IGLOOSECURITY

SPiDER TM

Integrated Security Management Solution with accumulated know-how and technology of Managed Security Services and Big data capabilities

SPiDER TM is an integrated security management solution with 20 years of experience of Managed Security Services and Big data capabilities from IGLOO SECURITY. It can enhance agility and efficiency of security monitoring services through centralized monitoring environment structure from initial detection to log analysis, at the same time, assuring complete visibility on the overall infrastructure.

Also, all logs are collected and saved in real time and analyze them in connection with the latest external threat information such as harmful IPs and malicious URLs, various threat elements can be quickly and effectively detected, blocked and prevented.

Advantages of SPiDER TM

Latest security threat information

Analyze internal information and external threats in connection with IGLOO CTI

+

Experience and knowhow in Managed Security Services

Provide process and function optimized for Managed Security Services

+

Big data log processing

Collect and analyze all types of logs

Work Flow

1 Real time monitoring

Comprehend the progress of correlation analysis results in real time by stage

2 Detailed analysis

Provide statistical information such as trend of attack, IP and attack type through analysis and raw data

3 Check Raw log

Analyze and check the raw log

4 Search related log

Provide a quick search result through big data based high speed file DB

SPiDER TM AI Edition

Machine learning based preemptive response and increased prediction capabilities through AI systems

The IT environment is becoming more complex due through various technological innovations such as; wide scale, IT Infrastructure, explosive increase in data, complex compliances, tightening of laws concerning IT. Alongside this development, cyber-attacks have become more threatening through automatized hacking attacks, intelligent security threats, indiscriminate attacks and the increasing danger of cyberwarfare. Now is the time for AI based security management. AI will allow users to respond and keep up with the exponentially expanding hi-tech security threats.

Advantages of SPiDER TM AI Edition

Improve processing efficiency of cyber threat event

- High-Risk Focused Analysis
- Expand processing range and reduce time via real-time incident event automatic analysis
- Efficient allocation of resources
- Unknown threats appear on the surface

Provide preemptive response system

- Share collected information related to organization
- Collect domestic/foreign threat intelligence and newest information of malicious codes
- Preemptive response to similar threat

Improve cyber security management efficiency

- Create an asset information vulnerability self assessment system
- Shorten vulnerability detection time
- Vulnerability updates through continued inspection

Machine learning based AI system

1 Automated alert event processing through supervised learning

- The SPiDER TM is capable of increasing alert event processing efficiency and preemptively responding to threats through supervised learning of various scenarios.
- It is capable of predicting threat levels of alert events by creating and learning data according to attack patterns. The analysis results are also continuously upgraded through feedback from analytics.

2 Unknown threat detections by unsupervised learning

- The SPiDER TM is capable of detecting unknown threats by utilizing scenario based and user activity based data learning of each attack scenario.
- It puts together then detects security logs and anomaly detections of alert events along with threat level prediction and is continuously upgraded through feedback from analytics.

WEBMON

Web-forgery monitoring solution that detects the forged webpage by integrated monitoring.

WEBMON is a solution maximizing the effectiveness of integrated management of websites that can immediately respond and report, and inspect flexible detection policies and various detection history by detecting the forged webpage in operation through 24/7 monitoring of websites exposed to risks at all times.

Offering Function

Monitoring
- Monitoring by website or group
- Detection information search and warning notice
- Excellent visibility with intuitive web UI structure
- Statistical analysis on detected event

Failure Management
- File size management
- Website response code management
- Website access status management

Security Management
- Forgery monitoring by inspecting threshold
- Forgery monitoring by inspecting hash value
- Various web content monitoring
- Decoding function for obfuscated code
- Detect rule based malicious code
- Detect transit and distribution point of malicious code

Alarm Function
- Failure warning according to abnormal website access
- Security warning according to website detection information
- Response processing according to alarm
- Warning according to crawler agent performance information
- Alarm management according to website security policy

History Management
- Failure detection event history management
- Security detection event history management
- Forged evidence data management by saving website source code and screen
- Audit history management

Policy Management
- User authority management
- Crawler agent management
- Failure policy management
- Security policy management
- Detection rule management
- DNS access management

Advantages of WEBMON

Improve monitoring efficiency with intuitive interface
- Easy to manage system by user authority
- Enable intuitive judgment by detection status dashboard by website and group
- Analyze changing trend in website through consistent statistical data

Reinforce incident response by real time detection
- Immediate respond and report in case of incident by monitoring consistently
- Stable operation of website by determining access failure and abnormal signs
- Establish improved incident response system by utilizing evidential data upon determining an abnormal symptom

Reinforce analyzing function
- Reduce false positive rate by providing detection exception rule on malicious code analysis
- Reinforce code detection function by disabling source code obfuscation function
- Maintain optimized analysis status by setting details according to event occurrence condition
- Provide URL information on website consistently

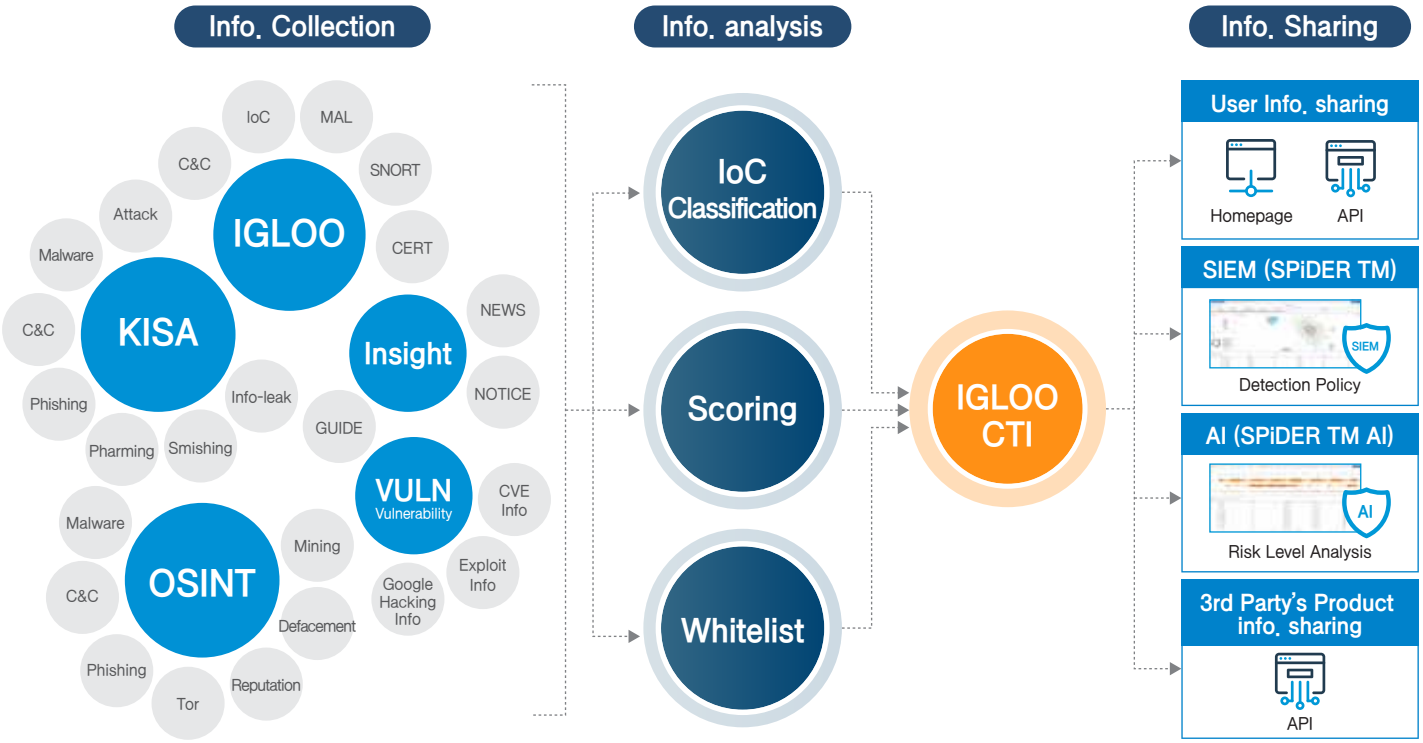
Provide ease of analysis by utilizing raw data Based statistical data
- Utilize history management and correlation analysis
- Detected statistical data based threat scenario analysis
- Utilize analysis data by providing evidential data for image and source code

IGLOO CTI

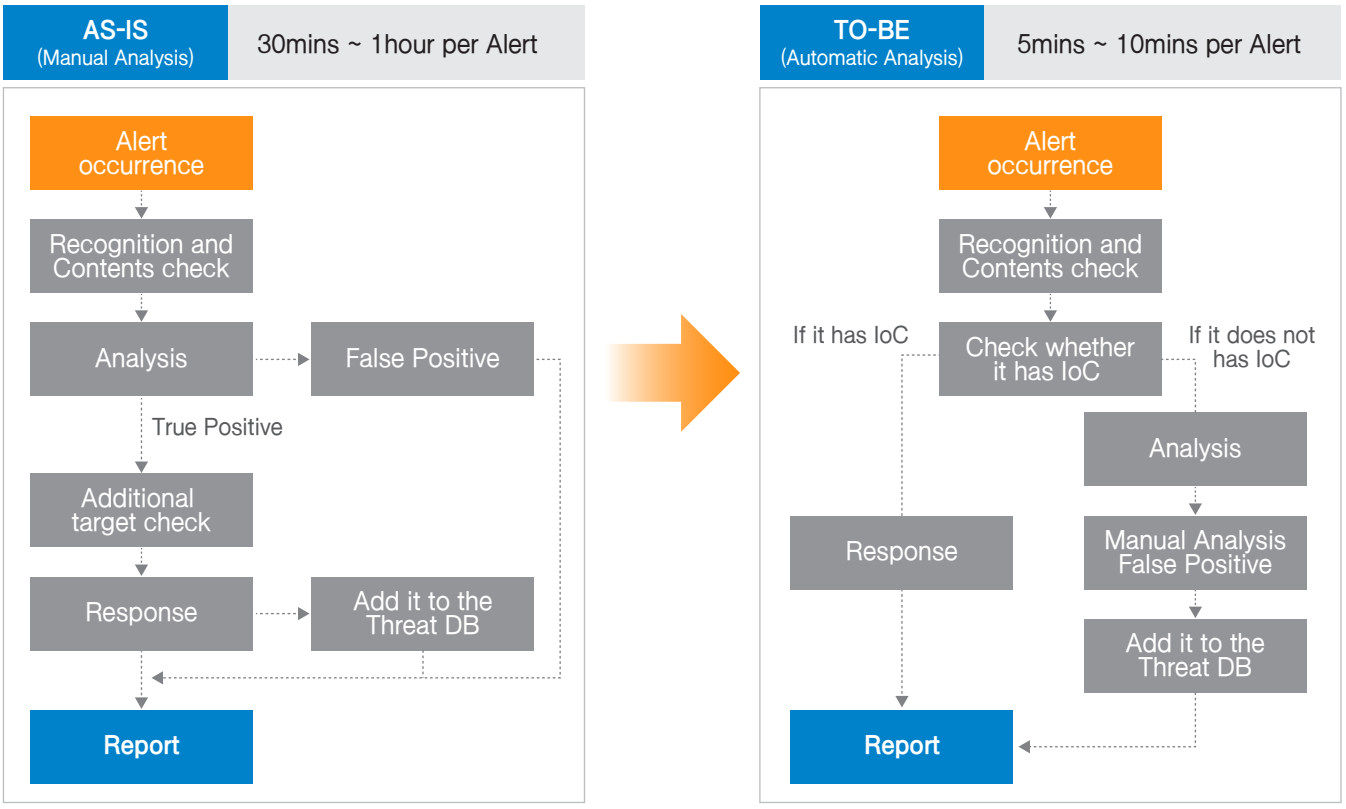
IGLOO CTI is a cyber threat information sharing system that collects and shares the latest global threat information.

IGLOO SECURITY continuously shares security threat information collected from various companies and organizations to help prevent cyber-attacks, and quickly identify attackers. IGLOO SECURITY selects and provides detailed information to enable proactive response by understanding the context and purpose of the attack against security threats targeting companies and institutions.

Overview



Introduction advantages



IGLOOSECURITY

We Know Security

To grow into a leading company of information security representing Asia, IGLOO SECURITY has devoted itself in continuous research and development in the convergence security area and customer satisfaction.

It is IGLOO SECURITY's corporate value to protect customers from all security risks and threats in the world and make them feel safe, and it is a mission of IGLOO SECURITY to become a company that can ultimately contribute to society by continuing corporate growth based on customer satisfaction.

6 Floor. 7, Jeongui-ro 8-gil, Songpa-gu,
Seoul, Republic of Korea

TEL +82-2-3452-8814

FAX +82-2-3452-8815

Homepage www.igloosec.com/en

E-mail osbiz@igloosec.com