STEP-BY-STEP GUIDE TO PQC MIGRATION

INSIGHTS

SECURE METRIC TECHNOLOGY

Step 1: Build Your Cryptographic Asset list (Cryptographic Bill of Materials)

The Zero Cost Method

i. Start by retrieving your existing IT asset list, or build a new inventory of IT servers (including virtual machines) and IT equipment.

ii. Assign headcounts based on the amount of time available to work on the Cryptographic Asset List. Distribute portions of the IT Asset list among the assigned personnel, and have them identify any applications that use common cryptography-related protocols (e.g., HTTPS, SSH, IPSec VPN) or contain files with common Cryptographic extensions (e.g., .pfx, .p12, .cer, .key, .pem, .jks)

iii. Once you are satisfied that you have covered majority of the IT Asset list, move on to Step 2.

#	IT System/ Equipment Name	Application Name	IP Address(es)	Type(s) of Cryptographic Protocol used	Type(s) of Cryptographic Asset	Identifier of each Asset	Owner Email Address
1	Corporate website	Apache	10.10.10.10	TLS 1.3	TLS Certificate – RSA 2048 Keys	0A10E4B.....	own@corp.com

Table 1: Simple Cryptographic Asset List

> *"Satisfaction" is subjective and varies from person to person. Take comfort in knowing that nobody knows what nobody knows. Do not get paralyzed trying to achieve 100% of the unknown.*

The Tool-Assisted Method

Onboard tools that can scan the network and file systems to discover both IT assets and Cryptographic assets. Select tools that align with your budget. Don't worry about finding the perfect tool. The goal is to reduce the time and effort required. The tool's cost should be justified by the time and effort it saves.

Securemetric has several tools for this purpose so please reach out to us for more information.

Step 2: Prioritize Your Efforts

How to Prioritize?

i. By Urgency
ii. By Criticality
iii. By Risk
iv. By Difficulty

CBOM #	Urgency (0-5)	Importance (0-5)	Risk (0-5)	Difficulty (0-5)	Total Score
0001	3	3	1	3	10

Table 2: Prioritization Matrix

A Prioritization Matrix can help guide the decision-making process. Start by listing all the cryptographic assets and evaluating each one based on the following factors:

Urgency: Assign a higher score when the need to migrate the cryptographic asset is immediate. For example, when there is a compliance violation that must be address.

Importance: Assign a higher score when the application hosting the asset is critical. For instance, applications that handle sensitive data should receive a higher importance rating.

Risk: Assign a higher score when not migrating the cryptographic asset poses significant risk to the business or to application security. For example, this applies to public-facing applications.

Difficulty: Assign a higher score when the migration effort is complex. For example, when it requires source code changes for a legacy application.

After summing up the scores, use a total score above 12 as a general rule of thumb for prioritization. Additionally, pay special attention to any item with an Urgency, Importance or Risk rating higher than 4. Items with a total score below 12 can typically be addressed at a later stage.

Step 3: Plan Based on Priority

Assign Project Manager(s) to plan the required changes and estimate the cost and effort based on the priorities identified in Step 2. It might be helpful to group related or interdependent applications together and separate particularly challenging applications into their own dedicated projects.

Step 4: Execute, Monitor and Review

i. Initiate the plan
ii. Monitor progress
iii. Review the CBOM and Priority list monthly. Make changes to the plan and activities if required.

> *The time it takes to complete the PQC Migration exercise depends on the number of systems, the amount of resources assigned to the task and readiness of hardware and software manufacturers. In general, prepare for this activity to last until 2030.*

Securemetric Technology is a leading digital security solutions provider with a strong presence across Southeast Asia. For over 18 years, we have specialized in delivering trusted, scalable, and future-ready security infrastructures for public sector agencies and global enterprises. Our expertise includes Mobile Trust & App Protection, Advanced Digital Identity & Authentication, Trusted Cryptography & Certificate Management, Data Security & Governance, and Digital & AI Transformation Enablement. Backed by a proven track record in research, development, and deployment, we help organizations safeguard their digital ecosystems and accelerate secure digital transformation.

Email: sales@securemetric.com

Website: securemetric.com

About The Author

Tan Yu Win
VP of Project Management & Support, Securemetric Technology

Tan Yu Win started his journey in the PKI industry in the year 2000 as a software engineer for a licensed CA in Malaysia. In 2014 he joined Securemetric as head of projects and from there, he has participated in numerous government and Enterprise CA projects in Malaysia, Singapore, Indonesia, Philippines, Vietnam, Thailand, Myanmar, Egypt and Hong Kong. He is currently working on Quantum safe migration for Securemetric's customers.