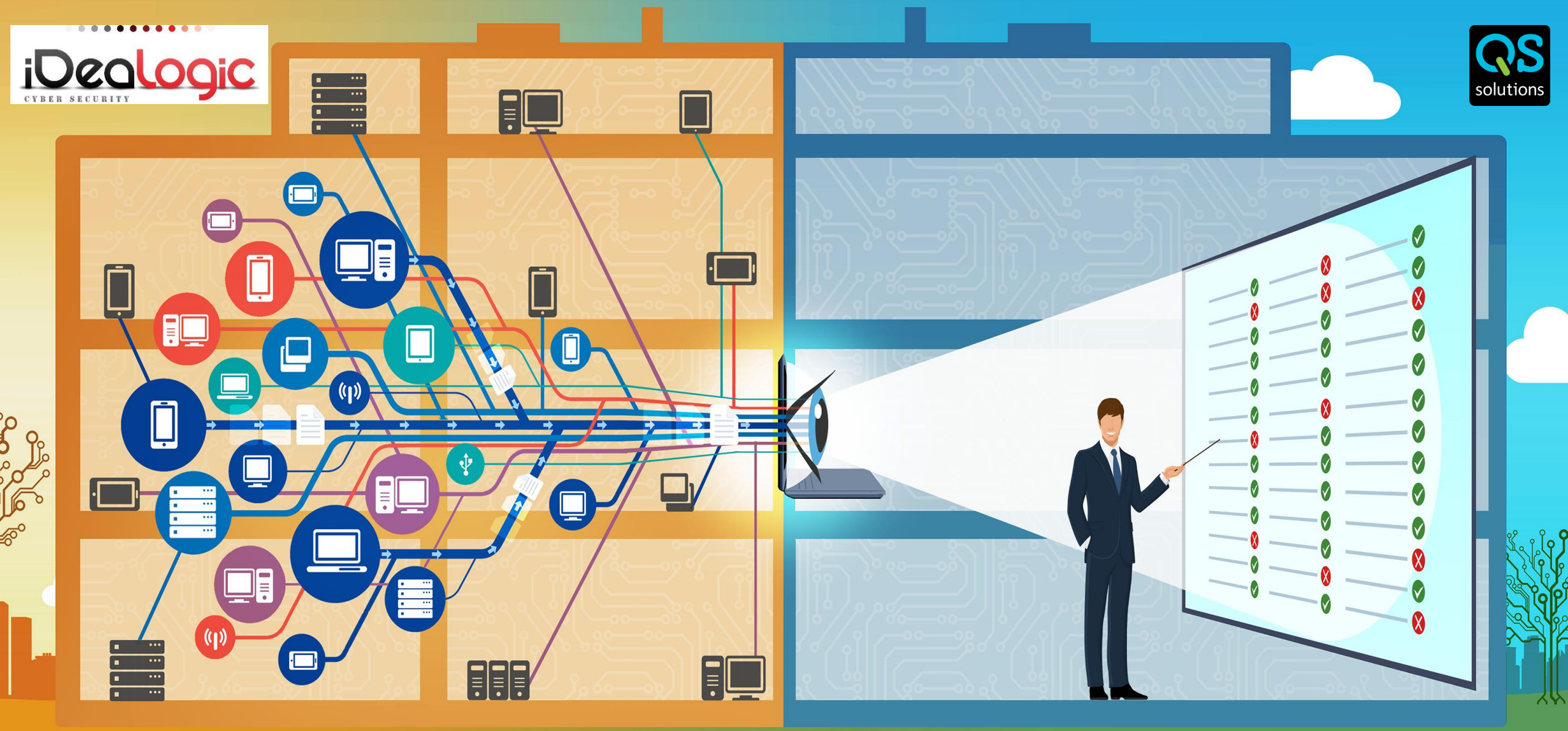
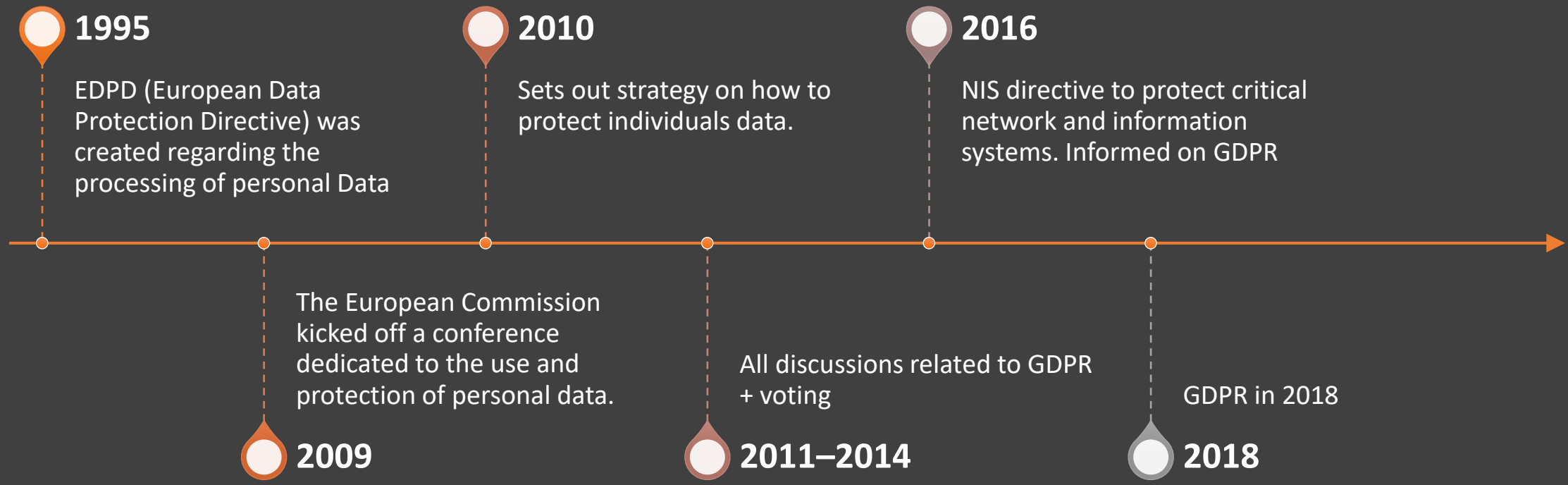


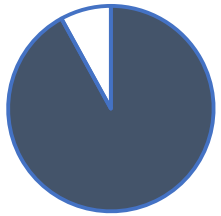

# Technical Requirements on GDRP

# Agenda

- Drivers – A bit of history
- Scope – What to cover?
- Technical Requirements – What to do + What to have
- Planning – What we offer at iDealogic

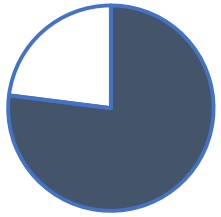
# History lessons





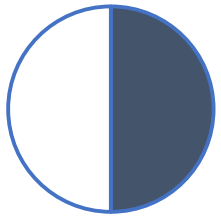
# 92%

of US organizations consider GDPR compliance their top data protection priority[1]



# 77%

plan to spend $1M USD or more on GDPR compliance[1]



# 50%

of EU organizations indicate they have documented the sensitive data they house[2]

"By the end of 2018, more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements."

Gartner

Organizations Are Unprepared for the 2018 European Data Protection Regulation, Gartner Newsroom; May 3, 2017 http://www.gartner.com/newsroom

1. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/gdpr-readiness.html
2. https://securityintelligence.com/prepared-for-the-general-data-protection-regulation-gdpr-top-10-findings-from-hurwitz-associates-survey/

# What are the key changes to address the GDPR?

## Personal privacy

Individuals have the right to:

- Access their personal data
- Correct errors in their personal data
- Erase their personal data
- Object to processing of their personal data
- Export personal data

## Controls and notifications

Organizations will need to:

- Protect personal data using appropriate security
- Notify authorities of personal data breaches
- Obtain appropriate consents for processing data
- Keep records detailing data processing

## Transparent policies

Organizations must:

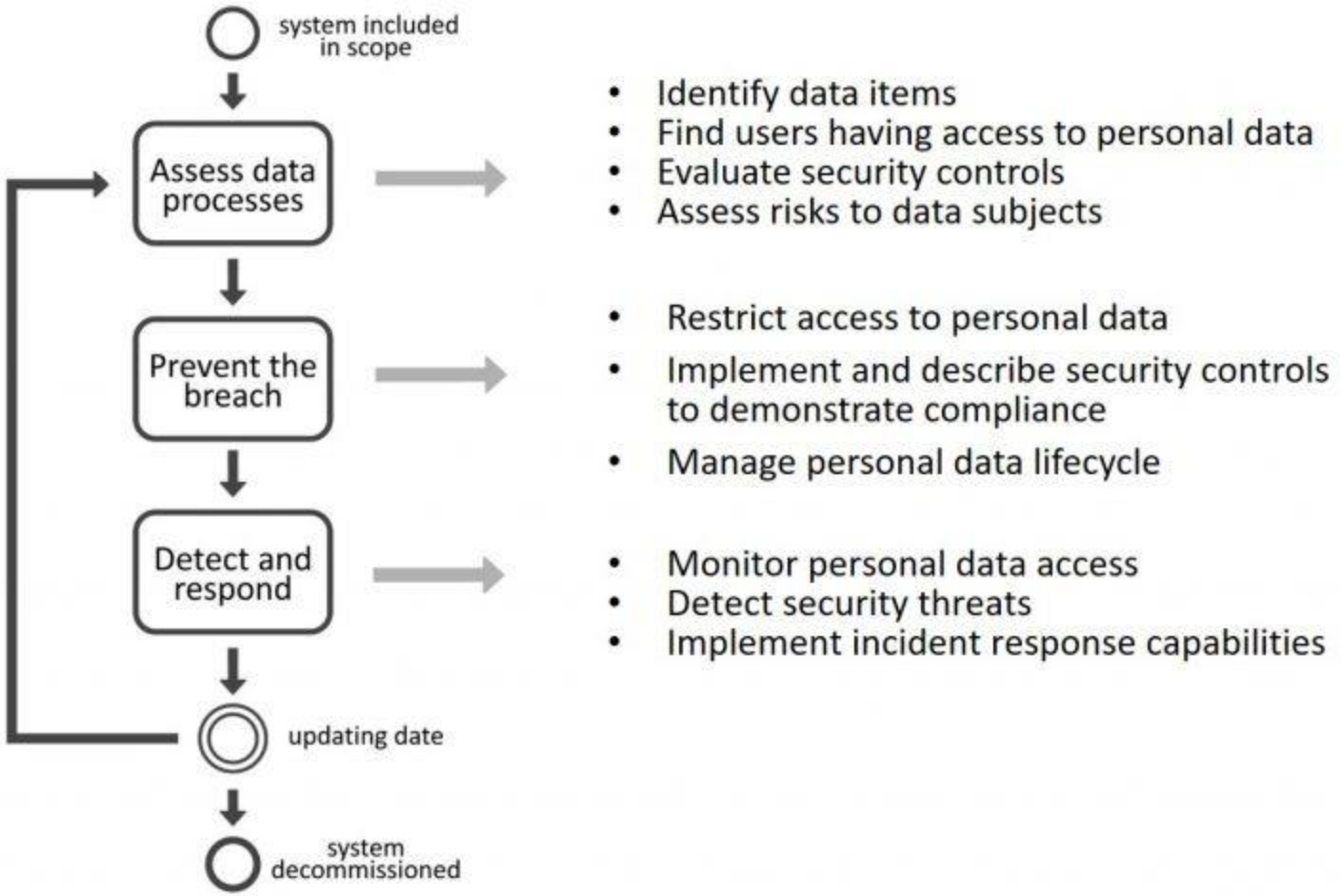
- Provide clear notice of data collection
- Outline processing purposes and use cases
- Define data retention and deletion policies

## IT and training

Organizations will need to:

- Train privacy personnel & employees
- Audit and update data policies
- Employ a Data Protection Officer (if required)
- Create & manage compliant vendor contracts

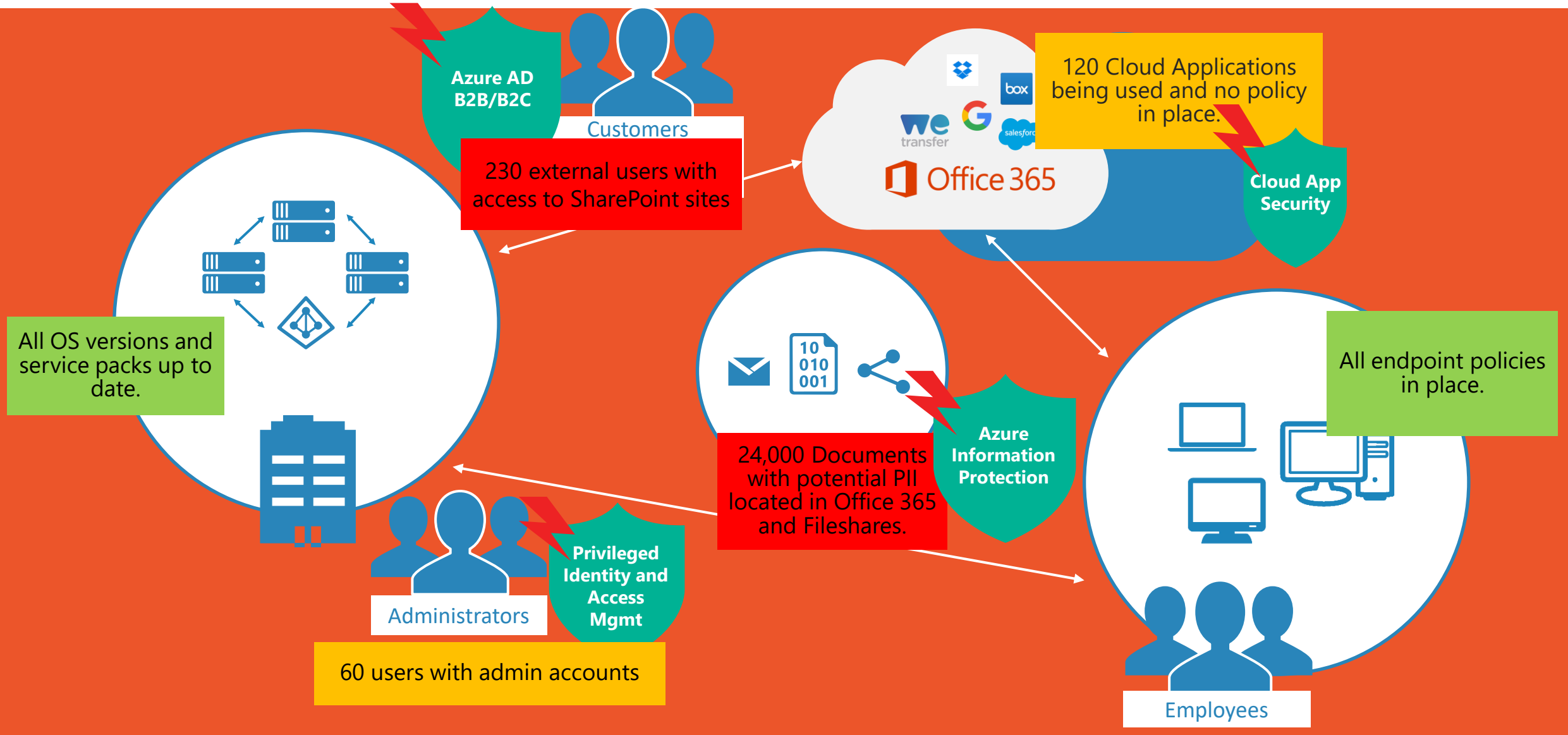
# GDPR Security Tasks



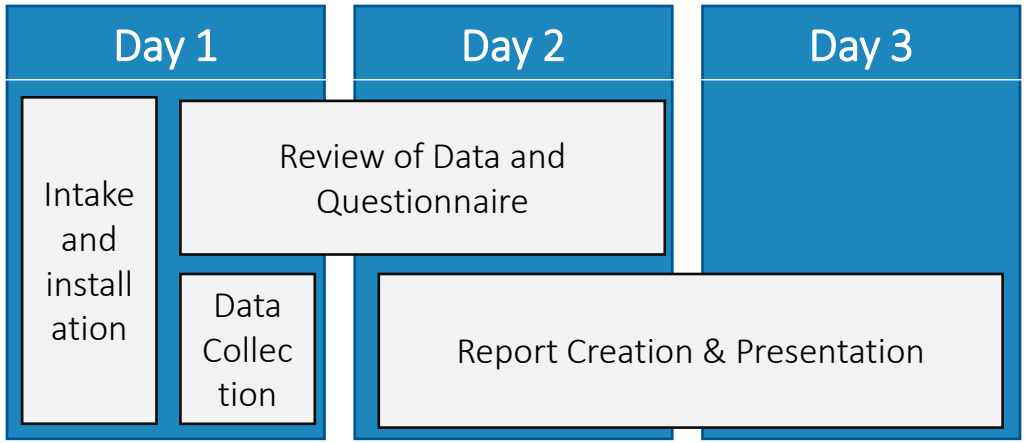

*Source: https://erpscan.com/press-center/blog/gdpr-explained-security-requirements/*

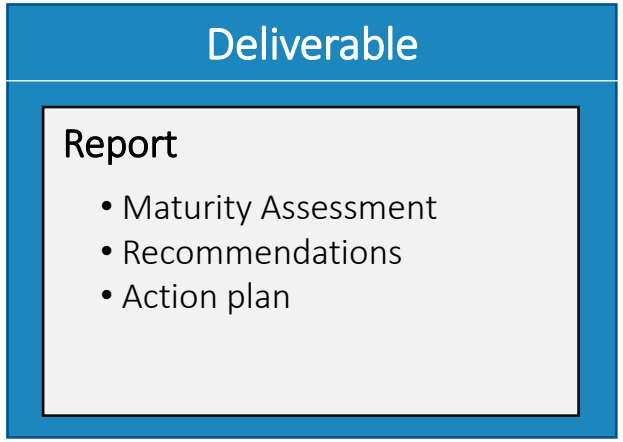
# Know yourself

# In detail


Azure AD B2B/B2C
Customers
230 external users with access to SharePoint sites
120 Cloud Applications being used and no policy in place.
Cloud App Security
Office 365
All OS versions and service packs up to date.
24,000 Documents with potential PII located in Office 365 and Fileshares.
Azure Information Protection
All endpoint policies in place.
Privileged Identity and Access Mgmt
Administrators
60 users with admin accounts
Employees

# Typical Engagement Timeline

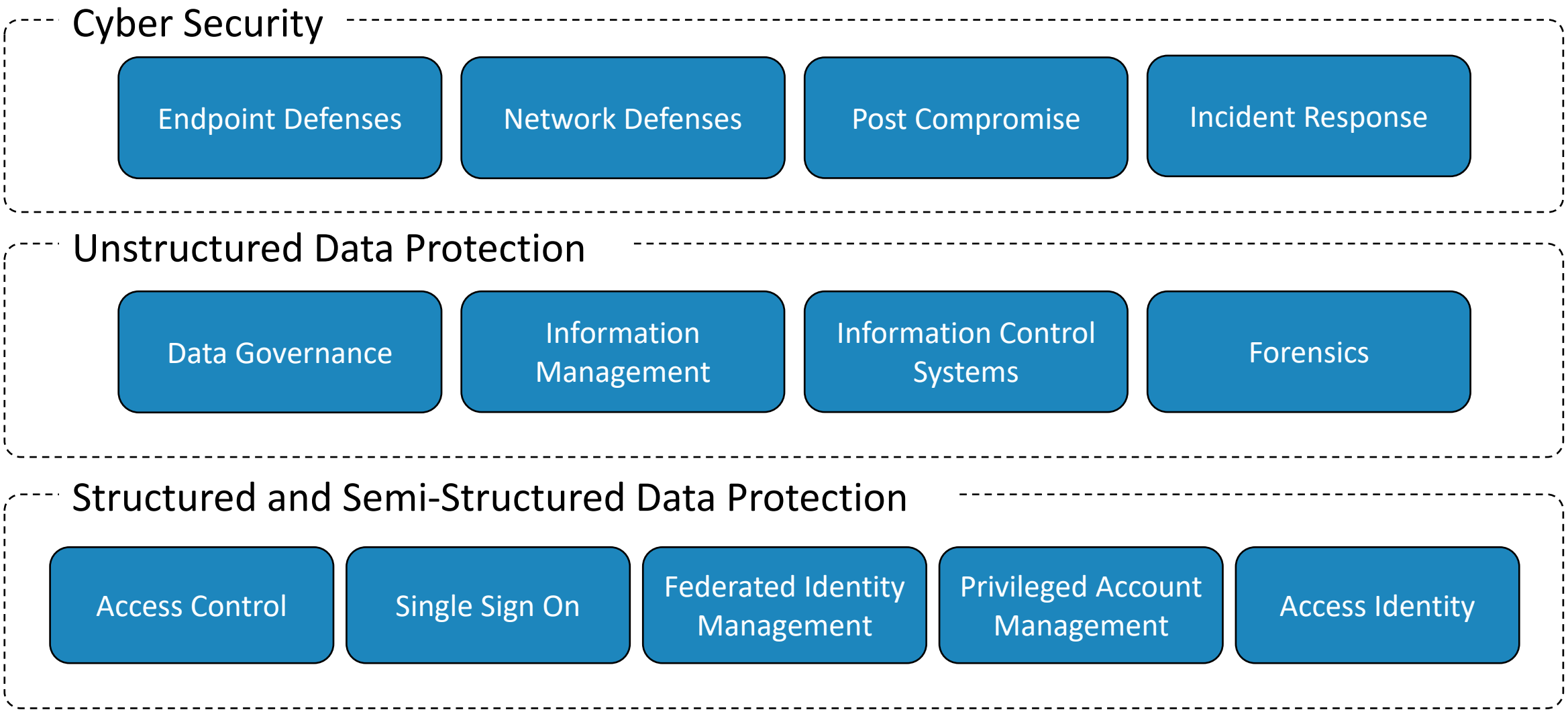



- Data collection involves running the CSAT. A three day engagement targets about 200 to 500 endpoints.
- Questionnaire answers are collected in the CSAT generally provided by the IT department.

- Analysis of data and questionnaire is focussed on identifying key indicators that indicate the maturity of the enterprise against each element of our assessment framework.
- Reports utilize data that is collected and provide evidence-based conclusions and recommendations.
- Reports map out a prioritized action plan to improve security.

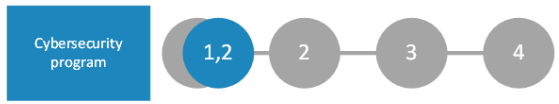
# Security Assessment Framework



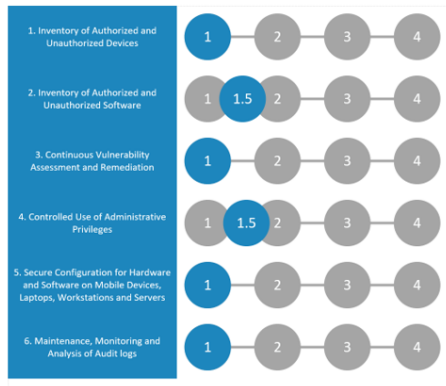
# Executive summary report

## Maturity status

After reviewing the findings for each of the Security Control Domains described in detail in the Report, the overall assessment of <Customer>'s cybersecurity program has a Maturity Rating of: **Basic (1)**.




What is more important than the single, all-up Cybersecurity Maturity Rating, are the specific maturity ratings associated with each control domain. The 6 Basic CIS controls are considered essential and represent a "Cyber Hygiene" starting level.




[Recommendation]
No clear governance and policies are available, think about Cyber security Policies, data governance policies, data retention policies and make sure they align with GDPR and ISO 27001 standards.

[Recommendation]
IT security is a top-level strategic issue requiring executive leadership participation as stakeholders in the process.

## Highest risk findings

The findings below require <Customer> to take immediate action.

| Finding | Action | Software products |
|---|---|---|
| • Contractors that are no longer working for <Company> still have access to classified documents | • Deploy MFA<br>• Deploy AIP | • In EMS E3 bundle, licenses already available |
| • 30 users with very high Administrative rights | • Deploy PIM | • Upgrade to EMS E5 |
| • 12 Windows XP machines were detected | • Upgrade the OS | • Windows 10 |

[Immediate action required]
Not taking action will keep <Customer> exposed to serious security incidents. Not addressing these findings could lead to negative consequence in case of inquiries after a breach.

# Detailed Report

## 5. Technical findings

### 5.1. Endpoints

#### 5.1.1. Applications

In total there are 138 applications installed over all endpoints. While a lot of these applications do not represent a risk, there are a few applications that could represent a risk to the endpoints. Point 4.2.4. pointed out that all users are local admin on their laptops. In the application list there are a few applications that were not installed by IT and can, therefore, be an issue. First there is Teamviewer, which is installed on almost all endpoints.

| | | | | | |
|---|---|---|---|---|---|
| TeamViewer 12 | 12.0.82216 | TeamViewer | 184 | Bad |

Dropbox is installed on four laptops. When the user was asked why this software has been installed they replied with the following “I use it to send documents to people outside the organization”

| | | | | |
|---|---|---|---|---|
| Dropbox | 39.4.94 | Dropbox Inc. | 4 | Bad |

Teamviewer and Dropbox represent the use of shadow IT in the company infrastructure. With the use of AppLocker, you can define applications which may be installed in the company infrastructure. AppLocker can be setup with a GPO.

#### 5.1.2. Browser URLs

This part of the scan has not been carried out due to privacy considerations.

#### 5.1.3. Firewall

Some of the firewalls are disabled on endpoints.

| Endpoint | # IN | # OUT | IP | All | Domain | Public | Private |
|---|---|---|---|---|---|---|---|
| Win2012R2_Clean.WORKGROUP | 107 | 60 | 192.168.150.21 | E B **N** | **E** B N | E B N | E B N |
| LT-ux305U-8038.qss.nl | 305 | 285 | 192.168.150.20 | E B **N** | **E** B **N** | **E** B **N** | **E** B **N** |
| Win7_Pro_X64_EN.WORKGROUP | 174 | 131 | 192.168.150.25 | E B **N** | **E** B **N** | E B **N** | E B **N** |

Windows firewall provides protection from network attacks on the endpoints that pass through your perimeter network or originate inside your organization, such as Trojan horse attacks, worms, or any other type of malicious program spread through unsolicited incoming traffic. Create GPO to enable

# Detailed Report

## Proposed Action items

The summary of Findings and Recommendations, associated with Actions and supportive software products, is in the table below.

| Priority | CIS control | Finding | Recommendation | Action | Software products |
|---|---|---|---|---|---|
| HIGH | 1 | • No automated asset discovery tools are used to build a preliminary asset inventory of systems connected to the organization's networks. | • Discovery of unauthorized network devices should be performed, for instance in the router/switching layer | • Implement the process. Start a project with own IT-resources.<br>• Acquire software to support the process | • SCOM, WSUS |
| HIGH | 4 | • Lots of Domain, Schema and Enterprise admins, no Fine grained Role Based Access Control available. | • Cleanup Domain, Enterprise and Schema admin groups<br>• | • Implement the process<br>• Acquire software to support the process | • Privileged Identity Management |
| Medium | 4 | • There are limited administrative privileges and no standard processes or controls to manage them. | • Implement Advanced Threat Analytics to detect stolen admin credentials/tickets and get notifications on admin group membership changes. | • Implement the process<br>• Acquire software to support the process | • Privileged Identity Management |
| Medium | 3 | • CSAT discovered missing updates on Servers, not all servers are structurally patched. No detection and alerting of missing updates is available at this moment | • Implement a vulnerability scanning system to help detect against unpatched and misconfigured systems.<br>• Policies should include the process to ensure all devices are updated to the latest patch level and who is responsible for patching | • Implement the process<br>• Scan regularly to check status and show progress<br>• Acquire software to support the process | • CSAT subscription |
| Medium | 2 | • Old versions of software(e.g. old Java versions, pdfcreators, VLC Mediaplayers) were found on endpoints. | • Place all older machines under software inventory control or replace them with Windows 10 images. | • Continue upgrading all older Operating Systems | • Windows 10 |
| HIGH | 6 | • Lots of failed login attempts on Azure/Office 365 were discovered during the scan | • Implement central logging and alerting, for example with Azure Log Analytics, OMS or SCOM. | • Implement the process. Start a project with own IT-resources.<br>• Deploy software to | • ATA<br>• ATP |

## Recommended Software

The SAM Cybersecurity Assessment revealed that <Customer> has not deployed all of the available security software licenses.

Additional license products are advised to mitigate security risks.

The table below shows the overview of recommended software products to deploy or acquire.

| Software product | Action |
|---|---|
| • Azure Log Analytics, OMS or SCOM | • Not available, acquire |
| • EMS E3 | • 3 out of 625 EMS E3 licenses are in use, deploy all licenses |
| • Intune | • Available in EMS E3, deploy |
| • Multi Factor Authentication | • Available in EMS E3, deploy |
| • Azure Information Protection | • Available in EMS E3, deploy |
| • Advanced Threat Analytics | • Available in EMS E3, deploy |
| • Privileged Identity Management | • Upgrade to EMS E5, acquire 44 licenses |
| • QS PortalTalk | • Not available, acquire |
| • QS CSAT Subscription | • Not available, acquire |

# Conclusions

iDealogic
CYBER SECURITY

- New regulations big impact world wide
- Start planning properly
- Become Cyber Resilient Security