RSA Authentication Manager Administration

Product and Technology Overview

- High level description of RSA Authentication Manager and its contribution to user authentication
- Authentication as a foundation of security, trust and confidence in digital identities
- RSA Authentication Manager system components and communication

RSA SecurID Authentication

- RSA SecurID authentication options
- Concepts of strong user authentication
- Token technology – time synchronization, authenticator types

Risk-Based Authentication

- Configuration and management of risk-based authentication
- Device fingerprinting and behavior data collection and analysis
- Selecting assurance levels

Deployment and Administrative Structure

- Deployment planning and establishing an administrative structure

Policy Management

- Defining and applying policies to the system and Security Domains
  - Password and Token policies
  - Lockout and self-service policies
  - Risk-based and Offline authentication policies

System Administration

- Establishing and maintaining organizational and administrative structures:
  - LDAP Identity Sources
  - Security Domains
  - User and User Group structures
  - Administrative roles and delegation
  - Authentication Agents

Authenticator Management

- **Managing RSA SecurID hardware tokens**
- **Software token deployment and installation**
- **Managing Risk-Based Authentication**
- **Managing On-Demand Authentication**

Auditing, Reports and Troubleshooting

- RSA Authentication Manager report functions
- Report customization
- Troubleshooting procedures

Self-Service Management and Support

- Configurations for user self-service functions
- User account and authenticator management and provisioning