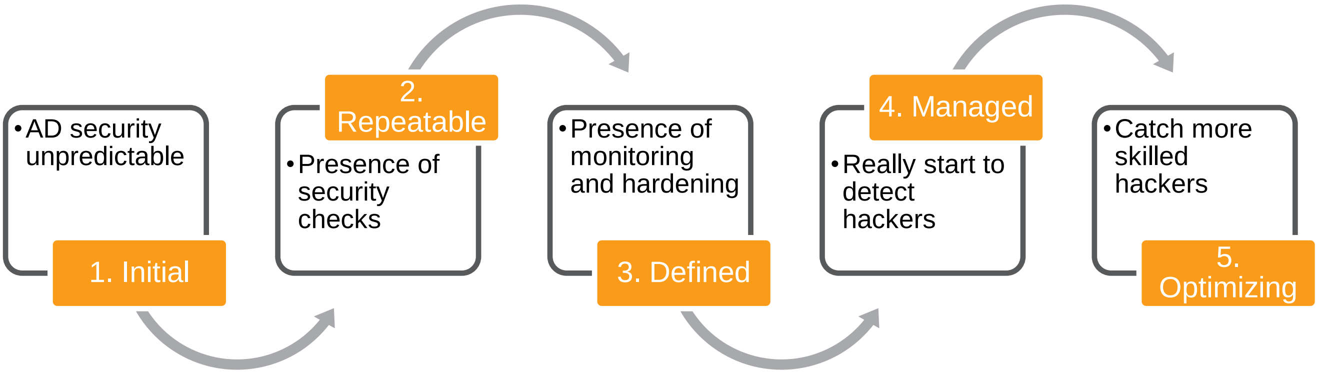
Active Directory Security Maturity Self-Assessment

Version: 1.4

Ping Castle SAS
46 rue de l'Alma
92400 Courbevoie
France

A. Maturity methodology

This maturity methodology is based on CMMI where each step has been adapted to the specificity of Active Directory. As a reminder CMMI is a brand from the Carnegie Mellon university and it is used in this document as a reference for the 5 maturity steps.



•AD security unpredictable
1. Initial
2. Repeatable
•Presence of security checks
•Presence of monitoring and hardening
3. Defined
4. Managed
•Really start to detect hackers
•Catch more skilled hackers
5. Optimizing

1. Initial

"Know your Backyard"

This step is what is called a scope. While it is relatively easy to define the scope for a project, this is a challenge on a security perspective given the fact that an Active Directory security project starts without knowing all the AD in an Enterprise scope. It can contains relationship with AD not in the company's scope.

2. Repeatable

"Perform Security Controls periodically"

This step ensures that a consistent set of actions are performed. There is no written document yet but ensure basic vulnerabilities are checked.

3. Defined

"Prove to the management and auditors you are doing something"

This step aims at document the processes already in place. For Active Directory that means that the process to detect hacker, aka monitoring is in place and the vulnerabilities are limited by an hardening project. Detection rules and hardening rules are written in an auditable document.

4. Managed

"Follow the effectiveness of your controls"

KPI are produced and checked in this step. This ensures the effectiveness of the processes in place.

5. Optimizing

"Be at the tail of hackers"

In this step, continuous improvement is in place. News attacks are mitigated quickly and hunting is in place.

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

Processes to follow on this step are:

1.1 Domain coverage

1.2. Ownership

1.3: External trusts

1.1 Domain coverage

"Do you actually know how many domains you have in your Active Directory?"

Description

The domain coverage is the first and foremost step in order to start securing your Active Directory. This step is there to ensure that the whole perimeter of the company is covered and that there is no hidden domains.

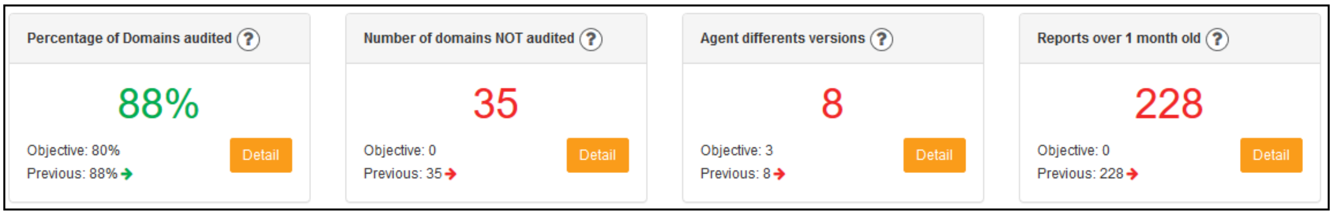
The section's purpose is to give insights of the current status of the deployment of the tool in your perimeter through relevant objectives and KPI.

Please note that if you identify a domain monitored by the PingCastle tool but that is out of your scope (external company for instance), we recommend to:

- **Remove** all the trusts
- **Scan** the domain where the trust has been detected
- **Classify** the domain as out of scope.

Furthermore, it is possible to completely remove a domain, but it is important to not forget **to scan this domain again after its removal** as well as to **set the domain as "removed".**

KPI to follow



Percentage of Domains audited ?
88%
Objective: 80%
Previous: 88% →

Number of domains NOT audited ?
35
Objective: 0
Previous: 35 →

Agent differents versions ?
8
Objective: 3
Previous: 8 →

Reports over 1 month old ?
228
Objective: 0
Previous: 228 →

- Percentage of domains audited

Objective: more or over 80%

- Number of domains not audited

Objective: 0

- Number of versions of PingCastle

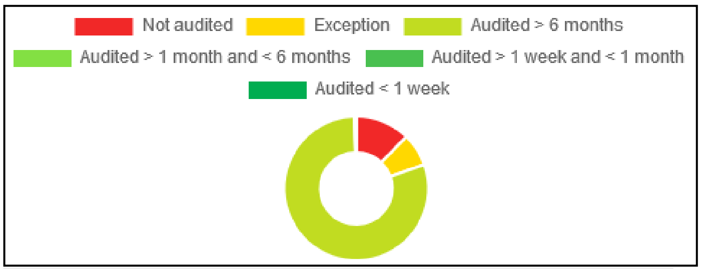
Objective: less or equal than 3

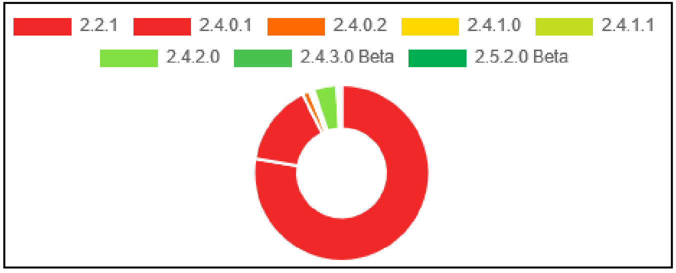
- PingCastle reports over 1 month old

Objective: 0

Indicators to collect:

- Status of the domains (not audited, in exception, audited > 6 months, audited > 1 months and < 6 months, audited > 1 week and <1 month and audited < 1 week)
- Versions of PingCastle deployed





1.2 Ownership

"Are you sure that all your domains are actually monitored by someone?"

Description

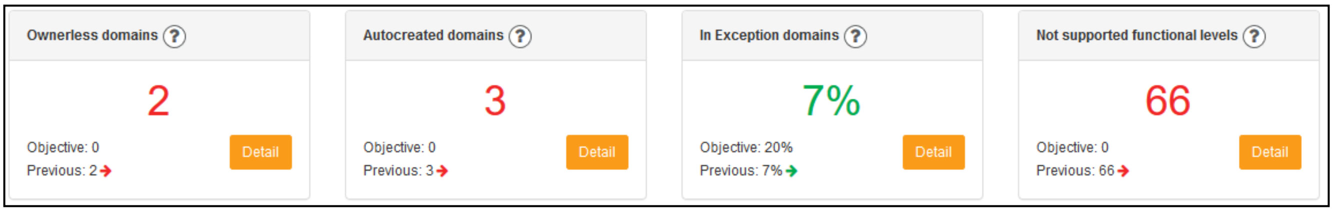
Once you have a clear view of your whole perimeter, the best course of action to define clearly the ownership of each and every domains.

It is critical that people actually feel included in the processes in order for the security to improve.

The purpose of this step to ensure that each and every domains are assigned to an Owner entity accountable for its security, because it is critical that people actually feel included in the processes. A few points about the Ownership :

- When a domain is added in the PingCastle solution, it will often be either **Ownerless**, **Auto Created**, or **both**. This has to be temporary
- It is possible to put a domain in exception, meaning the domain score won't impact the global score. Nevertheless, **this feature is exceptional**
- It is also highly recommended to ensure that functional levels used are still supported, both by the PingCastle tool but also by Microsoft itself.

KPI to follow:



Ownerless domains ?

2

Objective: 0
Previous: 2 →

Detail

Autocreated domains ?

3

Objective: 0
Previous: 3 →

Detail

In Exception domains ?

7%

Objective: 20%
Previous: 7% →

Detail

Not supported functional levels ?

66

Objective: 0
Previous: 66 →

Detail

- Number of ownerless domains

Objective: 0

- Number of domains auto-created

Objective: 0

- Percentage of domains in exception

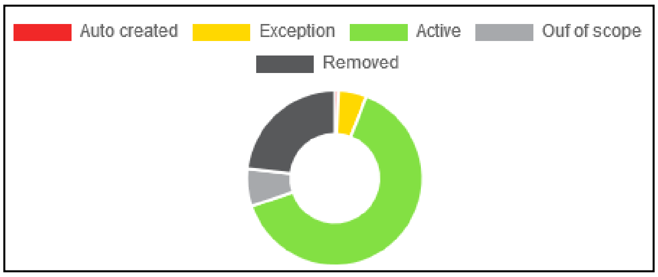
Objective: less than 20%

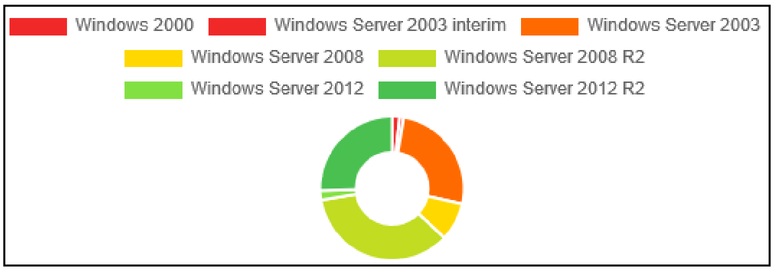
- Number of domains having an unsupported functional level

Objective: 0

Indicators to collect:

- Status of the domains (Auto created, in exception, active, out of scope, removed)
- Functional level of the Active Directory domains





1.3 External trusts

"Are you aware that your domains are exposed on the Internet without protection?"

Definitions

Here are the different type of trusts:

- **To Out of scope domains:** Between one of your domain and a domain not managed by you.

This trust should be removed

- **To Removed domains:** Between one of your domain and a removed domain. This trust should be removed
- **To Unsafe domains:** Between one of your domain and a domain not monitored by PingCastle. This trust Should either be removed or the non managed domain should be added to PingCastle
- **To Auto-Created domains:** Between one of your domain and a domain that is Auto-Created. The Auto-Created domain should be reviewed
- **Other**: Between domains without particular attention points

Description

Now that the perimeter is under control, the goal is to reduce the surface of exposition on the Internet of this perimeter.

Indeed, trusts towards uncontrolled domains can induce major security risks.

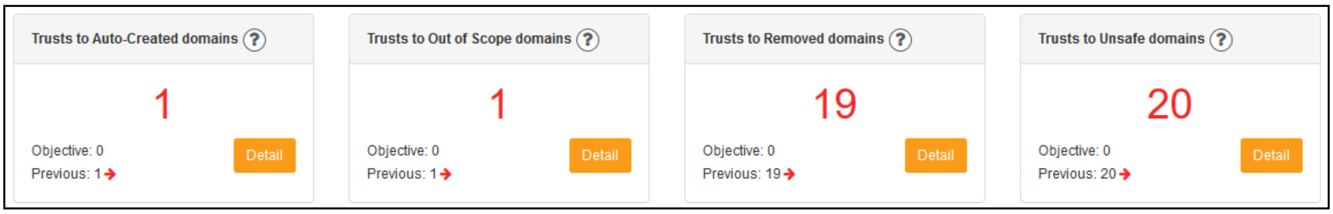
This final part of the level 1 maturity is about the exposure of the Active Directory on the Internet. External trusts are often overlooked while they represent one of the major entry point for a lot of elaborated and targeted attacks.

The goal of this section is to reduce as much as possible the number of external trusts that are neither controlled nor secured. This can apply to several types of trusts:

- Trusts to domains that don't have clearly identified ownership
- Trusts to domains that are out of your scope
- Trusts to domains that have been removed
- Trusts to domains neither protected nor monitored

Do remember that if you remove a trust, it is highly recommended to perform a scan on all domains again to notify the PingCastle tool of the trust removal

KPI to follow



Trusts to Auto-Created domains ?

1

Objective: 0

Previous: 1 →

Detail

Trusts to Out of Scope domains ?

1

Objective: 0

Previous: 1 →

Detail

Trusts to Removed domains ?

19

Objective: 0

Previous: 19 →

Detail

Trusts to Unsafe domains ?

20

Objective: 0

Previous: 20 →

Detail

- Number of trusts to auto-created domains

Objective: 0

- Number of trusts to out of scope domains

Objective: 0

- Number of trusts to remove domains

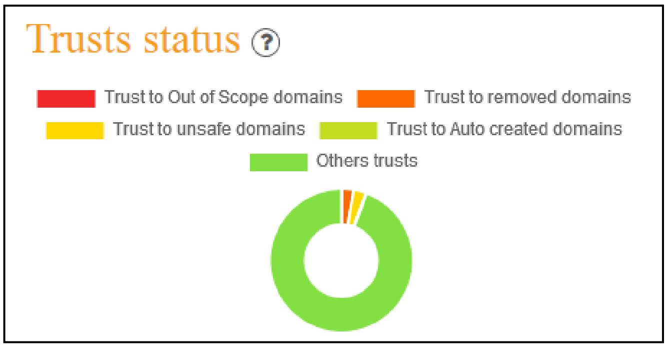
Objective: 0

- Number of trusts to unsafe domains

Objective: 0

Indicators to collect:

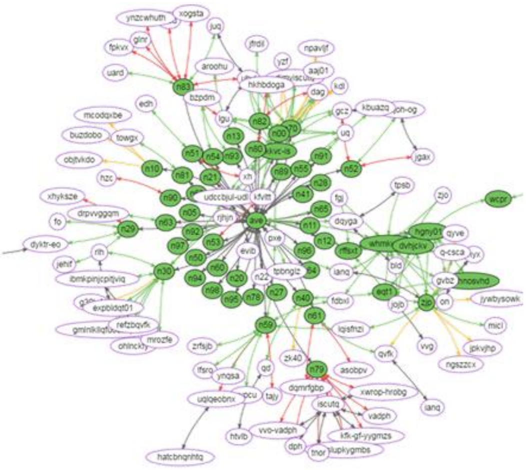
- Trusts
- Status of trusted domains



Management decisions

Here are the management decisions that should be taken:

- 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.



2. Repeatable

Processes to follow on this step are:

2.1 Internal trusts

2.2 Lower the risk score

2.1 Internal trusts

"Do you realize that badly implemented trusts provoke a major risk of cross-contamination?"

Description

The idea here is that now that all the perimeter is under control and that you have identified all your trusts, it is important to actually secure them properly.

Indeed, once a domain is compromised, it can be used to compromise others, so internal protections should be well enforced.

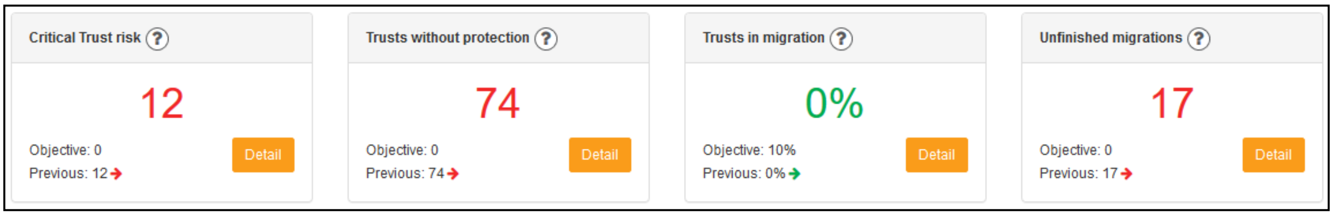
This step in the maturity process is about the internal exposure of domains caused by interconnections between domains. Indeed, each and every unprotected interconnections represents a risk of cross-contamination in case of security breach.

The aim of this section is to take actions regarding two main points:

- Internal trusts that are not following basic security rules
- Migrations between domains that are either ongoing or unfinished

Do remember that if you remove a trust, it is highly recommended to perform a scan on all domains again to notify the PingCastle tool of the trust removal

KPI to follow



Critical Trust risk ?
12
Objective: 0
Previous: 12 →
Detail

Trusts without protection ?
74
Objective: 0
Previous: 74 →
Detail

Trusts in migration ?
0%
Objective: 10%
Previous: 0% →
Detail

Unfinished migrations ?
17
Objective: 0
Previous: 17 →
Detail

- Number of trusts in critical status (trust score = 100)

Objective: 0

- Number of trusts without protection (without SID Filtering)

Objective: 0

- Number of trusts in migration (declared in the risk register)

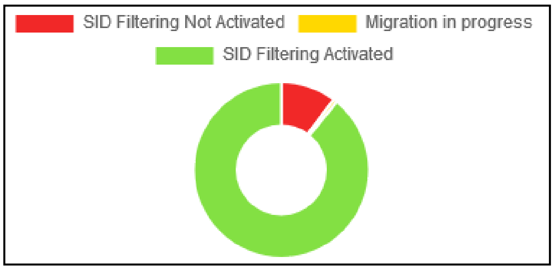
Objective: less or equal than 10%

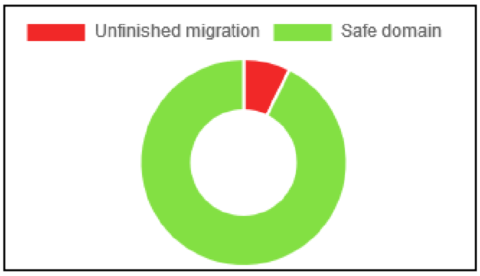
- Number of unfinished migration (presence of SID History)

Objective: 0

Indicators to collect:

- Activation status of SID Filtering
- Register of migrations in progress
- Absence of SIDHistory proving the completion of a migration





2.2 Lower the risk score

"Are you aware of all the possible security issues that may be in your Active Directory?"

Description

This step focus on the Global Risk of an AD. This Global score represents the level of risk of the AD and the long-term objective should be to lower this score.

This can be done by going step by step, focusing on the higher scores first.

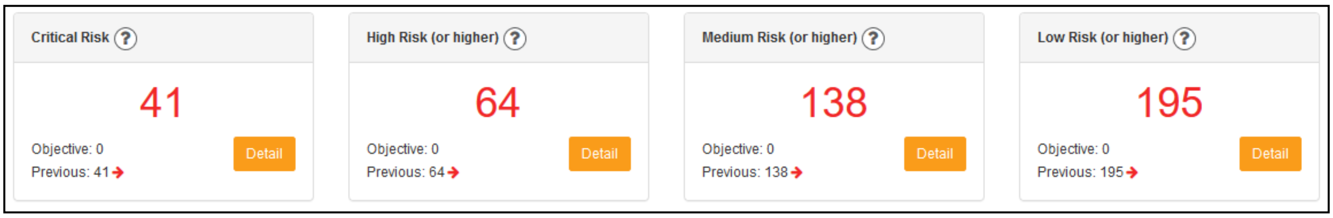
The goal of this section is to go further in the security assessment of your Active Directory using a Global Risk Score

This score is calculated by taking the maximum of the 4 sub-processes:

- Staled objects
- Privileged accounts
- Trusts
- Anomalies

Do note that the maximum is computed on a per report basis and is not the maximum of the sub processes average. Each sub-process score is calculated regarding many technical rules and automatically calculated by the Ping Castle tool.

KPI to follow



Critical Risk ?

41

Objective: 0

Previous: 41 →

Detail

High Risk (or higher) ?

64

Objective: 0

Previous: 64 →

Detail

Medium Risk (or higher) ?

138

Objective: 0

Previous: 138 →

Detail

Low Risk (or higher) ?

195

Objective: 0

Previous: 195 →

Detail

- Number of domain with critical risk (score = 100)

Objective: 0

- Number of domain with high risk (score >= 75 and < 100)

Objective: 0

- Number of domain with high risk (score >= 50 and < 75)

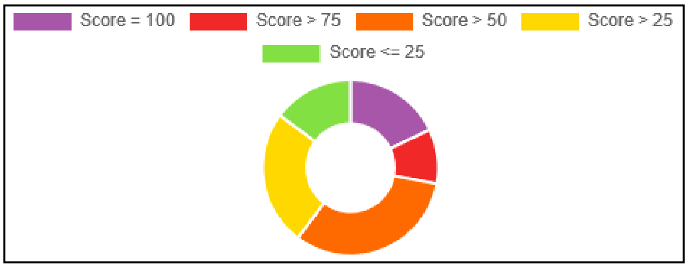
Objective: 0

- Number of domain with low risk (score >= 25 and < 50)

Objective: 0

Indicators to collect:

- Risk score of all Active Directory domains



Management decisions

Here are the management decisions that should be taken:

- 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.

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