mnemonic Enterprise Security Architecture (mESA) framework

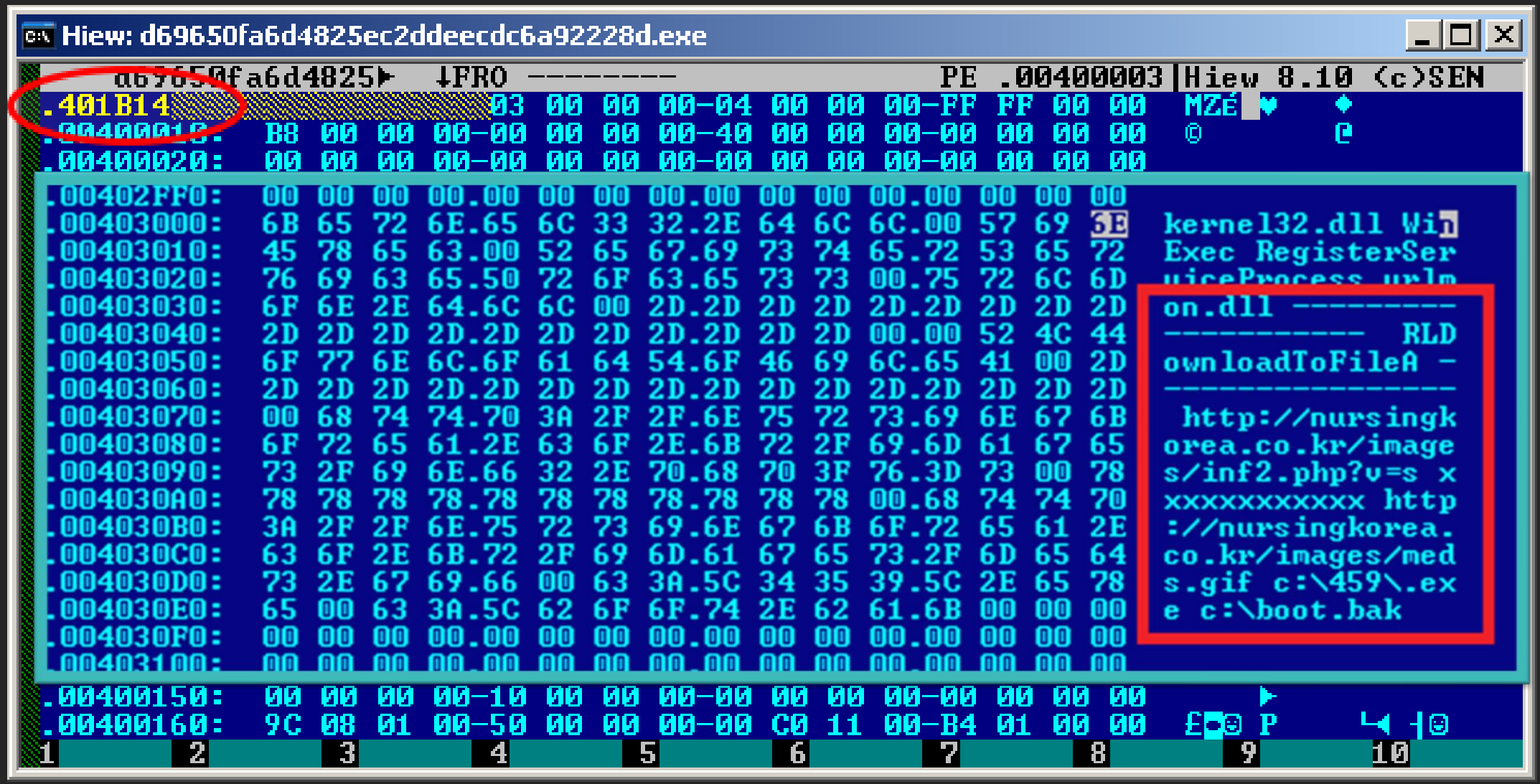
Managing the complexity of cybersecurity

Angel Alonso

alonso@mnemonic.no

Team leader GRC

CCISO CISM ISO27001 LI
CISSP CISA SABSA SCF
CCSP CDPSE CIPP/E CIPM
GCLD CCSK CCAK FAIR™


Hiew: d69650fa6d4825ec2ddeecdc6a92228d.exe
d69650fa6d4825▶ ↓FRO -------- PE .00400003 Hiew 8.10 (c)SEN
.401B14: 03 00 00 00-04 00 00 00-FF FF 00 00 MZÉ ♥ ♦
.00400010: B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00 © @
.00400020: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
.00402FF0: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00403000: 6B 65 72 6E.65 6C 33 32.2E 64 6C 6C.00 57 69 3E kernel32.dll Wi
.00403010: 45 78 65 63.00 52 65 67.69 73 74 65.72 53 65 72 Exec RegisterSer
.00403020: 76 69 63 65.50 72 6F 63.65 73 73 00.75 72 6C 6D
.00403030: 6F 6E 2E 64.6C 6C 00 2D.2D 2D 2D 2D.2D 2D 2D 2D on.dll ----------
.00403040: 2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 00.00 52 4C 44 ---------- RLD
.00403050: 6F 77 6E 6C.6F 61 64 54.6F 46 69 6C.65 41 00 2D ownloadToFileA -
.00403060: 2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D.2D 2D 2D 2D ----------
.00403070: 00 68 74 74.70 3A 2F 2F.6E 75 72 73.69 6E 67 6B http://nursingk
.00403080: 6F 72 65 61.2E 63 6F 2E.6B 72 2F 69.6D 61 67 65 orea.co.kr/image
.00403090: 73 2F 69 6E.66 32 2E 70.68 70 3F 76.3D 73 00 78 s/inf2.php?v=s x
.004030A0: 78 78 78 78.78 78 78 78.78 78 78 00.68 74 74 70 xxxxxxxxxxx http
.004030B0: 3A 2F 2F 6E.75 72 73 69.6E 67 6B 6F.72 65 61 2E ://nursingkorea.
.004030C0: 63 6F 2E 6B.72 2F 69 6D.61 67 65 73.2F 6D 65 64 co.kr/images/med
.004030D0: 73 2E 67 69.66 00 63 3A.5C 34 35 39.5C 2E 65 78 s.gif c:\459\.ex
.004030E0: 65 00 63 3A.5C 62 6F 6F.74 2E 62 61.6B 00 00 00 e c:\boot.bak
.004030F0: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00403100: 00 00 00 00.00 00 00 00.00 00 00 00.00 00 00 00
.00400150: 00 00 00 00-10 00 00 00-00 00 00 00-00 00 00 00 ▶
.00400160: 9C 08 01 00-50 00 00 00-00 C0 11 00-B4 01 00 00 £☺☺ P └┤☺
1 2 3 4 5 6 7 8 9 10

Working in cybersecurity today is really difficult

Cybersecurity is complex

CONSTANT CHANGE IN:

- the threat landscape
- legislations, government policies and regulatory requirements
- cyber-attack methods

SHORTAGE OF EXPERTISE:

Difficult to obtain the right security skills due to the general shortage in the market

Considerable consequences

$4.24m*

GLOBAL AVERAGE TOTAL COST OF A DATA BREACH

287 Days*

AVERAGE NUMBER TO IDENTIFY AND CONTAIN A DATA BREACH

**Ponemon Institute 2022*
***Statista, Nov. 2021*

mnemonic

Cybersecurity is complex and open to interpretation

enabler,
not stopper

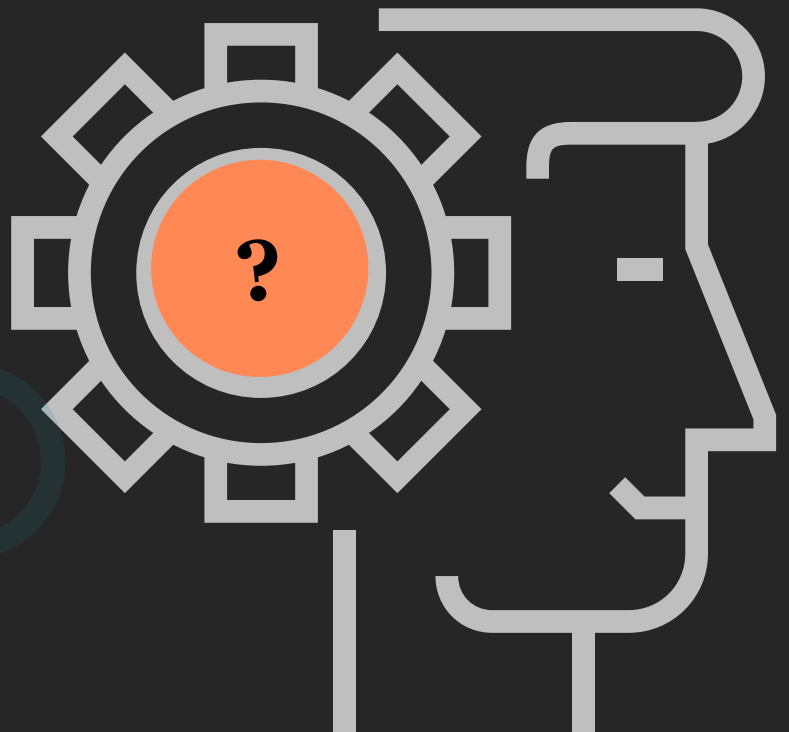
"**business**
-oriented"

"risk
-based"

relevant
threats

"reasonable"
security

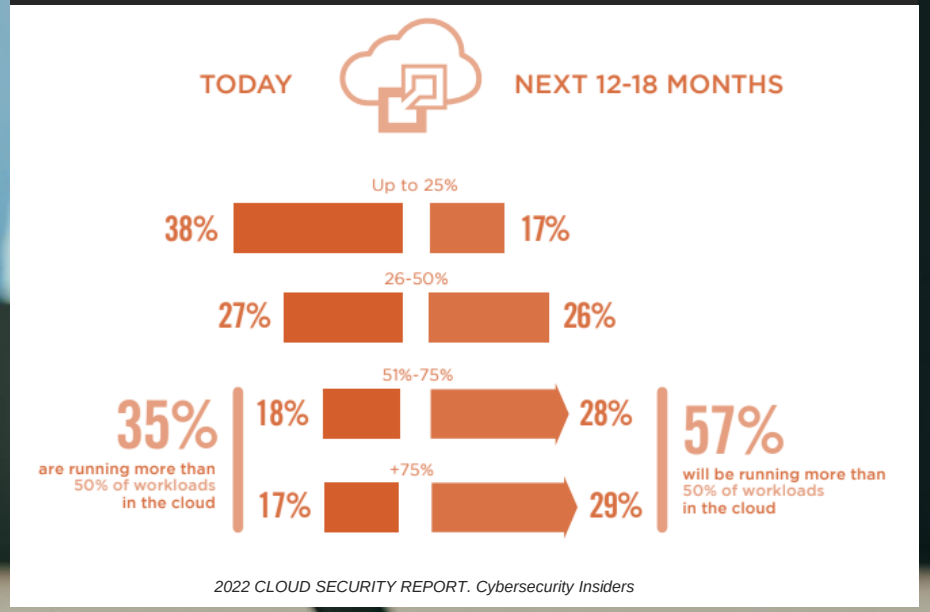
"adequate"
safeguards



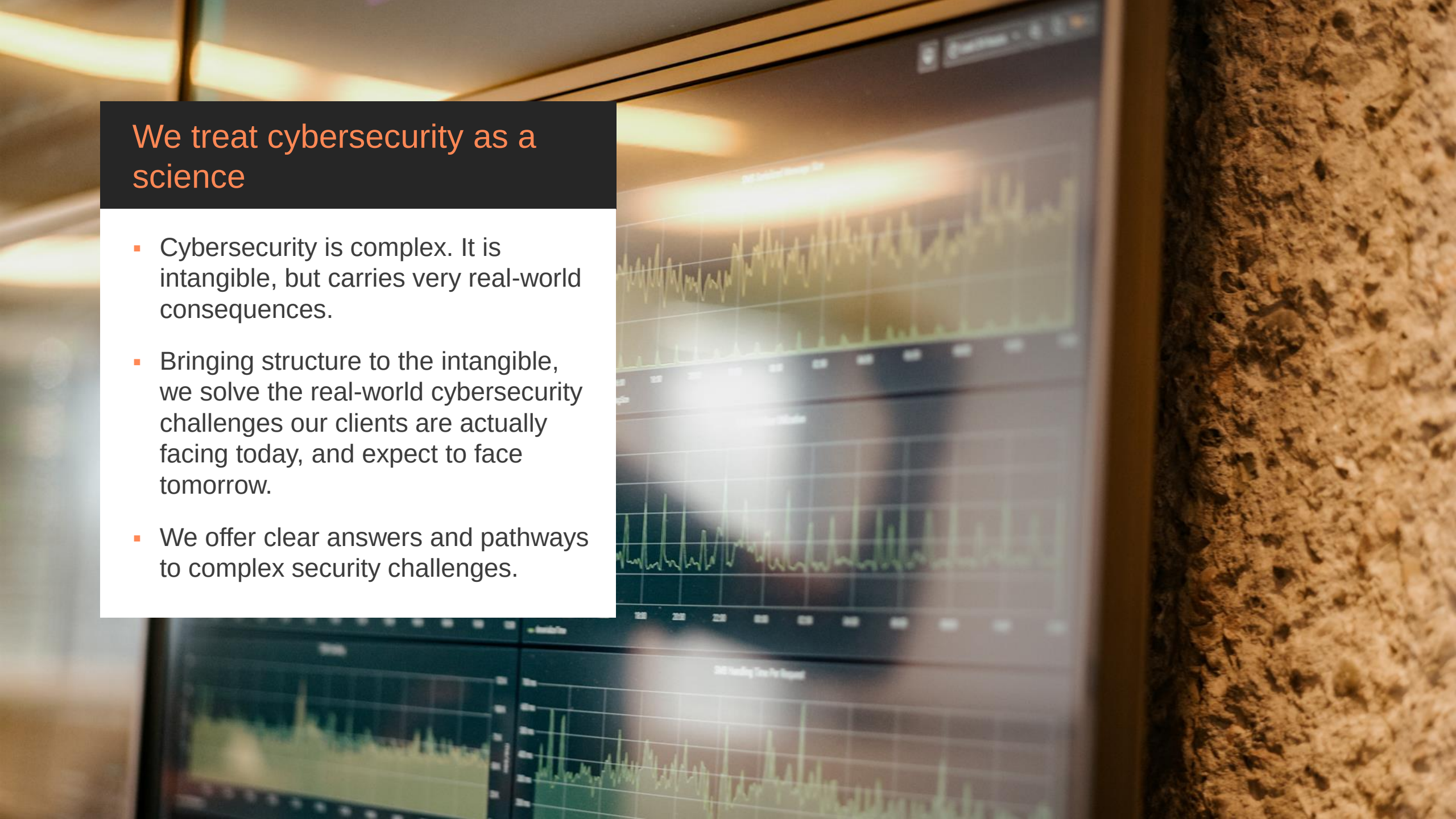
"appropriate"
security
measures

"defendable"
security

Customers and regulators are asking how are you doing security today, is your cybersecurity good enough?



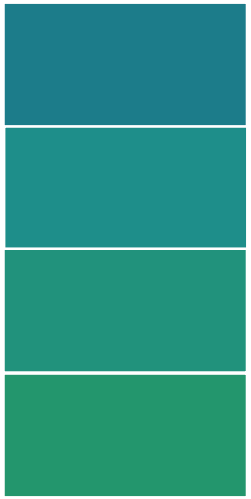
2022 CLOUD SECURITY REPORT. Cybersecurity Insiders



We treat cybersecurity as a science

- Cybersecurity is complex. It is intangible, but carries very real-world consequences.
- Bringing structure to the intangible, we solve the real-world cybersecurity challenges our clients are actually facing today, and expect to face tomorrow.
- We offer clear answers and pathways to complex security challenges.

Dealing with the complexity – using *mnemonic Enterprise Security Architecture (mESA)* framework



Problem #1

Choosing controls

There exist a myriad of different best practices, standards, industry specific guidelines and legislation for cyber security

Best practices

CIS Controls™

CCM™ Cloud Controls Matrix

NSMs Grunnprinsipper for IKT-sikkerhet

Standards

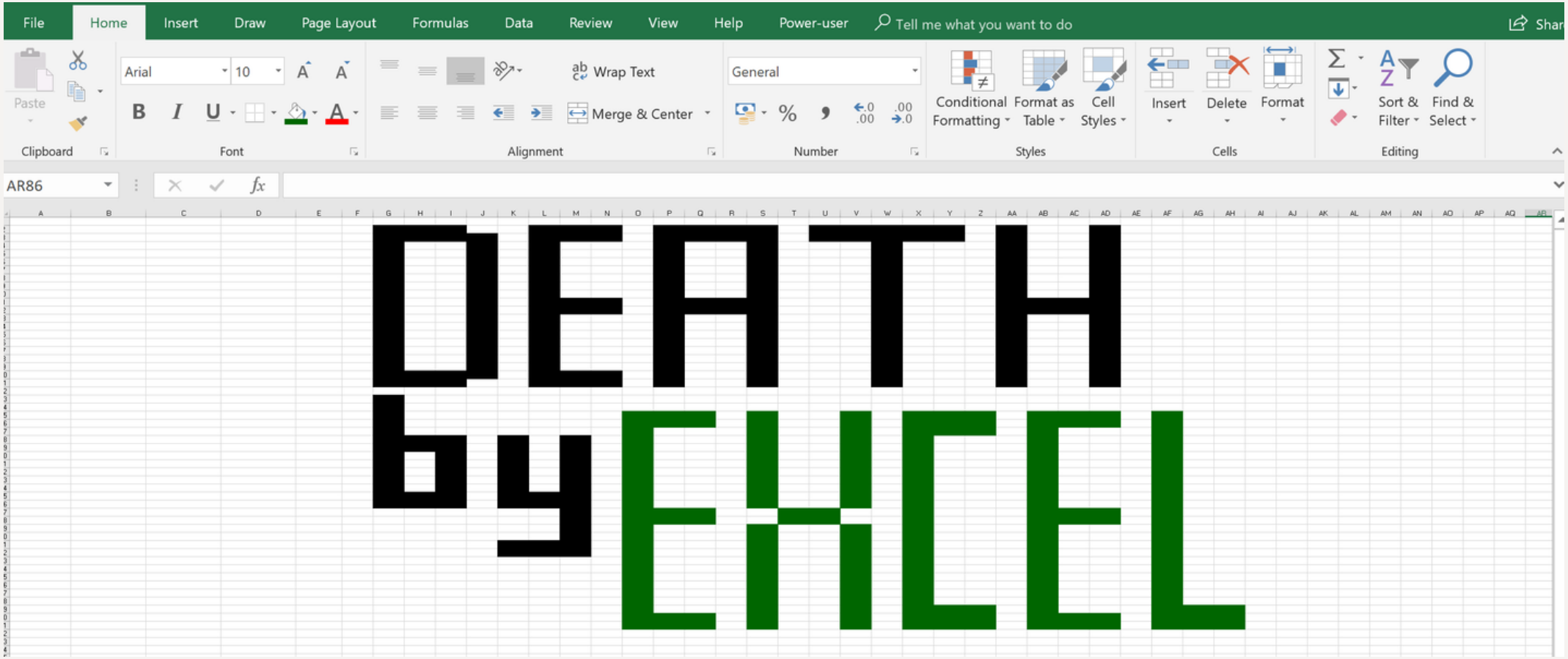
ISO 27001

Legislation

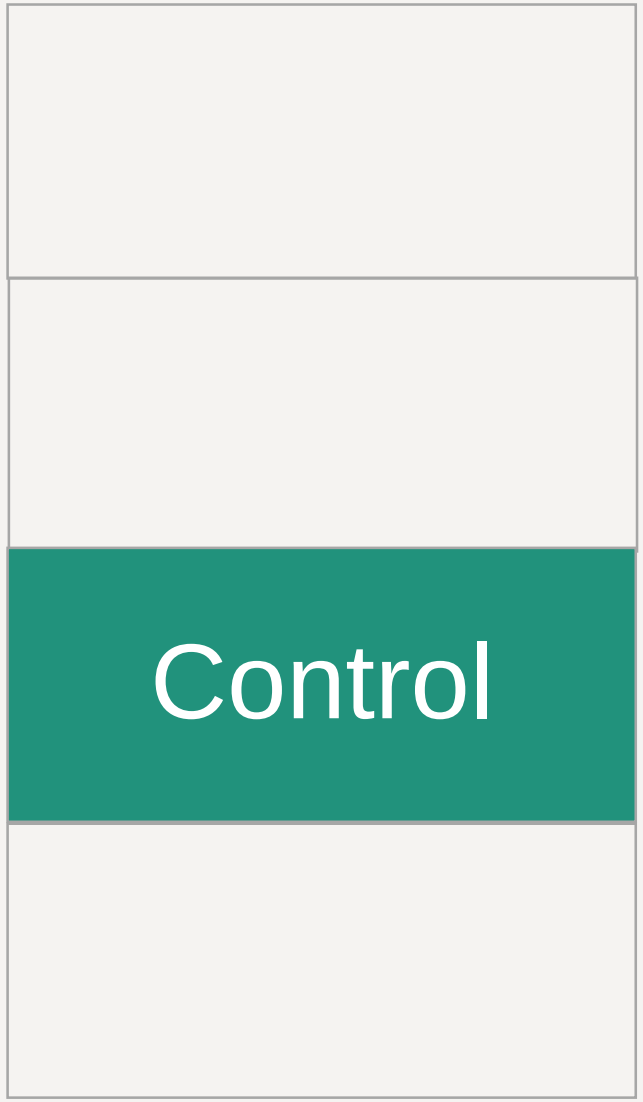
- Sikkerhetsloven
- General Data Protection Regulation (GDPR)
- Kraftberedskapsforskriften
- Normen[1]
- eIDAS[2]

Note 1: Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren
Note 2: Lov om elektroniske tillitstjenester og Forskrift om selvdeklarasjon av ordninger for eID

All frameworks have some form of logical structure that can be broken down where many refer to each other



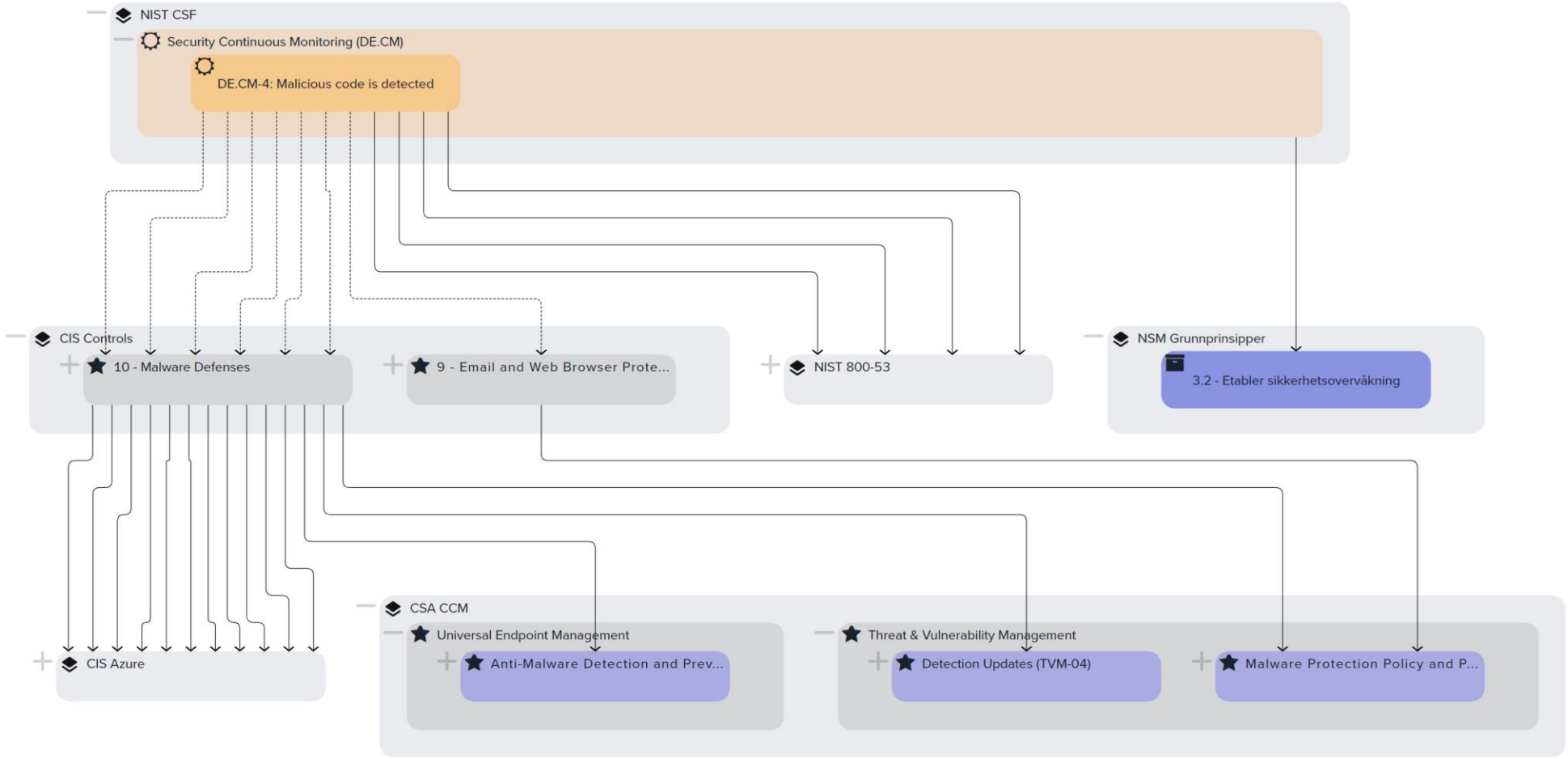
mESA – Control layer

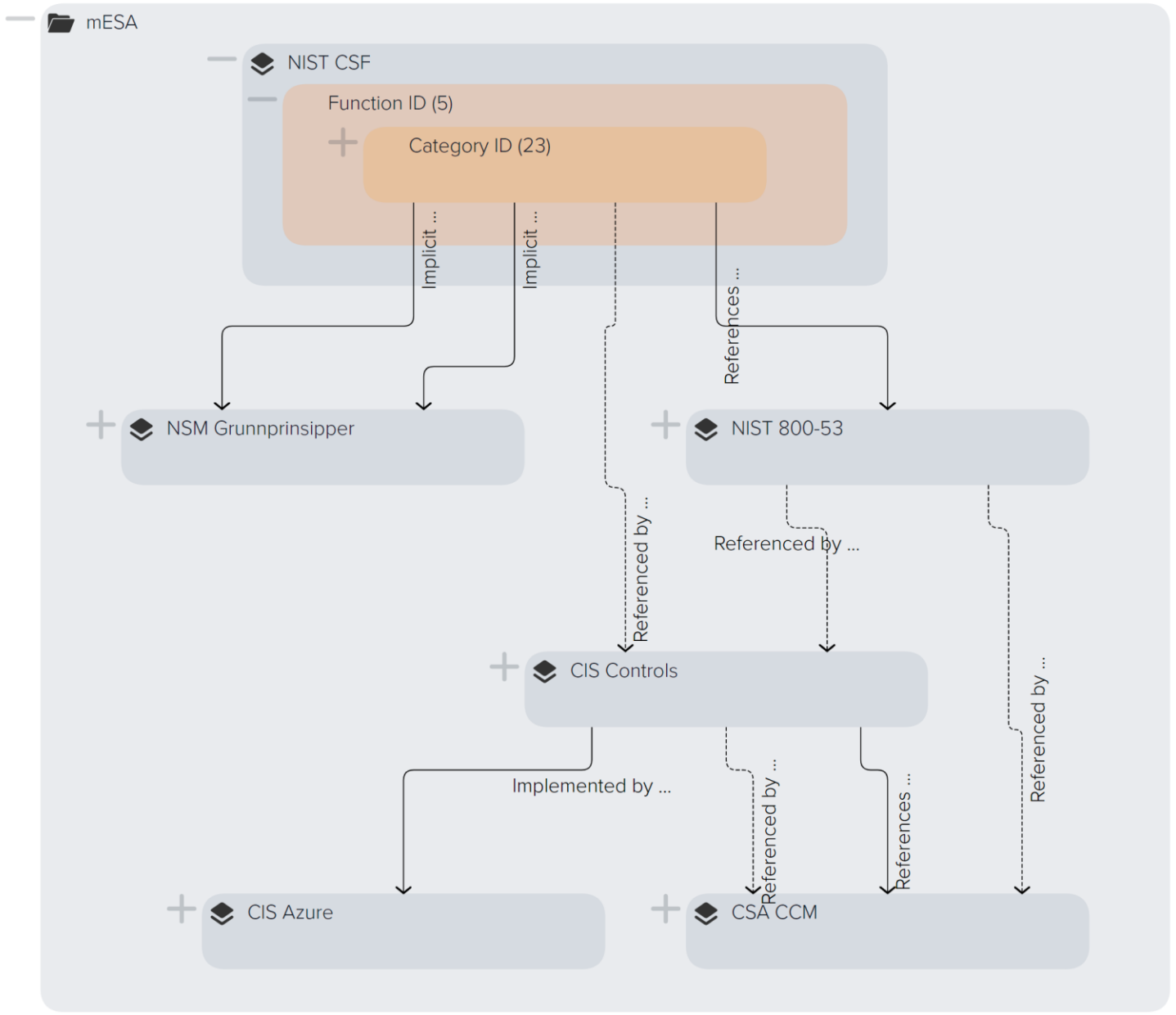


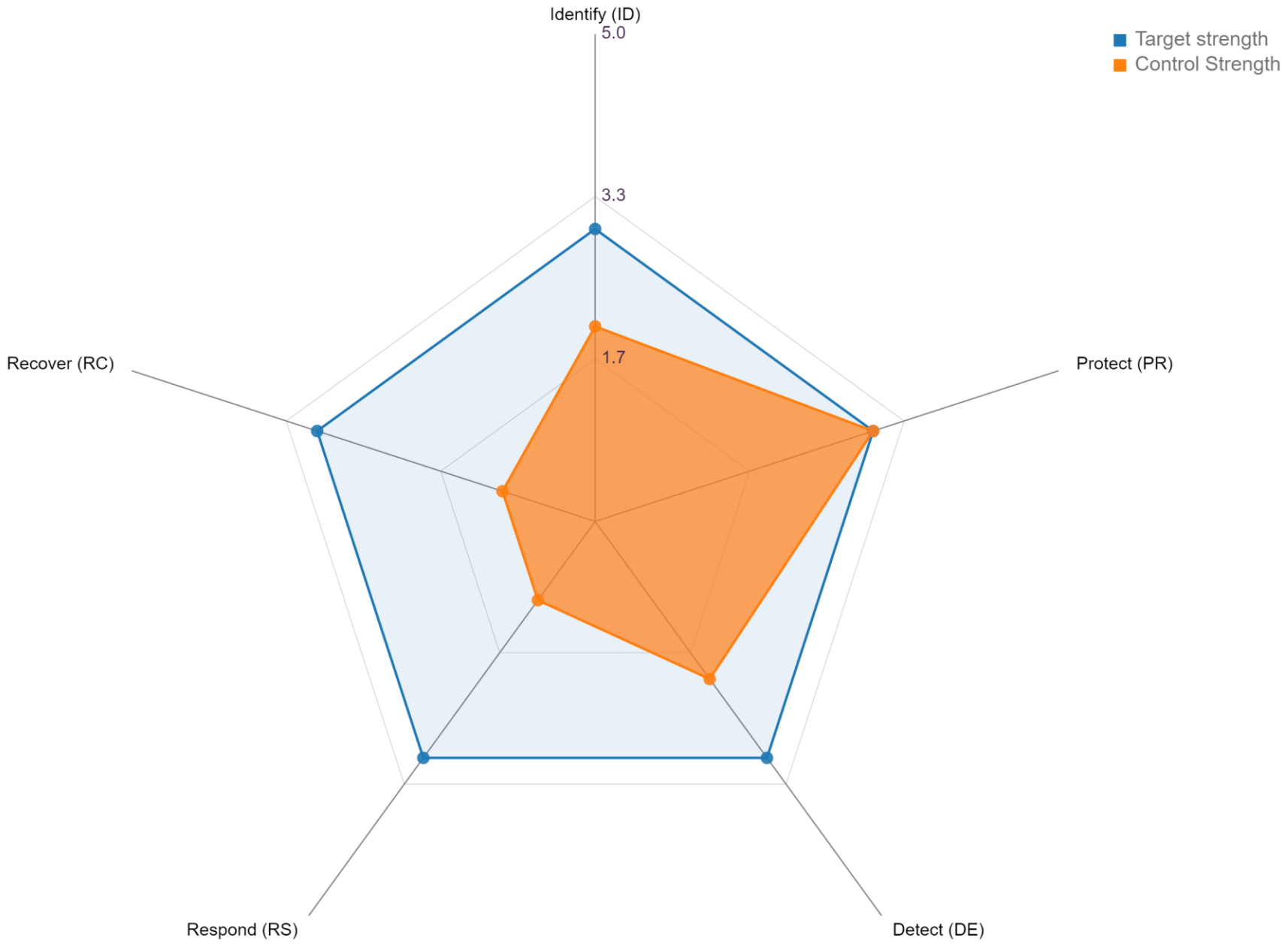
Control objectives
Controls measures

DE.CM-4: Malicious code is detected

Control frameworks




mESA
NIST CSF
Function ID (5)
Category ID (23)
Implicit ...
Implicit ...
References ...
NSM Grunnprinsipper
NIST 800-53
Referenced by ...
Referenced by ...
Referenced by ...
CIS Controls
Implemented by ...
Referenced by ...
References ...
Referenced by ...
CIS Azure
CSA CCM


Identify (ID)
5.0
3.3
1.7
Target strength
Control Strength
Protect (PR)
Detect (DE)
Respond (RS)
Recover (RC)

1 - Identifisere og kartlegge

- 1.1 - Kartlegg styringsstrukturer, leveranser og understøttende systemer
- 1.2 - Kartlegg enheter og programvare
- 1.3 - Kartlegg brukere og behov for tilgang

2 - Beskytte og opprettholde

- 2.1 - Ivareta sikkerhet i anskaffelses- og utviklingsprosesser
- 2.2 - Etabler en sikker IKT-arkitektur
- 2.3 - Ivareta en sikker konfigurasjon
- 2.4 - Beskytt virksomhetens nettverk
- 2.5 - Kontroller dataflyt
- 2.6 - Ha kontroll på identiteter og tilganger
- 2.7 - Beskytt data i ro og i transitt
- 2.8 - Beskytt e-post og nettleser
- 2.9 - Etabler evne til gjenoppretting av data
- 2.10 - Integrer sikkerhet i prosess for endringshåndtering

3 - Oppdage

- 3.1 - Oppdag og fjern kjente sårbarheter og trusler
- 3.2 - Etabler sikkerhetsovervåkning
- 3.3 - Analyser data fra sikkerhetsovervåkning
- 3.4 - Gjennomfør inntrengningstester

4 - Håndtere og gjenopprette

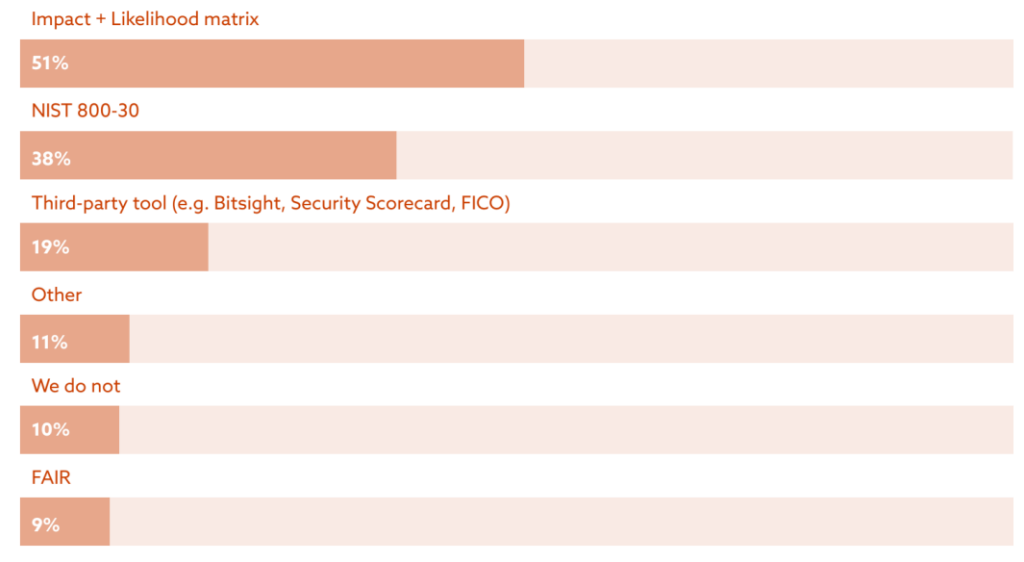
- 4.1 - Forbered virksomheten på håndtering av hendelser
- 4.2 - Vurder og klassifiser hendelser
- 4.3 - Kontroller og håndter hendelser
- 4.4 - Evaluer og lær av hendelser

Problem #2

Mitigating risk

“Risk-based approach”, what does it mean in practice?

Key Finding 4 - Monitoring, measuring, and reporting risk is difficult

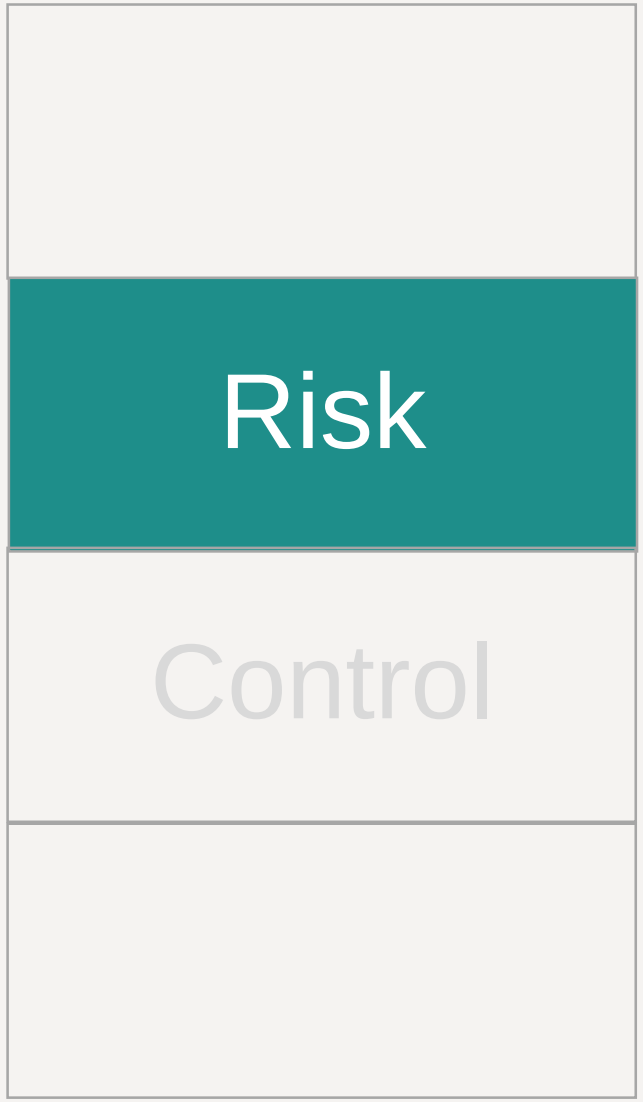


2022 Measuring Risk and Risk Governance report. Cloud Security Alliance

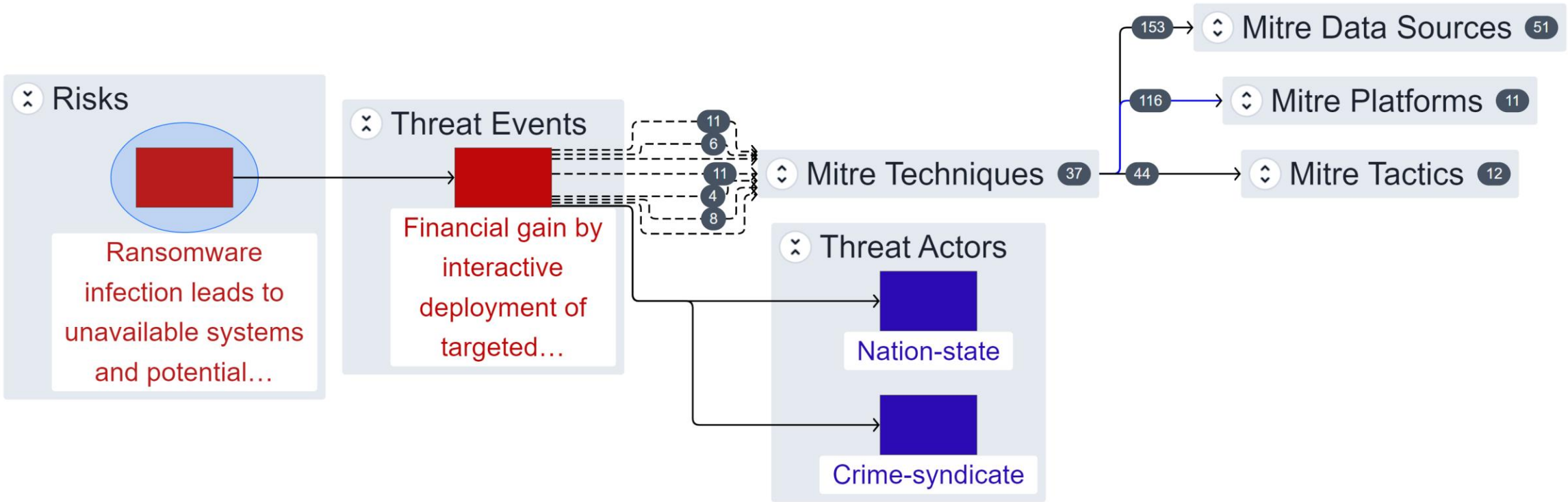
> “… take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.”

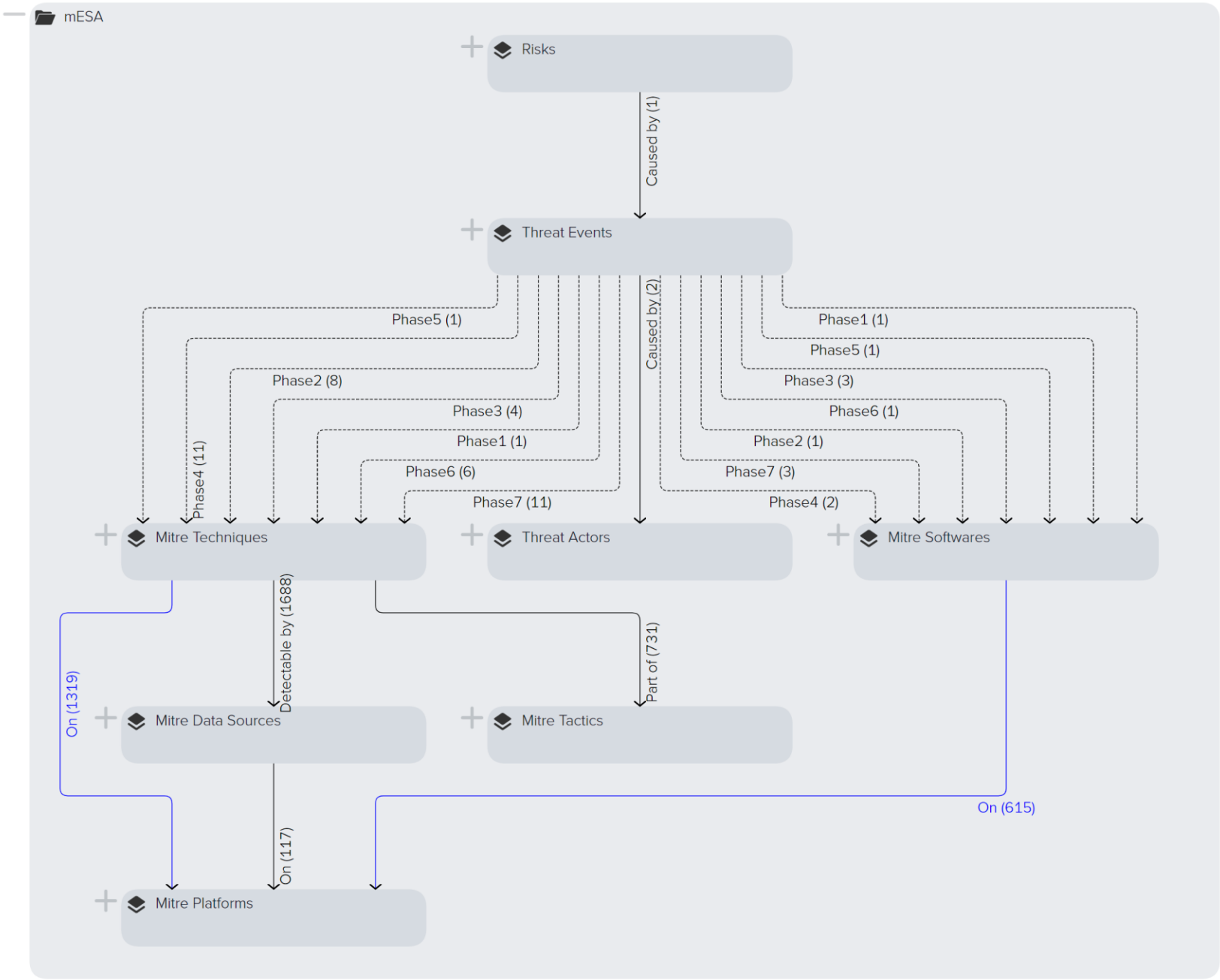
Network and information security (NIS) directive Article 14.1

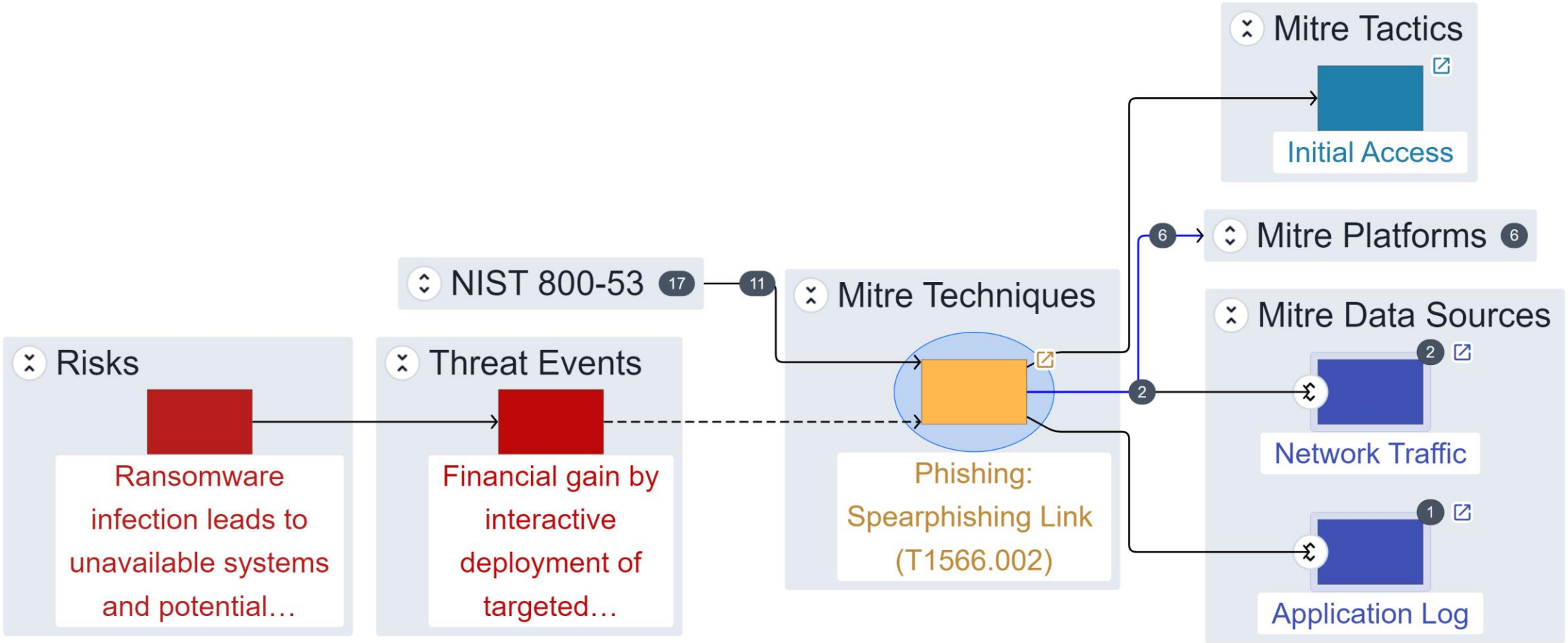
mESA - Risk layer



Threat events
Threat actors
Adversary techniques


Risks
Ransomware infection leads to unavailable systems and potential…
Threat Events
Financial gain by interactive deployment of targeted…
11
6
11
4
8
Mitre Techniques 37
153
Mitre Data Sources 51
116
Mitre Platforms 11
44
Mitre Tactics 12
Threat Actors
Nation-state
Crime-syndicate

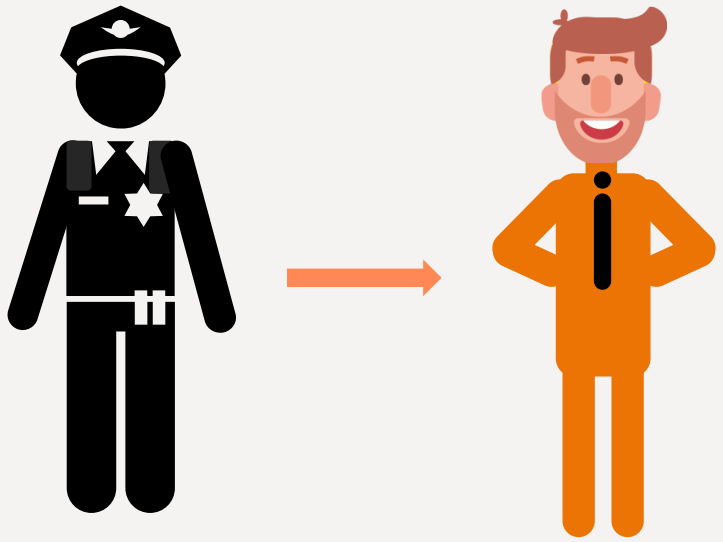

mESA
Risks
Caused by (1)
Threat Events
Phase5 (1)
Phase4 (11)
Phase2 (8)
Phase3 (4)
Phase1 (1)
Phase6 (6)
Phase7 (11)
Caused by (2)
Phase1 (1)
Phase5 (1)
Phase3 (3)
Phase6 (1)
Phase2 (1)
Phase7 (3)
Phase4 (2)
Mitre Techniques
Threat Actors
Mitre Softwares
Detectable by (1688)
Part of (731)
On (1319)
Mitre Data Sources
Mitre Tactics
On (615)
On (117)
Mitre Platforms


Mitre Tactics
Initial Access
6
Mitre Platforms 6
NIST 800-53 17
11
Mitre Techniques
Mitre Data Sources
Risks
Threat Events
2
2
Network Traffic
1
Application Log
Ransomware infection leads to unavailable systems and potential…
Financial gain by interactive deployment of targeted…
Phishing: Spearphishing Link (T1566.002)

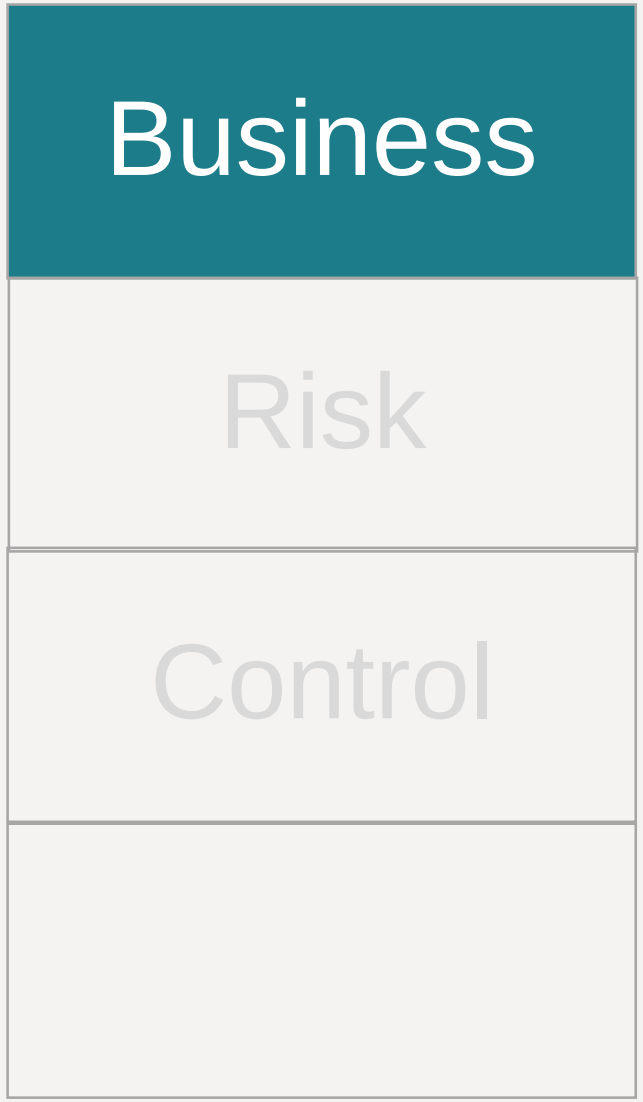
Problem #3

Supporting the business

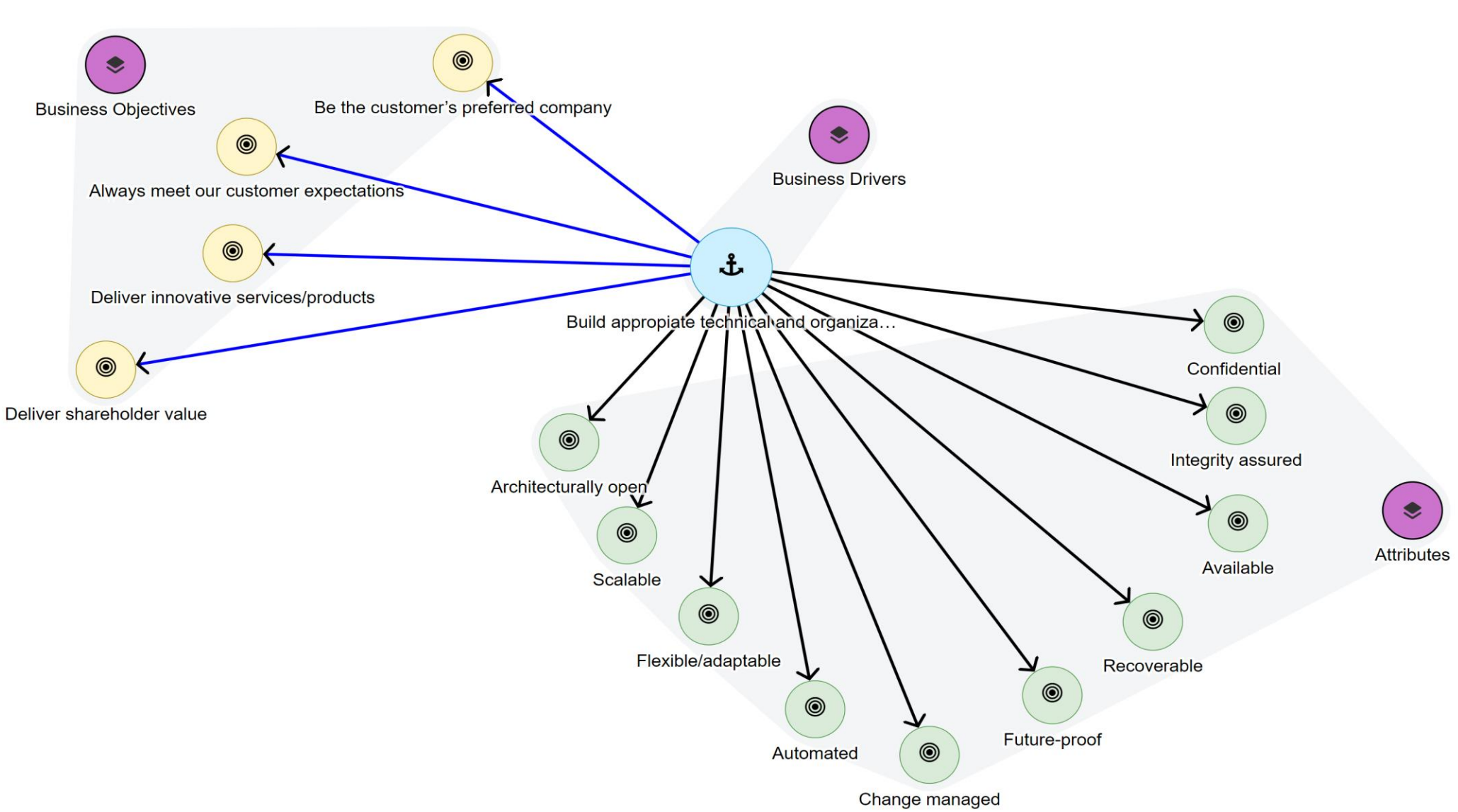
“Business-oriented”, how security can support the business?



mESA – Business layer



Business objectives
Business drivers for security
Attributes

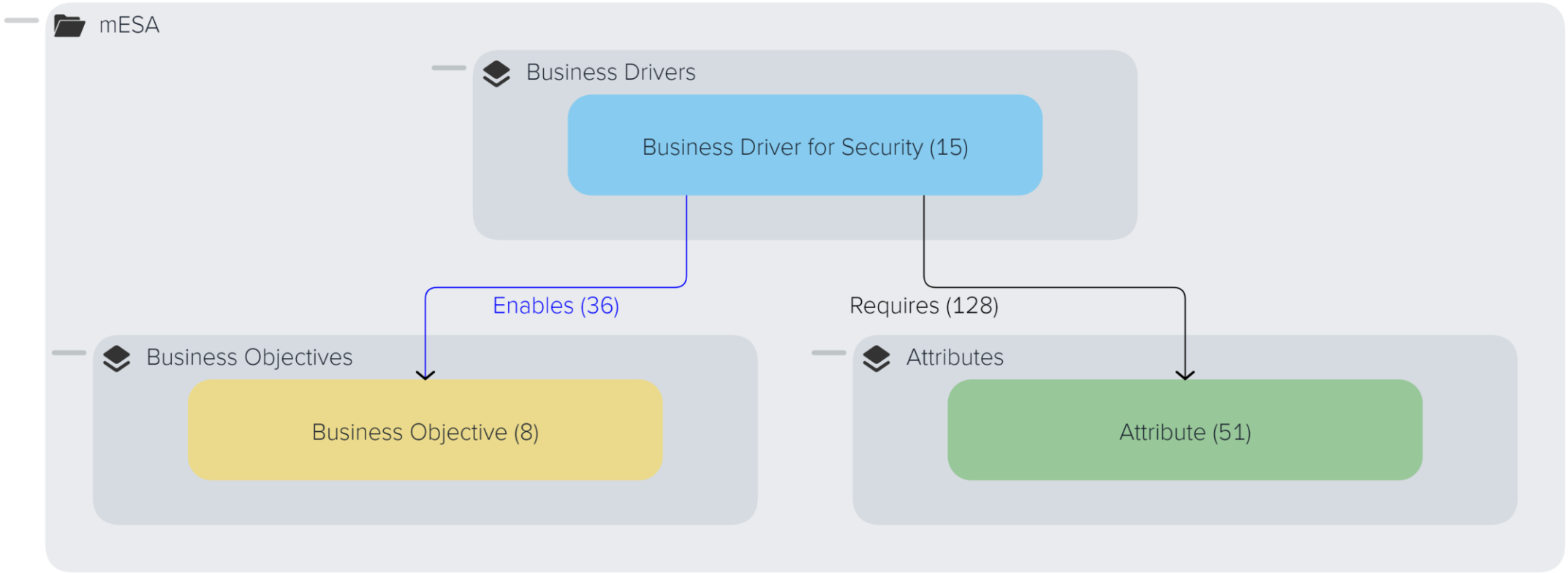


Components

- Business Driver for Security
- Attribute
- Business Objective

References

- Requires
- Enables

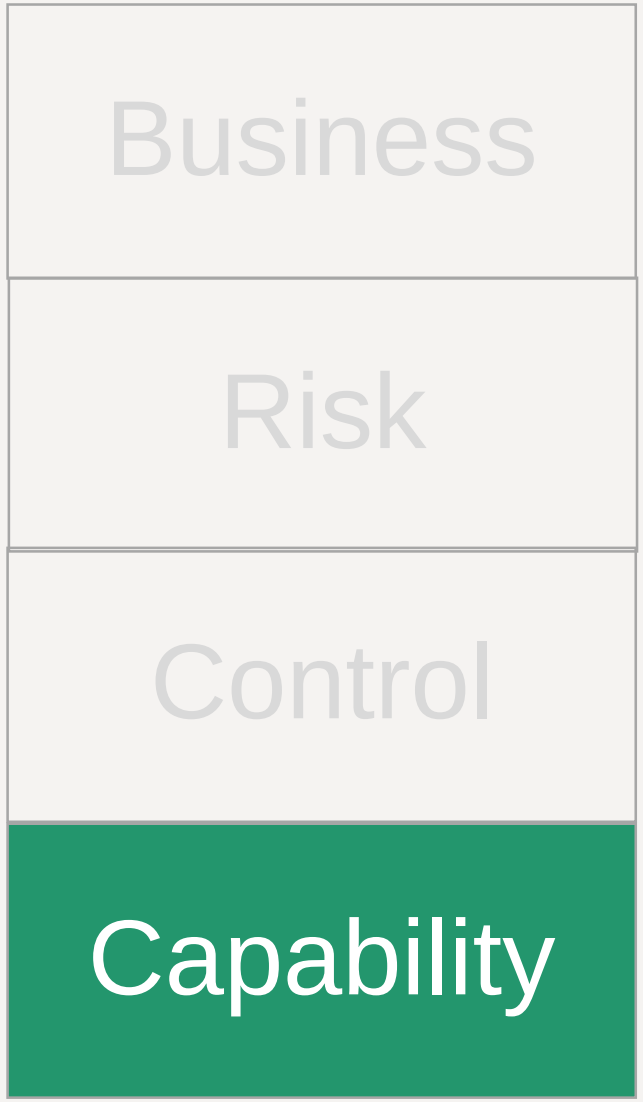

mESA
Business Drivers
Business Driver for Security (15)
Enables (36)
Requires (128)
Business Objectives
Business Objective (8)
Attributes
Attribute (51)

Problem #4

Effectively using your capabilities

Many vendors, many technologies. How to maintain a proper portfolio with limited resources ?

mESA – Capability layer



Services
Technologies
Vendors

mnemonic

Argus Endpoint Responder

mnemonic Portfolio

Managed Detection & Response

Argus Endpoint Responder

USES
Endpoint Detection and Response (EDR)

- DELIVERED BY Carbon Black
- DELIVERED BY Crowdstrike
- DELIVERED BY Guidance
- DELIVERED BY mnemonic
- DELIVERED BY Palo Alto Networks
- DELIVERED BY Trend Micro

USES
Extended Detection and Response (XDR)

- DELIVERED BY Crowdstrike
- DELIVERED BY Palo Alto Networks
- DELIVERED BY Trellix
- DELIVERED BY Trend Micro

RECOMMENDATION
3.1 Security events are identified, collected and monitored

RECOMMENDATION
3.2 Security events are analysed to detect anomalies and malicious activity

RECOMMENDATION
4.1 Response and Recovery processes are established and tested

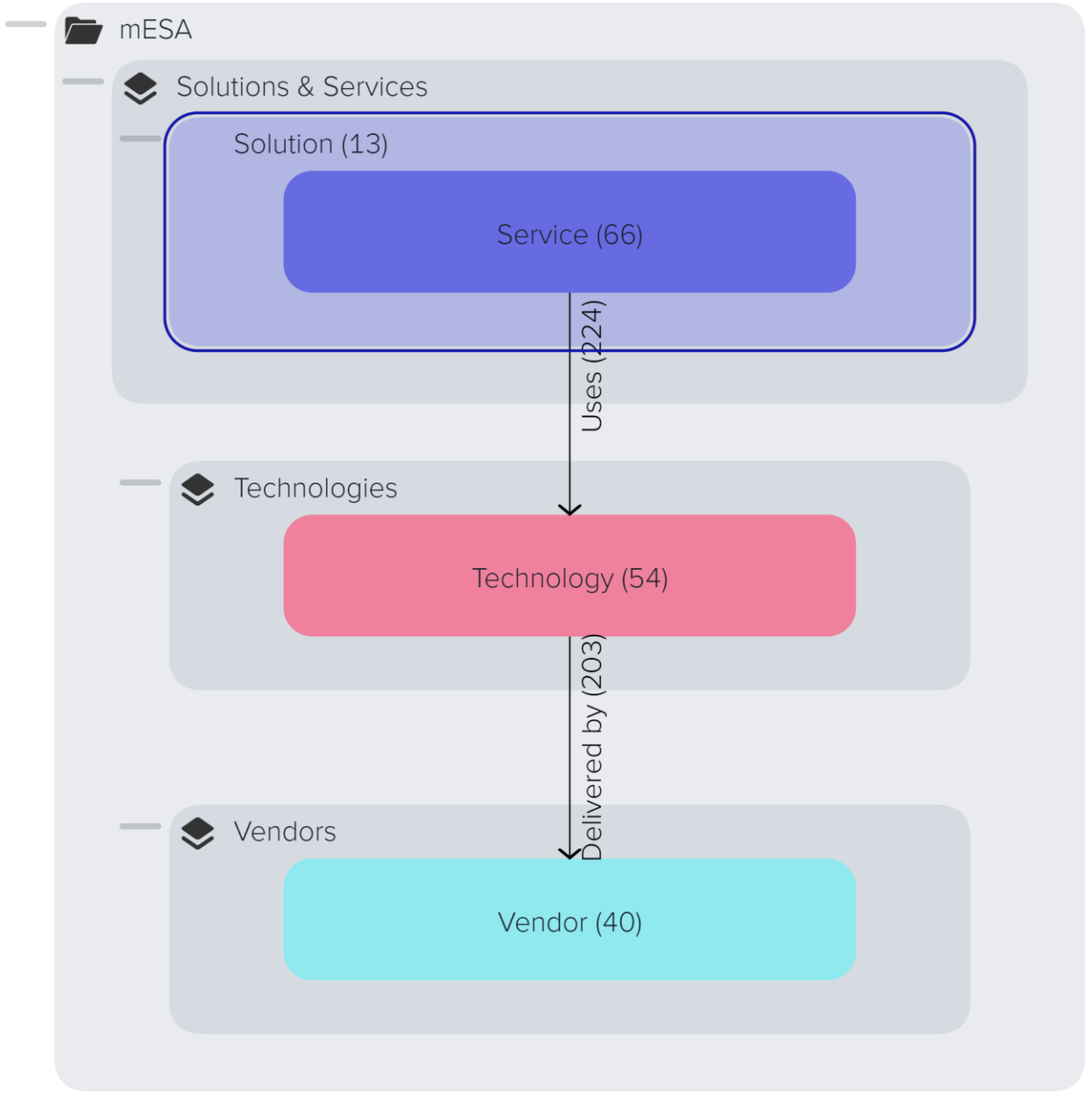
RECOMMENDATION
4.2 Incidents are evaluated and managed accordingly to established processes

RECOMMENDATION
4.3 Lessons learned are incorporated to improve Response and Recovery pr

Components

Component type

- Solution
- Service
- Technology
- Vendor
- Customer need

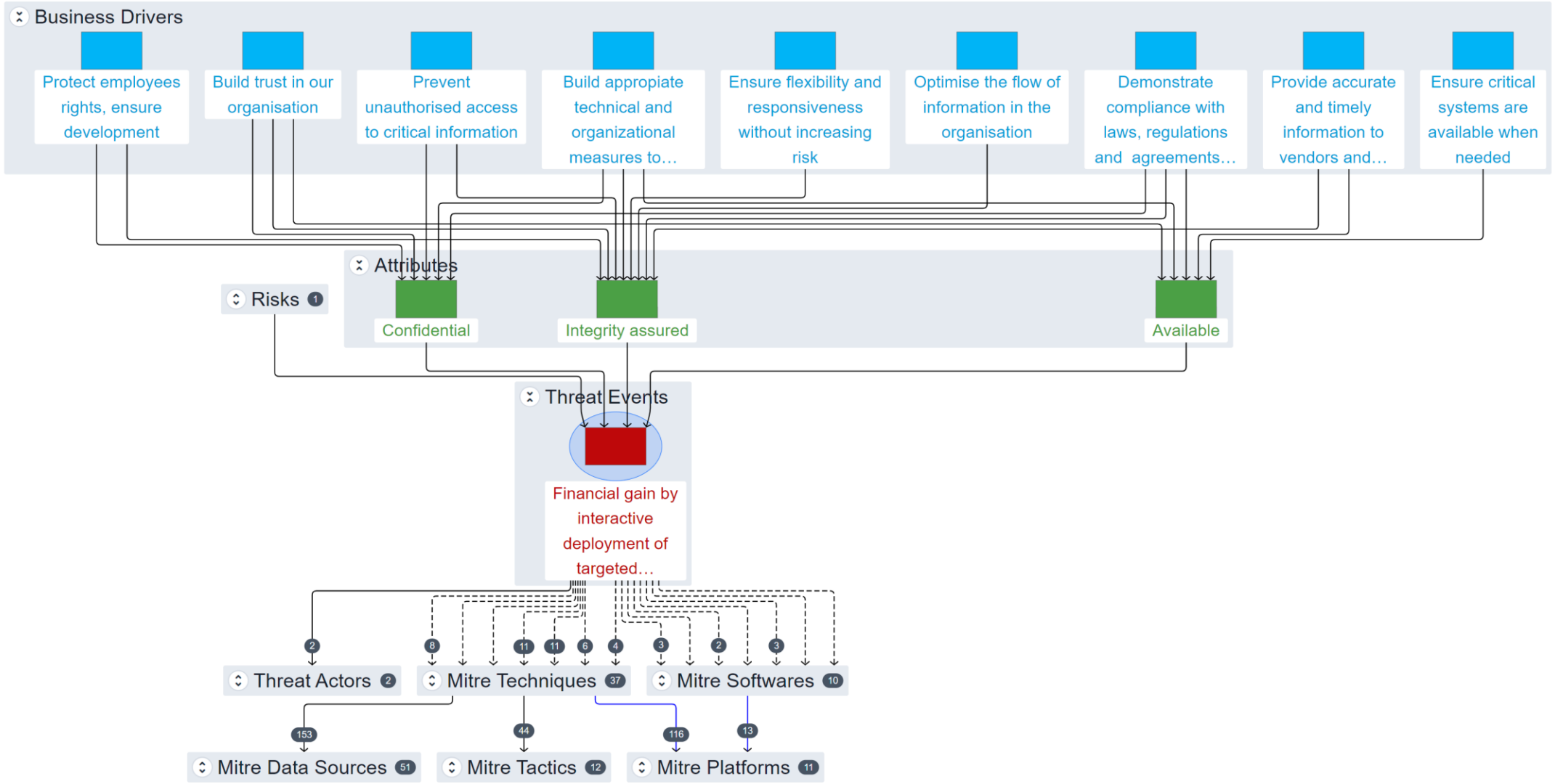

mESA
Solutions & Services
Solution (13)
Service (66)
Uses (224)
Technologies
Technology (54)
Delivered by (203)
Vendors
Vendor (40)

Final problem

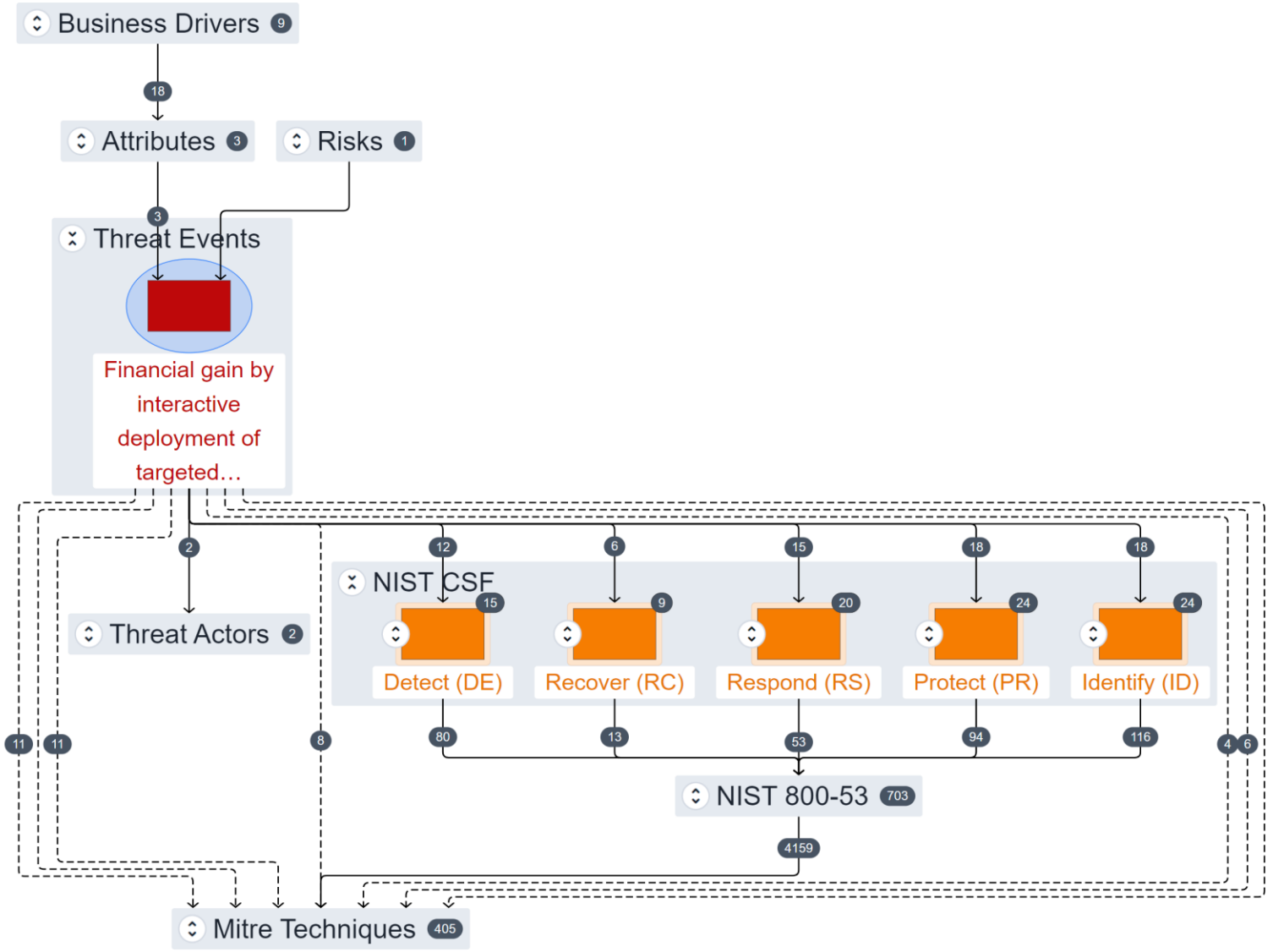
Optimizing your security investment

mnemonic

Putting it all together; using the traceability concept



Business
Risk
Control
Capability

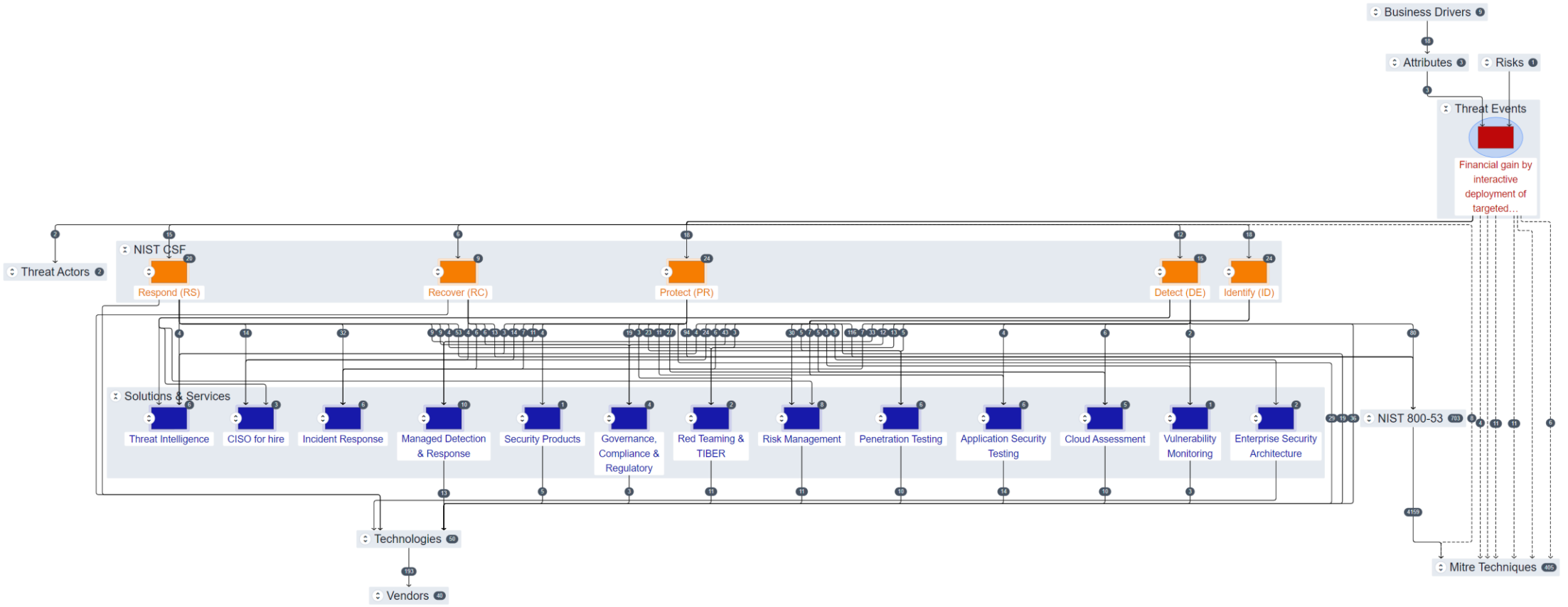


Business
Risk
Control
Capability

Ardoq

RANSOMWARE

Legend | Explore mode | Fullscreen



Business

Risk

Control

Capability

Dealing with the complexity – using *mnemonic Enterprise Security Architecture (mESA)* framework

- mESA is a unique way for companies to make informed business-driven decisions when making security investment.
- Using mESA will enable you to organize the complexity of cybersecurity, knowing that all your investment are pulling in the same direction.

Thank you!

- For more information visit https://www.mnemonic.io/solutions/enterprise-security-architecture/
- And see the mnemonic webinar Enterprise Security Architecture; optimise your security investments
- **alonso@mnemonic.no**