PING CASTLE

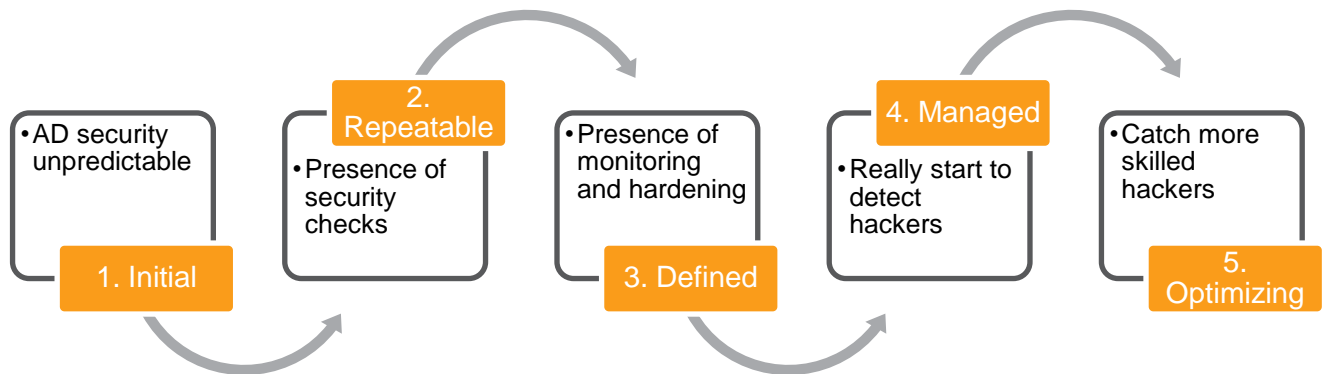**Active Directory Security Maturity Self-Assessment**

Version: 1.0

A. Maturity methodology

This maturity methodology is based on CMMI where each step has been adapted to the specificity of Active Directory.

B. Self evaluation

The goal of this self-Assessment is to evaluate your level of maturity in term of security regarding other peers. Answer these simple questions with "yes" or "no" based on your security current capabilities and practices.

1. Initial

- Do ALL Active Directory are being known and assigned to an owner accountable for its security?
- Do ALL trusts with third parties, external companies have been removed or does the risk associated with them has been mitigated through formal risk acceptance ?

2. Repeatable

- Does processes exist to regularly check if the basics (provisioning & deletion, privileged accounts management, AD interconnection, known vulnerabilities) are in place ?
- Has the risk of cross domain contamination (SID Filtering enforced everywhere except when a migration is in progress) has been evaluated ?

3. Defined

Basic monitoring

- Does the addition of a new administrator raise an alert ?
- Are there a log of all actions related to AD configuration changes (GPO, group membership) ?

Basic hardening

- Does an administrator have a specific account different from its day-to-day account for its admin activities ?

- Does a limit on the number of administrator is enforced on a forest basis and do the administrators have signed a charter defining their responsibilities ?

4. Managed

Effective monitoring & forensic

- Does a process exists to handle the monitoring alerts in an acceptable time frame ?
- Do the login logs being collected allowing to find in which computer a user logged on and vice-versa ?

Preventing some attacks

- Are there any enforcement prohibiting a domain administrator account to login on workstations ?
- Do you have a bastion or requesting domain administrators to use 2 factors authentication ? (ex: PIV, GIDS smart cards)
- Do old protocols (NTLMv1, LM, null session, SMBv1, …) being disabled including in domain controllers ?

5. Optimizing

- Do you have a watch process regarding new attacks ?

Hunting

- Does a process to check for Active Directory compromise (backdoor) is in place ?
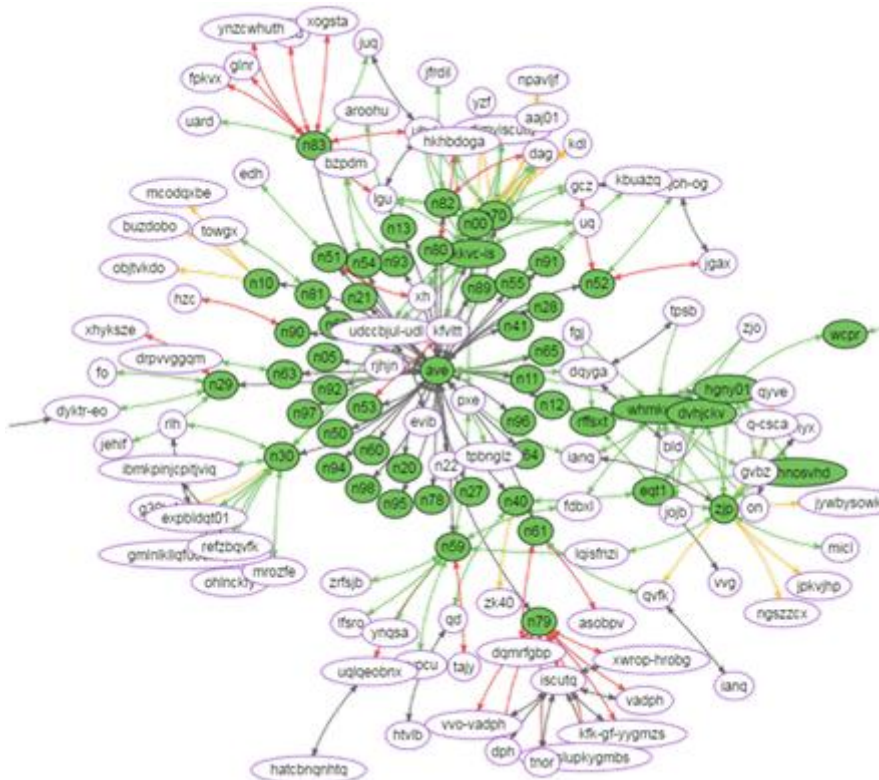- Can persistence or cross domain moves (Golden Ticket, DCSync) be detected ?

C. Improve your maturity level

1. Initial

- Execute PingCastle and build the domain cartography.
- Configure the PingCastle reporting by assigning each domain to its owner.
- Prepare the trust removal with unknown third party.

Indicators: # of domains found, # of domains without owner

2. Repeatable

- Run PingCastle on each domain on a weekly basis (to detect quickly new trusts) and report to the management about the deployment & score evolution.
- Involve all owners to put in place SID Filtering except for migrations which should be limited in time. Configure these migrations into the reporting configuration of PingCastle to follow them.

Indicators: # of domain covered, # of trust without SID Filtering, Average score

3. Defined

Basic monitoring

- Collect configuration change and membership events (example: Windows Event Forwarding, Log collection product or AD security product). This is the minimum set of events you have to collect.

- Configure alerts related to administrators' groups membership changes.

Basic hardening

- Built an Active Directory security standard which will specify for example that privileged accounts should not be used in day-to-day activities.
- Cross check the list of administrators reported in PingCastle with the list of users having sign your administrator charter.

Indicators: # of domain & DC covered, # of alerts configured, presence of security standard, # of admin signature

4. Managed

Effective monitoring & forensic

- Collect more logs and specifically the authentication log to be able to correlate user & computer activities. Multiply by 10 the storage used.
- See "Best Practices for Securing Active Directory" and its appendix L.
- Involve your SOC/CERT teams and design some detection rules (service account used on a workstation, multiple connections, connection of a VIP workstation, ...)

Preventing some attacks

- Involve the administrators to build security GPO:
- old protocols removing,
- login restriction
- new security settings activated
- Put in place a security bastion, or use dedicated workstations for admin and use 2 factor authentication using smart cards

Indicators: # of alert designed, # of sensitive assets covered by alerting, # of domains with better security settings

5. Optimizing

- Put in place a watch process for new attacks (twitter, conference, ...)

Hunting

- Use ACL analysis tool such as AD Control Path, BloodHound or PingCastle
- Establish rules or install product to cover specific AD attacks

Indicators: time between a new attack and its mitigation