SPIDER TM

SECURITY
INFORMATION &
EVENT
MANAGEMENT

SPiDER TM

IGLOOSECURITY
(株)イグルーセキュリティ

Cyber-Infinity
(株)シーアイシー

イグルーセキュリティが開発した次世代SIEM - SPiDER TM -

イグルーセキュリティの十数年間のセキュリティ監視ノウハウが集約されたSPiDER TMは、セキュリティデータの高速収集と保存によりログ管理の負担を軽減することができます。また、イグルーセキュリティ独自のセキュリティ・インテリジェンスを提供し、インシデントに対して効率的かつ迅速な対応ができるように支援します。

何が問題なのか？

多くの企業がますます巧妙化するセキュリティ脅威に対抗するために、多様なセキュリティ機器を導入していますが、セキュリティ情報の活用について頭を悩ましています。

イグルーセキュリティのSPiDER TM導入の必要性

Q1 SIEMを導入していますか?

セキュリティシステムの増加のため、人手では個々の機器から上がって来る大量のセキュリティデータを管理・分析することが難しくなりました。また、単一のセキュリティシステムだけではますます巧妙化するセキュリティ脅威を検知・対応するのが難しいため、統合的にセキュリティデータを収集・分析するSIEMの導入が必要です。

Q2 使用しているSIEM製品は、セキュリティ監視業務に最適ですか？

SPiDER TMは、イグルーセキュリティの十数年間のセキュリティ監視ノウハウと実際のセキュリティ監視担当者の業務の流れ及びニーズが反映され、セキュリティ監視業務に最適化されています。また、Knowledge Centerでは様々なセキュリティ脅威情報を継続的に提供します。

Q3 使用しているSIEM製品は、多様な分析機能を提供していますか？

シンプルな分析から多次元のシナリオ分析まで実行し、単純な攻撃だけでなく、APT攻撃や内部情報流出など、様々な脅威に対応することができます。また、インシデントタイプ別に分析ルールを簡単なスクリプトでユーザが直接設定することができ、リアルタイムおよび過去のデータ分析が可能です。

イグルーセキュリティのSPiDER TMとは

数多いセキュリティ製品とサーバから上がって来る膨大なセキュリティ・イベントログ及び多様なアプリケーションログを漏れなく収集し正規化して、リアルタイム又は過去のデータに対して的確な相関分析を行います。
また、セキュリティ監視業務に最適化されたプロセス及び機能の提供とイグルーセキュリティ独自のセキュリティ・インテリジェンスの提供により、**内・外部からの脅威から大事な顧客の情報資産を守ります。**

SPiDER TM 特長

Experience

SPiDER TMは、最初の検知からログの分析まで
一元化した監視環境を構成し、監視業務の効果を高めます。

リアルタイム アラート監視
リアルタイムで分析された
相関分析の結果について
段階別状況を把握

詳細分析
分析を通じて攻撃の推移と
IP、攻撃の種類などの
統計情報及び
生ログ形式のデータを提供

生ログ確認
詳細な分析を通じて
生ログを分析確認

関連ログ検索
ビッグデータベースの
ファイルDBで高速
検索結果を提供

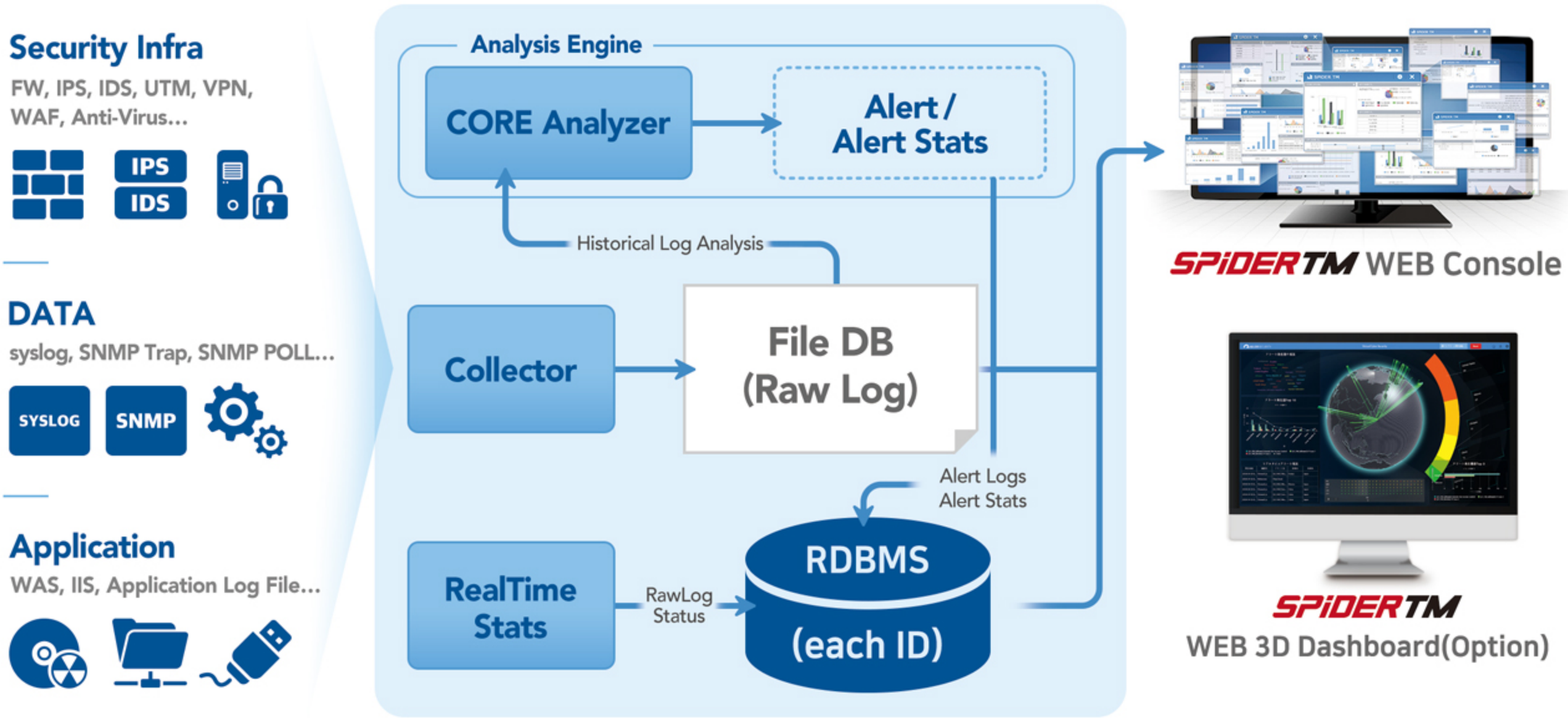
Intelligence

SPiDER TMは、イグルーセキュリティKnowledge Centerとの
連携により、様々なセキュリティ上の脅威情報を提供します。

Visibility

SPiDER TMは、3Dダッシュボードの画面構成により、直感的なデータの表現及び
ユーザーの特性を考慮した様々なカスタマイズ画面構成ができます。

SPiDER TM 構成図



SPiDER TM 主な機能

SPiDER TMの機能は、情報収集、分析、処理の3段階のプロセスで構成されます。

収集	大容量のログ収集	セキュリティ監視に必要な全てのログデータを収集・処理
	様々な製品のログ収集	セキュリティ機器だけでなく、サーバやアプリケーションログなど、様々なログを収集
分析	シナリオベースの相関分析	イグルーセキュリティの十数年間のノウハウが蓄積されたシナリオベースの相関分析ルールを提供
	高性能ファイルDB	高性能ファイルDBをベースにした検索結果を用いて効率的なログ分析を実行
	高度な分析エンジン	In-Memory 処理をベースに新しいアーキテクチャの多次元相関分析を支援
	効率的なログ分析	一つの画面でインシデントに関連した全てのトリガーデータの検索と分析が可能
処理	ユーザー定義 ダッシュボード&レポート	カテゴリ別に標準化したレポートの作成だけでなく、カスタマイズしたレポートも提供
	3Dダッシュボード	3Dベースのダッシュボード画面構成により、直感的にデータが認知でき、 ユーザーの特性を考慮した様々なカスタマイズ画面構成及びコンテンツの編集機能を提供
	多様な通知機能	インシデントのレベルによってメール、SMSなどでのアラート機能があり、アラートはリアルタイムで通知
	セキュリティ脅威情報共有	イグルーセキュリティ独自のKnowledge Center を通じてブラックリストIP/URLを自動的に 更新できるように支援し、最新のセキュリティ動向などを提供
	不正コード配布元自動 収集情報提供	自社開発の不正コード配布元自動収集システムにより世界中から収集した有害サイトの情報を提供
	インシデント対応	分析されたアラートについて体系的な対応プロセスを提供し、迅速なインシデント対応ができるように支援

SPiDER TM サービス

SPiDER TM

システム構築と導入、操作トレーニング、製品を用いた監視サービスまで
SPiDER TMの活用に関する悩みをワンストップで解決します。

導入支援サービス

- 製品導入コンサルティング
- 環境構成カスタマイズ支援
- ルール設定カスタマイズ支援

トレーニングサービス

- 製品運用･活用方法
- MSS運用方法
- 脆弱性診断、マルウェア分析など

監視サービス

- リモート監視サービス支援
- セキュリティシステム運用支援
- セキュリティ監視専門人材派遣

SPiDER TM 導入実績

公共

国家情報資源管理院	国家情報資源管理院	国会事務処	国会事務処
検察	検察	文化体育観光部	文化体育観光部
行政案全部	行政案全部	ソウル特別市庁	ソウル特別市庁

金融/教育

韓国銀行	韓国銀行	外換銀行	外換銀行
KB国民銀行	KB国民銀行	MIRAE ASSET	MIRAE ASSET
延世大学	延世大学	ソウル特別市教育庁	ソウル特別市教育庁

企業/通信

サムスン	サムスン	ロッテ	ロッテ
GS Caltex	GS Caltex	SK Telecom	SK Telecom
LG Telecom	LG Telecom	KT	KT

海外

日本	日本	エチオピア	エチオピア
モロッコ	モロッコ	インドネシア	インドネシア
中国	中国	UAE	UAE

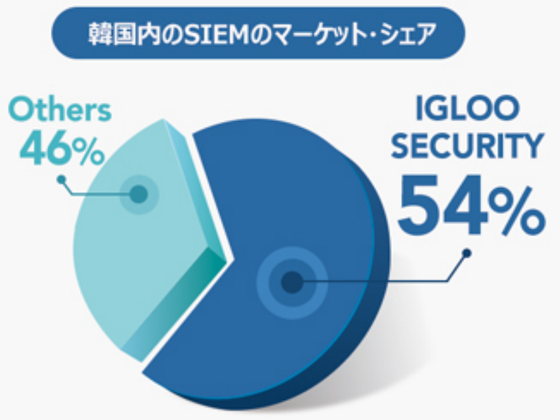
IGLOO SECURITY 会社概要

「SIEM」リーディングカンパニー

弊社は、統合セキュリティ管理システム「SIEM(Security Information and Event Management)」分野における、1999年に設立以来、過去10年以上技術開発に全力で取り組んでまいりました。業界トップレベルの開発人材を武器に、R&Dへの投資と技術革新へのたゆまぬ努力により、多様な情報セキュリティに関する脅威から、企業の重要な情報資産を守り、企業の運営とビジネスの継続性を支える優秀な商品を提供しています。また、弊社は、これまで培ってきた経験やノウハウ、専門知識、技術力などを最大限に活用し情報セキュリティの侵害から、顧客の大切な情報資産の保全と、IT基盤の運用体制を確立できるよう、最善の努力を傾けています。

(株)イグルーセキュリティ（IGLOO SECURITY Inc.）

- 設立：1999年
- 本社所在地：韓国ソウル
- KOSDAQ上場企業
- 事業分野：統合セキュリティ管理･監視ソリューション(SPiDER TM)
  マネージド･セキュリティ･サービス(HUSKY)
- 主要顧客：250ヶ所以上の政府、公共、教育、通信、企業など
  400サイト以上のマネージド･セキュリティ･サービス
- 日本支社：(株)シーアイシー(Cyber-Infinity Corp. 略称：CIC) 2017年設立、東京都千代田区所在



外風が強く気温が低くなればなるほど、より一層強固になるイグルーのように
外部の攻撃から情報システムを安全に守ります。

（株）イグルーセキュリティ

（株）シーアイシー

株式会社イグルーセキュリティ日本支社 | japan@igloosec.com | www.igloosec.com
株式会社シーアイシー | business@ci-corp.jp | www.ci-corp.jp
〒100-6005東京都千代田区霞が関3-2-5霞が関ビルディング5階KOTRA内 | 03.5501.0885