

SIA

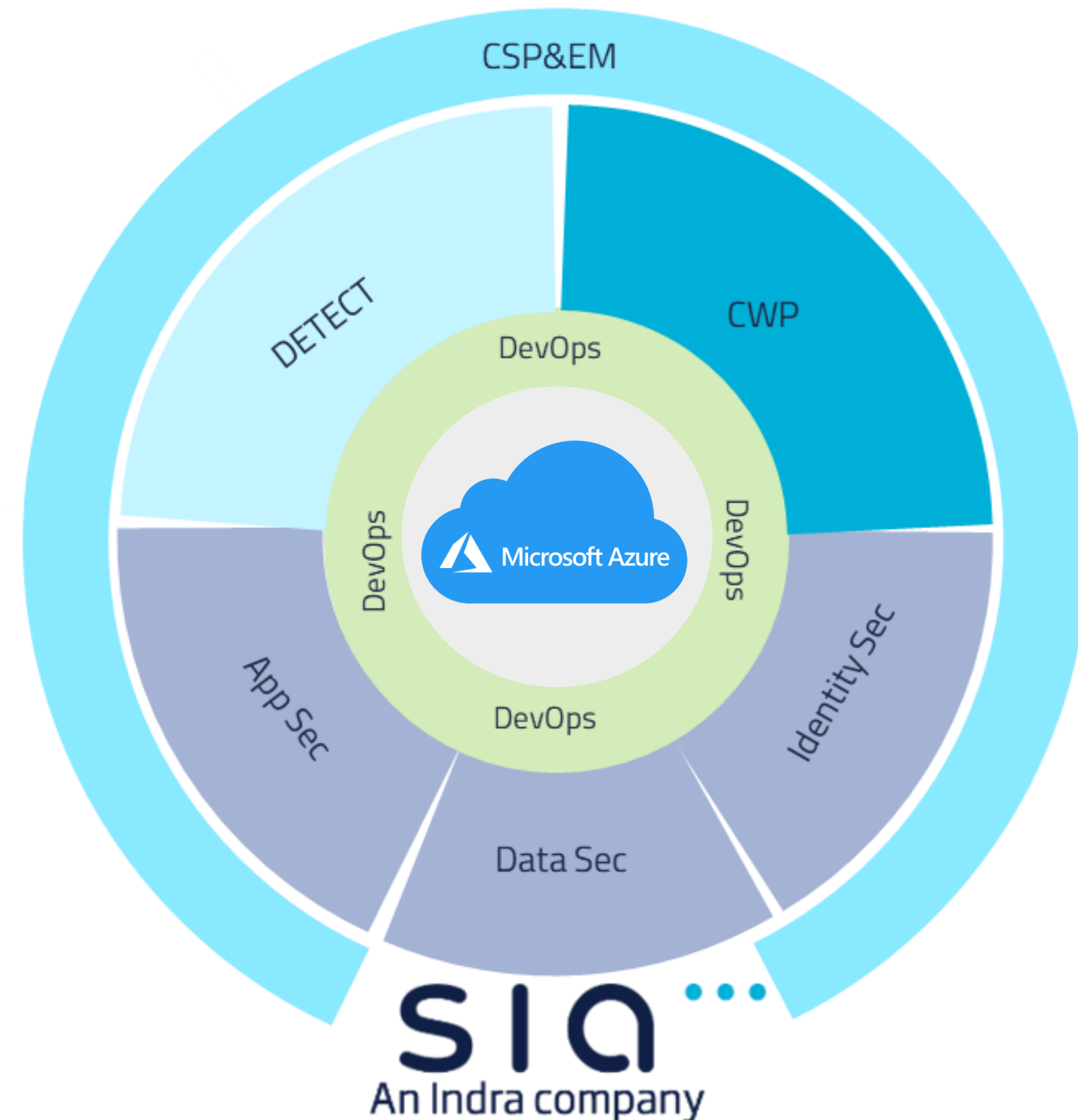
An Indra company

# SIA Cloud Security Posture Assessment



From a technological point of view, the Cloud Security Reference Architecture must implement CSP native Security controls integrated with specific solutions and services

### SIA Cloud Security Reference Architecture



... to implement Security over the “building”...

...and over the “content”... in an agile way

# SIA Cloud Security Posture Assessment (CSPA) – Microsoft Azure

SIA helps you to identify the Security Posture of your Azure environments and to design a full customized Security Action Plan, both technical and strategic, which will assure a high Security Posture Level against threats. Whether your organization is still in the Cloud migration process or there are already services in production, SIA CSPA will establish a Security program that allows you to start implementing robust Security mechanisms and maintain that high Security Posture Level.

During this assessment, SIA Cloud Security Architects will analyze your Cloud Adoption Strategy in order to align and prioritize all the recommendations that the Security Action Plan will include. We will take interviews with key stakeholders (Business, IT and Security) with the main aim of deeply understand the objectives, expectations and concerns of your journey to the Cloud. This Strategic Stage of the assessment will follow, as framework baseline, the Well-Architected Framework (WAF) of Microsoft Azure, adapted to you and from the SIA expertise perspective. Some of the key points that we address here are:

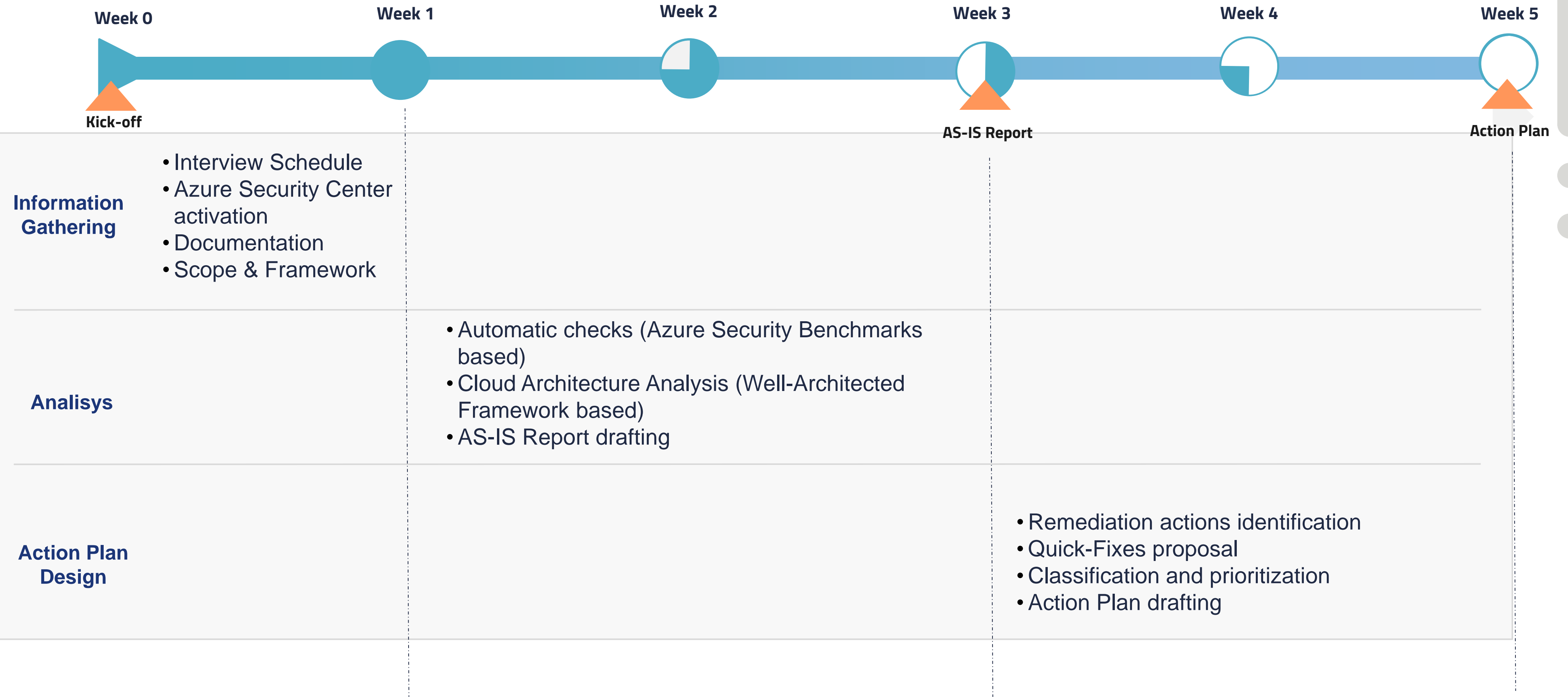
- Workloads & App/API protection
- DevSecOps
- Identity Sec
- Data Sec

Apart from that, SIA Cloud Security Specialists will work with your Cloud Admins on identifying technical misconfigurations present on the environments, which lead to security weaknesses that could be leveraged by attackers to compromise data and services hosted on your Azure environments. This analysis will be executed by activating and configuring CSPM module of Azure Security Center for you, that will allow us to identify any configuration that is not aligned with the Azure Security Benchmarks. The key point here is to be able to interpret and prioritize all technical remediations detected, in order to propose a customized mitigation plan that can be executed in an agile and automated way.

SIA CSPA includes:

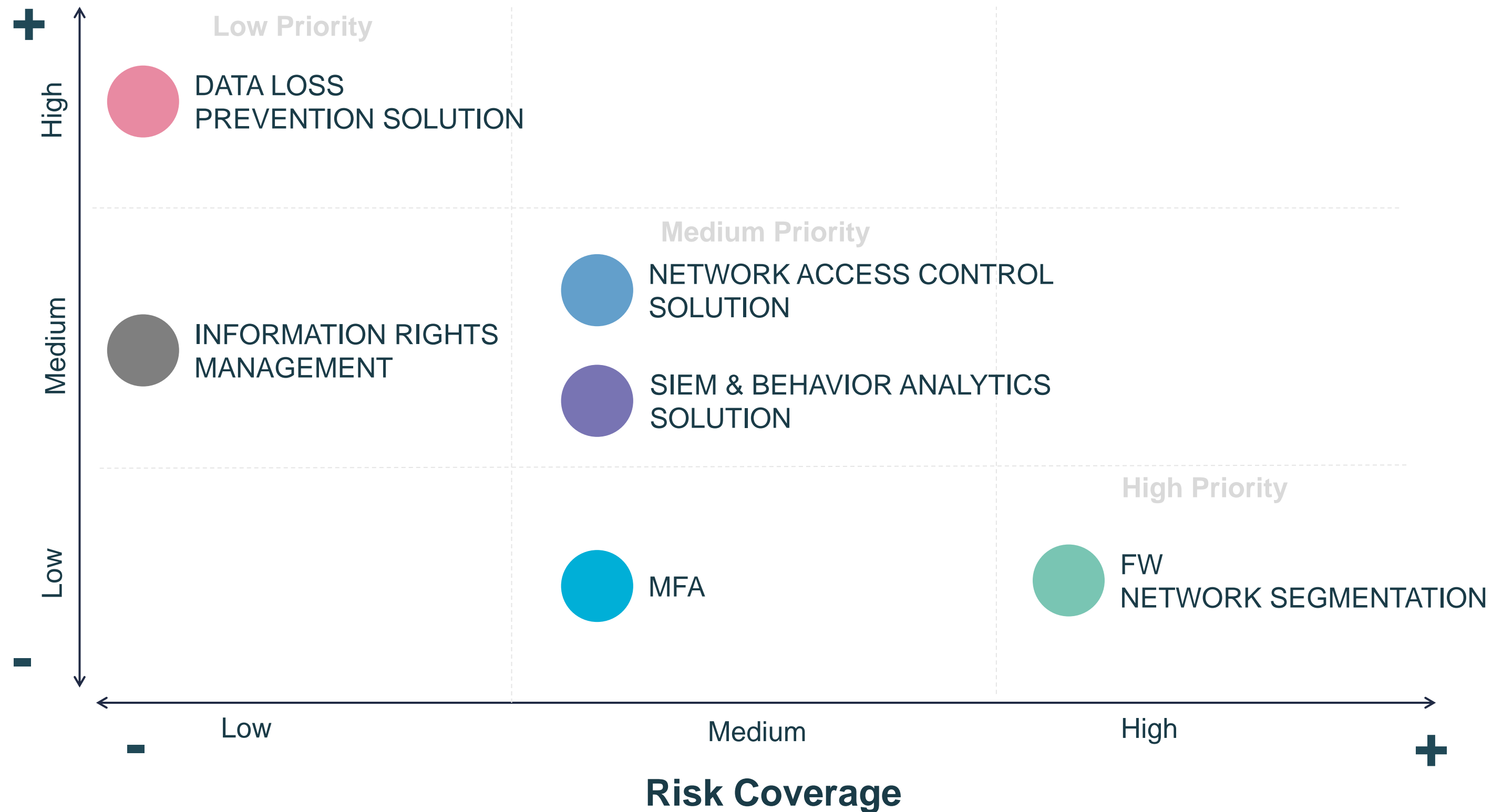
- Azure Security Center Activation
- Information Gathering (interviews, automated checks)
- Information Analysis
- AS-IS Report
- Action Plan report + Quick Fixes

# SIA CSPA Plan



# Strategic Solution Matrix - Example

## Implementation effort







**Risk coverage:** measures the level of threat covered given three possible levels:

- Low
- Medium
- High

**Effort required:** measures the effort required to implement the solution regarding difficulty of deployment and cost. Three possible values are given:


- Low
- Medium
- High


# Strategic Solution Detail - Example

Product Name	Usability impact	Maturity	Deployment difficulty	External Reference	Cost	Scoring
Microsoft Azure MFA	 Medium impact	 Advanced product	 High deployment difficulty	 High external references	-	18 / 25
Kind of solution	Strong 2FA/MFA					

Product Description	Technical Features	Covered Attack Vectors
<p>Azure MFA is the Multi-factor authentication tool included in Azure Active Directory Premium suite.</p> <p>Azure MFA conditional access is based on context of users, locations, devices, data and applications.</p>	<ul style="list-style-type: none"> <li>Adaptive access policies can assess a number of risk signals (user, group, device, network and location information) and apply a risk-mitigating action.</li> <li>Azure MFA Server, a software-delivered authentication solution, supports hardware OTP tokens and provides an LDAP interface allowing applications that already use LDAP to easily enable MFA</li> </ul>	<p>Covers 2 attack vectors from 1 categories (mobile hardening):</p> <ul style="list-style-type: none"> <li>Impersonation of the 2FA tool.</li> <li>Interception of the second authentication factor.</li> </ul>

## Conclusions

 It is very user friendly

 Azure conditional access does not provide sufficient granularity to enforce specific authentication methods used to mitigate risk.  
Initial deployment is complicated.

**Azure MFA is a good product for organizations that have or want Azure AD and not require granularity on authentication methods**



Home > **Security Center | Overview**  
Showing subscription 'CESECDEP - Internal'

Search (Ctrl+/) << Subscriptions >> What's new

Overview

- Getting started
- Pricing & settings
- Community
- Workflow automation

**POLICY & COMPLIANCE**

- Coverage
- Secure Score
- Security policy
- Regulatory compliance

**RESOURCE SECURITY HYGIENE**

- Recommendations
- Compute & apps
- Networking
- IoT Hubs & resources
- Data & storage
- Identity & access
- Security solutions

**ADVANCED CLOUD DEFENSE**

- Adaptive application controls
- Just in time VM access
- Adaptive network hardening
- File Integrity Monitoring

---

**Policy & compliance**

Overall Secure Score

**45%** (~27 of 60 points)

[Review your Secure Score >](#)

Regulatory compliance

- ISO 27001 4 of 21 passed controls
- Azure CIS 1.1.0 (New) 38 of 62 passed controls
- Azure CIS 1.1.0 15 of 24 passed controls

Subscription coverage

**1** TOTAL

- Fully covered: 1
- Partially covered: 0
- Not covered: 0

2.4K Covered resources

---

**Resource security hygiene**

Recommendations

**131** TOTAL

- High Severity: 18
- Medium Severity: 14
- Low Severity: 99

1.6K Unhealthy resources

Resource health by severity

- 1K Compute & apps resources
- 130 Data & storage resources
- 14 Identity & access resources
- 1 IoT Hubs & resources

Networking

- 250 Unhealthy resources
- 426 Monitored resources

There are 5 high severity recommendations

[Secure your network resources](#)

---

**Threat protection**

Security alerts by severity

**123** TOTAL

- High Severity: 24
- Medium Severity: 84
- Low Severity: 15

Security alerts over time

High severity: 24  
Medium severity: 84  
Low severity: 15

Home > **Security Center | Overview**  
Showing subscription 'CESECDEP - Internal'

Search (Ctrl+/) Subscriptions What's new

Overview

- Getting started
- Pricing & settings
- Community
- Workflow automation

**POLICY & COMPLIANCE**

- Coverage
- Secure Score
- Security policy
- Regulatory compliance

**RESOURCE SECURITY HYGIENE**

- Recommendations
- Compute & apps
- Networking
- IoT Hubs & resources
- Data & storage
- Identity & access
- Security solutions

**ADVANCED CLOUD DEFENSE**

- Adaptive application controls
- Just in time VM access
- Adaptive network hardening
- File Integrity Monitoring

---

**Policy & compliance**

Overall Secure Score

**45%** (~27 of 60 points)

[Review your Secure Score >](#)

Regulatory compliance

- ISO 27001 4 of 21 passed controls
- Azure CIS 1.1.0 (New) 38 of 62 passed controls
- Azure CIS 1.1.0 15 of 24 passed controls

Subscription coverage

**1** TOTAL

- Fully covered: 1
- Partially covered: 0
- Not covered: 0

2.4K Covered resources

---

**Resource security hygiene**

Recommendations

**131** TOTAL

- High Severity: 18
- Medium Severity: 14
- Low Severity: 99

1.6K Unhealthy resources

Resource health by severity

- 1K Compute & apps resources
- 130 Data & storage resources
- 14 Identity & access resources
- 1 IoT Hubs & resources

Networking

- 250 Unhealthy resources
- 426 Monitored resources

There are 5 high severity recommendations

[Secure your network resources](#)

---

**Threat protection**

Security alerts by severity

**123** TOTAL

- High Severity: 24
- Medium Severity: 84
- Low Severity: 15

Security alerts over time

High severity: 24  
Medium severity: 84  
Low severity: 15

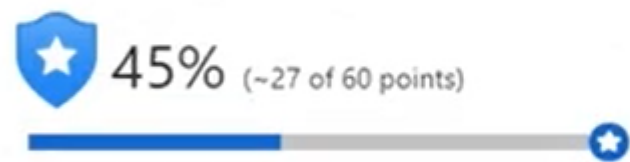


## Recommendations

Download CSV report

Security recommendations for identity and access are now available on free subscriptions. This will impact your secure score. [Learn more](#) →

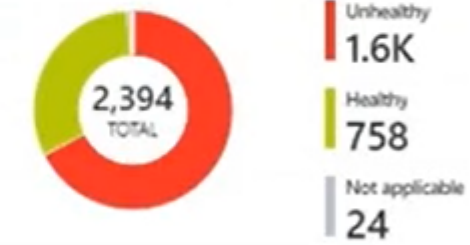
### Secure Score



### Recommendations status



### Resource health



Is the new Secure Score preview experience clear to you?  Yes  No

Each security control below represents a security risk you should mitigate. Address the recommendations in each control, focusing on the controls worth the most points. To get the max score, fix all recommendations for all resources in a control. [Learn more](#) >

Search recommendations

Controls	Potential score increase
> Remediate vulnerabilities	+ 10% (6 points)
> Secure management ports	+ 10% (6 points)
> Apply system updates	+ 6% (4 points)
> Enable encryption at rest	+ 6% (4 points)
> Restrict unauthorized network access	+ 5% (3 points)
> Remediate security configurations	+ 5% (3 points)
> Protect applications against DDoS attacks	+ 3% (2 points)
> Apply adaptive application control	+ 3% (2 points)

Home > Security Center | Overview >

## Recommendations

Download CSV report

Security recommendations for identity and access are now available on free subscriptions. This will impact your secure score. [Learn more](#) →

Not applicable  
24

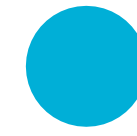
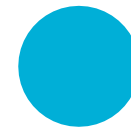
Is the new Secure Score preview experience clear to you?  Yes  No

Each security control below represents a security risk you should mitigate. Address the recommendations in each control, focusing on the controls worth the most points. To get the max score, fix all recommendations for all resources in a control. [Learn more](#) >

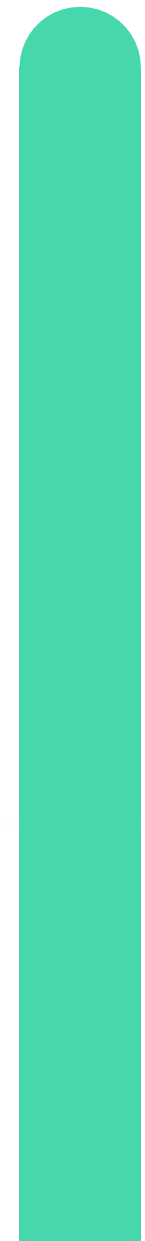
Search recommendations

Controls	Potential score increase
<input checked="" type="checkbox"/> Remediate vulnerabilities	+ 10% (6 points)
Advanced data security should be enabled on your SQL servers <span>✔ Completed</span>	
Vulnerability assessment should be enabled on your SQL servers <a href="#">Quick Fix</a>	
Vulnerabilities on your SQL databases should be remediated (Preview) /* Under Maintenance */	
Vulnerability assessment solution should be installed on your virtual machines	
Vulnerabilities should be remediated by a Vulnerability Assessment solution <span>✔ Completed</span>	
Enable the built-in vulnerability assessment solution on virtual machines (powered by Qualys) <a href="#">Quick Fix</a>	
Vulnerabilities in your virtual machines should be remediated (powered by Qualys)	
Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys)	

BEYOND CYBERSECURITY



Thank you



SIA...

An Indra company