SPiDERTM

A Next-Gen. SIEM Solution Developed by Security Experts

SPiDER TM is a SIEM developed by IGLOO SECURITY, who's experience in the industry dates back to 1999. SPiDER TM is capable of relieving the burden of log management through fast collection and storage of security data. It also provides administrators with a unique security intelligence platform to aid administrators in efficiently and swiftly responding to security concerns.

Identifying the Problem

> Many companies are responding to security threats by implementing multiple security devices due to security threats becoming increasingly more sophisticated than before. These limitations have made it increasingly difficult to carry out security monitoring duties.

Why use IGLOO SECURITY's SPiDER TM?

Q1 Are you currently using a SIEM Solution?

Along with the increase in the security infrastructure, it has become more difficult to manage and analyze security data generated by individual devices. Thus, a single security system may not be enough to detect and respond to sophisticated security threats. Therefore it is necessary to introduce a SIEM solution that integrates security data.

Q2 Is your SIEM solution optimized for security monitoring?

SPiDER TM was developed to reflect the work flow and the needs of the IGLOO SECURITY personnel with years of security monitoring know-how and actual experience in the field. The SPiDER TM is also optimized for security monitoring tasks and provides a variety of security intelligence through the 'Knowledge Center'

Q3 Does your SIEM solution offer a variety of analytical capabilities?

The SPiDER TM carries out tasks from simple analysis to multidimensional scenario analysis. In addition to simple attacks, it can respond to various threats such as APT attacks or internal information leaks. Analysis rules for incidents can be set by users through a simple script which allows real-time and historical data analysis.

The IGLOO SECURITY SPiDER TM...

...can rapidly collect and normalize large amounts of security event logs and various application logs from different security devices and servers without data loss. So you can accurately carry out correlation analysis through real-time or historical data. In addition, by providing optimized processes, functions and intelligence for security monitoring tasks, IGLOO SECURITY protects customers' assets from internal and external threats.

SPiDER TM Features

Experience

SPiDER TM improves the efficiency of security monitoring by providing a unified security monitoring process from initial detection up to log analysis.

Real-Time Alert Monitoring
Identifying the progress of each step on correlation analysis results in real time.

Detailed Analysis
Provides statistical information such as reason for attack, IP, attack type and original log data.

Raw logs
Raw logs can be analyzed through detailed analysis.

Correlated log search
Provides high-speed file search based on BIG DATA

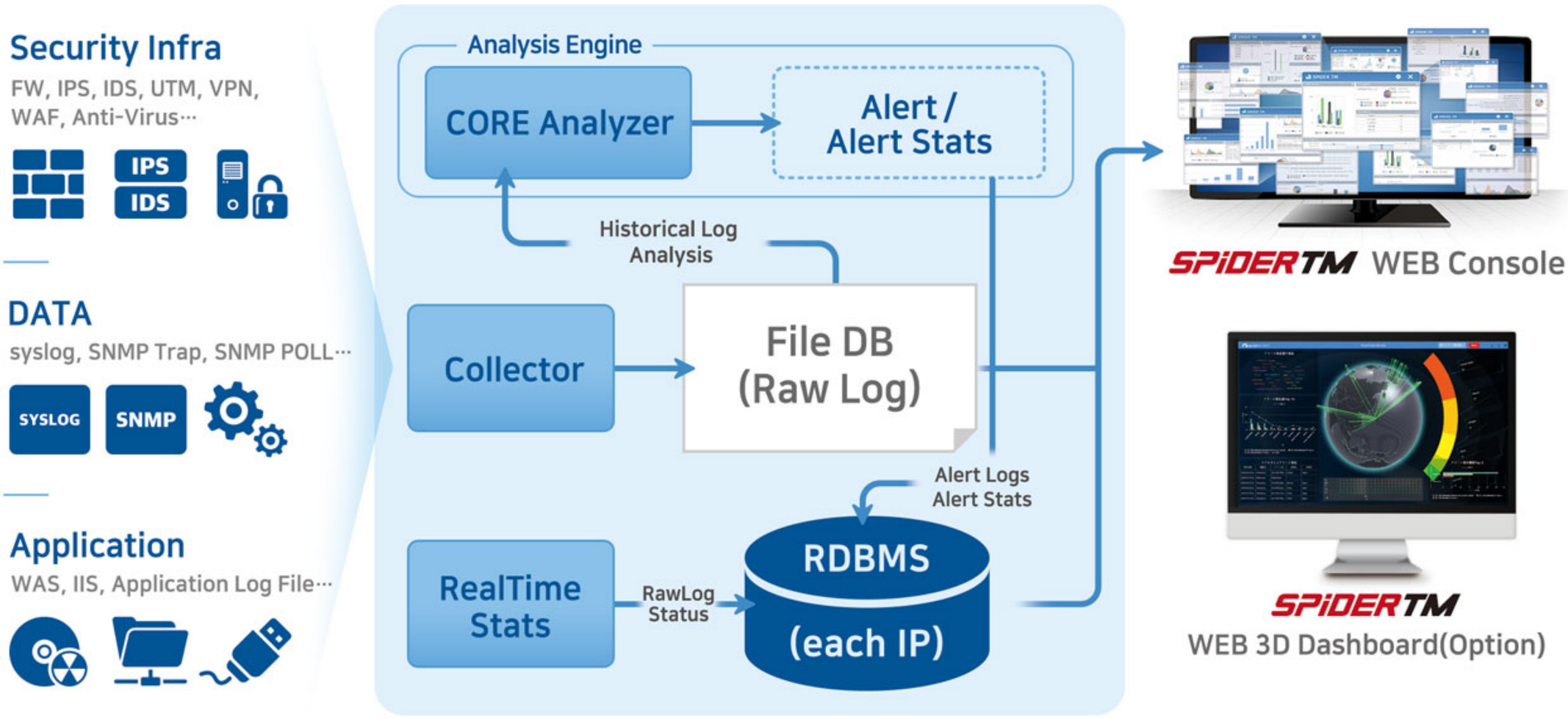
Intelligence

SPiDER TM provides various threat intelligence through its integration with IGLOO SECURITY's Knowledge Center.

Visibility

SPiDER TM allows you to customize a variety of screens on a 3D dashboard with intuitive data representation and screen composition based on the user's needs and characteristics.

SPiDER TM Diagram



SPiDER TM Main Functions

SPiDER TM is comprised of a three-step process: collecting, analyzing, and processing of information.

Collecting	Collects large amounts of logs	Can collect and process large amounts of log data based on regular expression.
	Collects logs from various devices	Can collect various logs from sources such as servers, applications as well as security devices
Analyzing	Scenario based correlation analysis	Provides a scenario-based correlation analysis rule which contains years of security experience from IGLOO SECURITY personnel.
	High performance file DB	Carries out efficient log analysis using the search results based on the high performance file DB.
	Advanced analysis engine	Can carry out multi-dimensional correlation analysis of a new architecture based on in-memory processing.
	Efficient log analysis	Can search and analyze all evidence events related to the infringement within a single screen.
Processing	User defined dashboard & report	Can create customized reports as well as standardized reports according to category.
	3D Dashboard	Intuitive data recognition is possible through a 3D screen display. It also provides various screen customizations and editing features considering the user's characteristics.
	Various alert functions	Provides alerts by voice, mail, sms, etc. according to the threat level of the incident, and also generates alarms in real time.
	Shared security threat intelligence	Provides the latest trends and supports automatic renewal of blacklist IP/URL through IGLOO SECURITY's own ‘Knowledge Center’.
	Provides intelligence on malicious code sources	Automatically provides intelligence on malicious sites collected from all over the world through an in-developed malware distribution system.
	Incident response	Provides a systematic response process for analyzed alarm events which enables rapid incident response

SPiDER TM Service

SPiDER TM

IGLOO SECURITY provides an all-in-one solution from system implementation, operation training up to security monitoring service through SPiDER TM.

Implementation support service

- Product implementation consulting
- Support for customizing environment configurations
- Support for customizing rule configuration

Training service

- Product operation and training on 'how to use' SPiDER TM
- How to operate managed security service (MSS)
- Vulnerability assessment and malicious code analysis etc.

Security monitoring service

- Remote Security Monitoring Service
- Security device operation
- Dispatch a professional security monitoring operator

SPiDER TM Clients

Public

- National Information Resources Service
- National Secretariat
- Prosecution Office
- Ministry of Culture, Sports and Tourism
- Ministry of the Interior and Safety
- Seoul Metropolitan Government

Financial/ Education

- Bank of Korea
- KEB Bank
- KB Kookmin Bank
- Mirae Asset
- Yonsei University
- Seoul Metropolitan Office of Education

Enterprise/ Communication

- Samsung
- Lotte
- GS Caltex
- SK Telecom
- LG Telecom
- KT

Overseas

- Japan
- Ethiopia
- Morocco
- Indonesia
- China
- UAE

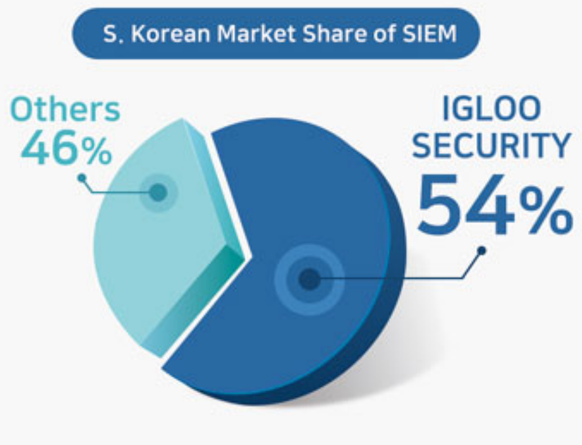
IGLOO SECURITY Company Introduction

Leaders in the 'SIEM' industry

Since it was founded in 1999, IGLOO SECURITY has been committed to developing the integrated security management system also known as "Security Information and Event Management" (SIEM) for more than 10 years. With the industry's top developers, IGLOO SECURITY has made constant efforts in R&D investment and technological innovation as well as protecting critical assets from various cyber attacks. We also deliver the best products which support corporate operations and businesses. On a final note, IGLOO SECURITY is committed to protecting your valuable information assets and establishing an IT-based operating system through our experience, expertise and technology.

IGLOO SECURITY INC.

- Founded : 1999
- Headquarters : Seoul, South Korea
- KOSDAQ Listed Company (Public)
- Business : Integrated Security Management and Monitoring Solution (SPiDER TM)Managed Security Services
- Major clients : 250 government, public, educational, communications, corporate, etc. Over 400 Managed Security Services sites



6th Floor, 7, Jeongui-ro 8-gil, Songpa-gu, Seoul, Korea | E-mail : overseas@igloosec.com | www.igloosec.com

IGLOO SECURITY