How to implement #security as #code

Security as Code in a large-scale DevOps environment

Christoph Hartmann
@chri_hartmann

mondoo

Hi, I am Chris. I am CTO at Mondoo - leader in Security Posture Management

What is your background?

Y

I co-created the open source security projects **DevSec Project** and **InSpec**, Co-Founded **Vulcano Security** (acquired by Chef Software) and was **Director of Engineering** at Chef Software

What is Security as Code?

Security as code is the practice of integrating security controls and practices into the software development process through the use of code and automation tools.

Why is that a problem?

Hackers used to look like this

mondoo

Ransomware is a business

Sales Quotas

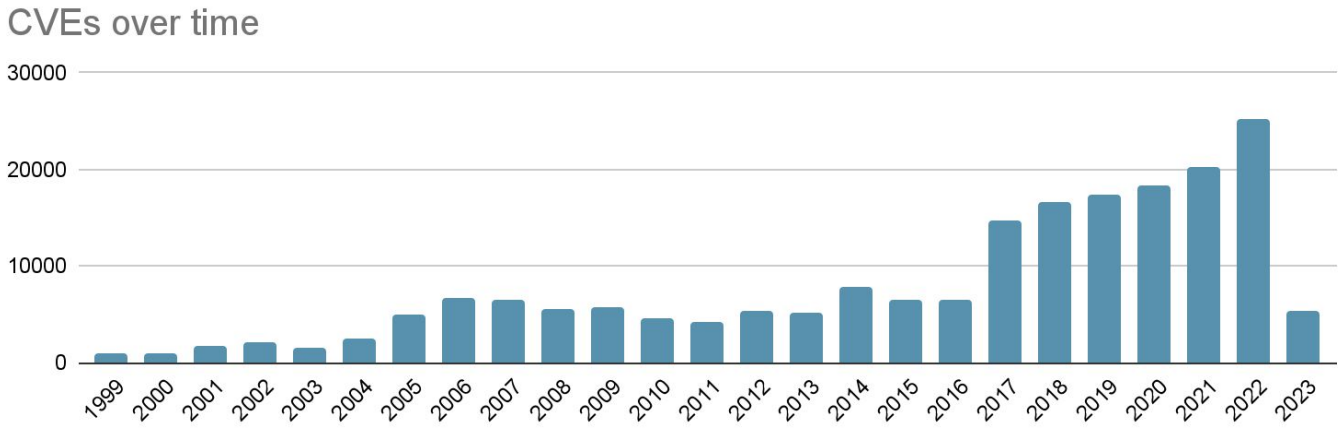
Playbooks

Customer Support

Affiliate Programs

mondoo

Average of 20% increase of YoY CVE publication



mondoo

Vulnerability Discovery

Vulnerability
discovered

CVE
assigned

Patch
by vendor

CVE
published

0-Day
Exploit

Exploit

~25% of CVEs have known exploits
14% exploits published before the patches
23% exploits published in the first week after CVE
50% exploits were published in the first month after CVE

mondoo

Patch Rollout

Identify
in dev

Report
created

Tickets
created

Fixed
in dev

Rollout
Slow

According to NTT Application Security average time to fix high severity vulnerabilities is about 246 days

mondoo

Issues outpace the fix

Yearly increase of 20% of known vulnerabilities

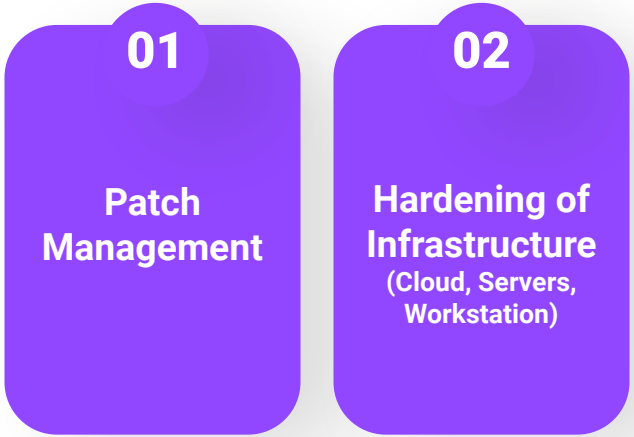
Hackers use full automation to discover and hack targets, about 90% of exploits are available within the first month after the CVE has been published

Rollout of fixes is way too slow

Independent survey of 1100 IT and security professionals

mondoo

Main Problems:
Why Hackers are so successful?



The same root causes are also corroborated in the Cyber Signals Report by Microsoft that revealed 80% of attacks can be attributed to outdated software and misconfiguration.

mondoo

Why is it so difficult?

Software delivery

Local Development | Source Control | CI/CD | Pre-Production | Production

mondoo

Use Case:
Ensure that Cloud Storage Buckets have a uniform bucket level access enabled

Security Engineers focus on attack paths

Ensure that Cloud Storage Buckets have a uniform bucket level access enabled

Google Cloud

aws

Microsoft Azure

mondoo

Platform Engineers focus on automation

Ensure that Cloud Storage Buckets have a uniform bucket level access enabled

HashiCorp Terraform

Software delivery

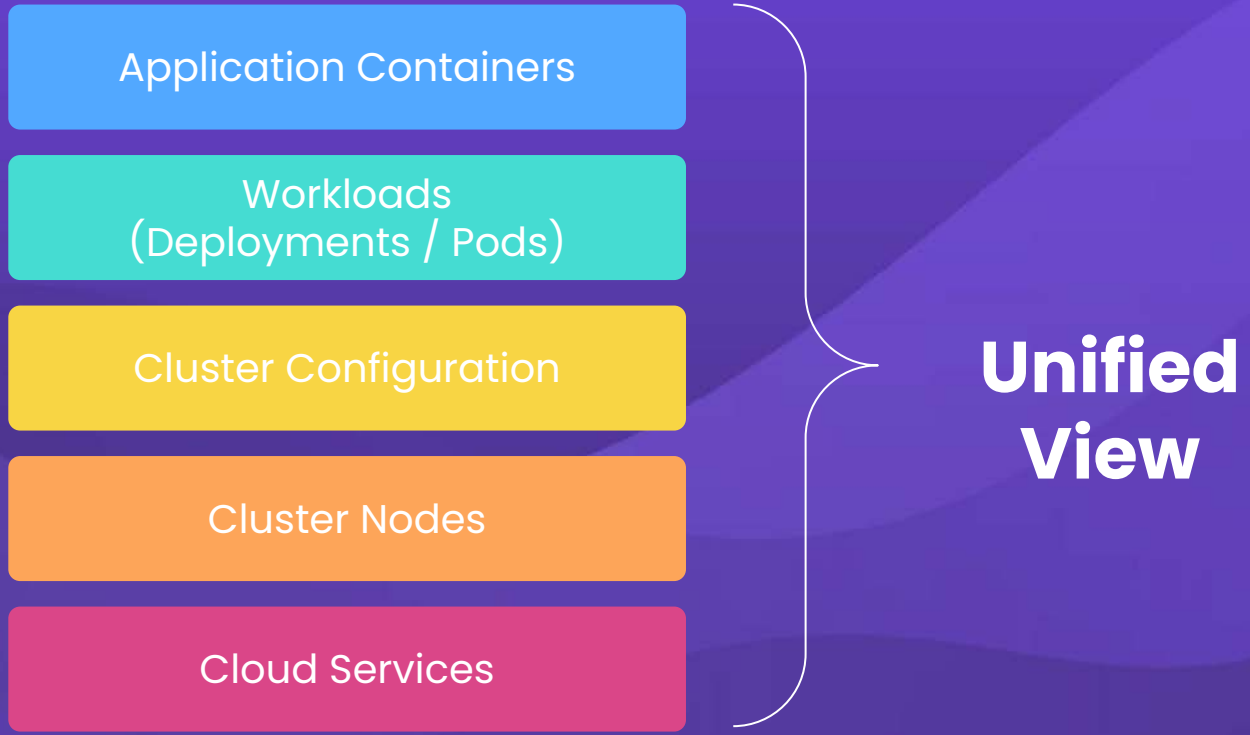
Local Development | Source Control | CI/CD | Pre-Production | Production

mondoo

Leads to frustration

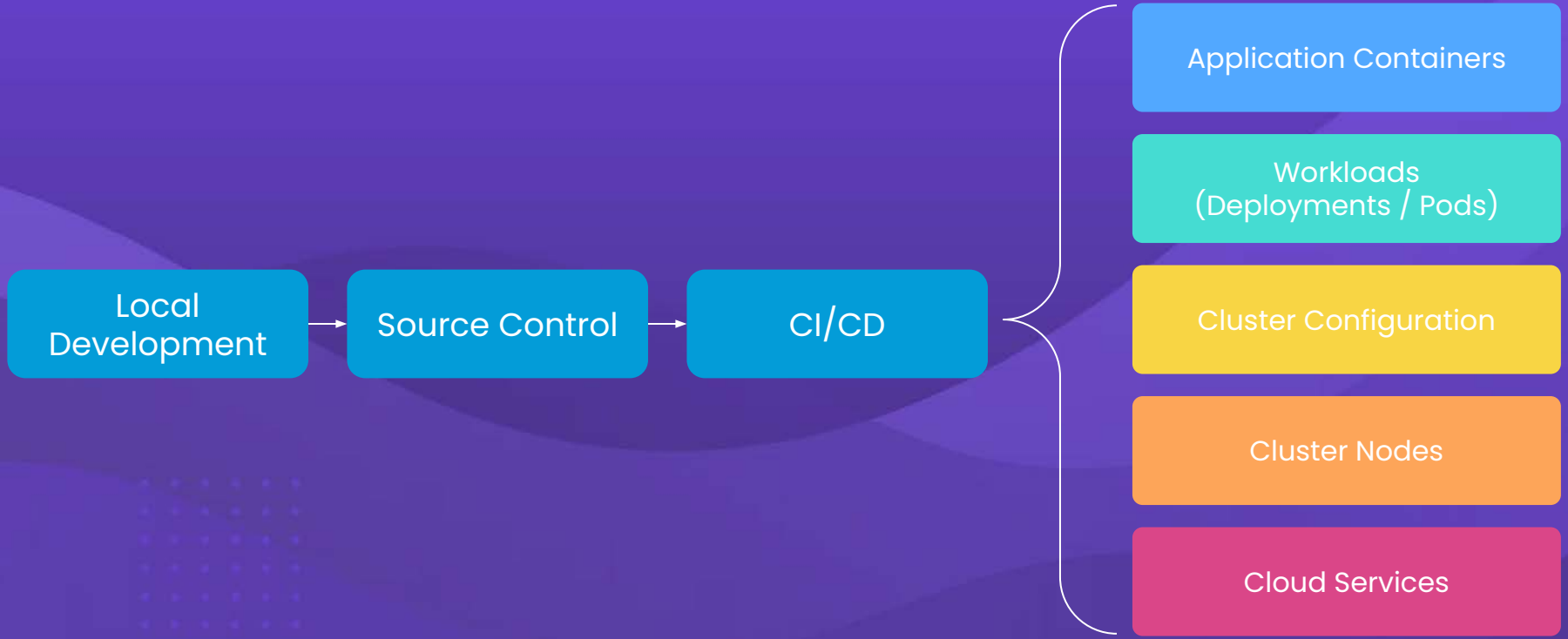
What is the solution?

Tech Stack



mondoo

Application Delivery Pipeline



mondoo

What do we need for Security as Code?

Static and dynamic testing

eg.
Terraform,
Kubernetes Manifests

Package vulnerability management

eg.
Container in Build and Runtime

Continuous Security testing

eg.
AWS and MS 365

Secure Coding Practices

eg.
Input Validation

mondoo

Reach the next level: Focus on Problem

Ensure that Cloud Storage Buckets have a uniform bucket level access enabled

Microsoft Azure

aws

HashiCorp Terraform

Google Cloud

Software delivery

Local Development | Source Control | CI/CD | Pre-Production | Production

mondoo

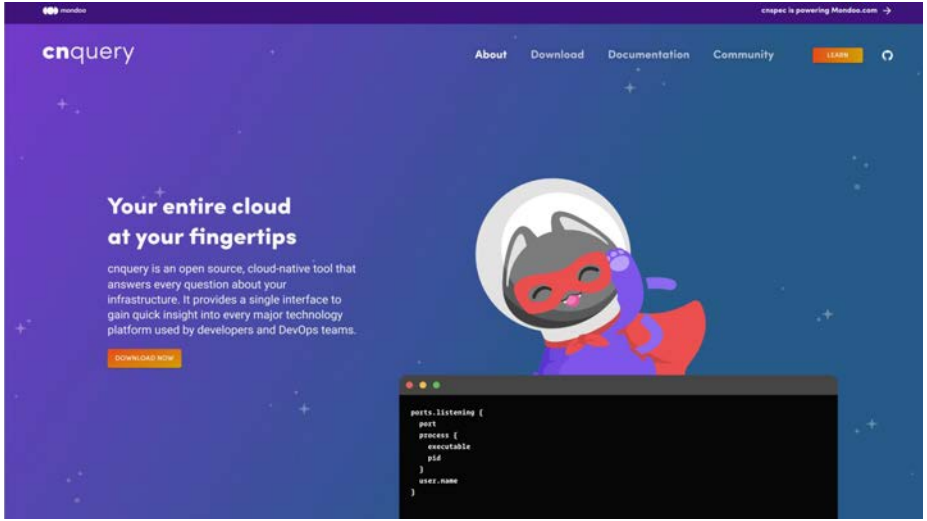
IaC and Policy as Code?

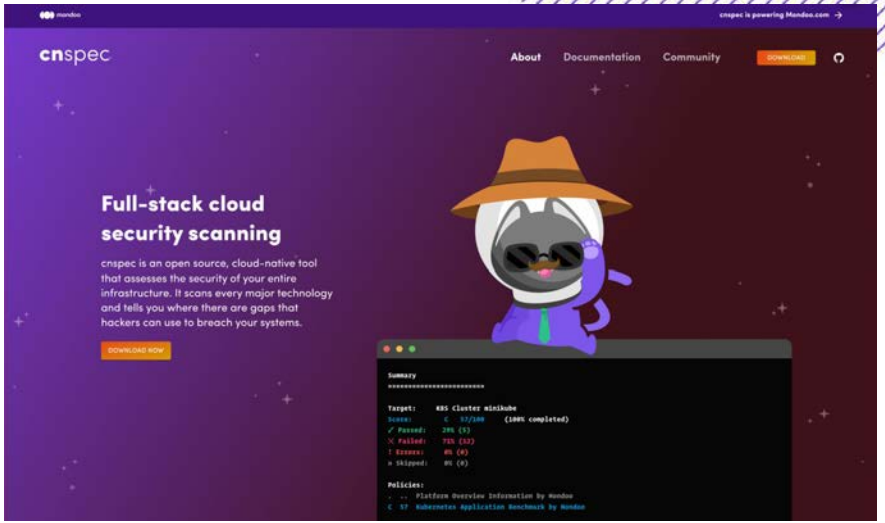
	Infrastructure as Code	Policy as Code
Approach	define and manage infrastructure resources, such as cloud accounts, vms, networks, and storage.	define security policies that cover security, operational and compliance requirements.
Extensibility	- Provider - Resources - HCL	- Provider - Resources - Queries & Policies
Examples	terraform (cloud, saas) ansible (os)	- cnspec (cloud, saas, os, container) - InSpec (cloud, os)
Benefits	Increased efficiency, improved consistency, and reduced human error	

Successful Security as Code practices

1. **Access**: Every developer and security engineer has access to the same tooling
2. **Coverage**: security tooling that supports build and runtime
3. **Automation**: security tooling that works hand-in-hand with automation
4. **Extensible**: security tooling that has open source foundation, not hard-coded rules

open source security





github.com/mondoohq/cnquery

Graph-based asset inventory

github.com/mondoohq/cnspec

Secure everything from development to production

mondoo

Easily ask questions with GraphQL-based MQL

Amazon S3 buckets do not allow public read access

```
terraform.resources.where(
  nameLabel == 'aws_s3_bucket_public_access_block'
) {
  arguments['block_public_acls'] == true
  arguments['block_public_policy'] == true
  arguments['ignore_public_acls'] == true
  arguments['restrict_public_buckets'] == true
}
```

S3 Buckets are configured with 'Block public access'

```
aws.s3.buckets.all(
  publicAccessBlock['BlockPublicAcls'] == true &&
  publicAccessBlock['BlockPublicPolicy'] == true
)
```


mondoo

Use Security as Code to define requirements

```yaml
policies:
  - uid: cloud-security
    name: Public Bucket Policy
    version: "1.0.0"
    authors:
      - name: Mondoo
        email: hello@mondoo.com
    groups:
      - title: Permissions
        checks:
          - uid: check-public-bucket
            title: Bucket is not public
            variants:
              - uid: check-public-bucket-terraform
              - uid: check-public-bucket-aws-s3
```

```
queries:
  - uid: check-public-bucket-terraform
    filters: asset.platform == "terraform-hcl"
    title: Bucket is not public (terraform)
    mql: |
      terraform.resources.where(
        nameLabel == 'aws_s3_bucket_public_access_block'
      ) {
        arguments['block_public_acls'] == true
        arguments['block_public_policy'] == true
        arguments['ignore_public_acls'] == true
        arguments['restrict_public_buckets'] == true
      }
  - uid: check-public-bucket-aws-s3
    filters: asset.platform == "aws"
    title: Bucket is not public (aws)
    mql: |
      aws.s3.buckets.all(
        publicAccessBlock['BlockPublicAcls'] == true &&
        publicAccessBlock['BlockPublicPolicy'] == true
      )
```

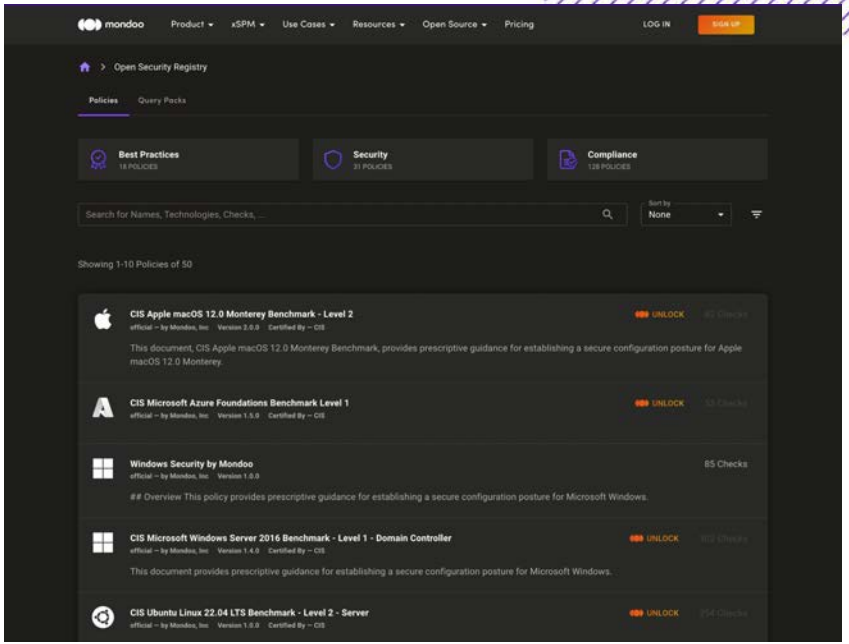

mondoo

Discover Security Content

Security Registry
mondoo.com/registry

Security Policies
github.com/mondoohq/cnspec-policies

Inventory and Incident Response Query Packs
github.com/mondoohq/cnquery-packs



mondoo

We can be more secure!

Local Development | Source Control | CI/CD | Pre-Production | Production

mondoo

Find anything.
Secure everything.

Reveal vulnerabilities, lost assets, and policy violations in every part of your infrastructure—before they become exploits.

xSPM – Extensible Security Posture Management

1. Continuous monitoring of the complete infrastructure stack (from local via CI/CD to production)
2. Open Source based Policy as Code (easy extensible + customizable)
3. Detection of security threats / vulnerabilities
   Detection of configuration drift
4. Alerting and notification of security issues
5. Remediation of security issues through automated or manual processes
6. Continuous Compliance reporting and tracking

mondoo

We built a platform we are using

Soo Choi
CEO

Christoph Hartmann
CTO

Dominik Richter
CPO

Patrick Münch
CISO

we worked at

Google DORA DEVOPS RESEARCH & ASSESSMENT CHEF NASA rackspace VulcanoSec SVA

mondoo

Thank you

Christoph Hartmann

🐦 @chri_hartmann
✉️ chris@mondoo.com
🏠 mondoo.com

mondoo