レポートダッシュボード

レポートダッシュボードは、エグゼクティブ、ネットワーク管理者、およびセキュリティアナリスト向けに設計されており、重要なワークフローステータスの視覚表示、トラブルシューティング機能、およびレポート作成機能を提供します。

[レポートダッシュボード（Reporting Dashboard）] ページを使用するには、UI の [レポート（Reporting）] に移動します。以下の項では、レポートの概要と、レポートのスケジュール設定と電子メール送信の方法について説明します。

レポートダッシュボード

レポートダッシュボードは、エグゼクティブ、ネットワーク管理者、およびセキュリティアナリスト向けに設計されており、重要なワークフローステータスの視覚表示、トラブルシューティング機能、およびレポート作成機能を提供します。

[レポートダッシュボード（Reporting Dashboard）] ページを使用するには、UI の [レポート（Reporting）] に移動します。以下の項では、レポートの概要と、レポートのスケジュール設定と電子メール送信の方法について説明します。

概要

概要セクションでは、ネットワークフロー情報、セキュリティポリシー、システムパフォーマンス、およびセキュリティ脅威に関するリアルタイムのインサイトが提供されます。これにより、セキュリティアナリストとネットワーク管理者は、情報に基づいた意思決定を行い、データに基づいてリソースを保護するためのプロアクティブな対策を講じることができます。

セグメンテーションの概要

ワークスペースは、クラスタ内のポリシーと適用を検出、適用、および管理するための構成要素です。ユーザーは、適切な範囲を選択してセグメンテーションのメンバーシップを定義します。

セグメンテーションの概要では、導入されている各ワークスペースの設定の詳細がキャプチャされます。ワークスペース内の特定の範囲、またはその範囲に関連付けられたワークスペースのポリシーの定義、分析、適用など、すべてのポリシー関連のアクティビティが実行されます。

次のグラフは、ワークスペースに関連付けられているさまざまなポリシーの概要を示しています。

図 *1*: セグメンテーションの概要

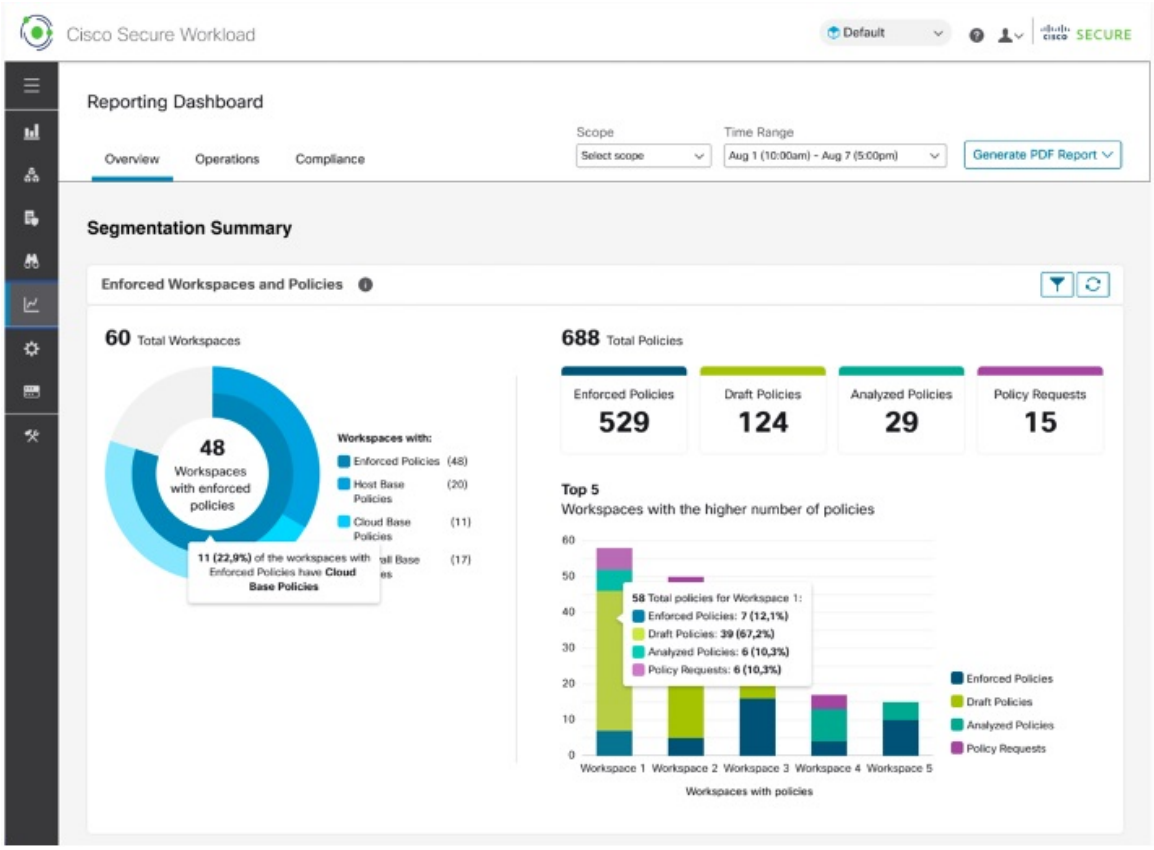
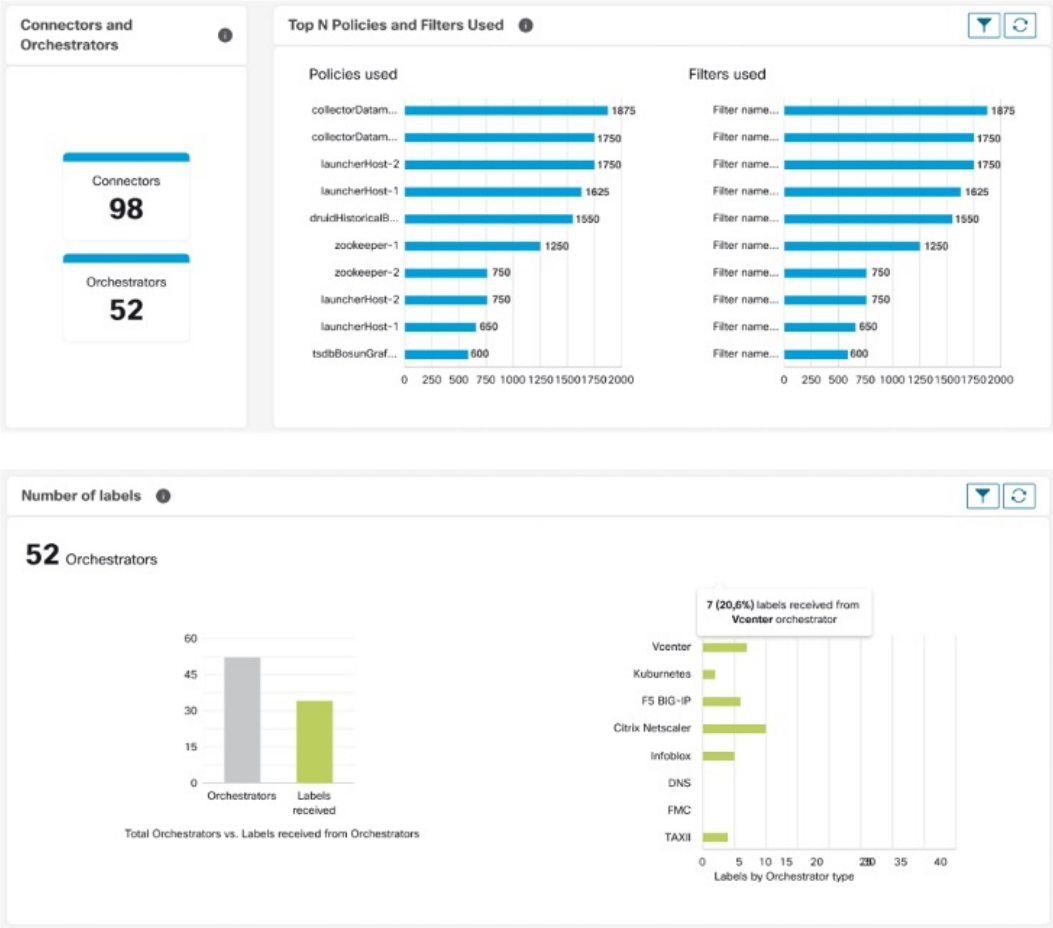


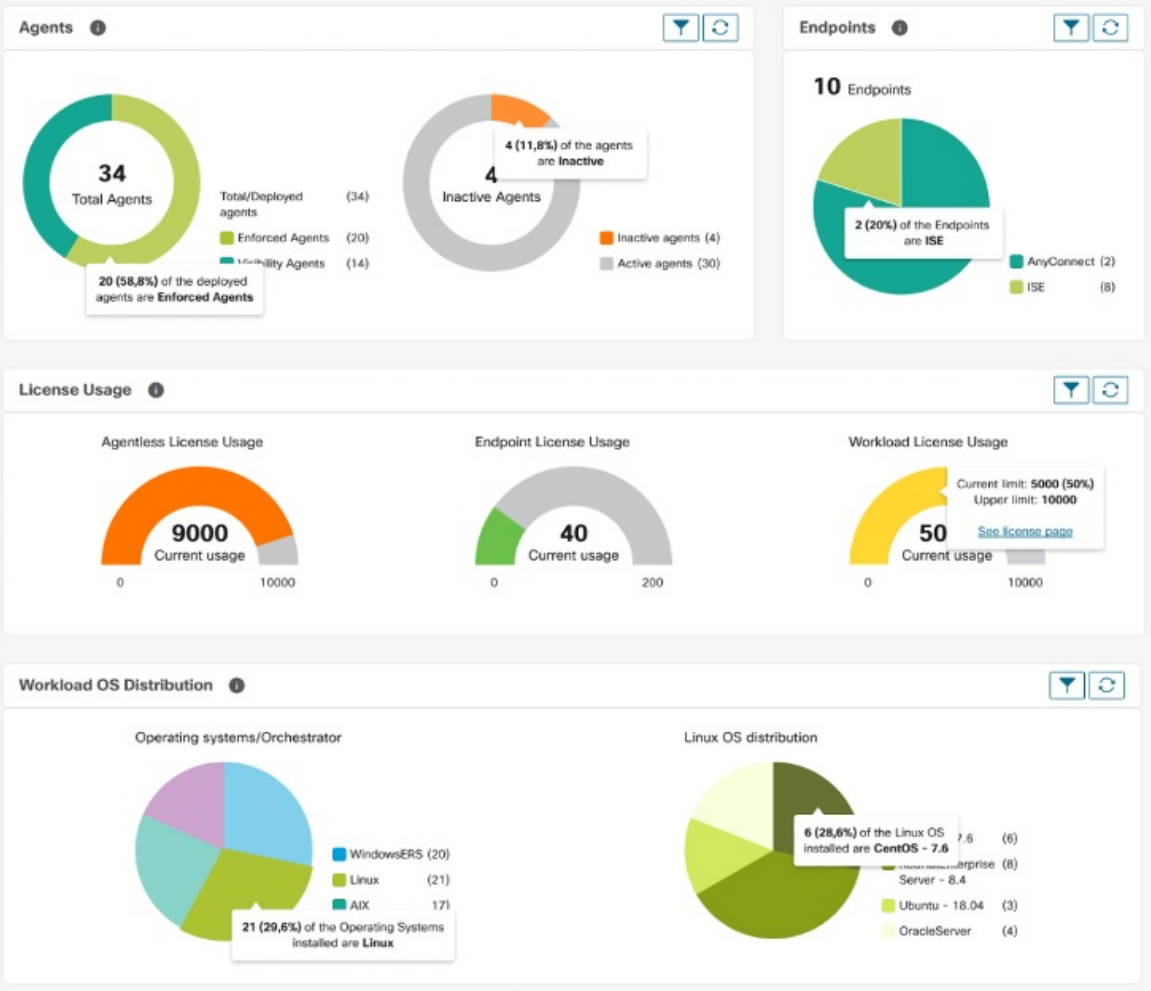
図 *2:* コネクタとオーケストレータ



ワークロードの概要

ワークロードの概要では、インフラストラクチャ内のサーバーとエンドポイントに展開されているエージェントの合計数の詳細が提供されます。エージェントは、ネットワークフロー情報をモニターおよび収集し、インストールされたホストにファイアウォールルールを使用してセキュリティポリシーを適用し、ワークロードのステータスを伝達し、セキュリティポリシーの更新を受信します。

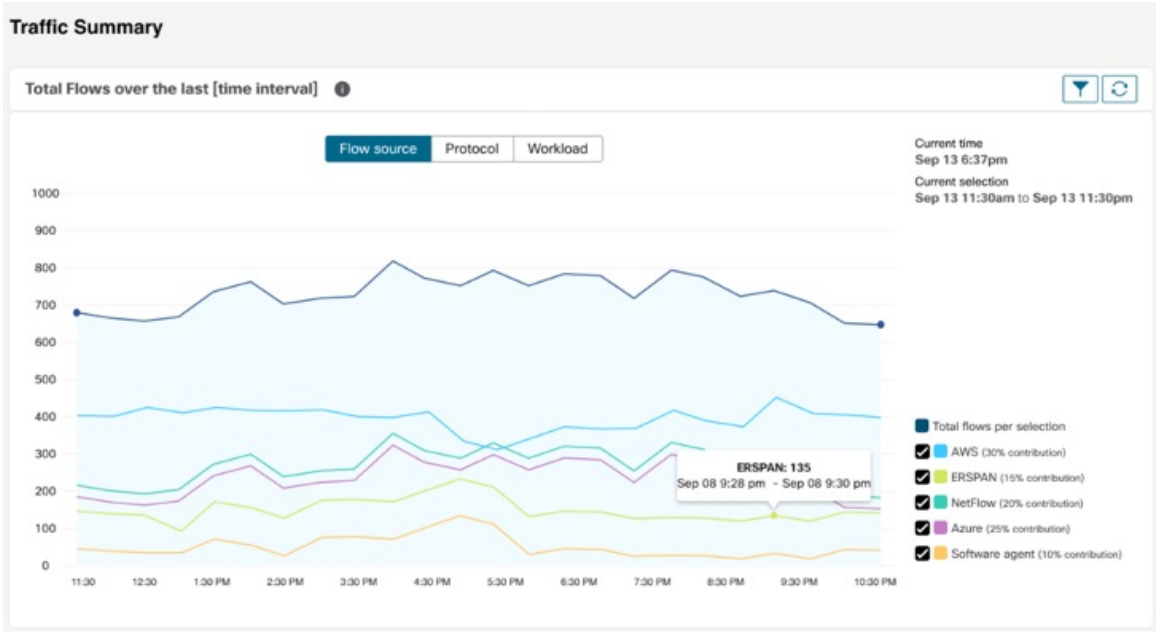
図 *3:* ワークロードの概要



Traffic Summary

トラフィックの概要では、各フローのフロー観測がキャプチャされます。フローソースの各観測で、フローのパケット数、バイト数、およびその他のメトリックが追跡されます。

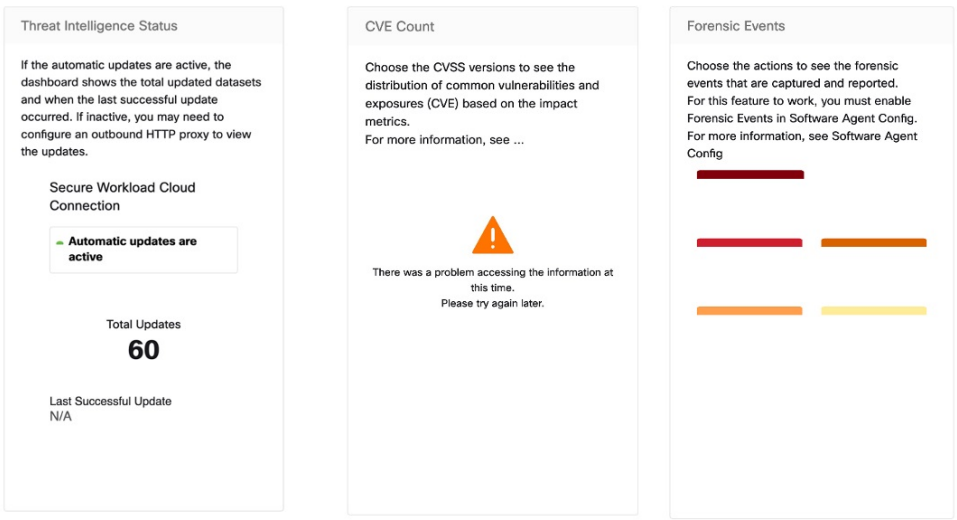
図 *4 : Traffic Summary*



セキュリティ サマリー

セキュリティの概要には、脅威インテリジェンスのステータス（脅威インテリジェンスのステータスの更新を最後に受信した時刻が表示されます）、CVEの数、およびフォレンジックイベントの分布が表示されます。

図 *5 :* セキュリティ サマリー

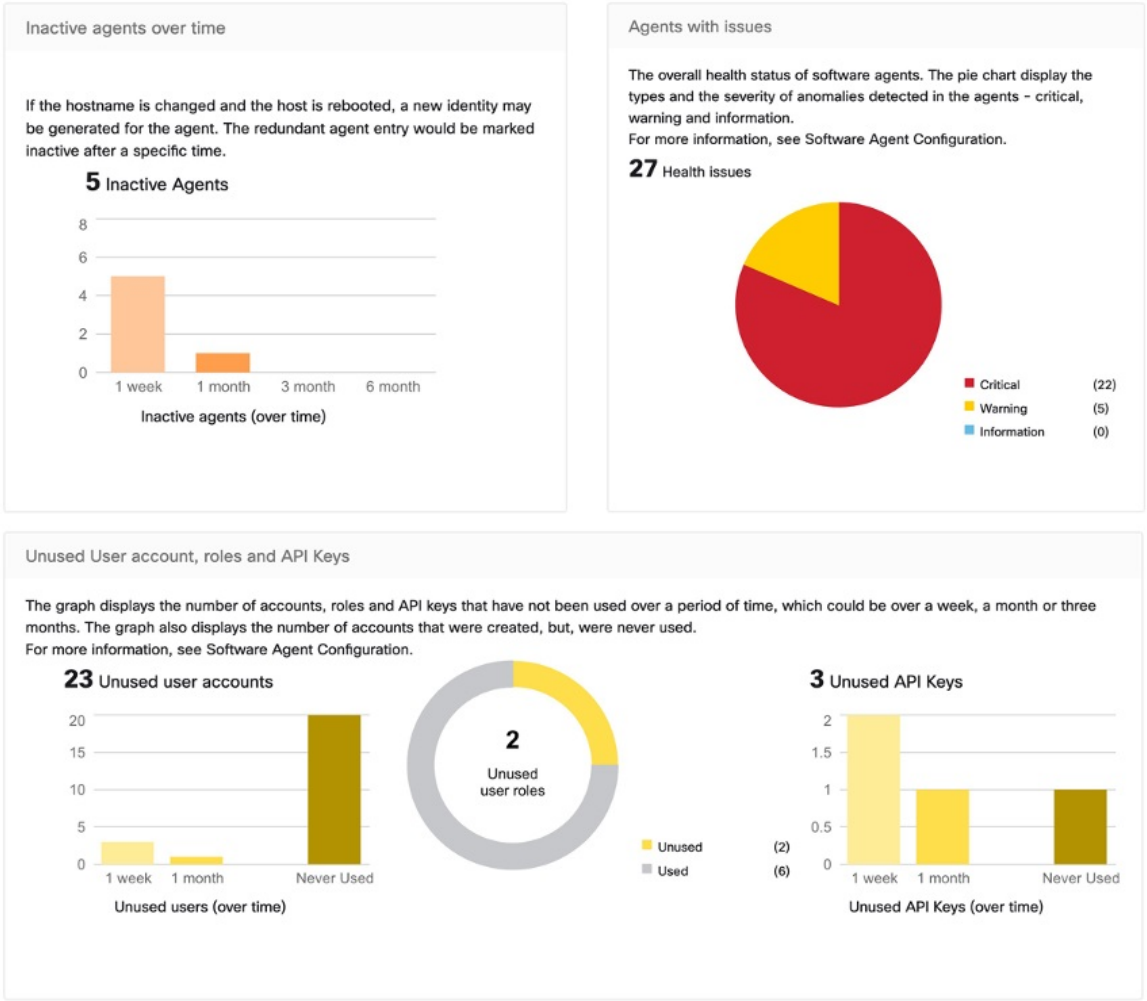


動作

ワークロードの概要

ワークロードの概要には、ネットワーク内のサーバーとエンドポイントに展開されているエージェントの合計数が表示されます。エージェントは、ネットワークフロー情報をモニターおよび収集し、インストールされたホストにファイアウォールルールを使用してセキュリティポリシーを適用し、ワークロードのステータスを伝達し、セキュリティポリシーの更新を受信します。

図 *6:* ワークロードの概要

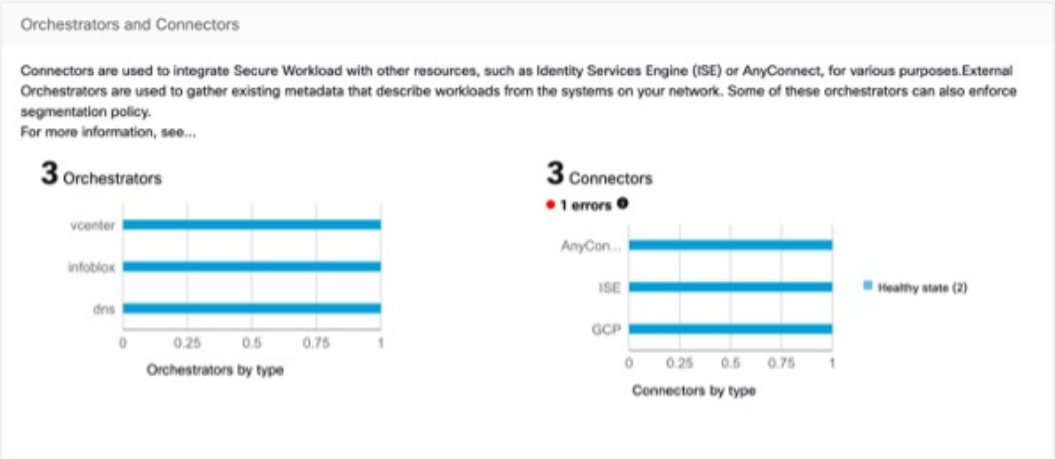


テレメトリの概要

仮想アプライアンスに展開された多くのコネクタは、ネットワーク内のさまざまなポイントからテレメトリを収集します。これらのコネクタは、アプライアンスの特定のポートでリッスンする必要があります。特定のセキュリティグループのフローログを設定している場合、コネク

タはフローログを取り込むことができます。また、可視化およびセグメンテーションポリシーの生成にテレメトリデータを使用することもできます。

図 7:テレメトリの概要



クラスタ要約

サイト管理者はクラスタステータスページにアクセスできますが、アクションはカスタマーサポートユーザーのみが実行できます。Cisco Secure Workload ラック内にあるすべての物理サーバーのステータスが表示されます。

クラスタの処理時間と保持時間は、クラスタ内でデータが保存および処理される期間を指します。具体的な処理時間と保持時間は、ワークロードの要件と組織のポリシーによって異なります。

クラスタを設定する際は、処理時間の要件を考慮することが重要です。これは、ワークロードのニーズを満たすために必要なストレージ容量と処理能力に影響を与える可能性があるためです。

保持時間は、データがクラスタ内に保持される時間の長さを指します。一部のワークロードでは規制またはコンプライアンスに関連する目的のためにデータを保持する必要が生じる場合がありますが、他のワークロードでは処理後に削除される場合もあります。ワークロードの保持ポリシーを確立して、データを適切な期間保持し、その後安全に削除して不正アクセスを防ぐことが重要です。

図 *8:* クラスタ要約

セグメンテーションの概要

セグメンテーションまたはアプリケーションワークスペースは、クラスタ内のポリシーと適用を検出、適用、および管理するための構成要素です。セグメンテーションの概要では、導入されている各アプリケーションワークスペースの設定の詳細がキャプチャされます。これには、適用があるワークスペースとないワークスペースの数、有効化/無効化されたポリシーの数、最新のポリシーがあるワークスペースまたは同期されていないワークスペースの数、およびドラフトポリシーがあるワークスペースとないワークスペースの数が含まれています。

図 *9 :* セグメンテーションの概要

コンプライアンス

ワークロードの概要

ワークロードの概要には、インフラストラクチャ内のサーバーとエンドポイントに展開されているエージェントの合計数が表示されます。エージェントは、ネットワークフロー情報をモニターおよび収集し、インストールされたホストにファイアウォールルールを使用してセキュリティポリシーを適用し、ワークロードのステータスを伝達し、セキュリティポリシーの更新を受信します。

図 *10 :*

セキュリティ サマリー

フォレンジックイベントを設定します。設定すると、すべての戦術がその下のルールなし、カウント 0 の状態で表示されます。戦術レベルで選択するには、フォレンジックルールを 1 つ以上選択します。戦術を選択すると、その下にあるすべてのルールが選択されます。デフォルトの MITRE ATT&CK ルールは、MITRE ATT&CK フレームワークからのアラート手法に対して指定されています。

図 *11 :*

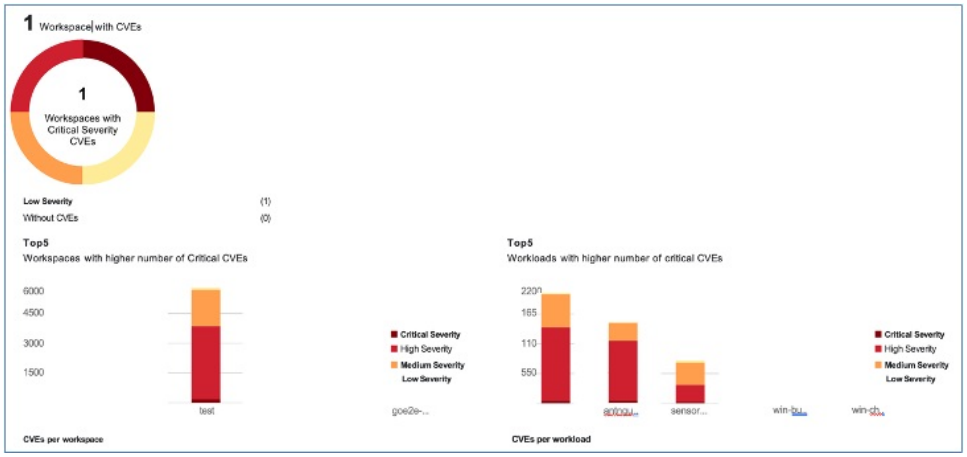
CVE を含むワークスペース

CVE のカウントでは、選択した範囲とスコアリングシステム（v2 または v3）に基づいて、選択した範囲内のワークロードの脆弱性（スコア順に並べ替え）が強調表示されます。重大な CVE の数が最も多いワークスペースとワークロードの分布を確認します。

ワークロード上のソフトウェアパッケージは、既知の脆弱性（CVE）に関連付けられている可能性があります。共通脆弱性評価システム（CVSS）は、CVE の影響を評価するために使用されます。CVE には、CVSS v2 および CVSS v3 スコアを設定できます。脆弱性スコアを計算するために、使用可能な場合は CVSS v3 が考慮され、それ以外の場合は CVSS v2 が考慮されます。

ワークロードの脆弱性スコアは、そのワークロードで検出された脆弱なソフトウェアのスコアから導き出されます。ワークロード脆弱性スコアは、CVSS スコアおよびベンダーデータに基づいて計算され、データが欠落しているか不正確な場合、セキュリティ調査チームによって調整される場合があります。最も重大な脆弱性の重大度が高いほど、スコアは低くなります。

図 *12 :*


1 Workspace with CVEs
1
Workspaces with Critical Severity CVEs
Low Severity (1)
Without CVEs (0)
Top5
Workspaces with higher number of Critical CVEs
6000
4500
3000
1500
test
goe2e-...
Critical Severity
High Severity
Medium Severity
Low Severity
CVEs per workspace
Top5
Workloads with higher number of critical CVEs
220
165
110
550
sensor...
win-bz...
win-cb...
Critical Severity
High Severity
Medium Severity
Low Severity
CVEs per workload

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。