Microsoft Azure and Office 365 Security Training Syllabus

Keeping up with Microsoft's rapid innovation and release of security capabilities can be a challenge. With this one day course, Systems Engineers, CISOs, and other IT professionals can get quickly sync'd in a live, interactive online course with an Enabling cloud expert.

For each topic/technology, Enabling's engineer will provide:

1) Overview of what's possible
2) Tour of the admin interface, and review of relevant options
3) What product/licensing is needed for each capability
4) What's commonly done/best practices
5) Major caveats/need-to-know's

Identity Mgmt/SSO:

a. ADFS https://msdn.microsoft.com/en-us/library/azure/jj205462.aspx
b. Azure AD Connect (same sign on) https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/
    1. Differences between
c. Azure AD federation to 3rd party SaaS apps https://azure.microsoft.com/en-us/marketplace/active-directory/
d. Self-service password reset
e. Audits
    1. Anomalous activity reports
    2. Activity Logs
    3. Integrated Applications

Mobile Device Management (MDM) within O365

a. Native capabilities of Office 365 to control access to online apps
b. Enrollment and policies to control access
    - Password strength, expiration, attempts
    - Encryption (Android only, note limits on iOS)
    - Jail break capabilities
    - Application/device/system/cloud settings
c. Managed email profiles
d. Pros/cons/differences against ActiveSync
e. Differences in capabilities between iOS, Android (Windows if applicable)

f. Wiping devices
    - Admin experience
    - User experience

Mobile Application Management (MAM) within Intune

a. Device Enrollment
    a. Review Client-Based Access Control (CBAC): Certificate Provisioning on devices as part of enrollment
b. Review Device Settings and Policies
    a. PIN requirements
    b. Email profiles
    c. VPN profiles
c. Review Application Policies: blacklist/whitelist; cut/copy/paste/save-as restrictions between corporate and personal apps
d. Enabling Selective Wipe
e. Self-Service Enrollment Portal
f. App Management to push company standard app package
g. Conditional access (location, device, ID)
h. Audit capabilities

Azure Multifactor Authentication (MFA)

a. Techniques to provide one-time passwords via Azure AD Premium authentication app/Intune (app, call, SMS)
b. Conditional access options (i.e. users on net needn't submit secondary creds, remote users do)
c. Temporary bypassing
d. Caveats/application passwords for thick clients
e. Blocking/unblocking users
f. Fraud Alerts, reports, and audits

Data Loss Prevention

a. Content detection flow for Exchange Online, SharePoint Online, OneDrive for Business
b. Microsoft templates for baseline DLP rules for Office (i.e. PII, GLBA, PCI)
c. Making organization-specific templates, or importing existing templates
d. Adding Policy Tips to notify users in the mail program about policy violations
e. Querying for and ID'ing sensitive data
f. Exporting results
g. Reports https://technet.microsoft.com/en-us/library/dn904484(v=exchg.150).aspx

Azure Rights Management Service (RMS)

a. Review the default RMS Templates provided by Microsoft

        a. Confidential View Only
        b. Confidential
    b. Overview the Azure Rights Management sharing app/Connector (Optional)
    c. Matrix of client devices and applications supporting RMS (i.e. email, pdf, Office)
    d. User experience

Compliance

a. In-place legal hold
    a. The recoverable items folder and Subfolders
    b. Tracing forwarded messages
    c. Validating it's working
b. In-place e-Discovery (for Exchange and SharePoint, if applicable)
    a. Configuring
        i. Configuring roles for authorized users
        ii. Creating custom management scopes
        iii. Setting up discovery mailboxes
        iv. Selecting output (i.e. preview, export)
    b. Using
        i. Logging
        ii. Handling terminated employees

Security Monitoring and Event Management

a. Advanced Threat Analytics (for on-premises and Azure servers)
    i. ATA capabilities
    ii. Terminology
    iii. Architecture
    iv. Network requirements
    v. ATA center tour
    vi. Configuring suspicious activity alerts
    vii. Logging and audit capabilities
    viii. Suggestions to get started
b. Advanced Security Management (within Office 365)
    i. ASM capabilities
    ii. Activating and burn-in period
    iii. Understanding the general anomaly report
    iv. When it makes sense to create a specific policy