

Protecting Your Users Against Phishing Attacks

Peter Schmidt

MVP: Office Apps & Services

MCM: Exchange, MCSM: Exchange, MCT

Twitter: @petsch

Massive Thanks to Our Sponsors!

Gold Partner



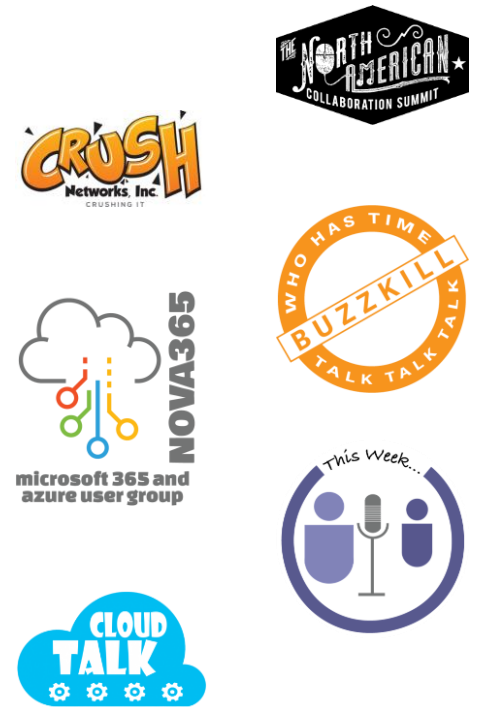
Silver Partners



M365 Chicago is an OTSN Conference



Community Partners



[Chicago Power Platform Users Group](#)
[M365 Friday Cabo San Lucas](#)

Donate
Today!



<https://otsn.live/M365CHI-CFFDonation>



Please join M365 Chicago in supporting Chicago Public Schools through the Children First Fund

As the Chicago Public Schools Foundation, the Children First Fund works to promote equity in education. Chicago Public Schools is the third largest school district in the country. We know that talent is equally distributed among our 355,000 CPS students--but opportunity and resources are not. We wake up every day on a mission to improve the lives and futures of CPS students.



**Children
First Fund**

The Chicago Public Schools Foundation

@ChiFirstFund

ChildrenFirstFund.org

Peter Schmidt

- **Cloud & Messaging Architect**
- MVP: Office Apps & Services
- MCM: Exchange, MCSM: Exchange, MCT
- Blog: www.msdigest.net
- Twitter: @petsch
- Business e-mail: peter@neoconsulting.dk



Agenda

- Intro
- Spoofing & Phishing
- SPF / DKIM / DMARC
- Defender for Office 365
- DEMO
- Summary



What Are We Talking About?

Phish

- The fraudulent attempt to obtain sensitive information

Spoofing

- Creation of email messages with a forged sender address

Impersonation

- Common technique in targeted phishing attacks

Authentication

- A way to prove the sender really is the sender

SPF

- Sender Policy Framework

DKIM

- DomainKeys Identified Mail

DMARC

- Domain Message Authentication Reporting & Conformance

Types of Phishing



CLONE PHISHING

CLONE PHISHING IS WHERE A LEGITIMATE, AND PREVIOUSLY DELIVERED, BIT OF ONLINE CORRESPONDENCE IS USED TO CREATE AN ALMOST IDENTICAL OR "CLONE" EMAIL.



SPEAR PHISHING

SPEAR PHISHING IS A PHISHING ATTEMPT DIRECTED AT A PARTICULAR INDIVIDUAL OR COMPANY.



WHALING

WHALING IS A PHISHING ATTEMPT DIRECTED SPECIFICALLY AT A SENIOR EXECUTIVE OR ANOTHER HIGH-PROFILE TARGET WITHIN A BUSINESS.

Phishing Insights

- Most common disguises:
 - Bill / invoice (15.9%)
 - Email delivery failure (15.3%)
 - Legal / law enforcement (13.2%)
 - Scanned document (11.5%)
 - Package delivery (3.9%)
- The most common malicious attachment types:
 - Office
 - Archive
 - PDF



What is the issue ?



SMTP has always, by default, been anonymous



You can easily send an email pretending it came from someone else



“Proper” use of this include outsourced marketing and mailing lists



Its difficult to implement this well and the perceived complexity means that companies worry their email will get blocked if they implement it badly

How Do We Authenticate Emails We Receive

SPF

- `v=spf1 ip4:1.2.5.5 ip4:8.2.7.4 ip4:7.3.2.2 ip4:5.5.1.8 include:_spf.salesforce.com include:spf.protection.outlook.com -all`

DKIM

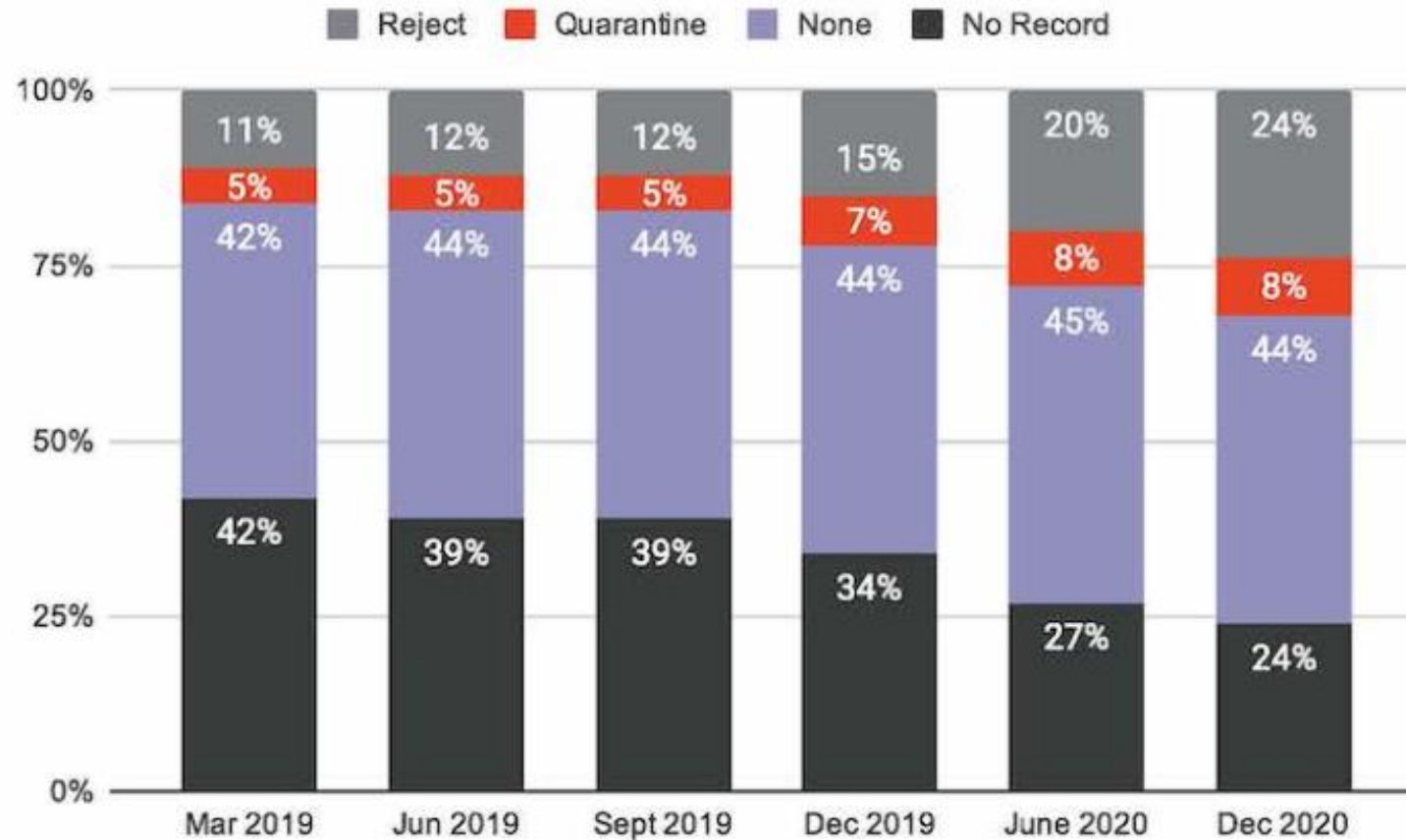
- `"v=DKIM1; p=MIGfMA0GDQEBgQCrZ6z ... 6UvqP3QIDAQAB"`

DMARC

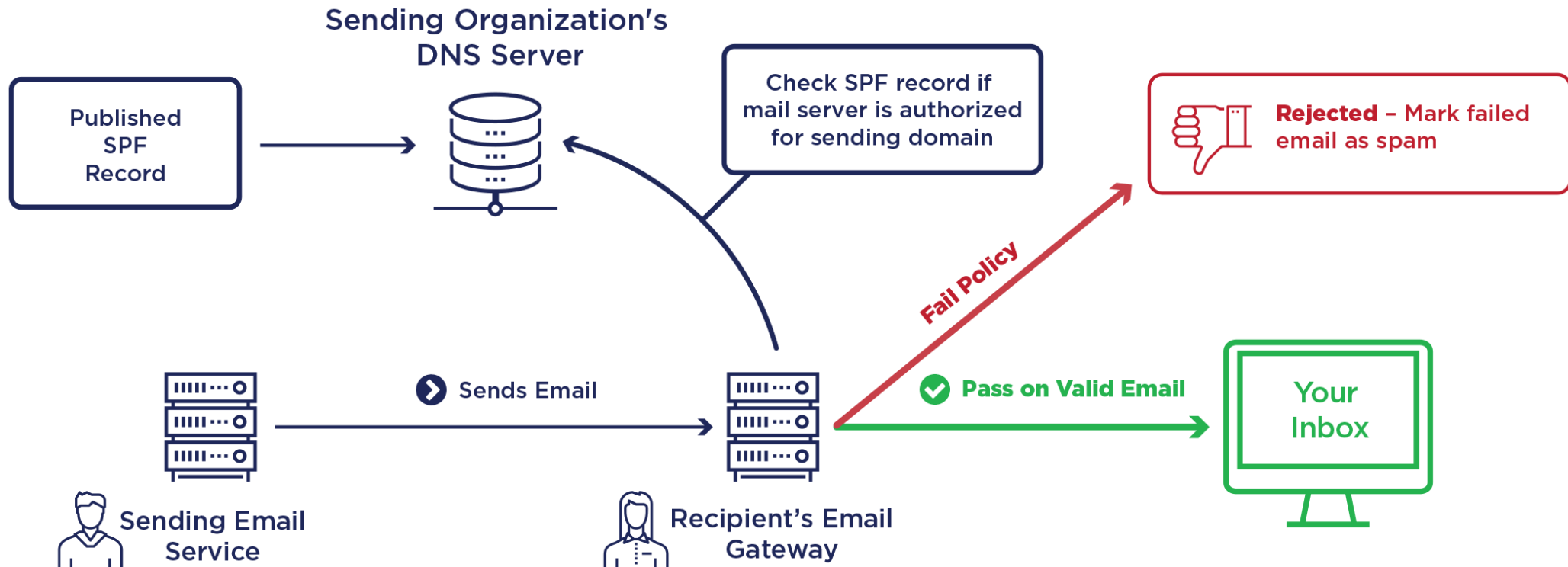
- `v=DMARC1; p=reject; rua=mailto:dmarc@dmarc-aggregator.com; ruf=mailto:dmarc-ruf@dmarc-aggregator.com`

To send email to Microsoft (i.e. to an Office 365 user or Outlook.com) then you need to implement this to stop your email being marked as spam

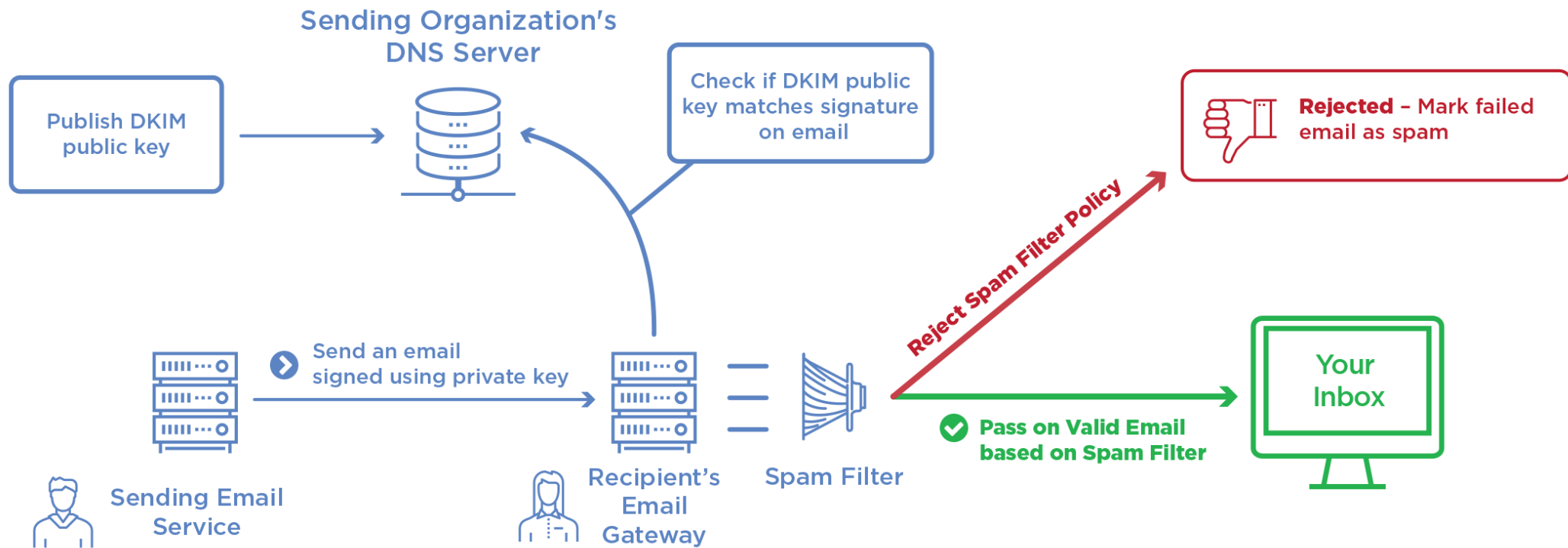
DMARC Policies of Fortune 500 Companies



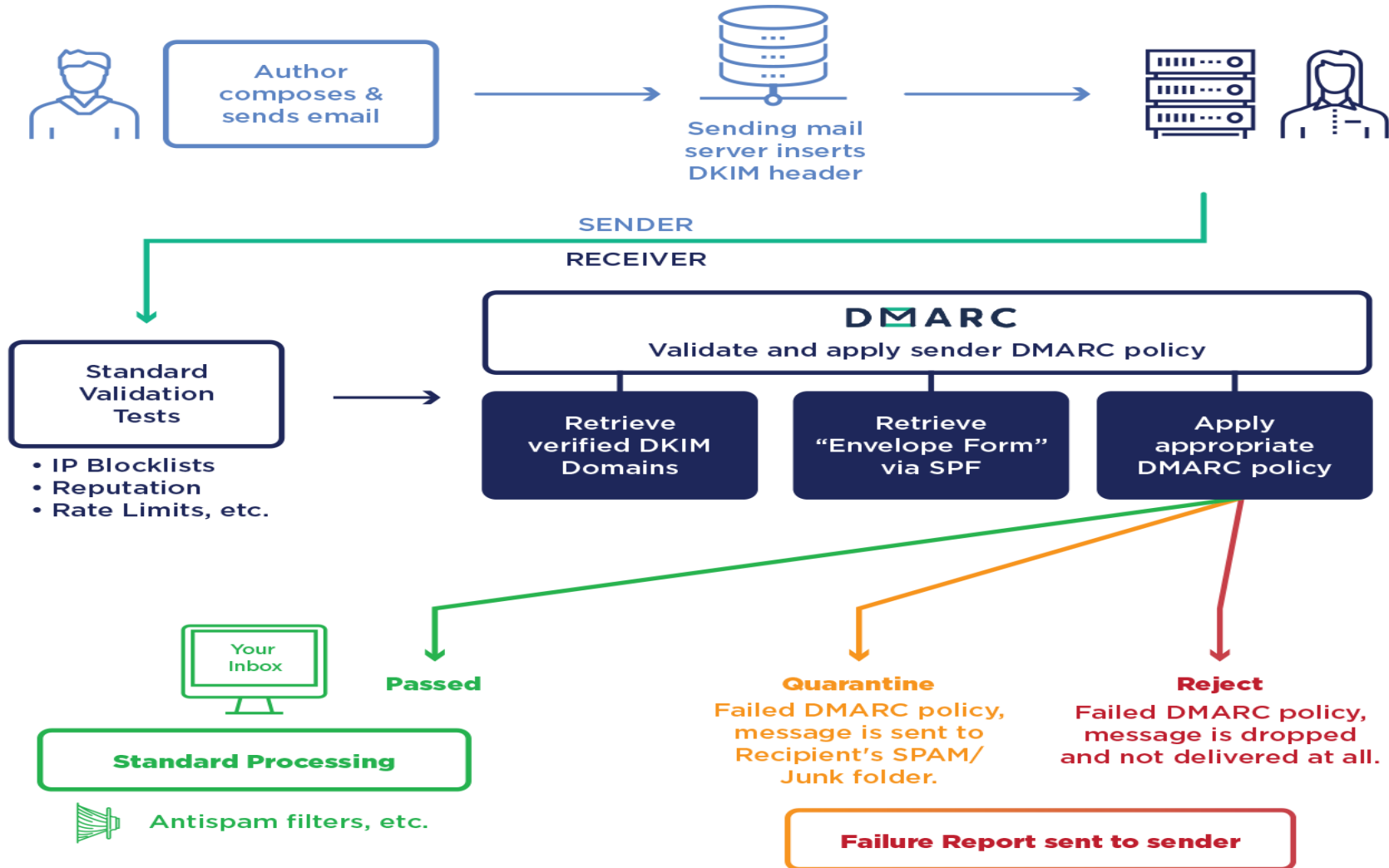
Sender Policy Framework (SPF)



DKIM



DMARC



Microsoft Defender for Office 365 (MDO)



Exchange Online Protection

Preventing broad and volume-based & known attacks



MDO P1

Protects email and collaboration from zero-day malware, phish, and business email compromise



MDO P2

Adds post-breach investigation, hunting, and response, as well as automation, and simulation (for training)

Microsoft Defender for Office 365

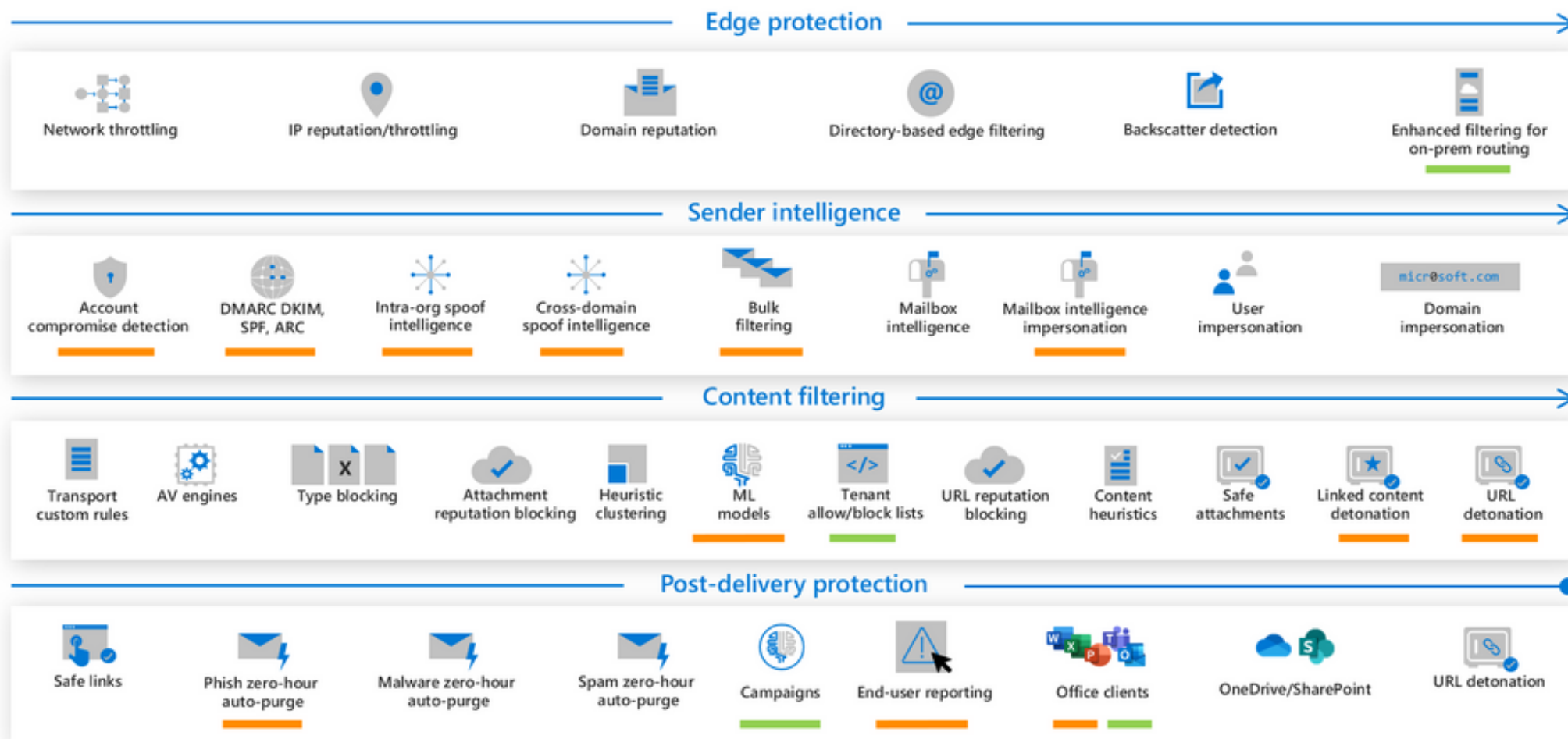
- Microsoft is positioned as a leader in The Forrester Wave™: Enterprise Email Security, Q2 2021
- Microsoft Defender for Office 365 received the highest possible score in the incident response, threat intelligence, and endpoint and endpoint detection and response (EDR) solutions integration criteria, as well as in the product strategy, customer success, and performance and operations criteria.



Defender for Office 365 Protection Stack

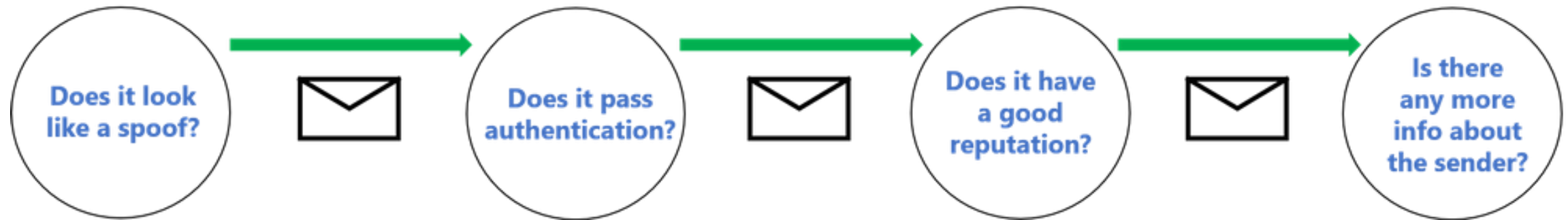
Multi-Layered protection stack

Updated
New



Anti-Spoofing in Exchange Online

Exchange Online Protection (EOP) Anti-Spoofing Capabilities



Defender for Office 365

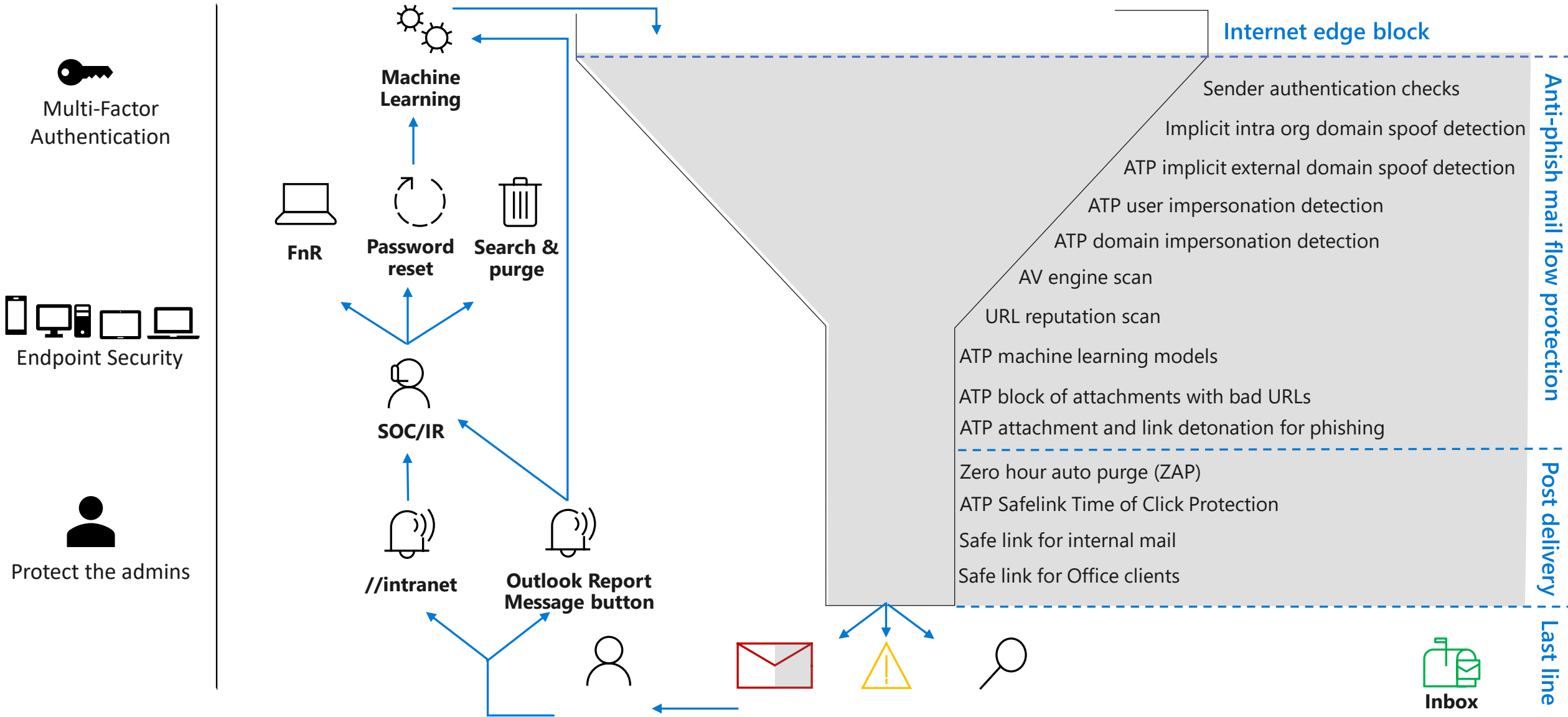
Composite Authentication (compauth) – aka Machine Learning

- MDO and EOP Anti-Spoof Protection. Microsoft using the power of the cloud to determine if spoofed email
- Default Anti-Phish Policy
- Additional Policies

How To Configure

- In the Office 365 Security
- Via PowerShell

Phishing protection end-to-end



Microsoft Defender for Office 365 Recommended Configuration Analyzer Report

Version 1.10.6

This report details any tenant configuration changes recommended within your tenant.

Recommendations

19

OK

42

64 %

Configuration Health Index

The configuration health index is a weighted value representing your configuration. Not all configuration is considered and some configuration is weighted higher than others. The index is represented as a percentage. How the configuration impacts the configuration health index is shown next to the recommendation in the report below as a positive or negative number. The impact to your security posture is a large consideration factor when rating the configuration.

Configuration Analyzer

- Threat Policies – Configuration Analyzer
- Office 365 Advanced Threat Protection Recommended Configuration Analyzer (ORCA)
- Install in PowerShell using:
 - Install-Module -Name ORCA

This all sounds hard - how to get started

- SPF, DKIM
- DMARC
- Office 365
 - Anti-Spoof
 - Anti-Phishing
 - Report Add-in
 - Configuration Analyzer

The screenshot shows the Microsoft AppSource interface. At the top, there's a navigation bar with the Microsoft logo and links for Cloud, Mobility, and Productivity. Below this is a blue header with 'AppSource', 'Apps', 'Consulting Services', and 'List on AppSource'. The main content area is divided into two columns. The left column has a 'Products' section with links for Web Apps, Add-Ins, Dynamics 365, Office 365, Power BI apps, Power BI visuals, and Dynamics NAV. Below this is a 'Categories' section with a list of checkboxes for various business functions like Analytics, Artificial intelligence, Collaboration, etc. The right column features a 'Report Message' app card. It includes a 'Report Message' button with a close icon, the app title 'Report Message', its developer 'Microsoft Corporation Outlook', a description 'Submit missed phishing, spam, and false positive e-mails to Microsoft.', a 4.5-star rating from 121 reviews, and a 'Free' price tag. At the bottom of the card are 'Get it now' and a heart icon. To the right of the app card is a link 'View consulting services' and a 'Report Bee' app card with a bee icon, developer 'Report Bee', description 'Generate customised report cards & view dashboard of students', and a 'Contact' button.

Microsoft Cloud Mobility Productivity

AppSource Apps Consulting Services List on AppSource

Products

Web Apps

Add-Ins

Dynamics 365

Office 365

Power BI apps

Power BI visuals

Dynamics NAV

Categories

- ☐ Analytics
- ☐ Artificial intelligence
- ☐ Collaboration
- ☐ Customer service
- ☐ Finance
- ☐ Human resources
- ☐ IT + administration
- ☐ Internet of things
- ☐ Marketing
- ☐ Operations + supply ...

Report Message

By Microsoft Corporation Outlook

Submit missed phishing, spam, and false positive e-mails to Microsoft.

★★★★★ (121)

Free

Get it now

View consulting services

Report Bee

By Report Bee Web apps

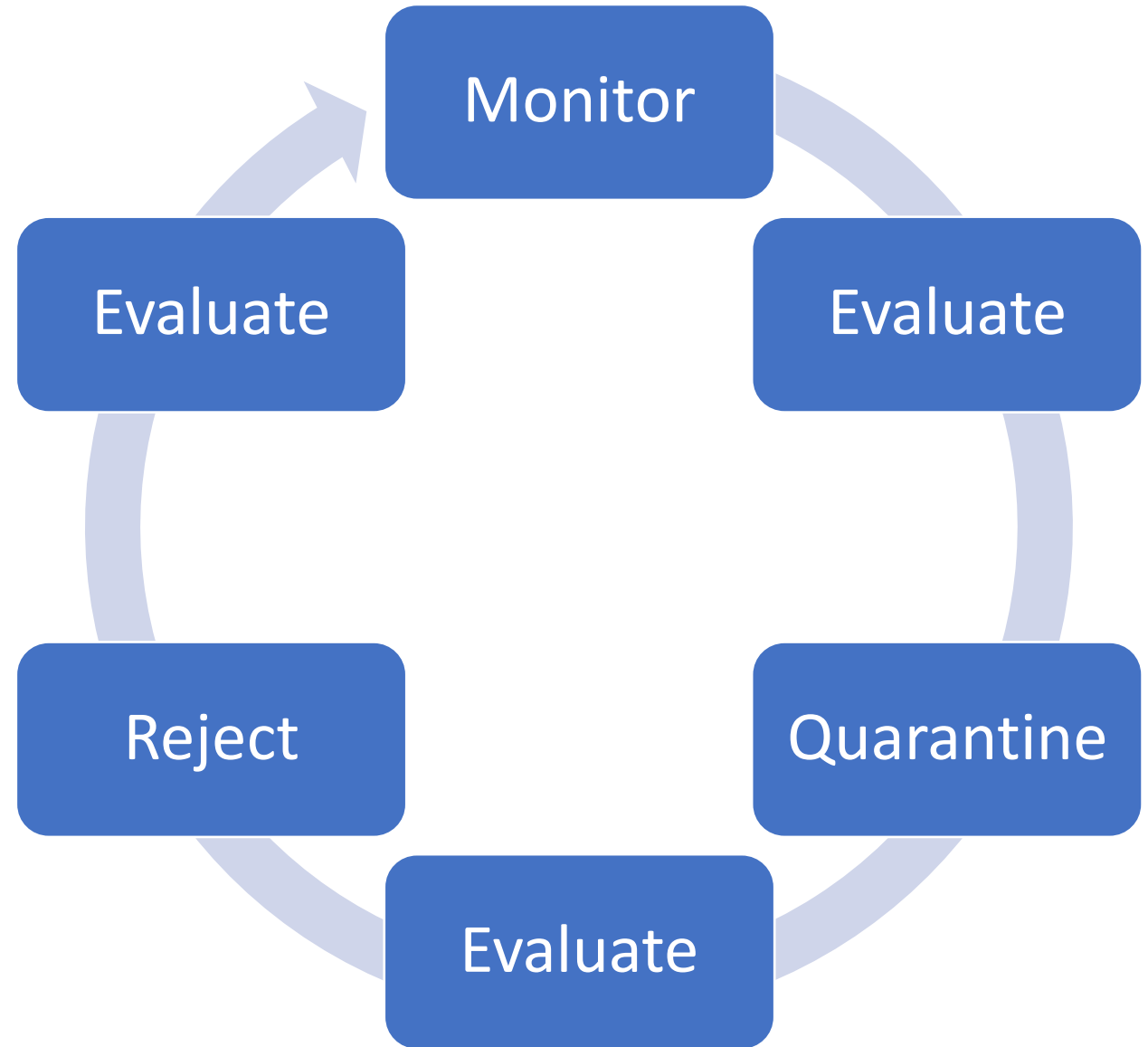
Generate customised report cards & view dashboard of students

Contact

- Let's have a look at:
 - SPF
 - DKIM
 - DMARC
- MDO Impersonation
- MDO Configuration
- Report Message

DEMO

Implementing DMARC in phases

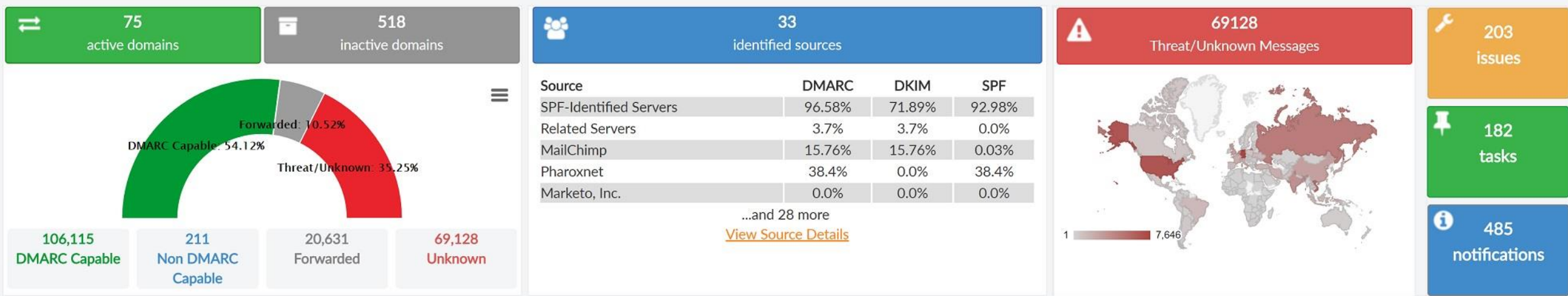


DMARC Analyzers

- Reporting and Analyzer tool for overview
- Some of the tools available:
 - DmarcAnalyzer
 - www.dmarcanalyzer.com
 - PostMarkApp
 - <https://dmarc.postmarkapp.com>
 - EasyDmarc
 - <https://easydmarc.com/>
 - MXToolbox
 - <https://mxtoolbox.com/dmarcsetup>
 - Dmarcian
 - www.dmarcian.com
 - ValiMail
 - <https://www.valimail.com/office-365-free-dmarc-monitoring/>

DMARC Report Example

Domain Overview



Q Domain Discovery

Domain Groups

Click cells for details.

0 Selected

Select Action

Go

export all as CSV

add a domain group

reorder groups

+ Add Domains

Turn Off Domain Discovery

Domain Group

Issues (0)

Tasks (0)

Group Management

No domains have been added to this group. Add domains with this form, or select domains and move them into this group

Add Domains:

Add Domain(s)

User Awareness



Simulations

- ✓ Construct mails that match the level of sophistication that is trending in the wild.
- ✓ Data is your best friend. Use exercise results to determine your next move.
- ✓ Might as well test “the system” while you’re at it!



Training

- ✓ Leverage large scale training programs for in-depth education.
- ✓ Phishing isn’t just an email thing - include guidance on attack vectors such as “Smishing” and “Vishing”.
- ✓ Keep the conversation going through ongoing awareness campaigns.



Reporting

- ✓ What’s your 911? Make sure your community knows when and how to report.
- ✓ Make reporting as quick and easy as possible.
- ✓ Use reporting trends to inform program needs.

Best Practices

- Architectural design of your mail flow and domains
- Use both SPF and DKIM
- Use DMARC authorization record
- Do this for all your domains
- Common mistakes:
 - DMARC needs SPF and DKIM to succeed
- Follow-up on DMARC Reports and Reports in Office 365
- Microsoft Office Defender for 365
 - Phishing
 - ORCA reports



SPF

Best Practice

-
- Simple SPF: v=spf1
include:spf.protection.outlook.com -all
 - More Advanced SPF:
 - **neoconsulting.dk:**
v=sf1 include:spf-internal.neoconsulting.dk
include:spf-external.neoconsulting.dk -all
 - **spf-internal.neoconsulting.dk:**
v=spf1 include:spf.protection.outlook.com
ip4:37.123.123.4 ip4:37.123.123.5 -all
 - **spf-external.neoconsulting.dk:**
v=spf1 include:sendgrid.net a:c.spf.service-
now.com -all



How Can We Protect Our Users ?

- MDO features
 - MDO for Safe Links and Safe Attachments
 - Anti-Phishing Features
 - Attack Simulator and training
- Multi-Factor Authentication
- Conditional Access
- Stopping Weak Password, Legacy Auth etc.
- Authenticators and Hardware Tokens
- E-mail Encryption (TLS) and Office 365 Message Encryption

Lessons Learned

- SPF, DKIM, DMARC is important
- Plan your DMARC
- Defender for Office 365
- User Awareness Campaigns
- Report Spam – End User
- Phishing Campaigns / Attack Simulations



Help Us Improve Our Conference!

Fill out a short speaker survey for each session you attend AND for the conference, overall!

<https://otsn.live/M365CHI-Feedback>

<https://otsn.live/M365CHI-Feedback>

Raffles and Giveaways



Chicago Prize Pack
Twitter Giveaway
1 Winner



\$100 Gift Card for
Opt-in Raffle
5 Winners



\$250 Gift Card for
Partner Raffle
2 Winners



Xbox One for Attendee
Opt-in Raffle
1 Winner

TWITTER GIVEAWAY!!!

Tweet about the conference using #M365CHI22 for a chance to win a Chicago Prize Pack. One Winner selected at random!

OPT-IN REGISTRATION RAFFLE

Did you opt-in to talk to our partners during registration? Thank you! Join us in the General Channel at 5:50 to see if you won an Opt-In Raffle prize!

PARTNER RAFFLE

Please, visit our Partners! While you're there, ask for their Special Phrase and gain an entry for our Partner Raffle prize!

Submit your Partner Raffle entries to <https://otsn.live/M365Chi-SponsorContest>

References #1

- SPF

- <https://www.kitterman.com/spf/validate.html>
- <https://www.spfwizard.net/>

- DKIM

- <https://dkimvalidator.com/>

- DMARC

- <https://mxtoolbox.com/dmarc.aspx>
- <https://dmarcguide.globalcyberalliance.org/#/>

References #2

- Secure SMTP connections using TLS
 - <https://www.checktls.com/TestReceiver>
- Defender for Office 365
 - <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp>
- Mastering Configuration
 - <https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/mastering-configuration-in-defender-for-office-365-part-one/ba-p/2300064>
- User Adoption & Awareness Campaigns
 - <https://phishingquiz.withgoogle.com>