GHENT
UNIVERSITY

GHENT
UNIVERSITY

FACULTY OF ENGINEERING
AND ARCHITECTURE

DEPARTMENT INTEC
RESEARCH GROUP IDLAB

WHAT IS DEVOPS?

Prof. Dr. Bruno Volckaert – IDLab – Ghent University / IMEC

GHENT
UNIVERSITY

SITUATION

- Everything needs software nowadays
- Software has to run on a server to become a service
- Delivering a service from inception to its users is too slow and error prone due to internal friction
  - This makes companies lose money (delay = loss)
  - IT is frequently the bottleneck in the transition of concept to cash

TRADITIONAL DEVELOPMENT AND OPERATIONS TEAMS

1. Development teams
   - Requirements analysis
   - Software design
   - Planning
   - Software implementation
   - Testing (typically in development environment)
2. Operations teams
   - Receive application (artefacts) from development teams
   - Deploy applications on infrastructure (outward facing production versions)
   - Manage infrastructure and operational services (e.g. web server, firewall, ticketing system)
   - Deal with security (authentication/authorization), infrastructure separation, etc.
   - Monitoring
   - Provide support to end-users

vb. examenvraag: wat is het verschil tussen... : whitespace heel deze page geven

caak in bedrijven twee volledige verschillende teams niet goed

kritische infrastructuur en development infrastructuur separatie

SYMPTOMS OF DEVELOPMENT / OPERATIONS MISMATCH

- Defects are released into production, causing outages
- Inability to diagnose production issues quickly
- Problems appear in some environments (e.g. production) only
- Blame shifting / finger pointing prroductie vs development
- Long delays while development, Quality Assurance or another team wait on resource or response from other teams
- “Manual error” is a commonly cited root cause
- Release slip / fail missen van vooropgezette deadlines
- Quality of Life issues in IT

CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft says

20 July 2024

Microsoft says it estimates that 8.5m computers around the world were disabled by the global IT outage.

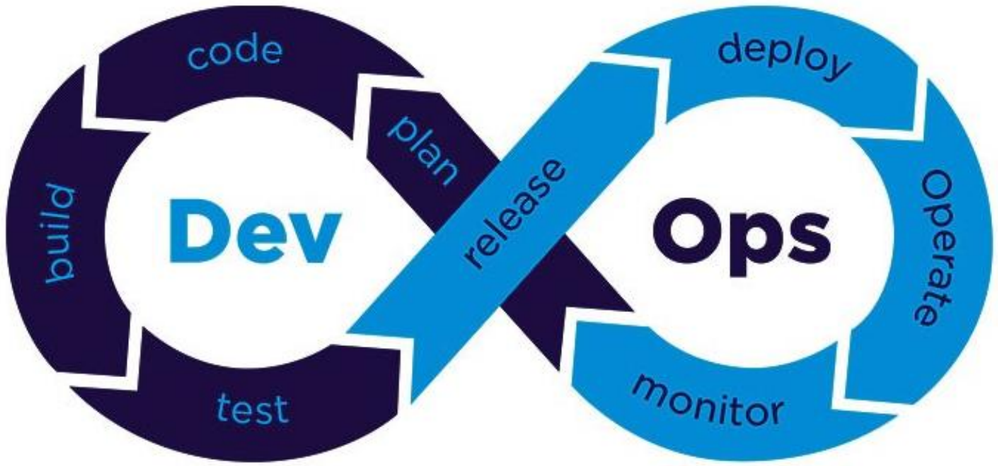
It’s the first time a figure has been put on the incident and suggests it could be the worst cyber event in history.

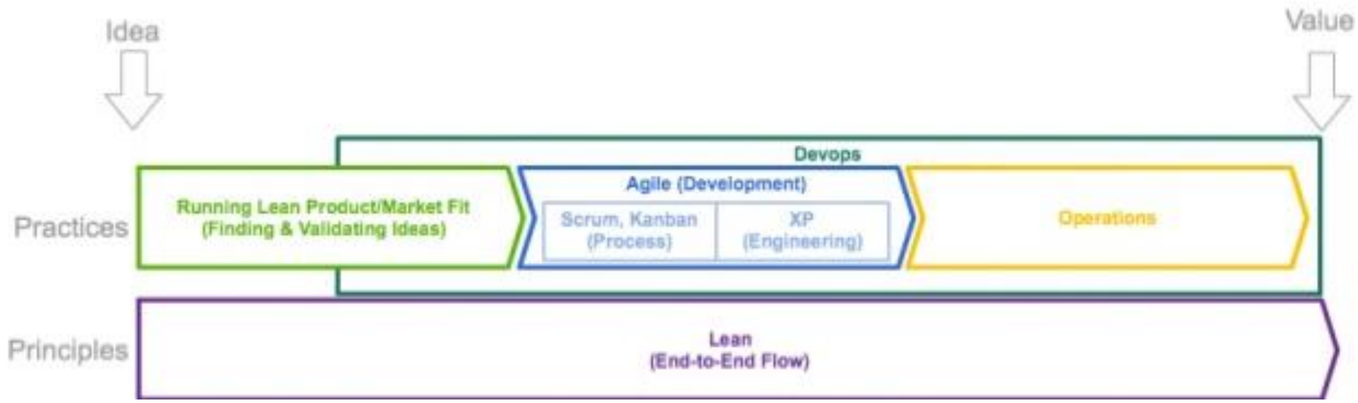
The glitch came from a security company called CrowdStrike which sent out a corrupted software update to its huge number of customers.

DEVOPS

- Practice of operations and development engineers participating **together** in the entire service lifecycle from design through development to production support
- The application of agile methodology to system administration
- High performance IT organisations deploy 30x more frequently with 200x shorter lead times; they have 60x fewer failures and recover from issues 168x faster (source: Puppet Labs State of DevOps report)

symbiose tusssen dev en ops





GHENT UNIVERSITY

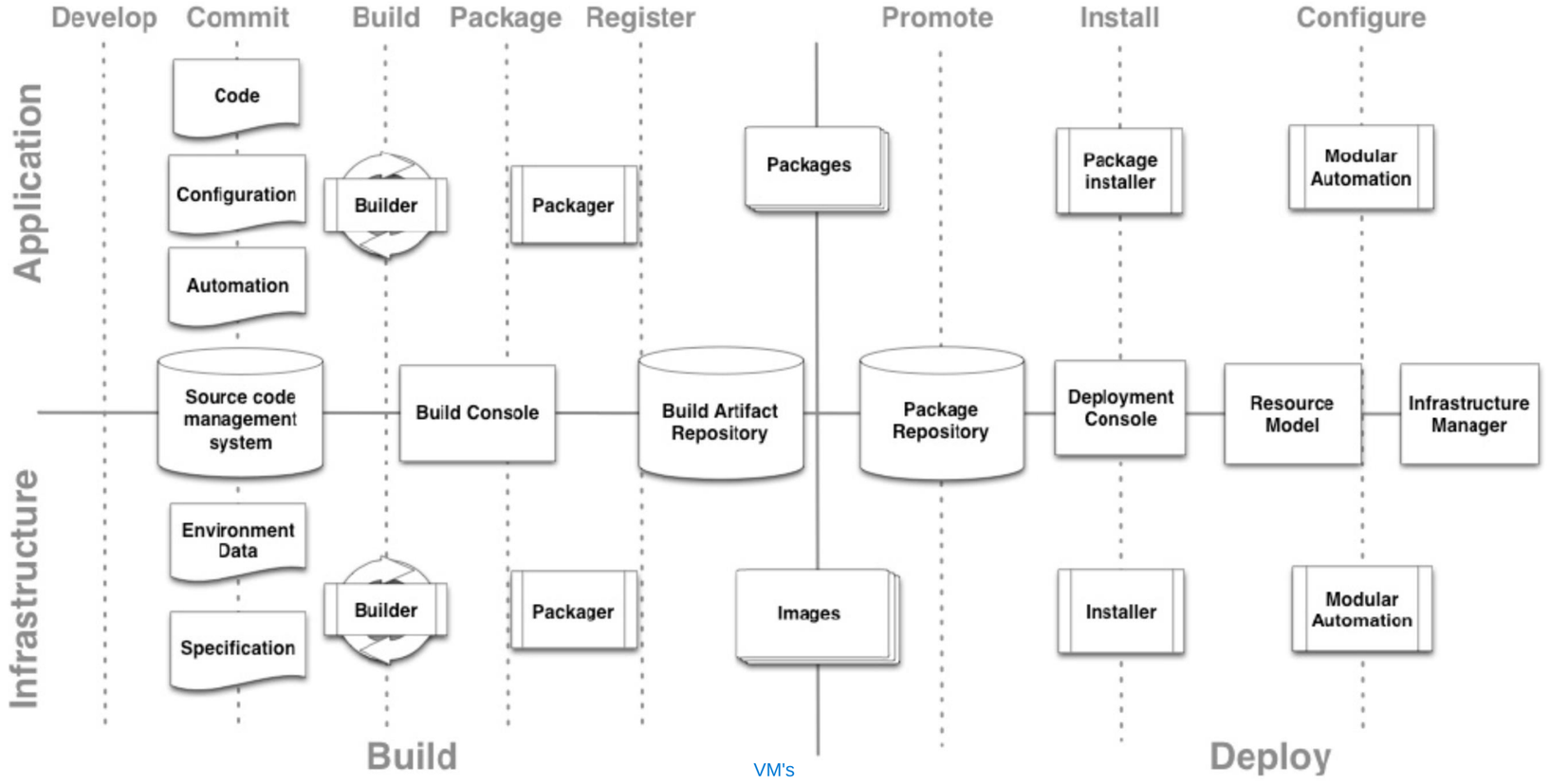
DEVOPS CORE VALUES

sense of ownership naar werknemers. flexibel zijn met gebruikte software

- Culture and People > Processes and Tools
  - People become product owners throughout its lifecycle = gives responsibility
- Automation – Infrastructure as Code
  - Automation critical as things need to move fast, without human error
- Measurement – measure everything
  - Knowledge of the (operational) systems is key
  - Know when things go wrong in an automated manner
- Sharing – collaboration – feedback
  - Intense collaboration and knowledge sharing between devs and ops
  - In some cases devs = ops

INFRASTRUCTURE AUTOMATION – INFRASTRUCTURE AS CODE

- Automate everything
  - Infrastructure provisioning
  - Application deployment
  - Runtime orchestration
- Model driven automation
- Dev workflow
  - Write it in code
  - Validate the code
  - Unit test the code
  - Build it into an artifact
  - Deploy artifact to test
  - Integration test
  - Deploy artifact to production



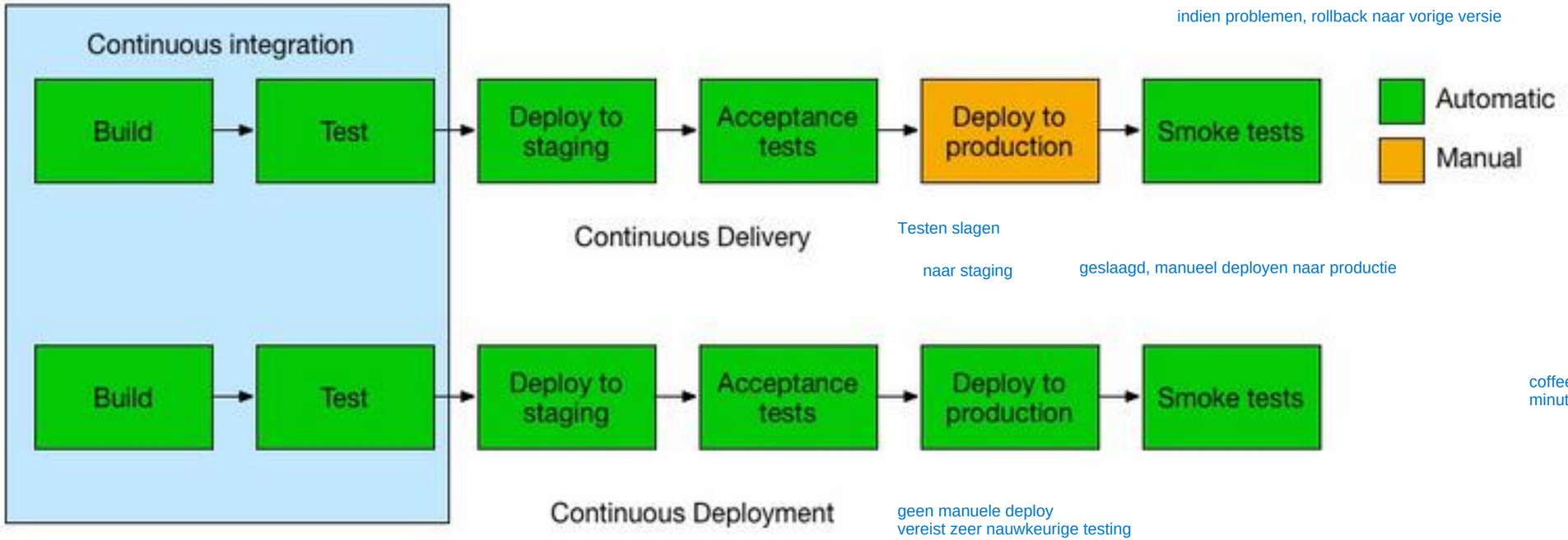
CONTINUOUS DELIVERY/DEPLOYMENT

vaak examenvragen met figuren te geven

- **Continuous integration**: build and test
- **Continuous delivery**: deploy and acceptance/integration test
- **Continuous deployment**: build, test, deploy, acceptance/integration test and bring it all the way to production

staging zo goed mogelijke kopie van je productie

indien problemen, rollback naar vorige versie



Testen slagen

naar staging

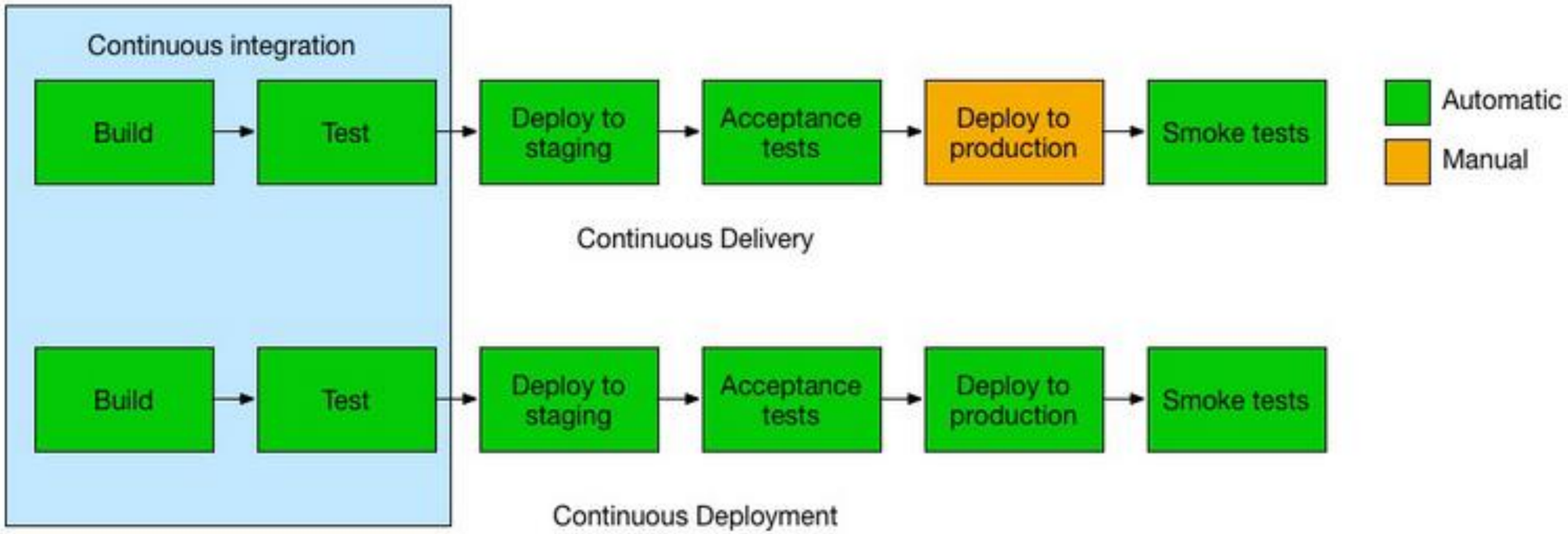
geslaagd, manueel deployen naar productie

coffeetest, build mag maximaal 5 minuten duuren

geen manuele deploy
vereist zeer nauwkeurige testing

CONTINUOUS DELIVERY/DEPLOYMENT

- Best practices
  - Builds should pass the coffee test (< 5 minutes)
  - Commit small bits Dagelijks indien mogelijk
  - Do not leave the build broken
  - Deployment should go to a copy of production (e.g. staging) before going into production
  - Stop deploys if a previous step fails



AUTOMATED TESTING MANDATORY FOR CONTINUOUS DEPLOYMENT

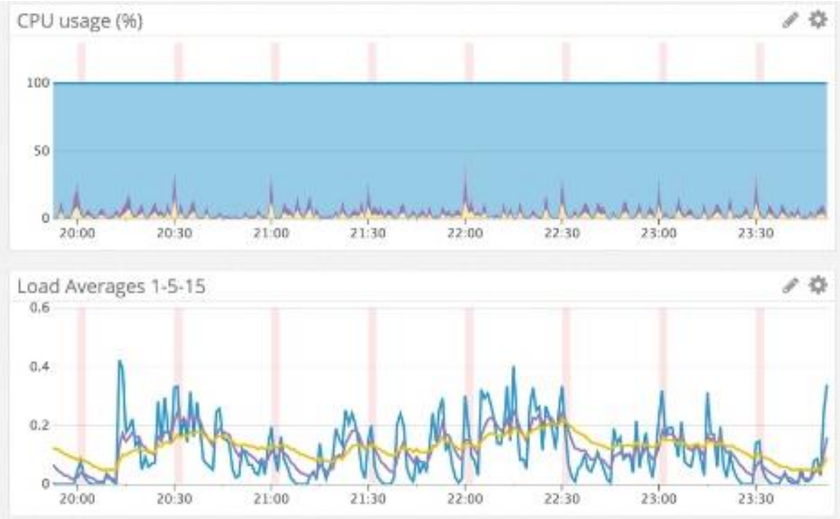
- Automated testing is incredibly important
  - Unit tests
  - Integration tests communiceren tussen verschillende
  - Crossbrowser, performance, security tests
- Continuous Deployment near-impossible without an expansive automated test suite
- Schedule time to design and write these tests
  - NOT an afterthought or when waiting for builds

neemt tijd en

RELIABILITY ENGINEERING

fouten zelf introduceren
- te weinig geheugne
-wegvallen netwerk
....

- Design patterns exist for creating resilient systems (bulkheads, connection pools, etc.)
  - Books: 12-factor apps, Release it!
- If your app is badly designed, there's only so much an ops team can do about it once it is deployed
  - Foster culture of responsibility: your code = your responsibility
  - Developers need to take responsibility for their app all the way through deployment
- Build – Measure – Learn - Repeat



RESILIENT TO FAILURE: NETFLIX'S SIMIAN ARMY

- Chaos monkey
  - Introducing random failures in their production AWS services
  - Team of engineers ready to intervene
- Chaos gorilla: disables an entire AWS availability zone
- Latency monkey: introduces configurable artificial delays

vertraging op bv berichttresponsen

- Utilities
  - Janitor monkey: seeks unused resources and disposes of them
    - Replaced by swabbie (cleanup service)
  - Security monkey: seeks misconfigured services / security issues

The best defense against failures is to fail often, forcing your services to be built in a resilient way

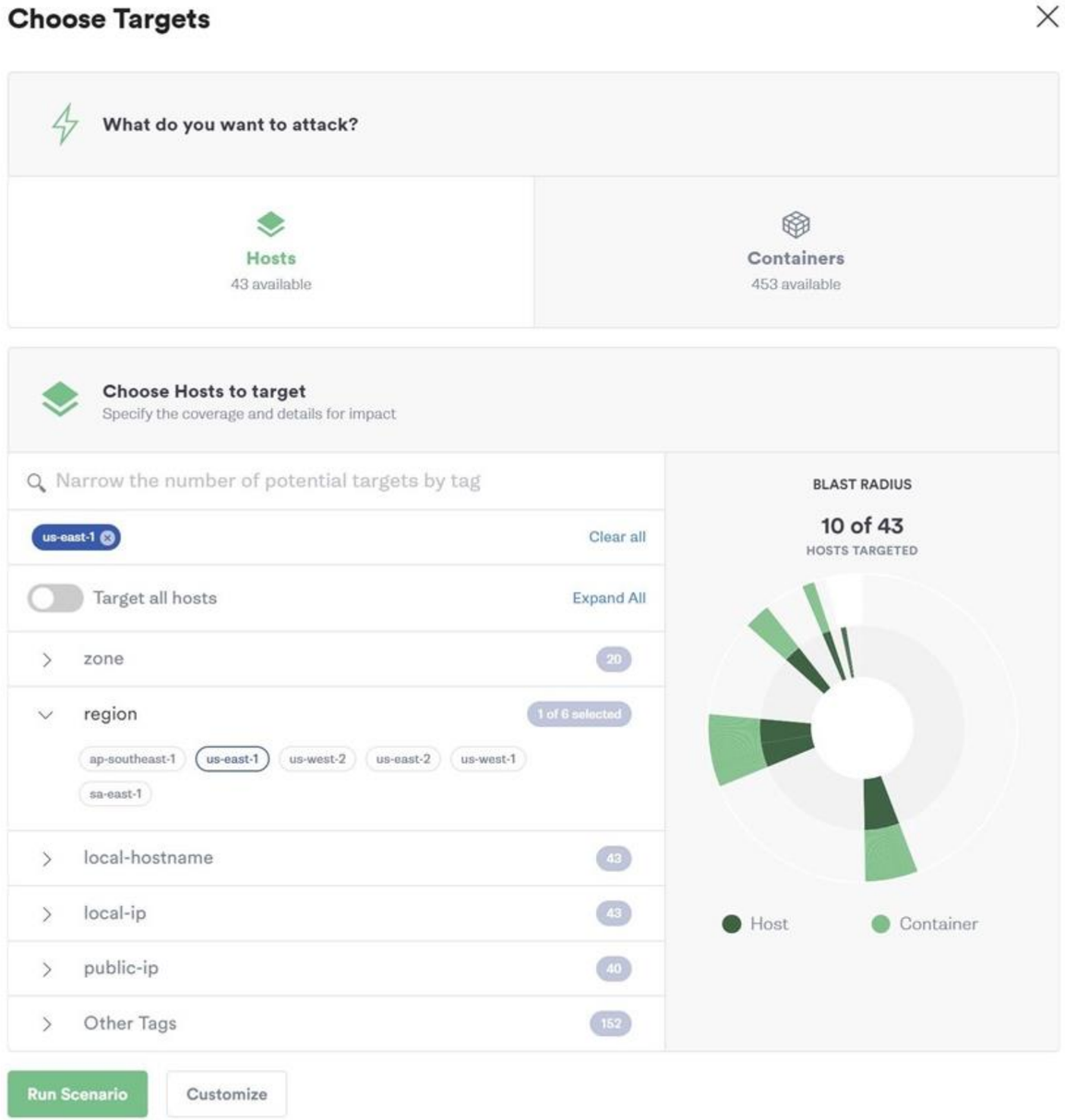
GHENT UNIVERSITY

CHAOS ENGINEERING

- The discipline of experimenting on a distributed system in order to build confidence in the system's capability to withstand turbulent conditions in production
- Find weaknesses and fix them before they break when least expected
- Gremlin (https://www.gremlin.com)

Category	Impact
Resource	Starve your application of critical resources
State	Change the state of the environment your application is running within
Network	Simulate the inherently unreliable behavior of the network
Request	Impact individual requests as they hit the wire

Gremlin	Impact
Shutdown	Performs a shutdown (and an optional reboot) on the host operating system to test how your system behaves when losing one or more cluster machines.
Time Travel	Changes the host's system time, which can be used to simulate adjusting to daylight saving time and other time-related events.
Process Killer	Kills the specified process, which can be used to simulate application or dependency crashes. (Note: does not work for PID 1, consider a Shutdown attack instead)

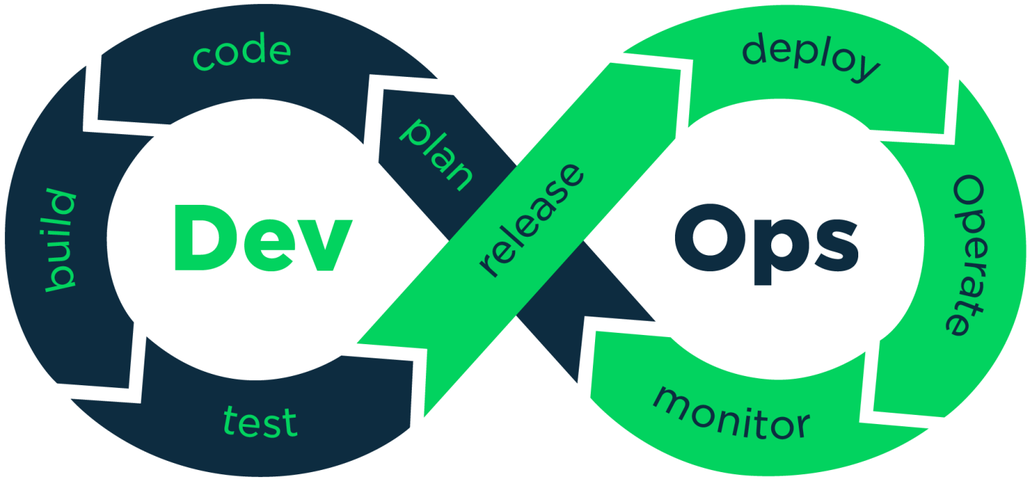


ADDING DEV INTO OPS

- Ops should not “do tasks for people”
  - Ops should build tools so people can do their own work
- Set up automation tools
- Build feedback paths back to dev from production
  - Monitoring, logging and metrics – ensure these feed back into dev
  - Blameless incident postmortems
- Developers do on-call production support
- SRE (Site Reliability Engineering) model – devs support product until it gets big and Ops accepts support

AMAZON HAS BEEN ONE OF MANY DEVOPS PROPONENTS

"The traditional model is that you take your software to the wall that separates development and operations, throw it over and then forget about it.
Not at Amazon.
You build it, you run it."



Werner Vogels, CTO Amazon

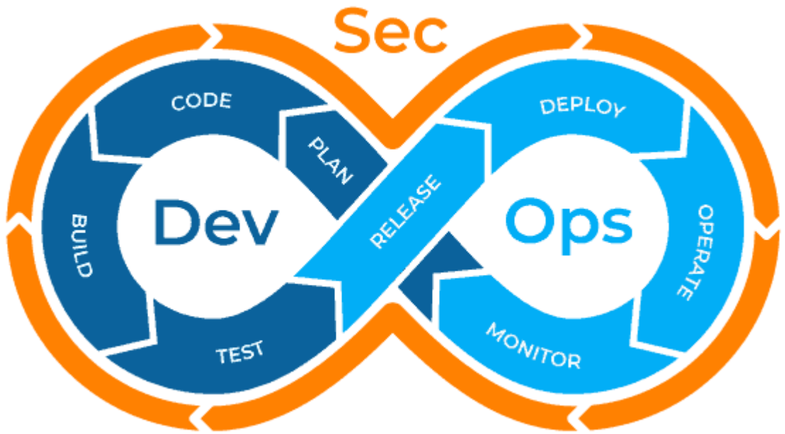
DEVSECOPS

Security vaak een probleem

direct meenemen in dev

- Extension of DevOps to include security from the get-go
- Security now a shared responsibility integrated from end-to-end
- Approaches
  - Secure coding: developers need to be capable of coding securely (e.g. no buffer overflows)
    - Static code analysis tools can be used to scan for vulnerabilities
  - Security testing tools integrated into CI/CD pipeline
    - E.g. scanning dependencies / containers for known vulnerabilities
  - Shift-left testing: approach to software testing in which testing is performed earlier in the lifecycle

veel vroeger starten met security testing te implementeren



TOOLS TO IMPLEMENT DEVSECOPS

1. SAST – Static Application Security Testing
   - Scan proprietary / custom code for coding errors and design flaws that could lead to exploitable weaknesses
   - Used primarily during the code, build and development phases of the Software Development Life Cycle
   - Coverity is an example of a SAST tool https://scan.coverity.com/
2. SCA – Software Component Analysis
   - Scan source code and binaries to identify known vulnerabilities in open source and third-party components
   - Provide insight into security and license risks to accelerate prioritization and remediation efforts
   - Can be integrated seamlessly into a CI/CD process to continuously detect new open-source vulnerabilities, from build integration to pre-production release
   - Black Duck is an example of a SCA tool https://www.blackducksoftware.com/
3. IAST – Interactive Application Security Testing
   - Work in the background during manual or automated functional tests, analyze web application runtime behavior
   - Uses instrumentation to observe application request/response interactions, behavior, and dataflow
   - Detects runtime vulnerabilities and automatically replays and tests the findings, providing insights to developers down to the line of code where they occur
   - Invicti is an example of an IAST tool https://www.invicti.com/

duur

4. DAST – Dynamic Application Security Testing
   - Automated black box testing technology that mimics how a hacker would interact with your web application or API - tests applications over a network connection
   - Do not require access to source code or customization to scan the application stack
   - Example: Acunetix DAST tools (https://www.acunetix.com/web-vulnerability-scanner/) identify vulnerabilities on web applications and API

KEY POINTS

KEY POINTS

belangrijke, slide

waaarom

zo snel mogelijk van idee naar product geraken

- Devops is the practice of ops and dev engineers participating in the entire service lifecycle from design → development → production
  - Culture and People > Processes and Tools
  - Automation – Infrastructure as Code
  - Measurement – measure everything
  - Sharing – collaboration – feedback
- Automated infrastructure and automated testing give safety
- Making builds continuous gives speed and safety
- Engineering for reliability gives even more safety
- Accelerating flow makes money
- DevSecOps is integrating security from the get-go in the DevOps process