Securing Active Directory

Presented by Michael Ivy

Presenter:

Michael Ivy

Consultant, Rook Security

Michael Ivy

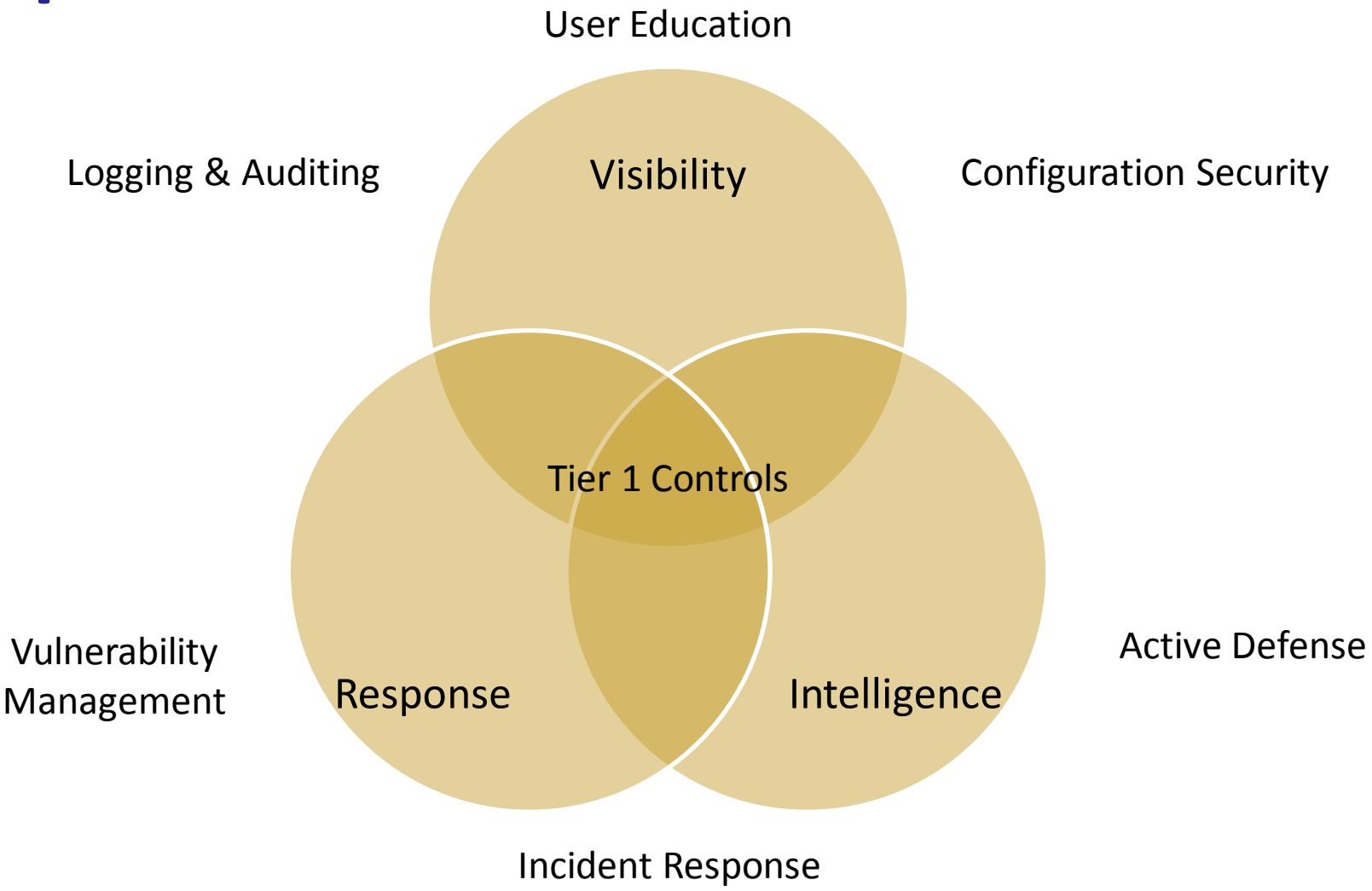
Thank you for being here today

August 20, 2014

Brief Overview

- Securing NTDS and Replication
- Permission, Delegation and Auditing
- Forests and Trust Design
- Securing DNS

Visibility, Intelligence, & Response™



Key Components

VISIBILITY

INTELLIGENCE

RESPONSE

0.0 Foundational Tools	Firewall	IPS/Threat	Log/SIEM	
1.0 Configuration	Tier 1 Controls™	Tier 2 Controls™		
2.0 Monitoring	Technical Activity (Standard IOCs)	Compliance & Standards	Digital Asset Management	Social Media Management
3.0 Intelligence	Threat Enrichment Data	Timely, Custom IOCs	Business Intelligence	Event Correlation
4.0 Response	ROE & Timely Remote and/or Hands-on IR	Tracking to Resolution	Identify & Resolve Root Causes	Key Performance Indicators (KPIs)

Tier 1 Controls™

LOGGING	
All logs (firewall, VPN, DHCP, DNS, etc) into SIEM	
If no SIEM, store key logs in central location as flat file	
Synchronized NTP	
DNS logs include queried domain name & requestor	
Windows app, system & security logs configured	
Success/failure logged on all systems	
Increase storage size of key logs to prevent overwrites	
AV & HIPS logs to SIEM	
Internal web proxy servers logging	
All firewalls log all traffic to SIEM	
ACTIVE SCANNING & MONITORING	
Deploy scanning capabilities for every network hosts	
Monitor for IOCs	
Monitor traffic to known C&C servers	
Increase visibility on ingress and egress traffic	
FILE SHARING	
Restrict permissions to only those that are necessary	

DNS
All known malware domains redirec
Use blacklists to block obvious bad traf
Blacklist all unnecessary countries
Scrape DNS logs minimum once per w
Log failed lookups (NX domain) to help
Extract/cache DNS queries/answers
Evaluate suspect DNS anomalies
EMAIL
End user phishing education and traini
Filtering in place
Set up phishing assistance
FIREWALL RU
Block all suspicious netblocks
Actively update known bad netblock
ACTIVE DIRECT
Audit/disable unused accounts
Accounts disabled and set to "Default

Securing NTDS and Replication

Securing NTDS and Replication

- DC's should be in a locked, access controlled room
- Consider surveillance equipment
- Prefer granting access via Terminal Services
- Prefer locating in a locking rack
- Don't forget about power – UPS, RPS etc…

Encrypt Hashes/Keys with SYSKEY.EXE

- SYSKEY.EXE creates a 128-bit RC4 key which is used to protect:
  - Protection keys for users' passwords in AD or the local SAM database
  - User's "Master Keys" that protect private keys for digital certificates
  - Protection key for "LSA Secrets" in the registry
  - Protection key for the local administrator account used when booting into Safe Mode

SYSKEY.EXE continued

- SYSKEY.EXE can be executed from the command line to reconfigure how System Key is created and stored
  - The System Key can be stored locally (default)
  - The System Key can be derived from a password that must then be entered at boot
  - The System Key can lastly be derived randomly and stored on a floppy which is then required to boot

Whole Disk Encryption Server 2008 and Later

- Bitlocker Benefits:
  - Boot-up Verification
  - 128 or 256bit AES sector level encryption
  - Transparent to user
  - Optional TPM chip integration is preferred
  - Emergency recovery options including AD backup

Read Only Domain Controllers

- Used for insecure locations (like remote offices)
- Limited Replication and attack surface
- When Compromised – Delete the RODC computer account and clean up
- Requires:
  - Server 2008+
  - Forest Level 2003+
  - PDC Emulator must be 2008+

Backups for DR and Auditing

- What would you choose, a firewall or good backups?
- Authoritative Restore Issues:
  - For both the AD and the SYSVOL share
  - There is no authoritative restore for the Schema
- NTDSUTIL.EXE
- 2008-R2 + Recycle Bin

Securing Replication Traffic

- Leased Lines (though MPLS is not encrypted)
- Dial-up
- VPN
- IPSec
- SMTPS + S/MIME
- Always have redundant pathways

Secure the Schema

- Schema defines classes of objects in the AD and their attributes
- Physical Security
- Read-Only DCs
- Empty the Schema Admins group
- Have good backups
- Audit all Changes

Permission, Delegation and Auditing

Active Directory Permissions

- ADUC: View > Advanced will reveal the “Security” tab on all objects
- Every “Property” of every object in AD can have it’s own ACL
- Objects also have “Owners”

AD Access Control List Tools

- DSACLS.EXE
- ACLDIAG.EXE
- SDCHECK.EXE
- DSREVOKE.EXE
- ADSI

Delegation of Control

- Delegate authority using:
  - Active Directory Permission
  - Group Policy
- Delegation of AD objects is much like delegation of control in NTFS
- Leading Practices
  - Have Written Policies
  - Focus Delegation on OU's
  - Assign Permissions to Groups
  - Use GPO's to restrict access to powerful snap-ins
  - Consider customized MMC Consoles
  - Audit - everything

Auditing Access to Active Directory

- Every “Property” of every object in AD can have its own separate set of audit settings
- Active Directory SACLs are mostly built in unlike NTFS SACLs
- Enable the audit policy for:
  - Audit Directory Service Access (S/F)
  - Audit Account Logon Events (S/F)
  - Audit Logon Events (S/F)
  - Audit Account Management (S/F)
  - Audit Object Access (S/F)
  - Audit Policy Change (S/F)
  - Audit System Events (S/F)

Directory Service Change Auditing

- Requires Server 2008 or later on DC's
- Adds auditing subcategory for change:
  - Logs both pre and post values for altered attributes
  - Logs non-default values added during the creation of a new object
  - Logs Previous and new locations when objects are moved or undeleted
- CMD > auditpol.exe /get /category:*

Forest and Trust Design

Forest Design Affects Security

- Trust Types:
  - External
  - Intra-Forest
  - Cross-Forest
  - Shortcut
  - Kerberos Realm
- Issues for consideration:
  - Logon Location
  - Permissions
  - Authentication protocols
  - RADIUS, LDAP, PKI
  - Replication
  - Firewalling

Three Scenarios

- Federated Forests
- Empty Root Domains
- Extranet Forests

When to Create More Forests

- To isolate mission-critical resources
- To isolate dangerous users/computers
- Testing/Training labs
- Applications with schema modifications
- Acquisitions/mergers of other forests
- Legal/Contractual mandates
- Need for fault tolerance is top priority
- Lack of bandwidth

When to Create More Domains

- For differing domain-wide GPO's
- With poor but manageable bandwidth
- For separate DNS names
- For international organizations

Securing DNS

DNS Tools

- DNS MMC Snap-In
- IPCONFIG.EXE
- NSLOOKUP.EXE
- DIG.EXE
- DNSCMD.EXE
- DNSLINT.EXE
- DNSDIAG.EXE
- Performance Monitor
- Event Viewer DNS Log

Active Directory Swallows DNS

- DNS Records have become more AD objects
  - No zone files
  - No zone transfers
  - No more primary/secondary distinction
  - DNS Servers must be DC's
- All this adds up to:
  - No separate DNS replication topology
  - No single point of failure
  - Permissions on DNS records for secure dynamic updates
  - More efficient replication

Use Secure Dynamic Updates

- Requires AD-integrated DNS servers
  - Adds permissions on DNS records
  - Requires Kerberos
  - Does not support Unix-esque secure dynamic updates
- Secure Updates can be mandatory
- Windows DHCP Server can update DNS records on behalf of computers/devices that don't support MS-style secure dynamic updates

DNS Security Leading Practices

- Use a split DNS architecture
- Require secure Dynamic updates from everyone
- Disable Zone Transfers
- Secure against cache poisoning attacks
- Enable Logging
- Harden ACL’s on critical DNS records, including SACL’s

Questions

We'll now open it up for questions

Thank You

Presenter:

Michael Ivy

Consultant, Rook Security

www.rooksecurity.com

@rooksecurity

ROOK