ARTEFACT

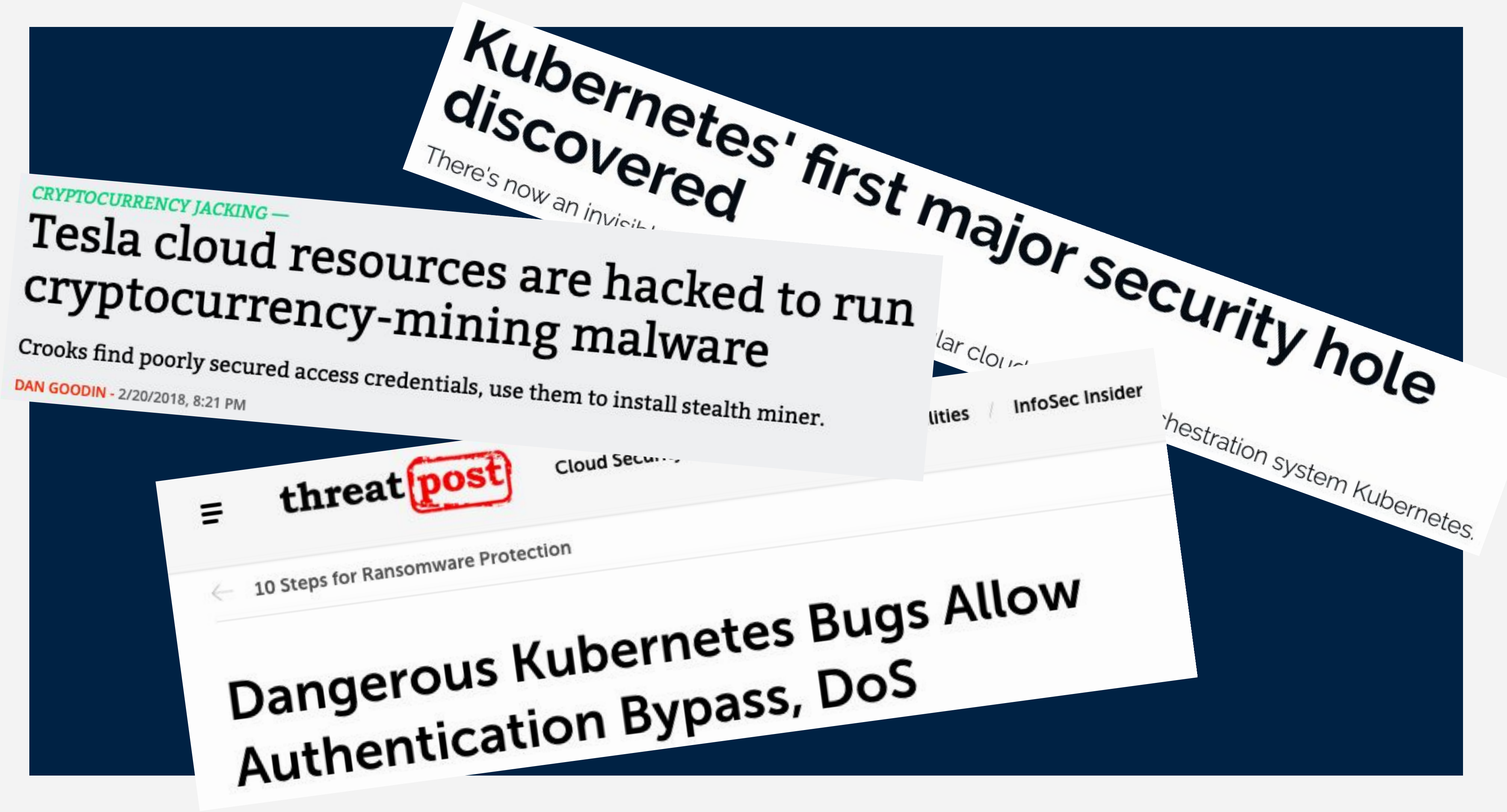
VALUE BY DATA

ARTEFACT

VALUE BY DATA

Kubernetes security

How to secure your Kubernetes cluster
Benoît Goujon



Kubernetes' first major security hole discovered

There's now an invisib

lar clou

hestration system Kubernetes.

CRYPTOCURRENCY JACKING —

Tesla cloud resources are hacked to run cryptocurrency-mining malware

Crooks find poorly secured access credentials, use them to install stealth miner.

DAN GOODIN - 2/20/2018, 8:21 PM

≡ threatpost

Cloud Secu

lities | InfoSec Insider

← 10 Steps for Ransomware Protection

Dangerous Kubernetes Bugs Allow Authentication Bypass, DoS

The CNCF started to take Kubernetes vulnerabilities seriously

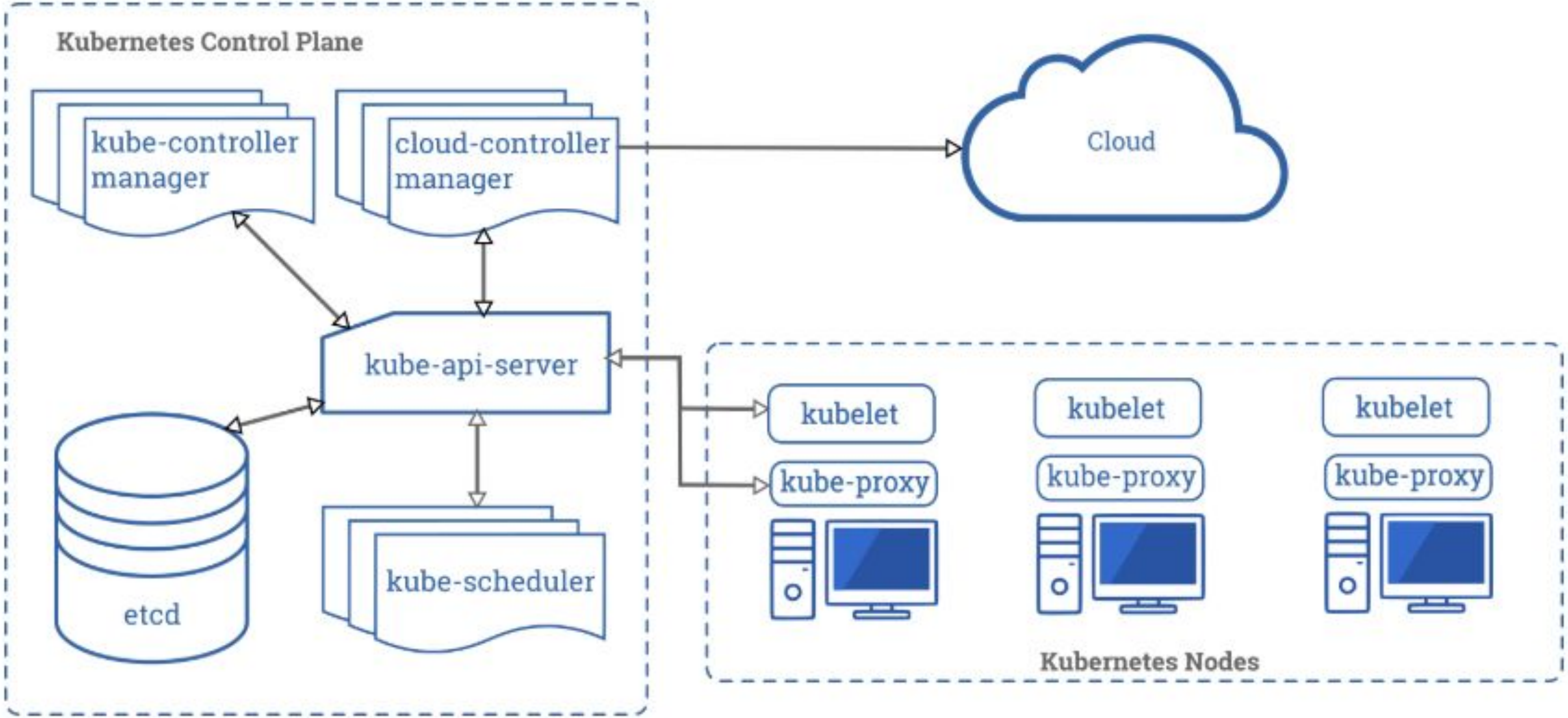
They launched a bunch of initiatives to help everyone secure their Kubernetes clusters

Open source security audit

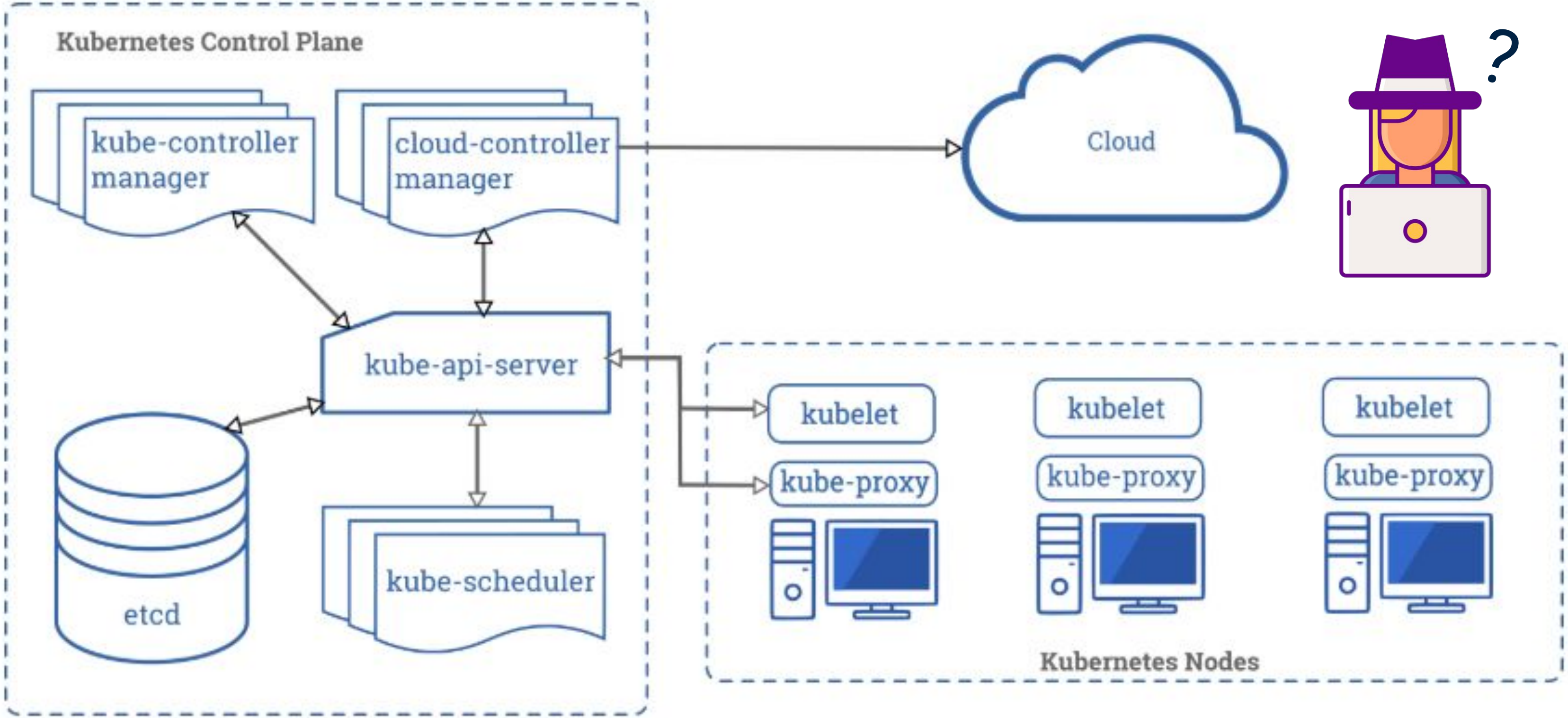
Bug Bounty program

Framework and tools

Kubernetes components

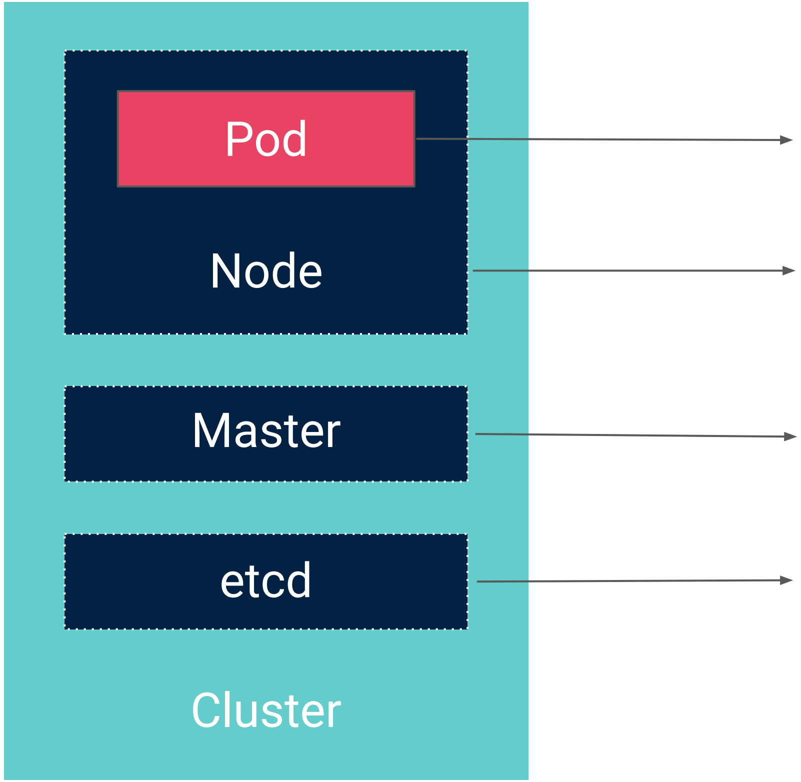


Kubernetes components



What is the most interesting component for a malicious hacker like Alice?

Kubernetes components sensitivity



If attacker controls the container, they might be able to escape and control the node.

If attacker controls nodes they control the pods running on them and might abuse compute.

If attacker controls the master, they control the cluster.

If attacker controls etcd, they can access, modify or destroy your cluster.

How to protect against malicious attackers?

Defense in depth

- Combine multiple layers of security
- Example: secret protection
  - limit kubectl access
  - API server authentication
  - Close default ports
  - permissions for reading etcd content (authorization)
  - Encryption

Least privilege principle

- restrict access so that different components can access only the information and resources they need to operate correctly
- Example: Use IAM roles of your organisation

Limiting the attack surface

- Set of all possible ways a system can be attacked. The greater the complexity, the bigger the attack surface.
- Example: reduce the size of your Docker images

Is Kubernetes security a concern when you use a cluster managed by a public cloud provider?

Shared responsibility principle

Cloud provider responsibility:

- Operating system
- Physical hosts
- Physical network
- Physical datacenter
- Control plane security

Your responsibility:

- Client endpoints
- Account & Access management
- Application

How to protect your application?

Best practices

Reduce Image size

Carefully manage dependencies

clair

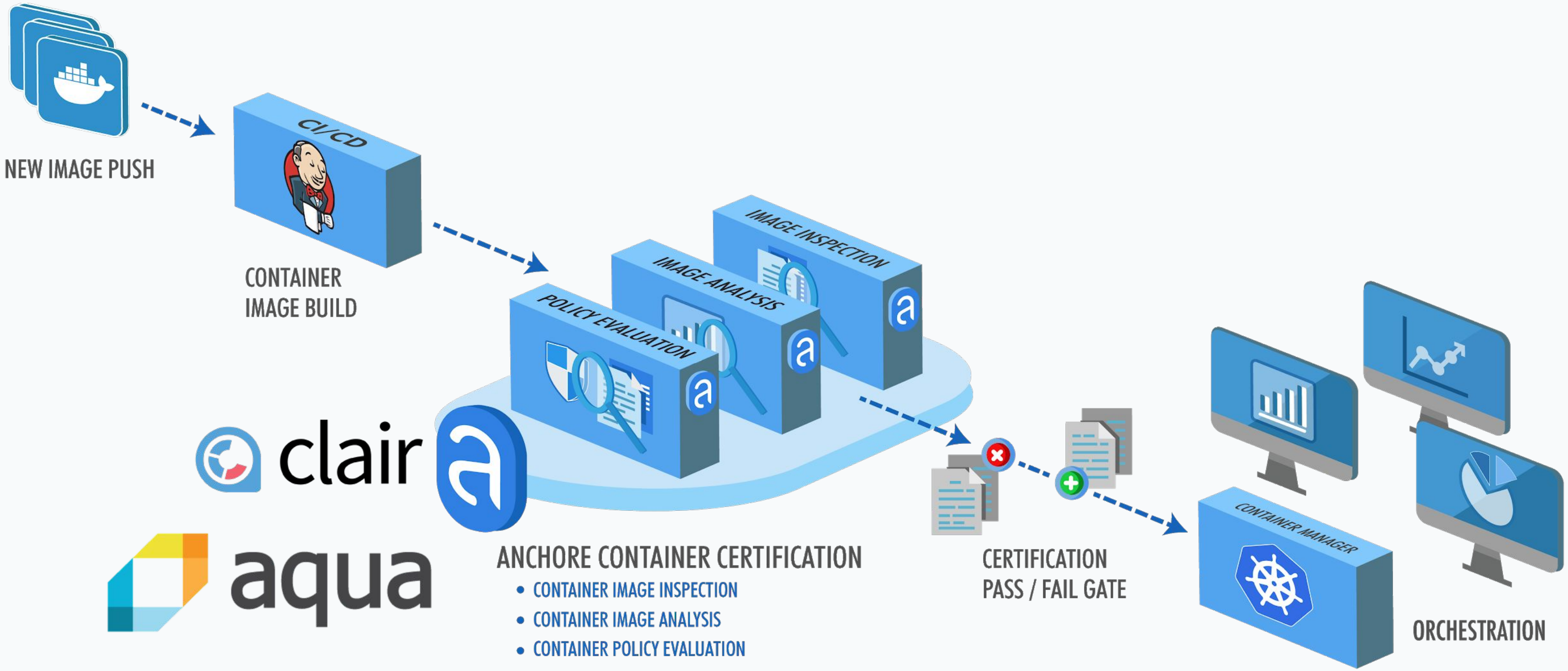
aqua

Add security checks in your CI pipeline

Download trustworthy images

Keep your Secrets

Integrate scan for vulnerabilities directly in your CI pipeline



ANCHORE CONTAINER CERTIFICATION

- CONTAINER IMAGE INSPECTION
- CONTAINER IMAGE ANALYSIS
- CONTAINER POLICY EVALUATION

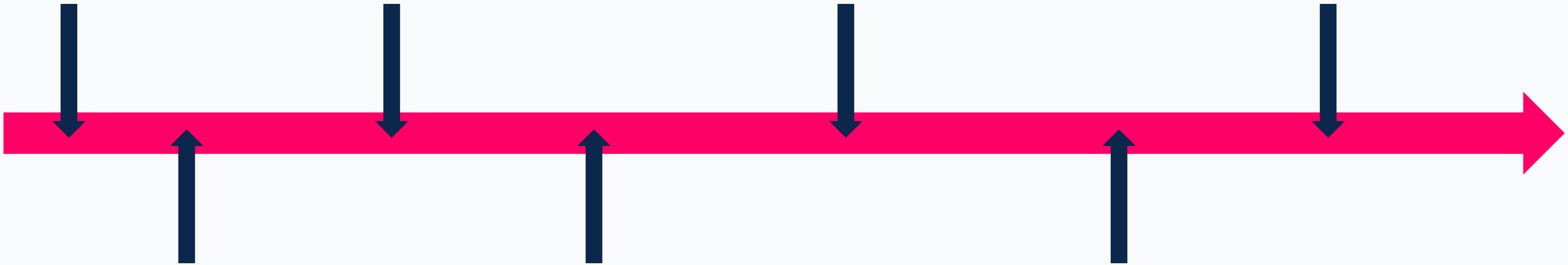
CERTIFICATION PASS / FAIL GATE

Sandboxing and runtime protection

Create an environment that isolates your application

- Sandboxing: ability to isolate containers from each other and from the underlying host
- Runtime protection: limiting the set of code that can be executed within the container itself
- Seccomp is a kernel mechanism for limiting system calls
- AppArmor and SELinux are also good kernel security modules

Key takeaways



K8s is insecure by default and has already suffered from cyber attacks.

Security is nowadays a concern for the CNCF.

Each component has its own weaknesses an attacker can exploit.

Traditional cybersecurity principles apply to K8s.

Even with managed clusters, this is your responsibility to secure your cluster.

Leverage existing tools to help you secure your applications and your cluster.

Separate your workloads from the cluster for better defense.

Thank you for your attention!

We’re hiring!
-> benoit.goujon@artefact.com