

NextComputing 社 可搬型キャプチャ装置の新製品「CyberPro Plus 20G」をリリース



CYBERPRO PLUS^{20G}

- ・ CyberPro Plus 20G は、20Gbpsトラフィックの連続ロスレスキャプチャ、大容量ストレージ、またリアルタイム分析用ディスプレイを統合して提供する可搬型キャプチャ装置です。
- ・ ネットワークのあらゆるシーンで、パケットキャプチャから解析まで、ネットワークインシデントにワンストップで対応でき、ハイパフォーマンス、高い拡張性、柔軟なモニタシステム構成、優れたポータビリティのすべてを実現可能です。

特に、取得データから目的の情報を高速検索し、IDS アラートやMITER ATT&CK マトリックスによる不正アクセス検出をリアルタイム実行するサイバーセキュリティ利用にも最適なソリューションです。

[製品の特長]

- 20Gbps の連続ロスレスパケットキャプチャ性能。
- ストレージは、オプションのリムーバブルドライブで、標準 20TB から 40TB まで拡張可能。
- MITER ATT&CK マトリックスのポリシーマッピングをサポート。
- PCAP、IPFIX/netflow(フロー情報)、ログファイルを同時検索。
- リアルタイム実行/ユーザ定義可能な Active Trigger 機能を搭載。BPF 構文で設定し、条件に該当した場合にアラート表示可能。
- SNORT、SURICATA がラインレートで実行可能。
- 機能統合された Web GUI でデータ取得からサイバー調査まで本製品ワンストップで対応。
- CLUSTER / FEDERATION 構成が可能(後述)。複数ユニット間でのキャプチャトラフィック負荷分散やストレージクラス構成も可能。用途に応じてモニタシステム構成を容易かつ柔軟に実現。

[製品の仕様・諸元]

- パケットキャプチャ・インターフェース: 2 × 10GbE ポート(SFP+)
- ロスレスキャプチャ・レート: 20Gbps(10Gbps × 2)
- タイムスタンプ精度: 150 nanoseconds
- キャプチャ用ストレージ: 標準 20TB(40TB まで拡張可能)
- データ抽出用ストレージ: 2TB
- 制御 GUI: 本体ディスプレイ、リモートアクセス WebGUI
- リモートアクセス・インターフェース: 1GbE(RJ-45)ポート
- 筐体サイズ: 430(幅) × 360(高さ) × 181(奥行) cm
- 筐体重量: 約 13kg(ソフトキャリングバッグを含む)

[ユースケース]

● リアルタイムのインシデント対応支援ツール

ATT&CK マトリックスにより得られる情報をリアルタイムに GUI 表示。サイバー攻撃や疑わしいネットワーク挙動を早期に検出できます。



● 長時間のデータ取得、100Gbpsトラフィックの取得

あらたな機能として、CLUSTER 構成・FEDERATION 構成をサポート。

CLUSTER: 複数ユニットのストレージを一括利用。

FEDERATION: 複数ユニットで 100Gbps トラフィックを分割取得。1 台の GUI から全ユニットのデータ検索が可能。

