



Styrk din IT-sikkerhed i praksis

MB Solutions



Hvem er jeg?



Jacob Dahlgaard
Security Team Lead

- 8 År i MB-Solutions
- Ansvarlig for MB-Solutions IT-sikkerhedsaktiviteter
- Arbejder med løbende udvikling og drift af IT-sikkerhed hos danske virksomheder
- Fokus på at få sikkerhed til at fungere i praksis – ikke kun på papiret



Dagsorden

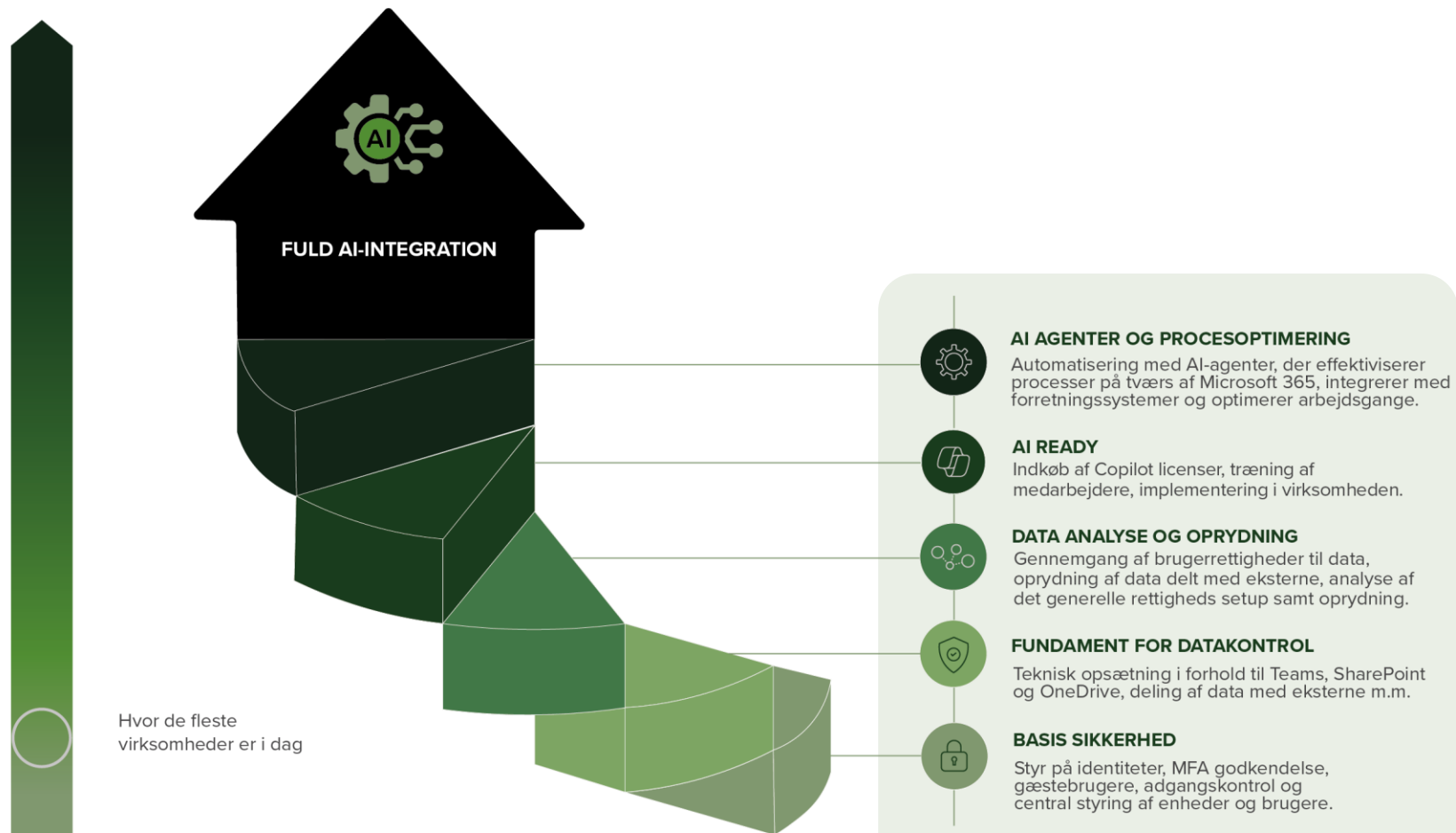
- Forebyggelse & beredskab
- MBS' tilgang til IT-sikkerhed
- Struktur med IT-sikkerhedsårshjul
- Fra anbefaling til implementering
- Prioritering – størst effekt først
- De 5 klassiske sikkerhedshuller
- Det aktuelle trusselsbillede (Arctic Wolf)





AI & IT Sikkerhed

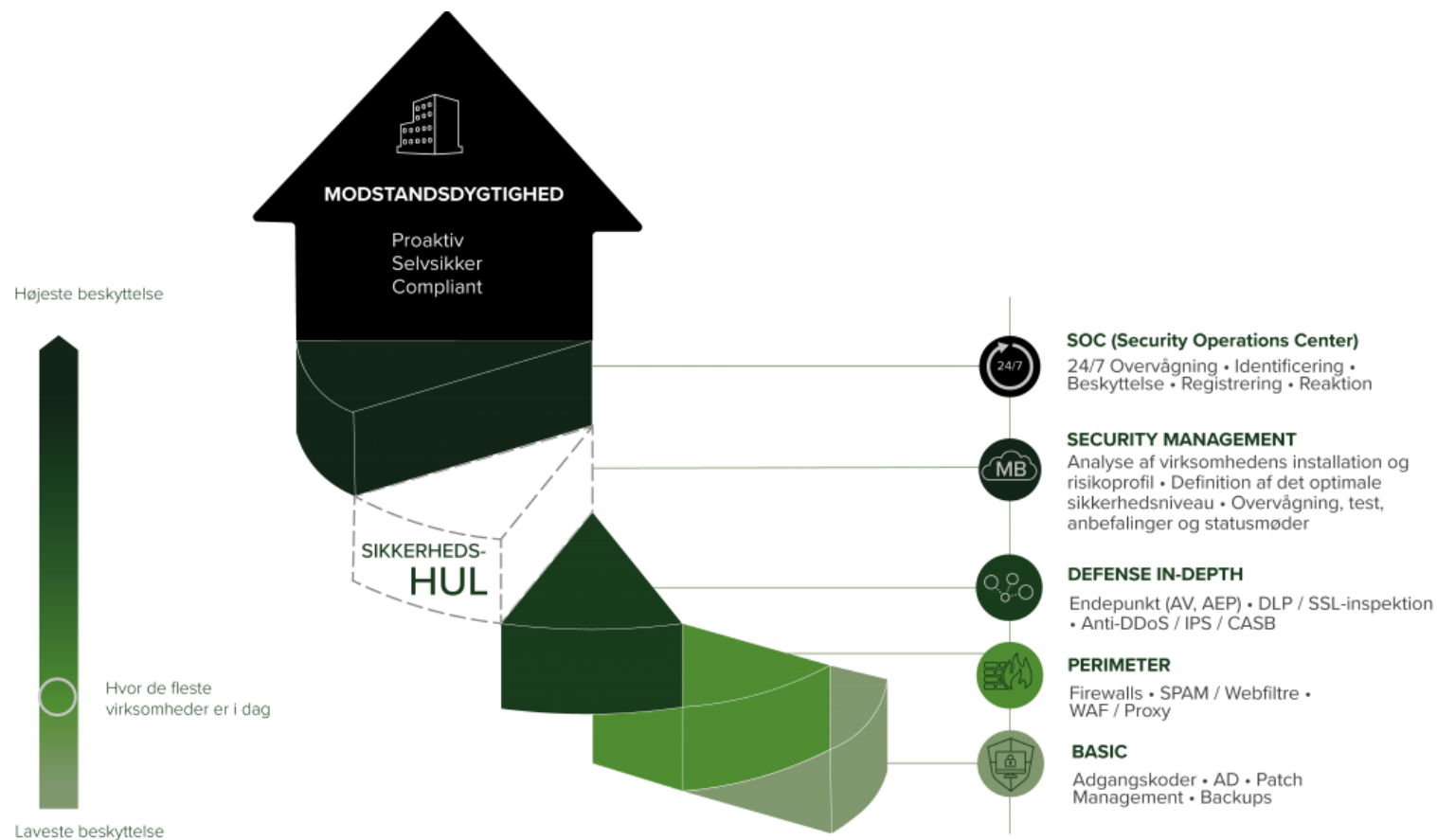
HØJESTE BESKYTTELSE



LAVESTE BESKYTTELSE



Forebyggelse



- Awareness træning
- Tilpasning af teknisk opsætning
- Patch & sårbarhedsstyring
- Overblik over enheder og identiteter
- IT beredskabsplan



Beredskab

Arctic Wolf



SOC

+1000 Security Engineers across SOC and Incident response teams. Infused with AI capabilities to deliver outcome in the modern IT era.



Aurora Platform



Security Teams



Concierge Partner Model



Arctic Wolf Labs

SOC as a Service



Managed Detection and Response

24/7/365 Detection and Response.



Incident Response

Eradication & Remediation
Forensics analysis & reporting
Negotiation with threat actors.
Recover & Restore Operations

MB Solutions



NEXT Generation Cloud Provider

Local presences, tailored services and innovative solutions to meet the specific needs of each client.



Vulnerability assessment



Compliance



Managed IT Services



Hvordan MBS arbejder med IT-sikkerhed

1

Vi starter med en grundig onboarding og analyse

- Fakta før anbefalinger
- Overblik over miljøet
- Fælles udgangspunkt

2

Sikkerhed tilpasses virksomhedens risikoprofil

- Ikke one-size-fits-all
- Realistisk og relevant sikkerhedsniveau

3

Anbefalinger bliver omsat til konkrete handlinger

- Ikke kun rapporter
- Prioriterede opgaver
- Aftalt plan & implementering



Opgave håndtering

Security Management Tas... Sammenkædet plan

Gitter Tavle Diagrammer Tidsplan ...

Generelle sikkerheds opgaver

- Tilføj opgave
- MB-Solutions Afventer afklaring
 - Lokale enheder / Intune enheder
 - 17.06.
 - MB-Solutions Afventer afklaring
 - Løbende compliance kontrol af enheder
 - Forfalder
 - MB-Solutions
 - ...
 - Forfalder
 - Afventer afklaring
 - MacOS opsætning i intune & MS Defender?

Pingcastle

- Tilføj opgave
- Fuldførte opgaver 2

CSAT

- Tilføj opgave
- Ikke gennemgået
 - LocalAD - A high number of built in Administrators group members: 90
- Fuldførte opgaver 2

Greenbone Scan

- Tilføj opgave
- Ikke gennemgået
 - ...
 - Ikke gennemgået
 - ...
- Fuldførte opgaver 2












Microsoft Secure Score

- Tilføj opgave
- MB-Solutions Afventer afklaring
 - Microsoft Defender for serveres
 - Forfalder
 - Afventer afklaring
 - Update Microsoft Defender for Endpoint core components (7/19 exposed devices)
 - 15.05.
 - Ikke gennemgået
 - ASR Rules
 - Ikke gennemgået
 - Ensure multifactor authentication is enabled for all users (275/615 users that aren't registered with MFA.)
 - 1



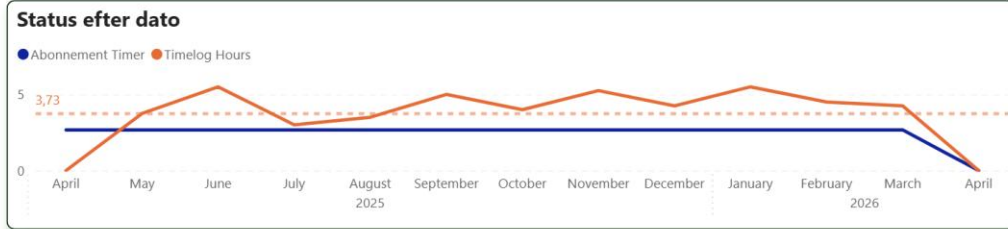
IT-sikkerhedsårshjul

Redskab

								
		Microsoft Secure Score	Azure Secure Score	Greenbone Scan	Pingcastle	Exposure Score	Cloud DockID	Generelle anbefalinger
Frekvens	 Månedlig	X	X			X		X
	 Kvartalvis			X	X			
	 1/2 årlig						X	
	 Årlig							

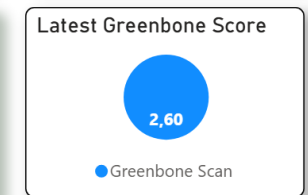
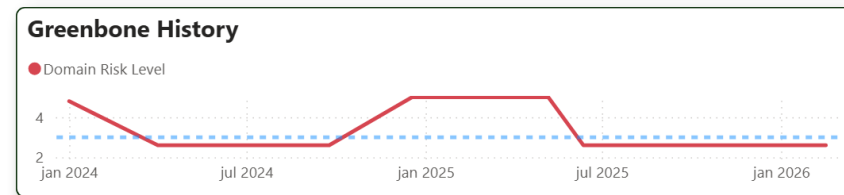
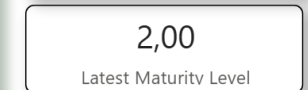
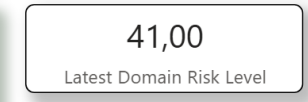
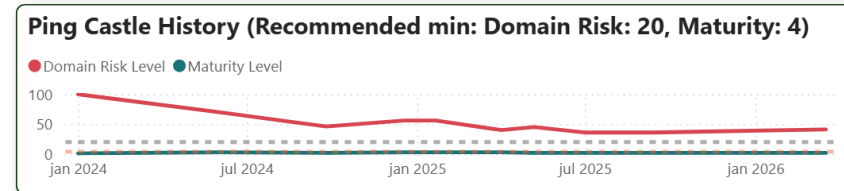
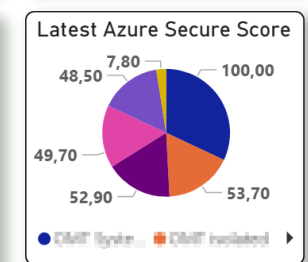
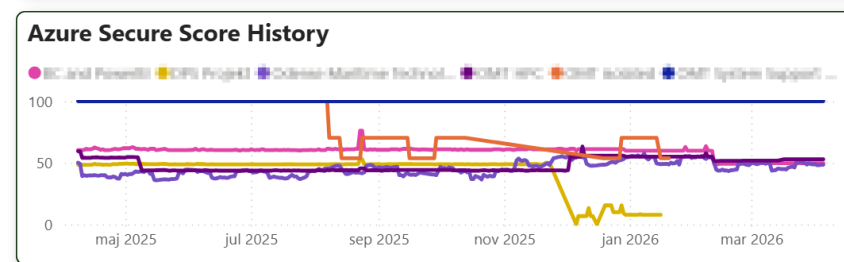
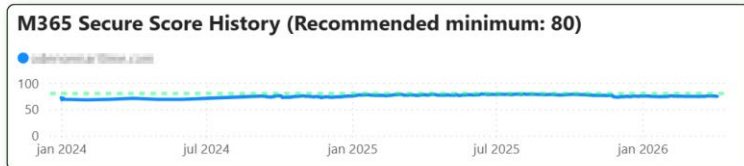
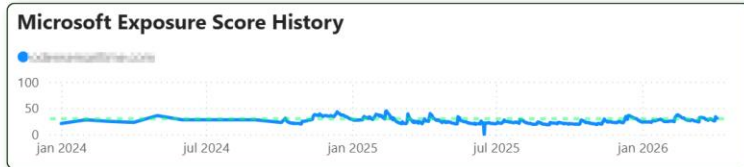


Alt data på ét sted



Årshjul

Frekvens	Azure Secure Score	CloudDocIT	Exposure Score	Greenbone Scan	Microsoft Secure Score	Pingcastle
HalfYearly		X				X
Monthly	X		X		X	
Quarterly				X		





Prioritering i IT-sikkerhed – hvad giver mest værdi først?

Microsoft Secure Score

Overview Recommended actions History Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

↓ Eksportér 198 elementer Filtre

Rank	Recommended action	Score i...	Points achi...	Status	Regress...
<input type="checkbox"/> 1	Block Office applications from creating executable content	+0.77%	0/9	<input type="radio"/> To address	No
<input type="checkbox"/> 2	Block process creations originating from PSEXEC and WMI com	+0.77%	0/9	<input type="radio"/> To address	No
<input type="checkbox"/> 3	Block all Office applications from creating child processes	+0.77%	0/9	<input type="radio"/> To address	No
<input type="checkbox"/> 4	Block abuse of exploited vulnerable signed drivers	+0.77%	0/9	<input type="radio"/> To address	No
<input type="checkbox"/> 5	Block executable files from running unless they meet a prevale	+0.77%	0/9	<input type="radio"/> To address	No
<input type="checkbox"/> 6	Block executable content from email client and webmail	+0.77%	0/9	<input type="radio"/> To address	No
<input type="checkbox"/> 7	Block untrusted and unsigned processes that run from USB	+0.77%	0/9	<input type="radio"/> To address	No
<input type="checkbox"/> 8	Block persistence through WMI event subscription	+0.77%	0/9	<input type="radio"/> To address	No

- **IT-sikkerhed prioriteres ud fra et 360-graders perspektiv**
- **Beslutninger baseres på data fra hele IT-miljøet**
- **Tekniske anbefalinger omsættes til en prioriteret handlingsliste**
- **Vi starter med få tiltag, der giver størst effekt**



De klassiske 5 huller (OneDrive/SharePoint deling af data)

Deling

Brug disse indstillinger til at styre deling på organisationsniveau i SharePoint og på OneDrive.
[Få mere at vide om administration af indstillinger for deling](#)

Ekstern deling

Indhold kan deles med:

SharePoint

OneDrive

Mest tilladelig	Alle Brugerne kan dele filer og mapper ved hjælp af links, der ikke kræver logon.
	Nye og eksisterende gæster Gæster skal logge på eller angive en bekræftelseskode.
	Eksisterende gæster Kun gæster, der allerede findes i organisationens mappe.
Mindst tilladelig	Kun personer i organisationen Ekstern deling er ikke tilladt.

Du kan begrænse delingen yderligere for hvert enkelt websted og for OneDrive. [Få at vide hvordan](#)

Flere indstillinger for ekstern deling ▾

- Begræns ekstern deling efter domæne
- Tillad kun brugere i bestemte sikkerhedsgrupper at dele eksternt
- Tillad, at gæster deler elementer, de ikke ejer

- **Deling kan ske uden krav om login eller MFA**
- **Begrænset sporbarhed**
- **Gæster kan dele videre med andre gæster**
- **Ukontrolleret adgang til kritiske data**



De klassiske 5 huller (Unmanaged enheder)

Microsoft Endpoint Manager admin center

Home > Devices

Devices | All devices

Search Refresh Filter Columns Export Bulk Device Actions

Showing 1 to 25 of 46 records

Device name ↑↓	Managed by ↑↓	Ownership ↑↓	Compliance ↑↓	OS
Unknown	Intune	Unknown	Compliant	Other
APN2COMANT1	Intune	Corporate	Compliant	Windows
APRILVIVEERA	Co-managed	Corporate	Not Compliant	Windows
Amos's MacBook Air	Intune	Corporate	Compliant	macOS
Chrome-0MWB91BH001--	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-0Q9L91BJ401731	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-SCD1460WZ4	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-8B25G04/TV	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-NXH8WAA0031--	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-NXHKGSG00402--	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-NXHWNAAD010--	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-PF32F6BH	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-YX024RZJ	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-YX029#88	Intune	Corporate	Not Evaluated	Chrome OS
Chrome-YX02D0XW	Intune	Corporate	Not Evaluated	Chrome OS
DESKTOP-15IBSS5	Intune	Corporate	Not Compliant	Windows
DESKTOP-1APLGOA	Intune	Corporate	Not Compliant	Windows
DESKTOP-4EJ8DCH	Intune	Corporate	Not Compliant	Windows
DESKTOP-50KQFMJ	Intune	Corporate	Not Compliant	Windows

Navigation menu:

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Left sidebar (By platform):

- Windows
- iOS/iPadOS
- macOS
- Android
- Chrome OS

Left sidebar (Device enrollment):

- Enroll devices

Left sidebar (Provisioning):

- Windows 365

Left sidebar (Policy):

- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Group Policy analytics (preview)
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later (preview)



De klassiske 5 huller (MFA)

Ensure multifactor authentication is enabled for all users

Planned

[Edit status & action plan](#) [Manage tags](#)

General Implementation History (10)

Description

Multifactor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.

Implementation status

You have 81 out of 159 users that aren't registered with MFA.

User impact

After registering, users are prompted to authenticate with a second factor when accessing applications or other resources.

Users affected

All of your Microsoft 365 users

- **MFA-policy - brugere med aktiveret MFA**
- **MFA kræves ikke altid ved login (fx fra kontoret)**
- **Brugere kan eksistere uden MFA i lang tid**
- **Hacker kan selv opsætte MFA efter password-kompromittering**



De klassiske 5 huller (MFA)

Ensure multifactor authentication is enabled for all users

Planned

[Edit status & action plan](#) [Manage tags](#)

General Implementation History (10)

Description

Multifactor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised.

Implementation status

You have 81 out of 159 users that aren't registered with MFA.

User impact

After registering, users are prompted to authenticate with a second factor when accessing applications or other resources.

Users affected

All of your Microsoft 365 users

- **MFA-policy - brugere med aktiveret MFA**
- **MFA kræves ikke altid ved login (fx fra kontoret)**
- **Brugere kan eksistere uden MFA i lang tid**
- **Hacker kan selv opsætte MFA efter password-kompromittering**



De klassiske 5 huller (Adgang til admin portaler)

The screenshot shows the Microsoft Entra ID 'Roles and administrators' page. The left sidebar contains navigation options like Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agents, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Tenant governance (Preview), Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Account recovery, and Password reset.

The main content area is titled 'Roles and administrators | All roles'. It includes a search bar and a table of roles. The table has columns for Role, Description, Privileged, Ass... (Assignments), and Type. The 'Privileged' column contains a 'PRIVILEGED' badge for several roles.

Role	Description	Privileged	Ass...	Type
<input type="checkbox"/> Security Operator	Creates and manages security events.	PRIVILEGED	95	Built-in
<input type="checkbox"/> Security Reader	Can read security information and reports in Microsoft Entra ID and Microsoft 365.	PRIVILEGED	62	Built-in
<input type="checkbox"/> Dynamics 365 Administrator	Can manage all aspects of the Dynamics 365 product.		12	Built-in
<input type="checkbox"/> Global Reader	Can read everything that a Global Administrator can, but not update anything.	PRIVILEGED	11	Built-in
<input type="checkbox"/> Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and view groups activity and audit reports.		11	Built-in
<input type="checkbox"/> Power Platform Administrator	Can create and manage all aspects of Microsoft Dynamics 365, PowerApps and Microsoft Flow.		11	Built-in
<input type="checkbox"/> Teams Administrator	Can manage the Microsoft Teams service.		11	Built-in
<input type="checkbox"/> User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	PRIVILEGED	11	Built-in
<input type="checkbox"/> Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	10	Built-in
<input type="checkbox"/> Attack Payload Author	Can create attack payloads that an administrator can initiate later.		10	Built-in
<input type="checkbox"/> Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.		10	Built-in
<input type="checkbox"/> Attribute Assignment Administrator	Assign custom security attribute keys and values to supported Microsoft Entra objects.		10	Built-in
<input type="checkbox"/> Attribute Definition Administrator	Define and manage the definition of custom security attributes.		10	Built-in
<input type="checkbox"/> Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	PRIVILEGED	10	Built-in
<input type="checkbox"/> Authentication Policy Administrator	Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and verifiable credentials.		10	Built-in



De klassiske 5 huller (Data Sikkerhed & AI)

The screenshot shows the Microsoft Excel interface with a sensitivity label dialog box open. The dialog box is titled 'Sensitivity' and contains the following information:

- File name: Financial Summary.xlsx
- Location: Reports (Sales and Marketing)
- Sensitivity: Confidential (All Employees)
- User: rsimone@vanarsdelltd.com
- Options: Personal, Public, General, Confidential (checked), Highly Confidential
- Learn More link

The background spreadsheet shows financial data for Year 2 and Year 1. The data is as follows:

	Year 2	Year 1
Revenue	0.00	93,580.00
Gross margin	0.00	60,543.00
Operating income	2.00	18,161.00
Net income	3.00	12,193.00
Diluted earnings per share	2.1	1.48
Cash dividends declared	1.44	1.24
Cash, cash equivalents	0.00	96,526.00
Total assets	9.00	174,303.00
Long-term obligations	4.00	44,574.00

- AI arbejder direkte på virksomhedens data
- Sensitivity labels styrer hvad AI må bruge
- Klassificér data - Offentligt / Internt / Fortroligt
- Klassificering kan startes simpelt (2-3 labels)



 MB Solutions