SIEM

Solution ELK qui comprend les outils Elasticsearch, Logstash et Kibana

---

1. Compréhension de Vos Besoins

Nous avons pris connaissance de vos exigences en matière de sécurité et de surveillance informatique, notamment la nécessité de détecter les menaces en temps réel, de gérer efficacement les logs et d'assurer la conformité réglementaire. Notre solution ELK Stack est conçue pour répondre à ces besoins en fournissant une plateforme intégrée de gestion des informations et des événements de sécurité.

2. Proposition de la Solution

ELK Stack, combinant Elasticsearch, Logstash et Kibana, offre une solution complète pour la collecte, l'analyse et la visualisation de données de logs en temps réel. Voici comment notre proposition répond à vos besoins spécifiques :

Elasticsearch :

Elasticsearch est un moteur de recherche et d'analyse de données open source, conçu pour stocker, rechercher et analyser de grands volumes de données rapidement et en temps réel. Il appartient à la suite Elastic, qui comprend également des produits tels que Kibana et Logstash.

Voici quelques points clés à propos d'Elasticsearch :

1. **Stockage des données :** Elasticsearch utilise une structure de données appelée "index" pour stocker les informations. Les données sont stockées de manière distribuée sur différents nœuds, ce qui permet une grande évolutivité et une haute disponibilité.

2. **Recherche :** Il est conçu pour effectuer des recherches complexes et rapides sur de grandes quantités de données. Il prend en charge des recherches en texte intégral, des requêtes booléennes, des filtres géographiques, etc.
3. **Analyse :** Elasticsearch offre des fonctionnalités d'analyse puissantes, telles que l'agrégation de données, permettant de générer des statistiques et des résumés sur les données. Cela facilite l'exploration et la visualisation des informations.
4. **Temps réel :** Il est particulièrement adapté pour les cas d'utilisation nécessitant des mises à jour en temps réel. Cela en fait un choix populaire pour les journaux d'application, les analyses de sécurité et d'autres applications nécessitant une réponse en temps réel.
5. **Extensibilité :** Elasticsearch peut être étendu avec des plugins pour prendre en charge diverses fonctionnalités et intégrations. Il est souvent utilisé en combinaison avec Kibana pour la visualisation des données et Logstash pour l'ingestion des données.
6. **Langage de requête :** Il utilise un langage de requête appelé Query DSL (Domain-Specific Language) qui permet aux utilisateurs de spécifier des critères de recherche de manière détaillée et flexible.
7. **Open Source :** Elasticsearch est distribué sous la licence Apache 2.0, ce qui signifie qu'il est libre d'utilisation, de modification et de distribution.

Elasticsearch est largement utilisé dans divers domaines, tels que la recherche sur le web, l'analyse des journaux, la surveillance des applications, la recherche en texte intégral, et plus encore. Il joue un rôle clé dans la gestion de données volumineuses et dans la fourniture de réponses rapides aux requêtes complexes.

Logstash :

1. **Collecte des logs :** Logstash prend en charge la collecte de logs à partir de diverses sources telles que des fichiers journaux, des flux réseau (syslog, SNMP, etc.), des bases de données, des API, et d'autres sources de données.
2. **Transformation des données :** Il permet de transformer les données collectées grâce à des filtres. Ces filtres peuvent être utilisés pour enrichir, nettoyer, et structurer les logs avant leur stockage ou leur transfert vers d'autres systèmes. Logstash utilise une syntaxe appelée "filter plugins" pour définir ces transformations.

3. **Parsing des logs :** Logstash facilite l'extraction de champs spécifiques des logs en utilisant des filtres prédéfinis ou personnalisés. Cela est particulièrement utile pour normaliser les données et les rendre compatibles avec des schémas prédéfinis.
4. **Formats de sortie multiples :** Une fois les données traitées, Logstash peut les envoyer vers différentes destinations, notamment Elasticsearch pour l'indexation et la recherche, mais aussi vers des systèmes de stockage tels que des bases de données, des entrepôts de données, des systèmes de files d'attente, etc.
5. **Extensibilité :** Logstash peut être étendu grâce à des plugins, ce qui permet d'ajouter des fonctionnalités supplémentaires en fonction des besoins spécifiques. Il existe une variété de plugins disponibles pour la collecte de logs à partir de sources spécifiques, ainsi que pour la transformation et l'acheminement des données.
6. **Pipeline de traitement :** Logstash utilise des pipelines de traitement qui définissent le flux de travail des données depuis la collecte jusqu'à la sortie. Chaque pipeline se compose de trois étapes principales : l'entrée (input), le filtre (filter), et la sortie (output).
7. **Gestion des erreurs :** Logstash offre des mécanismes de gestion des erreurs et de récupération en cas de problèmes lors de la collecte, du traitement ou de l'envoi des logs.

Kibana :

1. **Interface Web Interactive :** Kibana fournit une interface utilisateur web conviviale qui permet aux utilisateurs de visualiser et d'interagir avec les données stockées dans Elasticsearch. Il est accessible via un navigateur web, ce qui facilite l'accès à partir de diverses plates-formes.
2. **Création de Tableaux de Bord :** Les utilisateurs peuvent créer des tableaux de bord personnalisés en rassemblant différentes visualisations et graphiques. Ces tableaux de bord peuvent être configurés pour afficher des métriques spécifiques, des tendances temporelles, des cartes géographiques, etc.
3. **Visualisations Personnalisables :** Kibana offre une variété de visualisations prédéfinies, telles que des histogrammes, des camemberts, des cartes géographiques, des jauges, etc. De plus, les utilisateurs peuvent créer des visualisations personnalisées pour répondre à des besoins spécifiques.

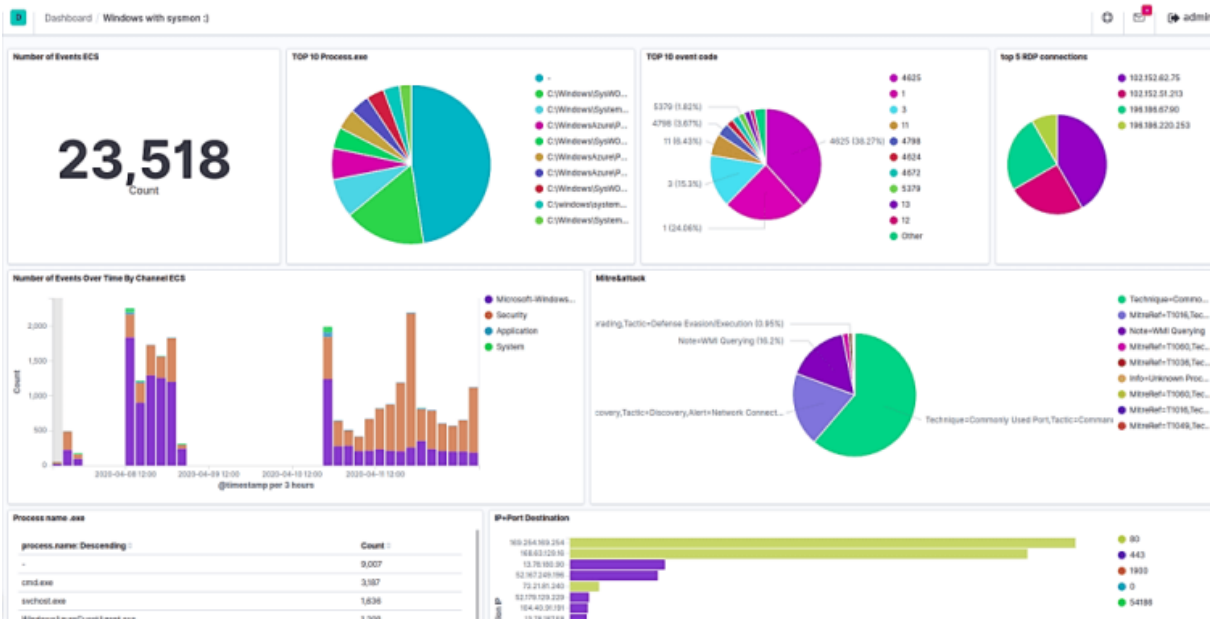
4. **Exploration des Données :** Kibana permet aux utilisateurs d'explorer les données en effectuant des requêtes, en filtrant les résultats et en zoomant sur des périodes spécifiques. Cela facilite l'analyse approfondie des données stockées dans Elasticsearch.
5. **Intégration avec Elasticsearch :** Kibana est étroitement intégré avec Elasticsearch, permettant une configuration simple et une interaction directe avec les index et les données stockées dans Elasticsearch.
6. **Gestion des Utilisateurs et des Rôles :** Kibana propose des fonctionnalités de gestion des utilisateurs et des rôles pour sécuriser l'accès aux données et aux fonctionnalités spécifiques de l'interface.
7. **Support de Plusieurs Sources de Données :** Bien que Kibana soit principalement utilisé avec Elasticsearch, il peut également être configuré pour se connecter à d'autres sources de données, élargissant ainsi sa polyvalence.
8. **Extensions :** Kibana peut être étendu avec des plugins pour ajouter des fonctionnalités supplémentaires ou intégrer des sources de données spécifiques.

Kibana est une interface web open source qui fait partie de la suite Elastic. Elle est conçue pour permettre la visualisation, l'analyse et l'interaction avec les données stockées dans Elasticsearch. Kibana facilite la création de tableaux de bord interactifs, de graphiques et de visualisations pour explorer et comprendre les données

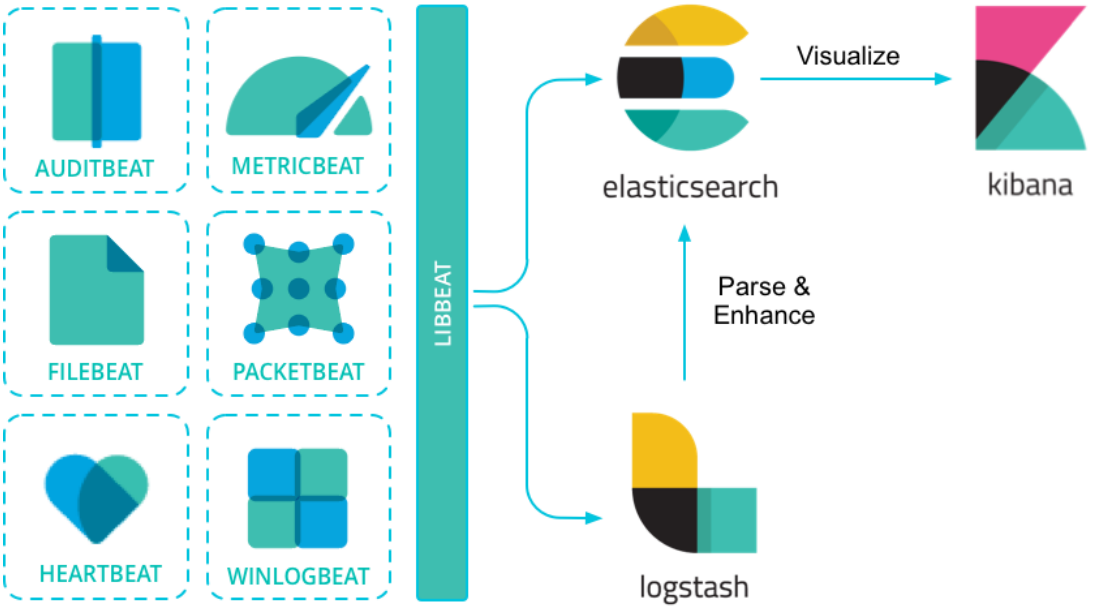
Beat (Facultatif) :

Dans le contexte d'Elasticsearch, "beat" se réfère à la famille de logiciels open source conçus pour expédier différents types de données dans Elasticsearch. Les beats agissent comme des agents légers qui collectent et expédient des données opérationnelles pour l'analyse. Ils peuvent être utilisés pour surveiller différents types de données, tels que les journaux, les métriques système, les données de réseau, etc., et les envoyer à Elasticsearch ou à Logstash pour l'indexation et l'analyse ultérieures. Les exemples de beats populaires incluent Filebeat pour l'expédition de fichiers journaux, Metricbeat pour la surveillance des métriques système, Packetbeat pour l'analyse du trafic réseau, etc. En bref, dans Elasticsearch, "beat" est un élément clé pour collecter et expédier des données vers le cluster Elasticsearch pour l'analyse et la visualisation.

Ci-dessous un exemple de dashboard avec Kibana



Ci-desous le fonctionnement d'ELK ainsi que les Beat



Nous proposerons selon la volumétrie de chaque entreprise une offre ELK adapté à ses besoins.

Quatre types de volumétrie ont étaient défini : très petite, petite, moyenne et grande.

	Standard	Gold	Platinium	Enterprise
Prix	95 USD/Mois	109 USD/Mois	125 USD/Mois	175 USD/Mois
• Principales fonctionnalités de la Suite Elastic, dont la sécurité	✅	✅	✅	✅
Discover, statistiques de champ, Kibana Lens, Elastic Maps et Canvas	✅	✅	✅	✅
Alerting et actions dans la suite	✅	✅	✅	✅
Alerting, avec un moteur de détection et des règles prédéfinies	✅	✅	✅	✅
• Ingestion et gestion des agents centralisées	✅	✅	✅	✅
• Collecte des données d'hôte et prévention contre les malwares	✅	✅	✅	✅
• Gestion des incidents	✅	✅	✅	✅
• Gestion de la posture de sécurité cloud (CSPM) et gestion des vulnérabilités cloud (CNVM)	✅	✅	✅	✅
• Applications pour APM, logging et indicateurs	✅	✅	✅	✅
• Intégrations prêtes à l'emploi	✅	✅	✅	✅

par centaines				
• Ingestion et gestion des agents centralisées	✅	✅	✅	✅
• Accès au service mondial de tests gérés pour le monitoring synthétique2	✅	✅	✅	✅
• Universal Profiling	✅	✅	✅	✅
• Base de données et recherche vectorielles	✅	✅	✅	✅
• Pertinence personnalisable	✅	✅	✅	✅
• Tableaux de bord d'analyse du comportement	✅	✅	✅	✅
• Monitoring en un clic	✅	✅	✅	✅
• Contrôle d'accès basé sur les rôles	✅	✅	✅	✅
• Connector Frameword en code ouvert pour les clients de connecteur personnalisés	✅	✅	✅	✅
• Support technique web	✅	✅	✅	✅
• 2 contacts dédiés	✅	✅	✅	✅
• Temps de réponse cible de 3 jours ouvrés (Elastic Cloud uniquement)	✅	✅	✅	✅
Reporting	❌	✅	✅	✅
• Actions d'alerting tierces	❌	✅	✅	✅

Watcher	❌	✅	✅	✅
• Monitoring multi-stack	❌	✅	✅	✅
• Workflows optimisés, y compris workflows de réponse aux incidents tiers	❌	✅	✅	✅
• Notifications externes et actions selon les alertes de détection	❌	✅	✅	✅
• Configuration avancée de gestion des hôtes	❌	✅	✅	✅
• Support technique aux heures ouvrées	❌	✅	✅	✅
• Support technique par téléphone et sur le web	❌	✅	✅	✅
• 6 contacts dédiés	❌	✅	✅	✅
Temps de réponse initial : Urgent : 4 heures ouvrables Élevé : 1 jour ouvrable Normal : 2 jours ouvrables	❌	✅	✅	✅
• Fonctionnalités de sécurité avancées de la Suite Elastic	❌	❌	✅	✅
• Machine Learning – détection des anomalies, apprentissage	❌	❌	✅	✅

supervisé, gestion des modèles tiers				
• Réplication inter-clusters	❌	❌	✅	✅
• Détection des anomalies par Machine Learning et tâches SIEM prédéfinies	❌	❌	✅	✅
• Protection contre les ransomwares basée sur les comportements	❌	❌	✅	✅
• Catégorisation des logs	❌	❌	✅	✅
• Cartes de services	❌	❌	✅	✅
• Corrélations APM	❌	❌	✅	✅
• Règles de Machine Learning spécifiques au domaine	❌	❌	✅	✅
• Accès au service mondial de tests gérés pour le monitoring synthétique2	❌	❌	✅	✅
• Universal Profiling	❌	❌	✅	✅
• Recherche sémantique grâce au modèle de ML Learned Sparse Encoder d'Elastic	❌	❌	✅	✅
• Prise en charge des modèles d'inférence de Machine Learning tiers	❌	❌	✅	✅
• Classement hybride avec	❌	❌	✅	✅

fusion des rangs réciproques				
• Connecteur natif et intégrations du robot d'indexation3	❌	❌	✅	✅
• Sécurité au niveau des documents	❌	❌	✅	✅
• Support technique 24 h/24, 7 j/7, 365 j par an	❌	❌	✅	✅
• Support technique par téléphone et sur le web	❌	❌	✅	✅
• 8 contacts dédiés	❌	❌	✅	✅
Temps de réponse initial : Urgent : 1 heure Élevé : 4 heures Normal : 1 jour ouvrable	❌	❌	✅	✅
• Snapshots interrogeables	❌	❌	❌	✅
• Prise en charge des niveaux interrogeables "cold" et "frozen"	❌	❌	❌	✅
• Serveur Elastic Maps	❌	❌	❌	✅
• Snapshots interrogeables pour une conservation de longue durée des archives exploitables	❌	❌	❌	✅
• Actions de réponse de l'hôte	❌	❌	❌	✅
• Protection des charges de travail cloud pour une	❌	❌	❌	✅

visibilité approfondie sur les charges de travail				
• Elastic AI Assistant pour obtenir des conseils sur l'IA générative	❌	❌	❌	✅
• Snapshots interrogeables pour plus de données de logs, d'indicateurs et d'APM	❌	❌	❌	✅
• Accès au service mondial de tests gérés pour le monitoring synthétique2	❌	❌	❌	✅
• Universal Profiling	❌	❌	❌	✅
• Elastic AI Assistant pour obtenir des conseils sur l'IA générative	❌	❌	❌	✅
• Snapshots interrogeables pour plus de données de contenus d'application et d'enregistrements d'espace de travail historiques	❌	❌	❌	✅
• Support technique 24 h/24, 7 j/7, 365 j par an	❌	❌	❌	✅
• Support technique par téléphone et sur le web	❌	❌	❌	✅
• 8 contacts dédiés	❌	❌	❌	✅

Temps de réponse initial : Urgent : Offre autogérée : 1 heure Elastic Cloud : 30 minutes Élevé : 4 heures Normal : 1 jour ouvrable	❌	❌	❌	✅

3. Plan de Mise en Œuvre

Notre équipe de spécialistes en sécurité informatique proposera un plan de mise en œuvre en plusieurs étapes, incluant :

1. **Audit Initial et Planification :** Évaluation de votre infrastructure actuelle et identification des sources de données clés.
2. **Configuration et Déploiement :** Installation de ELK Stack, configuration des pipelines de données et intégration des sources de logs.
3. **Personnalisation et Optimisation :** Développement de tableaux de bord sur mesure dans Kibana et optimisation des performances d'Elasticsearch.
4. **Formation et Transfert de Connaissances :** Sessions de formation pour vos équipes afin de les rendre autonomes dans la gestion quotidienne du SIEM.
5. **Support et Maintenance :** Offre de services de support et de maintenance pour garantir la pérennité de la solution.

Veuillez vous référez au 2023-R035-001_CCTP_BinaryArmor pour plus de précision.

4. Budget et Conditions

Le coût total estimé pour la mise en place de la solution SIEM avec ELK Stack est affiché dans le document Excel, incluant le matériel, le logiciel, la personnalisation et les services professionnels. Ce prix est une estimation et pourrait être ajusté en fonction des besoins spécifiques identifiés lors de l'audit initial.

La création d'un catalogue de coûts pour l'installation d'un ELK (Elasticsearch, Logstash, Kibana) dépend de plusieurs facteurs, notamment la taille de votre infrastructure, les besoins spécifiques de votre organisation, et si vous envisagez une configuration sur site ou dans le cloud. Voici une liste générale des coûts associés à l'installation d'un ELK stack défini dans un document Excel.

Veuillez vous référez au 2023-R035-001_BPU+DQE_BinaryArmor pour plus de précision.