TOSHIBA

商品情報 2021 -12

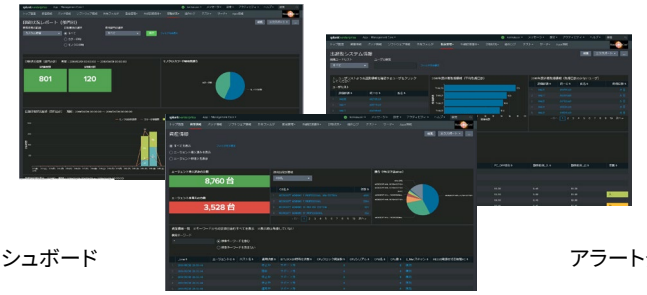
セキュリティ・IT資産・働き方見える化ソリューション

ログ解析テンプレート For MCore

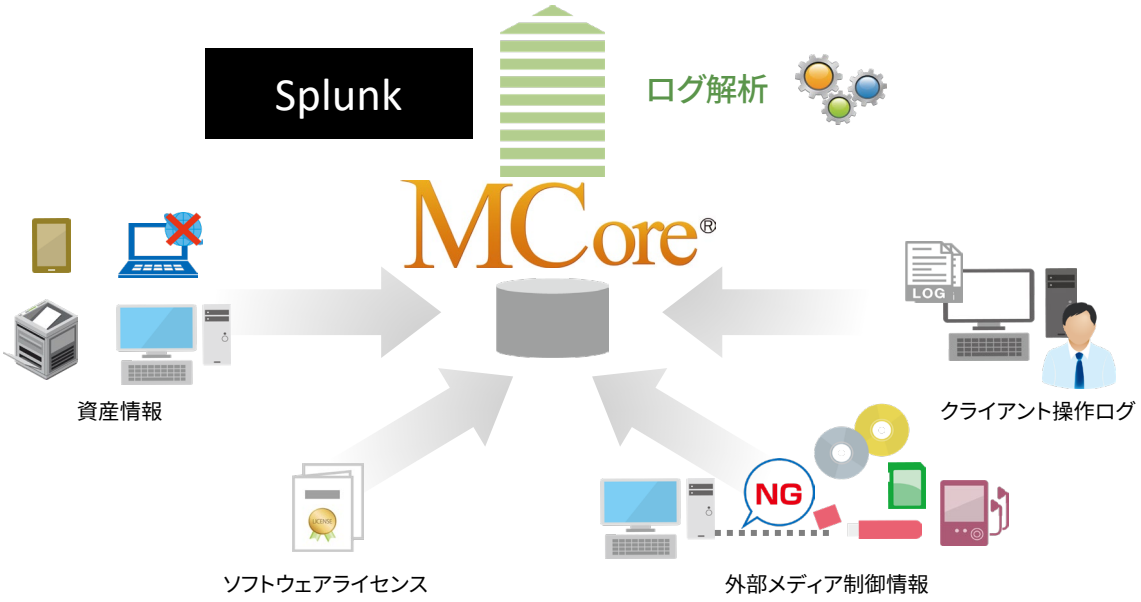
MCoreのインベントリや操作ログを Splunkにより管理・分析するAppを提供

「ログ解析テンプレート For MCore」は、MCoreのインベントリや操作ログをSplunkに取り込み蓄積することにより、今までは困難であったIT資産の継続的な変更管理を容易に実現。
また、他システムのログをSplunkに取り込み、MCoreの持つデータと合わせて多角的な分析を実現するデータ統合分析基盤を提供します。

MCore各種ログ蓄積　**資産使用状況管理インタフェース**　**証跡管理フォレンジック**



ダッシュボード　　アラート発報



資産情報　　クライアント操作ログ

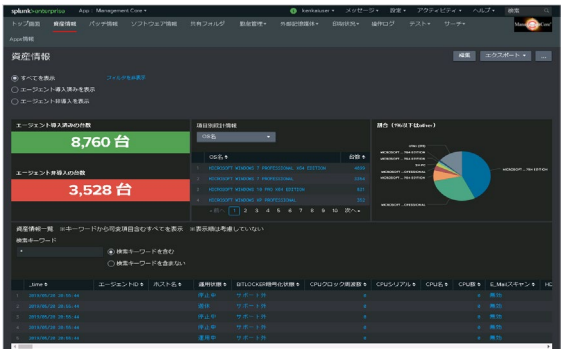
ソフトウェアライセンス　　外部メディア制御情報

東芝デジタルエンジニアリング株式会社

機能

■MCoreデータ蓄積・検索機能

MCoreが収集するインベントリデータの蓄積が可能。
蓄積した各種IT資産の変更管理情報をキーワードで一括検索でき、IT基盤の健全性や変動管理を簡単に実現します。



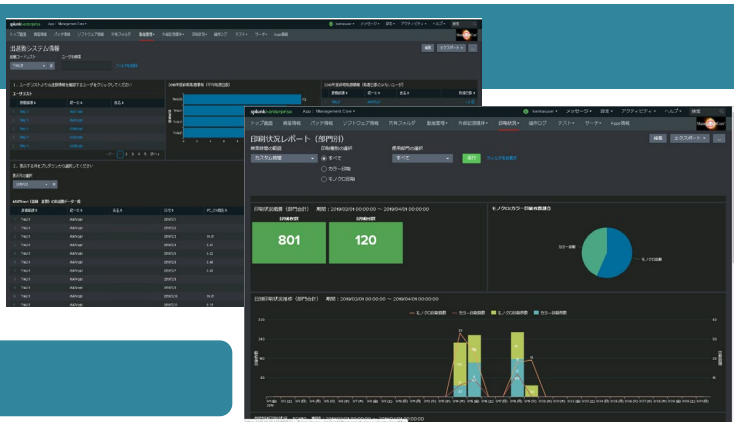
■データ統合分析基盤

勤怠データやメールサーバーログ、ネットワークログなど、
社内のさまざまなデータをMCoreのデータと組合わせ
多角的に解析。これまでとは違う観点で分析が可能です。

■閾値監視とアラート機能

MCoreのデータを分析し、あらかじめ設定した閾値を超えた
場合はアラートを発報するように設定可能。

カスタムダッシュボード例



1. 勤務状況分析

MCoreの操作ログからPCの稼働時間やアプリケーションの使用時間などのパソコン稼働状況を集計・表示することができます。
更に既設CASやICカードによる出退勤システムの入出時間データをSplunkに取り込み突合することで、
複合的な勤務状況、業務負荷状況など働き方改革に必要な現状分析が可能です。

2.情報流出インシデント分析

MCoreの操作ログから外部接続デバイスの使用状況とファイルの操作、メールサーバログからメール送信・受信履歴、Proxyサーバログから外部Webアクセス履歴、これらの情報を統合的に分析することで内部情報持ち出しの可能性のあるユーザ・PCの洗い出し・特定を行うことができます。

3.ネットワークセキュリティ分析

既設のFireWallやUTM、Proxyサーバなどのログを Splunkに取り込み、MCoreの操作ログと組み合わせて複合的に分析。標的型攻撃などでbot化した内部PCからのC&Cサーバへの通信、ダークウェブへのアクセスなどを検索・特定することができます。

□MCore®は住友電工情報システム株式会社の登録商標です。 □Splunk® はSplunk Inc.の米国、及び他の法域における登録商標です。
□一部機能はMCoreの純正オプション、及びSplunkのカスタマイズ等が必要です。
□本文中の会社名および製品名は各社が商標または登録商標として使用している場合があります。
□本資料の内容は予告なく変更される場合がありますのでご了承下さい。

(LS00021)

東芝デジタルエンジニアリング株式会社

E-mail: TDEN-sales@ml.toshiba.co.jp
https://www.toshiba-tden.co.jp/