Securing Data in ServiceNow

Best Practices and Security Features

Presented by: [Your Name]

Date: [Date]

Introduction

- ServiceNow is a cloud-based platform for ITSM and workflows.

- Data security is essential.

- Goal: Learn how to secure data in ServiceNow.

Key Areas of Data Security

- Authentication & Authorization
- Data Encryption
- Access Controls (ACLs)
- Data Privacy & Compliance
- Auditing and Monitoring

Authentication & Authorization

- SSO (SAML, OAuth, LDAP)
- Multi-Factor Authentication (MFA)
- Role-based access (RBAC)
- Scoped Applications

Data Encryption

- Encryption at Rest: AES-256

- In Transit: TLS/SSL

- Field-level encryption for sensitive data

Access Controls (ACLs)

- Restrict access to records and fields

- Types: Record and Field ACLs

- Use conditions and scripts with caution

Data Privacy & Compliance

- Compliance: GDPR, HIPAA, FedRAMP
- Data retention policies
- User consent and anonymization

Auditing and Monitoring

- Track changes and user actions

- Use real-time dashboards

- Security Operations (SecOps) for response

Best Practices

- Principle of Least Privilege
- ACL audits
- MFA and strong passwords
- Encrypt PII
- Scoped app use

Common Pitfalls

- Over-permissive roles
- Hardcoded credentials
- Ignoring updates
- Lack of third-party visibility

Conclusion

- Strong tools for security in ServiceNow

- Requires correct configuration

- Continuous monitoring is key

Questions?

Thank you!

[Your Contact Info]