

VMware NSX-T Data Center for Intrinsic Security (本質的なセキュリティのための VMware NSX-T Data Center)

コースについて

この 5 日間の実習トレーニング コースでは、本質的なセキュリティのための VMware NSX-T™ Data Center の構成、運用、およびトラブルシューティングに必要な知識、スキル、ツールについて学習します。このコースでは、分散ファイアウォールとゲートウェイ ファイアウォール、侵入検知と侵入防止 (IDS/IPS)、VMware NSX® Intelligence™、ネットワーク検出と応答 (NDR) など、NSX-T Data Center のすべてのセキュリティ機能について説明します。

また、構成に関する一般的な問題とその解決方法についても説明します。

コースの目標

このコースを修了すると、次のことができるようになります。

- 情報セキュリティ関連の概念を把握する
- 各種ファイアウォールとそのユースケースについて理解する
- 侵入検知システムと侵入防止システムの操作について理解する
- VMware が提供する本質的なセキュリティ ポートフォリオについて理解する
- VMware NSX® セグメンテーションを使用してゼロトラスト セキュリティを実装する
- ユーザーとロールの管理を構成する
- 分散ファイアウォール、ID 認証ファイアウォール、および時間ベースのポリシーを構成およびトラブルシューティングする
- ゲートウェイ セキュリティを構成およびトラブルシューティングする
- VMware vRealize® Log Insight™、VMware vRealize® Network Insight™、および NSX Intelligence を使用して、NSX ファイアウォールを運用し、セキュリティに関する推奨事項を実現する
- グループ化、タグ付け、およびルール構成に関連するセキュリティのベスト プラクティスを理解する
- North-South および East-West サービス インサーションについて理解する
- エンドポイント保護について理解する
- 分散 IDS/IPS を構成およびトラブルシューティングする
- ネットワークの検出と応答の機能を理解する

対象者

- 上級セキュリティ管理者

前提条件

以下について理解している、または以下の知識を有している必要があります。

- TCP/IP サービスとプロトコルについて詳細に理解していること
- 以下を含むネットワーク セキュリティの知識と実務経験：
 - L2-L7 ファイアウォール
 - 侵入検知システムおよび侵入防止システム
- VMware vSphere® 環境と KVM ベースの環境の知識と実務経験

「VMware Certified Technical Associate - Network Virtualization」認定資格を取得していることが推奨されます。

受講方法

- 教室開催
- ライブ オンライン
- [一社様向けオンサイトトレーニング](#)
- [オンデマンド](#)

使用製品

- VMware NSX-T Data Center 3.1

コースのモジュール

1 コースについて

- 概要およびコースの流れ
- コースの目標

2 セキュリティの基本

- 情報セキュリティ関連の概念を把握する
- 各種ファイアウォールとそのユースケースについて理解する
- 侵入検知システムと侵入防止システムの操作について理解する

3 VMware が提供する本質的なセキュリティ

- VMware が提供する本質的なセキュリティ戦略を把握する
- VMware が提供する本質的なセキュリティ ポートフォリオについて理解する
- NSX-T Data Center が本質的なセキュリティ戦略にどのように対応しているかについて理解する

4 ゼロトラスト セキュリティの実装

- ゼロトラスト セキュリティを把握する
- ゼロトラスト アーキテクチャの 5 つの柱を理解する
- NSX セグメンテーションとそのユースケースを把握する
- NSX セグメンテーションでゼロトラストを適用するのに必要な手順を理解する

5 ユーザーとロールの管理

- NSX-T Data Center と VMware Identity Manager™ を統合する
- NSX-T Data Center と LDAP を統合する
- NSX-T Data Center のネイティブ ユーザーとロールについて理解する
- カスタム ユーザー ロールを作成して割り当てる

6 分散ファイアウォール

- 分散ファイアウォールのルールとポリシーを構成する
- 分散ファイアウォールのアーキテクチャについて理解する
- 分散ファイアウォールに関する一般的な問題をトラブルシューティングする
- 時間ベースのポリシーを構成する
- ID 認証ファイアウォールのルールを構成する

7 ゲートウェイ セキュリティ

- ゲートウェイ ファイアウォールのルールとポリシーを構成する
- ゲートウェイ ファイアウォールのアーキテクチャについて理解する
- ゲートウェイ ファイアウォールの一般的な問題を特定してトラブルシューティングする
- URL の分析を構成し、構成の一般的な問題を特定する

8 内部ファイアウォールの運用

- vRealize Log Insight、vRealize Network Insight、および NSX Intelligence を使用して NSX ファイアウォールを運用する
- NSX Intelligence の可視化および推奨機能について理解する
- グループ化、タグ付け、およびルール構成に関連するセキュリティのベスト プラクティスを理解する

9 ネットワーク内部監視

- ネットワーク内部監視について理解する
- North-South および East-West サービス インサーションのアーキテクチャとワークフローを理解する
- North-South および East-West サービス インサーションをトラブルシューティングする

10 エンドポイントの保護

- エンドポイント保護について理解する
- エンドポイント保護のアーキテクチャとワークフローを理解する
- エンドポイント保護をトラブルシューティングする

11 脅威に対する高度な防御

- MITRE ATT&CK フレームワークについて理解する
- サイバー攻撃のさまざまなフェーズを理解する
- NSX セキュリティ ソリューションを使用してサイバー攻撃から保護する方法を理解する
- 分散 IDS/IPS を構成およびトラブルシューティングする
- ネットワークの検出と応答の機能を理解する

お問い合わせ

このコースに関するご質問や登録方法については、japan-education@vmware.com までお問い合わせください。



VMware 株式会社 〒108-0023 東京都港区芝浦 3-1-1 田町ステーションタワーN 18 階 www.vmware.com/jp

© 2021 VMware, Inc. All rights reserved. 本製品またはワークショップ資料は、米国および国際的著作権法および知的財産法によって保護されています。VMware 製品は、<https://www.vmware.com/download/patents.html> のリストに表示されている 1 件または複数の特許対象です。VMware は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。

VMware は、一般的に認められている業界基準と慣例を使用して妥当な方法で、ここで記載されているワークショップ サービスを提供することを保証します。上記明示保証は、VMware が提供するサービスおよび成果物、ならびにそれらのサービスおよび成果物から得られる結果に関する、明示、黙示、法定、その他のあらゆる保証（商品性に対する黙示保証および特定目的に対する適合性の黙示保証を含みます）に代わるものです。VMware は、お客様に対して特定または参照した、いかなる第三者のサービスまたは製品に対しても責任を負いません。本ワークショップにおいて提供される資料（以下「ワークショップ資料」といいます）の著作権は VMware に帰属します。VMware は、お客様が許諾を受けた VMware 製品についての社内での理解、利用、運用を促進する目的に厳格に本ワークショップのお客様にワークショップ資料の使用および合理的な範囲でコピーを作成することを許諾します。前述の明示された場合を除き、本ワークショップの条件の下で許諾された知的財産権およびその他のいかなる許諾された権利を他者に譲渡することを禁止します。米国内のお客様の場合、サービスに関する VMware の契約当事者は、VMware, Inc. になります。米国外のお客様の場合、サービスに関する VMware の契約当事者は、VMware International Limited になります。