Tableau de bord de production de rapports

Le tableau de bord de création de rapports, conçu pour les responsables, les administrateurs réseau et les analystes de sécurité, fournit des représentations visuelles de l'état des flux de travail critiques, des fonctionnalités de dépannage et des fonctionnalités de création de rapports. Dans le volet de navigation, choisissez **Reporting (Création de rapport)** > **Reporting Dashboard (Tableau de bord de création de rapport)** pour accéder au tableau de bord.

- Tableau de bord de production de rapports, on page 1

Tableau de bord de production de rapports

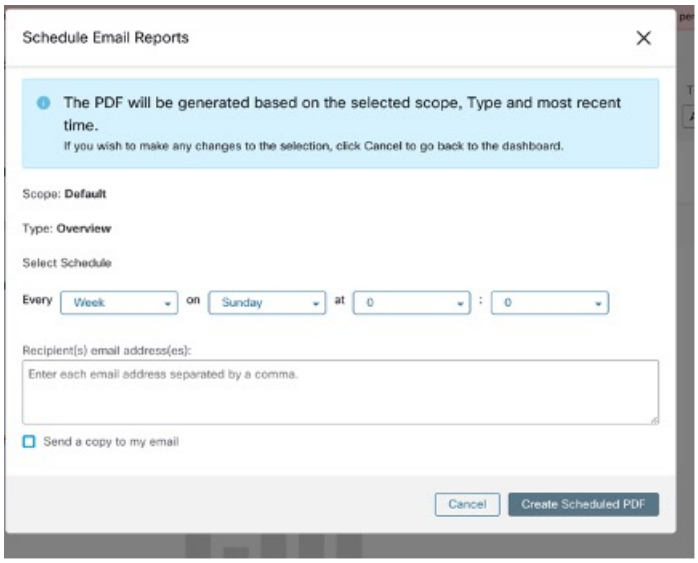
Les sections ci-dessous fournissent un aperçu des rapports et la façon de planifier et d'envoyer des rapports par courriel.

Planifier des rapports par courriel

Pour générer un rapport, choisissez l'une des options suivantes :

- **Télécharger** : après avoir généré un rapport, vous pouvez télécharger et enregistrer une copie du rapport pour consultation future.
- **Courriel** : si vous choisissez l'option des rapports par courriel, un courriel sera envoyé aux destinataires avec le rapport en pièce jointe.
- **Planifier** : vous avez le choix entre deux options pour planifier la production d'un rapport.
  - Tous les jours
  - Hebdomadaire

    Pour planifier la production d'un rapport, saisissez les détails de la planification pour déclencher le rapport. Sélectionnez Chaque semaine ou Tous les jours, saisissez le jour et l'heure, ainsi que les adresses courriel des destinataires. Cliquez sur **Create Scheduled PDF** (Créer un PDF planifié) pour enregistrer les détails.



Note Si la planification du rapport échoue, vérifiez le calendrier pour déterminer les adresses de courriel incorrectes ou les date et heure saisies de façon incorrecte.

Pour accéder aux planifications de rapports générées précédemment, choisissez **Generated Reports > Schedules** (Rapports générés > Planifications). Si la planification du rapport échoue, vérifiez le calendrier pour déterminer toute adresse de courriel incorrecte ou les date et heure incorrectes.

Note Le nombre maximal de planifications que vous pouvez stocker dans le tableau de bord des planifications est de cinq.

Aperçu

La section Aperçu fournit des renseignements en temps réel sur les informations relatives aux flux du réseau, les politiques de sécurité, le rendement du système et les menaces à la sécurité. Elle permet aux analystes de sécurité et aux administrateurs réseau de prendre des décisions éclairées et de prendre des mesures pour protéger leurs ressources de données.

Résumé de la segmentation

Les espaces de travail sont les pierres angulaires de la découverte, de l'application et de la gestion des politiques et de leur mise en application au sein de la grappe. Vous pouvez définir les adhésions à la segmentation en sélectionnant la portée appropriée.

Le résumé de la segmentation saisit les détails de configuration de chaque espace de travail, pour toutes les activités liées aux politiques, telles que la définition, l'analyse et l'application des politiques pour une portée particulière dans l'espace de travail ou les espaces de travail associés à cette portée.

Le graphique affiche un résumé des différentes politiques associées aux espaces de travail.

Figure 1: Résumé de la segmentation

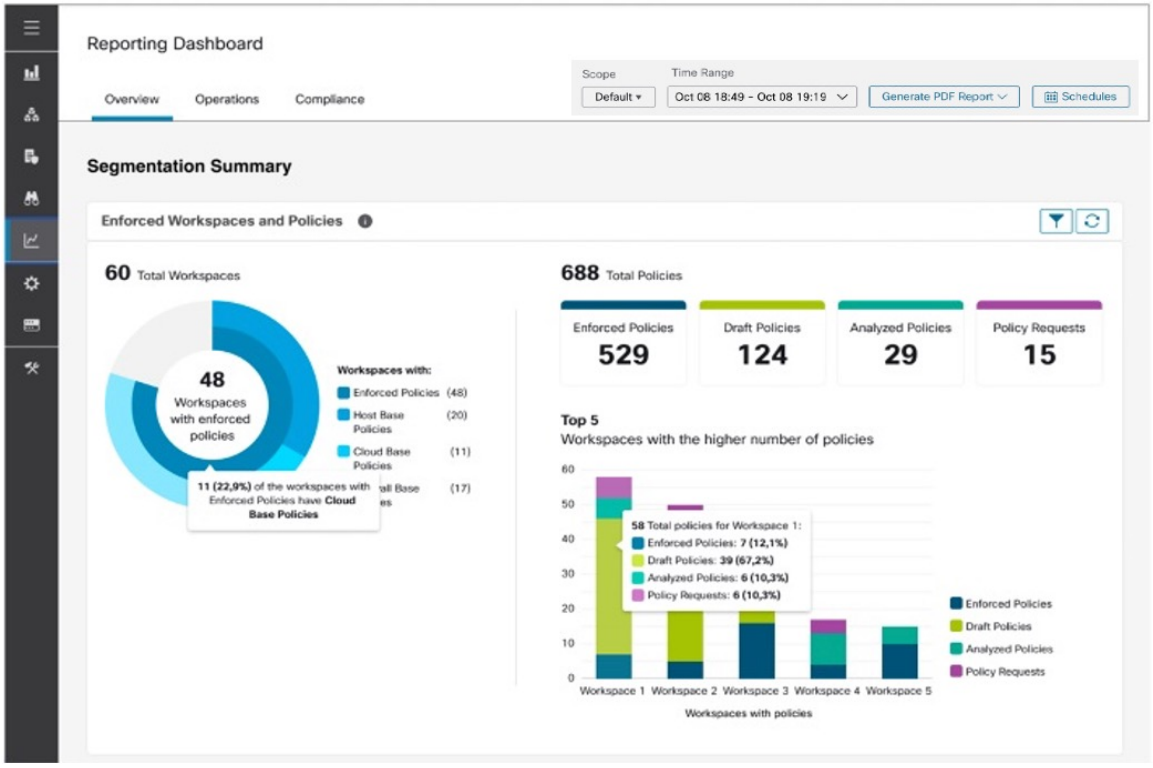
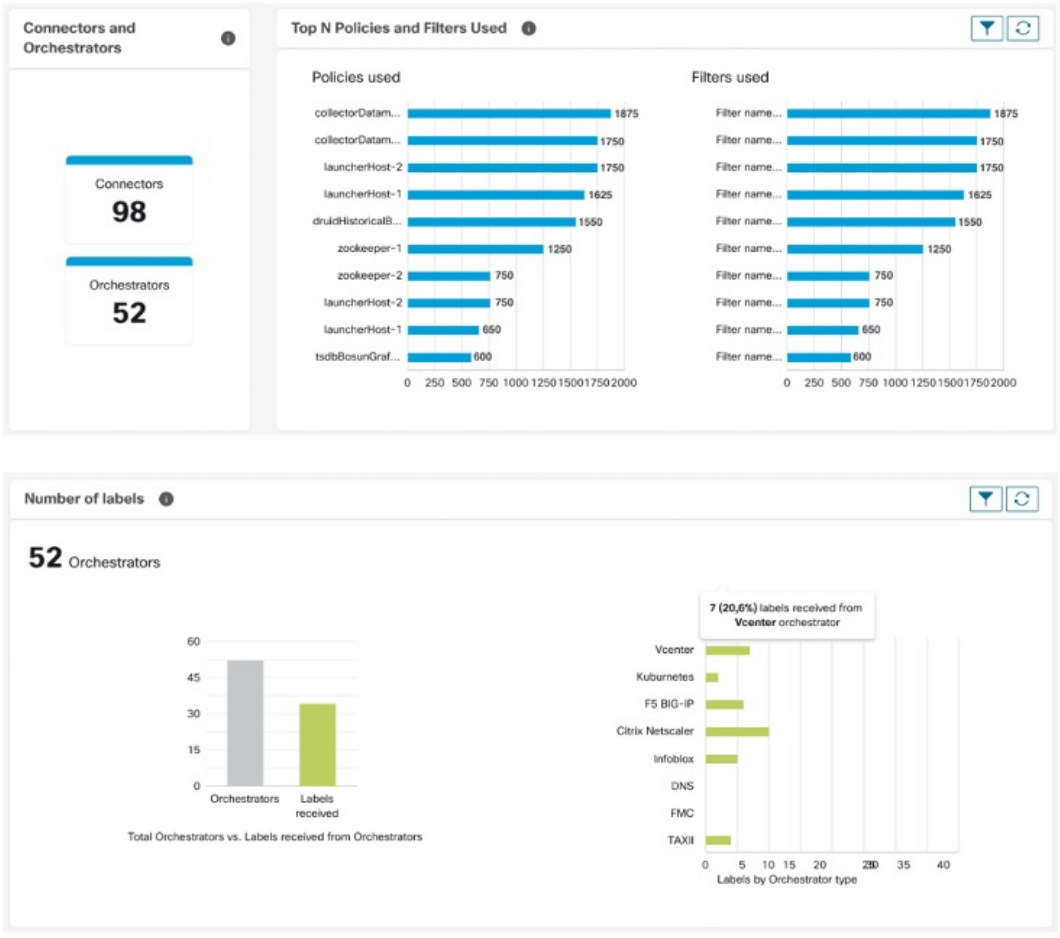


Figure 2: Connecteurs et orchestrateurs

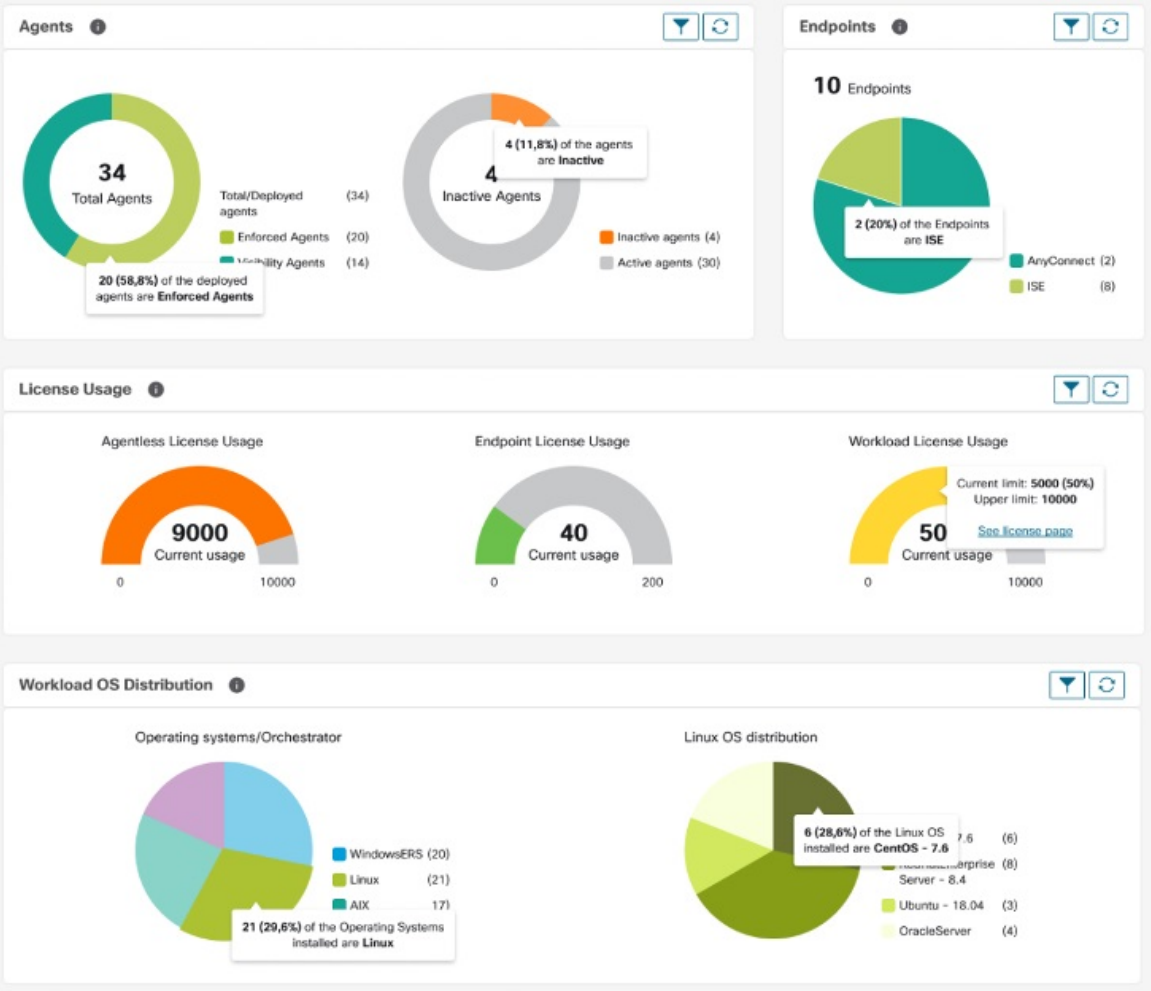


Résumé de la charge de travail

Le résumé de la charge de travail fournit les détails suivants sur les agents déployés sur un ou plusieurs serveurs et points terminaux de l'infrastructure :

- Les agents surveillent et recueillent des informations sur les flux du réseau.
- Les agents appliquent les politiques de sécurité avec les règles de pare-feu sur les hôtes installés.
- Les agents communiquent l'état de la charge de travail.
- Les agents reçoivent des mises à jour des politiques de sécurité.

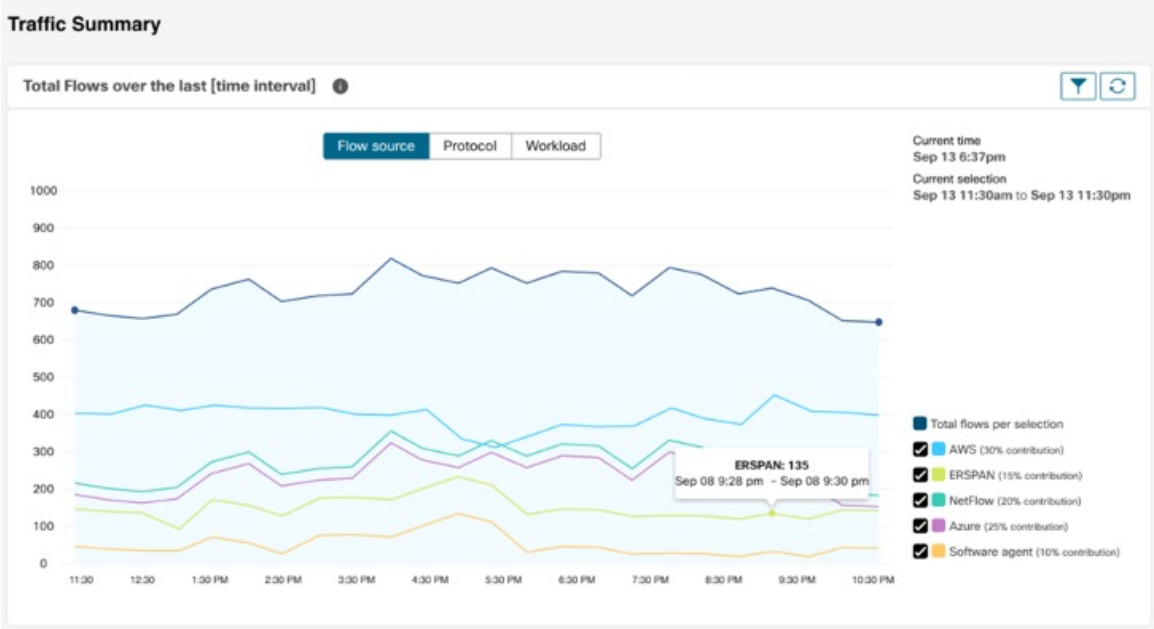
Figure 3: Résumé de la charge de travail



Résumé du trafic

Le résumé du trafic contient les observations de flux de chaque flux. Chaque observation de la source de flux suit le nombre de paquets, d'octets et d'autres mesures relatives aux flux.

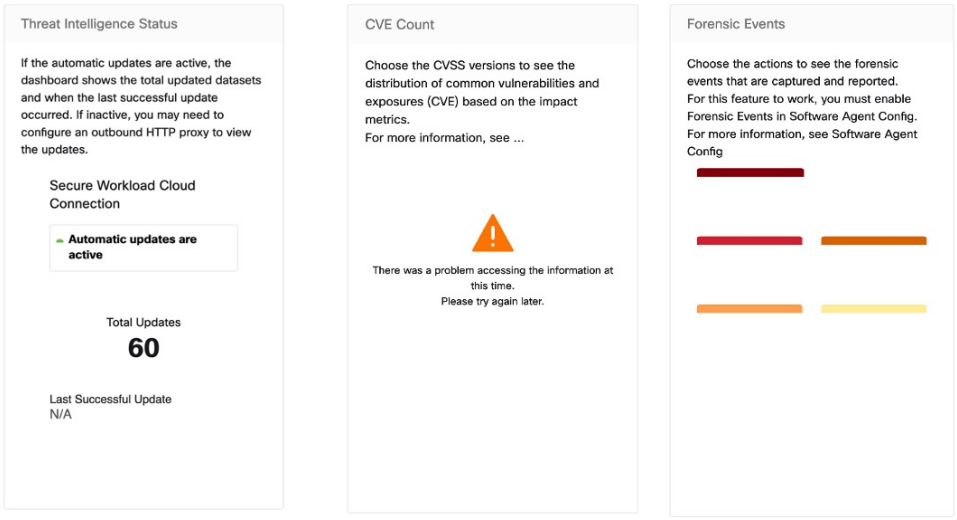
Figure 4: Résumé du trafic



Résumé de la sécurité

Le résumé de la sécurité fournit l'état des renseignements sur les menaces (la dernière fois que les mises à jour de l'état des renseignements sur les menaces ont été reçues est indiquée), le nombre de CVE et la distribution des événements criminalistiques.

Figure 5: Résumé de la sécurité

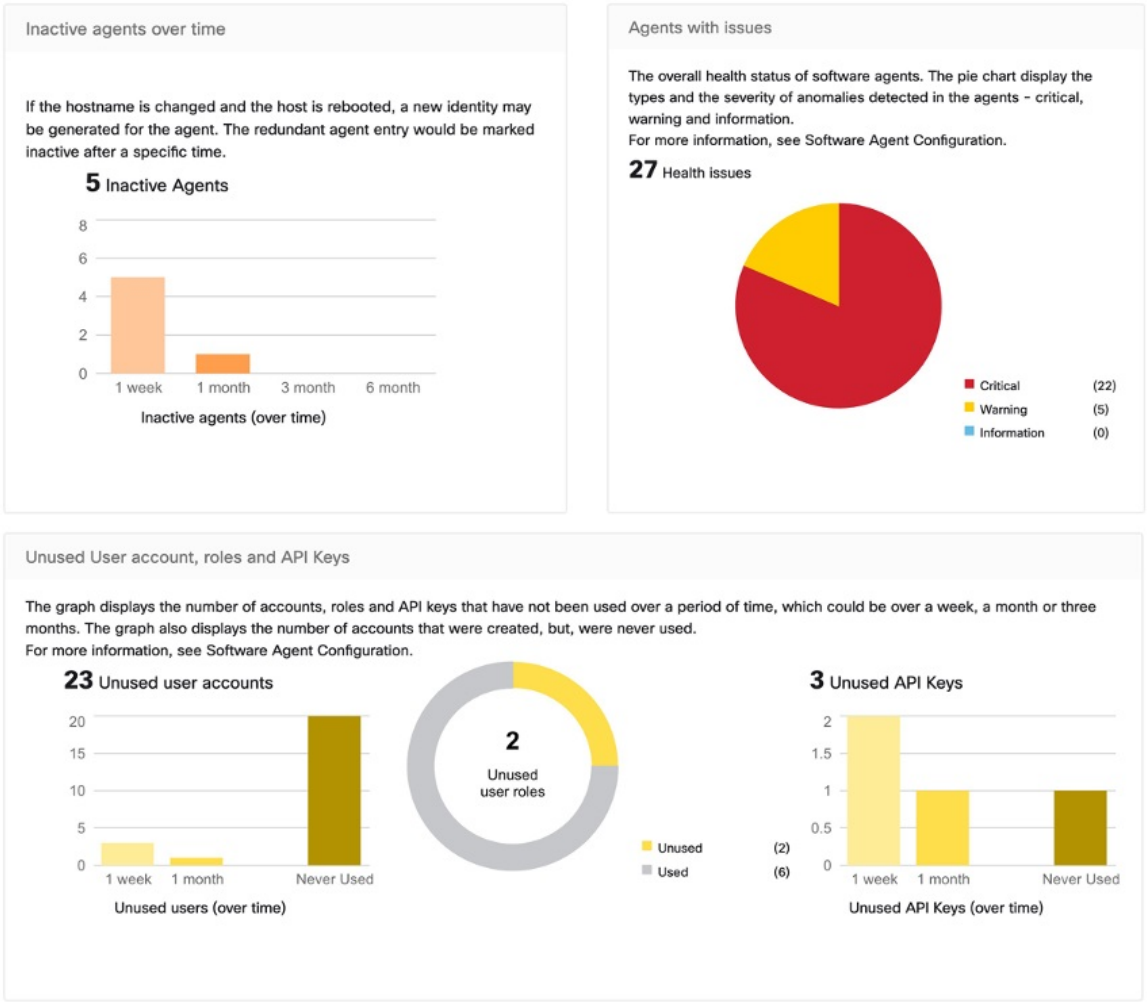


Operation (Opération)

Résumé de la charge de travail

Le résumé de la charge de travail fournit une vue du nombre total d'agents déployés sur un ou plusieurs serveurs et points terminaux du réseau. Les agents surveillent et recueillent des renseignements sur les flux de réseau, appliquent les politiques de sécurité à l'aide de règles de pare-feu sur les hôtes installés, communiquent l'état de la charge de travail et reçoivent les mises à jour des politiques de sécurité.

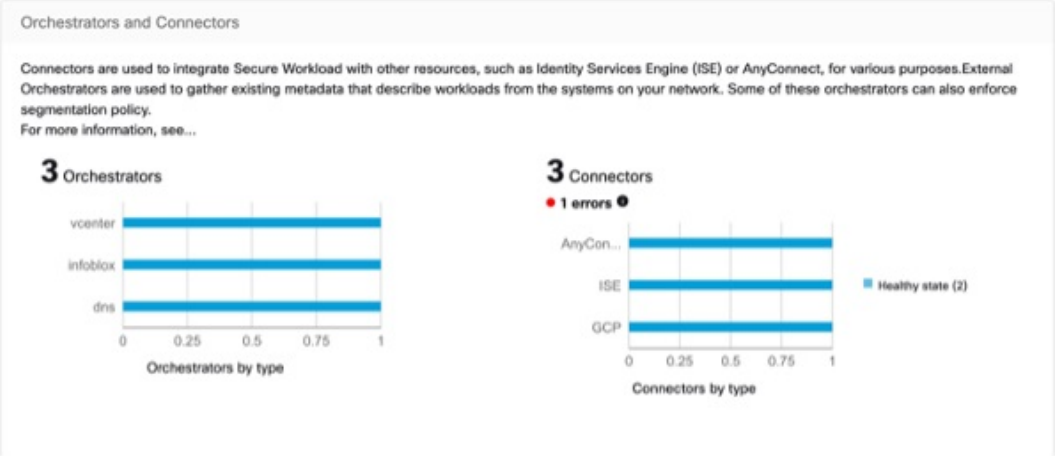
Figure 6: Résumé de la charge de travail



Résumé de la télémétrie

De nombreux connecteurs qui sont déployés sur l'appliance virtuelle recueillent la télémétrie à partir de divers points du réseau, ces connecteurs doivent être à l'écoute sur des ports spécifiques de l'appareil.appliance. Les connecteurs peuvent acquérir des journaux de flux si vous avez configuré ces derniers pour vos groupes de sécurité spécifiques. Vous pouvez également utiliser les données de télémétrie pour la génération de politiques de visualisation et de segmentation.

Figure 7: Résumé de la télémétrie



Résumé de la grappe

Les administrateurs de site peuvent accéder à la page d'état de la grappe, mais les actions ne peuvent être effectuées que par les utilisateurs du service d'assistance à la clientèle. Il indique l'état de tous les serveurs physiques dans le châssis (rack) Cisco Secure Workload.

La durée de traitement et de conservation des grappes fait référence à la durée pendant laquelle les données sont stockées et traitées dans une grappe. Les durées de traitement et de conservation spécifiques dépendent des exigences de la charge de travail et des politiques de l'organisation.

Il est important de prendre en compte les exigences de temps de traitement lors de la configuration de la grappe, car cela peut avoir une incidence sur la capacité de stockage et la puissance de traitement nécessaires pour répondre aux besoins de la charge de travail.

La durée de conservation fait référence à la durée pendant laquelle les données sont conservées dans une grappe. Pour certaines charges de travail, les données peuvent devoir être conservées à des fins réglementaires ou de conformité, tandis que pour d'autres, elles peuvent être supprimées après avoir été traitées. Il est important d'établir des politiques de rétention pour la charge de travail afin de garantir que les données sont conservées pendant la durée appropriée, puis supprimées de manière sécurisée pour empêcher tout accès non autorisé.

Figure 8: Résumé de la grappe

Résumé de la segmentation

La segmentation ou les espaces de travail d'application sont les éléments constitutifs de la découverte, de l'application et de la gestion des politiques et de leur mise en application au sein de la grappe. Le résumé de segmentation saisit les détails de configuration pour chacun des espaces de travail d'application mis en œuvre, le n° des espaces de travail avec et sans application, des politiques qui ont été activées ou désactivées, des espaces de travail qui ont des politiques à jour ou non synchronisées, avec ou sans politiques en cours d'élaboration.

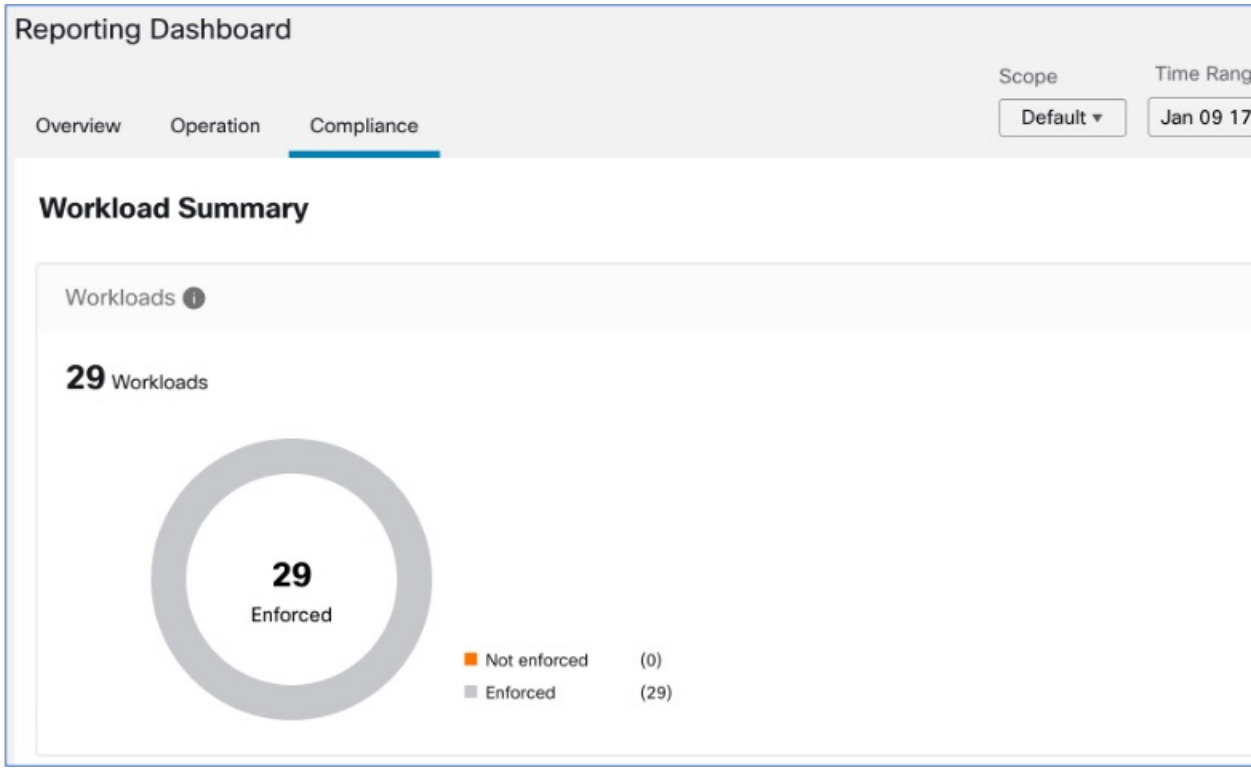
Figure 9: Résumé de la segmentation

Conformité

Résumé de la charge de travail

Le résumé de la charge de travail fournit une vue du nombre total d'agents déployés sur un ou plusieurs serveurs et points terminaux de l'infrastructure. Les agents surveillent et recueillent des renseignements sur les flux de réseau, appliquent les politiques de sécurité à l'aide de règles de pare-feu sur les hôtes installés, communiquent l'état de la charge de travail et reçoivent les mises à jour des politiques de sécurité.

Figure 10: Résumé de la charge de travail



Résumé de la sécurité

Configurez vos événements criminalistiques; une fois configurées, toutes les tactiques sont affichées sans aucune règle, avec un nombre de 0. Sélectionnez une ou plusieurs règles criminalistiques pour effectuer la sélection au niveau de la tactique. Sélectionner une tactique sélectionne toutes les règles qu'elle contient. Les règles par défaut de la fonction MITRE ATT&CK sont fournies pour envoyer des alertes techniques à partir du cadre de la fonction MITRE ATT&CK.

Figure 11: Résumé de la sécurité

Espaces de travail avec des CVE

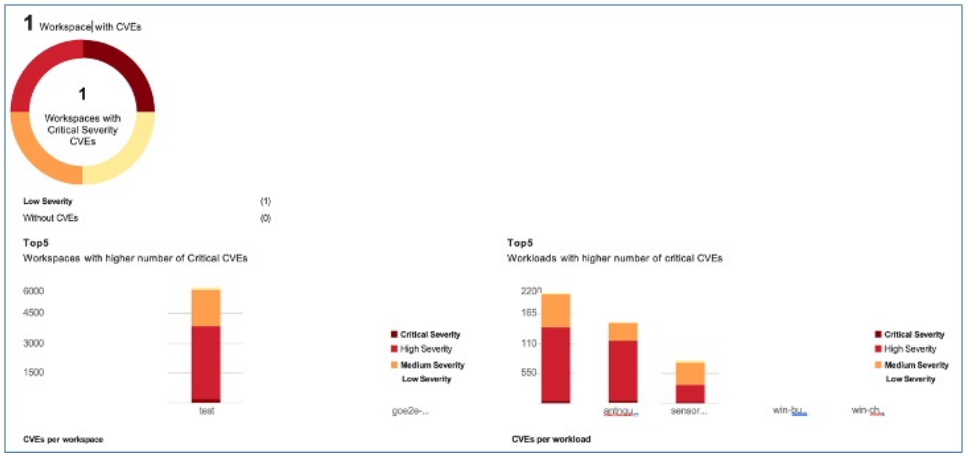
En fonction de la portée sélectionnée et du système de notation (v2 ou v3), le décompte des vulnérabilités et expositions communes (CVE) met en évidence les vulnérabilités (classées en fonction des notes) sur les

charges de travail dans les portées sélectionnées. Consultez la répartition des espaces de travail et des charges de travail avec le plus grand nombre de CVE critiques.

Les paquets logiciels d'une charge de travail pourraient être associés à des vulnérabilités connues (CVE). Le système Common Vulnerability Scoring System (CVSS) est utilisé pour évaluer l'impact d'une CVE. Une CVE peut avoir une note CVSS v2 et CVSS v3. Pour calculer la note de vulnérabilité, prenez en compte CVSS v3 s'il est disponible, sinon CVSS v2 est pris en compte.

La note de vulnérabilité pour une charge de travail est dérivée des notes des logiciels vulnérables détectés sur cette charge de travail. La note de vulnérabilité de la charge de travail est calculée sur la base des notes CVSS et des données du fournisseur. L'équipe de recherche en sécurité peut procéder à des ajustements lorsque les données sont manquantes ou inexactes. Plus la gravité de la vulnérabilité la plus grave est élevée, plus la note est faible.

Figure 12: Espaces de travail avec des CVE



À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.