Departmental Council in France improves cyber resilience.

The Eure-et-Loir Departmental Council reduces the risks from attacks with solutions from Quest.

Eure-et-Loir
LE DÉPARTEMENT

Country: **France**

Employees: **2,500**

Industry: **Government**

Website: **https://eurelien.fr/**

Cyber resilience starts with Active Directory.

The Department of Eure-et-Loir is a territorial authority in northern France. The Departmental Council is responsible for matters such as social services, roads and colleges.

The Eure-et-Loir Departmental Council recognizes the importance of the IT ecosystem to fulfill its mission, with Active Directory at its center providing vital authentication and authorization services. Indeed, when an attack brought down their AD, they were able to restore everything, thanks to the measures that had been put in place by the IT team.

However, the incident raised a key question: “We asked ourselves, why didn’t we receive an alert before everything was blocked?” recalls Diaga Gueye, Infrastructure Manager at the Eure-et-Loir Departmental Council.

Challenges

Faced with a proliferation of attacks based on identity, the Departmental Council of Eure-et-Loir wanted improve the cyber resilience of its Active Directory. As satisfied users of Quest’s management tool for Oracle databases, they were pleased to discover that Quest is also the clear leader in solutions for AD and Entra ID.

Solution

With Change Auditor by Quest®, the Departmental Council can now quickly detect and analyze active threats to enable faster and more effective response. And SpecterOps BloodHound Enterprise empowers them to proactively identify and mitigate AD security weaknesses to reduce their attack surface.

Benefits

- Enables proactive remediation of security vulnerabilities like over-provisioned accounts
- Provides real-time alerts on active threats
- Blocks risky changes such as adding members to Domain Admins
- Visualizes attack paths that could enable
- an adversary to take over the domain
- Identifies choke points shared by attack paths and provides mitigation guidance

Real-time threat detection enables the IT team to quickly shut down risky activities.

To address this major concern, the Departmental Council of Eure-et-Loir turned to its trusted partner, Quest Software. “Most of our critical applications are on Oracle, and we have managed them effectively for years with Toad® for Oracle,” notes Mr. Gueye. “Our pre-sales engineer at Quest introduced us to Change Auditor. After his excellent presentation and product demo, I immediately said to myself, ‘This is exactly what we need.’”

After careful evaluation of other solutions available on the market, the council deployed Change Auditor. The results confirmed their initial assessment. “Change Auditor provides real-time monitoring and centralized logging of all security changes across our AD and Entra ID environment,” explains Mr. Gueye. “If an administrator modifies a sensitive group, changes a GPO or adds a DNS entry, Change Auditor alerts us so we can investigate immediately. As a result, we have reduced our threat detection and response time significantly.”

Plus, Change Auditor provides more information than Microsoft event logs capture — and makes that information much easier to understand. “Native logs are so large and cryptic that it’s easy to get lost trying to understand them,” says Mr. Gueye. “Change Auditor makes events easy to read and provides details immediately, allowing me to know the activity on my servers in real time. It’s so simple and intuitive.”

> **Native logs are so large and cryptic that it’s easy to get lost trying to understand them. Change Auditor makes events easy to read and provides details immediately, allowing me to know the activity on my servers in real time.**
>
> *Diaga Gueye, Infrastructure Manager, Eure-et-Loir Departmental Council*

Change Auditor can even prevent risky changes from happening in the first place.

In addition to detecting risky actions in real time, Change Auditor for Active Directory can also block risky actions: Regardless of what privileges a user has, the solution can prevent them from modifying critical security groups and Group Policy settings or exfiltrating the AD database to steal credentials.

“The icing on the cake is Change Auditor’s ability to block certain events,” says Mr. Gueye. “For example, we locked down the Domain Admin group so that hackers can’t elevate their privileges by adding an account they’ve hacked to that powerful group.”

The council began to see the value of its investment almost immediately.

Mr. Gueye offers several examples of how Change Auditor enabled his team to detect security issues they were not able to see before:

- “As soon as we deployed Change Auditor, we received an alert about a Windows 2000 computer that our previous tools had never seen. A little investigation confirmed that there was no reason for this computer to be connected to the domain. Thanks to Change Auditor, we were able to remove it from the AD and eliminate an entry point for hackers.”
- “Change Auditor also alerted us that a server was bombarding our AD with thousands of LDAP sync requests per second. It turned out that the server was simply misconfigured; with a simple change to its settings, we were able to stop the massive LDAP queries.”
- “Change Auditor notified us about attempts from all over the world to log into one of our service accounts, probably because it was called ‘Support.’ By renaming the account, we stopped the flood of connection requests.”
- “We also received alerts from Change Auditor regarding the use of NTLMv1 in our environment. As a result, we were able to update our Group Policy to prevent the use of this insecure protocol.”

> **BloodHound Enterprise provides a graphical representation of attack paths so we can see exactly how an attacker could start from a standard account and escalate their privileges to reach a critical part of the AD.**
>
> *Diaga Gueye, Infrastructure Manager, Eure-et-Loir Departmental Council*

Cyber resilience also requires finding and mitigating AD attack paths.

While effective change management is essential to cyber resilience, the Eure-et-Loir Departmental Council also wanted to proactively identify and mitigate weaknesses in its Active Directory before adversaries could abuse them. By performing penetration testing using the free version of BloodHound, the IT team had discovered some of the attack avenues in their AD that could allow an attacker with a compromised user account to obtain administrator rights.

However, analyzing the attack paths with the open-source tool was very difficult and time consuming. So the IT team was happy to learn that Quest offers a much more robust version, SpecterOps BloodHound Enterprise. This powerful solution identifies an organization's Tier 0 assets and provides a clear map of the attack paths putting them at risk.

"BloodHound Enterprise provides a graphical representation of attack paths so we can see exactly how an attacker could start from a standard account and escalate their privileges to reach a critical part of the AD," explains Mr. Gueye. "For example, we immediately uncovered some service accounts that had too many rights."

Moreover, BloodHound Enterprise provides actionable information on how to mitigate the attack paths it identifies. Organizations often have tens of thousands of attack paths, so the solution identifies the key actions administrators can take to choke off hundreds or even thousands of attack paths at once.

"Thanks to BloodHound Enterprise, we have a clear map of the attack paths in our AD — and we know how to remediate them," Mr. Gueye notes. "For example, BloodHound found a service account that had too many privileged permissions. By installing a newer version of the associated product that did not require all of those rights, we were able to quickly fix the security gap."

Quest is a trusted partner for the long term.

The Departmental Council of Eure-et-Loir highly appreciates its continued partnership with Quest. "All the Quest solutions we have are extremely intuitive and easy to use," reports Mr. Gueye. "Additionally, Quest has always provided excellent support throughout the entire process, from pre-sales to sales to technical support." In fact, the IT team is already planning to explore other Quest solutions, including Change Auditor for Windows File Servers, Change Auditor for NetApp and Change Auditor for EMC.

PRODUCTS AND SERVICES

Products

- Change Auditor for Active Directory
- SpecterOps BloodHound Enterprise

Solutions

- Microsoft Platform Management

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.