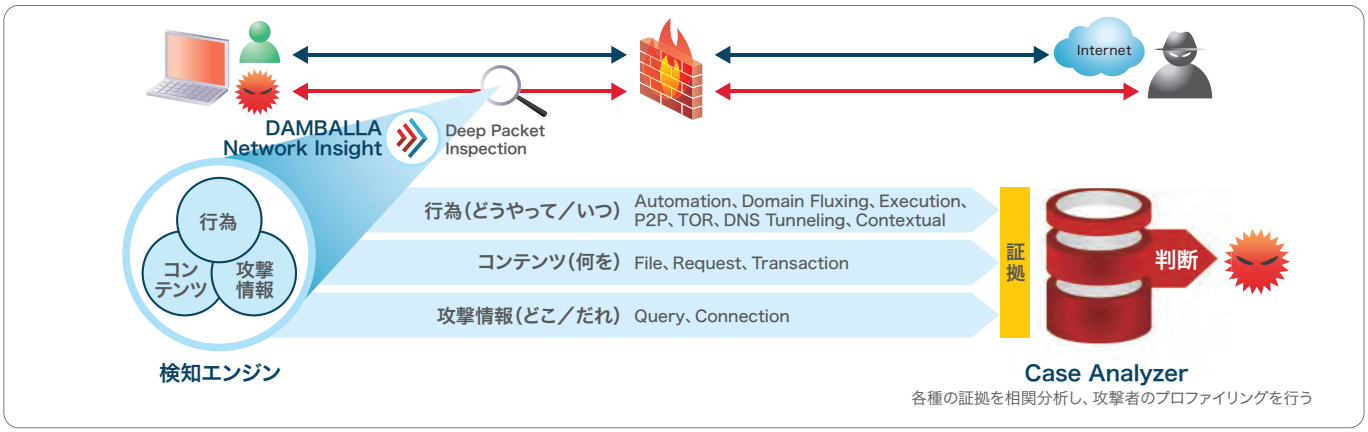
One Step Ahead of The Game
Asgent アズジェント

AIで未知のサイバー攻撃を検知
DAMBALLA Network Insight

巧妙化する脅威による不正アクセスや情報漏洩などの被害が後を絶ちません。ゲートウェイやエンドポイントで予防的セキュリティ対策を施しているにもかかわらず、時として脅威に屈する場面が現実にあります。数百数千の脅威を遮断することができたとしても、たった1つの脅威の侵入だけで、被害は発生してしまうのです。**DAMBALLA Network Insightは、予防対策をすり抜けた脅威を確実に検知し、被害が発生する前に対処することに主眼を置いたソリューションです。**

構内ネットワークのトラフィックを監視するセンサーにより、疑わしき挙動を検知。更に独自のリスク分析エンジンによる相関分析で被疑端末を特定、管理者に正確な感染状況と対処策を提供します。

■DAMBALLA Network Insight エンジンの動作



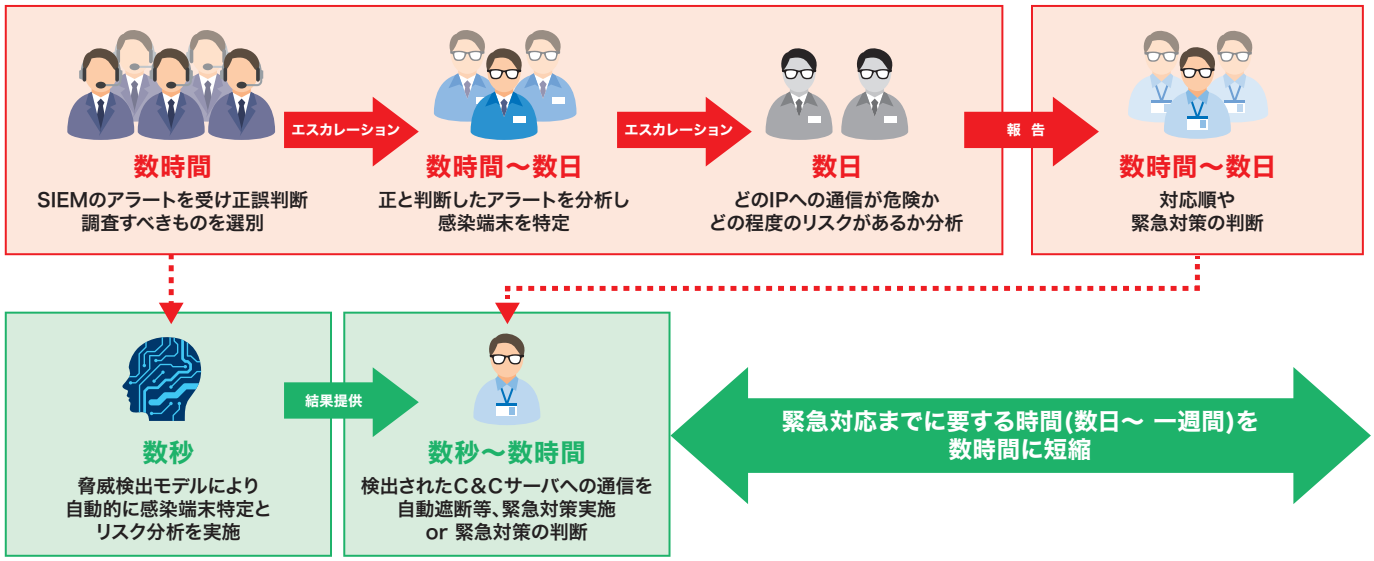
人工知能がインターネットからのサイバー攻撃を自動検知

攻撃の内容、使われたC&Cサーバを特定するため、即座に緊急対応可能

SOC / CSIRTの作業工数・費用を大幅削減

■SOC / CSIRTの監視・緊急対応業務を改善

【人力の場合】



【DAMBALLAの場合】

■（正確な検知）＋（高度な相関分析）＝感染端末の特定

12の検知エンジン

C&Cサーバなど外部のサーバと通信を実施している機器を見つけ出す。

- ✓ Connection
- ✓ Query
- ✓ File
- ✓ Request
- ✓ Domain Fluxing
- ✓ Automation
- ✓ Execution
- ✓ Peer-To-Peer
- ✓ TOR
- ✓ DNS Tunneling
- ✓ Transaction
- ✓ Contextual

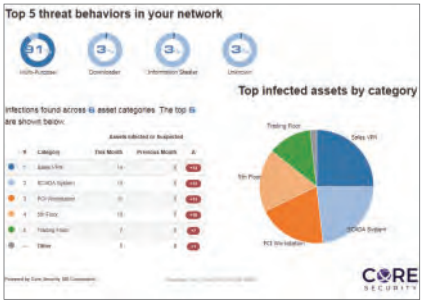
9つのリスク分析エンジン

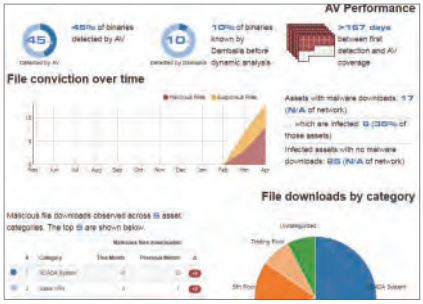
エンドポイントをリスク分析し優先付け、急対応が必要な端末を判断する。

- ✓ Data Transferred
- ✓ PCAP
- ✓ Communication Success
- ✓ Malicious File Availability
- ✓ Sequence of Events
- ✓ Importance of Endpoint
- ✓ Malware Family Intent
- ✓ Severity
- ✓ AV Coverage

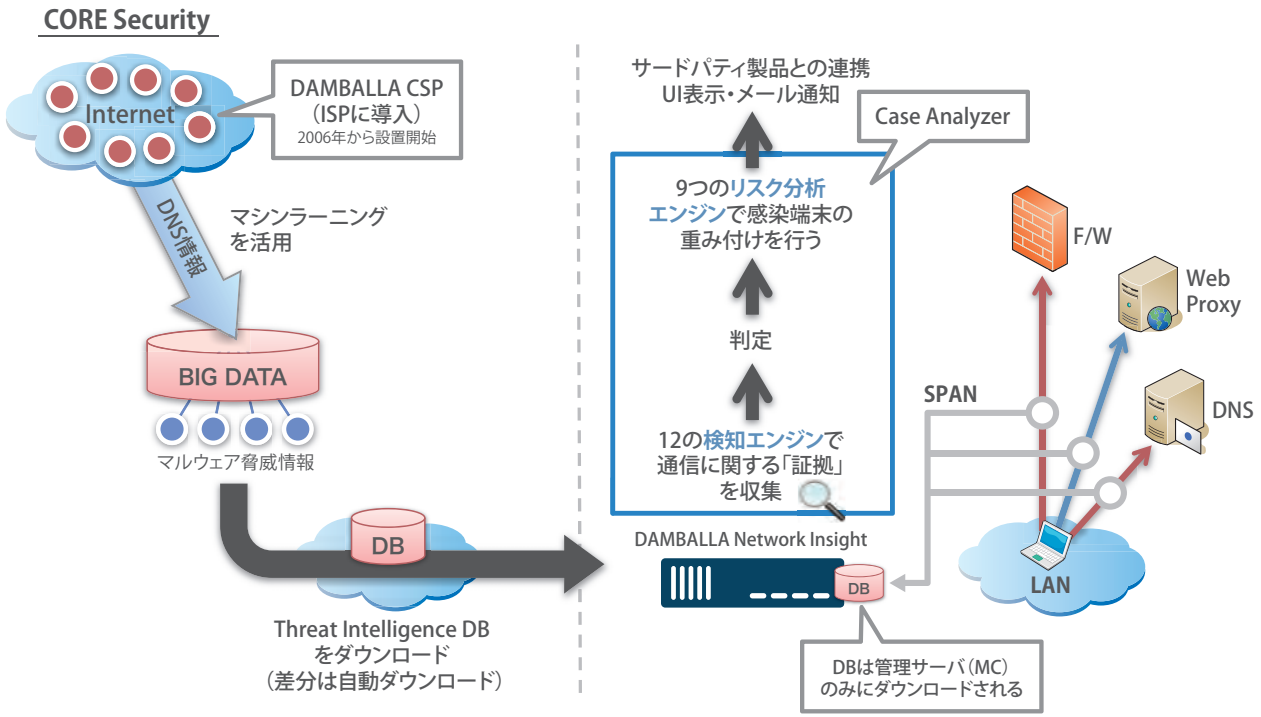
■ネットワーク感染を可視化

ネットワーク感染状況を把握するとともに、どの端末の対策が重要課題なのか、一目で把握することができます。





■DAMBALLA Network Insightの仕組み



開発元

CORE SECURITY

販売元

Asgent アズジェント
株式会社アズジェント

〒104-0044 東京都中央区明石町6-4
TEL：03-6853-7402
E-mail：info@asgent.co.jp
URL：http://www.asgent.co.jp/