DELL Technologies

DevSecOps Overview & Bootcamp

DevSecOps Brochure

Foreword

The world is changing faster than ever before, and data is becoming ever more prevalent in the race to digitize. How we access and glean insights into our data is fueling innovation, driving positive change for the human race and pushing the boundaries for human potential.

But the world is not always a friendly place, and as we drive innovation with breakthroughs in connectivity, artificial intelligence and the way we manage huge amounts of data, we need to ensure that we can continue to do so without risk of ill-intention.

As the explosion of online data has driven regulation and compliance across the world, in a bid to ensure good practice in keeping our data safe, so to has it driven the opportunity for bad actors to exploit as more and more data comes online...

And as sure as night follows day, the more sophisticated the IT security ecosystem becomes, so to does the sophistication of those looking to exploit it.

Corporations, public sector organizations, sovereign nations all want to ensure data is safe from harm and want to ensure that advances in IT can be brought to bear for good use, without risk of consequence. To do this they must learn and employ the latest tools and techniques in a world that never stops moving forward, making use of those advances in IT to be more secure than ever before.

So keep moving forward & keep learning.

And remember…skills build confidence and confidence combined with skills helps us push the boundaries of human endeavour.

—Richard Thomas, EMEA Sales Director, Education Services

Innovation or Inertia

In Education Services we are finding that as more and more organizations embrace DevOps tools and practices as part of their Cloud Native journey's, evolving to Multi-Cloud, ensuring that the right infrastructure is used in the right place for the right workloads at the right times – to best serve the needs of the business – all with cost/compliance/business value in mind, that the speed of change for many is tough to keep up with and, of course, inertia is not an option for most.

More so as developers on board more and more tools that help them keep up with the speed of business. Whether that be Automation tools, Observability tools, or just the complexity of moving away from heavyweight virtual machine infrastructure towards more lightweight, agile, containerized environments that better serve DevOps lifecycles and the ability to move workloads more easily between clouds or cloud like infrastructure.

Furthermore, as organizations' move towards Microservices' architectures on their container platform of choice, or even multiple container platforms, that help them fuel innovation and speed to market, they are finding that an increased level of agility and sophistication is in turn driving an increased level of complexity.

Complexity & Risk

Architecture can often be dispersed. A particular business unit or cost center in many organizations may decide that one particular Cloud or DevOps toolchain set is most conducive to their requirements and skillsets – but that might not be the same across the whole organization. Another business unit, for example, might be more compelled towards another architecture, on different infrastructure, for compliance reasons perhaps. Test and Dev in a Cloud, production at scale on-prem. Edge, somewhere else.

Difficult to monitor and therefore difficult to manage, across the piece.

Which in turn exposes security risk… where inertia is not an option for anyone.

Containers & DevSecOps

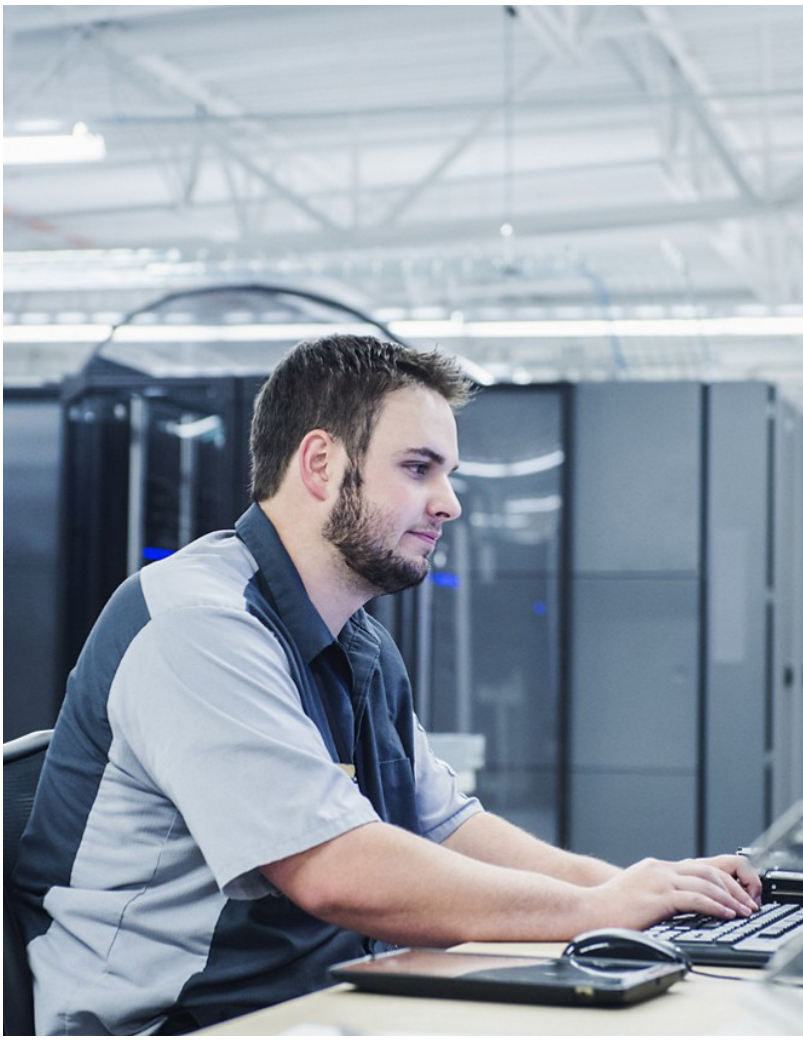
The move to containers makes sense – liberating infrastructure from OS dependency.

Containerized environments accelerate IT's ability to operate without shackles. Driving innovation. And whilst some use cases may be best suited to native Kubernetes architectures, others may be better served by proprietary platforms, like Azure (see our consultancy offerings for Microsoft DevSecOps here), or open source platforms, like Openshift (see our Openshift validated designs here). Depending on the requirements : best fit for purpose, but all of which necessitate a different mix of skills.

And all require the right skills.

And all require a unified standard of secure practice, of which below, are some activities to be mindful of:

- **Container image scanning:** Scan container images for vulnerabilities and known security issues before deploying them to production.
- **Runtime security:** Monitor and secure containers at runtime, including network segmentation, host-based firewalls, and intrusion detection and prevention systems.
- **Configuration management:** Automate the configuration of container hosts and ensure that all hosts are configured consistently and securely.
- **Continuous integration and delivery (CI/CD):** Implement CI/CD pipelines that automatically build, test, and deploy container images to production.
- **Access control:** Implement access controls to ensure that only authorized users can access and manage container images and hosts.
- **Continuous monitoring:** Continuously monitor the security of containers, including the host systems and the network, to detect and respond to security incidents.
- **Compliance:** Ensure that containers are deployed and managed in accordance with reguatory and compliance requirements.



A security mindset is imperative right from the get go. DevSecOps helps weave that security mindset into the business operation through the software development lifecycle, and of course, Education Services have training courses that can help with tomorrow's DevSecOps mindset.

DevSecOps

DevSecOps is a software development methodology that integrates security practices into the software development lifecycle (SDLC) from the start, rather than treating security as a separate and distinct phase.

This approach promotes collaboration and communication between development, security, and operations teams to ensure that security is considered at every stage of the SDLC, from design to deployment. The goal of DevSecOps is to improve the overall security and reduce the risk of security breaches by making security an integral part of the development process. It aims to shift security to the left in the development process so that security is integrated from the start and not an afterthought.

This can be achieved through the use of automation, testing, and other tools to ensure that security is built in from the beginning. Education Services can accelerate your journey with training on a wide variety of different tools through our rich partner eco-system.

Things to consider when adopting DevSecOps:

1. **Define security requirements:** Clearly define the security requirements for each project and ensure that these requirements are integrated into the development process from the start.
2. **Automate security testing:** Automate security testing processes such as vulnerability scans, penetration testing, and code analysis to ensure that security is integrated into the software development life cycle.
3. **Encourage collaboration:** Foster collaboration between development, security, and operations teams. This can be achieved through regular meetings, joint planning and decision-making, and a shared understanding of the importance of security.
4. **Embrace continuous integration and delivery:** Implement continuous integration and continuous delivery (CI/CD) pipelines to streamline the software development process and ensure that security is integrated at every stage.
5. **Use security tools:** Use security tools such as security information and event management (SIEM) systems, intrusion detection and prevention systems (IDPS), and firewalls to help detect and prevent security incidents.
6. **Implement a culture of security:** Create a culture of security by promoting security awareness, training and education, and encouraging employees to report security incidents.
7. **Continuously monitor and assess:** Continuously monitor and assess the security of your systems and applications, and use the data collected to improve your security posture over time.

There are an overwhelming amount of tools that help in these endeavours and Dell developer ready infrastructure, with API's for Automation tools and our Container Storage Interface plug-ins that expose infrastructure to Kubernetes environments, is very well suited to build out from. (See also our Cyber Recovery Solutions here)

Below are a handful of tools that help with some of the previous considerations:

- **GitLab:** An all-in-one DevOps platform that integrates source code management, continuous integration, and continuous delivery.
- **Snyk:** A vulnerability management platform that helps developers to find and fix vulnerabilities in their code.
- **Tenable.io:** A vulnerability management platform that provides continuous monitoring and assessment of network security.
- **Chef:** A configuration management tool that helps organizations to automate their infrastructure and application deployment.
- **Ansible:** An open-source configuration management tool that helps organizations to automate the deployment, configuration, and management of their systems and applications.
- **Jenkins:** An open-source continuous integration and continuous delivery (CI/CD) platform that helps organizations to automate the software development process.

These are just a few of the many DevSecOps tools available. The choice of tool will depend on the specific needs and requirements of the organization but we do look at some of these tools in our DevSecOps Bootcamp course.

DevSecOps is important because it helps organizations to:

1. **Improve security:** By integrating security into the software development process, organizations can improve the security of their systems and applications and reduce the risk of security incidents.
2. **Increase efficiency:** By automating security testing and incorporating security into the development process, organizations can reduce the time and resources required to build and deploy secure software.
3. **Foster collaboration:** DevSecOps encourages collaboration between development, security, and operations teams, helping to break down silos and ensure that everyone is working together towards a common goal.
4. **Embrace continuous delivery:** DevSecOps enables organizations to adopt continuous integration and delivery (CI/CD) pipelines, enabling them to release software more quickly and with greater confidence.
5. **Stay ahead of threats:** By continuously monitoring and assessing the security of their systems, organizations can stay ahead of new threats and vulnerabilities and be better prepared to respond to security incidents.
6. **Meet regulatory requirements:** DevSecOps helps organizations to comply with regulations such as PCI DSS and HIPAA, which require security to be integrated into the software development process.

DevSecOps Bootcamp - 3 Day Instructor Led

This course is designed as in introduction to DevSecOps by broadening students understanding of common DevOps tools, and how security plays with those tools. After an introduction to threat modeling, students will rethink existing DevOps pipelines to create Secure Software Development Lifecycles (SDLC). Lecture is used to drive hands on Kubernetes environments, where students will secure container-based applications, observe, and track activity.

Hands on Labs

- Threat Analysis
- CIS Benchmarking
- Cluster Audit Logging
- Deploying Falco to Monitor System Calls
- Encryption Configuration
- Creating a Docker Image
- Trivy
- Snyk Security
- Sonobuoy Kubernetes Security Validation Testing
- Tracee
- Understanding Security Contexts
- AppArmor
- gVisor
- Authorization
- Pod Limiting
- Securing Secrets
- HashiCorp Vault
- Deploying OSSEC
- Intro to Suricata
- Physical Intrusion Detection
- Building a DevSecOps Pipeline in GitLab
- GitHub Actions for DevSecOps
- “Shifting Left” with Jenkins

Connect with an Education Account Manager

Education Services Regional Sales Directors

Sarah Scardilli (NA)	Sarah.Scardilli@dell.com
Rich Thomas (EMEA)	Rich.Thomas@dell.com
Simone Malta (LATAM)	Simone.Malta@dell.com
Mike Rodwell (APJ)	Michael.Rodwell@gmail.com

Learn more about Dell Education services

Contact Education Services Support

View more training courses

Join the conversation with #DellTechLearn

DELL Technologies