Commencement of the eXtended Detection Investigation Response framework

Integrated SIEM solution enhancing security operational efficiency from a comprehensive perspective

IGLOO

spider ExD

Background

With the advent of the Digital Transformation (DX) era, we embrace the concepts of 'integration' and 'efficiency.'

With the digital transformation, the expanding attack surface provides cyber attackers with more targets, leading to an increasing challenge for businesses to counter new and evolving threats.

Today's security organizations must ensure visibility into the exponentially generated diverse security data to enhance detection accuracy and response speed against advanced threats.
However, security analysts and resources for this are limited.

As the security landscape becomes more complex, solutions must also evolve accordingly.
A next-generation SIEM solution is needed to enhance the efficiency of security operations from a comprehensive perspective.

Availability

Whether to collect and store all security-related data securely

Accuracy

Whether to rapidly and accurately detect/ investigate the collected voluminous data

Scalability

Whether to implement a unified security process by easily integrating various security functionalities

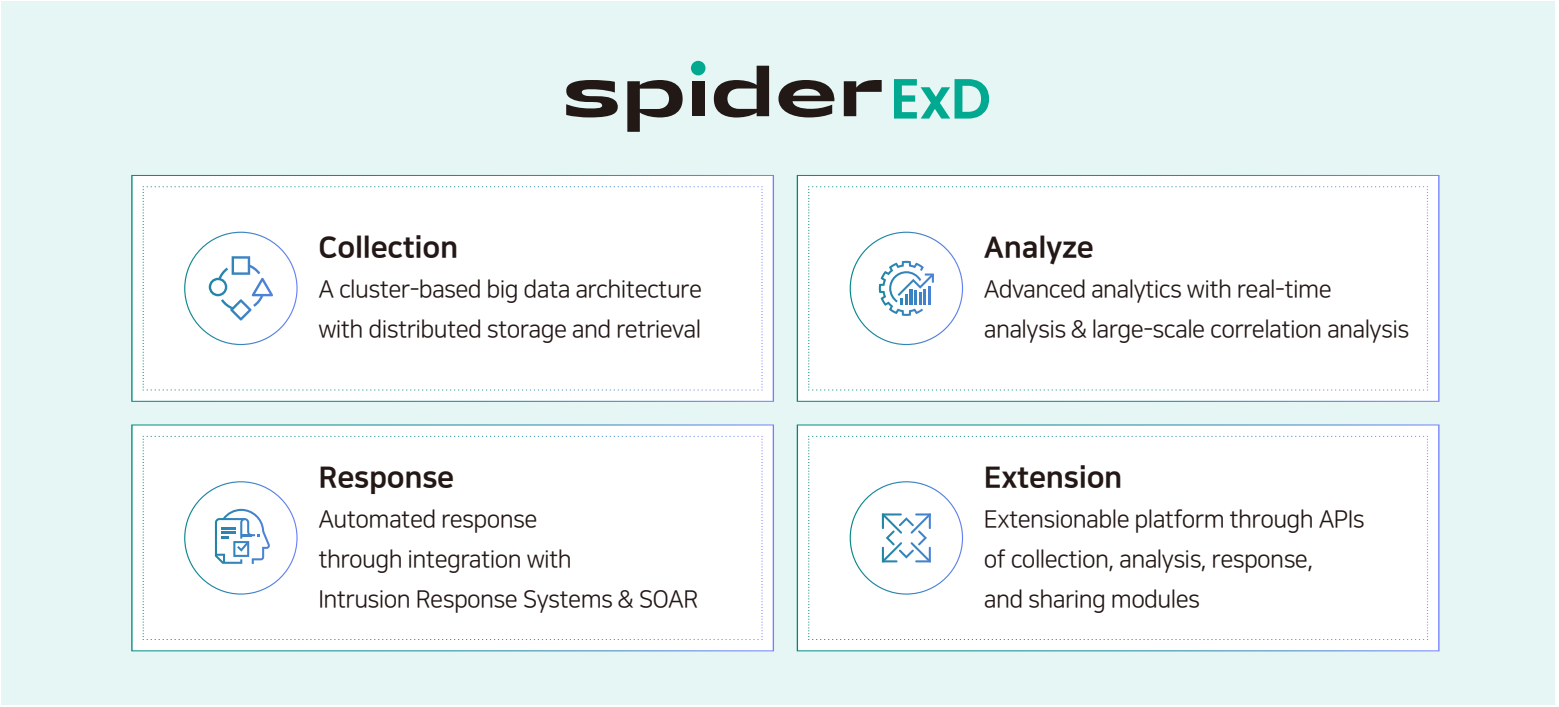
Built on **high availability, accuracy, and scalability,**
It's time for **a next-generation security information and event detection and analytics (SIEM) solution that can proactively adapt to the changing IT environment**

Overview

The SPiDER ExD is an integrated SIEM solution that ensures high levels of availability, accuracy, and scalability.

By adopting SPiDER ExD, which provides advanced collection, analysis, response, and expansion capabilities in an integrated manner, security organizations can implement a unified form of security process within a single workflow.
This allows for securing visibility across the enterprise and elevates the resilience against evolving security threats.

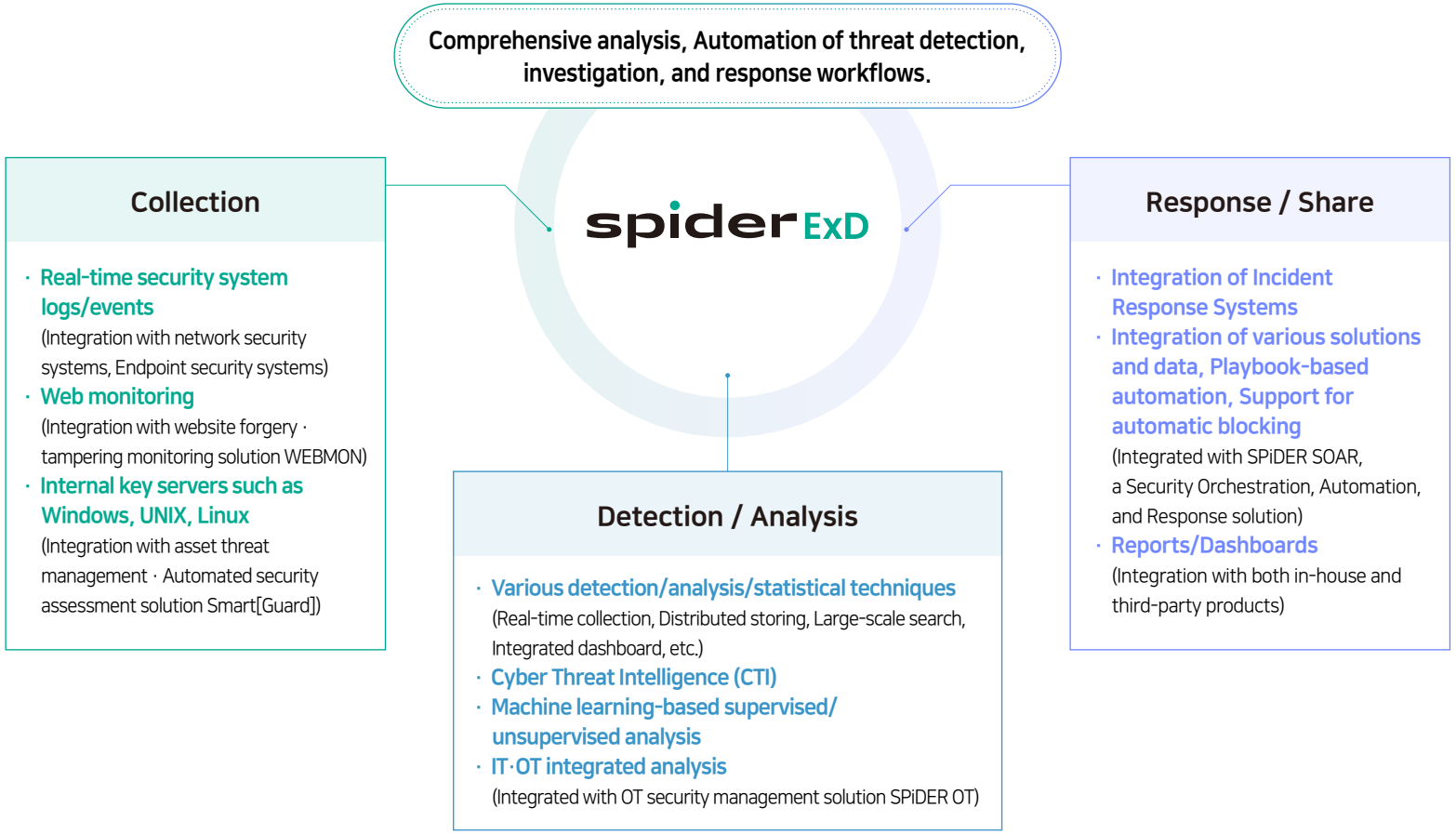
With SPiDER ExD, maximize the efficiency of security operations from a comprehensive perspective and embark on the journey to implement the eXtended Detection, Investigation, and Response (XDIR) framework.



Why SPiDER ExD

SPiDER ExD is the most comprehensive SIEM solution that supports flexible expansion and integration of security functionalities. Through a container-centric platform and UI integration, it enables an eXtended Detection Investigation Response (XDIR) architecture.

- **Expanding the scope of security threat data collection**, **Applying various detection and investigation techniques**, **Automating security operations and responses** to meet the demands of security organizations for ongoing scalability.
- By organically integrating vast security data and internal/external threat intelligence from a comprehensive perspective, maximizing the efficiency of security operations and threat responses through detection, investigation, and response.

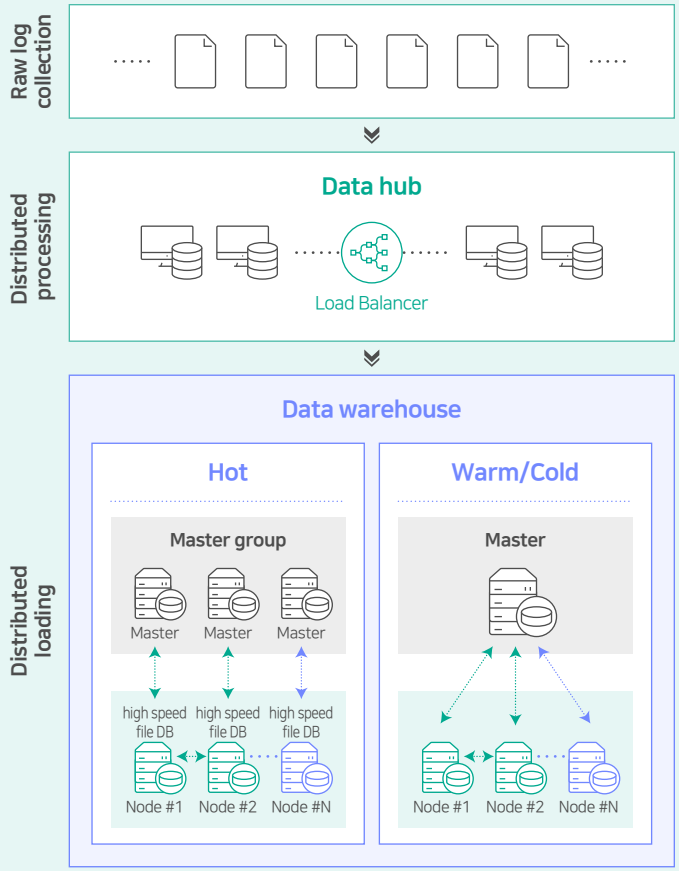


Features

A. High availability

Leveraging cluster-based big data architecture and Replica function to ensure service reliability

- Supporting horizontal scalability through cluster-based parallel Node expansion and distributed storage·search capabilities
- Supporting data protection and incident response through data replication storage, compression, encryption, and backup functionality



Cluster-based Parallel Node expansion

- Guaranteed scalability as log increases(Scale-Out)
- Ability to evenly distribute existing data nodes and storage capacity when new nodes are added
- Minimizes the time required for expansion without service interruption and ensures convenience of management through central management functions

Distributed storage / retrieval

- Distribute refined event logs to each data node for storage on a condition basis (Default: Day)

Replication Storing

- Store preprocessed event logs on two or more distributed nodes to ensure uninterrupted operation in case of storage device failure
- Replicas are created and stored separately from the stored data, and are distributed and stored on different data nodes
- In case of a data node (server) failure, automatic recovery using replicated data

Compression / Encryption / Backup

- Stored log data is compressed for efficient use of disk storage space
- For cold data, encryption is applied at the file level before storage
- Data backup and deletion management are performed according to backup configuration policies

Features

B. Enhancing convenience of data retrieval and accuracy of analysis

Securing a high level of data analysis accuracy based on one-step enhanced loading and retrieval capabilities

- Improving search convenience and analysis accuracy through collection and loading via regular expressions and real-time parsing
- Supporting advanced log search capabilities, including criteria set up comprehensively and original information inclusion
- Providing real-time and search-based analysis functionalities

Normalization of raw logs using a custom parser

Parser information

Stored as indexes for search and analysis purposes

Enhanced convenience in data retrieval

※ Log normalization approach :

- Define the log format using regular expressions, delimiters, etc., without processing the original logs, and utilize them for search and analysis
- The collected logs provide real-time parsing functionality for search and analysis purposes
- Store both the raw data and parsed data together
- Provide functionality to add or transform additional information for enhanced efficiency in log analysis

Real-time Analysis and Detection

Real-time data

In-memory based analysis engine

- Threshold exceedance
- Exclusion conditions
- Response conditions

- Comparison of condition by field
- Comparison with reputation database
- Identical conditions (distribution)

Enhanced analysis accuracy

alert event

- Evidence data #1
- Evidence data #2
- Evidence data #3
- Evidence data #4

Normalization for Collection and Loading

- Through normalization, data collection and loading are facilitated. Custom parser functionality supports field-specific configurations using regular expressions without the need for separate development.
- The indexing fields generated thereby are utilized for search and analysis, enhancing data search convenience and analytical efficiency.

Enhanced Log Searching

- Advanced log searching capabilities enable searches based on compound criteria (such as AND, OR, NOT)
- Original logs, along with all indexed fields, are displayed, and additional information such as country and harmful IP details is provided
- Various search functionalities are offered, including custom searches and interactive searches

Real-time Analysis and Detection

- Utilizing in-memory technology for swift analysis, real-time log analysis and detection enhance accuracy
- An extended analysis engine integrates SIEM and AI analysis models, providing advanced analytical capabilities

Advanced Search-Based Analysis

- Various analysis condition settings, including specific conditions and regular expressions, are supported for all fields of collected logs
- Exception condition functionality based on detection rules is provided, allowing for exceptions to be set for specific days and times
- A reputation database is constructed based on collected data, and analysis functionalities utilizing the data from that database are offered

Features

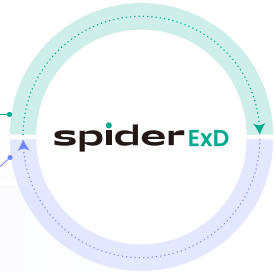
C. Extensive Scalability

Easy function extension through platform-based architecture

- Integration with internal modules and external systems via APIs
- Continued feature expansion through partner collaboration

Support seamless integration with heterogeneous solutions and systems around SPiDER ExD

Integration platformization through feature expansion, ensuring comprehensive visibility and maximizing security operational efficiency



Open API integration solution

- SOAR: Security Orchestration, Automation, and Response
- AI: Supervised/Unsupervised analysis based on machine learning
- Vulnerability Assessment: Integration with vulnerability assessment solutions and correlation of results
- Cyber Threat Intelligence (CTI): Integration with threat intelligence, risky IPs, URLs, IoCs, and detection policies
- Dashboards: Customizable dashboard
- Information Security Portal: Portal for affiliated organizations coordination
- Information Security Solutions: Integration of blocking and policy
- Integration with asset management solutions and system management solutions
- Integration with internal modules and external solutions by storing normalized data in message queues

D. Advanced Threat Detection and Response

Provides advanced threat detection, additional features, and integration support

- Variety of basic detection and investigation functions for accurate and rapid security threat insights
- (Basic) With built-in Cyber Threat Intelligence (CTI) service 'KLU:', Enhance resilience against the latest emerging threats
- (Optional) Integration with the Hybrid AI Detection Model service 'AiR (AI Road)' to increase the accuracy of security data analysis and derive suitable response measures

Advanced detection and investigation

Machine learning-based analysis & MITRE ATT&CK dashboard

- Advanced threat detection through various basic detection and investigation functions such as machine learning-based supervised/unsupervised analysis, Threat Hunting, and MITRE ATT&CK framework analysis processes

Threat intelligence integration

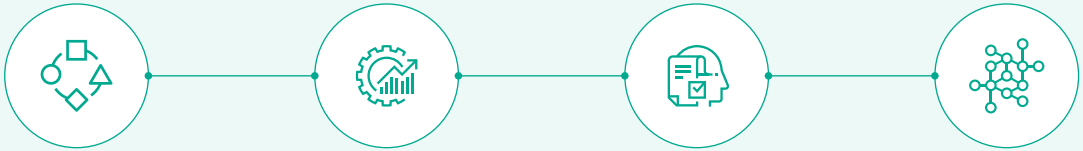
KLU: Cyber Threat Intelligence 'KLU: Threat Intelligence'

- Management functionalities for harmful IP/URLs, malicious code hashes/vulnerabilities
- Effective response to the latest threat situations through automatic updates of security content such as security news and vulnerability information provided directly by security companies
- Rapid and accurate investigation by integrating and sharing through the built-in CTI in real-time

Benefits

With SPiDER ExD, experience Expanded Detection, Diversified Analysis, and Accelerated Response.

SPiDER ExD will secure integrated visibility covering the entire attack surface and proactively respond to the constantly changing IT environment through the collection of vast security data, highly accurate analysis, implementation of automated response processes, and broad integration and expansion of security functions.



Collection

Comprehensive security data collection, storage, and processing

Analysis

Enhancement accuracy of correlation analysis between collected data

Response

Maximization of efficiency in threat detection and response

Integration

Expansion and integration for proactive response to changes

SPiDER ExD supports the building of a robust and efficient security structure by maximizing security operation efficiency from a comprehensive perspective.

Since its establishment in 1999, IGLOO Corporation has been focusing on implementing core technologies to drive innovation in organizational work environments and work methods. Starting with the launch of the first Security Information and Event Management (SIEM) solution in the domestic market, IGLOO Corporation has diversified its business to encompass Artificial Intelligence (AI), Security Operations, Automation, and Response (SOAR), Cyber Threat Intelligence (CTI), Operational Technology Security (OT), and specialized security services. This expansion has led IGLOO Corporation to grow into a comprehensive IT company covering the fields of security, artificial intelligence, cloud computing, and big data. IGLOO Corporation aims to continue its role as a key collaborator by providing solutions optimized for rapidly changing business environments based on its proprietary AI-based security operation and analysis platform.

6F, Hans Building, 7 Jeongui-ro 8-gil, Songpa-gu, Seoul | **TEL** 02-3452-8814 | **FAX** 02-3452-8815 | www.igloo.co.kr

IGLOO