APACHE METRON

Présentation de la solution de cybersécurité d'Hortonworks

UN LIVRE BLANC DE HORTONWORKS
MARS 2016

Contentu

Présentation

Les logiciels malveillants et les cyberattaques ne ciblent pas les systèmes informatiques, ce sont les gens qui le font. Ces individus exploitent les multiples vecteurs d'attaque comme les failles physiques, techniques et inhérentes aux réseaux sociaux, pour parvenir à leurs fins avec le moins d'effort et de risque possible ; si jamais ils sont stoppés par un outil basé sur les signatures, ils changent de méthode.

Pour détecter et se défendre contre les attaques ciblées, il est indispensable d'abandonner les systèmes basés sur les règles ou les signatures au profit d'une solution analytique intégrée permettant de créer rapidement de nouveaux modèles de détection. Cette solution doit permettre, d'une part, le déploiement de nombreuses plateformes analytiques distribuées au sein d'une agence gouvernementale donnée pour assurer une bonne rapidité de détection et d'intervention en local, et d'autre part, l'intégration croisée des plateformes analytiques pour pouvoir diffuser des informations sur les attaques en toute sécurité entre les organes internes. Ainsi, cela permet de voir l'ensemble des attaques et des interventions, à l'échelle de l'agence, afin de coordonner rapidement les ressources nécessaires pour intervenir.

Solution

Apache Metron est une solution logicielle de big data open source dédiée à la surveillance et aux analyses de sécurité. Elle fournit un traitement analytique en temps réel à des taux de rapidité extrêmement élevés ainsi que le stockage à long terme de toutes les données générées automatiquement dans votre datacentre. Apache Metron offre également un portail de surveillance centralisé permettant aux agents de voir les alertes en contexte avec des informations sur les attaques et d'autres enrichissements.

La solution de cybersécurité d'Hortonworks dispose des fonctionnalités suivantes, indispensables pour voir les attaques à l'échelle de l'agence en un seul endroit.

1 Une méthode sécurisée, avec protection complète des données, pour collecter les données à partir d'emplacements géographiquement séparés et les transmettre à travers des liaisons réseau non fiables en toute sécurité en s'appuyant sur Apache NiFi.

2 Un framework de cybersécurité ouvert et extensible dédié à la modélisation analytique et à l'apprentissage automatique de pointe, dans le but de détecter les attaques zero day dès qu'elles se produisent au moyen d'Apache Metron. Cela offre la possibilité de connecter des modèles analytiques sécurisés au framework à des fins de renseignement.

3 Une plateforme analytique ouverte, protégée au repos comme en transit via la gouvernance de sécurité reposant sur la politique d'Apache Atlas et via les fonctionnalités intégrées d'authentification, d'autorisation, d'audit et de chiffrage d'Apache Ranger.

4 Une plateforme ouverte permettant d'intégrer des outils existants et la fonctionnalité de visualisation, mais aussi la fonctionnalité de visualisation complète fournie par Hortonworks Data Platform (HDP®).

Apache Metron permet de compléter, et potentiellement remplacer, les outils hérités coûteux servant dans les centres d'opérations de sécurité des entreprises, en utilisant les outils évolutifs et rentables conçus sur Apache Hadoop®. Étant donné qu'Apache Metron est open source, les améliorations apportées par la communauté sont disponibles pour tous les utilisateurs de la solution Apache Metron. Apache Metron permet aux agences gouvernementales de collaborer directement et indirectement avec l'industrie. Hortonworks peut faciliter la participation des agences à Apache Metron à quelque niveau que ce soit. Sur ce type d'architecture sécurisée, la collaboration, les directives et les informations gouvernementales sont extrêmement souhaitées.

Architecture

Apache Metron intègre un éventail de technologies big data open source afin de fournir un outil centralisé dédié à la surveillance et aux analyses de sécurité. Apache Metron est doté de fonctionnalités d'agrégation des journaux, de capture et d'indexation complète des paquets, de stockage, d'analyses comportementales avancées et d'enrichissement des données, et applique les informations les plus récentes en matière de menaces à sa télémétrie de sécurité, au sein d'une plateforme unique

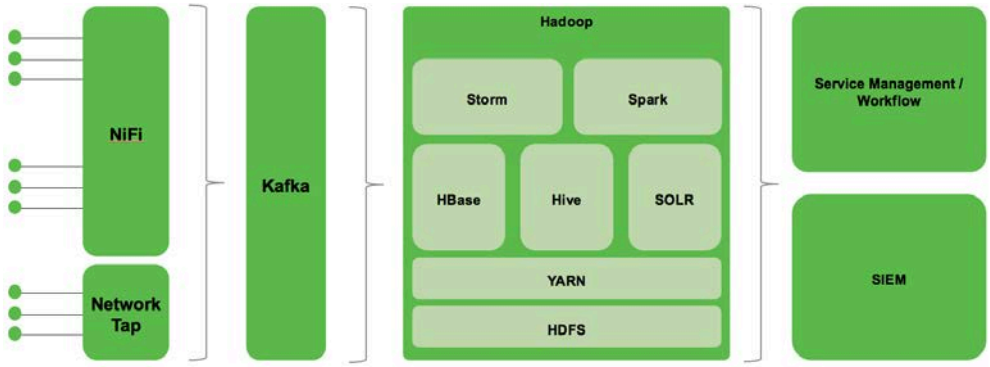

Figure 1 : Architecture globale d'Apache Metron

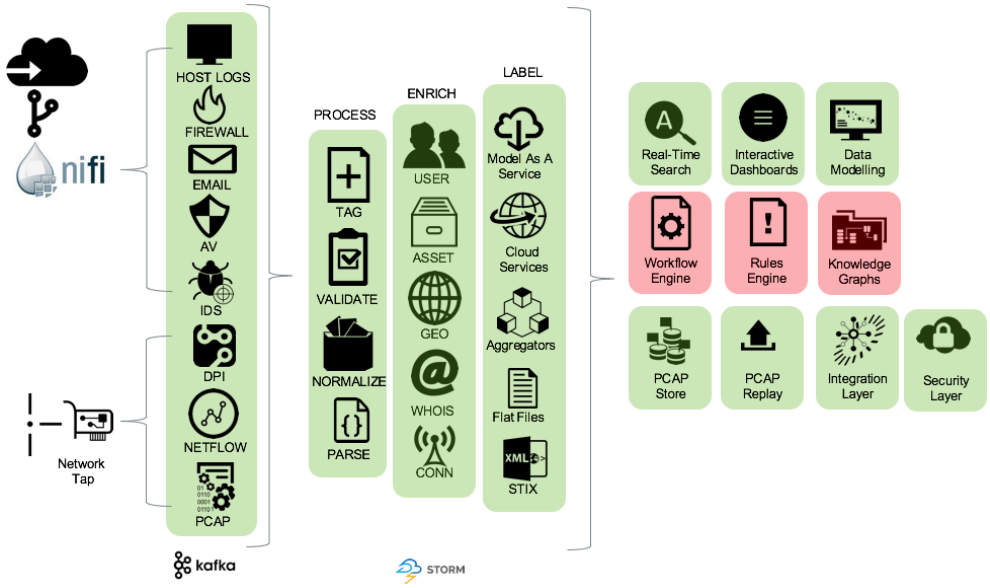

Figure 2 : Apache Metron est déployé sur un environnement d'entreprise afin d'ingérer et de traiter toutes données informatiques en temps réel, et permet aux entreprises d'interagir avec les données présentes sur la plateforme d'Apache Metron ou d'intégrer leurs propres ressources pour un traitement plus complet

Fonctionnalités principales

ÉLÉMENT	FONCTION
Capture de paquets haute fidélité (PCAP)	Apache Metron offre des fonctionnalités intégrées pour ingérer et traiter directement les données PCAP à partir des réseaux qui utilisent une dérivation passive. Apache Metron s'appuie sur Apache HBase™ pour stocker les données PCAP brutes à grande échelle, offrant ainsi un apprentissage plus poussé des immenses ensembles de données informatiques
Traitement de trains et par lots de données	Apache Metron est capable de traiter des données informatiques en passant par Apache Storm™ pour les flux de données en temps réel et par Apache Spark™ pour le traitement par lots de données en mémoire
Enrichissement des données et flux informatiques	Apache Metron est doté d'interfaces de programmation flexibles et extensibles pour ingérer et enrichir les données informatiques des clients à l'aide des flux CIF ainsi que d'autres flux d'enrichissement importants, puis obtenir une vue globale de l'analyse des données
Tableaux de bord et visualisation en temps réel	Apache Metron tire parti de plateformes de recherche open source pour déployer des index informatiques, puis stocker et visualiser en temps réel les flux informatiques traités par le framework d'Apache Metron. Sur Apache Metron, la visualisation fonctionne et peut être facilement étendue grâce à des tableaux de bord flexibles
Recherche interactive et analyse des données	Apache Metron permet d'effectuer des recherches en temps réel sur les données informatiques ingérées et traitées par lui-même, notamment les journaux PCAP, NetFlow, SysLog, et d'application

À propos d'Hortonworks

Hortonworks est l'entreprise la plus innovante du secteur. Elle crée, distribue et soutient des plateformes de données connectées et des applications de données modernes ouvertes et prêtes à l'emploi dans l'entreprise. Ces outils exploitent tous types de données (données au repos et en mouvement) pour vous fournir des informations utiles. Hortonworks se concentre sur la promotion de l'innovation au sein de communautés open source telles que Apache Hadoop, Apache NiFi et Apache Spark. Avec plus de 1 800 partenaires, Hortonworks fournit le savoir-faire, la formation et les services permettant aux clients de débloquer de la valeur transformationelle pour tous les secteurs d'activité de leur entreprise.

Contact

Pour en savoir plus, consultez
www.hortonworks.com

+1 408 675-0983
+1 855 8-HORTON
INTL: +44 (0) 20 3826 1405

HORTONWORKS