Digital Security
Progress. Protected.

Synthèse EPDR

Endpoint Prevention, Detection & Response

05/07/2022 | V.1.0

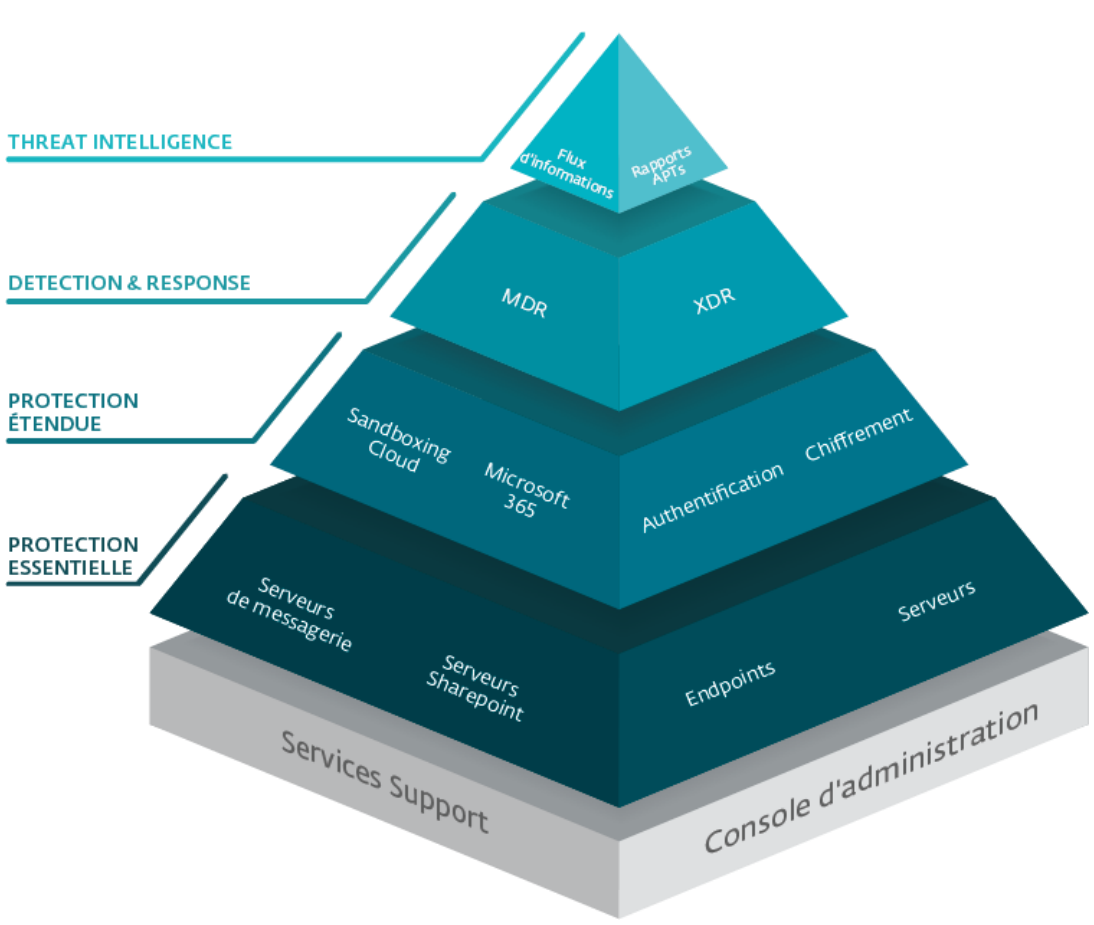
Introduction

État du marché

La technologie de Detection & Response est apparue récemment dans le but de couvrir un spectre plus large de détection. Les logiciels antimalwares standards sont certes efficaces, mais face à l'évolution rapide des tendances et des environnements, le besoin s'est prononcé naturellement d'ajouter des couches de protection supplémentaires. Aucun outil traditionnel n'est initialement conçu pour faire face aux menaces modernes et sophistiquées que nous rencontrons aujourd'hui, et malgré les outils déployés, les équipes de sécurité sont dépassées en nombre et en efficacité face aux innombrables alertes, logs, données, vecteurs d'attaques et outils différents à surveiller.

Technologie

EPDR, EDR, NDR, XDR, MDR… Des acronymes représentant des solutions permettant d'améliorer la **visibilité** et d'être en mesure **d'analyser, de détecter, de rechercher, de répondre et de remédier** aux risques cyber. Contrairement aux produits de sécurité que nous connaissions jusqu'à présent, qui n'agissaient que sur une partie spécifique de l'infrastructure d'une entreprise, et de manière ponctuelle, La technologie de Detection & Response a pour but d'agir sur l'ensemble de cette dernière. C'est-à-dire sur les endpoints, mais aussi sur le réseau, le Cloud…



Au sein d'une protection multicouche, la technologie de **Detection & Response** se situe un cran au-dessus de la protection « Étendue » (Chiffrement, Sandboxing Cloud…), qui se trouve elle-même au-dessus de la protection « Essentielle » (plateforme de protection des endpoints, serveurs et messagerie).

ESET PROTECT : Plateforme XDR

I - Des capacités de détection incomparables

Dans un premier temps, lorsque nous parlons de la technologie de l'XDR, il est primordial d'avoir une **visibilité complète** ainsi que de grandes **capacités de détection.** Sans visuel ni contexte clair, il est impossible d'analyser les menaces potentielles, et donc encore moins de les arrêter. C'est pourquoi une plateforme XDR doit être capable de s'adapter à tous types d'infrastructures, d'utiliser à bon escient le Machine Learning et l'analyse comportementale, de consommer des flux d'informations et de télémétrie de multiples sources, de conserver les logs sur une durée donnée, de mettre à disposition de multiples règles manuelles et automatisées personnalisables, d'analyser le flux venant de l'intérieur ou de l'extérieur du parc informatique, et de mettre en relation les analyses avec les techniques des attaques connues dans le monde entier.

Centralisez votre sécurité informatique

ESET PROTECT est notre console d'administration, déployable **sur site ou dans le Cloud**. Elle assure à la fois une visibilité en temps réel des Endpoints et l'administration des solutions multiplateformes ESET sur une interface unique. Elle permet de **déployer, de gérer et de surveiller** l'état du système afin de résoudre rapidement les problèmes et les menaces en toute sécurité. Notons également que l'authentification à double facteur (2FA) est une méthode de connexion disponible avec ESET Secure Authentication, et assurer une protection toujours plus efficiente grâce à notre **chiffrement transparent intégré** à la console, ESET Full Disk Encryption.

Groupes dynamiques, politiques, règles et tâches personnalisables et adaptées

Avec ESET PROTECT**, Les endpoints peuvent être classés** dans des groupes dynamiques en fonction de leur état ou de de multiples autres critères. Vous pouvez **ainsi configurer le déclenchement automatisé de tâches** telles que des analyses, des modifications à apporter aux politiques ou des installations et désinstallations de logiciels, sur la base des changements d'appartenance à ces groupes dynamiques. Il est ensuite possible de **configurer des politiques** pour chaque ordinateur ou groupe, d'en définir assurément les permissions et ainsi choisir de fermer un certain nombre d'accès. La création **de règles de détections personnalisées** constitue également une partie importante des outils d'XDR.

ESET
Machine Learning

ESET a développé son propre Machine Learning, baptisé ESET Augur. Notre moteur puissant combine les réseaux neuronaux avec des algorithmes spécialement sélectionnés pour **étiqueter correctement les échantillons entrants comme inoffensifs, potentiellement indésirables ou malveillants**. Pour permettre les meilleurs taux de détection et le plus petit nombre de faux positifs, le moteur ESET Augur est conçu pour coopérer avec d'autres technologies de protection telles que l'analyse de l'ADN, la Sandbox, l'analyse de la mémoire et l'extraction de caractéristiques comportementales.

Utilisation des flux d'informations des produits ESET

ESET PROTECT possède des qualités de télémétrie réellement complètes, en provenance de la large gamme de solutions pour entreprises d'ESET. Ces solutions sont **complètement multiplateformes** : Windows, macOS, Linux, Android, iOS, iPadOs, Machines Virtuelles, Microsoft Exchange, Domino, Sharepoint Online, Exchange Online, MS365, Teams, OneDrive, OneNote…

ESET Inspect, **notre console EDR, est interconnectée avec ESET PROTECT**. Elle reflète l'état de l'infrastructure ESET Inspect et **remonte les détections et évènements**, garantissant des actions de réponses et de remédiations rapides et efficaces.

Ces deux consoles ont été conçues distinctement dans le but d'exercer deux rôles qui leur sont propres. D'une part, **ESET PROTECT existe pour la partie gestion des solutions de sécurité**, et d'une autre part, **ESET Inspect permet l'analyse et le forensic**.

Nous travaillons continuellement afin de que notre plateforme XDR ESET PROTECT & INSPECT remonte le maximum de données et d'informations en provenance des solutions de sécurité ESET pour **endpoints, serveurs, appareils mobiles, passerelles de messagerie, serveurs de collaboration, Cloud Office**… Mais pas seulement ; les données collectées depuis notre **Sandbox Cloud** ou encore depuis **Threat Intelligence, VirusRadar, Livegrid, Mitre&Attack, les accès Web, le pare-feu et les détections réseau entrant/sortant** remontent également sur l'une ou l'autre de nos consoles.

II - Des options de réponses rapides et efficaces

Vous avez désormais toutes les informations sur les menaces potentielles dans votre environnement, c'est à ce moment que le deuxième rôle de l'XDR intervient. Il s'agit à présent d'être capable de **trier le danger réel ainsi que d'examiner les risques rapidement et de manière efficace**. C'est de cette phase qu'il s'agit lorsque nous évoquions l'obsolescence des outils de sécurités traditionnels, principalement lorsque la menace s'attaque à diverses sections de votre environnement. Nos capacités d'XDR chez ESET vont améliorer considérablement ce processus grâce à des **capacités de recherche et de surveillance des menaces** ainsi qu'en proposant **des actions de réponse et remédiations** qu'il est possible d'automatiser.

Capacités de recherches des menaces

Afin d'enquêter rapidement et de manière optimale, il est important d'avoir des outils puissants comme notre plateforme **ESET PROTECT & Inspect**. Cela permet d'accéder instantanément à tous types de renseignements sur les menaces : incidents, évènements, bibliothèque d'exécutables, scripts… sur une seule et même console.

Nos experts **surveillent les menaces tous les jours**, de manière proactive (Threat Monitoring), permettant de compiler leurs conclusions dans des rapports clairs et compréhensibles afin d'avertir instinctivement l'entreprise de tout évènement critique qui nécessiterait une attention ou une intervention immédiate. **Toutes les anomalies sont détectées** lors de la surveillance, et si elles doivent faire l'objet d'une enquête plus approfondie, toutes les recommandations sur la façon de procéder seront fournies.

Par-dessus cela s'ajoute la phase de recherche des menaces (Threat Hunting), lors de laquelle des activités plus approfondies sont effectuées. Il s'agit d'actions ponctuelles ou **l'environnement informatique est inspecté à l'aide de**

nos outils d'EDR, qui aide ainsi l'entreprise ou les équipes informatiques à enquêter sur des ensembles spécifiques de **données, d'alarmes et d'événements** générés par notre solution ESET Inspect (EDR).

Réponses rapides

Une fois les menaces détectées et examinées, il est important de **prendre des mesures correctives**. Votre système doit être capable de répondre rapidement et de prévenir les futures attaques sur l'ensemble du réseau, des endpoints et des environnements Cloud. ESET Inspect propose ainsi des :

- **Réponses automatisées** présentes au sein de notre LiveGuard ainsi qu'au sein de nos technologies de détection. Vous pouvez bloquer, mettre en quarantaine, restaurer partiellement avec notamment un nettoyage des entrées de registre... Il est possible de configurer un mode permettant de détecter uniquement, avec différents niveaux de granularité.

- **Réponses semi-automatisées** via les groupes dynamiques qui permettent des actions comme l'exécution de script, l'isolation du réseau, l'arrêt, le redémarrage... Les règles peuvent donc être ajustées pour appliquer automatiquement une action corrective.

- **Réponses manuelles** avec une multitude d'actions disponibles : Scan, Reboot, Shutdown, Exclude, Kill, Block, Download, Sysinspector, Remote Console, RDP Connect, Run command, Quarantaine...

Certains autres éléments qui pourraient paraitre évident, ne le sont pas pour autant, malgré qu'ils soient très importants afin d'avoir un outil de détection et de réponse réellement complet.

Prise en charge des SIEM & des SOC

ESET PROTECT **prend entièrement en charge les outils de SIEM** et exporte des journaux d'événements aux **formats JSON et LEEF**, pour une intégration avec les SOC (Security Operations Centers).

Visualisation des chaînes d'exécution

Notons que dans ESET Inspect, il est possible de **visualiser les processus d'exécution** menant à une alerte, et donc d'afficher l'ordre chronologique des actions passées.

Threat Intelligence

Le service ESET Threat Intelligence fournit des connaissances mondiales collectées par les experts d'ESET sur les **attaques ciblées, les menaces persistantes avancées (APT), les vulnérabilités zero-day et les activités des botnets**. Ces éléments sont difficiles à découvrir pour les entreprises et leurs équipes de sécurité, qui ne peuvent accéder qu'aux informations concernant leur réseau local. En possession de ces informations (vecteurs d'attaque, indicateurs de compromissions…), **les entreprises réduisent considérablement le délai de remédiation** grâce à une **visibilité globale** sur l'attaque et sur les éléments à rechercher.

Flux de renseignements

Nos flux proviennent exclusivement de nos centres de recherche basés dans le monde entier. Obtenez une image globale, et bloquer rapidement les IoC dans votre environnement. Les flux sont dans les formats JSON et STIX 2.0.

- **Flux de fichiers malveillants :** Comprenez les fichiers malveillants qui sont vus dans la nature. Ce flux comprend des domaines considérés comme malveillants, notamment le nom de domaine, l'adresse IP, la détection du fichier téléchargé à partir de l'URL et la détection du fichier qui a tenté d'accéder à l'URL. Ce flux comprend les hachages partagés des fichiers exécutables malveillants et les données associées.

- **Flux de domaines :** Bloque les domaines considérés comme malveillants, y compris le nom de domaine, l'adresse IP et la date qui leur est associée. Le flux classe les domaines en fonction de leur gravité, ce qui vous permet d'adapter votre réponse en conséquence, par exemple en ne bloquant que les domaines de haute gravité.

- **Flux de botnets :** Basé sur le réseau propriétaire de traqueurs de botnet d'ESET, Botnet feed présente trois types de sous-flux - botnet, C&C et cibles. Les données fournies comprennent des éléments tels que la détection, le hachage, la dernière vie, les fichiers téléchargés, les adresses IP, les protocoles, les cibles et d'autres informations.

- **Flux URL :** Semblable au flux de domaines, le flux d'URL examine des adresses spécifiques. Il comprend des informations détaillées sur les données relatives à l'URL, ainsi que des informations sur les domaines qui les hébergent. Toutes les informations sont filtrées pour n'afficher que les résultats hautement fiables et comprennent des informations lisibles par l'homme sur la raison pour laquelle l'URL a été signalée.

- **Flux APT :** Ce flux consiste en des informations APT produites par la recherche ESET. En général, le flux est une exportation du serveur interne MISP d'ESET. Toutes les données qui sont partagées sont également expliquées plus en détail dans les rapports APT. Le flux APT fait également partie de l'offre des rapports APT, mais le flux peut aussi être acheté séparément.

- **Flux IP :** Ce flux partage les adresses IP considérées comme malveillantes et les données qui leur sont associées. La structure des données est très similaire à celle utilisée pour les flux de domaines et d'URL. Le principal objectif est de comprendre quelles sont les IP malveillantes actuellement répandues dans la nature, de bloquer celles qui sont très graves, de repérer celles qui le sont moins et d'enquêter davantage, sur la base de données supplémentaires, pour voir si elles ont déjà causé des dommages.

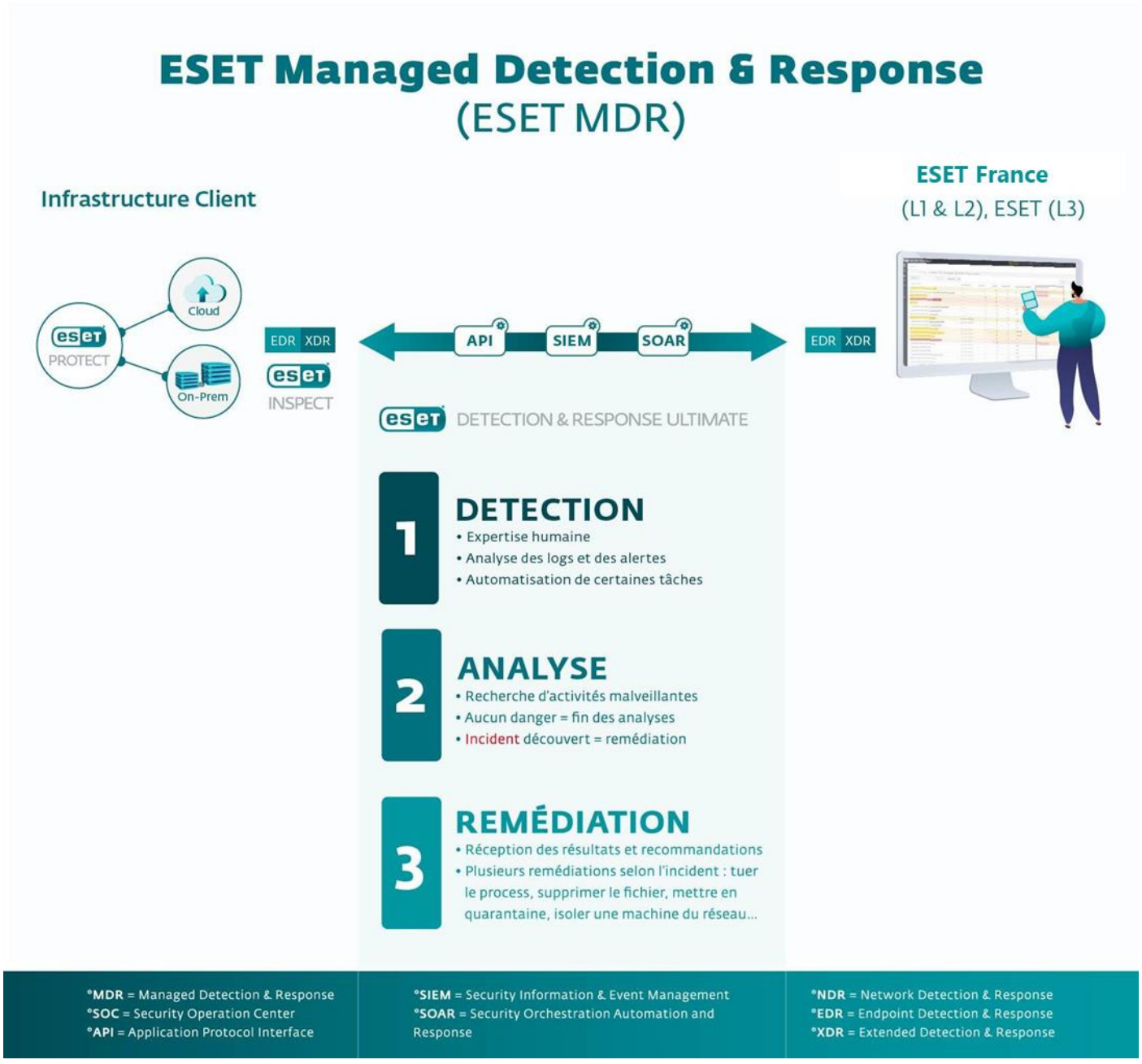
Les plateformes de renseignement sur les menaces peuvent fournir une **grande quantité de données** et potentiellement submerger les organisations d'informations. Il est essentiel que les entreprises soient en mesure d'agir rapidement sur les informations qu'elles reçoivent, sans avoir besoin d'une analyse épuisante. **La rapidité est essentielle** lorsqu'il s'agit d'extraire les données de renseignement sur les menaces d'un rapport et d'un flux, et de mettre sur liste noire les indicateurs de compromission (IoC) ou d'alerter le personnel de sécurité interne. Les flux et les **rapports doivent être très contextuels pour garantir une réponse rapide.**

Il est important que les données de renseignement sur les menaces que vous recevez soient non seulement exploitables, mais aussi facilement et **complètement intégrées dans votre environnement.**

Managed Detection & Response (MDR)

De nombreuses entreprises font le choix d'**externaliser la détection et la réponse aux incidents autour de l'EDR/EPP.** On parle alors de **MDR (Managed Detection & Response)** ou de MSSP (Managed Security Services Provider), un ensemble de service permettant l'externalisation de l'expertise en matière de sécurité, la centralisation des informations de sécurité, l'obtention de conseil de haute qualité, la certitude d'une conformité en matière de sécurité ainsi que la remédiation lorsqu'une menace est détectée et confirmée.

Comment ESET S'intègre dans ce paysage du MDR ?



Toujours dans l'optique de délivrer un accompagnement supplémentaire afin de s'adapter à vos besoins, nous proposons un support 24/7 ainsi que des services de HealthCheck ou encore de Déploiement & Upgrade.

Produits & Services ESET

PROTECT ENTERPRISE

Notre **Bundle ESET PROTECT Enterprise** est composé de :

- Console d'administration sur site ou dans le Cloud ESET PROTECT
- Solutions de protection des endpoints
- Solutions de protection des serveurs
- Sandboxing Cloud
- Chiffrement complet du disque
- EDR – XDR

Nous proposons **deux niveaux de service de MDR.** ESET Detection & Response Advanced et Ultimate.

Ces niveaux sont détaillés dans le tableau ci-dessous :

		DETECTION & RESPONSE ADVANCED	DETECTION & RESPONSE ULTIMATE
Délai de réponse		Garanti par SLA	Garanti par SLA
Services de sécurité pour endpoints	Malwares : Absence de détection	✓	✓
	Malwares : Problème de désinfection	✓	⌄
	Malwares : Infection de ransomware	✓	⌄
	Faux positifs	✓	⌄
	Général : Enquête sur les comportements suspects	✓	✓
Analyse et traitement des incidents	Analyse de base des fichiers	✓	✓
	Analyse détaillée des fichiers	✓	⌄
	Enquêtes approfondies	✓	⌄
	Assistance au traitement des incidents avec enquêtes approfondies	✓	⌄
Support EDR	Support : Règles	✓	✓
	Support : Exclusions	✓	✓
	Général : Questions relatives à l'EDR	✓	✓
	EDR : Optimisation initiale	✓	✓
	EDR : Recherche des menaces (à la demande)	✓	✓
Service de sécurité EDR	EDR : Surveillance des menaces (Threat Monitoring)	✗	✓
	EDR : Recherche des menaces proactive (Threat Hunting)	✗	✓
Service professionnel	Déploiement & mise à jour	✗	✓

Glossaire

	SOC	API	SOAR	SIEM	EDR	NDR	XDR	MDR
Nom	Security Operation Center	Application Protocol Interface	Security Orchestration Automation and Response	Security Information & Event Management	Endpoint Detection & Response	Network Detection & Response	Extended Detection & Response	Managed Detection & Response
Typologie	Expertise Humaine / Service	Connecteur	Outil	Outil	Logiciel	Logiciel	Logiciel	Expertise Humaine / Service
Champs d'application	Organisations	Endpoints / Applications	SOC / Équipe de sécurité	SOC / Équipe de sécurité	Endpoints & serveurs	Réseau & flux d'informations entre appareils	Endpoints, serveurs, réseaux, flux de données entre appareils & applications	Organisations
Objectifs	Assurer la sécurité de l'information, détecter, analyser et remédier aux incidents de cybersécurité à l'aide de solutions technologiques et d'un ensemble de démarches	Permettre à votre ordinateur, produit ou service de communiquer avec d'autres produits et services sans connaître les détails de leur mise en œuvre	Assurer la gestion des menaces, automatiser les opérations de sécurité et répondre aux incidents. Évaluer, détecter ou rechercher des incidents et des processus. Intervenir sans qu'une interaction humaine systématique soit nécessaire	Collecter et regrouper des données à partir de diverses sources internes et externes pour identifier les comportements anormaux qui peuvent être le signe d'une cyberattaque	Protéger les endpoints contre l'infiltration, surveiller et atténuer, évaluer les vulnérabilités, alerter et répondre. Protéger à la fois contre les attaques connues et inconnues, en analysant des comportements suspects	Rendre visible le trafic réseau, détecter les menaces connues, inconnues et les mouvements latéraux, alerter et répondre. Détecter le comportement d'attaquants possiblement cachés, ciblant les infrastructures physiques, virtuelles et cloud	Détecter les menaces connues et inconnues à tous les niveaux (endpoints, serveurs, réseaux, apps) incluant tous les composants, surveiller et atténuer de manière holistique, évaluer les vulnérabilités, alerter et répondre efficacement	Externaliser l'expertise en matière de sécurité, centraliser des informations de sécurité, conseiller et atteindre une conformité en matière de sécurité, remédier lorsqu'une menace est détectée et confirmée
Méthodes	Utiliser des outils de collecte, de corrélation d'événements et d'intervention à distance. (SIEM, SOAR, Scanner de vulnérabilité, Machine Learning, conformité réglementaire, engagement temps de réponse…)	Permettre d'accéder aux fonctions ou aux données d'une application à distance, depuis une autre application, en passant par un une interface applicative standard. Une requête est envoyée à au logiciel cible dans un langage universel	Utiliser des renseignements sur les menaces pour comprendre les attaques et dangers de manière préventive, accélérer la hiérarchisation et confirmer la résolution de l'incident après une menace de sécurité	Utiliser le Machine Learning et d'autres technologies avancées afin de configurer des règles adaptées à la politique de sécurité	Utiliser l'analyse des comportements malveillants, les indicateurs d'attaque (IoA), les indicateurs de compromission (IoC), les signatures…	Utiliser les indicateurs d'attaque (IoA), les détections d'anomalies, le comportement de l'utilisateur, le Machine Learning…	Mélange des deux précédents en utilisant donc le Machine Learning, les indicateurs d'attaque (IoA), les détections d'anomalies, les comportements de l'utilisateur, les comportements malveillants, les indicateurs de compromission…	Intégration des systèmes du client via diverses interfaces (API, logging, DataLake, etc.) afin de prendre en charge la sécurité de leur organisation
Défis	Répondre au manque de compétences, corrélation de logs, analyse des comportements anormaux, réduction des faux-positifs, traitement, rapidité d'intervention après incident, minimisation des alertes & événements	Simplifier le développement d'applications, gagner du temps et de l'argent, offrir plus de flexibilité, simplifier la conception, l'administration et l'utilisation, et donner les moyens d'innover	Hiérarchisation des menaces potentielles, évaluation de l'impact potentiel, triage des menaces les plus importantes, réponse aux menaces en conséquence	Collecter, normaliser, corréler, agréger et détecter les anomalies sur une variété de sources de données, puis notifier les parties appropriées lorsqu'un comportement suspect est détecté ou des alarmes configurables sont déclenchées	Lutter contre les menaces persistantes avancées (APT), ransomware, scripts malveillants…	Lutter contre les attaques et intrusions avancées, les attaques sans logiciels malveillants… Assurer une visibilité totale des menaces connues et inconnues qui passent par le réseau	Répondre aux possibilités d'intégrations tierces (interfaces fabricants…) Répondre aux lacunes en matière de visibilité et aux défis en partie typiques de l'EDR et du NDR	Répondre au manque de compétences en matière de sécurité au sein d'une organisation (déploiement d'outils XDR, simplification de la sécurité au quotidien, traitement/minimisation des alertes & événements…)