ARCTIC WOLF

THE LEADER IN **SECURITY OPERATIONS**

Cyber **D**efense **M**aturity **A**ssessment zur schnellen Feststellung der eigenen Verteidigungsreife

– Best Practice Sharing Session –

Fabian Lochmann M.Sc. (Arctic Wolf Network Germany GmbH)

Agenda

01 Customization Journey

02 Assessment with CIS

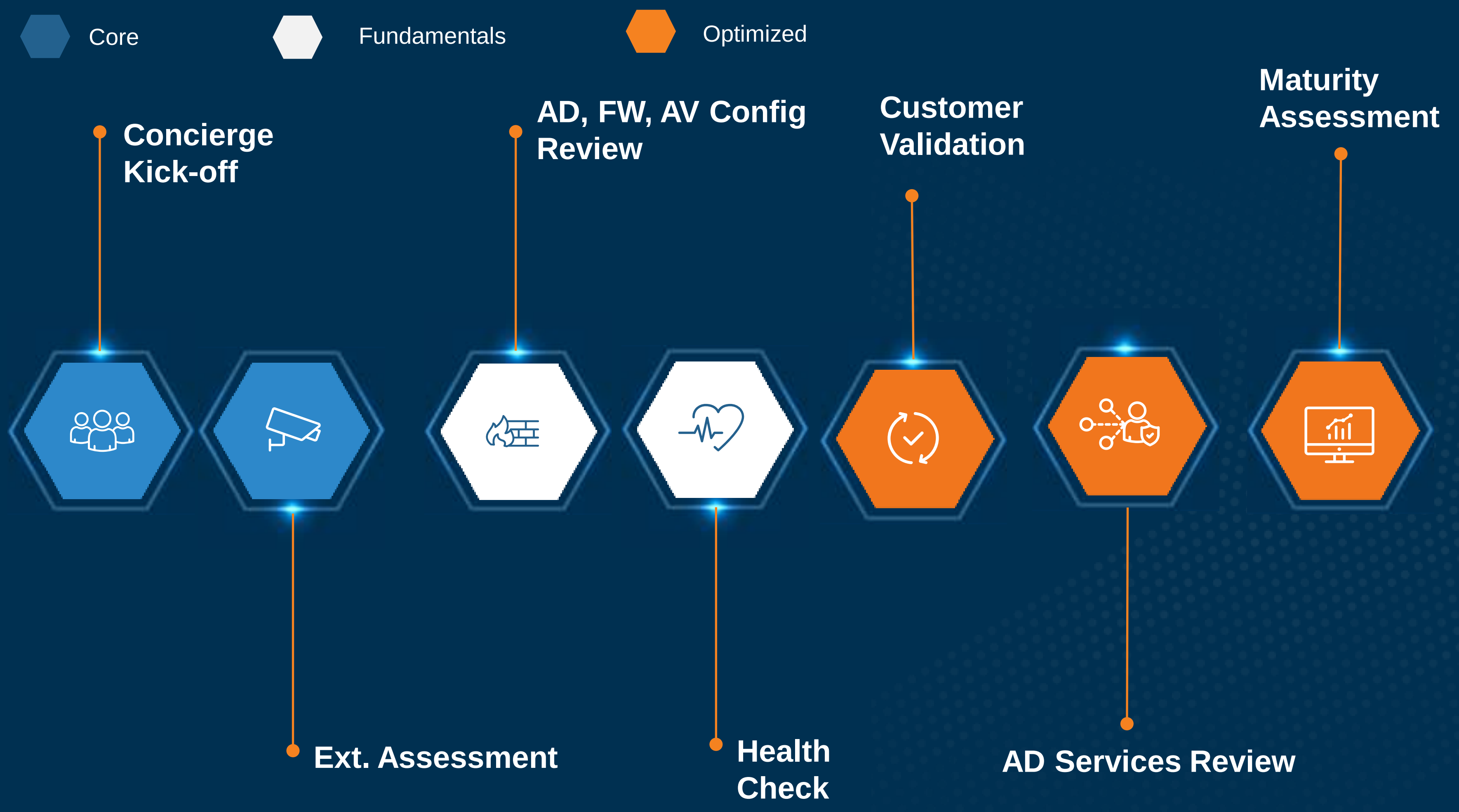
03 Critical Security Controls

04 Implementation Groups

05 CDMA Workflow

06 Summary

3 Month Customization Journey



Assessment with CIS

- The **Center for Internet Security** (CIS) is a nonprofit organization that publishes baseline configurations for different technologies

- The **CIS Critical Security Controls** (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.

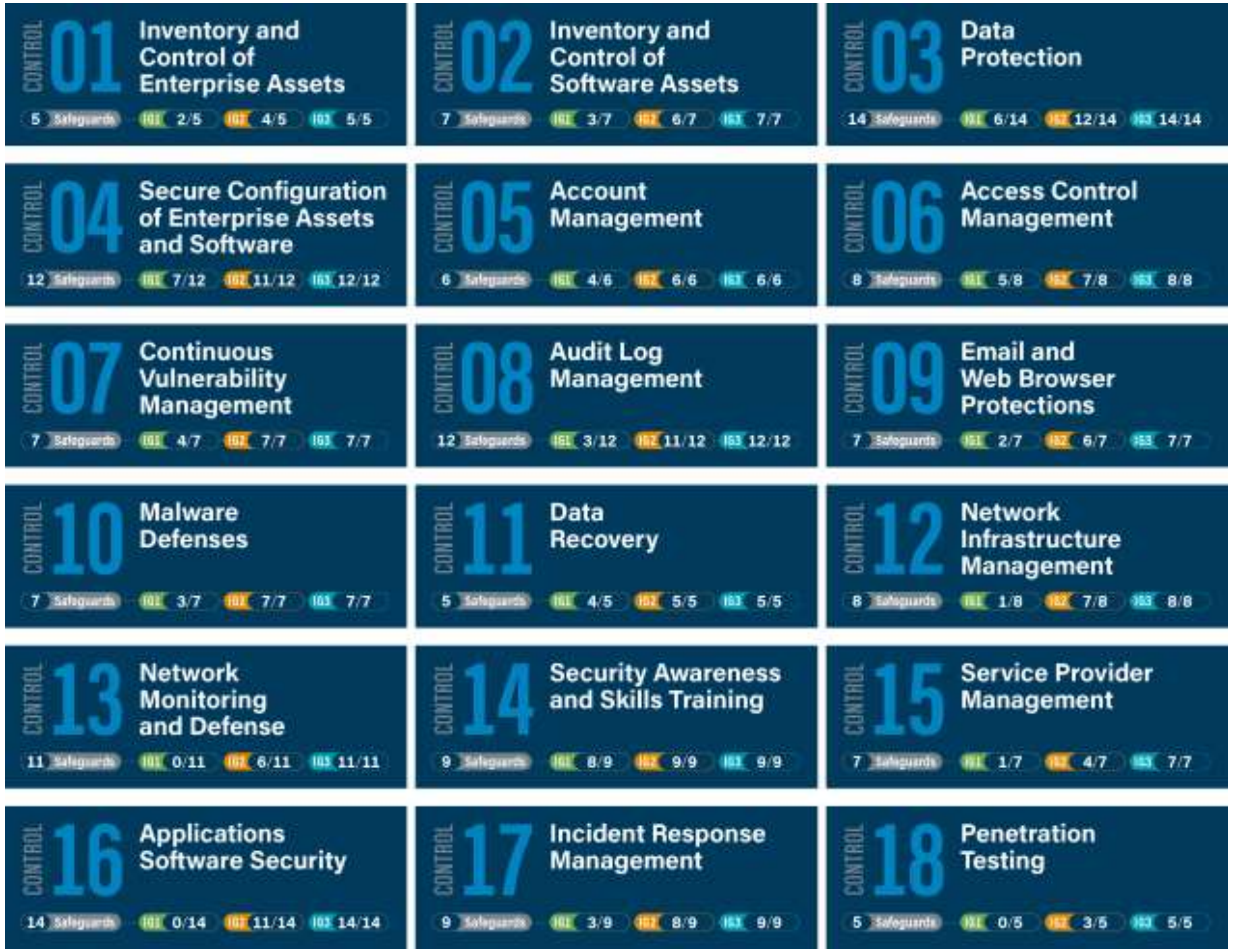
- The **CDMA** is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Controls cybersecurity best practices.

Critical Security Controls

- Implementing Critical Security Controls (CIS Controls) help provide a security focused baseline across the organization and enterprise.

- The Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

- Review current findings and recommendations



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11

CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9

CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

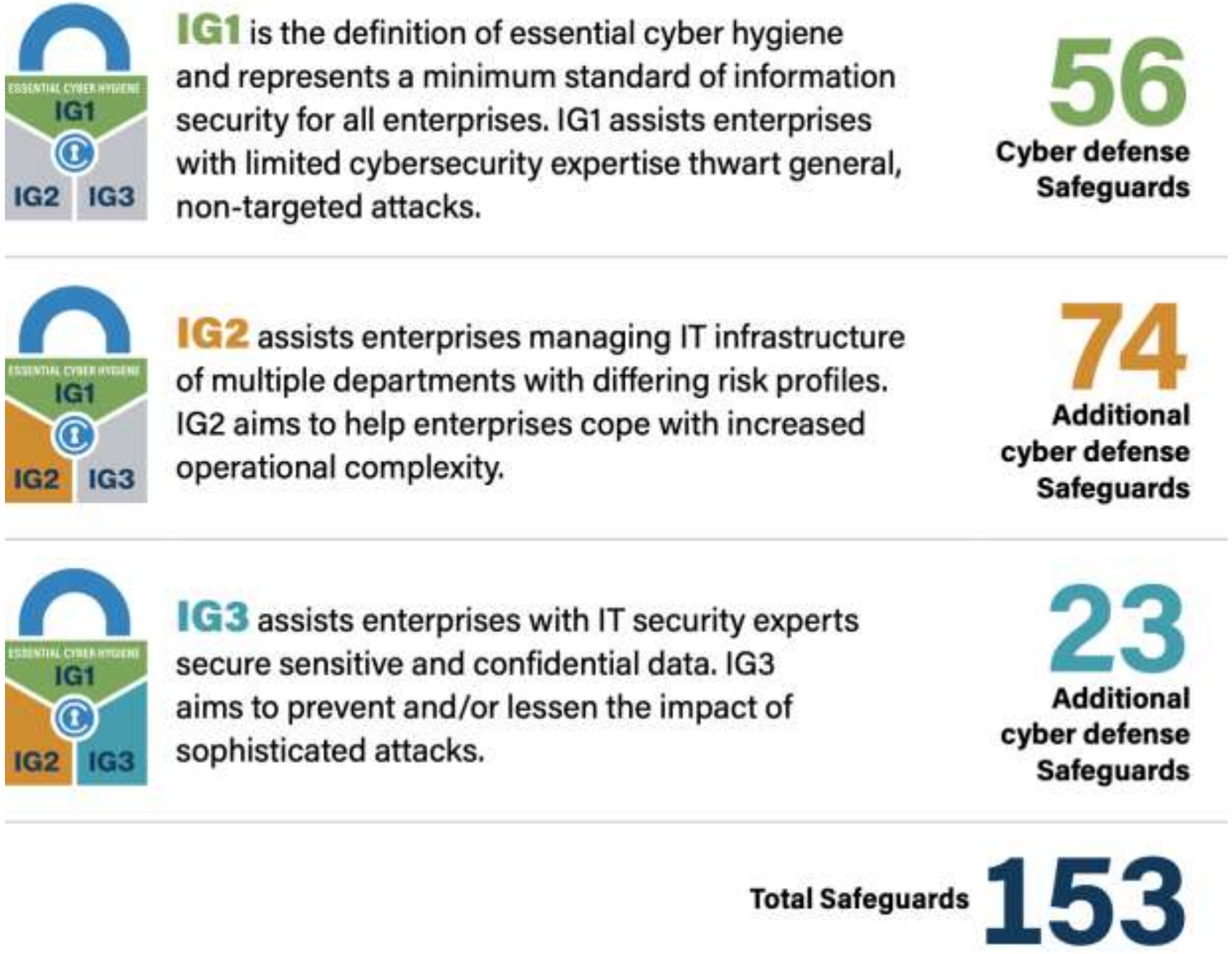
CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9

CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

Implementation Groups

- **IG1** is the definition of basic cyber hygiene and represents an emerging minimum standard of information security for all enterprises.
- **IG1** is a foundational set of cyber defense Safeguards that every enterprise should apply to guard against the most common attacks.
- **IG2** and **IG3** build upon previous IGs, with IG1 being the on-ramp to the Controls.



IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 Additional cyber defense Safeguards

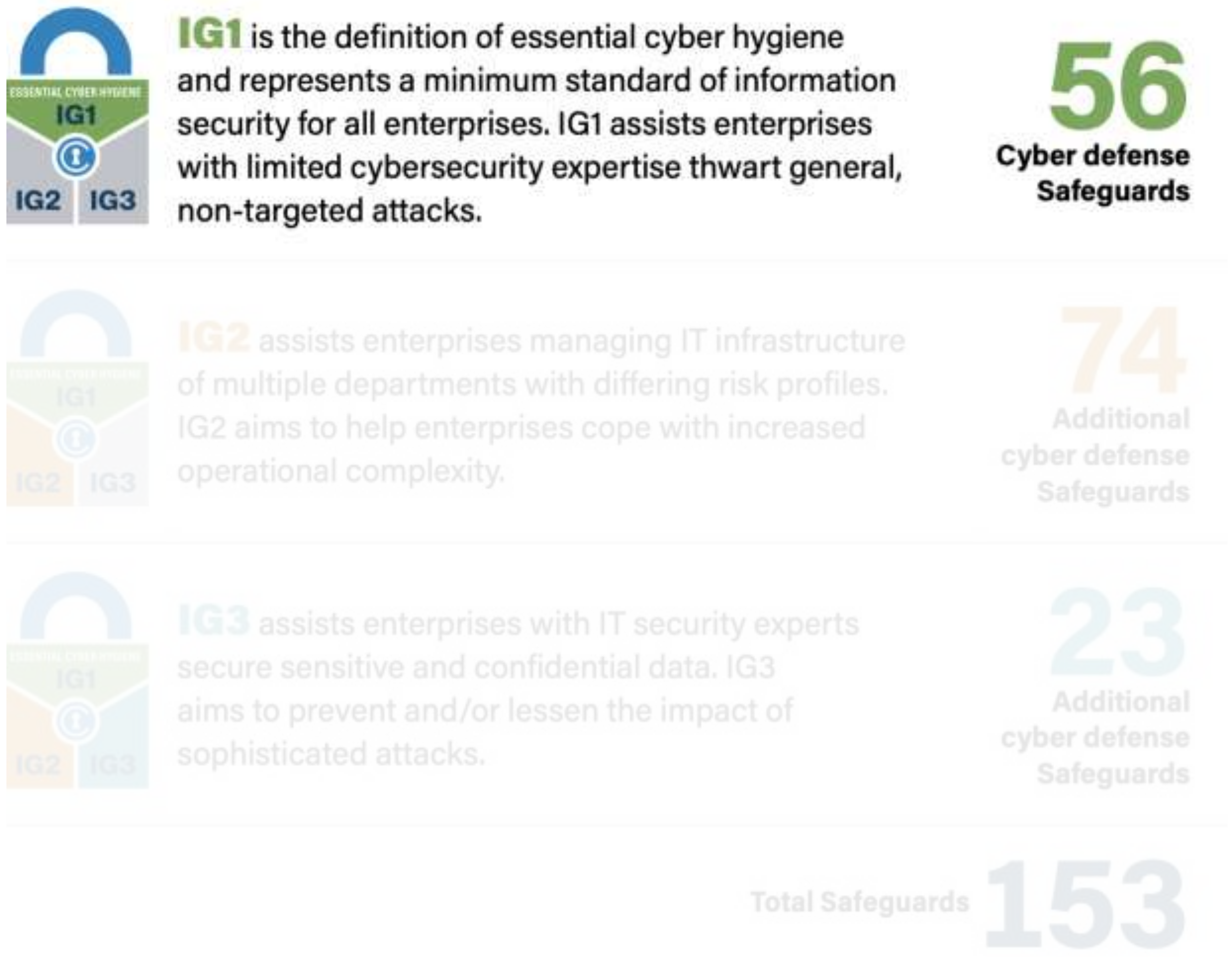
IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

Total Safeguards **153**

Implementation Groups

- **IG1** is the definition of basic cyber hygiene and represents an emerging minimum standard of information security for all enterprises.
- **IG1** is a foundational set of cyber defense Safeguards that every enterprise should apply to guard against the most common attacks.
- **IG2** and **IG3** build upon previous IGs, with IG1 being the on-ramp to the Controls.


ESSENTIAL CYBER HYGIENE
IG1
IG2
IG3

IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 Additional cyber defense Safeguards

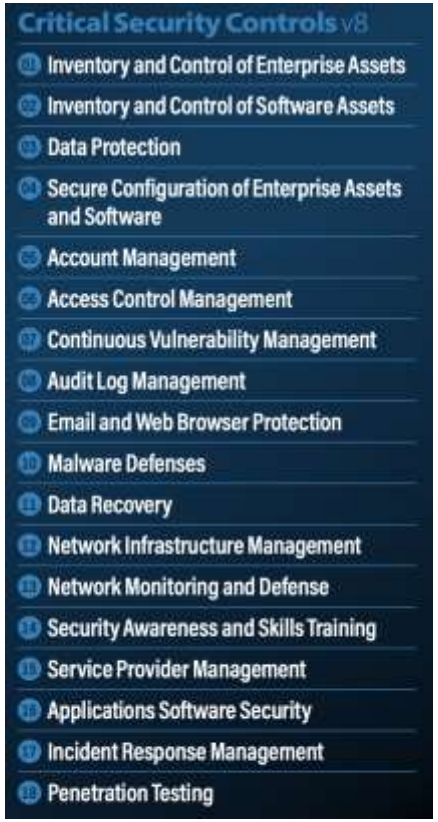
IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

Total Safeguards **153**

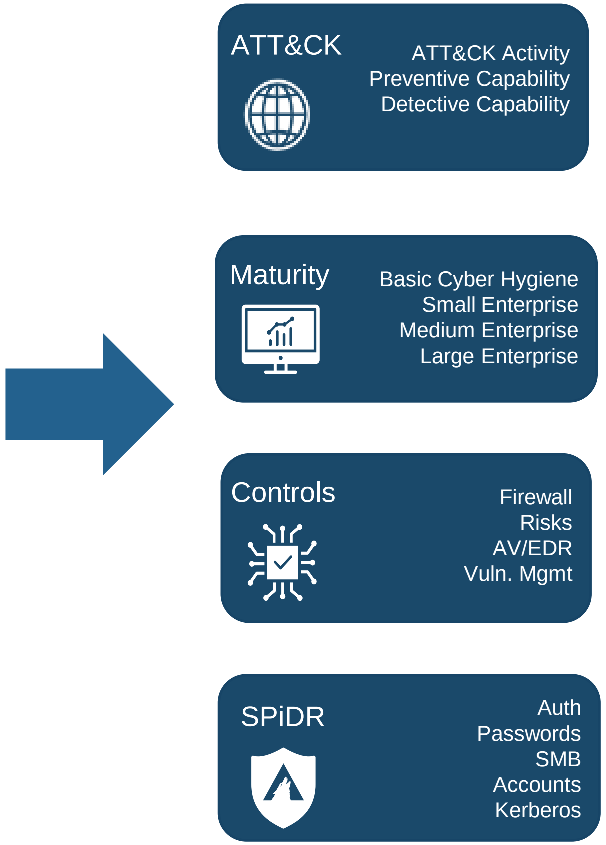
CDMA Workflow

1. Tag Critical Security Controls with SPiDR libary



Critical Security Controls v8

- 01 Inventory and Control of Enterprise Assets
- 02 Inventory and Control of Software Assets
- 03 Data Protection
- 04 Secure Configuration of Enterprise Assets and Software
- 05 Account Management
- 06 Access Control Management
- 07 Continuous Vulnerability Management
- 08 Audit Log Management
- 09 Email and Web Browser Protection
- 10 Malware Defenses
- 11 Data Recovery
- 12 Network Infrastructure Management
- 13 Network Monitoring and Defense
- 14 Security Awareness and Skills Training
- 15 Service Provider Management
- 16 Applications Software Security
- 17 Incident Response Management
- 18 Penetration Testing



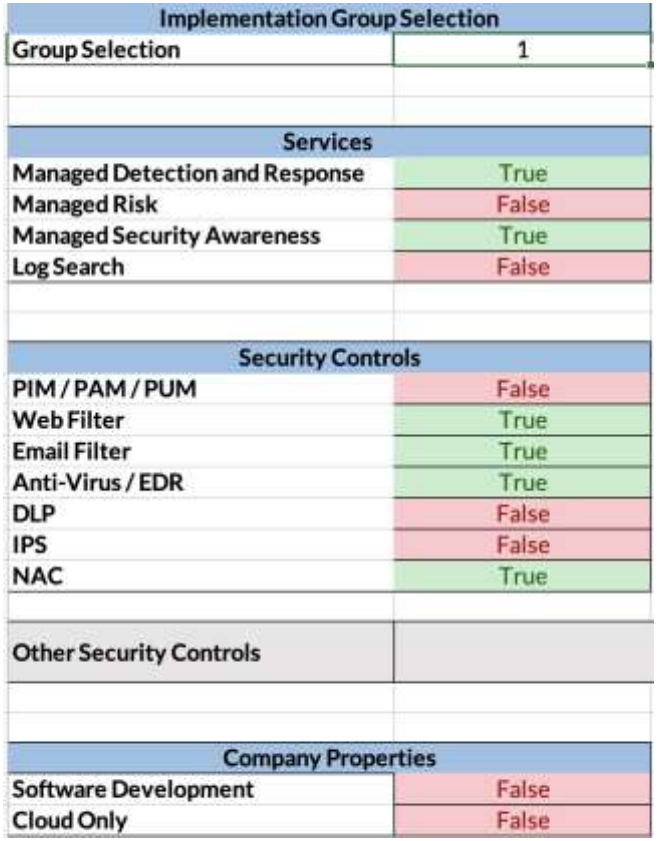
ATT&CK
ATT&CK Activity
Preventive Capability
Detective Capability

Maturity
Basic Cyber Hygiene
Small Enterprise
Medium Enterprise
Large Enterprise

Controls
Firewall
Risks
AV/EDR
Vuln. Mgmt

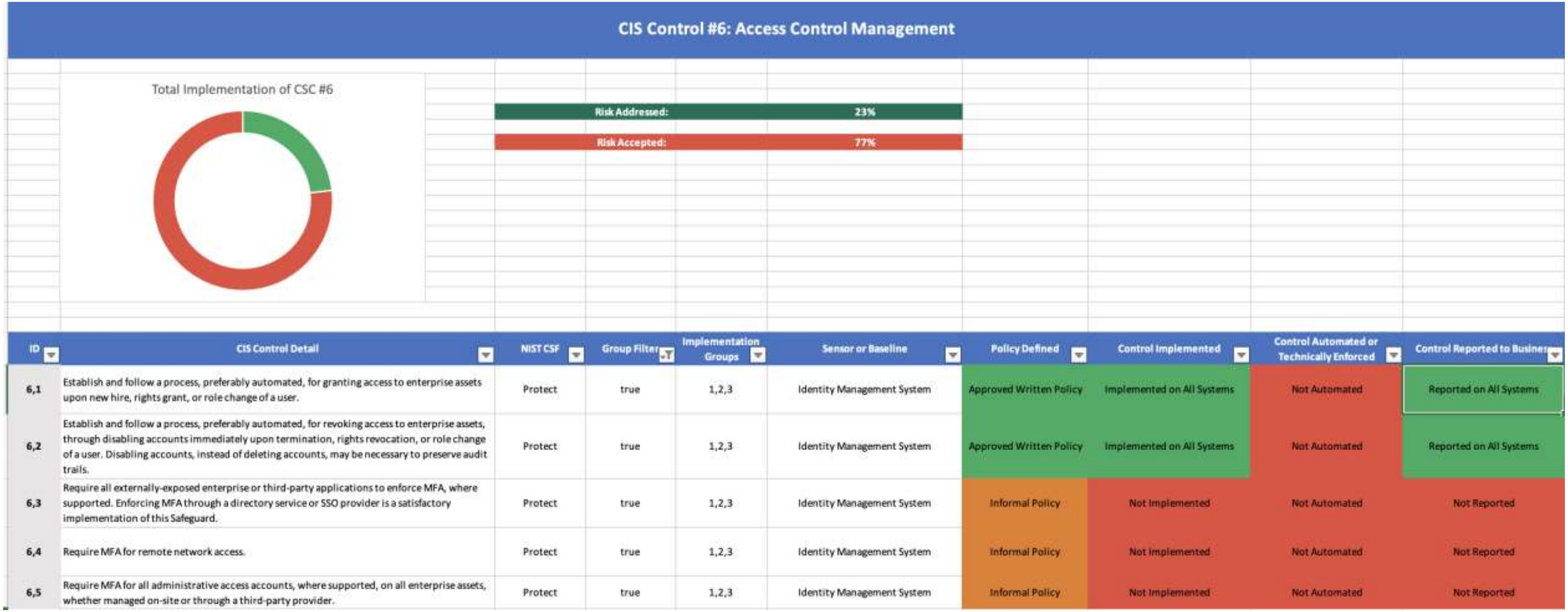
SPiDR
Auth
Passwords
SMB
Accounts
Kerberos

2. Map your SOC services our Security Framework



Implementation Group Selection	
Group Selection	1
Services	
Managed Detection and Response	True
Managed Risk	False
Managed Security Awareness	True
Log Search	False
Security Controls	
PIM / PAM / PUM	False
Web Filter	True
Email Filter	True
Anti-Virus / EDR	True
DLP	False
IPS	False
NAC	True
Other Security Controls	
Company Properties	
Software Development	False
Cloud Only	False

CDMA Workflow



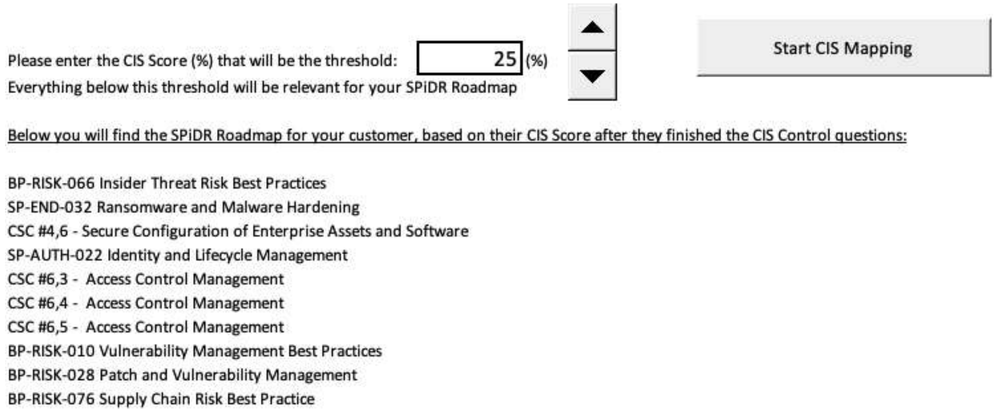
CIS Control #6: Access Control Management

Total Implementation of CSC #6

Risk Addressed:	23%
Risk Accepted:	77%

ID	CIS Control Detail	NIST CSF	Group Filter	Implementation Groups	Sensor or Baseline	Policy Defined	Control Implemented	Control Automated or Technically Enforced	Control Reported to Busines
6,1	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	Protect	true	1,2,3	Identity Management System	Approved Written Policy	Implemented on All Systems	Not Automated	Reported on All Systems
6,2	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Protect	true	1,2,3	Identity Management System	Approved Written Policy	Implemented on All Systems	Not Automated	Reported on All Systems
6,3	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	Protect	true	1,2,3	Identity Management System	Informal Policy	Not Implemented	Not Automated	Not Reported
6,4	Require MFA for remote network access.	Protect	true	1,2,3	Identity Management System	Informal Policy	Not Implemented	Not Automated	Not Reported
6,5	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	Protect	true	1,2,3	Identity Management System	Informal Policy	Not Implemented	Not Automated	Not Reported

3. Generate the results

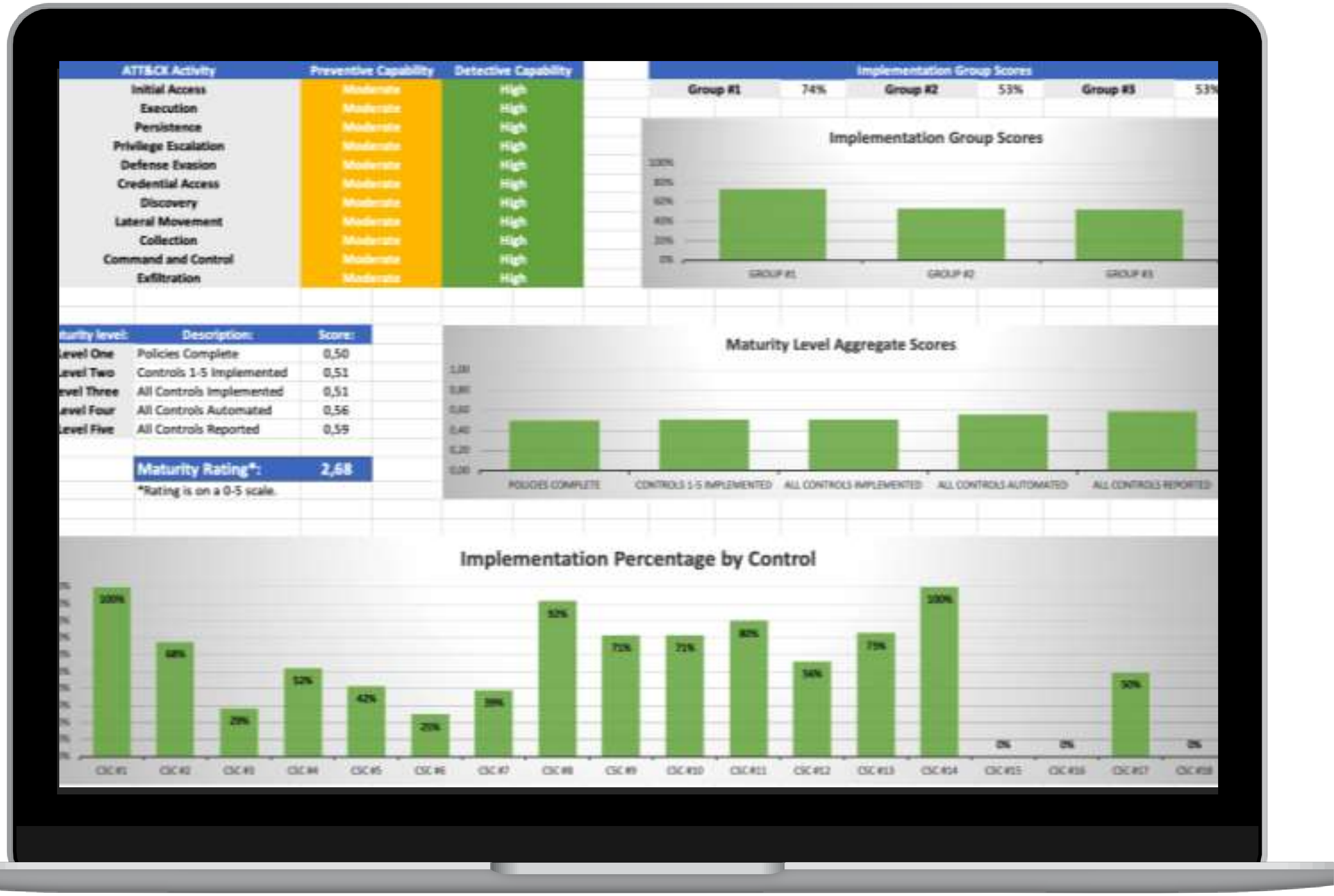


Please enter the CIS Score (%) that will be the threshold: 25 (%)

Everything below this threshold will be relevant for your SPiDR Roadmap

Below you will find the SPiDR Roadmap for your customer, based on their CIS Score after they finished the CIS Control questions:

BP-RISK-066 Insider Threat Risk Best Practices
SP-END-032 Ransomware and Malware Hardening
CSC #4,6 - Secure Configuration of Enterprise Assets and Software
SP-AUTH-022 Identity and Lifecycle Management
CSC #6,3 - Access Control Management
CSC #6,4 - Access Control Management
CSC #6,5 - Access Control Management
BP-RISK-010 Vulnerability Management Best Practices
BP-RISK-028 Patch and Vulnerability Management
BP-RISK-076 Supply Chain Risk Best Practice



ATT&CK Activity	Preventive Capability	Detective Capability
Initial Access	Moderate	High
Execution	Moderate	High
Persistence	Moderate	High
Privilege Escalation	Moderate	High
Defense Evasion	Moderate	High
Credential Access	Moderate	High
Discovery	Moderate	High
Lateral Movement	Moderate	High
Collection	Moderate	High
Command and Control	Moderate	High
Exfiltration	Moderate	High

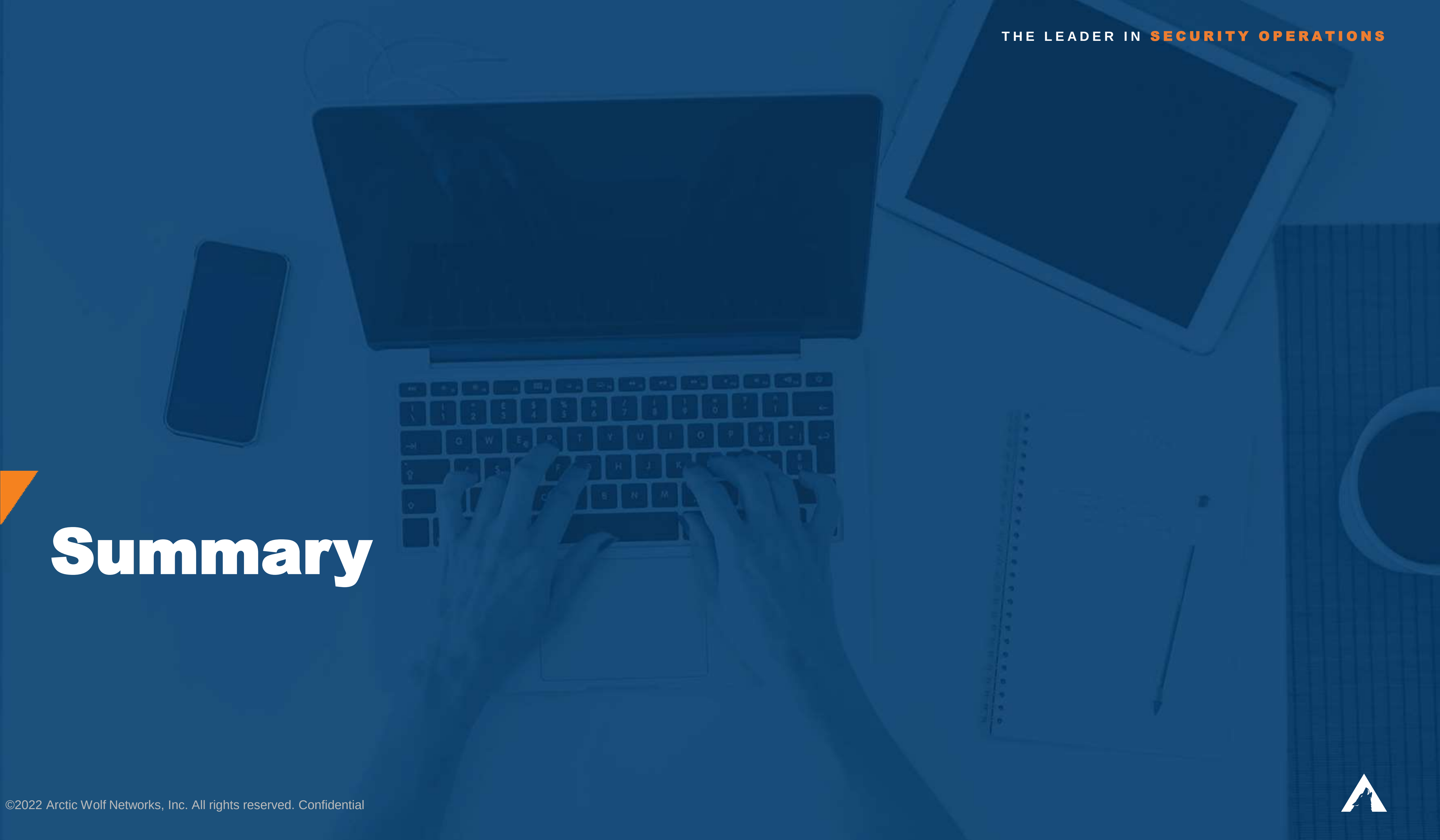
Implementation Group Scores

Group #1	74%	Group #2	53%	Group #3	53%

turity level:	Description:	Score:
Level One	Policies Complete	0,50
Level Two	Controls 1-5 Implemented	0,51
evel Three	All Controls Implemented	0,51
Level Four	All Controls Automated	0,56
Level Five	All Controls Reported	0,59

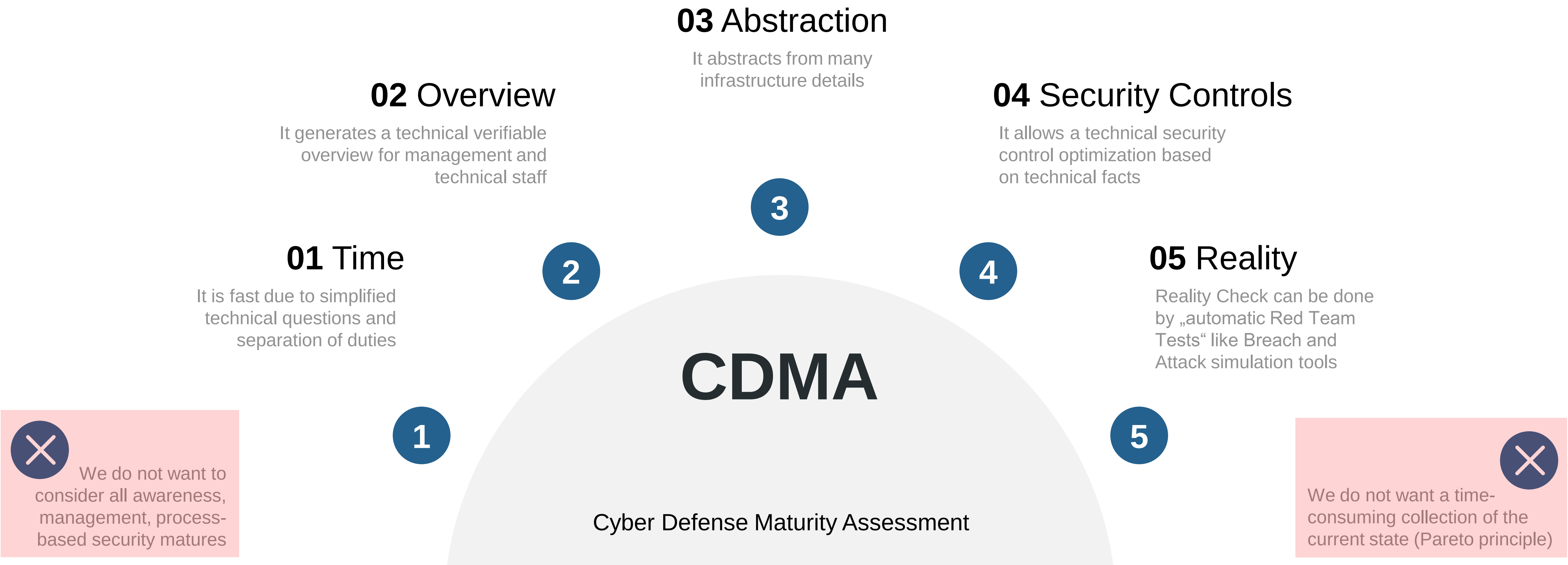
Maturity Rating*: 2,68

*Rating is on a 0-5 scale.



Summary

Summary



01 Time

It is fast due to simplified technical questions and separation of duties

02 Overview

It generates a technical verifiable overview for management and technical staff

03 Abstraction

It abstracts from many infrastructure details

04 Security Controls

It allows a technical security control optimization based on technical facts

05 Reality

Reality Check can be done by „automatic Red Team Tests“ like Breach and Attack simulation tools

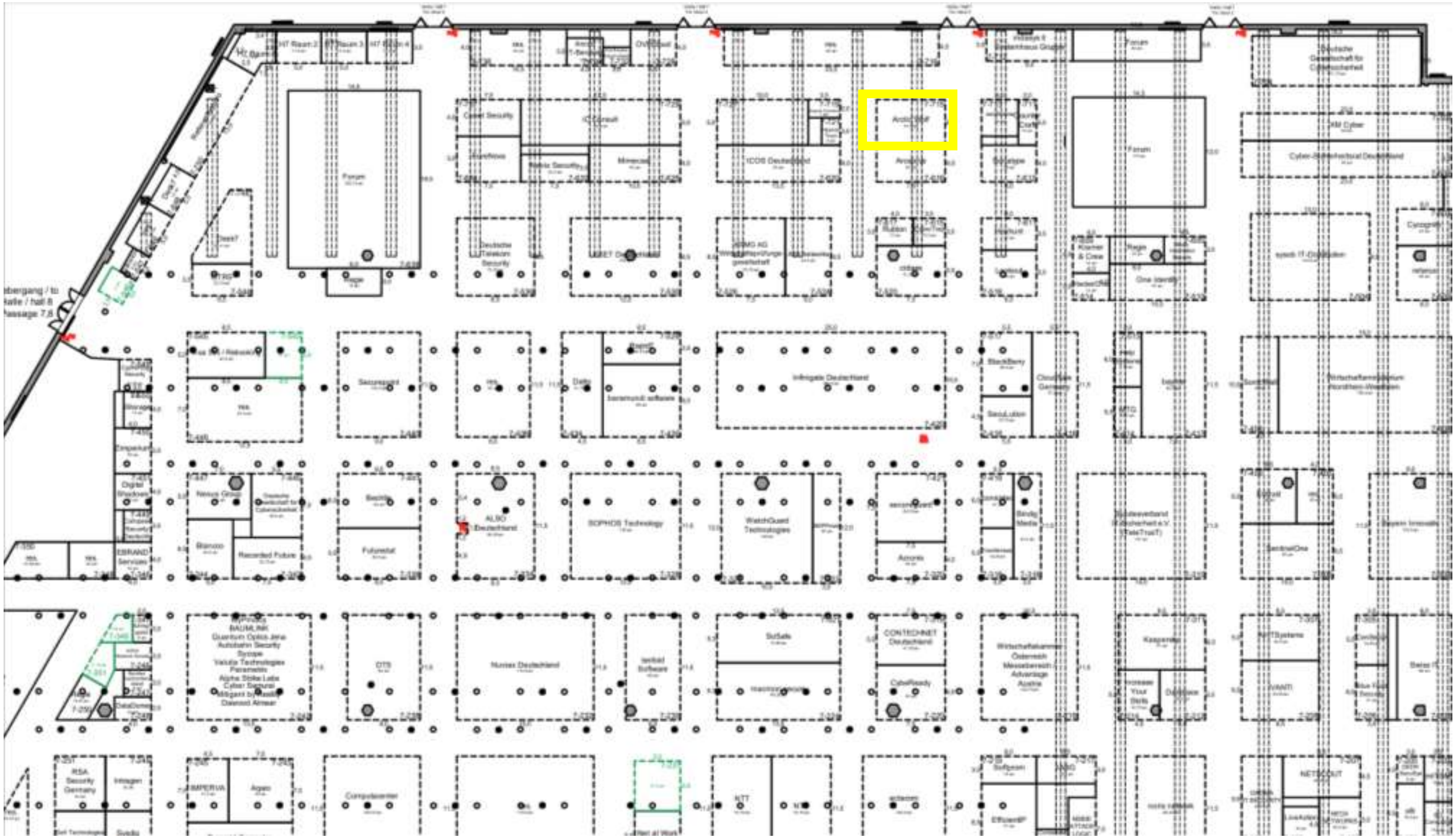
CDMA

Cyber Defense Maturity Assessment

✗ We do not want to consider all awareness, management, process-based security matures

✗ We do not want a time-consuming collection of the current state (Pareto principle)

Wo sind wir: Halle 7, Stand 7-715



Thank You