# SERVICE PORTFOLIO DESCRIPTION

## 04 CONTINUOUS IMPROVEMENT

ALICE&
BOB.
COMPANY

**CONTENTS**

# OVERVIEW



IDEA

## 01 HEALTH-CHECK

**SCOPE** AWS Security experts assess your current AWS platform setup and give you short-term consultation.

**GOAL** First best practice feedback from AWS certified solutions architect

- FREE HEALTH CHECK
- WELL ARCHITECTED FRAMEWORK REVIEW

## 02 WARM-UP

**SCOPE** Technical deep dive on your individual platform, either risk or best practice based to identify specific improvement potentials.

**GOAL** Consolidated overview of your platform's current security posture, including t-shirt-sized issue and measure list

- SECURITY ASSESSMENT
- PENETRATION TESTING
- THREAT MODELING WORKSHOP

## 03 LAUNCH

**SCOPE** Platform improvement in individually defined project work (AWS Security Service Portfolio, Shift Left, Continuous Security, Automated Auditing).

**GOAL** Hardened and secure platform with improved overall security posture

- SECURE QUICKSTARTER
- SECURE PLATFORM
- CUSTOMER PROVIDED PLATFORM
- SECURITY CONSULTING

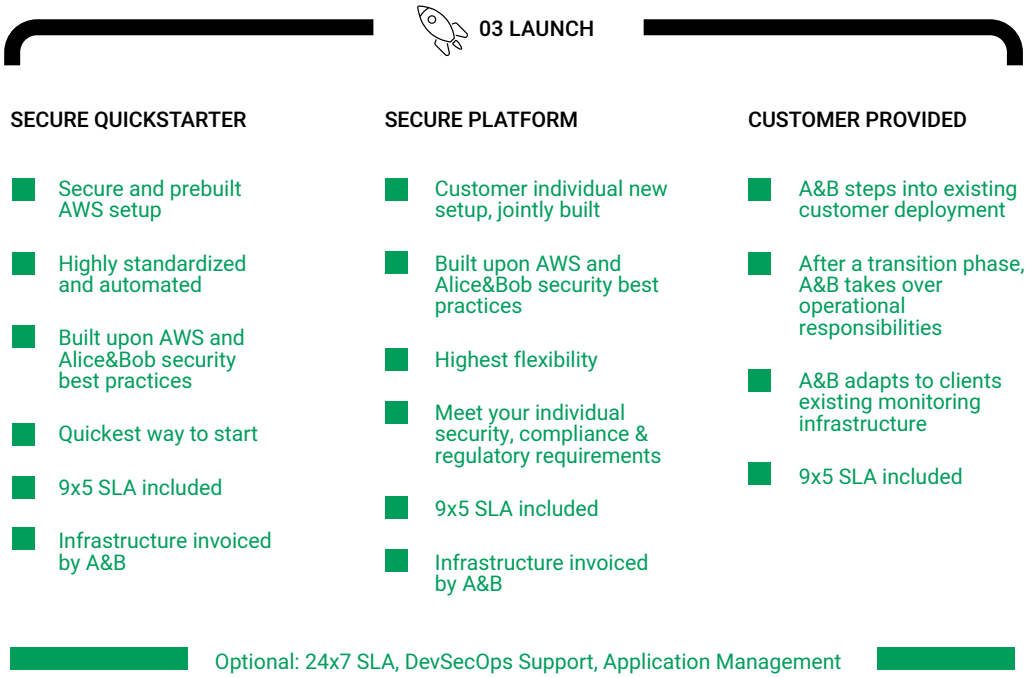
## 04 CONTINUOUS IMPROVEMENT

**SCOPE** Iterative, proactive managed security services or consulting solutions

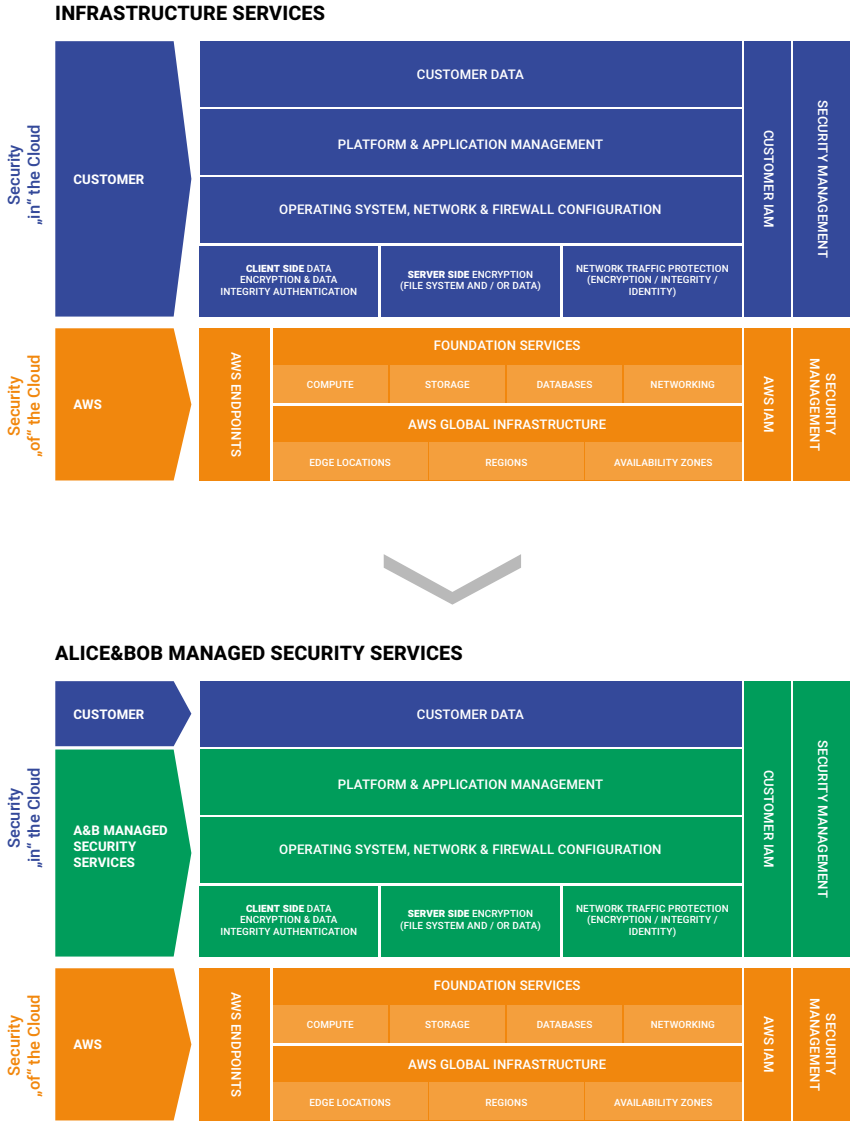
**GOAL** Stay safe with a highly automated and secure platform

- SECURITY CHAMPIONS PROGRAM
- MANAGED SECURITY SERVICES

During phases 1 and 2, A&B takes a consultative approach. In phase 3, A&B delivers continuous Managed Cloud Security services, targeting the basic cloud infrastructure, and introducing security service processes.



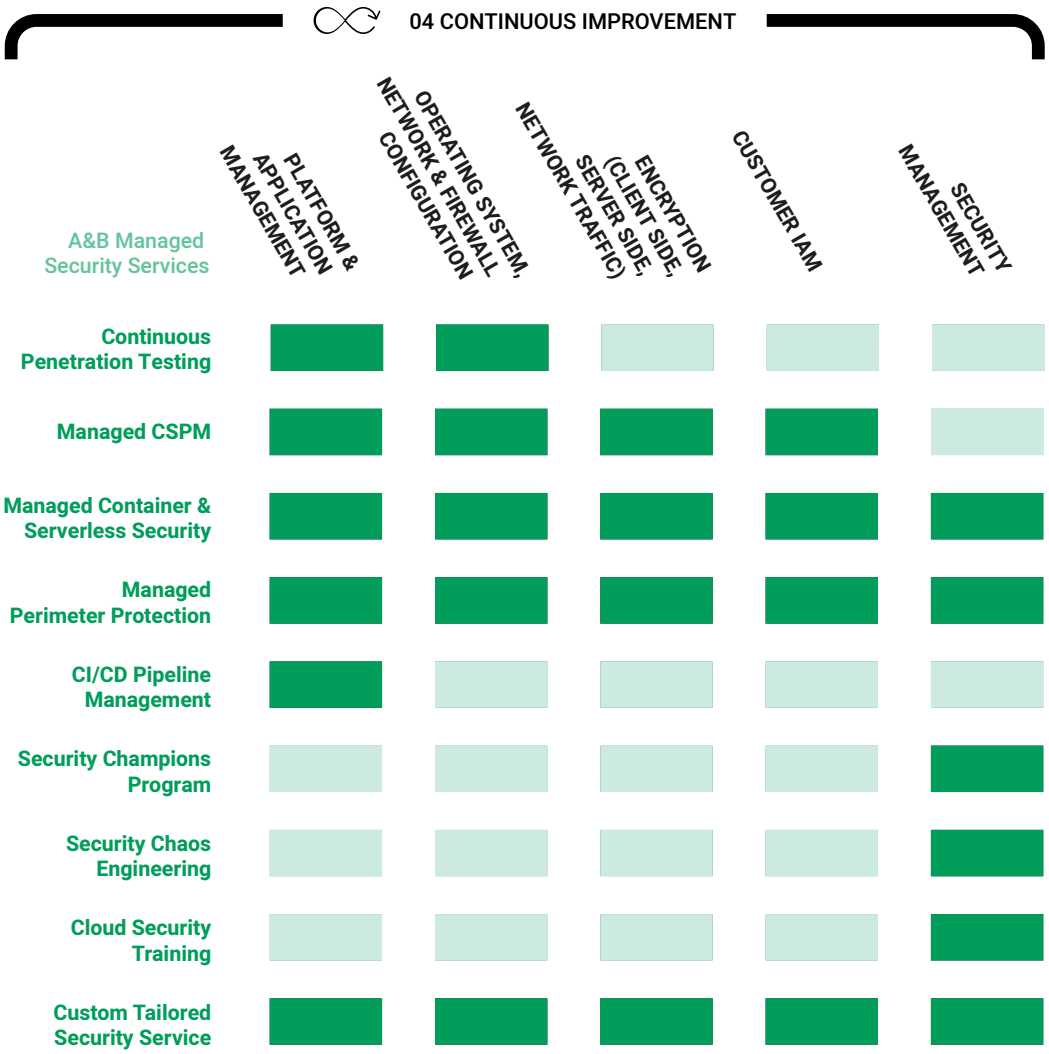

The AWS Shared Responsibility model clearly differentiates between the “security of the cloud” and the “security in the cloud”. On the one hand, AWS takes care of providing highly secure and available infrastructure of all provided infrastructure and services components. On the other hand, the customer themself is responsible for consuming these services securely.




This is where the 04 Continuous Improvement offerings step in, as shown above in green. Alice&Bob.Company provides Managed Security Services to assist you getting the most out of your AWS platform, in terms of performance and security.

We help our clients to ship secure software faster!

In phase 4, the customer can book additional managed services, focused on specific aspects of modern cloud and container architectures. These 04 Continuous Improvement services address different aspects of the AWS Shared Responsibility model:




Customers can choose from the above list of services according to their individual needs and book individual or multiple services.

# MANAGED CLOUD SECURITY SERVICES

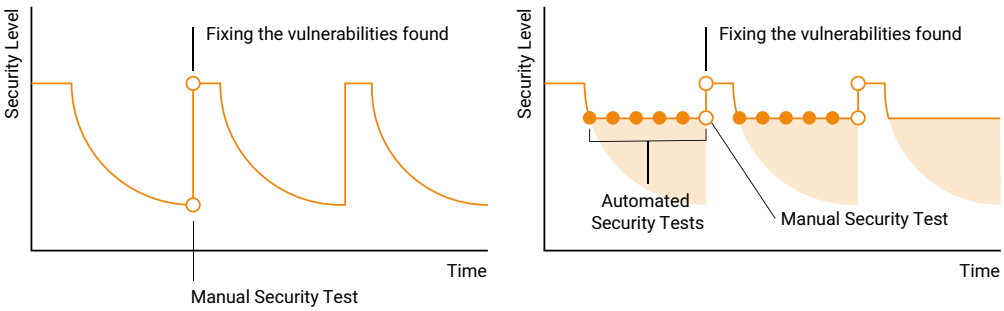
# CONTINUOUS PENETRATION TESTING

## WHY

To minimize risks of application vulnerabilities, software should be penetration tested on a regular interval. We take this burden, perform tests on agreed URLs (Websites & APIs) and deliver regular reports with structured results and weighted findings to you.

## WHAT

We offer a managed continuous penetration testing service, combining manual and automated penetration testing. Manual penetration tests can simulate sophisticated attack vectors, while automated tests cover a broad range of common vulnerabilities, and can be regularly triggered by a CI/CD pipeline.



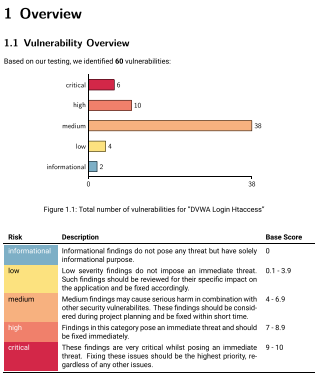

The penetration testing results are evaluated and commented on by an A&B security expert.

Within our continuous penetration testing we perform Dynamic Application Security Testing, focusing on

- Scanning for the OWASP Top 10 vulnerabilities
- Web Application and REST API scanning
- Advanced automated testing of JavaScript applications (Deep Scan)
- Integration in your pipeline

You will receive

- meaningful reporting,
- key statistics, as well as
- actionable and commented insights.

# 1 Overview

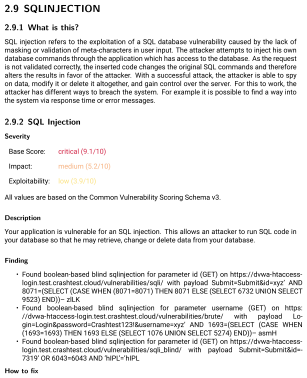
## 1.1 Vulnerability Overview

Based on our testing, we identified **60** vulnerabilities:



Figure 1.1: Total number of vulnerabilities for "DVWA Login Htaccess"

| Risk | Description | Base Score |
|---|---|---|
| informational | Informational findings do not pose any threat but have solely informational purpose. | 0 |
| low | Low severity findings do not impose an immediate threat. Such findings should be reviewed for their specific impact on the application and be fixed accordingly. | 0.1 - 3.9 |
| medium | Medium findings may cause serious harm in combination with other security vulnerabilities. These findings should be considered during project planning and be fixed within short time. | 4 - 6.9 |
| high | Findings in this category pose an immediate threat and should be fixed immediately. | 7 - 8.9 |
| critical | These findings are very critical whilst posing an immediate threat. Fixing these issues should be the highest priority, regardless of any other issues. | 9 - 10 |



## 2.9 SQLINJECTION

### 2.9.1 What is this?

SQL injection refers to the exploitation of a SQL database vulnerability caused by the lack of masking or validation of meta-characters in user input. The attacker attempts to inject his own database commands through the application which has access to the database. As the request is not validated correctly, the inserted code changes the original SQL commands and therefore alters the results in favor of the attacker. With a successful attack, the attacker is able to spy on data, modify it or delete it altogether, and gain control over the server. For this to work, the attacker has different ways to breach the system. For example it is possible to find a way into the system via response time or error messages.

### 2.9.2 SQL Injection

**Severity**

Base Score: critical (9.1/10)

Impact: medium (5.2/10)

Exploitability: low (3.9/10)

All values are based on the Common Vulnerability Scoring Schema v3.

**Description**

Your application is vulnerable for an SQL injection. This allows an attacker to run SQL code in your database so that he may retrieve, change or delete data from your database.

**Finding**

- Found boolean-based blind sqlinjection for parameter id (GET) on https://dvwa-htaccess-login.test.crashtest.cloud/vulnerabilities/sqli/ with payload Submit=Submit&id=xyz' AND 8071=(SELECT (CASE WHEN (8071=8071) THEN 8071 ELSE (SELECT 6732 UNION SELECT 9523) END))-- zILK
- Found boolean-based blind sqlinjection for parameter username (GET) on https://dvwa-htaccess-login.test.crashtest.cloud/vulnerabilities/brute/ with payload Login=Login&password=Crashtest123!&username=xyz' AND 1693=(SELECT (CASE WHEN (1693=1693) THEN 1693 ELSE (SELECT 1076 UNION SELECT 5274) END))-- asmH
- Found boolean-based blind sqlinjection for parameter id (GET) on https://dvwa-htaccess-login.test.crashtest.cloud/vulnerabilities/sqli_blind/ with payload Submit=Submit&id=7319' OR 6043=6043 AND 'hiPL'='hiPL

**How to fix**

## HOW

Alice&Bob.Company provides a custom tailored penetration testing solution to meet the reuirements of the customers application. Initially, to provide the best possible test coverage, the customer defines an application profile by answering a short questionnaire. A&B then configures automated penetration tests, aligns a manual penetration test interval and enables the customer to book additional manual penetration test by simply submitting a request through the helpdesk system.

Penetration tests will be carried out using a best of breed mix of tools and services, in line with the application profile, and according to our experience. Our automated penetration testing will be centered around Crashtest Security Suite, whereas manual penetration testing will be delivered in accordance with

- the application testing profile
- A&B's proven experts' take on potential application specific attack vectors
- automated testing results

Manual penetration tests can involve utilties such as

- Zed Attack Proxy (ZAP)
- S3 bucket enumeration and attack utilities
- internally developed utilities addressing common AWS configuration pitfalls

Resulting reports, both for automated and manual testing, are consolidated and are provided on a secured communication channel. This service is built upon 03 Launch services.

# CLOUD SECURITY POSTURE MANAGEMENT

**WHY**

Keeping visibility across public cloud accounts – probably across multiple public cloud vendors – is difficult. Hundreds and thousands of deployed cloud resources require an automated audit and mitigation approach.

A Cloud Security Posture Management (CSPM) delivers visibility into risk and compliance posture in modern cloud computing environments. It helps to automate cross account audits. Fix configuration errors before they get exploited! Take the Cloud Native security approach!

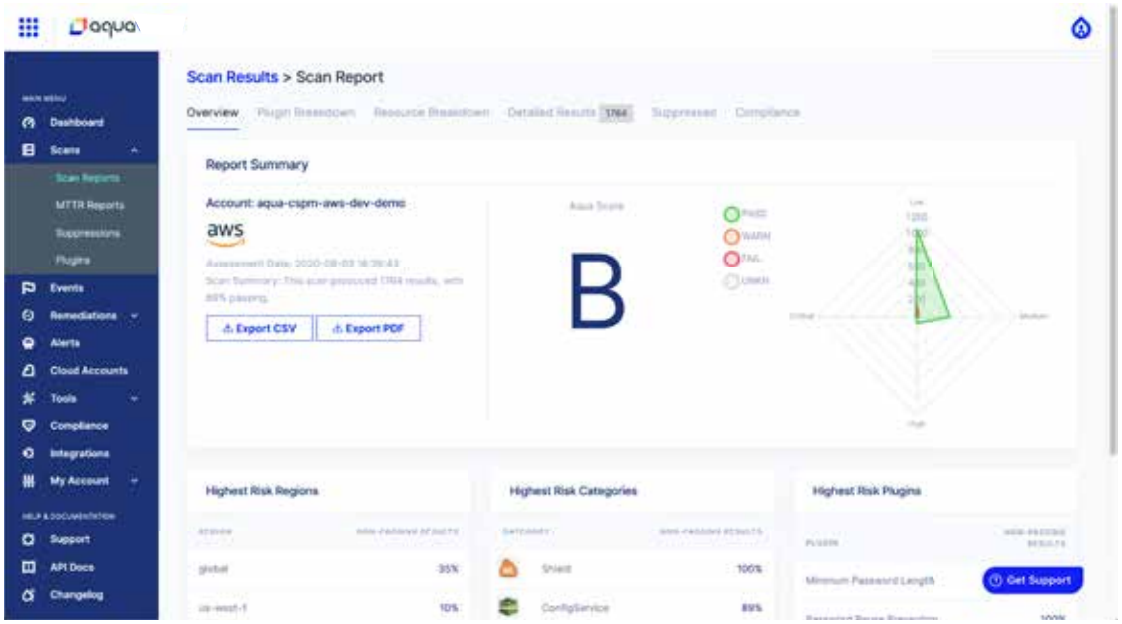
**WHAT**

Alice&Bob.Company provides a managed CSPM solution, based upon Aqua. As a certified Aqua Sec partner and reseller, we set up the environment on your behalf and take over the operational responsibility.

This, on the one hand, frees up your resources to improve your digital product, and on the other hand generates continuous insights into your cloud deployments, even across multiple public cloud vendors.

The most relevant public cloud platforms available are supported:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform




Some examples of what the CSPM platform provides:

- Continuous scanning and CIS Benchmark auditing,
- Auto-Remediation for Self-Securing Infrastructure,
- Infrastructure-as-Code (CloudFormation and Terraform) Template Scanning,
- Integration into SIEM and client's collaboration tools,
- Extensive Compliance Reporting, i.e. PCI, HIPPA, GDPR, ISO27001, ISO270017, ISO270018, NIST, Well-Architected,
- Real-Time Control Plane Events Monitoring and
- Extensible Open Source Architecture.

**HOW**

We will setup a dedicated instance of the Aqua platform for you. This service is provided as a SaaS solution.

A&B will do all the initial configuration necessary. We attach the CSPM platform, read-only, to your multiple cloud accounts. Afterwards we integrate into automation, set thresholds, and configure required alerting.

Once the platform is up and running, we continuously maintain the CSPM platform for you. A&B tweaks and optimizes the CSPM configuration rules to minimize false positives and to automate as much as possible.

We take over operational responsibility and integrate into the alert and notification chain. This also includes real-time alerting. In collaboration with you - and considering the concrete scope of the contract – we can fix simple security issues proactively.

More complex security incidents are tracked and handled by Alice&Bob.Company's Security Incident Management process. They are resolved in tandem with your team.

You, as a client, will get direct access to the CSPM tool and can take advantage of the detailed reporting.

This service is built upon 03 Launch services.

# MANAGED CONTAINER & SERVERLESS SECURITY

**WHY**

Container and serverless environments are highly dynamic. Compute instances, i.e. are volatile, and spin up and down highly automated. Kubernetes for example is an extremely powerful platform, but can also be the source of innumerable security breaches. Container security expert know-how is hard to find and even harder to scale.

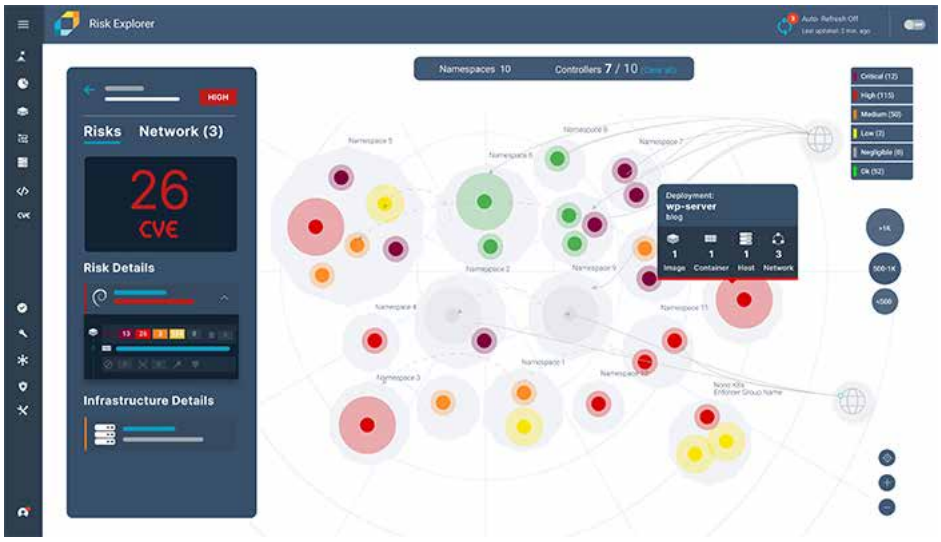
Enhance the security of your container and serverless environments, while leveraging all the benefits of these technologies.

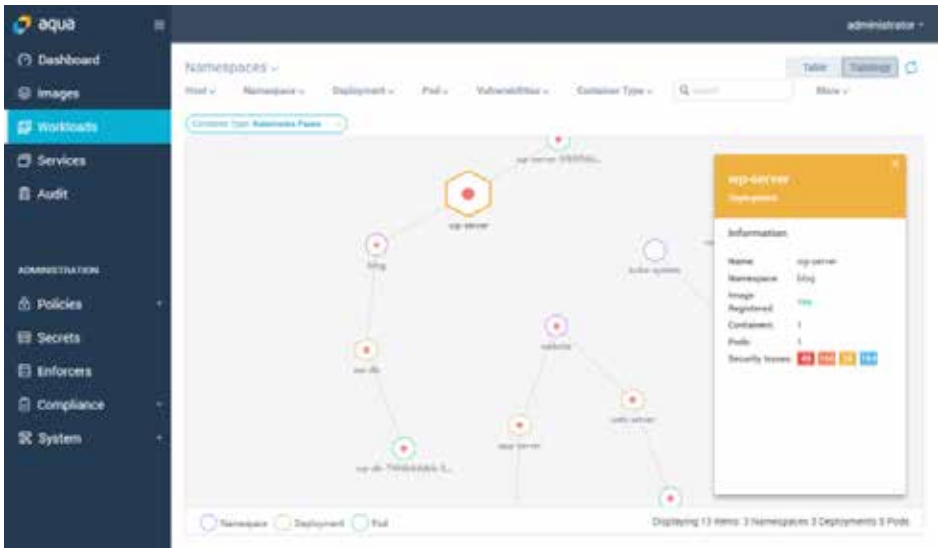
**WHAT**

We provide a managed security solution, based upon Aqua CSP. As a certified Aqua Sec partner and reseller, A&B experts set up the environment on your behalf and take over operational responsibility.


This, on the one hand, releases resources in your team to improve your digital product, and on the other hand generates continuous insights into your cloud deployment, even across multiple public cloud vendors.

Alice&Bob.Company provides managed full lifecycle security for images, containers and serverless environments.




**HOW**

First, we set up a new instance of the Aqua Wave Enterprise for you. This service is provided as a managed installation by Alice&Bob.Company.

The platform is installed in a dedicated AWS account in the Region eu-central-1 (Frankfurt).

Next we apply Aqua licenses, according to the distinct and contractually agreed client requirements.

The platform comes with the following features enabled:

- Easy identification of high-risk areas with a condensed dashboard overview
- Vulnerability scanning in CI pipelines that can be easily integrated into Jenkins, Gitlab, Bamboo, Azure DevOps und CodeFresh
- Kubernetes Security, covering most prominent K8s platforms, i.e. Amazon EKS, Azure AKS, Google GKE, Red Hat OpenShift, VMware, TKGI and Rancher
- Behavioral Profiles
- Workloads Firewall
- Secrets Injection
- Real-time auditing and Forensics
- Drift prevention helps to prevent a large array of attack vectors, including zero-day attacks, based on an image‘s digital signature

Options are:

- Dynamic Threat Analysis (DTA)
- Vulnerability Shield (vShield)
- Kubernetes Security Posture Management (KSPM)
- Serverless Security Assurance
- Virtual Machine Scanning

The platform scans CI builds and images and can make use of Dynamic Threat Analysis (DTA) to dynamically analyze images before they are even deployed. The analysis is executed in a securely isolated sandboxed environment, examining and tracing behavioral anomalies to uncover advanced malware that cannot be detected by static scanners.

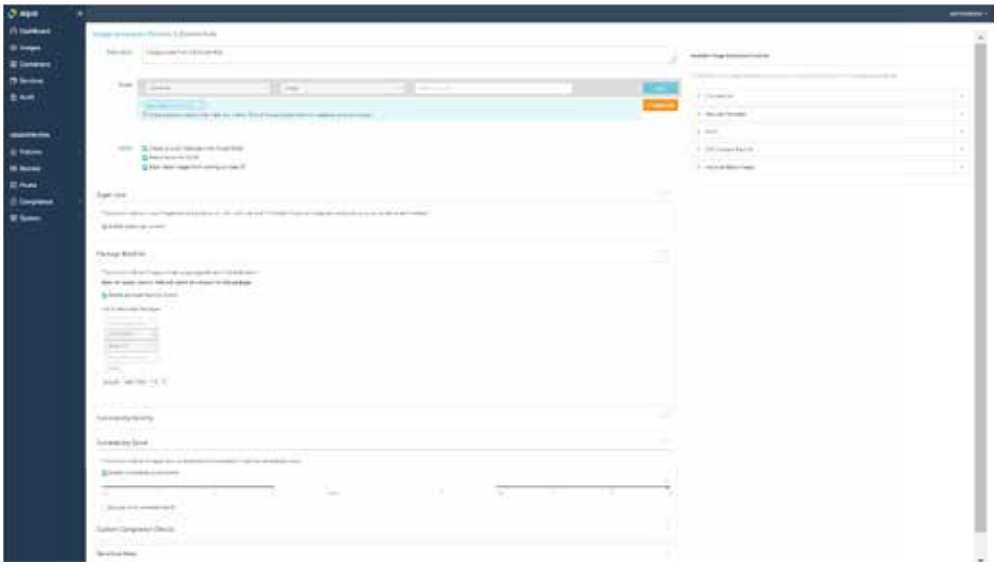
A&B mitigates the risk of so called "unfixable vulnerabilities" with Aqua Vulnerability Shield.

Additionally, we can extend security on serverless functions (FaaS), i.e. AWS Lambda or Google Functions. This includes:

- Discovery and Visibility
- Risk Assessment & Mitigation
- Runtime protection, to block malicious code injection
- Honeypots, by luring attackers to exploit what is perceived to be "low hanging fruit"
- CI/CD Integration

We will perform all of the initial configuration necessary and attach the platform to the multiple cloud accounts of your container platform. For serverless, an Aqua layer has to be embedded into the code. We arrange this with your teams, integrate into automation, set thresholds, and configure required alerting.

When the platform starts working, we continuously maintain the cloud native security platform for you. Configuration is tweaked and optimized to make you get the most out of the platform.



We take over operational responsibility. Therefore, Alice&Bob.Company needs to be added to the alert and notification chain. This also includes real-time alerting.

After analysis of an alert-only phase, we recommend creating policies, that will preventively mitigate risks. In tight collaboration with your team - and considering the specific scope of the contract – we can proactively fix simple security issues.

More complex security incidents are tracked and handled by Alice&Bob.Company's Security Incident Management process. They are resolved in collaboration with your team.

You will get direct access to the CSPM tool, and can take advantage of the detailed reporting without giving you the hassle and burden to manage the platform.

This service is built upon 03 Launch services.

# MANAGED PERIMETER PROTECTION

**WHY**

Running public services, such as e-commerce websites, web APIs, RPC interfaces, IoT applications and portals, requires enabling access from all over the Internet. To protect those dynamic web applications against external attackers as effectively as possible, you need to implement so-called perimeter protection.

With Perimeter protection, you establish a resilient multi-layer security strategy, and protect your applications against exploitation of several classes of bugs and vulnerabilities, including against zero-day vulnerabilities. Additionally, you protect your applications against multiple types of Distributed Denial of Service (DDoS) attacks.

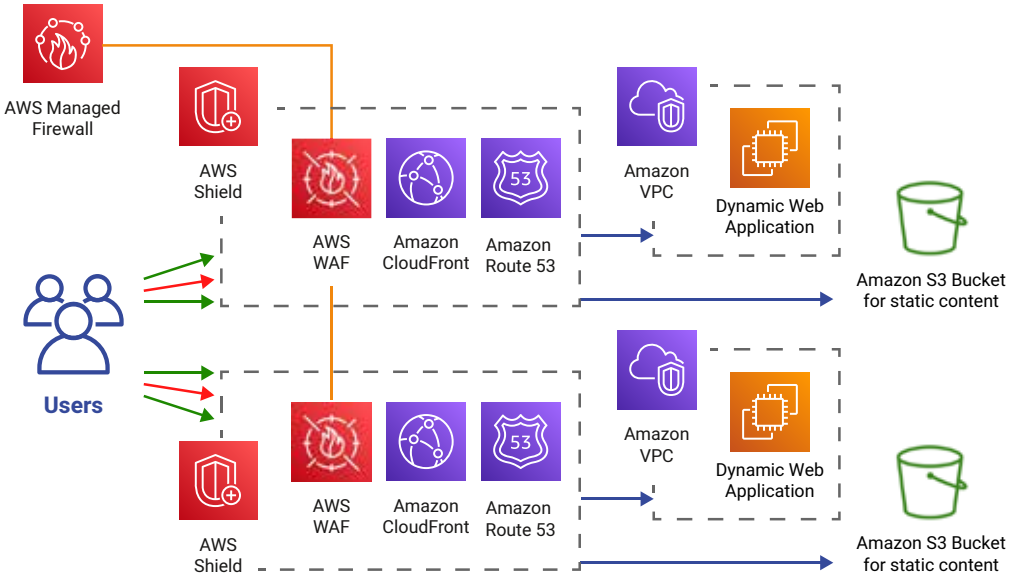
**WHAT**

We provide perimeter protection as a managed service. The goal is to secure your applications and origin infrastructure from cyber security attacks such as Distributed Denial of Service attacks (DDoS), SQL Injection or Cross-Site Scripting.

This suite of services includes

- AWS Managed Firewall,
- AWS Web Application Firewall (WAF),
- AWS Shield, and
- AWS Firewall Manager

The A&B team is directly connected with the AWS DDoS Response Team (DRT). This means, in case of a cyber-attack affecting your infrastructure, we will quickly escalate the incident in the organization, within known processes and structures.



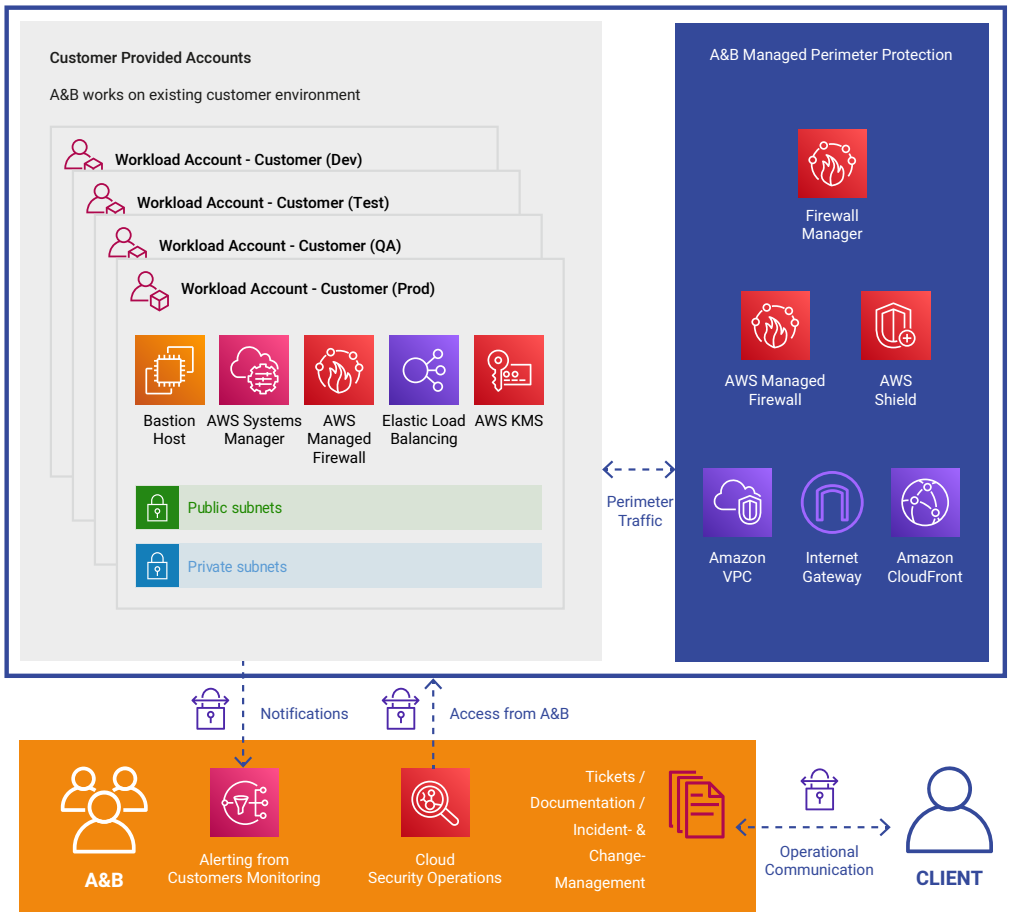

A&B Managed Perimeter Protection includes the following services:

- AWS account management
- Defining a security posture, including the applications, environments, and resources that are most critical to protect
- Full configuration of AWS Shield Advanced and AWS WAF
- Migration from other application security vendors
- Implementation of AWS Best Practices for DDoS Resiliency and Guidelines for Implementing AWS WAF
- Tuning of AWS Shield Advanced and AWS WAF to ensure optimal performance
- Monitoring resource health by testing architecture resiliency, to avoid false negatives and false positives
- Building and maintaining customer specific runbooks
- First line support for all application security issues
- Escalation to the AWS DDoS Response Team (DRT) during events via Alice&Bob.Company support team

Optionally to the basic AWS WAF service, A&B provides third-party WAF solutions based on the market leading f5´s Advanced WAF and supports with extended f5 expertise.

## HOW

Alice&Bob.Company connects existing AWS cloud infrastructure to Alice&Bob.Company's Managed Perimeter Security environment. Alice&Bob.Company maintains a dedicated AWS account for each client and routes the egress/ingress traffic through it.



According to your specific requirements, A&B implements one or more of the following services:

- We activate WAF services and set up a ruleset to secure customer applications on layer 7
- We manage the rulesets according to an established workflow and setup subscriptions of rules to ensure up-to-date protection
- We enable AWS Shield (Standard or Advanced) and implement defensive workflows in close collaboration with your team and the AWS DDoS Response Team
- We deploy and operate AWS Firewall Manager for central & cross-account firewall management integrated into AWS Organizations

We will start our integration with a testing and tuning environment first. While assessing risks and implementing health monitoring, we ensure optimal performance for real user traffic and avoid false positives.

Afterwards, the Managed Perimeter Protection is put into production.

Therefore we:

- Place the AWS WAF into Allow/Block Mode,
- Apply WAF to required resources with the AWS Firewall Manager, and
- Apply Shield Advanced to all required resources.

Our team of specialists will proactively handle events according to the proven incident management process, to minimize customer impact.

This service is built upon 03 Launch services.

# CI/CD PIPELINE MANAGEMENT

**WHY**

An automated, bullet-proof CI/CD pipeline is vital to the foundation of a secure and reliable architecture. An automated pipeline minimizes human errors, and enforces quality and security checks when deploying code. A proper automated pipeline leads to faster releases, increases developer velocity, and simplifies maintenance and updates of customer workloads. It is fundamental to security automation.

**WHAT**

We provide CI/CD pipepline as a managed service. It gives you visibility and control inside and outside of your CI/CD pipeline, and increases code quality, leading to cost reductions and an increasing ROI. We consider the CI/CD pipeline as the technical heart of the DevSecOps approach.

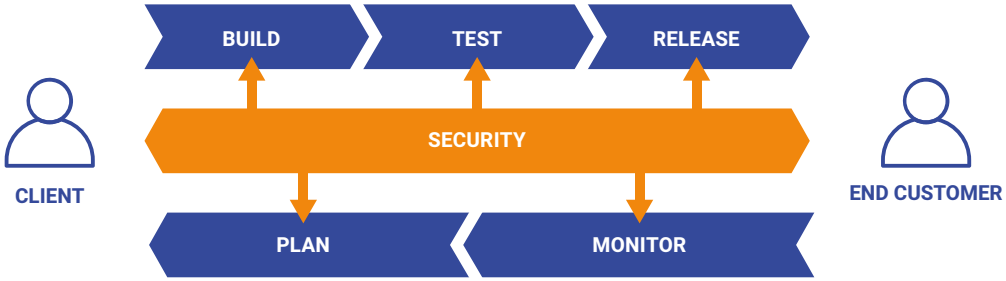
In order to provide the pipeline(s) as managed service, we create, automate, manage and continuously optimize your CI/CD pipeline(s). This covers infrastructure, application and security.

Alice&Bob.Company develops a consistent, streamlined and continuously improved process incorporating:

- Security steps like code analysis,
- Security/CVE checks,
- Dependency checks,
- Comprehensive release steps containing pre-commit checks,
- Reviewed merge requests, and
- Controlled commits individually tailored to the toolchain used by the client (e.g. gitlab, AWS Developer Tools, ...)

Additionally, A&B integrates and configures specific AWS services according to your individual requirements, including

- AWS Config,
- AWS GuardDuty and/or
- Amazon Security Hub.




**HOW**

We analyze your deployment processes and its requirements, and develop a CI/CD pipeline architecture, taking into consideration your organizational, procedural and technical conditions. We create, optimize, automate and implement security in targeted CI/CD pipelines.

A&Bs course of action is as follows:

- CI/CD Pipeline Assessment and comparison to best practices
- Creation and adaption of the pipeline to defined best practices
- Monitoring the CI/CD Pipeline for 12 consecutive months after go-live

**CI/CD Pipeline Assessment**

During the assessment, we conduct a workshop focusing on the single stages of your software delivery process. Information about the state of the pipeline, its challenges and requirements, are revealed and gathered, combining interviews and checklists as well as code and data analysis.

Outcomes will be compared to best practices and presented in a report, together with recommendations for optimization.

**Pipeline Creation**

Building upon the results of the assessment, we either optimize an existing pipeline, or create a new pipeline with the goal of delivering a fully managed build service with integrated comprehensive security checks. We prefer to use AWS services (AWS CodeBuild, AWS CodeDeploy), but we are open to other solutions.

**Monitoring**

After provisioning, we monitor the CI/CD pipelineand the code that's actively being deployed. We constantly check the pipeline and its components for:

- Unauthorized access and violation of privileges
- Suspicious behaviour
- Misconfiguration
- Performance metrics
- Code quality scans (static and dynamic)

Monitoring will be made accessible and regular reports will be generated. Findings will be rated and described in a consolidated report. Optionally we provide resolution measures after consultation.

This service is built upon 03 Launch services.

# SECURITY CHAMPIONS PROGRAM

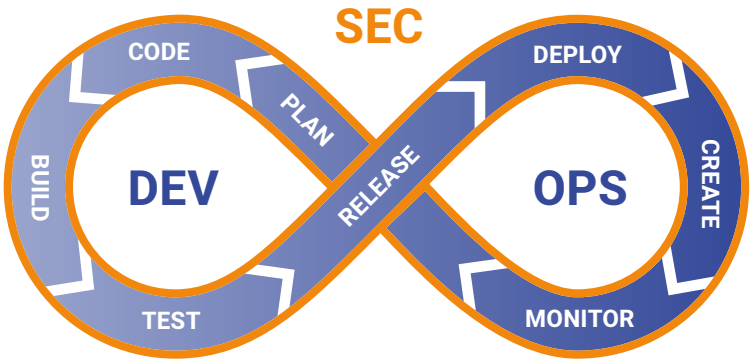
**WHY**

From a product development perspective security always seems to be "the bottleneck" or "the department of NO!". An increasing number of product releases and daily software deployments overwhelm the security department additionally.

Turn the tables by rolling out a Security Champions Program. Accelerate your product development while staying secure by establishing security-as-code and a security culture across your organization with A&B. Stay innovative and improve your overall security posture!

**WHAT**

We enable your team(s) to act as Security Champions by example. After integrating in the team, our security experts start to implement security-as-code in each phase of the DevSecOps pipeline to reach a high degree of security automation.




Together with your leadership team and in alignment with general companies' security policies, the Security Champions Program covers:

- Agile Threat Modeling
- DevSecOps
- Security-as-Code & -automation

Besides integrating the security-as-code, the A&B specialists take over the role of Security Influencer within the organization, and disseminate knowledge across various product teams to establish a strong security culture.

Additionally, Security Champions lead security automation programs and help your team(s) to integrate security-as-code in each phase of your software development lifecycle.

**HOW**

We follow our very own "integrate&enable" approach to get the most out of the program for you and create a customer centric program, that addresses organizations, teams, and tools.

**Integrate**

The A&B Security Champion integrates immediately into your product team(s), defines possible threats in mutual workshops and starts leading the change. After a joint definition of a desired security automation state, the Security Champion starts implementing Security-as-Code in all phases of the DevSecOps lifecycle.

**Enable**

As interim Security Champions and mentors, we will not only implement Security-as-Code, but onboard your novice Security Champions, empower them with recurring training on how to become a Security Champion themselves, and set up the right communication channels to build a network of Security Champions.

We follow the Security Champions Playbook initiated by OWASP

**Integrate and enable approach**


After starting with a "lighthouse" team, we continue to roll-out the program across various teams.

Once the initial rollout of the Security Champions Program, we take care of the continuous improvement of the program in bi-weekly moderated team retrospectives with the novice client Security Champions.

# SECURITY CHAOS ENGINEERING PROGRAM

## WHY

Modern digital platforms are becoming more and more distributed and automated. External services are often integrated when building your own services. This naturally adds complexity to your infrastructure and applications.

Security Chaos Engineering (SCE) does not rely on theoretical security architecture to protect digital companies. It provides you a fresh perspective and an innovative, chaos engineering based approach to build a new culture of cybersecurity to protect your digital assets.

## WHAT

Chaos Engineering is the discipline of experimenting on a distributed system in order to build confidence in its capability to withstand turbulent conditions in production. It focuses on availability.

SCE is about injecting turbulence; real world faults, not only tackling availability, but also integrity and confidentiality. It provides improved platform and application security, especially for real world security issues by cultivating the concepts of Security Chaos Testing. Experimenting with failure helps to uncover systemic weaknesses or gaps.

It focuses on simple vulnerabilities rooted in human error and system glitches, rather than attacks being initiated from sophisticated nation-state actors or hackers.

With Alice&Bob.Company's „integrate&enable" approach, we implement and maintain a SCE program into your existing DevOps or agile working culture.

**HOW**

We set up a 12 month program to establish SCE culture within your company. We work collaboratively with your management team and existing security organization to get the program ignited.

After the team kickoff, we start a number of initiatives to define the individual scope, coach the concepts of SCE and roll out a program which addresses:

- Organization
- Team
- Implementation
- Tools

A&B will introduce, roll-out and maintain the concept and ideas of Security Chaos Engineering. We:

- Set the scope,
- Teach the concepts of chaos experiments,
- Enable you to craft Security Chaos Experiments,
- Develop an experiment design process collaboratively,
- Implement automated Security Chaos Experiments in existing CI/CD pipelines, and
- Train and enable your team(s)

We will take care to continuously maintain and improve the program over the contractual period with moderated team retrospectives in bi-weekly intervals.

# CLOUD SECURITY TRAINING

**WHY**

Gain general security awareness and competency. The field of cloud security is evolving continuously. AWS provides more than 45 security related services, which need to be integrated and maintained in clients' individual cloud environments.

**WHAT**

AWS currently provides >199 ready-to-use cloud-native services. 45 of these services directly or indirectly influence the security of clients' cloud deployments. We train, consult and enable your team(s) on a mid- to long-term track on the latest releases and developments.

This allows you to focus on your core business: Making the best products!

HOW

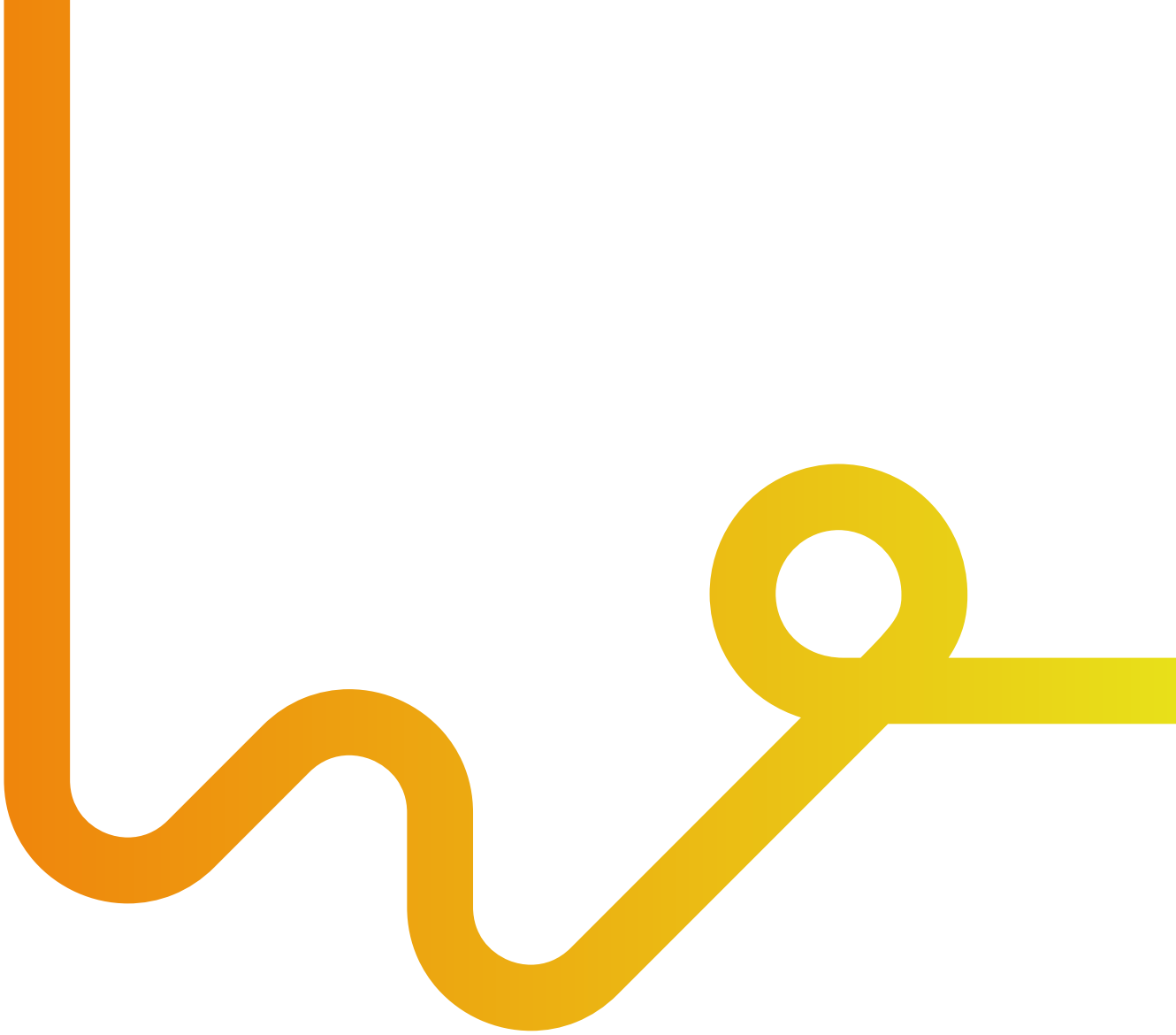
We integrate with your teams to understand their overall cloud expertise and individual cloud maturity level.

Based on our findings, we develop a customer individual training plan. The plan is usually scheduled over a timeframe of 6 to 24 month with recurring training on agreed topics.

This ensures greatest value and raises knowledge and competency across different teams.

The goals and training programs are agreed with your leadership team as well as product teams but can be changed upon need to meet your requirements as they change and grow.

The project is rolled out and managed by an A&B service manager.



# CUSTOM TAILORED MANAGED SERVICE

Profit directly from our long years of expertise in the design, implementation and operation of cloud environments. The founding team members of Alice&Bob.Company are early cloud pioneers in Germany and have more than 10 years of experience in providing managed services for demanding business customers.
We have lots of expertise with specific security requirements (e.g. regulated financial branches, insurance companies, transportation, p&u) and global Big Data and Machine Learning platforms.

Please get in touch with us and let us know your needs!

# PRICING

All A&B Managed Security Services consist of a Transition & Transformation phase as well as a recurring Managed Service fee (incl. Software Licensing fees, if applicable).

# SERVICE TERMS & CONDITIONS

Alice&Bob.Company provides all services described above in connection with one of the 03 Launch services.

All described services are directly linked to the service description in the 03 Launch document:

- Support
- Incident Management
- Alerting & Monitoring
- Service Level Agreements
- Alice&Bob.Company SLAs
- Amazon Web Service (AWS) SLAs
- Service Terms & Conditions

# COME TO OUR WEBSITE AND FOLLOW US ON SOCIAL MEDIA

aliceandbob.company

linkedin.com/company/alice-and-bob-company

facebook.com/aliceandbob.company/

twitter.com/_aliceandbob