**DHA preliminary testing notes of Menlo DLP features – 04JUN2020**

**Pros and Cons:**

**Pros:**

**1. File upload DLP detection has been consistently operating as expected:**

- When uploading txt files, docx, pptx, pdf, etc., the DLP engine has detected violations with 100% consistency based on dictionary logic and frequency criteria.

- Various successful tests have been conducted with PII, PHI and medical terminology, and document classification markings.

- Menlo is capable of detecting violating files up to 15 levels of compression. Tested and confirmed.

- More detailed testing is required to validate the extent of the dictionary logic and account for specific use cases.

**2. User interface is easy to navigate and has a lot of intuitive features/integration with existing CBII features:**

- From a UI perspective, the DLP policy, dictionary group creation, selection of premade dictionaries, and creation of custom dictionaries is intuitive and easy to learn.

- There is significant customization in the DLP policy to allow you to apply specific matching criteria, dictionary logic, AD groups, and actions for file uploads and user input.

- All DLP policy is managed in the same Menlo admin console as web policy which eases administration and reduces chances of policy conflicts.

- Note, there is no misconfiguration detection in the policy creation. For example, if you had drive.google.com in an “allow” web policy, the DLP policy configuration will not alert you that you are attempting to perform DLP inspection in isolation mode only for the same domain.

**3. Logging is detailed, email alerting is functional, and basic reporting is included:**

- The logging API provides all useful fields that you would expect including URL, file name, file type, action, dictionary name, dictionary match counts, user, file hash, etc.

- The admin console Insights page includes some additional logging fields as well.

- You can create a custom DLP auditor profile that includes a name, email addresses, and "send violating file" options.

- Reporting is available albeit somewhat limited to a few built-in queries from the "Insights" section of the admin console. Custom queries can be created but would require solid understanding of Menlo's unique query language and/or support from Menlo to customize.

**4. Admin roles allows for separating job duties and creating a custom role for DLP auditors:**

- Custom admin roles can be created that restrict read/write access to specifically DLP policy. This allows for separation of duties in large organizations such as DHA.

**5. Custom dictionaries using strings and regular expressions are available and are working based on initial testing:**

- Custom dictionaries are available and have been tested using strings thus far.

- Alert/block actions have been triggered via plain text that matches a string in the custom dictionary.

- Further testing needed using regex in custom dictionaries.

**6. Active directory security group integration works and allows the application of role based access control concepts to both Web and DLP policy:**

- Active Directory security groups can be sent to Menlo during SAML assertion and can be configured in both web and DLP policies. This functionality works as expected and allows an organization to limit web & DLP policy to only affect specifically identified AD groups.

**Cons:**

**1. DLP inspection currently only works on "isolate" web policies and not "allow" web policies:**

- Need inspection on "allow" policies to work with google drive and google docs in the current implementation

- **Update - This is now resolved.**

**2. User Input (HTTP POST) inspection is not working properly in the current build:**

- I've been unable to generate alerts or blocks on plaintext form POST at this time

- Tests have involved submitting fake SSN data to docs.google.com as well as other text input web services

- Menlo has acknowledged this is inconsistent at best and they are taking this troubleshooting for action

**- Update - Menlo has made several improvements that improved consistency of user input detection. Google Docs still produces inconsistent behavior due to multi-part uploads for this application.**

**3. Document decryption of password protected files with DLP inspection is not working currently:**

- When Menlo encounters an encrypted/password protected file upload, they will redirect to another page for decryption and inspection

* Initially, inspection would fail after decryption and not trigger alerts/blocks. Menlo acknowledged this is a bug that should be resolved soon.
* Presently, the redirect after encountering a password protected file fails and just lands on an about:blank page. Menlo has confirmed this is the result of a Chrome update and their Engineering team is working on a fix.

**Update - This is now resolved.**

**4. At the moment, there is no way to view pre existing Dictionary logic:**

- You can change the frequency criteria but there is no way to determine the specific strings/regex that the dictionary is triggering on.

- Testing can be ambiguous since there is no way to view the specific dictionary logic that is triggering an alert/block.

- Menlo claims they want to provide this capability and make this more transparent. Options to duplicate and customize premade dictionaries would also be preferable.

**5. There is current method to capture violating files/docs and store in a highly secured (FIPS 140-2+ Compliant, MFA access, etc.) location for further analysis:**

- The only current option is emailing the violating file to the identified DLP auditors.

- This presents problems as it may be insecure, cause further spillage, content can be arbitrarily stripped by EEMSG system, and does not scale.