Attacking the software supply chain - Research Bytes

Romain Aviolat 2020.09.23

Me

Cloud & Security Expert @KS Eng. dept.

Love to solve boring tasks with automation

- github.com/xens
- keybase.io/xens
- gitlab.kudelski.com/aviolat

KUDELSKI SECURITY

Agenda

- Supply Chain
- (S)SDLC
- Demo of a software supply chain attack (from the source code down to the end user)
- Conclusion

KUDELSKI SECURITY

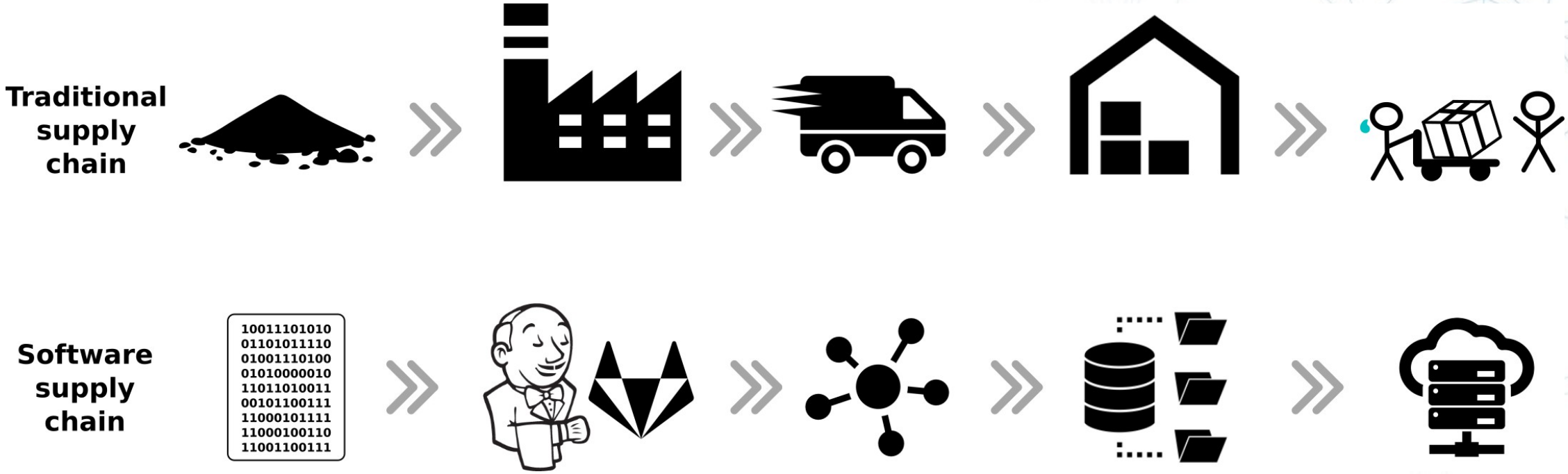
Disclaimer

This talk is based on my personal experience in the field building software pipelines in the KS Engineering dept or improving our infrastructure security.

It’s also based on many lectures, papers, talks, … .

KUDELSKI SECURITY

Supply-Chain



For both if we want the supply-chain to be a success (avoid delays, money-loss, poor-quality-products, …). We need rules or guidelines in place.

KUDELSKI SECURITY

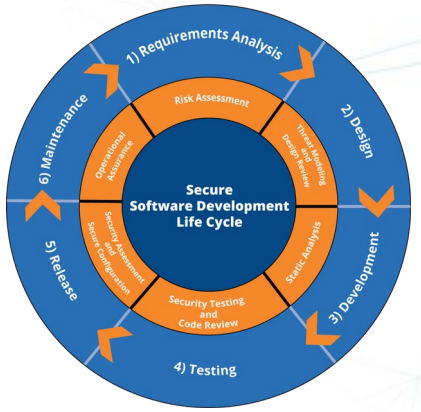
Software development **frameworks** or **methodologies**

Software **D**evelopment **L**ife **C**ycle

- Break down software creation process in multiple stages
- Flag errors rather sooner than later
- Get everything right the first time

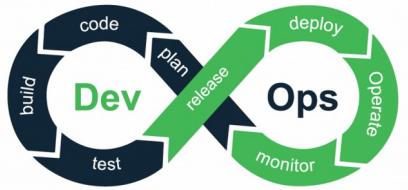
Multiple implementations

- Agile, Lean, Waterfall, Iterative, DevOps, Spiral, …



Common goal

- high-quality software as quickly and cost-effectively as possible.

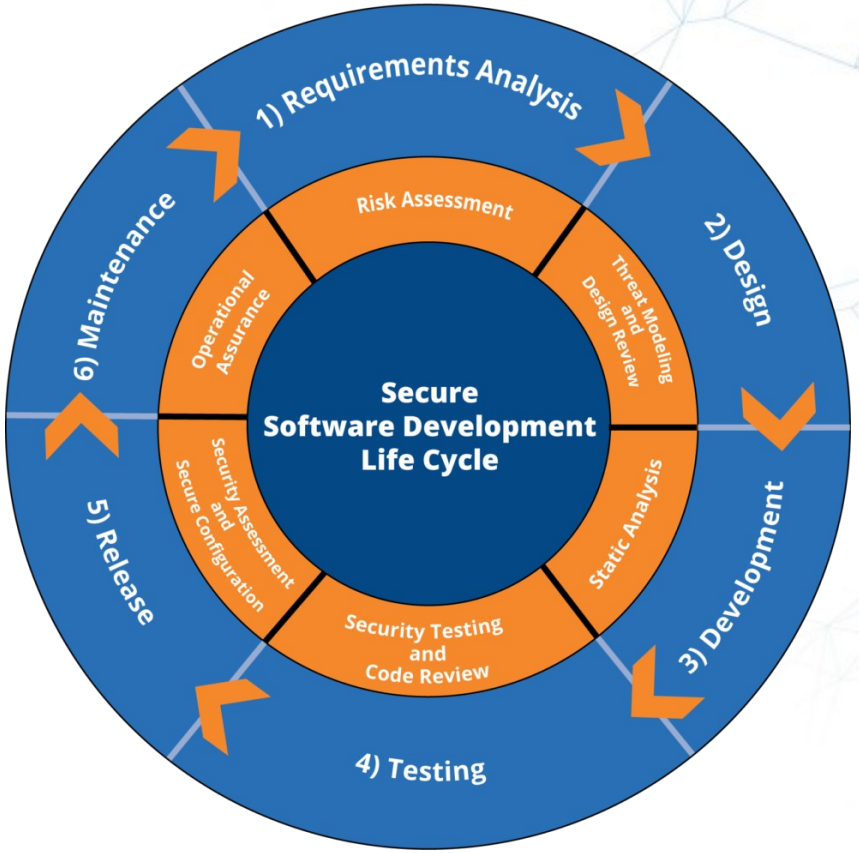


KUDELSKI SECURITY

Shifting security to the left

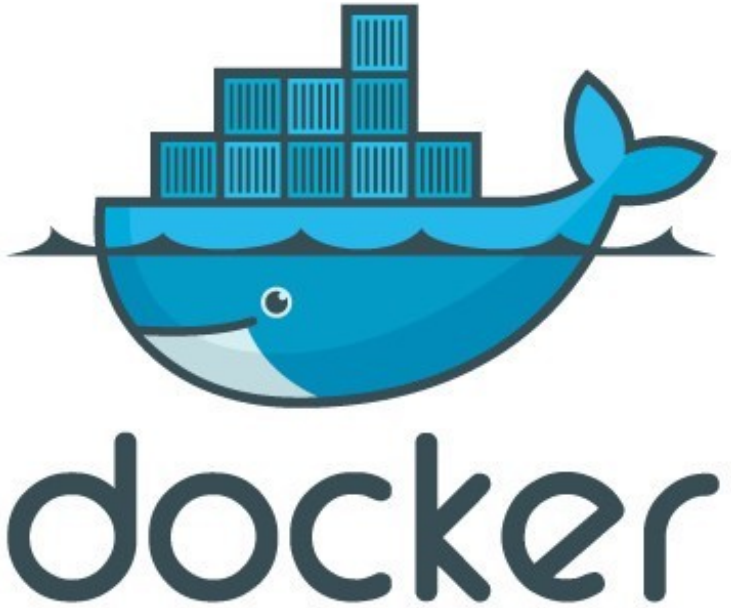
SSDLC → **S**ecure **S**oftware **D**evelopment **L**ife **C**ycle

- SDLC on steroids
- Include security components inside all stages
  - Risk Assessment
  - Threat Modeling
  - SAST
  - DAST, Code review
  - Audit
  - … .



KUDELSKI SECURITY

Similarities…



KUDELSKI SECURITY

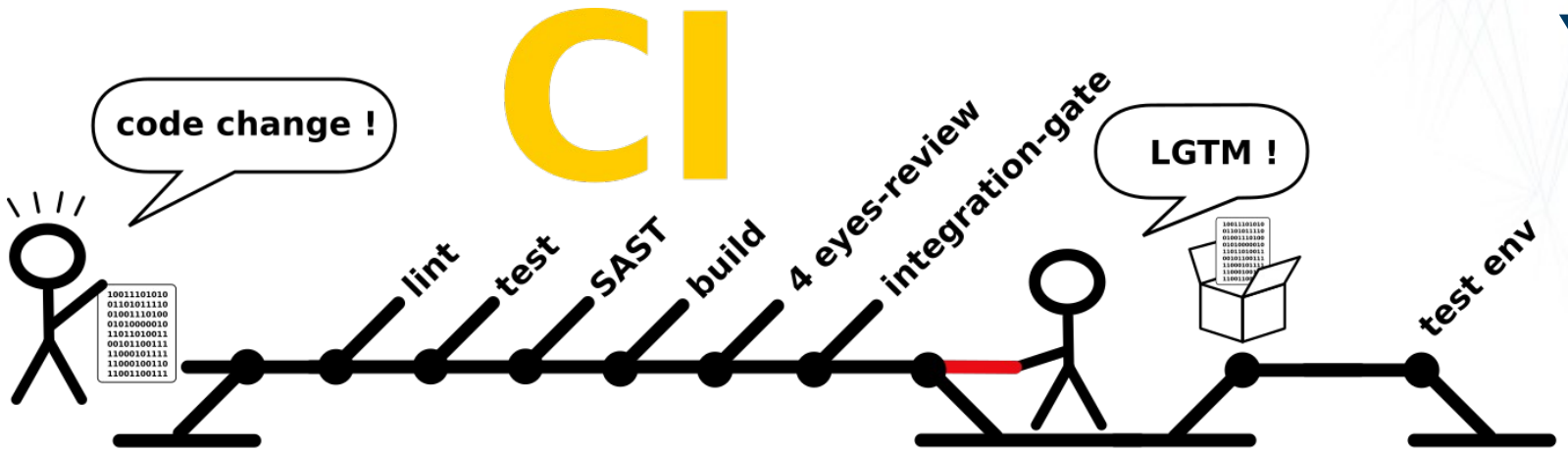
Similarities…

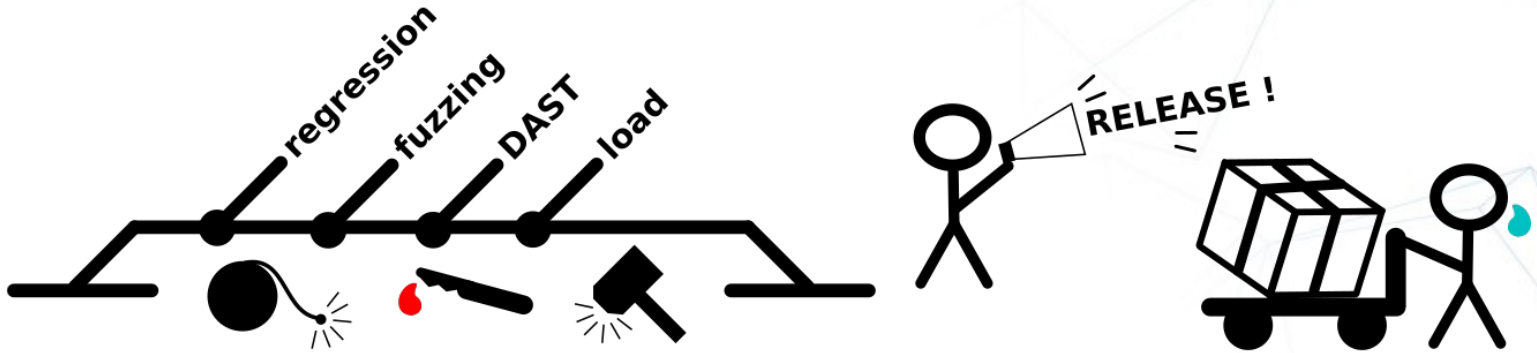
KUDELSKI SECURITY

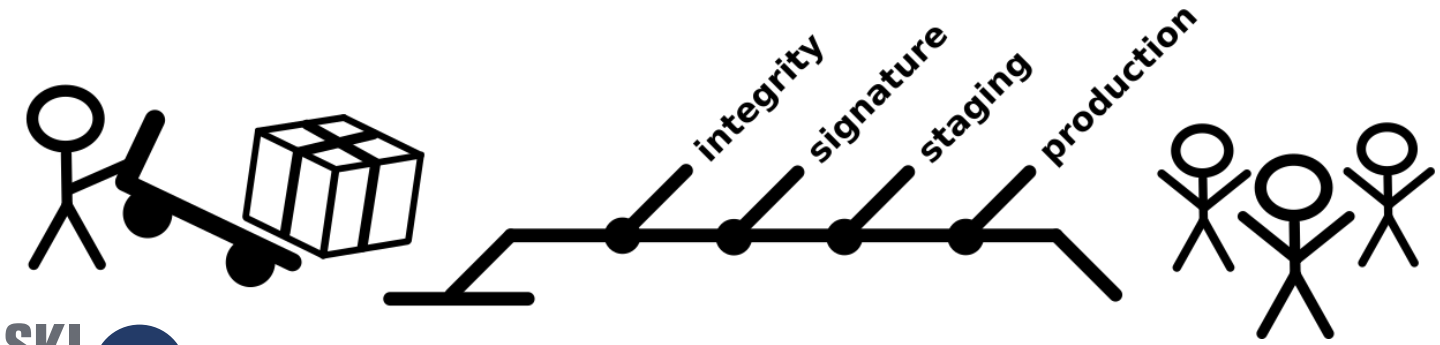
CI/CD - Supply-Chain

KUDELSKI SECURITY

Yet another CI/CD







KUDELSKI SECURITY

security in the software supply chain ?

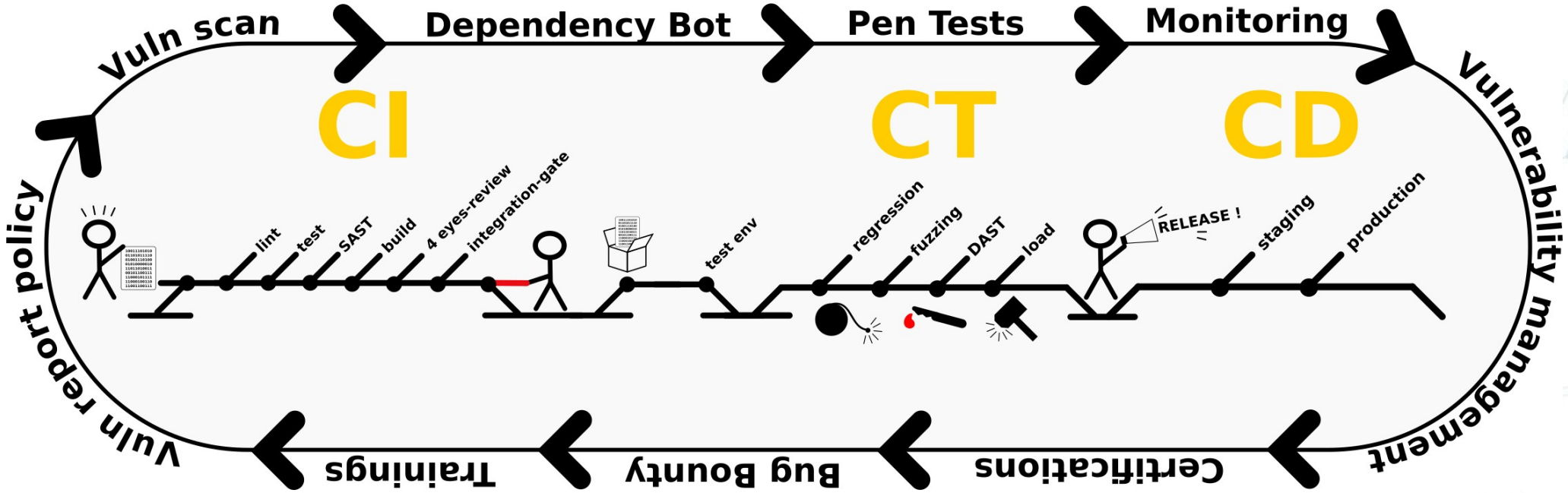
Why context matters

Your supply-chain workflow will be a **unique** combination of a lot of parameters*. To be relevant, the security you apply on top of it must take your context into account.

* [regulations, business requirements, certifications, SLAs, contracts with clients, scale, business criticality, exposure, reduced-staff, budget, tooling, …]

KUDELSKI SECURITY

Use-case 1 - Developing a SaaS product

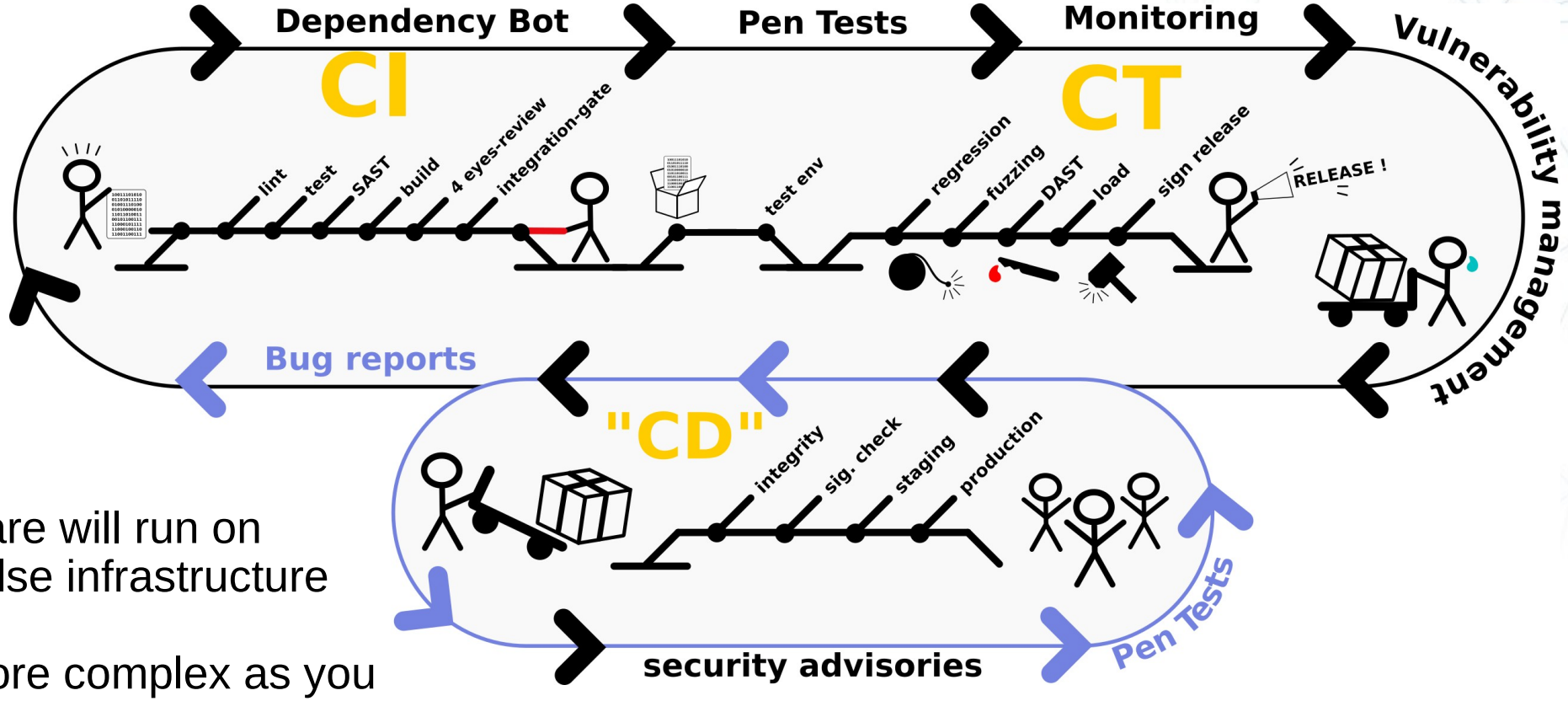


You develop and deploy your own product in production, consumed by your clients. You'll probably put a lot of focus on auditing / hardening your SaaS application.

As you're both the producer and the consumer, there's little challenge in term of trusting your production workloads.

KUDELSKI SECURITY

Use-case 2 - Developing software run by 3rd parties



Your software will run on someone else infrastructure

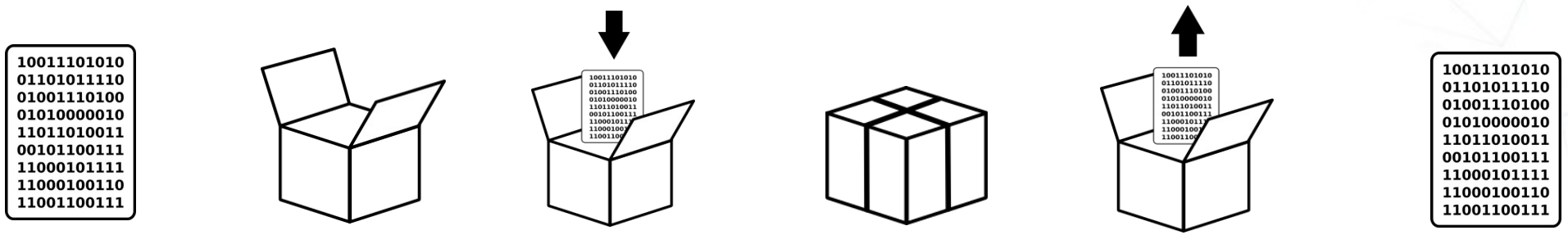
Chain is more complex as you need to deal with parts that are not under your control

- How your client can ensure that the software they run is legit (not tampered) ?
- How do you handle bug-reports coming from your client ?
- How do you handle security issues coming from your clients (Pen Tests, …)
- How to you provide security patches, upgrades to your clients ?
- What's your communication channel with your clients ?

KUDELSKI SECURITY

Many, many, many parameters

There’s an infinite number of factors that can influence the security of your supply chain.



“a supply chain is anything that’s needed to deliver your product”

[Github Security Engineering]

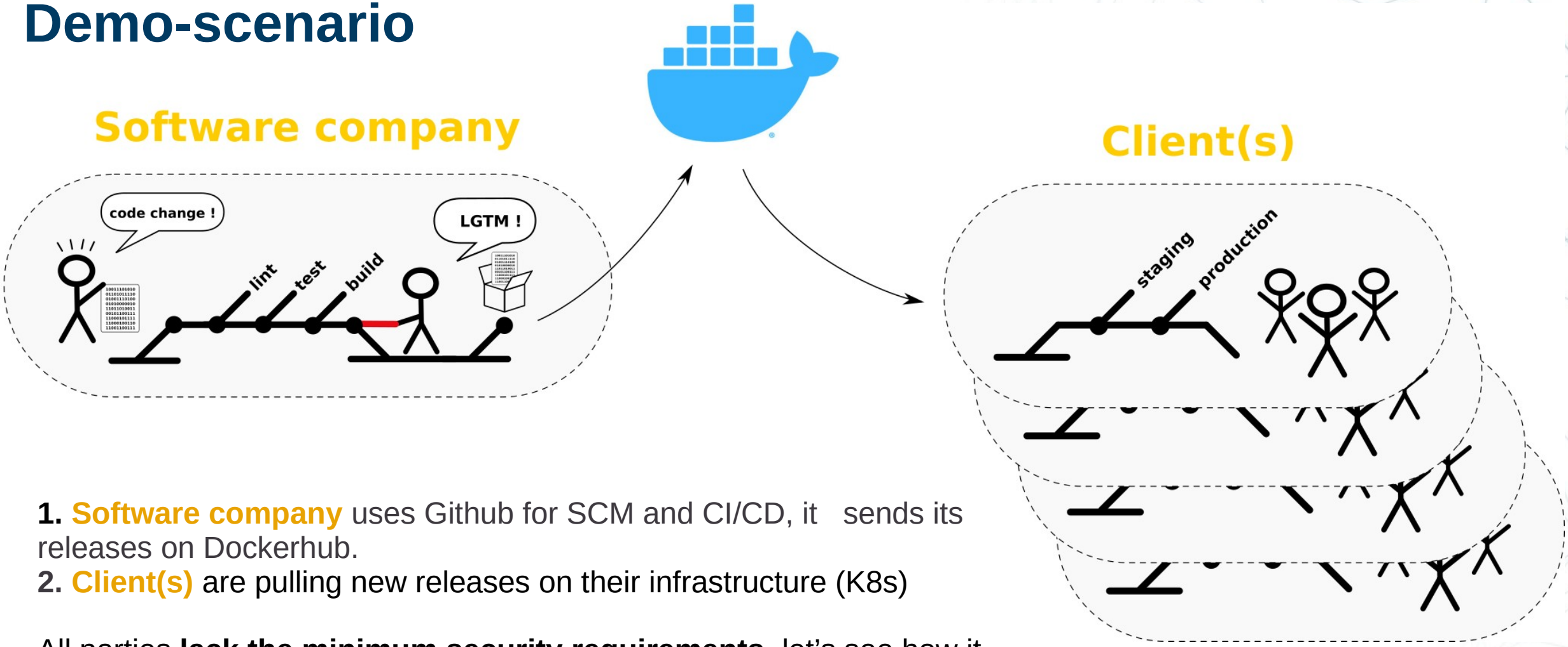
KUDELSKI SECURITY


Social engineering
Encryption in-transit
secure coding
credentials reuse
code quality
SAST
micro segmentation
hardware security tokens
Network-layer protections
up-to-date cryptography
fuzzing
secrets detection
Network-layer protections
Code signing
Encryption at-rest
Risk Assessment
pen-tests
Least privilege
security awareness
Code review
threat modeling
zero-trust
review gates
users off-boarding
perimeter scanning
DAST
Endpoint Detection (EDR)
MFA
credentials rotation
Encryption at-rest
library upgrades
Ephemeral credentials
OS upgrades
Container scanning

Live demo !

KUDELSKI SECURITY

Demo-scenario



1. **Software company** uses Github for SCM and CI/CD, it sends its releases on Dockerhub.
2. **Client(s)** are pulling new releases on their infrastructure (K8s)

All parties **lack the minimum security requirements**, let's see how it can impact them.

KUDELSKI SECURITY

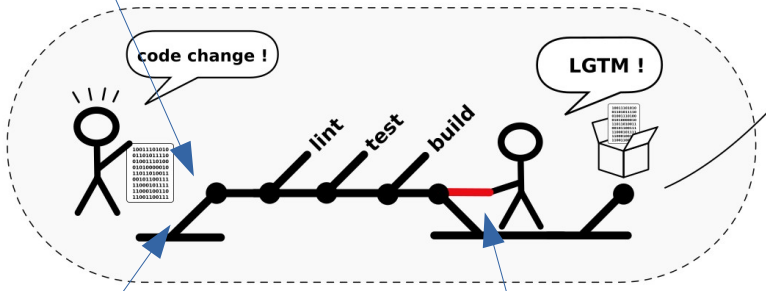
pre-commit-hooks

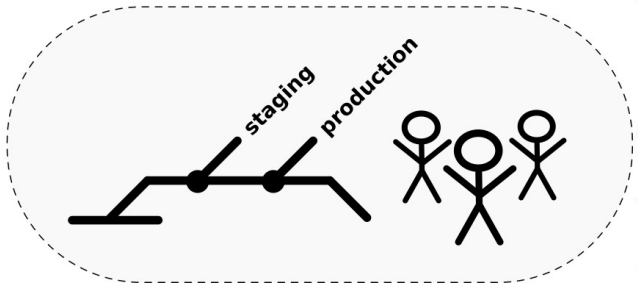
Lock main branch

Least-privilege

Filter egress traffic from PODs

Don’t expose ssh port on the Internet





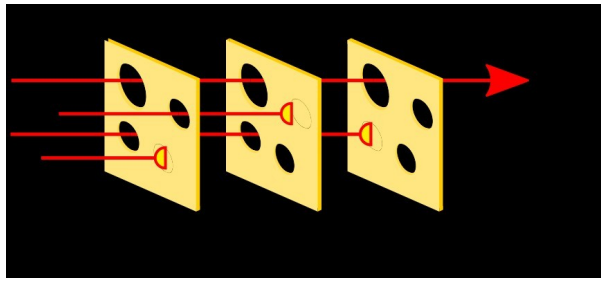
Force commit signatures

Force reviewers

Don’t allow privileged containers

Use the image SHA instead of SEMVER (immutability)

Harden the workers (SELinux, Apparmor, Seccomp, EDR,...)



Layered security

What could be done to avoid that ?

KUDELSKI SECURITY

Conclusion

KUDELSKI SECURITY

There’s no silver bullet when it comes to securing the software supply chain, it’s a trade-off between agility and security. A framework that make sense with your context must be put in place and reassessed over time.

KUDELSKI SECURITY

Famous supply-chain failure

KUDELSKI SECURITY

Cyberattacks on Ukraine

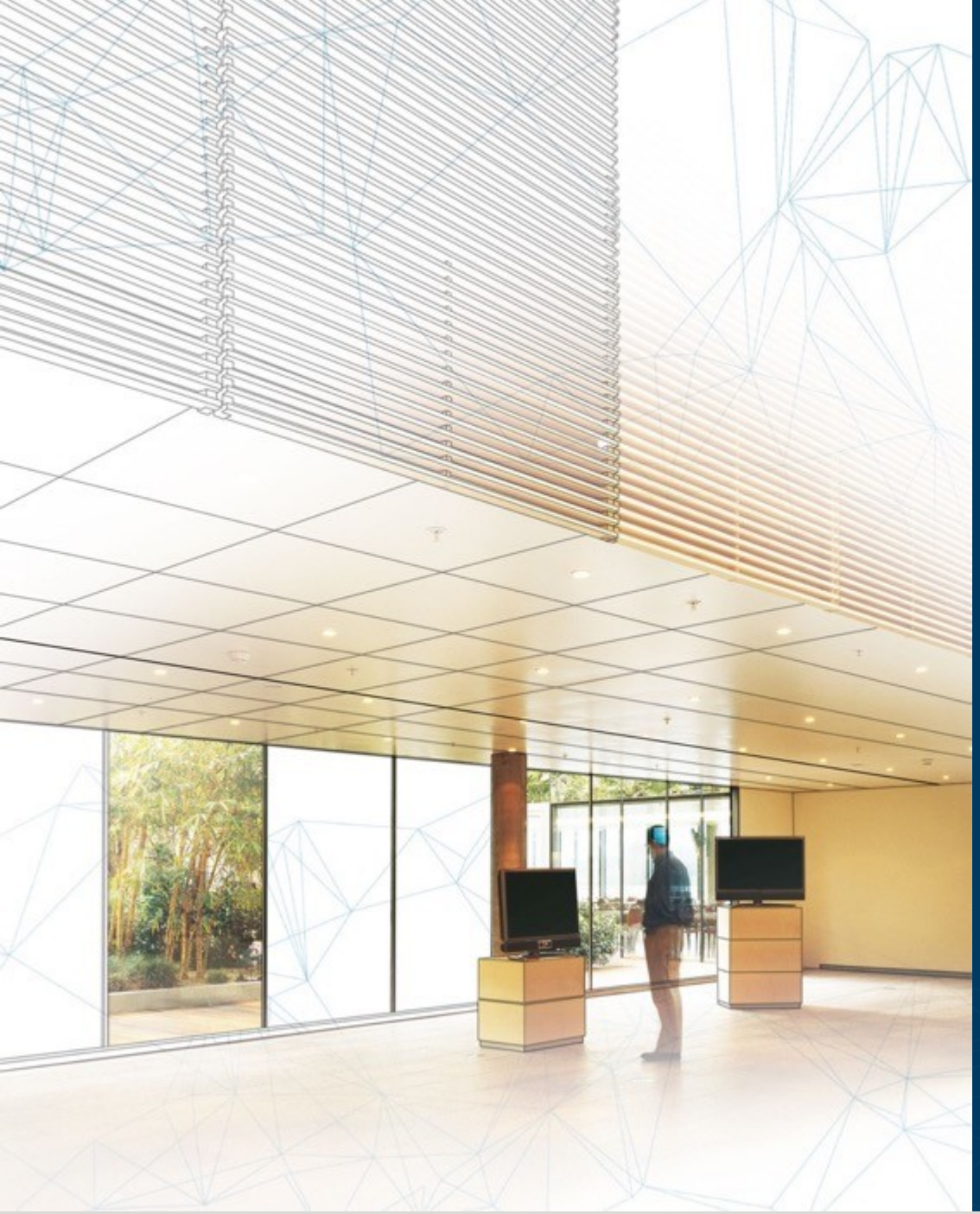
- “A series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms.” (Wikipedia)
- Petya ransomware embedded directly inside a software accounting (MeDoc) affected Ukraine
- MeDoc was installed on ~1M computers
- 27 June 2017 MeDoc automatic update system was compromised and used to download and run malware rather than updates for the software.
  -
  -

KUDELSKI SECURITY

A good read

- https://github.blog/2020-09-02-secure-your-software-supply-chain-and-protect-against-supply-chain-threats-github-blog/
- https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- https://utkusen.com/blog/security-by-obscurity-is-underrated.html
- https://www.wired.com/story/petya-plague-automatic-software-updates/
- https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine

KUDELSKI SECURITY



KUDELSKI SECURITY