Keelback Host

Solution de forensic d'entreprise

Description succincte :
Solution de forensic de masse sur tout ou partie du parc informatique de l'entreprise, afin de déterminer la présence d'une attaque sophistiquée sur le réseau informatique du client par analyse comparative.

Bénéfices client :
- Gain de temps: forensic de masse simultané sur des milliers de postes de travail
- Processus contrôlé : le client effectue lui-même le déploiement de l'agent, et garde un contrôle total sur la collection de métadonnées et leur transmission pour analyse.
- Efficacité et transparence : Keelback Host est un agent non résident, non intrusif, autonome et transparent pour l'utilisateur final. Le traitement des informations collectées est effectué hors ligne, garantissant ainsi un impact nul sur la productivité des utilisateurs.

Familles de services associés :
- Advanced Security Monitoring
- Advanced Incident Response

AIRBUS

Description de la solution

Description détaillée	**Détection de déviations :** • Plutôt que d'utiliser une base de signatures exigeant une mise à jour régulière, l'analyse des métadonnées collectées est effectuée par nos experts forensic utilisant nos outils d'analyse comparative. Cette méthode permet de détecter les menaces inconnues de type 0-day ou les attaques ciblées. **Agent personnalisé :** • Un agent non-résident dédié est généré pour chaque client selon ses besoins et ses contraintes. • La liste des métadonnées collectées et leur lieu de stockage sont également définis avec le client avant génération de l'agent. **Protection des données du client :** • Keelback Host est conçu pour ne collecter aucun fichier sur les machines cibles, mais uniquement les métadonnées ciblées pour analyse. • Le forensic de masse est opéré par les experts Airbus Defence and Space sur des machines dédiées, en zone restreinte ou sur le site du client. • L'analyse est opérée hors ligne, assurant ainsi une isolation complète des métadonnées du client. • Une fois l'analyse terminée, les métadonnées sont supprimées selon un processus agréé avec le client.
Caractéristiques techniques	**Systèmes d'exploitation :** • Windows XP, Vista, 7, 8 • Windows server 2003, 2008 R2, 2012 **Compatibilité :** • Compatible avec les solutions de management IT les plus courantes (SCCM, IBM Tivoli, etc…) • Compatible avec les antivirus et systèmes de détection les plus courants (Kaspersky, McAfee, Symantec, ZoneCentral, Stormshield) **Performances d'analyse :** • Forensic de masse jusqu'à plus de 50 000 machines • Environ 5MB de métadonnées collectées par poste de travail • Temps de collecte de métadonnées <20 minutes
Offres disponibles	• En mode service • Exemple de performances d'analyse : - 5 jours pour 1000 machines - 15 jours pour 10000 machines - 30 jours pour 50000 machines

AIRBUS

Document non contractuel.
Sous réserve de modification sans préavis. © 2017 Airbus CyberSecurity. Airbus, son logo et le nom de ses produits sont des marques déposées. Tous droits réservés. // 0917 F 0876

Airbus CyberSecurity
Metapole 1, boulevard Jean Moulin / CS 40001 / 78996 Elancourt Cedex / France
Willy-Messerschmitt-Str. 1 / 82024 Taufkirchen / Germany
Quadrant House / Celtic Springs / Coedkernew / South Wales NP10 8FZ / United Kingdom
Etihad Towers T3 / Corniche Road, 19th floor / P.O.Box: 72186 / Abu Dhabi / United Arab Emirates
www.airbus-cyber-security.com / contact.cybersecurity@airbus.com