Cryptography Inventory Cheat Sheet

cryptosense

Building a Cryptography Inventory has never been more important. So, what are the characteristics of a "best practice" Cryptography Inventory? We've drawn up a list of five key points to help you build an inventory as efficiently and accurately as possible.

1. Contains ALL your Cryptography

A good inventory includes everything. Not just certificates and keys, but also: algorithms, operations, IVs, Nonces, Signatures, MACs, key-derivations, salts, etc. You will also need to identify metadata; for example, how they are configured, what modes are used, reliance on other functions.

Just as important is looking in the right places. Scanning application code is a good start, but an application might pull cryptography from third party libraries, or middleware. There are also hosts, containers, hardware, infrastructure, and networks to scan. All contributors and relationships should be inventoried.

2. Covers ALL your Use Cases

From the start, you should identify every use case you will require your inventory for.

If your inventory is built with only one use case in mind - for example migration to post-quantum cryptography - then you may find it ill-adapted when another cryptography project arises further down the line.

As organisations adopt centralised "Crypto-COE" teams, the need for a unified inventory and management capability will become more acute.

> **70% of organisations either have or are planning to have a Crypto Centre of Excellence within the next 6 months.**[1]

Therefore a best practice inventory will be built with these wider use cases in mind.

3. Designed for Remediation

A great inventory won't just show you your cryptography but also the associated vulnerabilities and policy failures. An exceptional inventory will have the integrations and automations required to remediate them. What good is detection without remediation?

> **OWASP now ranks "cryptographic errors" as the #02 most likely vulnerability after broken access control.** [2]

This means integrations with Certificate Management Systems, CI/CD tools, and Key Managers, the ability to reconcile data across systems, and making it easy for developers to self-serve best practice cryptography.

4. Automated and Self-Updating

There are two main ways to build a cryptography inventory: manually, or using automated tools.

Studies show that developers should review no more than 400 lines of code per hour to keep the results accurate above 90%. So if you're going manual you will need to go slow, and go through multiple times. By the time you are finished it is likely that many systems will have changed and your inventory will be out of date and not fit for purpose.

> **The brain can process 400 lines of code per hour before accuracy dips below 70%.**[3]

Choosing a built-for-purpose automated cryptography inventory tool can address all these issues.

5. Maps Cryptographic Objects to their Dependencies

A best practice inventory shows you your cryptographic objects and maps them to their dependencies. It is in these dependency relationships that vulnerabilities and compliance issues often hide, and it is these that must be understood in order to migrate with confidence.

> **In the last 3 years there has been a 31% increase in organisations using multiple scanning techniques in combination.**[4]

Using Static Application Security Testing alone will not give you three dimensional visibility. Interactive Application Security Testing, however, will. By scanning at runtime you can see every cryptographic call that is made and which pieces are talking to the others. By combining both SAST & IAST you can get the most complete picture.

Are you starting a Cryptography Inventory Project?

Cryptosense Analyzer Platform finds your cryptography, maps your dependencies, and makes it easy to act on whatever you find. **Next Step: read our Agility White Paper.**