Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Hewlett Packard Enterprise

SOGETI

Application Security Testing

Powered by HPE Fortify on Demand

Managed application security testing available on demand

Powered by HPE Fortify on Demand, Sogeti Application security testing is a managed service that makes it simple to initiate security tests on a few applications or launch a comprehensive security program without upfront investment of technology and resources. Combining HPE's advanced dynamic and static security testing technologies with Capgemini/Sogeti world leader experience in testing and cybersecurity services, it brings professional-level software security expertise to organizations of any size.

Customer uploads software to the Sogeti platform or provides the URL of the application.

The Sogeti platform conducts a thorough security test (dynamic or static) of the application.

Our experts reviews and analyzes the results of the application test in the form of a detailed report or dashboard.

Enterprise application risk management

Assessing internal applications

With internally developed applications, Sogeti Application security testing helps in two primary ways. For companies with a secure development lifecycle already in place, we can provide a final test before deployment. For organizations new to security, Sogeti Application security can provide a quick and accurate application security test to baseline applications and prioritize efforts to improve application security. In addition, code assessments can be provided at any time during the development work.

Outsourced and open source application security testing and management

To accelerate time to market, companies are increasingly relying upon outsourced development resources and open source software. Third party developers may not follow the same best practices instituted with in-house developers while open source code can be filled with known or unknown vulnerabilities. Sogeti Application security testing enables companies to identify and assess the security risk of outsourced or open source content and implement the necessary security control strategies.

Vendor application security testing and management

Third-party code, including commercial software, represents a large percentage of deployed software, and therefore, a substantial area of potential risk. Yet most software vendors provide little or no visibility into the security state of their products and are, for a variety of reasons, resistant to having their software analyzed by anyone but themselves. They are concerned about providing access to their most precious intellectual property, their source code.

Companies should ensure their third-party software is tested for vulnerabilities during the procurement or upgrade process, and request that critical issues be addressed prior to acceptance. Sogeti Application security testing provides an easy way to use security-as-a-service based approach that doesn't require source code; it allows the vendor to test applications, resolve issues, and then publish a final report to the procurer. Sogeti Application security testing serves as an independent third party and system of record for conducting a consistent, unbiased analysis of vendor software.

Service features and benefits

Managed service

Fast and easy to start an application security program with minimal upfront investment that has the flexibility to scale with changing business needs. There is no need to install, procure, and maintain hardware or hire and retain a large staff of application security experts.

Fast results

Accurate, detailed results delivered on many assessments in just a few days.

Centralized portal

User-friendly dashboards and reporting make it simple to manage an application portfolio and collaborate across distributed teams. Assess risk, initiate scans, analyze results, and remediate vulnerabilities based on prioritized recommendations.

Europe-based

Sogeti Application security testing is provided from Europe, the platform is hosted in a Sogeti infrastructure in a European secure (Tier IV) datacenter in Luxemburg, out of scope of any “Patriot Act” legislation. It is entirely administered from Sogeti so that assessed applications and vulnerability reports are fully secure.

Software security research

The Sogeti Application security testing platform benefits from threat intelligence updates from HPE Security Research.

Personalized support

Results are manually reviewed by application security experts. A technical account manager (usually a local Capgemini/ Sogeti consultant) ensures overall customer satisfaction, drives adoption of the service, addresses issues, connects to experts and provides best practice guidance.

Comprehensive security testing solution

Integrate with security software offerings including HPE Software Security Center to build a powerful security program. IDE plug-ins, build server integration, WAF, digital vaccines, and bug tracking are supported as well.

Service description: A flexible model based on Assessment Units

Application security testing

Sogeti dynamic, static, and mobile application security testing services are available by purchasing Sogeti Application security testing Assessment Units. Assessment Units are pre-paid credits that are redeemed for single assessments or application subscriptions, offering flexibility to allocate your investment throughout the year. Assessment Units are valid for 12 months starting at the purchase order (PO) effective date and may be redeemed individually.

For each single assessment or subscription requested, the customer chooses a combination of one assessment type (dynamic, static, or mobile) and one assessment service level. Customers that perform a single assessment can request one remediation validation scan within one month of the assessment. An application subscription allows for one application to be assessed an unlimited number of times for a period of 12 months starting at the PO effective date (irrespective of when Sogeti Application security testing Assessment Units are redeemed).

Customers can purchase multiple years' worth of assessment units on a single PO (two or three years). Multi-year commitments, as well as bulk Assessment Units purchases, reduce customer costs. For multi-year commitments, a set annual allotment of assessment units is purchased and each year's allotments are issued on the anniversary of the PO effective date. Each year's allotment of assessment units must be used within 12 months and are not "rolled over" to subsequent years.

Table 1: Assessment Units

Assessment service level	Single assessment	Application subscription
Basic	2 Assessment Units	6 Assessment Units
Standard	4 Assessment Units	12 Assessment Units
Premium	8 Assessment Units	25 Assessment Units

Table 2: Assessment Service Levels

	Basic	Standard	Premium
Dynamic assessments			
Technique	Full automated	Full automated + manual	Full automated + manual
False positive removal	Yes	Yes	Yes
Authentication	Yes	Yes	Yes
Logic	No	No	Yes
Source code	No	No	Yes (1 assessment)
Web services	No	No	10 endpoints
Target turnaround	3 days	5 days	7 days
Static assessments			
Languages	21+*	N/A	N/A
Upload file size	All sizes	N/A	N/A
Vulnerability categories	All categories	N/A	N/A
Audit review	Yes	N/A	N/A
False positive removal	Yes	N/A	N/A
Target turnaround	2 days	N/A	N/A
Mobile assessments			
Platforms	iOS, Android, Windows®, BlackBerry	iOS, Android	iOS, Android, Windows®, BlackBerry
Client: automated binary	No	Yes	Yes
Client: manual binary	No	OWASP top 10	All categories
Client: source code	Yes	No	Yes
Network	No	OWASP top 10	All categories
Server: Web services (dynamic)	No	OWASP top 10	All categories
Server: Web services (source code)	No	No	Yes
False positive removal	Yes	Yes	Yes
Target turnaround	2 days	2 days	7 days

* Supported languages for static basic assessments are ABAP/BSP, ASP.NET, C, C#, C++, COBOL, Classic ASP, ColdFusion, FLEX, HTML, Java (with Android), JavaScript/AJAX, JSP, Objective-C, PHP, PL/SQL, Python, Ruby, Transact-SQL, VB.NET, VB6, VBScript, or XML.

Web services assessment

Web services assessments are offered in buckets of 10 endpoints and can be added to any level of dynamic testing. A customer can request a Web services assessment by redeeming four (4) Assessment Units.

Digital risk assessment

Sogeti Application security testing offers an internal or external digital discovery assessment on domains and Internet protocol space assets owned by the customer. This assessment helps the customer determine how many live or unknown websites the company owns, which of those websites house unknown application functionality, and the risk profile of these sites. A customer can request a digital risk assessment by redeeming fifty (50) Assessment Units.

Comprehensive operational services

Sogeti Application security testing delivers ongoing support services including the following:

Customer support

Sogeti maintains a team of support staff, which will be the single point of contact for all issues related to the Sogeti Application security testing service. The severity of the request determines the response and resolution time.

Technical account manager

All accounts include the service of a technical account manager (TAM) to help drive the success of a customer's application security program. The TAM (usually a local Capgemini/Sogeti consultant) serves as the customer's liaison via the platform and the testers; manages contract issues, renewals, and support requests; and coordinates Sogeti resources including system and process experts as necessary to drive adoption and customer success.

Capacity and performance management

All tiers of the Sogeti Application security testing infrastructure are proactively monitored for capacity and performance. Our architecture allows for addition of capacity to applications, databases, and storage. Capacity is increased as required as the customer's utilization of Sogeti Application security testing expands.

Additional security testing services

Other Sogeti security testing services can smoothly complement Sogeti Application security testing:

- Manual code review can add additional security expertise for highly critical software on top of static application security testing;
- Penetration testing can find and exploit remaining vulnerabilities, including infrastructure vulnerabilities, once the application is in production in the real deployment infrastructure;
- Product security evaluation, performed from our licensed IT Security Evaluation Facility, can guaranty best-in-class security and lead to official security certification (Common Criteria...);
- Security consulting can help remediate vulnerabilities and improve the secure software development lifecycle;
- Application security training and awareness can help developers adopt better security practices.

Availability service-level objective

Sogeti Application security testing is designed for an availability service-level objective of 99.5 percent. The availability service-level objective shall not apply to performance issues:

- Caused by overall Internet congestion, slowdown, or unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks, etc.
- That resulted from actions or inactions of the customer (unless undertaken at the express direction of Sogeti) or third parties beyond the control of Sogeti;
- That resulted from the customer's equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Sogeti;
- That resulted from scheduled infrastructure maintenance downtime to implement major version upgrades.

Assumptions

- For static assessments, an application is defined as a deployable unit of code consisting of a collection of source and/or byte code instruction files that:
  - Can deliver some or all of the functionality of a business application
  - Is written in the same technology family
  - Is built on a single platform
  - Does not include any loosely coupled components
  - Can be configured to run on an application server (e.g., a Web Application Archive [WAR] or Enterprise Archive [EAR] file for a Java application) or, for a .NET application, is defined as a solution in team foundation server. Mobile applications must meet the minimum requirements for the supported language version.
- For dynamic assessments, an application is defined as a fully qualified domain name (FQDN) and has a single authentication management system. Customer must confirm that its Web application and user credentials are functioning prior to the security assessment. In addition, all functional and performance testing should be completed by this time, and the application's code should be frozen for the duration of the security test engagement. The customer is required to provide a formal authorization to perform a security assessment of the application.
- A subscription is valid for a single application, which cannot be changed during the subscription term purchased.
- The customer is in charge of maintaining the list of authorized users who may access the system, including creation of usernames and passwords and keeping list accurate and confidential according to the customer's internal policies.
- Sogeti Application security testing service will be performed remotely by Sogeti testers. Sogeti may choose to utilize qualified HPE testers to perform the services.
- Sogeti Application security testing service does not contemplate the sale of products or support services, which shall require the necessary terms and conditions for such purchase pursuant to separate agreement between the parties. Any software that Sogeti uses to provide security assessments will not be provided to the customer.

How do I start?

Sogeti Application security testing service makes it simple and fast to initiate fundamental security controls, without upfront investment, whether you have just a few applications or are looking to launch a comprehensive security program across your organization.

You contract with your local Capgemini or Sogeti company to buy the number of Assessment Units your need, we install your customer portal within days and you're ready to start! There is no minimum quantity, you can begin with a small number and buy additional Assessment Units when the service has proved efficient in your organization and needs to be extended; or you can buy a large number to reduce costs. Just contact us and let's get started!

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Hewlett Packard Enterprise

SOGETI

For more details contact:

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

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 out more:

www.capgemini.com/cybersecurity
or
www.uk.sogeti.com/services/cyber-security/application-security

MCOS_GI_AP_20170201