Le Conseil Départemental en France améliore la cyber-résilience.

Le Conseil Départemental d'Eure-et-Loir réduit les risques d'attaques informatiques avec les solutions Quest.

Eure-et-Loir
LE DÉPARTEMENT

Pays : **France**

Employés : **2,500**

Industrie : **Gouvernement**

URL du site : **https://eurelien.fr/**

La cyber-résilience commence avec Active Directory.

Le département d'Eure-et-Loir est une collectivité territoriale du nord de la France. Le Conseil Départemental est compétent dans des domaines tels que les services sociaux, la voirie et les collèges.

Le Conseil Départemental d'Eure-et-Loir souligne l'importance de l'écosystème informatique pour remplir sa mission, avec Active Directory en son centre fournissant des services vitaux d'authentification et d'autorisation. En effet, lorsqu'une attaque a fait tomber leur AD, ils ont pu tout restaurer, grâce aux mesures qui avaient été mises en place par l'équipe informatique .

Cependant, l'incident a soulevé une question clé : « Nous nous sommes demandés pourquoi nous n'avions pas reçu d'alerte avant que tout

Défis

Face à la multiplication des attaques basées sur l'identité, le Conseil Départemental d'Eure-et-Loir a souhaité améliorer la cyber-résilience de son AD. En tant qu'utilisateurs satisfaits de l'outil de gestion de bases de données Oracle de Quest, ils ont été ravis de découvrir que Quest est également le leader incontesté des solutions pour AD et Entra ID.

Solutions

Avec Change Auditor by Quest®, le Conseil Départemental peut désormais détecter et analyser rapidement les menaces actives pour permettre une réponse plus rapide et plus efficace. Et SpecterOps BloodHound Enterprise leur permet d' identifier et d'atténuer de manière proactive les faiblesses de la sécurité AD afin de réduire leur surface d'attaque.

Avantages

- Permet une correction proactive des vulnérabilités de sécurité telles que les comptes surprovisionnés
- Fournit des alertes en temps réel sur les menaces actives
- Bloque les modifications risquées telles que l'ajout de membres aux administrateurs de domaine
- Visualise les chemins d'attaque qui pourraient permettre à un adversaire de s'emparer du domaine
- Identifie les points d'étranglement partagés par les chemins d'attaque et fournit des conseils de rémédiation

soit bloqué ", explique Diaga Gueye, responsable des infrastructures au Conseil Départemental d'Eure-et-Loir.

La détection des menaces en temps réel permet à l'équipe informatique d'arrêter rapidement les activités à risque.

Pour répondre à cette préoccupation majeure, le Conseil Départemental d'Eure-et-Loir s'est tourné vers son partenaire de confiance, Quest Software. « La plupart de nos applications critiques sont sur Oracle, et nous les gérons efficacement depuis des années avec Toad ® pour Oracle », note M. Gueye. « Notre ingénieur avant-vente chez Quest nous a présenté Change Auditor. Après son excellente présentation et démonstration du produit, je me suis immédiatement dit : « C'est exactement ce dont nous avons besoin. »

Après une évaluation minutieuse des autres solutions disponibles sur le marché, le conseil a déployé Change Auditor. Les résultats ont confirmé leur évaluation initiale. « Change Auditor fournit une surveillance en temps réel et une journalisation centralisée de tous les changements de sécurité dans notre environnement AD et Entra ID », explique M. Gueye. « Si un administrateur modifie un groupe sensible, change un GPO ou ajoute une entrée DNS, Change Auditor nous alerte afin que nous puissions enquêter immédiatement. En conséquence, nous avons considérablement réduit notre temps de détection des menaces et de réponse.

> **« Les journaux natifs sont si volumineux et si énigmatiques qu'il est facile de se perdre en essayant de les comprendre. Change Auditor rend les événements faciles à lire et fournit des détails immédiatement, me permettant de connaître l'activité sur mes serveurs en temps réel.**
>
> *Diaga Gueye, gestionnaire des infrastructures, Conseil Départemental d'Eure-et-Loir*

De plus, Change Auditor fournit plus d'informations que les journaux d'événements Microsoft n'en capturent et rend ces informations beaucoup plus faciles à comprendre. « Les journaux natifs sont si volumineux et si énigmatiques qu'il est facile de se perdre en essayant de les comprendre », explique M. Gueye. « Change Auditor rend les événements faciles à lire et fournit des détails immédiatement, me permettant de connaître l'activité sur mes serveurs en temps réel. C'est tellement simple et intuitif.

Change Auditor peut même empêcher que des changements risqués ne se produisent en premier lieu.

En plus de détecter les actions à risque en temps réel, Change Auditor pour Active Directory peut également bloquer les actions à risque : quels que soient les privilèges dont dispose un utilisateur , la solution peut l'empêcher de modifier les groupes de sécurité critiques et les paramètres de stratégie de groupe ou d'exfiltrer la base de données AD pour voler des informations d'identification .

«La cerise sur le gâteau, c'est la capacité de Change Auditor à bloquer certains événements», précise M. Gueye. "Par exemple, nous avons verrouillé le groupe Administrateur de domaine afin que les pirates ne puissent pas élever leurs privilèges en ajoutant un compte qu'ils ont piraté à ce groupe puissant."

Le Conseil a constaté presque immédiatement la valeur de son investissement.

M. Gueye propose plusieurs exemples de la manière dont Change Auditor a permis à son équipe de détecter des problèmes de sécurité qu'elle n'était pas en mesure de détecter auparavant :

- « Dès que nous avons déployé Change Auditor, nous avons reçu une alerte concernant un ordinateur Windows 2000 que nos outils précédents n'avaient jamais vu. Une petite enquête a confirmé qu'il n'y avait aucune raison pour que cet ordinateur soit connecté au domaine. Grâce à

Change Auditor, nous avons pu le supprimer de l'AD et éliminer un point d'entrée pour les pirates."

- « Change Auditor nous a également alerté qu'un serveur bombardait notre AD avec des milliers de requêtes de synchronisation LDAP par seconde. Il s'est avéré que le serveur était simplement mal configuré ; avec une simple modification de ses paramètres, nous avons pu arrêter les requêtes LDAP massives.
- « Change Auditor nous a signalé des tentatives venant du monde entier pour se connecter à l'un de nos comptes de service, probablement parce qu'il s'appelait « Support ». En renommant le compte, nous avons stoppé le flot de demandes de connexion.
- « Nous avons également reçu des alertes de Change Auditor concernant l'utilisation de NTLMv1 dans notre environnement. En conséquence, nous avons pu mettre à jour notre stratégie de groupe pour empêcher l'utilisation de ce protocole non sécurisé.

La cyber-résilience nécessite également de trouver et d'atténuer les chemins d'attaque AD.

Si une gestion efficace du changement est essentielle à la cyber-résilience, le Conseil Départemental d'Eure-et-Loir souhaitait également identifier et atténuer de manière proactive les faiblesses de son Active Directory avant que des adversaires ne puissent en abuser. En effectuant des tests d'intrusion à l'aide de la version gratuite de BloodHound, l'équipe informatique a découvert certaines des voies d'attaque dans leur AD qui pourraient permettre à un attaquant disposant d'un compte utilisateur compromis d'obtenir des droits d'administrateur.

Cependant, l'analyse des chemins d'attaque avec l'outil open source était très difficile et prenait beaucoup de temps. L'équipe informatique a donc été heureuse d'apprendre que Quest propose une version beaucoup plus robuste, SpecterOps BloodHound Enterprise . Cette solution puissante identifie les actifs de niveau 0 d'une organisation et fournit une carte claire des chemins d'attaque les mettant en danger.

« BloodHound Enterprise fournit une représentation graphique des chemins d'attaque afin que nous puissions voir exactement comment un attaquant pourrait partir d'un compte standard et élever ses privilèges pour atteindre une partie critique de l'AD" », explique M. Gueye. "Par exemple, nous avons immédiatement découvert certains comptes de service qui avaient trop de droits."

> **« BloodHound Enterprise fournit une représentation graphique des chemins d'attaque afin que nous puissions voir exactement comment un attaquant pourrait partir d'un compte standard et élever ses privilèges pour atteindre une partie critique de l'AD. Par exemple, nous avons immédiatement découvert certains comptes de service qui avaient trop de droits.**
>
> *Diaga Gueye, gestionnaire des infrastructures, Conseil Départemental d'Eure-et-Loir*

De plus, BloodHound Enterprise fournit des informations exploitables sur la manière de bloquer les chemins d'attaque qu'il identifie. Les organisations disposent souvent de dizaines de milliers de chemins d'attaque. La solution identifie donc les actions clés que les administrateurs peuvent entreprendre pour bloquer des centaines, voire des milliers de chemins d'attaque à la fois.

"Grâce à BloodHound Enterprise, nous disposons d'une carte claire des chemins d'attaque dans notre AD – et nous savons comment y remédier", note M. Gueye. « Par exemple, BloodHound a trouvé un compte de service qui disposait de trop d'autorisations privilégiées. En installant une version plus récente du produit associé qui ne nécessitait pas tous ces droits, nous avons pu rapidement combler la faille de sécurité.

Quest est un partenaire de confiance sur le long terme.

Le Conseil Départemental d'Eure-et-Loir apprécie vivement la poursuite de son partenariat avec Quest. « Toutes les solutions Quest dont nous disposons sont extrêmement intuitives et simples à utiliser », rapporte M. Gueye. « De plus, Quest a toujours fourni un excellent support tout au long du processus, de l'avant-vente à la vente en passant par le support technique. » En fait, l'équipe informatique envisage déjà d'explorer d'autres solutions Quest, notamment Change Auditor pour les serveurs de fichiers Windows , Change Auditor pour NetApp et Change Auditor pour EMC .

PRODUITS ET SERVICES

Produits présentés

- **Change Auditor for Active Directory**
- **SpecterOps BloodHound Enterprise**

Solutions présentées

- Gestion de la plateforme Microsoft

À propos de Quest

Quest crée des solutions logicielles qui exploitent les avantages des nouvelles technologies dans un paysage informatique toujours plus complexe. De la gestion des bases de données et des systèmes à la gestion d'Active Directory et Office 365, en passant par la cyber-résilience, Quest aide ses clients à relever leurs prochains défis informatiques dès à présent. Quest Software. Où demain rencontre aujourd'hui.