CYCRAFT

XENSOR

新世代のMDRエンドポイントセキュリティシステム

マシンラーニングと独自のFTAフォレンジック技術を融合させることで、高効率の自動情報セキュリティ脅威のトリアージ(ThreatTriage)を実現し、組織全体を対象に、リモートによるインシデント調査及び脅威ハンティング(Threat Hunting)等を行います。

Xensorは従来の情報セキュリティ商品と異なり、多次元の脅威情報を統合させたものであり、ユーザーアカウントのアクティビティ調査、プログラムメモリーフォレンジック、エンドポイントコンピュータフォレンジック及びネットワークトラフィック分析が含まれます。また、ウイルスシグネチャや機能ルールの追加は必要としません。スピーディーな対応により、情報セキュリティ対応コストの削減を実現します。

- Agentによるリアルタイム脅威ハンティングか、Agentlessフォレンジックモジュールのいずれかを選択できます
- 悪意あるプログラムの即時遮断と、リモート処理をサポートします
- SYSLOG通報に対応しており、カスタマイズ可能なAPIインターフェースにより、スピーディーなMSSP/SOCフローを導入できます
- IT管理フレームワークに合わせた、フルスタックフレームワークに対応しています

軽くてフレキシブル 容易なデプロイメント

システムリソースをほとんど使用せず、オンプレミやクラウドベースでの構築も可能。エンドポイントのデプロイメントにおいては、常駐型のリアルタイム脅威ハンティング、取付不要のフォレンジックモジュールスキャナのいずれかを選択できます。

フォレンジックの強化 積極的なハンティング

Windows、Linux、MacOSのプラットフォームをサポートしています。潜在的な脅威とハッカーの行為の形跡を自ら検出し、高い調査能力を発揮します。

合理的な投資リターンへの転換が可能

情報セキュリティチームの業務効率を高めます。スピーディーな対応により、ハッカーの侵入による損失を最小化し、会社のビジネス運営を強化します。

特徴

- APT悪意あるプログラムの侵入感知
- 高効率、軽量、マルチプラットフォーム
- 継続的なモニタリング、迅速な反応
- 悪意あるプログラムとメモリフォレンジック
- MITRE ATT&CK®による攻撃方法の識別に対応

対応オペレーティングシステム

- **Windows**
  Windows XP SP3/7/8/10
  Server 2003 R2 - 2019
- **Linux**
  Ubuntu 9.10 - 20.04
  Debian 7.0 - 9.0
  RHEL 6.0 - 8.1
  CentOS 6.0 ~ 8.0
- **MAC**
  MacOS X10.10 ～