“**Deep Dive: Data Protection Tools in Foundry**”是 learn.palantir.com 上的一门深度实战课程，旨在指导用户掌握 Foundry 平台中用于数据保护和治理的核心工具集 1。该课程强调通过技术手段确保数据安全，是数据治理框架的重要组成部分 1, 2。
根据来源，该标题涵盖的三个核心工具及其功能如下：

1. **Checkpoints**（检查点）：理由驱动的行为管控

- 核心定义：Checkpoint 是一种交互式提示，当用户在 Foundry 中执行敏感操作（如导出数据、下载文件）时，系统会强制要求用户提供操作理由或合规性确认 3, 4。
- 配置与触发：管理员可以根据命名空间、特定用户组或数据标记（Marking）来设置 Checkpoint 的触发范围 4, 5。
- 理由类型：支持多种证明方式，包括简单的确认勾选（**Acknowledgement**）、下拉菜单选择原因、文本回复或重新进行身份验证 6。系统会记录这些日志，以便后续审计 7。

2. **Sensitive Data Scanner**（敏感数据扫描器）：风险自动识别

- 核心定义：该工具用于自动扫描并标记项目中的敏感信息（如个人身份信息 PII），避免依赖人工检查庞大的数据集 7, 8。
- 匹配逻辑：支持使用平台预设的条件（如电子邮件、社保号 SSN、电话号码等）或通过**正则表达式（RegEx）**自定义匹配规则（例如匹配“婚姻状况”等特定字段） 9, 10。
- 自动化响应：扫描发现敏感数据后，系统可以执行自动操作，例如创建问题单（Issue）或自动应用**安全标记（Marking）**来限制访问 11。

3. **Cipher**（加密与脱敏）：数据混淆技术

- 核心定义：Cipher 是 Foundry 的核心混淆工具，用于对敏感字段进行加密处理，支持可逆加密和不可逆混淆 12-14。
- 管理机制：
- **Cipher Channel**（频道）：定义加密算法和加密系统（如确定性加密） 13, 14。
- **Cipher License**（许可证）：充当访问密钥。管理员可以分别针对数据集操作或本体（**Ontology**）操作创建许可证，严格控制谁能加密或解密特定数据 14, 15。
- 应用场景：用户可以在 Pipeline Builder 中对员工姓名等字段进行加密，使数据在物理存储中显示为密文 15, 16。在应用层（如 Object Explorer），只有拥有相应解密许可证的用户才能查看原始值 17, 18。

4. 治理角色与综合应用

- 权限要求：要配置和管理这些工具，用户通常需要在 Foundry 中具备 **Data Governance Officer**（数据治理专员） 角色 2。
- 安全防御体系：这些工具通常与 **Markings**（安全标记） 结合使用，共同实现“数据最小化”原则，确保只有获得授权的人员在合规的场景下才能接触敏感数据 2, 12。

通过学习这门课程，用户可以构建一个**从自动检测风险（Scanner）、到操作合规约束（Checkpoints）、再到物理数据加密（Cipher）**的完整数据保护链路 2, 18。