CAST

Software Intelligence for Digsial Leaders

Software Intelligence at your fingertips

Communicate - Decide – Measure - Protect – Discover- Improve

CAST Highlight - a full-proofed secured platform

Security is our concern

May 2022

A secure platform used by companies with high security requirements
Governments / BFSI / Utilities…

And many others…

ISO 27001 Certification

- Since 2015, CAST is ISO 27001 certified for the following activities:
  - Development
  - Quality Assurance
  - Release management
  - Operating and Facilities management
- Developers are trained on secure development
- Software and services are regularly assessed (penetration test and audit code) by third party specialists
- The latest certificate was delivered on April 1st 2021

Bureau Veritas Certification

CAST

3 RUE MARCEL ALLEGOT
92190 MEUDON
FRANCE

Bureau Veritas Certification Holding SAS – UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2013

Scope of certification

CAST INFORMATION SECURITY MANAGEMENT SYSTEM RELATED TO DEVELOPMENT, MAINTENANCE AND OPERATIONS OF THE CAST CLOUD BASED SOFTWARE ANALYSIS SERVICES

Statement of Applicability v 7.150 dated on 24/02/2021

Original cycle start date: **1 April 2015**

Expiry date of previous cycle: **31 March 2021**

Certification / Recertification Audit date: **26 February 2021**

Certification / Recertification cycle start date: **01 April 2021**

Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: **31 March 2024**

Certificate No. ***FR065258*** *Version:* ***1*** *Revision date:* ***19 March 2021***
Contract No. ***10231312***

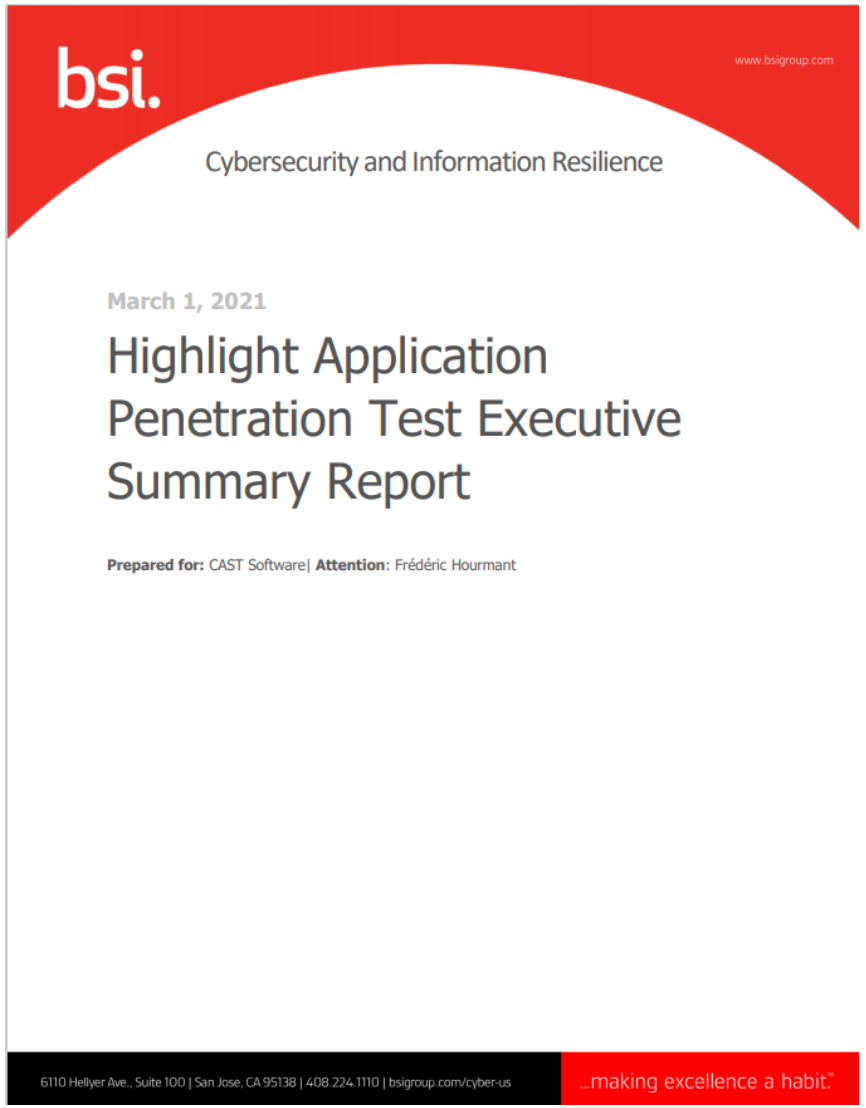
Laurent CROGUENNEC - President,
Signed on behalf of BVCH SAS UK Branch

Certification body address: 66 Prescot Street, London E1 8HG, United Kingdom.
Local office: Bureau Veritas Certification France : Le Triangle de l'Arche - 9 Cours du Triangle - 92937 Paris La Défense

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please call: *+ 33(0) 1 41 97 00 60.*

Audit – Penetration Testing

- BSI Cybersecurity and Information Resilience ("BSI") performs regularly penetration tests of the CAST Highlight application. This test focused on features, such as authentication, session management, and web server security. This was a detailed application-level test that employed a combination of manual testing by experienced professionals and automated testing tools.
- The first audit was done in November 2019, the last one in December 2020 .
- During the initial test in December 2020, BSI identified 15 distinct vulnerabilities, with the following breakdown of severity levels: 1 High, 2 Medium, 3 Low, and 9 Best Practices. CAST Software has remediated 5 of these vulnerabilities and 1 Low finding has been closed based on additional information. BSI validated during the remediation testing phase in February 2021 that all High and Medium vulnerabilities have been remediated, 1 Low and 8 Best Practice remain open.
- Based on this assessment and mitigating factors, BSI believes that CAST has adequate controls in place within the Highlight application to protect the security of customer information. CAST was able to quickly and effectively remediate findings that were identified in the initial security assessment report.


bsi.

www.bsigroup.com

Cybersecurity and Information Resilience

March 1, 2021

Highlight Application Penetration Test Executive Summary Report

Prepared for: CAST Software| **Attention**: Frédéric Hourmant

6110 Hellyer Ave., Suite 100 | San Jose, CA 95138 | 408.224.1110 | bsigroup.com/cyber-us

...making excellence a habit.™

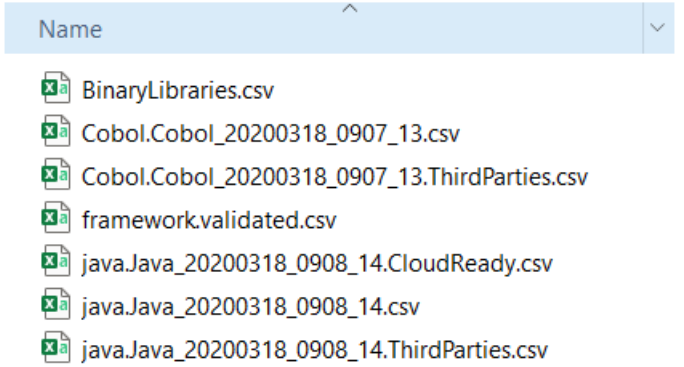
Information Security Policy - ISMSHL

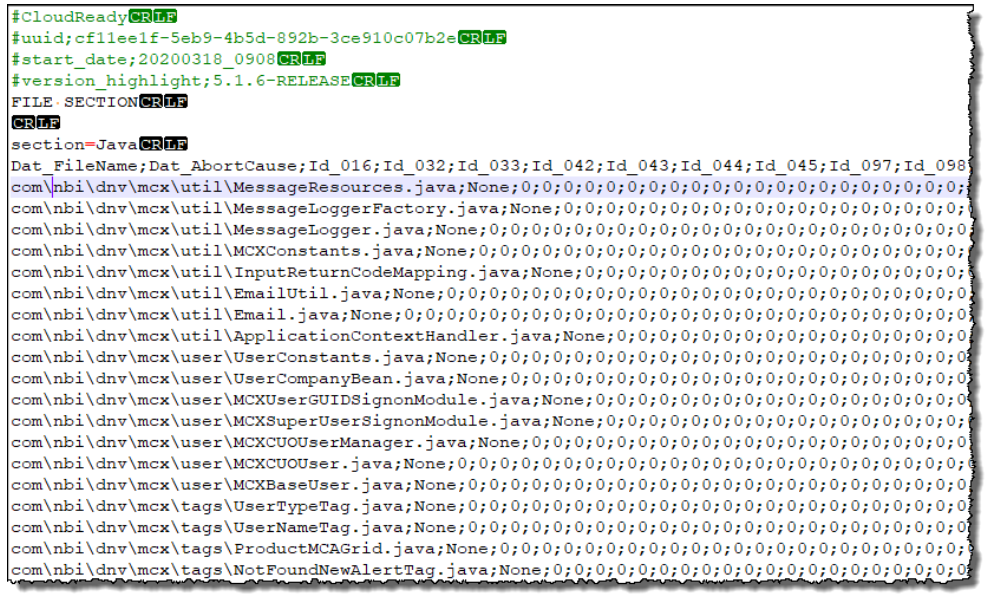
- Since 2008, CAST has implemented an information security policy that ensures that risk is minimized and that any security incidents can be effectively responded to.
- The communication of the Information Security policy to external interested parties is possible but subject to authorization from the group IT Director.

- Validation and tracking changes
- Executive endorsement
- Information security policy management
  - Roles and responsibilities
  - Review of the Information Security Policy
- Information Security policy
  - Information security objectives
  - Management commitment
  - Communication and awareness session
  - Organization for Risk Management
- Organization of information security
  - Information security roles and responsibilities and segregation of duties
  - Membership in associations
  - Security in project management
  - Mobile devices and teleworking
- Human resource security
  - Prior to employment
  - During employment
  - Termination and change of employment
- Asset Management
  - Responsibility for assets
  - Information classification
  - Media handling
- Access control
  - Business requirements of access control
  - User access management
  - User responsibilities
  - System and application access control
- Cryptography
- Physical and environmental security
  - Secure areas
  - Equipment
- Operations security
  - Operational procedures and responsibilities
  - Protection from malware
  - Backup
  - Logging and monitoring
  - Control of operational software
  - Technical vulnerability management
  - Information systems audit considerations
- Cloud services
  - Infrastructure
  - Responsibilities
  - User provisioning
- Communications security
  - Network security management
  - Information transfer
- System acquisition, development and maintenance
  - System requirements of information systems
  - Security in development and support processes and tests data
- Supplier relationships
  - Information security in supplier relationships and supplier service delivery management
- Information Security Incident Management
- Information security aspects of Business Continuity Management
- Compliance
  - Compliance with legal and contractual requirements
  - Information security review

Highlight Code Scan Outputs

- Highlight Agent generates csv files (executed on your computers – the source code never leaves your infrastructure)
- CSV files are text files that can be opened with any text editor so they can be audited by Security or Compliance officer. No source code is embedded into CAST Highlight CSV files.
- Those CSV files are not encrypted and can be read and reviewed by anybody.
- Those CSV files contains only metrics (numbers relevant to CAST Highlight measurement model) and the scanned source filenames.
- Customer can anonymize the source filenames if needed.
- Those CSV files are transmitted to the Highlight platform through HTTPS, which is an encrypted protocol using a 256-bit encryption mechanism.
- The zip file name and the csv file names are anonymous by default:
  - HighlightResult.05_07_2020_09_22.zip
  - Cf. screenshot of the right for the csv file names
- In the Highlight platform, the customer name and the customer application names can also be anonymized if needed.





CAST Highlight Operating Model

Initiate

Step 1

Launch & Planning

Executive sponsorship established through global communication (i.e. email to all project leads).

Scan & Assess

Step 2

Distributed Analysis

App owners across the globe complete an application survey and download agent from CAST Highlight portal to analyze code stacks. Analysis is performed in minutes, on their network.

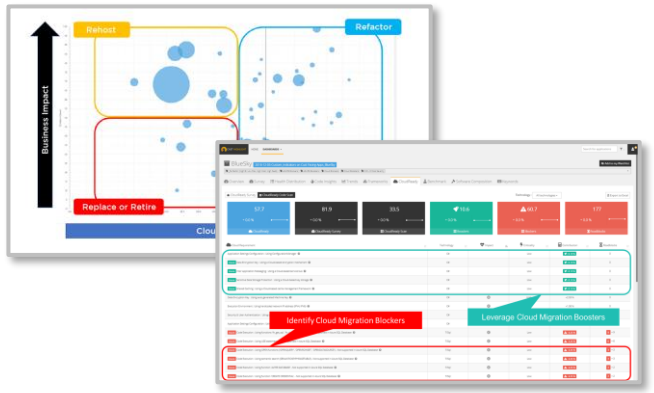
Insight

Step 3

Results interpretation & Recommendations

Actionable software analytics and portfolio-wide dashboards available online, includes: technology mix; app health and risks; business impact context; and cloud readiness.

Enterprise-wide portfolio intelligence available on a secure, private cloud.



Scan of applications in Step 2 can be executed using two possible scenarios:

1) App owners by executing Highlight Agent on their **desktop (Windows environment)** or
2) Install CLI or Docker agent on **server (Windows or Linux)** where execution can be achieved in batch mode for multiple applications