Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

BLACKDUCK

SOGETI

The value of Open Source Software is undeniable. Effectively securing and managing it remains a challenge

Open Source Software (OSS) is an essential element in today's application development environment because it lowers costs, frees internal developers to work on higher-level tasks, and accelerates time to market. Open Source use is ubiquitous worldwide and leading organizations are stepping up efforts to meet the security and management challenges that open source use presents.

The overriding open source management challenge is gaining good visibility into where it's used. Without that visibility, effectively managing and securing open source is impossible, exposing organizations to significant security vulnerability and license risk. Organizations cannot control what they can't see.

A recent report detailing the results of 200 Open Source Security Audits[1] in Q4 2015 and Q1 2016 underscores the need for better visibility and the consequences of not having it.

The audits found:

- On average organizations were aware of less than half the open source components in use
- 67% of the applications contained open source security vulnerabilities
- 39.5% of open source vulnerabilities in each application were "severe"
- On average there were 22.5 vulnerabilities in each application
- The average "age" of open source vulnerabilities at scan time was 1,894 Days

Companies are under pressure to develop new applications rapidly and open source helps them do that. Without an automated process for cataloguing Open Source usage, organizations often rely on manual tracking, which is error prone and difficult to scale. As the audits show, they quickly lose visibility and control of their open source and the capability to effectively manage it during the software development cycle.

There are three types of risk: security risks, when the OSS component contains a known vulnerability, opening doors for large-scale breaches; legal risks, when the OSS license obligations are not met; and operational risks, when the OSS community is not actively managing and improving the component.

Open Source Software Analysis – identify and fix vulnerabilities

Simply reacting to risks as they materialize is not the answer. Companies need to take proactive measures to protect their applications from security breaches, legal non-compliance, and operational uncertainties. To address this need, Capgemini, Sogeti and Black Duck® Software have come together to provide their customers with the visibility and control needed to find and remediate open source vulnerabilities and risks. Our comprehensive Open Source Software Analysis service is the solution to the growing challenge of effective OSS management and risk mitigation.

How does it work?

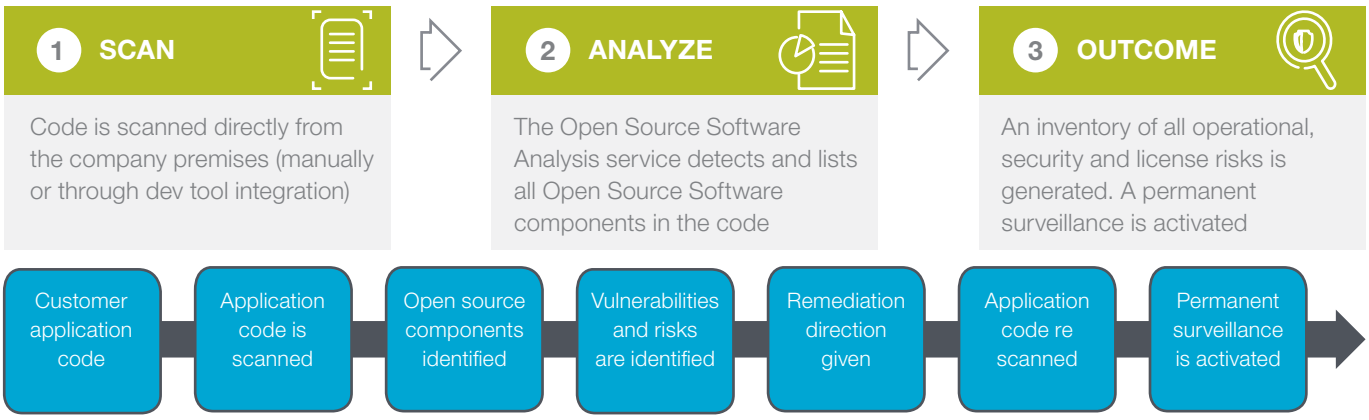
It is a simple 3-step process. The code is scanned to identify and inventory the open source; the inventory is compared against Black Duck's KnowledgeBase; the platform assigns a risk score – security, license, operational - and provides remediation-tracking capabilities. It also monitors the code and issues alerts if any new vulnerabilities are discovered.

Benefits of Open Source Software Analysis

The Capgemini and Sogeti Open Source Software Analysis powered by Black Duck equips you to automate the processes of identifying and inventorying open source components, to find open source software risks to your organization, including known open source vulnerabilities, and to fix them.

Managed service

It is quick and easy to start an OSS analysis program, requiring minimal upfront investment and offering the flexibility to scale with changing business needs.



1 Code audits conducted by Black Duck Software during merger and acquisition situations.

Fast results

Your Open Source Software Analysis delivers automated, accurate and detailed results as soon as you scan the application code.

Centralized portal

User-friendly dashboards and reporting enable you to manage your application portfolio and collaborate across distributed teams. The dashboard details security risks, license risks and operational risks, enabling remediation according to the type of risk.

OSS research

This invaluable service for the digital enterprise draws on Black Duck's expertise in finding and analyzing vulnerabilities in Open Source Software, along with the company's comprehensive abilities in managing open source components.

Personalized support

A technical account manager (usually your local Capgemini or Sogeti consultant) ensures overall customer satisfaction, drives adoption of the service, addresses issues, connects to experts, and provides you with best practice guidance.

Integration with third-party software

Open Source Software Analysis integrates with Continuous Integration (CI) tools such as Jenkins. It also provides APIs that enable development teams to easily integrate scanning and alerts with other development tools, including additional CI solutions, source and binary repositories and project management and tracking software. This provides visibility in a continuous build environment.

Reduced risk

By scanning and analyzing OSS components, you get much needed insight into the risks you face in terms of number and severity, and are able to greatly reduce the exposure to a damaging security breach and to legal license risks.

Reduced CAPEX

Instead of investing in costly and hard-to-maintain tools, which require special resources to operate, you can buy on-demand analysis services as needed.

Flexible model based on OSS Units

Our Open Source Software Analysis services are available as OSS Units. These are pre-paid credits that are redeemed for each new application being analyzed, offering flexibility to allocate your investment throughout the year. One OSS Unit is required for an analysis with surveillance covering 30 days; three OSS Units give you unlimited analysis with year-long (365 days) surveillance.

Getting started

The Capgemini and Sogeti Open Source Software Analysis service powered by Black Duck is simple and fast to initiate. You quickly put in place fundamental security controls, with minimal upfront investment, whether you have just a few applications or are looking to launch a comprehensive security/OSS program across your organization.

You simply buy the number of OSS Units you need, then we install your customer portal within days and you're ready to start. You can begin with a small number and buy additional OSS Units when the service has proved efficient in your organization and needs to be extended. Or you can buy a large number at the outset to reduce costs.

Why Capgemini, Sogeti and Black Duck?

Capgemini and Sogeti are part of the Capgemini Group, recognized in 2014 by Gartner as a leader in Application Testing[2]. The Group was also positioned as a leader by NelsonHall for Transformation-Focused Testing Services, and for Outsourced Testing Services[3] by Ovum in 2014-15[4].

With a strong 20-year heritage in testing and assurance heritage, coupled with unparalleled knowledge and experience, the Capgemini Group is trusted to deliver consistently, time after time, by clients in diverse industries.

Our 2,500 security consultants worldwide offer a wealth of expertise. Their deep know-how in security is complemented by our investment in Research & Development teams in Europe, our IT Security Evaluation Facility (ITSEF) and dedicated Security Operations Centers (SOCs).

Black Duck's KnowledgeBase is the most comprehensive open source database in the world, tracking 1.5 million projects and 350 billion lines of code. Black Duck is acknowledged by Gartner as a 'cool vendor' and is ranked 38 out of 500 security companies [5].

High standards

As you would expect from a global leader in application security testing, we work to the highest industry standards:

- Cybersecurity Maturity & Health Assessment (CMHA) – to benchmark and provide you with a security roadmap;
- TMap® – the de facto industry standard for structured testing;
- TPI® – the world's number one model for assessing and improving test processes;
- PointZERO® – a framework that delivers parallel step-by-step improvement based on an array of measures, methods and tools, leading to business solutions that are fit for purpose and right first time.

2 https://www.sogeti.com/explore/reports/capgemini-group-positioned-in-the-leaders-quadrant-by-gartner/

3 https://www.capgemini.com/news/capgemini-positioned-as-a-leader-in-software-testing-services-by-nelsonhall

4 https://www.capgemini.com/news/capgemini-positioned-as-a-leader-for-outsourced-testing-services-by-ovum

5 https://www.blackducksoftware.com/news/releases/black-duck-software-ranked-38th-globally-q3-2015-cybersecurity-500-list

Securing your digital transformation

The combined strengths of Capgemini, Sogeti and Black Duck will keep your organization ahead of current and emerging cyber threats in a rapidly changing business and information technology landscape.

For more details contact:

Darren Clews
CSO
Sogeti UK
darren.clews@sogeti.com
+44 (0) 3305 88 82 00

About Black Duck ® Software

Organizations worldwide use Black Duck Software's industry-leading products to automate the processes of securing and managing open source software, eliminating the pain related to security vulnerabilities, open source license compliance and operational risk. Black Duck is headquartered in Burlington, MA, and has offices in San Jose, CA, London, Frankfurt, Hong Kong, Tokyo, Seoul and Beijing. For more information, visit www.blackducksoftware.com.

About Capgemini and Sogeti

With more than 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Sogeti is a leading provider of Technology and Engineering Services. In the UK, Sogeti offers cutting-edge Consulting, Cloud, Cyber Security, DevOps, Digital, and Testing solutions, combining world class methodologies and a global delivery model, Rightshore®. Sogeti brings together 25,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 3,000 professional employees support you in defining and implementing your cybersecurity strategies. We protect your IT, industrial systems, and the Internet of Things (IoT) products & systems. We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, eight security operations centers (SOC) around the world, a Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

Find more information at:

www.capgemini.com/cybersecurity or
www.sogeti.com/cybersecurity

MCOS_GI_PT_20170203