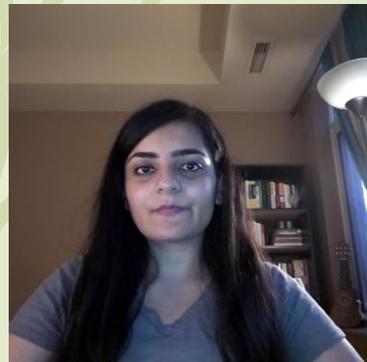# Agile to DevSecOps – One Mindset at a Time

Bhavyatta Bhardwaj

Agenda

- Let's talk Agile
- What is DevSecOps?
- The main distinction
- Do we want to move from Agile to DevSecOps?
- Challenges and Benefits
- Can we use DevSecOps in SDLC?
- DevSecOps Culture
- Key Take Aways

Agenda

- **Let's talk Agile**
- What is DevSecOps?
- The main distinction
- Do we want to move from Agile to DevSecOps?
- Challenges and Benefits
- Can we use DevSecOps in SDLC?
- DevSecOps Culture
- Key Take Aways

Let's talk Agile.

- Improved Quality.

- Focus on Users and Business Value.

- Stakeholder Engagement.

- Transparency and Visibility

- Early and Predictable Delivery.

- Predictable Costs and Schedule.

- Allows for Change
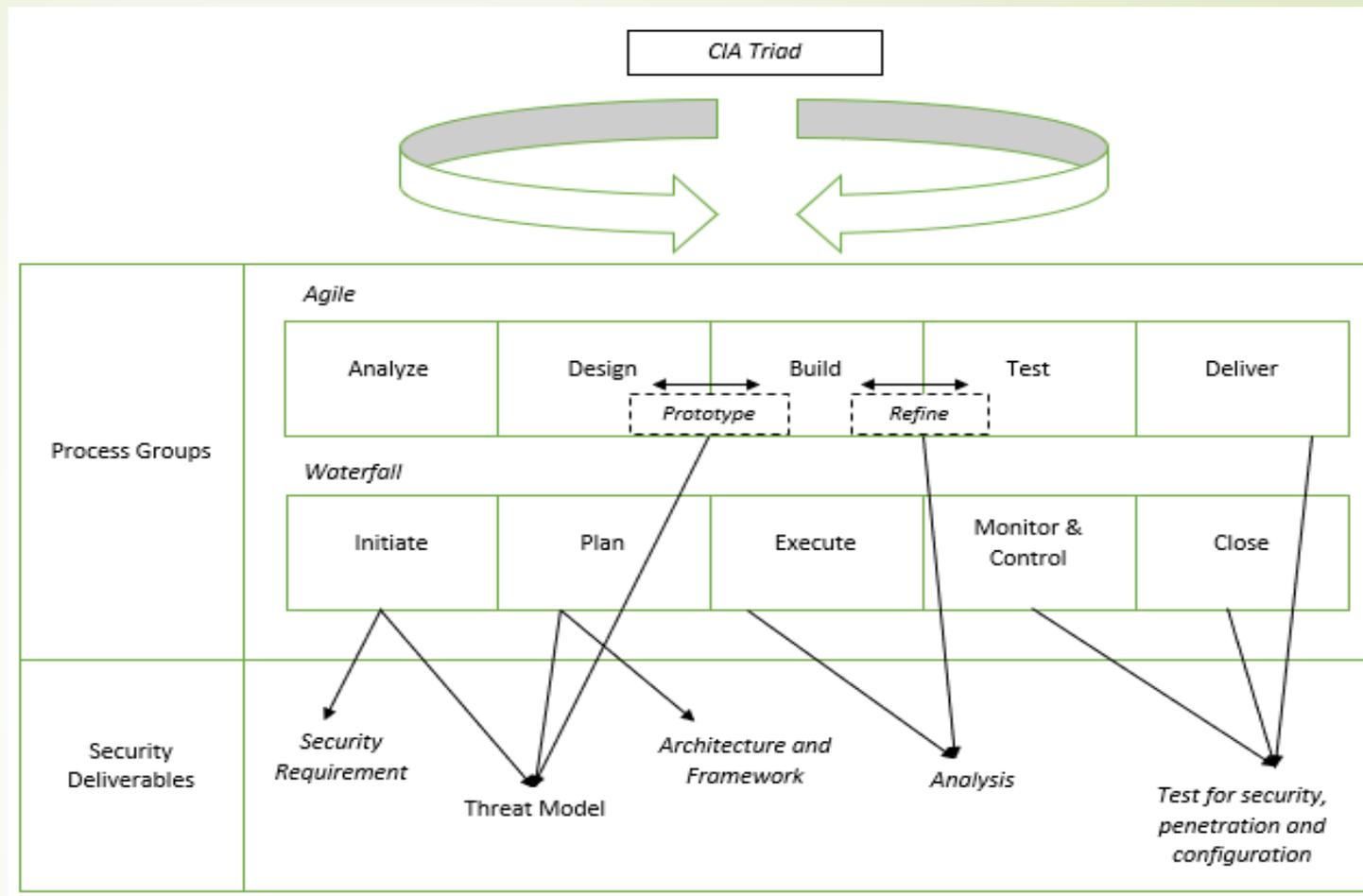
Streamlined project execution: Client requirements and any concerns need to be communicated across the team. A project manager will make sure that the project has well defined milestones and deliverables.

Strategic alignment: Keeping in mind the company's goals and security principles, a project manager will protect the project against threats or risks while ensuring delivery and measurable return of investment (ROI).

Optimized and Continuous resource allocation: A project manager makes sure that resources are assigned in priority, and that the cyber security projects are executed efficiently, keeping in mind the resource capacity.

Problem resolution: A project manager provides an objective to the cyber security project and ensures that the potential problems are addressed and resolved appropriately and in a timely fashion.

Risk management: Project evaluation may depend on risks to decide whether the   project should continue or not. Keeping that in mind, a project manager will lookout   for all the additional risks that may come in way.

- Let's talk Agile
- **What is DevSecOps?**
- The main distinction
- Do we want to move from Agile to DevSecOps?
- Challenges and Benefits
- Can we use DevSecOps in SDLC?
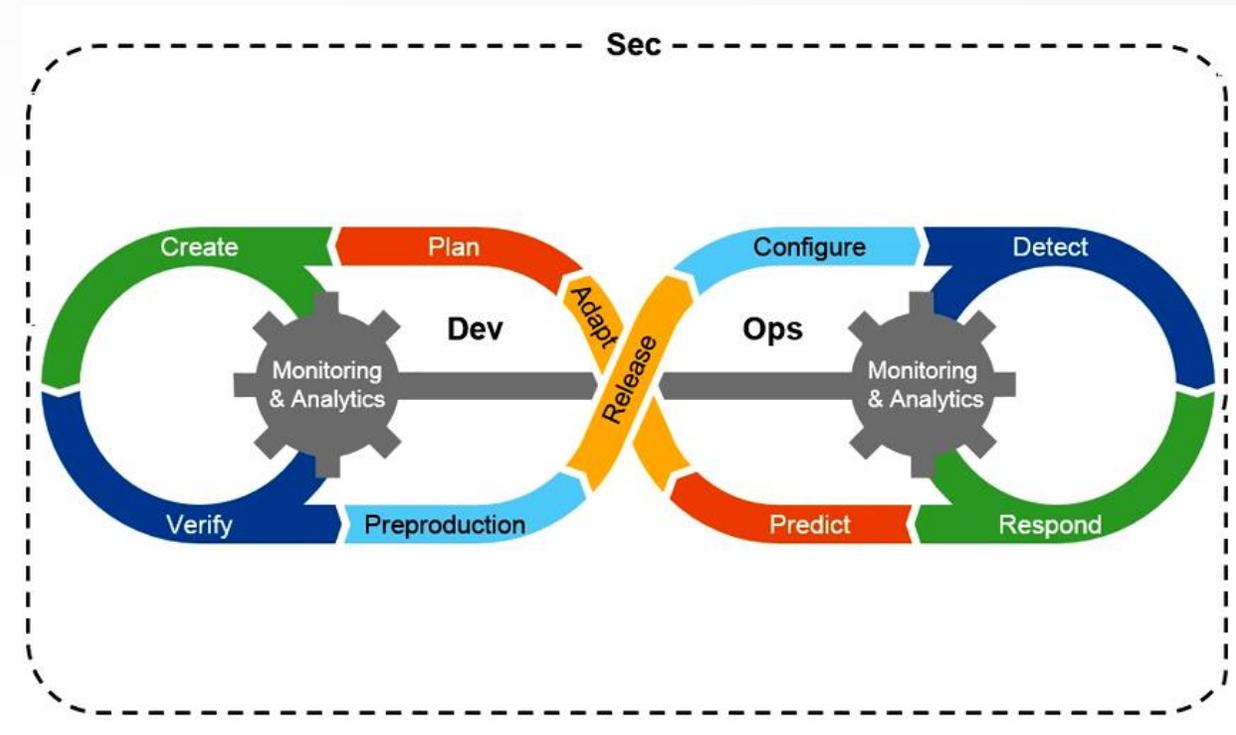- DevSecOps Culture
- Key Take Aways

What is DevSecOps?
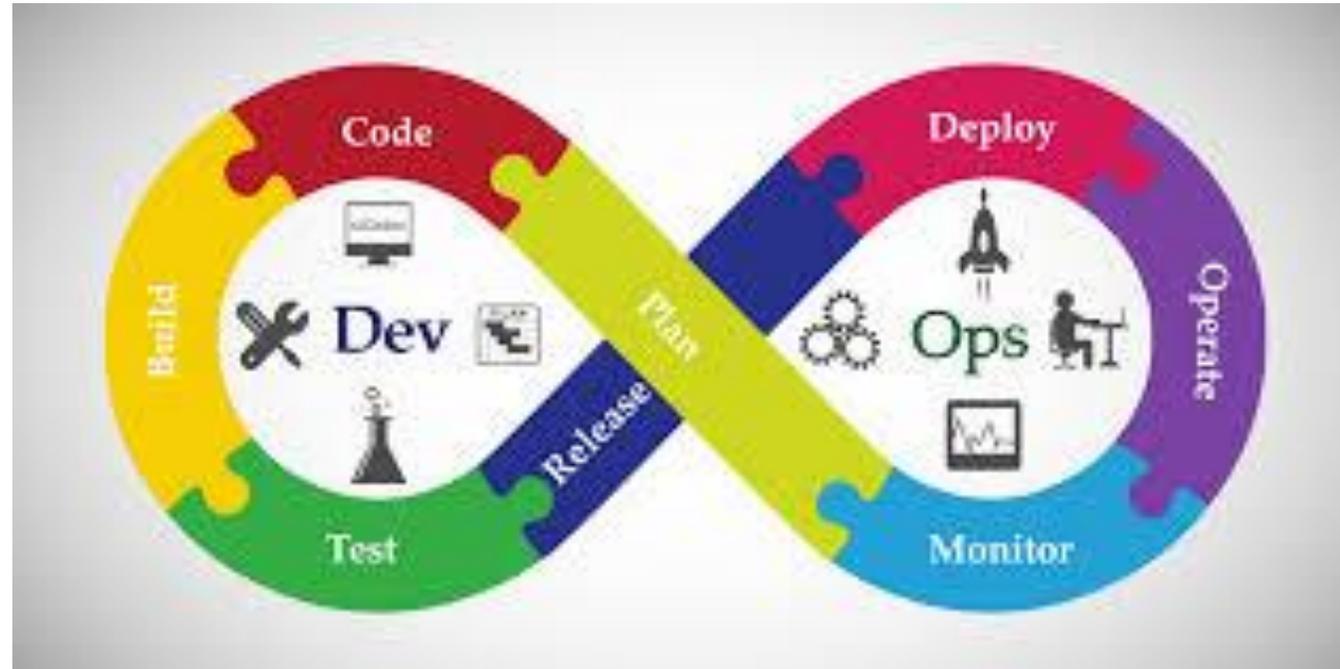
DevSecOps is an organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops) with its main characteristic being automation, monitoring, and applying security at all phases of the software lifecycle.

In DevSecOps, testing and security are shifted to the left through automated unit, functional, integration, and security testing - this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously.

- Let's talk Agile

- What is DevSecOps?

- **The main distinction**

- Do we want to move from Agile to DevSecOps?

- Challenges and Benefits

- Can we use DevSecOps in SDLC?

- DevSecOps Culture

- Key Take Aways

The main distinction

- Let's talk Agile

- What is DevSecOps?

- The main distinction

- **Do we want to move from Agile to DevSecOps?**

- Challenges and Benefits

- Can we use DevSecOps in SDLC?

- DevSecOps Culture

- Key Take Aways

Do we want to move from Agile to DevSecOps?

- According to globalnewswire, the DevSecOps market size is expected to grow from USD 1.5 billion in 2018 to USD 5.9 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 31.2% during the forecast period.

GREATER SPEED AND FLEXIBILITY, AND IT HELPS TO RESPOND TO CHANGE MORE EFFICIENTLY. BUT ONE OF THE MAJOR ADVANTAGES IS EARLY IDENTIFICATION OF VULNERABILITIES IN CODE.

WITH AGILE GETTING EVERYONE ONBOARD WITH PRIORITIZING SECURITY, AND HOLDING TEAMS ACCOUNTABLE FOR THE SECURITY OF THEIR PRODUCTS AND SERVICES IS A CHALLENGE

DEVSECOPS BRINGS BETTER COLLABORATION AND COMMUNICATION AMONG TEAMS.

- Let's talk Agile

- What is DevSecOps?

- The main distinction

- Do we want to move from Agile to DevSecOps?

- **Challenges and Benefits**

- Can we use DevSecOps in SDLC?

- DevSecOps Culture

- Key Take Aways

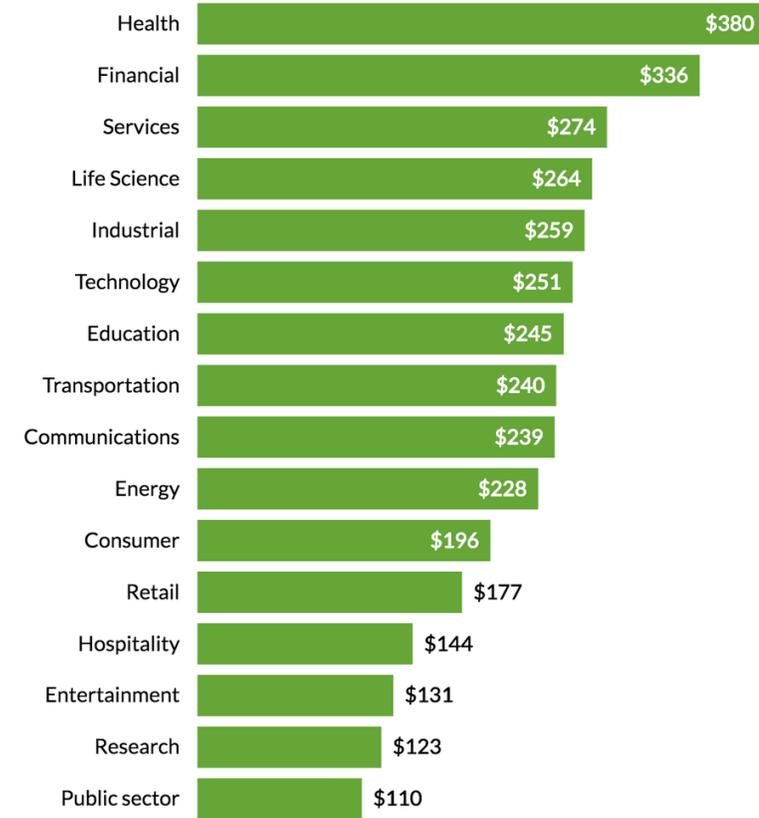# Challenges

- People

- Process

- Technology

Benefits

- Observability

- Collaboration

- Traceability

- Confidence and Compliance

⚠ WARNING A report by Cybersecurity Ventures reveals that in another two years, cybercrime will cost the world $6 trillion annually in damages.

The Industries Where Data Breaches Are Most Expensive
Cost per record breached

Industry	Cost
Health	$380
Financial	$336
Services	$274
Life Science	$264
Industrial	$259
Technology	$251
Education	$245
Transportation	$240
Communications	$239
Energy	$228
Consumer	$196
Retail	$177
Hospitality	$144
Entertainment	$131
Research	$123
Public sector	$110

Data source: IBM, Ponemon

splunk>

- Let's talk Agile

- What is DevSecOps?

- The main distinction

- Do we want to move from Agile to DevSecOps?

- Challenges and Benefits

- **Can we use DevSecOps in SDLC?**

- DevSecOps Culture

- Key Take Aways

Risk Mitigation

| Develop | Test | Artifacts | Deploy | Monitor |

- Risk Assessment and Control
- Security Architecture/Design

- Review
- Verification

- Test Case
- Scan reports
- Misuse case

- Change Management

- Security Monitoring
- Detection

Can we use it in SDLC?

- Infuses Risk Mitigation activities throughout the pipeline
- Reduces defect rate and vulnerabilities in code

- Let's talk Agile

- What is DevSecOps?

- The main distinction

- Do we want to move from Agile to DevSecOps?

- Challenges and Benefits

- Can we use DevSecOps in SDLC?

- **DevSecOps Culture**

- Key Take Aways

DevSecOps Culture

Mindset	Elimination of Silos	Shared Objectives

DevSecOps as a Culture

The basis of DevSecOps culture is a foundation of empowerment and transparency – with shared goals and metrics to help bring teams together and building the culture of trust.

- Mindset – Strategy is important but without an enabling and empowering mindset, it won't amount to much

- Elimination of Silos – Bringing transparency in work and allowing inter-departmental work a chance

- Shared Objectives – All teams increase their success rate when goals can be shared and clearly measured

Teams will need to think differently, behave differently, and eventually turn those changes into habits so that security becomes a natural part of their day-to-day work

- Culture change starts at the top

- Awareness, education, and mutual understanding

- Appoint security champions in dev

- Encourage cross-functional collaboration

- Give developers the tools they need

- Automate when and where appropriate

Agenda

- Let's talk Agile

- What is DevSecOps

- The main distinction

- Do we want to move from Agile to DevSecOps

- Challenges and Benefits

- Can we use DevSecOps in SDLC

- DevSecOps Culture

- **Key Take Aways**

Key Takeaways

- Security is everyone's responsibility

- Security is becoming an integral part of every process and sub-processes, and the feedback should be used for continuous improvement

- DevSecOps is not one size fits all – It will take time to adopt, but it's also here to stay

Then what is DevSecOps for you?