

June 10, 2026
DIGITAL HEARTS HOLDINGS Co., Ltd.

AGEST Enters into a Strategic Partnership Agreement with US-based Lazarus for the Joint Development and Commercialization of an Autonomous AI Cybersecurity Platform Leveraging “Clearwing,” a Zero-Day Vulnerability Discovery Tool Powered by Lazarus's Agent-Based AI



DIGITAL HEARTS HOLDINGS Co., Ltd. hereby announces that AGEST Inc. (hereinafter referred to as “AGEST”), our consolidated subsidiary that supports the improvement of software quality and safety utilizing advanced quality technologies, has entered into a strategic partnership agreement on June 9, 2026, with Lazarus Enterprises, Inc. (“Lazarus”) regarding the joint development, commercialization, and sales of an autonomous AI cybersecurity platform tentatively named “AGEST Defensive (tentative name),” based on Lazarus's agentic AI tool “Clearwing.”

■ **Background and Purpose**

In recent years, there has been a growing global urgency to establish advanced defense systems that leverage cutting-edge technologies, including generative AI, in the fields of cybersecurity and national security. In particular, spurred by “Project Glasswing”—an innovative initiative aimed at enhancing software security using the recently announced “Claude Mythos Preview” (“Mythos”)(^{*1})—the Japanese and U.S. governments, as well as financial and security-related organizations, are rapidly advancing similar initiatives and establishing corresponding frameworks.

One week after the announcement of Mythos, Eric Hartford, Chief Scientist at Lazarus, analyzed the published features of Mythos and released an open-source version using “Clearwing” as an Agentic Workflow designed to run similar approaches on general-purpose, open LLMs. This “Clearwing” can switch between various LLMs such as Claude, GPT, and Llama with a single environment variable, and can also operate in on-premises environments. Lazarus reported that by actually using OpenAI Codex, and their proprietary ReAligned and UnCut Qwen(^{*2}) models, they successfully detected a vulnerability that had remained hidden in FFmpeg(^{*3}) for 16 years, similar to what was announced in Project Glasswing. This proved that complex vulnerabilities could be discovered through agentic workflows using not only advanced frontier models like Mythos but also conventional AI models.

DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo
163-1441, Japan
<https://en.digitalhearts-hd.com/>

Aiming to contribute to the security market through the “democratization of critical security workflows using Clearwing”(*4), which is being discussed among global engineers, AGEST and Lazarus have reached an agreement on initiatives for the joint development and commercial service launch of “AGEST Defensive (tentative name)”. This enterprise-oriented solution eliminates the burden of expensive token fees and the mandatory requirement for external API integration, enabling reasonable cost burdens and usage in on-premises environments.

*1 An advanced AI model exclusively provided by Anthropic PBC, which is a frontier model specifically focused on the cybersecurity domain, such as zero-day vulnerability detection, vulnerability analysis, and attack path generation.

*2 ReAligned and UnCut are specialized, open-weight AI models released by Lazarus AI designed to remove ideological bias and production restrictions from frontier AI. Removes hardcoded censorship, propaganda, and state-backed framing from base models while retaining their high-level reasoning and coding capabilities.

*3 Free software for converting, editing, and playing video and audio files into different formats.

*4 Widely recognized in the tech community as having “released (democratized) the capabilities of Glasswing, which could only be used by a limited number of companies, to general developers.”

■ Outline of the Alliance

Lazarus is an advanced US AI technology company engaged in the development of AI systems for solving complex and advanced problems, specifically multimodal AI systems and technologies for enterprise and defense applications. The company has previously been responsible for developing AI information analysis platforms for the US Department of Defense, has received investment from the US government, and has advocated for AI operation in highly confidential on-premises environments from an early stage, possessing high technical capabilities and expertise. Their “Clearwing” is an open-source autonomous AI vulnerability discovery and penetration testing tool published on GitHub, featuring the following characteristics:

- **Alternative Security Capability:** Developed to realize similar security verification capabilities using conventional AI models (Claude, GPT, etc.) when general public access to high-performance models like “Mythos” is restricted.
- **Autonomous Exploration:** Simply by specifying the target IP address or URL, multiple AI agents autonomously explore and reproduce vulnerabilities.
- **Integrated Workflow:** An autonomous workflow that integrates hundreds of security tools to automatically map, evaluate, and scan the specified target's attack surface.
- **High-Precision Verification:** A process that goes beyond simply finding vulnerabilities by actually reproducing and verifying them in a sandbox environment, reducing false positives and outputting high-quality reports.

It is attracting significant attention as a resource in the AI era that allows even non-security experts to execute advanced penetration tests.

On the other hand, AGEST is an expert company in software quality and cybersecurity. In our security monitoring and operation service “DH-MDR (Managed Detection and Response),” which detects, analyzes, and addresses threats that have invaded a network, we have top-

DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo

163-1441, Japan

<https://en.digitalhearts-hd.com/>

class domestic achievements, such as monitoring a cumulative total of 930,000 EDR (Endpoint Detection and Response) devices, and possess unique operational expertise derived from this.

Through this alliance, we will combine Lazarus's expertise in artificial intelligence (AI) and platform development with our expertise in cybersecurity operations, testing/verification/QA, and commercialization to execute the commercial deployment of a next-generation platform for markets such as governments and enterprises, including:

- **Joint Development:** Joint development of the "Autonomous AI Cybersecurity Platform 'AGEST Defensive (tentative name)'," combining development investments and proprietary know-how from both companies.
- **Commercialization & Sales:** Commercialization and sales in the Japanese and global markets utilizing our security monitoring and operations, proprietary knowledge, and business commercialization know-how.

■ About "AGEST Defensive (tentative name) "

- A "comprehensive cybersecurity platform that defends against overwhelming attacks using autonomous AI," providing the optimal solution not only for vulnerability hunting but also for how to prevent them. (Details are scheduled to be disclosed upon service release.)
- Enables switching between diverse LLMs such as Claude, GPT, and Llama with a single environment variable.
- Supports operation with local LLMs in on-premises environments in addition to API connections (especially effective for providing to companies that emphasize strict confidentiality and usage in environments completely isolated from the outside).
- Reduces expensive token fee burdens through on-premises use.
- Provides a domestic security platform led by AGEST.

■ Future Initiatives

Currently, anticipating full-scale commercial deployment, AGEST has already initiated discussions with multiple companies to build a cross-sectional and large-scale partnership ecosystem across various industries, including IT and security. Through further collaboration with more companies and related organizations, we will strive for the dramatic development of economic activities through the advancement of cybersecurity and national security measures. Some features, such as vulnerability hunting, are scheduled to be rolled out within June 2026, while the comprehensive cybersecurity platform, which includes proposing remediation plans for detected vulnerabilities, is scheduled for release in September 2026.

■ Lazarus Endorsement

"At Lazarus, we believe the future of cybersecurity lies in making advanced AI-driven capabilities accessible to every organization, not just those with access to frontier models or unlimited resources. AGEST shares that conviction, and their deep expertise in security operations, QA, and enterprise commercialization makes them the ideal partner to bring Clearwing to the markets that need it most. This partnership is exactly the kind of collaboration we had in mind when we open-sourced Clearwing: a bridge between cutting-edge AI research

DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo

163-1441, Japan

<https://en.digitalhearts-hd.com/>

and real-world deployment, giving governments and enterprises the autonomous vulnerability discovery capabilities that were previously out of reach.”

- Alex Panait, CEO, Lazarus Enterprises, Inc.

* All brands, product names, company names, trademarks and service marks are the properties of their respective owners.

【About AGEST, Inc.】

Under the vision of “Bringing rich value and experiences to all DX with advanced quality technology,” AGEST promotes research into advanced technologies and the development of QA tech lead personnel capable of handling the latest technologies. Through the provision of next-generation QA solutions, we contribute to the development of an advanced digital society.
<https://agest.co.jp>

【Inquiries from the media】

AGEST, Inc. IR & Public Relations Office, Public Relations Contact
Mail: ml-pr@agest.co.jp
Tel: 03-5333-1246

DIGITAL HEARTS HOLDINGS Co., Ltd.

Tokyo Opera City Bldg. 41F, 3-20-2 Nishi-Shinjuku, Shinjuku-ku, Tokyo
163-1441, Japan
<https://en.digitalhearts-hd.com/>