Check Point
SOFTWARE TECHNOLOGIES LTD

ОБЛАКА, КОНТЕЙНЕРЫ, ЛЯМБДЫ

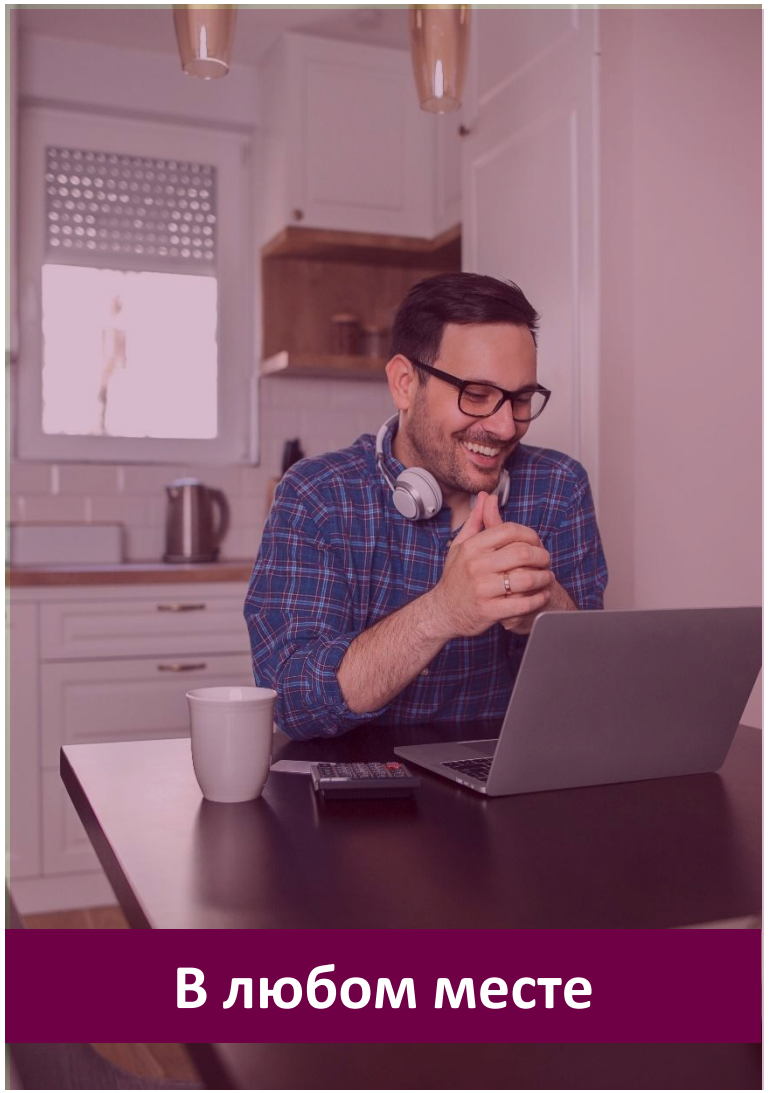
как выглядит информационная безопасность современных технологий и как легко ее обеспечить в публичных облаках

Денисов Валерий | Архитектор безопасности в облаках, Check Point

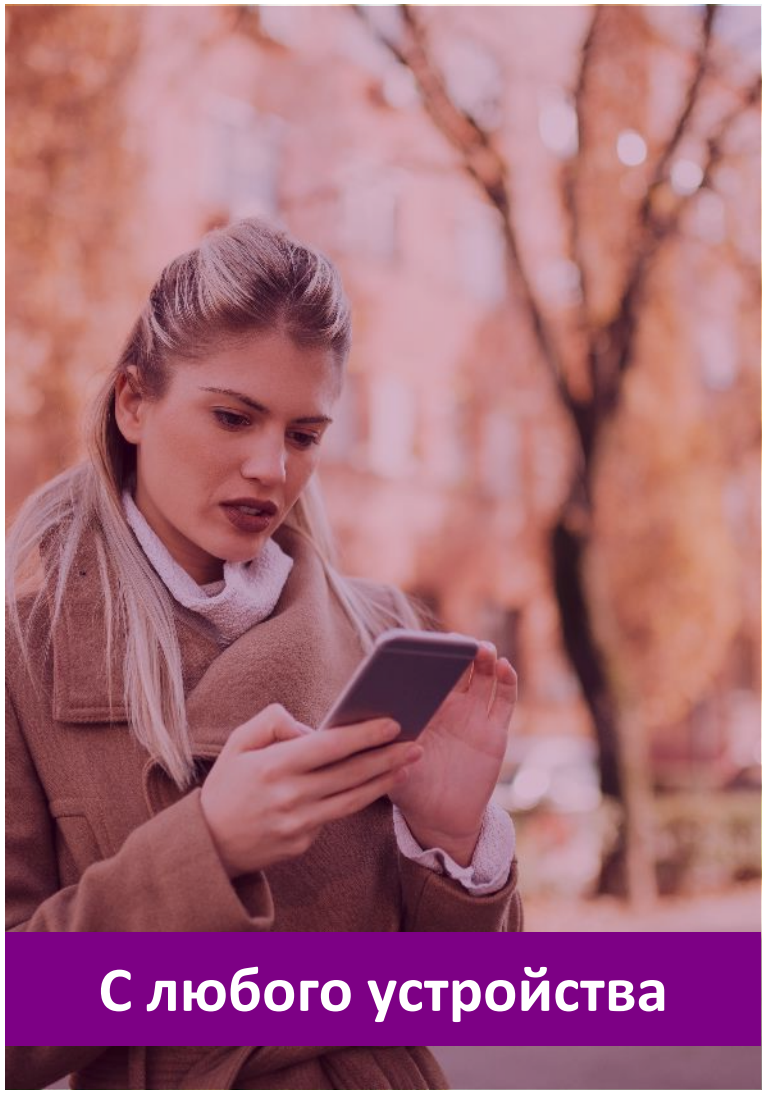
vdenisov@checkpoint.com

t.me/chkpstar

РАБОТАЕМ ОТКУДА УГОДНО И КАК УГОДНО



В любом месте

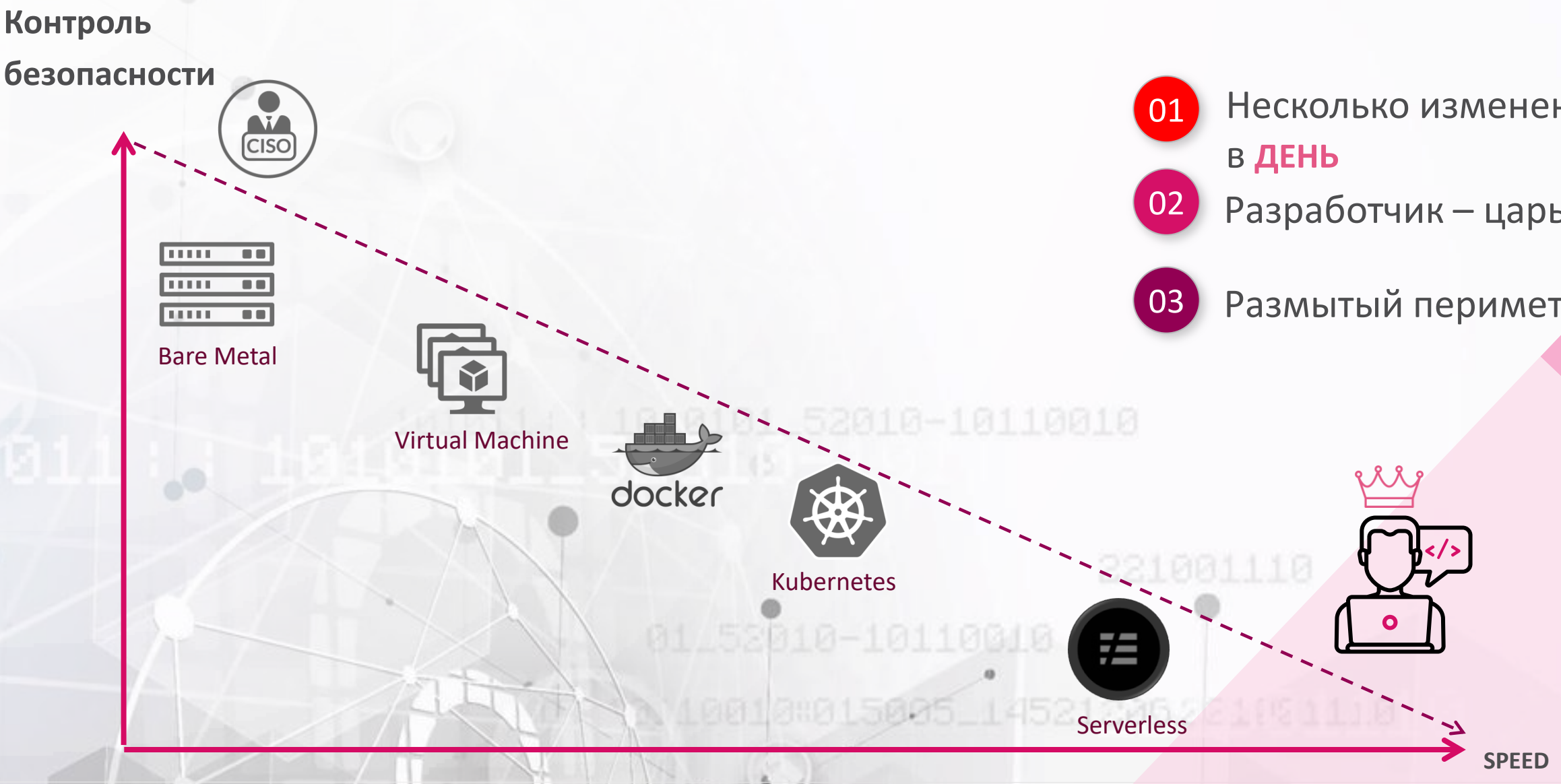


С любого устройства

Доступ к приложениям

©2021 Check Point Software Technologies Ltd.

СЛОЖНО ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ



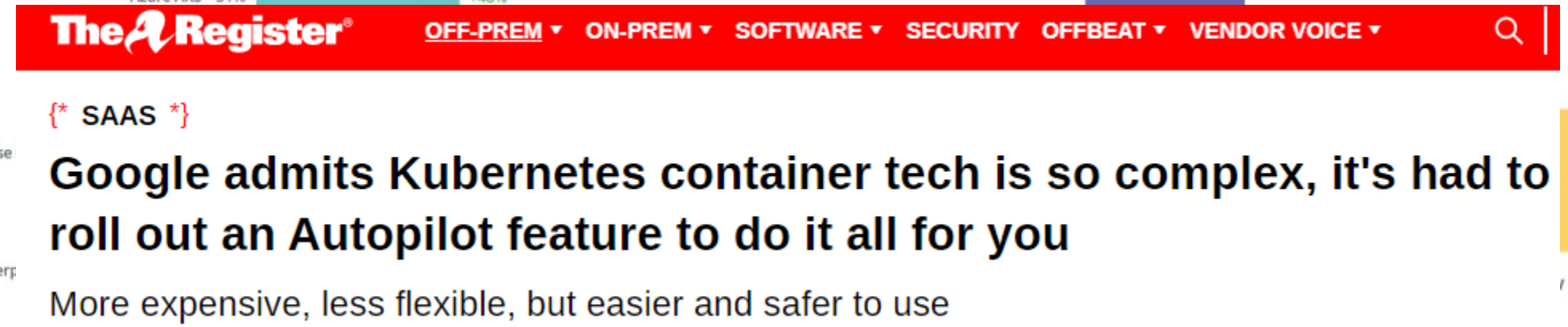
01 Несколько изменений в **ДЕНЬ**

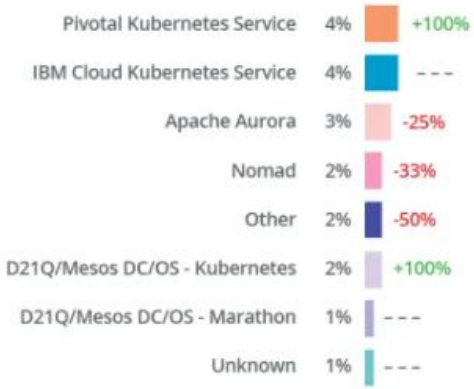
02 Разработчик – царь горы

03 Размытый периметр

©2021 Check Point Software Technologies Ltd.

Все больше контейнеров в продуктиве





https://www.stackrox.com/kubernetes-adoption-security-and-market-share-for-containers

©2021 Check Point Software Technologies Ltd.

Новые технологии – старые проблемы

KUBERNETES / SECURITY

Kubernetes ‘Billion Laughs’ Vulnerability Is No Laughing Matter

9 Oct 2019 8:11am, by Jack Wallen

CVE List | CNAs | WGs | Board | About | News & Blog

Common Vulnerabilities and Exposures

NVD Go to for: CVSS Scores, CPE Info, Advanced Search

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 127996

HOME > CVE > CVE-2019-11253

Printer-Friendly View

CVE-ID

CVE-2019-11253 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Improper input validation in the Kubernetes API server in versions v1.0-1.12 and versions prior to v1.13.12, v1.14.8, v1.15.5, and v1.16.2 allows authorized users to send malicious YAML or JSON payloads, causing the API server to consume excessive CPU or memory, potentially crashing and becoming unavailable. Prior to v1.14.0, default RBAC policy authorized anonymous users to submit requests that could trigger this vulnerability. Clusters upgraded from a version prior to v1.14.0 keep the more permissive policy by default for backwards compatibility.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Кладем кластер кубернетеса в три шага:

1. Шлем вредоносную конфигурацию (YAML или JSON)
2. Кластер начинает потреблять все ресурсы CPU
3. Кластер падает и становится неактивным ☹

А еще можно сделать MiTM в самом кластере и многое другое: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=kubernetes

©2020 Check Point Software Technologies Ltd.

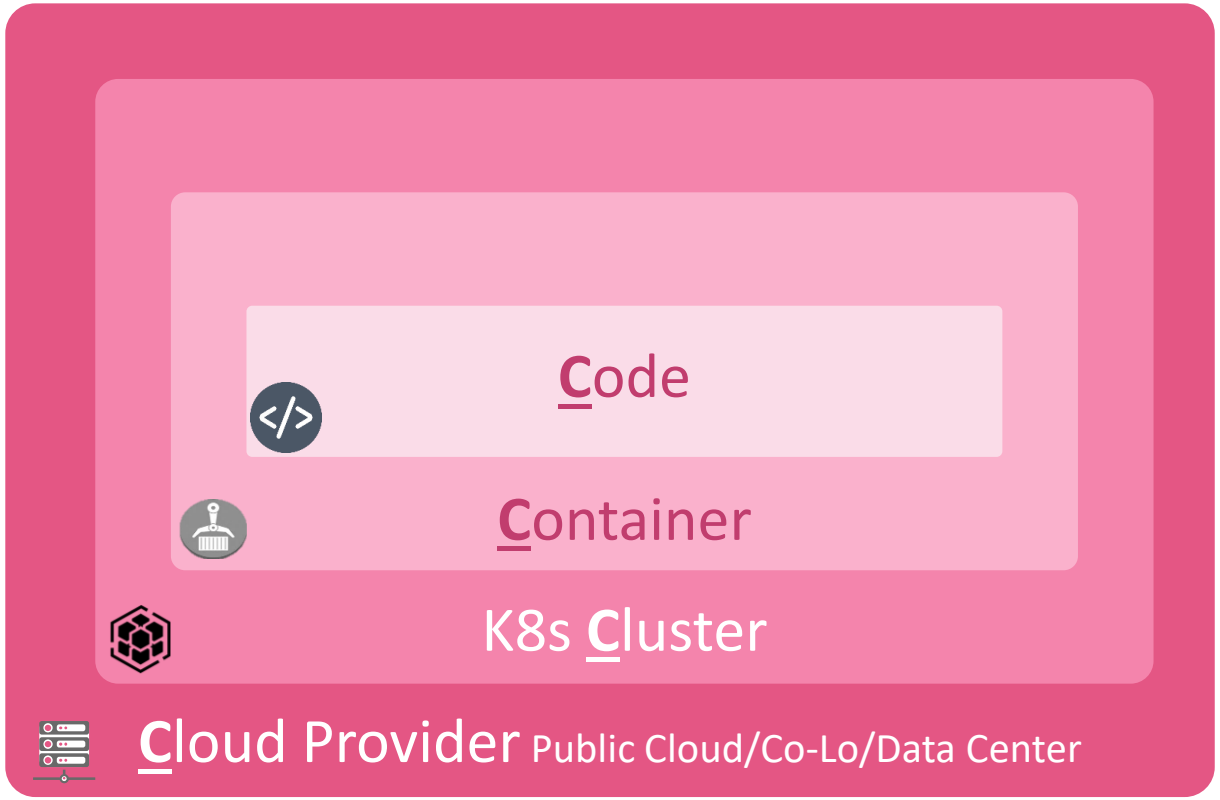
Модель «4С» – Концепция защиты облаков

Модель защиты «4С»

Эшелонированный подход:

- Защищаем облачный периметр
- Сами ресурсы внутри облака
- Контейнеры/приложения
- Сам код этих приложений

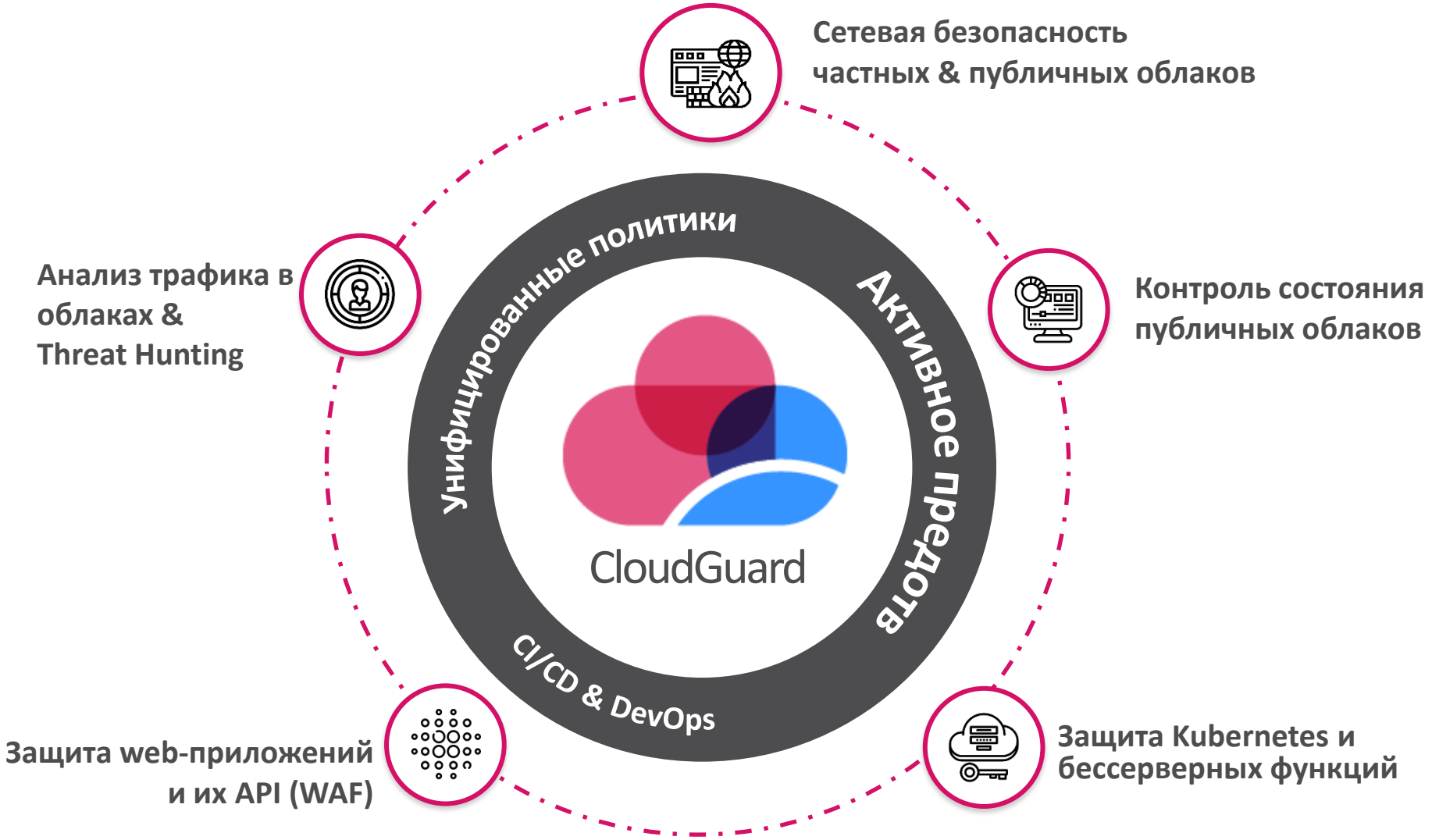
Дизайн защиты: Данный подход позволяет обеспечить безопасность на всех этапах жизни современных сервисов



https://kubernetes.io/docs/concepts/security/overview/

©2021 Check Point Software Technologies Ltd.

ЕДИНОЕ РЕШЕНИЕ ЗАЩИТЫ ЛЮБЫХ ОБЛАКОВ



©2020 Check Point Software Technologies Ltd.

Безопасная миграция в любое облако

С CHECK POINT

- API – First
- Бесшовная
- Безопасность
- В любом облаке

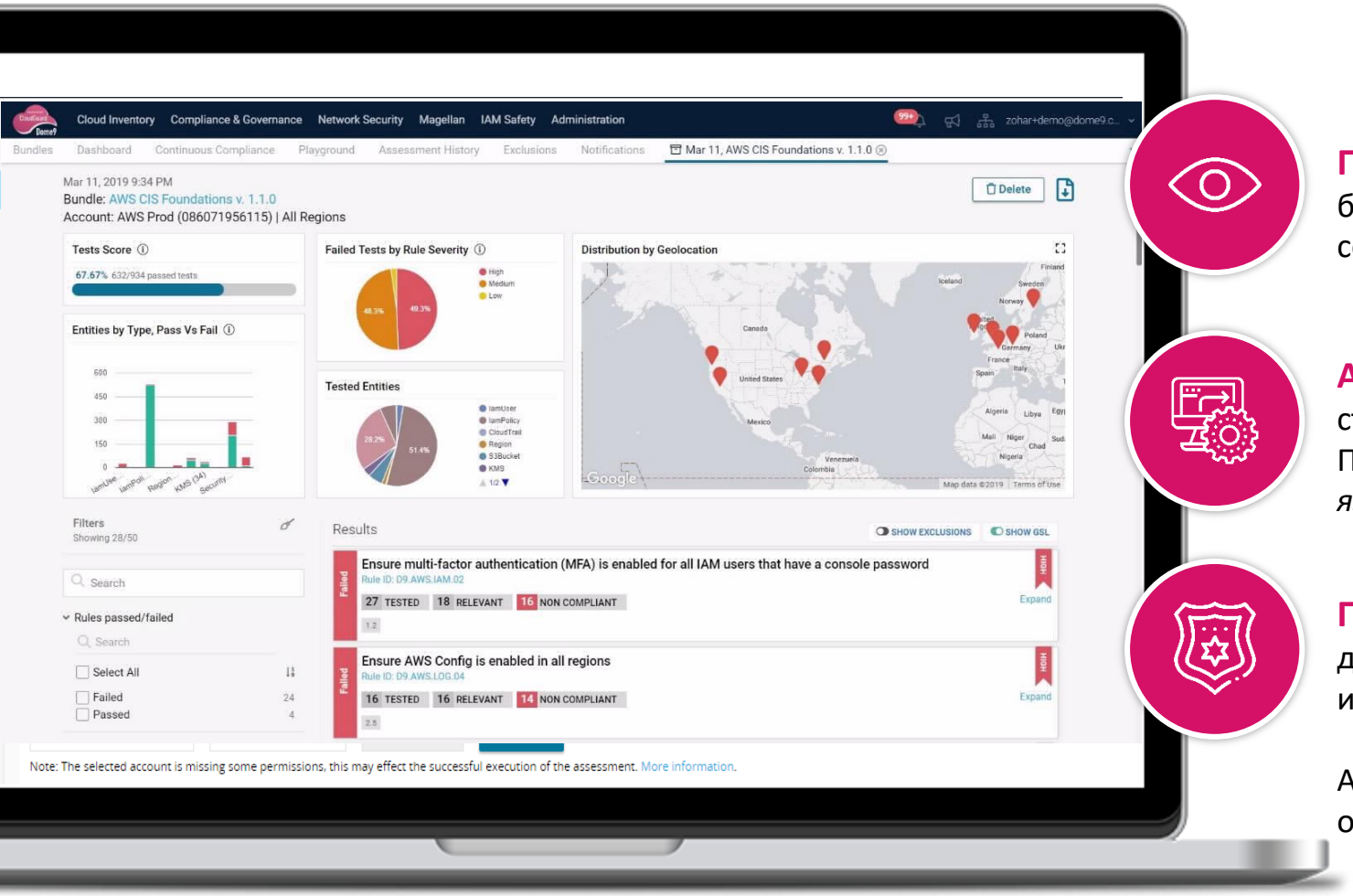
CloudGuard Native

©2021 Check Point Software Technologies Ltd.

Контроль настроек в облаке

4C - Cloud

Оценка безопасности, уровней доступа и политик для публичных облаков и контейнеров



Полный контроль над всеми серверами, функциями, бакетами, политиками безопасности, IAM, виртуальными сетями и аккаунтами в публичных облаках и K8S.

Автоматические отчеты на соответствие отраслевых стандартов защиты и лучших практик в ИБ.
Простая и понятная настройка правил на «*человеческом языке*»

Предотвращение *кражи* учетных *записей*, неавторизованного доступа к облакам, некорректных или злонамеренных изменений настроек безопасности.

Автоматическое исправление и коррекция политик и настроек облачных ресурсов

©2021 Check Point Software Technologies Ltd.

Защита облачных функций

4C - Cloud

Автоматическая защита Runtime

- ✓ Постоянное сканирование на поиск уязвимостей и прав доступа
- ✓ Визуализация взаимодействия с другими сервисами AWS
- ✓ Профилирование и whitelisting

Анализ уязвимостей в коде и слишком широких прав доступа

Feb 6, 2020 1:15 AM | PermissiveRole | Unassigned

Alert Title: PermissiveRole

Execution Role Arn: arn:aws:iam::293247823395:role/shalommSlackChatBotRole

Alert Description: Your function greatreads-slack-chat-bot-shalomm:$LATEST has redundant permissions. By statically analyzing your code , we could not find a path where your code requires these operations, Setting unnecessary permissions

Show more

Suggested Role Remediation: SHOW

Redundant Permissions

Alert ID: 6103ec43-7454-4b91-b657-5aeacfbe4610

Cloud Account: * Removed 'Aws' Cloud Account (01f27353-43db-4a9b-b375-a71105f3bf45)*

Region: N. Virginia

Finding Information

Entity Type

Assign User

Comments: No comments are available

Suggested Role Remediation

Search

```
Version: 2012-10-17
Statement:
  0:
    Action:
      0: s3:PutObject
    Resource:
      0: *
    Effect: Allow
    Sid: ProtegoGeneratedа9edf298
  1:
    Action:
      0: dynamodb:PutItem
    Resource:
      0: arn:aws:dynamodb:us-east-1:293247823395:table/shalomm-greatread-slack-messages
    Effect: Allow
    Sid: ProtegoGenerated50db6173
  2:
    Action:
      0: logs:CreateLogGroup
    Resource:
      0: arn:aws:logs:us-east-1:293247823395:log-group:/aws/lambda/*:*:*
    Effect: Allow
    Sid: ProtegoGenerated44bd56e8
  3:
    Action:
      0: logs:CreateLogStream
      1: logs:PutLogEvents
    Resource:
      0: arn:aws:logs:us-east-1:293247823395:log-group:/aws/lambda/greatreads-slack-chat-bot-shalomm:*:*
    Effect: Allow
    Sid: ProtegoGenerated26bbf0cc
```

Рекомендации по изменению ролей и прав доступа

Feb 13, 2020 8:56 AM | workshop_1... (468936707523) | Serverless | ApiEvent | DVSA-ORDER-MANAGER

Alert Title: Alert

ApiEvent

What Is This?
Protego has detected an attempt to call an unauthorized service api, which is not part of the function's approved access list.

What Could It Be?
Someone tried to use the function to access other cloud resources in the account. A successful attack could result in sensitive data leakage, modification of data or even in a complete cloud resource takeover, depending on the functions' permissions.

How Was This Detected?

What Was Detected?

Service: cognito-idp

Which Resources Are Involve

Function: arn:aws:lambda:us

862c3f5d-2467-49d8-915c-01fa1dafd114

Cloud Account: workshop_13_468936707523 (468936707523)

Region: N. Virginia

Finding Information

Анализ вызовов API и сторонних ресурсов

What is this?

Protego has detected a Code Injection attack.

Code Injection ([CWE-94](https://cwe.mitre.org/data/definitions/94.html)) is the general term for attack types which consist of injecting code that is then interpreted/executed by the application, limited by the functionality of the injected language itself. This type of attack exploits poor handling of untrusted data and is usually made possible due to lack of proper input/output data validation. Command injection consists of leveraging code to execute commands, usually within the context of a shell.

What Could It Be?
Someone tried to execute arbitrary code in the function. A successful attack can compromise the application confidentiality, integrity, availability and/or loss accountability.

How Was This Detected?
Protego FSP observed a suspicious data that matched a pattern which identifies

Cloud Account: * Removed 'Aws' Cloud Account (01f27353-43db-4a9b-b375-a71105f3bf45)*

Region: N. Virginia

Finding Information

Профилирование функций на базе их поведения

Анализ трафика внутри публичного облака/кластера K8S

4C - Cluster

CLOUDGUARD NATIVE

vdenisov+demo@checkpoint.com

CHECK POINT INFINITY PORTAL

OVERVIEW
EVENTS
ASSETS
POSTURE MANAGEMENT
NETWORK SECURITY
IDENTITY
WORKLOAD PROTECTION
INTELLIGENCE
SHIFTLEFT
SETTINGS
RESOURCES

Welcome

Visibility
Configuration Explorer
Traffic Explorer
IP Addresses

Policy
Security Groups
Access Leases

NETWORK

Explore your network and manage your network security. explore your traffic, browse enriched logs, set access leases, and monitor active leases.

Visibility
Your toolbox for inspecting the network and traffic

Configuration Explorer
Visually inspect your network configuration

Traffic Explorer
Explore your actual traffic

Traffic Logs
Investigate enriched traffic logs

IP addresses
View and define IP addresses in the system

Policy
View and manage your network security

Security Groups
View and manage security groups

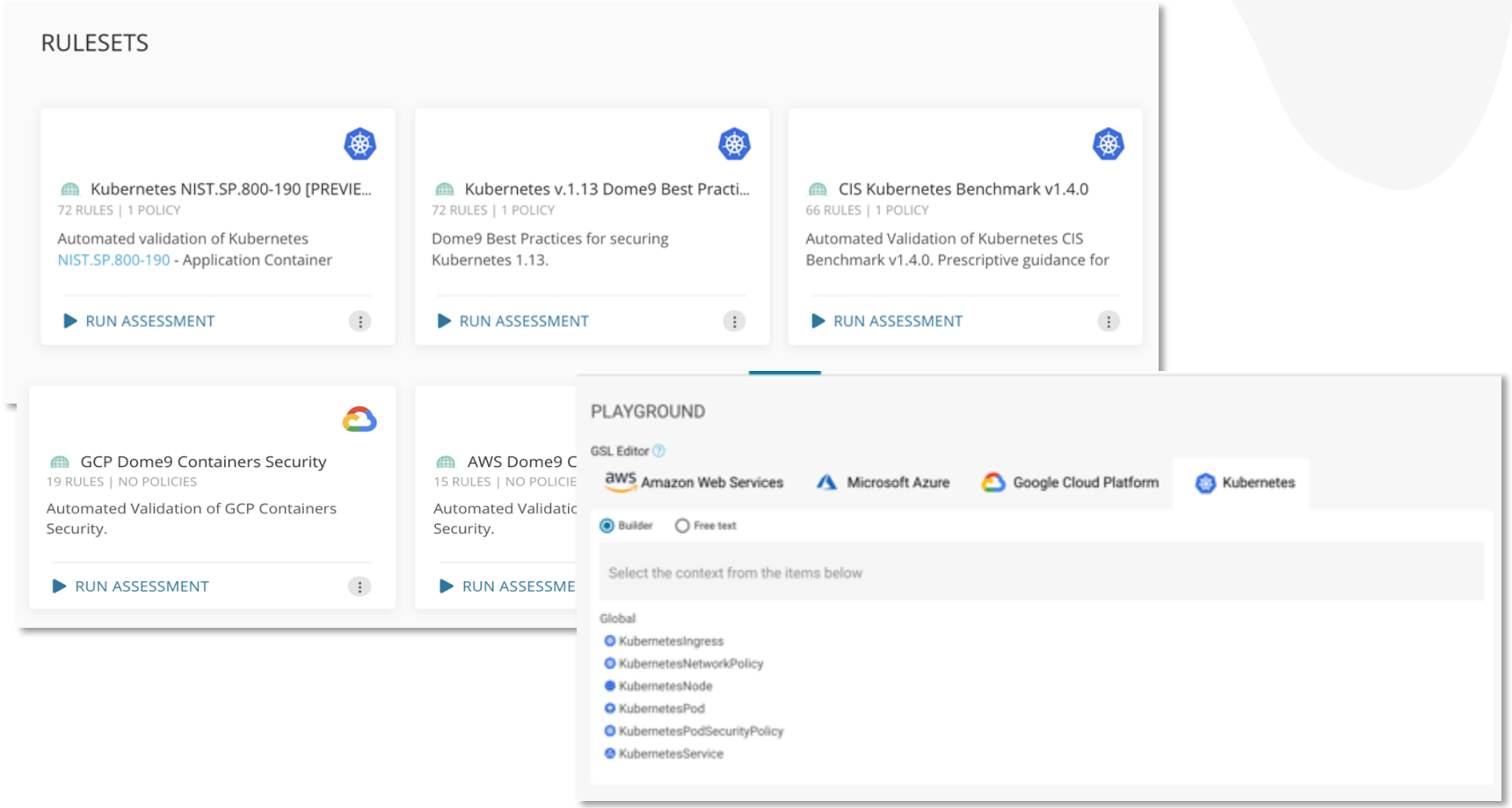
Access Leases
Define access groups and get access leases

Active Leases
View leases that are currently active

ЗАЩИТА КОНТЕЙНЕРОВ KUBERNETES

Анализ соответствия контейнеров

- ✓ Сотни готовых правил для оценки соответствия промышленным стандартам, например, **NIST 800-190** и **CIS Benchmarks для K8S**
- ✓ Постоянный анализ кластеров kubernetes и образов контейнеров на наличие уязвимостей и их конфигураций



©2021 Check Point Software Technologies Ltd.

Обнаружение критических уязвимостей в K8S

CLOUDGUARD NATIVE

vdenisov+demo@checkpoint.com

CHECK POINT INFINITY PORTAL

OVERVIEW
EVENTS
ASSETS
POSTURE MANAGEMENT
NETWORK SECURITY
IDENTITY
WORKLOAD PROTECTION
INTELLIGENCE
SHIFTLEFT
SETTINGS
RESOURCES

Welcome

Assets
Serverless Functions
Containers

Image Assurance (Preview)
Images
Vulnerability

CI-CD Tool

Admission Control (Preview)
Rulesets
Policies
GSL Builder

Runtime Protection (Preview)
Pod Groups

WORKLOADS

Serverless function and container security

Overview
View your workload security status, findings, and events

Containers Status
See an overview of the container security status

Serverless Status
See an overview of the serverless functions security status

Environments
Manage and onboard containers

Clusters
Manage your clusters

Cluster Onboarding
Onboard a cluster

Assets
View workloads protected assets

Serverless Functions

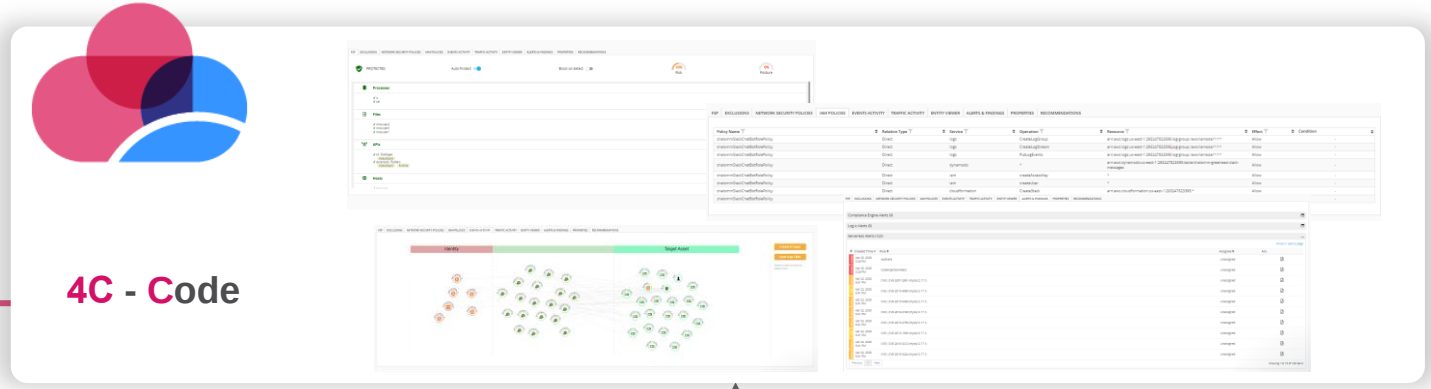
Containers

Images

Защита процесса разработки

Интеграция в CI/CD

1. Сканируем исходный код
2. Проверяем шаблон Terraform
3. Проверяем собранные контейнеры, фильтруем WEB-запросы (WAF)

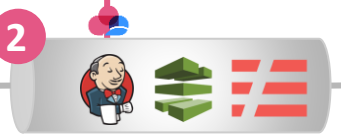


Разработчики

1

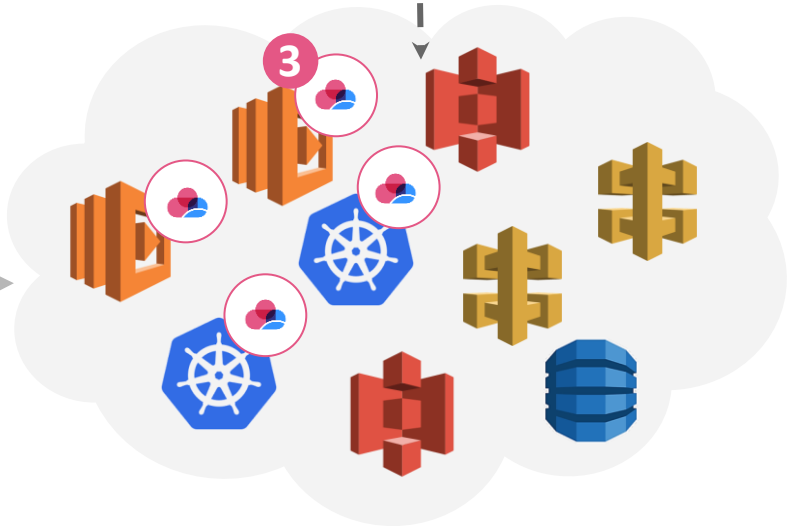
SourceGuard

2



Интегрируем плагины с CI/CD

3

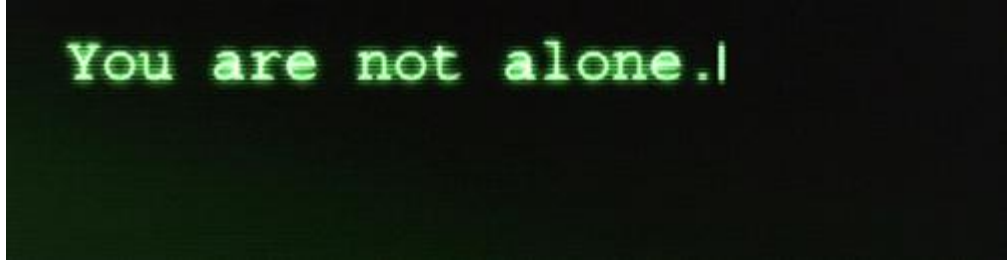


Современные приложения

Java, Node, Python, C Sharp

©2021 Check Point Software Technologies Ltd.

ЕЩЕ ПОЧТИ STACKOWERFLOW



- Система форумов/блогов CheckMates

community.checkpoint.com

CheckMates CODEHUB

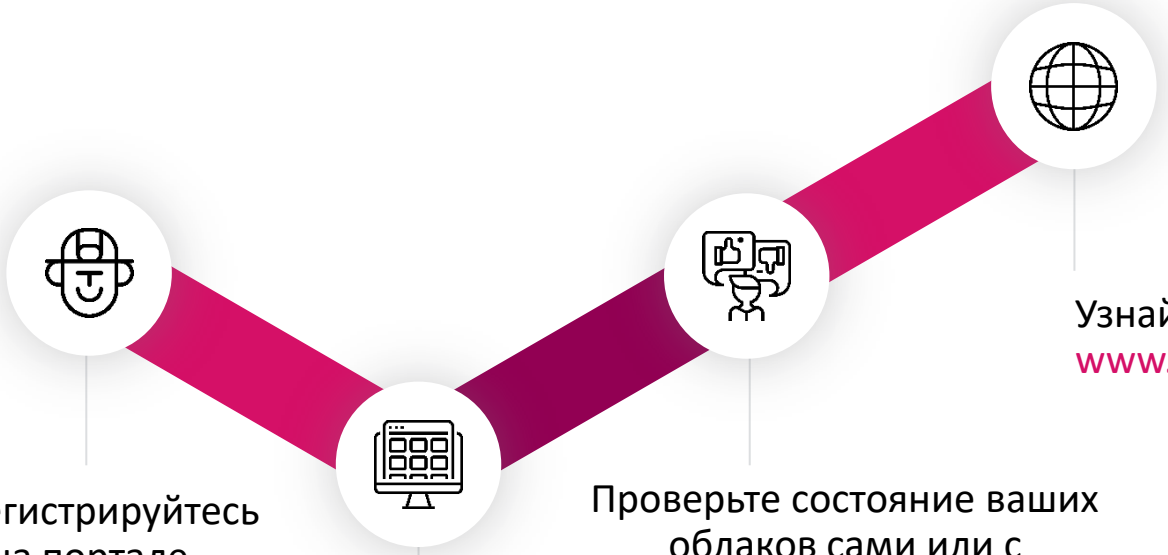
- Неофициальный Telegram-чат/канал

@chkpchat

@chkpstar

©2021 Check Point Software Technologies Ltd.

КАК ПРОТЕСТИРОВАТЬ CLOUD NATIVE (DOME9)?



Зарегистрируйтесь на портале **https://secure.dome9.com/v2/**

Зарегистрируйте аккаунт в Infinity Portal

Проверьте состояние ваших облаков сами или с помощью инженеров Check Point

Узнайте о защите облаков: www.checkpoint.com/cloud

CloudGuard Native

©2021 Check Point Software Technologies Ltd.

Check Point
SOFTWARE TECHNOLOGIES LTD

СПАСИБО!

CLOUD & DIGITAL
TRANSFORMATION

Денисов Валерий | Инженер, Check Point

vdenisov@checkpoint.com

t.me/chkpstar

@chkpbot