

Re-inventing Open Source **#Security** for DevOps and OT-Security

Christoph Hartmann
@chri_hartmann



Hi, I am Chris. I am CTO
at Mondoo

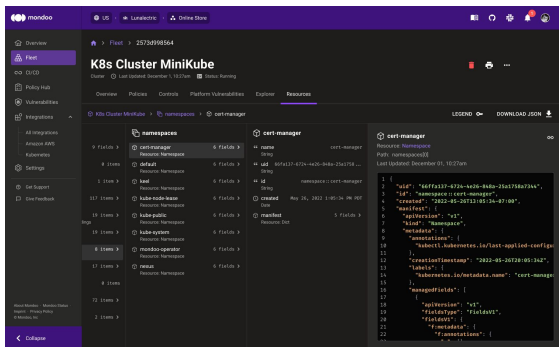
What is your
background?

Y

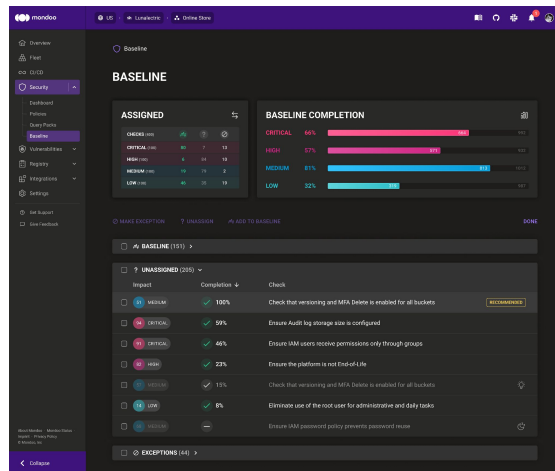
I co-created the open source
security projects **Dev-Sec.io** and
InSpec, Co-Founded **Vulcano
Security** (acquired by Chef
Software) and was **Director of
Engineering** at Chef Software

Mondoo is a security, risk and compliance platform that identifies vulnerabilities and misconfiguration from build to runtime.

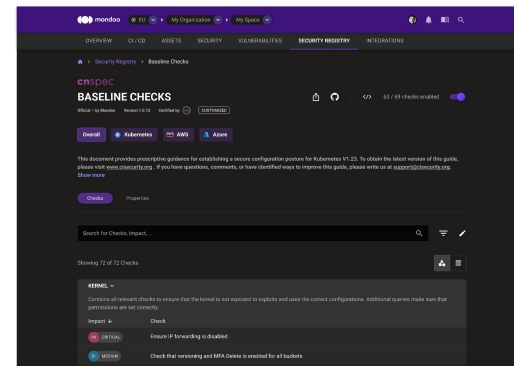
Asset Intelligence



Risk Actions



Smart Compliance



Find answers to complex questions at every layer through "Google Search" for Security Posture Management

Improve your overall posture by proactively identify, prioritize, remediate risks

Reduce compliance completion times with real-time compliance assessments and evidence across build and runtime

Security Therapy



Interviewed and worked with 100+ Sec/DevOps Leaders

Theme	In their words.....
More organized threats	Software is eating the world so hackers are having a feast
Wait days/weeks to data	Coordinating over 30+ security tools to answer if we have the vulnerability and then waiting for verification it's been fixed
Security owns all the tools	DevOps don't have consistent access to what security uses, just their outputs aka a giant spreadsheet
Security vendors are slow	Their product roadmap is the same every year, so we hacked a solution to dump into Splunk
Unclear on the right priority for the business	The trade off between shipping new features vs fixing what security wants us to fix.
Re-enforces good practices	I need my teams to have a way continuous improve our posture and for management to recognize the effort

Why is Security so difficult?

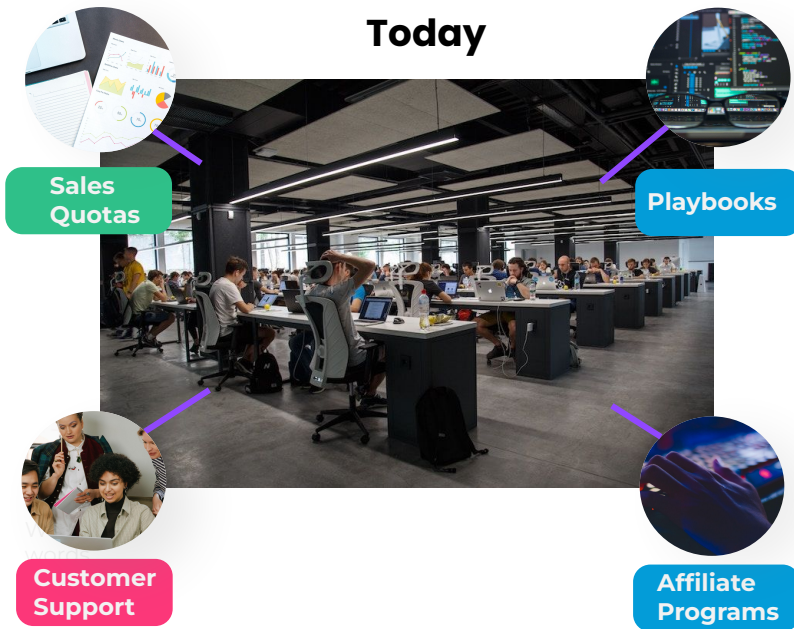


Times changed

Past

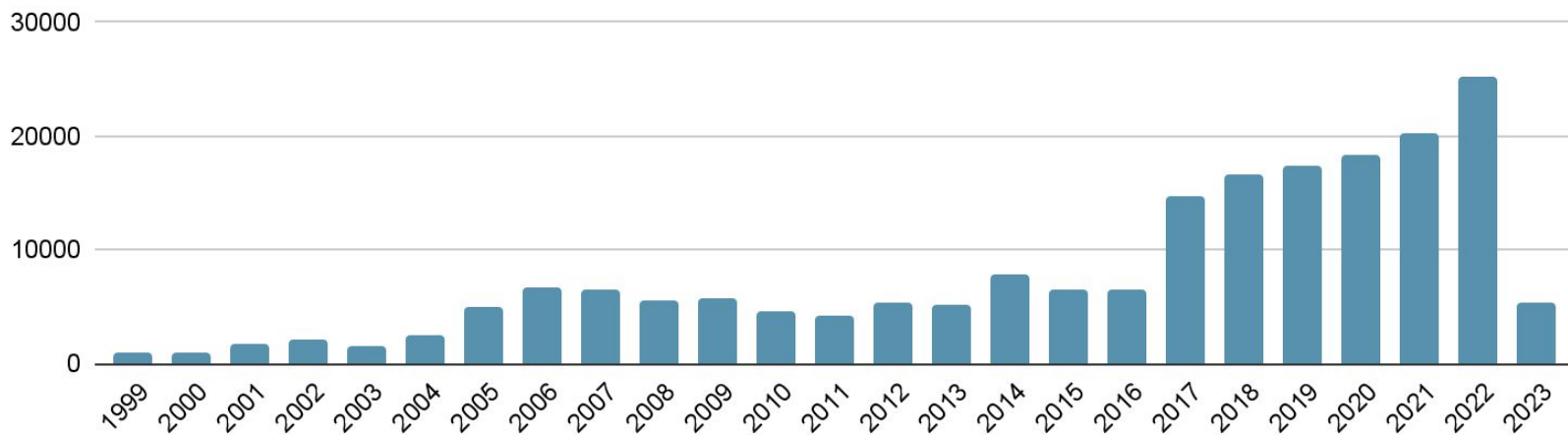


Today

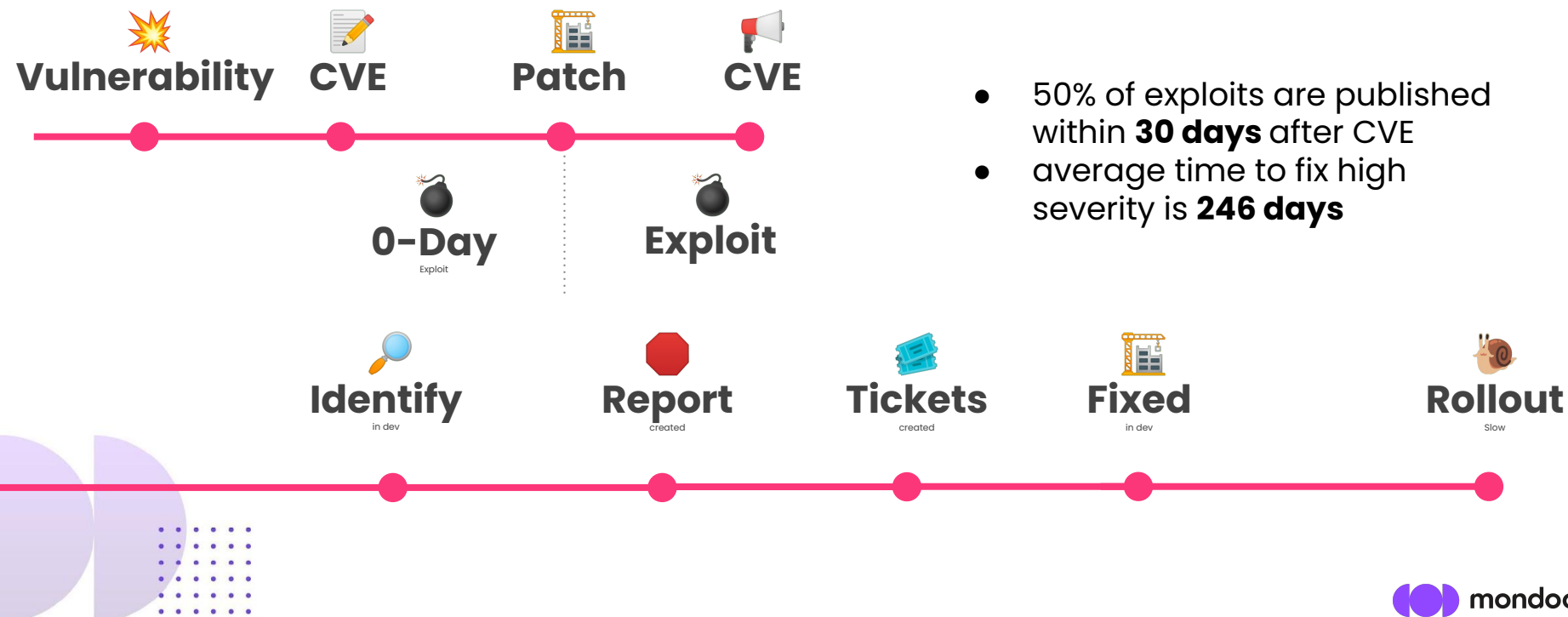


Avg 20% CVE YoY increase

CVEs over time



Exploit / Patch Time



Scan Internet in 5 min

Search or jump to...

Pull requests Issues Codespaces Marketplace Explore

robertdavidgraham / masscan Public

Watch 657 Fork 2.9k Star 20.9k

Code Issues 340 Pull requests 43 Actions Projects Wiki Security Insights

master 6 branches 11 tags

Go to file Add file Code

robertdavidgraham Merge pull request #617 from postmodern/fix_typos... 144c527 on Sep 6, 2021 705 commits

bin	bugs	10 years ago
data	mcGill physics	2 years ago
debian	New upstream release	9 years ago
doc	issue #574, fixed --retries	2 years ago
src	Fix typos in comments and in some log messages.	2 years ago
tmp	bugs	10 years ago
vs10	ndpv6 neighbor notification	2 years ago
xcode4	fixed issue #541	2 years ago
.gitattributes	faster --includefile	5 years ago
.gitignore	oproto	4 years ago
.travis.yml	added power support arch ppc64le on yml file.	3 years ago
LICENSE	Update LICENSE	10 years ago
Makefile	yet another change for gcc vs clang	2 years ago
README.md	typo	2 years ago
VULNINFO.md	1.3	3 years ago

README.md

Build Status

About

TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.

Readme

View license

20.9k stars

657 watching

2.9k forks

Report repository

Releases 11

1.3.2 (Latest) on Jan 31, 2021

+ 10 releases

Packages

No packages published

Contributors 50

80%
were victims of ransomware
attacks in 2022

MORE THAN 60%
of victims paid the
ransom

Source: Forbes:
Independent survey of
1100 IT and security
professionals



Compliance Frameworks

ISO27001:2022

A8.9 Configuration management

Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

BSI IT-Grundschatz-Compendium

SYS.1.1.A6 Disabling Unnecessary Services

All unnecessary services and applications—particularly network services—MUST be disabled or uninstalled....

Cyber Risk Insurance questionnaire

Questions for companies starting with 50.000.00 € revenue. Hardening is the first questions in sector "basics".

Are there guidelines for the secure configuration of servers and endpoints?

Compliance Frameworks

PCI-DSS

PCI Requirement 2

Apply Secure Configurations to All System Components

HIPAA

164.308 Administrative Safeguards

164.312 Technical safeguards

SOC2

The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Why do we need to deploy insecurely?



Developers +
Platform Engineers



Operations +
Security

DEVELOP

BUILD

RUNTIME

01

Patch
Management

02

Hardening of
Infrastructure
(Cloud, Servers,
Workstation, IoT)



Leads to frustration



AI will make attacks even easier



Home > News > Security > ChatGPT may be a bigger cybersecurity risk than an actual benefit

ChatGPT may be a bigger cybersecurity risk than an actual benefit

Sponsored by [Specops Software](#)

March 15, 2023 10:07 AM 3



ChatGPT made a splash with its user-friendly interface and believable AI-generated responses. With a single prompt, ChatGPT provided detailed answers that other AI assistants had not achieved. Powered by a massive dataset that ChatGPT had been trained on, the breadth and variety of topics it could address quickly amazed the tech industry and the public.

However the technology sophistication raises inevitable question: what are the drawbacks of ChatGPT and similar technologies? With capabilities to generate a multitude of realistic responses, ChatGPT could be used to create a host of responses capable of tricking an unassuming reader into thinking a real human is behind the content.

POPULAR STORIES



Microsoft PowerToys adds Windows Registry preview feature



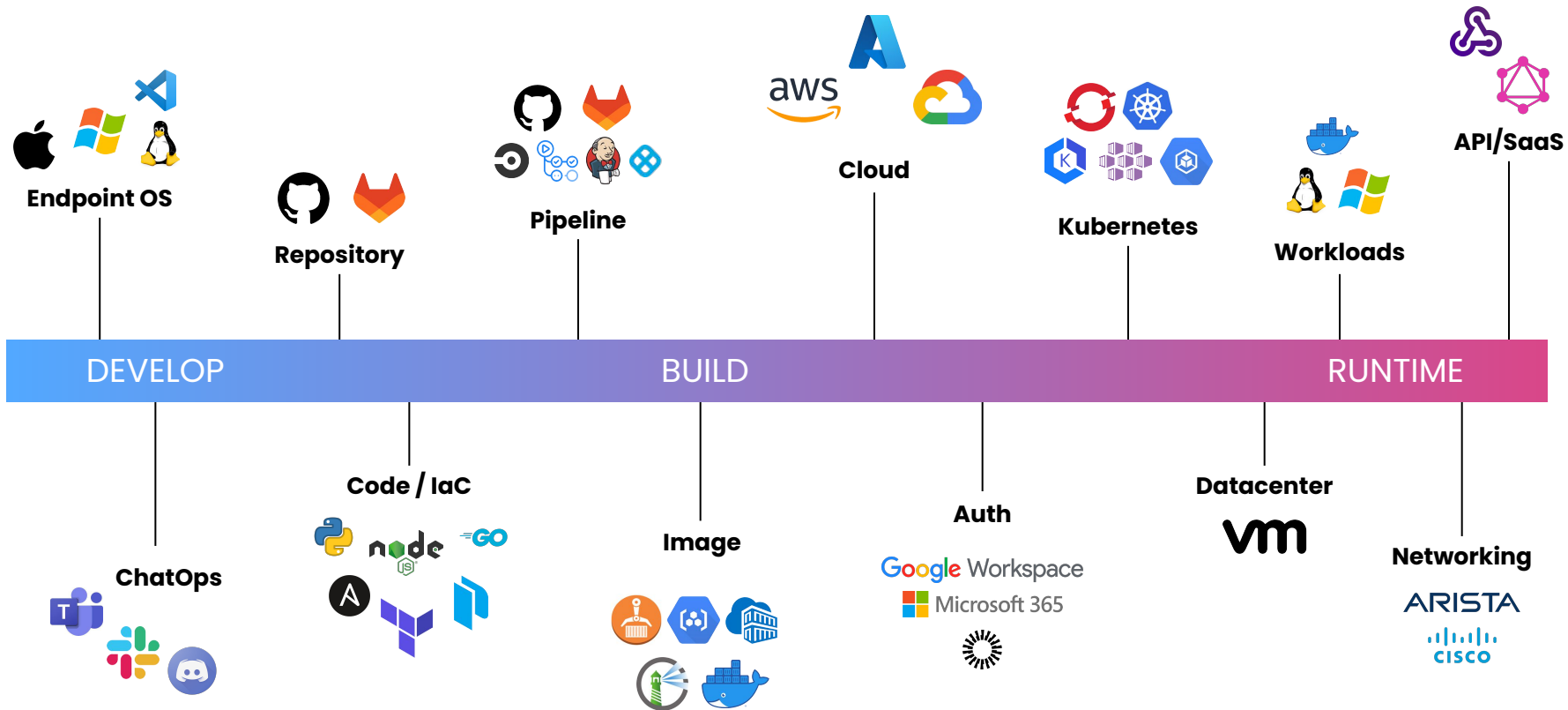
All Dutch gov't networks to use RPKI to prevent BGP hijacking

LATEST DOWNLOADS

	Malwarebytes Anti-Malware Version: 4.5.26	4M+ DOWNLOADS
	AdwCleaner Version: 8.4.0.0	56M+ DOWNLOADS
	Windows Repair (All In One) Version: 4.13.1	2M+ DOWNLOADS

Example

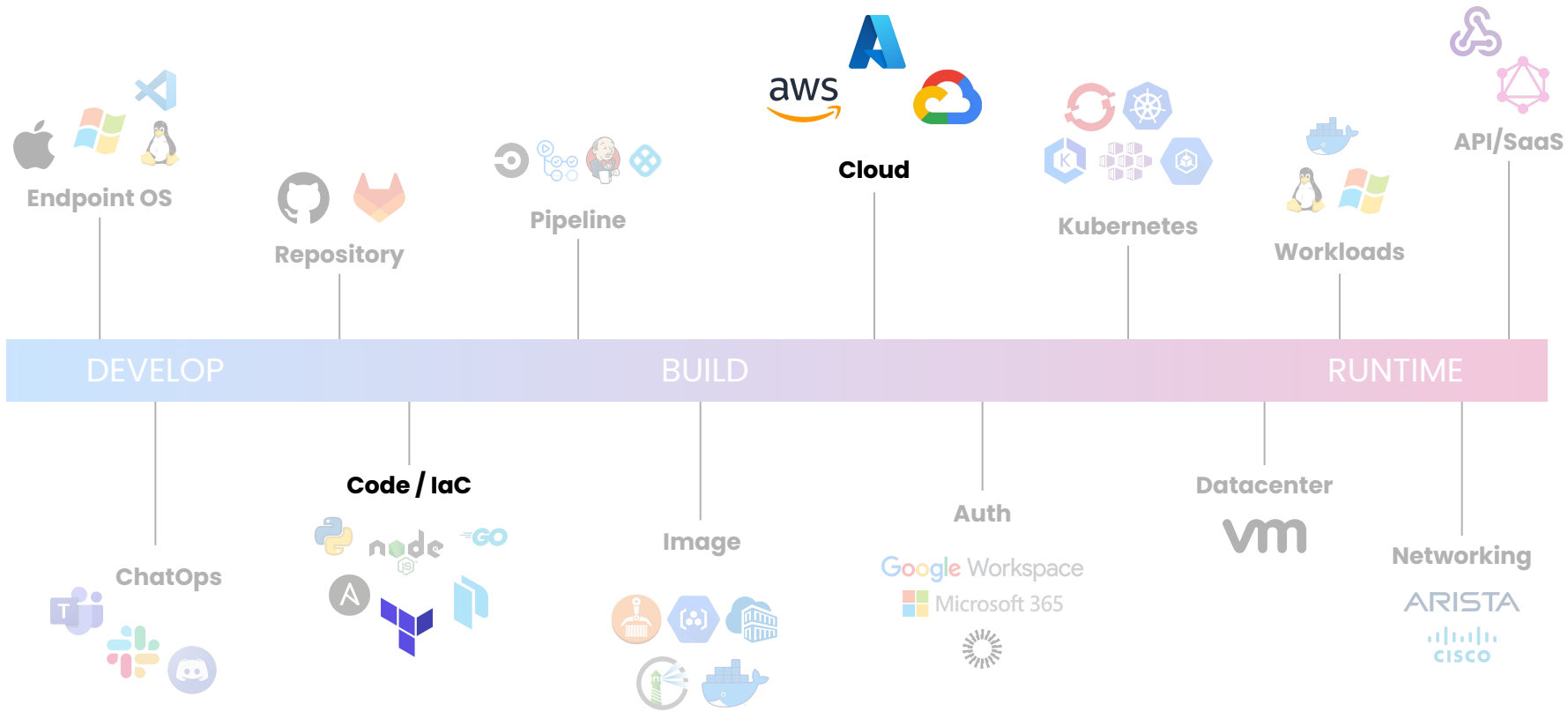






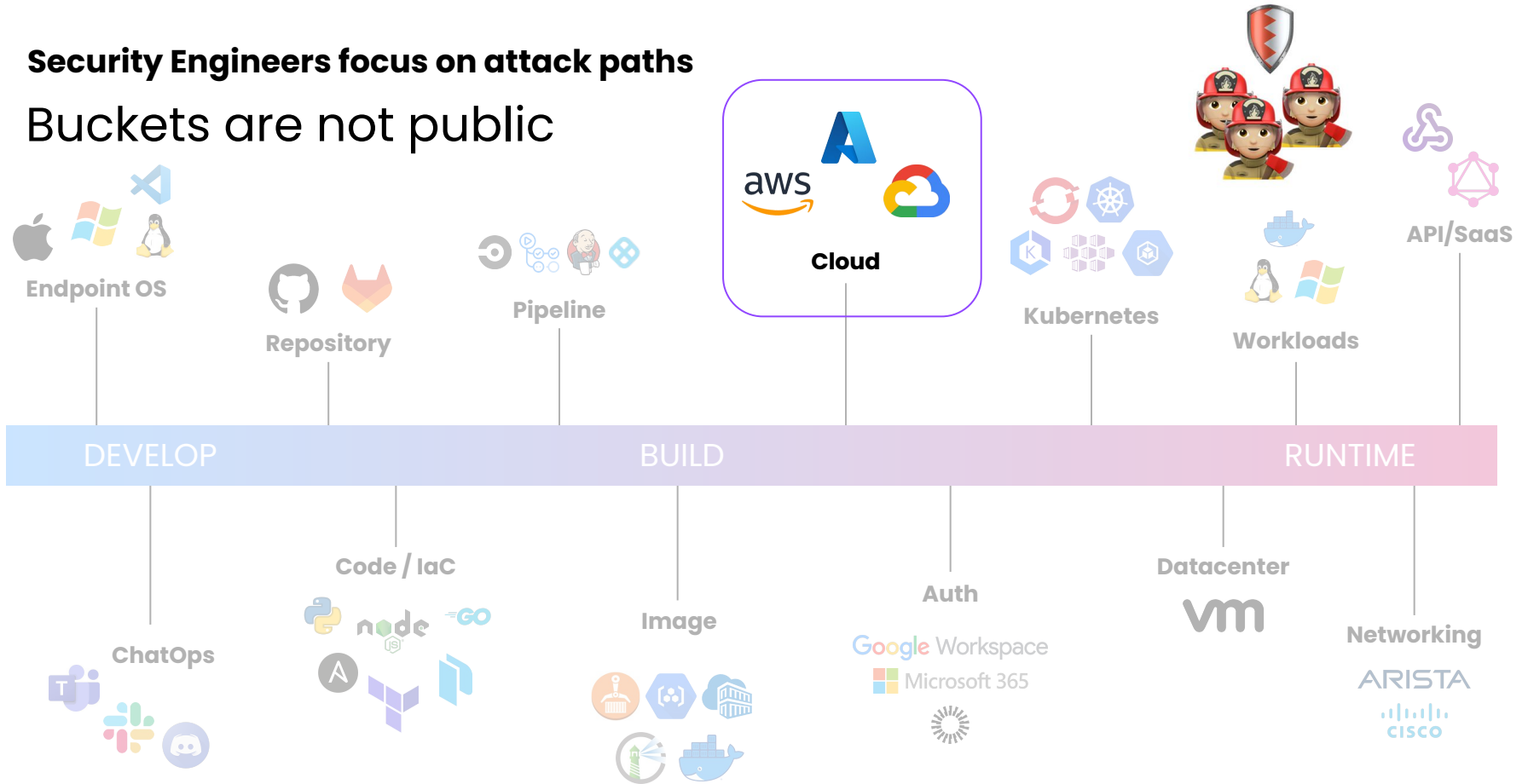
Use Case:

Ensure that Cloud Storage Buckets
are not public



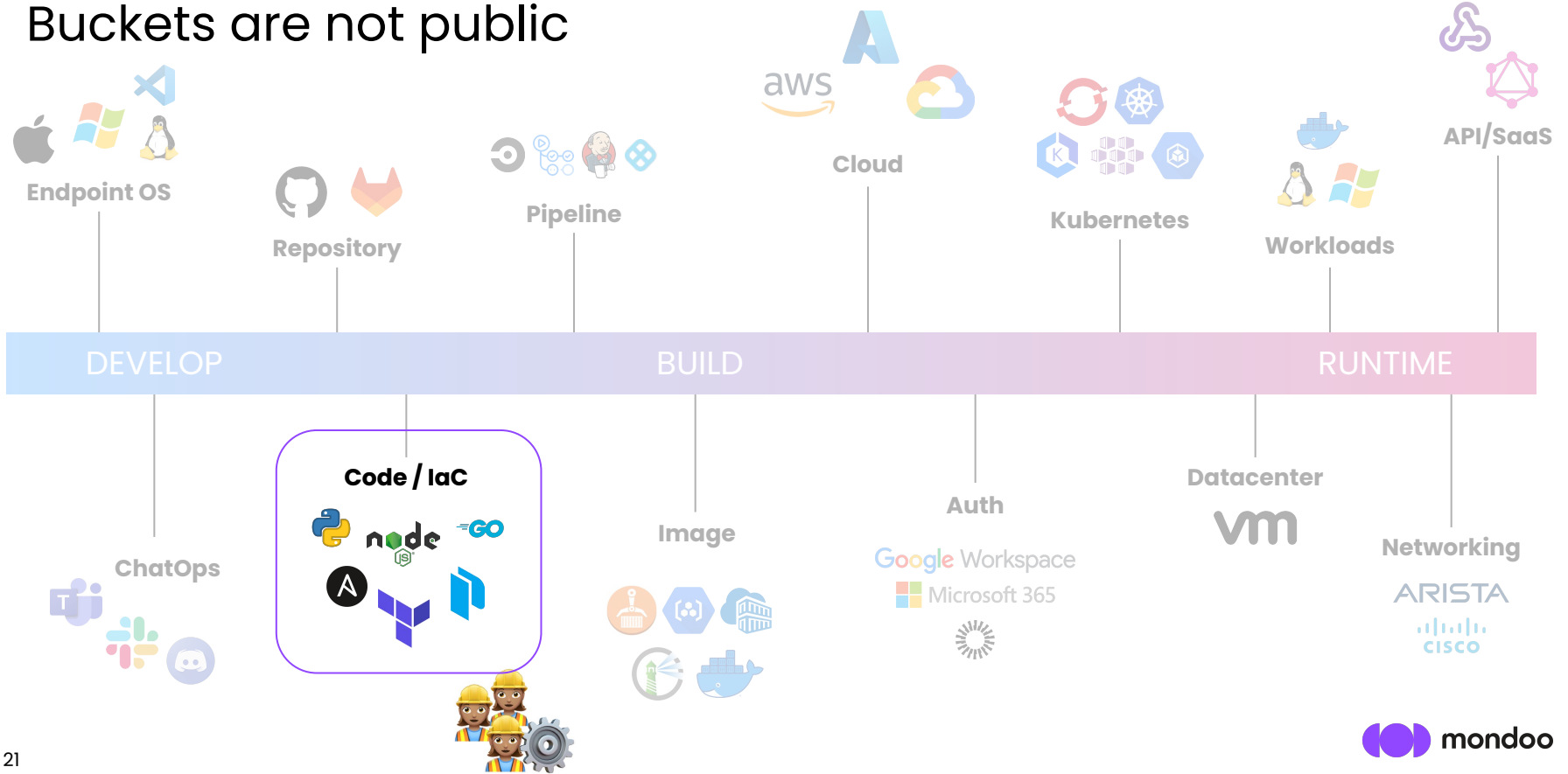
Security Engineers focus on attack paths

Buckets are not public



Platform Engineers focus on automation

Buckets are not public



Secure the Development Workflow

The development workflow is riddled with security gaps and toolsprawl. Lack of collaboration between development and security destroys productivity and increases risks.

Developers +
Platform Engineers

Operations +
Security

DEVELOP

BUILD

RUNTIME



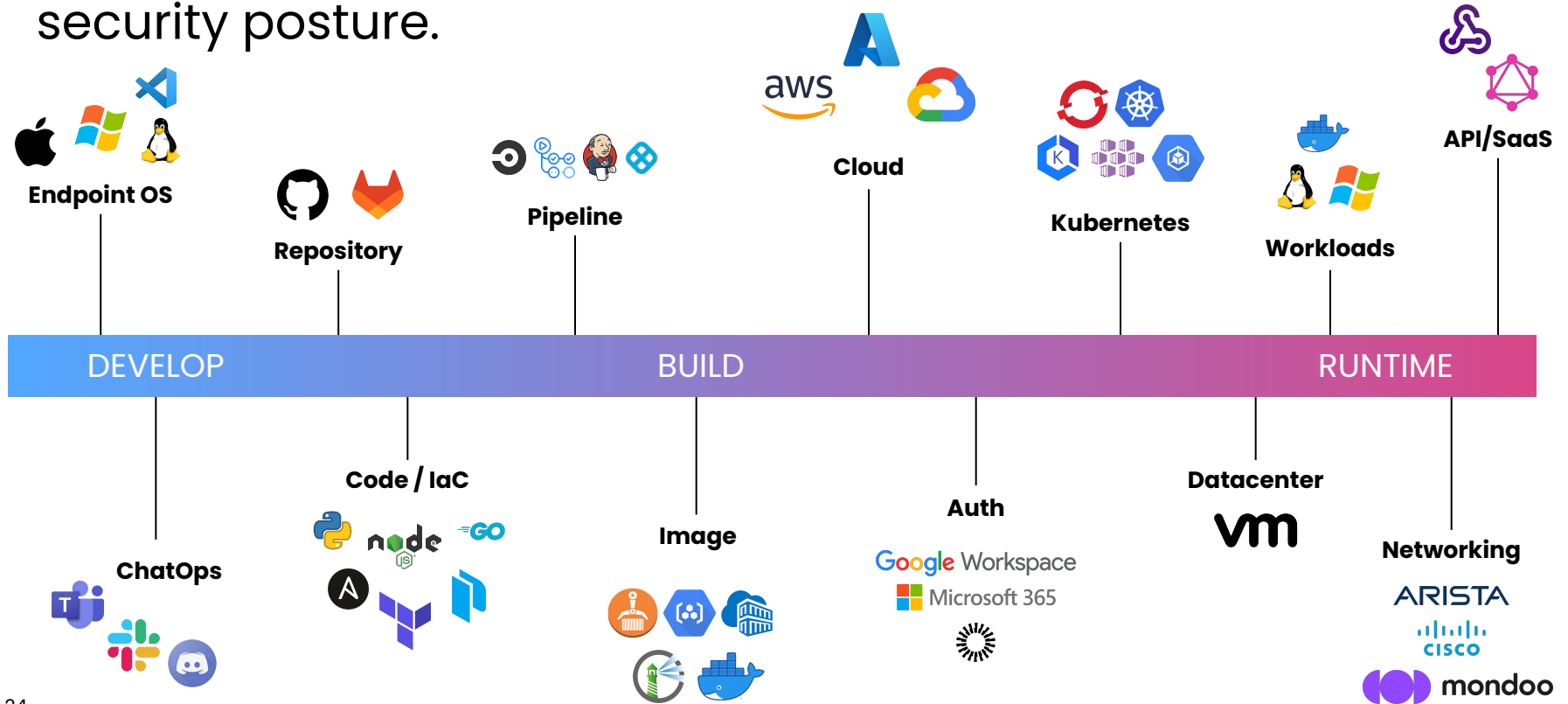
We need to think holistically about security

Ensure that Cloud Storage Buckets are not public



Focus on overall risk management

We need to bring all teams together to improve the security posture.



What can we do now?



Extensible and Open Security



Graph-based asset inventory

github.com/mondoohq/cnquery



**Secure everything from
development to production**

github.com/mondoohq/cnspec

Discover Security Content

Security Registry

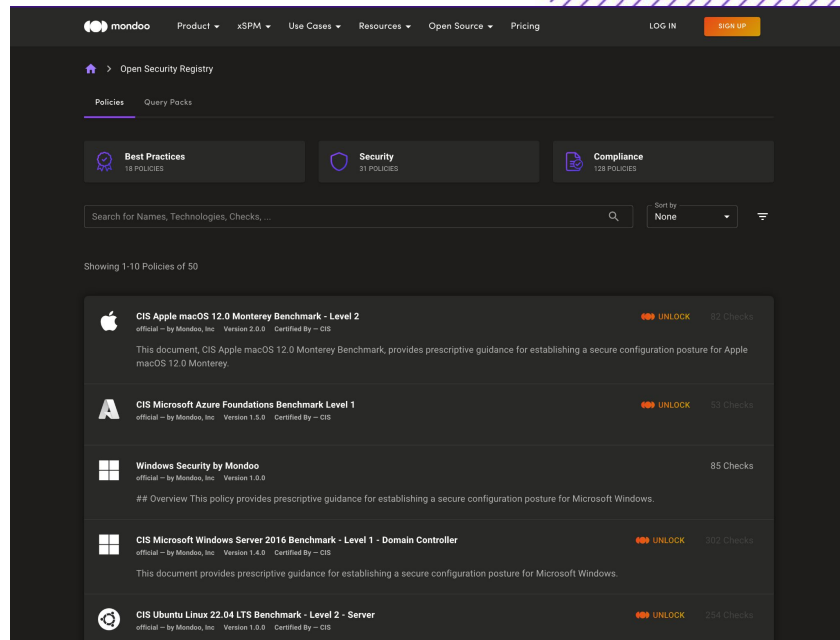
mondoo.com/registry

Security Policies

github.com/mondoohq/cnspec-policies

Inventory and Incident Response Query Packs

github.com/mondoohq/cnquery-packs



The screenshot displays the Mondoo Security Registry interface. At the top, there is a navigation bar with the Mondoo logo, a search bar, and links for Product, xSPM, Use Cases, Resources, Open Source, Pricing, LOG IN, and SIGN UP. Below the navigation bar, the main content area is titled "Open Security Registry" and features tabs for "Policies" and "Query Packs". Three main categories are highlighted: "Best Practices" (18 POLICIES), "Security" (31 POLICIES), and "Compliance" (128 POLICIES). A search bar is present with the placeholder text "Search for Names, Technologies, Checks, ...". Below the search bar, it indicates "Showing 1-10 Policies of 50". The list of policies includes:

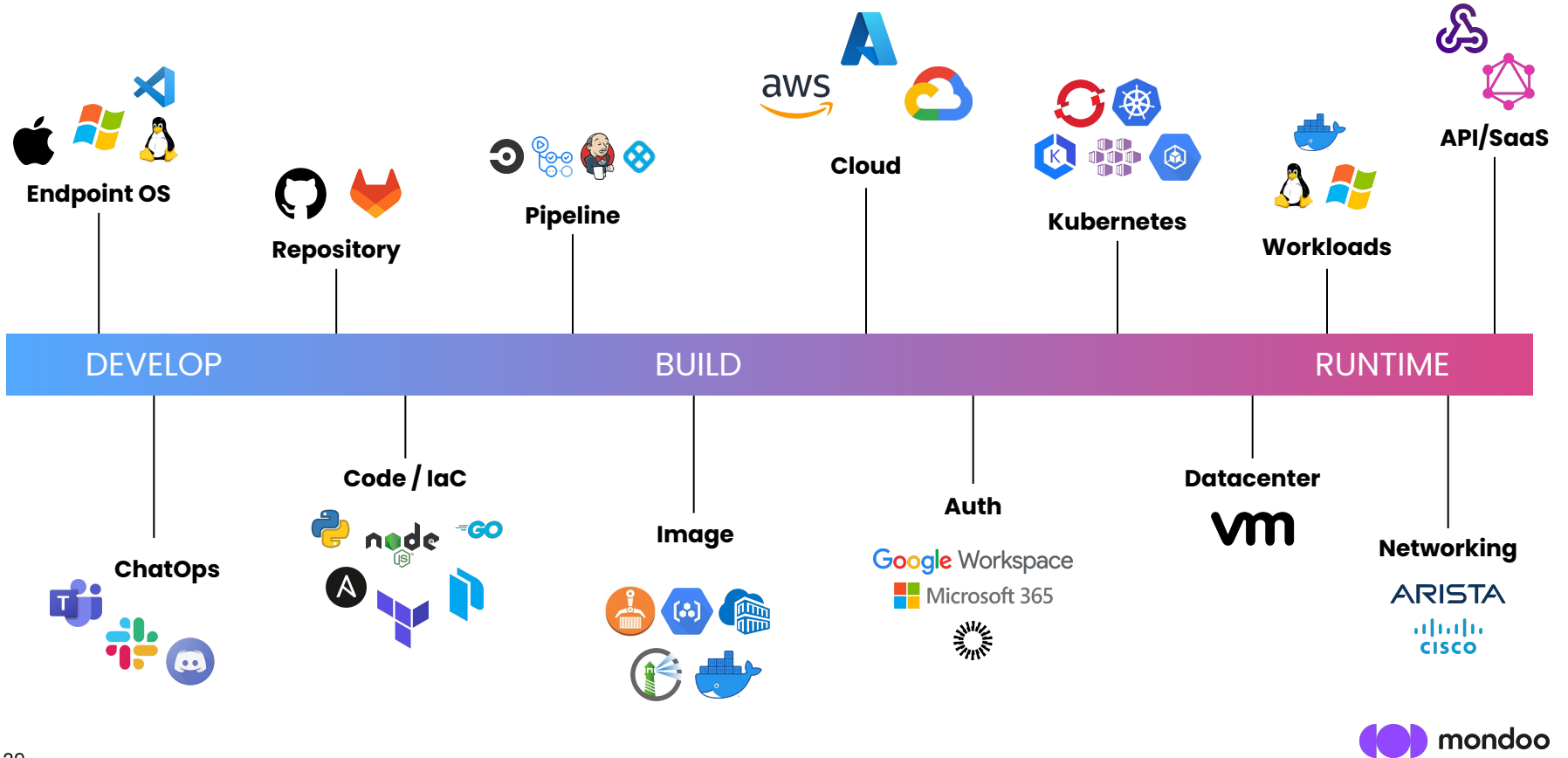
- CIS Apple macOS 12.0 Monterey Benchmark - Level 2**: official - by Mondoo, Inc. Version 2.0.0 Certified By - CIS. 82 Checks. UNLOCK
- CIS Microsoft Azure Foundations Benchmark Level 1**: official - by Mondoo, Inc. Version 1.0.0 Certified By - CIS. 50 Checks. UNLOCK
- Windows Security by Mondoo**: official - by Mondoo, Inc. Version 1.0.0. 85 Checks.
- CIS Microsoft Windows Server 2016 Benchmark - Level 1 - Domain Controller**: official - by Mondoo, Inc. Version 1.4.0 Certified By - CIS. 302 Checks. UNLOCK
- CIS Ubuntu Linux 22.04 LTS Benchmark - Level 2 - Server**: official - by Mondoo, Inc. Version 1.0.0 Certified By - CIS. 254 Checks. UNLOCK

Demo



@chri_hartmann

You can be more secure today!



Project Overview

	cnquery / cnspec
Project Health 2023	40+ releases
Runtime	Go, single-binary
Language	Extended GraphQL (MQL)
Pre-compiled Queries	yes, incl. AST
Code-Escalation	no, strict pre-compiled queries and policies
Data Gathering	asynchronous, parallel
Deduplication of queries	yes

Supported Targets

	cnquery / cnspec
Operating System	Local, SSH, SSH for Windows, WinRM, EC2 Instance Connect, EC2 SSM, Agentless Scanning
Cloud	AWS, Azure, GCP, VMware vsphere, OCI
Kubernetes & Container	AKS, EKS, GKE, OpenShift, Container Registries, Container Images
SaaS	Okta, Slack, Google Workspace, Microsoft 365, Github, Gitlab
IaC	Kubernetes Manifest, Terraform HCL, Terraform Plan, Terraform State

Anatomy of a Policy

```
vim examples/example.mql.yaml
# To run this file:
# cnspec scan -f examples/example.mql.yaml
#
# This section lists all the policies that are part of this bundle.
# In this example bundle there is only one policy: example1
policies:
- uid: example1
  name: Example policy 1
  version: "1.0.0"
  # If your policy has checks with impacts, specify the
  # "highest impact" scoring system. This system uses the lowest
  # score (the highest impact failure) as the overall report score.
  scoring_system: highest_impact
  authors:
  - name: Mondo
    email: helto@mondoo.com
  # Specs are a way to specify all the queries (and other policies)
  # to apply. Specs are grouped together and can be filtered.
  # This lets you apply a group of queries only if the condition is met.
  groups:
  - checks:
    # These are checks that will be scored and contribute to the
    # final score of this policy.
    - uid: sshd-01
      title: Ensure the port is set to 22
      mql: sshd.config.params["Port"] == 22
      # Impact is used for scoring. 100 = critical. 0 = informational.
      impact: 30
    - uid: sshd-02
      title: Prevent weaker CBC ciphers from being used
      mql: sshd.config.ciphers.none( /cbc/ )
      impact: 60
    # Here we use a referenced query. You can put multiple policies
    # in a bundle and share checks and queries between them.
    - uid: shared-query
  queries:
  # These are queries, which only collect data. They don't make
  # assertions or test against an ideal or expected result; they
  # only provide insights.
  - uid: sshd-01
    title: Gather SSH config params
    mql: sshd.config.params
  # Here is an example of a query that uses embedded properties.
  # These allow you to fine-tune the policy.
  - uid: home-info
    mql: file(props.home) { * }
    title: Gather info about the user's home
    props:
    - uid: home
      mql: |
        "/home"
  filters:
  # Here we specify that the queries in this spec only apply
  # when the asset satisfies this condition:
  - mql: asset.family.contains("unix")
# These are all the queries that are part of this bundle. They are used
# by the policies specified above.
queries:
# Every query can be identified by its UID.
# The title helps in printing.
- uid: shared-query
  title: Enable strict mode
  mql: sshd.config.params["StrictModes"] == "yes"
```

cnspec	InSpec
Policy	Profile
Group	Group (multiple files)
Check (metadata)	Control
MQL (sshd.config.params)	Describe

Anatomy of a Policy

```
vim linux.mql.yaml

Policies:
- uid: unix-temp
  name: Unix/Linux Temp Policy
  version: 1.0.0
  tags:
  another-key: another-value
  key: value
  authors:
  - name: Jane Doe
    email: jane@example.com
  groups:
  - filters: platform.family.contains(_ == 'unix')
    checks:
    - uid: tmp-10

queries:
- uid: tmp-10
  title: Create /tmp directory
  mql: file("/tmp").permissions.isDirectory
  docs:
  desc: An optional description
  audit: Create a new /tmp directory
  remediation: |
    Your instructions here
  ~
  ~
  ~
"linux.mql.yaml" 23L, 559B
```

```
chris-rock@Stargate:~/go/src/go.mondoo.com/workspace/cnspsec
→ cnspsec git:(chris-rock/record) x cnspsec scan local -f linux.mql.yaml
→ loaded configuration from /Users/chris-rock/.config/mondoo/mondoo.yml using source default
→ using service account credentials
→ discover related assets for 1 asset(s)
→ resolved assets resolved-assets=1

Stargate.fritz.box ██████████ 100% score: A

Asset: Stargate.fritz.box

Checks:
✓ Pass: Create /tmp directory

Scanned 1 assets

macOS
A Stargate.fritz.box

For detailed CLI output, run this scan with "-o full".

Do you want to view or share these scan results in a browser using Mondoo's reporting service? [Y/n] n
→ cnspsec git:(chris-rock/record) x █
```

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  
}
```

Easily ask questions with GraphQL-based MQL

S3 Buckets are configured with 'Block public access'

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

Use Policy as Code to define technical requirements

```
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  
    )
```

Use Policy as Code to define technical requirements

```
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
```

Use Compliance as Code to define higher-level compliance controls

```

policies:
- uid: ssh-policy
  name: SSH Policy
  groups:
  - filters: return true
    checks:
    - uid: sshd-ciphers-01
      title: Prevent weaker CBC ciphers from being used
      mql: sshd.config.ciphers.none( /cbc/ )
      impact: 60
    - uid: sshd-ciphers-02
      title: Do not allow ciphers with few bits
      mql: sshd.config.ciphers.none( /128/ )
      impact: 60
    - uid: sshd-config-permissions
      title: SSH config editing should be limited to admins
      mql: sshd.config.file.permissions.mode == 0644
      impact: 100

frameworks:
- uid: mondoo-ucf
  name: Unified Compliance Framework
  groups:
  - title: System hardening
    controls:
    - uid: mondoo-ucf-01
      title: Only use strong ciphers
      checks:
      - uid: sshd-ciphers-01
      - uid: sshd-ciphers-02
    - uid: mondoo-ucf-02
      title: Limit access to system configuration
      checks:
      - uid: sshd-config-permissions
    - uid: mondoo-ucf-03
      title: Harden systems to security recommendations
      policies:
      - uid: ssh-policy

```

Thank you



Christoph Hartmann



@chri_hartmann



chris@mondoo.com



mondoo.com



cnspec

**Secure everything from
development to production**

github.com/mondoohq/cnspec