SERVICE PORTFOLIO DESCRIPTION

04 CONTINUOUS IMPROVEMENT

ALICE&
BOB.
COMPANY

CONTENTS

Overview 2

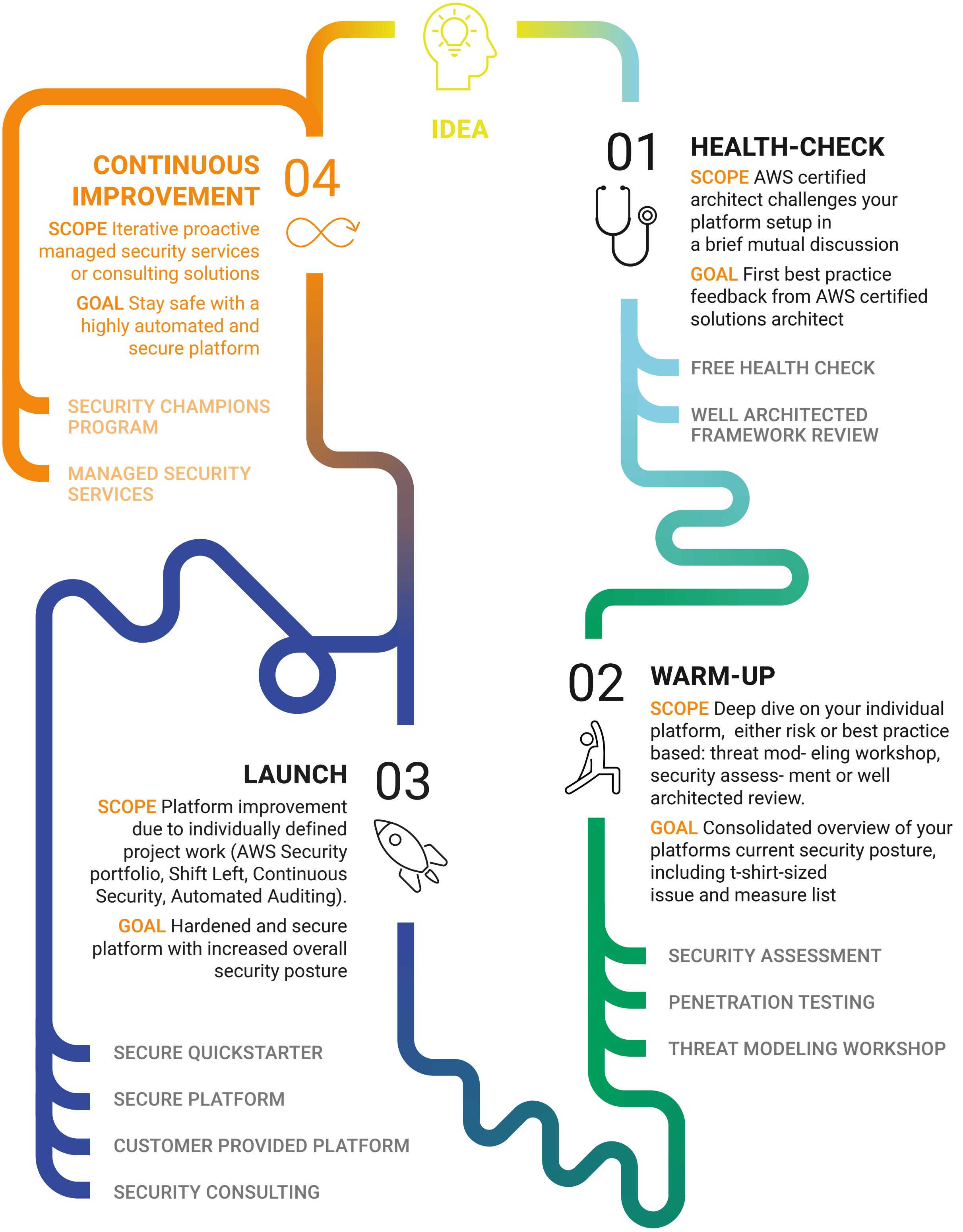
Managed Cloud Security Services 5

- Continuous Penetration Testing 6
- Cloud Security Posture Management 9
- Managed Container & Serverless Security 12
- Managed Perimeter Protection 17
- CI/CD Pipeline Management 21
- Security Champions Program 24
- Security Chaos Engineering Program 27
- Cloud Security Trainings 29
- Custom Tailored Managed Service 30

Pricing 31

Service Terms & Conditions 31

OVERVIEW



IDEA

01

HEALTH-CHECK

SCOPE AWS certified architect challenges your platform setup in a brief mutual discussion

GOAL First best practice feedback from AWS certified solutions architect

- FREE HEALTH CHECK
- WELL ARCHITECTED FRAMEWORK REVIEW

02

WARM-UP

SCOPE Deep dive on your individual platform, either risk or best practice based: threat mod- eling workshop, security assess- ment or well architected review.

GOAL Consolidated overview of your platforms current security posture, including t-shirt-sized issue and measure list

- SECURITY ASSESSMENT
- PENETRATION TESTING
- THREAT MODELING WORKSHOP

03

LAUNCH

SCOPE Platform improvement due to individually defined project work (AWS Security portfolio, Shift Left, Continuous Security, Automated Auditing).

GOAL Hardened and secure platform with increased 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

Within phase 1 to phase 3 customers already got familiar with the A&B approach to modern cloud security. While in phase 1 and phase 2 the client experienced some first consulting projects with A&B, phase 3 delivers continuous Managed Cloud Security Services, targeting the basic cloud infrastructure and introducing security service processes.

03 LAUNCH

SECURE QUICKSTARTER

- Secure and prebuilt AWS setup
- Highly standardized and automated
- Built upon AWS and Alice&Bob security best practices
- Quickest way to start
- 9x5 SLA included
- Infrastructure invoiced by A&B

SECURE PLATFORM

- Customer individual new setup, jointly built
- Built upon AWS and Alice&Bob security best practices
- Highest flexibility
- Meet your individual security, compliance & regulatory requirements
- 9x5 SLA included
- Infrastructure invoiced by A&B

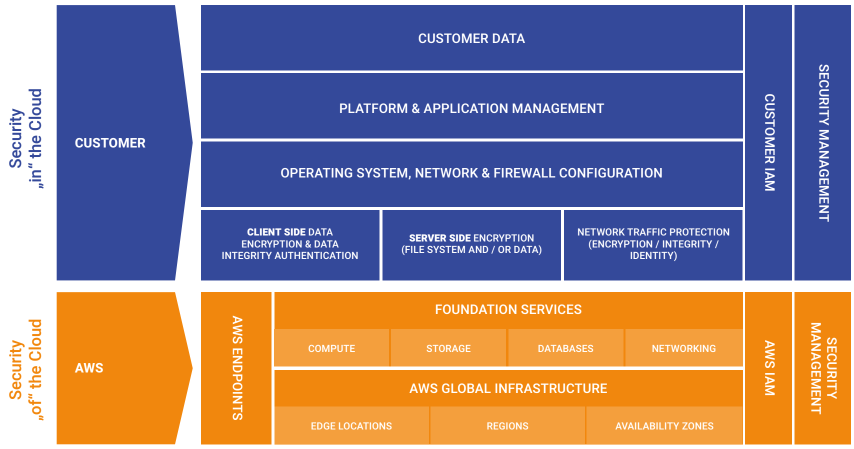
CUSTOMER PROVIDED

- A&B steps into existing customer deployment
- After a transition phase, A&B takes over operational responsibilities
- A&B adapts to clients existing monitoring infrastructure
- 9x5 SLA included

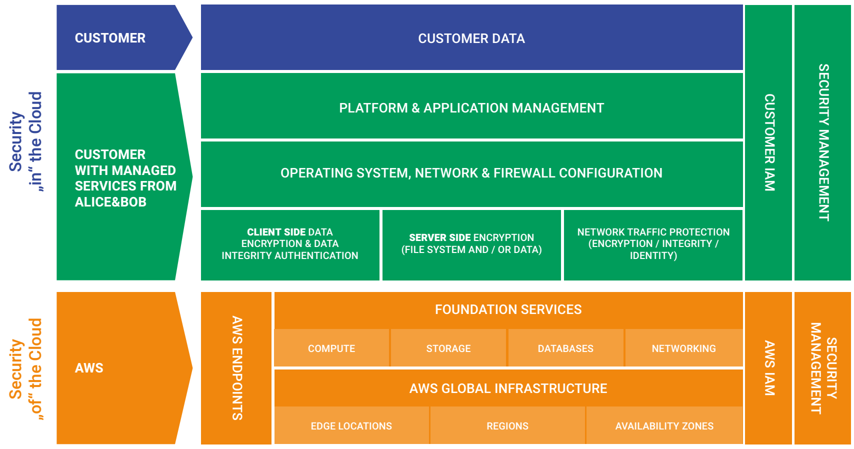
Optional: 24x7 SLA, DevSecOps Support, Application Management

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 himself is responsible for consuming these services securely.

INFRASTRUCTURE SERVICES


Security „in" the Cloud
CUSTOMER
CUSTOMER DATA
PLATFORM & APPLICATION MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER SIDE ENCRYPTION (FILE SYSTEM AND / OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION / INTEGRITY / IDENTITY)
CUSTOMER IAM
SECURITY MANAGEMENT
Security „of" the Cloud
AWS
AWS ENDPOINTS
FOUNDATION SERVICES
COMPUTE
STORAGE
DATABASES
NETWORKING
AWS GLOBAL INFRASTRUCTURE
EDGE LOCATIONS
REGIONS
AVAILABILITY ZONES
AWS IAM
SECURITY MANAGEMENT

ALICE&BOB MANAGED SECURITY SERVICES


Security „in" the Cloud
CUSTOMER
CUSTOMER DATA
CUSTOMER WITH MANAGED SERVICES FROM ALICE&BOB
PLATFORM & APPLICATION MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER SIDE ENCRYPTION (FILE SYSTEM AND / OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION / INTEGRITY / IDENTITY)
CUSTOMER IAM
SECURITY MANAGEMENT
Security „of" the Cloud
AWS
AWS ENDPOINTS
FOUNDATION SERVICES
COMPUTE
STORAGE
DATABASES
NETWORKING
AWS GLOBAL INFRASTRUCTURE
EDGE LOCATIONS
REGIONS
AVAILABILITY ZONES
AWS IAM
SECURITY MANAGEMENT

This is where the 04 Continuous Improvement offerings step in, as shown above in green. Alice&Bob.Company provides Managed Security Services to assist customers in taking the most out of the 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, very specialized and focused on different aspects of modern cloud and container architectures. These 04 Continuous Improvement services address different aspects of the AWS Shared Responsibility model:

04 CONTINUOUS IMPROVEMENT

A&B Managed Security Services	CONTINUOUS PENETRATION TESTING	MANAGED CSPM	MANAGED CONTAINER & SERVERLESS SECURITY	MANAGED PERIMETER PROTECTION	CI/CD PIPELINE MANAGEMENT	SECURITY CHAMPIONS PROGRAM	SECURITY CHAOS ENGINEERING	CLOUD SECURITY TRAININGS	CUSTOM TAILORED SECURITY SERVICE
Platform & Application Management	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	🟩
Operating System, Network & Firewall Configuration	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	🟩
Encryption (Client Side, Server Side, Network Traffic)	⬜	🟩	⬜	⬜	⬜	⬜	⬜	⬜	🟩
Customer IAM	⬜	🟩	⬜	⬜	⬜	⬜	⬜	⬜	🟩
Security Management	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩

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

MANAGED CLOUD SECURITY SERVICES

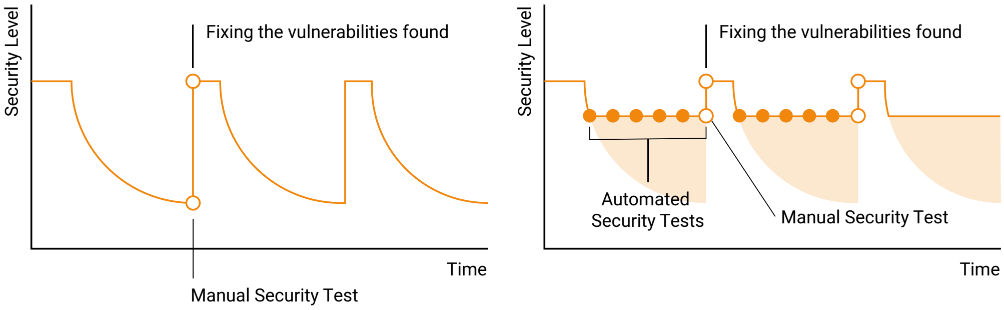
CONTINUOUS PENETRATION TESTING

WHY

To minimize risks of application vulnerabilities, software shall be penetration tested on a regular interval. Alice&Bob.Company takes this burden, performs tests on the agreed URLs (Websites & APIs) and delivers regular reports with structured results and weighted findings.

WHAT

Alice&Bob.Company offers a managed continuous penetration service. Therefor they combine manual testing with automated penetration test. Manual penetration tests can simulate very sophisticated attack vectors, while automated tests ensure a basic testing, even in case of continuous deployments.



The penetration testing results get valuated and commented by an A&B security expert.

Within this penetration testing A&B performs 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)
- Integrate in clients' pipeline

The client will receive

- a meaningful reporting,
- key statistics and
- actionable and commented insights.

CONTINUOUS PENETRATION TESTING

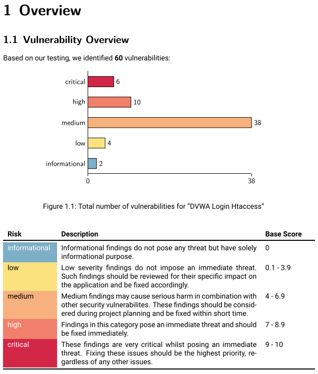
SCANNING REPORT

DVWA Login

Datum

URL

ALICE &
BOB.
COMPANY



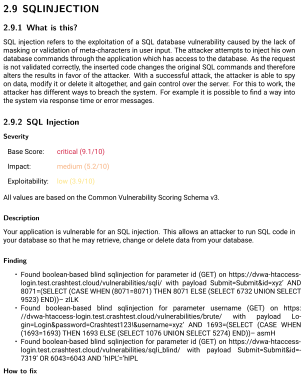
1 Overview

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 vulnerabilites. 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))– zlLK
- 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 flexible and tailored testing setup according to initial definitions.

A&B equips clients with the Alice&Bob.Company's standard penetration toolset. This is a best of breed mix of tools and services, according to our experience, i.e.

- Crashtest Security Suite
- Zed Attack Proxy (ZAP)

Resulting reports 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!

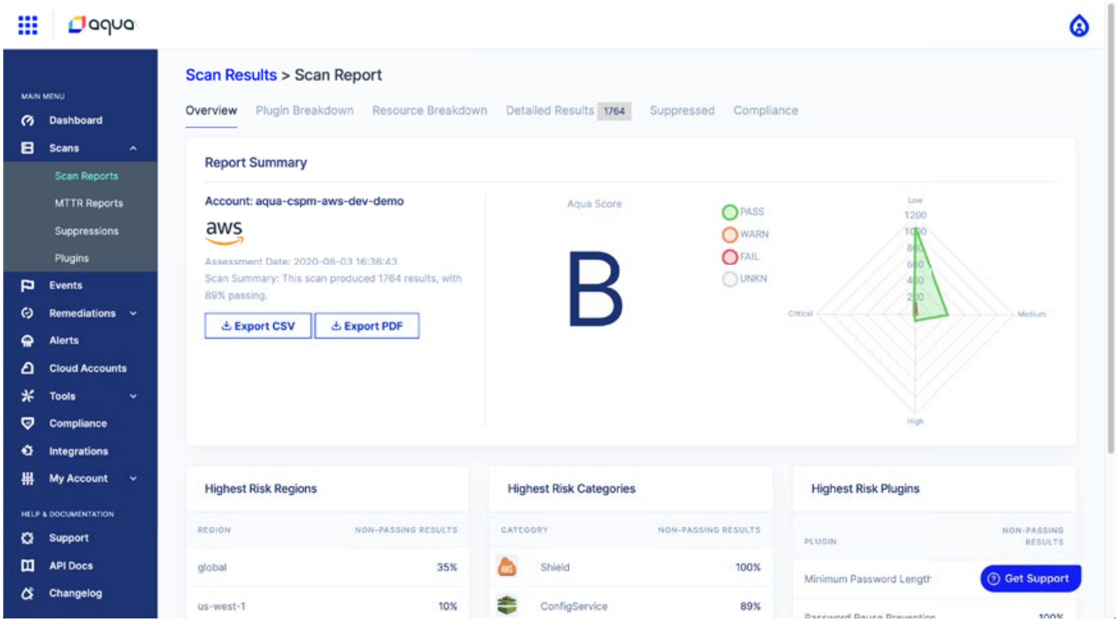
WHAT

Alice&Bob.Company provides a managed CSPM solution, based upon Aqua. As a certified Aqua Sec partner and reseller, Alice&Bob.Company sets up the environment on behalf of the clients and takes over the operational responsibility.

This, on the one hand, gives our clients free resources to improve their digital product, on the other hand generates continuous insights into their cloud deployments, also across multiple public cloud vendors.

The most relevant public cloud platforms available are supported:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform



Scan Results > Scan Report

Report Summary

Account: aqua-cspm-aws-dev-demo

Assessment Date: 2020-08-03 16:36:43

Scan Summary: This scan produced 1764 results, with 89% passing.

Highest Risk Regions

REGION	NON-PASSING RESULTS
global	35%
us-west-1	10%

Highest Risk Categories

CATEGORY	NON-PASSING RESULTS
Shield	100%
ConfigService	89%

Highest Risk Plugins

PLUGIN	NON-PASSING RESULTS
Minimum Password Length	
Password Reuse Prevention	100%

Among others, the CSPM platform covers

- 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

Alice&Bob.Company will setup a new instance of the Aqua platform for the customer. This service is provided as a SaaS solution.

A&B will do all the initial configuration necessary. A&B attaches the CSPM platform read-only to client’s multiple cloud accounts. Afterwards A&B integrates into automation, set thresholds, and configure required alerting.
When the platform starts working, Alice&Bob.Company constantly maintains the CSPM platform for you. A&B tweaks and optimizes the CSPM configuration rules to minimize false positives and automate as much as possible.

Alice&Bob.Company takes over the operational responsibility. integrates to the alert and notification chain. This also includes real-time alerting. In collaboration with the customer - and considering the concrete scope of the contract – Alice&Bob.Company can fix simple security issues themselves.

More complex security incidents are tracked and handled by Alice&Bob.Company’s Security Incident Management process. They are resolved tandem working with the client.

The customer 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 entities are volatile or even cannot be consumed in a traditional client/server way. Especially Kubernetes is extremely powerful, but also the source of innumerable security breaches. Container security expert know-how is very hard to find and even harder to scale.

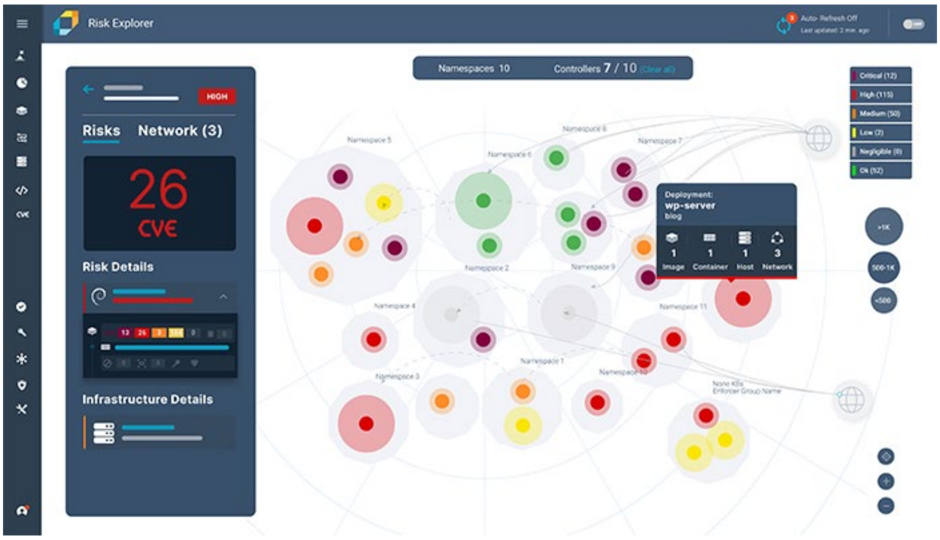
Enhance the security of your container and serverless environments, while leveraging all benefits of these technologies.

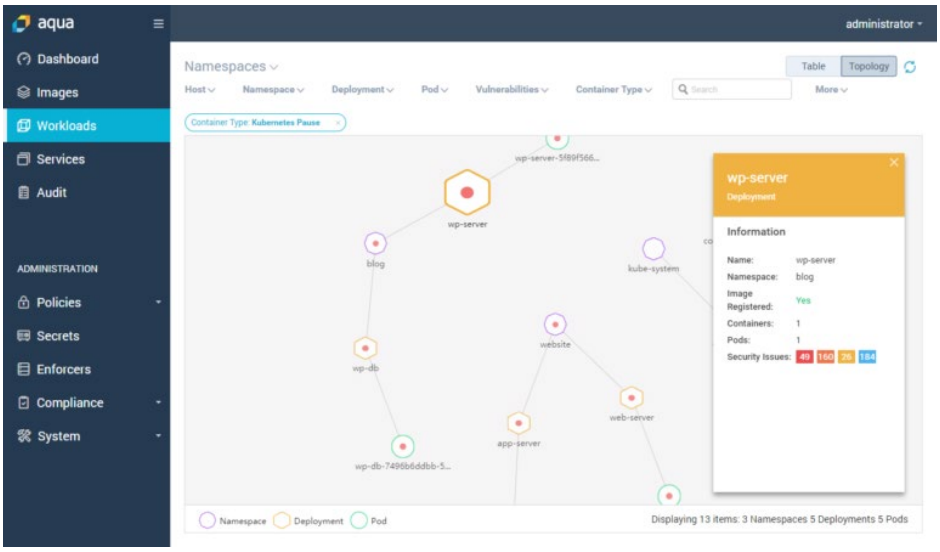
WHAT

Alice&Bob.Company provides a managed security solution, based upon Aqua CSP. As a certified Aqua Sec partner and reseller, Alice&Bob.Company sets up the environment on behalf of the clients and takes over the operational responsibility.

This, on the one hand, gives our clients free resources to improve their digital product, on the other hand generates continuous insights into their cloud deployment, also across multiple public cloud vendors.

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





wp-server
Deployment

Information

Name: wp-server
Namespace: blog
Image Registered: Yes
Containers: 1
Pods: 1
Security Issues: 49 160 26 184

Displaying 13 items: 3 Namespaces 5 Deployments 5 Pods

HOW

Alice&Bob.Company will setup a new instance of the Aqua Wave Enterprise for the customers. 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).

Alice&Bob.Company applies Aqua licenses, according to the distinct and contractual 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 can be easily integrated in Jenkins, Gitlab, Bamboo, Azure DevOps und CodeFresh
- Kubernetes Security, covering most prominent K8s platforms, i.e. Secure Red Hat OpenShift, TKGI, Rancher, Amazon EKS, Azure AKS, and Google GKE
- Behavioral Profiles
- Workloads Firewall
- Secrets Injection
- Real-time auditing and Forensics
- Drift preventing helps - based on an images digital signature - to prevent a large array of attack vectors, including zero-day attacks

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 deployed. The analysis is executed in a secure 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, A&B 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 fruits"
- CI/CD Integration

Alice&Bob.Company will perform all the initial configuration necessary and attaches the platform to client’s multiple cloud accounts your container platform. For serverless, an Aqua Layer has to be embedded into the code. A&B arranges this with corresponding teams. Afterwards A&B integrates into automation, sets thresholds, and configures required alerting.
When the platform starts working, Alice&Bob.Company constantly maintains the cloud native security platform for you. Configuration is tweaked and optimized to make you get the most out of the platform.

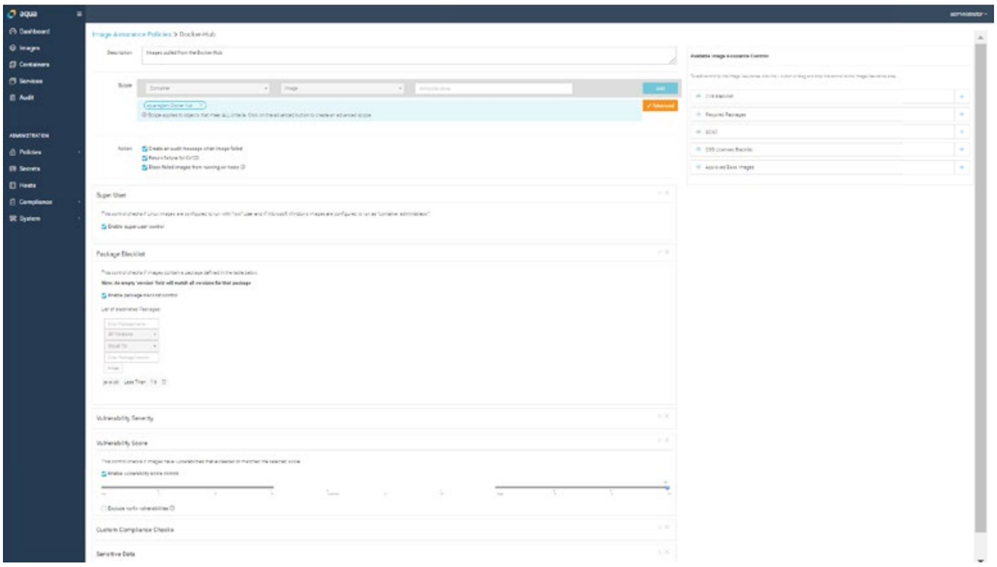


Image Assurance Policies > Docker-Hub

Description: Images pulled from the Docker Hub

Scope: Container · Image

Scope applies to objects that meet ALL criteria. Click on the advanced button to create an advanced scope

Action:
☑ Create an audit message when image failed
☑ Return failure for CI/CD
☑ Block failed images from running on hosts

Super User

This control checks if Linux images are configured to run with "root" user and if Microsoft Windows images are configured to run as "container administrator".

☑ Enable super user control

Package Blacklist

This control checks if images contain a package defined in the table below.

Note: An empty 'version' field will match all versions for that package

☑ Enable package blacklist control

List of blacklisted Packages

Less Than 1.6

Vulnerability Severity

Vulnerability Score

This control checks if images have vulnerabilities that exceeded or matched the selected score.

☑ Enable vulnerability score control

□ Exclude no-fix vulnerabilities

Custom Compliance Checks

Sensitive Data

Available Image Assurance Controls

CVE Blacklist

Required Packages

SCAP

OSS Licenses Blacklist

Approved Base Images

A&B takes over the operational responsibility. Therefore, Alice&Bob.Company will be added to the alert and notification chain. This also includes real-time alerting. After analysis of an alert-only phase, A&B recommends creating policies, that will preventively mitigate risks. In collaboration with the client - and considering the concrete scope of the contract – Alice&Bob.Company can fix simple security issues themselves.
More complex security incidents are tracked and handled by Alice&Bob.Company's Security Incident Management process. They are resolved tandem working with the client.

The customer will get direct access to the CSPM tool, can take advantage of the detailed reporting without the hassle and burden to get the platform managed.

This service is built upon 03 Launch services.

MANAGED PERIMETER PROTECTION

WHY

Running public websites, i.e. e-commerce platforms, IoT applications and portals, always require public access from all over the internet. To protect those dynamic web applications against external attackers as good as possible, you need to implement a so-called perimeter protection.

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

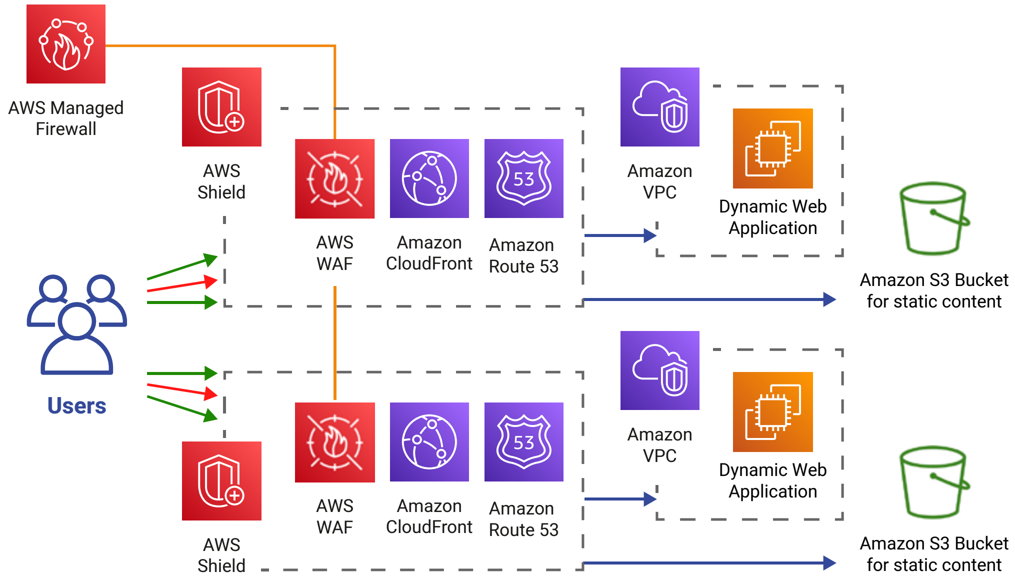
WHAT

Alice&Bob.Company provides perimeter protection as a managed service. The goal is to secure customers' applications and origin infrastructure from cyber security attacks such as Distributed Denial of Service attacks, SQL Injection or Cross-Site Scripting.

This suite of services includes

- AWS Managed Firewall,
- AWS WAF,
- AWS Shield, and
- AWS Firewall Manager

Alice&Bob.Company is directly connected with the AWS DDoS Response Team (DRT). This means, in case of a cyber-attack affecting your infrastructure, A&B is quickly able to escalate within the organization, within known processes and structures.



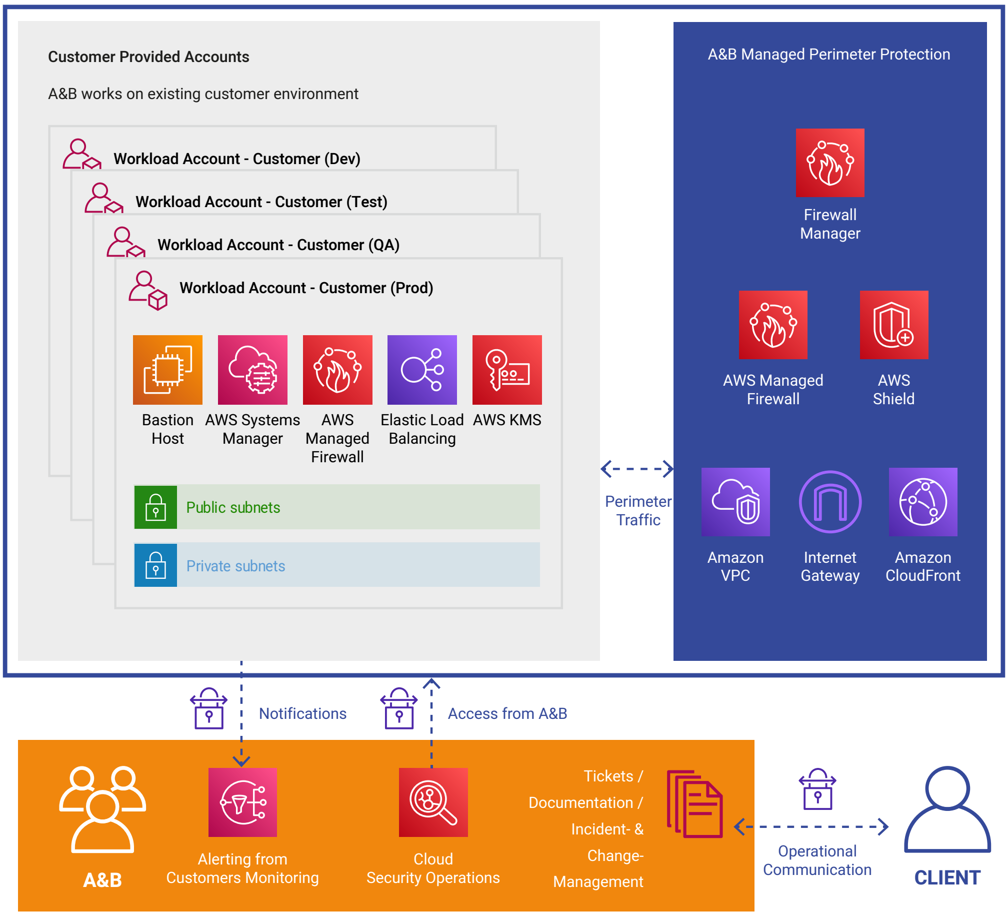
A&B Managed Perimeter Protection includes the following activities for customers:

- 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. Therefore Alice&Bob.Company maintains a dedicated AWS account for each client and routes the egress/ingress traffic through it.



Customer Provided Accounts
A&B works on existing customer environment
Workload Account - Customer (Dev)
Workload Account - Customer (Test)
Workload Account - Customer (QA)
Workload Account - Customer (Prod)
Bastion Host
AWS Systems Manager
AWS Managed Firewall
Elastic Load Balancing
AWS KMS
Public subnets
Private subnets
Perimeter Traffic
A&B Managed Perimeter Protection
Firewall Manager
AWS Managed Firewall
AWS Shield
Amazon VPC
Internet Gateway
Amazon CloudFront
Notifications
Access from A&B
A&B
Alerting from Customers Monitoring
Cloud Security Operations
Tickets / Documentation / Incident- & Change-Management
Operational Communication
CLIENT

According to customer´s requirements A&B implements one or more of the following services:

- A&B activates WAF services and sets up a ruleset to secure customers applications on layer 7
- Depending on customer requirements A&B will manage the rulesets according to an established workflow and setup subscriptions of rules to ensure up-to-date protection.
- A&B enables AWS Shield (Standard or Advanced) and implements defensive workflows in close collaboration with the customer and the AWS DDoS Response Team
- A&B deploys and operates AWS Firewall Manager for a central & cross-account firewall management integrated in AWS Organizations

Alice&Bob.Company will start integration with a testing and tuning environment first. While assessing risks and implementing health monitoring, Alice&Bob.Company ensures optimal performance for real user traffic and avoids false positives.

Afterwards, the Managed Perimeter Protection is put into production.

Therefore A&B

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

Alice&Bob.Company’s 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

Owning an automated, bullet-proof CI/CD pipeline is a vital fundament 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 customers workloads. It is the foundation for security automation.

WHAT

Alice&Bob.Company provide CI/CD pipepline as a managed service. It gives clients visibility and control inside and outside their CI/CD pipeline and increases code quality leading to cost reductions and an increasing ROI. A&B considers the CI/CD pipeline as the technical heart of the DevSecOps approach.

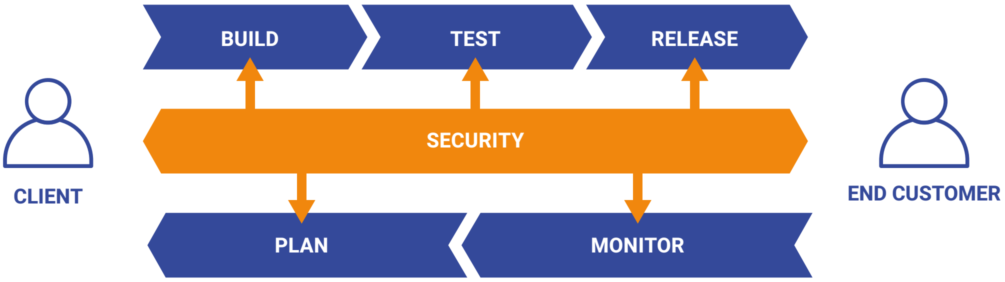
In order to provide the pipeline(s) as managed service A&B creates, automates, manages and continuously optimizes the clients CI/CD pipelines. This covers infrastructure, application and security.

Alice&Bob.Company develops a consistent process and continuously implements technical elements, i.e.

- 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 AWS specific services, including

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



HOW

Alice&Bob.Company analyzes the customers deployment processes and its requirements and develops a CI/CD pipeline architecture, which considers your organizational, procedural and technical conditions. A&B creates, optimizes, automates and implements security in targeted CI/CD pipelines.

A&Bs course of action is made of the following steps:

- CI/CD Pipeline Assessment and comparison to best practices
- Creating and adapting the pipeline in regard to defined best practices
- Monitoring the CI/CD Pipeline for 12 consecutive months after go-live

CI/CD Pipeline Assessment

During the assessment A&B runs a workshop focusing on the single stages of your software delivery. Information about the pipelines state, its challenges and requirements are being 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 assessments results A&B optimizes an existing pipeline or creates a new pipeline with the goal to deliver a fully managed build service with integrated comprehensive security checks. A&B prefers usage of AWS services (AWS CodeBuild, AWS CodeDeploy), nonetheless A&B is open to other solutions.

Monitoring

After provisioning of the pipeline A&B monitors the CI/CD pipeline itself as well as code that’s actively being deployed. A&B constantly checks the pipeline and its components for:

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

Monitoring will be made accessible and regular reports will be generated. Findings will be rated and described in a consolidated report. A&B optionally provides resolution measures after consultation.

This service is built upon **03 Launch** services.

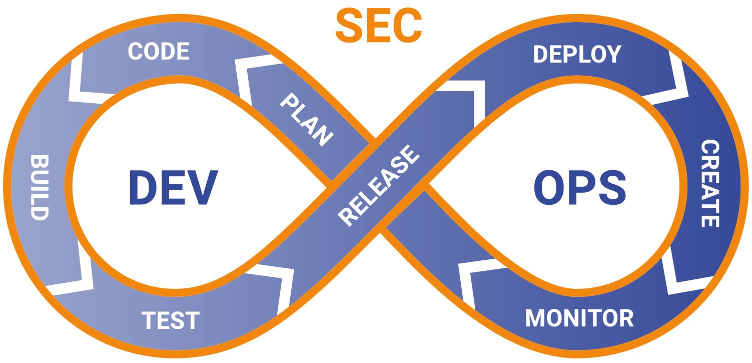
SECURITY CHAMPIONS PROGRAM

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 overwhelms 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

Alice&Bob.Company enables teams to act as Security Champions by example. After integrating in the team, A&B employees start to implement security-as-code in each phase of the DevSecOps pipeline and reach a high degree of security automation.



Together with the client’s leadership team and in alignment with the general companies’ security policies, the Security Champions Program covers e.g.

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

Besides integrating the measures, A&B acts as a security influencer within the organization and distributes the knowledge across various product teams to establish a security culture.

Additionally, Security Champions lead security automation programs and help teams to integrate security-as-code in each phase of their software development lifecycle.

HOW

The Alice&Bob.Company follows its very own "integrate&enable" approach to get the most out of the program for the client and create a customer centric program, that addresses organizations, teams, and tools.

Integrate

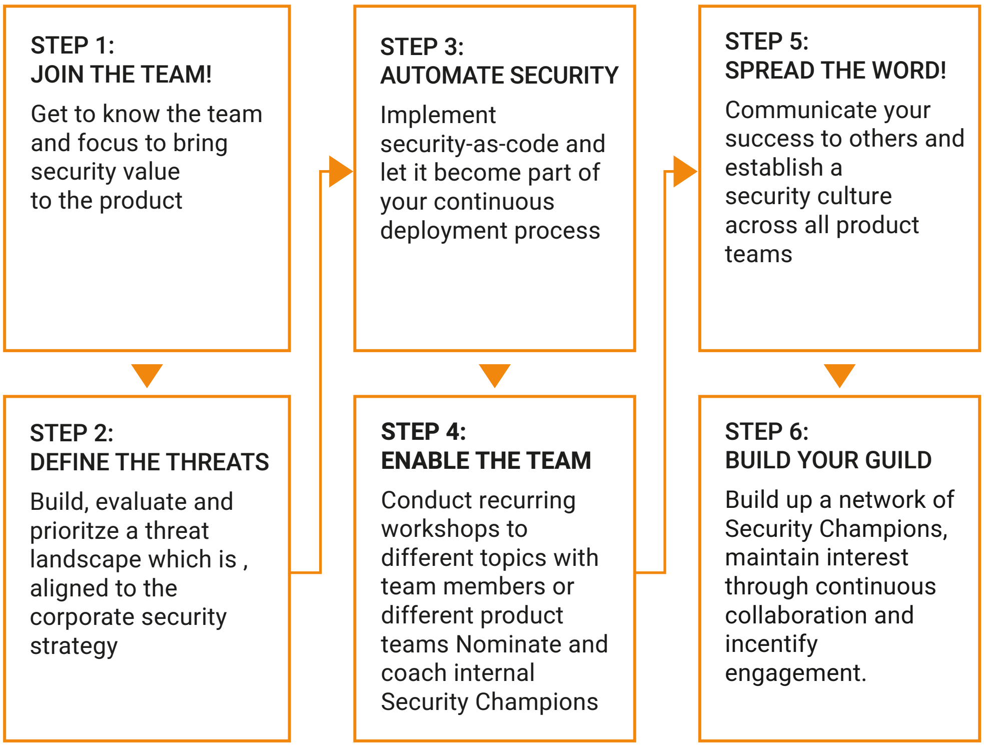
The A&B Security Champion integrates immediately in clients product team, defines possible threats in mutual workshops and starts leading the change. After clarification, the Security Champion starts implementing Security-as-Code in all phases of the DevSecOps lifecycle.

Enable

As interim Security Champions and mentors, A&B not only implements Security-as-Code, but onboards clients novice Security Champions, empowers them with recurring trainings on how to become a Security Champion and sets up the right communication channels to build a network of Security Champions.

A&B follows the Security Champions Playbook initiated by OWASP

Integrate and enable approach



STEP 1:
JOIN THE TEAM!
Get to know the team and focus to bring security value to the product

STEP 2:
DEFINE THE THREATS
Build, evaluate and prioritize a threat landscape which is , aligned to the corporate security strategy

STEP 3:
AUTOMATE SECURITY
Implement security-as-code and let it become part of your continuous deployment process

STEP 4:
ENABLE THE TEAM
Conduct recurring workshops to different topics with team members or different product teams Nominate and coach internal Security Champions

STEP 5:
SPREAD THE WORD!
Communicate your success to others and establish a security culture across all product teams

STEP 6:
BUILD YOUR GUILD
Build up a network of Security Champions, maintain interest through continuous collaboration and incentify engagement.

After starting with a "lighthouse" team, A&B continues to roll-out the program across various teams.

Once the Security Champions Program is initially rolled out, A&B will take care to continuously improve the program. There will be bi-weekly moderated team retrospectives with the novice client Security Champions.

SECURITY CHAOS ENGINEERING PROGRAM

WHY

Modern digital platform become more and more distributed and automated. The new way of including external services as source for building own services has become the natural way to go. Consequently, infrastructure and applications become somehow more complex.

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, i.e. faults in real world situations, 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 practically tackles rather simple vulnerabilities rooted in human error and system glitches, instead of assuming attacks being initiated from sophisticated nation-state actors or hacktivists.

With Alice&Bob.Company's integrate and enable approach, it implements and maintains a SCE program into clients existing DevOps or agile working culture.

HOW

Alice&Bob.Company delivers a 12 month program to establish SCE culture within your company. Therefore Alice&Bob.Company works collaboratively with the Clients Management Team and existing security organization in order to get the program ignited.

After performing the team kickoff, Alice&Bob.Company starts a number of initiatives to define the individual scope, coach the concepts of SCE and rolls 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. Therefore A&B

- Sets the scope,
- Teaches the concepts of chaos experiments,
- Enables the client to craft Security Chaos Experiments,
- Develops collaboratively an experiment design process,
- Implements automated Security Chaos Experiments in existing CI/CD pipelines and
- Trains and enables the team

A&B will take care to continuously maintain and improve the program over the contractual period. Therefore A&B will arrange moderated team retrospectives in bi-weekly intervals.

CLOUD SECURITY TRAININGS

WHY

Gain general security awareness and competency! The field of cloud security is continuously evolving. 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. Alice&Bob.Company trains, consults and enables clients teams on a mid- to long-term track on the latest releases and developments.

So, clients can focus on their core business: Making the best products!

HOW

A&B integrates with the targeted teams to understand their overall cloud expertise and individual cloud maturity level.

Based on that A&B develops a customer individual trainings plan. The plan is usually scheduled over a timeframe of 6 to 24 month with recurring trainings on agreed topics.

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

The goals and trainings are agreed with the clients' leadership team as well as product teams but can be changed upon need to meet clients vast changing requirements.

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

CUSTOM TAILORED MANAGED SERVICE

Profit directly from A&B’s long year team expertise in design, implementation and operation of cloud environments. The founding team members of Alice&Bob.Company are part of the early cloud pioneers in Germany and have more than 10 years experience in providing managed services for demanding business customers.
We earned 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