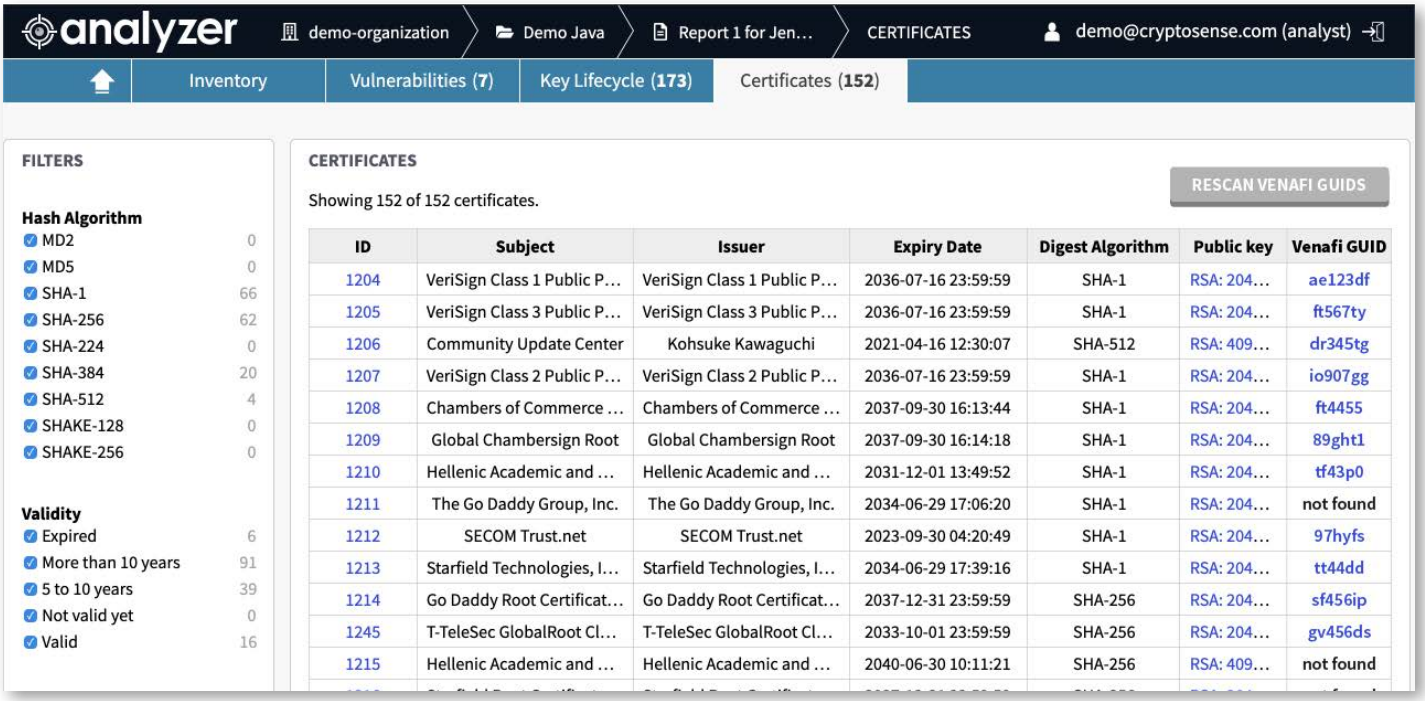
CRYPTOSENSE ANALYZER PLATFORM

Machine Identity Management for DevSecOps



Cryptosense Analyzer Platform (CAP) solves the problem of outages by providing full observability on cryptography, including certificates and other machine identifies.

Certificate Management Challenges

Certificate Outages

Many large organisations use Venafi to manage certificate renewals, but still suffer occasional certificate outages or similar issues.

There are several causes behind this: enterprise IT is evolving thanks to new technologies that speed up the software development lifecycle, yet this creates challenges for existing cert management procedures. Also, heterogeneity of IT means certificates are consumed in many different ways, making it hard to retain end-to-end visibility on the renewal process.

Outage Root Causes

Developers self-issue LetsEncrypt or Digicert certificates, and these move untracked into production; third-party code includes untracked or hard-coded certificates; or, new certificates are placed in the wrong keystore, or the application is not restarted to trigger a keystore reload

Underlying all these is a lack of full visibility on certificates and their use, and a lack of automations to use this visibility information.

CAP x Venafi Solution

CAP is a complete cryptography management solution. It offers full observability on cryptography, including certificates and other machine identifies.

CAP now integrates directly with Venafi. Certificates found by Cryptosense scans can be reconciled directly with Venafi Database. Missing certs can be added directly to Venafi.

Integration of CAP

CAP includes scanning modules:

- **Application tracers** integrate in CI workflows using Maven, Gradle, Jenkins, etc
- **Filesystem Scanners** integrate in deployment pipelines for container scanning, or can be triggered by endpoint management solutions (e.g Tanium).

Output can be routed to other management tools:

- **Venafi** to ingest new certificates for management
- **Jira** to register cryptography management issues with application owners

Automating Machine Identity Management in DevSecOps

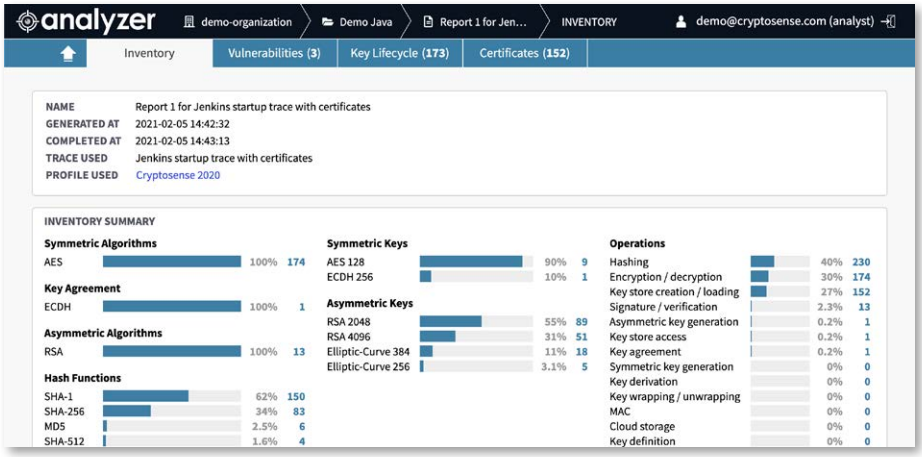
Once CAP is integrated with data sources and destinations, key productivity workflows can be automated, for example:

- Add found certificates to Venafi under certain conditions.
- Fail a build if unmanaged certificates are included.
- Register an issue in Jira for an unmanaged certificate.
- Alert on any scan containing a certificate that will expire in <3 months without a replacement.

Additional Benefits

Since CAP is a complete cryptography management platform, it offers more than just full visibility on certificates:

- A full inventory of persistent keys including where and how they are used.
- Compliance reports for internal and external cryptography audit
- Vulnerability analysis for cryptography use.
- Complete cryptography inventory for e.g. post-quantum crypto preparation or cloud migration readiness scoring.



Cryptosense Analyzer Platform provides a detailed inventory of keys, operations, algorithms etc. used inside your applications.

Visibility on Certificate Use

CAP's filesystem scanner integrates with our application tracers providing visibility on how certificates are used, from which line of code, and giving actionable information. Thanks to this integration, our filesystem scanner is able to provide greater coverage on certificate use than you would get by using a CMS Discovery Tool alone.

	Cryptosense File Scanner	CMS Discovery Tools
Scan standard certificate file formats in all locations	✔	✔
Automated reconciliation with certificates already in CMS	✔	✔
Discover and scan inside encrypted keystores	✔	x
Scan inside bytecode	✔	x
Scan inside binaries	✔	x
Scan container images	✔	x
Integration in CI	✔	x

Cryptosense SA
231 rue saint Honoré
Paris 75001, France

France Sales: +33 (0)9 72 42 35 31
International Sales: +1 646-893-7657
sales@cryptosense.com