Description

Delivering on Identity & Access Management is becoming a business imperative, as we are driven by sweeping regulations and portal-based application integration to provide robust authentication and authorization systems. Web Access Management SSO and portal technologies, multi-tenant distributed Cloud / Federated Identity, Privilege certification and audit, RBAC Provisioning and multi-factor authentication are becoming the norm, rather than bleeding-edge implementations. Further, getting Identity & Access Management implementation wrong can lead from simple issues, such as Martha not being able to login to her GL application, to severe issues causing financial losses and damage to an organization's reputation and brand when "nobody can log in".

Identity and Access Management requires holistic measures to address provisioning, authentication, fine-grained authorization, identity mapping, federation, metadata security, and fundamental issues of identity integrity and integrity controls.

This full day Master Class will share lessons learned in several major federation, single sign-on, identity and access management and token implementations. We will not only cover the basics, but also advanced lessons learned for implementation of advanced Identity & Access Management components, as well as emerging issues in identity requirements that will challenge old-school methodologies for authentication, identity management and the future of federation, when everything is pushing to the cloud.

Course Modules

- **Basic principles of Identity and Access Management (I&AM)**
- **Directory Services - enterprise, meta-directory and virtual**
- **Web-based Authentication / Web Access Management**
- **Provisioning, De-provisioning, and short name collision management**
- **Identity Mapping and Roll-up**
- **Detailed Single Sign-on Strategies**
- **Federation & Cross-company Authentication (CCA) Architecture**
- **Self-service tools in the I&AM arena**
- **Access/Entitlement Audit and Certification**
- **Infrastructure architecture -- critical underlying processes to run a successful enterprise**
- **Case Study: Standards-based and proprietary implementations of Federated Identity**
- **Biometrics, Tokens, Knowledge-based proofs and other multi-factor authentication devices: basics, challenges and lessons learned**
- **Man-in-the-Middle attacks and token/multi-factor attacks**
- **Strategies for Identity Management implementation**
- **Governance & Compliance issues addressed by identity management**
- **Cost justification for investment, typical stakeholders, and getting buy-in**
After this course, you'll be able to apply the following skills to your current role:

- Identify the drivers to developing and maintaining your enterprise identity architecture program
- Assess your “current identity infrastructure” to better set goals and targets for your strategic identity management program
- Establish the governance, roadmap and lifecycle process for your identity architecture
- Hit business targets through identity deliverables
- Specific deep-dive on advanced identity concepts: federation, identity mapping, provisioning integration, WAM/SSO, identity audit, infrastructure

Attendance Suggested For

- Information Security Officers
- Security Engineers
- Directory Services Engineers
- Systems & Information Architects
- Project Managers
- Consultants
- Auditors

Instructor Bio

Dan Houser, CISSP-ISSAP-ISSMP CSSLP CISA CISM

Dan Houser is Sr Security & Identity Architect for a Global 100 healthcare organization, based in Columbus, Ohio. He has over 20 years IT which includes experience in banking, financial services, education, consulting, telecommunications, and healthcare.