ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

Μελέτη DevSecOps εργαλείων

Πτυχιακή εργασία

Παναγιώτης Κολλιόπουλος

HAROKOPIO UNIVERSITY

SCHOOL OF DIGITAL TECHNOLOGY

DEPARTMENT OF INFORMATICS AND TELEMATICS

A study on DevSecOps tools

Bachelor thesis

Panagiotis Kolliopoulos

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

Τριμελής Εξεταστική Επιτροπή

Παναγιώτης Ριζομυλιώτης (Επιβλέπων)
Αναπληρωτής Καθηγητής, Πληροφορική και Τηλεματική,
Χαροκόπειο Πανεπιστήμιο

Καμαλάκης Θ.
Καθηγητής, Πληροφορική και Τηλεματική, Χαροκόπειο Πανεπιστήμιο

Τσαδήμας Α.
Ε.ΔΙ.Π., Πληροφορική και Τηλεματική, Χαροκόπειο Πανεπιστήμιο

Ο Παναγιώτης Κολλιόπουλος

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

3) Όπου υφίστανται δικαιώματα άλλων δημιουργών έχουν διασφαλιστεί όλες οι αναγκαίες άδειες χρήσης ενώ το αντίστοιχο υλικό είναι ευδιάκριτο στην υποβληθείσα εργασία.

Περιεχόμενα

Περίληψη

Η ραγδαία εξέλιξη των πρακτικών ανάπτυξης λογισμικού τα τελευταία χρόνια έχει οδηγήσει στην πρακτική του DevSecOps, όπου η ασφάλεια ενσωματώνεται απρόσκοπτα στον κύκλο ζωής της ανάπτυξης λογισμικού. Η παρούσα πτυχιακή εργασία, "Μελέτη DevSecOps εργαλείων", έχει ως στόχο να παράσχει μια ολοκληρωμένη εξέταση των εργαλείων και των τεχνολογιών που επιτρέπουν στους οργανισμούς να εφαρμόζουν αποτελεσματικά τις πρακτικές DevSecOps.

Η έρευνα ξεκινά με την παρουσίαση μιας εμπεριστατωμένης επισκόπησης της μεθοδολογίας DevSecOps, αναδεικνύοντας τη σημασία της για την αντιμετώπιση των αυξανόμενων προκλήσεων κυβερνοασφάλειας στην σύγχρονη εποχή. Διασαφηνίζει τις βασικές αρχές του DevSecOps, τονίζοντας την ανάγκη για συνεργασία, αυτοματοποίηση και συνεχή παρακολούθηση για την ενίσχυση της ασφάλειας σε όλη τη διαδρομή ανάπτυξης λογισμικού.

Η μελέτη αυτή εστιάζει κυρίως στην αξιολόγηση ενός ευρέος φάσματος εργαλείων DevSecOps, που κυμαίνονται από σαρωτές ευπαθειών και πλατφόρμες ανάλυσης κώδικα έως λύσεις orchestration και διαχείρισης ρυθμίσεων (configuration management). Τα εργαλεία αυτά εξετάζονται με βάση κριτήρια όπως η αποτελεσματικότητά τους στον εντοπισμό και τον μετριασμό των τρωτών σημείων ασφαλείας, οι δυνατότητες ενσωμάτωσης με δημοφιλείς αγωγούς development και deployment, η φιλικότητα προς τον χρήστη, η επεκτασιμότητα και η αποδοτικότητα κόστους.

Εκτός από την αξιολόγηση των επιμέρους εργαλείων, η παρούσα εργασία διερευνά τις προκλήσεις ενσωμάτωσης που ενδέχεται να αντιμετωπίσουν οι οργανισμοί κατά την εφαρμογή πρακτικών DevSecOps. Εμβαθύνει σε στρατηγικές για την ευθυγράμμιση των στόχων ασφάλειας με τις ομάδες ανάπτυξης και λειτουργίας και την προώθηση μιας κουλτούρας ευαισθητοποίησης σε θέματα ασφάλειας.

Για την απόκτηση των πληροφοριών αυτών χρειάστηκε να εξαντλήσουμε κάθε πηγή διαθέσιμη στον Ιστό, από επιστημονικά άρθρα, μέχρι διάφορες έρευνες, εργασίες και ιστοσελίδες στο Διαδίκτυο. Από την αναζήτησή μας αυτή εντοπίσαμε μια πληθώρα εργαλείων από τα οποία αποφασίσαμε να αναλύσουμε τα πιο δημοφιλή της σημερινής εποχής. Τέλος, από αυτά τα εργαλεία καταλήξαμε σε 8 εργαλεία τα οποία πληρούν ορισμένα κριτήρια που θέσαμε, τα οποία θα έθετε και όποιος οργανισμός σκεφτόταν να εντάξει στην καθημερινότητά του κάποιο εργαλείο DevSecOps.

Συνθέτοντας τα ευρήματα αυτής της ολοκληρωμένης μελέτης, η παρούσα εργασία αποσκοπεί στην παροχή πρακτικών συστάσεων για οργανισμούς που επιθυμούν να ξεκινήσουν ή να ενισχύσουν το ταξίδι τους στο DevSecOps. Συμβάλλει επίσης στην ευρύτερη γνώση του ρόλου των εργαλείων στη διαμόρφωση του μέλλοντος της ασφαλούς ανάπτυξης λογισμικού, με απώτερο στόχο την προώθηση ενός πιο ασφαλούς ψηφιακού οικοσυστήματος.

Λέξεις κλειδιά: DevSecOps, εργαλεία, κυβερνοασφάλεια, ανάπτυξη λογισμικού, ενσωμάτωση

Abstract (Περίληψη στα Αγγλικά)

The rapid evolution of software development practices in recent years has given rise to the paradigm of DevSecOps, where security considerations are seamlessly integrated into the software development lifecycle. This thesis, "DevSecOps Tools Study," aims to provide a comprehensive examination of the tools and technologies that enable organizations to implement DevSecOps practices effectively.

The research begins by presenting an in-depth review of the DevSecOps methodology, highlighting its significance in addressing the growing cybersecurity challenges in today's software landscape. It elucidates the core principles of DevSecOps, emphasizing the need for collaboration, automation, and continuous monitoring to enhance security throughout the software development pipeline.

The primary focus of this study is the evaluation of a wide array of DevSecOps tools, ranging from vulnerability scanners and code analysis platforms to orchestration and configuration management solutions. These tools are examined based on criteria such as their effectiveness in identifying and mitigating security vulnerabilities, integration capabilities with popular development and deployment pipelines, user-friendliness, scalability, and cost-efficiency.

In addition to assessing the individual tools, this thesis investigates the integration challenges that organizations might encounter when implementing DevSecOps practices. It delves into strategies for aligning security goals with development and operations teams and fostering a culture of security awareness.

To obtain this information, we had to exhaust every source available on the web, from scientific articles, to various research papers and Internet sites. From this search we came across a plethora of tools from which we decided to analyze the most popular ones of today. Finally, from these tools we came up with 8 tools that meet certain criteria that we set, which any organization would set and which would be considered by any organization thinking of integrating a DevSecOps tool in its daily routine.

By synthesizing the findings from this comprehensive study, this thesis aims to provide practical recommendations for organizations seeking to embark on or enhance their DevSecOps journey. It also contributes to the broader discourse on the role of tools in shaping

the future of secure software development, with the ultimate goal of fostering a more secure digital ecosystem.

Keywords: DevSecOps, tools, cybersecurity, software development, integration

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες/Ακρωνύμια

IaC	Infrastructure as Code
CI	Continuous Integration
CD	Continuous Delivery/Deployment
API	Application Programming Interface
SQL	Structured Query Language
XSS	Cross-Site Scripting
SCA	Software Composition Analysis
DAST	Dynamic Application Security Testing
IoT	Internet of Things
Ops	Operations
SAST	Static Application Security Testing
IDE	Integrated Development Environment
aws	Amazon Web Services
SSC	Security Standards Council
PCI	Payment Card Industry
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance
SOC2	Service Organization Control Type 2
SDLC	Software Development LifeCycle
SBOM	Software Bill of Materials

AST	Application Security Testing
AppSec	Application Security
IAST	Interactive Application Security Testing
RASP	Runtime Application Self-Protections
SLA	Service Level Agreements
SLO	Service Level Objectives
MTTR	Mean Time To Repair
QA	Quality Assurance
Devs	Development
InfoSec	Information Security
IP	Internet Protocol
VCS	Version Control System
MFA	Multi-Factor Authentication
OWASP	Open Web Application Security Project
SSRF	Server-Side Request Forgery
REST	Representational State Transfer
GraphQL	Graph Query Language
RBAC	Role-Based Access Control
SaaS	Software as a Service
JSON	JavaScript Object Notation
HTML5	Hyper Text Markup Language 5
AppScan	Application Scanning
CNAPP	Cloud Native Application Protection Platform
Aqua CSP	Aqua Container Security Platform
Microsoft ACI	Microsoft Azure Container Instances

GCP Marketplace	Google Cloud Platform Marketplace
IBM	International Business Machines
CISO	Chief Information Security Officer
JS	JavaScript
PHP	Hypertext Preprocessor
eBPF	Extended Berkeley Packet Filter
CPU	Central Processing Unit
CSPM	Cloud Security Pose Management
CDR	Cloud Detection & Response
LDAP	Lightweight Directory Access Protocol
CWE	Common Weakness Enumeration
RUM	Real User Monitoring
RCA	Root Cause Analysis
IDM	Identity Management
IPS	Intrusion Prevention System
URL	Uniform Resource Locator
VPN	Virtual Private Network
CPSM	Certified Professional in Supply Management
IT	Information Technology
CLI	Command-Line Interface
syslog	System Logging Protocol
SOAP	Simple Object Access Protocol
EC2	Elastic Compute Cloud
CPG	Code Property Graph
SAML	Security Assertion Markup Language

SSO	Single Sign-On
AI	Artificial Intelligence

Εισαγωγή

Στο διαρκώς εξελισσόμενο τοπίο της ανάπτυξης λογισμικού, η ασφάλεια έχει αναδειχθεί σε απαραίτητο κομμάτι της διαδικασίας ανάπτυξης. Καθώς οι οργανισμοί βασίζονται ολοένα και περισσότερο στην τεχνολογία για την προώθηση των λειτουργιών τους, η ανάγκη για ισχυρό και ανθεκτικό λογισμικό δεν ήταν ποτέ πιο κρίσιμη. Ο παραδοσιακός διαχωρισμός μεταξύ των ομάδων ανάπτυξης και λειτουργίας έχει δώσει τη θέση του σε μια πιο ολοκληρωμένη προσέγγιση γνωστή ως DevOps, με στόχο τον εξορθολογισμό και την επιτάχυνση του αγωγού παράδοσης λογισμικού. Ωστόσο, σε αυτή την εποχή των συνεχών απειλών και ευπαθειών της κυβερνοασφάλειας, το DevOps από μόνο του δεν επαρκεί. Εδώ έρχεται να βοηθήσει το DevSecOps, μια σημαντική αλλαγή που αγκαλιάζει την ασφάλεια ως αναπόσπαστο μέρος της διαδικασίας ανάπτυξης και λειτουργίας.

Το DevSecOps, μια σύντμηση των λέξεων Development, Security και Operations, αντιπροσωπεύει μια πολιτιστική και πρακτική αλλαγή που συγχωνεύει τις πρακτικές ασφάλειας στο πλαίσιο DevOps. Αυτή η συγχώνευση διασφαλίζει ότι η ασφάλεια δεν αποτελεί πλέον δυσχέρεια, ούτε και μεταγενέστερη σκέψη στη διαδικασία ανάπτυξης λογισμικού, αλλά μια προληπτική και συνεχή διαδικασία. Η ενσωμάτωση των πρακτικών ασφάλειας σε όλο τον κύκλο ζωής της ανάπτυξης λογισμικού επιτυγχάνεται μέσω μιας πληθώρας εξειδικευμένων εργαλείων και τεχνολογιών, συλλογικά γνωστών ως εργαλεία DevSecOps.

Η παρούσα εργασία, με τίτλο "Μελέτη DevSecOps εργαλείων", ξεκινά μια ολοκληρωμένη διερεύνηση του τοπίου των εργαλείων DevSecOps. Σε μια εποχή όπου οι κυβερνοεπιθέσεις έχουν γίνει όλο και πιο εξελιγμένες και διαδεδομένες, οι οργανισμοί πρέπει να υιοθετήσουν μια προληπτική στάση απέναντι στην ασφάλεια. Αυτή η προληπτική στάση καθιστά αναγκαία την κατανόηση και τη χρήση εργαλείων DevSecOps, τα οποία μπορούν να βοηθήσουν στον εντοπισμό και τον μετριασμό των ευπαθειών και των απειλών σε πρώιμο στάδιο της διαδικασίας ανάπτυξης.

Ο πρωταρχικός στόχος της παρούσας εργασίας είναι να παράσχει μια ανάλυση των εργαλείων DevSecOps, που περιλαμβάνει τις λειτουργίες, τα χαρακτηριστικά και τις δυνατότητες ενσωμάτωσής τους . Επιδιώκει να απαντήσει σε θεμελιώδη ερωτήματα όπως: Ποια είναι τα βασικά εργαλεία DevSecOps που διατίθενται στην αγορά; Ποιες είναι οι βέλτιστες πρακτικές για την επιλογή, την εφαρμογή και τη διαχείριση των εργαλείων DevSecOps;

Για την επίτευξη αυτών των στόχων, η παρούσα εργασία θα υιοθετήσει μια πολύπλευρη ερευνητική προσέγγιση. Θα ξεκινήσει με μια ολοκληρωμένη ανασκόπηση της βιβλιογραφίας γύρω από το DevSecOps, διερευνώντας το ιστορικό πλαίσιο, τα θεωρητικά θεμέλια και τις πρακτικές αυτού του αναδυόμενου κλάδου. Ακολούθως, θα διεξαχθεί μια έρευνα των εργαλείων DevSecOps, για να αναδειχθεί ο αντίκτυπος αυτών των εργαλείων στις προσπάθειες ασφάλειας των οργανισμών.

Τέλος, η έρευνα αυτή έχει ως στόχο να παράσχει πολύτιμες πληροφορίες για τους προγραμματιστές λογισμικού, τις ομάδες λειτουργίας, τους επαγγελματίες ασφαλείας και τους ηγέτες των οργανισμών που επιδιώκουν να υιοθετήσουν τις αρχές του DevSecOps και να ενσωματώσουν τα κατάλληλα εργαλεία στις ροές εργασίας τους. Φωτίζοντας το τοπίο των εργαλείων DevSecOps, η παρούσα εργασία φιλοδοξεί να συμβάλει σε όσα λέγονται σχετικά με την ασφάλεια του λογισμικού, σε έναν διασυνδεδεμένο κόσμο, όπου η καινοτομία και η ασφάλεια δεν είναι πλέον αμοιβαία αποκλειόμενες, αλλά μάλλον αλληλένδετες προς όφελος των οργανισμών και των ενδιαφερόμενών τους.

Τι ωθεί την υιοθέτηση DevSecOps

Καθώς τα λογισμικά συνεχίζουν να αναπτύσσονται ραγδαία στον τομέα της πληροφορικής, το DevSecOps και τα εργαλεία του γίνονται τα θεμέλια της ανταγωνιστικότητας στη σύγχρονη αγορά. Κάθε επιχείρηση πρέπει να γίνει μια ευέλικτη και καινοτόμα μηχανή παράδοσης λογισμικού για να επιβιώσει. Δεν πρέπει όμως να ξεχνάμε την ασφάλεια. Οι προγραμματιστές συχνά χρησιμοποιούν και κατεβάζουν ευάλωτα στοιχεία ανοιχτού κώδικα και πλαίσια εφαρμογών (application frameworks). Στον κόσμο του DevOps, οι οργανισμοί δημιουργούν εφαρμογές πιο γρήγορα, με αποτέλεσμα να έχουν ξεχάσει την σοβαρότητα της ασφάλειας. Οι πλατφόρμες cloud και οι συνεχείς κύκλοι ζωής παράδοσης συχνά παρακάμπτουν τις παραδοσιακές διαδικασίες και ελέγχους ασφαλείας. Η συνεργασία για την ασφάλεια πρέπει να είναι ευθύνη όλων. Οι οργανισμοί πρέπει να προσπαθήσουν να φέρουν άτομα όλων των ικανοτήτων σε υψηλό επίπεδο επάρκειας σε σύντομο χρονικό διάστημα ώστε να μπορούν να ανταποκρίνονται στα σύγχρονα δεδομένα. (Navdeep, 2023)

Τι είναι DevSecOps

Το DevSecOps είναι μια πρακτική κατά την οποία ενσωματώνουμε δοκιμές ασφάλειας (security tests) σε κάθε στάδιο της διαδικασίας ανάπτυξης λογισμικού. Περιλαμβάνει εργαλεία και διαδικασίες τα οποία ενθαρρύνουν την συνεργασία μεταξύ των προγραμματιστών, των ειδικών ασφάλειας, και των operation teams, να φτιάξουν λογισμικό, το οποίο είναι ταυτόχρονα αποδοτικό και ασφαλές. Η πρακτική αυτή φέρνει αλλαγές, που έχουν σαν συνέπεια, η ασφάλεια να είναι μια ευθύνη για όλους όσους φτιάχνουν το λογισμικό. (Amazon Web Services [aws], χ.χ)

Κεφ 1. DevOps και DevSecOps

1.1 Πως λειτουργεί το DevSecOps?

Για να υλοποιήσουμε την πρακτική DevSecOps οι ομάδες λογισμικού πρέπει πρώτα να υλοποιήσουν την μεθοδολογία DevOps και την συνεχή ενσωμάτωση (continuous integration).

DevOps

Η κουλτούρα DevOps είναι μια πρακτική ανάπτυξης λογισμικού που ενώνει τις ομάδες ανάπτυξης και λειτουργίας. Χρησιμοποιεί εργαλεία και αυτοματοματισμό ώστε να προωθήσει μεγαλύτερη συνεργασία, επικοινωνία και διαφάνεια μεταξύ των δύο ομάδων. Ως αποτέλεσμα, οι εταιρείες μειώνουν τον χρόνο ανάπτυξης λογισμικού, ενώ συνεχίζουν να μένουν ευέλικτοι σε αλλαγές.

Continuous Integration and Continuous Delivery

Η συνεχής ενσωμάτωση και η συνεχής παράδοση (CI/CD) είναι μια μοντέρνα πρακτική ανάπτυξης λογισμικού που χρησιμοποιεί αυτοματοποιημένα build-and-test βήματα για να παραδώσει μικρές αλλαγές στην εφαρμογή αξιόπιστα και αποδοτικά. Οι προγραμματιστές χρησιμοποιούν CI/CD για να κάνουν release νέες εκδόσεις της εφαρμογής και για να μπορούν να ανταπεξέλθουν γρήγορα σε θέματα που εμφανίζονται στην εφαρμογή ενώ αυτή είναι διαθέσιμη στους χρήστες.

DevSecOps

Το DevSecOps εισάγει την ασφάλεια στην πρακτική DevOps ενσωματώνοντας αξιολογήσεις ασφάλειας σε όλη τη διαδικασία CI/CD. Καθιστά την ασφάλεια κοινή ευθύνη μεταξύ όλων των μελών της ομάδας που συμμετέχουν στην κατασκευή του λογισμικού. Η ομάδα ανάπτυξης συνεργάζεται με την ομάδα ασφάλειας πριν γράψει οποιοδήποτε κώδικα. Ομοίως, οι ομάδες λειτουργίας συνεχίζουν να παρακολουθούν το λογισμικό για ζητήματα ασφάλειας μετά την ανάπτυξή του. Ως αποτέλεσμα, οι εταιρείες παρέχουν ασφαλές λογισμικό ταχύτερα, διασφαλίζοντας παράλληλα τη συμμόρφωση (compliance).

DevSecOps σε σύγκριση με DevOps

Το DevOps εστιάζει στο να φέρει μια εφαρμογή στην αγορά όσο το δυνατόν γρηγορότερα και η δοκιμή ασφάλειας είναι μια ξεχωριστή διαδικασία που λαμβάνει χώρα στο τέλος της ανάπτυξης της εφαρμογής, ακριβώς πριν από την παράδοσή της. Συνήθως, μια ξεχωριστή ομάδα ελέγχει και επιβάλλει την ασφάλεια στο λογισμικό. Για παράδειγμα, οι ομάδες ασφάλειας δημιουργούν ένα τείχος προστασίας για να δοκιμάσουν την εισβολή στην εφαρμογή μετά την κατασκευή της.

Το DevSecOps, από την άλλη πλευρά, κάνει τη δοκιμή ασφάλειας μέρος της ίδιας της διαδικασίας ανάπτυξης εφαρμογών και δίνει έμφαση στην μετατόπιση της ασφάλειας αριστερά ή αλλιώς στην μετακίνηση της ασφάλειας όσο το δυνατόν νωρίτερα στην διαδικασία της ανάπτυξης. Το DevSecOps επεκτείνει την κουλτούρα της μοιρασμένης ευθύνης του DevOps ώστε να συμπεριληφθούν πρακτικές ασφάλειας. Και οι δύο προσεγγίσεις είναι παρόμοιες από ορισμένες απόψεις, συμπεριλαμβάνοντας την χρήση αυτοματισμού και των συνεχών διαδικασιών ώστε να καθιερώσουν συνεργατικούς κύκλους ανάπτυξης. Ομάδες ασφάλειας και προγραμματιστές συνεργάζονται για την προστασία των χρηστών από ευπάθειες λογισμικού. Για παράδειγμα, οι ομάδες ασφάλειας στήνουν τείχη προστασίας, οι προγραμματιστές σχεδιάζουν τον κώδικα για να μην υπάρχουν τρωτά σημεία και οι testers δοκιμάζουν όλες τις αλλαγές για να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση από τρίτους. (aws, χ.χ)

1.2 Πώς να μεταβούμε από DevOps σε DevSecOps

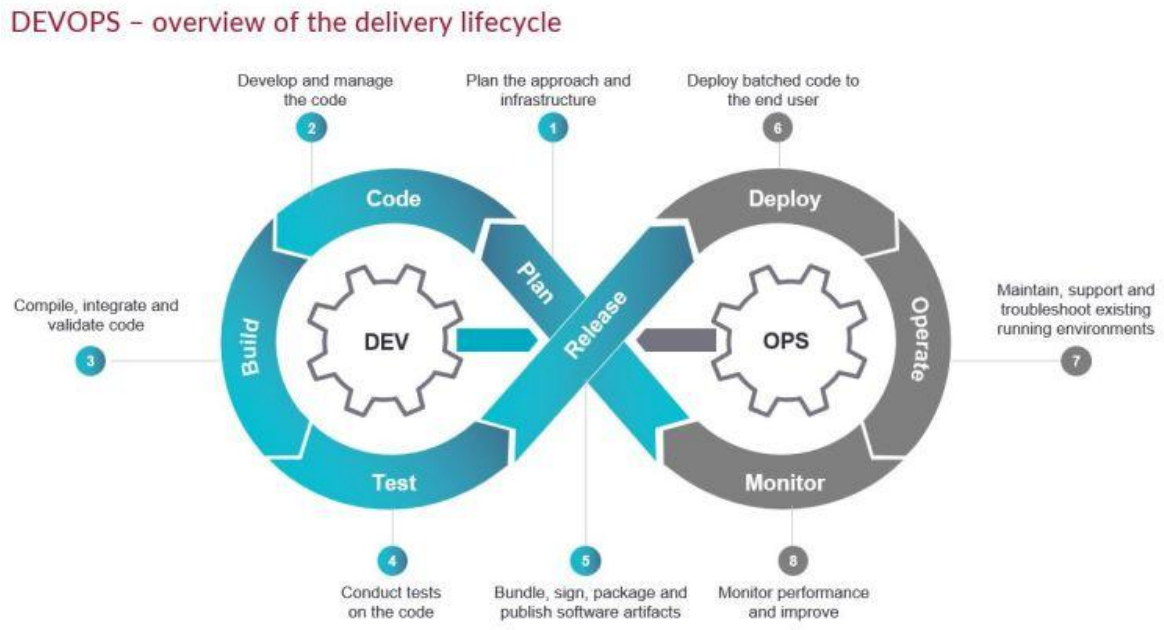
Ενσωματώνουμε την ασφάλεια σε υπάρχοντα μοτίβα εργασίας.
Ο πιο συνηθισμένος λόγος που οι προγραμματιστές παρακάμπτουν τις δοκιμές ασφαλείας είναι επειδή δεν είναι βολικές ή απαιτούν να γίνουν χειροκίνητα. Η νοοτροπία DevOps στοχεύει στη μείωση του διοικητικού φόρτου της ανάπτυξης λογισμικού και στην γρήγορη παράδοση κώδικα στην παραγωγή. Αυτή η ίδια προσέγγιση μπορεί να κάνει αποτελεσματικές τις προσπάθειες ασφάλειας κατά τη μετάβαση από το DevOps στο DevSecOps. Ο στόχος είναι να βοηθηθούν οι προγραμματιστές απλοποιώντας τις δοκιμές ασφαλείας. Τα εργαλεία θα πρέπει να είναι όσο το δυνατόν αυτοματοποιημένα και τα αποτελέσματα να είναι εύκολα ερμηνεύσιμα. Τα εργαλεία θα πρέπει να αναφέρουν προβλήματα απευθείας στο σύστημα παρακολούθησης προβλημάτων, το οποίο οι προγραμματιστές χρησιμοποιούν ήδη για να παρακολουθούν ελαττώματα λογισμικού, καθιστώντας εύκολο το κομμάτι της υπάρχουσας διαδικασίας εργασίας τους.

Επιλέγουμε συμβατά εργαλεία DevSecOps.
Για να αυτοματοποιήσουμε εργασίες και να παραδώσουμε αποτελέσματα που είναι εύκολο να ερμηνευτούν, αξιοποιούμε εργαλεία που έχουν σχεδιαστεί για ροές εργασίας (workflows) DevSecOps. Βρίσκουμε εργαλεία με πλήρως εξοπλισμένα API και ευέλικτες επιλογές αναφοράς (reporting options). Ακόμα κι αν υπάρχουν ήδη υπάρχοντα εργαλεία δοκιμών που χρησιμοποιούνται στον αγωγό (pipeline), πρέπει να είμαστε ανοιχτοί στην εξερεύνηση νέων εργαλείων που μπορούν να ενεργοποιήσουν ταχύτερες και πιο αυτοματοποιημένες δοκιμές ασφαλείας που δεν διακόπτουν τις υπάρχουσες ροές εργασίας.

Εκπαίδευση προγραμματιστών σχετικά με τα βασικά περί της ασφάλειας.
Οι προγραμματιστές πρέπει να κατανοούν ζητήματα ασφάλειας για να συμμετέχουν στην εύρεση κάποιου συμβάντος που προέκυψε. Χρειάζονται μια σταθερή κατανόηση των θεμάτων κυβερνοασφάλειας και των αντίστοιχων πρακτικών ασφαλούς κωδικοποίησης. Ένας προγραμματιστής πρέπει να γνωρίζει πώς να αποφεύγει συνηθισμένα τρωτά σημεία και γιατί

ένα συγκεκριμένο στυλ ή μέθοδος κωδικοποίησης μπορεί να οδηγήσει σε επίθεση. Η εκπαίδευση σε θέματα ασφάλειας δεν πρέπει να είναι ευθύνη μόνο της ομάδας ασφάλειας πληροφοριών ή άλλου ειδικού από το προσωπικό, διότι έχουν άλλες προτεραιότητες και πρέπει να ολοκληρώσουν τη δουλειά τους. Είναι σημαντική η αξιοποίηση εμπειρογνωμόνων ασφαλείας ή προγραμμάτων εκπαίδευσης που έχουν ανατεθεί σε εξωτερικούς συνεργάτες που μπορούν να παρέχουν αποτελεσματική και συνεχή εκπαίδευση για προγραμματιστές σχετικά με πρακτικές ασφαλούς κωδικοποίησης. Η εκπαίδευση πρέπει πρώτα να επικεντρωθεί στα βασικά. Τα πιο συνηθισμένα προβλήματα ασφάλειας στην κωδικοποίηση είναι η SQL injection και το cross-site scripting (XSS). Είναι σημαντικό να εστιάσουν πρώτα στα πιο βασικά ζητήματα, τα οποία μπορούν να προσφέρουν άμεση αξία, επειδή οι προγραμματιστές θα σταματήσουν να κάνουν αυτά τα συνηθισμένα λάθη, και στη συνέχεια να προχωρήσουν σε πιο προηγμένα θέματα. (Moradov, 2022)

1.3 Η ασφάλεια στις φάσεις DevOps



Εικόνα 1.1: Επισκόπηση του κύκλου ζωής της παράδοσης του λογισμικού. (2022)

Ανάπτυξη (Development)

Σχεδιασμός (Plan)

Οι σύγχρονες μεθοδολογίες ανάπτυξης έχουν δώσει έμφαση στη συνεχή ανατροφοδότηση που μπορεί να προέρχεται από μια ποικιλία πηγών, όπως η ανατροφοδότηση των χρηστών, η εξάλειψη απειλών ή οι γενικές βελτιώσεις χαρακτηριστικών. Οι εταιρείες θα πρέπει να προσαρμόζονται συνεχώς στις ανάγκες της επιχείρησης εφαρμόζοντας μια ισχυρή μεθοδολογία σχεδιασμού. Όσον αφορά την ασφάλεια των προϊόντων, οι οργανισμοί θα πρέπει να επιδιώξουν να ενσωματώσουν βήματα ασφαλούς σχεδιασμού στη διαδικασία

προγραμματισμού DevSecOps, είτε πρόκειται για το αποτέλεσμα από δραστηριότητες όπως η μοντελοποίηση απειλών ή η θέσπιση των πολιτικών του οργανισμού για απαιτήσεις (requirements) με επίκεντρο την ασφάλεια.

Κωδικοποίηση (Code)

Η φάση κωδικοποίησης απαιτεί αναμφισβήτητα το υψηλότερο επίπεδο ελέγχου στη μεθοδολογία DevSecOps. Οι προγραμματιστές θα πρέπει να εκπαιδεύονται συνεχώς σε πρακτικές ασφαλούς κωδικοποίησης, ενώ ταυτόχρονα χρησιμοποιούν μια ποικιλία εργαλείων που θα βοηθήσουν έγκαιρα στον εντοπισμό ευπαθειών (vulnerabilities). Είναι επιτακτική ανάγκη οι οργανισμοί να δημιουργήσουν μια βάση για τις στρατηγικές ανάπτυξης, όπως το branching και οι pre-commit rules. Αξίζει να σημειωθεί ότι η βελτίωση της ασφαλούς κωδικοποίησης μπορεί επίσης να βοηθήσει στη βελτίωση της ποιότητας και της συνέπειας του κώδικα που αναπτύσσεται.

Build

Μόλις ο κώδικας γίνει commit σε ένα κοινόχρηστο αποθετήριο (shared repository), εκτελούνται συχνά μια ποικιλία από γρήγορες δοκιμές λειτουργικών μονάδων (functional unit tests). Η ενσωμάτωση της ασφάλειας σε αυτό το βήμα επιτρέπει στους προγραμματιστές να αναλύουν τον πηγαίο κώδικα από την οπτική γωνία της Ανάλυσης Σύνθεσης Λογισμικού (Software Composition Analysis ή SCA). Συχνά οι προγραμματιστές τείνουν να αξιοποιούν τις βιβλιοθήκες τρίτων αποκλειστικά για το λειτουργικό τους όφελος χωρίς να λαμβάνουν υπόψη τις πιθανές επιπτώσεις στην ασφάλεια. Οι προγραμματιστές που μπορούν να κατανοήσουν τα dependencies καθώς εισάγονται σε ένα πρότζεκτ, μπορούν να γνωρίζουν περισσότερο τους πιθανούς κινδύνους ασφαλείας καθώς και τις παραβιάσεις αδειών που επηρεάζουν τον οργανισμό.

Δοκιμές (Test)

Ιστορικά η δοκιμή παλινδρόμησης (regression testing) ήταν μια κουραστική μη αυτόματη διαδικασία που απαιτεί χειροκίνητη αλληλεπίδραση για να επιβεβαιωθεί η βασική λειτουργικότητα. Όσο γίνονται γνωστές οι λύσεις Infrastructure-as-Code (IaC), εκτενείς δοκιμές αποδοχής/επικύρωσης μπορούν να πραγματοποιηθούν παράλληλα με τη Δοκιμή Ασφάλειας Δυναμικής Εφαρμογής (Dynamic Application Security Testing ή DAST). Εκτός από τις εκτεταμένες περιπτώσεις δοκιμών μονάδων (unit tests) που πιθανώς θα εκτελεστούν σε μια εφαρμογή, οι οργανισμοί θα πρέπει να είναι επιμελείς όσον αφορά τη δημιουργία δοκιμής μονάδων με επίκεντρο την ασφάλεια που στοχεύουν στον εντοπισμό ευπαθειών ασφαλείας χαμηλού επιπέδου που ενδέχεται να έχουν δημιουργηθεί. Να λάβουμε υπόψη ότι η δοκιμή μονάδων συσκευών IoT δεν είναι μια ασήμαντη εργασία και θα πρέπει να διατεθεί αρκετός χρόνος για να διασφαλιστεί ότι αυτές οι περιπτώσεις δοκιμών μπορούν να σχεδιαστούν και να εφαρμοστούν σωστά.

Λειτουργίες (Operations)

Η ενασχόληση με τη λειτουργία των συσκευών IoT που αξιοποιούνται στο δίκτυο ενός οργανισμού μπορεί να επιλυθεί με μια πληθώρα εργαλείων. Οι παραγωγοί συσκευών IoT

έχουν να λύσουν ένα εντελώς διαφορετικό σύνολο προβλημάτων. Ευτυχώς, στις περισσότερες περιπτώσεις, οι λύσεις μπορεί να είναι έτοιμες για υλοποίηση. Για να κατανοήσουμε καλύτερα την ανάγκη σε αυτό το στάδιο του DevSecOps, είναι χρήσιμο να έχουμε μια θεμελιώδη κατανόηση των φάσεων των Ops.

Απελευθέρωση (Release)
Αυτή η φάση αποτελεί την μετάβαση της ανάπτυξης (development) στις λειτουργίες (operations). Οι οργανισμοί θα πρέπει να διασφαλίζουν ότι έχει δημιουργηθεί ένα ισχυρό σύστημα διαχείρισης συσκευών για να διασφαλίζεται ότι οι εκδόσεις μπορούν να είναι συμβατές για απομακρυσμένα συστήματα.

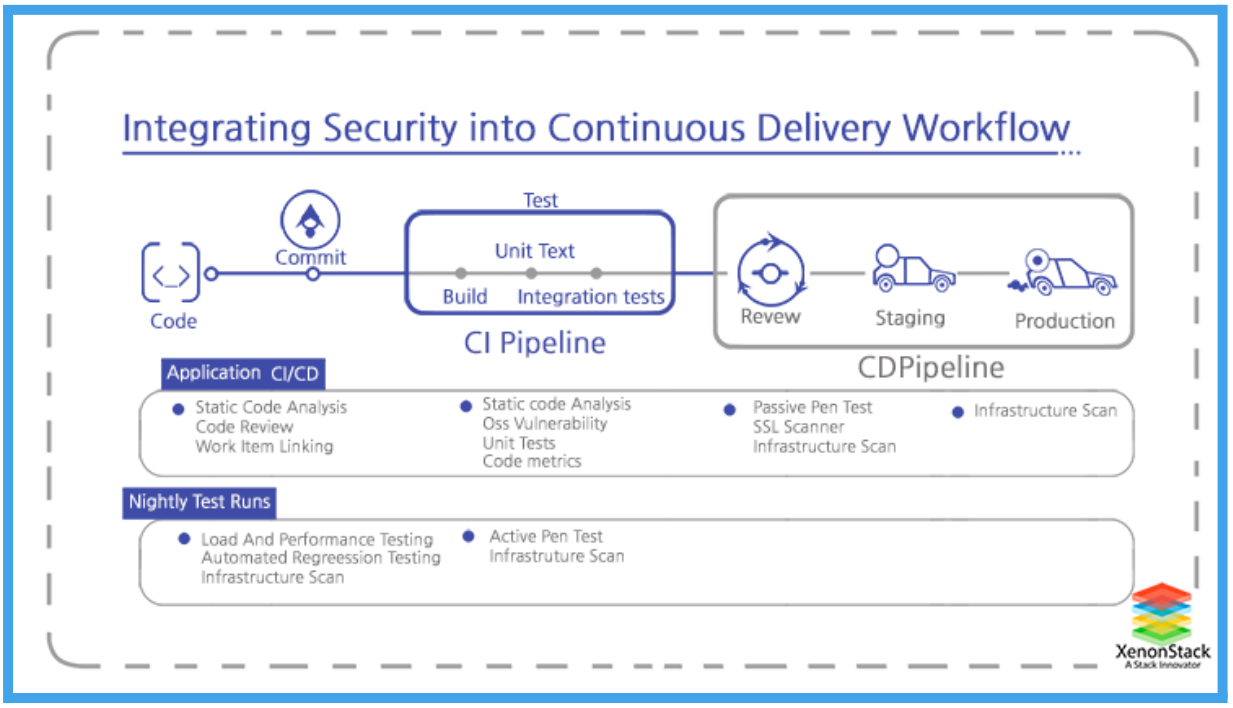
Deploy
Μια αυτοματοποιημένη μεθοδολογία deployment βοηθά στην εξάλειψη πιθανών προβλημάτων ασφάλειας και λειτουργικότητας που παρουσιάζονται κατά την μη αυτόματη ανάπτυξη ενημερώσεων σε απομακρυσμένα συστήματα και επιτρέπει να διαχειριζόμαστε τις εκδόσεις που έχουν αναπτυχθεί με βάση ετικετών μεταξύ άλλων παραγόντων.

Λειτουργίες (Operate)
Η διασφάλιση της σωστής λειτουργίας των απομακρυσμένων συσκευών μπορεί να επιτευχθεί με την αξιοποίηση των συστημάτων διαχείρισης συσκευών για την επεξεργασία δεδομένων συσκευών χρόνου εκτέλεσης (runtime), συμπεριλαμβανομένης της κατάστασης ενημέρωσης υλικολογισμικού (firmware update status), των συνθηκών λειτουργίας (operating conditions), των σφαλμάτων και πολλών άλλων.

Παρατήρηση/Ελεγχος (Monitor)
Οι κατασκευαστές θα πρέπει να χρησιμοποιούν την λύση διαχείρισης ασφάλειας συσκευών για να διασφαλίσουν ότι ανιχνεύονται και αντιμετωπίζονται κακόβουλα συστήματα με την εφαρμογή ενός κεντρικού συστήματος καταγραφής όπου οι συσκευές αναφέρουν συμβάντα ασφαλείας.

Ας ελπίσουμε ότι η λύση είναι ξεκάθαρη. Κάθε οργανισμός που παράγει και αναπτύσσει συσκευές IoT θα πρέπει να διασφαλίζει ότι έχει δημιουργηθεί ένα ισχυρό σύστημα διαχείρισης συσκευών για να χειρίζεται διάφορες πτυχές των λειτουργιών (operations). Προς όφελος κάθε κατασκευαστή, υπάρχει μια ποικιλία λύσεων που αντιμετωπίζουν κάθε φάση των Ops που περιγράφεται παραπάνω και μπορούν να αξιοποιηθούν με ελάχιστη προσπάθεια. Τέλος, γνωρίζουμε πως υπάρχει μια ποικιλία διαφορετικών εργαλείων DevSecOps που πρέπει να λάβουμε υπόψη κατά την εφαρμογή μιας λύσης DevSecOps σε μια εφαρμογή λογισμικού που θα δούμε παρακάτω. (Caleb, & Kendra, 2022)

1.4 Ενσωμάτωση της ασφάλειας στις ροές εργασίας των συνεχών παραδόσεων (Continuous Delivery workflows)



Εικόνα 1.2: Ενσωμάτωση ασφάλειας στην ροή εργασίας συνεχούς παράδοσης. (2023)

Ας δούμε πώς και πού να προσθέσουμε ελέγχους ασφαλείας σε μια ροή εργασιών Συνεχούς Παράδοσης.

1. Pre-commit

- Επαναληπτική μοντελοποίηση απειλών και εκτιμήσεις κινδύνων, χωρίς υπολογιστικό βάρος.
- Έλεγχος στατικής ανάλυσης (SAST) στο IDE του μηχανικού.
- Αξιολόγηση κώδικα από συναδέλφους.

2. Commit stage

- Συγκέντρωση και δημιουργία ελέγχων, διασφαλίζοντας ότι αυτά τα βήματα είναι καθαρά και ότι δεν υπάρχουν σφάλματα ή προειδοποιήσεις.
- Εντοπισμός κινδύνων σε στοιχεία τρίτων.
- Δημιουργία ειδοποιήσεων για τον κώδικα υψηλού κινδύνου.
- Αυτοματοποίηση μονάδων δοκιμής (unit testing) λειτουργιών ασφαλείας, με πλήρη κάλυψη ανάλυσης κώδικα.

3. Στάδιο αποδοχής

- Ασφαλής, αυτοματοποιημένη διαχείριση παραμέτρων μέσω εργαλείων όπως το Ansible και το Chef.
- Στοχευμένη δυναμική σάρωση (DAST).

- Αυτοματοποιημένη δοκιμή λειτουργίας και ενσωμάτωση χαρακτηριστικών ασφαλείας.
- Σάρωση βαθιάς στατικής ανάλυσης (SAST).
- Penetration testing με χρήση web exploitation frameworks όπως το Metasploit.

4. Deployment παραγωγής και post-deployment

- Αυτοματοποιημένο deployment και release orchestration.
- Αυτοματοποιημένες βεβαιώσεις χρόνου εκτέλεσης (runtime asserts) και έλεγχοι συμμόρφωσης (compliance checks).
- Παρακολούθηση/ανατροφοδότηση παραγωγής (Production monitoring/feedback).
- Runtime defense.
- Bug bounties.
- Μαθαίνοντας από τις αποτυχίες.

(Navdeep, 2023)

Κεφ 2. DevSecOps

2.1 Ποια είναι τα συστατικά στοιχεία του DevSecOps?

Η επιτυχής εφαρμογή της πρακτικής DevSecOps αποτελείται από τα ακόλουθα στοιχεία:

Ανάλυση κώδικα
Η ανάλυση κώδικα είναι η διαδικασία διερεύνησης του πηγαίου κώδικα μιας εφαρμογής για τρωτά σημεία και διασφάλισης ότι ακολουθεί τις βέλτιστες πρακτικές ασφάλειας. (aws, χ.χ)

Διαχείριση αλλαγών
Οι ομάδες λογισμικού χρησιμοποιούν εργαλεία διαχείρισης αλλαγών για την παρακολούθηση, τη διαχείριση και την αναφορά αλλαγών που σχετίζονται με το λογισμικό ή τις απαιτήσεις. Αυτό αποτρέπει ακούσιες ευπάθειες ασφάλειας λόγω αλλαγής λογισμικού. (aws, χ.χ)

Διαχείριση συμμόρφωσης
Η συμμόρφωση της ασφάλειας (Security compliance) αφορά την παρακολούθηση και την αξιολόγηση της ασφάλειας του δικτύου και των συστημάτων για τη διασφάλιση της συμμόρφωσης με τις κανονιστικές πολιτικές και τα πρότυπα ασφάλειας της επιχείρησης. Σε αντίθετη περίπτωση, ενδέχεται να προκληθούν παραβιάσεις δεδομένων οι οποίες είναι δαπανηρές και συνεπάγονται κυρώσεις και πρόστιμα. Ακολουθούν ορισμένες απαιτήσεις συμμόρφωσης για οργανισμούς, ανεξάρτητα από την εφαρμογή των DevOps και DevSecOps:

- Συμμόρφωση PCI: Η συμμόρφωση PCI αφορά τον κλάδο των καρτών πληρωμής. Οι οργανισμοί που επεξεργάζονται ή αποθηκεύουν πληροφορίες καρτών πληρωμής θα πρέπει να συμμορφώνονται με τα λειτουργικά και τεχνικά πρότυπα για την προστασία των κρίσιμων δεδομένων των κατόχων καρτών πληρωμής, ακολουθώντας ένα σύνολο οδηγιών ασφαλείας που αναπτύχθηκαν από το Συμβούλιο Προτύπων Ασφαλείας PCI (Security Standards Council PCI ή PCI SSC).

- Συμμόρφωση HIPAA: Η συμμόρφωση HIPAA αφορά τον κλάδο της υγειονομικής περίθαλψης. Οι οργανισμοί που εμπλέκονται στην υγειονομική περίθαλψη θα πρέπει να συμμορφώνονται με τον Νόμο Φορητότητας και Λογοδοσίας για την Ομοσπονδιακή Ασφάλιση Υγείας (Federal Health Insurance Portability and Accountability Act) του 1996 για την προστασία των ευαίσθητων δεδομένων που σχετίζονται με την υγεία των ασθενών.

- Συμμόρφωση HITRUST: Το HITRUST αναφέρεται στην Health Information Trust Alliance, που ιδρύθηκε το 2007. Είναι ένα πιστοποιημένο πλαίσιο ασφάλειας που παρέχει ένα σύνολο κατευθυντήριων γραμμών/ελέγχων για την απόδειξη της συμμόρφωσης με το HIPAA σε έναν οργανισμό. Είναι σημαντικό να σημειωθεί ότι το

HITRUST και το HIPAA δεν είναι το ίδιο. Ενώ το HIPAA είναι νόμος, το HITRUST είναι ένα πλαίσιο που βασίζεται στις απαιτήσεις της νομοθεσίας HIPAA.

- Συμμόρφωση SOC2: Το SOC2 είναι μια διαδικασία ελέγχου που ορίζει κριτήρια για την ασφαλή διαχείριση των δεδομένων πελατών με βάση πέντε αρχές εμπιστοσύνης: την Ασφάλεια, το Απόρρητο, την Εμπιστευτικότητα, τη Διαθεσιμότητα και την Ακεραιότητα της Διαδικασίας και αναπτύχθηκε από το Αμερικανικό Ινστιτούτο CPA.

(William, 2022)

Μοντελοποίηση απειλών

Οι ομάδες DevSecOps διερευνούν ζητήματα ασφάλειας που ενδέχεται να προκύψουν πριν και μετά την παράδοση της εφαρμογής. Διορθώνουν τυχόν γνωστά προβλήματα και κυκλοφορούν μια ενημερωμένη έκδοση της εφαρμογής. (aws, χ.χ)

Εκπαίδευση ασφάλειας

Η εκπαίδευση σε θέματα ασφάλειας περιλαμβάνει εκπαίδευση προγραμματιστών λογισμικού και ομάδων λειτουργιών με τις πιο πρόσφατες οδηγίες ασφάλειας. Με αυτόν τον τρόπο, οι ομάδες ανάπτυξης και λειτουργίας μπορούν να λαμβάνουν ανεξάρτητες αποφάσεις ασφάλειας κατά τη δημιουργία και την παράδοση της εφαρμογής. (aws, χ.χ)

2.2 Γιατί είναι σημαντικό το DevSecOps?

Στόχος του DevSecOps είναι να βοηθήσει τις ομάδες ανάπτυξης λογισμικού να αντιμετωπίζουν αποδοτικά τα διάφορα θέματα ασφάλειας. Είναι μια εναλλακτική, σε παλιές πρακτικές ασφάλειας λογισμικού, που δεν μπορούσαν να συμβαδίσουν με μικρά χρονικά περιθώρια παράδοσης και γρήγορες αναβαθμίσεις λογισμικού. Για να καταλάβουμε την σημαντικότητα της πρακτικής, θα αναφέρουμε εν συντομία την διαδικασία ανάπτυξης λογισμικού.

Κύκλος ζωής ανάπτυξης λογισμικού

Ο κύκλος ζωής ανάπτυξης λογισμικού ή αλλιώς software development lifecycle (SDLC), είναι μια δομημένη διαδικασία που οδηγεί τις ομάδες λογισμικού να παράγουν υψηλής ποιότητας εφαρμογές. Οι ομάδες λογισμικού χρησιμοποιούν το SDLC για να μειώσουν κόστη, να ελαχιστοποιήσουν τα λάθη, και να εξασφαλίσουν ότι το λογισμικό συμβαδιζει συνέχεια με τους στόχους του project. Ο κύκλος ζωής ανάπτυξης λογισμικού περνά την ομάδα λογισμικού μέσα από τα εξής στάδια:

- Ανάλυση απαιτήσεων
- Σχεδιασμός
- Αρχιτεκτονική σχεδίαση
- Ανάπτυξη λογισμικού

- Δοκιμές
- Deployment

Στις συνηθισμένες μεθόδους ανάπτυξης λογισμικού, οι δοκιμές ασφάλειας ήταν μια ξεχωριστή διαδικασία στην SDLC. Η ομάδα ασφάλειας έβρισκε αδυναμίες μόνο μετά την ολοκλήρωση της δημιουργίας του λογισμικού. Η δομή του DevSecOps βελτιώνει τον κύκλο ζωής ανάπτυξης λογισμικού ανιχνεύοντας ευπάθειες καθόλη την διάρκεια ανάπτυξης και παραδοσης της διαδικασίας του λογισμικού. (aws, χ.χ)

2.3 Πλεονεκτήματα του DevSecOps

Υπάρχουν αρκετά πλεονεκτήματα εξασκώντας την πρακτική DevSecOps.

- Πρώιμος εντοπισμός των ευπαθειών του λογισμικού.

Οι ομάδες που φτιάχνουν το λογισμικό εστιάζουν στον έλεγχο της ασφάλειας καθόλη την διάρκεια της ανάπτυξης λογισμικού. Αντί να περιμένουν μέχρι την ολοκλήρωση του λογισμικού, κάνουν ελέγχους σε κάθε στάδιο της δημιουργίας του. Έτσι, οι ανιχνεύσεις των αδυναμιών γίνονται σε νωρίτερα στάδια, μειώνοντας έτσι το κόστος και τον χρόνο αντιμετώπισής τους. Σαν αποτέλεσμα, οι χρήστες βιώνουν ελάχιστες αναστατώσεις και μεγαλύτερη ασφάλεια με το τέλος της παραγωγής του λογισμικού.

- Μειωμένος χρόνος για να βγει στην αγορά το λογισμικό.

Με την χρήση DevSecOps οι ομάδες δημιουργίας λογισμικού μπορούν να αυτοματοποιήσουν τους ελέγχους ασφάλειας και να μειώσουν τα ανθρώπινα λάθη. Επίσης, προλαμβάνει την εκτίμηση ασφάλειας από το να γίνεται εμπόδιο στην διαδικασία ανάπτυξης.

- Διασφάλιση της συμμόρφωσης των ρυθμιστικών κανόνων.

Οι ομάδες λογισμικού χρησιμοποιούν DevSecOps για να συμμορφώνονται με τις ρυθμιστικές απαιτήσεις υιοθετώντας επαγγελματικες πρακτικές και τεχνολογίες ασφάλειας αναγνωρίζοντας την προστασία δεδομένων και τις απαιτήσεις ασφάλειας στο σύστημα.

- Δημιουργία μιας κουλτούρας με επίγνωση της ασφάλειας.

Οι ομάδες δημιουργίας λογισμικού αποκτούν περισσότερη επίγνωση στις καλύτερες πρακτικές ασφάλειας όταν δημιουργουν το λογισμικό. Είναι πιο ενεργοί στο να εντοπίζουν θέματα ασφάλειας στον κωδικα, στα δομικά στοιχεία (modules), ή σε άλλες τεχνολογίες που χρησιμοποιούνται στην δημιουργία της εφαρμογής.

- Ανάπτυξη νέων χαρακτηριστικών με ασφάλεια

Η πρακτική αυτή ενθαρρύνει ευέλικτη συνεργασία μεταξύ των ομάδων προγραμματισμού, ασφάλειας και λειτουργιών (operations). Μοιράζονται την ίδια αντίληψη ασφάλειας λογισμικού και χρησιμοποιούν συνηθισμένα εργαλεία για να αυτοματοποιήσουν τις εκτιμήσεις και τις αναφορές που παρατηρούν. (aws, χ.χ)

2.4 Ποια είναι η κουλτούρα του DevSecOps?

Η κουλτούρα DevSecOps συνδυάζει την επικοινωνία, τους ανθρώπους, την τεχνολογία και τις διαδικασίες.

- Επικοινωνία

Οι εταιρείες εφαρμόζουν το DevSecOps προωθώντας μια πολιτιστική αλλαγή που ξεκινά από την αρχή. Αυτοί που ηγούνται την ανάπτυξη της εφαρμογής εξηγούν τη σημασία και τα οφέλη της υιοθέτησης πρακτικών ασφάλειας στην ομάδα DevOps. Οι προγραμματιστές και οι ομάδες λειτουργιών (operation teams) χρειάζονται τα κατάλληλα εργαλεία, συστήματα και προφανώς ενθάρρυνση για να υιοθετήσουν πρακτικές DevSecOps.

- Ανθρωποι

Το DevSecOps οδηγεί σε έναν πολιτισμικό μετασχηματισμό που περιλαμβάνει τις ομάδες λογισμικού, αφού δεν τηρούν πλέον τους συμβατικούς ρόλους κατασκευής, δοκιμής και ανάπτυξης κώδικα. Με το DevSecOps, οι προγραμματιστές και οι ομάδες λειτουργιών συνεργάζονται με ειδικούς σε θέματα ασφάλειας για τη βελτίωση της ασφάλειας σε όλη τη διαδικασία ανάπτυξης.

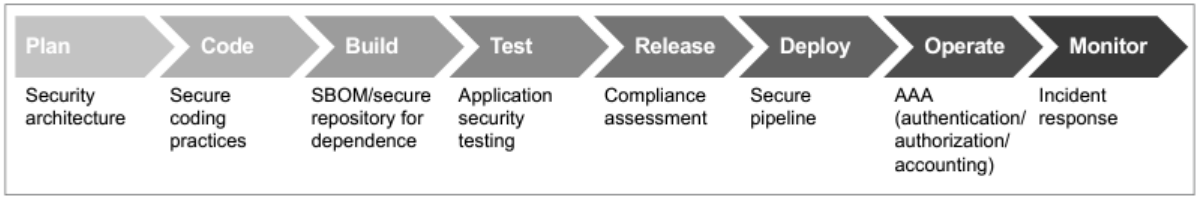
- Τεχνολογία

Οι ομάδες λογισμικού χρησιμοποιούν τεχνολογία για την εκτέλεση αυτοματοποιημένων δοκιμών ασφάλειας κατά την ανάπτυξη του λογισμικού. Οι ομάδες DevOps την χρησιμοποιούν για να ελέγχουν την εφαρμογή για ελαττώματα ασφάλειας χωρίς να διακυβεύεται το χρονοδιάγραμμα παράδοσης.

- Διαδικασίες (Process)

Το DevSecOps αλλάζει τη συμβατική διαδικασία κατασκευής λογισμικού. Με το DevSecOps, οι ομάδες λογισμικού πραγματοποιούν δοκιμές ασφαλείας και αξιολογήσεις σε κάθε στάδιο ανάπτυξης (development). Οι προγραμματιστές ελέγχουν για ελαττώματα ασφάλειας όταν γράφουν τον κώδικα. Στη συνέχεια, μια ομάδα ασφάλειας ελέγχει την εφαρμογή πριν εκδοθεί για ευπάθειες ασφάλειας. Θα ελέγξουν δηλαδή την εξουσιοδότηση ώστε οι χρήστες να έχουν πρόσβαση μόνο σε ό,τι μπορούν να έχουν πρόσβαση και την επικύρωση εισαγόμενων δεδομένων, ώστε το λογισμικό να λειτουργεί σωστά κατά τη λήψη μη φυσιολογικών δεδομένων. Στη συνέχεια, οι ομάδες λογισμικού διορθώνουν τυχόν ελαττώματα πριν από την κυκλοφορία της τελικής εφαρμογής στους τελικούς χρήστες. Οι δοκιμές ασφάλειας δεν τελειώνουν μετά την παράδοση της εφαρμογής. Η ομάδα λειτουργιών συνεχίζει να παρακολουθεί για πιθανά ζητήματα, να κάνει τροποποιήσεις, και να συνεργάζεται με τις ομάδες ασφάλειας και ανάπτυξης για την έκδοση ενημερωμένων εκδόσεων της εφαρμογής. (aws, χ.χ)

2.5 Ποιες είναι οι αρχές και οι καλές πρακτικές του DevSecOps?



Εικόνα 2.1: SDLC και μέτρα ασφαλείας για το κάθε βήμα. (2023)

Οι αρχές της πρακτικής DevSecOps επιτρέπουν σε μια ομάδα ανάπτυξης (development team) να δημιουργεί ασφαλείς και αξιόπιστες εφαρμογές με ταχύτητα μέσω της εκτέλεσης δοκιμών ασφαλείας. Εκτελώντας μια προσέγγιση DevSecOps, οι ομάδες ενσωματώνουν την ασφάλεια στον κύκλο ζωής ανάπτυξης λογισμικού (SDLC) από τον αρχικό σχεδιασμό έως τη συνεχή παράδοση και το deployment. Κάτι τέτοιο συμβάλλει στην αποτροπή κακόβουλων παραγόντων από αυτούς που εκμεταλλεύονται τα τρωτά σημεία του συστήματος με αποτέλεσμα να μειώνεται και ο συνολικός αριθμός επιθέσεων στον κυβερνοχώρο. Οι αρχές του DevSecOps περιλαμβάνουν: (Niall, 2023)

- ❖ Ασφάλεια σε κάθε στάδιο του SDLC

Η χρήση ασφάλειας σε κάθε στάδιο του SDLC διασφαλίζει την αποτελεσματική ανάπτυξη ασφαλών εφαρμογών χωρίς να θυσιάζεται η ποιότητά τους. Είναι απαραίτητο να καλύπτεται κάθε στάδιο του κύκλου ζωής από το σχεδιασμό έως την ανάπτυξη και την παράδοση.
Για να είναι αποτελεσματική η διαδικασία, οι προγραμματιστές πρέπει να σχεδιάζουν εφαρμογές με κατάλληλους ελέγχους ασφαλείας και οι ομάδες λειτουργιών (operation teams) θα πρέπει να τις αναπτύσσουν και να τις παρακολουθούν με ασφάλεια. (Niall, 2023)

- ❖ Προληπτικές στρατηγικές παρακολούθησης και απόκρισης

Οι στρατηγικές προληπτικής παρακολούθησης και απόκρισης είναι απαραίτητες για τη διατήρηση της ασφάλειας των εφαρμογών καθ' όλη τη διάρκεια ζωής τους. Η παρακολούθηση επιτυγχάνεται μέσω της ανάπτυξης αυτοματοποιημένων εργαλείων που εντοπίζουν πιθανές ευπάθειες και προειδοποιούν τις ομάδες όταν προκύπτουν.
Κάτι τέτοιο συμβάλλει στην ελαχιστοποίηση του κινδύνου και στη διασφάλιση της συνέπειας σε ολόκληρο τον οργανισμό. Η εφαρμογή μιας ολοκληρωμένης στρατηγικής απόκρισης επιτρέπει τον εντοπισμό και την επίλυση ζητημάτων πριν γίνουν κίνδυνοι για την ασφάλεια. (Niall, 2023)

- ❖ Δημιουργία και διαχείριση ασφαλών περιβαλλόντων προγραμματιστών και αλυσίδες εργαλείων (toolchains)

Για την υποστήριξη του αυτοματισμού DevSecOps, τα μελλοντικά περιβάλλοντα ανάπτυξης απαιτούν την ενσωμάτωση προτύπων ασφαλείας και κατευθυντήριων γραμμών μέσω ενός ολοκληρωμένου περιβάλλοντος ανάπτυξης (IDE). Οι οδηγίες πρέπει να είναι εφαρμόσιμες και σχετικές με τη χρήση κοντέινερ ή παραδειγμάτων κώδικα. Έπειτα, πρέπει να

υποστηρίξουμε τις πολιτικές μας με ένα πρόγραμμα ενσωμάτωσης προγραμματιστών που εκπαιδεύει νέους υπαλλήλους στα περιβάλλοντα, τα εργαλεία και τις διαδικασίες. Πρέπει να προσφέρουμε ένα πρόγραμμα ανανέωσης και συνεχή εκπαίδευση στους προγραμματιστές πέρα από την εκπαίδευση ενσωμάτωσης. Τέλος, πρέπει να γίνει βελτίωση των αλυσίδων εργαλείων (toolchains) στο ίδιο επίπεδο με άλλα σημεία στην επιχείρηση του οργανισμού για να προστατευτούμε από πιθανές επιθέσεις. Η διασφάλιση της αλυσίδας εργαλείων DevSecOps πρέπει να βρίσκεται στο επίκεντρο της προσοχής των ομάδων προγραμματισμού, λειτουργιών και κυβερνοασφάλειας. (Will, 2021)

- ❖ Σχεδιασμός αποτελεσματικών διαδικασιών αναθεώρησης κώδικα

Καθορίζουμε τη διαδικασία αναθεώρησης κώδικα για να κάνουμε την αναθεώρηση κώδικα πιο αποτελεσματική και συνεπή, εξοικονομώντας πολύτιμο χρόνο στους προγραμματιστές και τα εμπλεκόμενα άτομα. Είναι ιδιαίτερα σημαντικό να επανεξετάζουμε τον κώδικα για τυχόν ευπάθειες, ώστε να αυξήσουμε το επίπεδο της αποδοτικότητας και αυτό μπορεί να γίνει με μηχανισμούς ανατροφοδότησης και συνεχών αναφορών όπως είναι το κανάλι slack. (Will, 2021)

- ❖ Ενίσχυση των βασικών στοιχείων της ασφάλειας του Cloud

Τα δοκιμασμένα και θεμελιώδη στοιχεία ασφάλειας cloud βρίσκονται στην καρδιά του αυτοματισμού DevSecOps. Η ομάδα ασφαλείας στο cloud πρέπει να συνεργαστεί με τις ομάδες ανάπτυξης και λειτουργίας για να εφαρμόσει τα κατάλληλα στοιχεία ελέγχου ασφάλειας cloud στα περιβάλλοντα DevSecOps. Μερικά παραδείγματα μπορεί να περιλαμβάνουν το AWS Security Hub, το Microsoft Azure Monitor και το Google Cloud Policy Intelligence. (Will, 2021)

- ❖ Αξιοποίηση πλατφορμών κοντέινερ orchestration (Leverage Orchestration Container Platforms)

Τα κοντέινερ προσφέρουν απαράμιλλη αφαιρετικότητα (abstraction) και μπορούν να αναπτυχθούν σε οποιοδήποτε περιβάλλον ανάπτυξης ή παραγωγής. Δεδομένου ότι κάθε κοντέινερ εκτελεί ένα μεμονωμένο instance, τα κοντέινερ παρέχουν τη βέλτιστη ευαισθησία για την ανάπτυξη μέτρων ασφαλείας από τα αρχικά στάδια ενός κύκλου ζωής ανάπτυξης λογισμικού. Οι πλατφόρμες orchestration κοντέινερ, όπως το Kubernetes, απλοποιούν την ανάπτυξη και τη διαχείριση των κοντέινερ, επιτρέποντας την απρόσκοπτη συνεργασία μεταξύ ομάδων DevOps και ειδικών σε θέματα ασφάλειας. Οι πλατφόρμες αυτές προσφέρουν διάφορα μοτίβα ανάπτυξης με προτεινόμενες αρχιτεκτονικές και στοιχεία για ασφαλή σχεδιασμό και ανάπτυξη εφαρμογών σχετικών με το cloud. (Sudip, 2022)

- ❖ Υιοθέτηση Προσέγγισης Διαχείρισης Λογισμικού Bill of Materials (Software Bill of Materials ή SBOM).

Το SBOM είναι ένα απόθεμα διαφόρων στοιχείων λογισμικού τρίτων και ανοιχτού κώδικα που χρησιμοποιούνται σε μια βάση κώδικα. Μέσα σε ένα SBOM, οι επαγγελματίες ασφάλειας μπορούν να απαριθμήσουν όλα τα άμεσα και μεταβατικά dependencies στον αγωγό deployment (deployment pipeline), καθιστώντας ευκολότερο τον εντοπισμό απειλών ασφαλείας από ενσωματώσεις τρίτων. Ένας από τους πρωταρχικούς σκοπούς ενός SBOM

είναι να παρέχει επαρκή ευκρίνεια και ορατότητα για την ανάπτυξη αυτοματοποιημένων εργαλείων ασφαλείας για συνεχή παρακολούθηση και δοκιμή ασφάλειας σε σύγχρονες εφαρμογές. Ως ουσιαστικό αποτέλεσμα, τα εργαλεία διαχείρισης SBOM απαλλάσσουν τις ομάδες DevSecOps από τις μη αυτόματες εργασίες που εμπλέκονται στην αναθεώρηση λογισμικού ανοιχτού κώδικα ενώ βοηθούν στη Στατική Ανάλυση Κώδικα (Static Code Analysis) του λογισμικού.Το SBOM περιλαμβάνει επίσης πρόσθετες πολύτιμες πληροφορίες για την ανάλυση ασφαλείας, συμπεριλαμβανομένων αδειών τρίτων, εκδόσεων λογισμικού και της σχετικής ενημέρωσης κατάστασης κώδικα. (Sudip, 2022)

- ❖ Ενδυνάμωση των δοκιμών ασφαλείας εφαρμογών (Application Security Testing ή AST)

Οι δοκιμές ασφάλειας εφαρμογών (AST) περιλαμβάνουν επαναλαμβανόμενους ελέγχους ασφαλείας για την αυτοματοποίηση της αναθεώρησης και της αξιολόγησης της ασφάλειας του κώδικα μέσω συνεχών σαρώσεων. Το Static Application Security Testing (SAST) είναι ένας μηχανισμός που βοηθά στην ανάλυση του πηγαίου κώδικα του λογισμικού για κινδύνους ασφάλειας και εσφαλμένες ρυθμίσεις παραμέτρων και εκτελείται όταν το πρόγραμμα δεν τρέχει. Σε αντίθεση με το SAST, το Dynamic Application Security Testing (DAST) είναι μια προσέγγιση δοκιμής ασφαλείας μαύρου κουτιού (black box) που δεν απαιτεί πρόσβαση στον πηγαίο κώδικα. Το DAST είναι μια ανάλυση ασφάλειας front-end όπου οι ερευνητές ασφαλείας προσομοιώνουν επιθέσεις για να αποκαλύψουν πιθανά ζητήματα ασφάλειας εντός της εφαρμογής. Μέσω του DAST, οι ομάδες ασφαλείας μπορούν να βρουν ζητήματα ασφαλείας χρόνου εκτέλεσης, όπως ελαττώματα διαμόρφωσης διακομιστή και ελέγχου ταυτότητας, τα οποία είναι συνήθως ορατά σε ένα περιβάλλον παραγωγής. Άλλοι μηχανισμοί ασφάλειας εφαρμογών (AppSec) που χρησιμοποιούνται σε μια διοχέτευση ανάπτυξης περιλαμβάνουν τη Διαδραστική Δοκιμή Ασφάλειας Εφαρμογών (Interactive Application Security Testing ή IAST) και την Αυτοπροστασία εφαρμογών χρόνου εκτέλεσης (Runtime Application Self-Protections ή RASP). (Sudip, 2022)

- ❖ Ενεργοποίηση της εκπαίδευσης για ασφαλείς πρακτικές κωδικοποίησης σε όλο τον οργανισμό

Ένας αποτελεσματικός τρόπος για τον μετριασμό πιθανών προβλημάτων στην παραγωγή είναι να διασφαλίσουμε ότι δεν υπάρχουν εξαρχής στον κώδικα. Για να γίνει η ασφάλεια κοινή ευθύνη μεταξύ των προγραμματιστών, των επαγγελματιών ασφάλειας και της ομάδας λειτουργιών, είναι σημαντικό να εκπαιδεύσουμε κάθε ενδιαφερόμενο για τη δημιουργία ασφαλών εφαρμογών. Η ομάδα ασφαλείας θα πρέπει να εκπαιδεύει τους προγραμματιστές σχετικά με πρακτικές ασφαλούς κωδικοποίησης που τους βοηθούν να υιοθετήσουν μια προσέγγιση με προτεραιότητα την ασφάλεια στις καθημερινές τους εργασίες. Η εκπαίδευση θα πρέπει επίσης να περιλαμβάνει τη δημιουργία καναλιών επικοινωνίας για απρόσκοπτη συνεργασία μεταξύ επαγγελματιών ασφάλειας και προγραμματιστών. Ο κάθε οργανισμός πρέπει να επιβάλλει στην εκπαίδευσή του σχετικά με την ασφάλεια και τους εμπλεκόμενους, οδηγώντας την κρίσιμη αλλαγή συμπεριφοράς που απαιτείται για την αυτοματοποίηση των ελέγχων ασφαλείας. (Sudip, 2022)

❖ Εφαρμογή Μοντελοποίησης Απειλών

Κατά τη δημιουργία της πλατφόρμας αυτοματισμού DevSecOps, οι μηχανικοί ασφαλείας θα πρέπει να λαμβάνουν υπόψη όλες τις αδυναμίες του συστήματος και τον τρόπο με τον οποίο ένας εισβολέας θα μπορούσε να τις εκμεταλλευτεί. Η μοντελοποίηση απειλών περιλαμβάνει τη σάρωση της εφαρμογής μέσα από τα μάτια ενός κακόβουλου ανθρώπου. Η συνεχής μοντελοποίηση απειλών βοηθά τους ειδικούς σε θέματα ασφάλειας να κατανοήσουν το πως στέκεται η εφαρμογή σε θέματα ασφάλειας, η οποία βοηθά στην ανάπτυξη των σωστών εργαλείων ασφαλείας για τον αυτοματισμό DevSecOps. Η μοντελοποίηση απειλών λειτουργεί ως προσχέδιο για τη δημιουργία μιας συλλογικής κουλτούρας DevSecOps, καθώς βοηθά κάθε ομάδα να κατανοήσει καλύτερα τους ρόλους και τους στόχους της στη διατήρηση της ασφάλειας εφαρμογών και υποδομών. (Sudip, 2022)

❖ Καθορισμός Μετρικών Ασφαλείας

Οι μετρικές ασφαλείας επιτρέπουν στους βασικούς συμμετέχοντες του κύκλου ζωής ανάπτυξης εφαρμογών, συμπεριλαμβανομένης της ομάδας λειτουργιών, των προγραμματιστών και των ειδικών ασφαλείας, να αξιολογούν τις επιπλοκές της εκτέλεσης εφαρμογών σε ένα ασφαλές περιβάλλον. Οι βέλτιστα καθορισμένες μετρικές βοηθούν τους μηχανικούς ασφαλείας να βελτιώσουν τις πρακτικές αποκατάστασης για ακριβή μέτρηση και μετριασμό των απειλών στον κυβερνοχώρο. Τα εργαλεία συνεχούς παρακολούθησης βασίζονται επίσης σε δεδομένα μετρικών για την παρακολούθηση της απόδοσης και της ασφάλειας των εφαρμογών σε πραγματικό χρόνο. Οι μετρήσεις ασφαλείας χρησιμοποιούνται επίσης συνήθως για τον καθορισμό των συμφωνιών επιπέδου υπηρεσίας (Service Level Agreements ή SLA) και των στόχων επιπέδου υπηρεσίας (Service Level Objectives ή SLO) για να βοηθήσουν στη μέτρηση της απόδοσης διαφόρων στοιχείων λογισμικού μιας στοίβας τεχνολογίας (tech stack). Οι προγραμματιστές βασίζονται στις μετρικές DevSecOps για τα SAST, SCA και τις δοκιμές αποδοχής που διεξάγονται πριν από το deploy του πηγαίου κώδικα σε μια συνεχή ενσωμάτωση αγωγού (continuous integration pipeline). Ορισμένες μετρικές που χρησιμοποιούνται συνήθως στον αυτοματισμό DevSecOps περιλαμβάνουν:

- ➢ Συχνότητα deployment
- ➢ Μέσος χρόνος επισκευής (Mean time to repair ή MTTR)
- ➢ Χρόνος λειτουργίας/διακοπής λειτουργίας (Uptime/downtime)
- ➢ Patch cadence
- ➢ Πυκνότητα ευπάθειας (Vulnerability density)
- ➢ Απόπειρες εισβολής και αποκρίσεις (Intrusion attempts and responses)
- ➢ Κίνδυνος τρίτων
- ➢ Αξιολόγηση ασφαλείας. (Sudip, 2022)

❖ Μετατόπιση ασφαλείας αριστερά

Οι ομάδες DevSecOps συνεργάζονται νωρίς με ειδικούς στον τομέα της κυβερνοασφάλειας κατά τη διάρκεια της διαδικασίας SDLC, μια σημαντική αλλαγή για την παραδοσιακή πρακτική DevOps. Στο DevSecOps, η ασφάλεια στον κυβερνοχώρο γίνεται κοινή ευθύνη όλων των μελών των ομάδων τους. Αυτό σημαίνει ότι ο σχεδιασμός και η εφαρμογή λογισμικού ακολουθεί τις βέλτιστες πρακτικές ασφάλειας, λαμβάνοντας υπόψη τομείς όπως:

- ➢ Πιθανά τρωτά σημεία ασφαλείας

- ➢ Διανύσματα απειλών (Threat vectors)
- ➢ Κανονισμοί συμμόρφωσης (Compliance regulations).

Κατά τη μετατόπιση της ασφάλειας προς τα αριστερά (προς την αρχή του SDLC), κάθε έκδοση λογισμικού διαμορφώνεται με ασφάλεια, βελτιστοποιημένη απόδοση, μειωμένο κόστος και χρόνο για την αγορά και άλλους βασικούς επιχειρηματικούς στόχους. Αυτό επιτρέπει στην ομάδα να εντοπίζει έγκαιρα τον κίνδυνο ασφάλειας, επιτρέποντας μια ασφαλή κατασκευή για κάθε ενσωμάτωση στον αγωγό CI/CD. (Muhammad, 2023)

- ❖ Ολιστικός αυτοματισμός

Η υιοθέτηση αυτοματισμού από άκρο σε άκρο επιφέρει εκτεταμένες δοκιμές και επεξεργασία CI/CD. Στο DevSecOps, η αυτοματοποίηση υιοθετείται ως μια πολύ έξυπνη απόφαση και στρατηγική. Εξάλλου, η αυτοματοποίηση ανούσιων διαδικασιών υπονομεύει την ποιότητα του λογισμικού. Σε τέτοιες περιπτώσεις, οποιαδήποτε εργασία για την αντιμετώπιση ζητημάτων ποιότητας τείνει να αποβεί σε βάρος της απόδοσης της ασφάλειας. Αυτή η πρακτική έρχεται σε αντίθεση με την έννοια του DevSecOps. Αντίθετα, οι ομάδες DevSecOps διασφαλίζουν ότι οι δοκιμές ασφάλειας ενσωματώνονται πλήρως στην διαδικασία αυτοματισμού, ελέγχοντας για:

- ➢ Dependencies του λογισμικού
- ➢ Πώς κάθε αλλαγή επηρεάζει τη συνολική απόδοση ασφάλειας του λογισμικού της εφαρμογής. (Muhammad, 2023)

- ❖ Συνεχείς δοκιμές ασφαλείας

Η πρακτική του Continuous Testing επεκτείνεται με την εισαγωγή αυτοματοποιημένων δοκιμών σε λειτουργίες που αναλύουν την ποιότητα κατασκευής (build quality) για τρωτά σημεία ασφαλείας. Μέσα στο DevSecOps, οι ομάδες Devs και QA αναλαμβάνουν συλλογικά την ευθύνη για τη βελτίωση της ποιότητας του λογισμικού δοκιμάζοντας συνεχώς κάθε έκδοση, αν και στην πραγματικότητα, η διαδικασία ενσωματώνεται στον αγωγό CI/CD. Αυτά περιλαμβάνουν:

- ➢ Στατική δοκιμή ασφάλειας εφαρμογών
- ➢ Λειτουργίες δυναμικής δοκιμής.

Μπορούμε επίσης να αναπτύξουμε ένα μοντέλο απειλής και να δημιουργήσουμε πολιτικές ασφαλείας νωρίς κατά τη διάρκεια της διαδικασίας SDLC. Ενδέχεται να υιοθετηθούν εργαλεία αυτοματοποιημένης αποκατάστασης για την αντιμετώπιση συχνών τρωτών σημείων που παρουσιάζονται καθώς οι ομάδες προγραμματιστών και QA ακολουθούν κύκλους ταχείας κυκλοφορίας (rapid release cycles) και γρήγορα σπριντ (fast sprints) στις φάσεις DevOps. (Muhammad, 2023)

- ❖ Συνεργατική κουλτούρα και επικοινωνία

Οι οργανισμοί πρέπει να διευκολύνουν τα μέλη της ομάδας DevSecOps να συνεργάζονται και να επικοινωνούν. Σε ένα περιβάλλον πληροφορικής, οι ομάδες Devs, QA, Ops και InfoSec τείνουν να εργάζονται μεμονωμένα, με κάθε ομάδα να υιοθετεί τις δικές της πολιτικές και στόχους. Αυτοί οι στόχοι είναι συχνά αντικρουόμενοι και τελικά απαιτούν μια αλλαγή της πολιτικής από την κάθε ομάδα. Από την άποψη του DevSecOps, αυτό δεν είναι πρακτικό γιατί μια άγνωστη συνέπεια, αθέμιτη πρακτική ασφαλείας ή μη ενημερωμένη απόφαση

μπορεί να έχει μόνιμο αρνητικό αντίκτυπο στη συνολική ποιότητα και απόδοση του λογισμικού. (Muhammad, 2023)

- ❖ Ασφάλεια ως κώδικας (Security as code)

Για να διευκολυνθεί η διαμόρφωση και η ανάπτυξη προσαρμοσμένων ροών εργασιών αυτοματισμού για δοκιμές ασφαλείας για τις ομάδες προγραμματιστών και QA, οι χρήστες μπορούν να αντιμετωπίζουν τις πολιτικές ασφαλείας, τις διαδικασίες και τα στοιχεία ελέγχου ως κώδικα. Η ασφάλεια ως κώδικας διασφαλίζει ότι η συνεχής και αυτοματοποιημένη δοκιμή ασφαλείας δεν δημιουργεί περιττό κόστος και καθυστερήσεις στην επεξεργασία του SDLC. Οι διαδικασίες δοκιμών ασφαλείας εκτελούνται παράλληλα με τις λειτουργικές δοκιμές εντός των αυτοματοποιημένων ροών εργασίας CI/CD. Οι ομάδες προγραμματιστών και διασφάλισης ποιότητας (QA) μπορούν να βελτιώσουν την απόδοση ασφάλειας με την ασφάλεια που θέλουν να πετύχουν, καθώς τα εργαλεία, οι μετρικές, το εύρος δοκιμών (testing scope) και τα configurations επαναχρησιμοποιούνται. Η διαδικασία δοκιμών ακολουθεί επίσης συνεπείς πολιτικές, οι οποίες συμφωνούνται κατά τη διάρκεια του σχεδιασμού ασφάλειας και της αρχικής φάσης σχεδιασμού. (Muhammad, 2023)

- ❖ Ιχνηλασιμότητα, δυνατότητα ελέγχου και ορατότητα (Traceability, auditability & visibility)

Ένας από τους πιο σημαντικούς στόχους του DevSecOps είναι να παρέχει πληροφορίες που βοηθούν στη δημιουργία ενός αξιόπιστου περιβάλλοντος για την επίτευξη της επιθυμητής απόδοσης ασφαλείας του αγωγού SDLC. Για να επιτευχθεί αυτός ο στόχος, η πρακτική DevSecOps ακολουθεί τρία χαρακτηριστικά:

- ➢ Ιχνηλασιμότητα (Traceability): Προσεκτική παρακολούθηση των στοιχείων configuration για συμμόρφωση και κατανόηση του πώς αντιμετωπίζονται τα ζητήματα και οι πολιτικές ασφάλειας.
- ➢ Δυνατότητα ελέγχου (Auditability): Διασφάλιση ότι η διαδικασία είναι καλά τεκμηριωμένη. Οι διοικητικοί έλεγχοι, η εφαρμογή πολιτικών και οι αποφάσεις ασφάλειας θα πρέπει να παρακολουθούνται από ελέγχους (audits and accountability).
- ➢ Ορατότητα (Visibility): Υιοθετούνται ισχυρές δυνατότητες παρακολούθησης (monitoring) και παρατηρησιμότητας (observability) για να επιτευχθεί μια ολιστική και ολοκληρωμένη άποψη της απόδοσης ασφαλείας σε όλο τον αγωγό SDLC.

Το έργο που συνοψίζει αυτές τις έννοιες είναι η παρατηρησιμότητα (observability). (Muhammad, 2023)

- ❖ Συνεχής βελτίωση

Δεδομένου ότι οι απειλές ασφαλείας συνεχίζουν να εξελίσσονται και τα νέα αναπτυξιακά σπριντ (development sprints) μπορούν να εκτεθούν σε διαφορετικούς κινδύνους ασφάλειας, το DevSecOps στοχεύει να βελτιώσει επαναληπτικά την ασφάλεια ενσωματώνοντας ανατροφοδότηση (feedback) σε συνεχή βάση. Αυτή η ανατροφοδότηση προέρχεται από:

- ➢ Πολλαπλές λειτουργικές ομάδες (functional teams)
- ➢ Στελέχη και υπεύθυνοι λήψης επιχειρηματικών αποφάσεων
- ➢ Εξωτερικοί συνεργάτες
- ➢ Τελικοί χρήστες (end-users) στο πραγματικό περιβάλλον.

Ο οργανισμός πρέπει απλά να φροντίσει από την αρχή να διασφαλίσει ότι τα σχόλια σχετικά με την ασφάλεια μπορούν να ενσωματωθούν σε επαναληπτικά σπριντ (iterative sprints) και κύκλους κυκλοφορίας (release cycles). (Muhammad, 2023)

- ❖ Μετατόπιση δεξιά (shift right)

Η μετατόπιση προς τα δεξιά υποδεικνύει τη σημασία της εστίασης στην ασφάλεια μετά την ανάπτυξη της εφαρμογής. Ορισμένες ευπάθειες ενδέχεται να μην εντοπιστούν από προηγούμενους ελέγχους ασφάλειας και να γίνουν εμφανείς μόνο όταν οι πελάτες χρησιμοποιούν το λογισμικό. (aws, χ.χ)

- ❖ Προώθηση της ευαισθητοποίησης για την ασφάλεια

Οι εταιρείες καθιστούν την ευαισθητοποίηση σχετικά με την ασφάλεια μέρος των βασικών τους αξιών κατά την κατασκευή λογισμικού. Κάθε μέλος της ομάδας που παίζει ρόλο στην ανάπτυξη εφαρμογών πρέπει να μοιράζεται την ευθύνη της προστασίας των χρηστών λογισμικού από απειλές ασφάλειας. (aws, χ.χ)

- ❖ Αρχιτεκτονική Μηδενικής Εμπιστευτικότητας (Zero Trust Architecture)

Το κλειδί για την επίλυση προβλημάτων όπως οι επιθέσεις στην αλυσίδα εφοδιασμού είναι η διασφάλιση ότι η στοίβα τεχνολογίας (technology stack) δεν διακυβεύεται από παραβιάσεις ασφάλειας. Εάν ένας κακόβουλος εισβολέας καταφέρει να αποκτήσει διαπιστευτήρια σύνδεσης (login credentials), πρόσβαση στη βάση δεδομένων ή μια διεύθυνση IP εντός του δικτύου, δεν θα πρέπει να μπορεί να αποκτήσει πρόσβαση σε ολόκληρο το δίκτυο. Η μηδενική εμπιστοσύνη είναι ένας άλλος πυλώνας του DevSecOps επειδή διασφαλίζει περιβάλλοντα ανάπτυξης, δοκιμών και παραγωγής, έναντι εσωτερικών και εξωτερικών απειλών. Οι οργανισμοί πρέπει να υιοθετήσουν μια προσέγγιση μηδενικής εμπιστοσύνης όσον αφορά την ασφάλειά τους. Το μοντέλο μηδενικής εμπιστοσύνης αναγνωρίζει ότι η παραδοσιακή περίμετρος δικτύου, στην οποία οι οντότητες εντός της περιμέτρου θεωρούνταν αξιόπιστες, δεν επαρκεί για τα σύγχρονα περιβάλλοντα πληροφορικής. Η τεχνολογία Zero trust επιβάλλει την αρχή του ελάχιστου προνομίου (principle of least privilege) και παρέχει τη δυνατότητα αυτόματης τμηματοποίησης των δικτύων για την αποφυγή lateral movement και τη διασφάλιση της επαλήθευσης κάθε εσωτερικής σύνδεσης πριν γίνει αξιόπιστη. Ο αυτοματισμός μηδενικής εμπιστοσύνης καθιστά δυνατή τη χορήγηση δυναμικών και με λεπτομέρεια αδειών σε χρήστες και λογαριασμούς υπηρεσιών. Τέλος, παρέχει στους νόμιμους χρήστες επαρκή πρόσβαση για να κάνουν τη δουλειά τους, ενώ διασφαλίζει ότι η κακόβουλη ή ύποπτη πρόσβαση μπορεί να αποκλειστεί αμέσως. (Moradov, 2022)

2.6 Ευέλικτη ανάπτυξη (agile development) και DevSecOps?

Η ευελιξία (agile) είναι μια νοοτροπία που βοηθά τις ομάδες λογισμικού να γίνουν πιο αποτελεσματικές στη δημιουργία εφαρμογών και στην ανταπόκριση σε αλλαγές. Οι ομάδες λογισμικού συνήθιζαν να κατασκευάζουν ολόκληρο το σύστημα σε μια σειρά από άκαμπτα/συνεχή (inflexible) στάδια. Με το ευέλικτο πλαίσιο (agile framework), οι ομάδες λογισμικού εργάζονται σε μια συνεχή κυκλική ροή εργασίας. Χρησιμοποιούν ευέλικτες διαδικασίες για να συλλέγουν συνεχή ανατροφοδότηση και να βελτιώνουν τις εφαρμογές σε σύντομους, επαναληπτικούς κύκλους ανάπτυξης.
Το DevSecOps και η ευελιξία δεν αποτελούν ασυσχέτιστες πρακτικές. Η ευελιξία επιτρέπει στην ομάδα λογισμικού να ενεργεί γρήγορα σε αιτήματα αλλαγής και το DevSecOps εισάγει πρακτικές ασφάλειας σε κάθε επαναληπτικό κύκλο στην ευέλικτη ανάπτυξη. Με το DevSecOps, η ομάδα λογισμικού μπορεί να παράγει ασφαλέστερο κώδικα χρησιμοποιώντας ευέλικτες μεθόδους ανάπτυξης. (aws, χ.χ)

2.7 Ποιες είναι οι προκλήσεις εκτέλεσης της πρακτικής DevSecOps?

Οι εταιρείες ενδέχεται να αντιμετωπίσουν τις ακόλουθες προκλήσεις κατά την εισαγωγή της πρακτικής DevSecOps στις ομάδες λογισμικού τους.

- Αντίσταση στην πολιτιστική στροφή

Οι ομάδες λογισμικού και ασφάλειας ακολουθούν τις συμβατικές πρακτικές δημιουργίας λογισμικού εδώ και χρόνια. Οι εταιρείες μπορεί να δυσκολεύονται να υιοθετήσουν γρήγορα τη νοοτροπία DevSecOps στις ομάδες πληροφορικής τους. Οι ομάδες λογισμικού επικεντρώνονται στη δημιουργία, τη δοκιμή και την ανάπτυξη εφαρμογών. Εν τω μεταξύ, οι ομάδες ασφάλειας επικεντρώνονται στη διατήρηση της ασφάλειας της εφαρμογής. Έτσι, και οι δύο ομάδες πρέπει να συνεργαστούν, ώστε το αποτέλεσμα να συμπεριλαμβάνει και πρακτικές ασφάλειας λογισμικού και την έγκαιρη παράδοση. (aws, χ.χ)

- Μάχη των εργαλείων

Εάν οι ομάδες ανάπτυξης, λειτουργιών και ασφάλειας εργάζονταν χωριστά, πιθανότατα χρησιμοποιούσαν διαφορετικές μετρικές και εργαλεία. Κατά συνέπεια, μπορεί να διαφωνούν σχετικά με το ποια εργαλεία να χρησιμοποιήσουν, καθώς δεν είναι εύκολο να συγκεντρωθούν εργαλεία από διάφορα τμήματα και να τα ενσωματώσουν σε μία πλατφόρμα. Η πρόκληση είναι η επιλογή των σωστών εργαλείων και η σωστή ενσωμάτωσή τους για τη δημιουργία, την ανάπτυξη και τη δοκιμή λογισμικού με συνεχή τρόπο. (Rosencrance, 2022)

- Εφαρμογή ασφάλειας σε αγωγούς CI/CD

Γενικά, η ασφάλεια θεωρείται κάτι που έρχεται στο τέλος του κύκλου ανάπτυξης. Ωστόσο, με το DevSecOps, η ασφάλεια αποτελεί μέρος του CI/CD. Για να πετύχει αυτό, οι ομάδες δεν μπορούν να περιμένουν ότι οι διαδικασίες και τα εργαλεία DevOps θα προσαρμοστούν στις παλιές μεθόδους ασφάλειας. Με την ενσωμάτωση των ελέγχων ασφάλειας στις ροές εργασίας DevOps, οι οργανισμοί μπορούν να αξιοποιήσουν πλήρως τις δυνατότητες του CI/CD. Όταν

οι εταιρείες αναπτύσσουν τεχνολογίες ασφάλειας ή ελέγχου πρόσβασης από την αρχή, διασφαλίζουν ότι αυτοί οι έλεγχοι είναι σύμφωνοι με μια ροή CI/CD. (Rosencrance, 2022)

2.8 Καλές πρακτικές για την υποστήριξη μιας ομάδας DevSecOps

Ακολουθούν τρεις βέλτιστες πρακτικές για την υποστήριξη μιας ομάδας DevSecOps:

- Εφαρμογή αυτοματισμού για να ασφαλιστεί το περιβάλλον CI/CD.

Μία από τις βασικές πτυχές του περιβάλλοντος CI/CD είναι η ταχύτητα. Ο αυτοματισμός είναι απαραίτητος για την ενσωμάτωση της ασφάλειας σε αυτό το περιβάλλον, όπως και η ενσωμάτωση των βασικών ελέγχων και δοκιμών ασφάλειας σε όλο τον κύκλο ζωής της ανάπτυξης. Είναι επίσης σημαντική η προσθήκη αυτοματοποιημένων δοκιμών ασφάλειας σε αγωγούς CI/CD για να ενεργοποιηθεί η σάρωση ευπάθειας σε πραγματικό χρόνο.

- Αντιμετώπιση ανησυχιών για την ασφάλεια ανοιχτού κώδικα.

Η χρήση εργαλείων ανοιχτού κώδικα για την ανάπτυξη εφαρμογών αυξάνεται. Ως εκ τούτου, οι οργανισμοί πρέπει να αντιμετωπίσουν τις ανησυχίες για την ασφάλεια σχετικά με τη χρήση τέτοιων τεχνολογιών. Επειδή οι προγραμματιστές είναι συχνά πολύ απασχολημένοι για να ελέγχουν τον ανοιχτό κώδικα, είναι σημαντικό η εφαρμογή αυτοματοποιημένων διαδικασιών για τη διαχείριση του ανοιχτού κώδικα, καθώς και άλλων εργαλείων και τεχνολογιών τρίτων.

- Ενσωμάτωση συστημάτων ασφάλειας εφαρμογών με συστήματα διαχείρισης εργασιών.

Αυτό θα δημιουργήσει αυτόματα μια λίστα σφαλμάτων των εργασιών που μπορεί να εκτελέσει η ομάδα ασφάλειας πληροφοριών. Επιπλέον, θα παρέχει λεπτομέρειες σχετικά με την ανάληψη δράσης, συμπεριλαμβανομένης της φύσης του ελαττώματος, της σοβαρότητάς του και του απαραίτητου μετριασμού του. Ως εκ τούτου, η ομάδα ασφάλειας μπορεί να διορθώσει προβλήματα προτού καταλήξουν στα περιβάλλοντα ανάπτυξης και παραγωγής. (Rosencrance, 2022)

2.9 Δεξιότητες και κανόνες για κάποιον που συμμετέχει στη μεθοδολογία DevSecOps

Οι μηχανικοί DevSecOps χρειάζονται τις τεχνικές δεξιότητες των ειδικών ανάπτυξης και πληροφορικής καθώς και τη γνώση της μεθοδολογίας DevOps. Χρειάζονται επίσης βαθιά γνώση της ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένων των πιο πρόσφατων απειλών. Τα ακόλουθα είναι μεταξύ των βασικών δεξιοτήτων που χρειάζονται οι μηχανικοί DevSecOps:

- Κατανόηση των αρχών και της κουλτούρας της πρακτικής DevOps.
- Γνώση γλωσσών προγραμματισμού, όπως Bash, Go, Python και C.
- Ισχυρές δεξιότητες επικοινωνίας και ομαδικής εργασίας.

- Κατανόηση των τεχνικών εκτίμησης κινδύνου και της μοντελοποίησης απειλών.
- Ενημερωμένη γνώση των απειλών στον κυβερνοχώρο, του λογισμικού και των βέλτιστων πρακτικών.
- Κατανόηση των εργαλείων DevOps και DevSecOps όπως τα Kubernetes, Ansible, Chef, Puppet και Aqua.
- Ενσωμάτωση της ασφάλειας στη μηχανική (engineering).
- Συνεχείς αξιολογήσεις και έλεγχοι συμμόρφωσης.
- Ειδοποίηση απειλών σε πραγματικό χρόνο σε εφαρμογές και υπηρεσίες.
- Βελτίωση του DNA της ασφάλειας ενός προγραμματιστή με:

    - Ανάλυση Κώδικα
    - Διαχείριση Αλλαγών
    - Παρακολούθηση Συμμόρφωσης
    - Διερεύνηση απειλών
    - Διαχείριση ευπάθειας
    - Εκπαίδευση ασφάλειας

τα οποία θα αναλυθούν περαιτέρω παρακάτω.

- Ανάλυση Κώδικα (Code Analysis)
    - Ασφάλιση του αγωγού (pipeline) CI/CD.
    - Release σε μικρά και συχνά batches.
    - Ενσωμάτωση της ανάλυσης κώδικα στο Q/A.
    - Χρησιμοποίηση εργαλείων για εντοπισμό ότι τα ιδιωτικά κλειδιά ή οι πληροφορίες του API δεν προωθούνται στο στοιχείο ελέγχου έκδοσης (Version Control).

- Διαχείριση Αλλαγών (Change Management)
    - Ενδυνάμωση των ομάδων να βελτιώσουν τις πρακτικές ασφάλειας και να κάνουν αλλαγές όταν χρειάζεται.
    - Γρήγορη διαδικασία ελέγχου και έγκρισης.
    - Ικανοποίηση των απαιτήσεων συμμόρφωσης.

- Παρακολούθηση συμμόρφωσης (Compliance Monitoring)
    - Επιβολή καλών πρακτικών στις λειτουργίες και στην ασφάλεια.
    - Καθιέρωση αυστηρών πολιτικών κωδικών πρόσβασης.
    - Πλήρης έλεγχος, από προωθήσεις κώδικα (code pushes), μέχρι αγωγούς (pipelines) και συμμόρφωση (compliances).
    - Παρακολούθηση συστημάτων για κακή/παραβατική συμπεριφορά.

- Έρευνες απειλών (Threat Investigations)
    - Παρακολούθηση εφαρμογών και υπηρεσιών για εντοπισμό και ειδοποίηση απειλών.
    - Ενσωματωμένες ειδοποιήσεις και έλεγχοι σε πραγματικό χρόνο.

- ➢ Ανάπτυξη Ansible playbooks και σενάριων απόκρισης (response scenarios) για τους τομείς της πληροφορικής και της ασφάλειας.

❖ Έλεγχοι ευπάθειας (Vulnerability Checks)
- ➢ Διεξαγωγή σαρώσεων και πρακτικών ευπάθειας.
- ➢ Διεξαγωγή περιοδικών σαρώσεων της κατασκευής του προϊόντος (product build).
- ➢ Επανεξέταση κώδικα και penetration tests.
- ➢ Δημιουργία SLA αποκατάστασης (Establish remediation SLAs).

❖ Εκπαίδευση ασφάλειας
- ➢ Μετατροπή της ομάδας σε "νίντζα ασφαλείας".
- ➢ Συμμετοχή σε συνέδρια επιμόρφωσης.
- ➢ Επένδυση σε πιστοποιήσεις ασφαλείας.
- ➢ Εκπαίδευση των εργαζομένων σχετικά με τους κινδύνους ασφάλειας.
- ➢ Προετοιμασία των ομάδων για την αντιμετώπιση των περιστατικών.

(Rosencrance, 2022; Navdeep, 2023)

2.10 Τρεις περιπτώσεις χρήσης που οδηγούν τις εταιρείες να υιοθετήσουν πρακτικές DevSecOps

Οι τρεις μεγαλύτερες περιπτώσεις χρήσης DevSecOps για επιχειρήσεις περιλαμβάνουν την ασφάλεια εφαρμογών, την ασφάλεια IaC και την ασφάλεια αγωγών (pipeline security). Ας τα δούμε αυτά σε μεγαλύτερο βάθος για να δείξουμε τα θετικά αποτελέσματα του DevSecOps στην ανάπτυξη των επιχειρήσεων.

❖ Ασφάλεια Εφαρμογών (Application Security)

Η κύρια περίπτωση χρήσης DevSecOps σε μια εταιρεία είναι η ασφάλεια εφαρμογών ή το AppSec. Το AppSec ασχολείται με την εύρεση τρωτών σημείων σε κώδικα, εικόνες κοντέινερ και εξαρτήσεις τρίτων. Ως μέρος του DevSecOps, η ασφάλεια εφαρμογών είναι μια συνεχής διαδικασία που εστιάζει στην εύρεση και τη διόρθωση προβλημάτων όσο το δυνατόν νωρίτερα (γνωστή ως shifting-left). Το AppSec χρησιμοποιεί διάφορες μεθόδους δοκιμών για να το πετύχει αυτό, όπως:

- ➢ Στατική δοκιμή ασφάλειας εφαρμογών (SAST): Σαρώνει τον πηγαίο κώδικα για ευπάθειες πριν από τη μεταγλώττιση.
- ➢ Δυναμική δοκιμή ασφάλειας εφαρμογών (DAST): Προσομοιώνει μια ηλεκτρονική επίθεση χωρίς άμεση πρόσβαση στον πηγαίο κώδικα.
- ➢ Ανάλυση σύνθεσης λογισμικού (SCA): Προσδιορίζει και αξιολογεί την ασφάλεια πακέτων ανοιχτού κώδικα.
- ➢ Διαδραστική δοκιμή ασφάλειας εφαρμογών (IAST): Σαρώνει για ευπάθειες στον εκτελούμενο κώδικα σε πραγματικό χρόνο.

Το κλειδί για τις περιπτώσεις χρήσης του AppSec στο DevSecOps είναι ο έγκαιρος εντοπισμός των τρωτών σημείων με την ενσωμάτωση του αυτοματισμού δοκιμών απευθείας σε συστήματα ελέγχου έκδοσης. Αυτό το βήμα κάνει την ασφάλεια περισσότερο προληπτική παρά διαδραστική, επειδή εντοπίζονται ευπάθειες κατά τη διάρκεια της κατασκευής (build) του κώδικα, με αποτέλεσμα να είναι πιο εύκολο για τους προγραμματιστές να επιλύσουν το πρόβλημα. Κάτι τέτοιο αποτρέπει τα τρωτά σημεία να περάσουν σε μεταγενέστερα στάδια του αγωγού ή ακόμα και στην τελική απελευθέρωση (final release). Επιπλέον, η πρακτική DevSecOps εξομαλύνει το χάσμα μεταξύ των ομάδων ασφάλειας και ανάπτυξης. Οι ομάδες ασφαλείας επικεντρώνονται στην εύρεση και τη διόρθωση κάθε ευπάθειας και δεν γνωρίζουν (ή ακόμη και ενδιαφέρονται) πώς αυτές οι διορθώσεις θα επηρεάσουν τα χαρακτηριστικά της λειτουργίας. Οι ομάδες ανάπτυξης γνωρίζουν το πλαίσιο για κάθε ευπάθεια. Μπορεί να κατανοήσουν καλύτερα τι συνιστά πραγματικό κίνδυνο, αλλά η εστίασή τους στην απελευθέρωση εφαρμογών/λειτουργιών όσο το δυνατόν γρηγορότερα σημαίνει ότι μπορεί να χάσουν τις πραγματικές απειλές. Αυτοί οι διαφορετικοί στόχοι μπορεί να προκαλέσουν απογοήτευση και στις δύο πλευρές και να εμποδίσουν τη συνεργασία τους. Το AppSec στο DevSecOps παρέχει περισσότερη γνώση ασφάλειας στην ομάδα ανάπτυξης, εμφανίζοντας ευπάθειες κατά τη διαδικασία κατασκευής (build process) και αναγνωρίζοντας συμβάντα στον προγραμματιστή. Αυτός γνωρίζει ακριβώς πώς υποτίθεται ότι λειτουργεί αυτός ο κώδικας, ας είναι η ευπάθεια πραγματικός κίνδυνος ή ψευδώς θετική (false positive) και το τρόπο με τον οποίο η επιδιόρθωση θα επηρεάσει τη λειτουργικότητα των χαρακτηριστικών. Επενδύουν επίσης περισσότερο στην ασφάλεια των λειτουργιών, επειδή είναι υπεύθυνες για την επιδιόρθωση των τρωτών σημείων, πράγμα που σημαίνει ότι οι στόχοι τους ευθυγραμμίζονται στενά με την ομάδα ασφαλείας. Αυτή η συνθήκη ενθαρρύνει την ομαλότερη συνεργασία DevSecOps βελτιώνοντας παράλληλα την ασφάλεια των εκδόσεων.

- ❖ Η ασφάλεια υποδομής ως κώδικα (Infrastructure as Code ή IaC Security).

Το Infrastructure As Code (IaC) μετατρέπει τις διαμορφώσεις υποδομής (infrastructure configurations) του cloud ή της εσωτερικής εγκατάστασης (on-premises) σε αρχεία κώδικα λογισμικού αποσυνδεδεμένα από το υποκείμενο υλικό (hardware). Τα αρχεία διαμόρφωσης IaC αναπτύσσουν αυτόματα και ενημερώνουν τα περιβάλλοντα στην κλίμακα που απαιτείται για αγωγούς DevOps με γρήγορο ρυθμό. Το IaC επιταχύνει την παροχή υποδομής (infrastructure provisioning), αλλά προσθέτει και πολυπλοκότητα, η οποία μπορεί να προκαλέσει ευπάθειες ασφαλείας. Οι εσφαλμένες διαμορφώσεις του cloud είναι μια κύρια αιτία παραβιάσεων της ασφάλειας και η πολυπλοκότητα του κώδικα IaC αυξάνει σημαντικά τον κίνδυνο λάθους. Επιπλέον, λόγω του κενού στις δεξιότητες προγραμματισμού και αυτοματισμού σε πολλές ομάδες υποδομής (infrastructure teams), υπάρχει μεγάλη εξάρτηση από πρότυπα IaC ανοιχτού κώδικα, που συχνά περιέχουν εσφαλμένες διαμορφώσεις. Εάν αυτές οι εσφαλμένες διαμορφώσεις δεν εντοπιστούν και δεν επιδιορθωθούν έγκαιρα, εισάγουν ευπάθειες που θα πρέπει να αντιμετωπιστούν αργότερα, ή, ακόμη χειρότερα, θα μπορούσαν να φτάσουν στη φάση της παραγωγής και να οδηγήσουν σε μια δαπανηρή επιδιόρθωση. Τα εργαλεία σάρωσης ασφαλείας DevSecOps για το IaC επιτρέπουν στις ομάδες υποδομής να μετατοπίζουν την ασφάλεια προς τα αριστερά εντοπίζοντας εσφαλμένες διαμορφώσεις πριν από την ανάπτυξη. Αυτά τα εργαλεία μπορούν να συνδυαστούν με λύσεις

διαχείρισης διαμόρφωσης (configuration management solutions) που παρακολουθούν τους ενεργούς πόρους για αλλαγή της διαμόρφωσης για να διασφαλίσουν ότι οι ενημερώσεις και οι αλλαγές δεν εισάγουν νέα τρωτά σημεία. Οι περιπτώσεις χρήσης DevSecOps για IaC διευκολύνουν την αποτελεσματική και αυτόματη παροχή πόρων χωρίς να θυσιάζεται η ασφάλεια.

- ❖ Ασφάλεια αγωγών (Pipeline Security)

Ένας αγωγός DevSecOps αποτελείται από πολλά συστατικά μέρη, καθένα από τα οποία θα μπορούσε ενδεχομένως να εισάγει μια ευπάθεια. Το σύστημα ελέγχου έκδοσης (version control system ή VCS), το αποθετήριο πηγαίου κώδικα (source code repository), η σουίτα αυτοματισμού δοκιμών (test automation suite) και οι ροές εργασιών συνεχούς ενσωμάτωσης/συνεχούς ανάπτυξης θα μπορούσαν να αξιοποιηθούν για την πρόσβαση σε πιο πολύτιμα δεδομένα και πόρους. Επιπλέον, αυτά τα εργαλεία πρέπει να ενσωματωθούν σε μια συνεκτική διοχέτευση (cohesive pipeline) χρησιμοποιώντας API, το οποίο είναι ένα ακόμη πιθανό σημείο εισόδου για κακόβουλους εισβολείς. Αυτός είναι ο λόγος για τον οποίο η ασφάλεια αγωγών είναι μια σημαντική περίπτωση χρήσης DevSecOps για επιχειρήσεις. Τα εργαλεία ασφαλείας των αγωγών DevSecOps σαρώνουν τις διαμορφώσεις (configurations) για να διασφαλίσουν ότι ακολουθούνται οι βέλτιστες πρακτικές, όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων (multi-factor authentication ή MFA) και οι υπογεγραμμένες δεσμεύσεις (signed commits). Επιπλέον, οι λύσεις παρακολούθησης αγωγών (pipeline monitoring) και το orchestration παρέχουν ορατότητα στις συνδέσεις μεταξύ μεμονωμένων στοιχείων και του αγωγού στο σύνολό του. Εάν είναι κατανοητό κάθε στοιχείο του αγωγού, συμπεριλαμβανομένων όλων των συνδέσεων API, θα είναι ευκολότερο να εντοπίσουμε πιθανές ευπάθειες και να τις διορθώσουμε πριν γίνουν αντικείμενο εκμετάλλευσης. Οι περιπτώσεις χρήσης DevSecOps για επιχειρήσεις επικεντρώνονται στη μετατόπιση της ασφάλειας προς τα αριστερά για να διασφαλιστεί πιο ασφαλές λογισμικό, υποδομή και αγωγοί. (Copado, 2022)

Κεφ 3. OWASP Top Ten Μεθοδολογία

Το OWASP είναι ένα έργο ασφάλειας ανοιχτών εφαρμογών ιστού (open web application security project). Βασικά, είναι ένας μη κερδοσκοπικός οργανισμός που λειτουργεί κάτω από ένα μοντέλο ανοιχτής κοινότητας για τη βελτίωση της ασφάλειας λογισμικού. Προσφέρει δωρεάν πληροφορίες ασφαλείας στους χρήστες και οποιοσδήποτε μπορεί να ενταχθεί στην κοινότητα και να συνεισφέρει σε έργα που σχετίζονται με το OWASP.
Το OWASP Top 10 είναι ένα πρόγραμμα που προσφέρει τις 10 κορυφαίες ευπάθειες ασφαλείας μαζί με καθοδήγηση αποκατάστασης με βάση τη συναίνεση μεταξύ των κοινοτικών συνεργατών που είναι επίσης ειδικοί σε θέματα ασφάλειας και διαθέτουν τεράστια γνώση και εμπειρία σε αυτόν τον τομέα. Το πρόγραμμα Top 10 κατατάσσει τα τρωτά σημεία (vulnerabilities) με βάση τη συχνότητα των απειλών για την ασφάλεια και τη σοβαρότητα και το μέγεθος των επιπτώσεων. Από το 2003, το πρόγραμμα Top 10 ενημερώνει τη λίστα κάθε 2-3 χρόνια, λαμβάνοντας υπόψη τις μεταβαλλόμενες τάσεις στην αγορά AppSec. Οι οργανισμοί που κάνουν ελέγχους (auditing agencies), εξετάζουν το ενδεχόμενο εφαρμογής του Top 10 στο CI/CD ή το SDLC, ως τήρηση της συμμόρφωσης με την ασφάλεια και των βέλτιστων πρακτικών.
Αυτοί είναι οι 10 κορυφαίοι κίνδυνοι και πρακτικές που κάθε προγραμματιστής και μηχανικός DevOps πρέπει να λάβει υπόψη:

- Κατεστραμμένοι έλεγχοι πρόσβασης (Broken access controls)
- Κρυπτογραφικές αποτυχίες
- Injection
- Σχεδιασμός χωρίς ασφάλεια
- Λανθασμένες διαμορφώσεις ασφαλείας (Security misconfiguration)
- Ευάλωτα και ξεπερασμένα εξαρτήματα (components)
- Αποτυχίες αναγνώρισης και επαλήθευσης ταυτότητας
- Αποτυχίες ακεραιότητας λογισμικού και ακεραιότητας δεδομένων
- Αποτυχίες καταγραφής και παρακολούθησης ασφαλείας
- Παραχάραξη αιτημάτων από την πλευρά του διακομιστή (Server-side request forgery ή SSRF)

(William, 2022)

3.1 OWASP και DevSecOps

Οι οδηγίες DevSecOps του OWASP βοηθούν τους οργανισμούς όλων των μεγεθών να δημιουργήσουν έναν ασφαλή αγωγό CI/CD εφαρμόζοντας τα παρακάτω μέτρα ασφαλείας με μια προσέγγιση ασφάλειας μετατόπισης προς τα αριστερά. Ακολουθούν τα βήματα για την εφαρμογή των κατευθυντήριων γραμμών OWASP DevSecOps σε έναν βασικό αγωγό CI/CD ακολουθώντας αυτούς τους κορυφαίους ελέγχους ασφαλείας.

- Σάρωση Git Repo
- Στατική δοκιμή ασφάλειας εφαρμογών (SAST)
- Ανάλυση σύνθεσης λογισμικού (SCA)
- Διαδραστική δοκιμή ασφάλειας εφαρμογών (IAST)
- Δυναμική δοκιμή ασφάλειας εφαρμογών (DAST)
- Σάρωση υποδομής ως κώδικα (IaC).
- Σάρωση υποδομής (Infrastructure Scanning)
- Έλεγχος συμμόρφωσης (Compliance Check)

Αυτά τα βήματα μπορούν να προσαρμοστούν για να ταιριάζουν στις απαιτήσεις του οργανισμού. Εφαρμόζοντας αυτούς τους ελέγχους ασφαλείας, οι οργανισμοί μπορούν να μειώσουν τις λειτουργικές αποτυχίες και τα σφάλματα στα συστήματα, ενώ θωρακίζουν τις εφαρμογές έναντι επιθέσεων στον κυβερνοχώρο. Εκτός από την παροχή ισχυρότερης κρυπτογράφησης και πιο ασφαλών τελικών προϊόντων, οι οργανισμοί μπορούν να αυξήσουν την αυθεντικότητα και την εικόνα της επωνυμίας τους ως εταιρείες συμβατές με την ασφάλεια. (William, 2022)

Κεφ 4. Εργαλεία DevSecOps

4.1 Τι είναι τα εργαλεία DevSecOps?

Τα εργαλεία DevSecOps είναι μια σειρά προϊόντων και υπηρεσιών κυβερνοασφάλειας που επιτρέπουν στους οργανισμούς να αναπτύσσουν και να λειτουργούν συστήματα λογισμικού με ασφάλεια. Με ένα αυξανόμενο εύρος εφαρμογών Ιστού, τα εργαλεία DevSecOps διασφαλίζουν ότι οι παραδοσιακοί αγωγοί CI/CD διατηρούν την ασφάλεια σε κάθε στάδιο του κύκλου ζωής ανάπτυξης του συστήματος ή του λογισμικού. (Ingalls, 2022)
Τρεις κύριοι στόχοι των εργαλείων DevSecOps:

- Ελαχιστοποίηση του κινδύνου χωρίς επιβράδυνση της ταχύτητας – Επιτυγχάνεται με την εφαρμογή συνεχών δοκιμών ασφάλειας, οι οποίες βοηθούν στον εντοπισμό και τη διόρθωση τρωτών σημείων ασφαλείας.
- Υποστήριξη ομάδων ασφάλειας με αυτοματισμό – Βοηθά τις ομάδες να ασφαλίζουν έργα ανάπτυξης (development projects) χωρίς να εξετάζουν και να εγκρίνουν χειροκίνητα κάθε έκδοση.
- Μετατόπιση της ασφάλειας προς τα αριστερά (shift left) – Τα εργαλεία DevSecOps μπορούν να βοηθήσουν στην αυτοματοποίηση των εργασιών ασφάλειας για να τους βοηθήσουν να εκτελούνται νωρίτερα στον κύκλο ζωής της ανάπτυξης. (Tigera, χ.χ.)

Τα τελευταία χρόνια έχουμε δει πολλά νέα εργαλεία DevSecOps που έχουν σχεδιαστεί για να ασφαλίζουν αγωγούς (pipelines) και διαδικασίες DevOps για οργανισμούς και τελικά να παρέχουν ένα πιο αξιόπιστο τελικό προϊόν ή σύστημα. Οι προγραμματιστές μπορούν να χρησιμοποιήσουν τα εργαλεία DevSecOps για να δοκιμάσουν εφαρμογές σε όλη τη διαδικασία ανάπτυξης, διασφαλίζοντας παράλληλα ασφάλεια και συμμόρφωση (compliance). (Ingalls, 2022)

4.2 Ποιοι είναι οι διαφορετικοί τύποι των εργαλείων DevSecOps?

- Εργαλεία Αυτοματισμού (Automation Tools)

Ο αυτοματισμός είναι βασικό και μερικές φορές αναπόσπαστο μέρος του σύγχρονου αγωγού ανάπτυξης. Ο αυτοματισμός βοηθά τις ομάδες DevSecOps να εισαγάγουν ασφάλεια σε όλες τις φάσεις ανάπτυξης χωρίς να επιβραδύνουν τον αγωγό. (Tigera, χ.χ.)

- Εργαλεία ασφάλειας κοντέινερ ή σάρωσης εικόνων (Container Security Tools or Image Scanning)

Η τεχνολογία ασφάλειας κοντέινερ μπορεί να βοηθήσει να διασφαλιστεί ότι τα κοντέινερ, οι εικόνες κοντέινερ και τα σχετικά στοιχεία έχουν διαμορφωθεί με ασφάλεια και χωρίς τρωτά σημεία. Οι ομάδες DevOps αναπτύσσουν συνήθως στοιχεία χρησιμοποιώντας εικόνες Docker και κοντέινερ. Σε ένα περιβάλλον DevSecOps, μία από τις κύριες ανησυχίες είναι ο

εντοπισμός τρωτών σημείων σε εικόνες κοντέινερ, καθώς είναι σύνηθες να αντλούνται από δημόσια αποθετήρια ή άλλες μη αξιόπιστες πηγές. Οι εικόνες Docker, και οι βασικές εικόνες στις οποίες βασίζονται, ενδέχεται να περιέχουν πολλά στοιχεία λογισμικού που μπορεί να είναι παλιά, μη επιδιορθωμένα ή μπορεί να περιέχουν ευπάθειες ασφάλειας. Οι σαρωτές εικόνων κοντέινερ επαληθεύουν ότι οι εικόνες περιέχουν μόνο αξιόπιστο, ασφαλή κώδικα και ότι συμμορφώνονται με τις βέλτιστες πρακτικές ασφαλούς διαμόρφωσης (configuration). Οι διαδικασίες DevSecOps που περιλαμβάνουν κοντέινερ πρέπει να περιλαμβάνουν σάρωση εικόνας σε κάθε στάδιο CI/CD του αγωγού. (Aquasec, χ.χ.)

- Εργαλεία δοκιμών cloud (Cloud Testing Tools)

Τα εργαλεία δοκιμής cloud παρέχουν περιβάλλοντα δοκιμών ειδικά για το cloud, συμπεριλαμβανομένων όλων των απαραίτητων διαμορφώσεων λογισμικού-υλικού. Οι περισσότερες πλατφόρμες δοκιμών που βασίζονται σε cloud προσφέρουν ενσωματώσεις με εργαλεία DevSecOps και ροές εργασίας CI/CD. (Tigera, χ.χ.)

- Στατική δοκιμή ασφάλειας εφαρμογών (SAST)

Τα εργαλεία SAST σαρώνουν τον κώδικα για σφάλματα κωδικοποίησης και ελαττώματα σχεδιασμού που θα μπορούσαν να οδηγήσουν σε εκμεταλλεύσιμες αδυναμίες. (Synopsys, χ.χ.)

- Ανάλυση σύνθεσης λογισμικού (SCA)

Τα εργαλεία SCA σαρώνουν τον πηγαίο κώδικα και τα δυαδικά αρχεία για να εντοπίσουν γνωστές ευπάθειες σε στοιχεία ανοιχτού κώδικα και τρίτων. Παρέχουν επίσης πληροφορίες σχετικά με την ασφάλεια και τους κινδύνους αδειοδότησης για την επιτάχυνση των προσπαθειών ιεράρχησης και αποκατάστασης (remediation). Επιπλέον, μπορούν να ενσωματωθούν ομαλά σε μια διαδικασία CI/CD για την συνεχή ανίχνευση νέων ευπαθειών ανοιχτού κώδικα, από το build έως την κυκλοφορία της έκδοσης πριν από την παραγωγή. (Synopsys, χ.χ.)

- Διαδραστική δοκιμή ασφάλειας εφαρμογών (IAST)

Τα εργαλεία IAST λειτουργούν στο παρασκήνιο κατά τη διάρκεια χειροκίνητων ή αυτοματοποιημένων λειτουργικών δοκιμών για την ανάλυση της συμπεριφοράς του χρόνου εκτέλεσης των εφαρμογών του Ιστού. Για παράδειγμα, τα εργαλεία IAST χρησιμοποιούν instrumentation για να παρατηρούν τις αλληλεπιδράσεις αιτήματος/απόκρισης εφαρμογής, τη συμπεριφορά και τη ροή δεδομένων. Ανιχνεύουν ευπάθειες χρόνου εκτέλεσης και αναπαράγουν αυτόματα και δοκιμάζουν τα αποτελέσματα, παρέχοντας λεπτομερείς πληροφορίες στους προγραμματιστές, όπως, μέχρι και τη γραμμή κώδικα όπου εμφανίζονται αυτές οι ευπάθειες. Αυτό δίνει τη δυνατότητα στους προγραμματιστές να εστιάσουν σε κρίσιμα τρωτά σημεία. (Synopsys, χ.χ.)

- Δυναμική δοκιμή ασφάλειας εφαρμογών (DAST)

Το DAST είναι μια αυτοματοποιημένη τεχνολογία δοκιμών αδιαφανών κουτιών (opaque box or white box testing technology) που μιμείται τον τρόπο με τον οποίο ένας χάκερ θα αλληλεπιδράσει με την εφαρμογή Ιστού ή το API. Δοκιμάζει εφαρμογές μέσω μιας σύνδεσης

δικτύου και εξετάζει την απόδοση της εφαρμογής από την πλευρά του πελάτη, όπως θα έκανε ένας penetration tester. Τα εργαλεία DAST δεν απαιτούν πρόσβαση στον πηγαίο κώδικα ή προσαρμογή (customization) αλλά αλληλεπιδρούν με τον ιστότοπο και βρίσκουν τρωτά σημεία με χαμηλό ποσοστό ψευδών θετικών (false positive) αποτελεσμάτων. Για παράδειγμα, τα εργαλεία DAST εντοπίζουν τρωτά σημεία σε εφαρμογές ιστού και API, συμπεριλαμβανομένων συσκευών συνδεδεμένων στον Ιστό, όπως διακομιστές υποστήριξης για φορητές συσκευές, συσκευές IoT και API RESTful ή GraphQL. (Synopsys, χ.χ.)

- ❖ Παρακολούθησης προβλημάτων του συστήματος ή εργαλεία ειδοποίησης (Issue Tracking System or Alerting Tools)

Τα εργαλεία ειδοποίησης βοηθούν τις ομάδες DevSecOps να ανταποκρίνονται γρήγορα σε συμβάντα ασφάλειας. Ιδανικά, ένα εργαλείο ειδοποίησης, ειδοποιεί την ομάδα μόνο αφού το συμβάν αναλυθεί, ιεραρχηθεί και κριθεί άξιο της προσοχής της ομάδας. Αυτό είναι κρίσιμο για τη μείωση του θορύβου στο σύστημα και την αποφυγή διακοπής των ροών εργασίας DevSecOps. Μόλις ειδοποιηθούν οι ομάδες, μπορούν να διερευνήσουν γρήγορα το συμβάν και να εφαρμόσουν τις διορθώσεις που απαιτούνται. (Aquasec, χ.χ.)
Τα συστήματα παρακολούθησης ζητημάτων υποστηρίζουν πολλές βασικές φάσεις και δραστηριότητες DevSecOps. Τα βασικά χαρακτηριστικά των εργαλείων παρακολούθησης ζητημάτων περιλαμβάνουν:

- ➢ Αυτοματισμός: Βελτιώνει την αποτελεσματικότητα της μηχανικής (engineering) αυτοματοποιώντας διαδικασίες όπως το κλείσιμο ζητημάτων, η ειδοποίηση πελατών, η ανάθεση ζητημάτων και άλλα.
- ➢ Παρακολούθηση και ιστορικό επίλυσης προβλημάτων: Παρέχει ορατότητα και δομή για την αποτελεσματική διαχείριση σφαλμάτων. Δημιουργεί επίσης ένα αρχείο δραστηριοτήτων που σχετίζονται με την επίλυση προβλημάτων.
- ➢ Διαχείριση αλλαγών: Εξοπλίζει τις ομάδες με την ανάπτυξη νέων χαρακτηριστικών. Προσφέρει διαδραστικές ροές εργασίας και στρατηγικές (roadmaps) για την υποστήριξη του σχεδιασμού και της ανάπτυξης.
- ➢ Διαχείριση ιεράρχησης προτεραιοτήτων: Επιτρέπει στις ομάδες να ιεραρχούν εύκολα διαφορετικές επιδιορθώσεις και δραστηριότητες, ώστε να αντιμετωπίζουν συνεχώς τα πιο σημαντικά στοιχεία.
- ➢ Δυνατότητες αυτοματοποιημένων αναφορών: Προσφέρει μια ενοποιημένη προβολή άλυτων και επιλυμένων προβλημάτων, ταχύτητα επίλυσης, ταχύτητα ανάπτυξης και άλλες σημαντικές μετρήσεις. (Fossa, 2022)

- ❖ Ταμπλό και Εργαλεία Οπτικοποίησης (Dashboard and Visualization Tools)

Οι ομάδες DevSecOps χρειάζονται εργαλεία που καθιστούν δυνατή την προβολή και την κοινή χρήση πληροφοριών ασφάλειας μεταξύ των ομάδων προγραμματισμού, λειτουργιών, DevOps και ασφάλειας. Αποτελεσματικά εργαλεία δείχνουν τους KPI με τρόπο που να έχει νόημα για όλους τους εμπλεκόμενους, για παράδειγμα, οπτικοποιώντας την αύξηση ή τη μείωση των τρωτών σημείων για μια συγκεκριμένη εφαρμογή με την πάροδο του χρόνου. Οι προσαρμοσμένοι πίνακες εργαλείων (custom dashboards) μπορούν να συγκεντρώνουν όλα τα σχετικά δεδομένα ασφάλειας, δεδομένα καταγραφής, και άλλα στατιστικά στοιχεία παρακολούθησης εφαρμογών ορατά σε όλα τα μέλη της ομάδας. (Aquasec, χ.χ.)

- Εργαλεία μοντελοποίησης απειλών (Threat Modeling Tools)

Τα εργαλεία μοντελοποίησης απειλών βοηθούν την ομάδα DevSecOps να προβλέπει, να ανιχνεύει και να αξιολογεί απειλές σε ολόκληρη την επιφάνεια επίθεσης. Ο στόχος είναι να επιτραπεί στις ομάδες να λαμβάνουν γρήγορα αποφάσεις που βασίζονται σε δεδομένα και να ελαχιστοποιούν την έκθεσή τους στον κίνδυνο ασφάλειας. Υπάρχουν πολλά διαθέσιμα εργαλεία με ένα ευρύ φάσμα δυνατοτήτων και λύσεις, που μπορούν να χρησιμοποιήσουν δεδομένα για την αυτόματη δημιουργία μοντέλων απειλών όπως είναι οι οπτικοί πίνακες εργαλείων (visual dashboards). (Aquasec, χ.χ.)

4.3 Πως να επιλέξουμε ένα εργαλείο DevSecOps

Όπως τα περισσότερα προϊόντα κυβερνοασφάλειας, το ιδανικό εργαλείο DevSecOps πρέπει να καλύπτει τις συγκεκριμένες ανάγκες ενός οργανισμού ή μιας ομάδας. Υπάρχουν πολλές διαφορές στην τιμολόγηση και στις δυνατότητες μεταξύ των παραπάνω λύσεων που δίνουν στους οργανισμούς πολλά να αξιολογήσουν σε σχέση με τον προϋπολογισμό που διαθέτουν. Τα περισσότερα πακέτα για επιχειρήσεις κοστίζουν δεκάδες χιλιάδες δολάρια για μια ετήσια άδεια. Επομένως, η επιλογή μιας ολοκληρωμένης λύσης DevSecOps δεν είναι εύκολη δουλειά. Το πλεονέκτημα των πακέτων αυτών είναι η αυξανόμενη λίστα εργαλείων και δυνατοτήτων που διατίθενται για τη δημιουργία ενός ισχυρού μοντέλου λογισμικού ασφαλείας. Ο πολλαπλασιασμός των εφαρμογών σημαίνει ότι η ανάπτυξη λογισμικού θα λάβει αυξανόμενη ρυθμιστική προσοχή. Τα εργαλεία DevSecOps θα μπορούσαν να κάνουν τη διαφορά στη δημιουργία μιας αξιόπιστης, ασφαλούς και συμβατής λύσης λογισμικού για πελάτες ή ενδιαφερόμενους φορείς. (Ingalls, 2022)

Για να επιλέξει το καλύτερο εργαλείο DevSecOps ο κάθε οργανισμός, πρέπει να λάβει υπόψη τα εξής:

- Υποστήριξη περιβάλλοντος

Η επιλογή του καλύτερου εργαλείου DevSecOps για εμάς θα πρέπει να ξεκινήσει με το περιβάλλον ανάπτυξης που χρησιμοποιούμε. Η επιλογή ενός προϊόντος που δεν υποστηρίζει ενεργά το περιβάλλον DevOps θα εισαγάγει ακόμη περισσότερες ευπάθειες ασφαλείας, επομένως αυτό θα πρέπει να είναι το πρώτο βήμα στη διαδικασία λήψης αποφάσεων. Για παράδειγμα, εάν χρειαζόμαστε συγκεκριμένη προστασία για στοιχεία Ιστού, η Acunetix ειδικεύεται σε αυτό το είδος υποστήριξης. Εάν χρειαζόμαστε υποστήριξη για περιβάλλοντα με κοντέινερ, το Aqua Security διαθέτει εκτεταμένα εργαλεία για την συγκεκριμένη δουλειά.

- Γλώσσα προγραμματισμού

Όπως και με την υποστήριξη περιβάλλοντος, θα χρειαστούμε ένα εργαλείο DevSecOps που μπορεί να υποστηρίξει τη γλώσσα προγραμματισμού που χρησιμοποιεί η ομάδα μας. Ενώ οι

πιο κοινές γλώσσες όπως η SQL και η Java υποστηρίζονται ευρέως, οι πιο εξειδικευμένες γλώσσες, ενδέχεται να μην είναι συμβατές με όλα τα εργαλεία DevSecOps.

- Κουλτούρα ανάπτυξης

Το DevSecOps εκτός από φιλοσοφία είναι και μια κατηγορία προϊόντων. Αν και η συμπερίληψη της ασφάλειας σε έναν αγωγό DevOps γίνεται γρήγορα αποδεκτή, η εισαγωγή της σε μια υπάρχουσα ροή εργασίας μπορεί να έχει ως αποτέλεσμα να χαλάσει η συνολική εργασιακή κουλτούρα. Το πόσο ανθεκτικές μπορεί να είναι οι ομάδες στη συμπερίληψη της ασφάλειας είναι ένα περίπλοκο ζήτημα, αλλά γενικά θα θελήσουμε να εξετάσουμε ένα εργαλείο DevSecOps που είναι εύκολο στη χρήση σε όλα τα επίπεδα δεξιοτήτων και ενσωματώνεται επίσης καλά στις υπάρχουσες ροές εργασίας.

- Ανοιχτού κώδικα ή επί πληρωμή εργαλεία

Υπάρχει μια πληθώρα εργαλείων ανοιχτού κώδικα που καλύπτουν την ευρεία εμβέλεια των αναγκών του DevSecOps. Εργαλεία ανοιχτού κώδικα όπως το SonarSource SonarQube είναι δωρεάν και διαχειρίσιμα, καθιστώντας τα εξαιρετικά για μικρές ομάδες ή χρήστες που θέλουν μεγάλο βαθμό ελέγχου στην πλατφόρμα DevSecOps. Ωστόσο, απαιτούν χειροκίνητη συντήρηση και ενημέρωση. Επιπλέον, λόγω της φύσης τους, οι επιλογές ανοιχτού κώδικα απαιτούν μια έμπειρη κατανόηση του τρόπου με τον οποίο μπορούν να συμβάλλουν στα τρωτά σημεία ασφαλείας. Τα εργαλεία επί πληρωμή χειρίζονται τις εργασίες διαχείρισης και εξυπηρέτησης για τη διατήρηση ενημερωμένων εργαλείων DevSecOps, επομένως μπορεί να είναι καλύτερα για μεγαλύτερες ομάδες.
Υπάρχουν πολλά δωρεάν εργαλεία ανοιχτού κώδικα DevSecOps που μπορούν να χρησιμοποιηθούν, αν και αυτά τείνουν να συνιστώνται μόνο για μικρές ομάδες ή ομάδες με ισχυρές τεχνικές γνώσεις ασφάλειας. Τα προγράμματα επί πληρωμή κυμαίνονται μεταξύ 120 και 900 $ ετησίως στη χαμηλότερη τιμή, τα οποία υποστηρίζουν από 1 έως 20 χρήστες σε αυτά τα συγκεκριμένα επίπεδα. Ομάδες μεγαλύτερου μεγέθους μπορούν να επικοινωνήσουν με τους προμηθευτές για προσφορές. Οι περισσότεροι πωλητές προσφέρουν δωρεάν δοκιμές και επιδείξεις των προϊόντων τους. (Trustradius, χ.χ.)

4.4 Συμβουλές για να αξιοποιήσουμε τα εργαλεία DevSecOps στον μέγιστο βαθμό

- Διαλέγουμε αυτό που χρειαζόμαστε.

Τόσα πολλά εργαλεία DevSecOps είναι διαθέσιμα και όλο και περισσότερα εμφανίζονται συνεχώς. Μπορεί να είναι δελεαστικό να προσπαθήσουμε να χρησιμοποιήσουμε όσο το δυνατόν περισσότερα εργαλεία για να καλύψουμε όλους τους τομείς μας, αλλά αυτό μπορεί να είναι αντιπαραγωγικό. Αντίθετα, πρέπει να αφιερώσουμε χρόνο για να αξιολογήσουμε τις ανάγκες μας και να επιλέξουμε τα εργαλεία που θα λειτουργήσουν καλύτερα για εμάς.

- Επικοινωνούμε με την ομάδα μας.

Ένα από τα πλεονεκτήματα του DevSecOps είναι ότι ενθαρρύνει την επικοινωνία και τη συνεργασία μεταξύ των μελών της ομάδας. Φροντίζουμε να επωφεληθούμε από αυτό επικοινωνώντας συχνά και ανοιχτά με τα μέλη της ομάδας μας σχετικά με την εργασία μας και πώς μπορούν να βοηθήσουν σε αυτή.

- Αυτοματοποίηση όπου είναι δυνατόν.

Ο αυτοματισμός είναι μια από τις κρίσιμες αρχές του DevSecOps. Η αυτοματοποίηση βελτιώνει την αποτελεσματικότητα και την ακρίβεια και απελευθερώνει χρόνο που μπορεί να δαπανηθεί καλύτερα σε άλλες εργασίες. Επομένως, όταν επιλέγουμε εργαλεία, αναζητάμε αυτά που προσφέρουν δυνατότητες αυτοματισμού.

- Έχουμε το νου μας στο σύνολο.

Είναι εύκολο να εμπλακούμε στις λεπτομέρειες όταν εργαζόμαστε με εργαλεία DevSecOps, αλλά είναι σημαντικό να κάνουμε πίσω περιστασιακά και να διασφαλίζουμε ότι εξακολουθούμε να δίνουμε έμφαση στους γενικούς στόχους του έργου. Τα τακτικά check-in με την ομάδα μας μπορούν να βοηθήσουν σε αυτό.

- Είμαστε προετοιμασμένοι να προσαρμόσουμε την προσέγγισή μας.

Το DevSecOps είναι ένα διαρκώς εξελισσόμενο πεδίο και αυτό που λειτουργεί σήμερα μπορεί να μην λειτουργεί αύριο. Επομένως, πρέπει να είμαστε ευέλικτοι στο σύστημά μας και να είμαστε πρόθυμοι να αλλάξουμε τα πράγματα όπως χρειάζεται. (Thinksys, 2023)

4.5 Βασικά χαρακτηριστικά που πρέπει να αναζητήσουμε σε ένα εργαλείο DevSecOps

Όταν επιλέγουμε ένα εργαλείο DevSecOps, λαμβάνουμε υπόψη το περιβάλλον, την ομάδα, και την περίπτωση χρήσης μας. Τα βασικά χαρακτηριστικά αξιολόγησης περιλαμβάνουν:

- Ενσωμάτωση με τα τρέχοντα εργαλεία ανάπτυξης, ασφάλειας και λειτουργίας για να διασφαλίσουμε μια ομαλή ροή εργασίας.
- Ευκολία στη χρήση με σαφή τεκμηρίωση, ισχυρή υποστήριξη και ενεργή κοινότητα χρηστών για να βοηθήσουμε την ομάδα μας να προσαρμοστεί γρήγορα.
- Προσαρμοστικότητα και επεκτασιμότητα, ώστε το εργαλείο να μπορεί να αναπτυχθεί με τον οργανισμό μας και να φιλοξενεί νέες δυνατότητες, ενσωματώσεις ή χρήστες, όπως απαιτείται.
- Παρακολούθηση και ειδοποιήσεις σε πραγματικό χρόνο που επιτρέπουν στην ομάδα μας να εντοπίζει και να αντιμετωπίζει άμεσα ζητήματα ασφάλειας.
- Αυτοματοποιημένες δυνατότητες δοκιμών ασφαλείας και αποκατάστασης που βοηθούν στην αποδοτικότητα των ροών εργασίας.

- ❖ Συνεχής ανατροφοδότηση και αναφορές με πρακτικές ιδέες μέσω σαφών, συνοπτικών αναφορών που υποστηρίζουν τεκμηριωμένες αποφάσεις και συνεχή βελτίωση.
- ❖ Επιβολή πολιτικής και διαχείριση συμμόρφωσης για να βοηθήσει στην εκπλήρωση των κανονιστικών απαιτήσεων.
- ❖ Έλεγχος πρόσβασης βάσει ρόλου (Role-based access control ή RBAC), διασφαλίζοντας ότι μόνο εξουσιοδοτημένο προσωπικό έχει πρόσβαση σε ευαίσθητες πληροφορίες και στις λειτουργίες του οργανισμού. (Eyal, 2023)

4.6 Παραδείγματα εργαλείων DevSecOps

Κατά την αναζήτησή μας σε επιστημονικά άρθρα και ιστοσελίδες συναντήσαμε περίπου 200 εργαλεία DevSecOps. Από αυτά αποφασίσαμε να αναλύσουμε αυτά που θεωρούνται ως "καλύτερα" στις μέρες μας με βάση την δημοτικότητα, την χρηστικότητα, τις κριτικές και άλλα στοιχεία. Αυτά τα εργαλεία DevSecOps απαριθμούνται παρακάτω. Για κάθε εργαλείο έχουμε δώσει μια σύντομη περιγραφή, τα κύρια χαρακτηριστικά, καθώς και πληροφορίες για την τιμολόγηση του. Να σημειωθεί εδώ πως σε όσα εργαλεία δεν έχουμε συμπεριλάβει την τιμολόγησή τους, είναι, διότι, είτε θα είναι δωρεάν ή όπως αλλιώς αποκαλούνται ανοιχτού κώδικα (open source), είτε ο πάροχος δεν παρέχει πληροφορίες τιμολόγησης για αυτό το προϊόν ή την υπηρεσία. Αυτή είναι συνήθης πρακτική για τους πωλητές λογισμικού και τους παρόχους υπηρεσιών και σε τέτοιες περιπτώσεις ο ενδιαφερόμενος πρέπει να επικοινωνήσει μαζί τους για να λάβει τις τρέχουσες τιμές. Σε αυτές τις περιπτώσεις λοιπόν θα έχουμε συμπεριλάβει σχόλια και κριτικές από όσους οργανισμούς έχουν ήδη αγοράσει το συγκεκριμένο εργαλείο και έχουν άποψη πάνω στο συγκεκριμένο θέμα.

1. Astra Security Pentest

Το Astra Pentest είναι μια ολοκληρωμένη πλατφόρμα που διαθέτει αυτοματοποιημένο σαρωτή ευπάθειας, δυνατότητες χειροκίνητης δοκιμής (manual pentest capabilities) και έναν πίνακα εργαλείων διαχείρισης ευπάθειας για όλες τις χρήσεις που μας βοηθά να βελτιστοποιήσουμε κάθε βήμα της διαδικασίας του pentest, από τον εντοπισμό και την ιεράρχηση των τρωτών σημείων έως τη συλλογική αποκατάσταση (collaborative remediation). Η πλατφόρμα Pentest μιμείται τη συμπεριφορά των χάκερ για να βρει κρίσιμα τρωτά σημεία στην εφαρμογή μας. Το Astra ενσωματώνεται με το GitLab, το GitHub, το Bitbucket, το Slack και το Jira για να ενισχύσει τη στοίβα τεχνολογίας μας. Το Pentest της Astra λειτουργεί σε βιομηχανίες και τεχνολογίες. Είναι ιδανικό για τη δοκιμή εφαρμογών ιστού, εφαρμογών για κινητά, API, εργαλείων SaaS, συσκευών δικτύου και της υποδομής cloud. (Capterra, χ.χ.)

- ❖ Χαρακτηριστικά

Διαχείριση (Administration):
- ➢ Αναφορές και Analytics

Ανάλυση:
- ➢ Παρακολούθηση ζητημάτων
- ➢ Ελεγχος τρωτότητας (Vulnerability Scan)

Δοκιμές:
- ➢ Χειροκίνητη δοκιμή (Manual Testing)

Επίδοση (Performance):
- ➢ Αυτοματοποιημένες σαρώσεις

(G2, χ.χ.)

- ❖ Τιμολόγηση

- ➢ Ξεκινάει από 199,00$ ανά μήνα (Capterra, χ.χ.)

2. Alerta

Ένα εργαλείο που χρησιμοποιείται για την συλλογή και την αντιγραφή ειδοποιήσεων από πολλές πηγές για μια γρήγορη "με μια ματιά" οπτικοποίηση. Συνδυάζει έναν διακομιστή JSON API για λήψη, επεξεργασία και απόδοση ειδοποιήσεων με ένα απλό, αλλά αποτελεσματικό Alerta Web UI και εργαλείο γραμμής εντολών. Το Alerta είναι ένα εργαλείο στην κατηγορία εργαλεία παρακολούθησης (Monitoring Tools) μιας στοίβας τεχνολογίας. Τέλος, το Alerta είναι ένα εργαλείο ανοιχτού κώδικα με πολύ καλές αξιολογήσεις στο GitHub.

- ❖ Χαρακτηριστικά

- ➢ Υποστηρίζει SQL
- ➢ Ευέλικτη μορφή ειδοποιήσεων
- ➢ Αποδιπλασιασμός και απλή συσχέτιση (De-duplication and simple correlation)

❖ Τιμολόγηση

Παρέχεται δωρεάν.
(Alerta, χ.χ.)

3. Acunetix

Το Acunetix είναι ένα αυτοματοποιημένο εργαλείο δοκιμής ασφάλειας εφαρμογών Ιστού και χρησιμοποιείται από πολλούς πελάτες του Fortune 500. Το Acunetix εντοπίζει και αναφέρει μια σειρά από ευπάθειες εφαρμογών ιστού. Ο ανιχνευτής Acunetix υποστηρίζει HTML5 και JavaScript και εφαρμογές μιας σελίδας (single-page applications), επιτρέποντας τον έλεγχο σύνθετων, εμπιστευτικών (authenticated) εφαρμογών. Το Acunetix μπορεί να ανιχνεύσει αυτόματα, τρωτά σημεία εκτός ζώνης (out-of-band) και είναι διαθέσιμο τόσο ως online όσο και ως on premise. Το Acunetix περιλαμβάνει επίσης ενσωματωμένες δυνατότητες διαχείρισης ευπάθειας για να επεκτείνει την ικανότητα της επιχείρησης να διαχειρίζεται, να ιεραρχεί και να ελέγχει πλήρως τις απειλές ευπάθειας, ανάλογα με το πόσο σημαντική είναι για την επιχείρηση.

❖ Χαρακτηριστικά

➢ Ανακαλύπτει και σαρώνει όλες τις εφαρμογές Ιστού.
➢ Προσδιορίζει ευπάθειες ιστού, συμπεριλαμβανομένων των SQLi και XSS.
➢ Παρέχει αναφορές συμμόρφωσης (compliance reports).

❖ Τιμολόγηση

Το Acunetix by Invicti διαθέτει 6 πακέτα τιμολόγησης, από 4.500 $ έως 26.600 $. Διατίθεται επίσης μια δωρεάν δοκιμή. Δείτε παρακάτω τα διάφορα πακέτα τιμών:

➢ Websites scanned: 5, On-premise , 4.500$

➢ Websites scanned: 6-10, On-premise, 7.200$

➢ Websites scanned: 11-20, On-premise, 10.800$

➢ Websites scanned: 21-35, On-premise, 22.540$

➢ Websites scanned: 36-50, On-premise, 26.600$

➢ Websites scanned: 11-20, On-premise, 10.800$

➢ Websites scanned: Over 50, On-premise, Επικοινωνία με τον πάροχο
(Trustradius, χ.χ.)

4. HCL AppScan

Το HCL AppScan ενισχύει την ασφάλεια εφαρμογών web και την ασφάλεια εφαρμογών για κινητά, βελτιώνει τη διαχείριση προγραμμάτων ασφάλειας εφαρμογών και ενισχύει τη συμμόρφωση με τους κανονισμούς. Με τη σάρωση των εφαρμογών ιστού και κινητών πριν από το deployment, το AppScan μας δίνει τη δυνατότητα να εντοπίσουμε ευπάθειες ασφαλείας, να δημιουργήσουμε αναφορές και να διορθώσουμε λάθη. (PeerSpot, χ.χ.)

❖ Χαρακτηριστικά

➢ Οικονομική (Cost-effective) εφαρμογή
➢ Κεντρική Διοίκηση (Central Management)
➢ Βελτιωμένη νοημοσύνη μέσω της ενσωμάτωσης με άλλα εργαλεία
➢ Διαχείριση συμμόρφωσης
➢ Μειωμένος χρόνος και προσπάθεια
➢ Αυτόματη Ανίχνευση
➢ Σάρωση εφαρμογών
➢ Προηγμένη προστασία από απειλές
➢ Προστασία Endpoint
➢ Ασφάλεια
(HCL Software, χ.χ.)

❖ Τιμολόγηση

➢ "Το AppScan είναι λίγο ακριβό. Η HCL πρέπει να εργαστεί λίγο στο μοντέλο τιμολόγησης, μειώνοντας το κόστος της άδειας που παρέχει."
➢ "Με τις δυνατότητες και την υποστήριξη που προσφέρει, η τιμολόγηση του AppScan είναι σε υψηλότερο επίπεδο."
(PeerSpot, χ.χ.)

5. Jit.io

Το Jit είναι μια πλατφόρμα ασφαλείας ως υπηρεσία (security-as-a-service) που μπορεί να βοηθήσει στην επιτάχυνση της ανάπτυξης αυτοματοποιώντας τη διαδικασία επιλογής,

υλοποίησης, διαμόρφωσης και διαχείρισης της αλυσίδας εργαλείων (toolchain) ασφαλείας εφαρμογών.

- ❖ Χαρακτηριστικά
- ➢ Κωδικοποίηση γνώσεων ασφαλείας
- ➢ Ενσωμάτωση GitHub και AWS
- ➢ Προσαρμόσιμα σχέδια ασφαλείας
- ➢ Επίπεδο orchestration για διάφορα εργαλεία ασφαλείας που καλύπτουν κώδικα, αγωγό, υποδομή και ασφάλεια εφαρμογών χρόνου εκτέλεσης

- ❖ Τιμολόγηση

18$ ανά μήνα ανά χρήστη
(Jit, χ.χ.)

6. Aqua Security

Το Aqua Security επιτρέπει στους οργανισμούς να ενοποιούν την προστασία εγγενών εφαρμογών στο cloud (cloud native application) και να εντοπίζουν, να ιεραρχούν και να μειώνουν τους κινδύνους σε κάθε φάση του κύκλου ζωής ανάπτυξης του λογισμικού τους. Το Aqua Cloud Native Security Platform είναι μια λύση Cloud Native Application Protection Platform (CNAPP) που προστατεύει τις εγγενείς εφαρμογές στο cloud από την πρώτη μέρα και τις προστατεύει σε πραγματικό χρόνο. Με το πλήρως ενσωματωμένο σύνολο δυνατοτήτων ασφάλειας και συμμόρφωσης, μπορούμε να ανακαλύψουμε, να αξιολογήσουμε, να ιεραρχήσουμε και να μειώσουμε τον κίνδυνο μέσα σε λίγα λεπτά σε όλο τον κύκλο ζωής της ανάπτυξης λογισμικού, ενώ παράλληλα αυτοματοποιούμε την πρόληψη, τον εντοπισμό και την απόκριση.

- ❖ Χαρακτηριστικά

- ➢ Προβολή και τερματισμός των απειλών σε κάθε φάση του κύκλου ζωής ανάπτυξης λογισμικού.
- ➢ Ασφάλιση όλων των συνδέσμων στην αλυσίδα εφοδιασμού λογισμικού για την διατήρηση της ακεραιότητας του κώδικα και την ελαχιστοποίηση της επιφάνειας επίθεσης.
- ➢ Απόκτηση πλήρους ορατότητας σε περιβάλλοντα με πολλά cloud μέσα σε λίγα λεπτά.
- ➢ Προσαρμογή των κινδύνων με μια ενοποιημένη προβολή σε όλη την υποδομή cloud με τον τρέχοντα φόρτο εργασίας.
- ➢ Απόδειξη και διατήρηση με σιγουριά της τήρηση των κοινών πλαισίων συμμόρφωσης.

- ➢ Προστασία των φόρτων εργασίας σε πραγματικό χρόνο με λεπτομερή χειριστήρια (controls) που θα σταματήσουν τις επιθέσεις, διατηρώντας παράλληλα την επιχείρηση σε λειτουργία.
- ➢ Ενσωμάτωση με τη στοίβα τεχνολογίας του εγγενούς cloud του χρήστη.

❖ Τιμολόγηση

- ➢ Παρέχεται δωρεάν έκδοση.
- ➢ Aqua CSP: Ετήσια συνδρομή, η οποία κοστολογείται ανά κόμβο/κεντρικό υπολογιστή για «παραδοσιακά» orchestration περιβάλλοντα (έως 100 κοντέινερ ανά κόμβο) και με βάση τον αριθμό των εκτελούμενων κοντέινερ για αναπτύξεις AWS Fargate/Microsoft ACI. Η πραγματική τιμή ποικίλλει ανάλογα με το μέγεθος της ανάπτυξης. Περιλαμβάνει απεριόριστη σάρωση εικόνας, ενσωμάτωση CI/CD και τυπική υποστήριξη. Διατίθεται προαιρετική υποστήριξη Premium.
- ➢ Aqua Pay-per-scan σε AWS: Τιμή 0,29 $ ανά σάρωση.
- ➢ Aqua Container Security στο GCP Marketplace: Τιμή μεταξύ 0,05 $ και 0,33 $ ανά κόμβο ανά ώρα, ανάλογα με το μέγεθος του κόμβου.
- ➢ Aqua MicroScanner και Kube-Bench: Δωρεάν

(Aquasec, χ.χ.)

7. Contrast Security

Η Contrast προστατεύει από μεγάλες επιθέσεις κυβερνοασφάλειας για τη βάση των πελατών της, η οποία αντιπροσωπεύει μερικές από τις μεγαλύτερες επώνυμες εταιρείες στον κόσμο, συμπεριλαμβανομένων των BMW, AXA, Zurich, NTT, Sompo Japan και The American Red Cross, καθώς και πολλών άλλων κορυφαίων παγκόσμιων επιχειρήσεων του Fortune 500. Συνεργάζεται με παγκόσμιους οργανισμούς όπως AWS, Microsoft, IBM, GuidePoint Security, Trace3, Deloitte και Carahsoft, για την απρόσκοπτη ενσωμάτωση και την επίτευξη του υψηλότερου επιπέδου ασφάλειας για τους πελάτες της.

❖ Χαρακτηριστικά

- ➢ Λειτουργικότητα - Ανάλυση Σύνθεσης Λογισμικού
- ➢ Υποστήριξη Γλωσσών
- ➢ Ενσωμάτωση (Integration)
- ➢ Αποτελεσματικότητα - Ανάλυση Σύνθεσης Λογισμικού
- ➢ Προτάσεις αποκατάστασης (Remediation Suggestions)
- ➢ Συνεχής παρακολούθηση (Continuous Monitoring)
- ➢ Λεπτομερής ανίχνευση (Thorough Detection)

(G2, χ.χ.)

❖ Τιμολόγηση

- ➢ Παρέχεται δωρεάν δοκιμή και δωρεάν έκδοση.
- ➢ "Υπάρχουν μερικοί άνθρωποι που σκέφτηκαν ότι θα μπορούσαν να πάρουν ένα φθηνότερο εργαλείο, αλλά υπάρχει μια αντιστάθμιση εκεί. Θα μπορούσαν να είχαν πάρει ένα φθηνότερο εργαλείο SAST, αλλά όσα θα είχανε εξοικονομήσει σε χρήματα θα τα ξοδεύανε σε χρόνο μάθησης."
- ➢ "Μου αρέσει το μοντέλο αδειοδότησης ανά εφαρμογή... Απλώς χορηγούμε άδεια χρήσης για την εφαρμογή και εξετάζουμε διάφορα τρωτά σημεία σε αυτήν την εφαρμογή και κάνουμε επανόρθωση (remedate) εντός της εφαρμογής. Είναι απλό."
- ➢ "Λαμβάνετε μόνο μία άδεια για μια εφαρμογή. Οι δικές μας είναι πολύ μεγάλες, με εκατομμύρια γραμμές κώδικα και μπορέσαμε να εφαρμόσουμε μία άδεια, κάτι που είναι υπέροχο. Είμαστε ευχαριστημένοι με την αδειοδότηση. Από πλευράς τιμών , είναι industry-standard, κάτι που είναι εντάξει."

(PeerSpot, χ.χ.)

8. Checkmarx AST platform

Η Checkmarx ωθεί συνεχώς τα όρια των δοκιμών Ασφάλειας Εφαρμογών (AppSec) για να κάνει την ασφάλεια απρόσκοπτη και απλή για τους προγραμματιστές, ενώ παρέχει στους CISO (chief information security officer) την εμπιστοσύνη και τον έλεγχο που χρειάζονται. Ως ηγέτης δοκιμών AppSec, η Checkmarx παρέχει την πιο ολοκληρωμένη πλατφόρμα AST του κλάδου, το Checkmarx One, που παρέχει στους προγραμματιστές και τις ομάδες ασφαλείας απαράμιλλη ακρίβεια, κάλυψη, ορατότητα και καθοδήγηση για τη μείωση του κινδύνου σε όλα τα στοιχεία του σύγχρονου λογισμικού, συμπεριλαμβανομένου του ιδιόκτητου κώδικα, του ανοιχτού κώδικα, API και IaC. Περισσότεροι από 1.800 πελάτες, συμπεριλαμβανομένων των μισών από το Fortune 500, εμπιστεύονται την τεχνολογία ασφαλείας Checkmarx, που είναι ειδικοί στην έρευνα και τις παγκόσμιες υπηρεσίες για την ασφαλή βελτιστοποίηση της ανάπτυξης σε ταχύτητα και κλίμακα.

❖ Χαρακτηριστικά

Διαχείριση (Administration)

- ➢ API / Ενσωματώσεις
- ➢ Επεκτασιμότητα

Ανάλυση

- ➢ Αναφορές και Analytics
- ➢ Παρακολούθηση ζητημάτων
- ➢ Ελεγχος τρωτότητας

- ➢ Ανάλυση Κώδικα

Δοκιμές (Testing)
- ➢ Δοκιμή Συμμόρφωσης (Compliance Testing)
- ➢ Ρυθμός ανίχνευσης
- ➢ False Positives

Λειτουργικότητα - Ανάλυση Σύνθεσης Λογισμικού
- ➢ Υποστήριξη Γλωσσών
- ➢ Ενσωμάτωση
- ➢ Διαφάνεια (Transparency)

Αποτελεσματικότητα - Ανάλυση Σύνθεσης Λογισμικού
- ➢ Προτάσεις αποκατάστασης
- ➢ Συνεχής Παρακολούθηση
- ➢ Πλήρης Ανίχνευση

(G2, χ.χ.)

- ❖ Τιμολόγηση

- ➢ Παρέχεται δωρεάν δοκιμή.
- ➢ "Η τιμολόγηση είναι ανταγωνιστική και παρέχει χαμηλότερο συνολικό κόστος ιδιοκτησίας για την επίτευξη της ασφάλειας των εφαρμογών".
- ➢ "Πιστεύω ότι η τιμολόγηση είναι καλύτερη σε σύγκριση με άλλα εμπορικά εργαλεία."
- ➢ "Είναι η σωστή τιμή για ποιοτική παράδοση."

(PeerSpot, χ.χ.)

9. Checkmarx CxSAST

Το Checkmarx CxSAST είναι μέρος του Checkmarx Software Exposure Platform που αντιμετωπίζει τον κίνδυνο ασφάλειας λογισμικού σε ολόκληρο το SDLC. Το CxSAST είναι μια ευέλικτη και ακριβής λύση στατικής ανάλυσης που χρησιμοποιείται για τον εντοπισμό εκατοντάδων τρωτών σημείων ασφαλείας τόσο σε στοιχεία προσαρμοσμένου (custom) κώδικα όσο και σε στοιχεία ανοιχτού κώδικα. Χρησιμοποιείται από ομάδες ανάπτυξης, DevOps και ασφάλειας για τη σάρωση του πηγαίου κώδικα στην αρχή του SDLC σε περισσότερες από 25 γλώσσες κωδικοποίησης και scripting.

- ❖ Χαρακτηριστικά

- ➢ Γνωρίζει άπταιστα περισσότερες από 20 κύριες γλώσσες κωδικοποίησης και scripting.

- ➢ Προσδιορισμός εκατοντάδων γνωστών τρωτών σημείων κώδικα.
- ➢ Εξασφαλίζει την κάλυψη των προτύπων ασφαλείας και των κανονισμών συμμόρφωσης του κλάδου.
- ➢ Διορθώνει τα τρωτά σημεία στο καλύτερο σημείο του κώδικα για να διορθώσει πολλά προβλήματα σε ένα μόνο σημείο.
- ➢ Εύκολο στη χρήση για κάθε προγραμματιστή.
- ➢ Χωρίς περίπλοκες εντολές ή οδηγούς, χωρίς configuration και χωρίς απόκλιση στη μάθηση κατά την εναλλαγή γλωσσών.
- ➢ Δυνατότητα σταδιακής σάρωσης που επιτρέπει τη σάρωση μόνο νέου ή τροποποιημένου κώδικα.

(Checkmarx, χ.χ.)

- ❖ Τιμολόγηση

- ➢ Παρακάτω είναι το συνολικό κόστος για τις διαφορετικές διάρκειες συνδρομής.
- ➢ Ενδέχεται να ισχύουν πρόσθετοι φόροι ή τέλη.
- ➢ Παρέχεται δωρεάν δοκιμή.

Πίνακας 4.6.1: *Τιμολόγηση Checkmarx CxSAST.*

Χρήστες	Περιγραφή	12 μήνες	36 μήνες
πακέτο 12 χρηστών	12 χρήστες: SCA, SAST (10 πρότζεκτ, 1 ταυτόχρονο scan), Hosting	$64,041	$172,910
πακέτο 24 χρηστών	24 χρήστες: SCA, SAST (10 πρότζεκτ, 1 ταυτόχρονο scan), Hosting	$86,761	$234,254
πακέτο 50 χρηστών	50 χρήστες: SCA, SAST (10 πρότζεκτ, 1 ταυτόχρονο scan), Hosting	$117,321	$316,766
Checkmarx1 Professional	Checkmarx One Professional συνδρομή- ανά άδεια ανά χρόνο	$2,965	$7,740
Checkmarx1 API Security	Checkmarx One API Security Add On συνδρομή- ανά άδεια ανά χρόνο	$621	$1,620
Checkmarx1 DAST AddOn	Checkmarx One DAST AddOn συνδρομή- ανά άδεια ανά χρόνο	$483	$1,260
Checkmarx1ConcurrentScan	Checkmarx One Concurrent Scan συνδρομή- ανά άδεια ανά χρόνο	$9,500	$28,500

CxSCS ThreatAPIMalicious	Cx-SCS Threat API Malicious (ανά πακέτο) - ανά 2 άδειες ανά χρόνο	$101,800	$305,400
Checkmarx1 Prem Serv Pkg	Checkmarx One Premium Service Package - Variable @ 20% of SaaS Fee	$1	$1
Checkmarx1 Prof Serv Day	Checkmarx One PS days (Τιμή ανά ημέρα)	$2,200	$2,200

(aws,χ.χ.)

10. CyberArk

Το CyberArk είναι μια σουίτα ασφαλείας (security suite) που βοηθά στην προστασία των συσκευών, των κωδικών πρόσβασης και των προνομιακών λογαριασμών από τρίτους. Αποτελείται από διάφορες λύσεις ασφάλειας και μία από αυτές, η Προνομιακή Διαχείριση και Έλεγχος Κωδικών πρόσβασης (Privileged Password Management and Control), βοηθά τους οργανισμούς να πληρούν αυστηρά πρότυπα συμμόρφωσης και πληροφορικής και να διαχειριστούν προνομιούχους κωδικούς πρόσβασης. Ομοίως, αυτό το λογισμικό διασφαλίζει ότι ενημερωνόμαστε πάντα με τις πολιτικές και τα πρότυπα συμμόρφωσης και ελέγχου, ώστε να αποφεύγουμε τους κινδύνους απειλών και κυρώσεων στον κυβερνοχώρο. Το CyberArk ενισχύει τις διαδικασίες στην παρακολούθηση, την ασφάλεια και τη διαχείριση προνομιακών λογαριασμών.

❖ Χαρακτηριστικά

- ➢ Προηγμένη προστασία από απειλές
- ➢ Ασφάλεια Συστημάτων Βιομηχανικού Ελέγχου
- ➢ Ασφάλεια των Windows
- ➢ Έλεγχος πληροφοριακών συστημάτων και αναφορές
- ➢ DevOps Security
- ➢ Ασφάλεια Cloud & Virtualization
- ➢ Ασφάλεια Unix/Linux
- ➢ Εμπιστευτική ασφάλεια αρχείων
- ➢ Προστασία από εσωτερικές απειλές
- ➢ Ασφάλεια απομακρυσμένης πρόσβασης προμηθευτή
- ➢ Πρότυπο ασφάλειας δεδομένων βιομηχανίας καρτών πληρωμής (PCI)

(CompareCamp,χ.χ.)

❖ Τιμολόγηση

Το CyberArk έχει 5 πακέτα τιμολόγησης, από $2 έως $5. Διατίθεται επίσης μια δωρεάν δοκιμή του CyberArk Identity. Ας δούμε παρακάτω τις διάφορες εκδόσεις τιμολόγησης.

Πίνακας 4.6.2: *Τιμολόγηση CyberArk.*

CyberArk Adaptive MFA	Ξεκινάει στα $3.00, 1 χρήστης τον μήνα
CyberArk Single Sign-On	Ξεκινάει στα $2.00, 1 χρήστης τον μήνα
CyberArk Workforce Password Management	Ξεκινάει στα $5.00, 1 χρήστης τον μήνα
CyberArk Identity Lifecycle Management	Ξεκινάει στα $4.00, 1 χρήστης τον μήνα

(G2,χ.χ.)

11. Codacy

Το εργαλείο ανάλυσης στατικού κώδικα της Codacy επιτρέπει στους προγραμματιστές να εντοπίζουν αυτόματα και να αντιμετωπίζουν προβλήματα ασφάλειας, διπλότυπα, πολυπλοκότητα, style violations και drops in coverage σε κάθε αίτημα pull και request, απευθείας από τη ροή εργασίας τους στο Git. Ενσωματώνεται στο prem και στο cloud με το GitHub, το BitBucket και το Gitlab και αναλύει 30+ διαφορετικές γλώσσες προγραμματισμού όπως Python, Java, JS, Ruby, Go, PHP, C# και Scala.

❖ Χαρακτηριστικά

➢ Απεριόριστα αποθετήρια ανοιχτού κώδικα
➢ Απεριόριστοι χρήστες
➢ Ενσωμάτωση Github και Bitbucket
➢ Αυτόματα σχόλια στο αίτημα pull
➢ Παρακολούθηση κάλυψης κώδικα (Code coverage tracking)
➢ Ανάλυση κωδικών ασφαλείας
➢ Ενσωμάτωση Slack, Hipchat, JIRA και YouTrack
➢ Συγχρονίζεται με αρχεία ρύθμισης παραμέτρων linter (linter configuration files)
➢ Οργάνωση και διαχείριση ομάδας
➢ Αυτόματη επανεξέταση αιτήματος commit και pull
➢ Self-hosted servers, πίσω από το τείχος προστασίας
➢ Παρέχεται GitHub Enterprise, Bitbucket Server (πρώην Stash) και GitLab

- ➢ Αποκλειστική υποστήριξη και SLA
- ➢ Ενσωματώσεις Jenkins

(Capterra, χ.χ.)

- ❖ Τιμολόγηση

Το Codacy έχει 4 πακέτα τιμολόγησης, από 0 $ έως 40 $. Διατίθεται επίσης δωρεάν δοκιμή του Codacy. Ας δούμε παρακάτω τις διάφορες εκδόσεις τιμών.

Πίνακας 4.6.3: Τιμολόγηση Codacy.

Open Source	Startup	Pro	Enterprise
$0.00	$0.00	$15.00	
Cloud	Cloud	Cloud (χρήστης/μήνα)	40$

(TrustRadius, χ.χ.)

12. Calico Open Source

Το Project Calico είναι ένα πρότζεκτ ανοιχτού κώδικα με ενεργή κοινότητα ανάπτυξης και χρηστών. Το Calico Open Source γεννήθηκε από αυτό το πρότζεκτ και έγινε η πιο ευρέως διαδεδομένη λύση για δικτύωση και ασφάλεια κοντέινερ, τροφοδοτώντας περισσότερους από 2 εκατομμύρια κόμβους καθημερινά σε 166 χώρες. Το Calico Open Source είναι μια λύση δικτύωσης και ασφάλειας για κοντέινερ, εικονικές μηχανές και φόρτους εργασίας που βασίζονται σε εγγενείς κεντρικούς υπολογιστές. Το Calico υποστηρίζει ένα ευρύ φάσμα πλατφορμών, συμπεριλαμβανομένων των Kubernetes, OpenShift, Docker EE, OpenStack και υπηρεσιών γυμνού μετάλλου (bare metal services). Είτε επιλέξουμε να χρησιμοποιήσουμε το επίπεδο δεδομένων eBPF της Calico, την τυπική διοχέτευση δικτύωσης του Linux, είτε το επίπεδο δεδομένων των Windows, το Calico προσφέρει απίστευτα γρήγορη απόδοση με πραγματική επεκτασιμότητα εγγενή στο cloud (cloud-native). Το Calico παρέχει στους προγραμματιστές και στους cluster operators μια συνεπή εμπειρία και ένα σύνολο δυνατοτήτων, είτε εκτελούνται σε δημόσιο σύννεφο είτε εντός εγκατάστασης (on-premises), είτε σε έναν μόνο κόμβο ή σε ένα σύμπλεγμα πολλών χιλιάδων κόμβων.

- ❖ Χαρακτηριστικά

Επιλογή επιπέδου δεδομένων (Data plane choice)

- ➢ eBPF, τυπικά επίπεδα δεδομένων Linux και Windows

Διαλειτουργικότητα (Interoperability)

- ➢ Εργασία με φόρτους εργασίας που δεν ανήκουν στο Kubernetes

Βελτιστοποιημένη απόδοση

- ➢ Σχεδιασμένο για να πηγαίνει πιο γρήγορα με χαμηλότερη κατανάλωση CPU, για την καλύτερη δυνατή απόδοση από τις επενδύσεις σε clusters

Λειτουργία σε κλίμακα (Operate at scale)

- ➢ Κλείδωμα της επεκτασιμότητα κλίμακας με τα Kubernetes clusters, χωρίς απώλεια της απόδοσης

Λεπτομερείς έλεγχοι πρόσβασης (access controls)

- ➢ Πλούσιο μοντέλο πολιτικής δικτύου και ασφάλειας για ασφαλή επικοινωνία και κρυπτογράφηση WireGuard

Πλήρης υποστήριξη πολιτικής δικτύου Kubernetes

- ➢ Χρήση της αρχικής αναφοράς που εκτελείται με την πολιτική δικτύου Kubernetes

Ενεργή κοινότητα

- ➢ Αξιοποίηση της καινοτομίας που παρέχεται από 200+ συνεισφέροντες από ένα ευρύ φάσμα εταιρειών

- ❖ Τιμολόγηση

Παρέχεται δωρεάν.
(G2,χ.χ.)

13. DoControl

Το DoControl είναι ένα εργαλείο ασφαλείας προσανατολισμένο στο SaaS που αντιμετωπίζει τα δικαιώματα πρόσβασης των χρηστών και το προφίλ τους και διαχειρίζεται την έκθεση δεδομένων. Χρησιμοποιώντας το DoControl, αποκτάμε ορατότητα όλων των περιουσιακών στοιχείων, των χρηστών και των εξωτερικών συνεργατών. Αυτό το εργαλείο αυτοματοποιεί τους ελέγχους πρόσβασης δεδομένων, ενώ παράλληλα επιτρέπει την ασφάλεια χωρίς να διακυβεύεται η αποτελεσματικότητα.

- ❖ Χαρακτηριστικά

Προληπτικοί έλεγχοι πρόσβασης δεδομένων, ανακάλυψη πλέγματος υπηρεσιών (service mesh), ανίχνευση εσφαλμένης διαμόρφωσης υπηρεσίας (misconfiguration) SaaS και διαχείριση σκιωδών εφαρμογών (shadow application governance). (Eyal, 2023)

❖ Τιμολόγηση

Παρακάτω είναι το συνολικό κόστος για τις διαφορετικές διάρκειες συνδρομής.
Ενδέχεται να ισχύουν πρόσθετοι φόροι ή τέλη.

Πίνακας 4.6.4: *Τιμολόγηση DoControl.*

Χρήστες	Περιγραφή	12 μήνες	24 μήνες	36 μήνες
Core Platform: Μέχρι 500	Απεριόριστες ενσωματώσεις SaaS, SaaS χρήστης, ροές εργασίας, και enforcement	$50,000	$90,000	$127,500
Core Platform: 501-2,500	Απεριόριστες ενσωματώσεις SaaS, SaaS χρήστης, ροές εργασίας, και enforcement	$150,000	$270,000	$382,500
Core Platform: 2,501-10K	Απεριόριστες ενσωματώσεις SaaS, SaaS χρήστης, ροές εργασίας, και enforcement	$350,000	$630,000	$847,500
Core Platform: 10K+	Απεριόριστες ενσωματώσεις SaaS, SaaS χρήστης, ροές εργασίας, και enforcement	$500,000	$900,000	$1,275,000

(aws, χ.χ.)

14. Fortify Static Code Analyzer

Το Fortify Static Code Analyzer (SCA) χρησιμοποιεί πολλούς αλγόριθμους και μια δυναμική βάση πληροφοριών ασφαλών πρωτοκόλλων κωδικοποίησης για να διερευνήσει τον πηγαίο κώδικα μιας εφαρμογής για τυχόν κίνδυνο κακόβουλων ή επικίνδυνων απειλών. Επιπλέον, θα δώσει προτεραιότητα στις πιο κρίσιμες ανησυχίες και θα δώσει οδηγίες για το πώς οι χρήστες μπορούν να επιδιορθώσουν αυτές τις ανησυχίες. Αυτή η λύση ερευνά κάθε πιθανή διαδρομή που μπορεί να ταξιδέψει η ροή εργασίας και τα δεδομένα για να ανακαλύψει και να επιδιορθώσει όλες τις πιθανές ευπάθειες. Το Fortify SCA επιτρέπει στους χρήστες να δημιουργούν ασφαλές λογισμικό γρήγορα. Οι χρήστες μπορούν να ανακαλύψουν πιθανά κενά ασφαλείας πιο γρήγορα, με ακριβή αποτελέσματα και να τα επιδιορθώσουν αμέσως.

❖ Χαρακτηριστικά

Ανάλυση
- ➢ Αναφορές και Analytics
- ➢ Issue Tracking
- ➢ Static Code Analysis

Δοκιμές

- ➢ False positives

- ❖ Τιμολόγηση

"Έχει μερικά μοντέλα αδειών. Αυτό που χρησιμοποιούμε πιο συχνά ονομάζεται ευέλικτη ανάπτυξη. Το χρησιμοποιούμε επειδή είναι ευέλικτο και βασίζεται στον αριθμό των προγραμματιστών που συνεισφέρουν κώδικα στον οργανισμό. Περιλαμβάνει σχεδόν τα πάντα για μία τιμή προγραμματιστή. Μας δίνει πρόσβαση στο κέντρο ασφάλειας λογισμικού, που είναι η πλατφόρμα διαχείρισης ευπάθειας».
"Η τιμή του Fortify Static Code Analyzer θα μπορούσε να μειωθεί."
"Η αδειοδότηση είναι ακριβή και κυμαίνεται στα 50 χιλιάδες."
(PeerSpot, χ.χ.)

15. ELK or Elastic Stack

Το Elastic Stack είναι μια ομάδα προϊόντων ανοιχτού κώδικα από την Elastic που έχει σχεδιαστεί για να βοηθά τους χρήστες να λαμβάνουν δεδομένα από οποιονδήποτε τύπο πηγής και σε οποιαδήποτε μορφή και να αναζητούν, να αναλύουν και να οπτικοποιούν αυτά τα δεδομένα σε πραγματικό χρόνο. Η ομάδα προϊόντων ήταν παλαιότερα γνωστή ως ELK Stack για τα βασικά προϊόντα της ομάδας, Elasticsearch, Logstash και Kibana, αλλά έχει μετονομαστεί ως Elastic Stack. Ένα τέταρτο προϊόν, το Beats, προστέθηκε στη συνέχεια στη στοίβα. Το Elastic Stack μπορεί να αναπτυχθεί σε εγκαταστάσεις ή να διατεθεί ως λογισμικό ως υπηρεσία (SaaS). Το Elasticsearch υποστηρίζει τις υπηρεσίες Web Amazon (AWS), την πλατφόρμα Google Cloud και το Microsoft Azure.

- ❖ Χαρακτηριστικά

Αναφορές

- ➢ Διασύνδεση αναφορών (Reports Interface)
- ➢ Γραφήματα και διαγράμματα
- ➢ Κάρτες βαθμολογίας (Score Cards)
- ➢ Ταμπλό (Dashboards)
- ➢ Βήματα που οδηγούν στην απάντηση (Steps to Answer)

Ενημερώσεις δεδομένων

- ➢ Ιστορικά στιγμιότυπα (Historical Snapshots)
- ➢ Ενημέρωση σε πραγματικό χρόνο
- ➢ Αναφορές ηλεκτρονικού ταχυδρομείου

Οπτικοποίηση (Visualization)

- ➢ Γραφήματα και διαγράμματα
- ➢ Ταμπλό (Dashboards)
- ➢ Formats

Συνεργασία

- ➢ Συνεργατική επεξεργασία (Co-Editing)

❖ Τιμολόγηση

- ➢ Standard: 95$ τον μήνα (με βάση τη διαμόρφωση παραγωγής cloud, αποθήκευση 120GB / 2 ζώνες. Instance type usage-based pricing)
- ➢ Gold: 109$ τον μήνα (με βάση τη διαμόρφωση παραγωγής cloud, αποθήκευση 120GB / 2 ζώνες. Instance type usage-based pricing)
- ➢ Platinum: 125$ τον μήνα (με βάση τη διαμόρφωση παραγωγής cloud, αποθήκευση 120GB / 2 ζώνες. Instance type usage-based pricing)
- ➢ Enterprise: 175$ τον μήνα (με βάση τη διαμόρφωση παραγωγής cloud, αποθήκευση 120GB / 2 ζώνες. Instance type usage-based pricing)
- ➢ Παρέχεται δωρεάν δοκιμή.

(Elastic, χ.χ.)

16. Fortify WebInspect

Το Fortify WebInspect είναι μια αυτοματοποιημένη λύση DAST που βοηθά τους επαγγελματίες ασφαλείας και τους ελεγκτές QA να αποκαλύψουν ευπάθειες ασφαλείας και προβλήματα configuration παρέχοντας πλήρη ανίχνευση. Αυτό επιτυγχάνεται με τη μίμηση πραγματικών εξωτερικών επιθέσεων ασφαλείας σε μια ζωντανή εφαρμογή, προκειμένου να εντοπιστούν και να ιεραρχηθούν οι ανησυχίες για τη μελέτη βασικής αιτίας. Το Fortify WebInspect παρέχει διάφορα REST APIs για ευκολότερη ενσωμάτωση, καθώς και τη δυνατότητα συντήρησης μέσω ενός διαισθητικού ή πλήρως αυτοματοποιημένου UI.

❖ Χαρακτηριστικά

- ➢ Προσδιορισμός των τρωτών σημείων σε εφαρμογές Ιστού και API ενώ εκτελούνται στην παραγωγή.
- ➢ Υποστήριξη για τις πιο πρόσφατες τεχνολογίες Ιστού και προδιαμορφωμένες πολιτικές για σημαντικούς κανονισμούς συμμόρφωσης.
- ➢ Παρακολούθηση των τάσεων και χρήση δυναμικών αναλύσεων για την ανάληψη δράσης για τρωτά σημεία.

❖ Τιμολόγηση

➢ «Είναι μια δίκαιη τιμή για τη λύση».
➢ "Η τιμολόγηση για αυτή τη λύση είναι καλή."
➢ «Η τιμολόγηση δεν είναι σαφής και ενώ δεν είναι υψηλή, είναι δύσκολο να γίνει κατανοητή».
➢ Παρέχεται δωρεάν δοκιμή.

(PeerSpot, χ.χ.)

17. Skyhawk Security

Συσχετίζοντας το Cloud Security Pose Management (CSPM) με το Cloud Detection & Response (CDR), η πλατφόρμα Synthesis της Skyhawk Security βοηθά στην αποκάλυψη παραβιάσεων σε ολόκληρη την υποδομή cloud σε πραγματικό χρόνο. Με τα Realerts τους, οι ομάδες λύσεων μπορούν να δώσουν προτεραιότητα στον χρόνο που αφιερώνεται σε πραγματικές απειλές που προκαλούν αναστάτωση στον οργανισμό. Το Skyhawk Security επιλύει ορισμένα σημαντικά θέματα, όπως το alert fatigue και η έλλειψη ορατότητας (lack of visibility).

❖ Χαρακτηριστικά

Στατικές και δυναμικές δραστηριότητες
Runtime hub
Ανίχνευση απειλών

❖ Τιμολόγηση

Παρακάτω είναι το συνολικό κόστος για τις διαφορετικές διάρκειες συνδρομής.
Ενδέχεται να ισχύουν πρόσθετοι φόροι ή τέλη.

Πίνακας 4.6.5: *Τιμολόγηση Skyhawk Security.*

Units	Description	12 MONTHS	24 MONTHS	36 MONTHS
Πακέτο 1	Μέχρι 50 Cloud Assets	$13,500	$26,500	$40,000
Πακέτο 2	51 to 100 Cloud Assets	$24,000	$48,000	$72,000

Πακέτο 3	101 to 200 Cloud Assets	$44,000	$88,000	$132,000
Πακέτο 4	201 to 500 Cloud Assets	$106,500	$213,000	$319,000
Πακέτο 5	501 to 1000 Cloud Assets	$199,000	$399,000	$599,000
Πακέτο 6	1001 to 2500 Cloud Assets	$469,000	$938,000	$1,405,000

(aws, χ.χ.)

18. Grafana

Το Grafana είναι ένα εργαλείο οπτικοποίησης δεδομένων που αναπτύχθηκε από την Grafana Labs στη Νέα Υόρκη. Είναι διαθέσιμο δωρεάν και παρέχει και δύο εκδόσεις για επιχειρήσεις με βελτιωμένες δυνατότητες. Το Grafana διαθέτει μοντέλο πηγής δεδομένων με δυνατότητα σύνδεσης (pluggable) και συνοδεύεται από υποστήριξη για δημοφιλείς βάσεις δεδομένων χρονοσειρών (time series databases) όπως το Graphite. Διαθέτει επίσης ενσωματωμένη υποστήριξη για προμηθευτές παρακολούθησης cloud όπως το Amazon Cloudwatch, το Microsoft Azure και βάσεις δεδομένων SQL, όπως η MySQL. Τέλος , το Grafana μπορεί να συνδυάσει δεδομένα από πολλά μέρη σε έναν ενιαίο πίνακα ελέγχου.

❖ Χαρακτηριστικά

➢ Εκμετάλλευση πόρων
➢ Παρακολούθηση σε πραγματικό χρόνο
➢ Βασική γραμμή απόδοσης (Performance baseline)
➢ Παρακολούθηση API
➢ Αναζήτηση
➢ Αναφορές
➢ Οπτικοποίηση (Visualization)
➢ Παρακολούθηση των τάσεων
➢ Διαχείριση ειδοποιήσεων
➢ Ειδοποιήσεις πολλαπλών λειτουργιών
➢ Ειδοποιήσεις βελτιστοποίησης
➢ Ειδοποιήσεις συμβάντων
➢ Αυτοματοποίηση ανάλυσης (Resolution automation)
➢ Αυτοματοποίηση
➢ Επίλυση ζητημάτων

- ➢ Αναγνώριση αιτίας (Root cause identification)
- ➢ Προληπτική αναγνώριση (Proactive identification)

- ❖ Τιμολόγηση

- ➢ Cloud Free: Δωρεάν

Ένα πραγματικά χρήσιμο δωρεάν εργαλείο. Απόκτηση πρόσβασης στις λειτουργίες του Cloud, αλλά με περιορισμένη χρήση. Δεν απαιτείται πιστωτική κάρτα.

- ➢ Cloud Pro: 29$ τον μήνα

Για τις περισσότερες εταιρείες που έχουν περισσότερους χρήστες και δεδομένα.

- ➢ Cloud Advanced: 299$ τον μήνα

Όταν χρειάζεστε πολλά Enterprise Plugins και άλλες λειτουργίες σε επίπεδο επιχείρησης.

- ➢ Παρέχεται δωρεάν δοκιμή και δωρεάν έκδοση.

(Grafana, χ.χ.)

19. GitLab

Η πλατφόρμα GitLab DevSecOps επιτρέπει την καινοτομία λογισμικού, ενδυναμώνοντας τις ομάδες ανάπτυξης, ασφάλειας και λειτουργίας (operations) να δημιουργήσουν καλύτερο λογισμικό, πιο γρήγορα. Με το GitLab, οι ομάδες μπορούν να δημιουργούν, να παραδίδουν και να διαχειρίζονται κώδικα γρήγορα αντί να διαχειρίζονται ανόμοια εργαλεία και σενάρια. Το GitLab βοηθά τις ομάδες σε ολόκληρο τον κύκλο ζωής του DevSecOps, από την ανάπτυξη, την ασφάλεια και την ανάπτυξη λογισμικού.

- ❖ Χαρακτηριστικά:

Λειτουργικότητα

- ➢ Deployment-Ready Staging
- ➢ Επεκτασιμότητα
- ➢ Ενσωματώσεις
- ➢ Προσαρμογή δοκιμής (Test Customization)

Διαχείριση (Management)

- ➢ Αυτοματοποίηση
- ➢ Διαδικασίες και ροή εργασίας (Processes and Workflow)
- ➢ Αναφορές
- ➢ Αναφορά σφαλμάτων

- ➢ Αναφορές και σχόλια ομάδας

Παρακολούθηση σφαλμάτων
- ➢ Ιστορικό σφαλμάτων
- ➢ Διατήρηση δεδομένων

- ❖ Τιμολόγηση

Το GitLab διαθέτει 3 πακέτα τιμολόγησης, από $0 έως $99. Διατίθεται επίσης μια δωρεάν δοκιμή του GitLab.

Πίνακας 4.6.6: Τιμολόγηση GitLab.

GitLab Essential	GitLab Premium	GitLab Ultimate
$0	$29	$99
Cloud ανά χρήστη/μήνα	Cloud ανά χρήστη/μήνα	Cloud ανά χρήστη/μήνα

(GitLab, χ.χ.)

20. HashiCorp Vault

Το HashiCorp Vault ελέγχει αυστηρά την πρόσβαση σε κλειδιά κρυπτογράφησης μέσω του ελέγχου ταυτότητας έναντι αξιόπιστων πηγών ταυτότητας όπως οι πλατφόρμες Active Directory, LDAP, Kubernetes, CloudFoundry και cloud. Το Vault επιτρέπει την ακριβή εξουσιοδότηση της οποίας οι χρήστες και οι εφαρμογές έχουν πρόσβαση σε μυστικά και κλειδιά.
Μερικές από τις κύριες περιπτώσεις χρήσης του Vault περιλαμβάνουν:
Διαχείριση μυστικών
Διαμεσολάβηση ταυτότητας (Identity Brokering)
Κρυπτογράφηση δεδομένων

- ❖ Χαρακτηριστικά

- ➢ Διαχείριση Μυστικών
- ➢ Εναλλαγή διαπιστευτηρίων βάσης δεδομένων (Database Credential Rotation)
- ➢ Προηγμένη προστασία δεδομένων

- ❖ Τιμολόγηση

- ➢ Cloud: Cloud HCP-Vault: 0,03$/ώρα
- ➢ Cloud: Δωρεάν (ανοιχτού κώδικα)

➢ Cloud: Enterprise Price: Επικοινωνία με την ομάδα πωλήσεων
(TrustRadius, χ.χ.)

21. Invicti Security

Το Invicti, πρώην Netsparker, είναι ένα αυτοματοποιημένο εργαλείο δοκιμών ασφάλειας δικτύου που δίνει τη δυνατότητα στους εταιρικούς οργανισμούς να ασφαλίζουν χιλιάδες ιστότοπους και να μειώνουν εντυπωσιακά τον κίνδυνο επίθεσης. Ενισχύοντας τις ομάδες ασφαλείας με τις πιο μοναδικές δυνατότητες σάρωσης DAST και IAST στην αγορά, το Invicti επιτρέπει σε οργανισμούς με περίπλοκα περιβάλλοντα να αυτοματοποιούν την ασφάλειά τους στον ιστό με σιγουριά.

❖ Χαρακτηριστικά

➢ Σάρωση ευπάθειας
➢ Αναφορές & Αναλύσεις
➢ Παρακολούθηση ζητημάτων
➢ Αυτοματοποιημένες σαρώσεις
➢ Ρυθμός ανίχνευσης (Detection Rate)
➢ Ψευδής θετική ανίχνευση (False Positive Detection)
➢ Proof-Based Scanning
➢ Δοκιμή Συμμόρφωσης (Compliance Testing)
➢ Περιμετρική σάρωση (Perimeter Scanning)

❖ Τιμολόγηση

➢ «Δεν είχαμε ποτέ προβλήματα με την αδειοδότηση, η τιμή ήταν εντός των ορίων που είχαμε ορίσει».
➢ «Είναι ανταγωνιστική στην αγορά ασφάλειας».

➢ Παρέχεται δωρεάν δοκιμή.
(PeerSpot, χ.χ.)

22. IriusRisk

Το IriusRisk κάνει το DevSecOps πραγματικότητα με την πρωτοποριακή πλατφόρμα μοντελοποίησης απειλών και διαχείρισης κινδύνου του SDLC. Το IriusRisk είναι ένα ισχυρό εργαλείο για τη διασφάλιση της ασφάλειας που εντάσσεται στη φάση του σχεδιασμού και ακολουθεί στην παραγωγή. Λειτουργεί ως κεντρικό σημείο orchestration για τις ομάδες, ώστε να μοντελοποιήσουν απειλές και να διαχειριστούν τον κίνδυνο με ενημερώσεις σε

πραγματικό χρόνο σε όλο το SDLC. Σχεδιασμένο για ενοποίηση, απλότητα, κλίμακα και ταχύτητα, το IriusRisk συνδέει την ασφάλεια, τις λειτουργίες (operations) και την ανάπτυξη. Το IriusRisk είναι ένας αξιόπιστος συνεργάτης μερικών από τα μεγαλύτερα χρηματοπιστωτικά ιδρύματα στον κόσμο και είναι γρήγοροι στην προσαρμογή, ευέλικτοι και ανταποκρίνονται στις σύγχρονες αλλαγές.

- ❖ Χαρακτηριστικά

- ➢ IDE για αυτοματοποιημένη παραγωγή δοκιμών (IDE for automated test generation)
- ➢ Πολλές επιλογές εξαγωγής/εισαγωγής (export/import)
- ➢ Πρόσβαση σε API
- ➢ Συνδρομή AWS
- ➢ Διαχείριση ροής εργασιών

(G2, χ.χ.)

- ❖ Τιμολόγηση

- ➢ Ενδέχεται να ισχύουν πρόσθετοι φόροι ή τέλη.
- ➢ Παρέχεται δωρεάν έκδοση και δωρεάν δοκιμή.

Πίνακας 4.6.7: *Τιμολόγηση IriusRisk.*

Είδος	**Περιγραφή**	**12 μήνες**	**24 μήνες**	**36 μήνες**
Platform	Περιλαμβάνει 5 Threat models	$45,000	$90,000	$135,000

(aws, χ.χ.)

23. Kiuwan

Το Kiuwan Code Security, από την εταιρεία Idera Kiuvan, σαρώνει αυτόματα τον κώδικα για να εντοπίσει και να διορθώσει τις ευπάθειες. Συμμορφώνεται με τα πιο αυστηρά πρότυπα ασφαλείας, όπως OWASP και CWE, καλύπτει όλες τις σημαντικές γλώσσες και ενσωματώνεται με κορυφαία εργαλεία DevOps.

- ❖ Χαρακτηριστικά

- ➢ Αυτόματη ανίχνευση κακόβουλων επιθέσεων και τρωτών σημείων.

- ➢ Παρακολούθηση της ασφάλειας κώδικα σε πραγματικό χρόνο.
- ➢ Δημιουργία λεπτομερών αναφορών σχετικά με τη ασφάλεια.

❖ Τιμολόγηση

- ➢ Code Security (SAST) Scans: από $599
- ➢ Συνεχής (Continuous): κατόπιν αιτήματος
- ➢ Insights (SCA) Scans: από $1199
- ➢ Συνεχής (Continuous): κατόπιν αιτήματος

(GetApp, χ.χ.)

24. Kibana

Το Kibana είναι ένα εργαλείο οπτικοποίησης ανοιχτού κώδικα βασισμένο σε πρόγραμμα περιήγησης που χρησιμοποιείται κυρίως για την ανάλυση μεγάλου όγκου αρχείων καταγραφής με τη μορφή γραφημάτων γραμμής, ραβδογράμματα, διαγράμματα πίτας, χάρτες θερμότητας (heat maps), χάρτες περιοχών, χάρτες συντεταγμένων, στόχους, χρονοδιαγράμματα και άλλα. Εύκολο εργαλείο για να προβλέψουμε ή να δούμε τις αλλαγές στις τάσεις των σφαλμάτων ή άλλων σημαντικών γεγονότων της πηγής εισόδου. Το Kibana λειτουργεί σε συγχρονισμό με το Elasticsearch και το Logstash που μαζί σχηματίζουν τη λεγόμενη στοίβα ELK.

❖ Χαρακτηριστικά

- ➢ Ευέλικτη πλατφόρμα ανάλυσης και οπτικοποίησης.
- ➢ Σύνοψη σε πραγματικό χρόνο και χαρτογράφηση δεδομένων ροής (charting of streaming data).
- ➢ Εύκολο UI για ποικιλία χρηστών.
- ➢ Άμεση κοινή χρήση και ενσωμάτωση πινάκων εργαλείων.

❖ Τιμολόγηση

Παρέχεται δωρεάν.
(Stackshare, χ.χ.)

25. Micro Focus

Το Micro Focus είναι ένα οργανωτικό εργαλείο που βοηθά τις επιχειρήσεις να διατηρήσουν τη συμμόρφωση και να μειώσουν τις δαπάνες. Οι εταιρείες μπορούν να σχεδιάζουν και να διαχειρίζονται χαρτοφυλάκια, πόρους και οικονομικά. Προσφέρει μια προβολή πίνακα ελέγχου όλων των σχετικών πληροφοριών και ειδοποιεί τους χρήστες για τροποποιήσεις πόρων που πραγματοποιούνται εντός μιας εταιρείας. Προσφέρει δυνατότητες παροχής αποτελεσμάτων οδηγώντας τον μετασχηματισμό και ξεπερνώντας τις προκλήσεις του έργου. Βοηθά τους οργανισμούς να ξεπεράσουν τις προκλήσεις διαχείρισης κόστους, χρόνου και πόρων και επιτρέπει την ενοποίηση των δεδομένων και την προβολή στα χαρτοφυλάκια επιχειρήσεων. Τα στελέχη μπορούν να δώσουν προτεραιότητα στις εργασίες και να ρίξουν μια ματιά στη χρήση των πόρων, ενώ τα ευθυγραμμίζουν με τους επιχειρηματικούς στόχους. Παρέχει κρίσιμες πληροφορίες σε πραγματικό χρόνο καταγράφοντας τις λειτουργίες και την εκτέλεση του έργου για να βοηθήσει τις εταιρείες να λάβουν τις σωστές επενδυτικές αποφάσεις.

- ❖ Χαρακτηριστικά

- ➢ Στρατηγική Διαχείριση Χαρτοφυλακίου
- ➢ Προγραμματισμός πόρων έργου
- ➢ Agile Enterprise
- ➢ Επιτάχυνση της παράδοσης του έργου
- ➢ Κλίμακα κατ' απαίτηση
- ➢ Βελτιστοποίηση πόρων

(SelectHub, χ.χ.)

- ❖ Τιμολόγηση

Οι τιμές κυμαίνονται από 0 έως 7 δολάρια, από 7 έως 10 δολάρια και από 10 δολάρια και πάνω. Επιπλέον, οι τιμές καθορίζονται ως "ανά χρήστη, ανά μήνα" ή ως"ανά μήνα". Ωστόσο, αξίζει να σημειωθεί ότι αυτά τα εύρη τιμών αφορούν κυρίως τη χαμηλότερη προσφορά που βρίσκεται στον ιστότοπο κάθε προμηθευτή.
(Shlomi, 2022)

26. Mend.io

Το Mend.io είναι ένα εργαλείο ανάλυσης σύνθεσης λογισμικού που ασφαλίζει ότι δημιουργούν οι προγραμματιστές. Η λύση παρέχει αυτοματοποιημένη μείωση της επιφάνειας επίθεσης του λογισμικού, μείωση του φόρτου των προγραμματιστών και επιτάχυνση της παράδοσης της εφαρμογής. Το Mend.io παρέχει ανάλυση ανοιχτού κώδικα με τις εσωτερικές και άλλες πηγές ευπαθειών του λογισμικού. Επιπλέον, προσφέρει ειδοποιήσεις παραβίασης

αδειών και πολιτικής, έχει εξαιρετική ενσωμάτωση αγωγού και, δεδομένου ότι είναι SaaS, δεν απαιτεί από τους προγραμματιστές να διατηρούν φυσικούς διακομιστές ή κέντρα δεδομένων για οποιαδήποτε υλοποίηση. Το Mend.io όχι μόνο μειώνει τον κίνδυνο ασφάλειας των εταιρικών εφαρμογών, αλλά βοηθά επίσης τους προγραμματιστές να τηρούν τις προθεσμίες.

❖ Χαρακτηριστικά

➢ Ανάλυση τρωτότητας
➢ Αυτοματοποιημένη αποκατάσταση
➢ Απρόσκοπτη ενσωμάτωση (Seamless integration)
➢ Προτεραιοποίηση των σχεδίων της επιχείρησης
➢ Απεριόριστη επεκτασιμότητα
➢ Διαισθητική διεπαφή (Intuitive interface)
➢ Γλωσσική υποστήριξη
➢ Ενσωματώσεις
➢ Συνεχής παρακολούθηση
➢ Προτάσεις αποκατάστασης
➢ Προσαρμογή

❖ Τιμολόγηση

➢ Ομάδες: 12.000 $ ετησίως για έως και 20 προγραμματιστές
➢ Επιχείρηση: 32.000 $ ετησίως για έως και 40 προγραμματιστές
(Sourceforge, χ.χ.)

27. New Relic

Το New Relic ενδυναμώνει τους μηχανικούς με μια προσέγγιση που βασίζεται στα δεδομένα για το σχεδιασμό, την κατασκευή, την ανάπτυξη και την εκτέλεση λογισμικού. Προσφέροντας τη μοναδική ενοποιημένη πλατφόρμα δεδομένων που εξουσιοδοτεί τους μηχανικούς να αποκτήσουν όλη την τηλεμετρία σε συνδυασμό με ισχυρά εργαλεία ανάλυσης, το New Relic βοηθά τους τεχνικούς να ξεπεράσουν το ΄τι΄ για να ανακαλύψουν το ΄γιατί΄. Αυτό βελτιώνει το χρόνο λειτουργίας, την αξιοπιστία και την αποδοτικότητα για να παρέχει εξαιρετικές εμπειρίες πελατών που τροφοδοτούν την ανάπτυξη.

❖ Χαρακτηριστικά

Απόδοση
➢ Παρακολούθηση πραγματικού χρήστη (Real User Monitoring ή RUM)

- ➢ Second by Second Metrics

Παρακολούθηση
- ➢ Βασικές γραμμές απόδοσης (Performance Baselines)
- ➢ Ανάλυση απόδοσης
- ➢ Παρακολούθηση απόδοσης
- ➢ Παρακολούθηση πολλαπλών συστημάτων
- ➢ Παρακολούθηση σε πραγματικό χρόνο

Λειτουργικότητα
- ➢ Σύνθετη παρακολούθηση
- ➢ Δυναμική χαρτογράφηση συναλλαγών
- ➢ Παρατηρησιμότητα cloud

Ορατότητα (Visibility)
- ➢ Πίνακες παρακολούθησης και απεικονίσεις
- ➢ Αναφορές

Απόκριση (Response)
- ➢ Πίνακες παρακολούθησης και απεικόνιση
- ➢ Προειδοποίηση συμβάντος
- ➢ Ανάλυση ριζικής αιτίας (Root Cause Analysis ή RCA)

- ❖ Τιμολόγηση

Το New Relic έχει 4 πακέτα τιμολόγησης. Μια δωρεάν δοκιμή του New Relic είναι επίσης διαθέσιμη. Ας δούμε τις διάφορες τιμολογιακές εκδόσεις παρακάτω.

Πίνακας 4.6.8: *Τιμολόγηση New Relic.*

Free (Forever)	$0.00	Ξεκινήστε να χρησιμοποιείτε το New Relic με όλα τα χαρακτηριστικά δωρεάν για πάντα.
Standard	Pay As You Go	Όλα όσα χρειάζεστε για την αντιμετώπιση προβλημάτων για ομάδες μέχρι 5 χρήστες.
Pro	Επικοινωνία με τον πάροχο	Για ομάδες άνω των 5 χρηστών, προηγμένη αντιμετώπιση προβλημάτων και υποστήριξη.

Enterprise	Επικοινωνία με τον πάροχο	Εταιρική ασφάλεια, υποστήριξη, ταυτότητα, & συμμόρφωση με τους παγκόσμιους οργανισμούς.

(G2, χ.χ.)

28. OWASP ZAP

Το OWASP ZAP (Zed Attack Proxy) είναι ένα ελεύθερο, ανοικτού κώδικα web application security scanner που επιτρέπει στους προγραμματιστές λογισμικού και τους δοκιμαστές (testers) να εκτελούν penetration testing στις εφαρμογές τους για να ανακαλύψουν ευπάθειες και να αποτρέψουν εχθρικές επιθέσεις. Μέχρι σήμερα, είναι ένα από τα πιο αναζητημένα έργα Open Web Application Security Project (OWASP), και το διατηρεί μια διεθνής ομάδα εθελοντών. Αυτό το εργαλείο είναι τόσο ευέλικτο και επεκτάσιμο και προορίζεται για χρήση από χρήστες που είναι νέοι στην ασφάλεια εφαρμογών, καθώς και εμπειρογνώμονες δοκιμαστές. Για την ευκολία των χρηστών, το OWASP ZAP έχει εκδόσεις για κάθε κύριο λειτουργικό σύστημα και την πλατφόρμα Docker, έτσι ώστε να μην βασίζονται σε οποιοδήποτε ενιαίο λειτουργικό.

- Χαρακτηριστικά
  - Αναχαίτιση διαμεσολαβητή (Intercept Proxy)
  - Έλεγχος πολιτικής σάρωσης
  - Ενεργή και παθητική σάρωση
  - Σκανάρισμα θύρας (Port Scan)
  - Εκτεταμένο API
  - ZAP Fuzzer
  - Έλεγχος πρόσβασης
  - Πλατφόρμα αγοράς ZAP
- Τιμολόγηση

Παρέχεται δωρεάν.
(PeerSpot, χ.χ.)

29. OWASP Threat Dragon

Το OWASP Threat Dragon είναι μια ελεύθερη, ανοιχτού κώδικα, cross-platform εφαρμογή μοντελοποίησης απειλών. Χρησιμοποιείται για να σχεδιάσει διαγράμματα μοντελοποίησης

απειλών και να απαριθμήσει τις απειλές για στοιχεία στο διάγραμμα. Ο Mike Goodwin δημιούργησε το Threat Dragon ως κοινότητα ανοιχτού κώδικα που παρέχει έναν διαισθητικό και προσβάσιμο τρόπο μοντελοποίησης των απειλών. Το Threat Dragon έχει σχεδιαστεί για να είναι προσβάσιμο για διάφορους τύπους ομάδων, με έμφαση στην ευελιξία και την απλότητα. Πρόκειται για εργαστηριακό έργο της OWASP και ακολουθεί τις αξίες και τις αρχές του μανιφέστου μοντελοποίησης απειλών.

- ❖ Χαρακτηριστικά

- ➢ Ευκολία χρήσης και προσβασιμότητα
- ➢ Σχεδιασμός διαγράμματος ροής δεδομένων
- ➢ Υπόδειξη απειλών
- ➢ Εισαγωγή μετριαστικών και αντισταθμιστικών μέτρων

- ❖ Τιμολόγηση

Παρέχεται δωρεάν.
(Owasp, χ.χ.)

30. Palo Alto Networks NG Firewalls

Το Palo Alto Networks NG Firewalls είναι firewall επόμενης γενιάς που χρησιμοποιούνται για την ασφάλεια και την προστασία δικτύων από απειλές και επιθέσεις. Χρησιμοποιείται για την ασφάλεια της περιφέρειας (perimeter security), την προστασία του κέντρου δεδομένων και τη διαχείριση ασφαλούς πρόσβασης σε περιβάλλοντα.

- ❖ Χαρακτηριστικά

- ➢ Συμμετρία εφαρμογής (Application symmetries)
- ➢ Ενσωματωμένη μηχανική μάθηση για ανίχνευση και πρόληψη απειλών
- ➢ Μια ενιαία πλατφόρμα για την ενσωμάτωση όλων των δυνατοτήτων ασφαλείας
- ➢ Ευαισθητοποίηση εφαρμογών (Application awareness)
- ➢ Ιδιότητες απομακρυσμένης πρόσβασης και φιλτραρίσματος διευθύνσεων URL
- ➢ Έλεγχος πακέτων
- ➢ IDM (Identity Management)
- ➢ Τείχος προστασίας επιπέδου εφαρμογής
- ➢ GlobalProtect VPN
- ➢ Οφέλη εξοικονόμησης χρόνου
- ➢ Ευκολία ενσωμάτωσης
- ➢ Χαρακτηριστικά ασύρματου νέφους

- ➢ Συλλογή καταγραφών Prisma
- ➢ Πλήρεις δυνατότητες ασφαλείας
- ➢ Προχωρημένο φιλτράρισμα διευθύνσεων URL
- ➢ Απόδοση
- ➢ Προστασία δικτύου
- ➢ Υπογραφή μηδενικής καθυστέρησης
- ➢ IPS (Intrusion Prevention System)

Αυτά τα χαρακτηριστικά παρέχουν ασφάλεια, ευκολία διαχείρισης, πρόληψη απειλών, ανίχνευση επιθέσεων σε πραγματικό χρόνο, ενσωμάτωση με άλλες λύσεις ασφαλείας και βελτιστοποίηση απόδοσης.

- ❖ Τιμολόγηση

- ➢ "Η τιμολόγηση, το κόστος εγκατάστασης και η αδειοδότηση για το Palo Alto Networks NG Firewalls θεωρείται γενικά ακριβή σε σύγκριση με άλλους προμηθευτές. Το κόστος του ίδιου του τείχους προστασίας είναι υψηλό, και υπάρχουν πρόσθετα έξοδα για χαρακτηριστικά όπως οι άδειες GlobalProtect και τα σχέδια συντήρησης. Το μοντέλο τιμολόγησης θεωρείται πολύπλοκο και υπάρχουν επιπλέον χρεώσεις για κάθε χαρακτηριστικό που προστίθεται. Ωστόσο, πολλοί χρήστες πιστεύουν ότι η προστασία και οι δυνατότητες που παρέχονται από το Palo Alto αξίζουν την τιμή. Υπάρχουν επίσης συστάσεις για την εξέταση πολυετών αδειών για εξοικονόμηση κόστους."

(PeerSpot, χ.χ.)

31. Parasoft SOAtest

Το Parasoft SOAtest είναι ευρέως αναγνωρισμένο ως η κορυφαία λύση επιχείρησης για λειτουργικές και μη λειτουργικές δοκιμές API και ακεραιότητα API. Παρέχει δοκιμή σύνθετων εφαρμογών με ισχυρή υποστήριξη για υπηρεσίες REST και web, καθώς και πάνω από 120 υποστηριζόμενα πρωτόκολλα και τύπους μηνυμάτων.

- ❖ Χαρακτηριστικά

- ➢ Microservices Testing
- ➢ Web UI Integration Testing
- ➢ Mobile Testing
- ➢ Φόρτωση & Δοκιμή απόδοσης
- ➢ Δοκιμή ενοχρήστρωσης (orchestration) και επαναχρησιμοποίησης
- ➢ Αναφορές & ανάλυση
- ➢ Τεχνικές προδιαγραφές

❖ Τιμολόγηση

➢ "Από ό, τι καταλαβαίνω, το Parasoft SOAtest δεν είναι η φθηνότερη επιλογή. Αλλά έχει πολλά να προσφέρει."
➢ "Το κόστος της Parasoft φαίνεται να έχει αυξηθεί με μια πρόβλεψη που δεν ήταν πραγματικά προβλεπόμενη για την εταιρεία μας. Έχουν κάνει τεράστια δουλειά στη διαπραγμάτευση αυτών των συμφωνιών."
➢ "Νομίζω ότι θα ήταν ένα μεγάλο βήμα να μειωθεί η τιμή των αδειών."

➢ Παρέχεται δωρεάν δοκιμή.
(PeerSpot, χ.χ.)

32. Prisma Cloud

Το Prisma Cloud από το Palo Alto Networks είναι μια λύση ασφαλείας cloud που χρησιμοποιείται για τη διαχείριση της στάσης ασφάλειας cloud (cloud security posture management), την προστασία φόρτου εργασίας cloud, ασφάλεια κοντέινερ και ασφάλεια κώδικα. Παρέχει ορατότητα, παρακολούθηση και προειδοποίηση για ζητήματα ασφάλειας σε περιβάλλοντα πολλαπλών cloud.

❖ Χαρακτηριστικά

Το Prisma Cloud από το Palo Alto Networks έχει πολλαπλές πολύτιμες λειτουργίες σύμφωνα με τις κριτικές. Το χαρακτηριστικό αυτόματης αποκατάστασης (auto-remediation) είναι ένα χαρακτηριστικό για τη βελτίωση της στάσης (posture) ασφαλείας και τη μείωση του κινδύνου. Ο τομέας CSPM είναι επίσης ιδιαίτερα σεβαστός για την ευελιξία και τον έλεγχο της διαχείρισης της στάσης ασφαλείας στο cloud. Η αναφορά αποθεμάτων (inventory reporting), η αυτοματοποίηση της ασφάλειας και τα εργαλεία υποδομής ως κώδικα (infrastructure-as-code) επαινούνται επίσης για την ευκολία χρήσης και την ολοκληρωμένη προστασία τους. Άλλα χαρακτηριστικά όπως η παρακολούθηση των ρυθμίσεων (configuration monitoring), οι ειδοποιήσεις και οι προσαρμοσμένες δυνατότητες ερωτήσεων (custom query capabilities) παρέχουν αποτελεσματική και ολοκληρωμένη προστασία για περιβάλλοντα πολλαπλών και υβριδικών cloud.
(PeerSpot, χ.χ.)

❖ Τιμολόγηση

Παρακάτω είναι το συνολικό κόστος για τις διαφορετικές διάρκειες συνδρομής.
Ενδέχεται να ισχύουν πρόσθετοι φόροι ή τέλη.

Πίνακας 4.6.9: *Τιμολόγηση Prisma Cloud.*

Όνομα	Περιγραφή	12 μήνες	24 μήνες	36 μήνες
Business_100	100 Prisma Cloud Business Edition credits	$9,000	$18,000	$27,000
Enterprise_100	100 Prisma Cloud Enterprise Edition credits	$18,000	$36,000	$54,000

(aws, χ.χ.)

33. Rapid7 InsightVM

Το Rapid7 InsightVM είναι μια ολοκληρωμένη πλατφόρμα διαχείρισης ευπάθειας που προστατεύει τα συστήματα από επιτιθέμενους και είναι εύκολα επεκτάσιμη. Η πλατφόρμα αυτή παρέχει εύκολη πρόσβαση στη διαχείριση ευπάθειας, την ασφάλεια εφαρμογών, την ανίχνευση και ανταπόκριση, την πληροφορία εξωτερικών απειλών, το orchestration και τον αυτοματισμό, και πολλά άλλα. Το Rapid7 InsightVM είναι ιδανικό για τις ομάδες ασφάλειας, πληροφορικής και DevOps, βοηθώντας τους να μειώσουν τον κίνδυνο, επιτρέποντάς τους να ανιχνεύουν και να ανταποκρίνονται γρήγορα σε επιθέσεις.

- ❖ Χαρακτηριστικά

Απόδοση
- ➢ Παρακολούθηση προβλημάτων
- ➢ Ταχύτητα ανίχνευσης
- ➢ False Positives
- ➢ Αυτόματη σάρωση

Δίκτυο
- ➢ Δοκιμή συμμόρφωσης (Compliance Testing)
- ➢ Σκανάρισμα περιφέρειας (Perimeter Scanning)
- ➢ Παρακολούθηση ρυθμίσεων (Configuration Monitoring)

Ανάλυση κινδύνου
- ➢ Βαθμολογία κινδύνου
- ➢ Αναφορές
- ➢ Προτεραιότητα κινδύνου

Αξιολόγηση ευπάθειας
- ➢ Σκανάρισμα ευπάθειας
- ➢ Πληροφορίες ευπάθειας

- ➢ Πίνακες παρακολούθησης

Αυτοματισμός

- ➢ Δοκιμές ασφαλείας
- ➢ Αυτοματισμός δοκιμών

- ❖ Τιμολόγηση

- ➢ $22/asset* : *Τιμή με βάση 512 assets το ελάχιστο. Χρεώνεται ετησίως.
- ➢ Παρέχεται δωρεάν δοκιμή.

(G2, χ.χ.)

34. Red hat Ansible Automation Platform

Η πλατφόρμα Red Hat Ansible Automation είναι μια ισχυρή λύση αυτοματοποίησης δικτύου που επιτρέπει στους οργανισμούς να χειρίζονται κάθε πτυχή της διαδικασίας εκκίνησης εφαρμογών τους μέσα σε ένα ενιαίο προϊόν. Επιτρέπει στους χρήστες να μοιράζονται τις αυτοματοποιήσεις τους, έτσι ώστε οι ομάδες εντός ενός οργανισμού να μπορούν να συνεργάζονται σε διάφορα έργα με ευκολία. Η πλατφόρμα αυτοματισμού Ansible έχει σχεδιαστεί για χρήση από όλους τους υπαλλήλους που εμπλέκονται στη διαδικασία αυτοματοποίησης δικτύου.

- ❖ Χαρακτηριστικά

Διοίκηση (Administration)

- ➢ Διαχείριση ρυθμίσεων
- ➢ Έλεγχος πρόσβασης
- ➢ Κονσόλα διαχείρισης (Administration Console)
- ➢ Διαχείριση εργασιών
- ➢ Πίνακες παρακολούθησης και οπτικοποίηση

Λειτουργικότητα

- ➢ Αυτοματισμός deployment
- ➢ API / Ενσωματώσεις

Διαδικασίες (Processes)

- ➢ Orchestration

Αυτοματισμός

- ➢ Αυτοματισμός δοκιμών
- ➢ Ευφυής αυτοματοποίηση
- ➢ Αυτόματη παροχή (Automated Provisioning)

Διαχείριση Πληροφορικής (IT Management)

- ➢ Διαχείριση ροών εργασίας
- ➢ Διαχείριση υποδομών
- ➢ Ανακάλυψη πληροφορικής

- ❖ Τιμολόγηση

Πίνακας 4.6.10: *Τιμολόγηση Red Hat Ansible Automation Platform.*

Basic Tower	$5,000 τον χρόνο
Enterprise Tower	$10,000 τον χρόνο
Premium Tower	$14,000 τον χρόνο

(G2, χ.χ.)

35. Stackstorm

Το StackStorm συνδέει όλες τις εφαρμογές, τις υπηρεσίες και τις ροές εργασίας. Από απλούς κανόνες αν/τότε (if/then) σε περίπλοκες ροές εργασίας, το StackStorm επιτρέπει τον αυτοματισμό του DevOps. Χωρίς να χρειάζεται να γίνει αλλαγή των υπάρχουσων διαδικασιών ή των ροών εργασίας, το StackStorm συνδέει αυτά που ήδη υπάρχουν. Η κοινότητα είναι αυτό που κάνει ένα καλό προϊόν μεγάλο. Το StackStorm χρησιμοποιείται από πολλούς ανθρώπους σε όλο τον κόσμο, και πάντα απαντάει σε όλες τις τυχόν ερωτήσεις. Το Stackstorm μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση και τον εξορθολογισμό σχεδόν οποιουδήποτε τμήματος της επιχείρησής. Μερικές από τις πιο κοινές εφαρμογές είναι όταν συμβαίνουν αποτυχίες, το StackStorm μπορεί να αντιμετωπίσει προβλήματα και να τα διορθώσει. Αυτοματοποιεί τους αγωγούς CI/CD και τέλος το ChatOps φέρνει την αυτοματοποίηση και τη συνεργασία μαζί, μετασχηματίζοντας τις ομάδες του devops για να κάνουν τα πράγματα καλύτερα, πιο γρήγορα και με στυλ.

- ❖ Χαρακτηριστικά

- ➢ Αισθητήρες (Sensors)
  Οι αισθητήρες είναι πρόσθετα της Python για είτε εισερχόμενη είτε εξερχόμενη ενσωμάτωση που λαμβάνουν ή παρακολουθούν τα γεγονότα αντίστοιχα. Όταν ένα συμβάν από εξωτερικά συστήματα συμβαίνει και υποβάλλεται σε επεξεργασία από έναν αισθητήρα, ένα StackStorm trigger εκπέμπεται στο σύστημα.
- ➢ Πυροδότηση (Triggers)
  Τα triggers αντιπροσωπεύουν εξωτερικά γεγονότα. Υπάρχουν γενικά triggers (π.χ. χρονοδιακόπτες, webhooks) και triggers ενσωμάτωσης (Sensu alert, JIRA issue

updated). Ένας νέος τύπος trigger μπορεί να οριστεί γράφοντας ένα πρόσθετο αισθητήρα.

- ➢ Δράσεις (Actions)
  Οι δράσεις είναι εξωτερικές ενσωματώσεις του StackStorm. Υπάρχουν γενικές δράσεις(ssh, REST κλήση), ενσωμάτωση (OpenStack, Docker, Puppet), ή προσαρμοσμένες δράσεις. Οι δράσεις είναι είτε πρόσθετα της Python, ή οποιαδήποτε σενάρια, που καταναλώνονται στο StackStorm προσθέτοντας μερικές γραμμές μεταδεδομένων. Οι δράσεις μπορούν να επικαλεστούν απευθείας από τον χρήστη μέσω του CLI ή του API, ή να χρησιμοποιηθούν και να κληθούν ως μέρος των κανόνων και των ροών εργασίας.
- ➢ Κανόνες
  Οι κανόνες συνδέουν τα triggers με τα actions (ή με τις ροές εργασίας) εφαρμόζοντας κριτήρια αντιστοιχίας.
- ➢ Ροές εργασίας
  Οι ροές εργασίας παίρνουν τις ενέργειες μαζί και καθορίζουν τη σειρά, τις συνθήκες μετάβασης και τη διαβίβαση των δεδομένων. Οι περισσότεροι αυτοματισμοί είναι περισσότερα από ένα βήματα και συνεπώς χρειάζονται περισσότερες από μία ενέργειες. Οι ροές εργασίας, όπως και οι "ατομικές" ενέργειες, είναι διαθέσιμες στη βιβλιοθήκη "Action" και μπορούν να ενεργοποιηθούν χειροκίνητα ή με κανόνες.
- ➢ Πακέτα
  Τα πακέτα είναι οι μονάδες ανάπτυξης περιεχομένου. Απλοποιούν τη διαχείριση και την κοινή χρήση του περιεχομένου που μπορεί να συνδεθεί με το StackStorm με την ομαδοποίηση ενσωματώσεων (πυροδότηση και ενέργειες) και αυτοματισμού (κανόνες και ροές εργασίας). Ένας αυξανόμενος αριθμός πακέτων είναι διαθέσιμα στο StackStorm Exchange. Οι χρήστες μπορούν να δημιουργήσουν τα δικά τους πακέτα, να τα μοιραστούν στο Github, ή να τα υποβάλουν στο StackStorm Exchange.
- ➢ Έλεγχοι
  Το ίχνος ελέγχου των ενεργειών εκτέλεσης, χειροκίνητα ή αυτοματοποιημένα, καταγράφεται και αποθηκεύεται με πλήρεις λεπτομέρειες των αποτελεσμάτων εκτέλεσης. Καταγράφεται επίσης στα αρχεία καταγραφής ελέγχου για ενσωμάτωση με εξωτερικά εργαλεία καταγραφών και αναλύσεων: LogStash, Splunk, statsd, syslog.

(Sourceforge, χ.χ.)

- ❖ Τιμολόγηση

Δεν βρέθηκε κάποια πληροφορία για την τιμολόγηση του προϊόντος.

36. SonarQube

Το SonarQube είναι το κορυφαίο εργαλείο για τη συνεχή επιθεώρηση της ποιότητας του κώδικα και της ασφάλειάς του, καθώς και για την καθοδήγηση των ομάδων ανάπτυξης κατά

τη διάρκεια της επανεξέτασής του. Παρέχει σαφείς οδηγίες επιδιόρθωσης για 27 γλώσσες, έτσι ώστε οι προγραμματιστές να μπορούν να κατανοήσουν και να διορθώσουν τα προβλήματα και οι ομάδες να μπορούν να παραδώσουν καλύτερο και ασφαλέστερο λογισμικό. Το SonarQube ενσωματώνεται στη ροή εργασίας για να παρέχει τη σωστή ανατροφοδότηση την κατάλληλη στιγμή: σε IDE με το SonarLint, σε pull requests, και στο ίδιο το SonerQube. Με περισσότερες από 225.000 deployments που βοηθούν τις μικρές ομάδες ανάπτυξης και τους παγκόσμιους οργανισμούς, το SonarQube παρέχει τα μέσα για τις ομάδες και τις εταιρείες σε όλο τον κόσμο για να αποκτήσουν και να επηρεάσουν την ποιότητα και την ασφάλεια του κώδικά τους.

- ❖ Χαρακτηριστικά

Διαχείριση

- ➢ Δοκιμή ενσωμάτωσης (Testing Integration)

Λειτουργικότητα

- ➢ Ενσωμάτωση αποθήκης (Repository Integration)
- ➢ Αναλυτικά στοιχεία και τάσεις
- ➢ Ενημερώσεις παραγωγικότητας (Productivity Updates)

Documentation

- ➢ Ανατροφοδότηση (Feedback)
- ➢ Προτεραιότητα (Prioritization)
- ➢ Προτάσεις για διόρθωση (Remediation Suggestions)

- ❖ Τιμολόγηση

Το SonarQube έχει 4 πακέτα τιμολόγησης, ξεκινώντας από $0 με μια δωρεάν δοκιμή. Ας δούμε τις διάφορες τιμολογιακές εκδόσεις παρακάτω:

Πίνακας 4.6.11: *Τιμολόγηση SonarQube.*

Community	Δωρεάν	0$
Data Center	Δωρεάν δοκιμή	Ξεκινάει στα $130,000 τον χρόνο/instance
Developer	Δωρεάν δοκιμή	Ξεκινάει στα $150 τον χρόνο/instance
Enterprise	Δωρεάν δοκιμή	Επικοινωνία με τον πάροχο

(G2, χ.χ.)

37. Snyk

Η Πλατφόρμα Ασφάλειας Προγραμματιστών του Snyk ενσωματώνεται αυτόματα με τη ροή εργασίας ενός προγραμματιστή και βοηθά τις ομάδες ασφαλείας να συνεργαστούν με την ομάδα ανάπτυξής τους. Διαθέτει μια προσέγγιση προσανατολισμένη προς τους προγραμματιστές που διασφαλίζει ότι οι οργανισμοί μπορούν να εξασφαλίσουν όλα τα κρίσιμα στοιχεία των εφαρμογών τους από τον κώδικα έως το cloud, οδηγώντας στην παραγωγικότητα των προγραμματιστών, την αύξηση των εσόδων, την ικανοποίηση των πελατών, την εξοικονόμηση κόστους και τη βελτίωση της στάσης (posture) ασφαλείας. Το Snyk χρησιμοποιείται από 1.200 πελάτες σε όλο τον κόσμο σήμερα, συμπεριλαμβανομένων των Asurion, Google, Intuit, MongoDB, New Relic, Revolut και Salesforce. Τα προϊόντα του Snyk περιλαμβάνουν:

- ➔ Snyk Open Source - Αυτόματη ανίχνευση ευπαθειών και αυτόματη επιδιορθώσεις κατά τη διάρκεια της ανάπτυξης με SCA.
- ➔ Snyk Code - Στατική δοκιμή ασφάλειας εφαρμογών (SAST).
- ➔ Snyk Container - Container και Kubernetes ασφαλείας σχεδιασμένο για να βοηθήσει τους προγραμματιστές να βρουν και να διορθώσουν τις ευπάθειες σε cloud native εφαρμογές.
- ➔ Snyk Infrastructure as Code - Μείωση του κινδύνου με την αυτοματοποίηση της ασφάλειας και της συμμόρφωσης του IaC στις ροές εργασίας ανάπτυξης πριν από την ανάπτυξη και ανίχνευση μετακινούμενων και χαμένων πόρων μετά την ανάπτυξη.
- ➔ Snyk Cloud - Ασφάλεια cloud με μια ενοποιημένη πολιτική ως μηχανή κώδικα (code engine), έτσι ώστε κάθε ομάδα να μπορεί να αναπτύξει, να εφαρμόσει και να λειτουργήσει με ασφάλεια στο cloud.

❖ Χαρακτηριστικά

Τα πιο πολύτιμα χαρακτηριστικά του Snyk περιλαμβάνουν την ανάλυση σύνθεσης λογισμικού (SCA), ανίχνευση ευπάθειας ασφαλείας, εύκολη ενσωμάτωση, κεντρική επιδιόρθωση προβλημάτων, κατηγοριοποίηση των ευπαθειών, σάρωση container, σαρώσεις κώδικα, σταθερότητα, αυτοματοποίηση, προσφορά ανοικτού πηγαίου κειμένου, σαρωτική ανάλυση μυστικών (secrets scanning), στατική ανάλυση με SAST, σαφείς πληροφορίες και ανατροφοδότηση, εμπειρογνωμοσύνη στον τομέα της ασφάλειας, αυτόματη δημιουργία αιτημάτων pull, φιλικό προς τους προγραμματιστές προϊόν, ενσωματώσεις, πίνακας παρακολούθησης και αναφορές και εύκολη ενσωμάτωση χωρίς αγωγό. Το Snyk είναι χρήσιμο για τον εντοπισμό τρωτών σημείων ασφαλείας, τον καθορισμό προτεραιοτήτων και την παροχή κατάλληλων αναφορών και λύσεων. Είναι επίσης αξιόπιστο, ομαλό, και δεν απαιτεί πολλή προετοιμασία ή προϋποθέσεις.

❖ Τιμολόγηση

Το Snyk έχει ανταγωνιστική τιμή για την κάλυψη, την επεκτασιμότητα, την αξιοπιστία και τη σταθερότητά του, χωρίς πρόσθετα έξοδα για τα τυπικά τέλη αδειοδότησης. Μερικοί χρήστες

το θεωρούν λογικό, ενώ άλλοι το βρίσκουν ακριβό σε σύγκριση με άλλες λύσεις. Το μοντέλο αδειοδότησης βασίζεται στον αριθμό των προγραμματιστών που συνεισφέρουν, και η τιμή μπορεί να ποικίλει ανάλογα με το μέγεθος της εταιρείας. Ωστόσο, ορισμένοι χρήστες το βρίσκουν αποδεκτό, ειδικά για τις επιχειρήσεις. Η έκδοση ανοικτού κώδικα είναι επίσης διαθέσιμη και ενσωματωμένη με τον αγωγό αυτοματοποίησης Jenkins CI/CD, ο οποίος δίνει τα πάντα σε ένα μέρος.

Δωρεάν - Περιορισμένες δοκιμές, Απεριόριστοι προγραμματιστές - Δωρεάν
Ομάδα - Απεριόριστες δοκιμές - Ξεκινώντας από $98.00
Enterprise - Απεριόριστες δοκιμές - Επικοινωνία με τον πάροχο
(G2, χ.χ.)

38. SOOS

Το SOOS είναι μια λύση ανάλυσης σύνθεσης λογισμικού και δυναμικής δοκιμής ασφάλειας εφαρμογών. Οι χρήστες μπορούν να σαρώσουν το λογισμικό ανοιχτού κώδικα για τρωτά σημεία, να ελέγξουν την εισαγωγή νέων dependencies, να αποκλείσουν ανεπιθύμητους τύπους αδειών, να δημιουργήσουν SBOMs και να συμπληρώσουν φύλλα εργασίας συμμόρφωσης (compliance worksheets).

- ❖ Χαρακτηριστικά

SCA
- ➢ Έλεγχος και διαχείριση ευπάθειας ανοικτού κώδικα
- ➢ Ανάλυση άδειας χρήσης
- ➢ Συμμόρφωση & Διακυβέρνηση (Governance)
- ➢ Δημιουργία SBOM
- ➢ Ενσωμάτωση CI/CD (AWS CodeBuild, Azure DevOps, Bamboo, CircleCI, Codeship, Jenkins, TeamCity, Travis CI)
- ➢ Προβλήματα ενσωμάτωσης (Jira, Github, others)
- ➢ Ενσωμάτωση repository (Github Actions, Gitlab, others)

DAST
- ➢ Το SOOS DAST επιτρέπει την σάρωση για τρωτά σημεία στο web σε κάθε build και την παρακολούθηση της εφαρμογή με τον ενοποιημένο πίνακα ελέγχου (unified dashboard) που έρχεται με το SOOS Core, ώστε να υπάρχει ένα μέρος για την διαχείριση όλων των ζητημάτων ασφάλειας των εφαρμογών.
- ➢ Περιλαμβάνει SOOS Core SCA
- ➢ Σάρωση εφαρμογών ιστού για τρωτά σημεία
- ➢ Σκανάρισμα API-OpenAPI, GraphQL και SOAP
- ➢ Δεν υπάρχουν όρια στον αριθμό των τομέων (domains)

- ➢ Μετακίνηση προβλημάτων στο πίνακα ελέγχου ασφαλείας του GitHub
- ➢ Προβολή ιστορικού σάρωσης
- ➢ Ενοποιημένος πίνακας ελέγχου με SOOS Core SCA

- ❖ Τιμολόγηση

- ➢ Δωρεάν έκδοση της κοινότητας.
- ➢ SCA ξεκινώντας από $ 100 / μήνα
- ➢ DAST ξεκινώντας από $ 200 / μήνα
- ➢ Δωρεάν έκδοση διαθέσιμη.
- ➢ Δωρεάν δοκιμή διαθέσιμη.

(Sourceforge, χ.χ.)

39. Trivy

Πρόκειται για έναν απλό και ολοκληρωμένο σαρωτή ευπάθειας για containers και άλλα artifacts. Ανιχνεύει ευπάθειες των πακέτων λειτουργικού συστήματος (Alpine, RHEL, CentOS, κ.λπ.) και εξαρτήσεις εφαρμογών (Bundler, Composer, npm, yarn, etc.). Είναι εύκολο στη χρήση. Το μόνο που χρειάζεται να κάνετε για τη σάρωση είναι να καθορίσετε έναν στόχο, όπως ένα όνομα εικόνας του container. Το Trivy είναι ένα εργαλείο στην κατηγορία ασφάλειας ενός tech stac και είναι ανοιχτού κώδικα με 18 χιλιάδες αστέρια στο GitHub και 1.8 χιλιάδες Git Hub forks.

- ❖ Χαρακτηριστικά

- ➢ Απλό
- ➢ Γρήγορο
- ➢ Εύκολη εγκατάσταση
- ➢ Υψηλή ακρίβεια
- ➢ Ανίχνευση εκτεταμένων ευπαθειών
- ➢ Κατάλληλο για CI όπως Travis CI, CircleCI, Jenkins, GitLab CI, κλπ
- ➢ Υποστήριξη πολλαπλών μορφών

- ❖ Τιμολόγηση

Παρέχεται δωρεάν.
(Stackshare, χ.χ.)

40. ThreatModeler

Το ThreatModeler, μια εταιρική πλατφόρμα μοντελοποίησης απειλών, είναι μια αυτοματοποιημένη λύση που μειώνει την προσπάθεια που απαιτείται για την ανάπτυξη ασφαλών εφαρμογών. Οι σημερινοί επαγγελματίες ασφάλειας πληροφοριών έχουν μια επείγουσα ανάγκη να δημιουργήσουν μοντέλα απειλής των δεδομένων και του λογισμικού των οργανισμών τους και αυτό γίνεται λόγω της ταχύτητας της καινοτομίας. Το ThreatModeler, το οποίο ενδυναμώνει τους οργανισμούς IT επιχειρήσεων, τους επιτρέπει να χαρτογραφούν τις μοναδικές απαιτήσεις και πολιτικές ασφαλείας τους απευθείας στο περιβάλλον της επιχείρησης. Αυτό παρέχει σε πραγματικό χρόνο καταστατική επίγνωση του χαρτοφυλακίου (portfolio) απειλών και των κινδύνων τους. Οι υπεύθυνοι της InfoSec και οι CISOs αποκτούν πλήρη κατανόηση του συνολικού εύρους της επίθεσης και της στρατηγικής άμυνας σε βάθος, το οποίο τους επιτρέπει να κατανέμουν στρατηγικά τους πόρους και να αυξάνουν την παραγωγή τους.

❖ Χαρακτηριστικά:

➢ Οπτικοποίηση & συνεχές (Visual & Continuous)
Η μόνη πλατφόρμα για τον αυτόματο, οπτικό και συνεχή εντοπισμό σχεδιαστικών ατελειών.

➢ Κώδικας στο cloud
Γρηγορότερη και ασφαλέστερη επιχειρησιακή μετάβαση και ανάπτυξη στο cloud.

➢ Ενημερωμένο με λιγότερη προσπάθεια
Το Κέντρο Ερευνών Απειλών διατηρεί τις πληροφορίες για τις απειλές επίκαιρες με συνεχή έρευνα σχετικά με τις αναδυόμενες απειλές, τη συμμόρφωση και τις βέλτιστες πρακτικές.

➢ Ευελιξία
Λειτουργεί στο cloud, στα κινητά, στο IoT και σε όλη τη διάρκεια του DevOps.

➢ Συμμόρφωση
Ενσωματώνει τη συμμόρφωση στα θεμέλια της υποδομής με ενσωματωμένα πλαίσια κανονιστικής συμμόρφωσης.

➢ IaC
Παρέχει συνεχή ορατότητα σε μη ανακαλυφθέντα σφάλματα σχεδιασμού μέσω του infrastructure-as-code (IaC) σε πραγματικό χρόνο.

❖ Τιμολόγηση

Παρακάτω είναι το συνολικό κόστος για τις διαφορετικές διάρκειες συνδρομής. Ενδέχεται να ισχύουν πρόσθετοι φόροι ή τέλη.

Πίνακας 4.6.12: *Τιμολόγηση ThreatModeler.*

Όνομα	Περιγραφή	12 μήνες	24 μήνες	36 μήνες
LICENSE	LICENSE	$4,000	$6,800	$8,400

➢ Δωρεάν έκδοση: Ναι
➢ Δωρεάν δοκιμή: Ναι
(aws, χ.χ.)

41. Veracode

Η πλατφόρμα Veracode είναι μια λύση ασφάλειας λογισμικού που στοχεύει να είναι ευρέως διαδεδομένη και ενσωματωμένη στα περιβάλλοντα στα οποία εργάζονται οι προγραμματιστές, με τη συνιστώμενη επιδιόρθωση και μάθηση. Οι ομάδες ασφαλείας μπορούν να χρησιμοποιήσουν το Veracode για να διαχειριστούν τις πολιτικές, να αποκτήσουν μια ολοκληρωμένη εικόνα της στάσης ασφάλειας ενός οργανισμού μέσω αναλύσεων και αναφορών, να μετριάσουν τους κινδύνους και να παράγουν τα αποδεικτικά στοιχεία που απαιτούνται για την εκπλήρωση των κανονιστικών απαιτήσεων. Παρουσιάζεται ως μια συνεχής οργάνωση της ασφαλούς ανάπτυξης που δίνει στους οργανισμούς την εμπιστοσύνη ότι το λογισμικό που κατασκευάζεται είναι ασφαλές και πληροί τις απαιτήσεις συμμόρφωσης.

❖ Χαρακτηριστικά

➢ Συνεχής σάρωση για τη μείωση των κινδύνων σε κάθε στάδιο ανάπτυξης
Στατική Ανάλυση, δυναμική Ανάλυση, ανάλυση σύνθεσης λογισμικού και χειροκίνητο penetration test σε όλο το SDLC.
➢ Εμπειρία προγραμματιστή
Βρίσκει και διορθώνει τους νόμους σύμφωνα με την ενσωμάτωση της ασφάλειας στο χώρο εργασίας των προγραμμάτων, την αυτοματοποιημένη καθοδήγηση για την αποκατάσταση και τη μάθηση.
➢ Πλήρης εμπειρία πλατφόρμας
Ομαλές διαδικασίες διακυβέρνησης (governance), κινδύνου και συμμόρφωσης μέσω ευέλικτης διαχείρισης πολιτικής, ενοποιημένων αναφορών και αναλύσεων και αξιολόγησης από συναδέλφους για τον γρήγορο μετριασμό των κινδύνων και την παροχή ενός επιτυχημένου προγράμματος DevSecOps.
➢ Δεδομένα Πλατφόρμας

Εξαιρετικά προσαρμοσμένα με σχεδόν δύο δεκαετίες σάρωσης και μάθησης πελατών. Προβλέπει μελλοντικές ευπάθειες με δυνατότητες αυτοθεραπείας μέσω της εφαρμογής της μηχανικής μάθησης και της τεχνητής νοημοσύνης στα δεδομένα.

- ➢ Cloud-native SaaS Αρχιτεκτονική

Παρέχει ελαστική κλιμακωτότητα (elastic scalability), υψηλή απόδοση, και χαμηλότερο κόστος με cloud-nated αρχιτέκτονες Saas.

- ❖ Τιμολόγηση

- ➢ "Το Veracode είναι ακριβό. Έχουν διαφορετικά μοντέλα αδειών για διαφορετικούς πελάτες. Αυτό που είχαμε ήταν με βάση την ποσότητα του κώδικα που έχει αναλυθεί. Η άδεια που είχαμε περιορίστηκε σε ένα ορισμένο ποσό, για παράδειγμα, 5 Gig. Θα υπάρχει επιπλέον χρέωση για οτιδήποτε πάνω από 5 Gig."
- ➢ "Χρήστες σε ορισμένα φόρουμ ανέφεραν ότι η τιμολόγηση για αυτή τη λύση μπορεί να είναι αρκετά υψηλή."
- ➢ "Η τιμή της Στατικής Ανάλυσης Veracode είναι στην υψηλότερη πλευρά."

- ➢ Παρέχεται δωρεάν δοκιμή.

(PeerSpot, χ.χ.)

42. Kubernetes

Το Kubernetes (K8s) είναι ένα λογισμικό ανοικτού κώδικα για την αυτοματοποίηση της ανάπτυξης, της κλιμάκωσης και της διαχείρισης των εφαρμογών. Ομαδοποιεί τα κοντέινερ που συνθέτουν μια εφαρμογή σε λογικές μονάδες για εύκολη διαχείριση και ανακάλυψη. Η Kubernetes βασίζεται σε 15 χρόνια εμπειρίας στην εκτέλεση εργασιών παραγωγής στο Google, σε συνδυασμό με τις καλύτερες ιδέες και πρακτικές από την κοινότητα.

- ❖ Χαρακτηριστικά

Διαχείριση

- ➢ Έλεγχος πρόσβασης

Οργάνωση

- ➢ Packaging
- ➢ Δικτύωση container (Container Networking)

Ανάπτυξη (Development)

- ➢ Orchestration
- ➢ Εργαλεία προγραμματιστή (Developer toolkit)
- ➢ Αρχιτεκτονική

- ➢ Κέντρο δεδομένων
- ➢ Εικονικοποίηση (Virtualization)

❖ Τιμολόγηση

"Το επίπεδο διαχείρισης είναι ελεύθερο, το οποίο είναι τέλειο. Δεν χρειάζεται να πληρώσετε χρήματα για το επίπεδο διαχείρισης, αλλά στην υπηρεσία ανάπτυξης AWS, πρέπει να πληρώνετε. Νομίζω ότι είναι 75 ευρώ το μήνα για το επίπεδο διαχείρισης. Είναι δωρεάν, ώστε να μπορείτε να έχετε όσα Kubernetes clusters χρειάζεστε. Πληρώνετε μόνο για το φορτίο εργασίας, δηλαδή για το μηχάνημα, την CPU, τη μνήμη και τα πάντα."
"Το Google Kubernetes είναι δωρεάν στην απλούστερη ρύθμιση, το AWS kubernetes κοστίζει περίπου 50 δολάρια (ανάλογα με την περιοχή), σε τρεις κύριες ρυθμίσεις, οπότε είναι σχεδόν το ίδιο με το κόστος των περιπτώσεων EC2 και είναι εντελώς εντάξει από την άποψή μου."
"Το Kubernetes είναι ανοιχτού κώδικα."
(PeerSpot, χ.χ.)

43. Chef

Το Chef (aka Progress Chef) είναι ένα εργαλείο διαχείρισης ρυθμίσεων (configuration management tool) που βοηθά τους οργανισμούς να εξορθολογίσουν τις ροές εργασίας τους και να επιτύχουν συνέπεια και επεκτασιμότητα μέσω διαφόρων δυνατοτήτων αυτοματισμού υποδομής.

❖ Χαρακτηριστικά

Τα ακόλουθα χαρακτηριστικά είναι μερικοί από τους λόγους για τους οποίους το Progress Chef έχει γίνει τόσο δημοφιλές εργαλείο διαχείρισης ρυθμίσεων στην κοινότητα DevOps:

- ➢ Υποδομή ως κώδικας
- ➢ Αφαίρεση (abstraction) των πόρων του συστήματος
- ➢ Monitoring
- ➢ Μεγάλη ενεργή κοινότητα
- ➢ Ενσωματώσεις

Το Chef χρησιμοποιεί την υποδομή ως κώδικα (IaC), που επιτρέπει στις ομάδες να χρησιμοποιούν μορφές που μπορούν να διαβαστούν από τον άνθρωπο όταν περιγράφουν τις επιθυμητές καταστάσεις του συστήματος. Αυτό προάγει την επαναληψιμότητα των ρυθμίσεων, τη συνέπεια και τον έλεγχο εκδόσεων. Το Chef διαθέτει επίσης αφαίρεση πόρων συστήματος, η οποία επιτρέπει στο εργαλείο να παρέχει διαχείριση υποδομής πλατφόρμας. Με το Chef, υπάρχει υποστήριξη για διάφορες πλατφόρμες cloud και λειτουργικά συστήματα.

❖ Τιμολόγηση

Το Chef προσφέρει συνδρομές freemium με πληρωμένα προγράμματα που ξεκινούν από $72.00 / μήνα. Αυτό σημαίνει ότι το Chef προσφέρει ένα δωρεάν-για πάντα σχέδιο που δεν είναι χρονικά περιορισμένο, καθώς και πληρωμένες συνδρομές.
Παρακάτω είναι μια επισκόπηση των κύριων σχεδίων τιμολόγησης του Chef που προσφέρει:

➢ Chef Basics Plan
➔ Δωρεάν
➔ Chef Client
➔ Chef Server
➔ Chef DK
➔ Supermarket Content

➢ Hosted Chef Plan
➔ $72.00 ανά κόμβο
➔ Ελάχιστο 20 κόμβοι για την ετήσια τιμολόγηση
➔ Όλα τα χαρακτηριστικά του Chef Basics
➔ Hosting services για τον εξυπηρετητή Chef
➔ Υποστηριζόμενο περιεχόμενο

➢ Chef Automate Plan
➔ $137.00 ανά κόμβο
➔ Ορατότητα (Visibility)
➔ Συμμόρφωση
➔ Ροές εργασίας
➔ 24/7 υποστήριξη

Το Chef προσφέρει εκπτώσεις οι λεπτομέρειες των οποίων είναι διαθέσιμες με την επίσκεψη στην ιστοσελίδα της εταιρείας.
(Crozdesk, χ.χ.)

44. Splunk

Με το Splunk Enterprise μπορεί να γίνει γνωστό τι συμβαίνει στην επιχείρηση ώστε οι εμπλεκομενοι να αναλάβουν γρήγορα ουσιαστική δράση. Μπορεί επίσης να αυτοματοποιήσει τη συλλογή, την διευθυνσιοδότηση (indexing) και την ειδοποίηση των δεδομένων μηχανής

που είναι κρίσιμα για πολλές δραστηριότητες και να αποκαλύψει τις αξιοποιήσιμες πληροφορίες από όλα τα δεδομένα ανεξάρτητα από την πηγή ή τη μορφή τους. Τέλος, αξιοποιεί την τεχνητή νοημοσύνη και τη μηχανική μάθηση για προγνωστικές και προληπτικές επιχειρηματικές αποφάσεις.

- ❖ Χαρακτηριστικά

Λειτουργικότητα

- ➢ Παρακολούθηση ποικίλων συστημάτων
- ➢ Ανάλυση σε πραγματικό χρόνο
- ➢ Παρατηρησιμότητα (Observability)

Διαχείριση

- ➢ Baseline performance

Προετοιμασία δεδομένων

- ➢ Πηγές δεδομένων
- ➢ Indexing
- ➢ Αυτοματοποιημένο tagging
- ➢ Συνδυασμός δεδομένων

Ανάλυση

- ➢ Παρακολούθηση τάσεων
- ➢ Ανίχνευση ανωμαλιών
- ➢ Μετρικά δεδομένα και δεδομένα συμβάντων
- ➢ Αναζήτηση
- ➢ Ειδοποιήσεις

Οπτικοποίηση

- ➢ Πίνακες ελέγχου
- ➢ Ανακάλυψη δεδομένων

- ❖ Τιμολόγηση

Το Splunk Enterprise προσφέρει συνδρομές freemium με πληρωμένα πακέτα που ξεκινούν από $173,00/μήνα. Αυτό σημαίνει ότι το Splunk Enterprise προσφέρει ένα δωρεάν-για πάντα πακέτο που δεν είναι χρονικά περιορισμένο, καθώς και συνδρομές επί πληρωμή. Παρακάτω παρατίθεται μια επισκόπηση των κύριων πακέτων τιμολόγησης που προσφέρει το Splunk Enterprise.

Free

- ➢ Δωρεάν
- ➢ Ένας χρήστης

- ➢ Κλιμάκωση (Scale) έως 500 MB δεδομένων ανά ημέρα
- ➢ Συλλογή και indexing οποιωνδήποτε δεδομένων
- ➢ Αναζήτηση, ανάλυση και οπτικοποίηση σε πραγματικό χρόνο

Light

- ➢ $86.00
- ➢ Μηνιαία
- ➢ Κλιμάκωση έως και 20 GB δεδομένων ανά ημέρα
- ➢ Μέχρι 5 χρήστες
- ➢ Παρακολούθηση και ειδοποίηση
- ➢ Απεριόριστες αναζητήσεις
- ➢ Ανάπτυξη στις εγκαταστάσεις του οργανισμού, στο cloud ή χρήση της υπηρεσίας Splunk Light Cloud

Enterprise

- ➢ $173.00
- ➢ Μηνιαία
- ➢ Κλιμάκωση σε απεριόριστες ποσότητες δεδομένων ανά ημέρα
- ➢ Απεριόριστοι χρήστες
- ➢ Επιδόσεις, κλίμακα και αξιοπιστία
- ➢ Λύσεις και εφαρμογές Splunk Premium από την Splunkbase
- ➢ Υποστήριξη επιχειρηματικού επιπέδου

(Crozdesk, χ.χ.)

45. IBM X-Force Exchange

Το IBM X-Force Exchange είναι μια πλατφόρμα ανταλλαγής πληροφοριών σχετικά με απειλές, βασίζεται στο cloud και επιτρέπει στους χρήστες να διερευνούν γρήγορα τις τελευταίες απειλές ασφαλείας, να συγκεντρώνουν πληροφορίες που μπορούν να χρησιμοποιηθούν και να συνεργάζονται με την ομάδα τους. Το IBM X-Force Exchange υποστηρίζεται από πληροφορίες που παράγονται από ανθρώπους και μηχανές, αξιοποιώντας την κλίμακα της IBM X-Force.

- ❖ Χαρακτηριστικά

- ➢ IBM X-Force Exchange
- ➢ IBM Advanced Threat Protection Feed
- ➢ IBM X-Force Exchange Commercial API
- ➢ IBM Early Warning Feed

➢ IBM X-Force Premium Threat Intelligence Reports

❖ Τιμολόγηση

➢ "Το κόστος είναι σαφώς ένα στοιχείο, αλλά το σημαντικό είναι τι κάνουμε με τα δεδομένα και πώς τα προστατεύουμε."
➢ "Ένας από τους ταχύτερους τρόπους μείωσης του κόστους είναι η μείωση του προσωπικού, και αυτό το προϊόν μπορεί να μειώσει το προσωπικό κατά 70 τοις εκατό."

➢ Παρέχεται δωρεάν έκδοση και δωρεάν δοκιμή.
(PeerSpot, χ.χ.)

46. Sonatype

Το Sonatype ασφαλίζει την αλυσίδα εφοδιασμού λογισμικού και προστατεύει τον κύκλο ζωής ανάπτυξης λογισμικού (SDLC) των οργανισμών. Η πλατφόρμα ενώνει τις ομάδες ασφάλειας και τους προγραμματιστές για να επιταχύνουν την ψηφιακή καινοτομία χωρίς να θυσιάζουν την ασφάλεια ή την ποιότητα σε όλο το SDLC. Με χρήστες περισσότερους από 2.000 οργανισμούς και 15 εκατομμύρια προγραμματιστές λογισμικού, τα εργαλεία και η καθοδήγηση του Sonatype βοηθούν τους χρήστες να παραδώσουν και να διατηρήσουν ένα ιδιαίτερο και ασφαλές λογισμικό. Τα βασικά του προϊόντα αποτελούν:

➔ Το Sonatype Repository Firewall είναι η πρώτη γραμμή άμυνας κατά των επιθέσεων στην αλυσίδα εφοδιασμού λογισμικού. Αποκλείει τα κακόβουλα και ύποπτα πακέτα, αποτρέπει τη λήψη γνωστών ευπαθειών και επιβλαβών εκδόσεων ανοικτού κώδικα στο repository και απελευθερώνει αυτόματα τα ελεγμένα συστατικά πίσω στη γραμμή ανάπτυξης.
➔ Το Sonatype Lifecycle επιτρέπει τη συνεχή παρακολούθηση των κρίσιμων για τις επιχειρήσεις εφαρμογών που έχουν κυκλοφορήσει ή αναπτυχθεί για τον προσδιορισμό του επιπέδου κινδύνου και την ταχύτερη αποκατάσταση των ευπαθειών, με ακριβή πληροφόρηση για τα συστατικά τους. Αυτό συμβάλλει στην πρόληψη μη προγραμματισμένων εργασιών, παραβιάσεων ασφάλειας και προβλημάτων συντηρησιμότητας με έγκαιρη ανίχνευση και αποκατάσταση.
➔ Το Sonatype Nexus Repository βοηθά στη διαχείριση των συστατικών, των δυαδικών αρχείων και των αντικειμένων δημιουργίας (build artifacts) σε ολόκληρη την αλυσίδα εφοδιασμού λογισμικού, εξυπηρετώντας δισεκατομμύρια συστατικά (components), στους προγραμματιστές εβδομαδιαίως, ώστε να μπορούν να δημιουργούν πιο γρήγορα και αξιόπιστα.

- ❖ Χαρακτηριστικά

- ➢ Συνεχής παρακολούθηση
- ➢ Επιβολή πολιτικών
- ➢ Ενσωματώσεις και υποστήριξη γλωσσών
- ➢ Αναφορές και αναλύσεις
- ➢ Αποκατάσταση
- ➢ Επεκτασιμότητα
- ➢ SBOM
- ➢ Προστασία από άγνωστες ευπάθειες
- ➢ Προστασία του repository που φιλοξενείται από επίθεση namespace confusion
- ➢ Ύποπτη αυτόματη καραντίνα (Suspicious auto-quarantine)
- ➢ Αυτοματοποιημένη αντικατάσταση έκδοσης για εξαρτήσεις
- ➢ Υποστήριξη για artifactory enterprise

- ❖ Τιμολόγηση

Sonatype Nexus Repository
- ➢ $145 ανά έτος ανά χρήστη
- ➢ On premise

Sonatype Air-Gapped Environment Nexus Repository
- ➢ $175 ανά έτος ανά χρήστη
- ➢ On premise

Sonatype Repository Firewall
- ➢ $224 ανά έτος ανά χρήστη
- ➢ On premise

Απαιτείται φόρος εγκατάστασης.
(Trustradius, χ.χ.)

47. Synopsys

Το Synopsys είναι ένας μακροχρόνιος πωλητής στον τομέα του σχεδιασμού, της επαλήθευσης και της πνευματικής ιδιοκτησίας για πυρίτιο και εισήλθε στην αγορά δοκιμών ασφαλείας εφαρμογών (AST) το 2014. Οι τρεις τομείς λύσεων AppSec του Synopsys καλύπτουν το φάσμα των αναγκών του DevSecOps με έξυπνη διαχείριση κινδύνων, ολοκληρωμένη ανάλυση λογισμικού και ολιστική ανάπτυξη προγραμμάτων. Καθώς ασχολείται κυρίως με την αλυσίδα εφοδιασμού του λογισμικού, το Synopsys προσφέρει μια σειρά εργαλείων AST, συμπεριλαμβανομένων των penetration testing, της δυαδικής

ανάλυσης (binary analysis) και της σάρωσης για την ασφάλεια API. Οι πελάτες μπορούν να αξιοποιήσουν τα υπάρχοντα εργαλεία και να orchestrate το AST για να ελαχιστοποιήσουν τις επιπτώσεις στους αγωγούς build και έκδοσης release.

❖ Χαρακτηριστικά

➢ Εργαλεία AST, συμπεριλαμβανομένων SCA, διαδραστικών και δυναμικών δοκιμών ανάλυσης και SAST.
➢ Δεδομένα συσχέτισης ευπαθειών που προσφέρουν διορατικότητα κινδύνου για την ιεράρχηση της αποκατάστασης (remediation).
➢ Αξιολόγηση του κινδύνου με αξιολογήσεις απειλών, ελέγχους ανοικτού κώδικα και εκπαίδευση σε θέματα ασφάλειας.
➢ Πόροι (resources) στρατηγικής και σχεδιασμού για την ανάπτυξη ενός προγράμματος ασφάλειας λογισμικού.
➢ Ενσωματώσεις DevSecOps όπως Jenkins, CloudBees, Jira, Docker, Artifactory και GitHub.

❖ Τιμολόγηση

➢ "Η τιμή αυτής της λύσης είναι διαπραγματεύσιμη, ανάλογα με το μέγεθος του οργανισμού."
➢ "Το Synopsys είναι αρκετά ακριβό."
➢ "Τα τέλη αδειοδότησης βασίζονται στον αριθμό των γραμμών κώδικα."

(Synopsys, χ.χ.)

48. Spectral

Το Spectral είναι μια λύση ασφάλειας με προτεραιότητα στον προγραμματιστή, η οποία αυτοματοποιεί τη διαδικασία προστασίας των μυστικών (secrets) κατά τη στιγμή του build, υπερ φορτώνοντας (supercharging) το CI/CD.

❖ Χαρακτηριστικά

➢ Μηχανή σάρωσης με τεχνητή νοημοσύνη.
➢ Ανίχνευση εκτεθειμένων μυστικών και λανθασμένων ρυθμίσεων ασφαλείας σε πραγματικό χρόνο.
➢ Υποστήριξη διαφόρων περιπτώσεων χρήσης ασφάλειας κώδικα και εύκολη ενσωμάτωση με αγωγούς CI/CD.

❖ Τιμολόγηση

"Ενας από τους λόγους για τους οποίους επιλέξαμε το Spectral έναντι άλλων προϊόντων είναι ότι το Spectral έχει χαμηλά ψευδώς θετικά αποτελέσματα, γεγονός που μας δίνει υψηλό συντελεστή εμπιστοσύνης και μας εξοικονομεί πολύτιμο χρόνο ανάπτυξης".

Παρέχεται δωρεάν.
(Eyal, 2023)

49. Qwiet AI preZero

Η πλατφόρμα preZero της Qwiet AI είναι ένας σαρωτής SAST. Πρόκειται για τον ακριβέστερο δυνατό τύπο σάρωσης που οδηγεί σε εξαιρετικά γρήγορες σαρώσεις με δραστικά μειωμένα ψευδώς θετικά αποτελέσματα. Η πλατφόρμα παρέχει επίσης ανάλυση SBOM, ανάλυση αδειών OSS και ανίχνευση μυστικών, όλα με απαράμιλλη ακρίβεια και ταχύτητα. Η πλατφόρμα σαρώνει επίσης το σύνολο των container που χρησιμοποιούνται από τις εφαρμογές, παρέχοντας μια γρήγορη και ακριβή εικόνα των κινδύνων τόσο εντός όσο και εκτός του κώδικα. Το preZero μπορεί εύκολα να ενσωματωθεί σε αγωγούς CI/CD για να παρέχει έγκαιρες, συχνές και επαναλαμβανόμενες σαρώσεις. Τέλος η πλατφόρμα είναι ένα εγγενές προϊόν SaaS, που δεν στέλνει ποτέ τον πηγαίο κώδικα στο cloud.

❖ Χαρακτηριστικά

➢ Χαμηλά ψευδώς θετικά αποτελέσματα
➢ Ιεράρχηση προτεραιοτήτων
➢ CPG (γράφημα ιδιοτήτων κώδικα)
➢ Τεχνητή νοημοσύνη
➢ Διατήρηση μυστικών
➢ Ασφάλεια κοντέινερ
➢ Ευφυής SCA
➢ Ενσωματώσεις
➢ Προσβασιμότητα
➢ Ακρίβεια
➢ Ταχύτητα

❖ Τιμολόγηση

Το Qwiet AI διαθέτει 3 πακέτα τιμολόγησης, από 0 έως 10.000 δολάρια. Διατίθεται επίσης δωρεάν δοκιμαστική έκδοση του Qwiet AI. Ας δούμε τα διάφορα πακέτα τιμολόγησης παρακάτω:

Πίνακας 4.6.13: *Τιμολόγηση Qwiet AI.*

Free	$0.00	25 Scans/μήνα, 5 εφαρμογές, έξυπνο SCA, προβολή της ροής των δεδομένων και εκπαίδευση με βάση το πλαίσιο
Personal	$175.00	Μονή άδεια που χρεώνεται κάθε μήνα 50 Scans/μήνα, 5 εφαρμογές, έξυπνο SCA, προβολή της ροής των δεδομένων και εκπαίδευση με βάση το πλαίσιο
Enterprise	Ξεκινάει από $10,000.00	Απεριόριστα Scans έξυπνο SCA, προβολή της ροής των δεδομένων και εκπαίδευση με βάση το πλαίσιο, πρόσβαση με API ενσωμάτωση Jira, SAML SSO και 10+ εφαρμογές

(G2, χ.χ.)

4.7 Η μεθοδολογία και τα αποτελέσματα της επιλογής των "καλύτερων" εργαλείων DevSecOps

Εξετάσαμε την αγορά λογισμικού DevSecOps και αναλύσαμε περισσότερο τις παραπάνω επιλογές με βάση τα ακόλουθα κριτήρια:

- Ενσωμάτωση με πλατφόρμες ανάπτυξης κώδικα για τον έγκαιρο εντοπισμό σφαλμάτων κωδικοποίησης.
- Μια βάση δεδομένων που έχει τις λύσεις για περισσότερες τυπικές ευπάθειες.
- Δυνατότητα συνεχούς εκτέλεσης και ενσωμάτωσης με το λογισμικό ανάπτυξης.
- Περιοδικές σαρώσεις για ζωντανά συστήματα.
- Προτάσεις για διορθώσεις που θα αποκαταστήσουν τα εντοπισμένα τρωτά σημεία.
- Μια δωρεάν δοκιμή ή ένα demo για μια ευκαιρία αξιολόγησης χωρίς κίνδυνο σπατάλης χρημάτων.
- Αξία για τα χρήματα του οργανισμού σε όλο τον κλάδο της ασφάλειας τόσο σε περιβάλλοντα ανάπτυξης όσο και στη διαχείριση λειτουργιών.
- Τις πιο αξιόλογες κριτικές από τους χρήστες τους. (Pickard, 2023)

Με αυτά τα κριτήρια επιλογής κατά νου, καταφέραμε να επιλέξουμε από τα παραπάνω εργαλεία DevSecOps που ελέγχουν για ευπάθειες και διορθώνουν αδυναμίες ασφαλείας τόσο κατά τη διάρκεια της ανάπτυξης όσο και στην παραγωγή και να καταλήξουμε σε αυτά που ένας οργανισμός πρέπει να εντάξει στις διαδικασίες του χωρίς δεύτερη σκέψη:

1. SonarQube
2. Checkmarx

3. Aquasecurity
4. Veracode
5. GitLab
6. Acunetix
7. ThreatModeler
8. Fortify WebInspect

Συνεπώς, μετά από μια εκτενή έρευνα από όλα τα εργαλεία που υπάρχουν στην αγορά καταλήξαμε σε αυτά τα 8. Κάθε ένα από αυτά τα εργαλεία ξεχώρισε, και όποιος οργανισμός σκέφτεται να αρχίσει να χρησιμοποιεί κάποιο από αυτά, σίγουρα δεν θα βγει χαμένος.

Συμπεράσματα

Συμπερασματικά, η μελέτη για τα εργαλεία DevSecOps έριξε φως στον κρίσιμο ρόλο που διαδραματίζουν στη σύγχρονη διαδικασία ανάπτυξης λογισμικού. Η έρευνα αυτή ανέδειξε τη σημασία της ενσωμάτωσης των πρακτικών ασφάλειας στις διαδικασίες ανάπτυξης και λειτουργίας, προωθώντας έτσι μια προληπτική και ολιστική προσέγγιση για τη διασφάλιση των ψηφιακών στοιχείων.

Μέσω αυτής της ολοκληρωμένης ανάλυσης διαφόρων εργαλείων DevSecOps, είναι προφανές ότι οι οργανισμοί μπορούν να βελτιώσουν σημαντικά την ικανότητά τους να εντοπίζουν, να μετριάζουν και να προλαμβάνουν τα τρωτά σημεία ασφαλείας καθ' όλη τη διάρκεια του κύκλου ζωής της ανάπτυξης λογισμικού. Τα ευρήματα υπογραμμίζουν την αναγκαιότητα της συνεχούς παρακολούθησης, των αυτοματοποιημένων δοκιμών και της συνεργασίας μεταξύ των ομάδων για την αποτελεσματική αντιμετώπιση των προβλημάτων ασφάλειας χωρίς να διακυβεύεται ο ρυθμός ανάπτυξης.

Επιπλέον, η έρευνα έδωσε έμφαση στην ανάγκη για προσαρμοσμένη επιλογή και ενσωμάτωση εργαλείων, καθώς οι διάφοροι οργανισμοί διαθέτουν μοναδική υποδομή, απαιτήσεις και προφίλ κινδύνου. Ενώ τα εργαλεία DevSecOps παρέχουν μια σταθερή βάση, η βέλτιστη εφαρμογή τους απαιτεί ευθυγράμμιση με τους οργανωτικούς στόχους και κατανόηση των συγκεκριμένων προκλήσεων που αντιμετωπίζουν οι ομάδες ανάπτυξης και ασφάλειας.

Καθώς η τεχνολογία συνεχίζει να εξελίσσεται, τα συμπεράσματα της παρούσας μελέτης υπογραμμίζουν ότι η υιοθέτηση πρακτικών και εργαλείων DevSecOps δεν θα πρέπει να θεωρείται απλή τάση αλλά στρατηγική πολιτική. Οι οργανισμοί που δίνουν προτεραιότητα στην ασφάλεια στο πλαίσιο των διαδικασιών ανάπτυξής τους είναι σε καλύτερη θέση, όχι μόνο στο να αποτρέψουν παραβιάσεις, αλλά και να οικοδομήσουν και να διατηρήσουν την εμπιστοσύνη με τους πελάτες, τους συνεργάτες και τα εμπλεκόμενα μέλη τους.

Συμπερασματικά, η παρούσα εργασία συμβάλλει στο να εξοικειωθούμε σχετικά με το DevSecOps παρέχοντας μια ολοκληρωμένη διερεύνηση των διαφόρων εργαλείων, των λειτουργιών τους και των πλεονεκτημάτων που προσφέρουν. Καθώς το ψηφιακό πεδίο γίνεται όλο και πιο πολύπλοκο και ευάλωτο σε απειλές, η ενσωμάτωση της ασφάλειας στη πρακτική DevOps δεν αποτελεί απλώς βέλτιστη πρακτική, αλλά αναγκαιότητα, και οι γνώσεις που συγκεντρώθηκαν εδώ, παρέχουν πολύτιμη καθοδήγηση για τους επαγγελματίες και τους οργανισμούς που περιηγούνται σε αυτόν τον δυναμικό κλάδο.

Βιβλιογραφία

- Alerta (χ.χ.). Alerta. Ανακτήθηκε 20 Ιουνίου 2023 από https://alerta.io/
- Amazon Web Services (χ.χ). What is DevSecOps?. Ανακτήθηκε 10 Ιουνίου 2023 από https://aws.amazon.com/what-is/devsecops/
- Aquasec (χ.χ.). DevSecOps Tools: 9 Ways to Integrate Security Into the SDLC. https://www.aquasec.com/cloud-native-academy/devsecops/devsecops-tools/
- Aquasec (χ.χ.). Security, Container Security & Serverless Security. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.aquasec.com/
- aws (χ.χ.). Skyhawk Security Reviews. Ανακτήθηκε 22 Ιουνίου 2023 από https://aws.amazon.com/marketplace/pp/prodview-oh3aksztuvu7i
- aws (χ.χ.). ThreatModeler Reviews. Ανακτήθηκε 28 Ιουνίου 2023 από https://aws.amazon.com/marketplace/pp/prodview-l3baiviio2pfc
- aws (χ.χ.). *Τιμολόγηση Checkmarx CxSAST*. Ανακτήθηκε 22 Ιουνίου 2023 από https://aws.amazon.com/marketplace/pp/prodview-mw6aigodqjyke?sr=0-1&ref_=beagle&applicationId=AWSMPContessa
- aws (χ.χ.). *Τιμολόγηση DoControl.* Ανακτήθηκε 22 Ιουνίου 2023 από https://aws.amazon.com/marketplace/pp/prodview-usguqibakmhj4
- aws (χ.χ.). *Τιμολόγηση IriusRisk.* Ανακτήθηκε 24 Ιουνίου 2023 από https://aws.amazon.com/marketplace/pp/prodview-lw45ujzidwkf2
- aws (χ.χ.). *Τιμολόγηση Prisma Cloud.* Ανακτήθηκε 26 Ιουνίου 2023 από https://aws.amazon.com/marketplace/pp/prodview-fhoptf6o4hcyu
- aws (χ.χ.). *Τιμολόγηση Skyhawk Security.* Ανακτήθηκε 22 Ιουνίου 2023 από https://aws.amazon.com/marketplace/pp/prodview-oh3aksztuvu7i
- aws (χ.χ.). *Τιμολόγηση ThreatModeler.* Ανακτήθηκε 28 Ιουνίου 2023 από https://aws.amazon.com/marketplace/pp/prodview-l3baiviio2pfc
- Caleb, D., & Kendra, L. (2022, Νοέμβριος 10). DevSecOps + IoT: A Buzzword Bonanza. https://tcblog.protiviti.com/2022/11/10/devsecops-iot-a-buzzword-bonanza/
- Caleb, D., & Kendra, L. (2022, Νοέμβριος 10). Επισκόπηση του κύκλου ζωής της παράδοσης του λογισμικού. [Εικόνα]. Protiviti. https://tcblog.protiviti.com/2022/11/10/devsecops-iot-a-buzzword-bonanza/
- Capterra (χ.χ.). Astra Pentest. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.capterra.com/p/236573/Astra-Pentest/
- Checkmarx (χ.χ.). Checkmarx CxSAST Reviews. Ανακτήθηκε 22 Ιουνίου 2023 από https://checkmarx.com/cxsast-source-code-scanning/
- CompareCamp (χ.χ.). CyberArk Review. Ανακτήθηκε 22 Ιουνίου 2023 από https://comparecamp.com/cyberark-review-pricing-pros-cons-features/
- Copado. (2022, Σεπτέμβριος 22). DevSecOps Use Cases Driving Enterprise Adoption. https://www.copado.com/devops-hub/blog/devsecops-use-cases-driving-enterprise-adoption

- Crozdesk (χ.χ.). Chef Reviews. Ανακτήθηκε 28 Ιουνίου 2023 από https://crozdesk.com/software/chef
- Crozdesk (χ.χ.). Splunk Enterprise Reviews. Ανακτήθηκε 28 Ιουνίου 2023 από https://crozdesk.com/software/splunk-enterprise
- Elastic (χ.χ.). Elasticsearch Platform. Ανακτήθηκε 22 Ιουνίου 2023 από https://www.elastic.co/
- Eyal, K. (2023, Απρίλιος 28). Top 15 DevSecOps Tools that Accelerate Development. https://spectralops.io/blog/top-15-devsecops-tools-that-accelerate-development/#:~:text=Key%20Features%20to%20Look%20for,to%20ensure%20a%20smooth%20workflow.
- Fossa. (2022, Ιανουάριος 18). 5 Must-Have DevSecOps Tools. https://fossa.com/blog/must-have-devsecops-tools/
- G2 (χ.χ.). Astra Pentest Features. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.g2.com/products/astra-pentest/features
- G2 (χ.χ.). Calico Reviews. Ανακτήθηκε 22 Ιουνίου 2023 από https://www.g2.com/products/calico-ai-calico/reviews
- G2 (χ.χ.). Checkmarx Reviews. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.g2.com/products/checkmarx/reviews
- G2 (χ.χ.). Contrast Security Reviews. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.g2.com/products/contrast-security-contrast-security/reviews#details
- G2 (χ.χ.). InsightVM Reviews. Ανακτήθηκε 26 Ιουνίου 2023 από https://www.g2.com/products/insightvm-nexpose/reviews#details
- G2 (χ.χ.). IriusRisk Reviews. Ανακτήθηκε 24 Ιουνίου 2023 από https://www.g2.com/products/iriusrisk/reviews
- G2 (χ.χ.). New Relic Reviews. Ανακτήθηκε 26 Ιουνίου 2023 από https://www.g2.com/products/new-relic/reviews#details
- G2 (χ.χ.). Qwiet AI Reviews. Ανακτήθηκε 29 Ιουνίου 2023 από https://www.g2.com/products/qwiet-ai/reviews
- G2 (χ.χ.). Red Hat Ansible Automation Platform Reviews. Ανακτήθηκε 26 Ιουνίου 2023 από https://www.g2.com/products/red-hat-ansible-automation-platform/reviews#details
- G2 (χ.χ.). SonarQube Reviews. Ανακτήθηκε 27 Ιουνίου 2023 από https://www.g2.com/products/sonarqube/reviews#details
- G2 (χ.χ.). *Τιμολόγηση CyberArk.* Ανακτήθηκε 22 Ιουνίου 2023 από https://www.g2.com/products/cyberark-identity/pricing
- G2 (χ.χ.). *Τιμολόγηση New Relic.* Ανακτήθηκε 26 Ιουνίου 2023 από https://www.g2.com/products/new-relic/pricing
- G2 (χ.χ.). *Τιμολόγηση Qwiet AI.* Ανακτήθηκε 29 Ιουνίου 2023 από https://www.g2.com/products/qwiet-ai/pricing
- G2 (χ.χ.). *Τιμολόγηση Red Hat Ansible Automation Platform.* Ανακτήθηκε 26 Ιουνίου 2023 από https://www.g2.com/products/red-hat-ansible-automation-platform/pricing
- G2 (χ.χ.). *Τιμολόγηση SonarQube.* Ανακτήθηκε 27 Ιουνίου 2023 από https://www.g2.com/products/sonarqube/pricing

- G2 (χ.χ.) Snyk Reviews. Ανακτήθηκε 27 Ιουνίου 2023 από https://www.g2.com/products/snyk/reviews
- GetApp (χ.χ.). Kiuwan Reviews. Ανακτήθηκε 24 Ιουνίου 2023 από https://www.getapp.com/security-software/a/kiuwan/
- GitLab (χ.χ). The DevSecOps Platform | GitLab. Ανακτήθηκε 22 Ιουνίου 2023 από https://about.gitlab.com/
- GitLab (χ.χ). *Τιμολόγηση GitLab.* Ανακτήθηκε 22 Ιουνίου 2023 από https://about.gitlab.com/
- Grafana (χ.χ.). Grafana Labs. Ανακτήθηκε 22 Ιουνίου 2023 από https://grafana.com/
- HCL Software (χ.χ.). AppScan. Ανακτήθηκε 20 Ιουνίου 2023 από https://help.hcltechsw.com/appscan/Welcome.html
- Ingalls, S. (2022, Μάρτιος 17). The 10 Best DevSecOps Tools. https://www.esecurityplanet.com/products/devsecops-tools/
- Jit (χ.χ.). DevSecOps Toolchain. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.jit.io/
- Moradov, O. (2022, Ιούνιος 6). DevSecOps vs DevOps: What's Different and How to Make the Move. https://brightsec.com/blog/devsecops-vs-devops/
- Muhammad, R. (2023, Ιούλιος 17). SDLC και μέτρα ασφαλείας για το κάθε βήμα. [Εικόνα]. Splunk. https://www.splunk.com/en_us/blog/learn/devsecops-concepts-principles.html
- Muhammad, R. (2023, Ιούλιος 17). The DevSecOps Beginner's Guide: 7 Concepts To Ace for DevSecOps Success. https://www.splunk.com/en_us/blog/learn/devsecops-concepts-principles.html
- Navdeep, S. G. (2023, Μάιος 16). A Guide to DevSecOps Tools and Continuous Security For an Enterprise. https://www.xenonstack.com/blog/devsecops-tools
- Navdeep, S. G. (2023, Μάιος 16). Ενσωμάτωση ασφάλειας στην ροή εργασίας συνεχούς παράδοσης. [Εικόνα]. Xenonstack. https://www.xenonstack.com/blog/devsecops-tools
- Owasp (χ.χ.). Threat Dragon version 2.0. Ανακτήθηκε 26 Ιουνίου 2023 από https://owasp.org/www-project-threat-dragon/docs-2/about/
- PeerSpot (χ.χ.). Checkmarx Reviews. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.peerspot.com/products/checkmarx-reviews
- PeerSpot (χ.χ.). Contrast Security Reviews. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.peerspot.com/products/contrast-security-assess-reviews#pricing
- PeerSpot (χ.χ.). CyberRes Fortify Reviews. Ανακτήθηκε 22 Ιουνίου 2023 από https://www.peerspot.com/products/fortify-static-code-analyzer-reviews#reviews-container
- PeerSpot (χ.χ.). Fortify WebInspect Reviews. Ανακτήθηκε 22 Ιουνίου 2023 από https://www.peerspot.com/products/fortify-webinspect-reviews
- PeerSpot (χ.χ.). HCL AppScan Reviews. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.peerspot.com/products/hcl-appscan-reviews

- PeerSpot (χ.χ.). IBM X-Force Exchange Reviews. Ανακτήθηκε 29 Ιουνίου 2023 από https://www.peerspot.com/products/ibm-x-force-exchange-reviews
- PeerSpot (χ.χ.). Invicti Reviews. Ανακτήθηκε 24 Ιουνίου 2023 από https://www.peerspot.com/products/invicti-reviews
- PeerSpot (χ.χ.). Kubernetes Reviews. Ανακτήθηκε 28 Ιουνίου 2023 από https://www.peerspot.com/products/kubernetes-reviews
- PeerSpot (χ.χ.). OWASP Zap Reviews. Ανακτήθηκε 26 Ιουνίου 2023 από https://www.peerspot.com/products/owasp-zap-reviews
- PeerSpot (χ.χ.). Palo Alto Networks NG Firewalls Reviews. Ανακτήθηκε 26 Ιουνίου 2023 από https://www.peerspot.com/products/palo-alto-networks-ng-firewalls-reviews#pricing
- PeerSpot (χ.χ.). Parasoft SOAtest Reviews. Ανακτήθηκε 26 Ιουνίου 2023 από https://www.peerspot.com/products/parasoft-soatest-reviews
- PeerSpot (χ.χ.). Prisma Cloud Reviews. Ανακτήθηκε 26 Ιουνίου 2023 από https://www.peerspot.com/products/prisma-cloud-by-palo-alto-networks-reviews
- PeerSpot (χ.χ.). Veracode Reviews. Ανακτήθηκε 28 Ιουνίου 2023 από https://www.peerspot.com/products/veracode-reviews
- Pickard, S. (2023, Ιούνιος 7). The 10 Best DevSecOps Tools. https://www.pcwdld.com/best-devsecops-tools
- Rosencrance, L. (2022, Νοέμβριος). DevSecOps. https://www.techtarget.com/searchitoperations/definition/DevSecOps
- SelectHub (χ.χ.). Micro Focus Reviews. Ανακτήθηκε 24 Ιουνίου 2023 από https://www.selecthub.com/p/ppm-software/micro-focus/
- Shlomi, L. (2022, Οκτώβριος 24). Micro Focus Pricing Plans. https://www.itqlick.com/serena-business-manager/pricing
- Sourceforge (χ.χ.). Mend.io Reviews. Ανακτήθηκε 26 Ιουνίου 2023 από https://sourceforge.net/software/product/Mend.io/
- Sourceforge (χ.χ.). SOOS Reviews. Ανακτήθηκε 27 Ιουνίου 2023 από https://sourceforge.net/software/product/SOOS/
- Sourceforge (χ.χ.). StackStorm Reviews. Ανακτήθηκε 27 Ιουνίου 2023 από https://sourceforge.net/software/product/StackStorm/
- Stackshare (χ.χ.). Kibana Reviews. Ανακτήθηκε 24 Ιουνίου 2023 από https://stackshare.io/kibana#description
- Stackshare (χ.χ.). Trivy Reviews. Ανακτήθηκε 27 Ιουνίου 2023 από https://stackshare.io/trivy
- Sudip, S. (2023, Ιούλιος 18). Your Guide to DevSecOps Automation. https://crashtest-security.com/devsecops-automation/
- Synopsys (χ.χ.). Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. Ανακτήθηκε 29 Ιουνίου 2023 από https://www.synopsys.com/
- Synopsys (χ.χ.). What Is DevSecOps and How Does It Work?. Ανακτήθηκε 10 Ιουνίου 2023 από https://www.synopsys.com/glossary/what-is-devsecops.html
- Thinksys. (2023, Μάρτιος 1). An Overview of DevSecOps Tools to Secure Your Applications in 2023. An Overview Of DevSecOps Tools To Secure Your Applications In 2023 (thinksys.com)

- Tigera (χ.χ.). 16 Amazing DevSecOps Tools to Shift Your Security Left. Ανακτήθηκε 10 Ιουνίου 2023 από https://www.tigera.io/learn/guides/devsecops/devsecops-tools/
- Trustradius (χ.χ.). Acunetix by Invicti. Ανακτήθηκε 20 Ιουνίου 2023 από https://www.trustradius.com/products/acunetix/reviews#overview
- TrustRadius (χ.χ.). Codacy Reviews. Ανακτήθηκε 22 Ιουνίου 2023 από https://www.trustradius.com/products/codacy/reviews#overview
- TrustRadius (χ.χ.). HashiCorp Vault Reviews. Ανακτήθηκε 22 Ιουνίου 2023 από https://www.trustradius.com/products/hashicorp-vault/reviews
- Trustradius (χ.χ.). List of Top DevSecOps Tools 2023. Ανακτήθηκε 10 Ιουνίου 2023 από https://www.trustradius.com/devsecops
- Trustradius (χ.χ.). Sonatype Platform Reviews. Ανακτήθηκε 29 Ιουνίου 2023 από https://www.trustradius.com/products/sonatype-nexus-platform/reviews#pricing
- TrustRadius (χ.χ.). *Τιμολόγηση CyberArk.*. Ανακτήθηκε 22 Ιουνίου 2023 από https://www.trustradius.com/products/codacy/reviews#overview
- Will, K. (2021, Σεπτέμβριος 16). The 7 Principles of DevSecOps Automation. https://anchore.com/blog/the-7-principles-of-devsecops-automation/
- William. (2022, Οκτώβριος 6). DevOps vs DevSecOps: The debate. https://www.clickittech.com/devops/devops-vs-devsecops/#h-owasp-top-ten-methodology