NEWS RELEASE

2018 年 7 月 4 日
Ｓ＆Ｊ株式会社

大幅に機能を強化した SOC Engine のバージョン 3.0 が 大手証券会社に採用されました

S&J株式会社（以下「S&J」という。）は、自社開発SIEM（※）製品である「SOC Engine」の機能を大幅に強化したバージョン3.0を2018年７月１日より販売開始しました。

バージョン3.0は、大手証券会社に導入が決定しており、併せてＳ＆J監視センターにてセキュリティ監視を行うこととなっております。SOC Engineはこれまでも金融機関を中心に導入が進んでいますが、 バージョン3.0により他業種企業への展開が期待されます。

機能強化によりこれまで以上に精度の高い監視サービスを提供することができるようになり、お客様のCSIRTの負荷を軽減できるようになりました。

バージョン3.0の本年度売上は３億円を見込んでいます。

バージョン 3.0 による 主な機能強化	◆ これまでの相関分析に加えてAI（機械学習技術）を実装し、従来のSIEM機能よりも精度の高いマルウェアの動作検知ができるようになりました。 ◆ 常時SSL/TLS化と共にマルウェアが外部に行う通信もSSL/TLS化が進み、プロキシ等による従来の出口対策だけでは十分な監視が行えなくなってきていることに対応し、EDR（※）機能とPCの動作ログを収集する機能を提供する自社開発製品「KeepEye」からログを収集、分析する機能を追加しました。エンドポイントの動作ログと従来のプロキシなどのログを相関分析することにより、精度の高い監視サービスを提供できるようになりました。
SOC Engine の基本機能	◆ 様々なログを高速に取り込み、SIEMとして検知、分析するできることができます。 ◆ Ｓ＆Jのインシデント対応の経験や様々な調査による知見を基に開発された検知ロジックを組み込んでおり、複雑な相関分析とセキュリティイベントの検知を実現しています。 ◆ 提供形態としてオンプレミス（※）とクラウドがあり、要求される仕様により選ぶことができます。
監視センター	◆ SOC Engineを導入しているお客様のネットワークをサイバーセキュリティ専門のアナリストが監視・分析を24時間365日行っています。 ◆ サイバーセキュリティを監視するSOC（Security Operation Center）だけでなく各種機器の死活監視やパフォーマンス監視等も行うNOC（Network Operation Center）の機能も提供しています。

当社は、サイバーセキュリティのエキスパート集団として、これまでの豊富な経験と実績に基づき、日本のサイバーセキュリティ対策の向上に寄与してまいります。

プレスリリースに関する お問い合わせ先

S&J 株式会社　https://www.sandj.co.jp/
TEL：03-6205-8500　FAX：03-6205-8510
〒105-0003 東京都港区西新橋 1-18-17　明産西新橋ビル
経営管理部　中村 佳史　E-mail：　nakamura@sandj.co.jp

S&J 会社概要

S&J は、サイバー攻撃や内部関係者による情報漏えい等の内部犯行など、情報セキュリティは経営課題として認識されてきている状況下、「防御・検知・対処」や「技術・体制」のバランスを重視した製品やサービスを提供しています。
また、お客様に高いレベルのセキュリティサービスを提供するために、自社での製品やサービスの開発に積極的に取り組んでおります。政府機関や大企業におけるセキュリティアドバイザーやインシデントレスポンスの豊富な経験を活かしたコンサルティングサービスもご提供しております。

会社名	S&J 株式会社
資本金	9,865 万円
設立	2008 年 11 月 7 日
本社所在地	〒105-0003　東京都港区西新橋 1－18－17　明産西新橋ビル
代表者	三輪　信雄
ウェブサイト	https://www.sandj.co.jp/
事業内容	サイバー攻撃対策システムの開発及び運用、サイバー攻撃監視やセキュリティ診断、コンサルティング、インシデント対応などのサービス提供

※ SIEM（シーム：Security Information and Event Management）
様々なログを一元的に管理し、当該ログを自動的に相関分析して、セキュリティリスクの把握を行い、システム管理者の負担を軽減する「セキュリティ情報及びイベント管理製品」のこと。

※ EDR（イーディーアール：Endpoint Detection & Response）
「エンドポイントで脅威を検知して、対応を支援する」ことを主眼としているセキュリティ製品のこと。エンドポイントにおける脅威の動きを包括的に可視化し、ハッキング活動の検知・観察や記録、攻撃遮断などの応急措置といった機能を提供する。

※ オンプレミス
サーバーやソフトウェアなどの情報システムを使用者（ビジネス利用の場合は企業）が管理する設備内に設置し、運用することを指します。