elastic

Search. Observe. Protect.

EDR vs XDR

EDR（Endpoint Detection & Response、エンドポイント検知と応答）と、XDR（eXtended Detection & Response 拡張型検知と応答）は、1文字しか違いません。しかし、サイバーセキュリティチームが手にする成果は大きく異なります。2つのソリューションで“できること”の違いをリストにまとめました。

EDR	XDR
• エンドポイントに特化した保護	• エンドポイント、クラウド、ユーザー、ネットワークなど、各種ベクトルにわたる多様な統合を使用した幅広い検知
• 機械学習を使用して、マルウェアやランサムウェアを検知、防御	• EDRが持つ機能に加えて、機械学習を活用した分析によってアクティビティを相関付け、脅威を特定
• 最低限の統合機能を備えたスタンドアローンツール	• 他のツールを統合でき、アナリストには単一の参照ポイントとして機能する一元的セキュリティプラットフォーム
• 高いセキュリティ成熟度は不要	• 高いセキュリティ成熟度や確立されたセキュリティチームが必要
• エンドポイントで攻撃をブロック。検知アラート、ホスト分離、自動対応の機能を搭載	• EDRが持つ機能に加えて、さまざまな脅威ベクトル、環境、ソリューションへと拡張された一元的な管理および実行の機能を搭載

EDRが時間をかけてセキュリティチームの既存のツールセットに組み込まれるのに対し、XDRは組織の攻撃面全体にわたって効果的に監視、検知、対応する能力を引き上げます。

自社のニーズに最適なソリューションはどちらなのか、お悩みですか？ご安心ください。併用できます。ElasticセキュリティのLimitless XDRは、SIEMとクラウドセキュリティのほかに、EDRを主要コンポーネントとして内蔵する包括的なソリューションです。**詳しくは、elastic.co/jp/securityをご覧ください。**

