netwrix

Top 5 des incidents d’équipements réseau qui doivent pouvoir être détectés

Table des matières

#1: Modifications de configuration 3

#2: Échecs répétés de tentatives de connexion 4

#3: Tentatives de connexion VPN 5

#4: Dysfonctionnements matériels 6

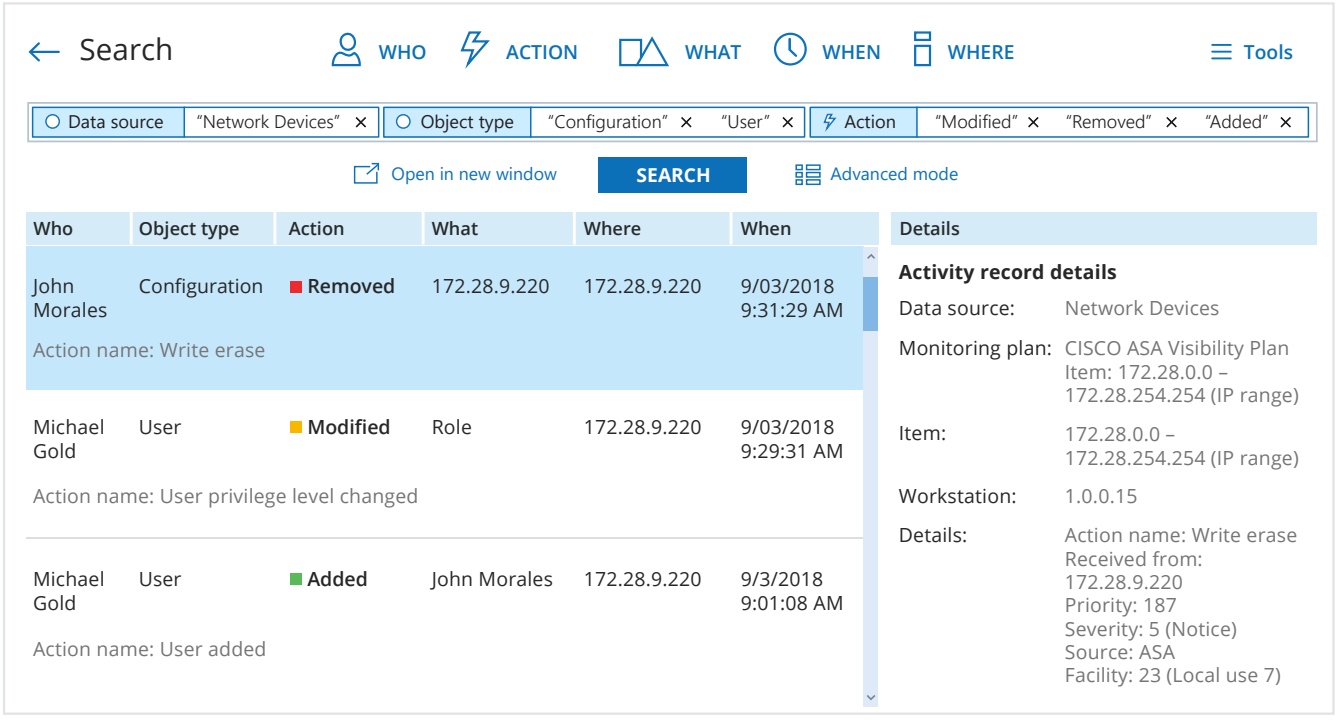
#5: Scan des menaces 7

À propos de Netwrix Corporation 8

#1: Modifications de configuration

Vous devez être en permanence au courant de tous les changements apportés à la configuration de vos périphériques réseau, tels que leurs protocoles, leurs ports et leurs limites de connexion, car toute modification non autorisée ou inappropriée peut entraîner des problèmes de connectivité, y compris l'inaccessibilité à tout le réseau. Vous devez également savoir rapidement si quelqu'un modifie une GPO (Group Policy) ou crée un nouvel utilisateur, car cela pourrait être le signe d'une attaque de la part d'un employé ou d'un abus de privilège. Netwrix Auditor suit les changements de configuration réussis et ceux qui ont échoué, vous permettant ainsi de répondre facilement à des questions comme celles-ci :

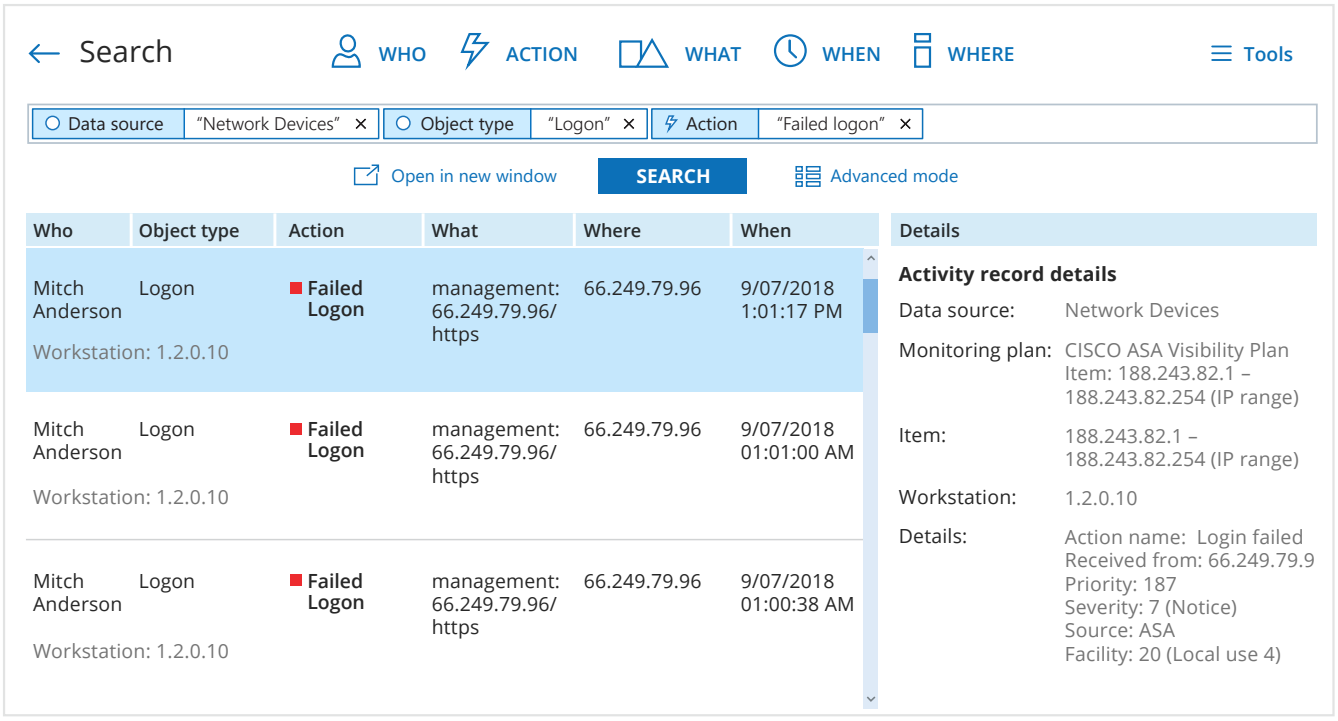
- Qui a effacé la configuration d'un périphérique particulier du réseau ?
- Quels paramètres spécifiques ont été modifiés dans le pare-feu ?
- A partir de quelle adresse IP la commande de rechargement a-t-elle été lancée ?
- Quand le mot de passe du routeur a-t-il été réinitialisé ?



#2: Échecs répétés de tentatives de connexion

Il est essentiel de surveiller les connexions réussies aux périphériques réseau pour s'assurer qu'elles sont entièrement autorisées. Cependant, vous devez également surveiller les tentatives de connexion multiples qui ont échoué, ce qui pourrait indiquer que quelqu'un essaie de forcer les informations d'identification administratives. Si des pirates accèdent à votre périphérique réseau, ils pourront prendre le contrôle de votre trafic réseau et voler des données sensibles. Netwrix Auditor suit à la fois les tentatives de connexion réussies et celles qui ont échoué, vous aidant à détecter rapidement les attaques potentielles en force brute et à répondre rapidement à des questions comme celles-ci :

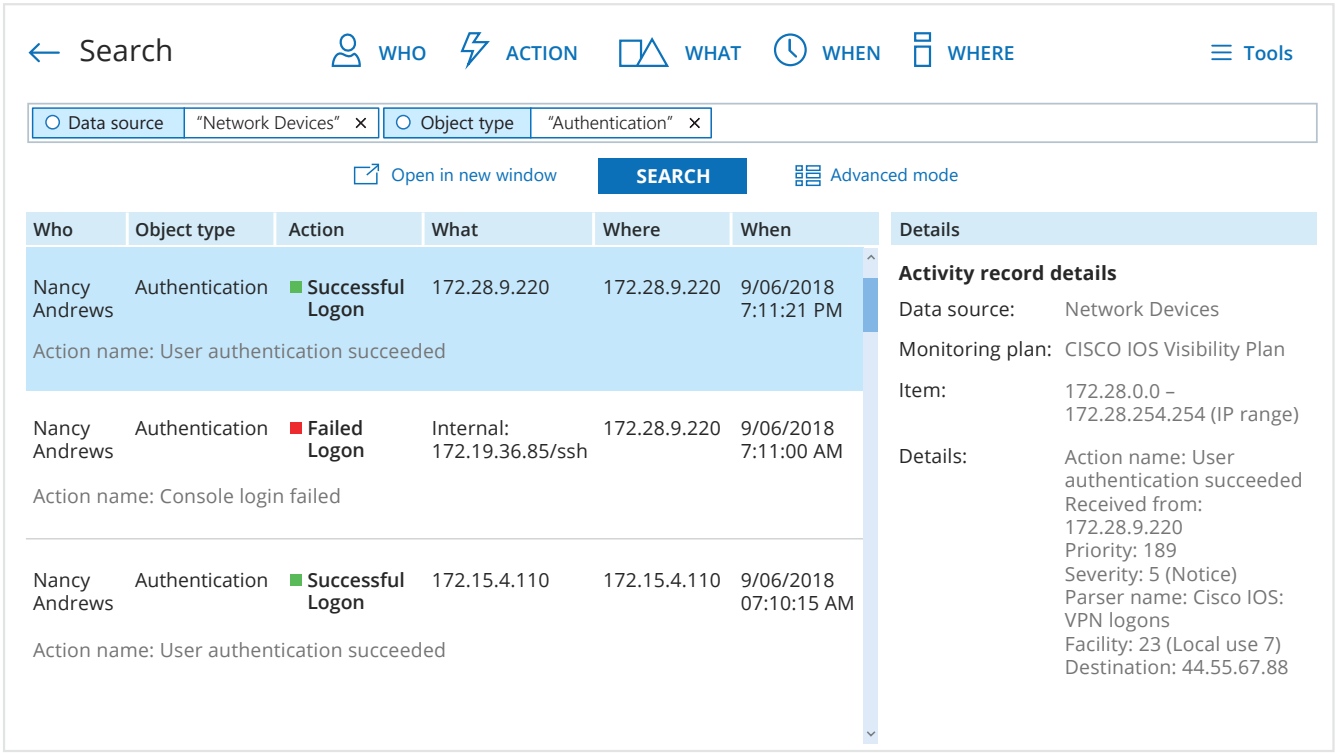
- Qui a dépassé le nombre maximum d'échecs d'authentification consécutifs ?
- Quelle était la cause de chaque échec de connexion ?
- A partir de quelle adresse IP la connexion a-t-elle été établie ?
- Combien de connexions ont été tentées ?
- Quand chaque demande d'authentification échouée a-t-elle été faite ?
- Sur quel appareil l'utilisateur essayait-il de se connecter ?



#3: Tentatives de connexion VPN

Les administrateurs ont rarement besoin de se connecter aux périphériques réseau à distance, il est donc important de garder une trace de chaque tentative de connexion VPN. De plus, même un appareil autorisé avec une connexion sécurisée au réseau de l'entreprise peut être piraté et utilisé pour accéder à des fichiers sensibles. Netwrix Auditor vous aide à surveiller les tentatives d'accès VPN réussies ou non pour vous connecter à vos périphériques réseau et répondre à des questions telles que les suivantes :

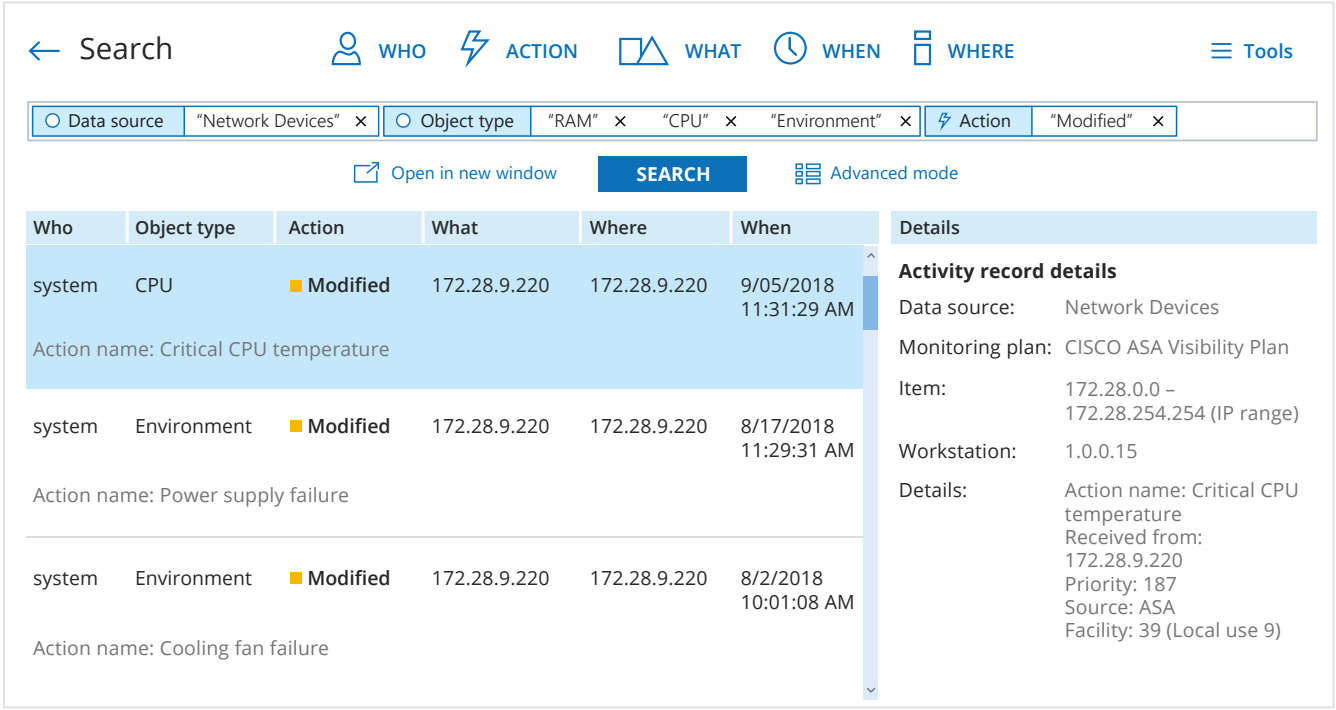
- Qui a essayé d'accéder aux périphériques réseau via un VPN ?
- A partir de quelle adresse IP la tentative d'authentification a-t-elle été faite ?
- Quelle était la cause de chaque échec de connexion VPN ?
- Quand chaque tentative de connexion VPN a-t-elle été initiée ?
- Sur quel périphérique l'utilisateur essayait-il de se connecter ?



#4: Dysfonctionnements matériels

En plus de suivre les modifications apportées à la configuration de vos périphériques réseau, vous devez également surveiller de près l'état de votre matériel. Si un périphérique réseau rencontre des conditions d'environnement ou d'alimentation qui violent ses spécifications, il peut surchauffer, subir des pannes de ventilation ou perdre de l'énergie, ce qui entraîne une sous-performance ou même l'arrêt complet de votre réseau. Netwrix Auditor surveille et alerte les défaillances matérielles critiques et vous aide à répondre à des questions comme celles-ci :

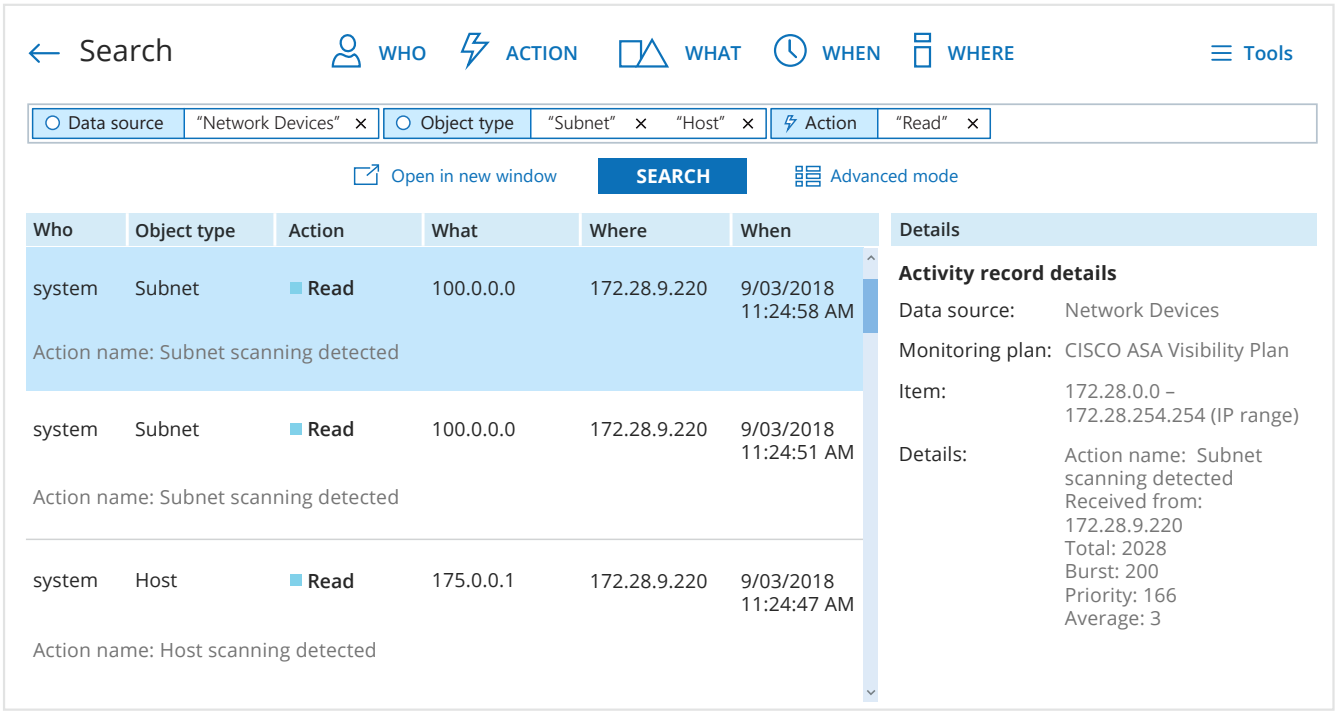
- Quelles actions se sont déroulées avant l'arrêt du périphérique réseau ?
- Quelle partie du périphérique réseau a été endommagée ?
- Quand la température a-t-elle atteint le niveau critique ?



#5: Scan des menaces

L'analyse de sous-réseau et l'analyse d'hôte ne sont pas des processus intrinsèquement hostiles pour connaître la structure et le comportement d'un réseau, mais les attaquants les utilisent souvent pour effectuer une reconnaissance avant d'essayer d'ouvrir une brèche dans un réseau et de voler des données sensibles. Netwrix Auditor suit ces actions et vous aide à enquêter sur les incidents potentiels en répondant à des questions telles que :

- Quels hôtes et sous-réseaux ont été scannés ?
- Quand chaque tentative de scan a-t-elle été effectuée ?
- A partir de quelle adresse IP l'analyse a-t-elle été lancée ?
- Combien de tentatives d'analyse ont été effectuées à partir de chaque adresse IP ?



À propos de Netwrix Corporation

Netwrix Corporation est une société éditrice de logiciels qui se consacre exclusivement à fournir aux équipes de sécurité informatique et d'exploitation une visibilité omniprésente sur le comportement des utilisateurs, les configurations système et la sensibilité des données dans les infrastructures informatiques hybrides afin de protéger les données, quel que soit leur emplacement. Plus de 9 000 entreprises dans le monde font confiance à Netwrix pour détecter et atténuer de manière proactive les menaces à la sécurité des données, passer avec succès les audits de conformité avec moins d'efforts et de dépenses, et augmenter la productivité de leurs équipes informatiques. Fondée en 2006, Netwrix a remporté plus de 140 prix de l'industrie et a été nommée à la fois au Prix de l'industrie de l'assurance de l'Inc. 5000 et dans la liste Deloitte Technology Fast 500, des entreprises qui connaissent la croissance la plus rapide aux États-Unis.

Netwrix Auditor est une plate-forme de visibilité pour l'analyse du comportement des utilisateurs et l'atténuation des risques qui permet de contrôler les modifications, les configurations et les accès dans les environnements informatiques hybrides pour protéger les données, où qu'elles se trouvent. La plate-forme fournit des renseignements de sécurité pour identifier les failles de sécurité, détecter les anomalies dans le comportement des utilisateurs et analyser les modèles de menaces à temps pour prévenir les dommages réels.

Netwrix Auditor comporte des applications pour Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware, Windows Server et Network devices. Dotée d'une API RESTful et d'un enregistrement vidéo de l'activité des utilisateurs, la plate-forme offre une visibilité et un contrôle unifiés sur l'ensemble de vos systèmes informatiques sur site et dans le Cloud.
Pour plus d'informations allez sur www.netwrix.fr.

Mise en œuvre sur site

Téléchargez un essai gratuit de 20 jours

netwrix.com/go/freetrial

Application Virtuelle

Télécharger l'image de notre machine virtuelle

netwrix.com/go/appliance

Mise en œuvre dans le Cloud

Mettez Netwrix Auditor en œuvre dans le Cloud

netwrix.com/go/cloud

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 | +33 9 75 18 11 19 **EMEA:** +44 (0) 203-588-3023
netwrix.com/social