# 政府机构加强网络安全。

州运输局在复杂的 Active Directory 中发现并关闭了攻击路径。

## 运输局

国家/地区： **美国**

员工数： **2,500**

行业： **政府**

## 找出并消除攻击路径对于保障安全性和合规性至关重要。

与私营部门一样，政府机构正面临大量日益复杂的网络攻击。遗憾的是，由于长期使用的旧式系统非常复杂，建立有效安全策略的任务变得越发艰难。美国一个州的运输局还面临另一挑战：疫情之后的退休潮导致经验丰富的 IT 专业人员流失。因此，IT 团队敏锐意识到，他们对 IT 环境中潜藏的风险“一无所知”。

此运输局转而向长期合作伙伴 Quest 寻求协助，了解如何使用 SpecterOps BloodHound Enterprise 管理攻击路径。利用这一解决方案，该机构发现了可能被用来入侵 Active Directory 的攻击路径、确定了有效的补救措施，重要的是，向其业务部门直观、清晰地证明风险得以降低，从而很快赢得他们对所需变更的支持。

## 关于此案例研究

在一个州运输局，疫情之后的退休潮意味着将失去大量经验丰富的 IT 专业人员。他们应用多年的 Active Directory 的复杂性充分说明了一个事实：IT 团队对未知领域一无所知，而这些未知领域使得安全性、业务连续性和合规性都处于风险之中。

### 解决方案

依托 SpecterOps BloodHound Enterprise，IT 团队得以快速洞悉 Active Directory 中的攻击路径；攻击者可能会利用这些路径存取宝贵的系统与数据，甚至完全控制整个域。通过清晰可视化这些攻击路径，他们可轻松说服其业务部门，告知这些部门急需删除某些权限，或限制特定访问权限。因此，该运输局得以显著提升其网络安全和合规性。

### 优势

- 识别攻击者可能用来控制 IT 环境的攻击路径
- 绘制出每种关系和联系，以确定有效的补救措施
- 向业务利益相关者清楚说明这些攻击路径，以获得他们对补救措施的支持
- 减轻因员工退休而缺乏经验知识给 IT 团队造成的压力

### 解决方案一览

- Microsoft 平台管理

此外，IT 团队使用 Quest Change Auditor 监控尚未得到消除的攻击路径，同时使用 Quest Recovery Manager for Active Directory 让他们确信可以恢复对特定 AD 对象所作的不必要更改，甚至还原整个林。因此，该运输局显著提升了网络安全性和合规性。

## Active Directory 中的未知漏洞会造成严重风险。

Active Directory 堪称该运输局运营的核心所在，提供重要的身份验证和授权服务，让用户能登录并访问开展工作所需的资源。但是，与其他身份管理系统一样，Active Directory 也很复杂，因此随着时间的推移，它会变得极其错综复杂。

因此，用户最终可能拥有自己不再需要的访问权限，恶意行为者可能趁机接管过时的对象，并且很难确定数十或数百个组策略对象 (GPO) 的实际影响，尤其是许多富有经验的 IT 团队成员退休，而其接任者对系统和流程的演变缺乏深入了解时。

## 每位用户目前拥有哪些权限？他们可轻松获取哪些访问权限？

IT 团队了解这些风险并开始实施相关策略，以强制实施最低权限原则，向每位用户精准授予开展工作所需的访问权限 — 不多也不少。运输局信息系统管理员解释说：“我们会为每位新用户创建一个 Active Directory 帐户。在这里工作期间，用户可能会调任三四个不同的职位。很多时候，即使他们不再需要旧权限，也会一直保留有这些权限。此外，在过去，大多数用户都获授其计算机的本地管理员权限，而这会带来不必要的风险。因此，我们的首要目标是撤销过多的权限并强制实施最低权限。”

然而，仅仅了解每位用户当前拥有哪些权限并不够；了解他们可利用已有权限来获得哪些权限同样至关重要。换言之，几乎任何正在使用的 Active Directory 都存在固有的复杂漏洞，这些漏洞为入侵普通用户帐户的攻击者创造了机会，即提供了攻击路径，让他们能快速升级权限并控制 Active Directory。

> **“尽管我们先前努力撤销了所有用户的本地管理员权限，但 BloodHound Enterprise 仍发现了大量用户的所属组是本地计算机管理员组的成员。”**
>
> *州运输局信息系统管理员*

## 如果没有合适的工具，最低权限是一项难以实现的目标。

最初，运输局的 IT 团队使用了 Microsoft 安全评估工具 (MSAT)，以期更深入地洞悉其 IT 基础架构的安全状态。然而，他们发现这款工具无法针对他们的特定环境提供有用的洞见和补救指导。运输局信息系统管理员强调说：“Microsoft 安全评估工具的输出数据过于模糊，难以理解，因此我们经常无法确定当中提出了哪些更改。而且，即便我们获得了清晰的建议，我们还会担心更改可能对我们用户及我们自己业务流程产生什么影响。您必须小心谨慎，准确了解自己所执行的操作，以免引发严重问题。”

> **“我们对未知领域一无所知。当 BloodHound Enterprise 将攻击路径铺开在您眼前，我们会感叹，天哪，我从来没有意识到我们这么易受攻击。”**
>
> *州运输局信息系统管理员*

然后，IT 团队执行了 Quest Active Directory Security Assessment，并在过程中使用了 SpecterOps BloodHound Enterprise。非常简单，令人惊讶！信息系统管理员表示：“在试用 BloodHound 之后，我们才知道自己非常容易受到攻击。BloodHound 向我们展示了 Active Directory 中嵌套的安全组。哇哦，我们竟然没意识到所有这些组还是其他组的成员。事实上，尽管我们先前努力撤销了所有用户的本地管理员权限，但 BloodHound Enterprise 仍发现了大量用户的所属组是本地计算机管理员组的成员。”

实际上，BloodHound Enterprise 甚至发现了 IT 团队以前不知道的 Tier Zero 资产。信息系统管理员回忆道：“我对发现 Tier Zero 资产感到非常惊讶。我们对未知领域一无所知。当 BloodHound Enterprise 将攻击路径铺开在您眼前，我们会感叹，天哪，我从来没有意识到我们这么易受攻击。我们已经采取大量出色的防御措施和最佳实践，却仍有如此多的攻击路径。”

## BloodHound Enterprise 明确了消除攻击路径的关卡点，并且提供了赢得业务部用户支持所需的清晰洞见。

此外，与 Microsoft 安全评估工具 (MSAT) 不同的是，BloodHound Enterprise 可以为 IT 团队提供切实可行的所需洞见，让他们能采取相应的措施来消除 Active Directory 中的攻击路径。信息系统管理员解释道：“在缓减风险方面，最棘手的部分实际上是沟通，要让业务部用户了解为什么需要作出更改。我们不能无缘无故就撤销他们的权限。BloodHound Enterprise 让我们可以清晰显示 Active Directory 中的攻击路径，从而让业务部用户能亲眼了解删除某些权限的紧迫性。”

因此，IT 团队能够快速获得受影响用户组的支持，包括应用程序开发人员、CAD 支持团队及其他用户组的支持。信息系统管理员说：“BloodHound Enterprise 的可视化功能为我们节省了大量时间。此言不虚，因为倘若我们没有这些视觉资料展示给业务部用户，必定会有诸多问题，我将不得不安排紧锣密鼓的会议来解决问题。”

事实上，BloodHound Enterprise 让整个过程变得非常简单，这让 IT 团队赞叹不已。信息系统管理员表示：“我们只需输入组名称，便能在一个展示所有攻击路径的视觉地图中看到组会接触的一切，就像一个庞大的蜘蛛网。然后我们只需单击即可进行深入探索。此功能可谓是无价之宝，我可以准确展示攻击者如何获得关键资产的访问权限。对此您无可否认；它就清楚地展示在您面前。团队看到路径并了解风险后，就会接受我们需要采取的缓减措施。”

> **“在缓减风险方面，最棘手的部分实际上是沟通，要让业务部用户了解为什么需要作出更改。BloodHound Enterprise 让我们可以清晰显示 Active Directory 中的攻击路径，从而让业务部用户能亲眼了解删除某些权限的紧迫性。这为我们节省了大量时间。”**
>
> *州运输局信息系统管理员*

## 只需做小小的正确改变，便可产生深远的影响。

IT 团队深知缓减风险是一个永无止境的过程，因为 IT 生态环境在不断改变。但有一点他们很放心，即他们知道，在加强网络安全方面，他们每一天都取得了可衡量的重大进展。信息系统管理员强调道：“BloodHound Enterprise 让我们能清晰地看到可一次切断整组攻击路径的关卡点。这非常令人兴奋，因为我们作出更改后，能够在可视化图示中看到其通过减少攻击路径数量所带来的确切影响。我们可以用可量化的方式跟踪我们所采取的措施，并向管理团队证明投资的价值。”

这些重大改进大大减轻了 IT 团队成员的压力。信息系统管理员解释说：“以前，我们对未知领域一无所知。现在，BloodHound 让我们掌握了所需知识。这让我充满信心，我回家时可以说，‘你知道吗？我们今天有所改进。我们阻断了更多可能被用来入侵我们 Tier Zero 资产的攻击路径。’我对自己的工作感到自豪，我回家时可以说我们今天取得了很多成果。”

> BloodHound Enterprise 让我们能清晰地看到可一次切断整组攻击路径的关卡点。我们可以用可量化的方式跟踪我们所采取的措施，并向管理团队证明投资的价值。

*州运输局信息系统管理员*

## 产品

- Quest Active Directory Security Assessment
- SpecterOps BloodHound Enterprise
- Change Auditor
- Recovery Manager for Active Directory

## Quest 不仅能够增强网络安全，还能提升网络抗风险能力。

运输局深知，虽然识别并消除攻击路径至关重要，但它只是大型网络抗风险策略的其中一部分。相应地，他们不仅依赖 BloodHound Enterprise，也依赖其他 Quest 解决方案。Quest Change Auditor 提供针对所有关键用户活动和管理员更改的实时威胁监控和安全跟踪。事实上，Change Auditor 在监控组织已识别但尚未消除的攻击路径方面发挥着重要作用，IT 团队渴望实现这个强大又灵活的解决方案的全部价值。

当然，组织还需要做好准备以防灾难发生。部署 Quest Recovery Manager for Active Directory 后，vAD 灾难不会发展成业务灾难，这让运输局的 IT 团队感到安心。该解决方案将 AD 林恢复时间从数天或数周缩短为短短数小时。

这些解决方案与 BloodHound Enterprise 完美互补，有助运输局同时增强网络安全和网络抗风险能力。

## 关于 Quest

Quest 致力打造软件解决方案，在日益复杂的 IT 环境中带来新技术的优势。从数据库和系统管理到 Active Directory 和 Microsoft 365 迁移和管理，以及网络抗风险能力，Quest 都可帮助客户在当下解决其面临的下一个 IT 挑战。Quest Software。Where Next Meets Now.