DEFEND & DELIVER
DMARC
Email authentication for better email security

ONLINE BOOTCAMP

Shehzad Mirza
Director of Operations
smirza@globalcyberalliance.org
gca-dmarc@globalcyberalliance.org
DMARC Reporting & Analysis: What Happens Next
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.
DMARC DNS TXT Record

Basic:
Host: _dmarc. <domainname>
Value: v=DMARC1; p=quarantine; rua=mailto:<email address>; ruf=mailto:<email address>;

Complex:
Host: _dmarc. <domainname>
Value: v=DMARC1; p=none; rua=mailto:<email address>; ruf=mailto:<email address>; fo=1; adkim=r; aspf=r; pct=100; rf=afrf; ri=86400; sp=reject;
Overview

1. **DMARC**
   - Published DMARC Record
   - Sends Email

2. **Sender’s Inbox**
   - Sends Email
   - Sending Org’s Email Server

3. **Sending Organization’s DNS Server**
   - Sends Email

4. **DMARC**
   - Check sending org’s DMARC record upon receipt

5. **DMARC**
   - **Reject Policy**
   - **Quarantine Policy**

6. **Recipient’s Inbox**
   - Pass on Valid Email

7. **Send Reports Back**
   - **Quarantine** - failed DMARC policy, message is sent to Recipient’s SPAM/Junk folder.
   - **Rejected** - failed DMARC policy, message is dropped and not delivered at all.
DMARC Reports

• DMARC generates two types of reports:
  • Aggregate
  • Forensic
Forensic/Failure Reports
(ruf tag)

• Number of reports is dependent on amount of email sent
• Reports will provide insight as to which messages were marked as suspicious
• Concerns with privacy
Sample Forensic/Failure Report
Aggregate Reports
(rua tag)

• 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
• Allows for:
  • IT staff to correct any issues with valid messages being dropped by the policy
  • Visibility into which systems are sending email using org’s domain name (authorized and unauthorized sending IP addresses)
<xml version="1.0" encoding="UTF-8" ?>
<feedback>
<report_metadata>
<org_name>google.com</org_name>
<email>noreply-dmarc-support@google.com</email>
<extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
<report_id>6156901232184779430</report_id>
<date_range>
<begin>1466121600</begin>
<end>1466207999</end>
</date_range>
</report_metadata>
<policy_published>
<domain>globalcyberalliance.org</domain>
<adkim>r</adkim>
<aspf>r</aspf>
<p>quarantine</p>
<sp>quarantine</sp>
<pct>100</pct>
</policy_published>
<record>
<row>
<source_ip>2607:f8b0:4001:c0b::22f</source_ip>
<count>2</count>
<policy_evaluated>
<disposition>none</disposition>
<dkim>pass</dkim>
<spf>pass</spf>
</policy_evaluated>
</row>
</record>
<identifiers>
<header_from>globalcyberalliance.org</header_from>
</identifiers>
<auth_results>
<dkim>
<domain>globalcyberalliance.org</domain>
<result>pass</result>
</dkim>
<spf>
<domain>globalcyberalliance.org</domain>
<result>pass</result>
</spf>
</auth_results>
</record>
### Aggregate Reports

<table>
<thead>
<tr>
<th>Domain</th>
<th>IP</th>
<th>PTR</th>
<th>Country</th>
<th>Message Count</th>
<th>Policy Applied</th>
<th>Override Reason</th>
<th>DKIM</th>
<th>SPF</th>
<th>Domain</th>
<th>DMARC</th>
<th>Raw</th>
<th>Domain</th>
<th>DMARC</th>
<th>Raw</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>globalcyberalliance.org</td>
<td>209.85.216.169</td>
<td>mail-qt0-f169.google.com</td>
<td>🇺🇸</td>
<td>1</td>
<td>None</td>
<td>none</td>
<td>aligned pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>209.85.216.178</td>
<td>mail-qt0-f178.google.com</td>
<td>🇺🇸</td>
<td>1</td>
<td>None</td>
<td>none</td>
<td>aligned pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>209.85.218.56</td>
<td>mail-oil-56.google.com</td>
<td>🇺🇸</td>
<td>1</td>
<td>None</td>
<td>none</td>
<td>aligned pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>209.85.218.71</td>
<td>mail-oil-f71.google.com</td>
<td>🇺🇸</td>
<td>1</td>
<td>None</td>
<td>none</td>
<td>aligned pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>209.85.218.74</td>
<td>mail-oil-f74.google.com</td>
<td>🇺🇸</td>
<td>1</td>
<td>None</td>
<td>none</td>
<td>aligned pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>209.85.220.173</td>
<td>mail-qko-f1173.google.com</td>
<td>🇺🇸</td>
<td>1</td>
<td>None</td>
<td>none</td>
<td>aligned pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
</tbody>
</table>
## DMARC Pass/Fail

<table>
<thead>
<tr>
<th>FROM: Domain</th>
<th>DKIM</th>
<th>DKIM Alignment</th>
<th>SPF</th>
<th>SPF Alignment</th>
<th>DMARC</th>
</tr>
</thead>
<tbody>
<tr>
<td>company.com</td>
<td>Pass</td>
<td>Aligned - company.com</td>
<td>Pass</td>
<td>Aligned - company.com</td>
<td>Pass</td>
</tr>
<tr>
<td>company.com</td>
<td>Pass</td>
<td>Unaligned - domain.com</td>
<td>Pass</td>
<td>Aligned - company.com</td>
<td>Pass</td>
</tr>
<tr>
<td>company.com</td>
<td>Pass</td>
<td>Aligned - company.com</td>
<td>Pass</td>
<td>Unaligned - domain.com</td>
<td>Pass</td>
</tr>
<tr>
<td>company.com</td>
<td>Fail</td>
<td>Unaligned - domain.com</td>
<td>Fail</td>
<td>Unaligned - domain.com</td>
<td>Fail</td>
</tr>
<tr>
<td>company.com</td>
<td>Fail</td>
<td>Unaligned - domain.com</td>
<td>Pass</td>
<td>Aligned - company.com</td>
<td>Pass</td>
</tr>
<tr>
<td>company.com</td>
<td>Pass</td>
<td>Aligned - company.com</td>
<td>Fail</td>
<td>Unaligned - domain.com</td>
<td>Pass</td>
</tr>
</tbody>
</table>
SPF Alignment

Pass:
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).
# SPF Alignment

<table>
<thead>
<tr>
<th>SPF DMARC</th>
<th>SPF Raw</th>
<th>SPF Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
<tr>
<td>aligned</td>
<td>pass</td>
<td>globalcyberalliance.org</td>
</tr>
</tbody>
</table>

*Fail-unaligned*
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;
## What to look for

### DKIM Issues

<table>
<thead>
<tr>
<th>Domain</th>
<th>IP</th>
<th>PTR</th>
<th>Country</th>
<th>Msg Count</th>
<th>Policy Applied</th>
<th>Override Reason</th>
<th>DKIM</th>
<th>SPF</th>
</tr>
</thead>
<tbody>
<tr>
<td>globalcyberalliance.org</td>
<td>74.125.82.54</td>
<td>mail-wmD-f54.google.com</td>
<td></td>
<td>1</td>
<td>None</td>
<td>none</td>
<td>fail</td>
<td>fail globalcyberalliance.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>209.85.213.48</td>
<td>mail-vk0-f48.google.com</td>
<td></td>
<td>1</td>
<td>None</td>
<td>none</td>
<td>fail</td>
<td>pass globalcyberalliance.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### DKIM and SPF Issues

<table>
<thead>
<tr>
<th>Domain</th>
<th>IP</th>
<th>PTR</th>
<th>Country</th>
<th>Msg Count</th>
<th>Policy Applied</th>
<th>Override Reason</th>
<th>DKIM</th>
<th>SPF</th>
</tr>
</thead>
<tbody>
<tr>
<td>globalcyberalliance.org</td>
<td>64.98.36.17</td>
<td>forward.b.hostedemail.com</td>
<td></td>
<td>1</td>
<td>Quarantine</td>
<td>none</td>
<td>fail</td>
<td>softfail globalcyberalliance.org</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Possible Spoofing

<table>
<thead>
<tr>
<th>From: Domain</th>
<th>IP</th>
<th>PTR</th>
<th>Country</th>
<th>Messages</th>
<th>Policy Applied</th>
<th>Override Reason</th>
<th>DKIM DMARC</th>
<th>DKIM Raw</th>
<th>DKIM d=</th>
<th>DKIM Selectors</th>
<th>SPF DMARC</th>
<th>SPF Raw</th>
<th>SPF Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>globalcyberalliance.org</td>
<td>54.240.11.129</td>
<td>a11-129.smtp-out.amazoneses.com</td>
<td></td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>amazoneses.com</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>amazoneses.com</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>79.19.140.127</td>
<td>host127-140-dynamic.19-79-r.retail.telecomitalia.it</td>
<td></td>
<td>4</td>
<td>Reject</td>
<td>none</td>
<td>fail</td>
<td>none</td>
<td>none</td>
<td>fail</td>
<td>fail</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>79.32.109.90</td>
<td>host90-109-dynamic.32-79-r.retail.telecomitalia.it</td>
<td></td>
<td>4</td>
<td>Reject</td>
<td>none</td>
<td>fail</td>
<td>none</td>
<td>none</td>
<td>fail</td>
<td>fail</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>79.59.82.74</td>
<td>host-79-59-82-74.business.telecomitalia.it</td>
<td></td>
<td>4</td>
<td>Reject</td>
<td>none</td>
<td>fail</td>
<td>none</td>
<td>none</td>
<td>fail</td>
<td>fail</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>89.64.62.8</td>
<td>89-64-62-8.dynamic.chello.pl</td>
<td></td>
<td>4</td>
<td>Reject</td>
<td>none</td>
<td>fail</td>
<td>none</td>
<td>none</td>
<td>fail</td>
<td>fail</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>89.79.119.222</td>
<td>89-79-119-222.dynamic.chello.pl</td>
<td></td>
<td>4</td>
<td>Reject</td>
<td>none</td>
<td>fail</td>
<td>none</td>
<td>none</td>
<td>fail</td>
<td>fail</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>89.79.180.168</td>
<td>89-79-180-168.dynamic.chello.pl</td>
<td></td>
<td>4</td>
<td>Reject</td>
<td>none</td>
<td>fail</td>
<td>none</td>
<td>none</td>
<td>fail</td>
<td>fail</td>
<td>globalcyberalliance.org</td>
<td></td>
</tr>
</tbody>
</table>
# Spoofing?

<table>
<thead>
<tr>
<th>From: Domain</th>
<th>IP</th>
<th>PTR</th>
<th>Country</th>
<th>Messages</th>
<th>Policy Applied</th>
<th>Override Reason</th>
<th>DKIM DMARC</th>
<th>DKIM Raw</th>
<th>DKIM d=</th>
<th>DKIM Selectors</th>
<th>SPF DMARC</th>
<th>SPF Raw</th>
<th>SPF Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.1.211</td>
<td>wrqvkhdp.outbound-mail.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.29.62</td>
<td>wrqvkdpl2.outbound-email.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.31.62</td>
<td>wrqvkypl2.outbound-email.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.33.214</td>
<td>wrqvnnks.outbound-mail.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.34.154</td>
<td>wrqvnnw2.outbound-mail.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.35.27</td>
<td>wrqvnpkb.outbound-mail.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.37.247</td>
<td>wrqvnrft.outbound-email.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.38.207</td>
<td>wrqvnscf.outbound-mail.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail</td>
<td>flanderscraft.be</td>
<td>smtpapi</td>
<td>fail</td>
<td>none</td>
<td>em9542.flanderscraft.be</td>
<td></td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.60.143</td>
<td>wrqvpcvf.outbound-email.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
<tr>
<td>globalcyberalliance.org</td>
<td>149.72.67.113</td>
<td>wrqvqptk.outbound-mail.sendgrid.net</td>
<td>🇺🇸</td>
<td>1</td>
<td>Reject</td>
<td>none</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
<td>smtpapi</td>
<td>fail-unaligned</td>
<td>pass</td>
<td>sendgrid.net</td>
</tr>
</tbody>
</table>
DMARC Service Providers

AGARI

VALIMAIL
TRUST YOUR EMAIL

ONDARC

DMARC Analyzer

250ok

DMARC360

DMarcian

proofpoint

ProDMARC
by ProgIST Solutions
“Free” Options

• UK National Cyber Security Centre - https://github.com/ukncsc/mail-check
• St. Louis County - https://github.com/wwalker0307/ElasticMARC
• Valimail Monitor - https://go.valimail.com/microsoft.html
• parsedmarc - https://github.com/domainaware/parsedmarc

• XML to Human Converters (best if small number of reports are received)
  • Dmarcian - XML Uploader

• DMARC analyzers (limited capabilities)
  • Postmark - https://dmarc.postmarkapp.com/
  • MXTOOLBOX - https://mxtoolbox.com/dmarcsetup

• 3rd Party tools
  • LinkedIn LaFayette - https://github.com/linkedin/lafayette/
  • SendGrid DMARC Parser - https://github.com/thinkingserious/sendgrid-python-dmarc-parser
  • Yahoo’s DMARC Report Processor - https://github.com/prbinu/dmarc-report-processor
• Additional resources are available on DMARC.org’s Code and Library page
By default you cannot send reports to external domains.

To send to external domains, the receiving end must create the following in DNS:
Name: `<reporting domain>._report._dmarc`
Value: “v=DMARC1;”

Example:
- `gotdmarc.com._report._dmarc.gotdmarc.org`
DMARC Reports and GDPR

• Forensic reports – privacy concern
  • Failure reports should be redacted

• Reports only send to the email addresses defined in the DMARC policy
• Provides visibility into all services that are sending email in your name
What Next?

• Review Reports
  • Adjust SPF and DKIM as needed

• Move to Quarantine/Reject
  • Continue to review reports
  • Adjust SPF and DKIM as needed when new mail services are added
Week 5 Bootcamp Wrap-up & Additional Email Security Protocols June 2nd
Additional Resources

• DMARC.org (http://www.dmarc.org) - Great source for DMARC information

• GCA DMARC - https://dmarc.globalcyberalliance.org

• GCA Community forum – https://community.globalcyberalliance.org

• Bootcamp resources: https://dmarc.globalcyberalliance.org/dmarc-bootcamp/
Q&A
Thank You!

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

Copyright @ 2020 Global Cyber Alliance