Okta Secures AI - Discovery Questions and Objection Handling

Discovery Questions

1. **AI Agent Roadmap and Strategy:** Start by understanding your customers' overall roadmap for AI Agents.
    - **Question:** What is your roadmap for AI agents over the next 12 months? Is your primary approach to build custom agents in-house, buy agents from a provider, or both?
        - **Listen for:** Clarity of vision, timeline, investment level, and the mix of agent development/creation vs internal agent management and utilization.
    - **Question:** What agentic platform are you building with?
    - **Question:** Which third party agents are you using?
    - **Question:** Which are the top ISV/ SaaS products your team is using? Particularly ones that you want to integrate with agents?
2. **AI Agent Use Cases:** Get curious about your customers' AI agent use cases and understand which use cases are a priority mapped to a specific business objective.
    - **Question:** What are the primary use cases you're targeting? Are they for internal workforce productivity, external customer-facing applications, or a new B2B SaaS offering?
        - **Listen for:** The business problem they are trying to solve. This helps map the opportunity to our solution (Auth0 for building AI agents, Okta for managing internal AI agents).
3. **AI Agent Identity:** Identify potential gaps in AI agent identity to map them to Okta solutions.
    - **Question:** How does the agent confirm it's the correct user making the request before it acts on their behalf?
        - **Listen for:** Reliance on implicit trust within an existing user session, which is a major security gap. Listen for the absence of authentication mechanisms that bind the user's identity directly to the agent's request, creating a risk of impersonation or unauthorized actions.
    - **Question:** How are you securing the API tokens and other credentials agents use to connect to downstream systems? How do you prevent them from being exposed?
        - **Listen for:** Use of static API keys, insecure credential storage, or a lack of process for token rotation and management.
    - **Question:** For AI that retrieves sensitive data, how do you enforce that the agent only sees information that the specific user is authorized to access?
        - **Listen for:** Lack of fine-grained permissions or an inability to filter data at the user level.
    - **Question:** As agent use scales across your organization, how do you plan to maintain central visibility, control, and governance over the entire agent population?
        - **Listen for:** Lack of a central registry, inconsistent security policies between teams, and no plan for managing the lifecycle (onboarding, offboarding) of agents.

Objection Handling

1. **“We’re not ready yet.”**
    - **Objection:** "This is interesting, but we're still in the experimental phase with AI. We don't need AI agent identity yet."
    - **Underlying Concern:** They see identity as a feature to be added later, not as a foundational requirement to scale.
    - **Response Framework:** Reframe their timeline for AI agent identity by positioning it as the foundation for all of their AI agent deployments.
    - **Example Talk Track:** “This is the perfect time to think about identity. The security decisions you make now will become the standard for your AI agent ecosystem. By giving your development, IT admin, and security teams the tools they need for AI agents now, you’re laying the foundation for a secure AI agent rollout now, and in the future.”
2. **“We can build identity ourselves.”**
    - **Objection:** "We have the right teams and expertise to build identity into our AI agent workflows on our own.”
    - **Underlying Concern:** Underestimation of the complexity and ongoing maintenance required for secure identity.
    - **Response Framework:** pivot from a question of “***can*** they” to one of “***should*** they”. Frame it as a choice between core innovation and complex infrastructure.
    - **Example Talk Track:** “AI agents introduce a completely new identity problem that goes far beyond just authenticating users. Do you want them building the agentic features that help you achieve your core business objectives, or building and maintaining your identity stack? The AI agent space is moving fast, we handle the identity, so you can focus on innovation.”
3. **“We already have an IAM solution, we’ll just use that.”**
    - **Objection:** "We’ve got an IAM provider we already use for our human identities. We plan to extend that to our AI agents."
    - **Underlying Concern:** Adding a new vendor to the mix; they’d rather just use an existing solution that’s familiar to them and their teams.
    - **Response Framework:** Traditional identity solutions weren’t built for AI agent identity.
    - **Example Talk Track:** “Your existing IAM solution is great for managing your human employees. But agents are different. They require their own lifecycle, credentials, and fine-grained authorization policies. Treating them like a standard application in your current system will create security gaps. Okta is purpose-built to manage this new class of machine identity, providing the central visibility and governance you need to secure them at scale.”
4. **“We don’t have budget.”**
    - **Objection:** "We’re investing in AI projects right now and don’t have budget for a separate identity solution.”
    - **Underlying Concern:** Identity is a cost center, not an enabler of their AI initiatives.
    - **Response Framework:** Reframe identity as something that enables them to adopt AI faster, and see ROI sooner.
    - **Example Talk Track:** “You’re investing a lot of money, and likely staking your career, on your AI investments. Okta helps you protect that investment. What if an AI agent project stalls

because of an insecure agent? What is the cost if an AI agent is breached and leaks sensitive data? Okta helps de-risk your AI agent roadmap so you can adopt faster, with more confidence."

5. **"We're already using an agentic platform that can handle this."**
    - **Objection:** "We've standardized on [LangChain / Microsoft Copilot Studio / Vercel AI SDK]. Doesn't that platform manage the agents for us?"
    - **Underlying Concern:** They believe their agent development or orchestration framework is the complete solution, including the security and identity components.
    - **Response Framework:** Separate the roles. "Your platform is for building and running agents. Okta is for securing and governing them."
    - **Example Talk Track:** "That's a great choice for building and orchestrating agent logic. But those platforms are designed to solve the 'how'—how to chain prompts and connect to tools. They don't solve for the 'who' and the 'what.' Who is the user behind the agent? What data are they allowed to access? Okta provides the identity layer that plugs into your chosen platform. We ensure every agent acts on behalf of a strongly authenticated user, inherits their exact permissions, and has its own secure lifecycle."