



..AND THE FUTURE IS LITE



海事産業は、サイバー犯罪者にとってますます「儲かる標的」になりつつあります。多くの船主、代理店、さらには船舶でさえ、サイバーセキュリティ犯罪に見舞われ、回復プロセスで数え切れないほどの時間と潜在的な資金を失っています。

Vanir Liteは、低コストで大企業に採用されるレベルのサイバーセキュリティ機能を提供することを目的に開発されました。

Vanir Lite は以下の5つの機能を有します。

1. 高度なエンドポイントプロテクション
2. 24/7 ログ収集及びモニタリング
3. アセットマネジメント・ネットワーク管理
4. リスクマネジメント
5. セキュリティレポート及び可視性

高度なエンドポイントセキュリティ

ESET Endpoint Securityをベースに定期的なデータベースのアップデートを自動で行うことにより、陸上にいるのと同様変わらないサイバーセキュリティ対策を船舶に提供します。



エンドポイントセキュリティには以下の機能が含まれます。

NAP (Network Attack Prevention)

2017年の広範なNotPetya攻撃で使用されたEternalblueなどのネットワーク攻撃を検出して停止できるネットワーク攻撃保護を備えています。

Botnet protection & Ransomware protection

ボットネット保護を使用して、デバイスと悪意のあるボットネット間の初期通信をブロックします。

Device, Application and site blocking

アプリケーション、USBフラッシュドライブなどの接続デバイス、およびWebサイトへのアクセスをブロックできます。

24/7 ログ収集及びモニタリング

Vanir Liteのすべてのコンポーネントは、認定されたネットワーク/セキュリティエンジニアによって、ISO27001認定のPort-ITセキュリティオペレーションセンターから24時間年中無休で監視およびログに記録されます。

デバイスからのログも収集され、船主に船内のサイバーセキュリティイベントを通知するアラートを作成できます。

アセットマネジメント・ネットワーク管理

強力なネットワークスキャンと監視モジュールを使用して、ネットワーク上の他のデバイスを検出します。

Vanir Liteが一旦インストールされると、インストールされた他のプログラム/実行中のプロセス/ハードウェア等の詳細な情報が収集され、陸側のWebポータルに送信されます。

リスクマネジメント

資産管理モジュールを介して収集されたデータを使用して

リスク評価を実行し、IMO2021への準拠を支援します。

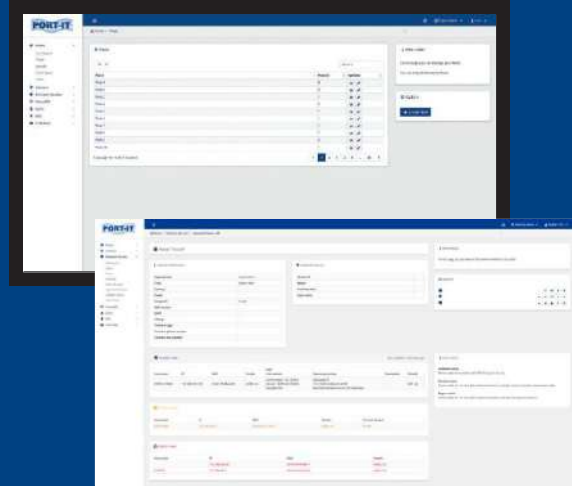
リスク評価には、ITネットワークに接続されているすべてのデバイスと、指定されたIT責任者または組織の情報が含まれます。

セキュリティレポート及び可視性

ネットワークに接続されているすべてのデバイス、インストールされているハードウェアおよびソフトウェアの記録を含む完全なレポートを船内で作成できます。このレポートは、PSCや他の当局に提出して、船内のサイバーセキュリティリスクを最小限に抑えるための適切な措置を講じていることを示すことができます。

Port-IT Web portal

Vanir Lite内のすべてのコンポーネントと機能は、Port-IT Web ポータルを使用して陸上スタッフが構成およびカスタマイズできます。すべてのレポートとログもここで表示できます。



The Endpoint Protection Solution included in Vanir Lite is specifically tailored for the maritime industry.

For a Total Security Suite, a UTM can be added to Vanir Lite. The UTM will intelligently analyze traffic and discern between malicious and safe traffic. Using a wide variety of network-based protection methods, the UTM is also able to dynamically switch between viable internet connections. Detailed bandwidth reports can be exported for extra visibility.



Using the data collected via the asset management module, a risk assessment can be performed to assist in IMO 2021 compliance. The Risk Assessment will include all devices connected to the IT network. The information of the designated IT responsible person or entity.



With human error playing a part in so many security breaches, security awareness plays an important role in preparing for IMO compliance.

A comprehensive approach to cyber security awareness training for employees is available. This program includes a highly engaged, customized online training that requires no wifi onboard and prepares crew for the most common security breaches that occur, and teaches them how to react upon it.

IMO 2021 COMPLIANCY

Cyber preparedness is required to meet the IMO safety requirements. In order to comply, ships must be able to demonstrate what assets, personnel and procedures are in place on board and ashore to deal with cyber risk issues, what happens if systems are compromised and who has control.

Compliance will depend on having the right risk management, infrastructure and procedures in place.

All of the components and features within Vanir Lite will help secure your vessel and prepare it for IMO 2021 compliance.

All components of Vanir are monitored and logged 24/7 from an ISO 27001 certified Port-IT security operations center by a certified network /security engineer. All data from the devices that are connected to the network is stored in a secure cloud environment.



Remote monitoring and assistance



Above features will not only help secure vessels but also prepares shipping companies for IMO 2021 compliance. We will continue to lead the way - continuously working on extending the Vanir portfolio.

As environments evolve...so will we.

31/12/2020

IMO 2021 Compliant