APPLICATION SECURITY TESTING SERVICES

Application security testing services

Applications often have badly written code, bugs or vulnerabilities in their source code. Developers can also inadvertently use vulnerable components during the application development process, and both situations can leave the application vulnerable to exploitation.

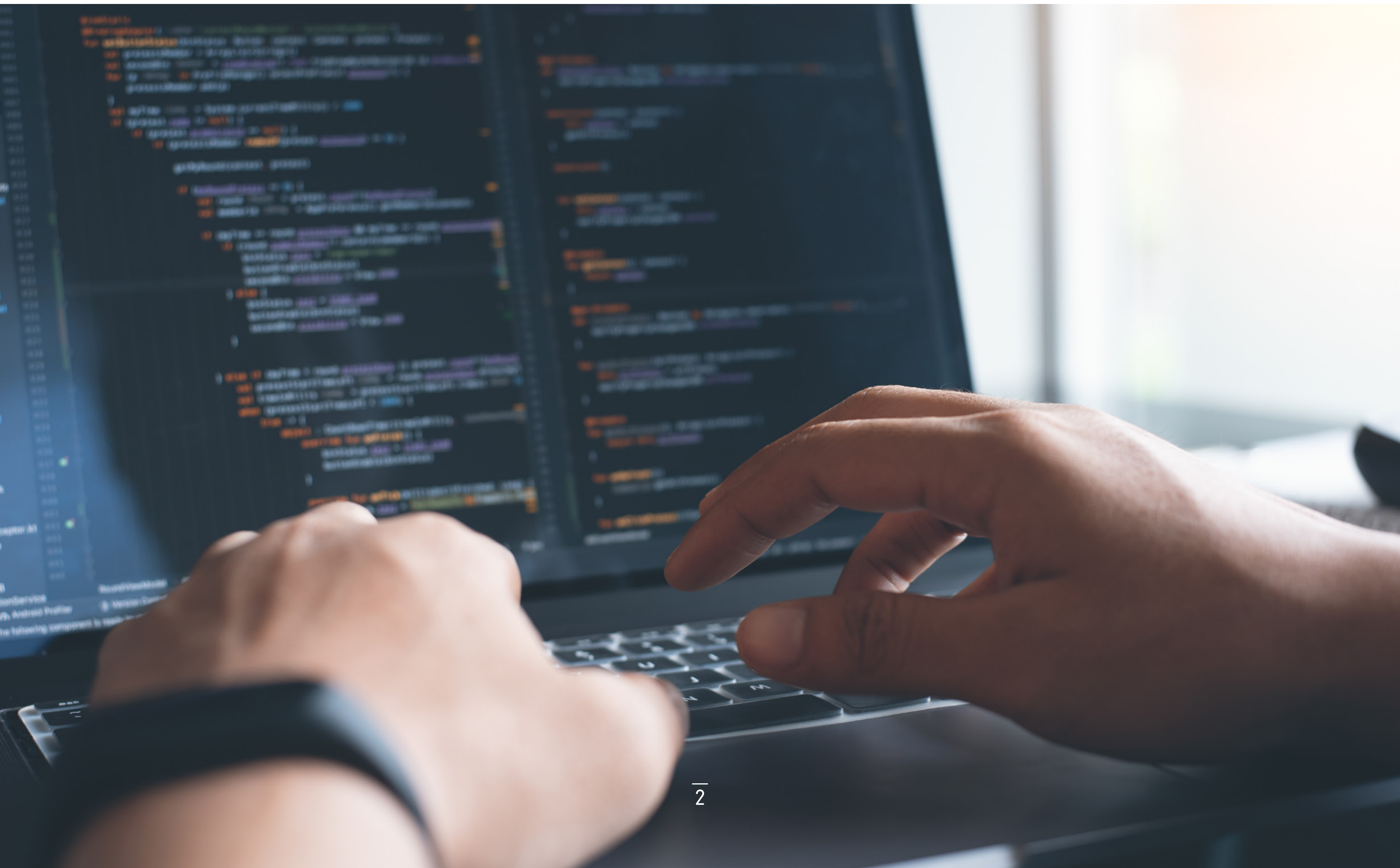
Application Security Testing (AST) is part of the software development lifecycle aimed at identifying and mitigating those issues. AST encompasses various techniques and tools to assess the security posture of an application, detect vulnerabilities, and provide recommendations for remediation.

It is now increasingly common for organisations to find their applications have been compromised because of failures to build adequate security into their source code or because they have been unable to control their software supply chain. In fact, some of the most famous hacks in history can be wholly or partly traced back to compromised software.

To help organisations mitigate this risk Computacenter delivers comprehensive Application Security Testing Services for our customers. We help customers to analyse source code and container images and to identify vulnerable code or bugs.

We also support in the Management of Software Bill of Materials lists (SBOMs), which detail the components of an application, helping to identify and resolve dependencies and license issues. We help organisations to choose the right solution for their environment, we will fully implement it into the development process and our experts can help developers enrich the application lifecycle with security measures. We also show developers how they can better interpret security insights and use them to improve their coding.

At Computacenter, we understand the dynamics of the evolving technology landscape and are skilled in the integration of security solutions into your development lifecycles. We can help ensure that your organisation is not only protected from today's threats but is also enabled to fully leverage the benefits of digital transformation.



Application security testing

Key types of testing

As part of our Application Security Testing (AST) services, Computacenter undertakes an Engineering Requirements assessment to collect the developer requirements for their next application development. We take these requirements, leverage our excellent market insight and utilise our huge partner network to help us select the right solution for our customers. Once selected we implement the solution into customer CI/CD pipelines, application runtimes and registries, and in doing so help organisations to better protect their applications. Our AST services covers all common AST types:

Static Application Security Testing (SAST)
SAST is a white-box testing method that analyses the source code, bytecode, or binary code of an application to identify vulnerabilities. It helps detect issues like code injection or improper access control during the development phase.

Dynamic Application Security Testing (DAST)
DAST is a black-box testing method that evaluates a live application for security vulnerabilities. It simulates attacks on the application and identifies issues like SQL injection, cross-site scripting, and insecure configurations.

Interactive Application Security Testing (IAST)
IAST combines aspects of both SAST and DAST, monitoring the application during runtime to provides real-time feedback on security vulnerabilities.

FEATURES	SAST	DAST	IAST
Reactive Scanning			✓
Proactive Scanning	✓	✓	
Black Box Testing		✓	
White Box Testing	✓		✓
Source Code Analysis	✓		
Runtime Testing		✓	✓

What is SBOM

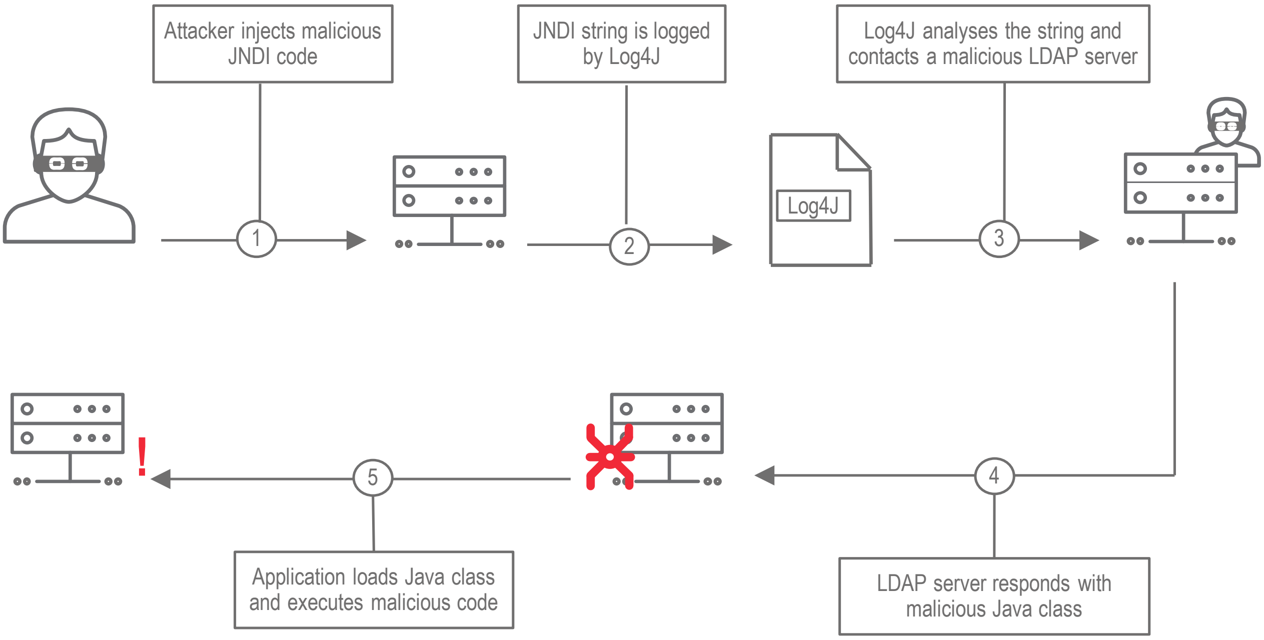
The notorious Log4j and the Log4Shell vulnerabilities highlighted the fact that companies often do not know which software components are being used in their applications. At the start of Log4Shell incident, many companies were still convinced that they were not affected by the vulnerability. However, more detailed analyses of their applications showed that Log4j was built into many of their applications by default, regardless of whether it was used or not. Full transparency about the software artefacts used or built-in is therefore becoming more and more critical to assessing the security risk of an application. The Cyber Resilience Act in the EU and Executive Order 14028 in the United States, which was issued to "improve the nation's cyber security", requires companies to create a software bill of materials (SBOM) for their products. This should lead to better insights into applications and a better understanding of the risks.

Log4j - What happened?

Log4j is a widely used Java library for logging messages in applications. In mid-December 2021, a critical vulnerability was discovered in Log4j, which became known as "Log4Shell".

The Log4Shell vulnerability allowed attackers to execute arbitrary programme code, load malware or steal data. Log4j is used in many applications, servers and network technologies. The vulnerability was initially considered very easy to exploit, and potentially made several billion computers worldwide vulnerable to exploitation.

Whilst updates have been made available to close the vulnerability, software vendors and those responsible were still required to integrate the updated Log4j library into their products and to check their systems for possible exploitation. Despite this there continue to be examples of criminals exploiting the vulnerability and successfully attacking systems.


Attacker injects malicious JNDI code
JNDI string is logged by Log4J
Log4J analyses the string and contacts a malicious LDAP server
1
2
Log4J
3
4
LDAP server responds with malicious Java class
5
!
Application loads Java class and executes malicious code

How an attack using the Log4Shell vulnerability operates

SBOM management

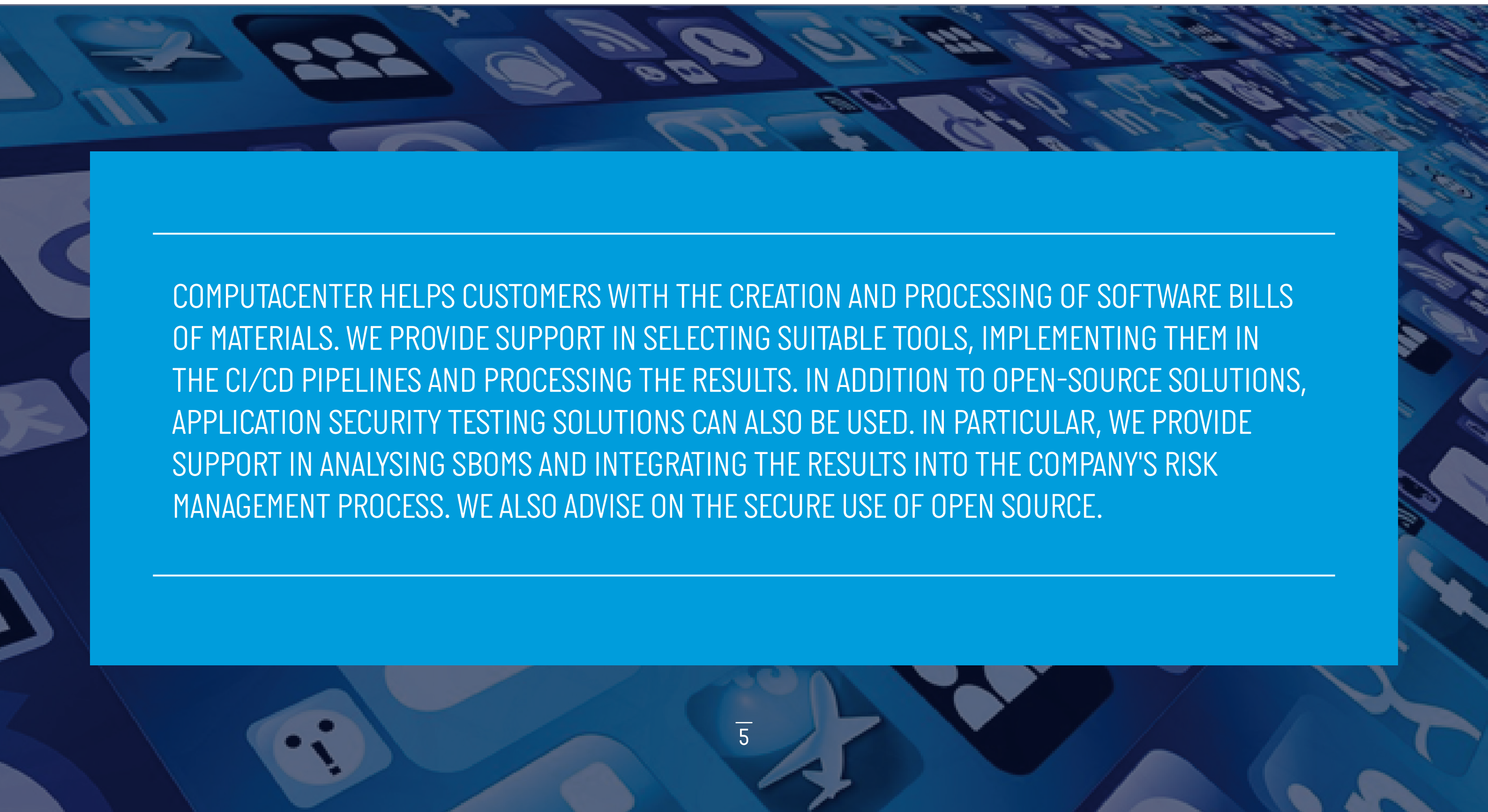
Software bill of material

A software bill of material (SBOM) lists the components of an application in detail. SBOMs can be generated using various tools that are integrated directly into the CI/CD pipelines. CycloneDX and SPDX are seen as the established standards for cataloguing open-source license compliance in SBOMs, but because the content of an SBOM is written in text form and can run to tens of thousands of lines long, human analysis is almost impossible.

In addition, effective analysis of an SBOM should look further than just the list of components and licences used in an application. Ideally the results of vulnerability scans should also be integrated into an SBOM. All of which means that most organisations struggle to address this issue in house and are increasingly reliant on outsourced expertise.

This should not prevent organisations from investing in SBOM assessment, in fact it is critical to minimising the risk of exploitation. In addition, companies should also request SBOMs for the commercial applications used by their suppliers, and the results of any SBOM analysis must be fed into the corporate risk management process where it exists. Although it should be noted that such corporate risk process often do not operate to excepted standards in most Open-Source Programme Offices (OSPO).

SOFTWARE BILLS OF MATERIALS ARE A VITAL PART OF SECURING THE WIDESPREAD USE OF OPEN SOURCE.



COMPUTACENTER HELPS CUSTOMERS WITH THE CREATION AND PROCESSING OF SOFTWARE BILLS OF MATERIALS. WE PROVIDE SUPPORT IN SELECTING SUITABLE TOOLS, IMPLEMENTING THEM IN THE CI/CD PIPELINES AND PROCESSING THE RESULTS. IN ADDITION TO OPEN-SOURCE SOLUTIONS, APPLICATION SECURITY TESTING SOLUTIONS CAN ALSO BE USED. IN PARTICULAR, WE PROVIDE SUPPORT IN ANALYSING SBOMS AND INTEGRATING THE RESULTS INTO THE COMPANY'S RISK MANAGEMENT PROCESS. WE ALSO ADVISE ON THE SECURE USE OF OPEN SOURCE.

Developer enablement

Application security testing tools, SBOM generation, bug reports will all generates security insights, often in the form of vulnerability descriptions. These can be difficult for software developers to read and interpret, particularly as the measures needed to rectify the findings are not always included in the descriptions.

So, whilst many developers may be aware that their code could have vulnerabilities, they don't really know how to deal with them. This leads to frustration within the developer community and in some cases the decision to completely ignore any reported security vulnerabilities.

To address this, Computacenter offers support for developer enablement. Our experienced consultants review vulnerability data together with the developers, help them to understand the risk context and discuss the possible measures for remediation. Our consultants will work as part of the product team, so that there are aware of current state of development and can suggest both code optimisation and contextual measures to address the identified vulnerabilities. This approach can benefit both highly experienced, and junior, developers.

In addition, Computacenter will develop tailored instructions to guide the organisation as to how they approach the creation of future secure code. These "Secure Coding Guidelines" are used to communicate to developers which security requirements must be adhered to in order to comply with both internal company policy and governance. Some customers have recorded videos explaining these guidelines and have then added them to central learning platforms to help ensure these guidelines are embedded into all future application development activity.

Cloud security

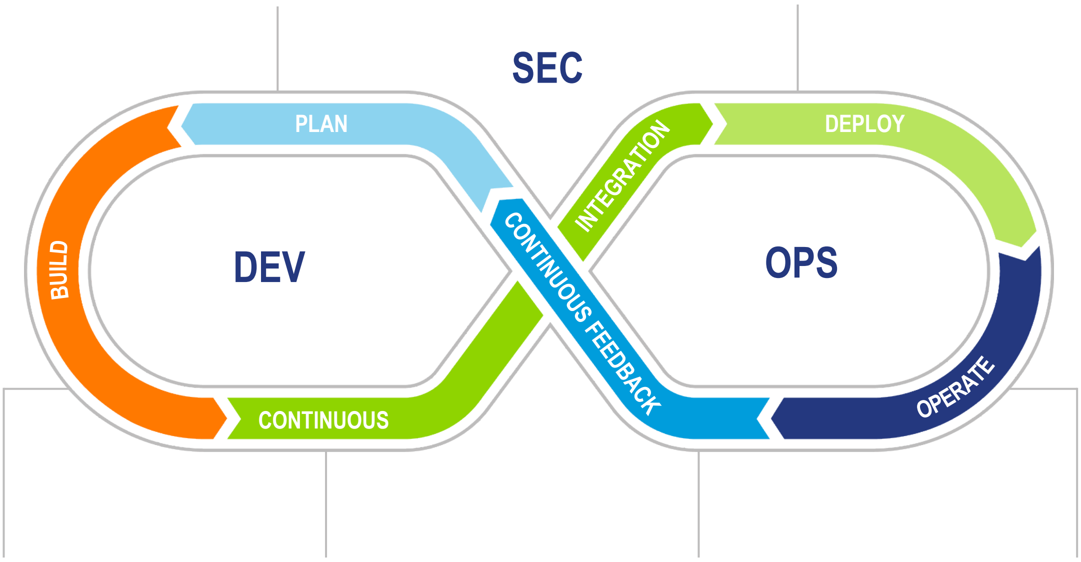
DevSecOps

Application Security Testing is a key part of Computacenter's DevSecOps portfolio of service offerings. DevSecOps, utilises the principles of software development to protect underlying platforms and applications throughout their entire lifecycles. This ensures that organisations can leverage the benefits of continuous software development and updates without exposing applications and platforms to new threats.

Computacenter offers consulting services to support the creation of operational processes, architectural advice to help secure apps and platforms, as well as technology solutions. We assist in establishing security guidelines to identify risks from the outset and implement appropriate countermeasures, all aimed at providing secure applications and platforms. Key areas of focus include container exposure and compliance management, secrets management within clusters, and role modelling for Kubernetes platforms. In terms of application security, our focus areas include static and dynamic application security testing (SAST, DAST), dependency tracking, SBOM generation, and security enablement for developers.

- Working Culture
- Security Framework
- Processes & Methods
- Security Enablement

- Automated Governance
- Admission Controller



- Nano Segmentation
- Kubernetes RBAC
- Access Management
- API Security
- Software Signing

- Embedded CI/CD Scanning
- Secret Management
- Software Signing
- Software Composition Analysis
- In-App Security (SAST/DAST)

- Vulnerability Management
- Posture Management
- Penetration Testing

- Runtime Protection
- DDoS Protection
- Cyber Defence Services
- Log Management

Why Computacenter

The current standard of cloud-native software development involves the use of microservices, pipelines, and container platforms, alongside public, private, or hybrid cloud platforms. Principles such as Infrastructure-as-Code, Immutable Infrastructures, and Application Lifecycle Frameworks are common standards. Protecting such environments effectively against threats requires a variety of security measures. Within its cloud security offerings, Computacenter assists companies to integrate security across the entire cloud-native stack, from developing security guidelines to implementing contemporary technologies like cloud-native application protection platforms and operating cloud environments. Our services include Cloud Security Advisory, DevSecOps, and XaaS Security, tailored to each platform. Computacenter offers a full spectrum of services, from empowering software developers, implementing cloud-native security mechanisms through to operating secure cloud environments, we help our customers to overcome challenges such as skill shortages, open-source management, or TCO optimisation. We understand the dynamics of the changing technology landscape and seamlessly integrate security solutions into our customers' digital initiatives.

Our services include

- Cloud Security Advisory - Security concepts for dynamic environments
- DevSecOps - Security for containers, orchestrators, pipelines and Shift-left security for developers
- XaaS Security – Security for private, public, multi or hybrid cloud. We have the right solution for every platform!

Computacenter offers a full spectrum of services, from empowering software developers, implementing cloud-native security mechanisms through to operating secure cloud environments, we help our customers to overcome challenges such as skill shortages, open-source management, or TCO optimisation. We understand the dynamics of the changing technology landscape and seamlessly integrate security solutions into our customers' digital initiatives.

Computacenter (UK) Ltd
Hatfield Avenue, Hatfield, Hertfordshire AL10 9TW, United Kingdom

computacenter.com
+44 (0)1707 631000

Computacenter is a leading independent technology and services provider, trusted by large corporate and public sector organisations. We help our customers to source, transform, and manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 20,000 people worldwide.