custom antivirus solution if necessary, and identifying endpoints suspected of compromise.

Third, if traces of a security incident were detected on PCs in the second stage, detailed forensic analysis measures were implemented on suspected endpoints and related systems using AhnLab Threat Intelligence (TI) and digital forensic tools. A detailed report, including a summary of the analysis results and a guide for action plans, was provided, and responses to identified new and variant threats were carried out.

After completing PC cleansing, the EDR Analyzer server was installed and linked with the EPP server. Then, EDR operational policies and V3 integration policies were set up, the EDR Agent was installed, and the EDR deployment policy was activated.

After completing EDR functionality testing and compatibility checks, monitoring was conducted to assess impact and fix bugs. If no anomalies were found up to this stage, the EDR Agent was deployed enterprise-wide group by group.

EDR Implementation Key Point 1

Preemptive removal of threat elements through PC cleansing and system hardening, followed by EDR Analyzer installation

EDR Implementation Key Point 2.

Implementing an optimal threat detection and response process through integration with other security solutions such as V3, MDS, PMS, and MDR

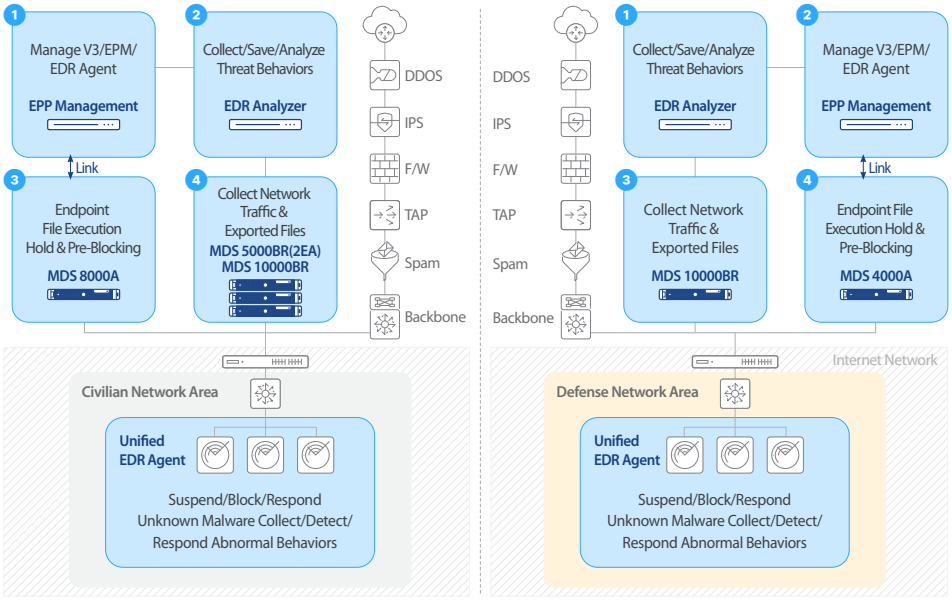

Figure 1. Solution Configuration Diagram

Solution Implementation Status and Roles

The solution implemented at Company A is composed of AhnLab EPP Management, AhnLab EDR Analyzer, AhnLab MDS Analysis and Unified Management Server, and Unified EDR Agent. The roles for each product are as follows.

AhnLab EPP Management Serve

It provides unified management of EDR and V3 in operation, along with the Patch Management System (PMS) solution, and interoperates with MDS. It primarily handles EDR policy management and providing dashboards and reports.

AhnLab EDR Analyzer Server

It stores intrusion threat activity information collected through EDR. It performs searches for threat investigations, analyzes threat activities, and conducts AhnReport and artifact collection.

AhnLab MDS Analysis Server (MDS 4000A)

It suspends execution or preemptively blocks unknown malware entering through the endpoint segment. It primarily handles APT attacks and manages the Cyber Kill Chain response.

AhnLab MDS Analysis and Unified Management Server (MDS 10000BR)

It provides unified management and monitoring of the MDS product line. Additionally, it identifies externally transmitted files and stores their originals.

Unified Agent

It includes V3, MDS, and EDR Agent, implements preemptive measures to detected unknown malware with automatic and manual removal, network isolation, and suspends execution. And through EDR, it collects anomalous behavior information and executes response commands.

Benefits

(1) Detect Unknown Threats and Automatic Response

AhnLab EDR detects and analyzes malicious files not detected by V3 and MDS, and performs visibility and analysis through the collection of complete activity logs. Additionally, based on the collected logs, it analyzes and monitors suspicious activities, enabling effective response to unknown threats. When integrated with V3, it also provides visibility into APT threats.

(2) Data Breach Trace Collection and Response

AhnLab EDR can conduct thorough inspections on suspicious files. It executes artifact collection commands on PCs suspected of malware infection or endpoints requiring detailed breach analysis. The collected detailed information is then analyzed in detail for breaches using the EPP web console viewer.

(3) Enhancing Malware Proactive Measures and Post-Analysis Capabilities

Through the V3+MDS+EDR threat response architecture, an incident attack response framework can be established, with a unified monitoring and security operations response system. By performing PC cleansing before installing EDR to initially remove threat elements and ensure endpoint integrity, proactive detection and response to security threats become easier.

(4) Automatic Analysis of Threat Detection Logs through MDR Integration

Through integration with AhnLab's MDR (Managed Detection and Response) service for expert malware analysis, it enables threat analysis and risk assessment, and allows setting response policies through risk analysis reports. This goes beyond simple monitoring and alerts of security threats in endpoint environments, to perform threat blocking and suppression.

Conclusion

The shipbuilding and marine industry, too, has reached a point where robust security systems must be considered to protect against evolving cybersecurity threats. AhnLab EDR implements excellent threat detection and response even in complex network and operating environments. AhnLab EDR, in conjunction with V3 and MDS, detects and analyzes not only known threats but also new threats and abnormal behaviors in real-time.

By adopting AhnLab EDR, you can effectively respond to unknown threats and conduct thorough inspections of suspicious files for detailed breach analysis. Additionally, you can establish a more stable and robust breach response system through a unified agent (V3/MDS/EDR) based threat response architecture. Additionally, by integrating MDR services, comprehensive and effective security can be implemented through expert-led threat analysis, blocking, and monitoring. AhnLab EDR will significantly contribute to strengthening the cybersecurity framework of the shipbuilding and marine industry and enhancing business safety.

AhnLab

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