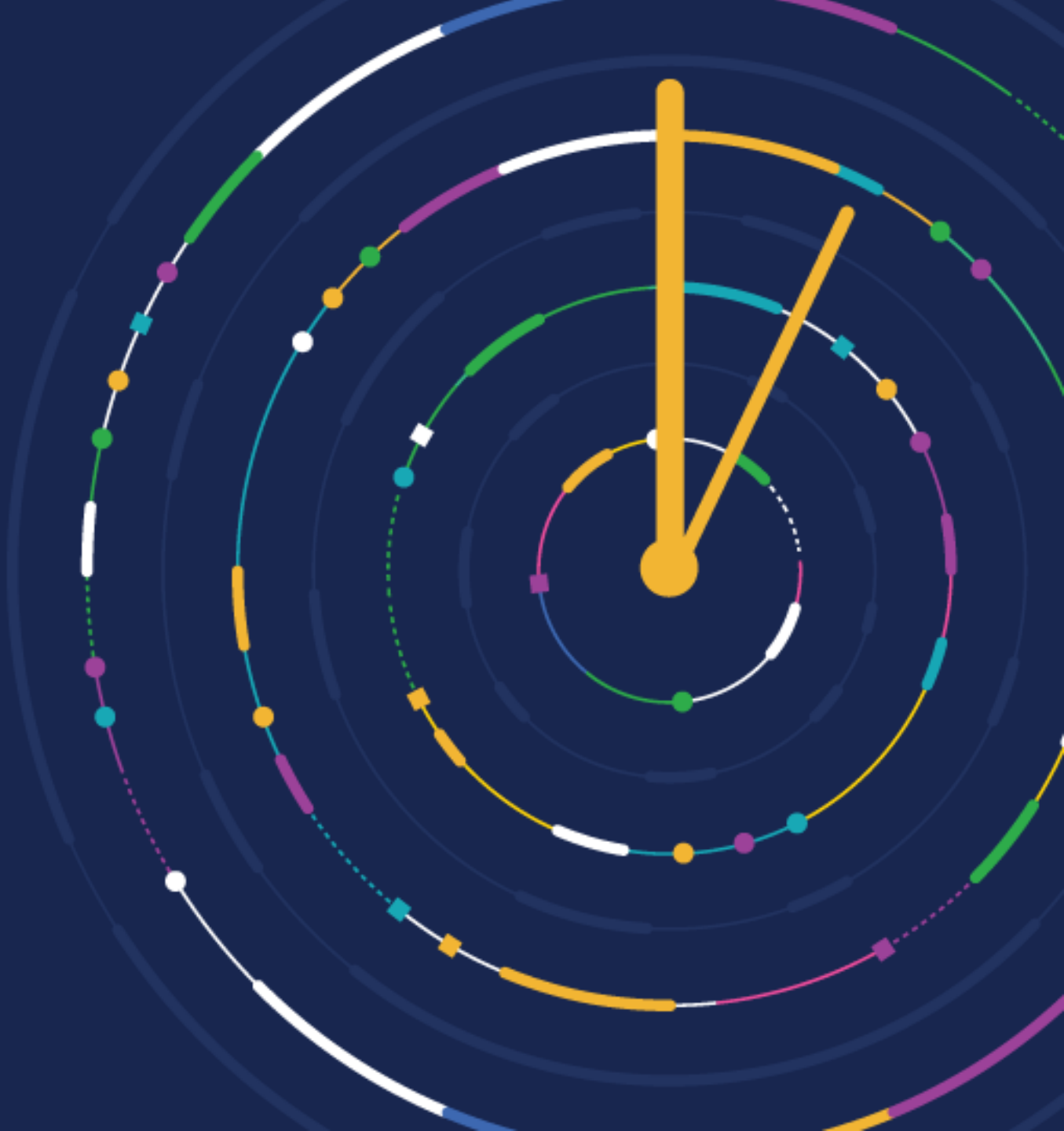
tecman

Protecting your Microsoft systems - how to sleep easily in a hostile world

Mark Connolly

CUSTOMER DAY 2023



tecman

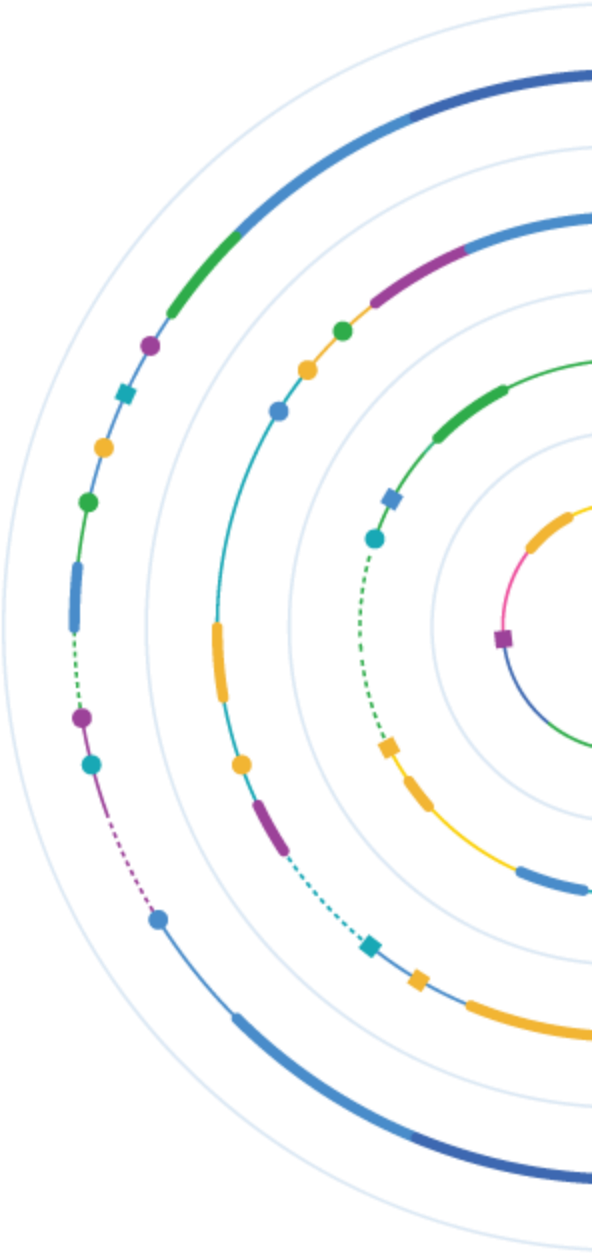
What we'll cover

1. Introduction – why we're here.
2. Basic Security Principles
3. PaaS / SaaS / On Prem
4. Business Central Specific
4. Entra ID (Formerly AAD)
5. Quick Wins
6. Entra Apps (Service Principles)
7. GDAP

Introduction

Why we're all here.

- Shared Responsibility (even on SaaS)
- **Onus no longer on BC\CRM Partner (GDAP)**
- Know it or not, you'll have cloud presence
- MS give us lots of tools – use them

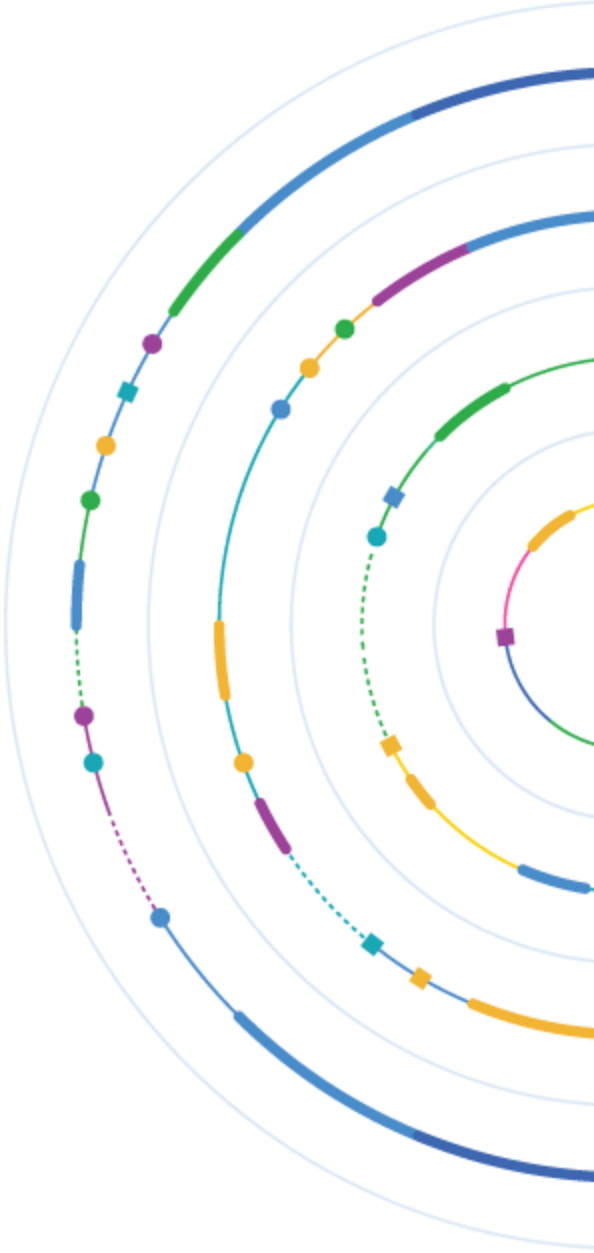


Why we're all here.

- 70% ransomware effected orgs have fewer than 500 employees
  - SME primary victims of ransomware attacks
- 200% increase Human operated attacks.
  - Ransomware as a service. Affiliate Program.
- 99% of attacks prevented by 'basic security practices'
- 4000 identity attacks block per second.
- 80-90% of all compromises originate from BYOD
  - Re-enforces message of user awareness\training

June '22 to June '23

Microsoft Digital Defense Report 2023



Basic Security Principles

- Assume breach!!
  - Continuous Monitoring. Zero Trust

- Policies and User Awareness
  - MFA\CA\Secure Defaults – no real expertise required
  - User Awareness and Training (i.e Simulated Phishing test – see KB)

- Monitor and log
  - Azure Monitor (alerts)
  - Sign in\Audit Logs
  - Regular Reviews (Risky Sign-ins)

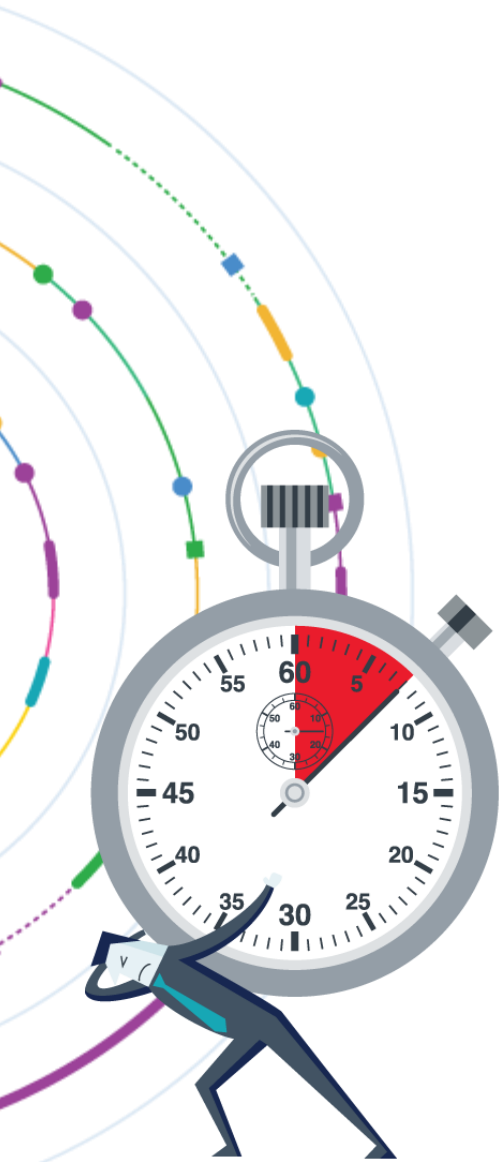
PaaS

- Strong Authentication (MFA\CA)
- Subscription RBAC
- NSG. Block 3389, 80
- AAG \ WAF
- Patching
- DR \ Backups
- Security Centre
  - Secure Score, Security Recommendations

SaaS

- Strong Authentication (MFA\CA)
- Admin Centre Access
- Service Tags
- Service Overview (QR next slide)
- Review Delegated Admins
- Telemetry
  - Deprecated Protocols
  - Sign-In Activity

BC SaaS Service Overview



CUSTOMER DAY 2023

tecman

On Prem

- Still use AAD\EntraID*
- SSL
- Server hardening\patching
- Disable old protocols. Tls1.0, 1.1

*Nav 2015 and above

General Azure

- App functions
  - Authentication
  - Key management – Key vault
- Storage Accounts
  - Shared Access Signature
  - Rotate Keys. Key Vault
  - NSG, Private Endpoint, Disable public access

Business Central – non platform specific

- Basic Auth
  - SharePoint
  - SMTP
- Change Log. Track permission and permission set changes
- Use Entra License and Security Groups for BC Users (QR next slide)
- New users – license configuration
  - Adding new users inherits permission sets
- BC Admin Centre (D365 Admin) - Review your own roles

Business Central – non platform specific

- Authentication for external apps*
  - Review Service Principles (App Reg)
  - Review expiring and expired secrets.

*BC22 - OAuth is only supported method

Business Central – non platform specific

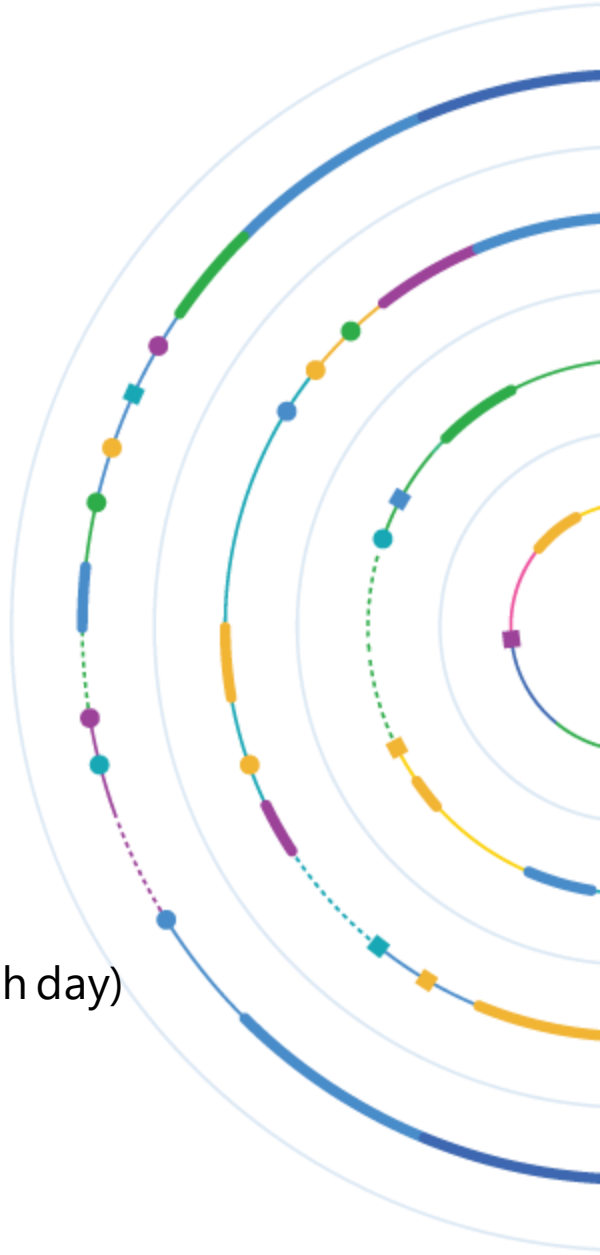
Tecman Training Video on Security Groups in BC

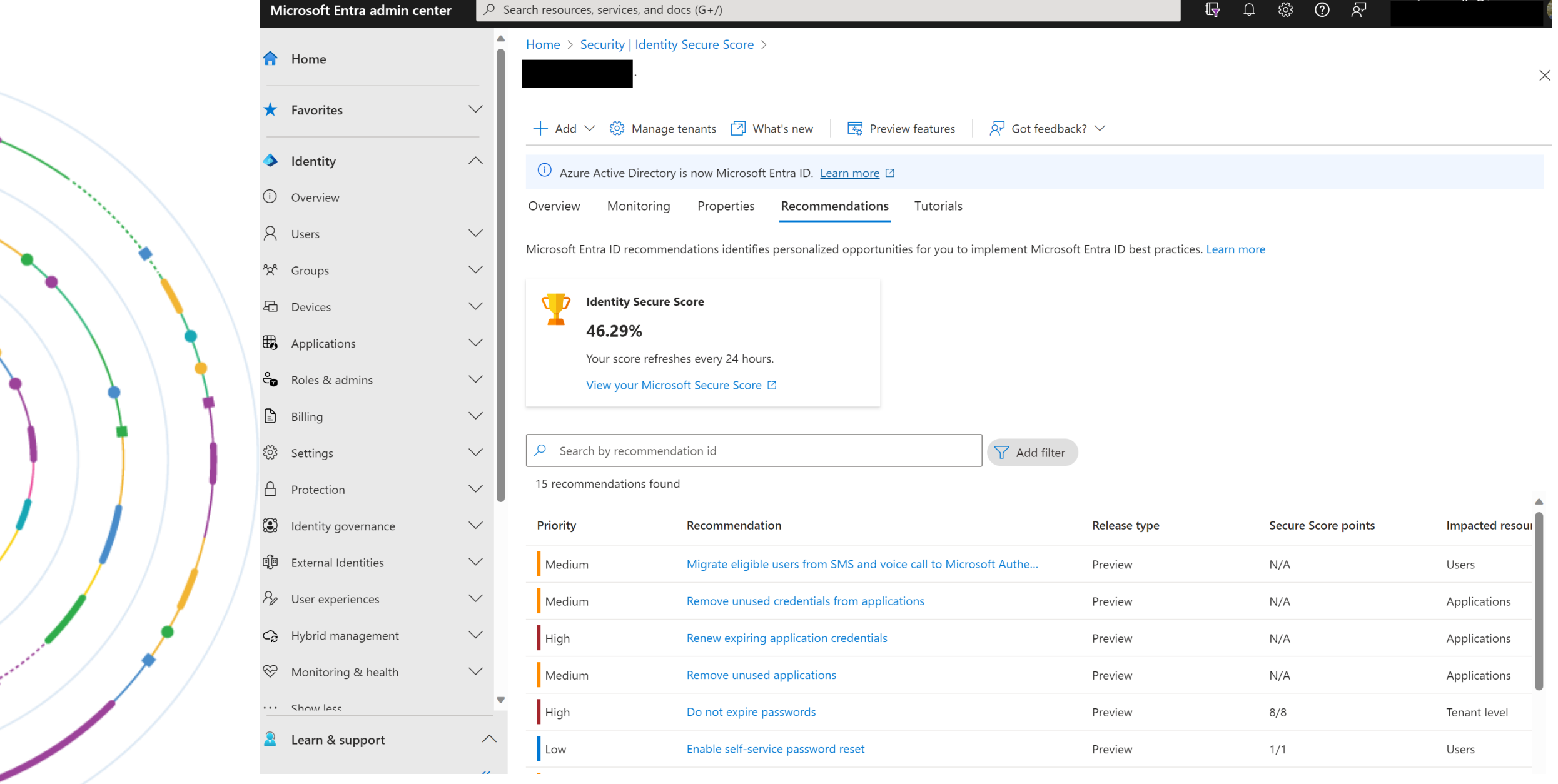
Entra (AAD)

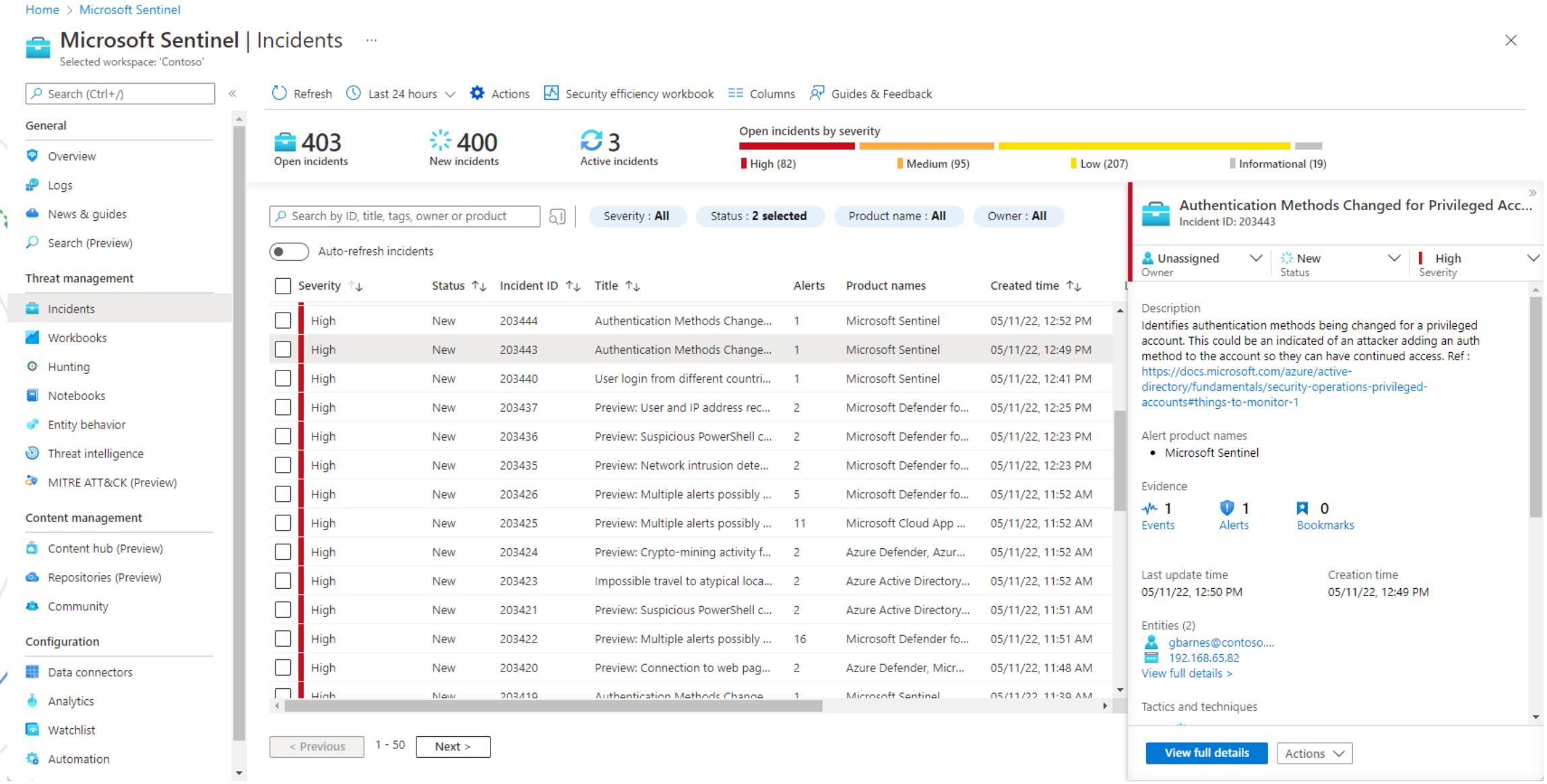

Microsoft Entra ID
Microsoft Entra Permissions Management
Microsoft Entra Verified ID
Microsoft Entra ID Governance
Microsoft Entra Workload ID
Coming soon
Microsoft Entra External ID
Microsoft Entra Private Access
Microsoft Entra Internet Access

Entra ID - Tools

- Defender for Cloud
  - Foundation (Free – Secure Score, policy ,management, multicloud)
  - Advanced (CSPM, Attack Path Analysis)
- Microsoft Sentinel. Security information and event management.
- PIM. Time based privileged access, notifications, review access, audit history
- Identity Protection (Preview, P2)
  - Identify Risky sign-on, PW spray attacks, Leaked Creds, using trillions of signals each day)
  - Automate Remediation (CA)




Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Roles & admins
Billing
Settings
Protection
Identity governance
External Identities
User experiences
Hybrid management
Monitoring & health
Show less
Learn & support
Home > Security | Identity Secure Score >
[redacted]
Add
Manage tenants
What's new
Preview features
Got feedback?
Azure Active Directory is now Microsoft Entra ID. Learn more
Overview
Monitoring
Properties
Recommendations
Tutorials
Microsoft Entra ID recommendations identifies personalized opportunities for you to implement Microsoft Entra ID best practices. Learn more
Identity Secure Score
46.29%
Your score refreshes every 24 hours.
View your Microsoft Secure Score
Search by recommendation id
Add filter
15 recommendations found
Priority
Recommendation
Release type
Secure Score points
Impacted resou
Medium
Migrate eligible users from SMS and voice call to Microsoft Authe...
Preview
N/A
Users
Medium
Remove unused credentials from applications
Preview
N/A
Applications
High
Renew expiring application credentials
Preview
N/A
Applications
Medium
Remove unused applications
Preview
N/A
Applications
High
Do not expire passwords
Preview
8/8
Tenant level
Low
Enable self-service password reset
Preview
1/1
Users


Home > Microsoft Sentinel
Microsoft Sentinel | Incidents
Selected workspace: 'Contoso'
Search (Ctrl+/)
General
Overview
Logs
News & guides
Search (Preview)
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
Content management
Content hub (Preview)
Repositories (Preview)
Community
Configuration
Data connectors
Analytics
Watchlist
Automation
Refresh
Last 24 hours
Actions
Security efficiency workbook
Columns
Guides & Feedback
403
Open incidents
400
New incidents
3
Active incidents
Open incidents by severity
High (82)
Medium (95)
Low (207)
Informational (19)
Search by ID, title, tags, owner or product
Severity : All
Status : 2 selected
Product name : All
Owner : All
Auto-refresh incidents
Severity
Status
Incident ID
Title
Alerts
Product names
Created time
High New 203444 Authentication Methods Change... 1 Microsoft Sentinel 05/11/22, 12:52 PM
High New 203443 Authentication Methods Change... 1 Microsoft Sentinel 05/11/22, 12:49 PM
High New 203440 User login from different countri... 1 Microsoft Sentinel 05/11/22, 12:41 PM
High New 203437 Preview: User and IP address rec... 2 Microsoft Defender fo... 05/11/22, 12:25 PM
High New 203436 Preview: Suspicious PowerShell c... 2 Microsoft Defender fo... 05/11/22, 12:23 PM
High New 203435 Preview: Network intrusion dete... 2 Microsoft Defender fo... 05/11/22, 12:23 PM
High New 203426 Preview: Multiple alerts possibly ... 5 Microsoft Defender fo... 05/11/22, 11:52 AM
High New 203425 Preview: Multiple alerts possibly ... 11 Microsoft Cloud App ... 05/11/22, 11:52 AM
High New 203424 Preview: Crypto-mining activity f... 2 Azure Defender, Azur... 05/11/22, 11:52 AM
High New 203423 Impossible travel to atypical loca... 2 Azure Active Directory... 05/11/22, 11:52 AM
High New 203421 Preview: Suspicious PowerShell c... 2 Azure Active Directory... 05/11/22, 11:51 AM
High New 203422 Preview: Multiple alerts possibly ... 16 Microsoft Defender fo... 05/11/22, 11:51 AM
High New 203420 Preview: Connection to web pag... 2 Azure Defender, Micr... 05/11/22, 11:48 AM
< Previous
1 - 50
Next >
Authentication Methods Changed for Privileged Acc...
Incident ID: 203443
Unassigned
Owner
New
Status
High
Severity
Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1
Alert product names
Microsoft Sentinel
Evidence
1 Events
1 Alerts
0 Bookmarks
Last update time
05/11/22, 12:50 PM
Creation time
05/11/22, 12:49 PM
Entities (2)
gbarnes@contoso....
192.168.65.82
View full details >
Tactics and techniques
View full details
Actions

Microsoft Azure

The Reports Reader role for the TecMan directory was assigned outside of PIM

Always use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to manage your privileged directory roles.

Assignment details:

Settings	Value
User:	[redacted]
Role:	Reports Reader
Assigner:	[redacted]
Detected on:	July 10, 2023 10:52 UTC

View assignment >

Microsoft Azure

Your weekly PIM digest for Technology Management

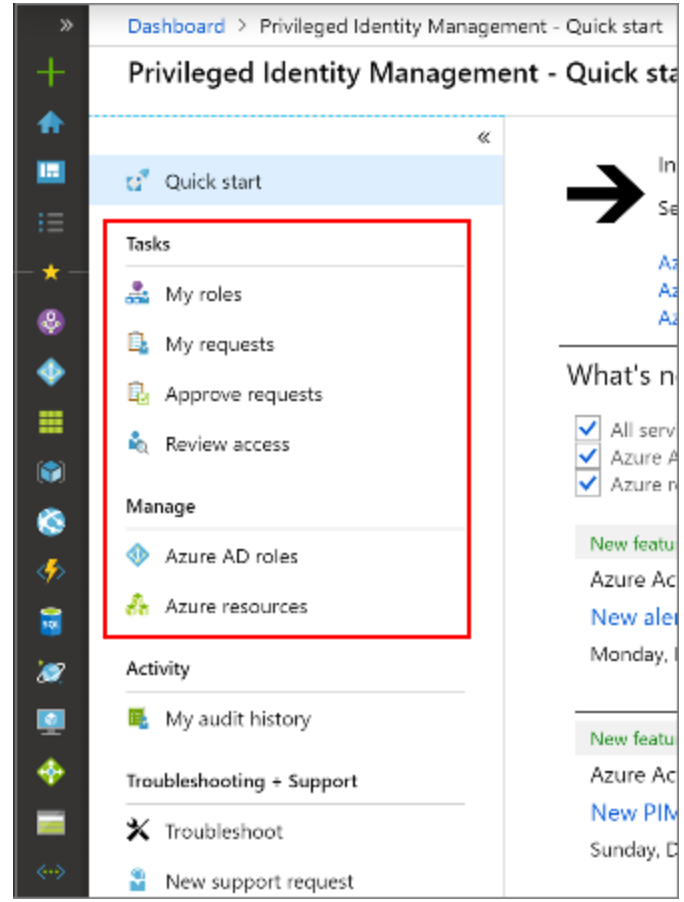
Thanks for using Azure Active Directory Privileged Identity Management (PIM). This weekly digest shows your PIM activities over the last seven days:

User activation	Users made permanent
0	0

Assignments made in PIM	Assignments made outside of PIM
0	0

Overview of your top roles

Role	Permanent	Eligible	Action
Directory Readers	16	0	Reduce permanent >
Global Administrator	6	0	Reduce permanent >
Dynamics 365 Administrator	6	0	Reduce permanent >



Quick Wins

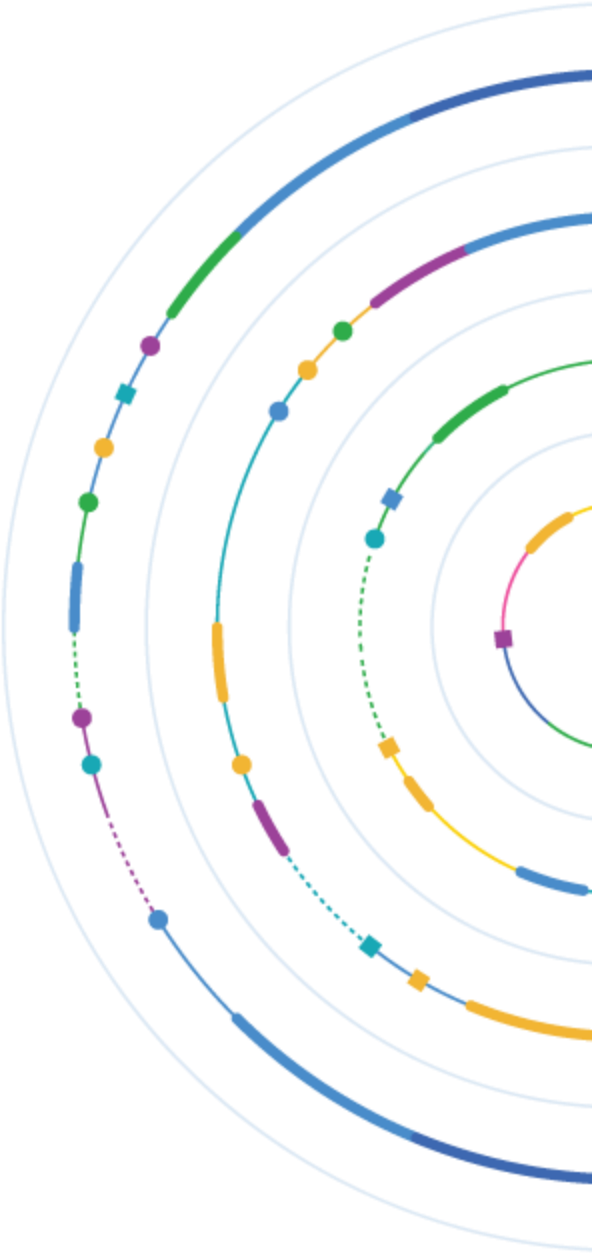
- Enable MFA (even non interactive – use app password)
- Review Secure Score
- Conditional Access (P1)
- Secure Defaults (Enforce 2fa, block legacy auth types)
- Review Apps and Expired Secrets
- POLP – Granular Admins. How many GAs?
- Password NOT to expire
- Service Tags

Entra Applications (service principles)

- Consent Flows
  - User consent (delegated permissions)
  - Admin consent

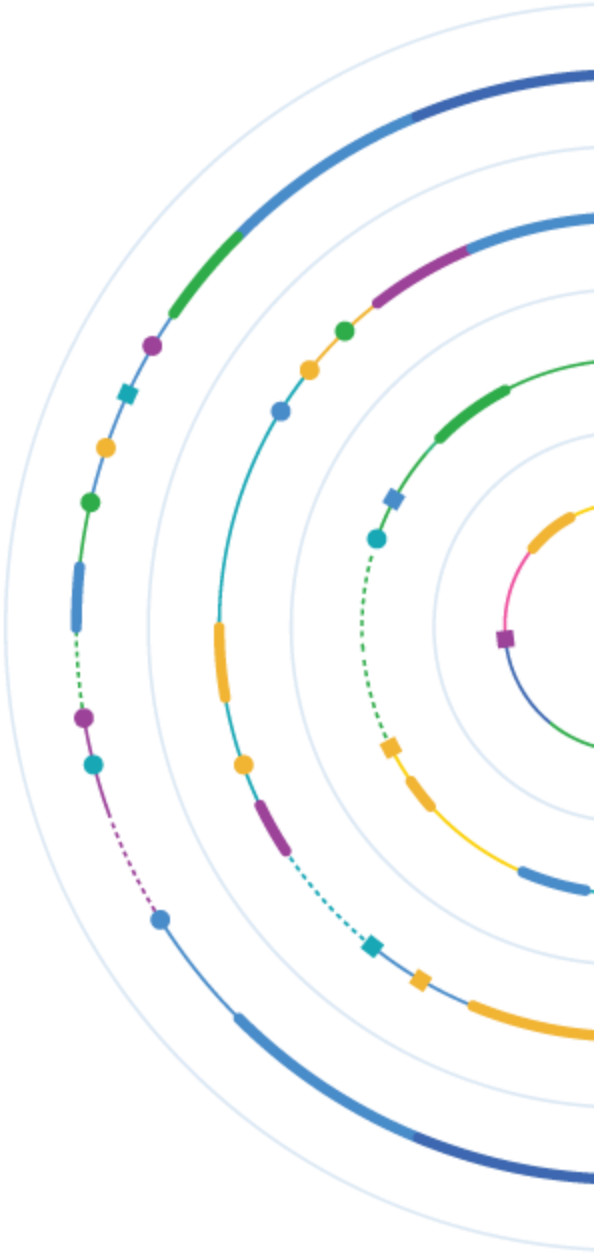
- SP represents an authenticating application.

- Secured by secret or certificate
  - Secrets longer life
  - Certs – more secure



Entra Applications (best practices)

- Restrict User Consent
- Admin consent workflow
- Audit and monitor Consent (Defender for cloud)
- Monitor Expiry of Secrets and certs - PowerAutomate, Logic Apps



Entra Apps

Home > Enterprise applications | Conditional Access >

Consent and permissions | User consent settings

Microsoft Entra ID for workforce

Manage

- User consent settings
- Admin consent settings
- Permission classifications

Save | Discard | Got feedback?

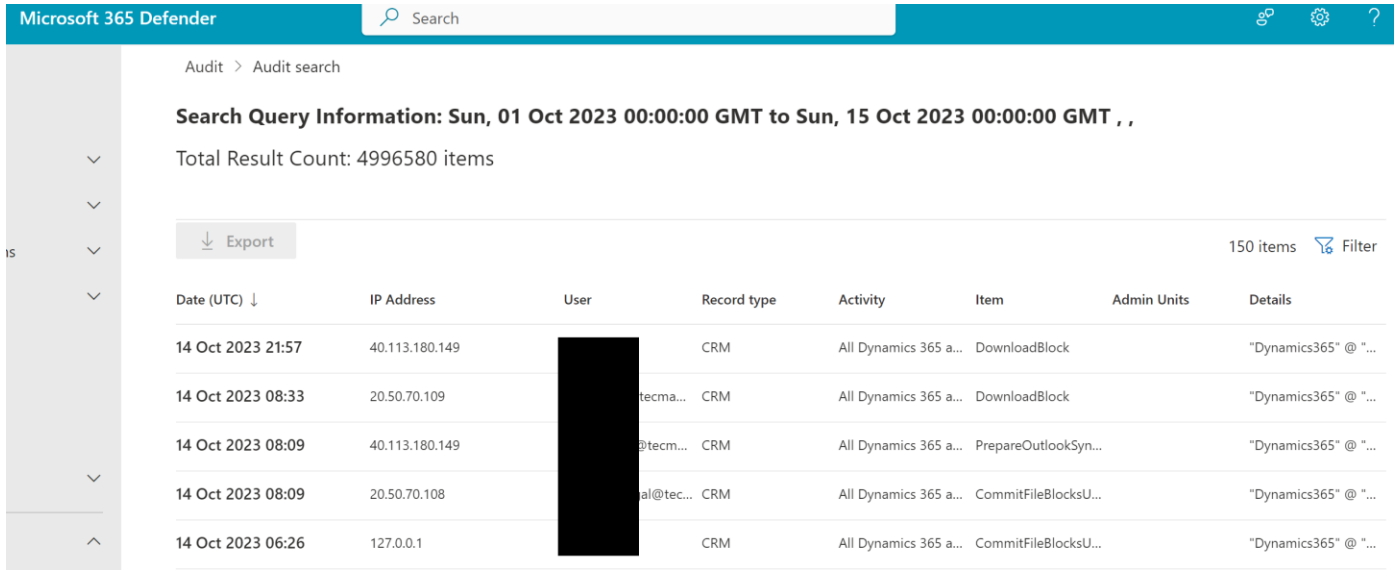
Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

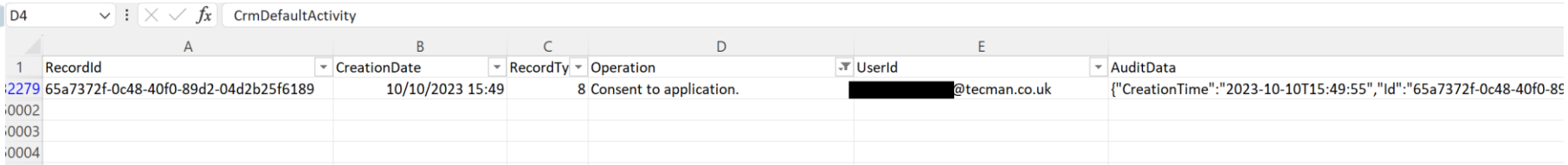
User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

- ○ Do not allow user consent
  An administrator will be required for all apps.
- ○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
  All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- ◉ Allow user consent for apps
  All users can consent for any app to access the organization's data.

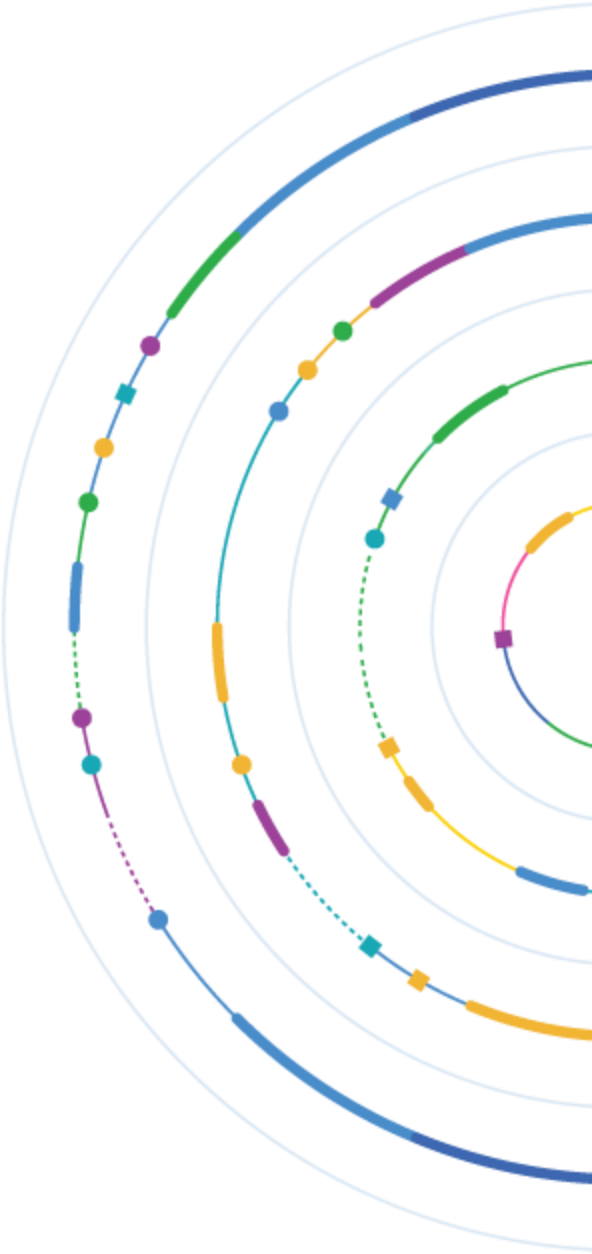
⚠ With your current user settings, all users can allow applications to access your organization's data on their behalf. Learn more about the risks
Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". Learn more

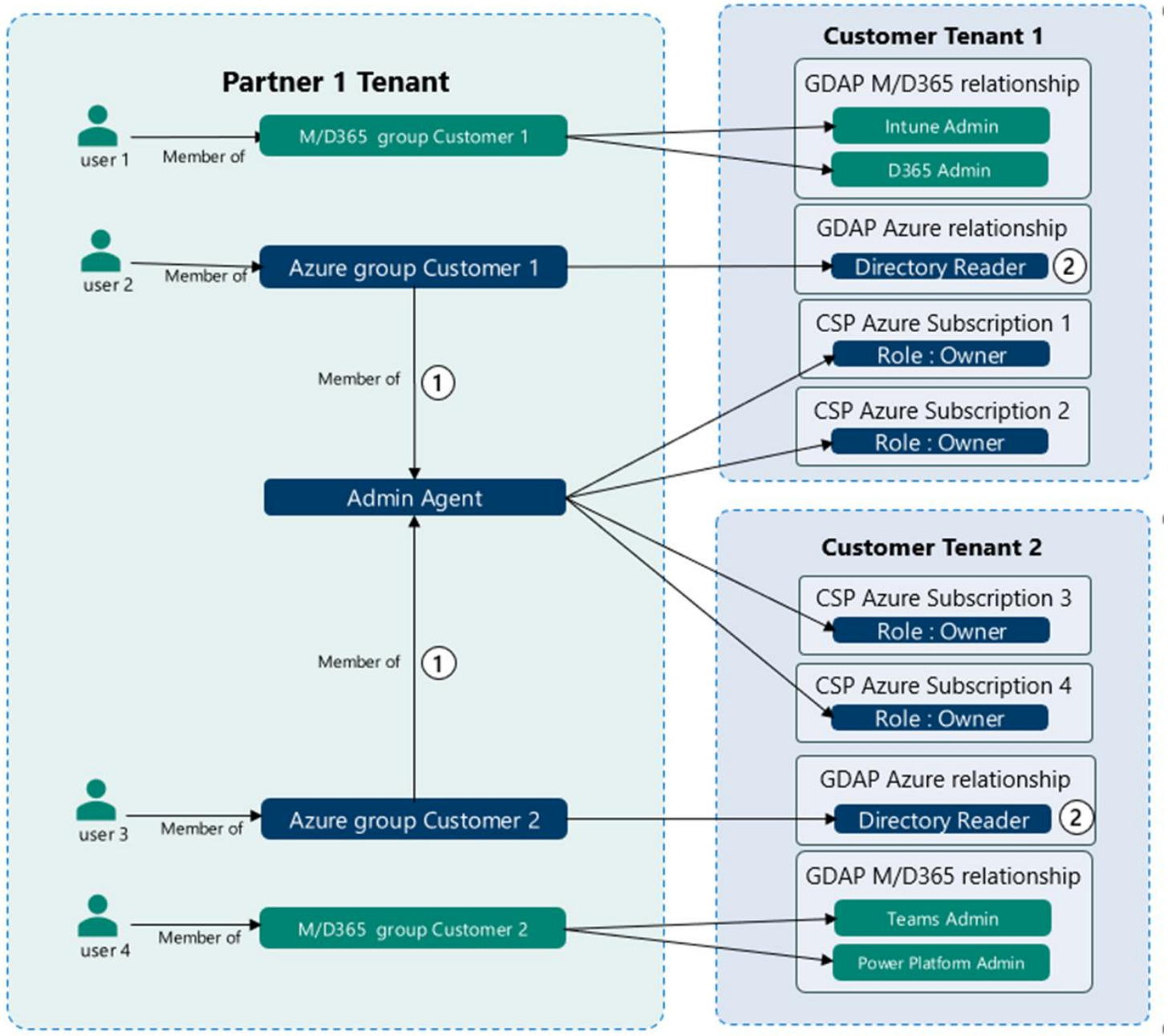

Microsoft 365 Defender
Search
Audit > Audit search
Search Query Information: Sun, 01 Oct 2023 00:00:00 GMT to Sun, 15 Oct 2023 00:00:00 GMT , ,
Total Result Count: 4996580 items
Export
150 items
Filter
Date (UTC)
IP Address
User
Record type
Activity
Item
Admin Units
Details
14 Oct 2023 21:57
40.113.180.149
CRM
All Dynamics 365 a...
DownloadBlock
"Dynamics365" @ "...
14 Oct 2023 08:33
20.50.70.109
CRM
All Dynamics 365 a...
DownloadBlock
"Dynamics365" @ "...
14 Oct 2023 08:09
40.113.180.149
CRM
All Dynamics 365 a...
PrepareOutlookSyn...
"Dynamics365" @ "...
14 Oct 2023 08:09
20.50.70.108
CRM
All Dynamics 365 a...
CommitFileBlocksU...
"Dynamics365" @ "...
14 Oct 2023 06:26
127.0.0.1
CRM
All Dynamics 365 a...
CommitFileBlocksU...
"Dynamics365" @ "...


D4
CrmDefaultActivity
RecordId
CreationDate
RecordTy
Operation
UserId
AuditData
65a7372f-0c48-40f0-89d2-04d2b25f6189
10/10/2023 15:49
8
Consent to application.
@tecman.co.uk
{"CreationTime":"2023-10-10T15:49:55","Id":"65a7372f-0c48-40f0-89

GDAP

- What is GDAP, why?
- Tecman's role
  - Read only access to Entra
- Customer responsibilities
  - Review your own DAP and GDAP
  - Even more changes last week (Dyn365 – BC)



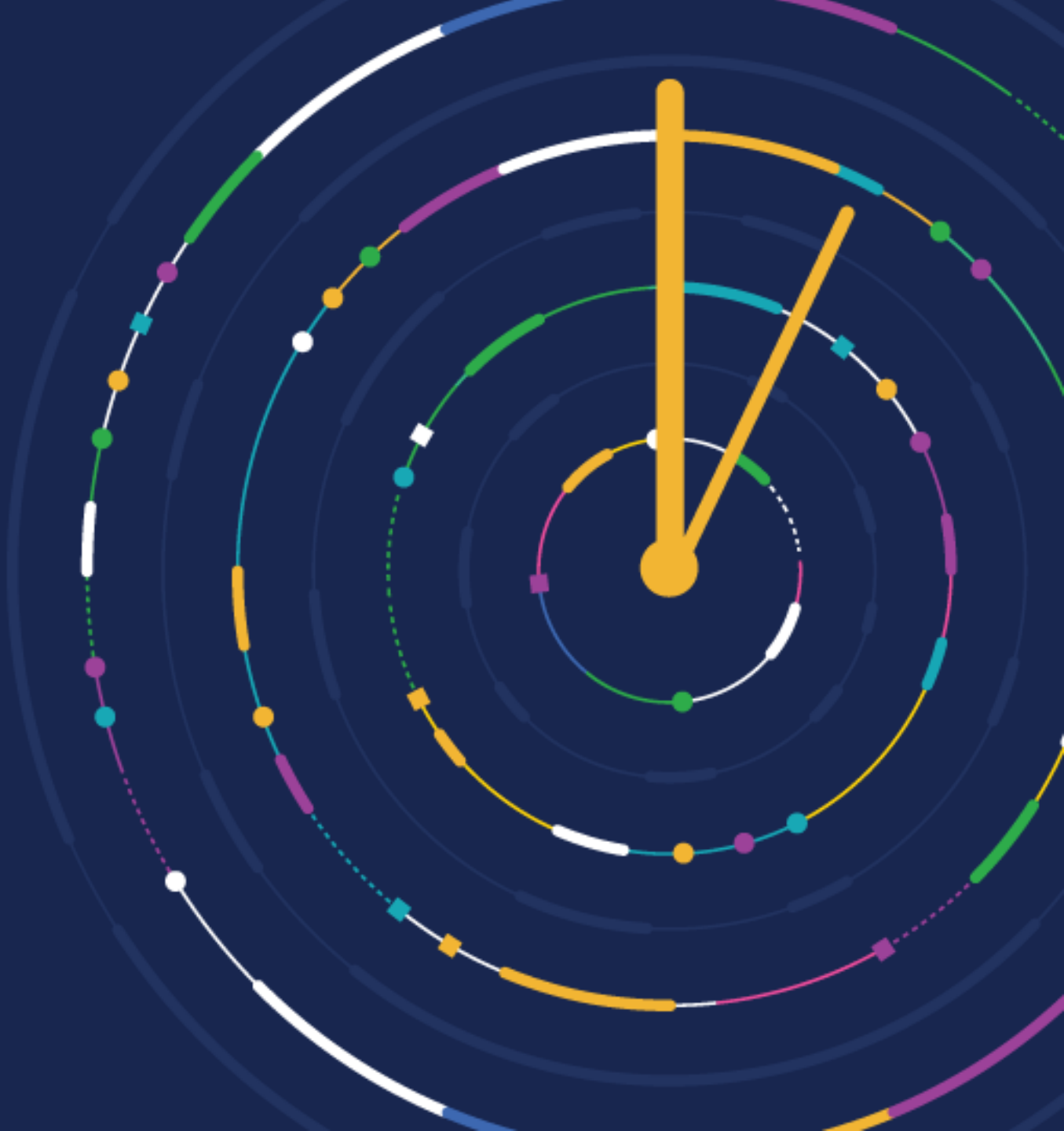

Partner 1 Tenant
user 1
Member of
M/D365 group Customer 1
user 2
Member of
Azure group Customer 1
Member of
1
Admin Agent
Member of
1
user 3
Member of
Azure group Customer 2
user 4
Member of
M/D365 group Customer 2
Customer Tenant 1
GDAP M/D365 relationship
Intune Admin
D365 Admin
GDAP Azure relationship
Directory Reader
2
CSP Azure Subscription 1
Role : Owner
CSP Azure Subscription 2
Role : Owner
Customer Tenant 2
CSP Azure Subscription 3
Role : Owner
CSP Azure Subscription 4
Role : Owner
GDAP Azure relationship
Directory Reader
2
GDAP M/D365 relationship
Teams Admin
Power Platform Admin

tecman

QUESTIONS ?

tecman

THANK YOU



CUSTOMER DAY 2023