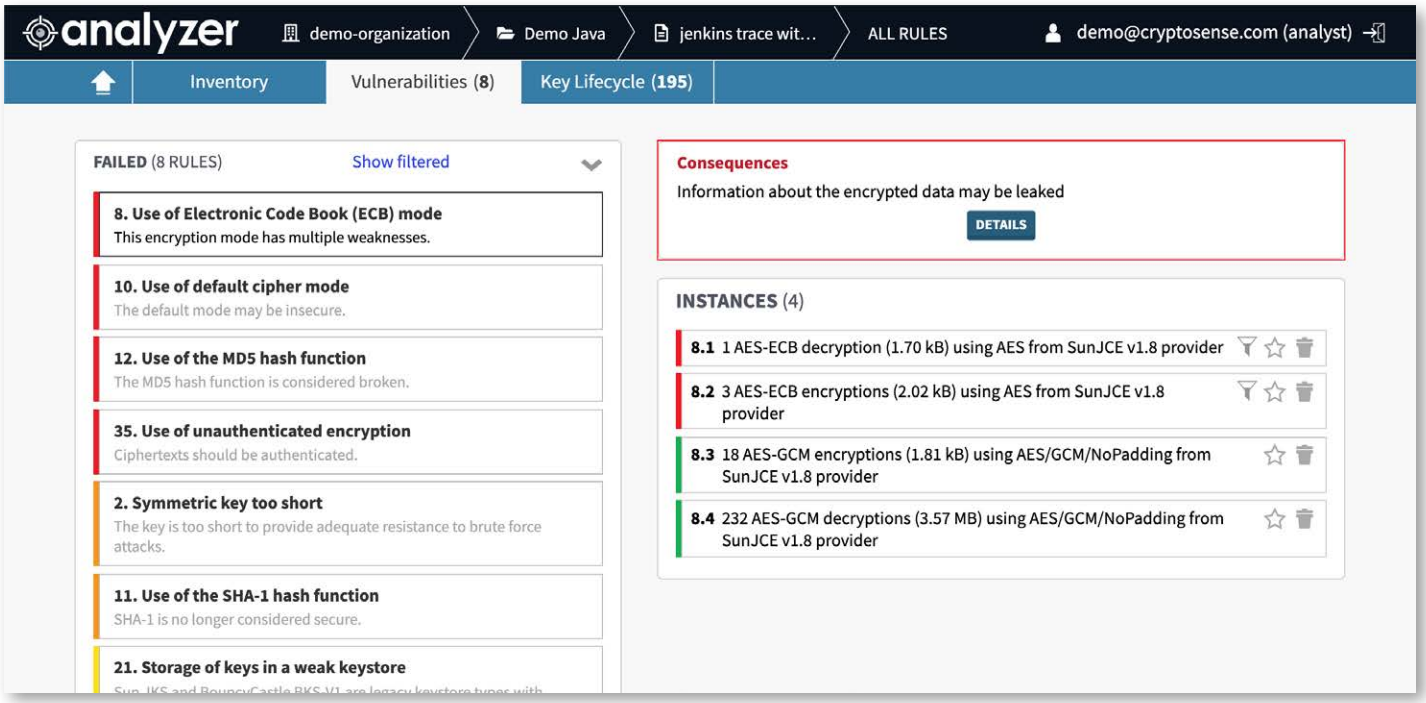
CRYPTOSENSE ANALYZER PLATFORM

State-of-the-art IAST tool for finding and fixing cryptographic vulnerabilities



Technical Specifications

Cryptosense Analyzer supports Java, .NET and OpenSSL. More APIs are being added continually.

Cryptosense Analyzer consists of:

1. The **analysis platform** which also hosts the reporting web application, available in SaaS hosted in our cloud or as a completely self-contained virtual machine licensed for use on-premises.
2. A number of **Tracers**, which are used locally in the environment of the application under test to trace calls from the application to its cryptographic library at run-time.

Analyzer Features

- The Analyzer web application works with all modern browsers, including Chrome (v55+), Firefox (v50+), Internet Explorer (11+).
- Filters allow exceptions to be recorded for future analyses of the same application.
- Full Rest API for integration into CI pipelines, GraphQL API as well as a REST one and we integrate with Jira for issue tracking and can give a timeline output suitable for Splunk or Elastic Search.

Tracer Features

- The tracer agents record the trace of calls in a file, which is compressed on the fly, and can be inspected by the user. The file can be written to storage for later upload via the Rest API or Web GUI, or encrypted and streamed directly over the network to the analysis platform.
- The trace contains calls to the cryptographic library including all their parameters and stack-traces to allow vulnerabilities to be pinpointed in source code.
- Traces can be obtained by leveraging existing test suites such as unit tests and integration tests.
- Cryptosense supplies scripts for measuring a trace's coverage of crypto calls in the code.
- Tracers work with all application frameworks including Tomcat, Wildfly, Weblogic, Websphere etc. They are also compatible with containerized environments such as Docker, etc.
- Tracers integrate with Cryptosense plugins for popular build frameworks including Maven and Gradle.

Vulnerability Types found by Cryptosense Analyzer Platform

Cryptographic Usage Errors

Cryptosense Analyzer treats all the crypto operations carried out by the application under test. This allows the detection of a comprehensive set cryptographic issues that lead to vulnerabilities, including reuse of values intended to be used once like IVs and nonces, unsafe protocol version choice, insecure combinations of operations, use of encryption modes susceptible to padding oracle attacks, weak keys, random number generation errors, reuse of keys for different operations, and more.

Algorithm and Key-Length Weaknesses

Cryptosense Analyzer detects the use of weak ciphers, hash functions, MACs and signature modes as well as short keys and vulnerable or non-compliant certificates. Key length and algorithm policy can be customized by the user.

Flaws in Cryptographic Libraries

Cryptosense Analyzer detects the precise libraries and versions used for each cryptographic call and cross-references these to our vulnerability database.

Key-Management Flaws

Thanks to our vulnerability research on common APIs, Cryptosense Analyzer can spot a variety of key management issues, including the insecure use of software keystores, hardcoded keys and passwords, weak master passwords, misconfiguration of hardware keystores, key derivation errors, and insecure Diffie-Hellman key exchange.

About our Analysis Rules

Security and Compliance Risk

For each finding, Analyzer explains in detail the level of risk in terms of the consequences of the attack, the level of expertise required to mount it, and the computing resources required. This allows an accurate risk assessment on the basis of the threat scenario pertinent to the application under test. Analyzer also reports on compliance with respect to cryptographic standards such as NIST 800-57, PCI-DSS, FedRAMP etc.

Remediation Information

In addition to risk assessment information, we provide instructions on how the problem can be resolved, whether by code changes, a library update or changes to configuration files. We continually update our remediation results to take into account the complex maze of configuration files and dependencies in modern application frameworks.

Always up-to-date

Our rules are derived from academic results in applied cryptography research, standards, hacking conferences, public vulnerabilities, and our own vulnerability research. Thanks to close links to the community and ongoing collaborations with top academic groups we keep our rules up to date with latest advances in cryptanalytic attacks.

Cryptosense Analyzer	
Tracer Compatibility	**Cryptographic Interface**
Java	
Oracle Hotspot JVM OpenJDK, etc. version 1.8, 1.9, 1.10	Java JCA (any provider such as Oracle JCE, Bouncycastle, IBM JCE, etc.).
Microsoft	
.Net Core v2.0+ on Windows or Linux, .Net Framework 4.5.2+	System.Security.Cryptography.*
OpenSSL†	
Lightweight LD_PRELOAD extension, compatible OpenSSL 1.0.x and 1.1.x	Traces libssl and libcrypto (EVP interface).
Coming soon: Python, Ruby, Go, and more...	

†*OpenSSL currently in private beta - contact us to take part in beta programme.*

Cryptosense SA
51 rue de Ponthieu
Paris 75008, France

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