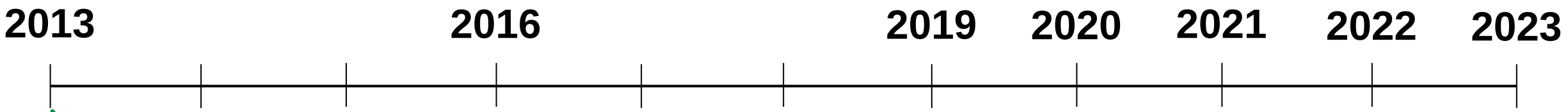
Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security

Eva Gerlitz[1], Maximilian Häring[2], Matthew Smith[1,2], Christian Tiefenau[2]

[1]: Fraunhofer FKIE, [2]: University of Bonn

Motivation

NIST deletes recommendation for password expiry



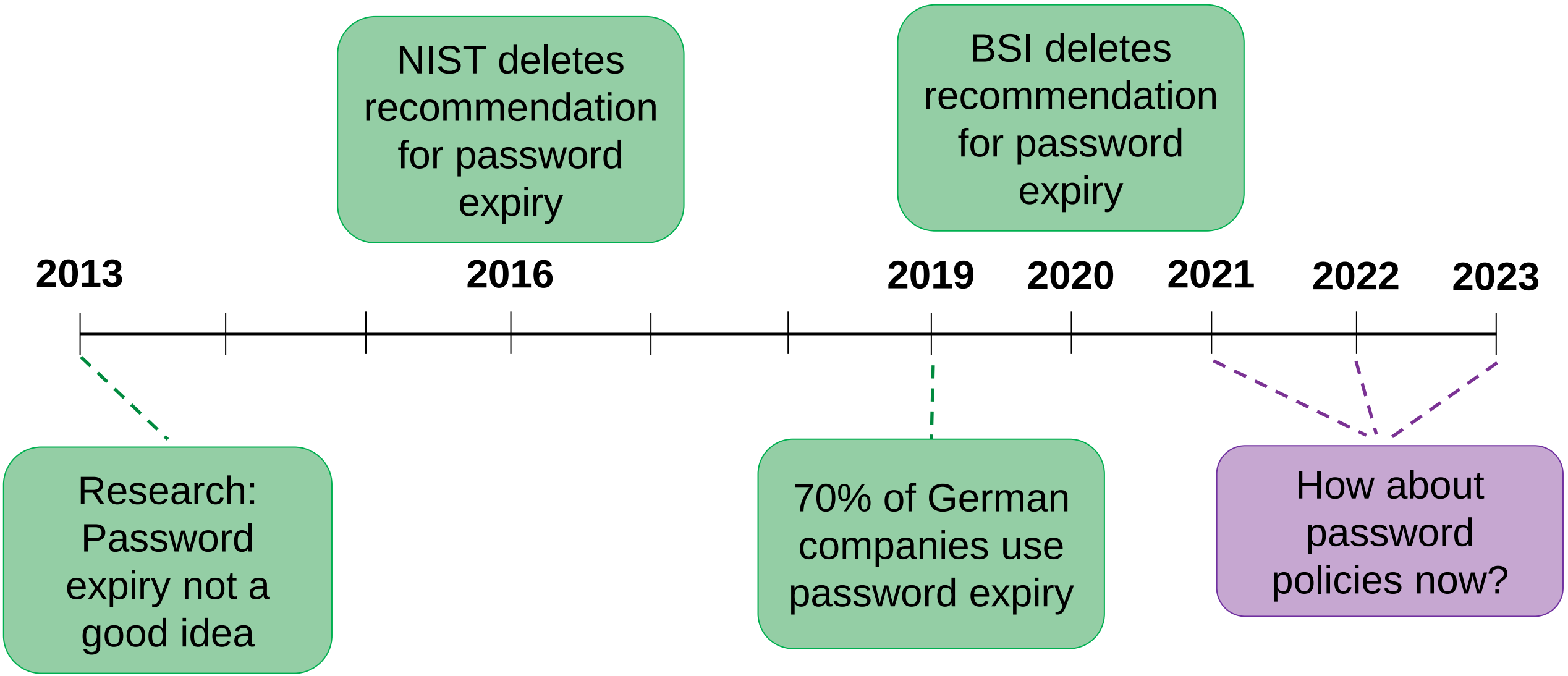
Research: Password expiry not a good idea

Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies

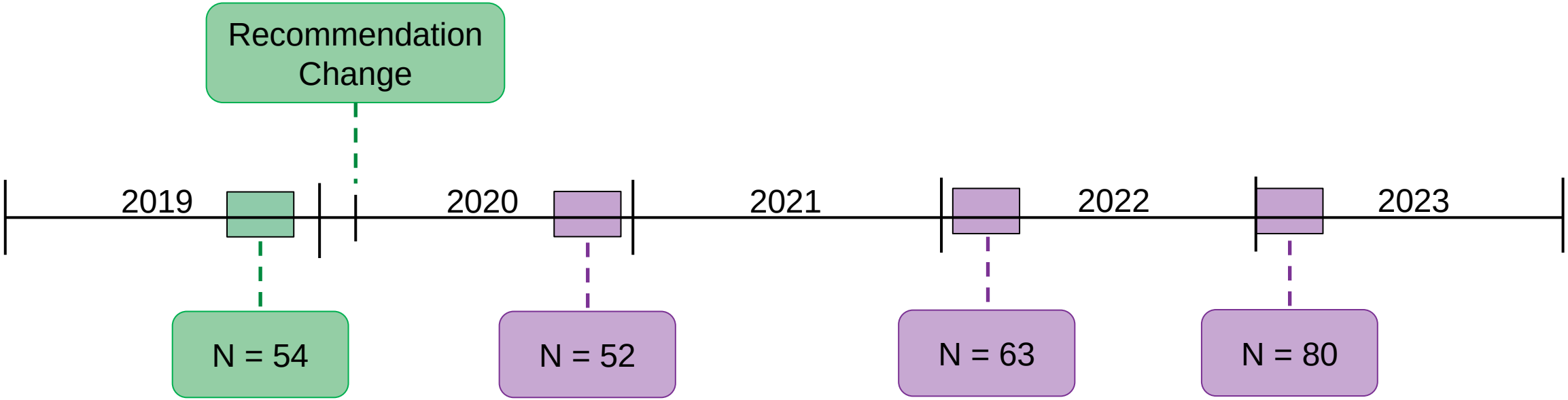
Eva Gerlitz, *Fraunhofer FKIE;* Maximilian Häring, *University of Bonn;*
Matthew Smith, *University of Bonn, Fraunhofer FKIE*

https://www.usenix.org/conference/soups2021/presentation/gerlitz

Motivation


NIST deletes recommendation for password expiry
BSI deletes recommendation for password expiry
2013
2016
2019
2020
2021
2022
2023
Research: Password expiry not a good idea
70% of German companies use password expiry
How about password policies now?

Methodology of **Expert** Study

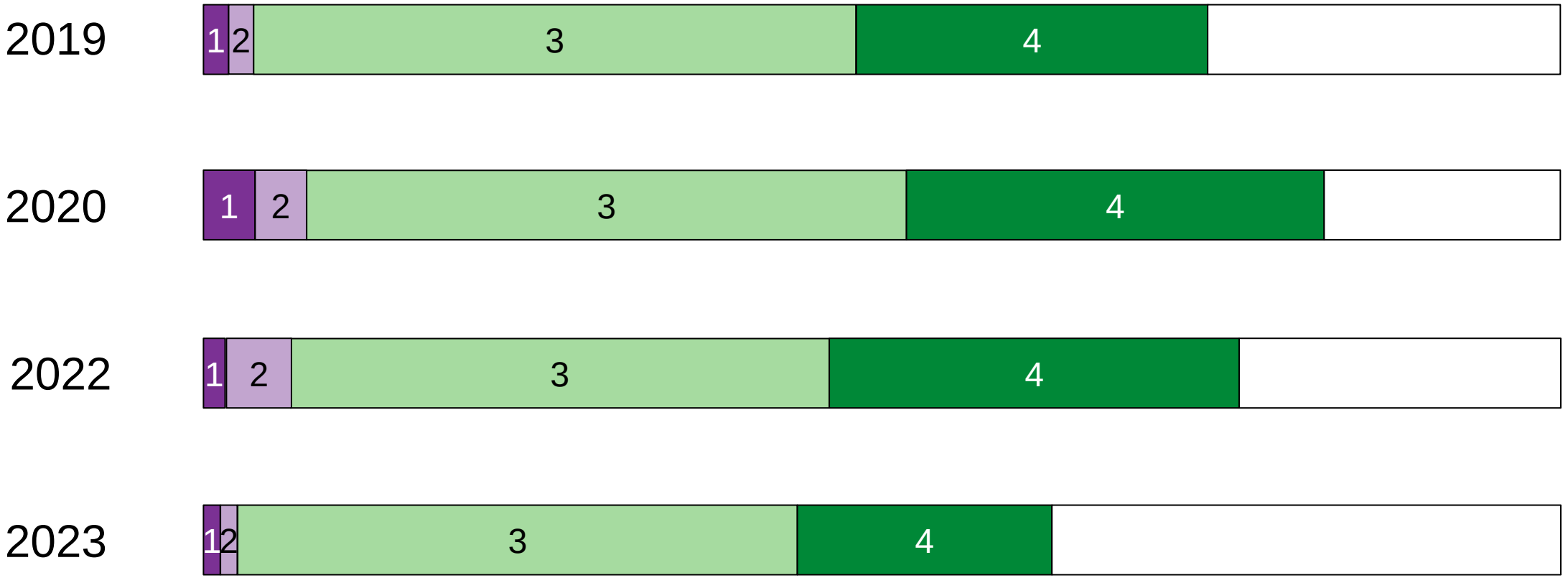


Participants

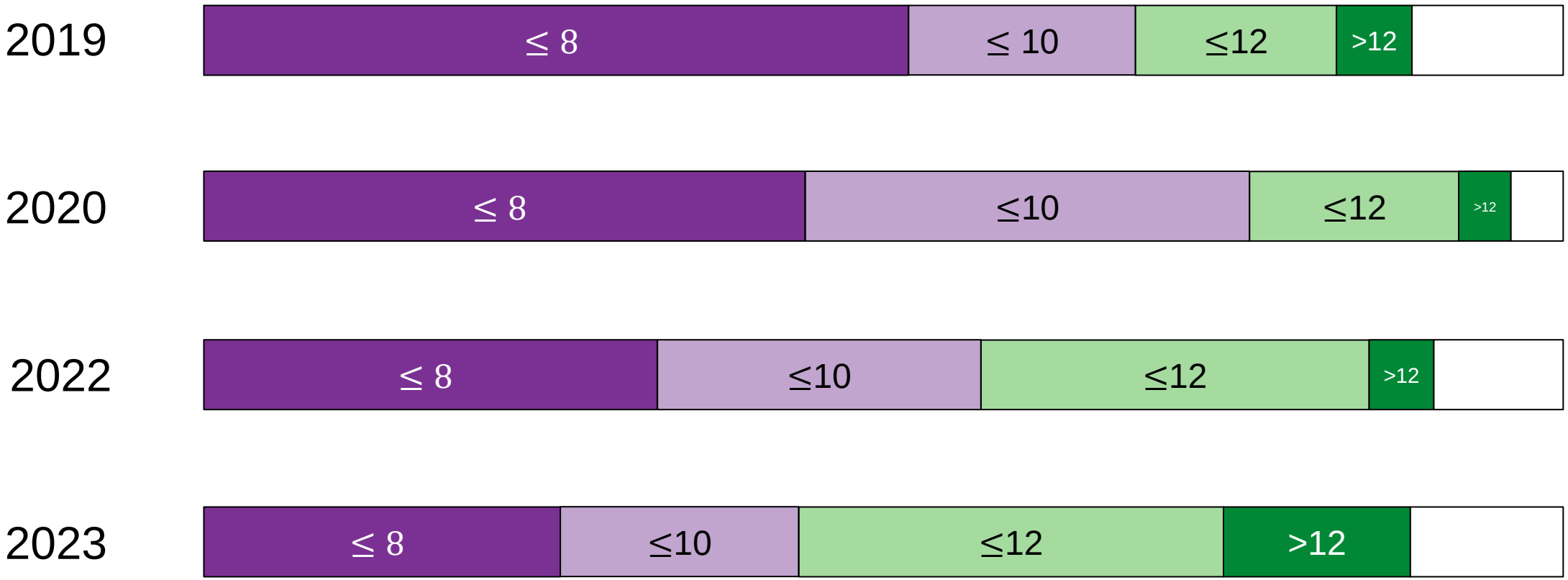
Asked for:

- Policy
- Password expiry (2023)
- Alternative checks (2023)

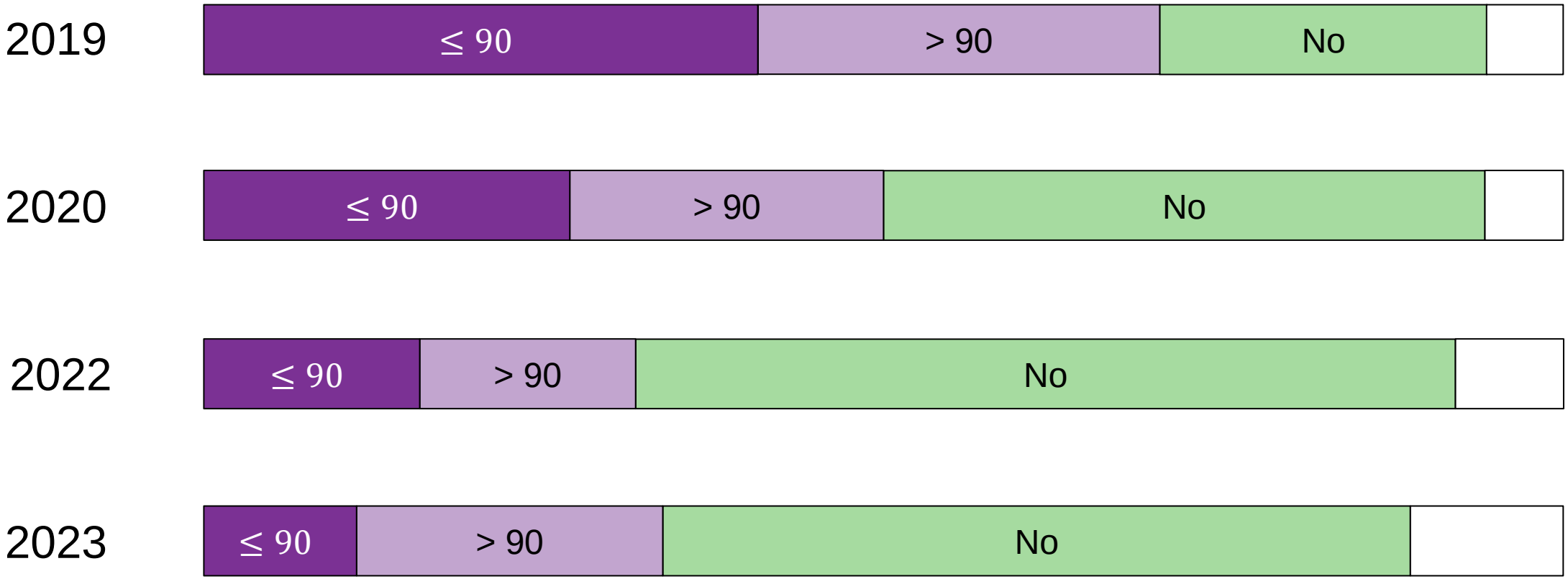
Usage of Character Classes (%)



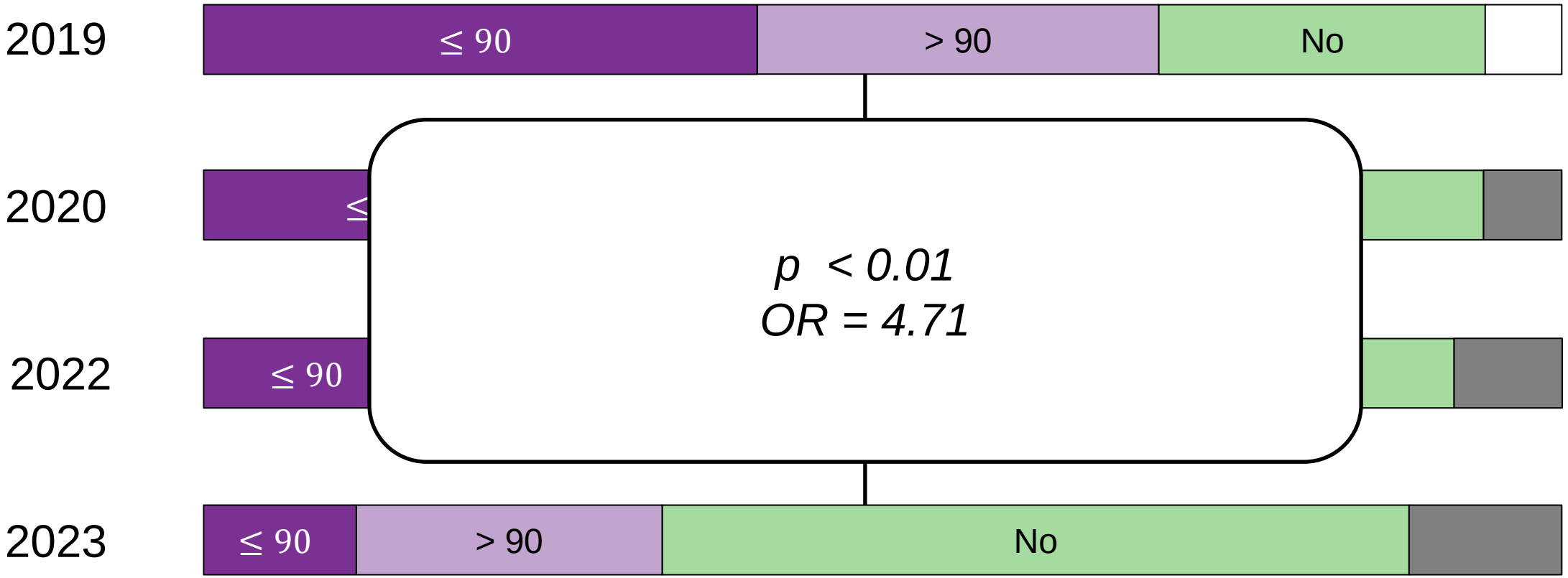
Usage of Minimal Length (%)



Usage of Password Expiry (%)

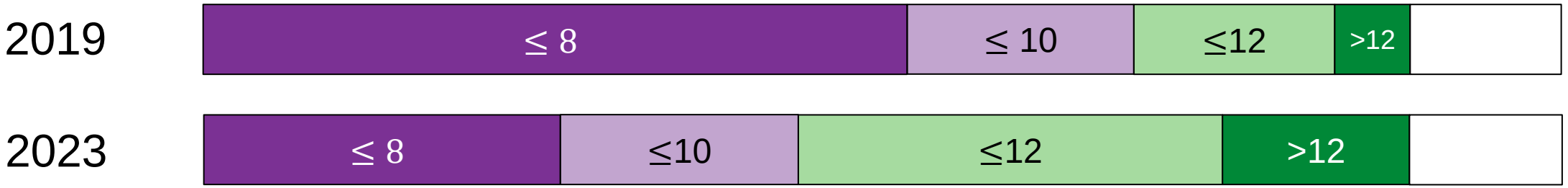


Usage of Password Expiry (%)

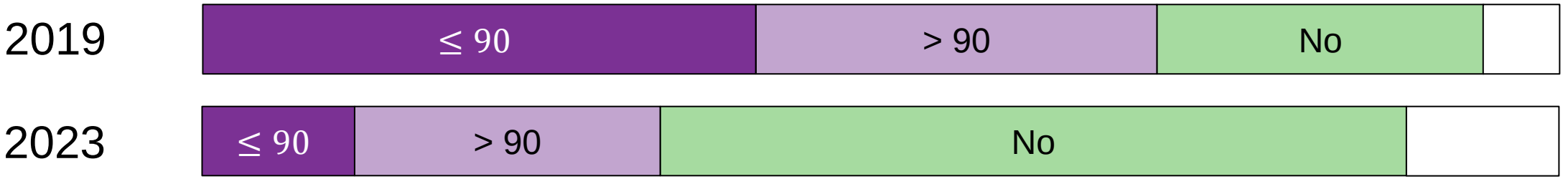


Summary

Minimal length



Password expiry



➡ Trend to longer minimal length and no password expiry

Elements of password policies

Expiry (days)	Min. Len	Complexity	2019	2020	2022	2023
90	8	3	5	4	3	0
90	8	4	4	3	1	0
90	10	3	3	1	1	0
180	8	3	3	0	0	2
180	8	4	1	3	0	1
Not mentioned	8	3	2	1	4	2
Not mentioned	8	4	3	3	3	2
Not mentioned	12	3	0	3	1	5
Not mentioned	12	4	2	2	6	2
Explicitly not	12	3	0	0	1	4

➡ But: 45% still use password expiry!

Why is password expiry still in use in 2023?

36 answers

Why is password expiry still in use? Security!

“Because after a year, the risk of misuse of the PW through reuse with other, potentially corrupted services, is too great.”

“… adds ‘some’ security”

Why is password expiry still in use? Requirements!

“Official (in my eyes outdated) requirements in handling officially classified data.”

„Internal policies require this change, contrary to the recommendation of the IT sec [department]“

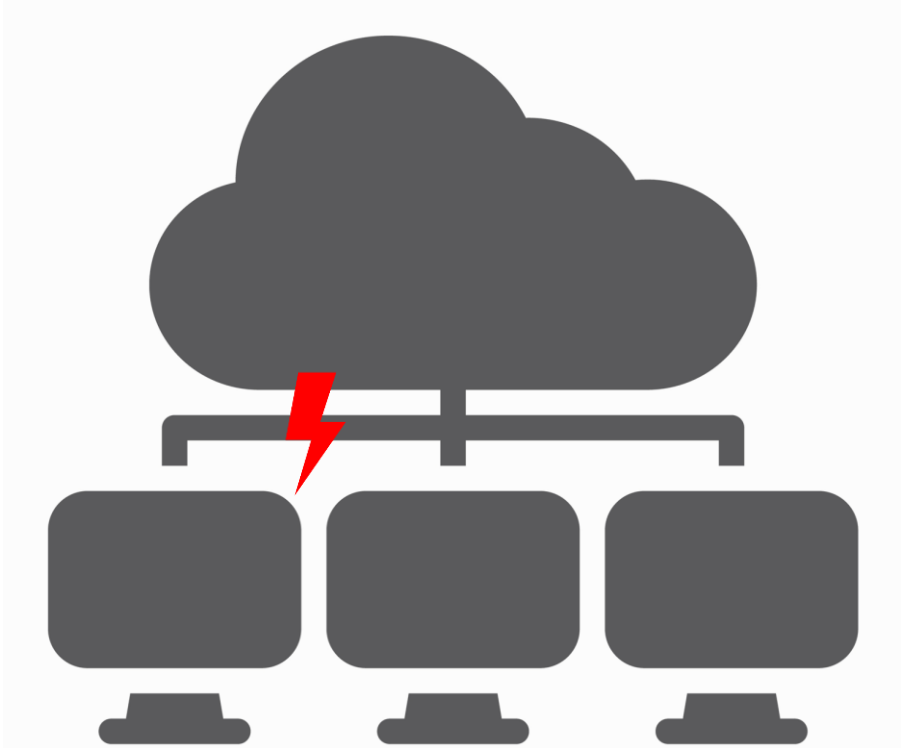
Why is password expiry still in use?
Technically difficult

“… there is currently no other technical solution.”

How do companies check for compromised accounts?

66 answers

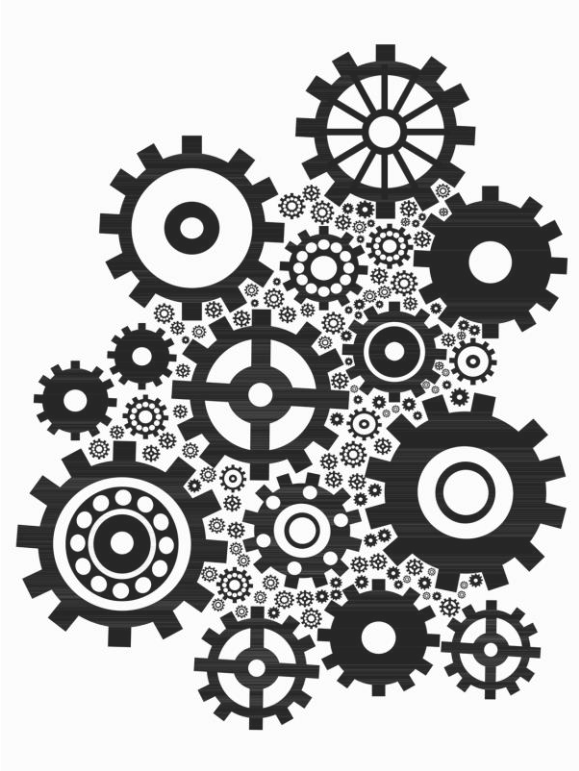
Check for compromised accounts



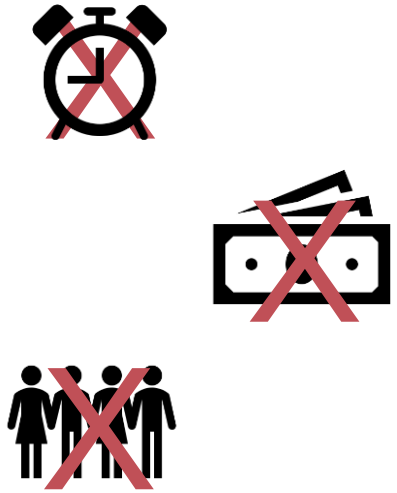
Anomaly detection
16

Leak check
8

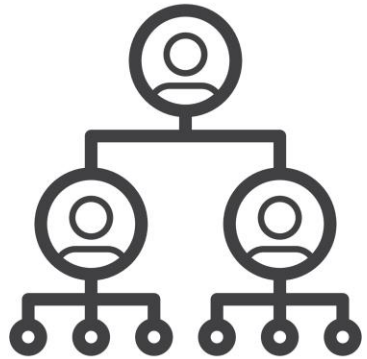
No check because …



Difficult
9



Resources
7



Structural
5

Summary

- Password expiry is still a thing.
  - Assumptions that might not hold
  - More hope for improvement than actual improvement
  - Management needs to be convinced
  - Technical issues

➡ We need to find easy solutions for implementing different checks and/or find out why current solutions are not used.

➡ We need to help experts in communicating necessary changes to management

Summary

Password expiry is still a thing.

- Assumptions that might not hold
- More hope for improvement than actual improvement
- Management needs to be convinced
- Technical issues

We need to find easy solutions for implementing different checks and/or find out why current solutions are not used.

We need to help experts in communicating necessary changes to management

Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security

Eva Gerlitz[1], Maximilian Häring[2], Matthew Smith[1,2], Christian Tiefenau[2]

[1]: Fraunhofer FKIE, [2]: University of Bonn