White paper

BROADCOM SOFTWARE

HOW BROADCOM® SOFTWARE INTEGRATES DEVSECOPS INTO THE DX NETOPS SDLC

INTRODUCTION

The recent rash of vulnerabilities such as Sun Burst and Log4j has led many enterprises to reimagine their DevOps security. To secure their DevOps environments – and ensure the continually flow of innovative applications and services – organizations recognize the need to remediate vulnerabilities the moment they arise.

This fundamental requirement to incorporate security into the development process had led to the emergence of DevSecOps. The focus of DevSecOps is on producing more secure software, including processes for secure development and delivery, as well as recommendations for securing deployment. Its primary focus is to ensure loopholes and weaknesses are discovered as early as possible through monitoring and analytics This way, remediation action can be implemented at an early stage and more efficiently.

Executive Summary

The future is all about connectivity. Forward-thinking organizations are dramatically expanding their network connectivity in response to trends such as hybrid working, cloud migration, and SD-WAN adoption. Make no mistake, the internet is the new network and the enterprise network is now...anywhere.

The DX NetOps network monitoring platform from Broadcom Software provides enterprises with the visibility to assure network delivery from the core network to beyond the edge of the data center.

The DX NetOps development organization within Broadcom® Software has recently transitioned from DevOps to DevSecOps to deliver enterprise-grade reliability and security. And as the teams move to DevSecOps, there are a plethora of potential concepts and approaches to apply.

This paper highlights several key approaches that have been adopted by the DX NetOps development organization. It explores the core systems the team uses for DevSecOps, including Jenkins, GitHub, and shift left security. It reveals how Broadcom Software adheres to security best practices – such as the Secure Software Development Lifecycle (SSDLC).

The paper also highlights how the organization works with expert teams to identify, report, and remediate vulnerabilities. Plus it shows how security is baked into every phase of the SDLC, from plan and build, to deploy and operate.

By adopting DevSecOps across the software development lifecycle (SDLC), Broadcom Software is ensuring DX NetOps remains current with enterprise security guidelines and adapts proactively and intelligently to new vulnerabilities.

AS PART OF ITS MOVE TO DEVSECOPS, BROADCOM SOFTWARE AIMS TO ENSURE STANDARD AND RELIABLE BUILD SYSTEMS

Securing Software Development

So how is the DX NetOps development organization using DevSecOps to secure DX NetOps network monitoring?

Like many enterprise software solutions, DX NetOps is written using multiple development languages, including C, C++, Java, and Python. It also supports various operating systems (OS) and hardware platforms. As part of its move to DevSecOps, Broadcom Software aims to ensure standard and reliable build systems.

The following are the core systems Broadcom Software uses for DevSecOps:

- **Jenkins:** Jenkins is the build automation system of choice for Broadcom Software. Jenkins is an open-source server that helps automate various software development efforts, including builds, testing, and deployment. With these capabilities, Jenkins facilitates continuous integration (CI) and continuous delivery (CD).

  A widely accepted system enables teams to create freestyle and pipeline-based build jobs. Using pipeline-based build jobs, Jenkins allows developers to customize automation code to their specific needs. To streamline the release process, Jenkins is also available with multiple plugins that support a range of actions, such as parameter-based execution and job sequencing.

  These capabilities give the product team complete control over software builds while limiting manual interventions and the risk of human errors. This is critical as builds are executed at high pace across multiple feature and maintenance code branches. In addition, Jenkins enables CI, ensuring the right automations are executed as soon as code changes are committed.

- **JFrog Artifactory:** This is the artifact hosting system used by Broadcom Software. JFrog Artifactory provides end-to-end automation and management of all the artifacts, binaries, packages, files, containers, and components for use throughout the software supply chain.

  This system helps Broadcom Software manage third-party and DX NetOps artifacts. The organization also leverages built-in security features of JFrog, such as Xray, for detecting potential vulnerabilities.

- **GitHub:** Broadcom Software uses GitHub as the source code control system and central repository. GitHub is the de facto standard for source code management. This tool helps the team manage the various development and release states of the source code.

TO ENSURE STRICT GOVERNANCE AND COMPLIANCE, BROADCOM SOFTWARE CONFIGURES THESE ENVIRONMENTS WITH APPLICABLE PERMISSIONS AND AUDIT CAPABILITIES.

- **Build Agents:** Build Agents are the environments in which the actual build takes place. These include physical, virtual, and containerized systems. Depending on build needs, the required compilers and development software are installed, managed, and audited on these systems. This can include C/C++ compilers and Java Development Kits.

  To ensure strict governance and compliance, Broadcom Software configures these environments with applicable permissions and audit capabilities. The security is also strengthened with appropriate firewall configuration, consistently updated anti-virus signatures, and regular OS security patches.

- **Shift-Left Security:** Broadcom Software has adopted a shift-left approach to detect vulnerabilities at an early stage during the development or build phase. The following tools are used to support these efforts:

  - **Coverity:** Provides a static analysis at the source code level and identifies security and code quality issues. Through the CI processes automated in Jenkins, Coverity scans are scheduled after every change into the source code. This helps eliminate issues even before the code is built and released for testing.

  - **Black Duck:** Another tool that helps identify third-party components integrated into the software and flag potential risks, including functional, security, and license issues. Once again, regular Black Duck scans of binaries and signatures help Broadcom Software to identify risks before the code is moved into subsequent pipeline stages.

BROADCOM SOFTWARE PRODUCT DEVELOPMENT TEAMS COMPLY WITH THE INTERNAL PRODUCT SECURITY PROCEDURE, WHICH PROVIDES GUIDELINES AND OBJECTIVES FOR THE SECURE DEVELOPMENT OF SOFTWARE PRODUCTS.

Securing Software Delivery

The organization adheres to the SSDLC and security-related best practices to build secure software and to enforce security requirements throughout the development cycle. Key aspects include education, architectural risk assessment, code analysis, penetration testing, and continuous tracking of known vulnerabilities and attack vectors.

Broadcom Software product development teams comply with the internal Product Security Procedure, which provides guidelines and objectives for the secure development of software products. The procedure identifies requirements for security standards and provides strategies and tactics for implementing security during each phase of a product's development lifecycle.

Responsibility for managing product security is not limited to the product teams. The Security Champions, the central SSDLC owners, and the Product Security Incident Response Team (PSIRT), work with product development and third-party security consultants on the identification, reporting, and remediation of vulnerabilities associated with the products. In addition, education and other resources are available to assist Broadcom Software developers with secure coding.

THE SSDLC MUST BE FIRM IN ITS APPROACH TO SECURITY BUT FLEXIBLE ENOUGH IN ITS APPLICATION TO ACCOMMODATE VARIATIONS, INCLUDING DIFFERENT TECHNOLOGIES AND THE RISK PROFILE OF THE APPLICATIONS.

Security at Every Stage of the Development Lifecycle

SAFECode states, in its Principles for Software Assurance Assessment that, "Software assurance assessment should primarily focus on the secure software development process and its application to the product being assessed, while taking into consideration the context of a product's intended operating environment. There is no single practice, tool, or checklist that acts as a 'silver bullet' and guarantees better software assurance. Rather, the efficacy and efficiency of software security practices and tools varies based on how they are applied and whether they are implemented as part of a holistic software development process within each unique organization."

In other words, software assurance is not achieved through a single practice, tool, or checklist. Rather, it is the result of a comprehensive secure software engineering process that spans development, from early planning through the end of life. It is also important to realize that, even within a single company and associated SSDLC, there is no one-size-fits-all approach. The SSDLC must be firm in its approach to security but flexible enough in its application to accommodate variations, including different technologies and the risk profile of the applications.

In simplest terms, a product's lifecycle can be divided into the seven stages of Plan, Code, Build, Test, Release, Deploy and Operate:

Over the course of its lifecycle, a product will often repeatedly move through each of these stages. In an agile environment, each sprint typically includes aspects of all or most of these steps compressed into a shortened cycle where product development does not follow a straight flow. Rather, the sprint contains frequent iterations of parts of this flow on a weekly or even daily basis. This lifecycle flow is a robust model to which Broadcom Software anchors security-related activities. Underlying these stages are basic foundational, cross-organizational services.

Foundation

A successful security program requires a strong internal security support organization that manages and provides the foundation for the SSDLC, including collecting and sharing knowledge and experiences across the organization. At Broadcom Software, this is managed by central SSDLC and PSIRT owners working together with cross-business unit Security Champions. These teams collaborate to set the internal standards for

THE SSDLC OWNER DEFINES THE PROCESS PRINCIPLES FOR BROADCOM SOFTWARE AND IS INDEPENDENT OF THE PRODUCT TEAMS

security and advise product teams during the SDLC. The teams also work closely with Support and IT organizations to ensure comprehensive coverage across the product life cycle.

The SSDLC Owner defines the process principles for Broadcom Software and is independent of the product teams. Their responsibilities include maintaining procedures, ensuring tools and services support the SSDLC. In partnership with Security Champions and third-party security consultants, they also act as an independent body to validate the security of the products.

Internal development procedures include guidelines and requirements on what, when, and how security activities should take place. This includes activities for all the life cycle stages and covers items such as Training, Coding Guidelines, Architectural Risk Analysis, Code Analysis, Penetration Testing, and Vulnerability Response.

When applicable, examples and template artifacts are used by the product teams in their development activities. The SSDLC Owner actively participates in Secure Development Best Practices (e.g., ISO27034, SAFECode, OWASP, BSIMM) to better understand how secure coding practices can be improved.

THE SSDLC OWNERS, SECURITY CHAMPIONS, AND THIRD-PARTY CONSULTANTS ALL PLAY IMPORTANT ROLES AS INDEPENDENT INTERNAL AND EXTERNAL CONSULTANTS TO VERIFY A PRODUCT'S SECURITY

The SSDLC Owners, Security Champions, and third-party consultants all play important roles as independent internal and external consultants to verify a product's security. However, everyone involved in product development is engaged in, has knowledge of, and shares secure development practices. The SSDLC Owners update internal guidance, training, and best practices to enhance the information provided to the development organization.

To simplify this process, Broadcom Software has an Internal Security Portal where current information is available, and cross organization collaboration with Security Champions. Channels also exist through which employees share security information or ask questions. The SSDLC Owners, the PSIRT, and the Security Champions act as a virtual security special interest group, that ensures all products move through appropriate SSDLC steps and also share information on their experiences with complex issues and how the process can be enhanced.

Plan

Broadcom Software believes that a focus on security from the outset, together with security 'baked' into the entire solution, can help bring products to market faster that are more secure. This includes ensuring that all teams have access to appropriate security training as well as comprehensive programs of role-based and web-based training spanning technologies, risks, and tools.

BROADCOM SOFTWARE BELIEVES THAT A FOCUS ON SECURITY FROM THE OUTSET, TOGETHER WITH SECURITY 'BAKED' INTO THE ENTIRE SOLUTION, CAN HELP BRING PRODUCTS TO MARKET FASTER THAT ARE MORE SECURE

During the planning phase, product teams create an initial mapping of privacy and security requirements applicable to a solution. Considerations include the type of data handled by the solution, how and where the solution is implemented, and industry requirements. Having checklists and central guidance from the central SSDLC Owner helps in planning and implementing data protection controls.

Based on the risk profile, the target market, and the development stage of the product, an Architectural Risk Analysis (also called Threat Modeling) helps identify design-level issues or threats in advance of implementation to help address flaws before coding begins.

Finally, this is also the appropriate time for the product team to register any third-party components included in the development, which ensures licensing compliance and provides an opportunity for a risk-based assessment of the components.

Code

During the coding phase, developers can take advantage of static application security testing tools (SAST), which focus on detecting security issues directly from the source code. This includes deprecated/unsafe functions as well as complex issues requiring further analysis, such as Data Flow, Semantic, Control Flow, Configuration, and Structural issues. By identifying different issues, including OWASP Top 10 vulnerabilities and CWE/SANS-Top 25 Programming Errors during coding, the developer can more quickly address the issue, learn from the findings, and better understand how to write secure code and/or identify the need for additional training.

DURING THE CODING PHASE, DEVELOPERS CAN TAKE ADVANTAGE OF STATIC APPLICATION SECURITY TESTING TOOLS (SAST), WHICH FOCUS ON DETECTING SECURITY ISSUES DIRECTLY FROM THE SOURCE CODE

Depending on the product's risk profile, peer code review may be required. This way, another senior developer familiar with the code, secure coding practices, and the expected functionality of the solution reviews the code.

Finally, the development teams determine whether vulnerabilities in a third-party component can affect the product. Automated scanners and procedures assist in identifying the best course of action, whether upgrading or substituting the component. If the component is replaced, the bill of materials is adjusted accordingly, and the new component or version is included in ongoing vulnerability tracking.

Build

The formal product build is issued on a regular basis, and the code base typically undergoes an audit using the same static application security testing tools used on the developer's workstation during the Code phase. This helps ensure all issues are captured and provides an additional layer of verification.

THE SYSTEM TEST TEAM CAN LEVERAGE THE EXPERIENCE AND THE TRAINING RECEIVED DURING THE PLANNING PHASE TO SET UP AUTOMATIC AND MANUAL TESTING.

During the build process, procedures are triggered to initiate code integrity tracking which creates unique fingerprints for the build, and links it to the source code, the bill of materials, and the system used to create the build. This ensures that the code has not been tampered with after the build and provides further confirmation that the team understand what went into the build.

Test

When builds are ready for integration into full system delivery, the team initiates a more complete system test. This is repeated on a regular basis throughout the SDLC. The product team works with the SSDLC owner and Security Champions to assess potential attack surfaces and to set up automatic penetration testing, scheduled regularly to scan the application for weaknesses.

In addition to the tool-based approach, the System Test team can leverage the experience and the training received during the planning phase to set up automatic and manual testing. These test plans may include tests derived from both internal procedures and industry best practices such as SAFECode Fundamental Practices and OWASP Testing Guide.

This can include low-level details such as testing of edge cases and boundary conditions based on the architecture in use, as well as higher-level requirements such as proper encryption of personally identifiable information (PII) at rest and in transit, for example by using least privilege access. Test cases are often a combination of verification of expected behavior as well as negative requirements where carefully selected data helps the auditors verify how the application handles edge cases.

HIGH-RISK PRODUCTS RECEIVE MORE ADVANCED PENETRATION TESTING, WHICH IS A COMBINATION OF AUTOMATIC AND MANUAL TESTS PERFORMED BY AUDITORS.

Release

Before a product is generally available, its risk profile is assessed. Based on this assessment, high-risk products receive more advanced penetration testing, which is a combination of automatic and manual tests performed by auditors. These tests are performed in an environment built using the planned template architecture and configured according to documented best practices.

The tests may include multiple weeks of testing various security aspects of the solution, interviews with developers and architects, manual penetration testing scans by penetration testing tools, fuzz testing, as well as automated scans of the infrastructure and known/common vulnerabilities in third-party components and their configuration. Identified vulnerabilities are tracked in a central defect tracking system together with an associated risk rating (Critical/High/Medium/Low + CVSS score) and are not approved as remediated until a security expert has performed a post fix validation.

Finally, before any product is released, Broadcom Software performs antivirus/antimalware scanning on the final master media.

TO ADDRESS VULNERABILITY INFORMATION, BROADCOM SOFTWARE HAS A SET OF POLICIES AND PROCEDURES, INCLUDING COMPREHENSIVE INTERNAL VULNERABILITY HANDLING PROCEDURES.

Deploy

For traditional distributed on-premises solutions, the Deploy phase is typically performed by the client or professional services team.

Operate

Through the remainder of the product's lifecycle, until it is no longer supported, the product team works with a number of central functions to manage the product from a security perspective. This can include continuous scanning for vulnerabilities in native code and in third-party components. This can also include remediating reported vulnerabilities, issues identified by development after the release, or by automated tools and processes to identify vulnerability reports concerning third-party components.

Broadcom Software has comprehensive incident response and vulnerability handling policies. The development team works closely with leading vulnerability research entities to monitor a large number of sources for vulnerability information, including vendor websites, public mailing lists, and other security-related websites.

To address vulnerability information, Broadcom Software has a set of policies and procedures, including comprehensive internal vulnerability handling procedures. In accordance with those procedures, vulnerability experts and Security Champions focus on complex vulnerability issues, and work with Technical Support, Sustaining Engineering, Development, and Product Management to ensure each vulnerability issue is properly resolved.

To address validated vulnerability issues, security notices, patches, and remediation information are posted on the Support website. Additionally, the team may disseminate security notices and advisories to customer email lists, public mailing lists (mentioned above), and to various vulnerability-related organizations such as CERT and Mitre CVE.

BROADCOM SOFTWARE IS ABLE TO DELIVER SOFTWARE THAT GIVES CUSTOMERS ENTERPRISE-GRADE RELIABILITY AND SECURITY.

Summary

With the above secure development and delivery processes, the DX NetOps product team was able to address Log4j 2.x and other vulnerabilities very quickly. With strong DevSecOps processes, Broadcom Software is able to deliver software that gives customers enterprise-grade reliability and security. With these approaches, Broadcom Software can ensure DX NetOps remains current with enterprise security guidelines and reacts quickly to new vulnerabilities.

To learn more about DX NetOps, please visit broadcom.com/netops

About Broadcom Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software has an extensive portfolio of industry-leading infrastructure and security software, including AIOps, Cybersecurity, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com

DXNETOPS-SDLC-WP100 September 6, 2022