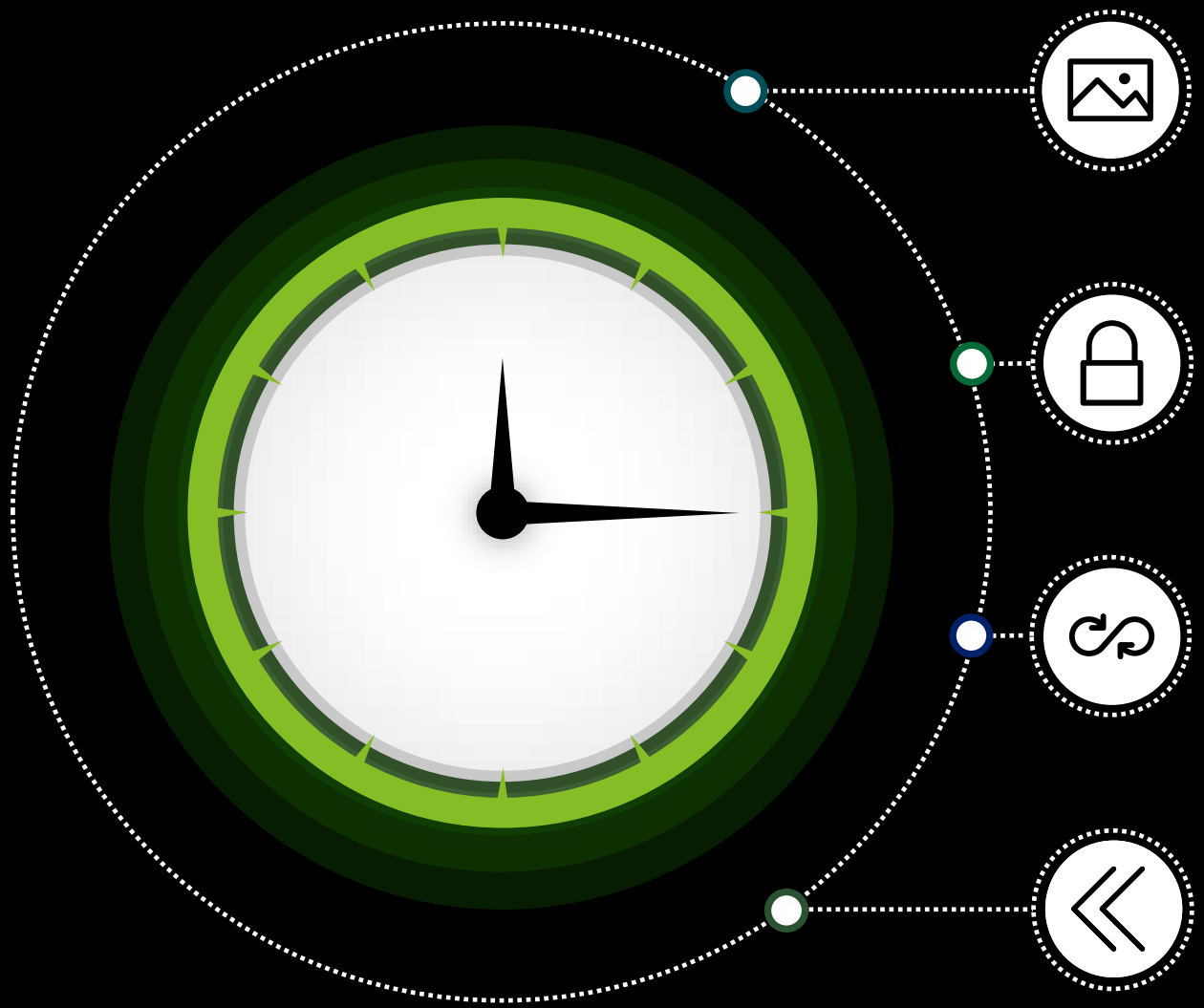
Deloitte.

Beneath the Surface

Keeping up with Modern Application Security

Deloitte & Touche LLP, Cyber and Strategic Risk

Agenda



Evolution of Software Landscape

Security in SDLC

Security in DevOps

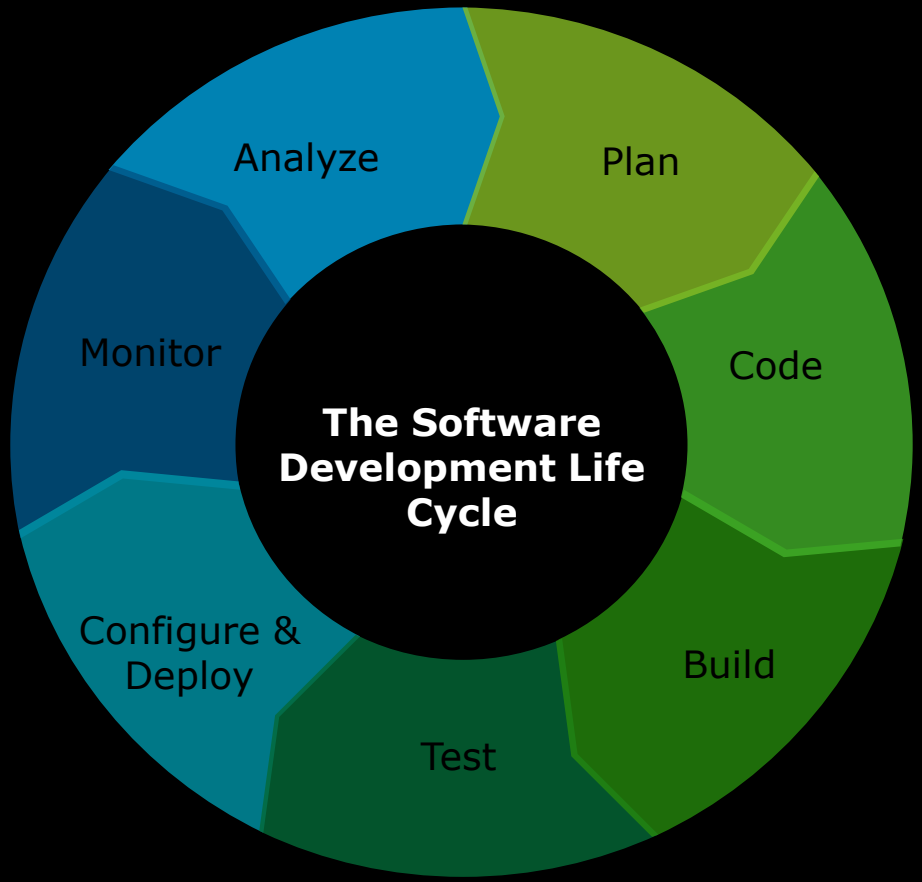
Shifting Left: Security by Design

No. 1 | Evolution of Software Landscape

Technology demand for speed and innovation

What is Software Development?

A Software Development Life Cycle (SDLC) is a process used by the software industry to design, develop, and test high quality software by breaking up design, development, and deployment activities into sequential steps. The SDLC aims to produce high quality software that meets or exceeds customer expectations and reaches completion within deadlines and budget limitations.



Waterfall

- Linear development lifecycle
- Project development team only moves to the next phase after previous is completed
- If a missing requirement is identified during any stage, return to the planning stage to start over again

Agile

- Iterative execution of planning, building, testing, and releasing software
- Built to regularly elicit customer feedback and better handle unclear / changing requirements, compared to Waterfall
- "Lighter weight" compared to waterfall

DevOps

- Expands upon the implementations of Agile
- Breaks down walls / silos of development and IT operations to enable more collaboration
- Heavy automation, smaller releases, and adoption of cloud and microservice architectures to enable quicker time to market

The importance of having a secure software development lifecycle

As the sophistication and frequency of cyber-attacks rise, securing applications is becoming more time consuming, resource intensive, and expensive.

In Verizon's 2021 Data Breach Investigation Report, web applications were the attack vector used in **over 90% of breaches** analyzed.

REPUTATION

Companies rely heavily on their reputation to attract customers and having a data breach caused by a malicious actor can **permanently damage** client relations and consumer trust.

CUSTOMER RELATIONS

Customers are increasingly putting pressure on institutions that handle and house their data to put controls in place to keep it safe.

COMPLIANCE

Regulatory bodies at multiple levels (federal, state, local, etc.) are progressively requiring regular security testing of **critical assets** and infrastructure.

FINANCIAL

According to 2020 Report: Inside Cybersecurity Remediation Cost Organizations $11.45 Million, the average cost of a data breach in 2020 is $14.30 million globally.

"More than half of all breaches involve web applications—yet **less than 10%** of organizations ensure all critical applications are reviewed for security before and during production." Deloitte – Application Security

Organizations need to have a secure SDLC in place to actively identify weaknesses and vulnerabilities within their systems in order to take appropriate actions to remediate and defend.

Challenges customers face with application security

Organizations are facing several obstacles across People, Process and Technology when introducing effective security into SDLC that can prevent vulnerabilities from reaching production.

Unknown Capabilities / Strategy

Many organization lack a defined application security strategy and/or don’t know their current capabilities

Delayed Security Testing

Security testing is often performed late which increases the cost of remediating identified vulnerabilities

Resource Challenges

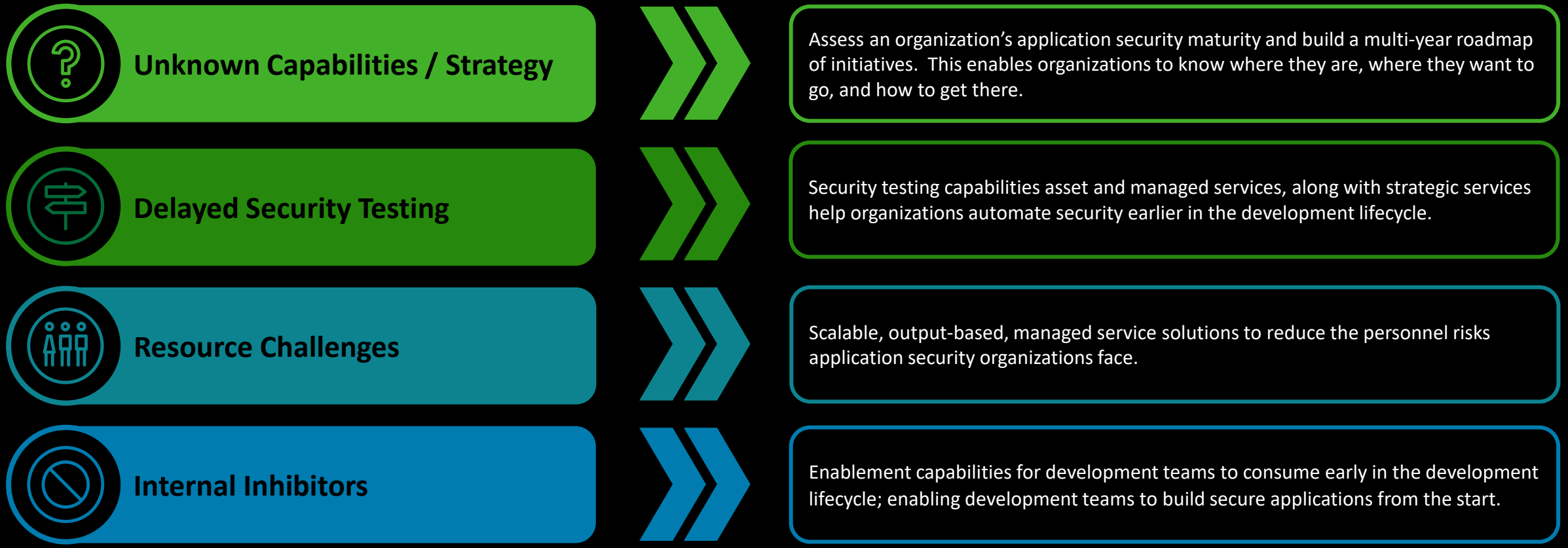
Application security professionals are in short supply and high demand, making them hard to find and keep

Internal Inhibitors

Application security setup as “gatekeepers” rather than “enablers”, causing friction with developers

How can we solve application security challenges?

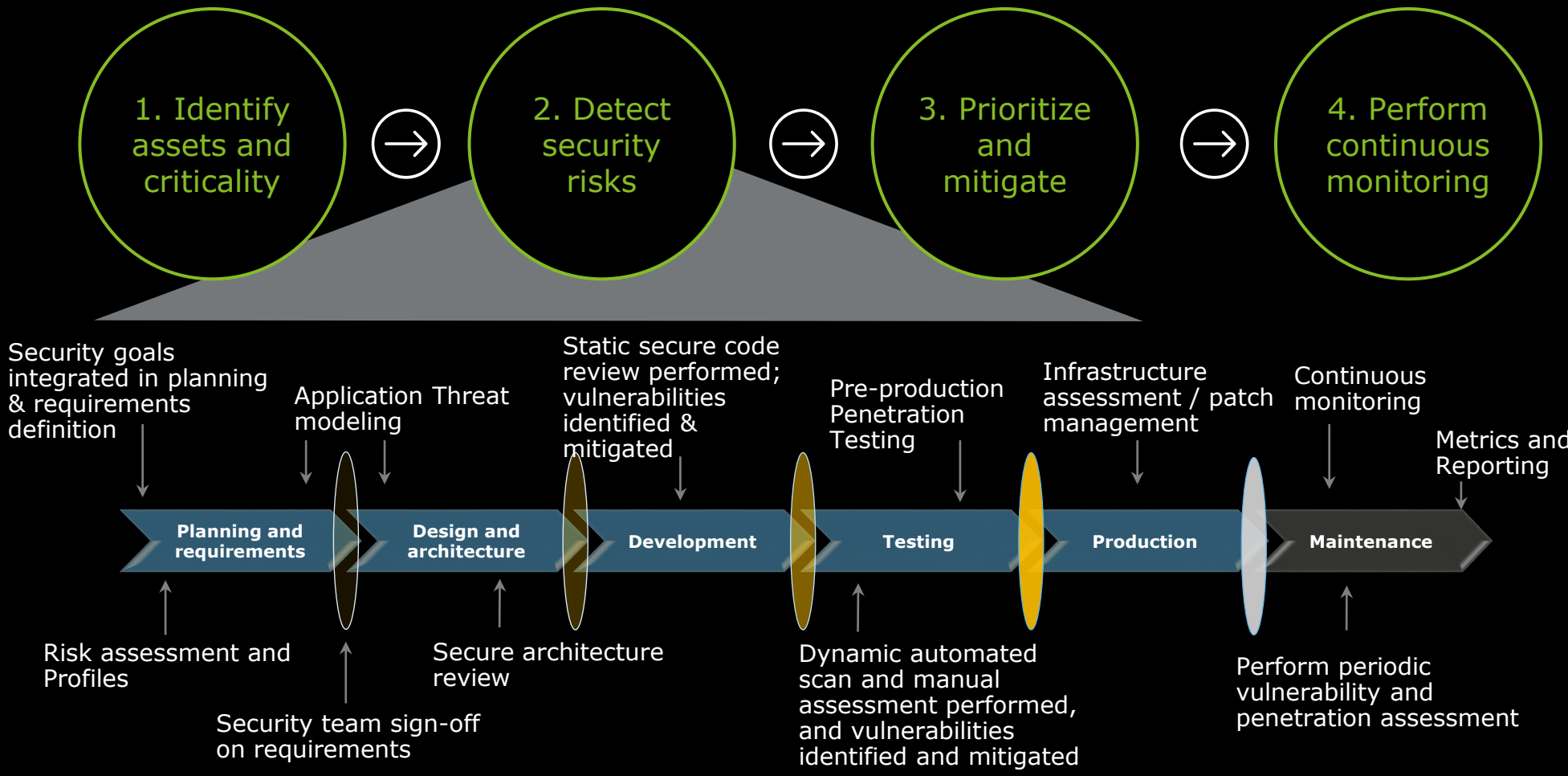
In today's world, it is important for organizations to enable the design, development, and deployment of secure applications and systems to better safeguard information assets and protect their business.



No. 2 | Security in SDLC

Integrating security at every step

Integrating security within a traditional SDLC – Illustrative



Integrating security within an Agile environment – Illustrative

Planning and requirements

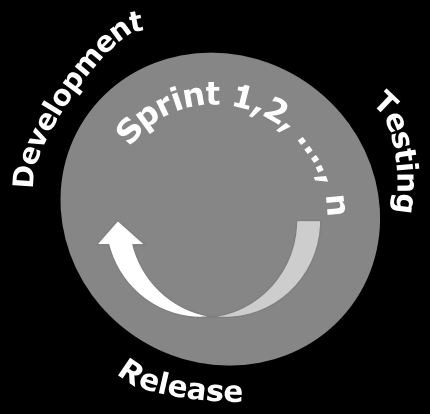
Activities

- Developers will loop in security to discuss any security concerns, including potential architecture changes
- Develop Security User stories (e.g., *As a user, want the application to validate input to be correct and fit for the intended purpose.*)
- Validate all data input from an external entity or client.

Design and architecture

Activities

- Develop Security Architecture – Identify and tailor controls based on NIST 800-53
- Review security architecture and confirm compliance to security requirements
- Security team will be looped in during story elaboration, review architecture/design changes, and approve any security related issues



Gate Check

Security Architecture and Security Requirements approved by Security team

Gate Check

Security Testing completed & Risk Management Plan in place

Testing/ hardening

Activities

- Developers will work with security team counterparts to timely resolve identified vulnerabilities and critical findings prior to deployment
- Conduct SAST, DAST, Code Review and Penetration Testing
- Map test cases following the STIG requirements executable scripts

(Pre) Production

Activities

- Perform Infrastructure Related Vulnerability Testing to Confirm no Vulnerabilities Introduced
- Analyze, Map, and Provision Access
- Security Assessment & Secure Configuration

Maintenance

Activities

- Application Security Recertification
- Perform Periodic Vulnerability and Penetration Testing
- Initiate Corrective Actions for Newly Discovered Issues and Managed to Disposition
- Perform continuous monitoring to monitor compliance and detect deviations from security controls

High-level Roles

Business Owner

Communicate the vision, scope and roadmap

Scrum Master

Coaches the agile team in self management

Developers

Create the software/product

Security Engineers

Ensure security of the product

No. 3 | Security in DevOps

From DevOps to DevSecOps

From DevOps to DevSecOps

Why do we need security in DevOps?

- The increase in amount and severity of data breaches, such as the SolarWinds and Microsoft Exchange Servers attacks, is a persistent issue
- Acceleration favors agility at the expense of security from traditional waterfall software development, putting security into a reactive mode
- DevSecOps enables the customer experience by bringing trust to the application by incorporating security throughout the development process

With the industry rush for Hyper-agile DevOps, security is still an after-thought!

How can we integrate security into DevOps?

- Tightly integrate security tools and processes throughout the DevOps pipeline
- Automate core security tasks by embedding security controls early in the software development life cycle
- Continuous monitoring and remediation of security defects across the application life cycle, including development and maintenance

Key Benefits

Continuous security
DevSecOps implements the 'secure by design' principle by using automated security review of code and automated application security testing

Increased efficiency and product quality
Security issues are detected and remediated during development phases, which increases the speed of delivery and enhances quality

Enhanced compliance
In DevSecOps, security auditing, monitoring, and notification systems are automated and continuously monitored, which facilitates enhanced compliance

Increased collaboration
By integrating development, security, and operations, DevSecOps fosters a culture of openness and transparency from the earliest stages of development

Resilience
DevSecOps helps organizations in designing and implementing resilient systems

Reliability
Customers need more secure, reliable and available systems. DevSecOps reduces failure rates with faster feedback

Flexibility
Organizations can be flexible with emerging technology and fast to deliver value to customers without risking loss of business

Automation
Automation helps to reduce complexity of modern systems and can scale as per needs

What is DevSecOps?

DevSecOps is the integration of security into DevOps across governance, people, process, and technology.

Governance

Establish security 'guardrails' and monitor results

- Redesign the operational and compliance framework
- Establish shared metrics to evaluate progress
- Embed cybersecurity into each process in the SDLC
- Compliance-as-code mind-set
- Adopt a flatter hierarchy to manage processes

People

Break down silos between security and DevOps teams and instill cyber awareness

- Incorporate security staff in DevOps teams
- Have security teams brief dev and ops teams on current threats / exploits/breaches
- Introduce shared goals as a whole
- Adopt secure coding practices as a by-product of increased cybersecurity understanding

Process

Orchestrate an integrated process flow and drive 'in- line' risk rationalized feedback

- Asset inventory and risk awareness
- Integrated backlog and pipeline
- Security telemetry and incident response
- Consistent development approaches
- Implement threat-modeling into the design

Technology

Automate recurring security tasks and harden the development pipeline

- Automate secure application development
- Protect the toolchain and infrastructure
- Consistent quality through automated processes
- Incorporating assorted pipeline tools for greater efficiency

DevSecOps is not a tool, but a transformational shift of operations.

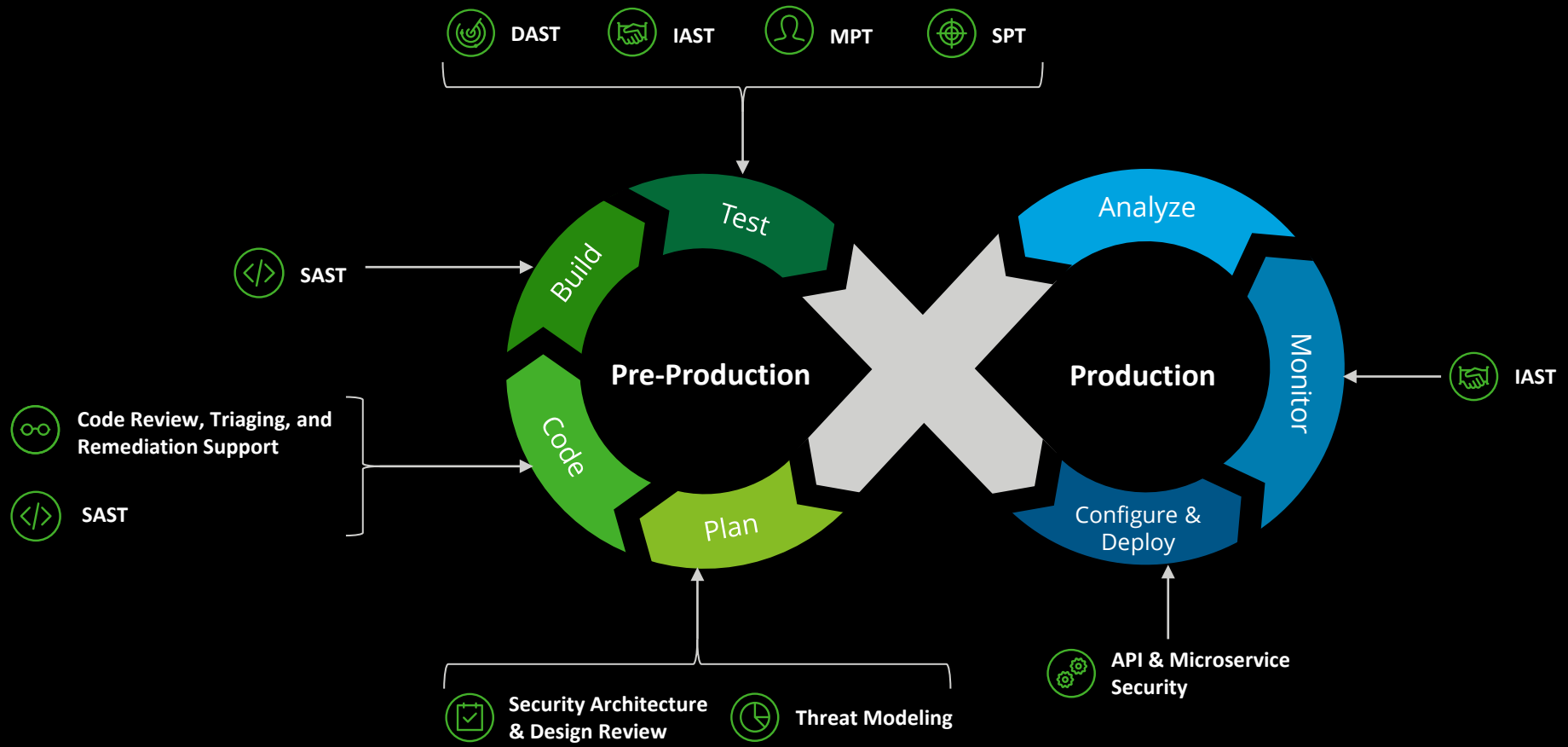
No. 4 | Shifting Left

Enabling Security by Design

Cyber processes mapped to DevOps

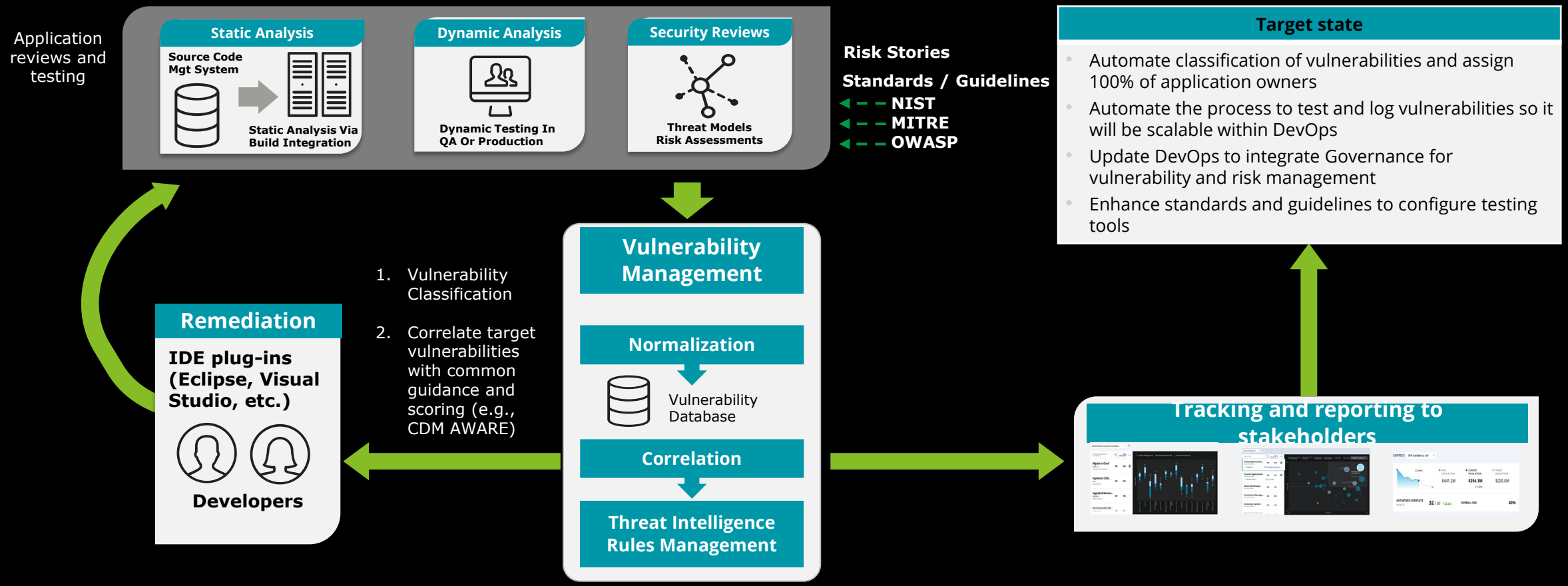
Program Governance as a Foundation to the SDLC

- AppSec Program Build
- Application Security Automation
- Secure by Design
- Application Governance
- Containers & Container Security
- AppSec Program Strategy & Roadmapping



What does DevSecOps Automation look like?

Proactive identification, remediation and reporting of application vulnerabilities helps to prevent them from being introduced into our live/production environments, with better equipped developers and testing tools



DevSecOps implementation

Shift security left

Use Continuous Integration/ Continuous Deployment (CI/CD) pipeline to embed security

Management buy-in

Financial commitments and reporting

Security by default

Use security by default framework and services

Self-service

Give developers and operations visibility into security activities

Everything as code

Save as code → configurations, infrastructure, and pipelines

Develop security coding policies and procedures

Applications and data are as safe as where you put it, what's in it, how you inspect it, who talks to it, and how it's protected

Deloitte.