
VARONIS
DATALERT SUITE

VARONIS DATALERT SUITE

Détectez les activités suspectes sur vos systèmes de fichiers et de messagerie et donnez l'alerte

DATALERT :

- Surveillez les ressources critiques pour détecter les activités suspectes et les comportements inhabituels
- Bénéficiez d'un contrôle des événements multiplateformes sur Windows, UNIX/Linux, NAS, Active Directory, SharePoint ou Exchange
- Déclenchez des alertes sur plusieurs plateformes, afin de vous aider à détecter les atteintes à la sécurité potentielles, les mauvaises configurations et d'autres problèmes encore
- Détectez les événements critiques et les ressources compromises
- Réduisez le temps nécessaire à l'identification et à l'évaluation d'un problème réel

DATALERT ANALYTICS :

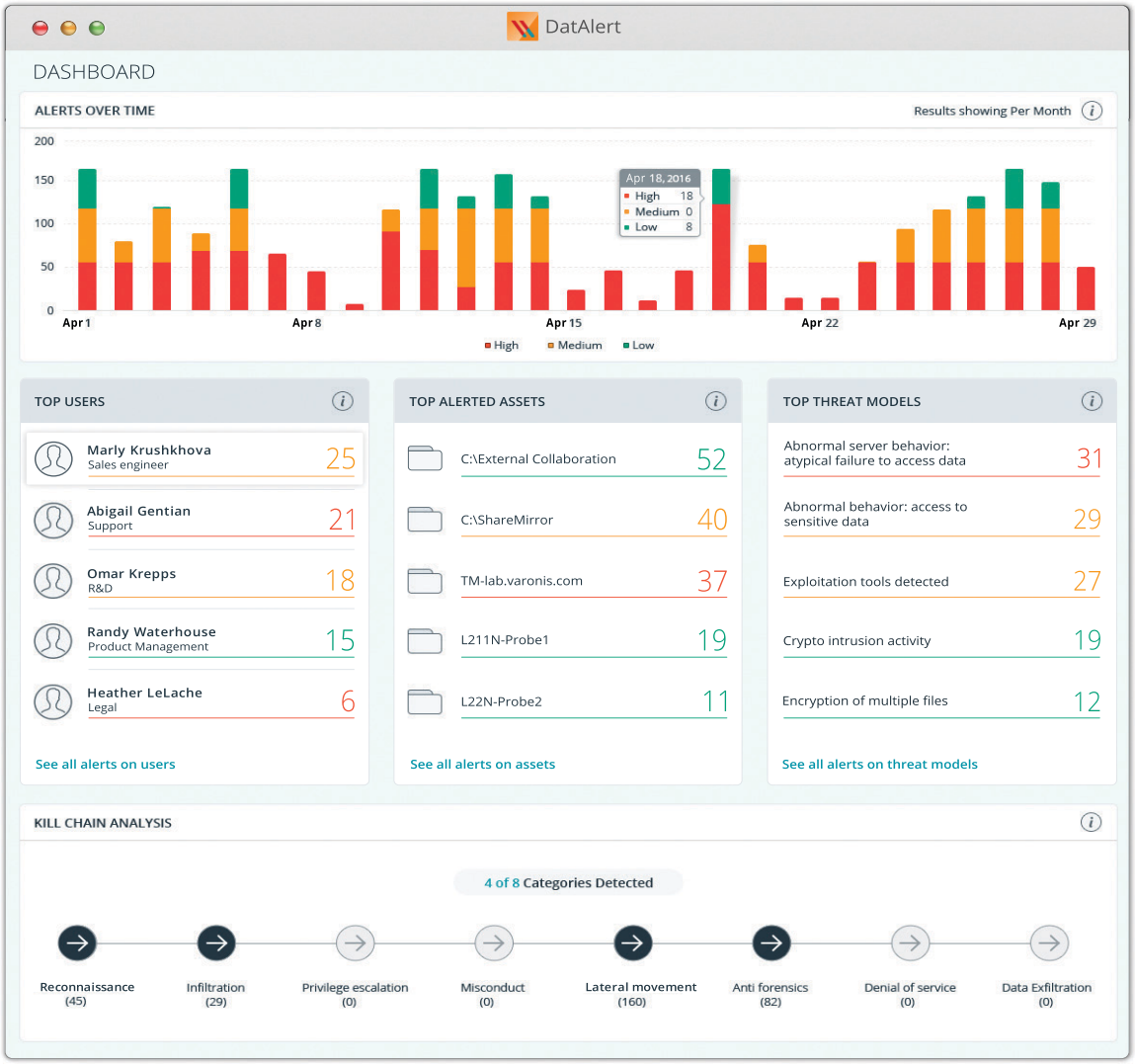
- Automatisez la détection des menaces grâce à des modèles de menace prédictifs élaborés d'après une analyse des données sophistiquée, le comportement des utilisateurs et l'apprentissage machine
- Identifiez les rôles des utilisateurs et des comptes de service, puis établissez une référence définissant la manière dont ils utilisent les systèmes de fichiers et de messagerie et interagissent avec Active Directory
- Obtenez un éclairage significatif sur les modèles relatifs aux utilisateurs et aux données, les risques de sécurité et les liens sociaux
- Défendez-vous contre les menaces internes, les rançongiciels et les atteintes à la sécurité potentielles

VISUALISEZ, INTERPRETEZ ET ANALYSEZ VOS DONNEES :

- Utilisez les tableaux de bord Web de DatAlert pour noter, trier, analyser et hiérarchiser les alertes, puis prendre les mesures nécessaires pour résoudre les incidents
- Configurez les critères et les résultats des alertes selon vos besoins
- Déclenchez des actions personnalisées avec exécution de commande en ligne
- Bénéficiez d'une intégration aisée avec les solutions SIEM et d'administration réseau

LE LABORATOIRE DE RECHERCHE SUR LE COMPORTEMENT DE VARONIS :

- Une équipe dédiée d'experts de la sécurité et de scientifiques spécialistes des données de Varonis introduit en permanence de nouveaux modèles de menace basés sur le comportement
- Restez informé sur les derniers problèmes en matière de sécurité, les menaces avancées persistantes (APT), les menaces internes, et les moyens de défense



CONTRÔLEZ, ANALYSEZ, DETECTEZ

- Comportement de rançongiciel
- Activité inhabituelle des fichiers
- Activité inhabituelle des boîtes de messagerie et des e-mails
- Accès à des données sensibles
- Tentatives d'accès non autorisé
- Activité de cryptage inhabituelle
- Analyse systématique des données inactives et sensibles
- Accès inhabituel aux fichiers système
- Accès non autorisé aux données
- Activité de cryptage inhabituelle
- Mauvaises configurations
- Intrusions dans le système
- Escalade de privilèges non autorisée
- Comportements de suppression massive
- Comportements de verrouillage anormaux
- Tentatives visant à endommager et détruire des fichiers opérationnels
- Outils d'exploitation
- Modification des adhésions
- Modification des GPO critiques
- Modifications apportées à des fichiers et unités critiques
- Activités suspectes liées aux accès
- Modification des permissions
- Attaques en force brute
- Tentatives d'exfiltration des données