# XDR managé

## Réduction du bruit • Corrélation • Pilotage par preuves

**Service opéré : intégration des sources, triage et qualification, escalade, reporting et revues périodiques.**

## Rendre la détection exploitable au quotidien

Un XDR opéré qui consolide les signaux prioritaires, corrèle les événements et transforme le bruit en alertes actionnables, avec traçabilité et reporting.

## Points clés

### Consolidation des signaux

Sur les surfaces prioritaires, afin de réduire les angles morts.

- Intégration des sources prioritaires afin de consolider les signaux utiles et réduire les angles morts.
- Normalisation des événements pour rendre l'analyse et la recherche cohérentes dans le temps.
- Couverture progressive par périmètre, en commençant par les actifs et services critiques.

### Corrélation et qualification

pour transformer les alertes en actions concrètes.

- Détections contextualisées pour limiter les faux positifs et privilégier les alertes exploitables.
- Corrélation multi-sources afin de reconstituer un scénario d'attaque et d'en mesurer la portée.
- Qualification managée des alertes, avec priorisation et éléments de décision.

### Réponse, pilotage et preuves

pour piloter, rendre compte, et soutenir les exigences de conformité.

- Recommandations opérationnelles de remédiation et de durcissement, orientées actions.
- Chronologies d'incident et éléments de traçabilité pour faciliter l'investigation et le retour d'expérience.
- Reporting exportable pour le pilotage, la communication à la direction, et les besoins d'audit.

## Surfaces couvertes


Endpoints


Identités


M365


Messagerie


Serveurs


Réseau


Sauvegarde

## Livrables opérationnels

- Alertes qualifiées avec niveau de criticité et contexte
- Chronologie de l'incident et périmètre impacté
- Actions recommandées de remédiation, priorisées
- Éléments de traçabilité et exports pour compte rendu
- Reporting périodique et suivi des actions correctives

## Exemples de signaux traités

- Connexions à risque et tentatives répétées d'authentification
- Élévation de privilèges et changements d'administration
- Règles de messagerie suspectes et redirections anormales
- Exécutions et comportements typiques de ransomware
- Communications sortantes inhabituelles et domaines suspects
- Suppressions ou modifications anormales sur les dépôts de sauvegarde

1 Sources → 2 Corrélation → 3 Qualification managée → 4 Actions et preuves

## Périmètre et livrables

| Source | Télémétrie et événements analysés | Livrable |
|---|---|---|
| Endpoints et serveurs | • Événements de sécurité<br>• Comportements<br>• Exécutions suspectes | • Alertes qualifiées<br>• Chronologie<br>• Actions recommandées |
| Identités | • Authentifications<br>• Échecs répétés<br>• Élévations de privilèges<br>• Changements d'administration | • Alertes contextualisées<br>• Éléments de preuve<br>• recommandations de durcissement |
| Microsoft 365 | • Activités d'audit<br>• Règles de messagerie<br>• Accès et partages<br>• Actions sensibles | • Alertes actionnables<br>• Chronologie<br>• Points de contrôle |
| Messagerie | • Signaux de phishing<br>• Redirections<br>• Comportements anormaux | • Qualification<br>• Priorisation<br>• Actions de remédiation |
| Réseau et périmètre | • Journaux réseau et périmètre, lorsque disponibles via intégrations et sources connectée | • Enrichissement des alertes<br>• Corrélation<br>• Hypothèses d'exfiltration |
| Sauvegarde et continuité | • Suppressions<br>• Changements de politique<br>• Échecs<br>• Signaux de sabotage | • Alertes à fort impact<br>• Recommandations de sécurisation<br>• Preuves exportables |

Le périmètre est défini selon vos priorités et la disponibilité des sources, afin de concentrer l'effort sur les signaux à plus forte valeur.

## Fonctionnement opérationnel

**1**

### Onboarding

Cartographie des sources disponibles, cadrage des priorités de détection, et définition des règles d'escalade.

**2**

### Intégration des sources

Connexion des sources prioritaires, Consolidation, enrichissement et corrélation des signaux, et vérification de la qualité des données.

**3**

### Exploitation managée

Corrélation, triage et qualification des alertes, avec priorisation et escalade selon criticité.

**4**

### Reporting et amélioration continue

Rapports exportables, retours d'expérience, et suivi des actions correctives pour renforcer la couverture dans le temps.

## Contrôles et traçabilité

- **Traçabilité des alertes et des décisions :** qualification, priorisation, escalade, et actions recommandées.
- **Chronologies d'incident reconstituées** à partir des signaux disponibles, afin de documenter les faits et le périmètre impacté.
- **Rapports exportables** utilisables pour le pilotage interne, les audits, la cyberassurance, et les démarches de conformité NIS2.
- **Historique et suivi des actions correctives** afin de démontrer la progression et la réduction des angles morts.
- **Revue périodique** de la couverture et des points d'amélioration, avec décisions et priorisation.

## Mettre la détection en condition opérationnelle

En 30 minutes, nous validons vos surfaces prioritaires et votre capacité d'exploitation, puis définissons une trajectoire pragmatique pour réduire les angles morts et améliorer la détection, en maîtrisant l'effort comme le budget.

**contact/vytalx.fr** **contact@vytalx.fr**