CLOUD SECURITY GUARDRAIL WORKSHOPS

Computacenter

COMPANIES ARE INCREASINGLY MOVING THEIR SERVICES TO THE PUBLIC CLOUD

In the era of digitization, companies are increasingly moving their services to the Public cloud. Cloud based offerings help organisations to give their customers more immediate and scalable access to their services. Cloud offerings are so prevalent now that customers expect to be able to consume services in this way, and actually not being able to offer cloud-based delivery can impact reputation.

Typically, such services are built on public cloud platforms such as AWS and Microsoft Azure. Whilst such platforms provide huge benefit to organisations and their customers, it is increasingly important that the appropriate security controls are implemented. The need to move quickly to bring new products to market that provide competitive advantages means that developers often move very quickly and are under pressure. The speed of development combined with a lack of cloud security expertise often results in engineers and developers bypassing certain security and compliance policies, and this can lead to things like data breaches. To help minimize the security risks associated with using Public cloud it is important for organisations to apply security configuration guidelines, often called Guardrails.

Computacenter has been working with our customers to develop Guardrails for their companies for several years. The Guardrails are developed jointly in workshops with the client for adoption by customer developers. Computacenter uses a set of rules based on industry best practice and our own experience, collected in the delivery of numerous cloud projects. However, we are also able to develop rulesets based on standards such as CSA, ENISA or BSI C5.

In order to understand the type and scope of the required Guardrails, Computacenter will first review previous security policies together with the customer and identify any gaps or difficulties that might hinder an effective cloud usage. Computacenter will then develop a roadmap to correct any non-conformities with Best-practice Standards.

The Guardrails are generic and can be used for different cloud platforms. Computacenter uses a framework that combines the international standard of the European Union Agency for Network and Information Security (ENISA) and the C5 catalogue of the German Federal Office for Information Security (BSI) as the basis for developing the guardrails.

CONTAINERS

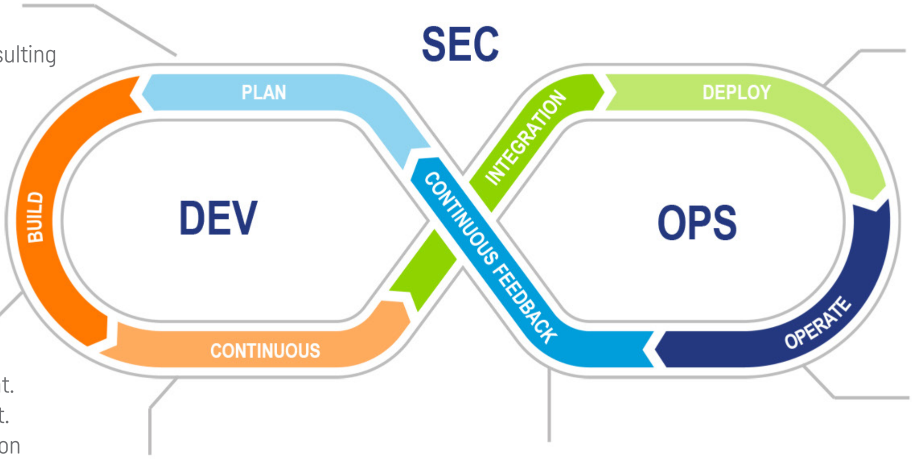
The increasing use of containers in today's datacentres also creates more attack vectors which could affect the safety of an environment.

The increasing use of containers in today's datacentres also creates more attack vectors which could affect the safety of an environment. Guardrails must therefore also be developed to protect this additional technology layer against attacks and malicious code. To this end, Computacenter has developed a multi-layered security approach, which enables comprehensive protection even at container level. Computacenter has expanded the its baseline framework, referred to above, for this purpose. The existing security categories have been redistributed and assigned to the extended layers. This means that Computacenter has a comprehensive approach to defining both security guidelines and guardrails that can also be integrated into application development. The requirements of software development and the associated working methods are also taken into account, as is the increased level of automation, by fully automating the security solutions used.

Security issues that are addresses with this approach include:

- How can security products be provided automatically and how can they continuously adapt to dynamic environments?
- How can security be integrated into CI / CD pipelines?
- Who has access to code repositories?
- How is the traffic between containers controlled?
- What log data from the container level can be used for security monitoring?
- What do incident response processes look like in containers?
- What kind of role model is there for users in orchestration solutions such as Ansible, Openshift or Kubernetes?

- Cloud Security Framework
- Threat Modelling
- Processes & Methods
- Data Classification consulting



- Load Balancing
- Web Application Firewall
- Nano Segmentation

- Network Security
- Identity & Lifecycle Mgmt.
- Privileged Account Mgmt.
- Storage & Data Encryption
- Access Management

- Embedded CI/CD Scanning
- Secret Management
- Software Signing
- Automated Security Solutions

- Vulnerability Management
- Log Management
- Audit & Compliance
- Penetration Testing
- Risk Assessments

- Runtime Protection
- DDoS Protection
- Cyberdefence Services

Figure 1 - Computacenter's multi-layered security for the DevOps lifecycle

OVERVIEW

To develop the initial Security Guidelines, workshops are held with Computacenter security Consultants and appropriate customers representatives. Computacenter will host and facilitate the workshop, and depending on the platform used, the following guidelines can be developed:

- Guidelines for SaaS services focusing on MS 0365
- Guidelines for IaaS / PaaS services
- Guidelines for DevOps environments

The guidelines to be drawn up are largely generic in order to ensure the largest possible coverage of all cloud platforms in scope of each type. Occasionally, the specific characteristics of a particular service must be also be included to ensure effective protection. Once drafted the guidelines can be used to discuss specific security measures and solutions and then to develop the technical security concepts required to develop the Guardrails.

The workshops are planned to complete in a day, running from 10:00am to 16:00am and a Computacenter facilitator will guide the conversation. If the content cannot be fully developed in one day, a second appointment can be arranged, which will be charged separately. Alternatively, any open points can be clarified afterwards in a direct discussion with the person responsible. The effectiveness of the workshops increases with the participation of the participants.

TYPICAL AGENDA

- Introductions and overview of agenda
- Presentation of Computacenter Cloud Security Framework, process model, security categories and best practices catalogue.
- Review of the best practices catalogue and identification of the relevant security categories
- Deepening of relevant security categories and development of the Guardrails
- Determine the next steps

WORKSHOPS

WORKSHOP OPTION 1 - GUIDELINES FOR SAAS SERVICES

This workshop is used to define the security categories to be used for SaaS services, and will discuss the threats and possible protective measures needed. The focus is on defining the best method of protection and establishing concrete technical solutions. The guidelines for dealing with SaaS offerings will consider and incorporate the following security categories:

- Governance
- Storage & data encryption
- Antimalware
- Data loss prevention & data classification
- Log management
- Threat detection
- Endpoint / Off premise Security
- Encryption
- Key management
- User identity & lifecycle management
- Access management
- Privileged account management

WORKSHOP 2 - GUIDELINES FOR IAAS / PAAS SERVICES

The IaaS / PaaS workshop builds on the SaaS workshop. The established guidelines for the security categories specified above are enhanced by the inclusion of additional infrastructure security controls.
The result will be a set of guidelines covering the following security categories:

- Governance
- Storage & data encryption
- Web application firewall & load balancing
- Antivirus
- Data loss prevention & data classification
- Log management
- Vulnerability and patch management
- Threat detection
- Network segmentation & firewalling
- Network IDS / IPS
- DDoS Protection
- Compliance checking
- Identity & Lifecycle Management
- Access management
- Privileged account management

WORKSHOP 3 - GUIDELINES FOR DEVOPS ENVIRONMENTS

The workshop for developing security guidelines in DevOps environments is fundamentally different from the other workshops. With a focus on building and securing CI / CD pipelines and containers, other measures for risk detection and minimization must be used, since classic approaches cannot be applied to this type of infrastructure.
The workshop will output a set of guidelines for the following security categories:

- Governance
- Audit & compliance
- Container guidelines
- Network & nano segmentation
- Identity & Access Management
- Storage & data encryption
- Backup
- Vulnerability and patch management in containers
- Malware
- Code release
- Security logging & audit
- Key management services
- API management

the more specialist and knowledgeable the customer attendees at the workshop are the more effective the output is.

SCOPE DEFINITION

Before the workshop, the platform to be discussed, for example a customer portal, the DevOps infrastructure in scope for development or the AWS platform that provides the service, is determined. This is necessary to determine the structure of the workshop and to maintain a consistent basis for discussion. The more precise the scope is defined, the more binding the guidelines that are subsequently developed will be. If several platforms are to be discussed, it is advisable to conduct several workshops. The scope definition also determines the group of participants.

PARTICIPANTS

As a rule, the more specialist and knowledgeable the customer attendees at the workshop are the more effective the output is. Typical attendees include architects, security managers, risk assessors as well as key individuals from development and operations who have an insight into the way departments operate and who can bring examples of how deployment and development activity is undertaken. The workshop benefits from a good mix of participants, as it is often the first time that such a wide range of skills have come together to discuss this sort of issue.

RESULT

At the end of a workshop, the customer receives a report providing an overview of existing and missing Guardrails. These are always presented in the context of best practice recommendations so that deviations can be easily identified. The report also provides additional context as to the urgency with which gaps are recommended to be fixed, and guidance as to the cost and high level timescales required to undertake any remediation work.

Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. We help our customers to Source, Transform and Manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 16,000 people worldwide.

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

computacenter.com
+44 (0)1707 631000