THE NEW VALUE FRONTIER

KYOCERA

SecureOWL

セキュリティ免疫システム

Darktrace「Enterprise Immune System」

正しい通信を定義することで、内部ネットワーク上の異常を検知！

https://www.kccs.co.jp/secureowl/solution/internal/darktrace/

現在のセキュリティ対策における限界

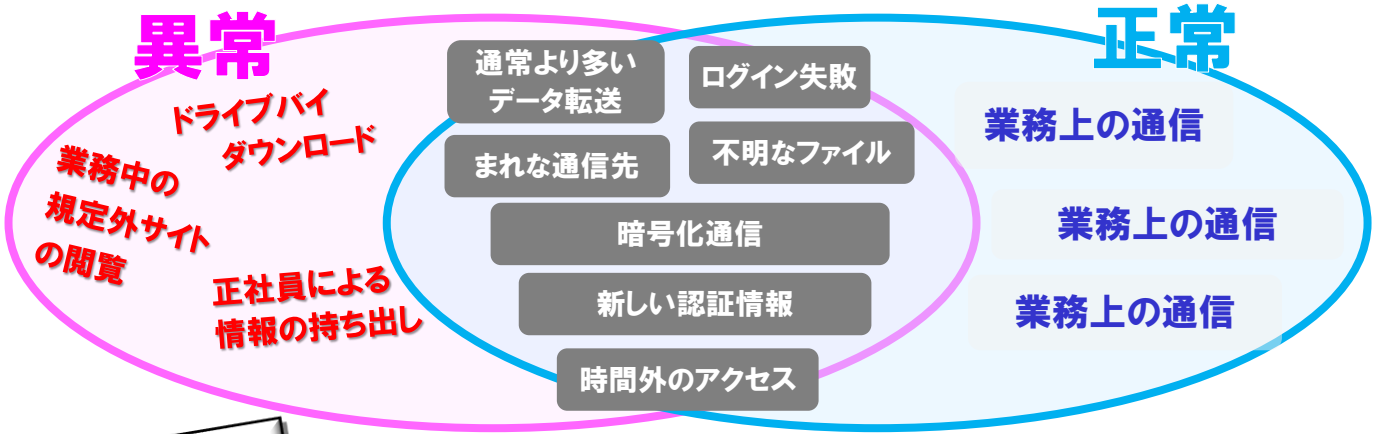
サイバー攻撃は日々進化しており、IDS/IPSやサンドボックス型のセキュリティ製品では検知できない攻撃が出現し、既存のセキュリティ対策での攻撃検知には限界がきています。
インシデントの報告がなかったとしても、安全とは言い切れない状態です。

たとえば・・・

- SSL 暗号化による SSL通信
- サンドボックスでは発動しないマルウェア
- 正社員による不正行為
- 標的型攻撃によるマルウェア感染

インシデントの報告がない＝本当に安全？

Darktraceが提供する新たなコンセプト



シグネチャレス

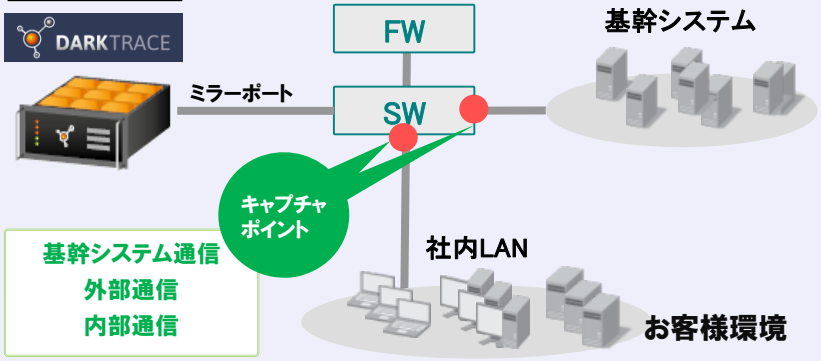
正しい業務上の通信を判別し、安全なネットワークであることを証明します！

Darktrace概要

製品概要

Darktraceは、**“AIによる機械学習”**により、ネットワーク内の通信を日々学習し、正常な通信を定義します。これにより、正常とは異なる異常な通信を検知を行います。アプライアンスをミラーポートに接続するため、既存のネットワーク環境を変更する必要がなく、導入が容易です。

構成イメージ



※監視する環境により、アプライアンスを複数台構成することも可能です。
※仮想アプライアンス版の利用も可能です。詳細はお問い合わせください。

検知例

- 機密情報が格納されたサーバに大量にログイン試行
- 営業担当者が、いつもと違うシステム管理者の権限でログイン
- 営業担当者が、夜中に人事情報へアクセス
- 業務用PCが外部（C&Cサーバ）と通信

Darktrace運用監視サービス

当社では、Darktraceの検知したアラートの報告／調査サービスをご用意しています。
報告対象のアラート内容を確認し、原因および影響調査後にメールにてご報告します（標準サービス）。

運用監視サービスメニュー

	標準サービス	オプションサービス
対応時間	当社稼働日　9:30-17:30 15時までに発生したアラートは当日対応	当社稼働日時間外、土日祝日
対象アラート	高危険度（70%以上）	
検知トリガー	アプライアンスからのアラートメール受信	
検知後アクション	・アラート内容確認 ・原因および影響調査 ・貴社セキュリティ担当者様にメール連絡	・貴社セキュリティ担当者様に電話連絡 ※発生連絡となり原因および影響調査は含みません。 ※アラート1件につき、お客様連絡先（最大3名）に順に1回電話連絡
対応件数	・30件 / 月を想定 ※想定件数を超える場合は、翌月に超過分をご発注いただきます。	・10件 / 月を想定 ※想定件数を超える場合は、翌月に超過分をご発注いただきます。

報告内容イメージ　※サンプル

【アラートNo】：24801 / 24802
【検知日時】：2017年1月19日 10:00:00
【検出脅威】：Data Sent to Rare Domain(75%) / Download and Upload(78%)
【検知内容】
対象端末より、短期間に内部サーバのポート番号 445 に対して SMB 接続し、約1.1GBのデータをダウンロード、同量のデータをまれな外部の通信先へアップロードした通信を検知しました。
このような挙動は社内のデータが外部に流出される不正な行動である可能性があるため、注意すべき事象であるとしてDarktraceによって検知されました。
－ 対象端末：PC001（172.168.1.1）
－ 内部サーバ：SV001（192.168.100.1）
－ 通信先：storage-kccs.co.jp（xxx.xxx.xxx.xxx）
内部サーバから読み取りに成功したファイルは以下となります（一部抜粋）
SMB Read Success ― share=¥¥192.168.100.1¥share file=customer¥ABC 株式会社¥運用¥個人情報¥DE本部¥34950284_201701.csv [445]
SMB Read Success ― share=¥¥192.168.100.1¥share file=customer¥ABC 株式会社¥運用¥個人情報¥FG本部¥34950285_201701.csv [445]

【確認事項】
外部への情報漏えいや社内ポリシーで許可されていない操作である可能性があります。当該端末の利用状況や操作ログを確認し、このデータ転送が業務上想定されたものであったかを確認することを推奨します。

※監視対象アラート、対応件数は、導入時のチューニングにて決定します。
※報告会、レポート作成は含まれておりません。

価格

■製品価格

月額 ¥195,000～／台
DCIP-S Small
（スループット300Mbps、250人規模）

■サービス価格

初期導入サービス（コンサルティング＋設置）：¥1,500,000～／回
運用サービス（標準）：　月額 ¥750,000～
運用サービス（オプション）：　月額 ¥250,000～

KYOCERA
京セラ コミュニケーションシステム株式会社
KCCSカスタマーサポートセンター
フリーコール　0120-911-901
携帯電話・PHS・IP電話など　050-2018-1827
受付時間　平日9:00 ～ 17:00
（17:00以降のお問い合わせは自動応答になります。）
KCCSホームページ　https://www.kccs.co.jp/
E-mail：kccs-support@kccs.co.jp

2017年1月現在