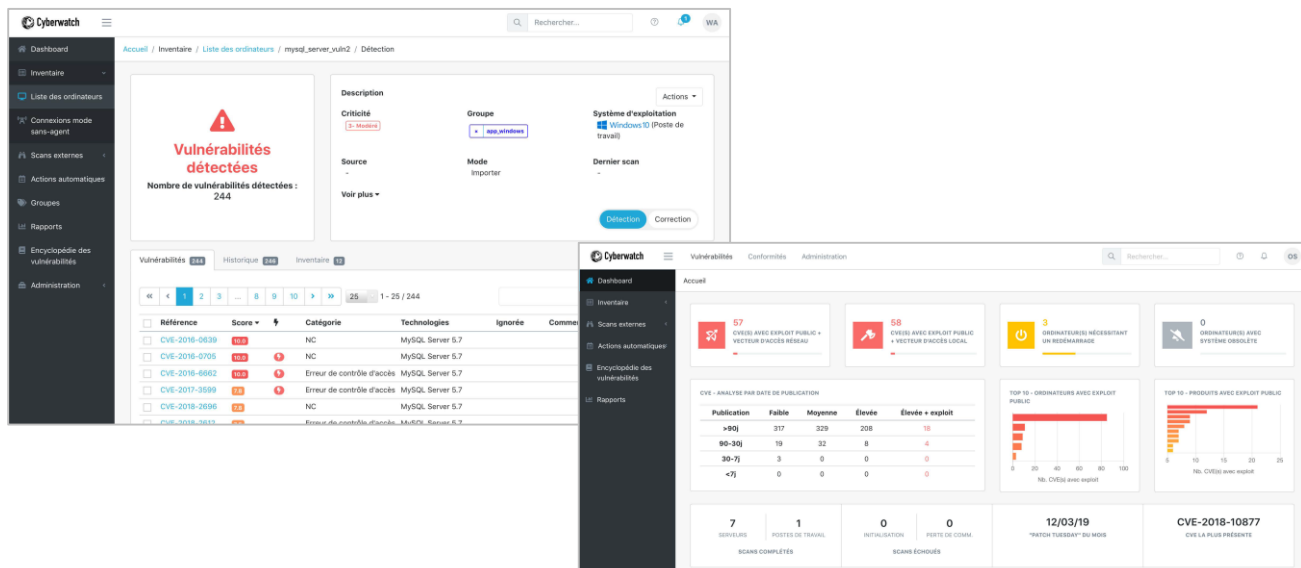


Fonctionnalités de Cyberwatch

- Gestion complète des vulnérabilités et des conformités
- Tableau de bord opérationnel adaptés à votre entreprise.
- Intégration simple dans votre environnement : installation On Premise (avec ou sans agent).
- Mise à jour quotidienne des bases de vulnérabilités, de correctifs et des référentiels de conformité.
- Module de Patch Management multiplateforme intégré : Linux, Windows, Mac.
- Module de création de vos propres règles de conformités et intégration de votre PSSI.



The screenshot displays the Cyberwatch web interface. The top section shows a dashboard with a red warning icon and the text "Vulnérabilités détectées" (Detected vulnerabilities) with a count of 244. Below this, there are filters for "Description", "Criticité" (Severity), "Groupe" (Group), "Source", and "Mode". The main area contains a table of vulnerabilities with columns for "Référence" (Reference), "Score", "Catégorie" (Category), and "Technologies".

Référence	Score	Catégorie	Technologies
CVE-2016-0839	NC	NC	MySQL Server 5.7
CVE-2016-0705	NC	NC	MySQL Server 5.7
CVE-2016-4662	NC	NC	MySQL Server 5.7
CVE-2017-3599	NC	NC	MySQL Server 5.7
CVE-2018-3596	NC	NC	MySQL Server 5.7
CVE-2018-3673	NC	NC	MySQL Server 5.7

The bottom section of the interface shows a summary dashboard with various metrics and charts, including "CVS - ANALYSE PAR DATE DE PUBLICATION" (CVS - ANALYSIS BY PUBLICATION DATE) and "TOP 10 - ORDINATEURS AVEC EXPLOIT PUBLIC" (TOP 10 - PUBLICLY EXPLOITED COMPUTERS).

Société française et logiciels labélisés

Cyberwatch module de gestion des vulnérabilités

- Gérer vos vulnérabilités.
- Accéder directement depuis le navigateur Web.
- Assurer une veille permanente et vous alerter de façon continue.
- Libérer les équipes informatiques d'un travail long et fastidieux.



Cartographiez

Obtenez la liste complète et contextualisez des machines et technologies du parc informatique.



Déterminez

Recherchez en continu des vulnérabilités publiées par les autorités et présentes dans le parc informatique.



Priorisez

Évaluez les vulnérabilités en fonction de leur score CVSS, de l'existence d'un exploit, et du contexte métier de la machine affectée.



Décidez

Prenez les bonnes décisions à l'aide de tableaux de bord et d'actions simples.



Corrigez

Embarquez nativement un module de Patch Management, compatible avec l'infrastructure utilisé.

Systemes couverts



Linux

Cyberwatch couvre les applicatifs du Package Manager Linux

macOS

Apple

Cyberwatch couvre les applicatifs des grands éditeurs (Adobe Reader, Adobe Flash...)



Microsoft

Cyberwatch couvre les applicatifs à installer par KBs Windows, & les applicatifs des grands éditeurs