GLOBAL CYBER ALLIANCE

DEFEND & DELIVER

DMARC

Email authentication for better email security

ONLINE BOOTCAMP

Shehzad Mirza

Director of Operations

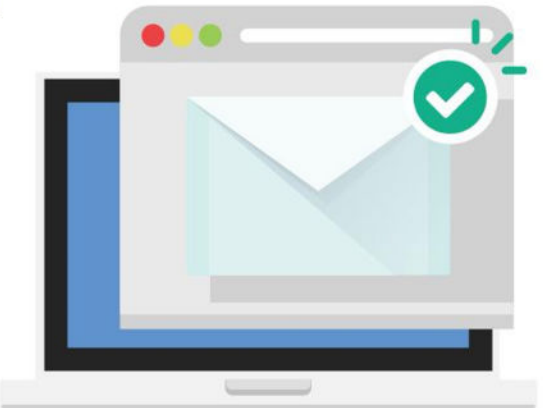
smirza@globalcyberalliance.org

gca-dmarc@globalcyberalliance.org

Key Items

SOLUTION:

DMARC



A PROVEN WAY TO MITIGATE RISK

Domain-based Message Authentication, Reporting and Conformance (DMARC)
It's like an identity check for your organization's domain name.

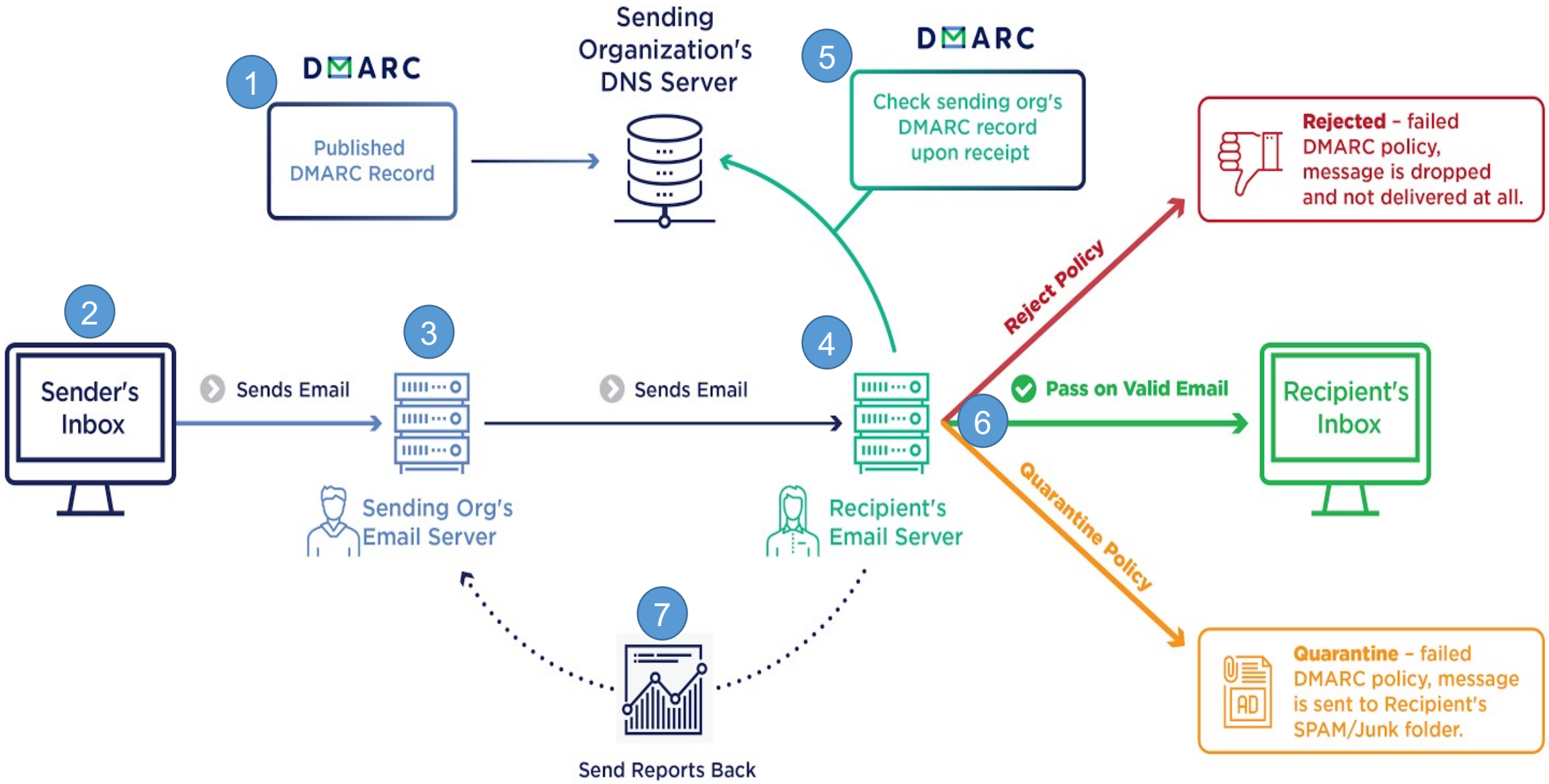
Additional Benefits of DMARC

- Inbox Protection on the Consumer Side:
  - **DMARC Verification, not policy**
  - 80 percent of the current total number of worldwide email accounts (source: Valimail).
- Deliverability
- Visibility: Provides insight into attempts to spam, phish, or even spear-phish using your organization's brand/name

DMARC cont’d

- Protects against Domain spoofing (person@company.com)
- **Create policy for all public domains**

Overview


1
DMARC
Published DMARC Record
Sending Organization's DNS Server
5
DMARC
Check sending org's DMARC record upon receipt
Rejected – failed DMARC policy, message is dropped and not delivered at all.
2
Sender's Inbox
Sends Email
3
Sending Org's Email Server
Sends Email
4
Recipient's Email Server
Reject Policy
Pass on Valid Email
6
Recipient's Inbox
Quarantine Policy
Quarantine – failed DMARC policy, message is sent to Recipient's SPAM/Junk folder.
7
Send Reports Back

DMARC DNS TXT Record

- Basic:

  Host: _dmarc

  Value: v=DMARC1; p=quarantine; **rua=mailto*:dmarc@gca-emailauth.org***; ruf=mailto*:<email address>;*

- Complex:

  Host: _dmarc

  Value: v=DMARC1; p=none; **rua=mailto*:dmarc@gca-emailauth.org***; ruf=mailto*:<email address>*; fo=1; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=reject;

What do each of the tags mean?

Required:

- v=DMARC1 - version
- p= - policy level
- rua= - aggregate reports

Recommended:

- ruf= - forensic/failure reports

Consider using

- sp= - sub-domain policy

Optional Tags:

- fo= send message samples of emails that failed either SPF and/or DKIM.
- adkim= Alignment mode for DKIM
- aspf= Alignment mode for SPF
- pct= - % of messages impacted
- rf= - report format
- ri= - reporting intervals

Proper Implementation

DMARC implementation requires Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) in order to work

- SPF is used to define which mail servers are authorized to send mail
- DKIM is used to add a digital signature for an additional layer to authenticate the sender

SPF

- use –all or ~all
- Can only have one record
- Flattening vs Dynamic (instant) SPF
  - 10 domain lookup issue
- Alignment vs Verification

SPF Alignment

Good:

From: info@globalcyberalliance.org

Return-Path: <info@globalcyberalliance.org>

Received-SPF: pass (google.com: domain of info@globalcyberalliance.org designates 2607:f8b0:4864:20::d34 as permitted sender) client-ip=2607:f8b0:4864:20::d34;

Fail:

From: info@globalcyberalliance.org

Return-Path: < bounce-mc.us15_71628198.660451-8bd9e9bfe7@mail58.atl11.rsgsv.net >

Received-SPF: pass (google.com: domain of bounce-mc.us15_71628198.660451-8bd9e9bfe7@mail58.atl11.rsgsv.net designates 205.201.133.58 as permitted sender) client-ip=205.201.133.58;

To achieve a passing SPF alignment, the From: header domain must match the domain used to authenticate SPF (e.g., envelope "mail from:" "return-path" domain).

DKIM

- Protect private key
- Publish public key
- Can have more than one record
- CNAME or TXT
- Use if using cloud service provider
- Alignment vs Verification

DKIM Alignment

Pass:

Message Header:

From: info@globalcyberalliance.org

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=globalcyberalliance.org; s=gca; h=mime-version:references:in-reply-to:from:date:message-id:subject:to :cc;

Fail:

Message Header:

From: info@globalcyberalliance.org

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mail8.mcsignup.com; s=default; h=mime-version:references:in-reply-to:from:date:message-id:subject:to :cc;

DKIM DMARC	DKIM Raw	DKIM d=
aligned	pass	globalcyberalliance.org
fail-unaligned	pass	mail9.mcsignup.com
aligned	pass	globalcyberalliance.org
aligned	pass	globalcyberalliance.org
aligned	pass	globalcyberalliance.org
fail-unaligned	pass	mail13.mcsignup.com
fail-unaligned	pass	mail8.mcsignup.com
fail-unaligned	pass	gmail.mctxapp.net
fail-unaligned	pass	mail10.mcsignup.com
fail-unaligned	pass	gmail.mctxapp.net

GLOBAL CYBER ALLIANCE

DNS Implementation

DMARC

- One record per domain

SPF

- One record per domain
- hostname set to @, null, or blank

DKIM

- Multiple records per domain
- must start with <selector>._domainkey.

Linux

- check for $ORIGIN <domain>
- requires quotation marks

All DNS

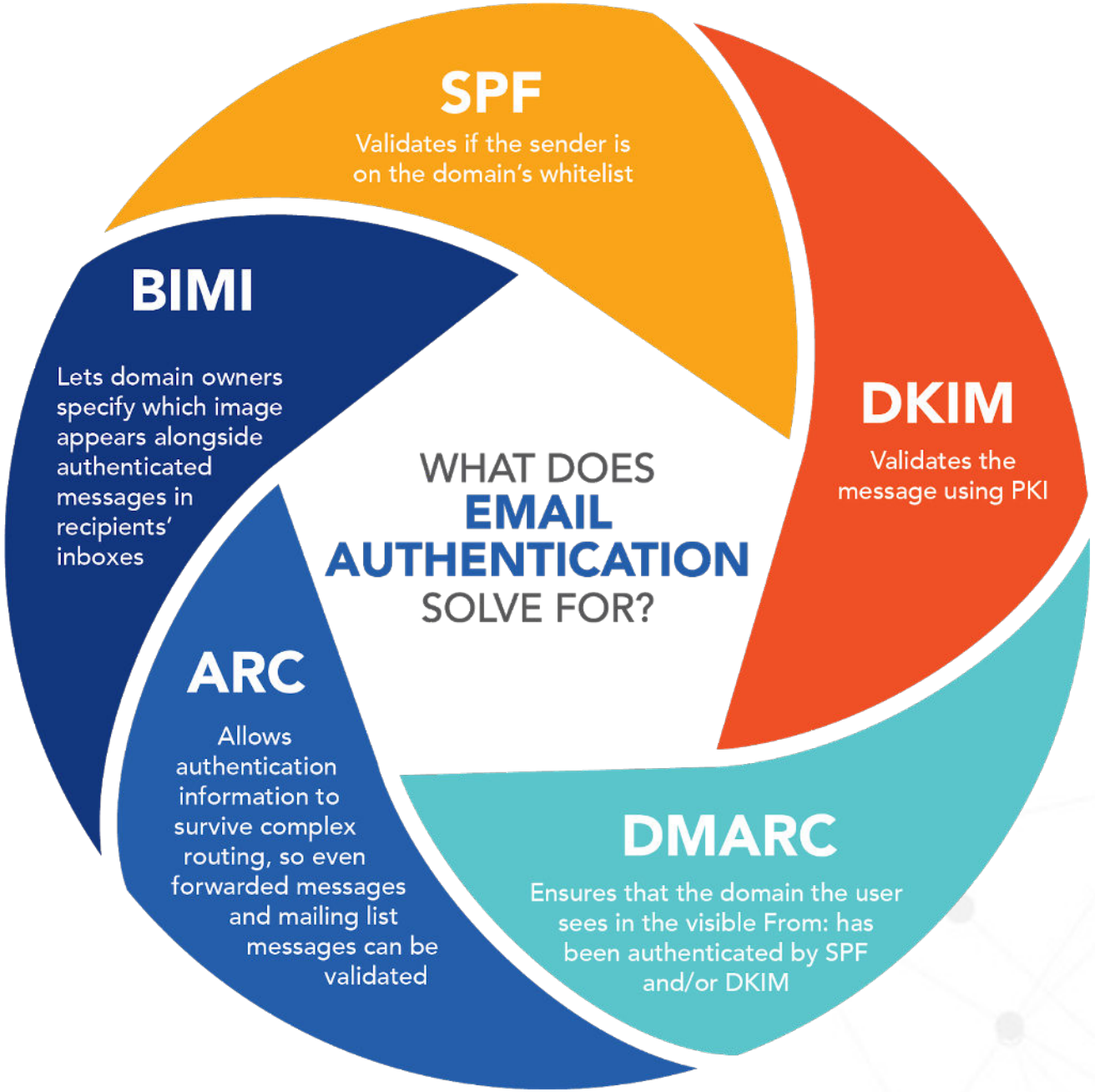
- may not need FQDN
- may not need quotation marks

DMARC Reports

- DMARC generates two types of reports:
  - Aggregate (rua)
  - Forensic (ruf)
- Reports sent in XML format to email of choice (can be sent to multiple addresses)
- Number and length of reports is dependent on amount of email sent
- Reports will provide insight as to which messages were marked as suspicious
- Allows for IT staff to correct any issues with valid messages being dropped by the policy

What Next?

- Review reports
  - Adjust SPF and DKIM as needed
- Apply p=reject to all public domains not used for email
- Move to Quarantine/Reject
  - Continue to review reports
  - Adjust SPF and DKIM as needed when new mail services are added
- Use additional email security mechanisms



Source: https://medium.com/@ykhan30/an-easy-win-for-email-security-2b84ac2a22da

ARC

- Authenticated Received Chain
- “preserves email authentication results across subsequent intermediaries (“hops”) that may modify the message”
  - http://arc-spec.org
- Used on Mail forwarders or Mail List servers
- RFC 8617
- Tools: OpenARC (https://github.com/trusteddomainproject/OpenARC/releases)

BIMI

- Brand Indicators for Message Identification
- Requires DMARC policy of reject or quarantine
- DNS TXT record

  hostname: default._bimi.

  value: “v=BIMI1; l=<location of image file>;a=<location of certificate file>;”
- Image file must be an SVG file
- Reference:
  - http://bimigroup.org/
  - https://bimi.agari.com/

DANE for SMTP

- DNS-Based Authentication of Named Entities
- Establish encrypted TLS connections without the disadvantages of STARTTLS
- Internet security protocol to allow X.509 digital certificates
- Bound to domain names using Domain Name System Security Extensions (DNSSEC)
  - Offers a second source of verification
- RFC 6698

DANE con't

- Things to consider:
  - Does your registrar support DNSSEC
  - Does your email cloud service provider support DNSSEC
  - Need to create appropriate DNS records
- Supported by Microsoft

MTA-STS
Mail Transfer Agent - Strict Transport Security

- Enables mail service providers to receive TLS secure SMTP connections
- Lives on web server with a special hostname (requires SSL)
- Enables domains to achieve 2 things
  - Opt into robust transport layer security
  - Securely communicate what their MX servers should be
- RFC 8461

MTA-STS con't

Things to consider:

- must have a valid SSL certificate
- Need to create appropriate DNS TXT record
  - Name: _mta-sts
  - Value: "v=STSv1; id=20190423085700;"
- create a .txt file with MX information
  - location of file:
  - https://mta-sts.domain.com/.well-known/mta-sts.txt
  - Use TLS-RPT for reports
- Supported by Google

TLS RPT: TLS Reporting

- Reporting that allows you to monitor the secure transport of email to a domain
- Only requires a DNS TXT record
  - _smtp._tls.yourdomain.com. 300 IN TXT “v=TLSRPTv1;rua=mailto:tlsrpt@yourdomain.com;”
- RFC 8460

Resources

- **DMARC.org** (http://www.dmarc.org) - Great source for DMARC information
- **GCA DMARC -** https://dmarc.globalcyberalliance.org
- **GCA YouTube Channel**
- **Community Forum –** https://community.globalcyberalliance.org
- **Bootcamp Resource page -** https://www.globalcyberalliance.org/bootcamp-2021/

Final Items

- Survey
- Certification of Completion

GCA Projects

- Cyber Security Toolkit (gcatoolkit.org)
  - Small Business
  - Elections

- AIDE (gcaaide.org)
- Domain Trust

GLOBAL CYBER ALLIANCE

Q&A

Thank You!

Shehzad Mirza
gca-dmarc@globalcyberalliance.org
smirza@globalcyberalliance.org