WHAT IS...?

DevSecOps

www.itsmacademy.com

What's inside:

Integrating Security into DevOps

The digital transformation is real. Today, the idea that every company is a software company is well understood. According to the **2021 State of DevOps Report**, "highly evolved DevOps teams have consistently demonstrated better performance across four key software performance metrics: deploying to production on demand, reporting change lead times and mean times to recover under one hour, and change fail rates under five percent."

It's not enough, however, to just develop software quickly. At a time when the world is witnessing record security breaches and hackers are getting bolder and more sophisticated, companies must also integrate security practices throughout the software development lifecycle to better defend their applications and protect their data.

As more organizations embrace DevOps to accelerate software delivery and operational performance, understaffed security teams and long security reviews are increasingly viewed as a constraint.

DevSecOps offers a better way.

Gartner predicts that by 2022, 90% of software development projects will leverage DevSecOps practices, a 50% increase from 2019.

Everyone is responsible for security.

Integrating security into DevOps to deliver 'DevSecOps' requires changing mindsets, processes and technology. Security and risk management leaders must adhere to the collaborative, agile nature of DevOps to be seamless and transparent in the development process, making the Sec in DevSecOps silent.

Continue reading to learn more....

DevSecOps Defined

By definition, ***DevSecOps*** is “a mindset that "everyone is responsible for security" with the goal of safely distributing security decisions at speed and scale to those who hold the highest level of context without sacrificing the safety required.”

DevSecOps:

- Includes security professionals as part of the DevOps team
- Helps Dev and Ops professionals understand
  - How their decisions affect security
  - How they can work with security professionals to decrease and respond quickly to attacks
- Integrates security practices into DevOps processes
- Strives to automate core security tasks

Key Principles of DevSecOps

DevSecOps is built around a few important principles:

- ***Shifting Left*** – Addressing security much earlier in the process, whether that be earlier application security testing, being part of the application design team, helping harden/pre-secure images with security tools pre-baked-into those images, or even simply being consulted before development or infrastructure work begins.
- ***Cooperation > Internal Competition*** – Too much time and energy is wasted on building, protecting and fighting over turf. Everyone should be working toward the same organizational objectives, helping deliver on the mission of the organization, which means not focusing so intently on what each individual wants/needs, but instead looking at how we can all help each other. DevOps initiatives help tear down some walls, and DevSecOps seeks to continue that mission by tearing down all the walls.
- ***Scaling Through Automation*** – There is no way to scale human resources fast enough to keep up with the ever-changing cyberthreat landscape. The only way to “win” against attackers will be to apply a generous measure of automation.
- ***Measurable Outcomes*** – A lesson that we can learn from test-driven development (TDD) is that we must be able to measure for desirable outcomes, whether that be to add functionality to software or to make changes that are intended to provide positive security benefit such as cyber risk reduction.
- ***Business Transformation*** – Ultimately, the purpose of DevSecOps is to fundamentally change how the business functions. Making this a reality means changing culture, processes and technologies in order to better align everyone around delivering on the organization’s mission.

Culture and Management

DevOps and DevSecOps connect through a set of strong values – Culture, Automation, Lean, Measurement and Sharing (CALMS). Organizational culture represents the values and behaviors that contribute to the unique social and psychological environment of an organization.

For security professionals to be accepted within DevOps programs and eventually earn respect and equal treatment, they must not be viewed as threatening to the DevOps programs, nor can they be obstacles (real or perceived) to progress.

A good first step is to look at the prevailing incentive model. While there is a time and place for punitive punishments (sticks), security professionals will likely find better success altering the incentive model (carrots). They can start by modeling the desired behavior and by focusing on resilience as the goal, not the mythical "perfect security." A resilient organization is tolerant to change and incidents.

FAIL FAST.
RECOVER FAST.
LEARN FAST.

Resilience is achieved by putting The Three Ways – Flow, Feedback, Continual Experimentation and Learning – into action and by investing in a culture that puts a premium on learning.

DevOps and DevSecOps practitioners can learn a lot by exploring the many philosophies and models that are increasingly influencing the technology industry such as:

- Lean manufacturing
- Safety culture
- Culture models
  - Erickson's stages of psychosocial development
  - Westrum's organization types
  - Laloux's culture model

Lean manufacturing is a production philosophy that focuses on reducing waste and improving the flow of processes to improve overall customer value. It's imperative to apply Lean thinking for security to DevOps environments. This means minimizing overhead and waste, automating as much as possible, and placing emphasis on measurable results and effectiveness.

Wikipedia defines ***safety culture*** as **"**the collection of the beliefs, perceptions and values that employees share in relation to risks within an organization." Professor Sidney Dekker, who coined the term '**safety differently**' in 2012, promotes concepts such as learning from mistakes, no-blame management and accountable teams, all of which are applicable to DevSecOps.

Cultural models describe the dimensions of culture and how cultures evolve over time as prevailing values and beliefs change. Culture is a key component of DevOps and technology transformations and leaders play an important role in influencing culture. Moving to a generative, or high-performing organization, requires that organizations look closely at dimensions such as how information flows, how decisions are made and how the organization handles failures, to name just a few.

High-trust organizations encourage good information flow, cross-functional collaboration, shared responsibilities, learning from failure and embracing new ideas; all hallmarks of a generative (performance oriented) and high-trust cultural (**as defined by R Westrum**).

Laloux also emphasizes the importance of trust and the need to replace bureaucratic hierarchies with concepts such as freedom and responsibility, self-management and informed decision making, achieved via The Advice Process. The Advice Process states that "Any person making a decision must seek advice from everyone meaningfully affected by the decision and people with expertise in the matter." (Frederic Laloux, Reinventing Organizations)

Within organizations, individuals (and in the context of DevSecOps, security professionals) must look also at their personal progression through the **stages of psychosocial development**, as outlined by Erik Erikson. A first step may be rethinking both the positive ("trust") and negative ("mistrust") concepts that form the foundation of current ways of thinking and working.

Strategic Considerations

For DevSecOps to succeed, security professionals must be a cooperative partner, not an obstacle or adversary. This involves understanding that security is not about checking boxes or blindly following "best practices." A better approach is for security professionals to be a collaborative advisor who can help the organization answer the question: "How much security is enough?"

Useful practices include:

- Threat modeling
- Creating meaningful metrics
- Establishing context
- Performing risk management

By using these practices, organizations can strike a balance on exposure (real vs. perceived) and can also ensure that risks are defined in the context of the organization's activities and objectives.

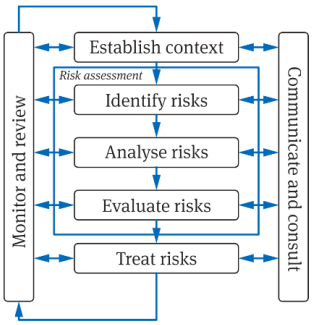


Figure 2 — The ISO 31000:2009 risk management process

ISO 31000 states that the risk management process starts by first establishing context, then assesses risk, and finally allows for treatment of risk if deemed appropriate.

In the context of DevOps, it's important to keep in mind that risk analysis is only useful if it can be provided in a timely manner. In a high-velocity environment where changes are being made on a daily basis, it is impractical to think that a full risk assessment work-up can be done on each of those changes.

Here again collaboration can be used to differentiate between low- and high-risk changes and to look at compensating controls you can put in place to improve resiliency.

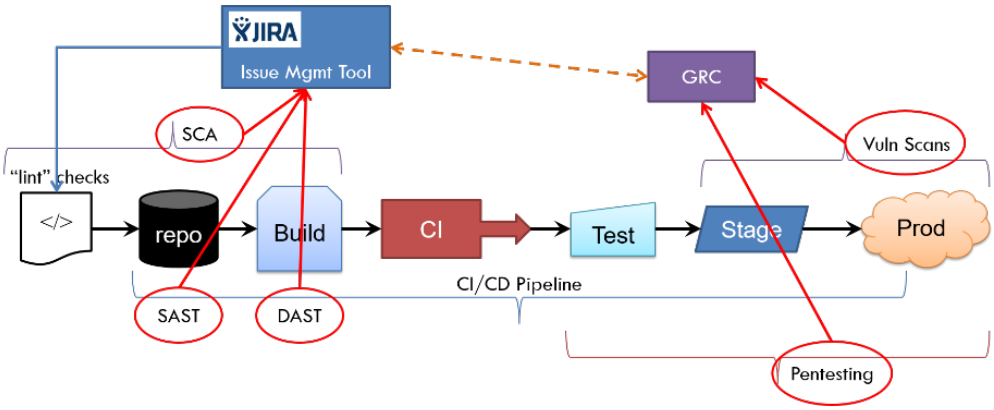
Application Security

There are a wide array of options for addressing application security and secure coding including automated testing and education and awareness. All of these practices can be applied in both legacy and DevOps environments, but become much easier in the DevOps world.

Automated Testing

Tremendous opportunity exists to integrate automated application security testing tools within the CI/CD pipeline. While not all tests can be automated (e.g., penetration testing cannot generally be automated), many can be. By understanding the pros and cons of these various testing methods, organizations can determine which to invest in automating and which testing capabilities should be reserved for the most critical applications or environments hosting the most sensitive data.

It's also important to consider how the data from these tests should be integrated into the organization's issue management (e.g., Jira) and Governance, Risk Management and Compliance (GRC) tools.



A major goal of application security testing should be to provide feedback in a way that developers can absorb and resolve findings in a "work as usual" manner.

Findings cannot be put into one-off reports that are handed to developers outside their normal operating cycles. Such a practice extends the feedback loop and often causes waste as developers have long since moved onto other things. Optimally, automate the collection of findings so that they can be addressed in a "work as usual" manner.

Education and Awareness

Education and awareness are important activities and can be delivered in a variety of ways. It is imperative to tailor training methods to the needs of the audience and measure those methods for effectiveness.

The Open Web Application Security Project Software Assurance Maturity Model (OWASP SAMM) Education & Guidance (EG) practice is focused on arming personnel involved in the software lifecycle with knowledge and resources to design, develop and deploy secure software.

The better developers understand how to write secure code and the reason it's necessary, as well as understanding application security testing and how to get the most value from it, the better off your overall application security will be.

GRC and Audit

Applying "shift left" thinking also to audit and compliance enables organizations to proactively identify, integrate and meet audit and compliance requirements.

GRC stands for Governance, Risk Management and Compliance and is a term that is often misunderstood. The misunderstandings arise as the term GRC may be used to describe:

- A class of tools/platforms
- A practice/program area

GRC tools/platforms typically hold policies, audit data, vulnerability and threat intelligence data, business continuity management plans and so forth. They are essentially large data repositories, but with APIs and the ability to automate data collection and perform at least some lightweight data analytics in support of dashboards and reporting requirements.

GRC may also describe a practice/program area, typically oriented around policy, compliance, audit, and risk management. These teams tend to be comprised of non-technical resources and are often at most a step or two removed from company executives and directors, at least in terms of routine reporting. As such, if there are concerns that need to be raised to the board level, GRC teams are a great partner to have in getting the message communicated.

GRC represents another big opportunity to tackle automation and integration within a DevOps environment. For example, many policies, standards and guidelines pertain to specific configuration requirements and recommendations and so can be implemented as code.

***Policy as code* is the idea of writing code to manage and automate policies.**

By representing policies as code, proven software development best practices can be adopted such as version control, automated testing and automated deployment.

Logging, Monitoring and Response

Log Management is the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving and ultimate disposal of the large volumes of log data created within an information system.

It is vital to setup a single common repository to collect log data.

It is understood that different teams will have different needs, which may in turn require different tools. Even if different teams need different interfaces for queries, reporting, alerts, dashboards, etc., it is still vital to setup a single common repository to collect log data. That way, you'll have a database of valuable information that you can access and analyze at any time.

Log data and threat intelligence are two major triggers for the incident response process.

Incident response is the method by which organizations identify and mitigate risks created as the result of a security breach or attack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Threat intelligence is data shared between concerned entities about attacks, hazards and mitigation details. It represents useful information about attacker means and methods (including about ongoing attacks) that can be shared among organizations to help protect each other.

Both incident response and threat intelligence provide integration and automation opportunities in a DevSecOps environment.

Summary

DevSecOps includes security professionals as part of the DevOps team and helps Dev and Ops professionals understand how they can work with security professionals to decrease and respond quickly to attacks.

Everyone is responsible for security!

For security professionals to be accepted within DevOps programs and eventually earn respect and equal treatment, they must not be viewed as threatening to the DevOps programs, nor can they be obstacles (real or perceived) to progress. They must be collaborative advisors.

Ultimately, the purpose of DevSecOps is to fundamentally change how the business functions. Making this a reality means changing culture, processes and technologies in order to better align everyone around delivering on the organization's mission.

Get Involved!

DevSecOps practices will continue to evolve through communities of practice. Seek out opportunities to collaborate with others and to share what you've learned.

BE A DEVSECOPS LEADER!

Culture change and progress cannot happen without the support of people like you. **Take action!**

Change related to DevSecOps initiatives will affect organizational culture. Effective communication plans, training and clear policies and procedures are all needed to achieve the desired performance outcomes and enable collaboration between the many stakeholders. Culture change and progress cannot happen without the support of people like you.

Contribute to your organization's DevSecOps effort by expanding your knowledge of DevOps and DevSecOps principles and practices and by using what you learn to lead improvement activities.

Want to Learn More?

Training helps organizations build and maintain their capabilities. Training also provides individuals the knowledge, skills and information needed to fill their role(s) in an organization or achieve their career goals, along with a place to test and develop the confidence to use these skills in the workplace.

ITSM Academy's **DevOps Campus** provides the courses you need to build a solid foundation and sharpen your skills as a DevOps practitioner.

Our **DevSecOps Foundation (DSOF)** course specifically addresses how DevOps security practices differ from other security approaches. Candidates obtain the education needed to understand and apply data and security sciences and learn the purpose, benefits, concepts and vocabulary of DevSecOps; particularly in how DevSecOps roles fit with a DevOps culture and organization.

For modern IT organizations, we believe that continuous improvement is achieved by leveraging and integrating the practices of multiple methods and frameworks. **Our portfolio** includes a full line of IT Service Management (ITIL), Agile Service Management, process design (CPDE), DevOps, Lean, and Site Reliability Engineering (SRE) courses – including certification courses, workshops and simulations.

Contact us to schedule time with a subject matter expert.

+1-954-491-3442	http://itsmacademy.com	info@itsmacademy.com

Additional Resources:

- ITSM Professor Blog - a WEALTH of knowledge published weekly since 2008
- Webinar Archives - Monthly since 2007
- ITSM Academy Resource Center

ITSM Academy

We are a female owned small business, established in 2004. Our extensive catalog contains accredited and sustainable IT Service Management (ITSM) education and advice including; ITIL®, DevOps, Process Design (CPDE), Agile, Site Reliability Engineering (SRE), Value Stream Mapping (VSM) and Experience Level Agreement (XLA). Our business values are founded on trust, loyalty, professionalism and long term relationships.

...educate and inspire is not just our corporate slogan, it speaks to our core mission and goal.

Follow our founder and CXO, Lisa Schwartz, on **LinkedIn**.

Instructors

Every ITSM Academy instructor is certified to the highest levels in the areas they train. They have years of hands-on IT practitioner experience, enabling them to effectively intertwine theory and real-life stories and scenarios. Using the highest quality content, this engaging training style encourages active group participation, allowing all learners to bring from class a wealth of practical and actionable knowledge.

Accreditations

All of ITSM Academy's certification courseware is developed or enhanced in-house and is accredited by independent, international organizations where applicable.

Game On! - Interactive Learning

Involves students in active learning, using the engaging qualities of a game, fueled by our subject matter experts.

Courseware Licensing (all developed or enhanced in house)

In addition to our public and corporate/onsite training, our courseware is available for licensing / co-branding under our flexible licensing program, including Train-the-Trainer (for qualifying organizations).

my.itsmacademy.com (digital portal)

Extends the learning experience with games, videos, exercises, sample exams, and course materials. It also provides instructors a vast repository of information and guidance to successfully prepare for and teach our courses.

Professional Education Hours (CPDs/PDUs/CPEs/CEUs):

ITSM Academy is proud to make it possible for individuals who attend our classes to earn professional education hours. (e.g., CPDs, PDUs, CPEs, CEUs). These professional education hours can be submitted to associations such as PeopleCert, the Project Management Institute and ISACA, if applicable.

Read More

The Story of the Academy

Today, ITSM Academy is widely recognized for its expertise in multiple IT frameworks (ITSM, ITIL, Process Engineering (CPDE), DevOps, Agile Service Management, Lean) and, more importantly, how they work together. But that's not where we started.