DKT. 127-10

(REDACTED)

EXHIBIT 2

UNREDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

SRX Space

Space to Store SRX related Items

Argon SRX file hash lookup

Sky-Advance Threat Prevention solution comprises of content extraction, policy enforcement on multi-services security gateway (SRX) and state-of-art malware analysis performed in the Cloud.

Use-case #1: Lookup digest alone

Problem statement: Current implementation does not offer selectively sending the content to Cloud based on content category filter.

Several customers are requesting for administrative control over what content categories they would like to NOT send to Cloud, based on their enterprise content policy. For e.g. customer A want to send executables and not send documents to Cloud.

No changes to Meta-data being submitted and reported. PLM does not see sensitivity around URL.

Support for HTTP(S) protocol.

Implementation notes on SRX:

1. Like for a normal submission SRX starts transaction by sending START message with sample metadata. **Sample metadata includes flag indicating it's going to be hash-lookup only with no data transferred(*hash_only* top level property in sample metadata JSON).**
2. SRX computes file digest (cryptographic hash with SHA256 algorithm) on file completion and send a message to Sky-ATP cloud for hash lookup. This message is expected to be delivered on the existing MsgPack/Websocket/TLS session on service plane.
3. SRX receives verdict from Sky-ATP cloud and associated policy is enforced. If there is no verdict, a configured policy action is enforced.
4. SHA256 is defacto in Sky-ATP for object ID and will be the same algorithm used to create digest string in the initial implementation. The request and response messages indicates the type of algorithm used for extensibility.
5. Digest is computed on SRX using OpenSSL SW Crypto. Though the JSF libcrypto library has HW acceleration for crypto via Intel QAT or Cavium/Nitrox on SRX High-end, the incremental nature of updating data and finalizing the digest isn't supported in JSF libcrypto library
6. Hash Lookup is done after sample rate limit checks. For now, Cloud treats hash lookups as sample submission with content, hence the same rate limit applies to hash lookups. We need to revisit the logic after discussing user experience/solution behavior.
7. Any partial content (content range) with File ID done, for a category that is marked for Hash Lookup only, will not be submitted to Cloud. That mean, Cloud will receive parts of the file via separate sessions but will not be able to fully assemble the sample.
8. "show services advanced-anti-malware statistics" op command on SRX displays File hash lookup statistics as follows. Total samples eligible are 11, some samples took fallback action due to resource/ratelimit/other errors, 5 samples are known (hit on the cloud cache) and 1 is unknown.

```
Advanced-anti-malware hash lookup statistics:
  Samples total:      11
  Samples known:      5
  Samples unknown:    1
```

9. [redacted] command shows much elaborated version as follows.