Developing a Comprehensive Active Directory Security Metric

Friedwart Kuhn, Heinrich Wiederkehr, Nina Matysiak

Friedwart Kuhn
Digitally signed by Friedwart Kuhn
Date: 2018.03.15 13:54:43 +01'00'

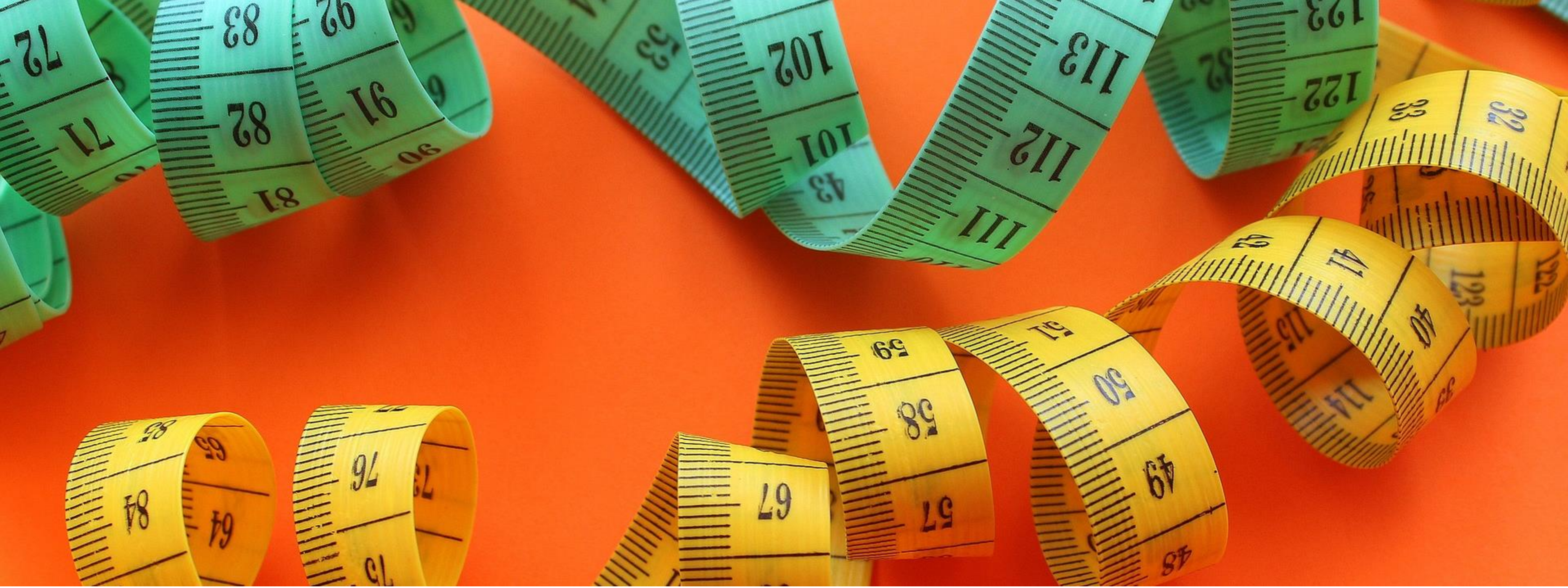
TROOPERS
MAKE THE WORLD A SAFER PLACE

Agenda

- Who We Are
- Introduction: Problem Statement & Why Security Metrics
- Development of an Active Directory Security Metric
- Where Do We Stand
- Where Do We Want To Go
- Lessons Learned

Who We Are

- Friedwart Kuhn
  - Head of Microsoft Security Team @ERNW
  - 15+ years experience in security assessments, administration, publications and trainings
  - IT security professional with a strong focus on Active Directory Security
- Heinrich Wiederkehr
  - Member of Microsoft Security Team @ERNW
  - 5+ years in security assessments and trainings
  - IT security professional with a focus on Windows Security and Active Directory Security
- Nina Matysiak
  - Member of Microsoft Security Team @ERNW
  - 3+ years in security assessments
  - IT security professional with a focus on Windows Security and Active Directory Security



Introduction

Problem Statement & Why Security Metrics

Memo *From: CEO*
To: ISO

“Dear John,

I am under renewed pressure from the board to clarify a few things about your budget proposals for the financial year ahead. Please, would you address the following issues in writing before the next board meeting:

A) We have spent a small fortune on information security in the past three years: naturally, this seemed justified at the time, but it is perfectly reasonable for the board to ask what we have actually achieved in the way of a return on our investment to date? Can you put a figure on it? Can you demonstrate the value?

…Continuation of the Memo

B) **How does our information security stack up against our peers in the industry? How secure are we, and how secure do we need to be?** Some of the more cynical members of the board are starting to express the opinion that we are going for gold when silver will do, and I must admit I have some sympathy for that viewpoint.

C) If budget cuts are necessary (which looks increasingly likely), **in which areas can we safely trim back on security spending** without jeopardizing the excellent progress we have already made?

Looking forward maybe three to five years, can you please give us a clearer picture of how the information security management system will pan out?

Regards, Fred B (CEO)”

From [2], p. xvii

What do you feel…?

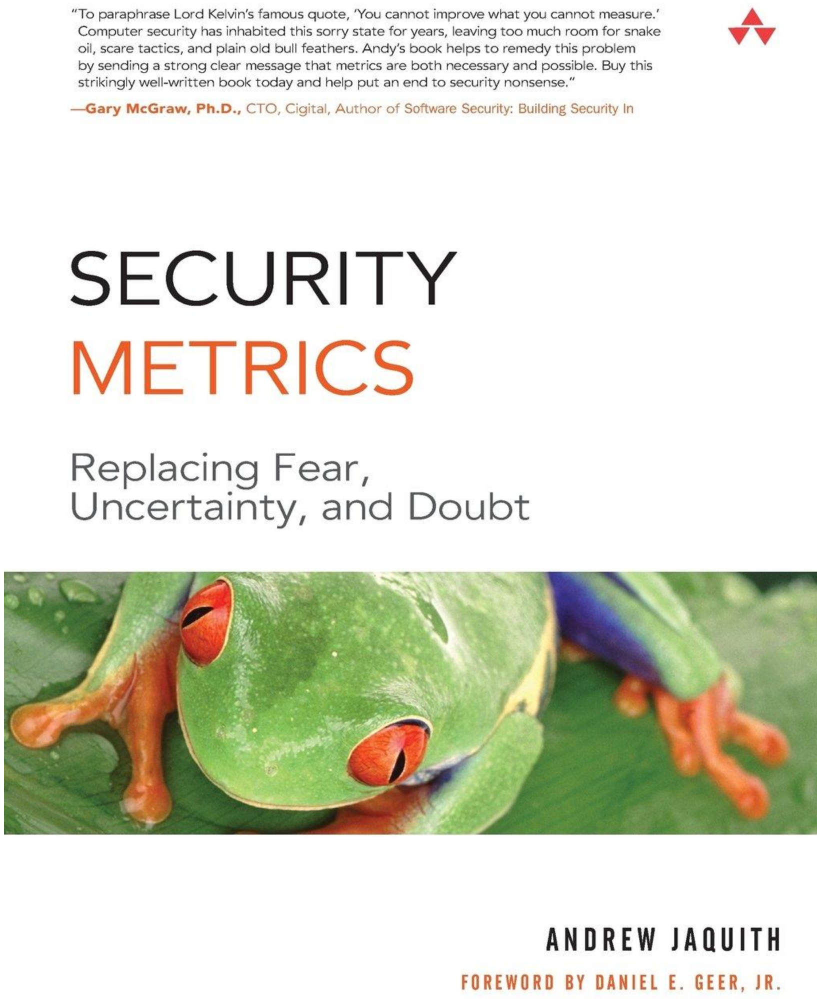
- Indisposition…?
- Uncertainty…?
- Headaches…?

Why??

Reasons for a (Security) Metric

○ “To measure is to know.” (Lord Kelvin)

○ “If you can not measure it, you can not improve it.” (Lord Kelvin)



“To paraphrase Lord Kelvin’s famous quote, ‘You cannot improve what you cannot measure.’ Computer security has inhabited this sorry state for years, leaving too much room for snake oil, scare tactics, and plain old bull feathers. Andy’s book helps to remedy this problem by sending a strong clear message that metrics are both necessary and possible. Buy this strikingly well-written book today and help put an end to security nonsense.”

—**Gary McGraw, Ph.D.,** CTO, Cigital, Author of Software Security: Building Security In

SECURITY METRICS

Replacing Fear, Uncertainty, and Doubt

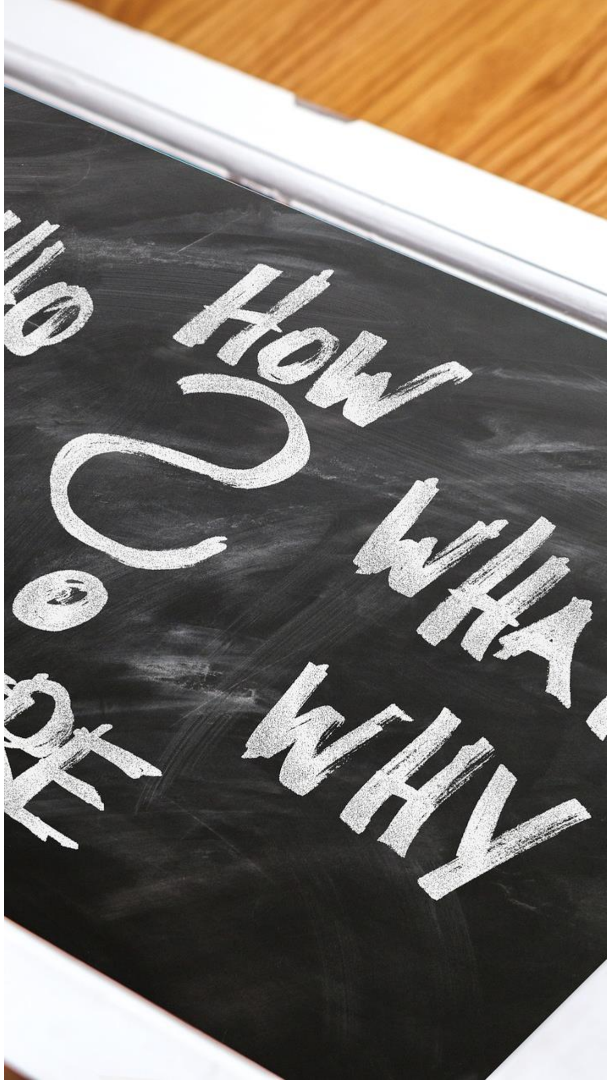
ANDREW JAQUITH

FOREWORD BY DANIEL E. GEER, JR.

ERNW
providing security.

Reasons for an *Active Directory* Security Metric?

- 1. Because it does not exist!



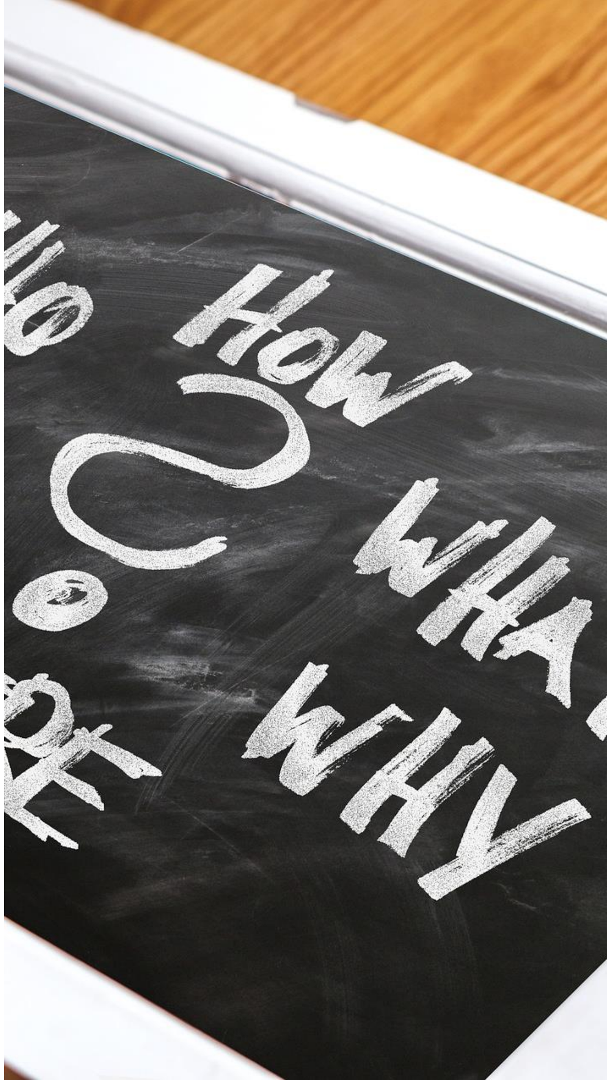
The Goal

- To design a well-defined Active Directory security metric that:
  a) 'looks' at the security-relevant indicators of Active Directory
  b) and that measures these indicators in a meaningful way

- The metric is intended for Active Directory responsible personnel and experts

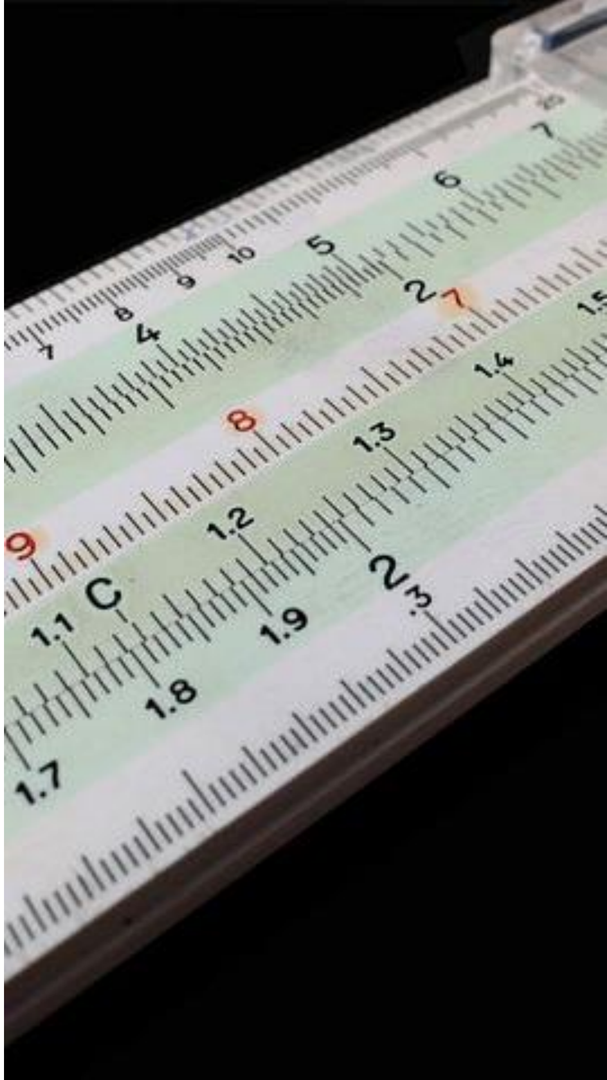
Reasons for an *Active Directory* Security Metric?

- 2. To measure Active Directory security and thus being enabled to answer the awkward questions.



Terminology

- "**Metric**" is "a system or standard of measurement" (Oxford American Dictionary)

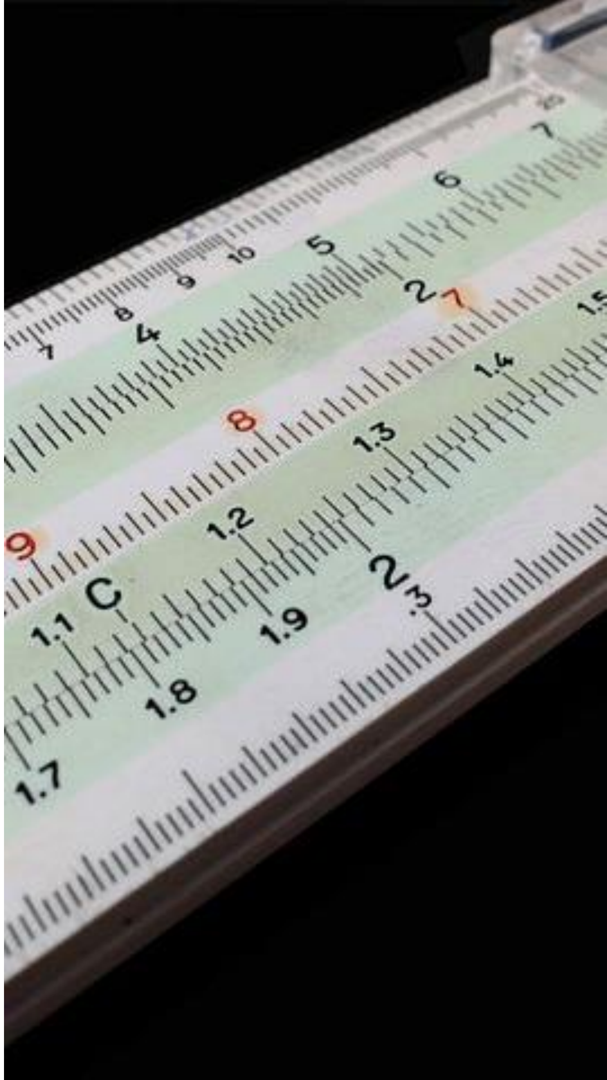


ERNW
providing security.

Terminology (well-known)

- **Measure**: (verb) action to determine one or more parameters of something
- **Measuring point**: is the “location”, where the measure is taken (‘height’ of a door)
- **Measurement**: is the result of the action of measuring, the value of a parameter for something, ideally expressed in defined units (the height of the door is 2 meters)
- **Measuring Instrument**: in short “instrument” is, a “device“ for measuring (‘measuring tape’)

Cf. [2], p. 10.



Terminology - Key Security Indicator (KSI)

- *KSI*: A quantifiable measure used to evaluate the security state of an IT security-relevant component
    - (cf. *KPI* in Oxford Living Dictionary)
  - A KSI can equal a measurement (i. e. the value of the measurement) or it can be the result of a (mathematical and/or logical) operation applied to the measurement

- KSI with respect to AD:
  - **A quantifiable measure used to evaluate the security state of a security-relevant item of an AD**

KSIs Are Derived/Defined From…

- (AD) Findings, Respectively Their Corresponding Security Best Practices
  - Security best practice: No end-of-life systems
  - KSI: Number of EoL systems in use

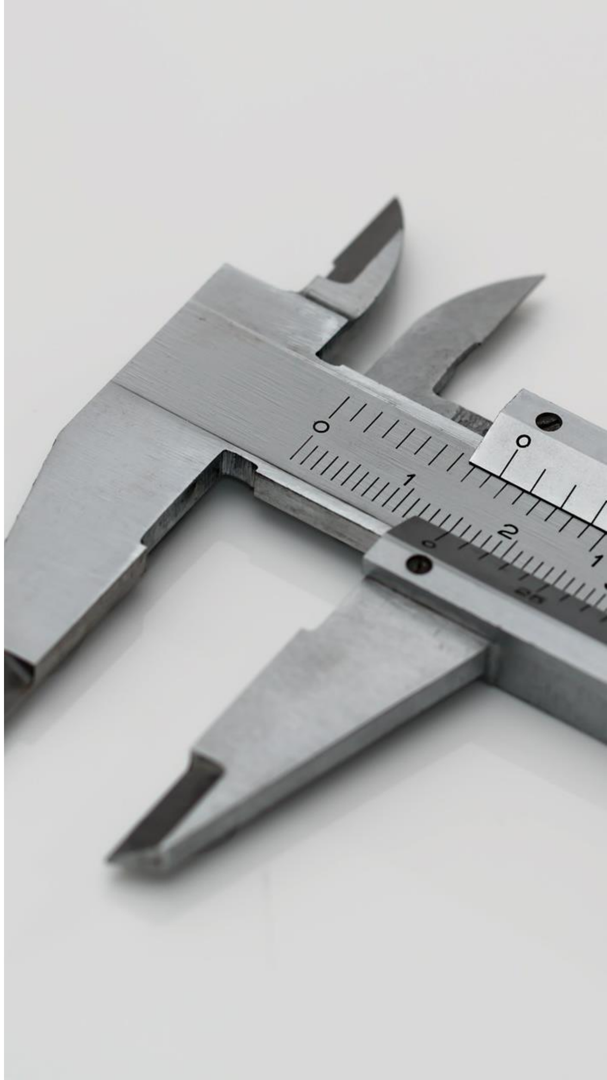
- Recommendations From (AD) Security Professionals' Experience
  - Recommendation: Secure configuration of the ACL of the AdminSDHolder object
  - KSI: Number of accounts with read and write permissions on the object that differ from the default

KSIs Are Derived/Defined From…

- (AD) Vendor Recommendations
  - Recommendation: No DC of internal AD in DMZ
  - KSI: Number of DCs of internal AD in DMZ

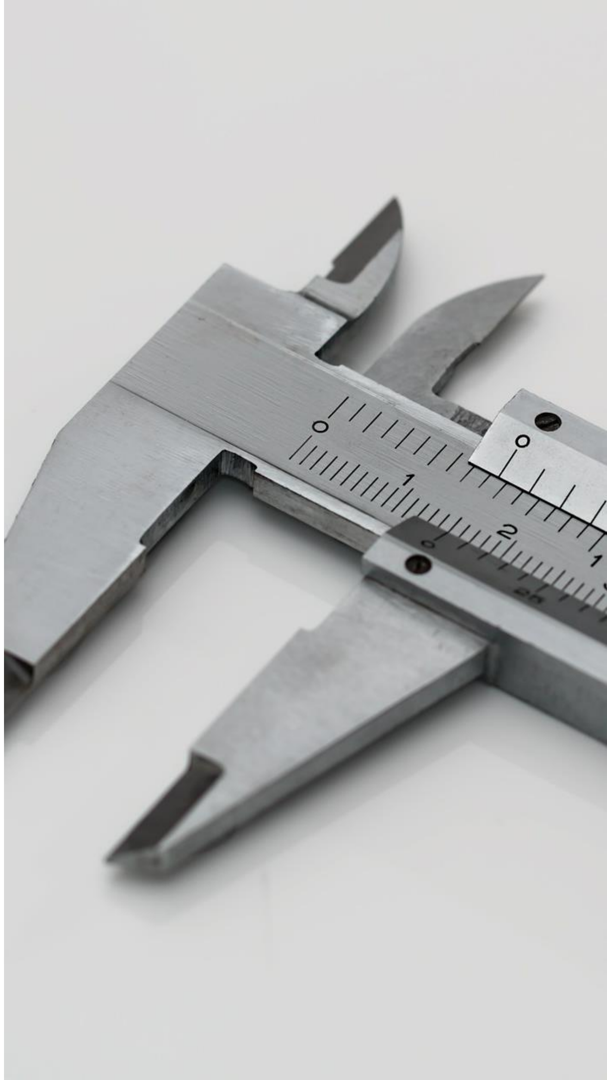
Prerequisites of a Well-Designed AD Security Metric

- “Good Metric”
- Well-designed with respect to AD



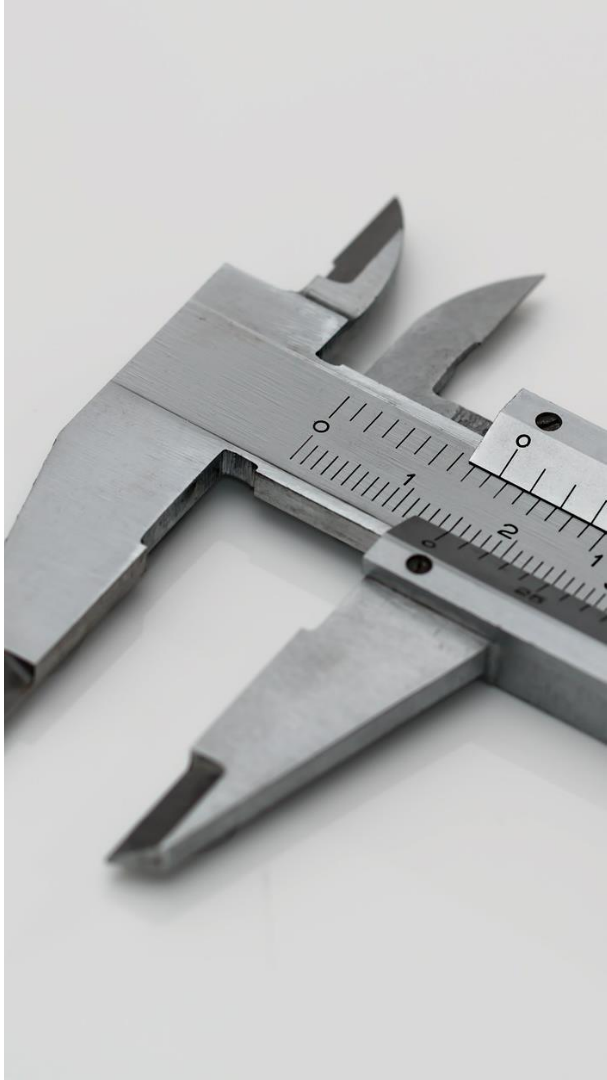
Attributes of a Good Metric

- Consistently measured
  - Sample: number of systems with disabled UAC collected via PS script
- Cheap to gather
  - Sample: GPO data can be accessed with standard user rights (including GPOs with UAC settings)
- Expressed as a number or percentage
  - Sample: number/percentage of systems with UAC disabled per Domain
- Contextually specific



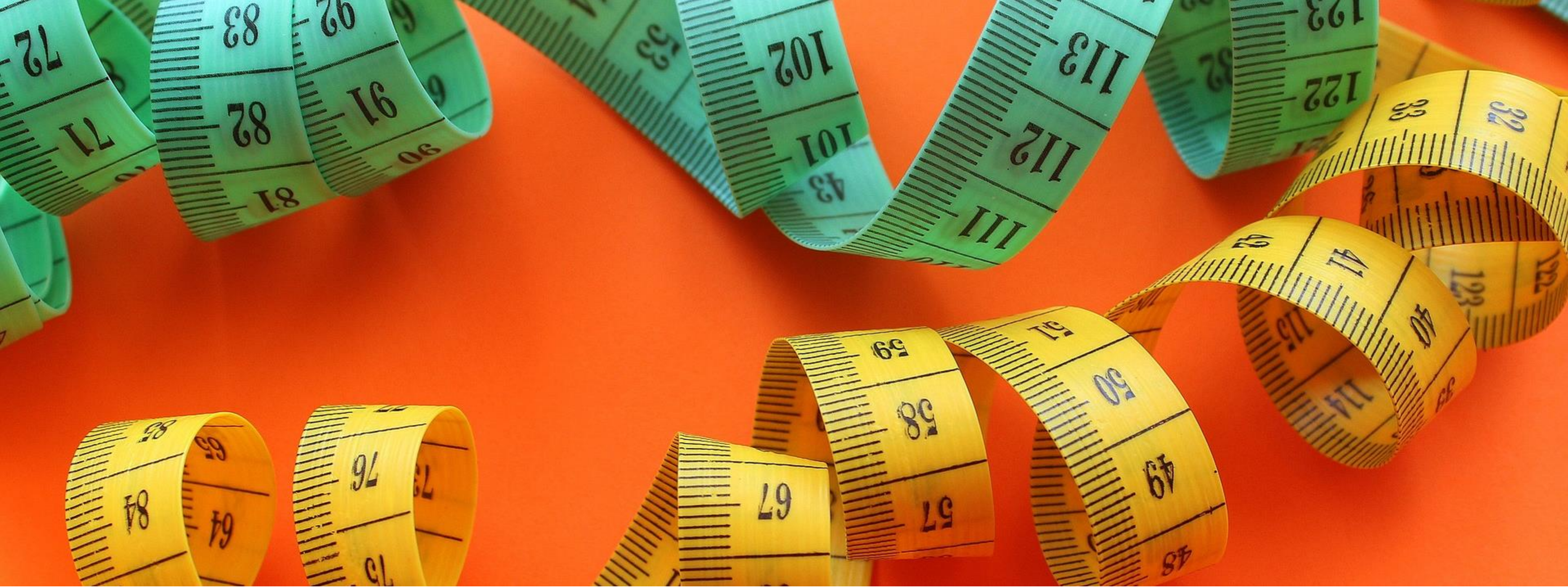
Prerequisites of a Well-Designed *Active Directory* Security Metric

- Carefully chosen measuring points
- Well-defined measuring methods (operations/algorithms) to measure these KSIs (How do you measure the security of UAC?)
  - Laborious part of the work



Disclaimer

- This talk…
  - …describes the development process of an AD security metric
  - …describes where we came from, where we currently stand and where we want to go
- It´s not about…
  - …an already completed metric
  - …a security monitoring framework



Development of an Active Directory Security Metric

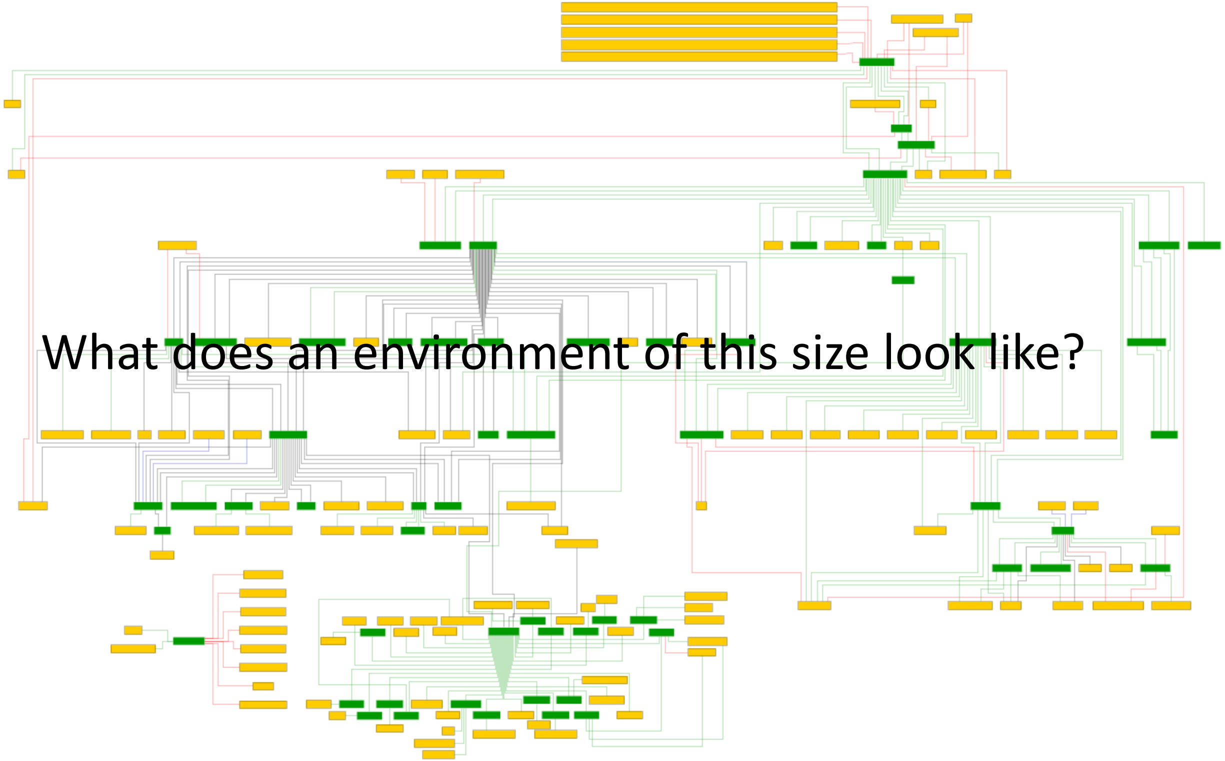
Before the Idea of an AD Security Metric

ERNW
providing security.

Initial Situation

- Project:
  - Extensive AD security assessment in form of an audit of more than 50 international AD forests

- Our goals and requirements:
  - Standardize the assessment methodology to (rapidly) gather and analyze information of multiple AD environments
  - Do not require direct access to the AD environments
  - Perform assessment with least possible privileges
  - Still obtain data that enables us to meaningfully assess the security of an AD

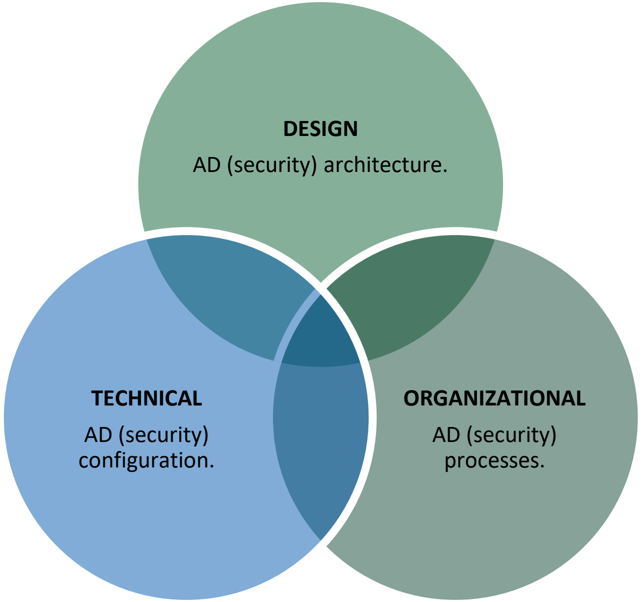


What does an environment of this size look like?

Implications of the Project Goals for the Assessment

- Define possible findings, ratings, and recommendations beforehand
  - Creates a static framework applicable to every AD
- Define clear guidelines for the assessment
  - Different people come to the same conclusions
- Automate as much as possible
  - Makes the assessment consistent and less error prone
- Information gathering in AD only with standard user permissions
  - Raises acceptance of performing the assessment
  - Limits discussions with administrators

Assessed Areas



DESIGN

AD (security) architecture.

TECHNICAL

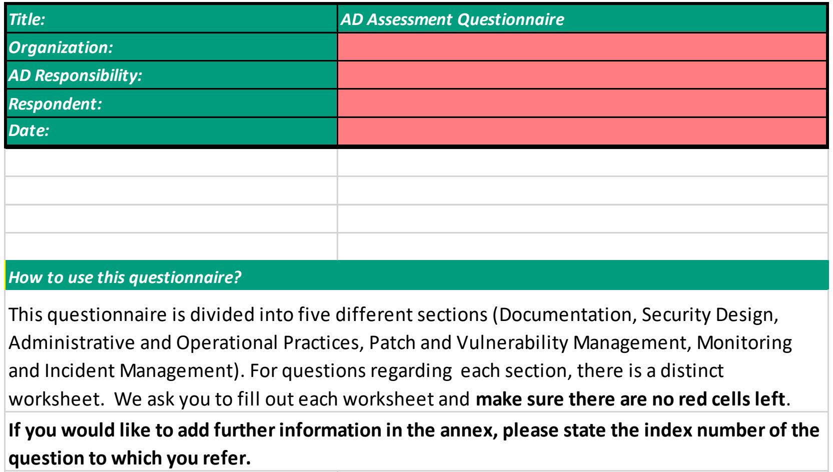
AD (security) configuration.

ORGANIZATIONAL

AD (security) processes.

Assessment Tools We Created I

- AD Auditing Questionnaire
  - Covering five areas of AD security
    - Documentation
    - Security Design
    - Admin and Operational Practice
    - Patch and Vulnerability Management
    - Monitoring and Incident Handling



Title:	*AD Assessment Questionnaire*
Organization:	
AD Responsibility:	
Respondent:	
Date:	

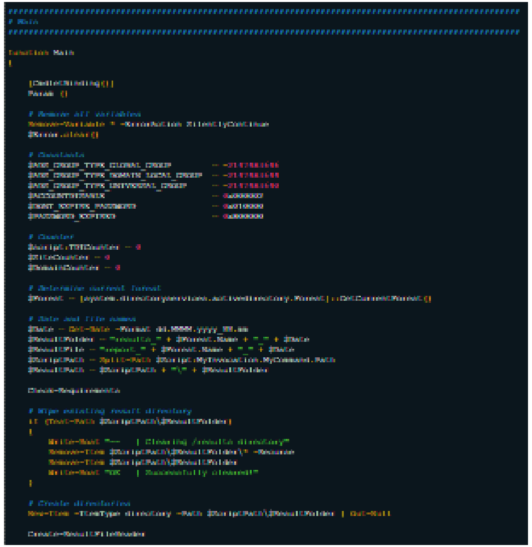
How to use this questionnaire?

This questionnaire is divided into five different sections (Documentation, Security Design, Administrative and Operational Practices, Patch and Vulnerability Management, Monitoring and Incident Management). For questions regarding each section, there is a distinct worksheet. We ask you to fill out each worksheet and **make sure there are no red cells left**.

If you would like to add further information in the annex, please state the index number of the question to which you refer.

Assessment Tools We Created II

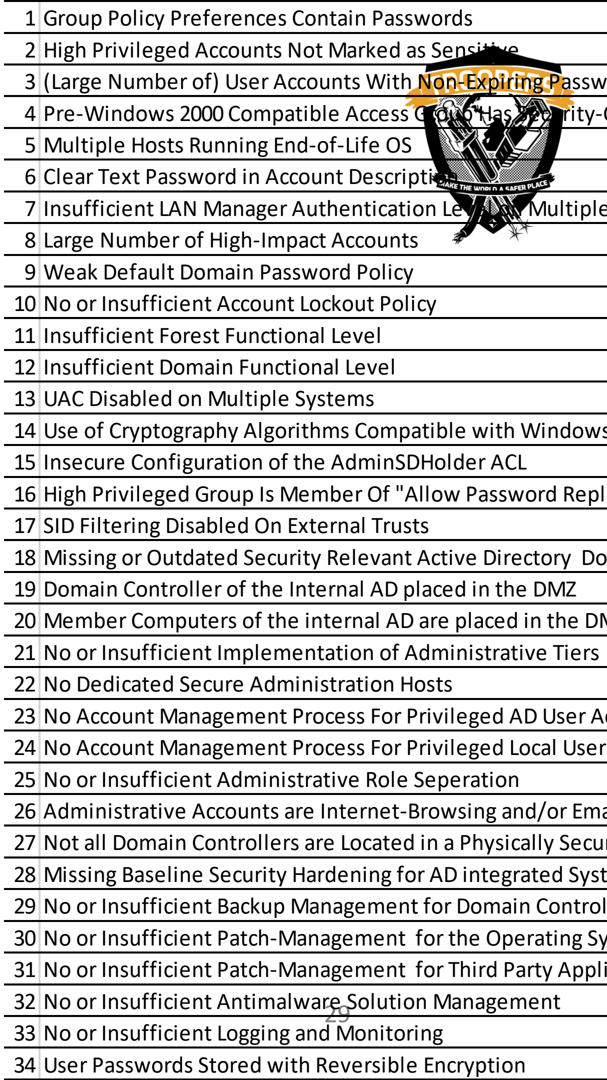
- AD Auditing script(s)
  - PowerShell-based
  - Requires only standard domain user permissions
  - Collects relevant technical AD configuration
  - Interprets collected data



```
##########################################################################
# Main
##########################################################################

function Main
{

    [CmdletBinding()]
    Param ()

    # Remove all variables
    Remove-Variable * -ErrorAction SilentlyContinue
    $Error.clear()

    # Constants
    $ADS_GROUP_TYPE_GLOBAL_GROUP         = -2147483646
    $ADS_GROUP_TYPE_DOMAIN_LOCAL_GROUP   = -2147483644
    $ADS_GROUP_TYPE_UNIVERSAL_GROUP      = -2147483640
    $ACCOUNTDISABLE                      = 0x000002
    $DONT_EXPIRE_PASSWORD                = 0x010000
    $PASSWORD_EXPIRED                    = 0x800000

    # Counter
    $script:TOTCounter = 0
    $FileCounter = 0
    $DomainCounter = 0

    # Determine current forest
    $Forest = [System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()

    # Date and file names
    $Date = Get-Date -Format dd.MMMM.yyyy_HH.mm
    $ResultFolder = "results_" + $Forest.Name + "_" + $Date
    $ResultFile = "report_" + $Forest.Name + "_" + $Date
    $ScriptPath = Split-Path $Script:MyInvocation.MyCommand.Path
    $ResultPath = $ScriptPath + "\" + $ResultFolder

    Check-Requirements

    # Wipe existing result directory
    if (Test-Path $ScriptPath\$ResultFolder)
    {
        Write-Host "--    | Cleaning /results directory"
        Remove-Item $ScriptPath\$ResultFolder\* -Recurse
        Remove-Item $ScriptPath\$ResultFolder
        Write-Host "OK    | Successfully cleaned!"
    }

    # Create directories
    New-Item -ItemType directory -Path $ScriptPath\$ResultFolder | Out-Null

    Create-ResultFileHeader
```

Assessment Tools We Created III

- Evaluation of the script and questionnaire data could lead to 34 possible pre-defined findings
  - Findings 1-17 + 34 are from the audit script
  - Findings 18-33 are from the audit questionnaire
  - Findings pre-defined but rating and finding text may differ depending on the evaluation



1	Group Policy Preferences Contain Passwords
2	High Privileged Accounts Not Marked as Sensitive
3	(Large Number of) User Accounts With Non-Expiring Passw
4	Pre-Windows 2000 Compatible Access Group Has Security-(
5	Multiple Hosts Running End-of-Life OS
6	Clear Text Password in Account Description
7	Insufficient LAN Manager Authentication Level on Multiple
8	Large Number of High-Impact Accounts
9	Weak Default Domain Password Policy
10	No or Insufficient Account Lockout Policy
11	Insufficient Forest Functional Level
12	Insufficient Domain Functional Level
13	UAC Disabled on Multiple Systems
14	Use of Cryptography Algorithms Compatible with Windows
15	Insecure Configuration of the AdminSDHolder ACL
16	High Privileged Group Is Member Of "Allow Password Repl
17	SID Filtering Disabled On External Trusts
18	Missing or Outdated Security Relevant Active Directory Do
19	Domain Controller of the Internal AD placed in the DMZ
20	Member Computers of the internal AD are placed in the DM
21	No or Insufficient Implementation of Administrative Tiers
22	No Dedicated Secure Administration Hosts
23	No Account Management Process For Privileged AD User A
24	No Account Management Process For Privileged Local User
25	No or Insufficient Administrative Role Seperation
26	Administrative Accounts are Internet-Browsing and/or Ema
27	Not all Domain Controllers are Located in a Physically Secu
28	Missing Baseline Security Hardening for AD integrated Syst
29	No or Insufficient Backup Management for Domain Control
30	No or Insufficient Patch-Management for the Operating Sy
31	No or Insufficient Patch-Management for Third Party Appli
32	No or Insufficient Antimalware Solution Management
33	No or Insufficient Logging and Monitoring
34	User Passwords Stored with Reversible Encryption

Presentation of Results

- The traditional report consisted of:
  - Management summary
  - All identified findings
  - Corresponding finding ratings (traffic light scheme)
  - Recommended controls

- The Excel sheet consisted of:
  - Overview of all identified findings
  - Corresponding finding ratings
  - Recommended controls
  - Some statitics

Presentation of Results

- Overall report
  - Overall management summary
  - Aggregation of all results of all assessed ADs
  - Graphical representations of the results
  - Statistics regarding the findings

ERNW
providing security.

Project Summary:
Lessons Learned

- Assessment and report creation greatly benefitted from the standardized and automated approach
  - Additionally: some characteristics of a good metric were indirectly satisfied
    - Data was cheap to gather (script and questionnaire)
    - Partly the results were consistently measured

ERNW
providing security.

Project Summary:
Lessons Learned

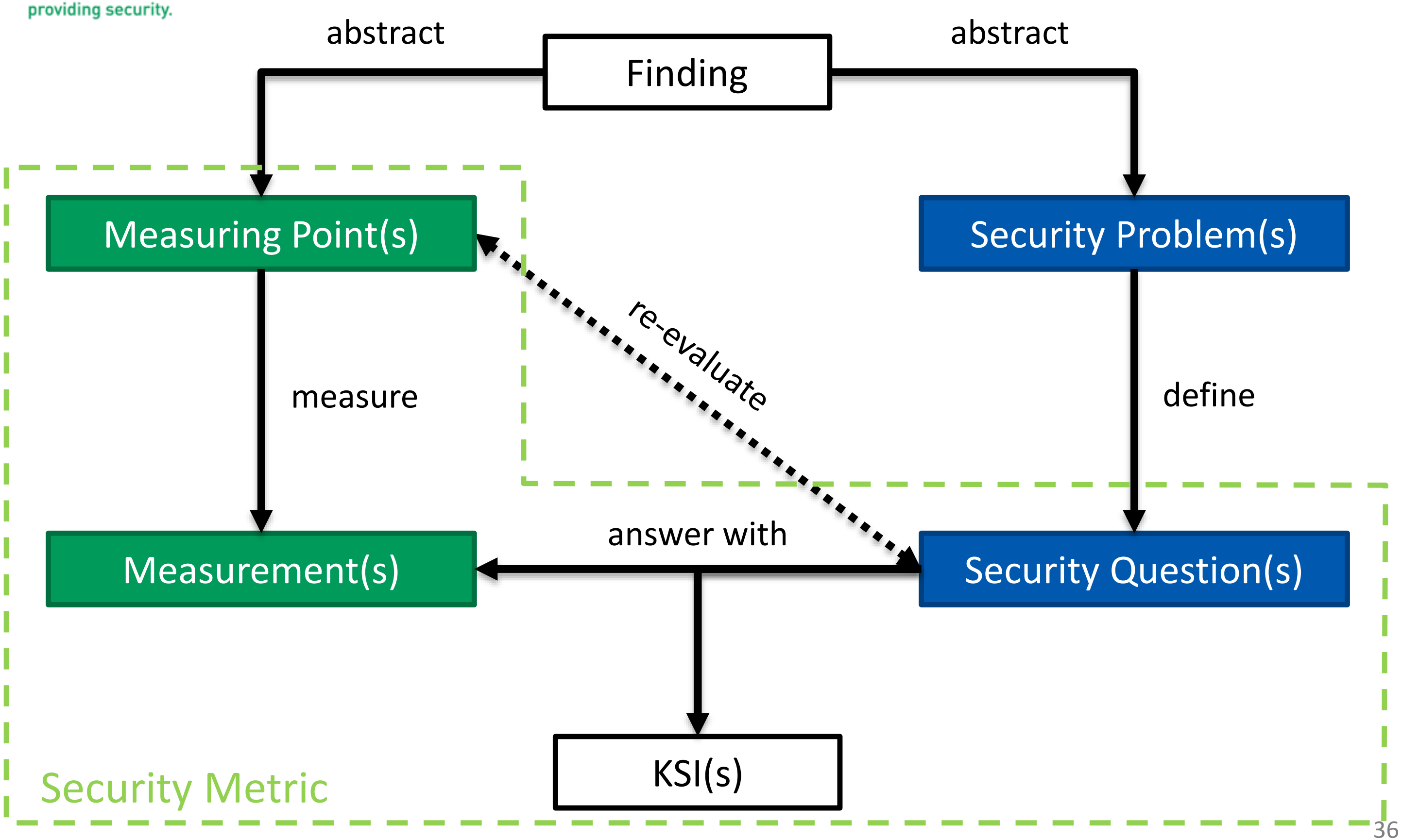
- Some inherent problems with a traditional assessment in style of an audit
  - Findings were treated independently
  - Ratings were very subjective
  - Reports are interpreted by the client (can lead to misunderstandings)
  - Individual parts of the report do not make sense on their own
  - Results do not allow for a direct comparison between different ADs
- The idea for an AD Security Metric was born!

How To: Translate Audit Findings into Security Metrics

ERNW
providing security.

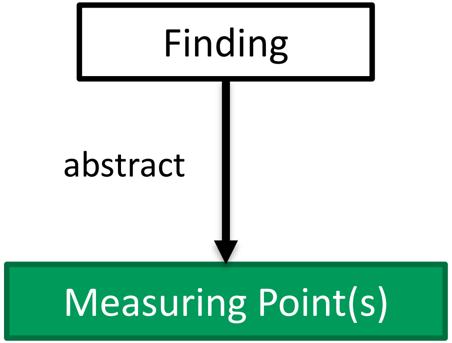
How To: Translate Audit Findings into Security Metrics

- We did not want to start at zero
  - Idea: translate audit findings into security metrics
- But: audit findings have inherent problems in context of metrics
  - Results are not always consistently measured (especially the user-defined text fields from the questionnaire)
  - Results are not expressed as a cardinal number or percentage (only qualitative labels used as ratings)
  - Results are not expressed using at least one unit of measure
- A process must be defined for correct translation!


abstract
Finding
abstract
Measuring Point(s)
Security Problem(s)
re-evaluate
measure
define
answer with
Measurement(s)
Security Question(s)
KSI(s)
Security Metric

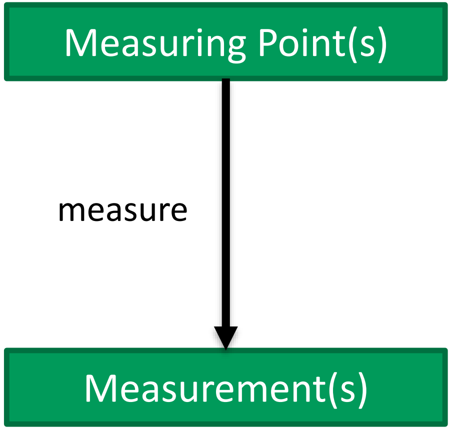
Security Metric: Measuring Point(s)

- From every finding one or more measuring points can be abstracted
- Tells you where to measure something
- Measuring points are measured with measuring instruments



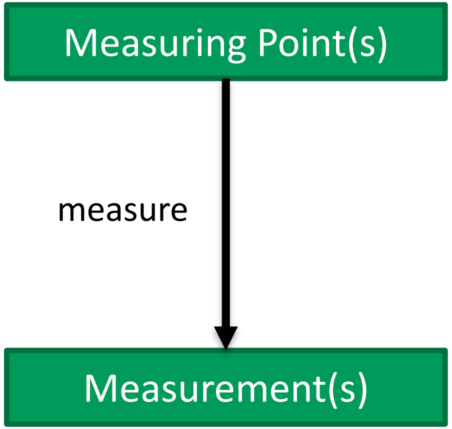
Security Metric: Measuring Instruments

- Device for measuring the measuring points
- Results are measurements
- In AD these can be for example:
  - Scripts
  - Questionnaires
  - Interviews
  - Documentation
  - Monitoring tools
  - Event logs



Security Metric: Measurement(s)

- Measurements result from the measuring process
- Every measuring point has one or more measurements
- Some measuring points have a pre-defined set of measurements

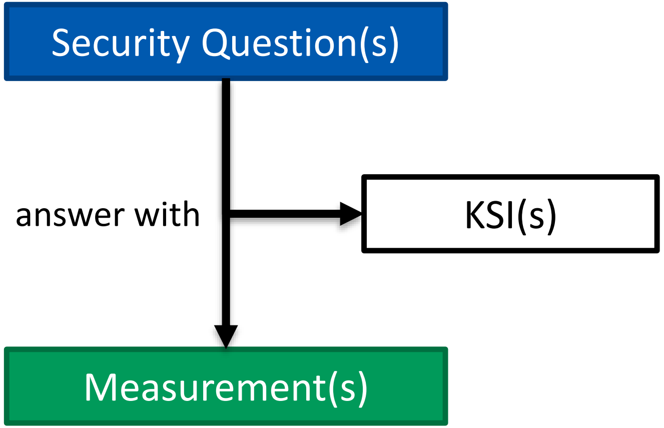


Security Metric: Security Question(s)

- Well-defined security questions result in relevant answers
  - These answers are the KSIs

- Can be answered with one or more measurements

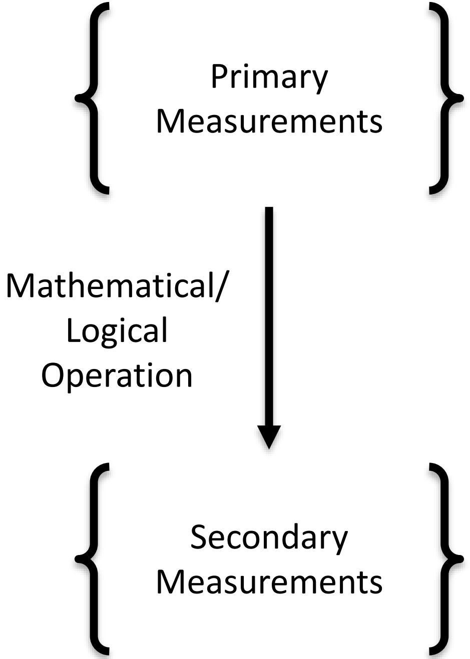
- Note: Not all security-related questions can be answered with measurements coming directly from the measuring points



Security Metric: Levels of Measurement(s)

- Measurements from the initial measuring points do not always answer the security question posed
  - Requires mathematical or logical operations with one or more other measurements

- Can be repeated if necessary to receive tertiary measurements



Primary Measurements

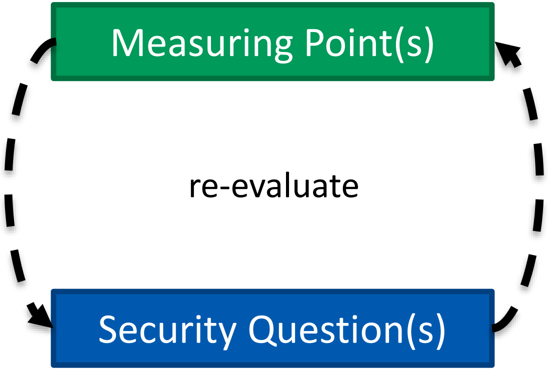
Mathematical/ Logical Operation

Secondary Measurements

Re-evaluate Measuring Points and Security Questions

- If the posed security questions cannot be answered this can be due to two reasons:
  - The security question is not precise enough or wrong
  - The selected measuring points are not sufficient or wrong

- In an iterative process both must be re-evaluated. This leads to:
  - More or other measuring points
  - Reformulation of the security questions



Example: Audit Finding to Metric(s)

„Insufficient LAN Manager authentication level on multiple systems“

Audit Finding

- Audit finding: „Insufficient LAN Manager authentication level on multiple systems“
  - Underlying security problem: Potentially enabling the use of the LM or NTLMv1 authentication protocol

- Rating: High

Abstraction from Finding to Measuring Points and Measurements

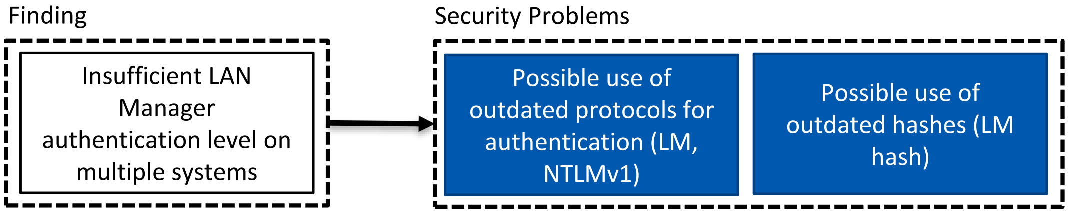
- Measuring points: GPOs containing the LAN Manager authentication level and where they are linked

- Set of possible measurements =
  - {"Send LM & NTLM responses", "Send LM & NTLM - use NTLMv2 session security if negotiated", "Send NTLM response only", "**Send NTLMv2 response only**", "Send NTLMv2 response only\refuse LM", "Send NTLMv2 response only\refuse LM & NTLM"}

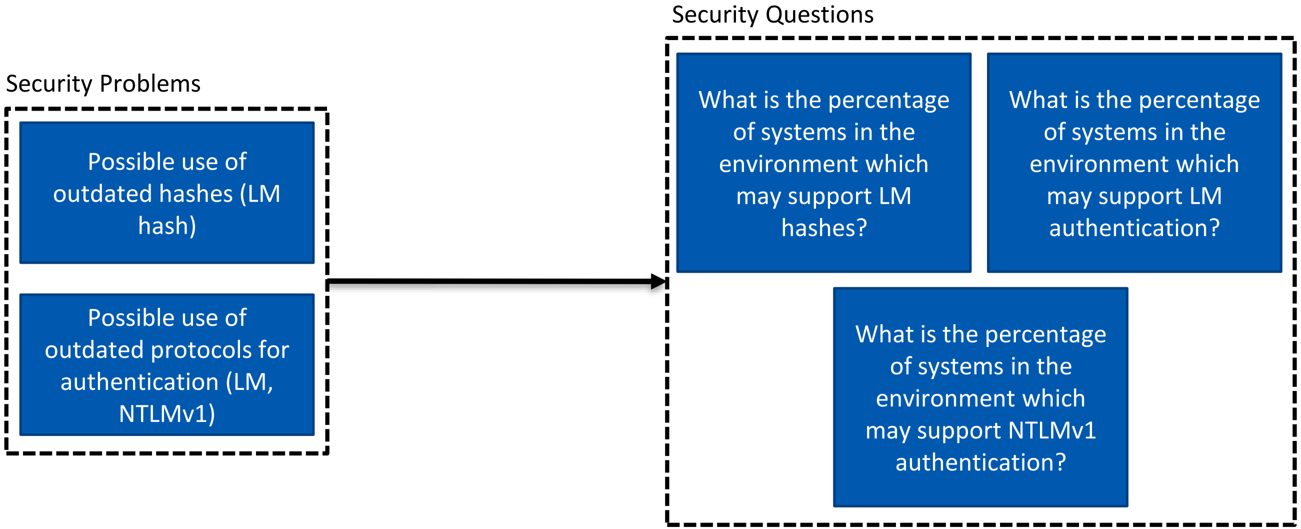
- Measurement < "Send NTLMv2 response only" -> audit finding is triggered

Security Problems Behind the Finding

- This finding mixes different security problems:
  - Possible use of outdated protocols for authentication (LM, NTLMv1)
  - Possible use of outdated hash (LM hash)
  - Shouldn‘t there be a differentiation between LM and NTLMv1?


Finding
Insufficient LAN Manager authentication level on multiple systems
Security Problems
Possible use of outdated protocols for authentication (LM, NTLMv1)
Possible use of outdated hashes (LM hash)

Security Questions Defined by the Security Problems



Security Problems

- Possible use of outdated hashes (LM hash)
- Possible use of outdated protocols for authentication (LM, NTLMv1)

Security Questions

- What is the percentage of systems in the environment which may support LM hashes?
- What is the percentage of systems in the environment which may support LM authentication?
- What is the percentage of systems in the environment which may support NTLMv1 authentication?

ERNW
providing security.

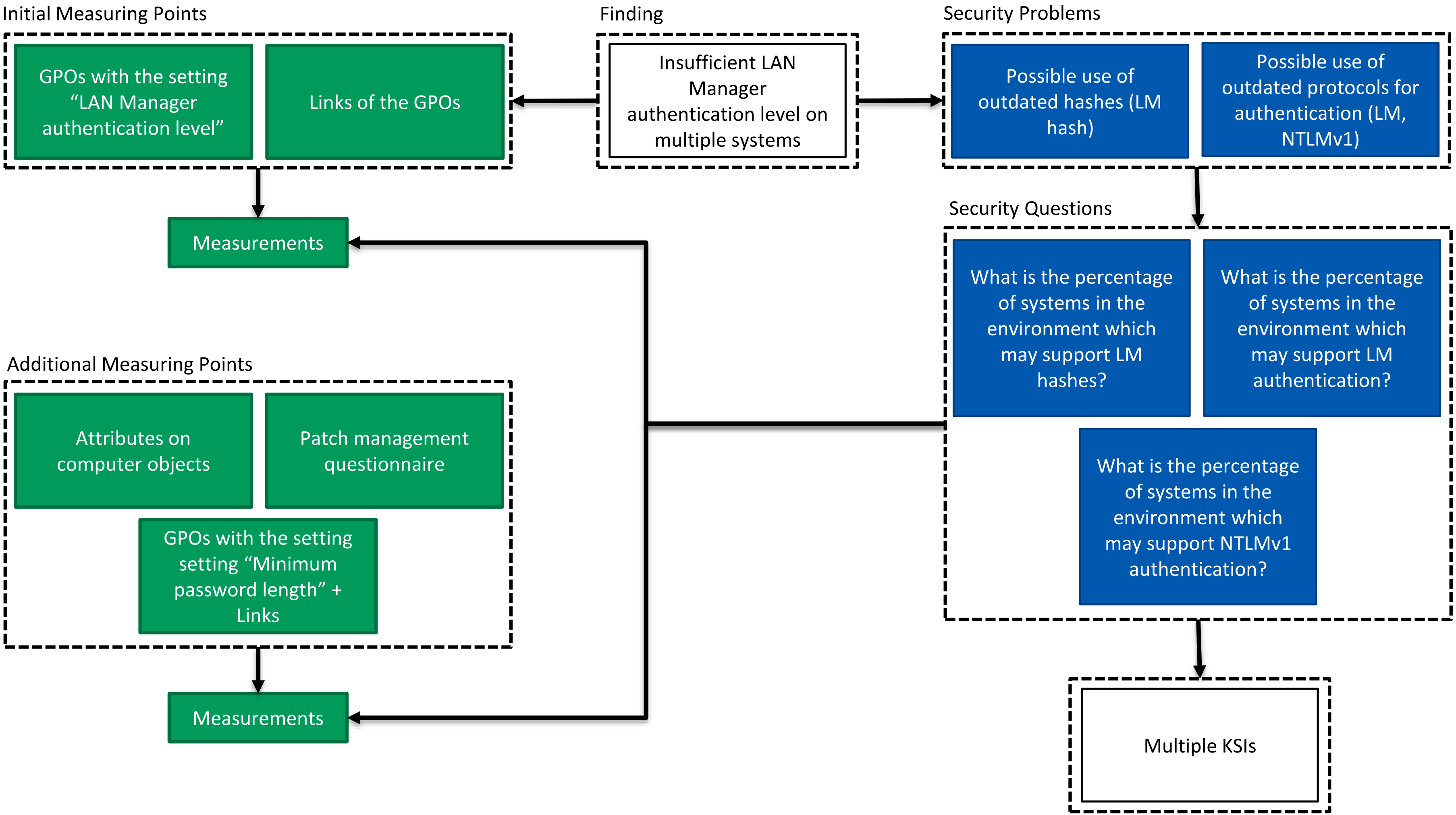
Security Questions Fully Answered…?

- …Through the measurement of GPO setting and where GPOs with this setting are linked?
- Translation: Does the use of LM hash depend solely on the "Send NTLMv2 response only" setting?

From Additional Influencing Factors to Additional Measuring Points

- Other factors that may influence the hash and protocols used:
  - Windows operating system version
  - Patch level
  - Password length

- From these factors result additional measuring points:
  - Attributes on computer objects "OperatingSystem“, “OperatingSystemVersion“
  - Questions regarding the patch management in the questionnaire
  - GPO setting “minimum password length”
  - Where GPO is linked


Initial Measuring Points
GPOs with the setting "LAN Manager authentication level"
Links of the GPOs
Finding
Insufficient LAN Manager authentication level on multiple systems
Security Problems
Possible use of outdated hashes (LM hash)
Possible use of outdated protocols for authentication (LM, NTLMv1)
Measurements
Security Questions
What is the percentage of systems in the environment which may support LM hashes?
What is the percentage of systems in the environment which may support LM authentication?
Additional Measuring Points
Attributes on computer objects
Patch management questionnaire
GPOs with the setting setting "Minimum password length" + Links
What is the percentage of systems in the environment which may support NTLMv1 authentication?
Measurements
Multiple KSIs

Statement of Finding vs. Statement of Metric (KSI)

- **Statement of the Finding**
- „Insufficient LAN Manager authentication level on multiple systems“

- **Statement of the Metric (= KSI)**
- Number/percentage of systems that may support LM hashes
- Number/percentage of systems that may support LM auth
- Number/percentage of systems that may support NTLMv1 auth

☑ Consistently measured

☑ Cheap to gather

☑ Expressed as a cardinal number or percentage

☑ Expressed using at least one unit of measure

☑ Contextually specific

Obstacles in the Translation Process

ERNW
providing security.

Encountered Obstacles

- Asking the wrong questions

↓

- Getting lost in data

↓

- Trying to fix the unfixable

Encountered Obstacles

Example: “User Account Control Disabled on Multiple Systems”

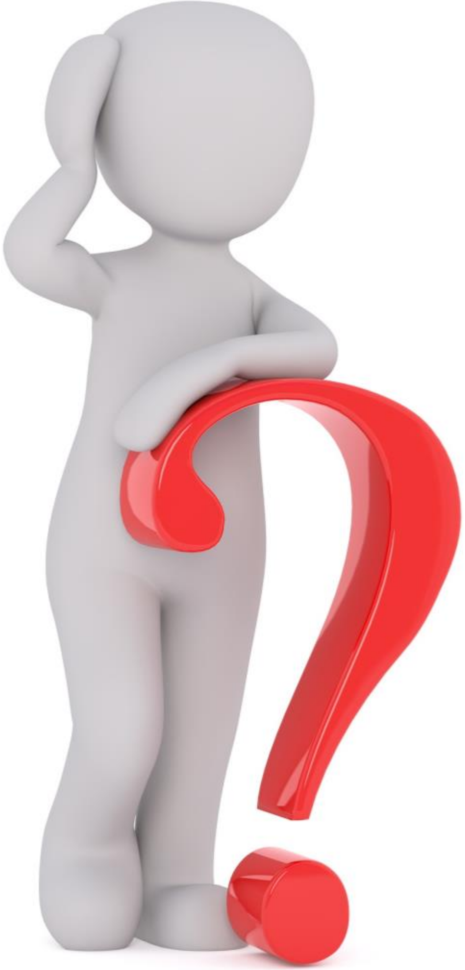
ERNW
providing security.

The Starting Point

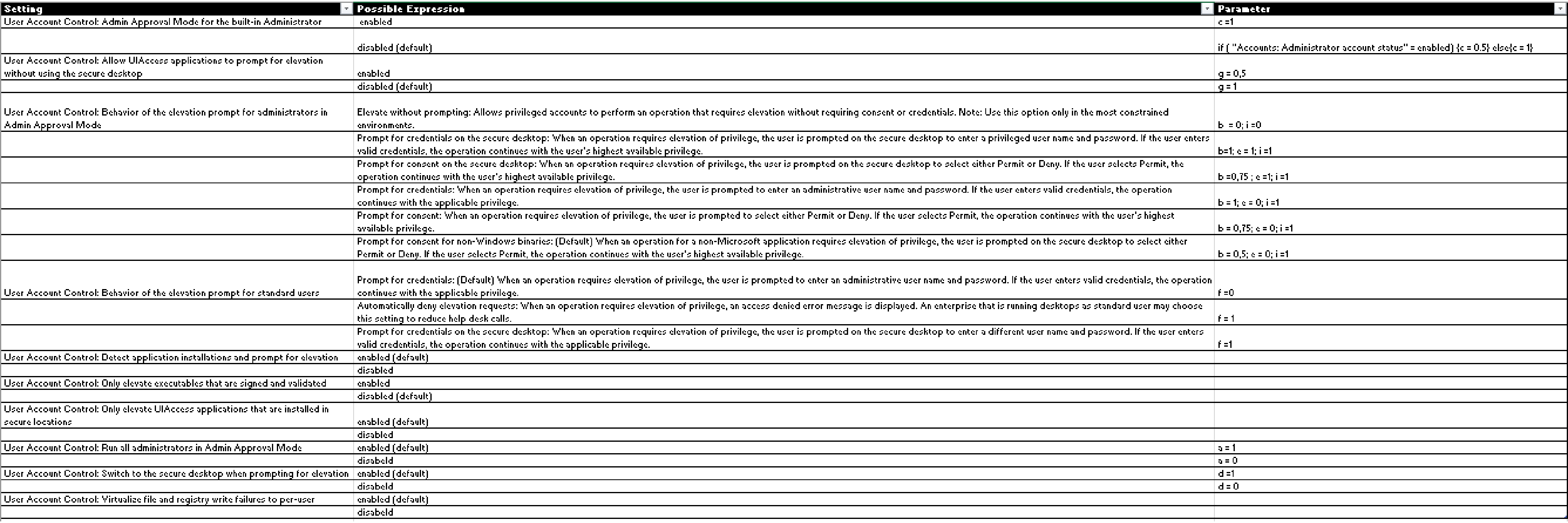
- Audit finding: „User Account Control Disabled on Multiple Systems "
- Underlying security problem: any application started by an administrator runs in the user and privilege context of the administrator.

Asking the Wrong Question

- Not specific enough:
  - How good is the UAC configuration in the environment?
- A good question
  - Should frame the problem space
  - Should be answerable by a KSI that conforms to the criteria for a *good metric*



Getting Lost in Data



Setting	Possible Expression	Parameter
User Account Control: Admin Approval Mode for the built-in Administrator	enabled	c =1
	disabled (default)	if ("Accounts: Administrator account status" = enabled) {c = 0.5} else{c = 1}
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	enabled	g = 0,5
	disabled (default)	g = 1
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments.	b = 0; i =0
	Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege.	b=1; e = 1; i =1
	Prompt for consent on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.	b =0,75 ; e =1; i =1
	Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.	b = 1; e = 0; i =1
	Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.	b = 0,75; e = 0; i =1
	Prompt for consent for non-Windows binaries: (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.	b = 0,5; e = 0; i =1
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials: (Default) When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.	f =0
	Automatically deny elevation requests: When an operation requires elevation of privilege, an access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.	f = 1
	Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.	f =1
User Account Control: Detect application installations and prompt for elevation	enabled (default)	
	disabled	
User Account Control: Only elevate executables that are signed and validated	enabled	
	disabled (default)	
User Account Control: Only elevate UIAccess applications that are installed in secure locations	enabled (default)	
	disabled	
User Account Control: Run all administrators in Admin Approval Mode	enabled (default)	a = 1
	disabeld	a = 0
User Account Control: Switch to the secure desktop when prompting for elevation	enabled (default)	d =1
	disabeld	d = 0
User Account Control: Virtualize file and registry write failures to per-user	enabled (default)	
	disabeld	

Getting Lost in Data

- Pro GPO: UAC = a * b * c * 0,8 + a * i * 0,2 * (g * (d OR (e AND f)))
  - $0 <= UAC <= 1$

- $UAC_{total} = \Sigma (UAC_{GPO} * n)$
  - With: n = number of computer objects the GPO applies to

- And still not every measuring point is considered...

ERNW
providing security.

Getting Lost in Data

- 10 GPO settings relating to UAC
  - Wanting to use them all as measuring points to answer the broad question: How good is the UAC configuration in the environment?
- Measuring points mix different aspects of UAC
  - How to connect the resulting measurements?
- Qualitative differences between different measurements
  - How to quantify them?

Trying to Fix the Unfixable

- Instead of going back and reconsidering the taken approach and the question asked:
  - Weightings are applied
    - According to “gut feeling”
- Sounds all good until…

- ☑ Consistently measured
- ☑ Cheap to gather
- ☑ Expressed as a cardinal number or percentage
- ☒ Expressed using at least one unit of measure
- ☒ Contextually specific

How to Make it Better

- Always have the criteria of a good metric in mind

- "Posing appropriate questions is the real art to information security metrics.“

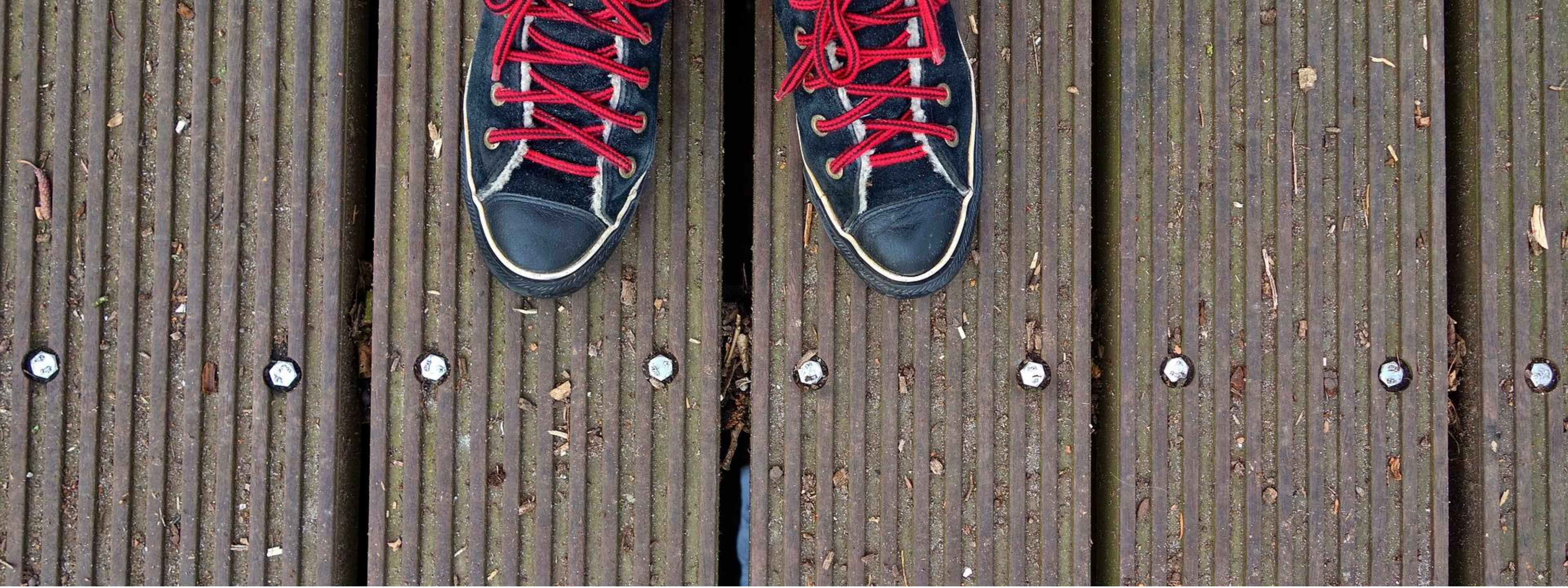
  See [2], p.15.

- Select the measuring points according to your question, not the other way around
  - This might lead to questions not being answerable with your existing data
  - Then change your measuring points or even your measuring instrument

Examples For Better UAC Related Security Questions

- What is the percentage of systems in the environment where UAC not used (for every high-privileged user/operation)?
  - To derive the KSI include the following measuring points:
    - Attributes on computer objects "OperatingSystem“, “OperatingSystemVersion“

- On how many systems in the environment is UAC configured according to Security Best Practices?



Where Do We Stand?

ERNW
providing security.

Where Do We Stand?

- Number of original audit findings: 34
- Number of measuring points: > 200
- Number of well-defined (according to a 'good metric') KSIs: 22
- Number of KSIs in process: 16

Where Do We Want to Go?

ERNW
providing security.

Where Do We Want to Go?

- Answer More and Broader Security Questions
  - Define more KSIs, use KSIs as measurements
- Include More Measuring Instruments
  - Get access to more measuring points (and thereby create more KSIs)
- Test For Construct Validity
  - Assess the reliability of the security metric

ERNW
providing security.

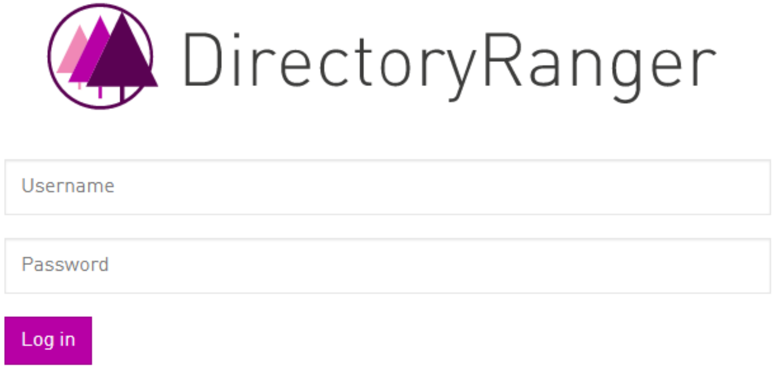
Lessons Learned

- Doing/developing metrics is hard ;-)
- Consider subject areas with more metric experience (e.g. Psychology)
- Posing the right questions is crucial!
- Keep criteria for a good metric permanently in your mind ;-)

ERNW
providing security.

Call to Action

- Get in contact and discussion with us to improve Active Directory security *measurably!*



@DirectoryRanger

ERNW
providing security.

TROOPERS
MAKE THE WORLD A SAFER PLACE

Thank you for your attention!

fkuhn@ernw.de
hwiederkehr@ernw.de
nmatysiak@ernw.de

www.ernw.de

www.insinuator.net

ERNW
providing security.

Sources

- [1]: Andrew Jaquith: Security Metrics. Replacing Fear, Uncertainty, and Doubt. Addison-Wesley, March 2007
- [2]: W. Krag Brotby and Gary Hinson: PRAGMATIC Security Metrics. CRC Press, 2013
- Icons
  - https://icons8.com/