BLOODHOUND ENTERPRISE

CASE STUDY

Energy Company Improves Identity Directory Hygiene & Cyber Resilience

Edison Slashes Risk with Attack Path Management from BloodHound Enterprise and Auditing Tools from Quest

Keeping Active Directory Functional and Secure Is Vital To Cyber Resilience

Active Directory (AD), which provides the authentication and authorization services required for users to do their jobs and most business processes to run, is critical to Edison's operations.

"Since the beginning of our cyber resilience project, Active Directory has been classified as one of our vital applications. If we are not able to deliver this application, the company would be in serious trouble to survive."

Giampaolo Tacchini
CISO of Edison

Challenges

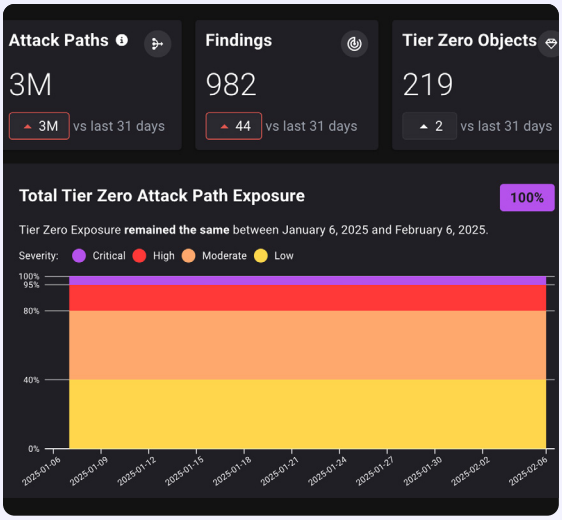
Edison S.p.A has been serving Italy through responsible energy production for over 135 years. A consequence of this long history, however, was an Active Directory (AD) infrastructure that had grown in both size and complexity over the years. The IT team recognized that AD was one of the most vital technologies in use, so they used a variety of Microsoft, open-source, and custom tools to try to uncover its vulnerabilities and monitor changes and other activity. However, they were all too aware that those tools were not providing the deep visibility they needed to ensure cyber resilience.

Solutions

Working with Microsys and using solutions from Quest, Edison dramatically expanded its ability to thwart adversaries by both identifying attack paths in AD using BloodHound Enterprise and seeing exactly how to remediate them. Moreover, the IT team can promptly spot and respond to threats in progress by efficiently auditing and alerting on activity across their entire hybrid AD environment.

Benefits

- **Identified attack paths in Active Directory that other tools missed**
- **Clearly visualized those attack paths with BloodHound Enterprise, facilitating communication among IT teams**
- **Provided clear remediation strategies**
- **Delivered comprehensive monitoring of the hybrid environment from a single dashboard**
- **Improved threat investigation and response with actionable, customizable alerts**



Getting a Complete Understanding of Tier Zero Assets Was Challenging

With that classification of AD in mind, Edison began working with its trusted partner Microsys to analyze, consolidate and restructure the AD environment using migration solutions from Quest and its partners.

A key goal was to identify all the company's most valuable, or Tier Zero, assets. Tier Zero includes critical servers like domain controllers (DCs) and all highly privileged accounts, as well as all accounts that could gain elevated privileges through a series of steps known as an Attack Path, which abuses factors like concealed permissions, nested group membership and inherent security gaps in AD architecture.

Lack of Insight Into Active Directory Means Business Risk

The team was acutely aware that lack of comprehensive insight into AD put the company at risk.

"We needed to improve the resilience of our Active Directory to warranty the availability of the entire information system of the company," Tacchini explains. "But the tools we had did not allow us to have the proper level of control over the system. We were not confident in our ability to determine if we were exposed to a serious security threat."

The risk to security and cyber resilience was increasingly serious. "We had identified more than 20,000 issues within our Active Directory, and we were aware that the situation was worsening," Tacchini said.

To address the problem, Edison and Microsys considered solutions from Quest, Semperis and Tenable. After careful evaluation, they chose SpecterOps' BloodHound Enterprise for advanced Attack Path Management, and Quest's Change Auditor and On Demand Audit for auditing and change management across the hybrid IT ecosystem.

In particular, the Quest solutions paired with BloodHound Enterprise deliver the powerful combination of Attack Path Management and Attack Path Monitoring.

> **"We were already using BloodHound in red teaming activities and we knew that it was the right choice from an offensive point of view.**
>
> **So, the Quest integration with BloodHound was another big advantage, BloodHound Enterprise enables us to visualize attack paths and understand the choke points, and the Quest auditing tools allow us to continuously monitor all attack paths we have not yet addressed."**
>
> **Francesco Contardi**
> Project Manager of the Active Directory resilience program at Edison

BloodHound Enterprise Provides Insight into Attack Paths, Choke Points and Tier Zero Assets

SpecterOps' BloodHound Enterprise provided far deeper insight into attack path management than Edison and Microsys had been able to glean with their previous tools. While the team had already identified some weaknesses in AD, they were surprised at the number and types of issues that were posing a risk.

"BloodHound Enterprise highlighted a wide variety of vulnerabilities in our Active Directory," Contardi said. "In addition, it has helped us further map out our Tier Zero assets to inform our AD restructuring initiative. It is very helpful indeed."

SpecterOps' BloodHound Enterprise also delivers visibility not only into the security weaknesses in AD but how to remediate them.

"The graph analysis in BloodHound Enterprise is extremely valuable because it highlights the choke points where we can intervene to reduce the risk most efficiently," Contardi explains. "From a technical point of view, it was quite complex because we had to communicate the misconfiguration or other issue to all the different teams and get them all on board to fix the problem. Having better visibility enabled us to do it easier and faster."

Change Auditor and On Demand Audit provide attack path monitoring as part of broader activity auditing and change management. With Change Auditor and On Demand Audit, Edison can effectively monitor the attack paths they have identified but have not yet been able to mitigate.

"From an organic point of view, remediation is complicated because of possible impacts on the teams, applications, teams and other factors involved. We need to be sure that any change that we apply does not fix one problem only to generate two new ones," Contardi said.

More broadly, these integrated solutions pinpoint suspicious activity across the hybrid IT ecosystem and provide advanced alerting and search capabilities to speed investigation and informed response.

With the right tools and partners, Edison was able to achieve the next step in their plan for cyber resilience, untangling their AD environment and setting themselves on the path to remediation and proactive security measures.

Learn more at specterops.io/get-a-demo ›

BloodHound Enterprise Provides

- **Continuous attack path mapping**
- **Attack path choke point prioritization**
- **Real-world remediation guidance**
- **Continuous security posture measurement**