Experts Live US

Securing The Defaults

Building and maintaining your security baseline

Chris Goosen
cgoosen.me

Thank you to our Sponsors!

Platinum Sponsors

BlueVoyant

protiviti®

xillio
liberate. innovate. elevate.

Rimo3

eSHARE

TANIUM™

Silver & Event Sponsors

PORTUNUSTECH

Microsoft®

run events

Feedback, Prizes & After-Party

Run.Events App

Download the app: https://run.events/app

Fill in the feedback form

- You need to add the session to the favorite
- Only available when the session is over can you provide feedback

Join us for Chance to win a prize from 4 – 4:30pm in the Central Park West room

- You must fill out at least one feedback form to enter the prize draw
- You need to be present at the end of the day to win!

Join us at **Beer Authority** just after **5pm** for drinks, snacks and networking!

Support STEM Kids NYC

Experts Live US is proud to support STEM Kids NYC and all the great work they do bringing STEM programming to children and local schools in New York!

All proceeds from this event go to supporting STEM Kids NYC!

Join us during the closing remarks to meet their founder and hear about this great organization!

STEM Kids NYC

Dream it. Code it. Make it.

Get-SpeakerInfo

- Secure Modern Work Consultant - Arinco
- Based in Sydney, Australia
- Cloud Security / Microsoft 365 Apps & Services MVP
- Co-host of df3ndr.io / thearchitects.cloud podcasts
- My socials: cgoosen.me

Microsoft® Most Valuable Professional

Find us on your preferred podcast platform or at **https://df3ndr.io**

Get-SessionInfo

- Introduction
- Why are we here?
- Security Baseline Lifecycle
- Understanding your current posture
- Establishing a security baseline
- Applying controls
- Continuously tracking security posture
- Demos, code and fun stuff
- Continuously maturing your operations

"Most users don't go in and change things. They just assume someone smarter than them chose the settings that are best for them..."

"The tyranny of the default" - Steve Gibson

Why are we here?

Microsoft 365 defaults promote productivity, not security - these goals don't always align. Many breaches don't start with a sophisticated zero-day - they start because something was left open by default, misconfigured, or never hardened.

Baseline Security ≠ Threat Actor Defense

Baseline security: *inherent risk* from configuration, complexity, and human error

Threat actor defense: *active risk* from malicious external adversaries.

Why are we here?

Microsoft 365 settings convenient by default, but risky by design:

Microsoft 365 Admin Center

- External sharing of calendars
- Idle session timeout for Web Apps
- User owned apps and services

SharePoint Admin Center

- OneDrive content sharing
- SharePoint external sharing
- OneDrive/SharePoint link sharing

Entra Admin Center

- Users can register applications
- ‘Stay signed in?’ option
- User consent for applications
- External collaboration settings

Teams Admin Center

- External domain collaboration
- Communication with unmanaged users
- Anonymous users in meetings

Security Baseline Lifecycle

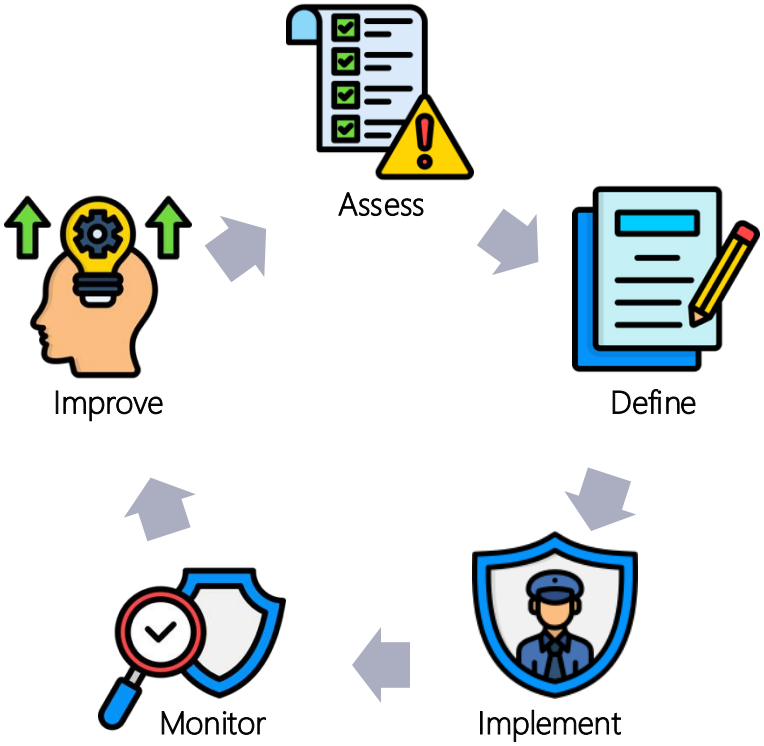
Assess – Understand your current posture

Define – Establising a baseline

Implement – Apply controls

Monitor – Continuously track security posture

Improve – Continuously mature your operations



Assess – Understand your current posture

Frameworks

- NIST Cybersecurity Framework (CSF)
  https://www.nist.gov/cyberframework
- CIS Controls
  https://www.cisecurity.org/controls
- ISO/IEC 27001
  https://www.iso.org/standard/27001
- ASD Essential Eight
  https://www.cyber.gov.au/
- Microsoft Secure Score
  https://security.microsoft.com/securescore

Tools

- Monkey365
  Frameworks/Controls: CIS
  https://silverhack.github.io/monkey365/
- ScubaGear
  Frameworks/Controls: CISA
  https://github.com/cisagov/ScubaGear
- Maester
  Frameworks/Controls: CISA, CIS, Custom
  https://maester.dev

Define – Establishing a baseline

The **Define** step is about moving from “what good looks like” (frameworks) to “what’s non-negotiable in our Microsoft 365 tenant” (baseline)

Famework Requirement

Baseline Definition

Technical Control

This is where the magic starts - it rarely feels magical!

Define – Establising a baseline

- Understand Business & Compliance Requirements
- Map to Framework
- Define Scope & Boundaries
- Don’t forget about Process
- Define Ownership & Accountability
- Create Baseline Documentation

Tip: Write down what you want to achieve, not just the technical setting/toggle.

Control Objective: “All administrative access must require MFA.”

Control Implementation:

- Entra Conditional Access policy requiring MFA for Admin Roles
- Entra PIM for Admin Roles

Process Implementation:

- Admin Role Lifecycle Management
- Access Reviews

Define – Establising a baseline

Sample Security Baseline Catalog for Microsoft 365

Framework Control	Baseline Definition	Implementation
CIS Control 6.3 – Require MFA for all users	All accounts (admins, users, service accounts) must use MFA, with phishing-resistant methods preferred. Exceptions must be formally approved.	• Conditional Access "Require MFA" for all users • Conditional Access "Require MFA" for all Admin roles • Block legacy authentication
NIST CSF PR.AC-4 – Access permissions are managed	All privileged accounts are just-in-time, reviewed quarterly, and must use PIM. No standing global admin access allowed.	• Entra ID Privileged Identity Management (PIM) • RBAC enforcement for workloads • Review access logs quarterly
ISO 27001 A.9.4.2 – Secure log-on procedures	Strong authentication must be enforced for all user logins to corporate resources.	• Entra ID sign-in risk policies • Require compliant devices • Disable "Stay Signed In"
NIST CSF DE.CM-7 – Monitoring for unauthorized use	Audit logs must be retained for at least 90 days and reviewed weekly; alerts generated for anomalous admin activity.	• Unified Audit Log is enabled • Defender for Cloud Apps anomalous activity policies • Azure Monitor / Sentinel alerting on admin events
NIST CSF PR.DS-5 – Protection of data-at-rest	Sensitive data must be labeled, encrypted, and governed by DLP policies.	• Purview Information Protection sensitivity labels • DLP for Teams, SharePoint, Exchange

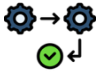
Implement – Apply controls

The **Implement** step is where the planning becomes real - It's critical to make sure both technical controls and process controls are considered

Technical Controls

- CIS Benchmarks
  https://www.cisecurity.org/cis-benchmarks
- Microsoft Secure Score
  https://security.microsoft.com/securescore

Processes



- User and Admin Lifecycle Management
- Access Requests/Reviews
- App Registration/Consent Requests
- Monitoring, etc.

Implement – Apply controls

CIS Benchmark Example

Audit:

To audi

1. N
2. C
3. Ir
4. V

y

To audi

1. C
2. R

Get-Sha

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com.
2. Click to expand `Settings` select `Org settings`.
3. In the `Services` section click `Calendar`.
4. Uncheck `Let your users share their calendars with people outside of your organization who have Office 365 or Exchange`.
5. Click `Save`.

To remediate using PowerShell:

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Run the following Exchange Online PowerShell command:

```
Set-SharingPolicy -Identity "Default Sharing Policy" -Enabled $False
```

Default Value:

Enabled (True)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/admin/manage/share-calendars-with-external-users?view=o365-worldwide

Monitor – Continuously track posture

The **Monitor** step is about making sure your security baseline doesn't become "set and forget." It's where you continuously evaluate your Microsoft 365 security posture, detect deviations, and generate actionable insights.

What to monitor

- Security baseline deviations
- Entra ID sign-ins, risky users, risky sign-ins
- Endpoint compliance and risk signals
- Insider risk signals
- Alerts - DLP, Email hygiene, etc.

How to monitor

- Monkey365 / ScubaGear / Maester
- Microsoft 365 Defender portal
- Microsoft Purview Compliance Manager
- Azure Automation / Power Platform
- Microsoft Graph, KQL, etc..

Demo

Continuous Evaluation PoC

Demo – Continuous Evaluation PoC

Demo building blocks:

- Azure Storage Account
- Azure Automation Account
- PowerShell Runtime Environment
- 2 x PowerShell Runbooks
- Maester (PowerShell Module)
  https://maester.dev/
- MaesterDiff (PowerShell Script)
  https://rksolutions.nl/maesterdiff-because-comparing-maesters-just-got-twice-as-fun/

Tip: Download the code here: https://github.com/cgoosen/ELDemo25

Improve – Continuously mature

The **Improve** step is where the feedback loop closes - after monitoring your Microsoft 365 baseline, this step ensures that lessons learned, new threats, and evolving business needs feed back into your security program

- Analyze Monitoring Insights
- Review Incidents & Lessons Learned
- Stay Current with Threat Intelligence & Guidance
- Optimize User Experience & Business Fit
- Update & Expand the Baseline
- Maturity & Automation Improvements

Please evaluate this session in the App.

THANK YOU

Are there any questions?