Tenable Identity Exposure 主要功能指南

上次修订时间：2025 年 7 月 2 日

目录

欢迎使用 Tenable Identity Exposure 主要功能指南

欢迎使用 Tenable Identity Exposure(之前称为 Tenable AD) 。本文档旨在通过全面概述产品的特性和功能来提升您的体验，无论您是在本地部署还是通过 SAAS 部署。此资源旨在为您提供帮助，无论您是寻求指导的新用户，还是希望加深理解的经验丰富的用户。

本文档由多个部分组成，涉及一系列可供探索的主题，包括优化产品使用以及管理攻击指标和风险暴露指标。请注意，尽管本文档提供了宝贵的见解，但其中的内容从严格意义而言并不能构成 Tenable Identity Exposure 使用手册。相反，本文档旨在提供各种建议，以便您可以顺畅、有效地利用此平台。

关于本指南

本指南以 **Tenable Identity Exposure SaaS 用户指南**为基础，您可以查阅该指南以了解详细信息。

本指南中的示例旨在重点介绍 Tenable Identity Exposure 的功能，并未列出详尽的功能清单，并且可能无法直接应用至每个独特的环境。对于最佳安全措施，建议您访问我们的官方文档或联系专业服务团队，以获取更多详细信息和指导。

主要利益相关者

Tenable Identity Exposure 中的各个利益相关者因贵组织的规模、结构、安全策略和预期用例而异。明确每个利益相关者的角色和权限有助于有效采用和利用产品。

使用 Tenable Identity Exposure 时，了解所涉及的不同利益相关者至关重要。这些个人和组在识别、缓解和报告基于身份的安全风险方面担任不同的角色。综合细分如下：

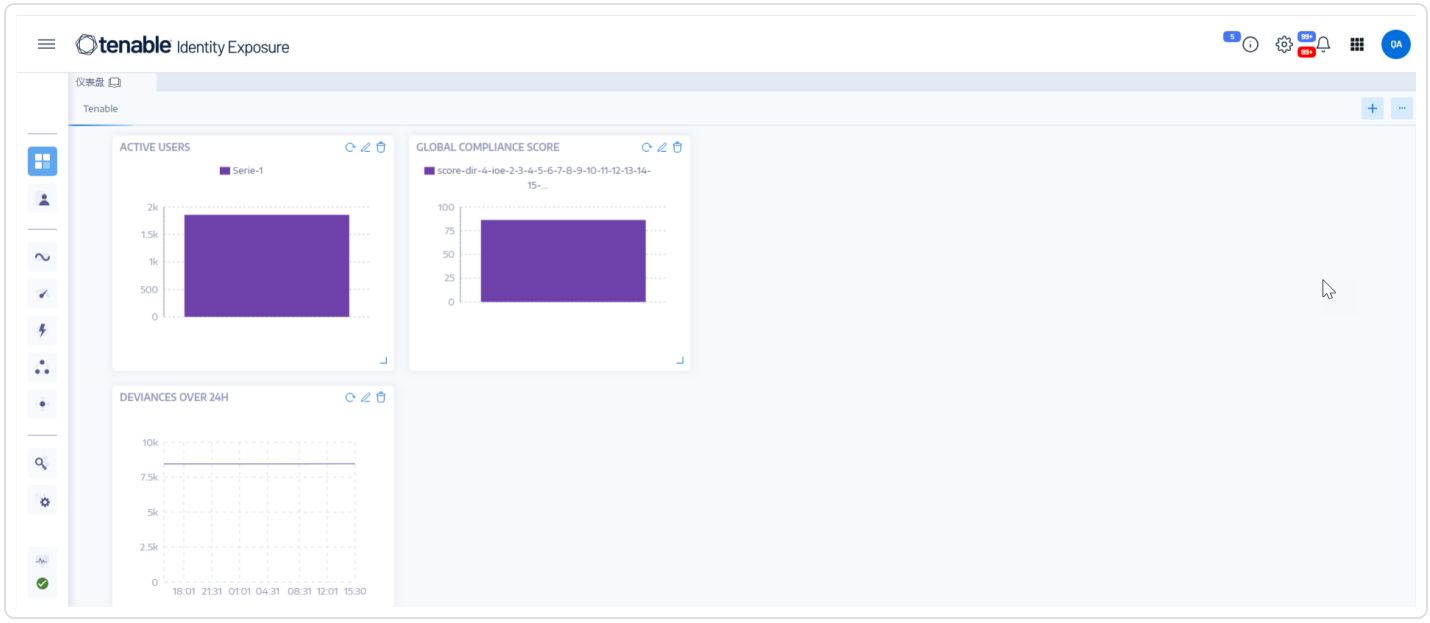
- **安全团队**：监督和管理 Tenable 解决方案，利用数据分析识别漏洞和风险并做出及时响应。
- **IT 运营团队**：为 Tenable 解决方案提供基础架构和集成支持，同时确保与其他安全工具和用户目录的顺畅连接。
- **应用程序开发团队**：负责确保应用程序安全并及时解决 Tenable 标记的已暴露的身份。
- **身份和访问管理** (IAM) 团队：管理用户帐户、权限和访问控制，与 IT 安全团队密切协作以解决 Tenable Identity Exposure 指出的问题。

- **业务部门负责人**:对团队和应用程序的安全状况负最终责任。他们会审查报告、确定风险缓解策略的优先级、分配资源,以增强 Active Directory 安全措施。

仪表盘

仪表盘允许将影响 Active Directory 安全性的数据和趋势可视化。可以使用小组件对其进行定制，以便根据个人要求显示图表和计数器。

Tenable Identity Exposure 仪表盘起着实时命令中心的作用，旨在确保贵组织的 Active Directory (AD) 安全。它不仅提供身份环境的全面概述（例如，实时、集中式视图），突出显示严重漏洞，查明潜在攻击向量，还能实现主动风险缓解。



仪表盘主要功能

- **一目了然的概述**：借助突出显示的合规性分数、主要风险和用户活动趋势等关键指标，快速了解安全状态。
- **深入了解详细信息**：利用按严重性、用户类别和其他相关条件对风险因素细分的交互式小组件，更深入地了解特定区域。
- **可定制的重点项**：使用预先构建的模板或制作专属布局，根据您确定的优先级创建个性化的仪表盘。例如，针对导致以下 IoE 经常重复出现的常见错误配置创建仪表盘：

    - 确保 SDProp 一致性
    - 由非法用户管理的域控制器
    - 存在风险的 Kerberos 委派
- **实时监控**：借助持续更新和警报，随时了解新出现的威胁和可疑活动。
- **切实可行的见解**：获得按优先顺序排列的实用修复建议，排列依据为严重性和潜在影响。

另请参阅：

- 仪表盘
- 关于仪表盘的视频教程

跟踪事件流

Tenable Identity Exposure 的“跟踪事件流”显示影响 AD 基础设施的事件的实时监控和分析。它允许您识别严重漏洞及其建议的修复过程。

可以使用“**跟踪事件流**”页面，返回到过去并加载以前的事件或搜索特定事件。还可以使用此页面顶部的搜索框搜索威胁和检测恶意模式。

“跟踪事件流”会跟踪以下事件：

- **用户和组更改**：包括帐户与组的创建、删除和修改。
- **权限变更**：包含对文件、文件夹和打印机等对象的访问控制的修改。
- **系统配置调整**：涉及变更组策略对象 (GPO) 及其他关键设置。
- **可疑活动**：包含未经授权的尝试、特权提升及其他引发危险信号的事件。

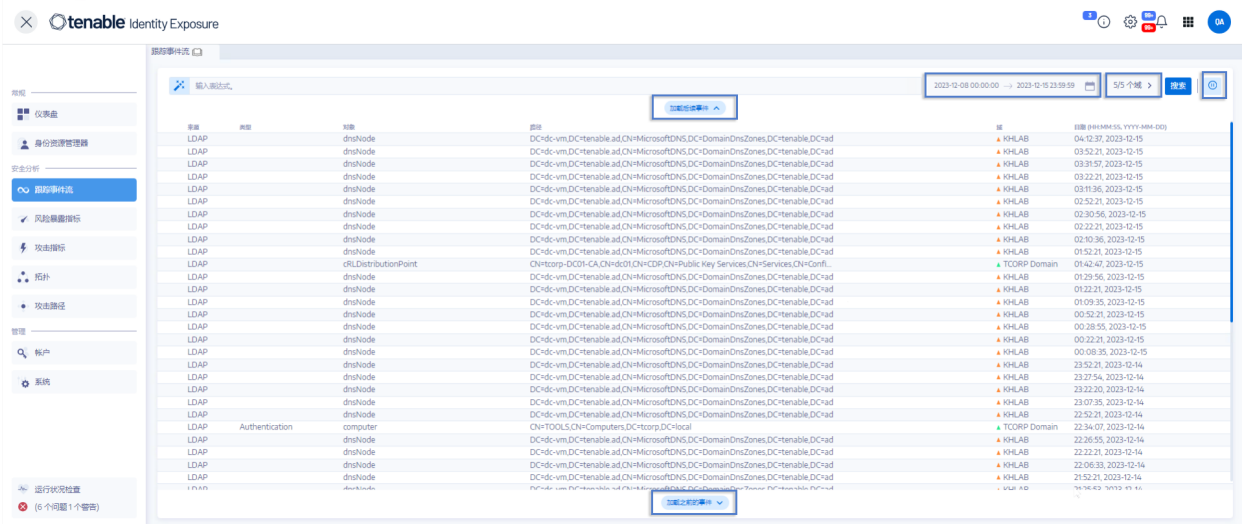
Tenable Identity Exposure 提供以下功能以利用跟踪事件流数据：

- **可搜索和可筛选**：通过使用关键词或特定条件轻松导航事件流，使重点集中在相关活动上，同时最大限度地减少无关信息的干扰。
- **详细的事件信息**：每个事件条目都提供详尽的详细信息，包括受影响的对象、负责变更的用户、使用的协议以及相关的风险暴露指标 (IoE)。
- **关系可视化**：展示事件之间的关系，阐明看似无关的活动如何促成更广泛的攻击活动。

若要访问“跟踪事件流”，请执行以下步骤：

- 在 Tenable Identity Exposure 中，点击左侧导航栏中的“**跟踪事件流**”。

  “跟踪事件流”页面随即打开，其中包含事件列表。有关更多信息，请参阅“Trail Flow Table”。



若要选择时间范围，请执行以下操作：

若要选择域，请执行以下操作：

若要查看事件，请执行以下操作：

若要暂停和重新启动“跟踪事件流”，请执行以下操作：

若要加载后面的或以前的事件，请执行以下操作：

在“跟踪事件流”中，数据如何显示？

1. 当您在 Active Directory (AD) 界面中执行以下操作时：
    - 创建新的用户帐户
    - 修改用户的组成员身份
    - 重置密码
    - 禁用帐户
    - 启用帐户
    - 删除帐户

- 移动对象
- 修改权限

2. Active Directory (AD) 会自动生成事件日志条目，以捕获操作的详细信息，包括：
    - 时间戳
    - 执行操作的管理员
    - 受影响的对象
    - 具体的更改
3. Tenable Identity Exposure 会持续收集和分析这些事件日志、关联事件、识别模式以及检测异常。
4. “跟踪事件流”页面会直观呈现操作流及其影响：
    - 时间线：显示按时间顺序排列的事件，并突出显示最近的操作。
    - 对象详细信息：提供受影响对象的具体信息，包括其属性和关系。
    - 变更历史记录：显示对象被修改的历史记录，包括当前操作。
    - 风险见解：识别与操作相关的潜在风险，例如过多权限或敏感组中的成员资格。
    - 合规性信息：表示与操作相关的任何违规行为。

另请参阅：

- 跟踪事件流 概述
- Trail Flow Use Cases
- 跟踪事件流视频教程

报告中心

Tenable Identity Exposure 中的**报告中心**拥有一个强大功能，可让您以报告形式向组织中的关键利益相关者导出重要数据。报告中心提供一种从预定义列表创建报告的方法，以确保过程高效且简化。

报告中心提供以下功能：

- **精细筛选**：使用基于日期范围、域、攻击指标 (IoA)、风险暴露指标 (IoE) 等内容的精细筛选条件来优化报告，确保获得精准的见解。
- **自动交付**：安排报告按所需时间间隔自动生成和交付，从而简化安全监控和报告流程。
- **灵活导出**：导出多种格式的报告，如 CSV，以便进一步分析、使用报告访问密钥共享或与现有报告工作流集成。

管理员可为不同的用户创建不同类型的报告，并灵活设置报告的时间范围，最长可以设置为一个季度。从 Tenable Identity Exposure 共享重要身份数据的能力增强了该组织主动缓解风险的能力以及识别基于身份的潜在攻击的能力。

如要下载报告，用户会收到一封电子邮件，其中包含页面的 URL，用户可在其中输入从管理员处收到的报告访问密钥。报告的下载期限为 30 天，过期后 Tenable Identity Exposure 将删除这些报告。用户必须尽快下载报告，因为 Tenable Identity Exposure 会针对指定的时间范围生成新的报告并覆盖旧报告。

若要访问报告中心，请执行以下操作：

1. 在 Tenable Identity Exposure 中，选择“**系统**”>“**配置**”。
2. 在“**报告**”下，点击“**报告中心**”。

   此时会打开一个窗格，其中包含已配置报告及其相关信息的列表，例如报告名称、类型、域、配置文件、时段、重复周期和收件人电子邮件。

另请参阅：

- 报告中心
- Set Permissions for a Role

风险暴露指标

Tenable Identity Exposure 通过风险暴露指标 (IoE) 衡量 AD 基础设施的安全成熟度，并为监控和分析的事件流分配严重程度。Tenable Identity Exposure 在检测到安全回退时触发警报。

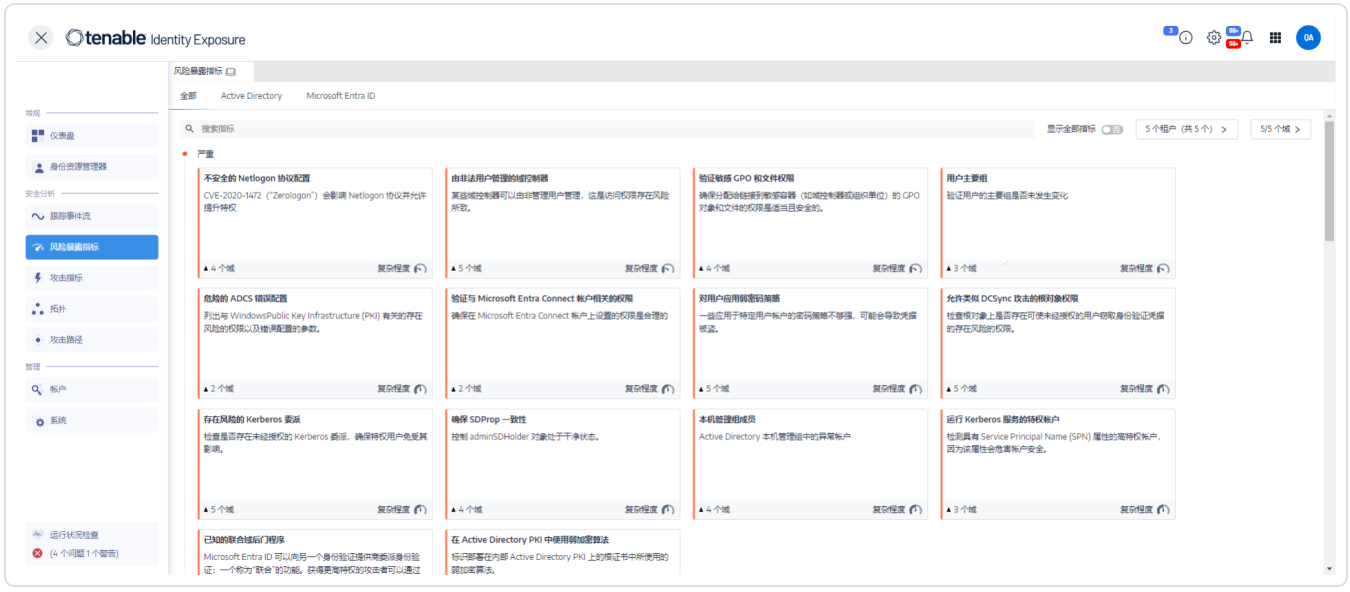
这些 IoE 均经过预先配置，并且任何偏离既定规范的情况都会触发相应警报。

若要显示 IoE，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击导航窗格中的“**风险暴露指标**”。

   此时会打开“**风险暴露指标**”窗格。默认情况下，Tenable Identity Exposure 仅显示包含异常行为的 IoE。

2. （可选）要显示所有 IoE，点击以将“**显示全部指标**”开关切换为“**是**”。



Tenable Identity Exposure IoE 附带一系列旨在提升您调查能力的功能：

- **搜索和筛选**：根据林和域应用筛选条件，轻松探索 IoE。
- **导出功能**：异常对象允许以 CSV 格式导出 IoE。
- **对 IoE 事件采取操作**：从白名单中删除风险暴露项/重新启用。

IoE 的数据包括：

- **"信息"部分**:此部分提供每个风险暴露指标 (IoE) 的执行概述,包括已知的攻击工具、受影响的域以及相关文档。
- **漏洞详细信息**:此部分提供有关 Active Directory 中的错误配置的更深入信息。
- **异常对象**:此部分重点介绍 Active Directory 中可能导致攻击面扩大的错误配置。
- **建议**:此部分指导您通过有效的配置策略来尽可能缩小攻击面。

严重程度

严重程度允许评估检测到的漏洞的严重程度,并确定修复措施的优先级。

"**风险暴露指标**"窗格按照如下方式显示 IoE:

- 使用颜色代码按严重程度显示。
- 垂直方向:从最严重到最不严重(红色表示优先级最高,蓝色表示优先级最低)。
- 水平方向:从最复杂到最不复杂。Tenable Identity Exposure 可动态计算复杂程度指标,以指示修复异常 IoE 的难易程度。

严重程度	描述
严重:红色	显示如何防止某些非特权用户对 Active Directory 的攻击和危害。
高危:橙色	处理后渗透利用技术攻击(导致凭据窃取或安全绕过),或者处理需要链接才能带来危险的渗透利用技术。
中危 - 黄色	表示 Active Directory 基础设施的风险有限。
低危 - 蓝色	显示良好的安全实践。某些业务环境可能会导致低影响异常行为,但不一定影响会 AD 安全。仅当管理员做出错误行为(例如激活不活动帐户)时,这些异常行为才会对 AD 产生影响。

修复的优先级

您可以为系统识别的高危 IoE 确定修复工作的优先级。此外,您可以在重要程度类别中使用 IoE 风险量表进一步确定优先级。

如果您认为根据贵组织的权限或运营要求，应该监控 IoE，则可以将其加入允许列表。

用例

以下用例侧重于名为“密码永不过期的帐户”的 IoE。

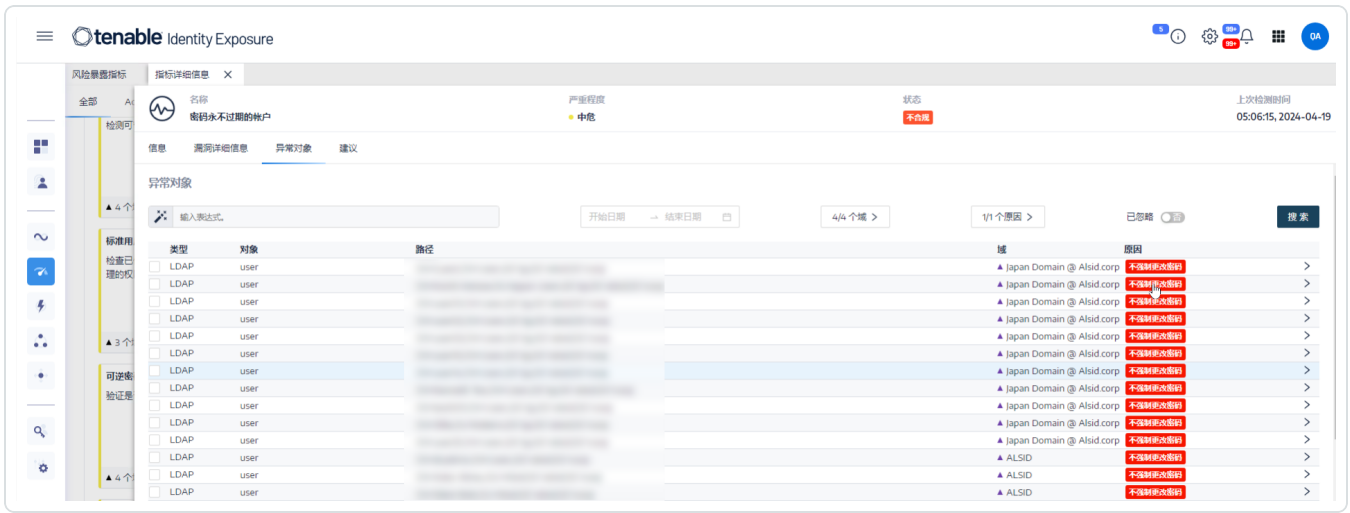
1. 被 Tenable Identity Exposure 标记后，IoE 会显示在“风险暴露指标”窗格中：

2. 要获取有关 IoE 的更多见解，请单击 IoE 以访问更多详细信息。在信息页面中，您会发现包含简明概述的执行摘要、与 IoE 相关的潜在攻击工具的详细信息、受影响的域以及相关文档，这些内容可以帮助您了解并有效解决问题。

3. 

4. 有关 IoE 的更多详细信息，请单击“漏洞详细信息”选项卡。

5. 要验证哪些帐户启用了“密码永不过期的帐户”设置，请单击“异常对象”。然后，您便可以访问系统中拥有此配置的帐户列表。



6. 单击异常对象可查看 IoE 标记了的帐户。

7. 请咨询 Active Directory 管理员，以了解受影响的帐户为何启用“密码永不过期的帐户”选项。
8. 根据响应，您可以选择将帐户列入白名单，或协助 Active Directory 管理员提出解决问题的建议。
9. 有关建议，您可以参阅 IoE 的建议部分。

10. 如果帐户出现异常或已知帐户按预期运行，您可以忽略 IoE，方法是导航至“**异常对象**”>“选择相应异常”>“根据要求**忽略**所选对象或停止忽略所选对象”。

另请参阅：

- Indicators of Exposure
- 风险暴露指标视频教程
- Customize an Indicator

攻击指标

Tenable Identity Exposure 攻击指标 (IoA) 可帮助贵组织检测尝试通过最先进的漏洞利用技术入侵 Active Directory (AD) 基础设施的行为，并立即采取相应措施，包括：

- **三大事件**：我们以统一方式呈现 IoA，并在单个界面中显示实时时间线、影响 AD 的三大事件以及攻击的分布情况。
- **IoA 详细信息**：在 Tenable Identity Exposure 中，IoA 面板可提供 AD 中已发生的攻击的信息。
- **涉及 IoA 的事件**：IoA 事件列表可提供针对 AD 发起的特定攻击的全面详细信息。利用这些信息，您可以根据 IoA 的严重性做出适当响应。

攻击指标附带一系列旨在提升您调查能力的功能：

- **搜索和筛选**：利用时间线轻松探索 IoA，或根据林、域和重要程度应用筛选条件，以高效获得有针对性的结果。
- **导出功能**：允许以 PDF、CSV 或 PPTX 格式导出 IoA 数据。
- **修改图表类型**：提供更改图表类型的选项，可让您查看攻击严重性的分布情况或 3 大高频攻击及其各自的发生次数。
- **对 IoA 事件采取操作**：允许您选择要关闭或重新打开的事件。

严重程度

Tenable Identity Exposure 检测攻击并为其分配严重程度：

等级	描述
严重 - 红色	检测到经证实的后渗透利用攻击，攻击者需要先控制域才能实施该攻击。
高危 - 橙色	检测到允许攻击者控制域的重大攻击。
中危 - 黄色	IoA 与可导致危险的特权提升或允许访问敏感资源的攻击有关。
低危 - 蓝色	通过警报提醒存在与侦察操作或低影响事件相关的可疑行为。

修复的优先级

识别影响较大且与您的特定安全风险和关注点一致的关键 IoA。

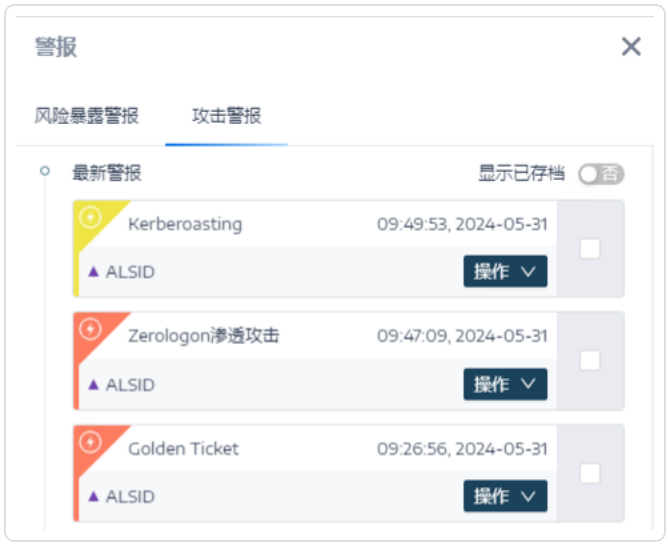
要降低误报风险或忽略合法攻击，根据您的环境校准 IoA 至关重要。要求如下：

- 调整阈值：校准 IoA 敏感度可减少误报，从而确保警报有意义且可操作。
- 将帐户和活动列入白名单：防止合法活动触发 IoA，从而提高警报的准确性并简化调查。
- 关联 IoA：分析不同 IoA 之间的关系，确定更广泛的攻击模式。

提示：要获取有关选项和推荐值的更多详细信息，请参阅 Tenable Identity Exposure 攻击指标参考指南（网址：https://zh-cn.tenable.com/downloads/identity-exposure）。将这些选项和值应用至安全配置文件中的每个 IoA。

用例

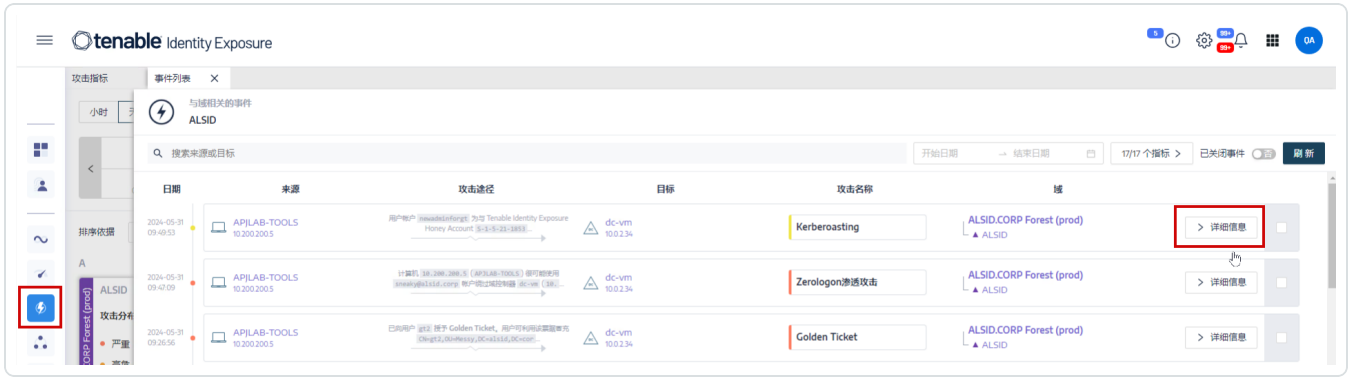
1. 激活 IoA 后，选择导航窗格中的“攻击指标”或单击主页右上角的铃铛图标。



2. 每个指标都会为您提供有关事件的详细信息，供您在查看后采取适当的操作：
    - 攻击发生的时间
    - 攻击描述
    - 攻击来源
    - 攻击目标

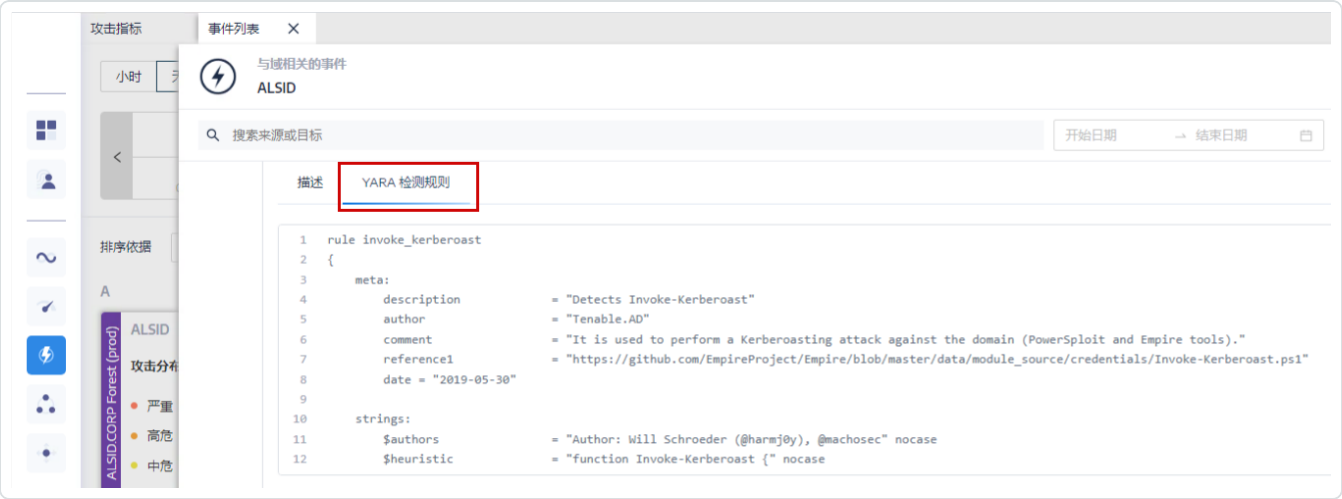
- MITRE ATT&CK® 信息
- YARA 检测规则
- 其他资源

3. 选择“详细信息”以访问“描述”(如此例中所示),并重点关注“本地管理员枚举”。



4. “描述”选项卡提供有关针对 Active Directory (AD) 发起的特定攻击的信息。

5. “YARA 检测规则”选项卡提供有关 YARA 规则的信息,Tenable Identity Exposure 利用这些规则来检测网络级别的 Active Directory 攻击、增强 Tenable Identity Exposure 的整体检测功能。



6. 与 Active Directory 管理员或相关利益相关者协作检查和解决事件，决定是关闭还是重新打开事件，并采取措施防止其再次发生。
7. 如果是经过识别或获得授权的攻击，您可以相应地选择自定义 IoA，以防 IoA 在未来的实例中对其进行标记。

另请参阅：

- Indicators of Attack
- Customize an Indicator
- 攻击指标视频教程

Microsoft Entra ID 支持

除了 Active Directory 之外，Tenable Identity Exposure 还支持 Microsoft Entra ID（原名 Azure AD 或 AAD）以扩展组织中的标识范围。此功能利用专注于 Microsoft Entra ID 特定风险的新风险暴露指标。

若要将 Microsoft Entra ID 与 Tenable Identity Exposure 集成，请严格遵循指导流程：

1. 拥有 先决条件
2. 检查 权限
3. 检查 网络流
4. 配置 Microsoft Entra ID 设置
5. 激活 Microsoft Entra ID 支持
6. 启用租户扫描

先决条件

需要 Tenable Cloud 帐户才能登录“cloud.tenable.com”并使用 Microsoft Entra ID 支持功能。此 Tenable Cloud 帐户就是您接收欢迎电子邮件时所使用的同一电子邮件地址。如果您不知道“cloud.tenable.com”的电子邮件地址，请联系支持部门。所有拥有有效许可证（无论是本地部署还是 SaaS 版）的客户都可以通过 cloud.tenable.com 访问 Tenable Cloud。此帐户可让您为 Microsoft Entra ID 配置 Tenable 扫描并收集扫描结果。

注意：无需有效的 **Tenable Vulnerability Management** 许可证即可访问 Tenable Cloud。有当前有效的独立 Tenable Identity Exposure 许可证（无论是本地部署还是 SaaS 版）就足够了。

注意：Tenable Identity Exposure **不支持在国家云中使用 Microsoft Entra ID**，包括中国和美国政府专用区域。Microsoft Entra ID 提供的国家云是物理上独立的 Azure 实例，专为满足特定的法规与合规性需求而设计。Tenable Identity Exposure 仅支持全局 Microsoft Entra ID 环境，不包括中国国家云和美国政府国家云。有关 Microsoft Entra ID 国家云的更多信息，请参阅 Microsoft Entra 身份验证和国家云 - Microsoft 标识平台。

权限

Microsoft Entra ID 支持功能需要从 Microsoft Entra ID 收集数据，例如用户、组、应用程序、服务主体、角色、权限、策略、日志等。它使用 Microsoft Graph API 和遵循 Microsoft 建议的服务主体凭据收集此数据。

- 根据 Microsoft 的要求，您必须以**有权在租户范围内授予对 Microsoft Graph 的管理员同意**的用户身份登录到 Microsoft Entra ID，该身份必须具有全局管理员或特权角色管理员角色(或具有相应权限的任何自定义角色)。
- 如要访问 Microsoft Entra ID 的配置和数据可视化，您的 **Tenable Identity Exposure 用户角色**必须具有相应的权限。有关更多信息，请参阅“Set Permissions for a Role”。

网络流

允许端口 443 上的以下地址从安全引擎节点服务器出站，以激活 Entra ID 支持：

- sensor.cloud.tenable.com
- cloud.tenable.com

许可证计数

只有在启用 Tenable 云同步功能时，Tenable 才不会将重复的身份计入许可数量。如果未启用此功能，则系统无法匹配来自 Microsoft Entra ID 和 Active Directory 的帐户，导致每个帐户被分别计数。

- **未启用 Tenable 云同步**：一个同时拥有 AD 帐户和 Entra ID 帐户的用户将被视为两个独立用户，并分别计入许可数量。
- **启用 Tenable Cloud 同步**：系统会将多个帐户合并为一个身份，确保拥有多个帐户的用户仅被计为一个身份。

配置 Microsoft Entra ID 设置

通过以下过程(改编自 Microsoft 《快速入门：向 Microsoft 标识平台注册应用程序》文档)，在 Microsoft Entra ID 中配置所有必需的设置。

1. **创建应用程序：**

   a. 在 Azure 管理员门户中，打开“应用程序注册”页面。

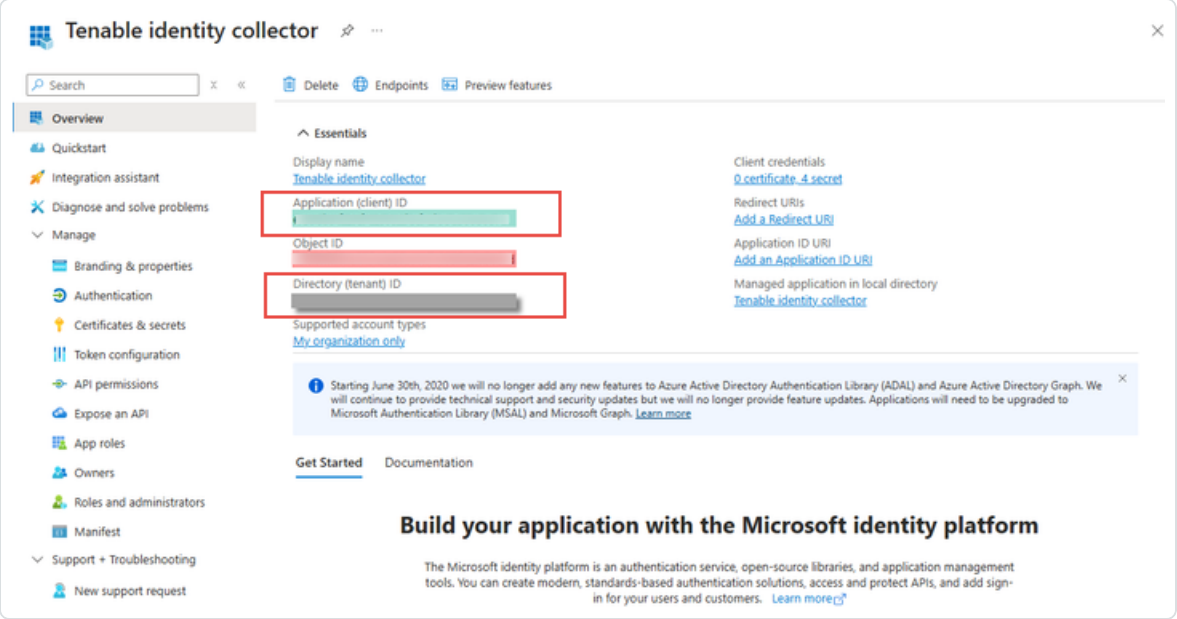
   b. 点击“**+ 新注册**”。

   c. 为应用程序命名（示例：“Tenable Identity Collector”）。对于其他选项，您可以保留默认值。

   d. 点击“**注册**”。

   e. 在此新创建应用程序的“概述”页面上，记录“应用程序（客户端）ID”和“目录（租户）ID”，您稍后需要在步骤 如要添加新的 Microsoft Entra ID 租户，请执行以下操作： 中使用这些 ID

   > **注意**：务必选择**应用程序 ID 而非对象 ID**，以便配置生效。



2. **向应用程序添加凭据：**

   a. 在 Azure 管理员门户中，打开“应用程序注册”页面。

   b. 点击已您创建的应用程序。

   c. 在左侧菜单中，点击“**证书和密钥**”。

d. 点击“**+ 新客户端密钥**”。

e. 在“**描述**”框中，为此密钥指定一个实用名称和一个符合您策略的“**到期**”值。请记住在接近到期日时更新此密钥。

f. 请将密钥值保存在安全位置，因为 Azure 只会显示一次，如果丢失，必须重新创建。

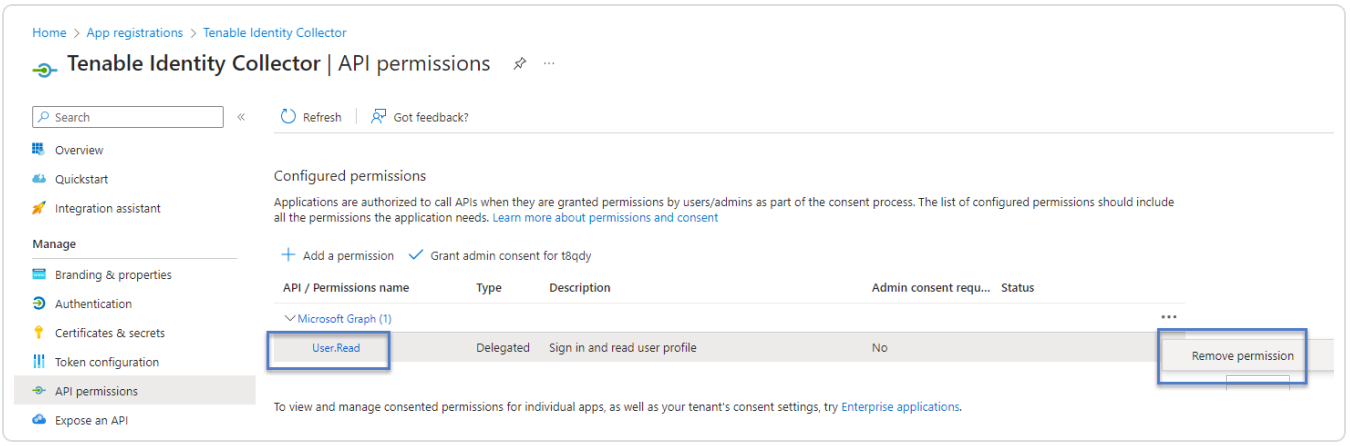
3. **为应用程序分配权限：**

a. 在 Azure 管理员门户中，打开“应用程序注册”页面。

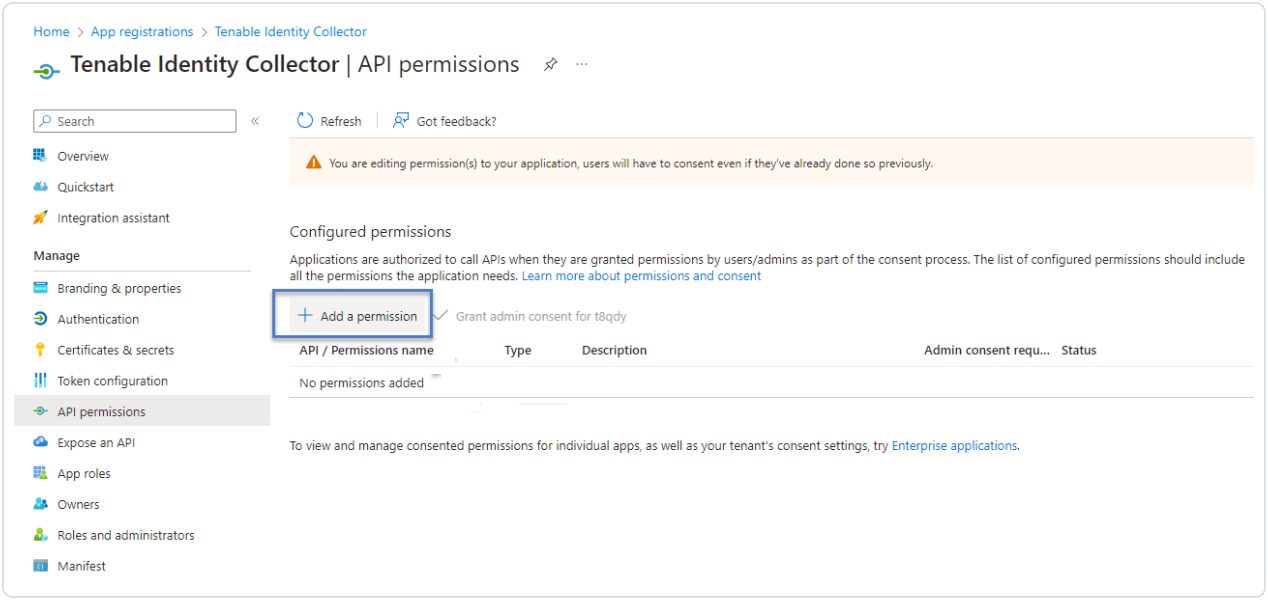
b. 点击已您创建的应用程序。

c. 在左侧菜单中，点击“**API 权限**”。

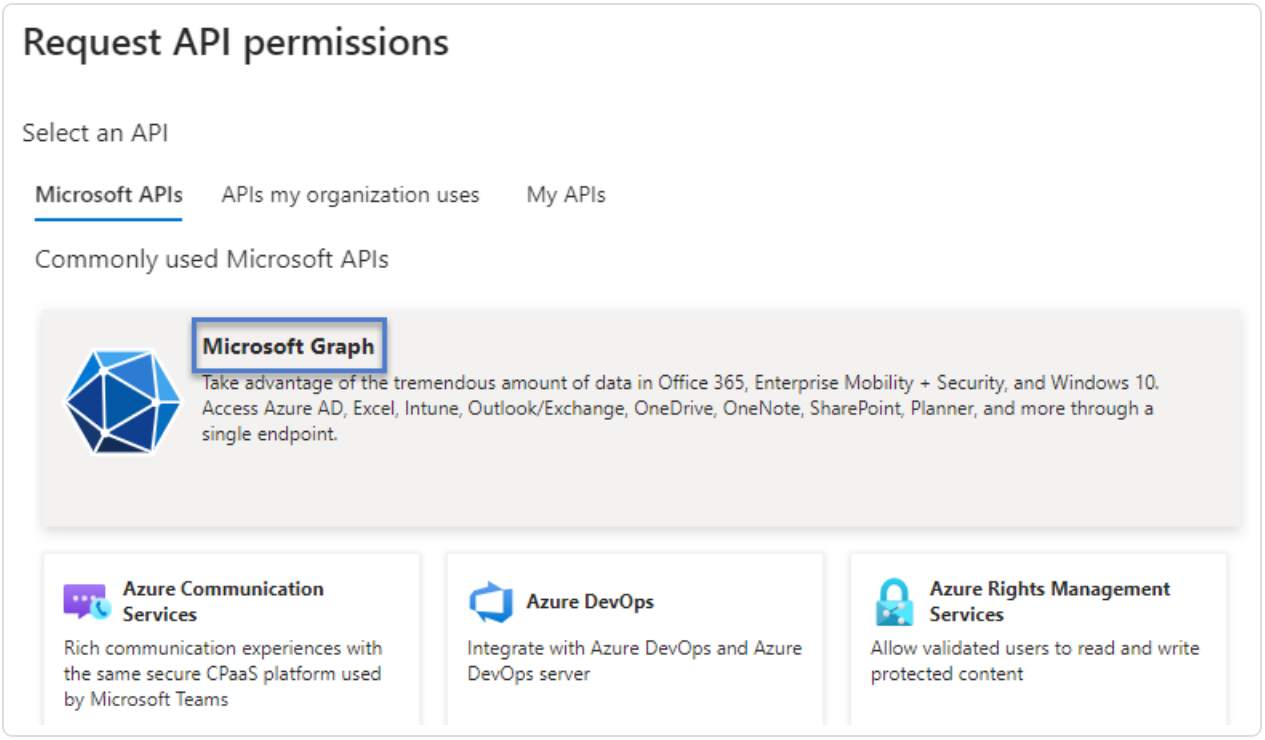
d. 删除现有 `User.Read` 权限：



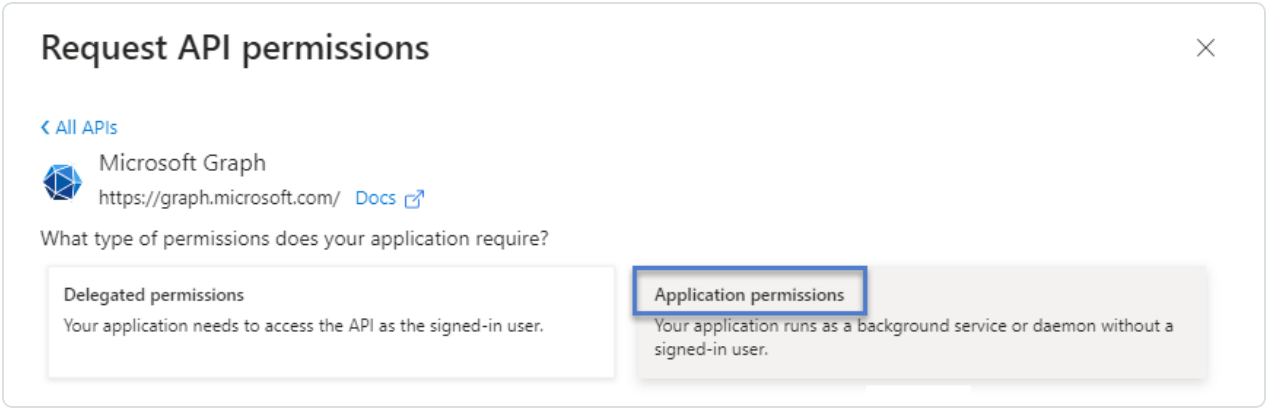
e. 点击“**+ 添加权限**”：



f. 选择“**Microsoft Graph**”:



g. 选择“**应用程序权限**”(非“委派权限”)。

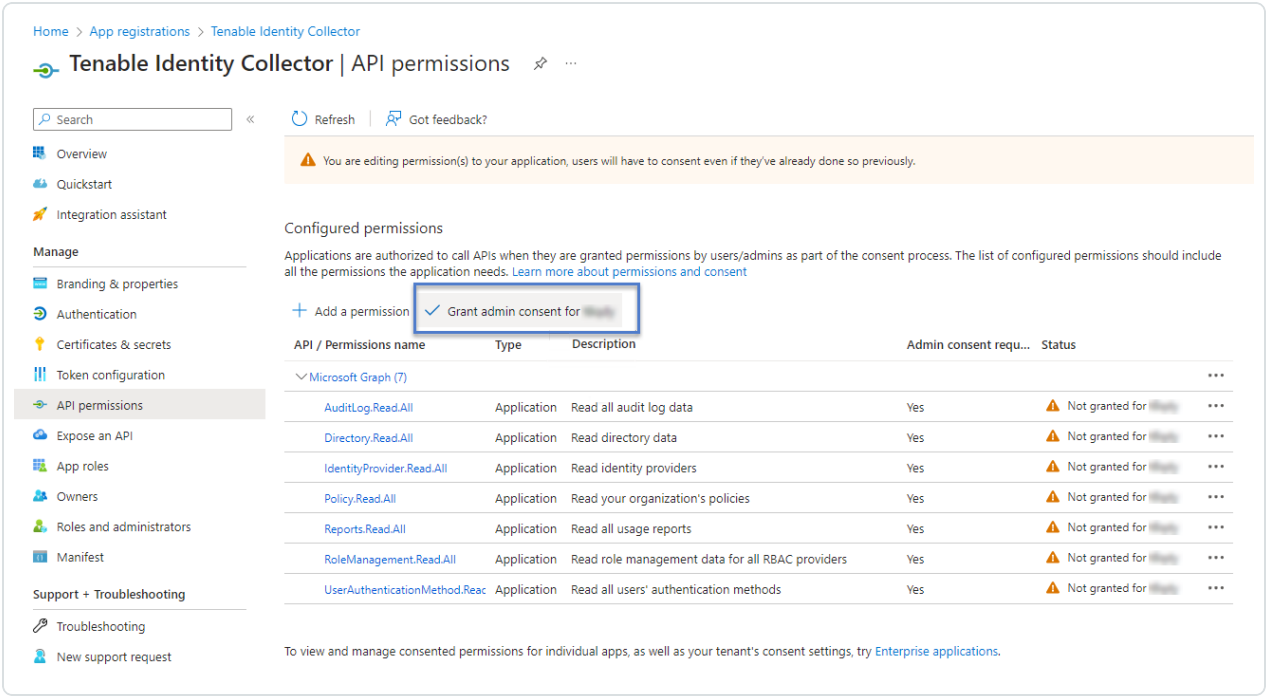


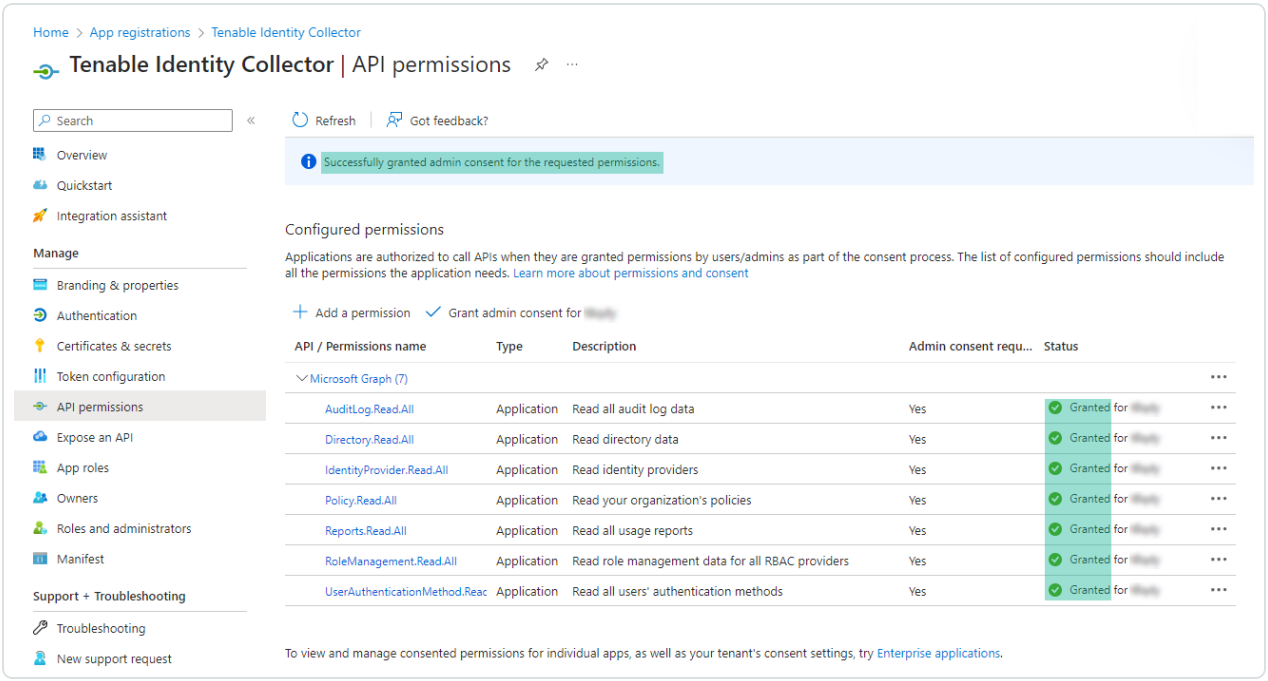
h. 使用列表或搜索栏查找并选择以下所有权限：

- `AuditLog.Read.All`
- `Directory.Read.All`
- `IdentityProvider.Read.All`
- `Policy.Read.All`
- `Reports.Read.All`
- `RoleManagement.Read.All`
- `UserAuthenticationMethod.Read.All`

i. 点击“**添加权限**”。

j. 点击“**为 <tenant name> 授予管理员同意**”并点击“**是**”以确认：





4. 在 Microsoft Entra ID 中配置所有必需的设置之后：

   a. 在 Tenable Vulnerability Management 中创建‘Microsoft Azure’类型的新凭据。

   b. 选择“密钥”身份验证方法并输入在之前的流程中检索到的值：租户 ID、应用程序 ID 和客户端密码。

激活 Microsoft Entra ID 支持

- 要使用 **Microsoft Entra ID**，必须在 Tenable Identity Exposure 设置中激活该功能。
- 请参阅 Identity 360, Exposure Center, and Microsoft Entra ID Support Activation 获取相关说明。

启用租户扫描

如要添加新的 Microsoft Entra ID 租户，请执行以下操作：

添加租户会将 Tenable Identity Exposure 与 Microsoft Entra ID 链接起来以对该租户执行扫描。

1. 在“配置”页面中，点击“**租户管理**”选项卡。

   “**租户管理**”页面随即打开。

2. 点击“**添加租户**”。

   “**添加租户**”页面随即打开。

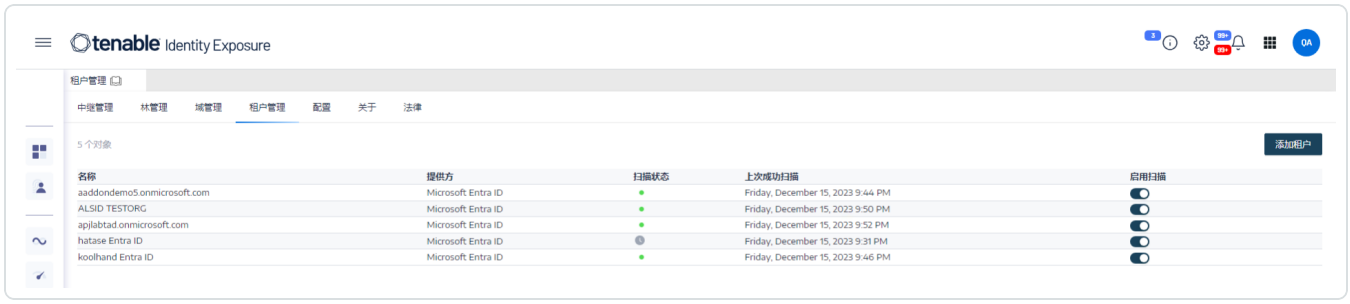
3. 在“**租户名称**”框中，输入名称。
4. 在“**凭据**”框中，点击下拉列表以选择凭据。
5. 如果您的凭据未出现在列表中，您可以：
    - 在 Tenable Vulnerability Management 中创建一个（通过“Tenable Vulnerability Management”>“**设置**”>“**凭据**”）。有关更多信息，请参阅“在 Tenable Vulnerability Management 中创建 Azure 类型凭据的过程”。
    - 检查您是否在 Tenable Vulnerability Management 中具有凭据的“可使用”或“可编辑”权限。除非您拥有这些权限，否则 Tenable Identity Exposure 不会在下拉列表中显示凭据。
6. 点击“**刷新**”以更新凭据下拉列表。
7. 选择您已创建的凭据。
8. 单击“**添加**”。

    此时会出现一条消息，确认 Tenable Identity Exposure 添加了租户，该租户现在显示在“租户管理”页面的列表中。

若要为租户启用扫描，请执行以下操作：

注意：租户扫描不会实时发生，且至少需要 45 分钟的时间才能在 Identity Explorer 中看到 Microsoft Entra ID 数据。

- 在列表中选择一个租户，然后点击以切换至“**已启用扫描**”。



Tenable Identity Exposure 请求对租户进行扫描，随后结果会显示在“风险暴露指标”页面

中。

> **注意**:两次扫描之间的强制性最短时间延迟为 **30 分钟**。

攻击路径

Tenable Identity Exposure 提供多种方式来通过图形展示方式可视化业务资产的潜在漏洞。

- **攻击路径**：显示攻击者可从进入点危害资产的路径。
- **爆炸半径**：显示从任何资产到 Active Directory 可能的横向移动。
- **资产风险**：显示可能控制某项资产的所有路径。

了解攻击路径能够让您确定必要的缓解步骤，从而阻止攻击者利用漏洞。这可能涉及修补系统、强化配置、实施更强的访问控制或提高用户的安全意识。

在 Tenable Identity Exposure 中使用攻击路径的好处：

- **主动安全**：有助于在潜在攻击载体受到利用之前预测并加以解决。
- **优先级**：可引导您将安全工作重点放在最关键的漏洞和攻击路径上。
- **可视化**：以清晰易懂的方式展示 AD 内的复杂安全关系。
- **通信**：通过提供潜在攻击场景的可视化证据，方便您向相关方传达安全风险。

若要显示攻击路径，请执行以下操作：

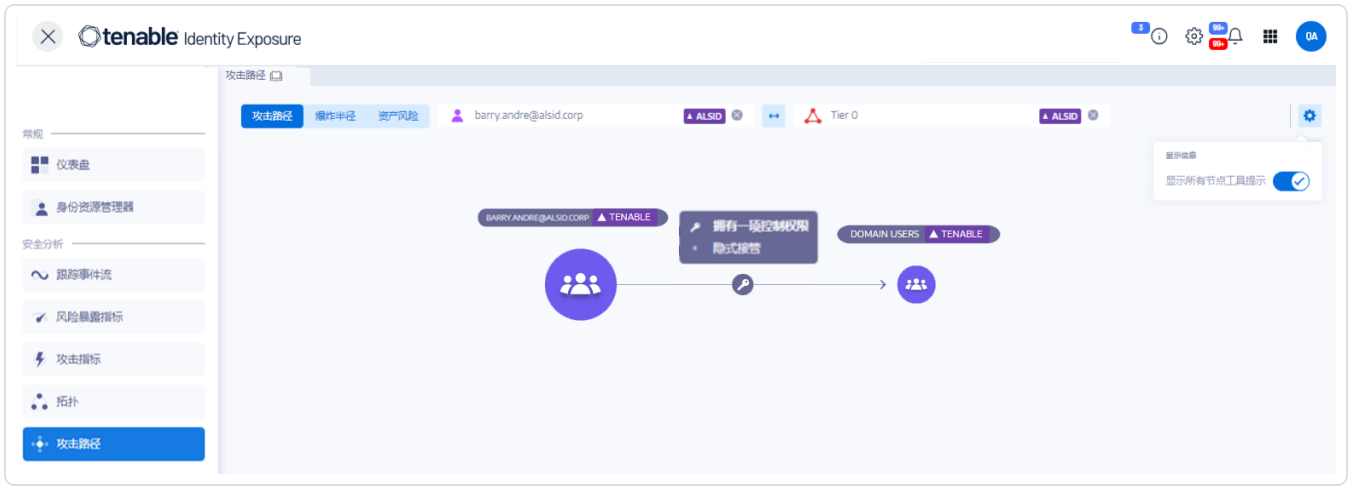
您可以指定 AD 中的任何资产（例如用户帐户、计算机、组）作为起点。您可以定义到达点，该点代表攻击者最终旨在入侵的资产（例如域控制器、敏感数据服务器）。

1. 在 Tenable Identity Exposure 中，点击侧边栏菜单上的“**攻击路径**”。

   “**攻击路径**”窗格随即出现。

2. 在标题栏中，点击“**攻击路径**”。
3. 在“**起点**”框中，输入进入点的资产。
4. 在“**终点**”框中，输入路径末端的资产。
5. 单击 图标。

   Tenable Identity Exposure 显示两个资产之间的攻击路径。



6. 或者，可以点击 图标来执行以下操作：
   - 点击“**缩放**”滑块以调整图形的放大倍数。
   - 点击“**显示所有节点工具提示**”开关，以显示有关资产的信息。

若要显示爆炸半径，请执行以下操作：

Tenable Identity Exposure 以图形方式显示潜在攻击路径，并突出显示资产之间的连接。每个连接都代表一个潜在漏洞或错误配置，攻击者可利用此漏洞在 AD 内横向移动。连接可以放大和缩小，以便更好地展示路径的详细信息。

1. 在 Tenable Identity Exposure 中，点击侧边栏菜单上的“**攻击路径**”。

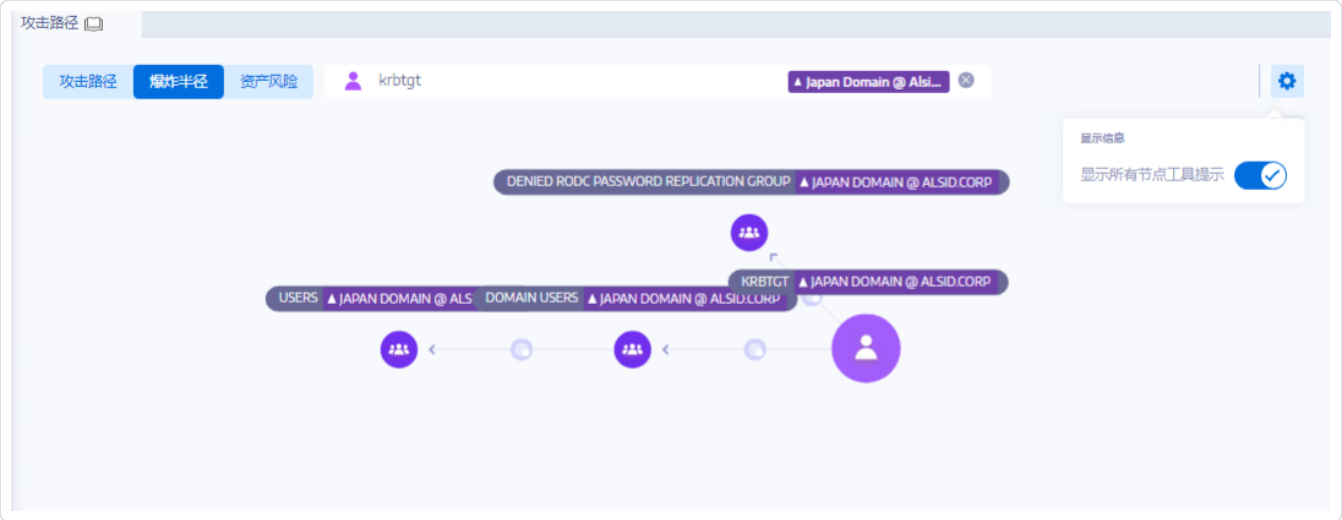
   “**攻击路径**”窗格随即出现。

2. 在标题栏中，点击“**爆炸半径**”。

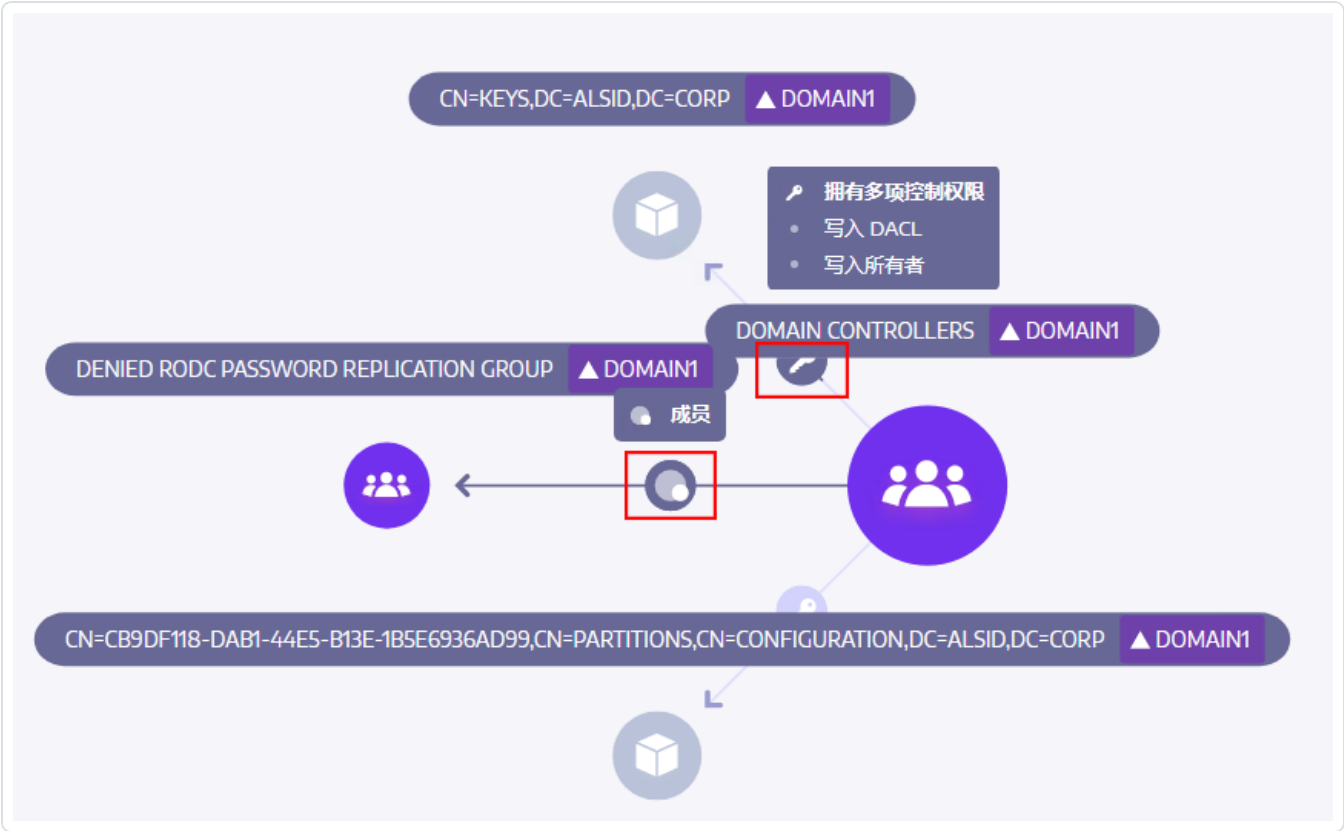
3. 在“**搜索对象**”框中，输入资产的名称。

4. 单击 图标。

   Tenable Identity Exposure 显示该资产辐射的横向连接：



5. 点击资产之间的箭头上的图标，以显示它们之间的关系。



若要显示资产风险暴露，请执行以下操作：

攻击路径中的每个步骤都与一个风险评分相关联，以指示漏洞的严重程度。这有助于您优先处理那些造成最严重威胁并需要立即关注的路径。您也可以单击各个连接点，以获取有关所涉及的特定漏洞或错误配置的更多详细信息。

1. 在 Tenable Identity Exposure 中，点击侧边栏菜单上的“**攻击路径**”。

   “**攻击路径**”窗格随即出现。

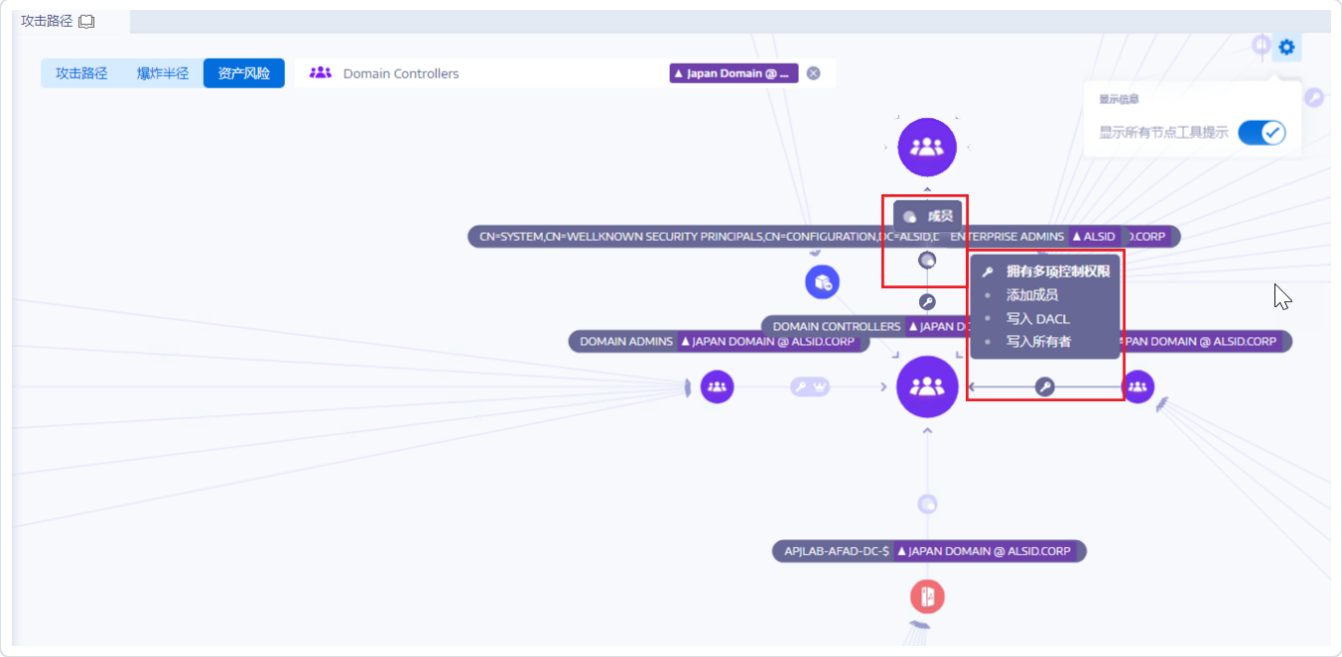
2. 在标题栏中，点击“**资产风险**”。

3. 在“**搜索对象**”框中，输入资产的名称。

4. 单击 图标。

   Tenable Identity Exposure 显示通向资产的路径以及资产之间的关系。

5. 点击资产之间的箭头上的图标，以显示它们之间的关系。



若要固定攻击路径：

另请参阅：

- Attack Relations
- Identifying Tier 0 Assets
- Accounts with Attack Paths
- Attack Path Node Types

用户管理

关键方面

- **角色**:默认角色包括管理员、安全分析师、用户和访客,每种角色都有不同的权限。自定义角色可对特定需求进行精细控制。
- **权限**:权限用于定义用户在 Tenable Identity Exposure 内可访问的内容和可执行的操作。权限范围包括查看报告和仪表盘、管理用户、配置指标以及执行禁用帐户等操作。
- **界定 Tenable Identity Exposure 范围**允许将权限范围界定至特定域、组,甚至 Active Directory 内的单个对象。这样可确保用户仅能根据自己的角色和权限访问相关数据。

优点

- **增强 Active Directory 安全性**:精细访问控制可将敏感身份数据遭到未经授权的访问的风险降至最低。
- **改进效率和工作流**:用户可以访问所需的工具和数据,从而简化调查和事件响应。
- **遵守合规性要求**:基于角色的访问控制有助于满足 Active Directory 中对身份和访问管理的合规性要求。

另请参阅:

- User Roles

Tenable Identity Exposure 集成

将 Tenable Identity Exposure 与 SIEM、SOC 或 SOAR 解决方案集成，以实现实时监控、自动响应和警报管理改进。

通过 Syslog 集成进行实时监控

通过无缝集成 Syslog，获取关键风险暴露指标 (IoE) 的即时警报。

主要优点

- **集中式日志记录**：使用其他安全解决方案汇总 Tenable Identity Exposure 事件，以进行全面分析。
- **实时通知**：接收潜在身份暴露和攻击的即时通知。
- **改进安全管理**：关联不同来源的事件，更快识别复杂威胁。
- **提高 SIEM 可见性**：将 Tenable Identity Exposure 数据无缝集成到 SIEM 中，促进态势感知和相关性分析。
- **简化工作流程**：利用 Syslog 数据实现警报分类和响应自动化，从而优化安全操作。

要实时监控的 IoE 的示例

- **存在风险的 ADCS 错误配置**：检测/识别可能表示“Certified Pre-owned”攻击的 AD 证书服务器变更。
- **GPO 执行的合理性**：检测/识别尝试通过组策略内的脚本执行安装后门程序的行为。
- **获准将计算机加入到域的用户**：识别未经授权添加的域计算机，即“RBCD”后门程序攻击的标志性预攻击。

通过 SOAR 平台实现响应自动化

利用现有的安全编排、自动化和响应 (SOAR) 平台，根据 TIE 数据执行自动化的修复操作。主要优点如下：

- **快速缓解**：自动响应关键 IoE 可最大程度减少停机时间和影响。
- **提高效率**：安全团队无需再处理重复性任务，而是可以专注于战略安全计划。
- **强化安全措施**：主动解决检测到的错误配置并巩固整体安全状况。

重要事项：Tenable 支持部门不负责解决自动化脚本问题或提供相关帮助。如需帮助，请联系我们的专业服务团队。