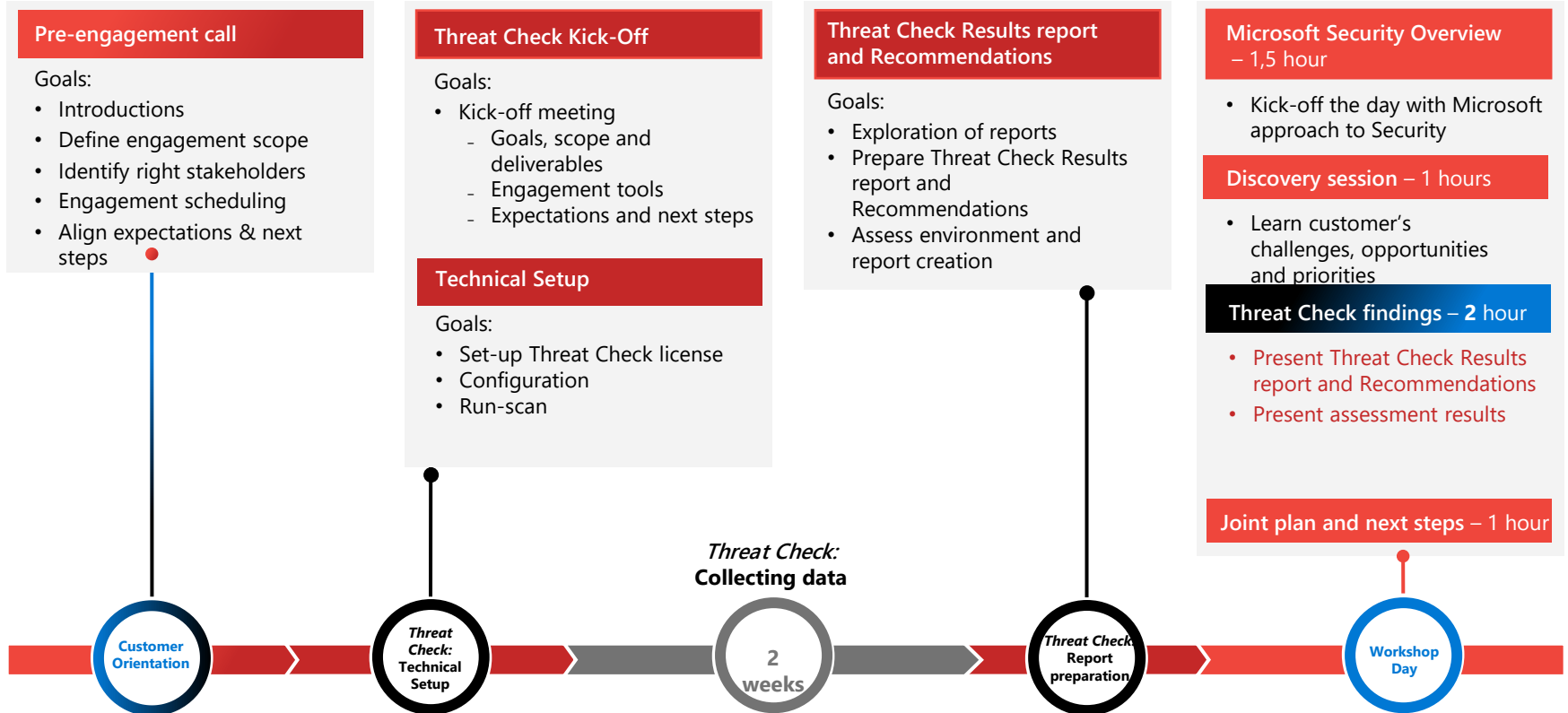


delaware

Digital workplace
Security
Assessment and
Workshop



Security Workshop engagement timeline



FOR WHOM?

- Organizations with an Office 365 or Microsoft 365 license that want to improve their security.
- Organizations using SharePoint online, Exchange online, Microsoft 365, ...

WHAT?

- Security presentation to make you aware about the different security features
- Security analysis of your current environment. (Assessment and threat check)
- Advising and designing a roadmap for short-, medium- and long-term security projects.

BENEFITS

- Get an security overview of your environment and detect possibilities to improve security.
- Increase the security of your organization.
- Having access to a partner who is eager to assist you.

We do an analysis and offer you advice

- **Pre-Engagement**
 - Define scope and align expectations to guide workshop and deliverables.
 - Threat Check and Assessment
- **Discover threats in your Microsoft 365 cloud environment by enabling our analyzing tools**
 - Review the environment based on Microsoft best practices
 - Determine risks and the maturity of your current Microsoft 365 security environment.
 - Identify unused security features included in the current license bundle.
- **Workshop**
 - Raise awareness of available Microsoft 365 security features.
 - Determine your security needs
 - Present the threat check and assessment report
 - Demo the preferred features
 - Discuss a possible roadmap for quick wins and short-, medium- and long-term

Security Workshop

Initial Engagement



Security Workshop



Microsoft
Security
Overview



Discovery
Session



Threat Check



Customer
Immersion
Experience



Recommendations
and Next Steps

Security overview presentation

- > Presentation
- > Demo video on how security features work
- > Attack video's for awareness

The screenshot shows a presentation slide with a table of contents on the left and a list of security features on the right. The table of contents lists slides 11 through 16, with slide 13 highlighted. The right side of the slide features a vertical list of security services, each with an icon and a description. The services are: Information Protection, Identity & Access Management, Behaviour Based Threat Analytics, Azure Infrastructure Protection, and Device & App Management. The slide also includes a footer with 'Slide 13 of 122' and 'Dutch (belgium)'.

| | |
|----|--|
| 11 | |
| 12 | |
| 13 | |
| 14 | |
| 15 | |
| 16 | |

- > **Information protection:** Locate and classify information anywhere it lives
- > **Identity & access management:** Protect against credential compromises.
- > **Threat protection:** Help stop damaging attacks with integrated and automated security.
- > **Azure Infrastructure protection:** Protect azure components
- > **Mobile Device Management:** Manage and protect endpoints

Slide 13 of 122 Dutch (belgium)



Security Workshop

Initial Engagement



Security Workshop



Microsoft
Security
Overview



Discovery
Session



Threat Check



Customer
Immersion
Experience



Recommendations
and Next Steps

Discovery session

Understanding your security state of the world

- What is your current security landscape?
- What are your greatest security concerns?
- What are your top three desired improvement areas?



Security Workshop brings modular flexibility

Initial Engagement



Security Workshop



Microsoft
Security
Overview



Discovery
Session



Threat Check



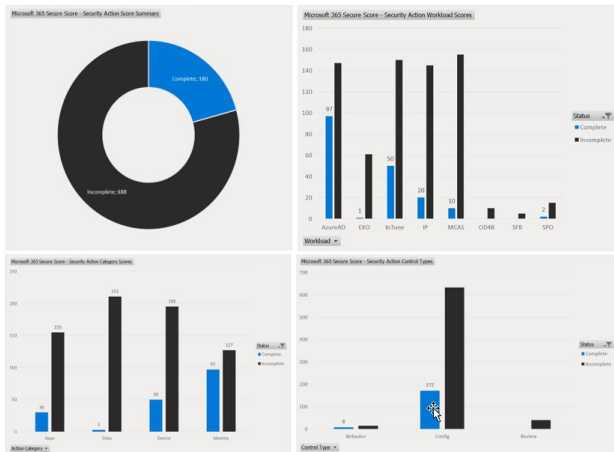
Customer
Immersion
Experience



Recommendations
and Next Steps

Assessment report

2 Current Score



Navigation

Search document

Headings Pages Results

- 1 Intro
 - 1.1 Question yourself
 - 1.2 Challenges
- 2 Current Score
- 3 Approach
- 4 General Security Questionnaire
- 5 Current Available licenses
- 6 Configuration check
 - 6.1 Account breach
 - 6.1.1 Turn on mailbox auditing for all users
 - 6.1.1.1 What does it do
 - 6.1.1.2 Current state
 - 6.1.1.3 Why is it important
 - 6.1.2 Require MFA for Azure AD privileged roles
 - 6.1.3 Register all users for multi-factor authen...
 - 6.1.4 Require MFA for all users
 - 6.1.5 Delete/block accounts not used in last 30...
 - 6.1.6 Turn on sign-in risk policy
 - 6.1.7 Turn on user risk policy
 - 6.1.8 Enable policy to block legacy authenticat...
 - 6.1.9 Do not expire passwords
 - 6.1.10 Consume audit data weekly
 - 6.1.11 Designate less than 5 global admins

6.1 Account breach

6.1.1 Turn on mailbox auditing for all users

6.1.1.1 What does it do

This will enable all mailbox auditing for all users.

6.1.1.2 Current state

Mailbox auditing is not implemented.

6.1.1.3 Why is it important

It is important to enable mailbox auditing to be able to check what user did with their mailboxes. You can keep track of who logs on to the mailboxes of your organization and to track access to mailboxes by users other than the mailbox owner. Audit logs also keep track of host names and IP addresses. If a user is deleting, forwarding moving, ... mails from a mailbox that isn't theirs they can have malicious intents without anyone knowing so it is very important to keep an eye on who does what in mailboxes that aren't their own. It's not only to monitor malicious users but also monitor human errors. If a mail with sensitive data is deleted or send to a wrong person you might want to know who did it and with mailbox auditing you can.

6.1.2 Require MFA for Azure AD privileged roles

6.1.2.1 What does it do

This action will require you to use MFA for privileged roles.

6.1.2.2 Current state

Not fully implemented. A few privileged accounts use MFA to login to cloud components.



Security Workshop

Initial Engagement



Security Workshop



Microsoft
Security
Overview



Discovery
Session



Threat Check



Customer
Immersion
Experience



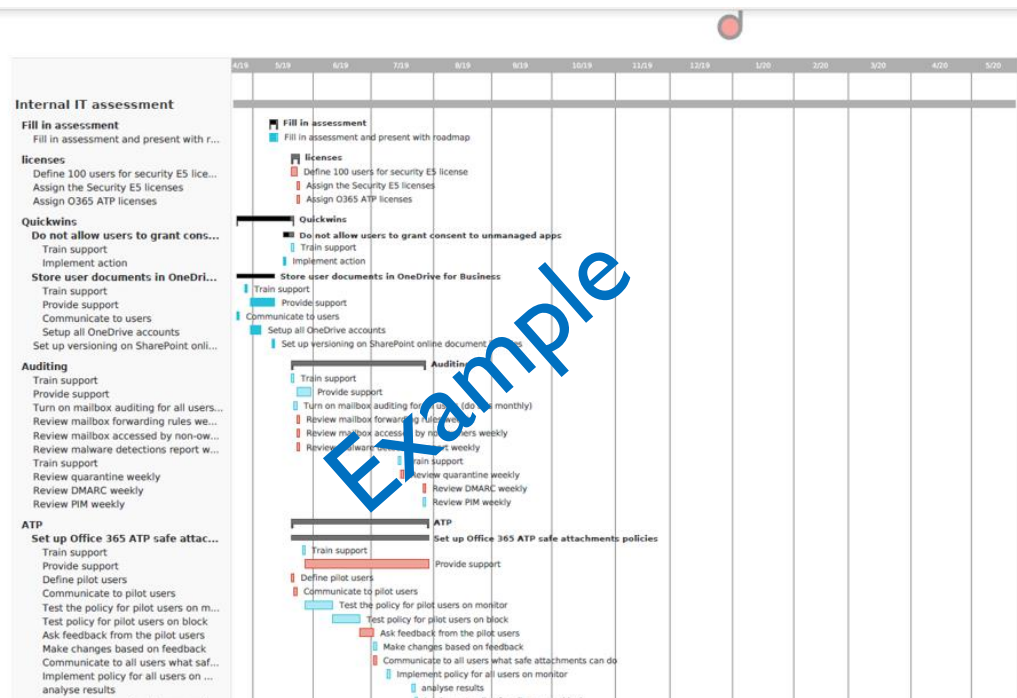
Recommendations
and Next Steps

Roadmap

7.1.1 High level

Estimation:

| Project | Estimation |
|------------------------------------|------------|
| Assessment | 2,5 |
| Quick wins | 1,5 |
| Unused users | 2 |
| Auditing | 2 |
| ATP | 3 |
| Email protection (spf, dkim,dmarc) | 2 |
| Secure privileged user management | 2 |
| Self-service password reset | 8 |
| MFA | 8 |
| Not yet on roadmap | TBD |



Pricing: Digital workplace Security Assessment and Workshop

Scope of work

- › Questionnaire
- › Assess the current M365 environment
- › Workshop and define next steps
 - › General security presentation
 - › Discovery session
 - › Present assessment report
 - › Define next steps (if needed show demos)
- › Deliverables:
 - › Roadmap and assessment report

Price: 3500 euro





> Maarten Leyman

Summary

Maarten is a senior security consultant with experience in the full Microsoft 365 security suite and Azure security.

He started his career at delaware in September 2013 after graduating in New Media and Communication Technology with a specialization in networking at HOWEST.

First, he joined the “Core Technology Services” team where he was support engineer and worked with Windows server, VMware, Azure, Networking, Monitoring, Security, ... After that, he joined the “Cloud Enablement & Operations” team where he focusses on cloud security

Maarten performs security assessments and workshops at customers to identify security risks. Further he helps with the IT architecture and implementations to increase overall security at customers and mitigate possible threats.

Languages

Dutch: Native

English: Full professional proficiency

Expertise

Maarten has expertise in the full Microsoft 365 security suite and Azure security such as Azure Active Directory Security, Privileged Identity Management, Defender for Identity, Defender for Endpoint, Defender for Office 365, Defender for Azure and Information protection.

He has acquired multiple certificates such as:

- 2014 Cisco SMB Specialization for Account managers (700-505)
- 2015 Installing and Configuring Windows Server 2012 (70-410)
- 2018 Cisco express networking(Meraki) (700-901)
- 2018 Implementing Microsoft Azure Infrastructure Solutions (70-533)
- 2019 Microsoft 365 security administration (MS-500)
- 2019 Azure security engineer (AZ-500)

Experience at

Since high school Maarten has been intrigued by security. He took the opportunity to become the security lead within delaware with both hands when delaware decided to start a security practice in partnership with NVISIO. Maarten guided many customers already to improve their security posture with Microsoft cloud technologies.

- Internal delaware
- Kom op tegen kanker
- Le Tec/ OWT (Opérateur de transport de Wallonie)
- Associated Weavers
- Ar Metallizing
- Sports & Leisure
- Renson
- Niko
- Oil search
- Orac
- PSS
- Centre du translation (Europe)
- Ferra
- Flexsoft
- Eggo
- BIO-INVEST
- EFSA
- Tuc Rail
- ...