MATERNA
Information & Communications

DevSecOps Guide to Leveraging a Culture of Security

EBOOK

aws

Table of contents

INTRODUCTION

Why AWS for DevOps?

Organizational culture—shared values, mindsets, and behaviors that guide all employees—has everything to do with how successful an organization can be. Smaller teams within the business can adopt a specific culture that guides decisions on their focus area. A culture of security applies across a business from everyday best practices to developing modern applications in the cloud.

In this eBook, you'll discover how AWS enables you to start creating a culture of security by combining your organization's own guiding principles and the DevOps philosophy of working. You'll explore how this approach impacts modernization and development strategies, and you'll learn how to build a pipeline of continuous integration and development that elevates every level of the business.

A culture of security unites employees on a common path to business stability and modernization.

Organizations that are migrating to the cloud as a step toward modernizing must adopt an entirely new mindset around security and start to better leverage modern technologies and operational models, such as DevOps.

DevOps—bringing together formerly siloed development and operations teams—is a combination of cultural philosophies, practices, and tools that merges software development with information technology (IT) operations. DevOps enables companies to accelerate delivery of new application features and improved services to customers.

DevSecOps integrates security processes into the DevOps model. With DevSecOps, businesses can rapidly deliver secure and compliant application changes while running operations consistently with automation. This starts with developing operating tenets they can apply when shaping their vision for security as their business evolves.

When updating their security culture, successful organizations ensure that everyone understands the need for change and the path to reaching their common goal. Crucial steps in developing actionable tenets include:

- Working with all employees to identify the organization’s core values that serve as the foundation for the tenets.
- Establishing guidelines, expectations, and accountability for following the tenets—while empowering every team to follow them.
- Garnering company-wide buy-in for the tenets and the new culture they support.

At the highest level, each tenet should:

1. Be memorable.
2. Relay only a single idea.
3. Be specific to a program (e.g., security).
4. Guide, not proscribe.
5. Keep the business focused on the overall goal.

To guide their decisions and actions, businesses can apply the AWS-created tenets below. Organizations with an established culture of security with DevSecOps use the most common tenets to address:

Constant attacks
Build the understanding that the business is constantly under attack—both deliberately and accidentally—into every process.

Education
Prioritize security education for all employees. Stay abreast of developing threats, accept advice from security specialists, and seek to understand the organization’s security policies and rules.

Hygiene
Evangelize company-wide that good security hygiene is part of doing things right. Do not share passwords or user accounts or expose personal information. Use secure coding practices.

Continuous improvement
After an error in protocol, take feedback to ensure it doesn’t happen again.

Zero-defect approach
Do not accept any known vulnerabilities. Do not triage security defects and problems: Fix every issue as soon as it arises.

Reusable tools

Build and share security tools and processes—such as reusable logging and monitoring, enterprise-wide user provisioning, and standardized onboarding and offboarding processes for employees—across all IT systems.

Unified team

Ensure that all parts of the organization collaborate to strengthen security and enable resilient systems.

Testing

Rigorously test systems for vulnerabilities with automation—including failure scenarios and quality of response—both during development and production.

Threat modeling

Think as bad actors do to identify possible entries to attack, and then test to defend against them.

Peer reviews

Consider any possible defects and security vulnerabilities in the work and ensure peers always review the code.

Learn more about how tenets come into play on a cloud journey.

In an established culture of security, an organization educates every employee in how to detect a potential threat, minimizes risk, and establishes a recovery plan. By acting proactively rather than reactively, the business is better positioned to protect themselves, their products and services, and their customers.

Below are just a few examples of what a culture of security looks like in action.

Employee-exposed passwords

Today

IT resets password(s), updates anti-virus software, and sends employee a link to reread the organization’s security policy.

In a culture of security

Multi-factor authentication (MFA) is set by the organization; even though the password was exposed, the account is not compromised as a second factor is required to authenticate. The user will reset their own password and notify IT of the incident.

Hacked customer loyalty database

Today

A phishing email with undetected malware exposes thousands of customer credit cards.

In a culture of security

Users are aware that email phishing is a threat, and don’t click or respond to potentially malicious content. Additionally, the user reports the questionable email to the organization’s security team.

Unauthorized internal access to data

Today

The organization defaults to granting employees full access to internal data.

In a culture of security

The organization establishes identity and access management practices (IAMs) that limit an employee’s access to only need-to-know data.

Skunkwork cloud infrastructure projects

Today

The dev team cuts a ticket and gets a help desk request to provision a cloud instance for staging.

In a culture of security

The team uses a cloud formation template that includes security policies and governance, then provisions the cloud on that automated script.

Code typo

Today

After being informed of the software failure, the business releases a patch that users must download from the website and manually install.

In a culture of security

DevSecOps team undergoes threat detection and modeling during software development; if a fix is required, the business automatically pushes it out to registered users.

After identifying and evangelizing their tenets through the business, the next step is to align them with design principles that guide security in their cloud strategy. Below are design principles that can help strengthen workload security.

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Restrict unauthorized access to data
- Prepare for security events

"The most popular misconception about moving to the cloud is that it’s a set-and-forget proposition. Everything will run like clockwork, right? Instead of falling into this trap, [businesses] should be thinking about what happens on Day 2—the day after the last server has been decommissioned, and everything is fully running in the cloud—and what [their] cloud governance strategy will be."

Dr. James Bland
Global Technology Lead for DevOps, Amazon Web Services (AWS)

After an organization develops and rolls out their tenets and design principles, they’re ready to set in motion their DevSecOps pipeline, which is critical to building a successful software factory that includes continuous:

- Integration (CI).
- Delivery and deployment (CD).
- Testing.
- Logging and monitoring.
- Auditing.
- Governance.
- Operations.

Identifying vulnerabilities during the initial stages of the software development process can significantly help reduce the overall cost of developing application changes, but doing it in an automated fashion can accelerate the delivery of these changes as well.

Leveraging AWS

To identify security vulnerabilities at various stages, organizations can integrate various tools and services (both cloud and third-party) into their DevSecOps pipelines. The advantage of AWS native tools and partner integrations is the ability to template an organization's CI/CD pipeline as infrastructure and scale it in the cloud.

Organizations that build cloud-native applications can leverage services and AWS Software Developer Kits (SDKs) so they don't have to reinvent the wheel when working around technical limitations. Integrating various tools and aggregating the vulnerability and security findings from scratch can be a challenge. AWS has the services and tools necessary to accelerate this objective and provides the ease and flexibility to build DevSecOps pipelines by integrating AWS cloud-native and third-party tools. The AWS DevSecOps pipeline reference architecture illustrates these DevSecOps practices—including Software Composite Analysis (SCA), Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST)—and the aggregation of vulnerability findings into a single pane of glass.

Start the DevSecOps journey with this step-by-step guide.

1. Undergo threat modeling

Define any threat vectors:

- What will move to the cloud in the next 18 months?
- How many points of entry are there?
- How does the business secure data in transit and data at rest?

Outcome:
An established point-in-time state of the state. It’s important to note that the business will continually add variables during the transformation.

2. Upskill, enable, and empower all teams

Having an excellent security posture means having teams that are constantly on top of all threats across the infrastructure with a focus on continuing education. Security is a constantly moving target and a shared responsibility among all teams: developer, operations, security, and non-IT.

Outcome:
A detailed plan to upskill teams and shape the culture around collaboration to meet the organization’s ever-changing security needs.

3. Implement a continuous security feedback loop across all stages of the delivery lifecycle

Establish and evangelize best practices around security coding standards, integrated security testing models for all pipelines, application security testing (AST), and vulnerability management.

Outcome:
Issue identification during code development and feedback loops, which helps accelerate remediation and reduce costs.

4. Establish policies and governance

It’s critical to ensure the business follows their policy and governance guardrails. Automate security policies to notify and remediate any violations or abnormalities.

Outcome:
Well-defined policy, governance, and automated remediation across the infrastructure and applications.

5. Gamify security and make it fun!

Consider implementing bug bounties for development, operations, and security teams. It’s a fun way to drive education and collaboration and to incentivize a security mindset—and help meet education and upskilling goals.

Outcome:
An engaged, always-on security focus with an element of fun.

About Materna

Why rely on Materna

As a long-standing and reliable partner of Amazon Web Services (AWS), Materna has excellent competencies in the areas of infrastructure, migration and cloud-native application development and modernisation.

The IT service provider presents itself as very competent across the entire software lifecycle in all project phases of a customer solution: from process consulting, functional and technical conception, security conception, customising and implementation, infrastructure construction and deployment processes to infrastructure and application opera-tion

Materna successfully uses Amazon Web Services (AWS) services to implement solutions for digital transformation. Materna is an AWS Advanced Consulting Partner, AWS Solution Provider and AWS Public Sector Partner with a focus on the competencies IoT, Customer Experience, Cloud Native Development and Mobile Applications and offers consulting, migration, modernisation, agile application development (cloud-native) as well as managed services in these areas.

Benefits of working with Materna

Holistic DevOps solutions
We offer a comprehensive range of services and software products that cover various aspects of DevOps. Whether it's infrastructure provisioning, application deployment, release automation or performance monitoring, we offer all services from a single source.

Comprehensive technical expertise

Our team has in-depth knowledge of AWS services, infrastructure and DevOps principles. Our team always stays up to date with the latest AWS technologies so that you benefit from the latest solutions.

Proven track record

We are proud of a number of successful DevOps implementations in various industries. Our past projects serve as tangible proof of our ability to deliver results.

Acceleration of time-to-market

We help you accelerate your software development and deployment processes by optimising every stage of your software development cycle. This includes automating processes, fine-tuning resource management and streamlining code delivery.

CASE STUDY

Mercedes-Benz AG

Challenge

The customer Mercedes-Benz AG receives daily support requests with attachments. The support team receives these requests via a ticket system, which is now being transferred to a modern, cloud-based solution and processes customer enquiries ever more efficiently.

Solution

A cloud-based application was realised as a customised solution for the implementation of the attachment service. This was implemented quickly and reliably by the DevOps team using the AWS services for storage, network and computing services and delivered automatically on a regular basis. delivered regularly and automatically.

Benefits

The use of the new attachment service permanently relieves the individual ticket systems. The cloud-based approach also has the advantage that storage space and processing power can always be scaled according to requirements over time.

Learn more

Read more about Materna and DevOps

Read more

Why AWS for DevOps?

Read more

You have questions?

Marcus Rieks
Senior Vice President Software Factory
E-Mail marcus.rieks@materna.group