|  |  |
| --- | --- |
| Blueprint name | Email Gateway |
| Description | Extractor for Email gateway will be built using this blueprint document. |
| Blueprint creation date | 15 Jan 2021 |
| Author | Sharron, Lenora |
| Review Date | 16 Jan 2021 |

**Requirement Gathering and Analysis -**

**Useful Links:**

Mimecast - <https://www.mimecast.com/tech-connect/documentation/tutorials/understanding-siem-logs/>

Proofpoint - <https://help.proofpoint.com/Threat_Insight_Dashboard/API_Documentation/SIEM_API>

CISCO IRONPORT (Cisco IronPort Email Security Appliances)

<https://www.cisco.com/c/en/us/td/docs/security/esa/esa11-1/user_guide/b_ESA_Admin_Guide_11_1/b_ESA_Admin_Guide_chapter_0100110.html>

Barracuda - <https://campus.barracuda.com/product/emailsecuritygateway/doc/12193950/syslog-and-the-barracuda-email-security-gateway/>

TrendMicro Deep Discovery Email Inspector (from Parsers by clients file) -

<https://docs.trendmicro.com/all/ent/ddei/3.2/en-us/ddei_3.2_sg.pdf>

<https://community.mimecast.com/s/article/Administration-Console-Audit-Logs-1478129523>

**Email Gateway DNIF Data Model-**

**Number of Streams - 4**

Stream 1 - EMAIL-GATEWAY

1. Sender - The sender of the email.
2. Recipient - The recipient of the email.
3. Action - The action code indicating what action was taken for the message.
4. Subject -The subject of the email.
5. ~~Response - The response given back by the mail server if available.~~
6. SpamConfidence - The spam score of the message.
   1. Values - low, medium,high

(Mimecast : Aggressive triggers on any score >= 3

Moderate triggers on any score >=5

Relaxed triggers on any score >=7)

(Proofpoint: 0-100)

1. Source IP - The source IP of the original message.
2. Destination IP - The destination IP address for the delivery attempt.
3. ~~Status - Status of emails - delivered / bounced~~
4. AttachmentName - The filenames of all attachments on the email
5. AttachmentSize - The total size of all attachments on the email.
6. Direction - Detects the flow inbound or outbound
7. ~~TaggedExternal - Tagged as external email~~
8. Attachment Count - The number of attachments on the email.
9. ~~Sender Domain - The domain of the sender.~~

Stream 2 - THREAT

Vector - Email

1. Vector = “EMAIL” (This field needs to be pre-populated with the value ‘Email’)
2. Reason - The reason that the action was taken.
3. Action - The action code indicating what action was taken for the message.
4. URL - The URL clicked
5. Threat Type - The type of the threat identified (Malware, Phish, Spam)
6. Threat Name - Names of threats in the email (Attachment/URL)
7. File Name - Attachment name in the email
8. Src entity - Sender - The sender of the email.
9. Dest entity -Recipient - The recipient of the email.
10. TaggedExternal - Tagged as external email
11. Sender Domain - The domain of the sender.
12. Source IP - The source IP of the original message.
13. Destination IP - The destination IP address for the delivery attempt

Stream 3 - Authentication

1. User - email address of the user who triggered the event.
2. Src IP - Client IP
3. Dst IP- Destination IP of the server
4. Action -User Logged On, Logon Authentication Failed(Events)
5. Reason - Reason for auth failure actions

Stream 4 - IAM

1. User - Email address of the user
2. Admin User - Admin user details who makes user accounts changes/adds policies
3. Policy Details - Details regarding policy modification, addition or deletion
4. Action - Action taken by an admin user for accounts / policies
5. Role Name- Details regarding role name for role updation or modification events

**Log availability**

Logs for following devices are available.

1. Mimecast

------------------------------------------------------------------------------------------------------------

Rough work - (DO NOT DELETE)

Extractor discussion 16/01/21 with Nikhil

Streams for any mail gateway-

Email-gateway

Threat

Authentication

IAM

Generalise the stream Threat:

Changed from Network threat to threat

Will have multiple vectors - Email, Network, Endpoint

Use minimal fields - suspect, target, cause } Should have just enough fields to raise a signal

Consider fields from multiple email gateways and form a generic field list

------------------------------------------------------------------------------------------------------------