FAMILLES DE PRODUITS

Endpoint Detection and Response

Le volet cyber de France Relance

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est en charge du volet cybersécurité de France Relance pour concevoir des offres de service destinées à **élever le niveau de cybersécurité de l'État, des collectivités territoriales et des organismes au service des citoyens** (social, santé, formation, audiovisuel, sécurité).

Les appels à projets, l'une des réponses de l'ANSSI au volet cyber de France Relance

Différentes solutions ont déjà été identifiées par l'ANSSI comme pouvant faire l'objet d'un projet d'acquisition dans le cadre du plan France Relance :

Analyse de risque EBIOS Risk Manager	Bug Bounty	**Endpoint Detection and Response**	Gestionnaire de vulnérabilités	Bastion
Pare-feu applicatif web (WAF)	Sauvegarde sécurisée	Sécurisation de l'Active Directory	Sécurisation de la messagerie mail	Gestion des identifiants utilisateur

Endpoint Detection and Response

47 %
des attaques sont détectées par les antivirus classiques*

Qu'est-ce que le Endpoint Detection and Response ?

Un EDR permet **de détecter et bloquer les menaces connues et inconnues** sur les terminaux en s'appuyant sur l'analyse comportementale, l'apprentissage automatique et la corrélation des événements. Un EDR possède de fortes capacités **de détection** (comportements suspects, attaques sans dépôt de fichier), **d'investigation** (visualisation de la séquence complète d'une attaque) et **de remédiation** (restauration de fichiers, fermeture de programmes, isolation réseau de machines).

Quelle est la différence avec un antivirus classique ? Avec un antivirus « next gen » ? Avec un EDR ?

Un antivirus classique détecte les menaces dont la signature est connue. **Un antivirus « next gen »** peut bloquer des menaces avancées grâce à ses moteurs d'analyse. **L'EDR** va, quant à lui, être capable de corréler les données des terminaux, détecter les comportements suspects et bloquer l'attaque en redescendant l'information aux autres terminaux.

(*) Rapport CESIN – Baromètre de la cybersécurité des entreprises

Pourquoi cette famille de solutions ?

- **La menace liée aux ransomwares** est prédominante, notamment au sein des collectivités territoriales.
- La solution est adaptée à **différents types d'organisations, ayant des niveaux de maturité différents**, car elle peut être opérée de différentes manières.
- C'est la principale solution technologique qui permet de **faire face aux menaces avancées et persistantes** sur les terminaux, pour lesquelles l'efficacité des antivirus n'est pas suffisante.

Menaces couvertes

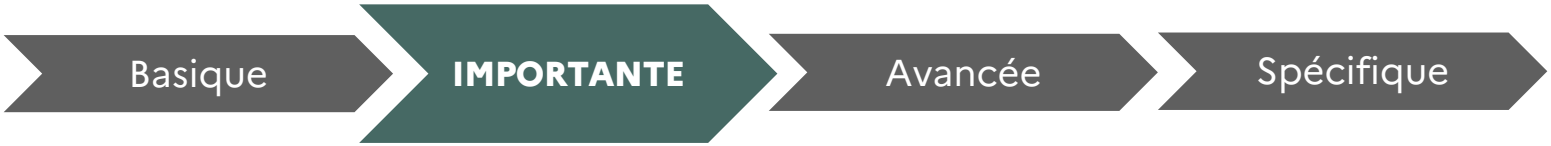
Menace persistante
(connexions malveillantes, exécution de code, etc.)

Malware
(ransomware, ver, virus, spyware, cryptominer, etc.)

Périmètre

L'ensemble des terminaux à protéger (postes de travail, serveurs, smartphones, etc.)

Maturité sécurité attendue pour la solution



Déploiement (1/2)

1. Créer le tenant de la console dans le **Cloud** (plateforme centralisée)

   Déployer la console (plateforme centralisée) **on-premise** (s'assurer des comptabilités et des ressources nécessaires de l'équipement matériel)

2. Déployer **les agents** sur les systèmes (en mode détection)

3. **Créer les politiques de détection et de remédiation**

   Exploiter les EDR: traiter les faux positifs, réagir en cas d'incident, adapter les politiques et préparer des actions de remédiation manuelles.

Phase d'apprentissage (entre 2 et 4 semaines)

Déploiement (2/2)

Phase de BUILD

- **Équipe d'intégration** nécessaire pour le déploiement d'un agent sur chaque système à protéger.
- **Équipe d'intégration** nécessaire pour la personnalisation des règles de détection et de remédiation, en accord avec la stratégie de détection.

Complexité : moyenne

Phase de RUN

- **RSSI, gestionnaire du SOC** pour suivre l'état général de la sécurité du système d'information.
- **Gestionnaire de la console** (en interne ou managé par un tiers) pour la supervision des événements, le traitement des alertes et le traitement des faux positifs.
- **Gestionnaire de la console** (en interne ou managé par un tiers) pour l'évolution des règles de détection et de la remédiation au cours du temps.
- **Administrateur système** pour le maintien en condition opérationnelle de l'outil et des agents.

Complexité : élevée

Recommandations d'usage

- **Se faire accompagner par un prestataire** de confiance pour l'intégration et la gestion de l'EDR de manière à optimiser ses politiques de sécurité (détection et remédiation) et par conséquent, garantir le bénéfice sécurité.

- En parallèle, assurer une **configuration sécurisée des terminaux** (durcissement de configuration, revue de la gestion des accès, déploiement des patchs, etc.).

- **Traiter les faux positifs et affiner les politiques** pour ne pas noyer les administrateurs.

- Préparer **des actions de remédiation manuelles** à mettre en place en cas de menaces critiques détectées sur l'environnement.

- Mettre en place un **processus de gestion des incidents** (politique, fiches réflexes, etc.) de manière à réagir efficacement en cas de compromission d'un terminal.

Complémentarité avec d'autres outils

Comment optimiser l'efficacité de la solution ?

- SIEM et SOC (analystes, MSSP, équipe de réponse à incident)
- Solution de patch management

Quelles autres solutions celle-ci peut-elle compléter ?

- Compléter les sondes sur les réseaux / terminaux
- Compléter les solutions classiques d'antivirus/EPP (plateforme de protection des endpoints)

Services associés

Accompagnement possible pour le pilotage de la solution par un tiers :

- Gestion managée de l'EDR pour son exploitation et son administration (supervision des événements, traitement des alertes et des faux positifs).
- Accompagnement pour la création des plans de remédiation.