PowerShell Conference Europe

Introducing Maester: Your Microsoft 365 test automation framework

Fabian Bader

Antwerp24

Many thanks to our sponsors:

Chocolatey

PATCH MY PC

semperis

ScriptRunner®
Your #1 for PowerShell Automation

Fabian Bader

- Cyber Security Architect @ glueckkanja AG
- Azure and Security MVP
- Blog: cloudbrother.info
- Organizer of
  - HH PowerShell UG
  - Purple Elbe Security UG

MVP Microsoft Most Valuable Professional

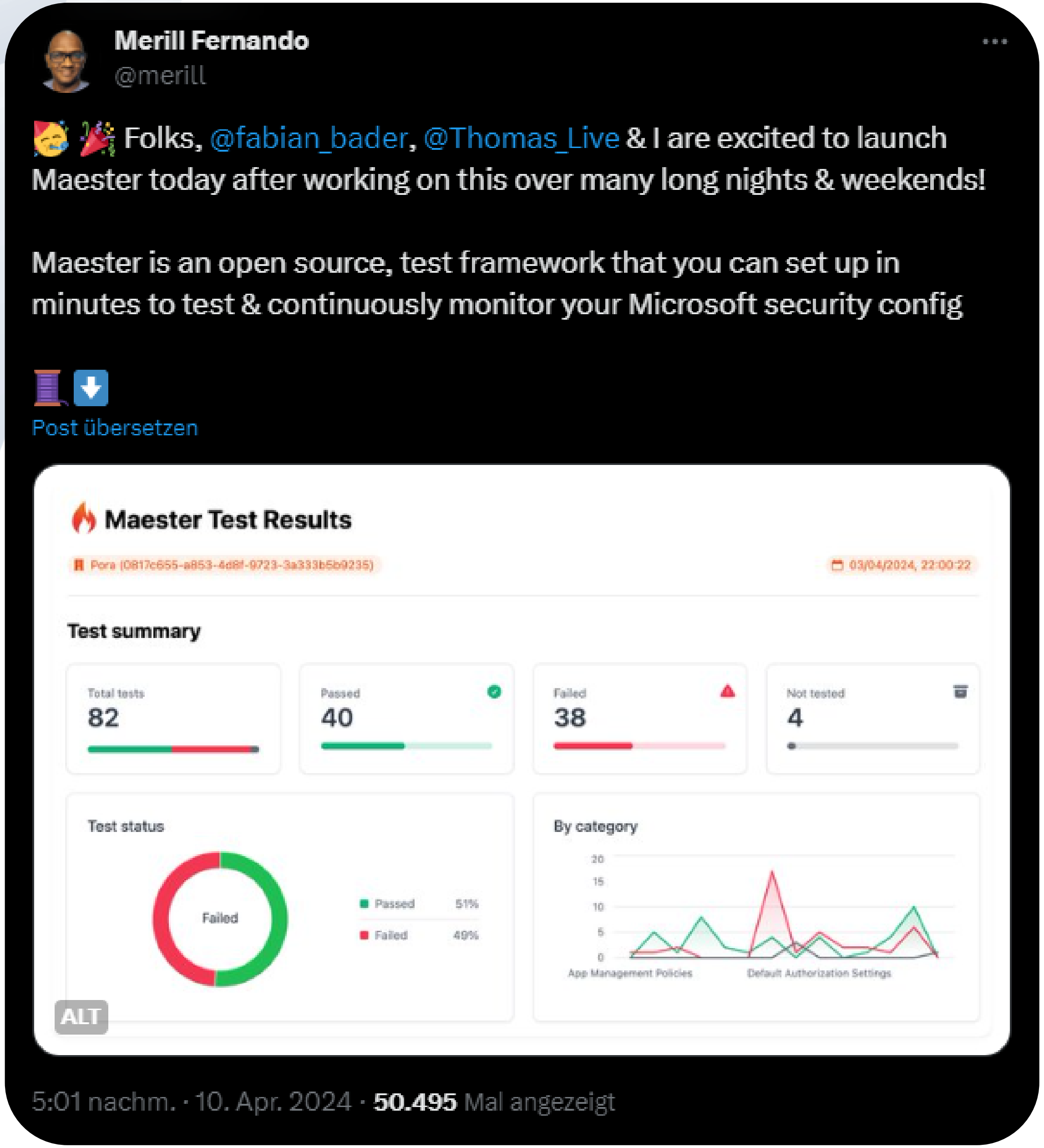
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

Microsoft CERTIFIED IDENTITY AND ACCESS ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED SECURITY OPERATIONS ANALYST ASSOCIATE

@fabian_bader



Merill Fernando
@merill

🥳 🎉 Folks, @fabian_bader, @Thomas_Live & I are excited to launch Maester today after working on this over many long nights & weekends!

Maester is an open source, test framework that you can set up in minutes to test & continuously monitor your Microsoft security config

🧵 ⬇️

Post übersetzen

🔥 Maester Test Results

Pora (0817c655-a853-4d8f-9723-3a333b5b9235)   03/04/2024, 22:00:22

Test summary

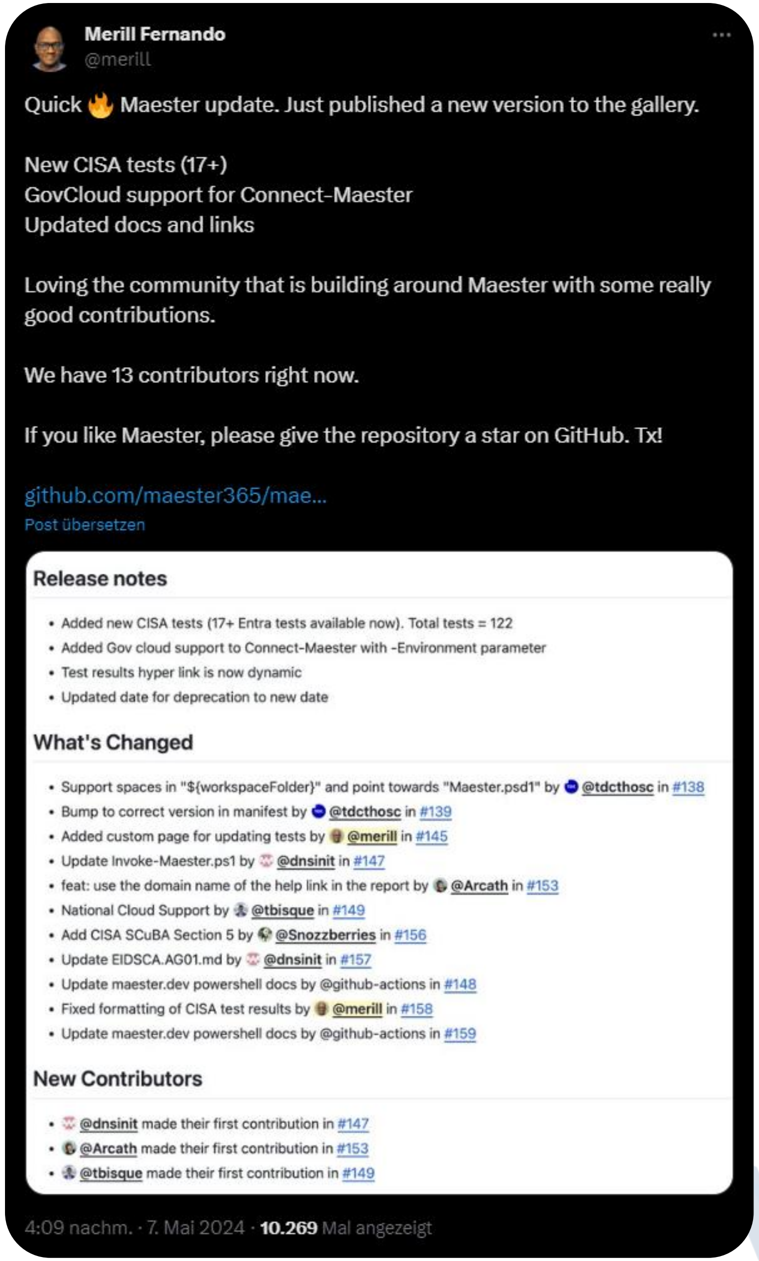
Total tests	Passed	Failed	Not tested
82	40	38	4

Test status

🟩 Passed	51%
🟥 Failed	49%

By category

5:01 nachm. · 10. Apr. 2024 · **50.495** Mal angezeigt



Merill Fernando
@merill

Quick 🔥 Maester update. Just published a new version to the gallery.

New CISA tests (17+)
GovCloud support for Connect-Maester
Updated docs and links

Loving the community that is building around Maester with some really good contributions.

We have 13 contributors right now.

If you like Maester, please give the repository a star on GitHub. Tx!

github.com/maester365/mae...

Post übersetzen

Release notes

- Added new CISA tests (17+ Entra tests available now). Total tests = 122
- Added Gov cloud support to Connect-Maester with -Environment parameter
- Test results hyper link is now dynamic
- Updated date for deprecation to new date

What's Changed

- Support spaces in "${workspaceFolder}" and point towards "Maester.psd1" by @tdcthosc in #138
- Bump to correct version in manifest by @tdcthosc in #139
- Added custom page for updating tests by @merill in #145
- Update Invoke-Maester.ps1 by @dnsinit in #147
- feat: use the domain name of the help link in the report by @Arcath in #153
- National Cloud Support by @tbisque in #149
- Add CISA SCuBA Section 5 by @Snozzberries in #156
- Update EIDSCA.AG01.md by @dnsinit in #157
- Update maester.dev powershell docs by @github-actions in #148
- Fixed formatting of CISA test results by @merill in #158
- Update maester.dev powershell docs by @github-actions in #159

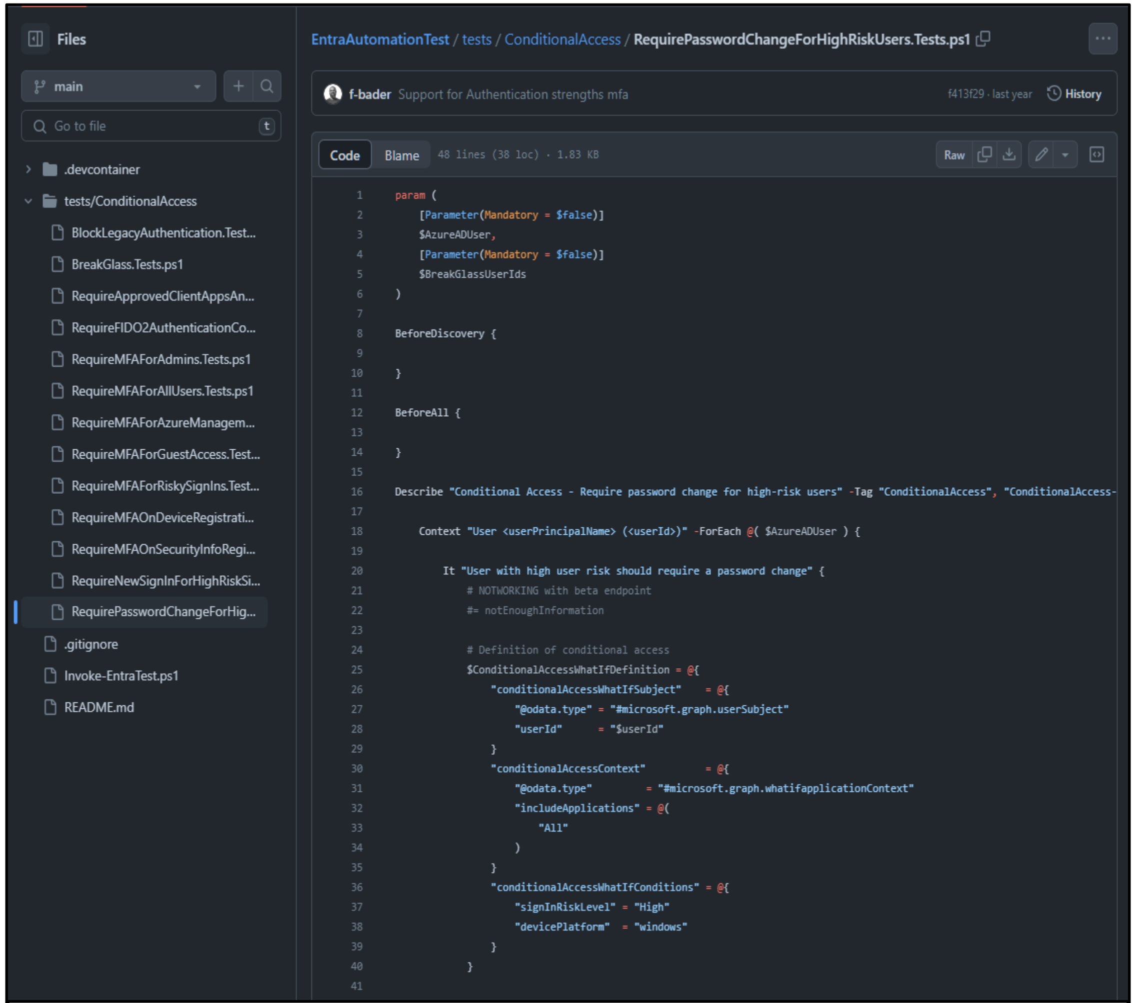
New Contributors

- @dnsinit made their first contribution in #147
- @Arcath made their first contribution in #153
- @tbisque made their first contribution in #149

4:09 nachm. · 7. Mai 2024 · **10.269** Mal angezeigt

PSCONF.EU
Antwerp24

𝕏 @fabian_bader


Files
main
Go to file
t
.devcontainer
tests/ConditionalAccess
BlockLegacyAuthentication.Test...
BreakGlass.Tests.ps1
RequireApprovedClientAppsAn...
RequireFIDO2AuthenticationCo...
RequireMFAForAdmins.Tests.ps1
RequireMFAForAllUsers.Tests.ps1
RequireMFAForAzureManagem...
RequireMFAForGuestAccess.Test...
RequireMFAForRiskySignIns.Test...
RequireMFAOnDeviceRegistrati...
RequireMFAOnSecurityInfoRegi...
RequireNewSignInForHighRiskSi...
RequirePasswordChangeForHig...
.gitignore
Invoke-EntraTest.ps1
README.md
Code
Blame
Raw
History

EntraAutomationTest / tests / ConditionalAccess / RequirePasswordChangeForHighRiskUsers.Tests.ps1

f-bader Support for Authentication strengths mfa f413f29 · last year

48 lines (38 loc) · 1.83 KB

```powershell
param (
    [Parameter(Mandatory = $false)]
    $AzureADUser,
    [Parameter(Mandatory = $false)]
    $BreakGlassUserIds
)

BeforeDiscovery {

}

BeforeAll {

}

Describe "Conditional Access - Require password change for high-risk users" -Tag "ConditionalAccess", "ConditionalAccess-

    Context "User <userPrincipalName> (<userId>)" -ForEach @( $AzureADUser ) {

        It "User with high user risk should require a password change" {
            # NOTWORKING with beta endpoint
            #= notEnoughInformation

            # Definition of conditional access
            $ConditionalAccessWhatIfDefinition = @{
                "conditionalAccessWhatIfSubject"    = @{
                    "@odata.type" = "#microsoft.graph.userSubject"
                    "userId"      = "$userId"
                }
                "conditionalAccessContext"          = @{
                    "@odata.type"         = "#microsoft.graph.whatifapplicationContext"
                    "includeApplications" = @(
                        "All"
                    )
                }
                "conditionalAccessWhatIfConditions" = @{
                    "signInRiskLevel" = "High"
                    "devicePlatform"  = "windows"
                }
            }

```

HOW IT STARTED

@fabian_bader

Best practices for all isolation architectures

Article • 10/23/2023 • 6 contributors

Feedback

In this article

The following are design considerations for all isolation configurations. Throughout this content, there are many links. We link to content, rather than duplicate it here, so you'll always have access to the most up-to-date information.

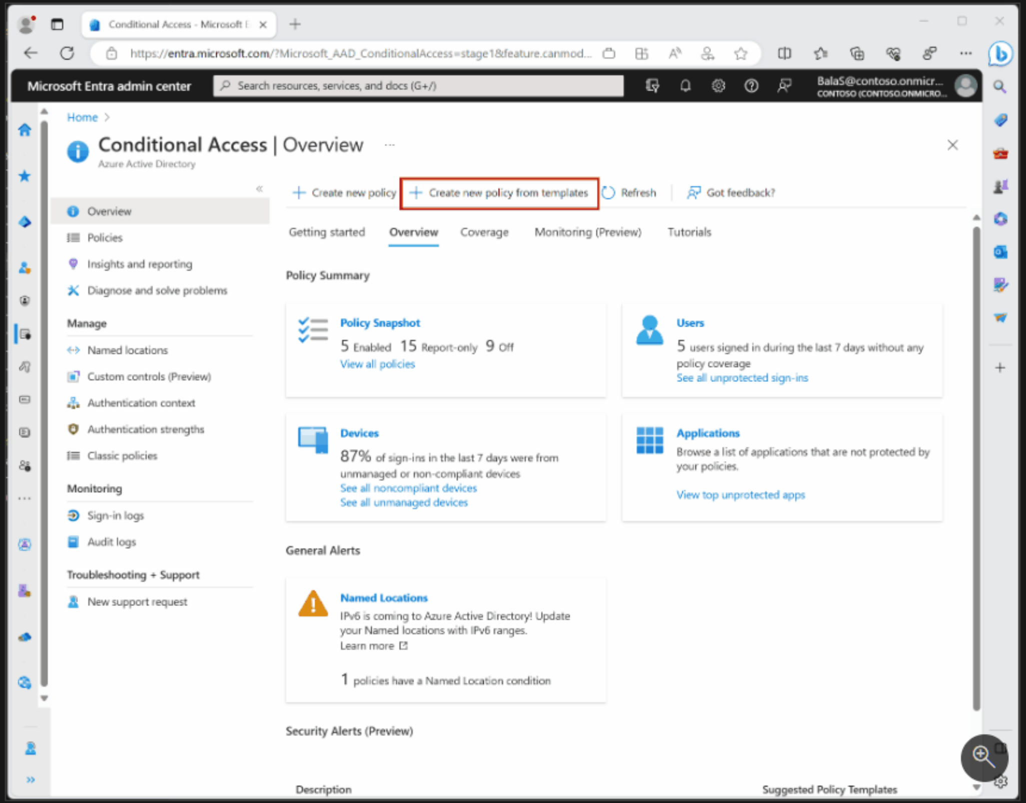
For general guidance on how to configure Microsoft Entra tenants (isolated or not), refer to the Microsoft Entra feature deployment guide.

> **Note**
>
> For all isolated tenants we suggest you use clear and differentiated branding to help avoid human error of working in the wrong tenant.

Isolation security principles

When designing isolated environments, it's important to consider the following principles:

- **Use only modern authentication** - Applications deployed in isolated environments must use claims-based modern authentication (for example, SAML, * Auth, OAuth2, and OpenID Connect) to use capabilities such as federation, Microsoft Entra B2B collaboration, delegation, and the consent framework. This way, legacy applications that have dependency on legacy authentication methods such as NT LAN Manager (NTLM) won't carry forward in isolated environments.
- **Enforce strong authentication** - Strong authentication must always be used when accessing the isolated environment services and infrastructure. Whenever possible, passwordless authentication such as Windows for Business Hello or a FIDO2 security keys should be used.
- **Deploy secure workstations** - Secure workstations provide the mechanism to ensure that the platform and the identity that platform represents is properly attested and secured against exploitation. Two other approaches to consider are:
  - Use Windows 365 Cloud PCs (Cloud PC) with the Microsoft Graph API.
  - Use Conditional Access and filter for devices as a condition.


Conditional Access - Microsoft E
https://entra.microsoft.com/?Microsoft_AAD_ConditionalAccess=stage1&feature.canmod...
Microsoft Entra admin center
Search resources, services, and docs (G+/)
BalaS@contoso.onmicr...
CONTOSO (CONTOSO.ONMICRO...
Home
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Authentication context
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
New support request
Create new policy
Create new policy from templates
Refresh
Got feedback?
Getting started
Overview
Coverage
Monitoring (Preview)
Tutorials

Conditional Access | Overview
Azure Active Directory

Policy Summary

Policy Snapshot
5 Enabled 15 Report-only 9 Off
View all policies

Users
5 users signed in during the last 7 days without any policy coverage
See all unprotected sign-ins

Devices
87% of sign-ins in the last 7 days were from unmanaged or non-compliant devices
See all noncompliant devices
See all unmanaged devices

Applications
Browse a list of applications that are not protected by your policies.
View top unprotected apps

General Alerts

Named Locations
IPv6 is coming to Azure Active Directory! Update your Named locations with IPv6 ranges.
Learn more

1 policies have a Named Location condition

Security Alerts (Preview)

Description | Suggested Policy Templates

Template categories

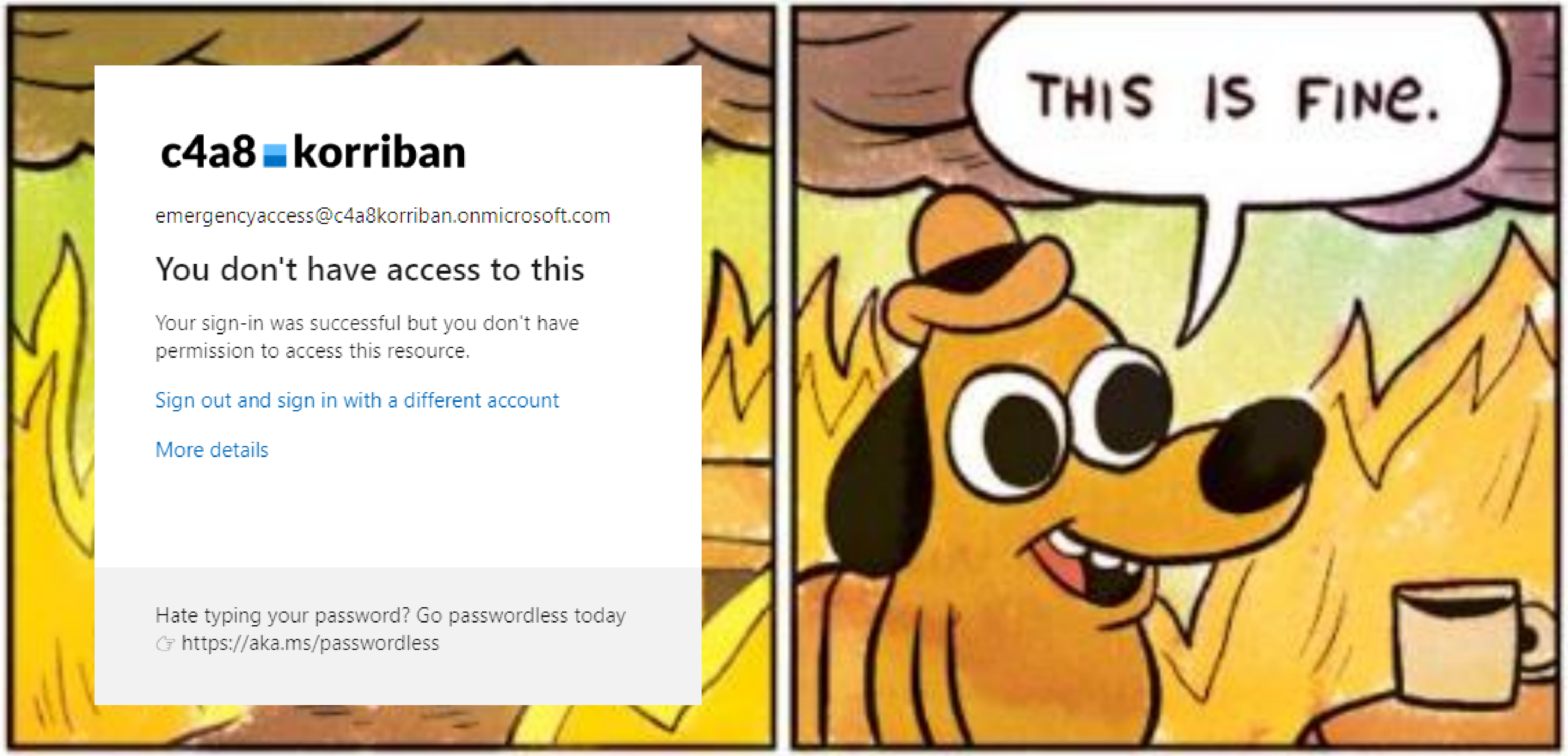
Conditional Access policy templates are organized into the following categories:

Secure foundation | Zero Trust | Remote work | Protect administrator | Emerging threats

Microsoft recommends these policies as the base for all organizations. We recommend these policies be deployed as a group.

- Require multifactor authentication for admins
- Securing security info registration
- Block legacy authentication
- Require multifactor authentication for admins accessing Microsoft admin portals
- Require multifactor authentication for all users
- Require multifactor authentication for Azure management
- Require compliant or Microsoft Entra hybrid joined device or multifactor authentication for all users

Find these templates in the Microsoft Entra admin center > **Protection** > **Conditional Access** > **Create new policy**



c4a8 korriban

emergencyaccess@c4a8korriban.onmicrosoft.com

You don't have access to this

Your sign-in was successful but you don't have permission to access this resource.

Sign out and sign in with a different account

More details

Hate typing your password? Go passwordless today
https://aka.ms/passwordless

Insecure configuration of identity platform

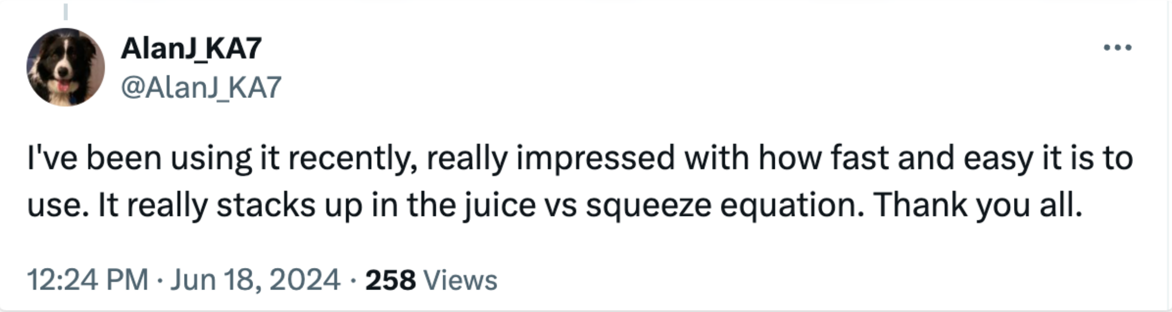
Misconfigurations and exposure of identity platforms and their components are common vectors for attackers to gain unauthorized high-privilege access.

Basic security hygiene still protects against 99% of attacks.

Microsoft Digital Defense Report 2023
aka.ms/mddr

Use cases

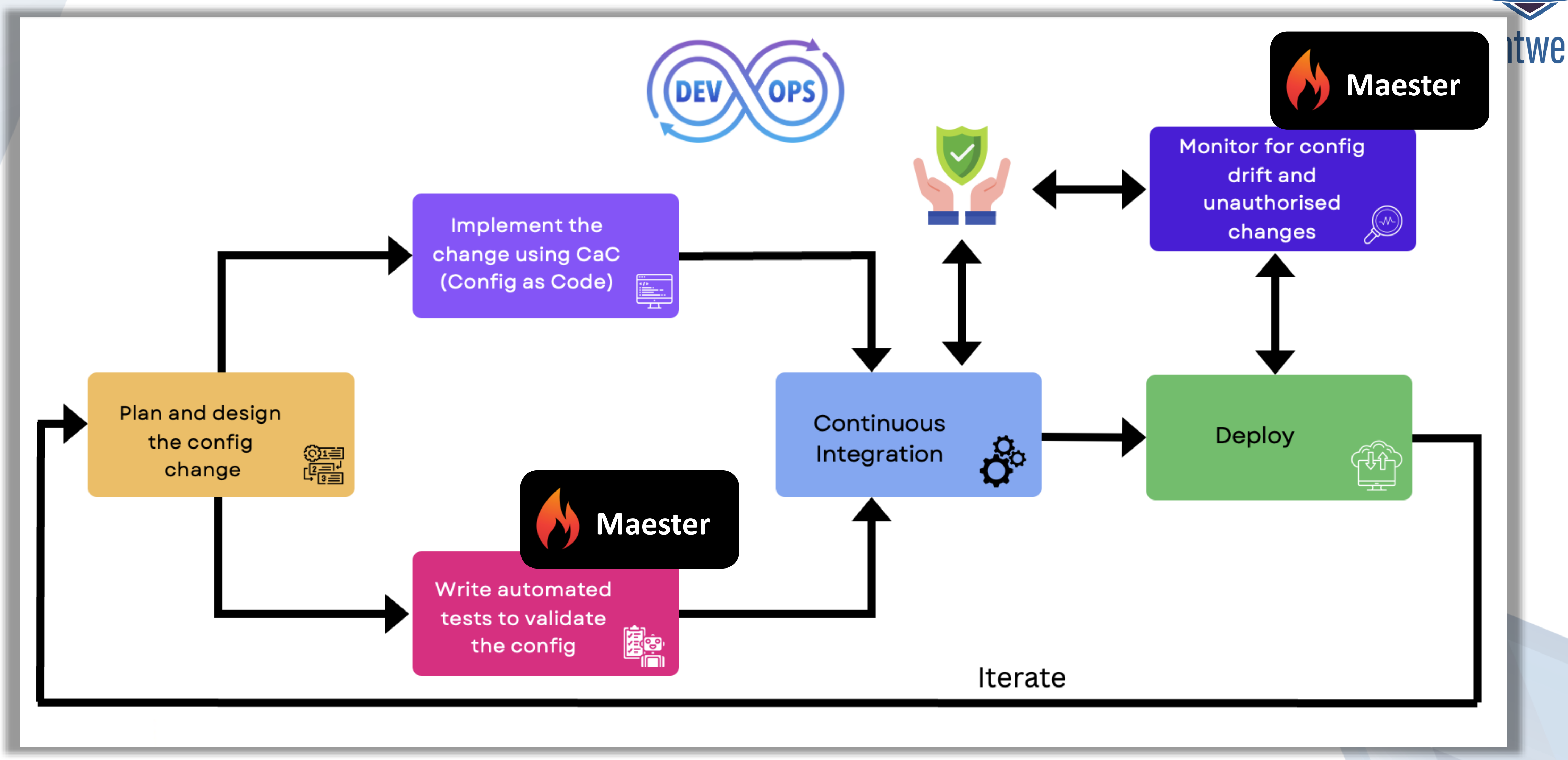
- One off assessment
  - Admins
  - Consultants
  - Custom added tests
- Continuous evaluation using CI/CD
  - IT departments
  - IAM/SecOps/Exchange change monitoring



AlanJ_KA7
@AlanJ_KA7

I've been using it recently, really impressed with how fast and easy it is to use. It really stacks up in the juice vs squeeze equation. Thank you all.

12:24 PM · Jun 18, 2024 · **258** Views

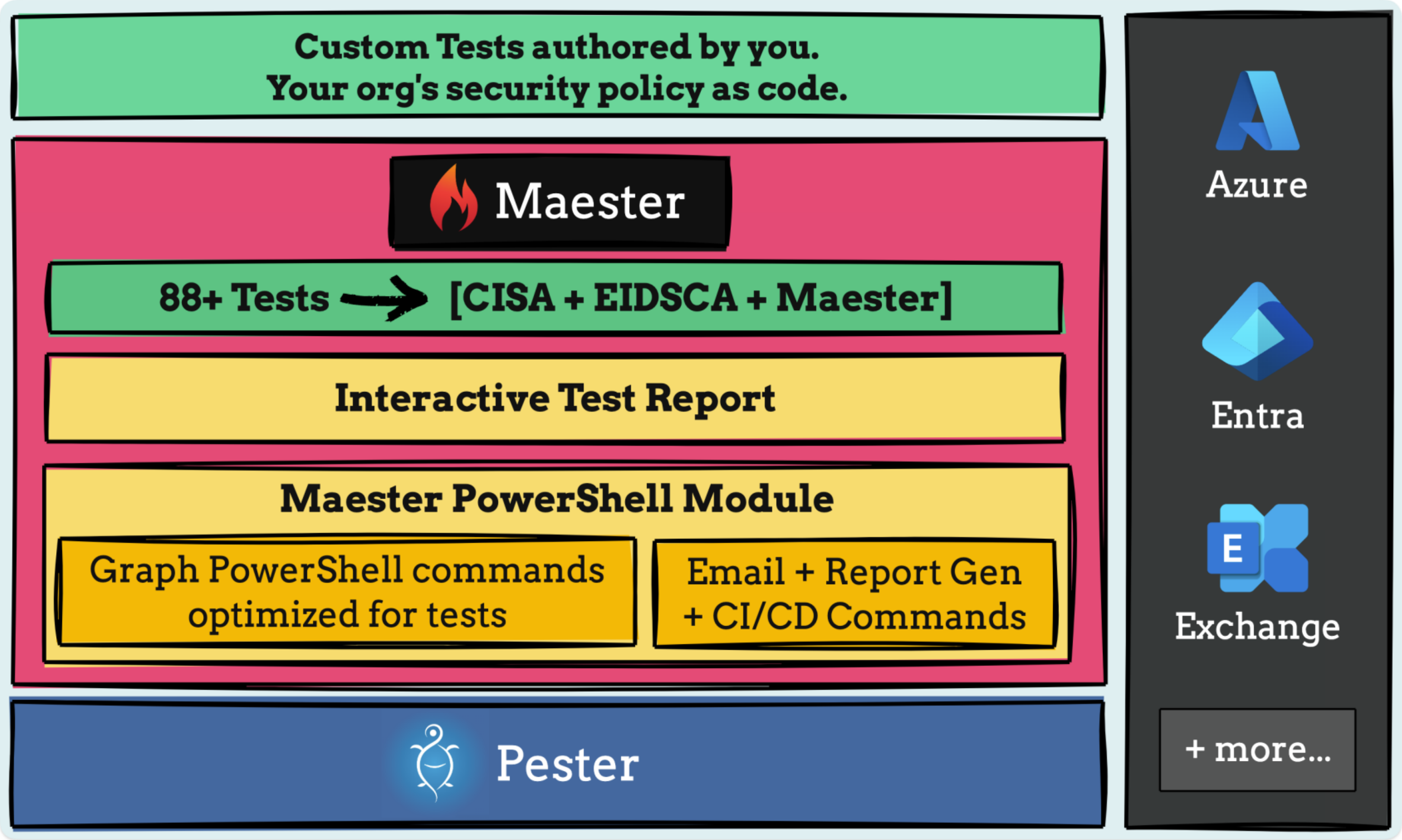


DEV OPS
Maester
Monitor for config drift and unauthorised changes
Implement the change using CaC (Config as Code)
Plan and design the config change
Continuous Integration
Deploy
Maester
Write automated tests to validate the config
Iterate

Demo

Slides are boring…

Maester framework



Custom Tests authored by you.
Your org's security policy as code.

Maester

88+ Tests → [CISA + EIDSCA + Maester]

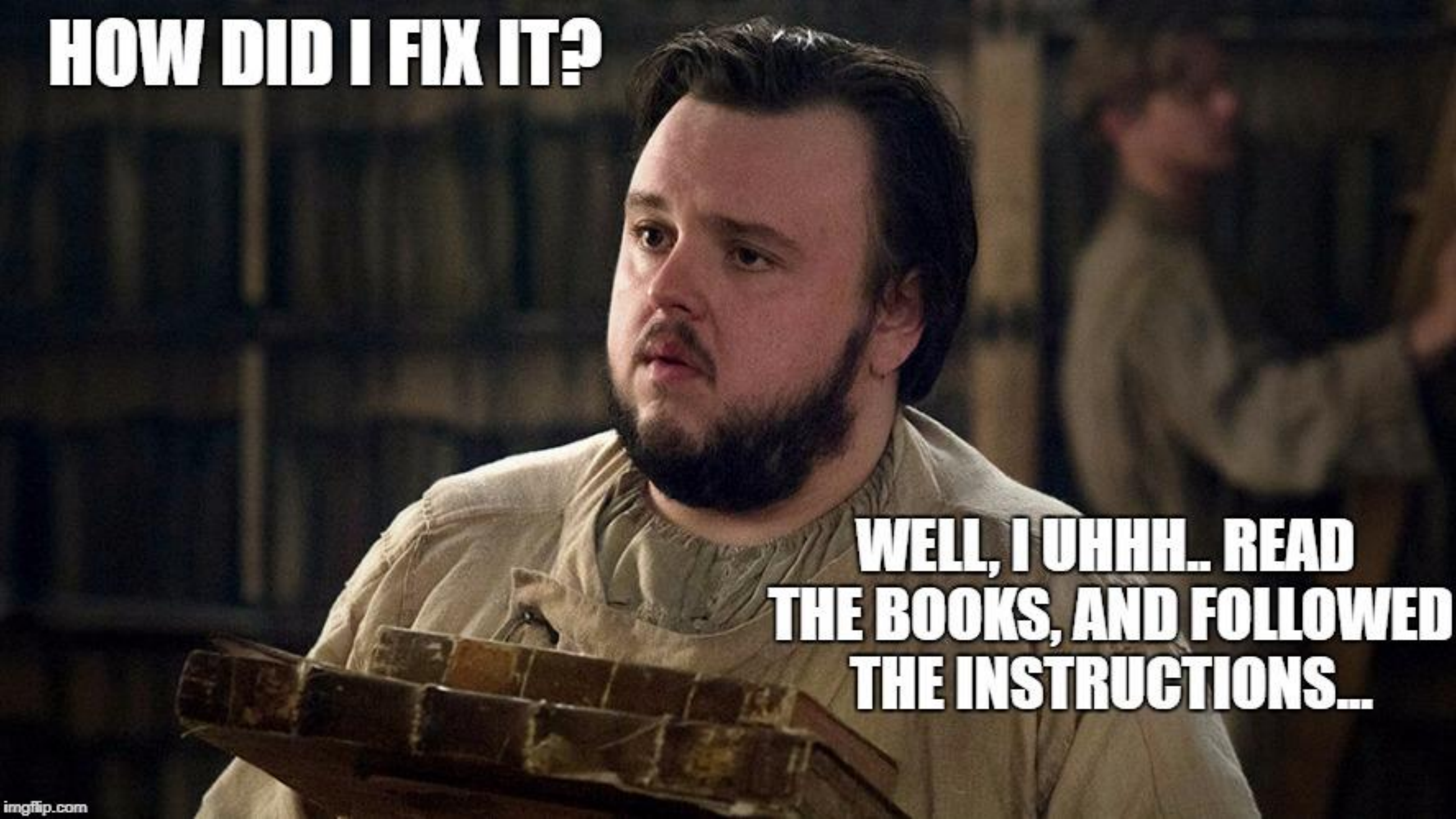
Interactive Test Report

Maester PowerShell Module

Graph PowerShell commands optimized for tests

Email + Report Gen + CI/CD Commands

Pester


HOW DID I FIX IT?
WELL, I UHHH.. READ THE BOOKS, AND FOLLOWED THE INSTRUCTIONS...

But why a “new” testing framework?

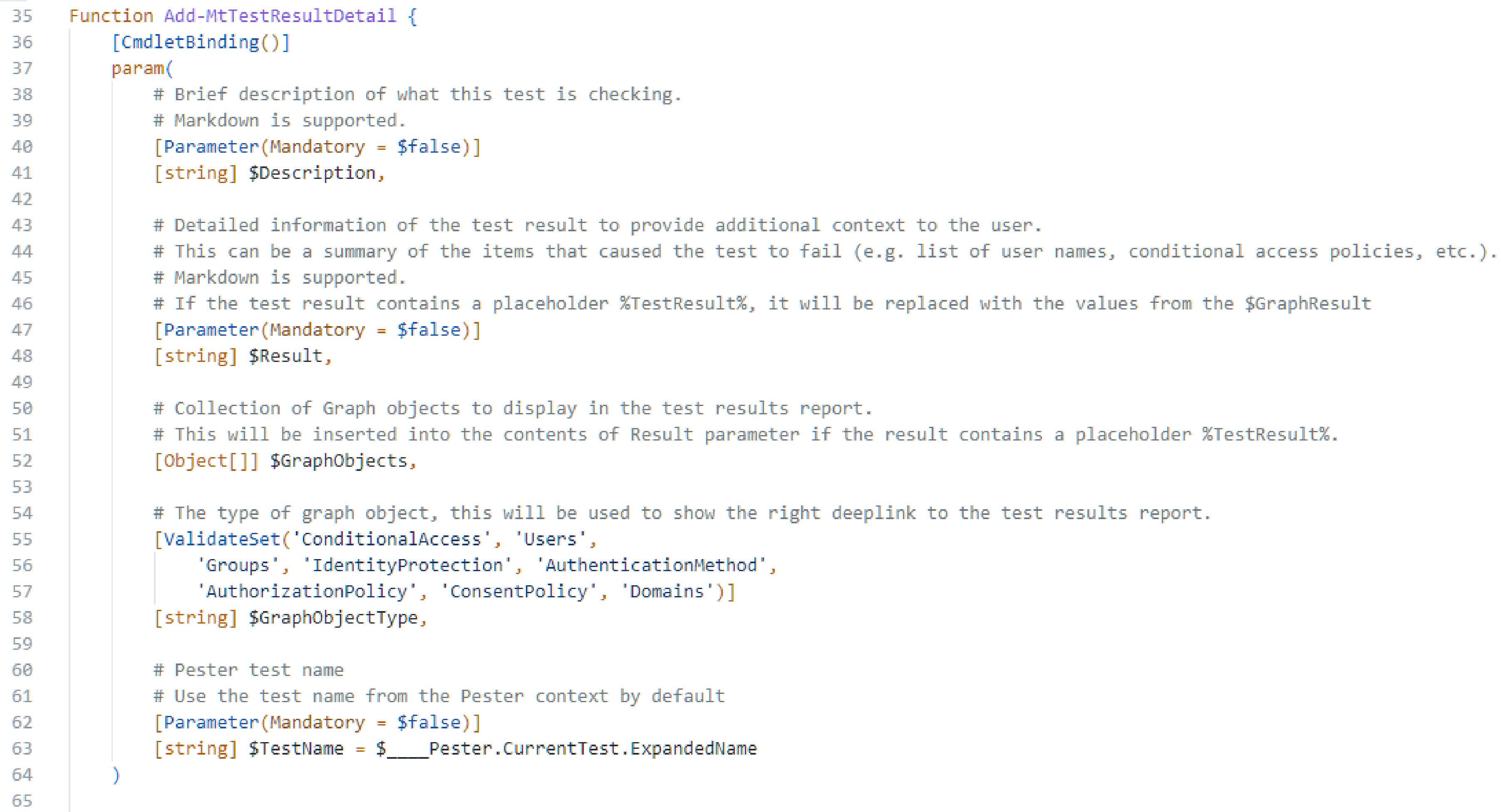
- Pester is the core for maester

- All tests are written in Pester

Explain it like a Maester

- Maester tests include
  - Detailed descriptions of the tests
  - Help to guide you how to fix it
- Maester tests can be consumed
  - As HTML report
  - As CI/CD pipeline output
  - As email

How we did it?



```
Function Add-MtTestResultDetail {
    [CmdletBinding()]
    param(
        # Brief description of what this test is checking.
        # Markdown is supported.
        [Parameter(Mandatory = $false)]
        [string] $Description,

        # Detailed information of the test result to provide additional context to the user.
        # This can be a summary of the items that caused the test to fail (e.g. list of user names, conditional access policies, etc.).
        # Markdown is supported.
        # If the test result contains a placeholder %TestResult%, it will be replaced with the values from the $GraphResult
        [Parameter(Mandatory = $false)]
        [string] $Result,

        # Collection of Graph objects to display in the test results report.
        # This will be inserted into the contents of Result parameter if the result contains a placeholder %TestResult%.
        [Object[]] $GraphObjects,

        # The type of graph object, this will be used to show the right deeplink to the test results report.
        [ValidateSet('ConditionalAccess', 'Users',
            'Groups', 'IdentityProtection', 'AuthenticationMethod',
            'AuthorizationPolicy', 'ConsentPolicy', 'Domains')]
        [string] $GraphObjectType,

        # Pester test name
        # Use the test name from the Pester context by default
        [Parameter(Mandatory = $false)]
        [string] $TestName = $____Pester.CurrentTest.ExpandedName
    )

```

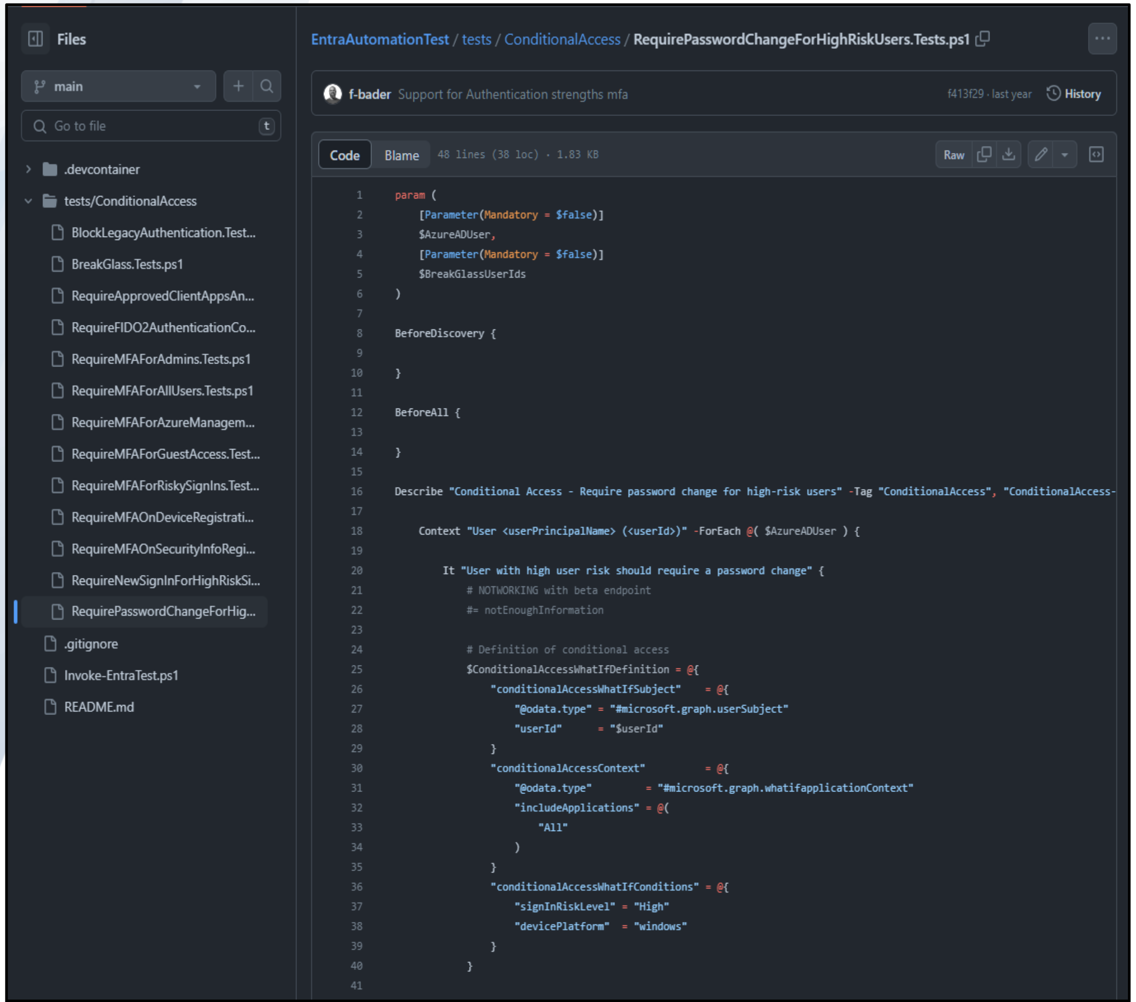
Demo

Slides are boring…

PSCONF.EU Antwerp24

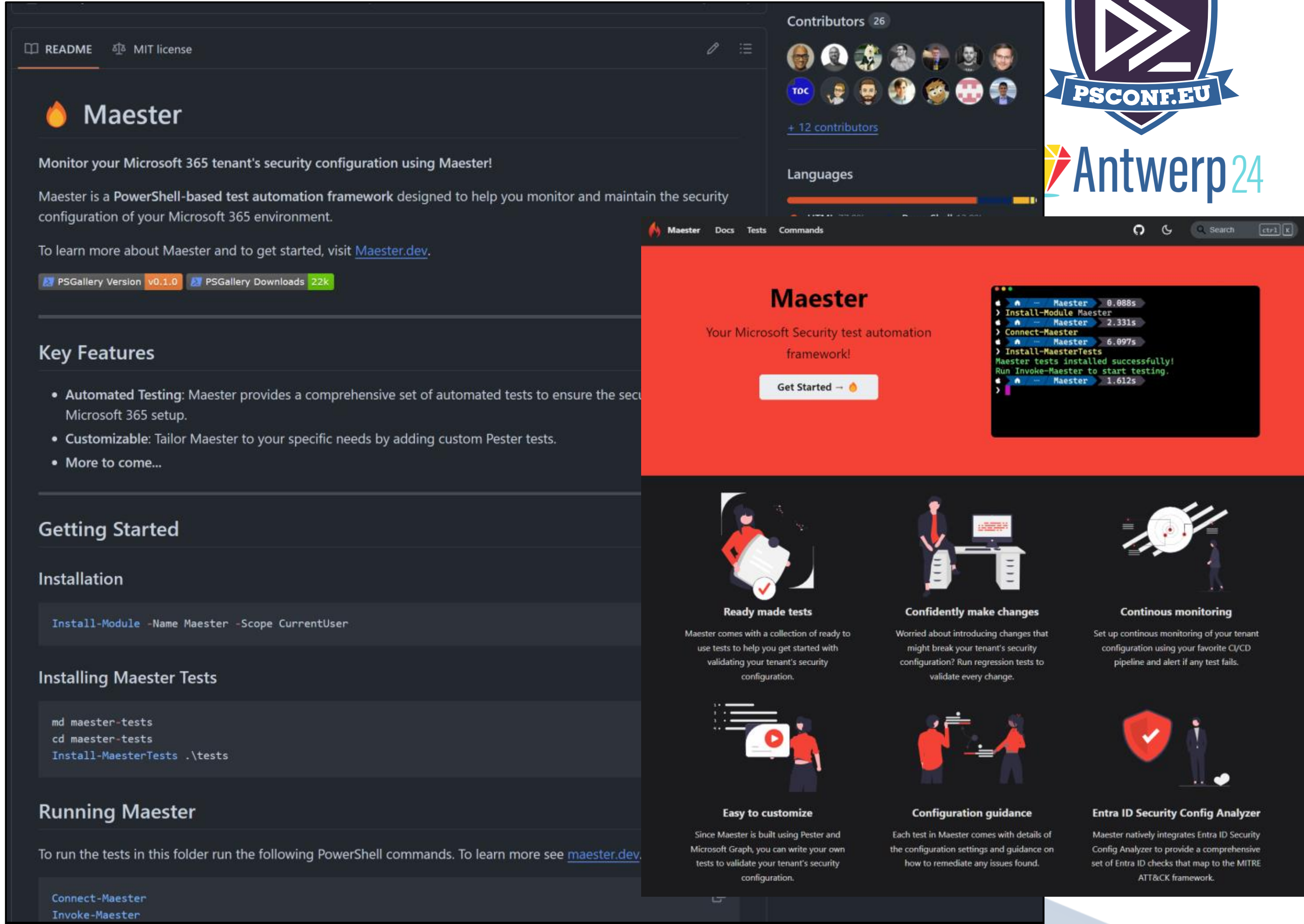
@fabian_bader

PSCONF.EU
Antwerp24


Files
main
Go to file
.devcontainer
tests/ConditionalAccess
BlockLegacyAuthentication.Test...
BreakGlass.Tests.ps1
RequireApprovedClientAppsAn...
RequireFIDO2AuthenticationCo...
RequireMFAForAdmins.Tests.ps1
RequireMFAForAllUsers.Tests.ps1
RequireMFAForAzureManagem...
RequireMFAForGuestAccess.Test...
RequireMFAForRiskySignIns.Test...
RequireMFAOnDeviceRegistrati...
RequireMFAOnSecurityInfoRegi...
RequireNewSignInForHighRiskSi...
RequirePasswordChangeForHig...
.gitignore
Invoke-EntraTest.ps1
README.md
EntraAutomationTest / tests / ConditionalAccess / RequirePasswordChangeForHighRiskUsers.Tests.ps1
f-bader Support for Authentication strengths mfa
f413f29 · last year
History
Code
Blame
48 lines (38 loc) · 1.83 KB
Raw

```powershell
param (
    [Parameter(Mandatory = $false)]
    $AzureADUser,
    [Parameter(Mandatory = $false)]
    $BreakGlassUserIds
)

BeforeDiscovery {

}

BeforeAll {

}

Describe "Conditional Access - Require password change for high-risk users" -Tag "ConditionalAccess", "ConditionalAccess-

    Context "User <userPrincipalName> (<userId>)" -ForEach @( $AzureADUser ) {

        It "User with high user risk should require a password change" {
            # NOTWORKING with beta endpoint
            #= notEnoughInformation

            # Definition of conditional access
            $ConditionalAccessWhatIfDefinition = @{
                "conditionalAccessWhatIfSubject"    = @{
                    "@odata.type" = "#microsoft.graph.userSubject"
                    "userId"      = "$userId"
                }
                "conditionalAccessContext"          = @{
                    "@odata.type"         = "#microsoft.graph.whatifapplicationContext"
                    "includeApplications" = @(
                        "All"
                    )
                }
                "conditionalAccessWhatIfConditions" = @{
                    "signInRiskLevel" = "High"
                    "devicePlatform"  = "windows"
                }
            }

```

HOW IT STARTED



Maester

Monitor your Microsoft 365 tenant's security configuration using Maester!

Maester is a **PowerShell-based test automation framework** designed to help you monitor and maintain the security configuration of your Microsoft 365 environment.

To learn more about Maester and to get started, visit Maester.dev.

PSGallery Version v0.1.0 PSGallery Downloads 22k

Key Features

- **Automated Testing**: Maester provides a comprehensive set of automated tests to ensure the secu Microsoft 365 setup.
- **Customizable**: Tailor Maester to your specific needs by adding custom Pester tests.
- More to come...

Getting Started

Installation

```
Install-Module -Name Maester -Scope CurrentUser
```

Installing Maester Tests

```
md maester-tests
cd maester-tests
Install-MaesterTests .\tests
```

Running Maester

To run the tests in this folder run the following PowerShell commands. To learn more see maester.dev.

```
Connect-Maester
Invoke-Maester
```

Maester

Your Microsoft Security test automation framework!

Get Started →

```
 ⌂ ··· Maester  0.088s
❯ Install-Module Maester
 ⌂ ··· Maester  2.331s
❯ Connect-Maester
 ⌂ ··· Maester  6.097s
❯ Install-MaesterTests
Maester tests installed successfully!
Run Invoke-Maester to start testing.
 ⌂ ··· Maester  1.612s
❯
```

Ready made tests

Maester comes with a collection of ready to use tests to help you get started with validating your tenant's security configuration.

Confidently make changes

Worried about introducing changes that might break your tenant's security configuration? Run regression tests to validate every change.

Continous monitoring

Set up continous monitoring of your tenant configuration using your favorite CI/CD pipeline and alert if any test fails.

Easy to customize

Since Maester is built using Pester and Microsoft Graph, you can write your own tests to validate your tenant's security configuration.

Configuration guidance

Each test in Maester comes with details of the configuration settings and guidance on how to remediate any issues found.

Entra ID Security Config Analyzer

Maester natively integrates Entra ID Security Config Analyzer to provide a comprehensive set of Entra ID checks that map to the MITRE ATT&CK framework.

HOW ITS GOING

@fabian_bader

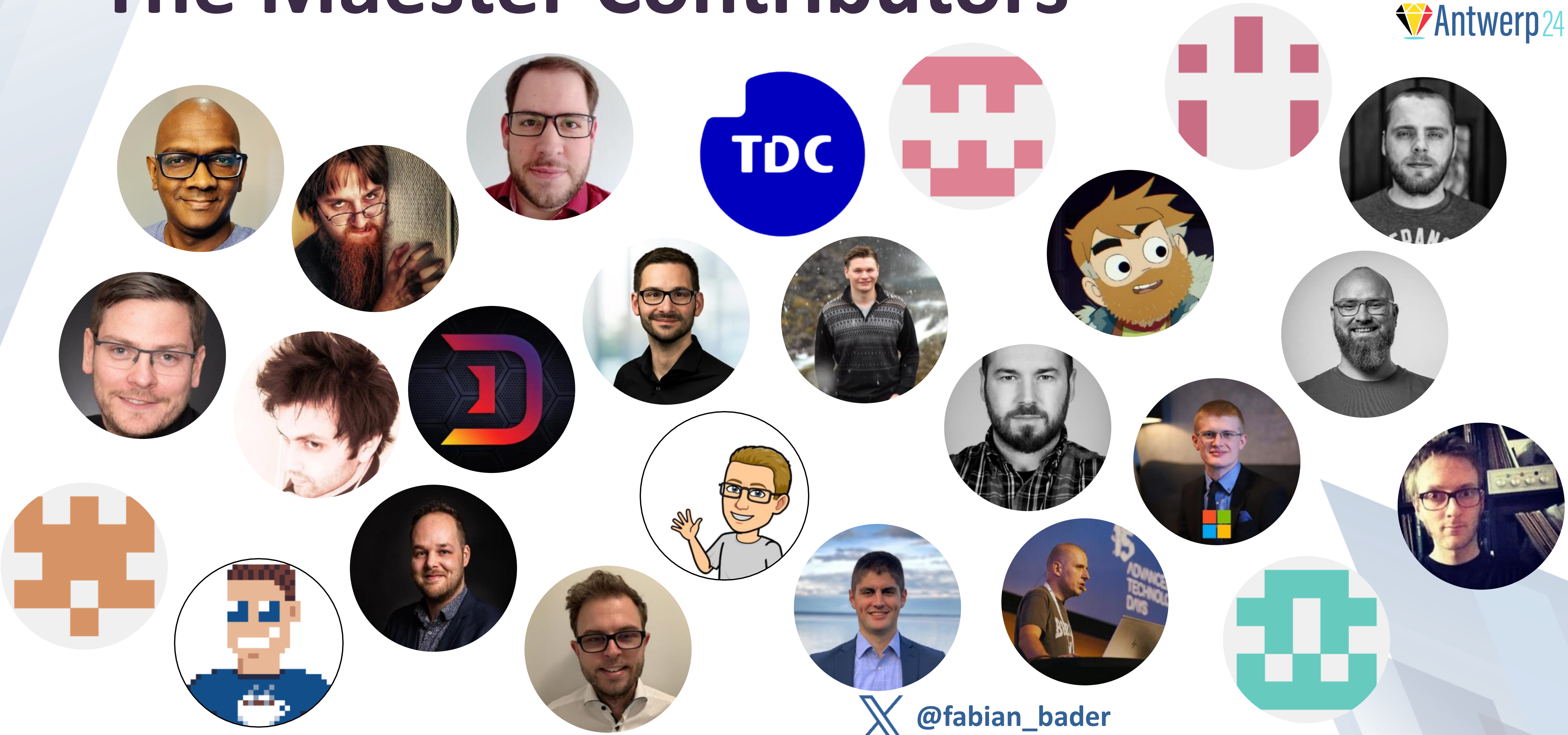
The Maester Core Team

Merill Fernando
Microsoft PM
@merill

Thomas Naunheim
Microsoft MVP
@Thomas_Live

Fabian Bader
Microsoft MVP
@fabian_bader

The Maester Contributors



@fabian_bader

We need your help!

- Updating docs/markdown including adding links to admin portals to resolve issues
- Writing new tests (CISA, Exchange, Intune...)
- Writing automated scripts that can help fix issues
- any other ideas you have to contribute...

Q&A

15 minutes

PSCONF.EU Antwerp24

@fabian_bader