Cloud Native Security

The Challenges and The Opportunities

Tim Miller, PhD – Technical Marketing Engineer
@broadcaststorm

BRKETI-2491

Mission Statement

Outshift by Cisco is the **incubation** engine delivering what's next and new for Cisco: **Emerging** technologies that target **adjacent** markets and **personas** to build **meaningful** businesses and achieve innovative results.

1. Power (**adoption**) metrics
2. **End-to-End**, solving for more than tech

Innovation, full speed ahead

At Outshift, we turn ideas into action, breaking new ground in **agentic AI**, **quantum**, **next-gen infrastructure**, and more.

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

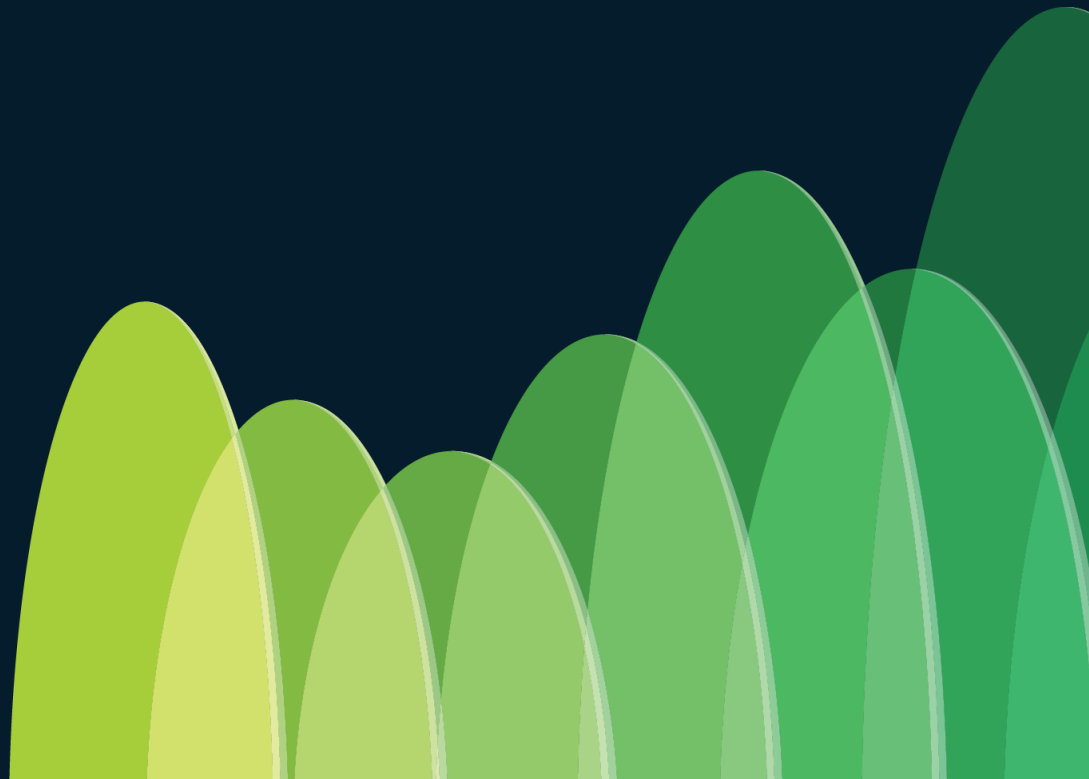
1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

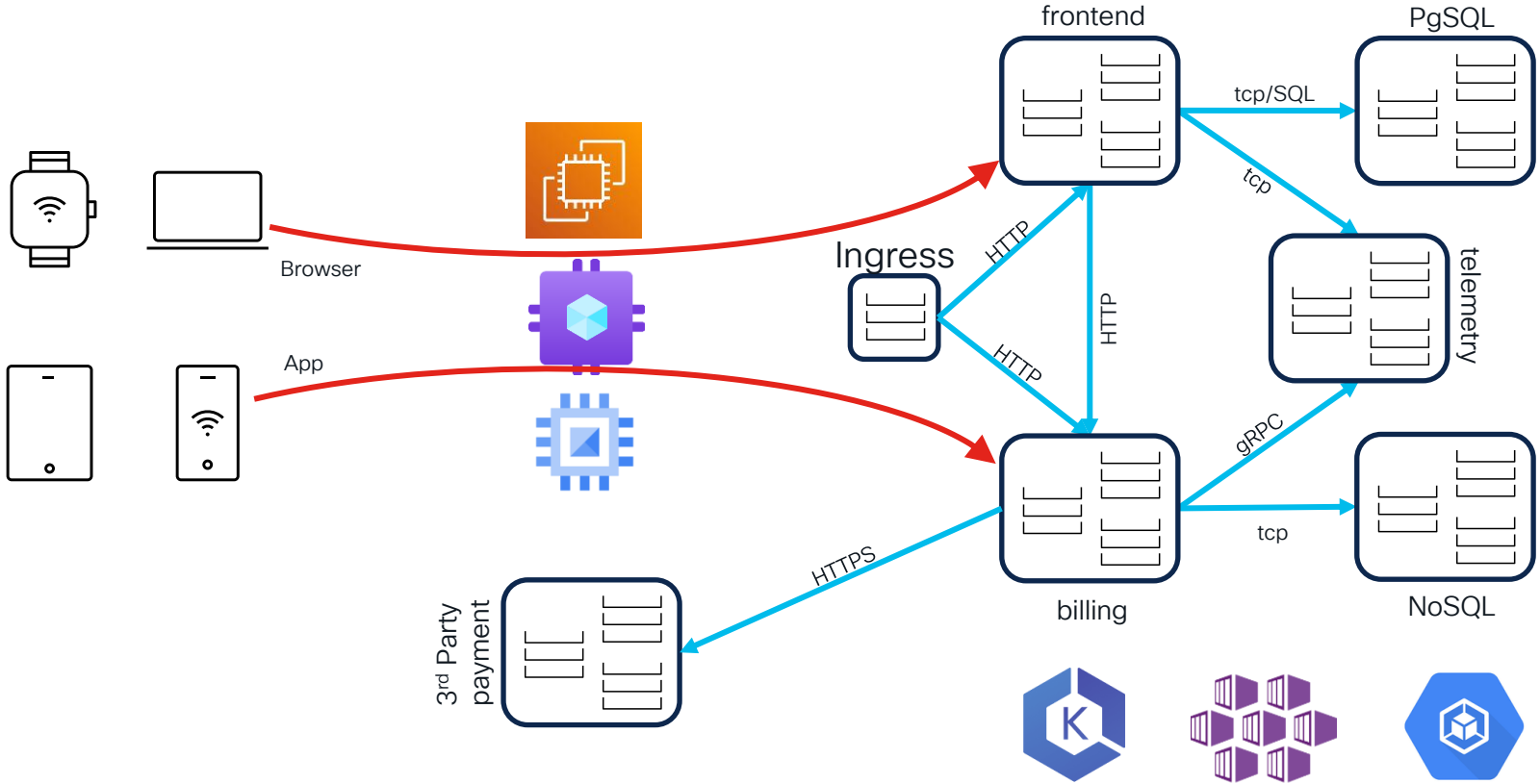
Agenda

- Introduction
- Cloud Native Apps
  - Industry Challenges
  - Context and Complexities
- Cloud Security Posture
- Code Security
- Realtime Security
- Conclusion

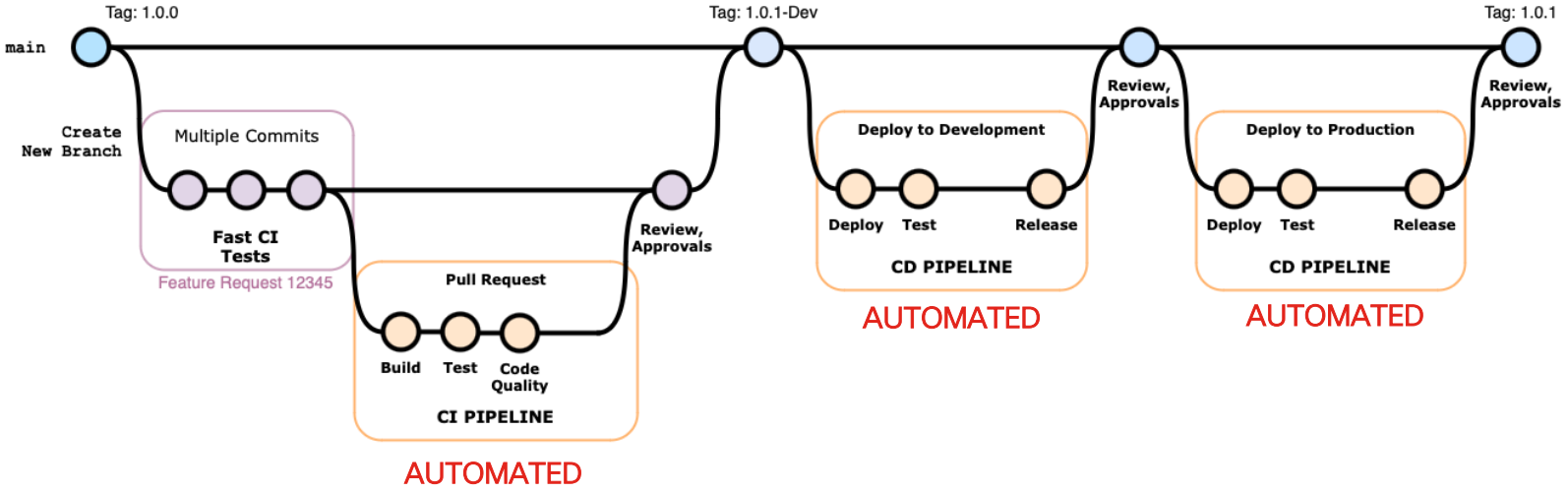
What defines a cloud native application?



A New Application Architecture



A New Application Development Process



A New Application Paradigm

Agility

Can pivot to new ideas

Velocity

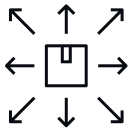
Bring features to market faster

Specificity

Can leverage new technologies as new problems emerge

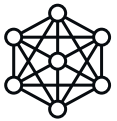
Visibility

Hard to track new things being released and cleaning up old things left behind



Scale

Larger attack surface as we publish more features and services

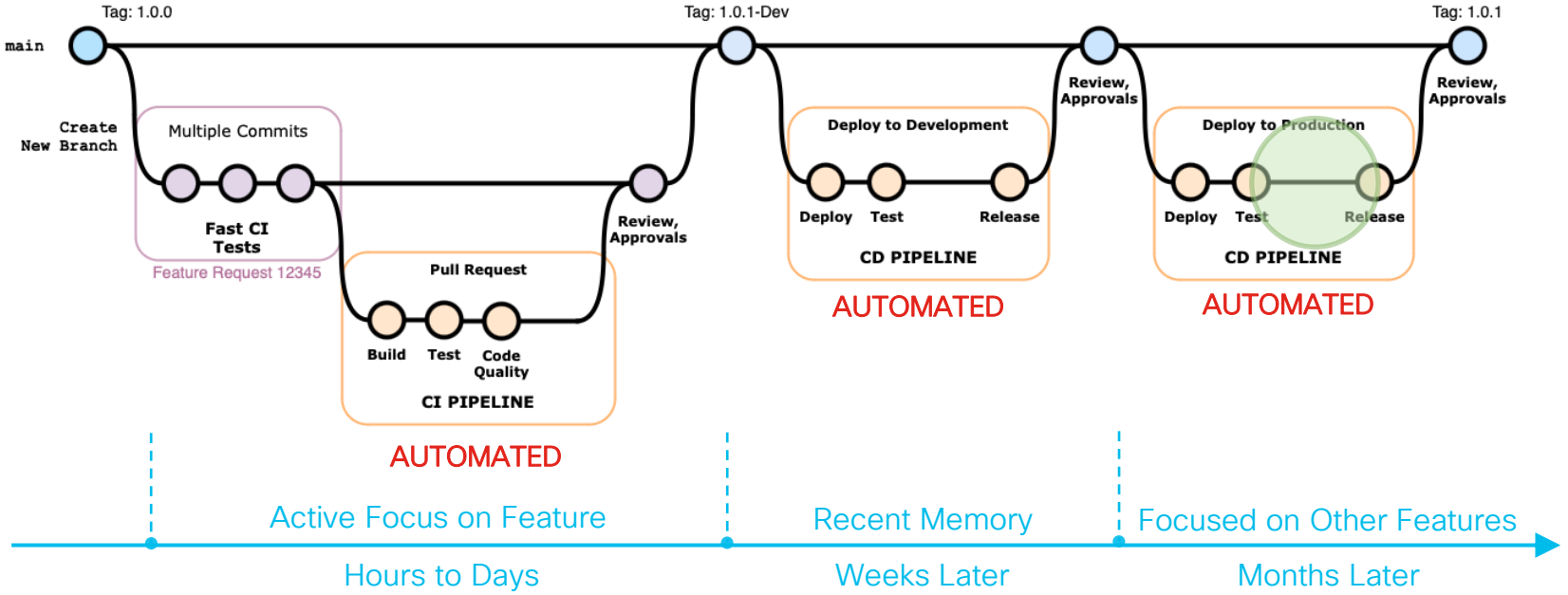


Complexity

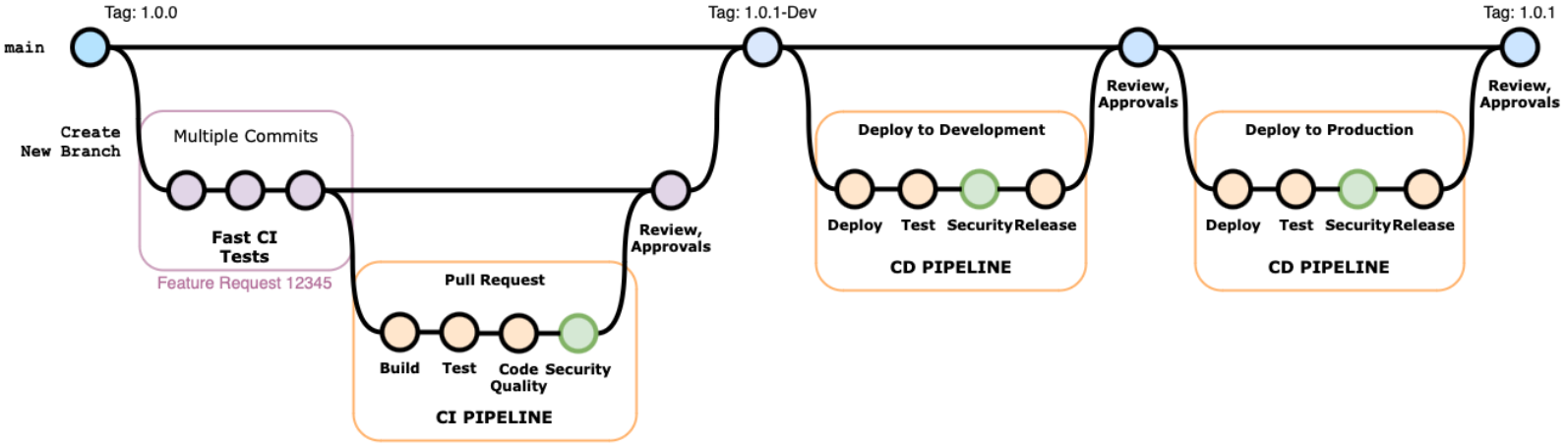
New attack vectors emerge based on new technology

A New Application Development Process

Challenging security to scale with its feature velocity



A New Application Security Approach



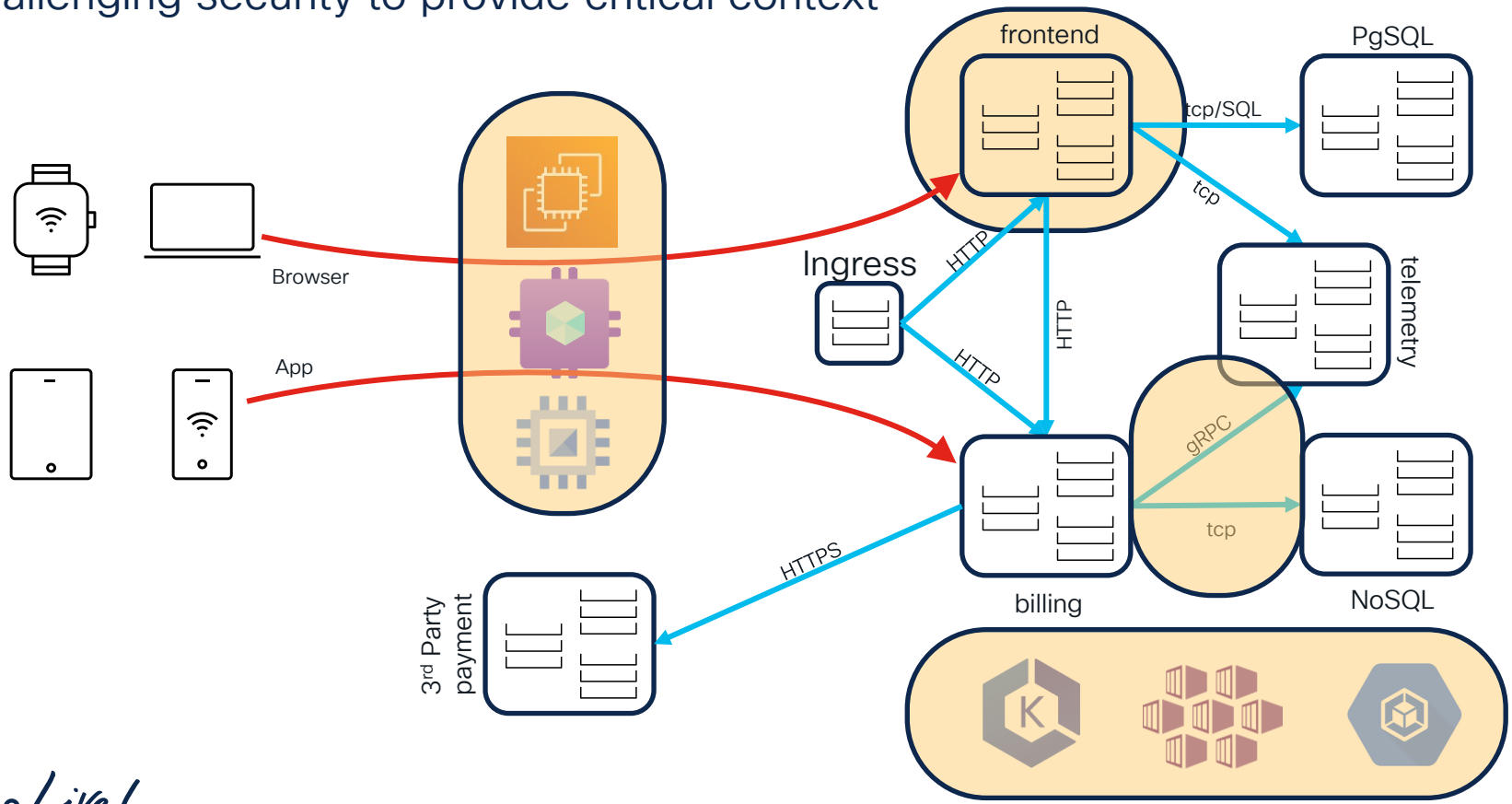
Apply Security Before *Any* Integration

Apply Security Before *Every* Deployment

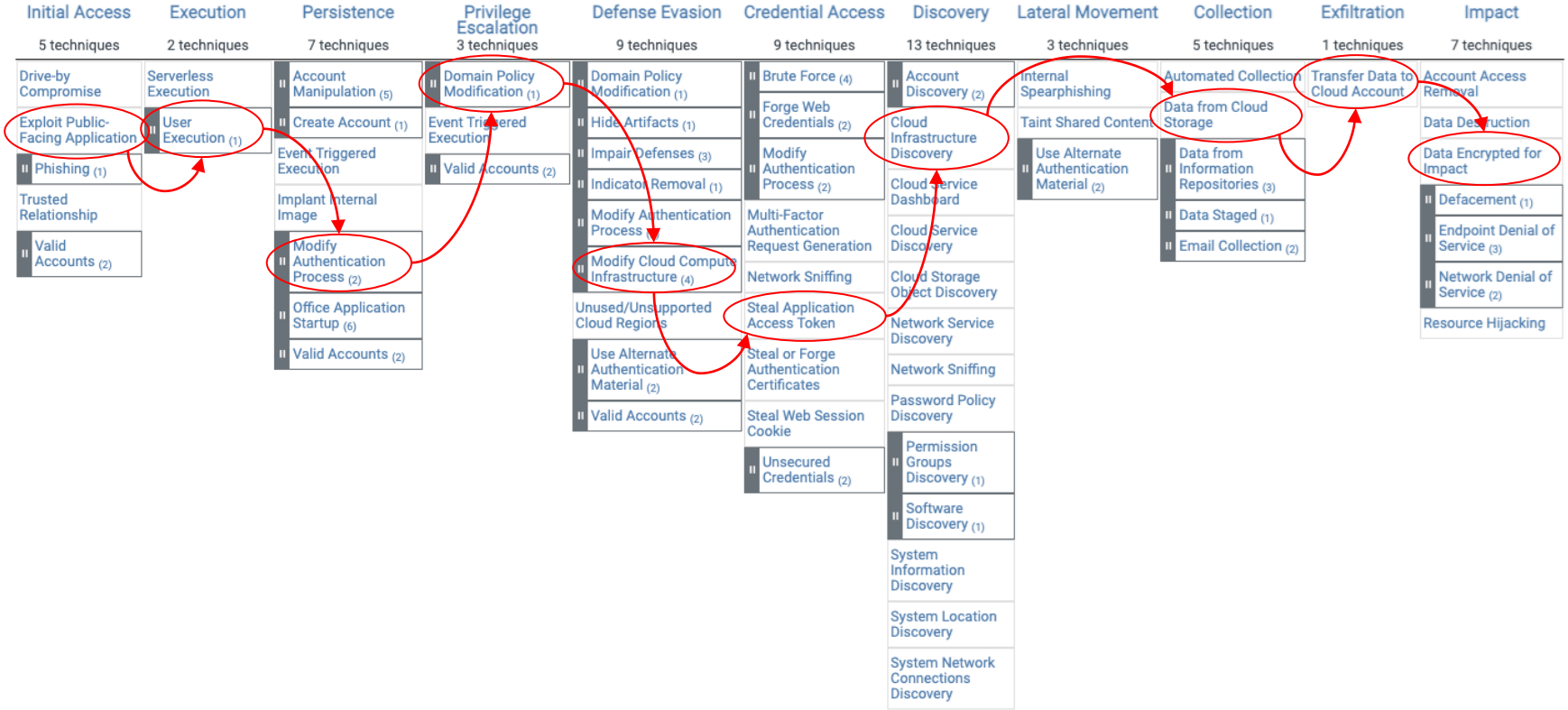
Shifting Security to the Left

A New Application Security Architecture

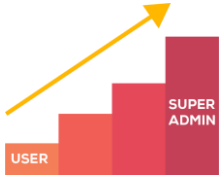
Challenging security to provide critical context



Threats Are Becoming More **Complex**



Complex threats built upon avoidable mistakes



80%

of security breaches involve privileged credentials

78%

of identified attack paths use known vulnerabilities (CVEs) as an initial access attack vector

36%

of organizations keep unencrypted secrets and personally identifiable information (PII) in these cloud services.

3

the average number of steps in an attack path to reach a crown jewel asset

99%

of cloud failures are due to cloud misconfigurations

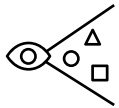
Source: Orca 2022 State of Public Cloud Security Report

Source: Forrester

Source: Gartner

Common theme in cloud native security

Security Posture Management



Visibility

Cloud environments are complex, multiple services, multiple regions, multiple accounts/subscriptions.

All too easy to have resources deployed that are forgotten or difficult to find.

Assessment

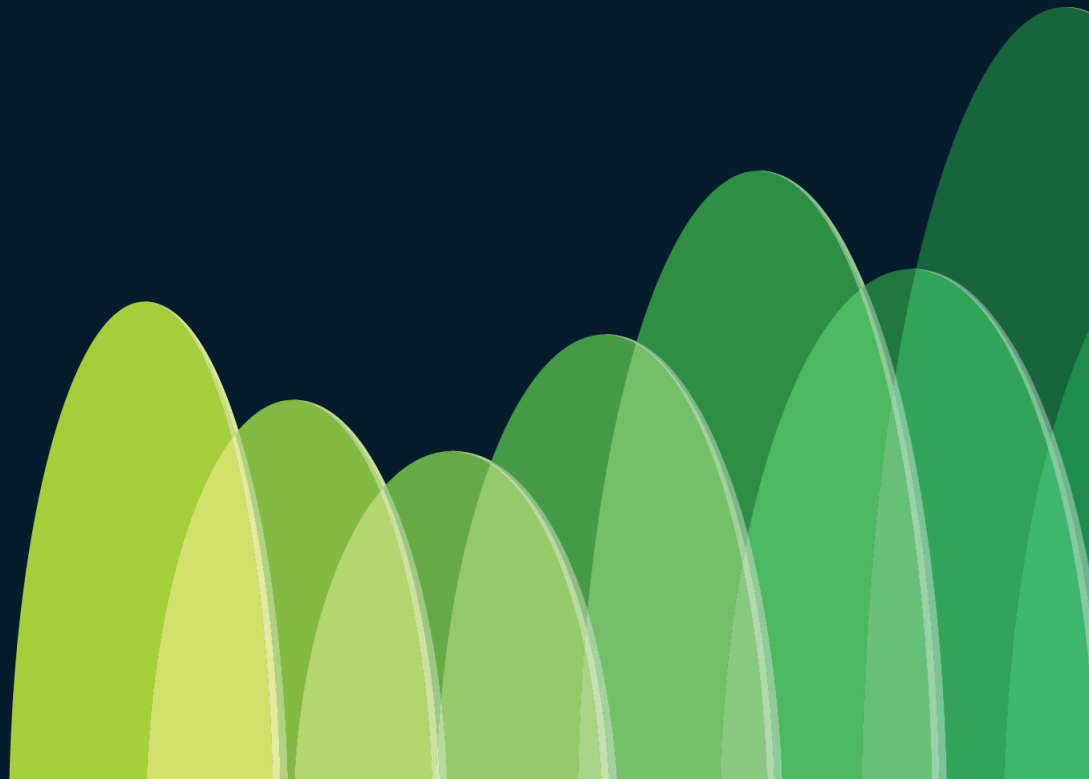
Industry best practices in cloud security are fairly well established and codified.

Many mature, open source tools exist from the industry as well as the standards bodies to provide robust scoring of risks.

Prioritization

Criticality of those risks is important. While there are known issues with scoring, industry standards help establish a baseline from which to improve.

Cloud Security Posture Management



cisco Live!

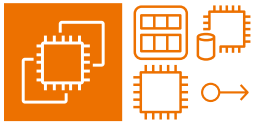
Anatomy of a Cloud Account

Serverless

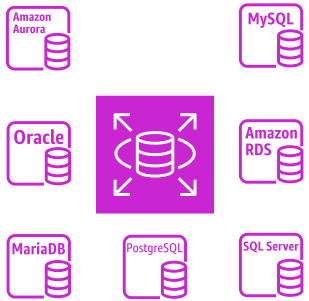
Public Exposure
Leaked credentials
Vulnerabilities
Malware

Networking

K8s Service, Registries



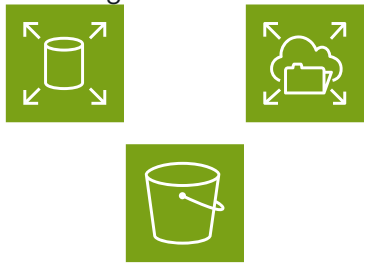
Compute Instances

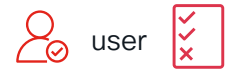


Databases

Public Exposure
Data Encryption
Sensitive Data
Exfiltration

Storage and Fileshares



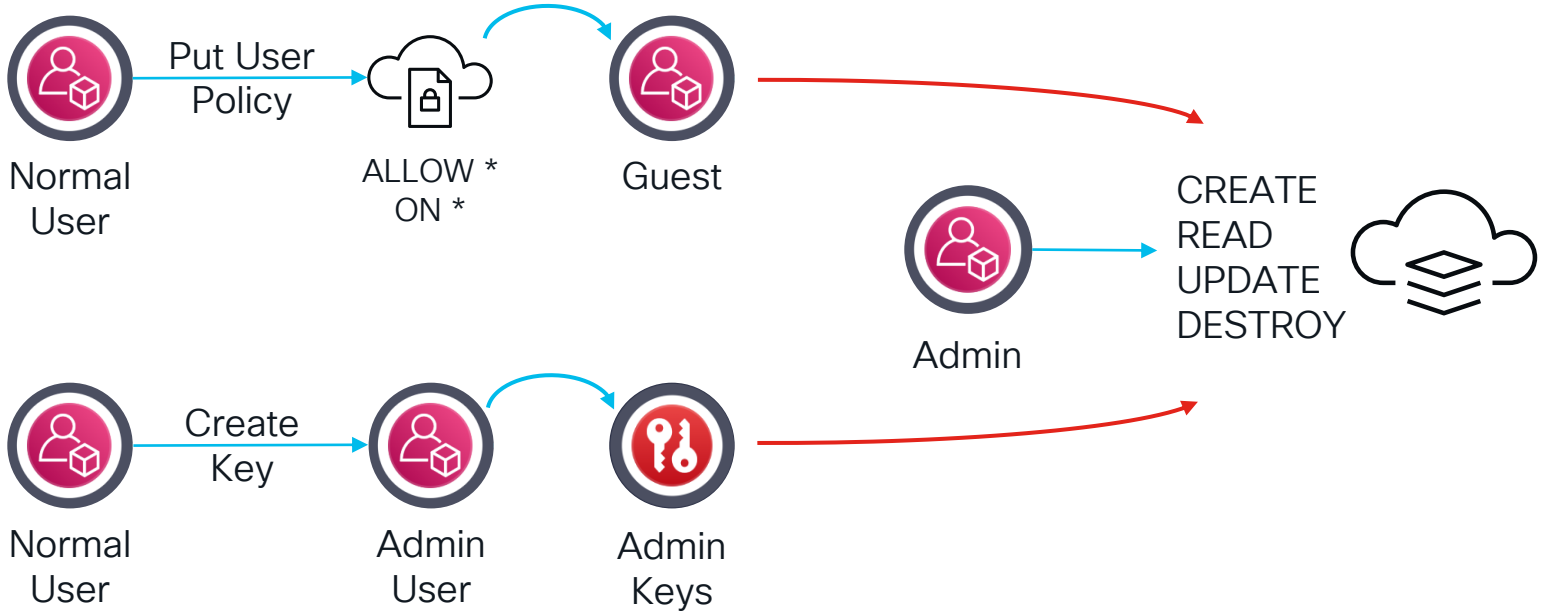


Insufficient Access Control
Excessive Privileges
Stale Secrets
Privilege Escalation

Organization and Accounts

Privilege Escalation

Examples of Normal Users Escalating to Administrator Privileges



Building a Cloud Account: VPC and Security Grps

```
module "vpc" {
  source  = "terraform-aws-modules/vpc/aws"
  version = "5.8.1" # Use the version suitable for your use
case.

  name = var.cmcd_demo_prefix
  cidr = var.cmcd_workload_cidr

  azs             = keys(local.vpc_public_subnets)
  public_subnets  = values(local.vpc_public_subnets)
  private_subnets = values(local.vpc_private_subnets)

  enable_nat_gateway     = true
  single_nat_gateway     = true
  one_nat_gateway_per_az = false

  tags = {
    Terraform = "true"
    Scenario  = "Cisco Multicloud Defense"
  }
}
```

```
resource "aws_security_group" "demo_ec2_security_group" {
  name   = "${var.module_prefix}_jenkins_sg"
  vpc_id = var.vpc_id

  egress {
    from_port   = 0
    to_port     = 0
    protocol    = -1
    cidr_blocks = ["0.0.0.0/0"]
  }

  ingress {
    from_port   = 22
    to_port     = 22
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }

  tags = {
    Terraform = "true"
    Scenario  = "Cisco Multicloud Defense"
  }
}
```

Building a Cloud Account – S3 Buckets

```
# Cloud name attribute, rule-based classification example
resource "aws_s3_bucket" "pci-bucket" {
  bucket = "${var.s3-prefix}-pci-bucket"

  tags = {
    name            = "${var.s3-prefix}-pci-bucket"
    Terraform       = "true"
    Scenario        = "Metadata Classification"
    data_class_type = "class-none"
  }
}

# Make it public
resource "aws_s3_bucket_public_access_block" "pci-bucket" {
  bucket = aws_s3_bucket.pci-bucket.id

  block_public_acls       = false
  block_public_policy     = false
  ignore_public_acls      = false
  restrict_public_buckets = false
}
```

These safety controls are relatively recent additions to AWS storage buckets.

Deliberate configuration required to expose S3 buckets now.

```
resource "aws_s3_bucket_acl" "pci-bucket" {
  depends_on = [
    aws_s3_bucket_ownership_controls.pci-bucket,
    aws_s3_bucket_public_access_block.pci-bucket,
  ]

  bucket = aws_s3_bucket.pci-bucket.id
  acl    = "public-read"
}

resource "aws_s3_bucket_policy" "pci-bucket" {
  bucket = aws_s3_bucket.pci-bucket.id
  depends_on = [
    aws_s3_bucket_public_access_block.pci-bucket
  ]

  policy = jsonencode({
    Version = "2012-10-17",
    Statement = [
      {
        Sid       = "PublicReadGetObject",
        Effect    = "Allow",
        Principal = "*",
        Action    = ["s3:GetObject"],
        Resource  = ["${aws_s3_bucket.pci-bucket.arn}/*"]
      },
    ],
  })
}
```

KICS – Keeping Infrastructure as Code Secure

Infrastructure Deployment Assessments

```
S3 Bucket Access to Any Principal, Severity: CRITICAL, Results: 1
Description: S3 Buckets must not allow Actions From All Principals, as to prevent leaking private information to the entire internet or a
llow unauthorized data tampering / deletion. This means the 'Effect' must not be 'Allow' when there are All Principals
Platform: Terraform
CWE: 284
Learn more about this vulnerability: https://docs.kics.io/latest/queries/terraform-queries/aws/7af43613-6bb9-4a0e-8c4d-1314b799425e

        [1]: cloud-infrastructure/data-classification/05-s3-metadata-name-classification.tf:54

                053:
                054:    policy = jsonencode({
                055:      Version = "2012-10-17",


S3 Bucket ACL Allows Read Or Write to All Users, Severity: CRITICAL, Results: 2
Description: S3 Buckets should not be readable and writable to all users
Platform: Terraform
CWE: 732
Learn more about this vulnerability: https://docs.kics.io/latest/queries/terraform-queries/aws/38c5ee0d-7f22-4260-ab72-5073048df100

        [1]: cloud-infrastructure/data-classification/06-s3-manual-classification.tf:39

                038:    bucket = aws_s3_bucket.manual-tagged.id
                039:    acl    = "public-read"
                040: }


        [2]: cloud-infrastructure/data-classification/05-s3-metadata-name-classification.tf:37

                036:    bucket = aws_s3_bucket.pci-bucket.id
                037:    acl    = "public-read"
                038: }
```

```
Results Summary:
CRITICAL: 3
HIGH: 120
MEDIUM: 24
LOW: 13
INFO: 50
TOTAL: 210
```

```
$ kics scan --report-formats json \
    --output-path . --output-name kics-cloud.json \
    --queries-path /opt/homebrew/Cellar/kics/2.1.5/share/kics/assets/queries \
    --path cloud-infrastructure
```

KICS - Keeping Infrastructure as Code Secure

Infrastructure Deployment Assessments


```
"queries": [
    {
        "query_name": "S3 Bucket ACL Allows Read Or Write to All Users",
        "query_id": "38c5ee0d-7f22-4260-ab72-5073048df100",
        "query_url": "https://registry.terraform.io/providers/hashicorp/aws/latest/docs/resources/s3_bucket",
        "severity": "CRITICAL",
        "platform": "Terraform",
        "cwe": "732",
        "cloud_provider": "AWS",
        "category": "Access Control",
        "experimental": false,
        "description": "S3 Buckets should not be readable and writable to all users",
        "description_id": "d535387f",
        "files": [
            {
                "file_name": "cloud-infrastructure/data-classification/06-s3-manual-classification.tf",
                "similarity_id": "75144f9bede91aa775cca35b65debe7251457a33e4d9f18dcc81018fff5079b3",
                "line": 39,
                "resource_type": "aws_s3_bucket_acl",
                "resource_name": "manual-tagged",
                "issue_type": "IncorrectValue",
                "search_key": "aws_s3_bucket_acl[manual-tagged].acl",
                "search_line": 39,
                "search_value": "",
                "expected_value": "aws_s3_bucket_acl[manual-tagged].acl should be private",
                "actual_value": "aws_s3_bucket_acl[public-read].acl is %!s(MISSING)"
            },
```

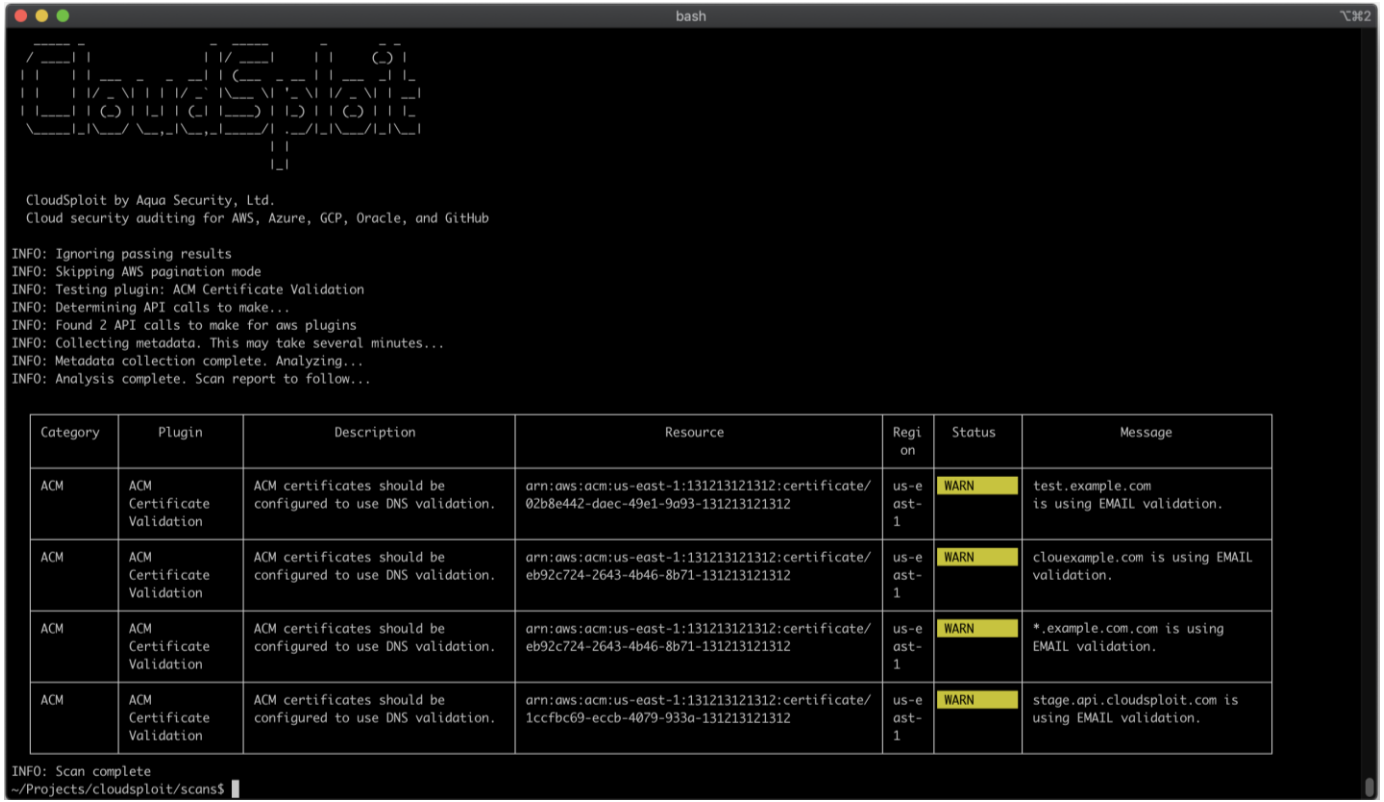
Shift Left IaC Scanning (GitHub Actions)

```yaml
name: kics
on:
  push:
    branches: [ "main" ]
  pull_request:
    branches: [ "main" ]
permissions:
  contents: read
jobs:
  build:
    permissions:
      contents: read
    name: Build
    runs-on: ubuntu-latest
    steps:
    - uses: actions/checkout@v3
      name: Checkout the repository
    - name: Run KICS Scan
      uses: checkmarx/kics-github-action@v2.1.5
      with:
        path: './'
        fail_on: critical
        output_path: ./
    - name: display kics results
      run: |
        cat ./results.json
```

```
"kics_version": "v2.1.5",
"files_scanned": 110,
"lines_scanned": 21799,
. . . .
"severity_counters": {
  "CRITICAL": 0,
  "HIGH": 7,
  "INFO": 9,
  "LOW": 292,
  "MEDIUM": 351,
  "TRACE": 0
},
. . . .
"queries": [
  {
    "query_name": "Missing User Instruction",
    "description": "A user should be specified in the
dockerfile, otherwise the image will run as root",
    . . . .
    "files": [
      {
        "file_name": "src/currencyservice/Dockerfile",
      },
      {
        "file_name": "src/loadgenerator/Dockerfile",
      },
      . . . .
  }
]
```

CloudSploit

Cloud Security Scans – OSS by Aqua Security



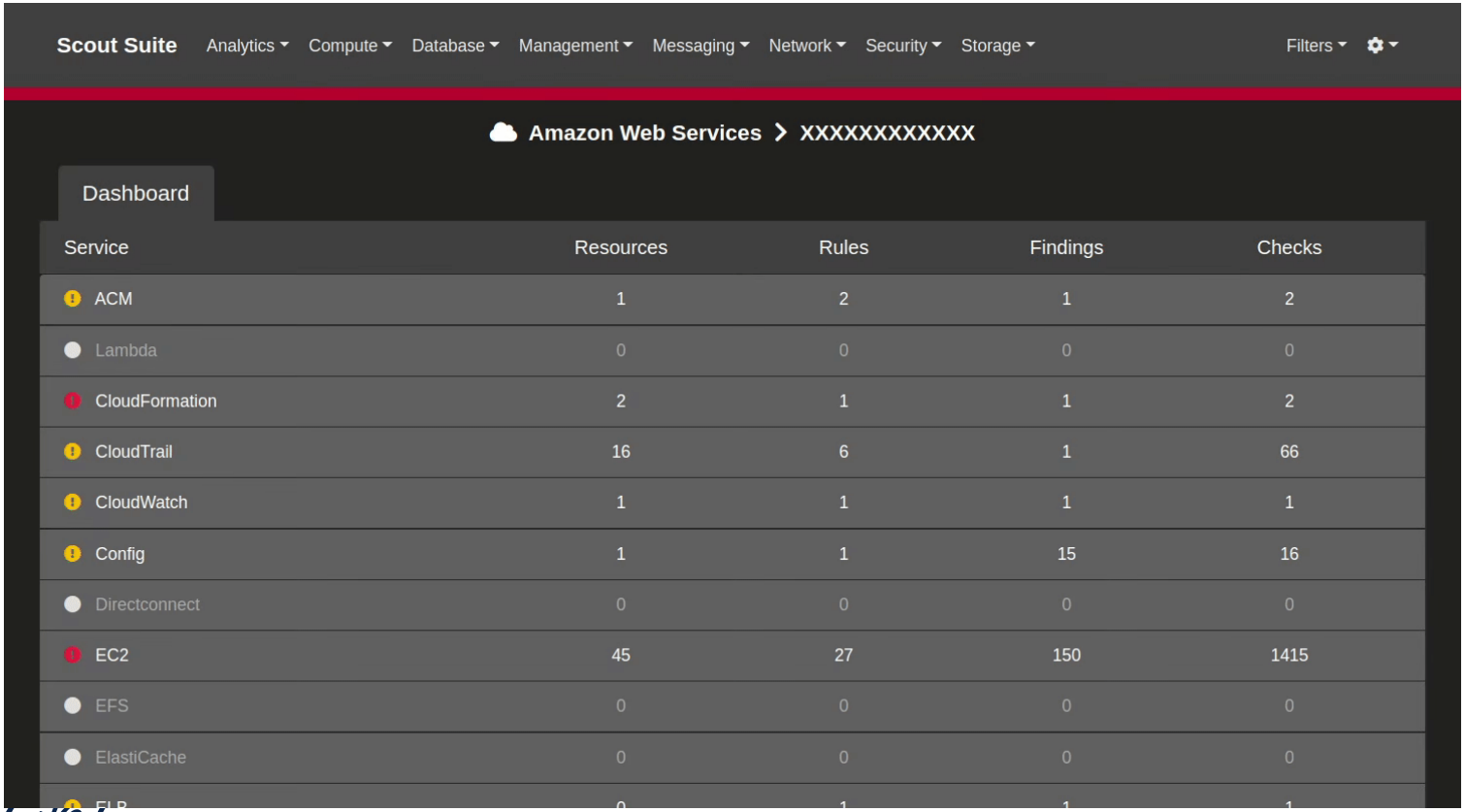
Category	Plugin	Description	Resource	Region	Status	Message
ACM	ACM Certificate Validation	ACM certificates should be configured to use DNS validation.	arn:aws:acm:us-east-1:131213121312:certificate/02b8e442-daec-49e1-9a93-131213121312	us-east-1	WARN	test.example.com is using EMAIL validation.
ACM	ACM Certificate Validation	ACM certificates should be configured to use DNS validation.	arn:aws:acm:us-east-1:131213121312:certificate/eb92c724-2643-4b46-8b71-131213121312	us-east-1	WARN	clouexample.com is using EMAIL validation.
ACM	ACM Certificate Validation	ACM certificates should be configured to use DNS validation.	arn:aws:acm:us-east-1:131213121312:certificate/eb92c724-2643-4b46-8b71-131213121312	us-east-1	WARN	*.example.com.com is using EMAIL validation.
ACM	ACM Certificate Validation	ACM certificates should be configured to use DNS validation.	arn:aws:acm:us-east-1:131213121312:certificate/1ccfbc69-eccb-4079-933a-131213121312	us-east-1	WARN	stage.api.cloudsploit.com is using EMAIL validation.

https://github.com/nccgroup/ScoutSuite

Manual

ScoutSuite

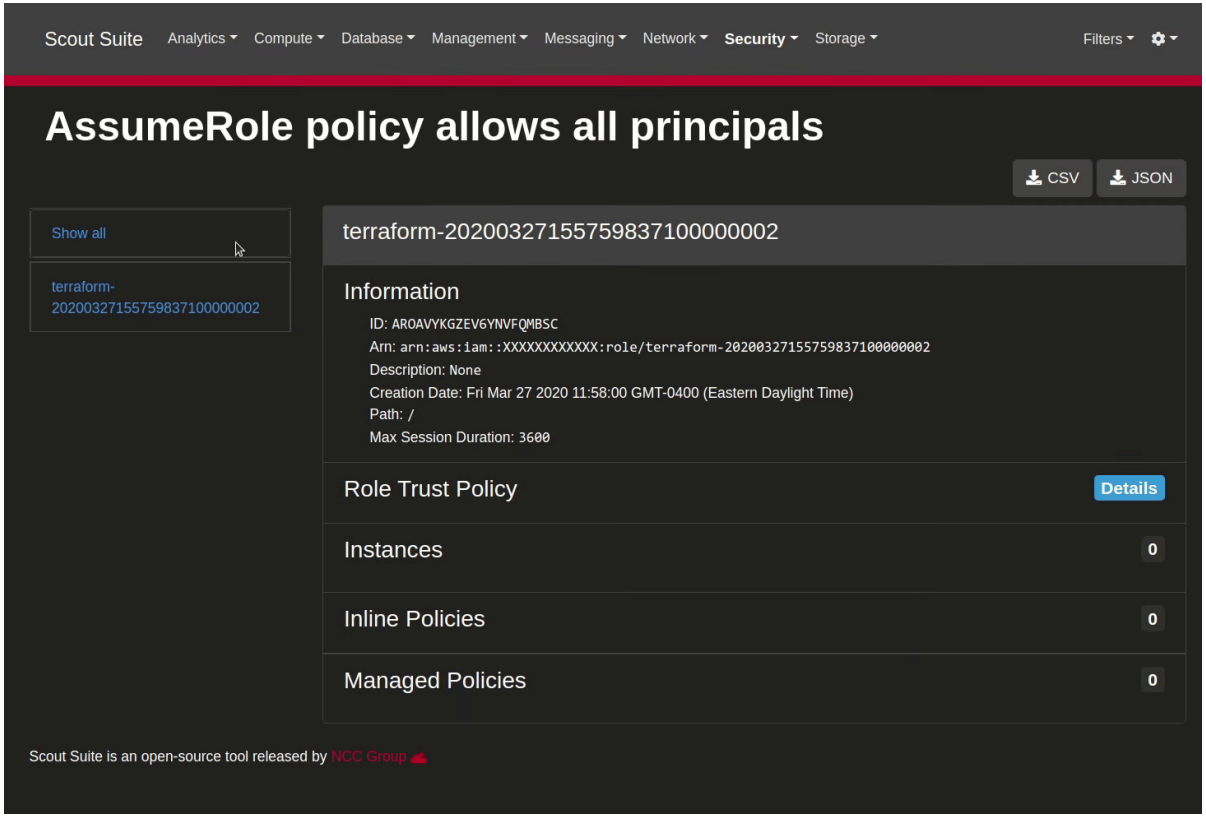
Multicloud Security Posture Assessment – NCCgroup



https://github.com/nccgroup/ScoutSuite Manual

ScoutSuite

Multicloud Security Posture Assessment – NCCgroup



Cloud Security Posture Management

Identify common cloud misconfigurations, excessive permissions, and other security risks that open your cloud to platform and infrastructure attacks.

Shift Left CSPM – KICS

- IaC scanning
- OpenAPI specification

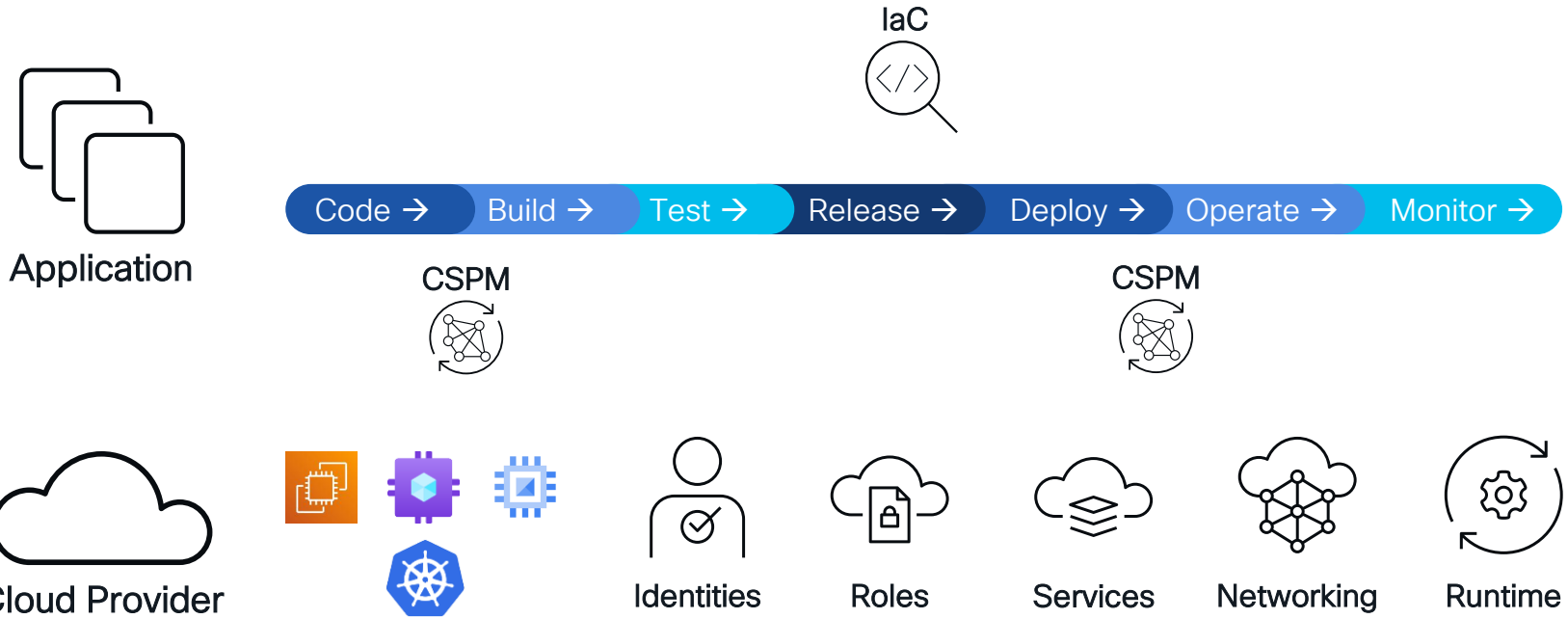
Shift Left CSPM – gitleaks

- Secret Leakage

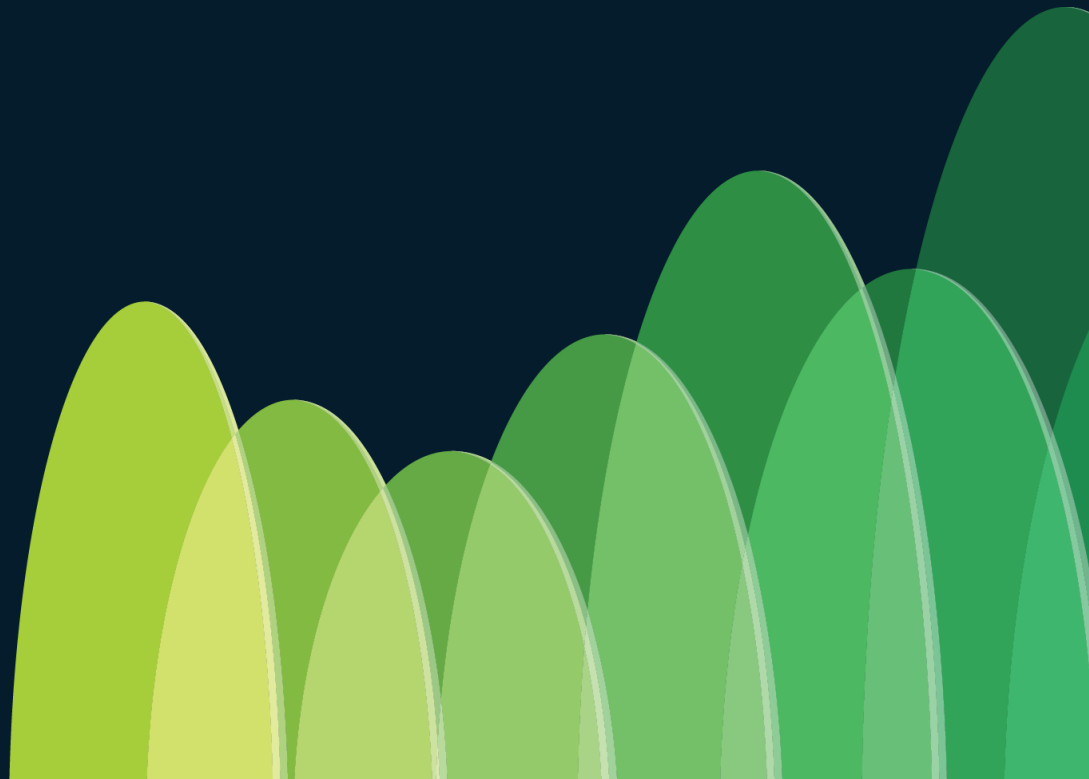
Runtime CSPM – CloudSploit, ScoutSuite

- Cloud IAM Analysis
- Cloud PaaS Posture
- Cloud IaaS Posture

Cloud Native Application Stack

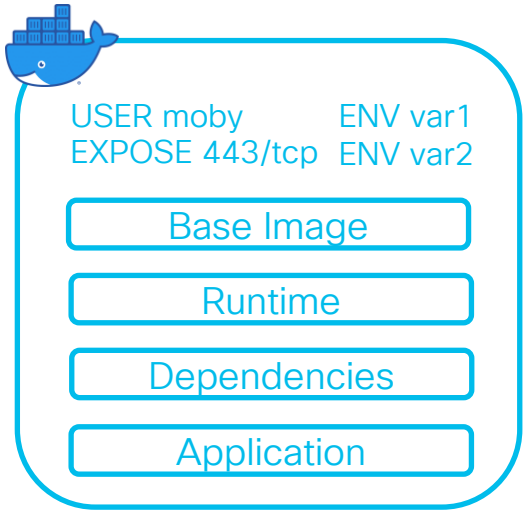


Code and Build Security



cisco Live!

Anatomy of a Container

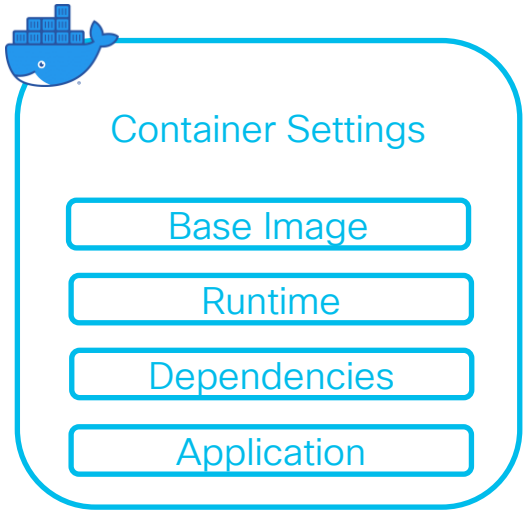


Dockerfile

```
# BASE LAYER
FROM rockylinux:9.1.20221123 AS base

# RUNTIME LAYER
RUN dnf install -y python3 python3-pip python3-setuptools && \
    dnf clean all

# DEPENDENCIES
RUN pip install wheel && pip install "fastapi[all]" "uvicorn[standard]"

# APPLICATION
WORKDIR /app
COPY ./src /app

RUN useradd -u 5678 appuser && chown -R appuser /app

# SETTINGS
USER appuser
EXPOSE 8080

ENV STORAGE_SVC storage-service
ENV STORAGE_PORT 8080
ENV ACCESS_KEY never_do_this_in_prod
ENV SECRET_KEY cross_the_streams_bad

CMD ["uvicorn", "--host", "0.0.0.0", "--port", "8080", "example:api"]
```

Software Bill of Materials

```
8   # DEPENDENCIES
9   RUN pip install wheel && pip install "fastapi[all]" "uvicorn[standard]"
```



identified.layer.dependencies.txt

1	Jinja2	3.1.2	python
2	MarkupSafe	2.1.1	python
3	PyYAML	6.0	python
4	anyio	3.6.2	python
5	certifi	2022.12.7	python
6	click	8.1.3	python
7	dnspython	2.2.1	python
8	email-validator	1.3.0	python
9	fastapi	0.88.0	python
10	h11	0.14.0	python
11	httpcore	0.16.3	python
12	httptools	0.5.0	python
13	httpx	0.23.3	python
14	idna	3.4	python
15	itsdangerous	2.1.2	python
16	orjson	3.8.4	python
17	pydantic	1.10.4	python
18	python-dotenv	0.21.0	python
19	python-multipart	0.0.5	python
20	rfc3986	1.5.0	python
21	six	1.16.0	python
22	sniffio	1.3.0	python
23	starlette	0.22.0	python
24	typing_extensions	4.4.0	python
25	ujson	5.6.0	python
26	uvicorn	0.20.0	python
27	uvloop	0.17.0	python
28	watchfiles	0.18.1	python
29	websockets	10.4	python
30	wheel	0.38.4	python

https://trivy.dev/latest/ Manual

Trivy

CVE Scanning of Software and Containers

```
$ trivy filesystem online-boutique --detection-priority precise --severity CRITICAL --ignore-unfixed > trivy.txt
2025-02-12T10:14:48+01:00       INFO    [vuln] Vulnerability scanning is enabled
2025-02-12T10:14:48+01:00       INFO    [secret] Secret scanning is enabled
2025-02-12T10:14:48+01:00       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable
secret scanning
2025-02-12T10:14:48+01:00       INFO    [secret] Please see also
https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendation for faster secret detection
2025-02-12T10:14:48+01:00       INFO    [npm] To collect the license information of packages, "npm install" needs to
be performed beforehand    dir="src/currencyservice/node_modules"
2025-02-12T10:14:48+01:00       INFO    [npm] To collect the license information of packages, "npm install" needs to
be performed beforehand    dir="src/paymentservice/node_modules"
2025-02-12T10:14:48+01:00       INFO    [python] Licenses acquired from one or more METADATA files may be subject to
additional terms. Use `--debug` flag to see all affected packages.
2025-02-12T10:14:48+01:00       INFO    Number of language-specific files       num=10
2025-02-12T10:14:48+01:00       INFO    [gomod] Detecting vulnerabilities...
2025-02-12T10:14:48+01:00       INFO    [npm] Detecting vulnerabilities...
2025-02-12T10:14:48+01:00       INFO    [pip] Detecting vulnerabilities...
```

```
src/checkoutservice/go.mod (gomod)
==================================
Total: 1 (CRITICAL: 1)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
golang.org/x/crypto	CVE-2024-45337	CRITICAL	fixed	v0.27.0	0.31.0	golang.org/x/crypto/ssh: Misuse of ServerConfig.PublicKeyCallback may cause authorization bypass in golang.org/x/crypto https://avd.aquasec.com/nvd/cve-2024-45337

Trivy

CVE Scanning of Software and Containers

```
$ trivy image nginx
2024-12-09T19:10:32.590Z        INFO    Detected OS: debian
2024-12-09T19:10:32.591Z        INFO    Detecting Debian vulnerabilities...
2024-12-09T19:10:32.620Z        INFO    Number of language-specific files: 0

nginx (debian 12.8)
===================
Total: 88 (UNKNOWN: 8, LOW: 72, MEDIUM: 6, HIGH: 2, CRITICAL: 0)
…

$ trivy image nginx | grep HIGH
Total: 88 (UNKNOWN: 8, LOW: 72, MEDIUM: 6, HIGH: 2, CRITICAL: 0)
| libssl3          | CVE-2023-0286    | HIGH     | 3.0.15-1~deb12u1      |     | X.400 address type confusion
| openssl          | CVE-2023-0286    | HIGH     | 3.0.15-1~deb12u1      |     | X.400 address type confusion
$

$ trivy image nginx | grep CVE-2023-0217
|                  | CVE-2023-0217    |          |                       |     | -->avd.aquasec.com/nvd/cve-2023-0217
…
$
```

Shift Left CVE Evaluation (GitHub Actions)

```yaml
name: trivy
on:
  push:
    branches: [ "main" ]
  pull_request:
    branches: [ "main" ]
permissions:
  contents: read
jobs:
  build:
    name: Build
    runs-on: ubuntu-latest
    steps:
      - name: Checkout code
        uses: actions/checkout@v4
      - name: Install trivy scanner
        run: |
          # (omitted repo setup)
          sudo apt-get update
          sudo apt-get install trivy
      - name: Run Trivy vulnerability scanner
        run: |
          trivy filesystem ./ --detection-priority precise --severity CRITICAL \
                --ignore-unfixed --format sarif --output trivy-results.sarif
```

```
"ruleId": "CVE-2024-45337",
"level": "error",
"message": {
  "text": "Package: golang.org/x/crypto\nInstalled Version:
v0.27.0\nVulnerability CVE-2024-45337\nSeverity: CRITICAL\nFixed Version:
0.31.0\nLink: [CVE-2024-45337](https://avd.aquasec.com/nvd/cve-2024-45337)"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "src/checkoutservice/go.mod",
      }
    },
    "message": {
      "text": "src/checkoutservice/go.mod: golang.org/x/crypto@v0.27.0"
    }
```

semgrep

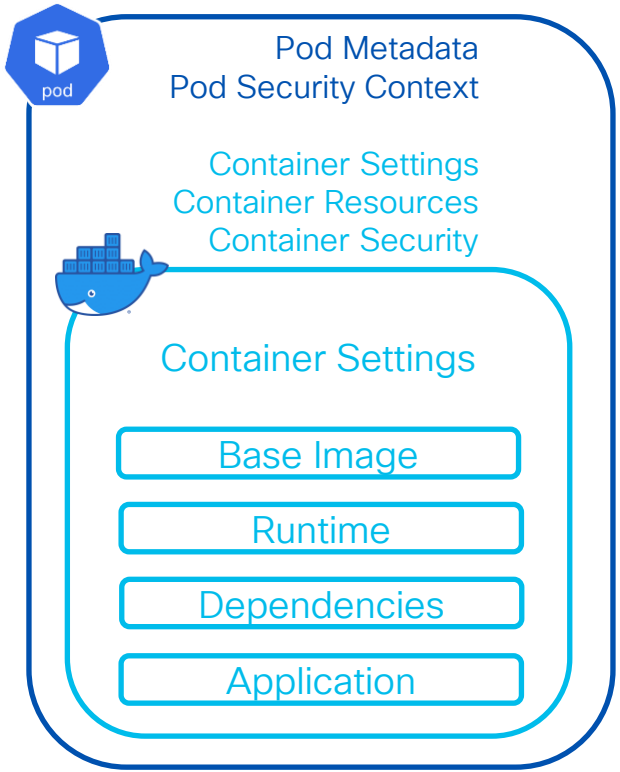
Static Application Security Testing

```
online-boutique/src/frontend/handlers.go
❯❯ go.lang.security.audit.crypto.math_random.math-random-used
      Do not use `math/rand`. Use `crypto/rand` instead.
      Details: https://sg.run/6nK6

       ▶▶┆ Autofix ▶ crypto/rand
       23┆ "math/rand"

❯❯ go.lang.security.audit.xss.no-direct-write-to-responsewriter.no-direct-write-to-responsewriter
      Detected directly writing or similar in 'http.ResponseWriter.write()'. This bypasses HTML escaping
      that prevents cross-site scripting vulnerabilities. Instead, use the 'html/template' package and
      render data using 'template.Execute()'.
      Details: https://sg.run/EkbA

      447┆ w.Write(jsonData)

❯❯ go.lang.security.audit.net.cookie-missing-httponly.cookie-missing-httponly
      A session cookie was detected without setting the 'HttpOnly' flag. The 'HttpOnly' flag for cookies
      instructs the browser to forbid client-side scripts from reading the cookie which mitigates XSS
      attacks. Set the 'HttpOnly' flag by setting 'HttpOnly' to 'true' in the Cookie.
      Details: https://sg.run/b73e

       ▶▶┆ Autofix ▶ http.Cookie{ Name:   cookieCurrency, Value:  payload.Currency, MaxAge: cookieMaxAge,
      511┆ http.SetCookie(w, &http.Cookie{
      513┆   Value:  payload.Currency,
      514┆   MaxAge: cookieMaxAge,
      515┆ })

❯❯ go.lang.security.audit.net.cookie-missing-secure.cookie-missing-secure
      A session cookie was detected without setting the 'Secure' flag. The 'secure' flag for cookies
      prevents the client from transmitting the cookie over insecure channels such as HTTP. Set the
      'Secure' flag by setting 'Secure' to 'true' in the Options struct.
      Details: https://sg.run/N4G7

       ▶▶┆ Autofix ▶ http.Cookie{ Name:   cookieCurrency, Value:  payload.Currency, MaxAge: cookieMaxAge,
      511┆ http.SetCookie(w, &http.Cookie{
      512┆   Name:   cookieCurrency,
      513┆   Value:  payload.Currency,
      514┆   MaxAge: cookieMaxAge,
      515┆ })
```


```
{
  "check_id": "go.lang.security.audit.crypto.math_random.math-random-used",
  "path": "online-boutique/src/frontend/handlers.go",
  "start": {
    "line": 23,
    "col": 3,
    "offset": 672
  },
  "end": {
    "line": 23,
    "col": 12,
    "offset": 681
  },
  "extra": {
    "message": "Do not use `math/rand`. Use `crypto/rand` instead.",
    "fix": "crypto/rand",
    "metadata": {
      "cwe": [
        "CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)"
      ],
      "owasp": [
        "A02:2021 - Cryptographic Failures"
      ],
      "references": [
        "https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html#secure-random-number-generation"
      ],
      "category": "security",
      "technology": [
        "go"
      ],
      "confidence": "MEDIUM",
      "subcategory": [
        "vuln"
      ],
      "likelihood": "MEDIUM",
      "impact": "MEDIUM",
      "license": "Semgrep Rules License v1.0. For more details, visit semgrep.dev/legal/rules-license",
      "vulnerability_class": [
        "Cryptographic Issues"
      ],
      "source": "https://semgrep.dev/r/go.lang.security.audit.crypto.math_random.math-random-used",
```


Poor practices or mistakes in software development that peer reviews could easily miss

Anatomy of a Kubernetes Application



namespace
name
labels
annotations

runAsNonRoot
runAsUser
runAsGroup
fsGroup

containerPort
protocol

resources (cpu/memory)
readinessProbe
livenessProbe

volumes
tolerations

environment variables
var1=value1
var2=value2

allowPrivilegeEscalation
privileged (container)
capabilities (NET_ADMIN, e.g)

readOnlyRootFilesystem

Anatomy of a Kubernetes Application

```
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: front-end
  namespace: sock-shop
spec:
  replicas: 1
  selector:
    matchLabels:
      name: front-end
  template:
    metadata:
      labels:
        name: front-end
```

```
    spec:
      containers:
      - name: front-end
        image: weaveworksdemos/front-
end:0.3.12
        ports:
        - containerPort: 8079
        env:
        - name: SESSION_REDIS
          value: "true"
        securityContext:
          runAsNonRoot: true
          runAsUser: 10001
          capabilities:
            drop:
              - all
          readOnlyRootFilesystem: true
```

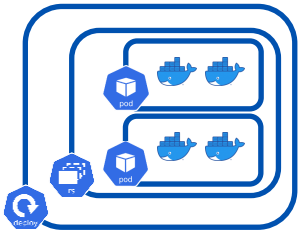
Anatomy of a Kubernetes Cluster

- user
- role
- system account
- config map
- secret

Insufficient Access Control

Excessive Privileges

Exposed Secrets



- API Server
- etcd Database
- Scheduler
- Controller

Control Plane

Unrestricted APIs

Cluster Data Loss

Excessive Resource Consumption

Unrestricted APIs

Weak OS Controls

Software Vulnerabilities

- kubelet
- kube proxy
- container runtime
- operating system

node

Anatomy of a Kubernetes Cluster

```
module "vpc" {
  source  = "terraform-aws-modules/vpc/aws"
  version = "5.0.0"

  name = "education-vpc"

  cidr = "10.0.0.0/16"
  azs  = slice(data.aws_availability_zones.available.names, 0, 3)

  private_subnets = ["10.0.1.0/24", "10.0.2.0/24", "10.0.3.0/24"]
  public_subnets  = ["10.0.4.0/24", "10.0.5.0/24", "10.0.6.0/24"]

  enable_nat_gateway   = true
  single_nat_gateway   = true
  enable_dns_hostnames = true

  public_subnet_tags = {
    "kubernetes.io/cluster/${local.cluster_name}" = "shared"
    "kubernetes.io/role/elb"                      = 1
  }

  private_subnet_tags = {
    "kubernetes.io/cluster/${local.cluster_name}" = "shared"
    "kubernetes.io/role/internal-elb"             = 1
  }
}
```

https://github.com/hashicorp/learn-terraform-provision-eks-cluster

```
module "eks" {
  source  = "terraform-aws-modules/eks/aws"
  version = "19.15.3"

  cluster_name    = local.cluster_name
  cluster_version = "1.27"

  vpc_id                         = module.vpc.vpc_id
  subnet_ids                     = module.vpc.private_subnets
  cluster_endpoint_public_access = true

  eks_managed_node_group_defaults = {
    ami_type = "AL2_x86_64"

  }

  eks_managed_node_groups = {
    one = {
      name = "node-group-1"

      instance_types = ["t3.small"]

      min_size     = 1
      max_size     = 3
      desired_size = 2
    }
  }
}
```

KICS

Keeping Infrastructure as Code Secure – OSS by Checkmarx

```
Missing User Instruction, Severity: HIGH, Results: 7
Description: A user should be specified in the dockerfile, otherwise the image will run as root
Platform: Dockerfile
CWE: 250
Learn more about this vulnerability: https://docs.kics.io/latest/queries/dockerfile-queries/fd54f200-402c-4333-a5a4-36ef6709af2f

        [1]: online-boutique/src/emailservice/Dockerfile:15

                014:
                015: FROM python:3.12.6-slim@sha256:15bad989b293be1dd5eb26a87ecacadaee1559f98e29f02bf6d00c8d86129f39 AS base
                016:

        [2]: online-boutique/src/paymentservice/Dockerfile:30

                029:
                030: FROM alpine:3.20.3@sha256:beefdbd8a1da6d2915566fde36db9db0b524eb737fc57cd1367effd16dc0d06d

        [3]: online-boutique/src/recommendationservice/Dockerfile:15

                014:
                015: FROM python:3.12.6-slim@sha256:15bad989b293be1dd5eb26a87ecacadaee1559f98e29f02bf6d00c8d86129f39 AS base
                016:

        [4]: online-boutique/src/currencyservice/Dockerfile:30

                029:
                030: FROM alpine:3.20.3@sha256:beefdbd8a1da6d2915566fde36db9db0b524eb737fc57cd1367effd16dc0d06d
                031:
```

```
$ kics scan --report-formats json \
    --output-path . --output-name kics-cloud.json \
    --queries-path /opt/homebrew/Cellar/kics/2.1.5/share/kics/assets/queries \
    --path online-boutique
```

KICS

Keeping Infrastructure as Code Secure – OSS by Checkmarx


```
"queries": [
    {
        "query_name": "Missing User Instruction",
        "query_id": "fd54f200-402c-4333-a5a4-36ef6709af2f",
        "query_url": "https://docs.docker.com/engine/reference/builder/#user",
        "severity": "HIGH",
        "platform": "Dockerfile",
        "cwe": "250",
        "category": "Build Process",
        "experimental": false,
        "description": "A user should be specified in the dockerfile, otherwise the image will run as root",
        "description_id": "eb49caf6",
        "files": [
            {
                "file_name": "online-boutique/src/emailservice/Dockerfile",
                "similarity_id": "0be7413357fa33ab50505db53b873ed7a6c782389ce34a586037d9eab43114d8",
                "line": 15,
                "issue_type": "MissingAttribute",
                "search_key": "FROM={{base}}",
                "search_line": -1,
                "search_value": "",
                "expected_value": "The 'Docke
                "actual_value": "The 'Dockerf
            },
```


```
$ kics scan --report-formats json \
    --output-path . --output-name kics-cloud.json \
    --queries-path /opt/homebrew/Cellar/kics/2.1.5/share/kics/assets/queries \
    --path online-boutique
```

gitleaks

Secret Leakage


```
[
 {
  "RuleID": "private-key",
  "Description": "Identified a Private Key, which may compromise cryptographic
security and sensitive data encryption.",
  "StartLine": 1,
  "EndLine": 21,
  "StartColumn": 1,
  "EndColumn": 34,
  "Match": "-----BEGIN OPENSSH PRIVATE KEY---- (omitted)",
  "Secret": "-----BEGIN OPENSSH PRIVATE KEY----- (omitted)”,
  "File": "online-boutique/example.id_dsa",
  "SymlinkFile": "",
  "Commit": "",
  "Entropy": 5.9529686,
  "Author": "",
  "Email": "",
  "Date": "",
  "Message": "",
  "Tags": [],
  "Fingerprint": "online-boutique/
 }
]
```


```
$ gitleaks dir -report-format json -report-path ./gitleaks.json online-boutique

    ○
    │╲
    │ ○
    ○ ░
    ░    gitleaks

1:50PM INF scanned ~5050270 bytes (5.05 MB) in 159ms
1:50PM WRN leaks found: 7
```

Runtime Kubernetes Scanning (Trivy Operator)

```
$ helm repo add aqua https://aquasecurity.github.io/helm-charts/
$ helm repo update
$ helm upgrade trivy-operator aqua/trivy-operator --install \
    --namespace trivy-system --create-namespace --version 0.26.0 \
    --set nodeCollector.tolerations[0].key=node-role.kubernetes.io/control-plane \
    --set nodeCollector.tolerations[0].operator=Exists \
    --set nodeCollector.tolerations[0].effect=NoSchedule
NAME: trivy-operator
LAST DEPLOYED: Sat Feb  8 11:16:00 2025
NAMESPACE: trivy-system
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
You have installed Trivy Operator in the trivy-system namespace.
It is configured to discover Kubernetes workloads and resources in
all namespace(s).

Inspect created VulnerabilityReports by:
    kubectl get vulnerabilityreports --all-namespaces -o wide

Inspect created ConfigAuditReports by:
    kubectl get configauditreports --all-namespaces -o wide

Inspect the work log of trivy-operator by:
    kubectl logs -n trivy-system deployment/trivy-operator
```

Toleration permits node scanning of control plane. Otherwise, control plane nodes must be excluded.

Deploys Trivy Operator in cluster to regularly scan the cluster from container vulnerability, Kubernetes security, and compliance perspectives.

This is also the output of the command:
helm status trivy-operator

Trivy Vulnerability Reports

```
$ kubectl get vulnerabilityreports -n bookinfo
NAME                                                REPOSITORY                                      TAG      SCANNER
replicaset-details-v1-54ffdd5947-details            istio/examples-bookinfo-details-v1              1.20.2   Trivy
replicaset-productpage-v1-d49bb79b4-productpage     istio/examples-bookinfo-productpage-v1          1.20.2   Trivy
replicaset-ratings-v1-856f65bcff-ratings            istio/examples-bookinfo-ratings-v1              1.20.2   Trivy
replicaset-reviews-v1-848b8749df-reviews            istio/examples-bookinfo-reviews-v1              1.20.2   Trivy
replicaset-reviews-v2-5fdf9886c7-reviews            istio/examples-bookinfo-reviews-v2              1.20.2   Trivy
replicaset-reviews-v3-bb6b8ddc7-reviews             istio/examples-bookinfo-reviews-v3              1.20.2   Trivy

$ kubectl get vulnerabilityreports -n bookinfo replicaset-details-v1-54ffdd5947-details \
     -o json | jq -r '.report.artifact.repository, .report.summary'

istio/examples-bookinfo-details-v1

{
  "criticalCount": 7,
  "highCount": 468,
  "lowCount": 181,
  "mediumCount": 1873,
  "noneCount": 0,
  "unknownCount": 1
}
```

Trivy Configuration Audit Reports

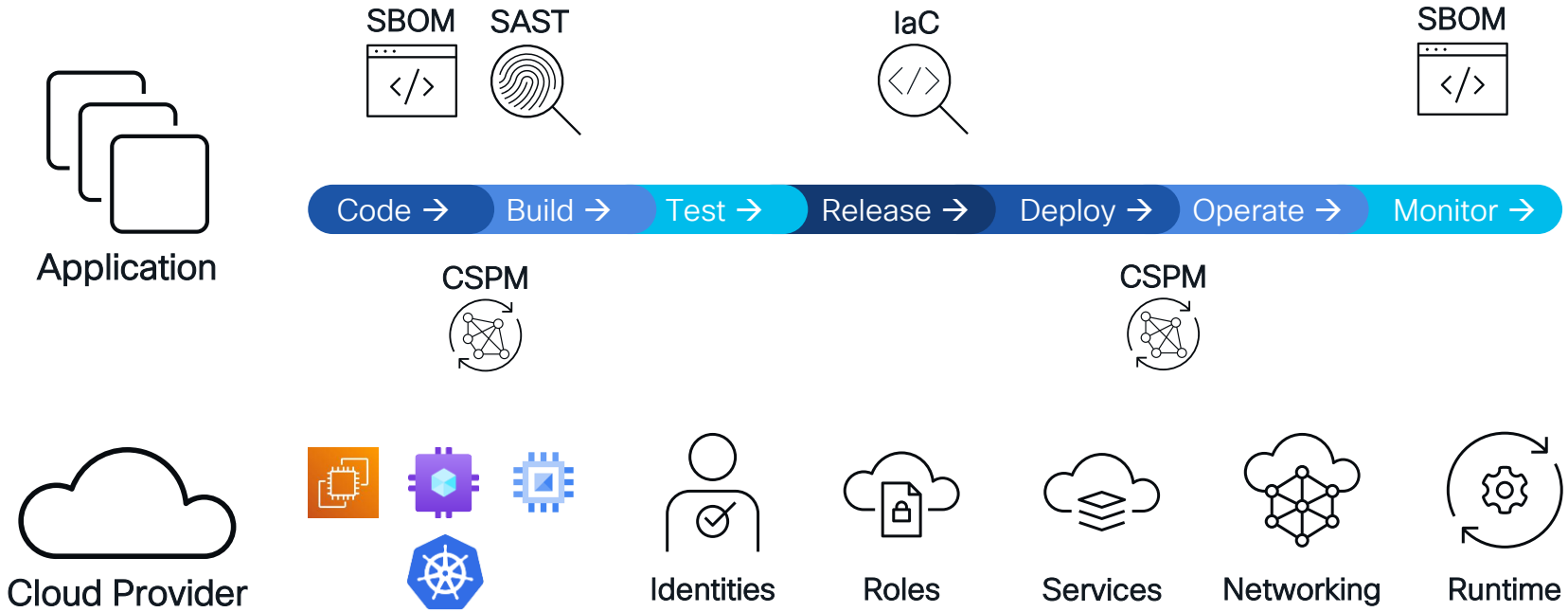
```
$ kubectl get configauditreports -n bookinfo
NAME                                          SCANNER
replicaset-details-v1-54ffdd5947              Trivy
replicaset-productpage-v1-d49bb79b4           Trivy
replicaset-ratings-v1-856f65bcff              Trivy
replicaset-reviews-v1-848b8749df              Trivy
replicaset-reviews-v2-5fdf9886c7              Trivy
replicaset-reviews-v3-bb6b8ddc7               Trivy
service-cilium-gateway-bookinfo-gateway       Trivy
service-details                               Trivy
service-details-v1                            Trivy
service-productpage                           Trivy
service-productpage-v1                        Trivy
service-ratings                               Trivy
service-ratings-v1                            Trivy
service-reviews                               Trivy
service-reviews-v1                            Trivy
service-reviews-v2                            Trivy
service-reviews-v3                            Trivy
```

```
$ kubectl get configauditreports replicaset-details-v1-54ffdd5947 \
    -n bookinfo -o json | jq -r \
    '.metadata.name, .report.summary, .report.checks[0]'

replicaset-details-v1-54ffdd5947

{
  "criticalCount": 0,
  "highCount": 2,
  "lowCount": 9,
  "mediumCount": 3
}

{
  "category": "Kubernetes Security Check",
  "checkID": "KSV015",
  "description": "When containers have resource requests specified, the
scheduler can make better decisions about which nodes to place pods on,
and how to deal with resource contention.",
  "messages": [
    "Container 'details' of ReplicaSet 'details-v1-54ffdd5947' should
set 'resources.requests.cpu'"
  ],
  "remediation": "Set 'containers[].resources.requests.cpu'.",
  "severity": "LOW",
  "success": false,
  "title": "CPU requests not specified"
}
```

Additional Trivy Reports

```
$ kubectl get crds | grep aquasecurity
clustercompliancereports.aquasecurity.github.io         2025-02-12T15:58:21Z
clusterconfigauditreports.aquasecurity.github.io        2025-02-12T15:58:21Z
clusterinfraassessmentreports.aquasecurity.github.io    2025-02-12T15:58:21Z
clusterrbacassessmentreports.aquasecurity.github.io     2025-02-12T15:58:21Z
clustersbomreports.aquasecurity.github.io               2025-02-12T15:58:21Z
clustervulnerabilityreports.aquasecurity.github.io      2025-02-12T15:58:21Z
configauditreports.aquasecurity.github.io               2025-02-12T15:58:21Z
exposedsecretreports.aquasecurity.github.io             2025-02-12T15:58:21Z
infraassessmentreports.aquasecurity.github.io           2025-02-12T15:58:21Z
rbacassessmentreports.aquasecurity.github.io            2025-02-12T15:58:21Z
sbomreports.aquasecurity.github.io                      2025-02-12T15:58:21Z
vulnerabilityreports.aquasecurity.github.io             2025-02-12T15:58:21Z

$ kubectl get clustercompliancereports.aquasecurity.github.io
NAME                      AGE
k8s-cis-1.23              5m33s
k8s-nsa-1.0               5m33s
k8s-pss-baseline-0.1      5m33s
k8s-pss-restricted-0.1    5m33s
```

Cloud Native Application Stack



Code and Build Security

Identify, prioritize, & remediate risk throughout SDLC, covering APIs designed, code developed, and the automation used to deploy it.

SCM Repository Scanning

- SaST

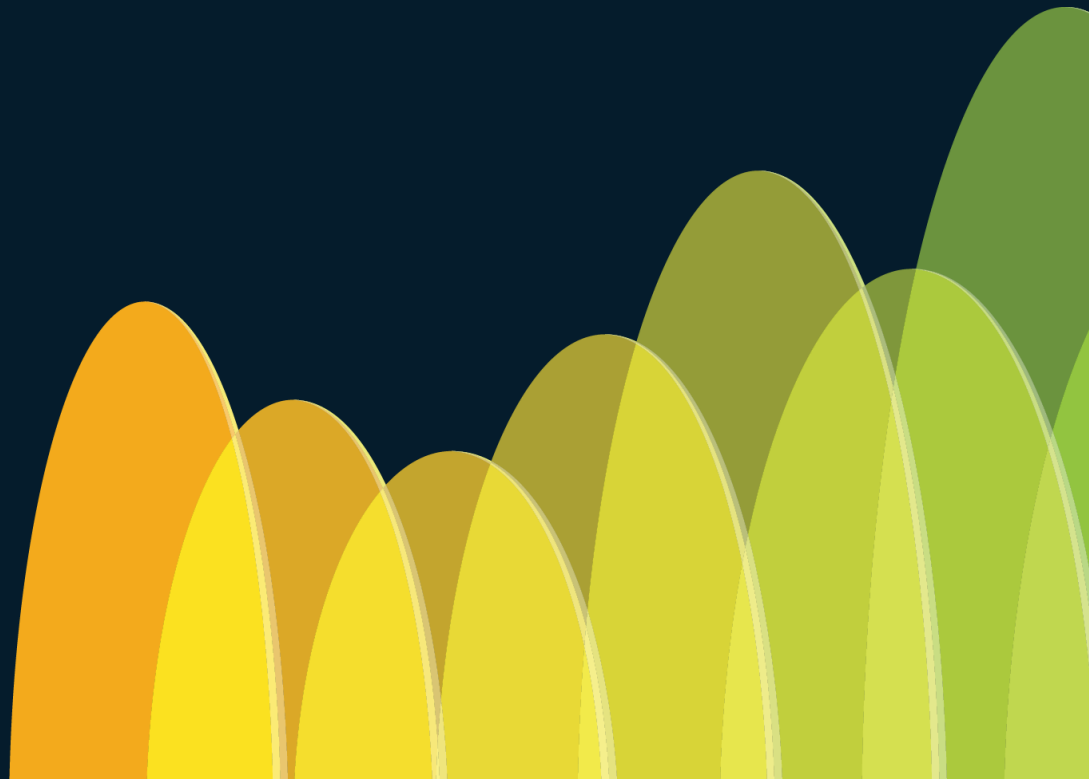
SBOM and CVE Assessment

- Pipeline Image Scanning

Kubernetes Admission Controller

- CVE Vulnerabilities

Realtime Security



cisco Live!

Attacks are dynamic, exploiting existing paths

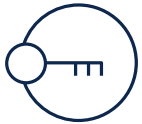
Proactive but Stagnant

Shift Left Security and Posture Assessments provide cost effective cloud application security but are limited to static, point-in-time views.

Remediated but Exploitable

Threats are dynamic and the threat landscape constantly evolves.

New zero-day vulnerabilities, new attack vectors, increased sophistication are the norm.



Secured but Vulnerable

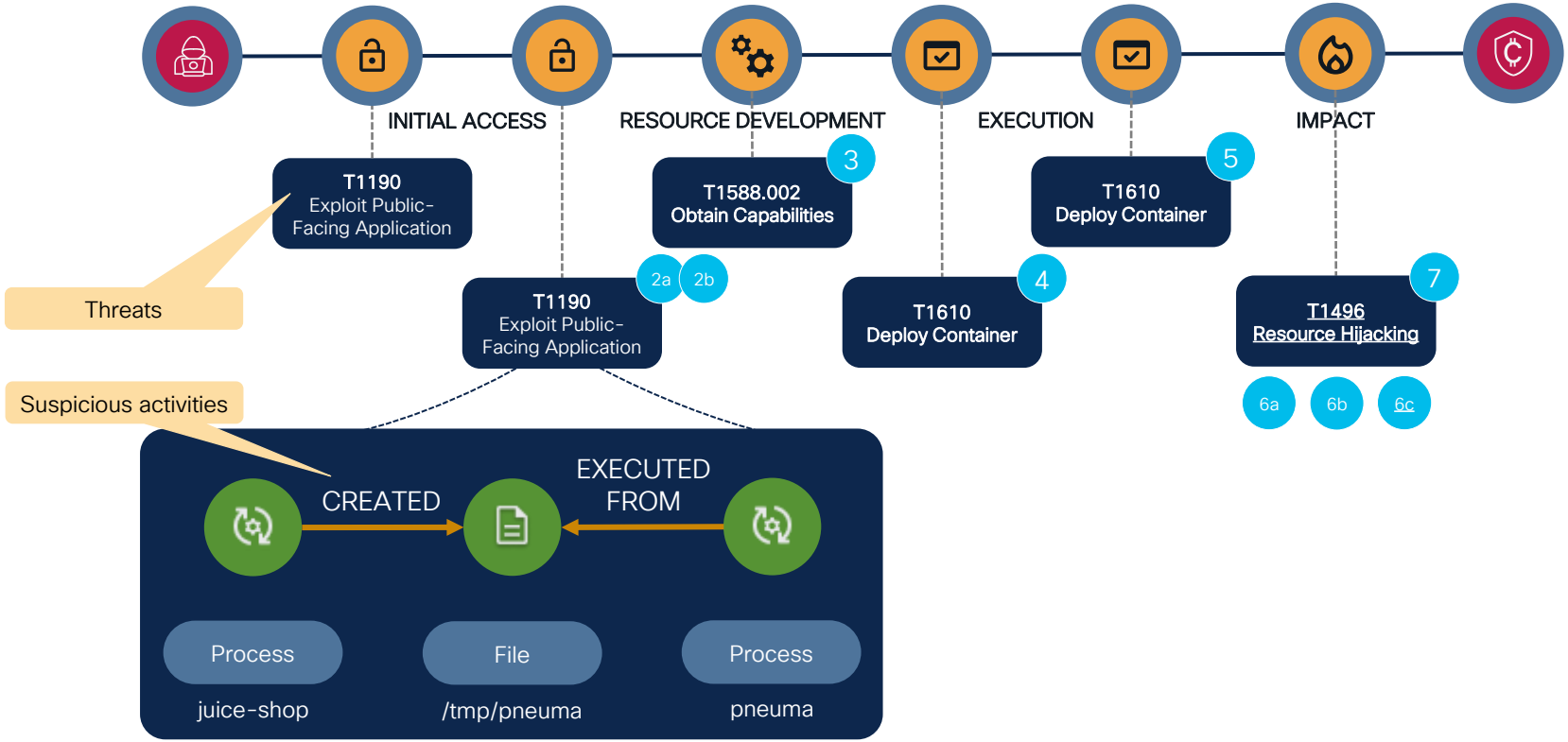
Many attacks leverage leaked secrets and otherwise valid points of entry.

Initial breach attack vectors:

- 16% phishing
- 15% stolen/ leaked credentials
- 6% malicious insider

Anatomy of an Attack

Cryptojacking attack

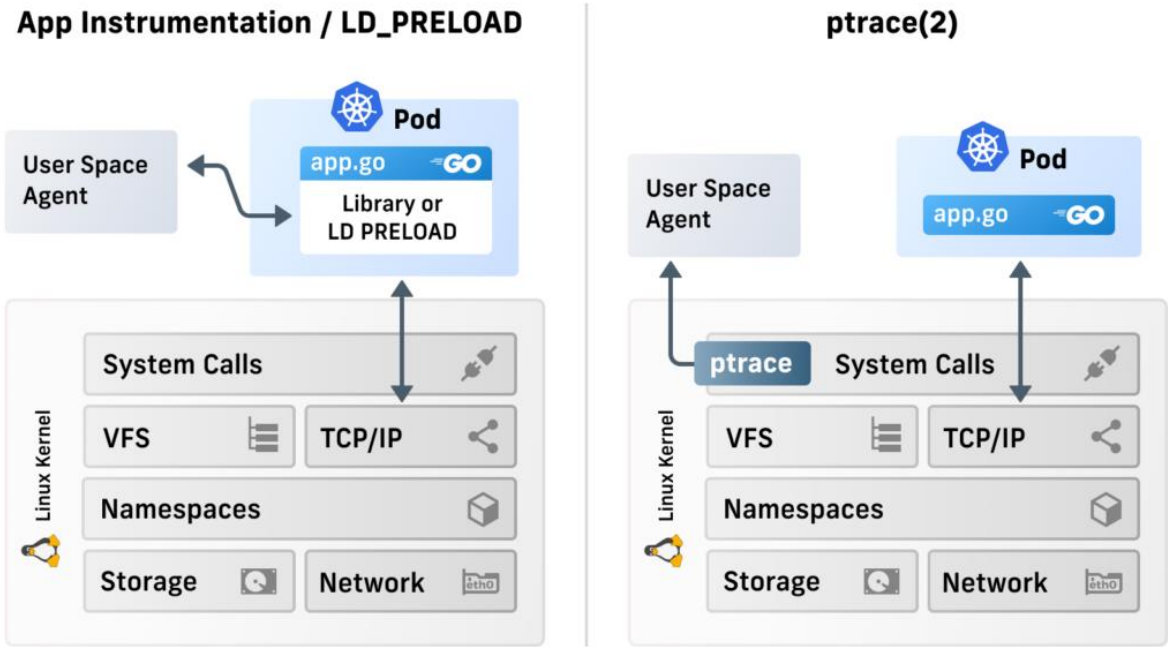


Real Time Event Visibility

Traditional User Space Techniques

Pros:
- Efficient
- Good application visibility
- Varying levels of transparency

Cons:
- Varying levels of app changes and evasion
- Not usable for enforcement
- No visibility into the system

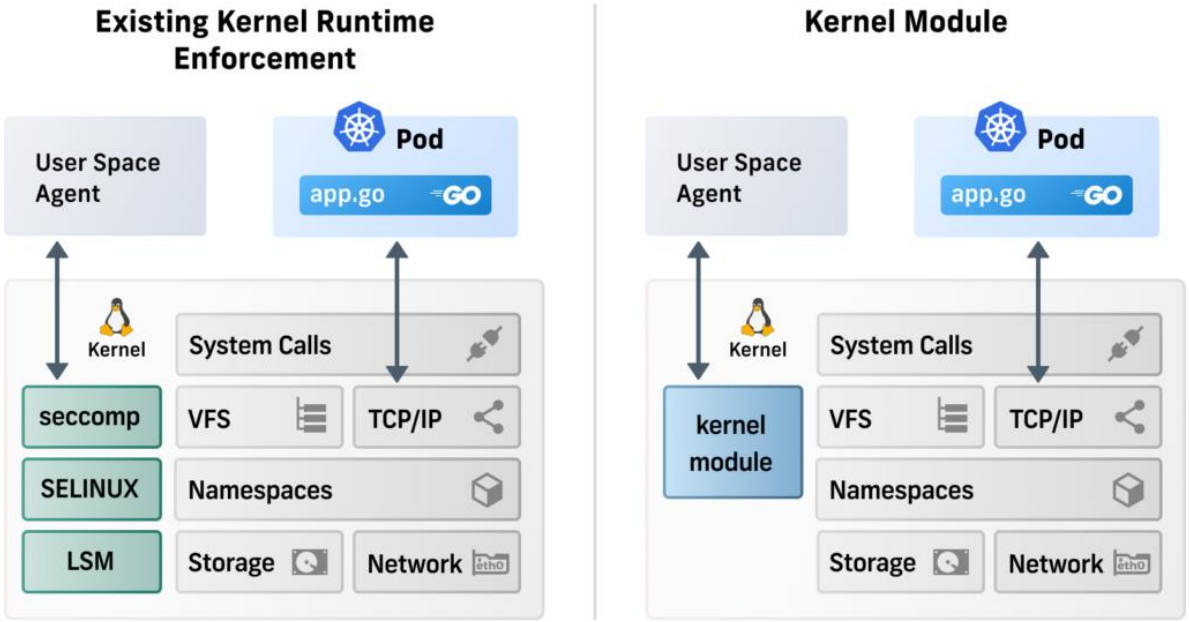


Real Time Event Visibility

Traditional In-Kernel Techniques

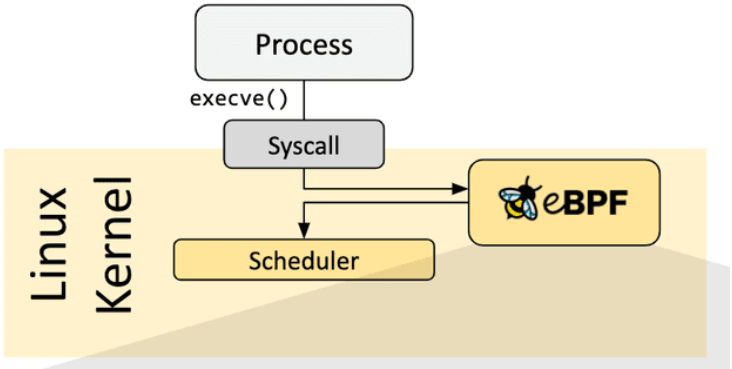
Pros:
- Efficient
- Complete transparency to applications

Cons:
- Varying levels of visibility into how system calls are used.
- Inflexible and non-extensible (KRE)
- Maximum flexibility but security restrictions and instability challenges (module)



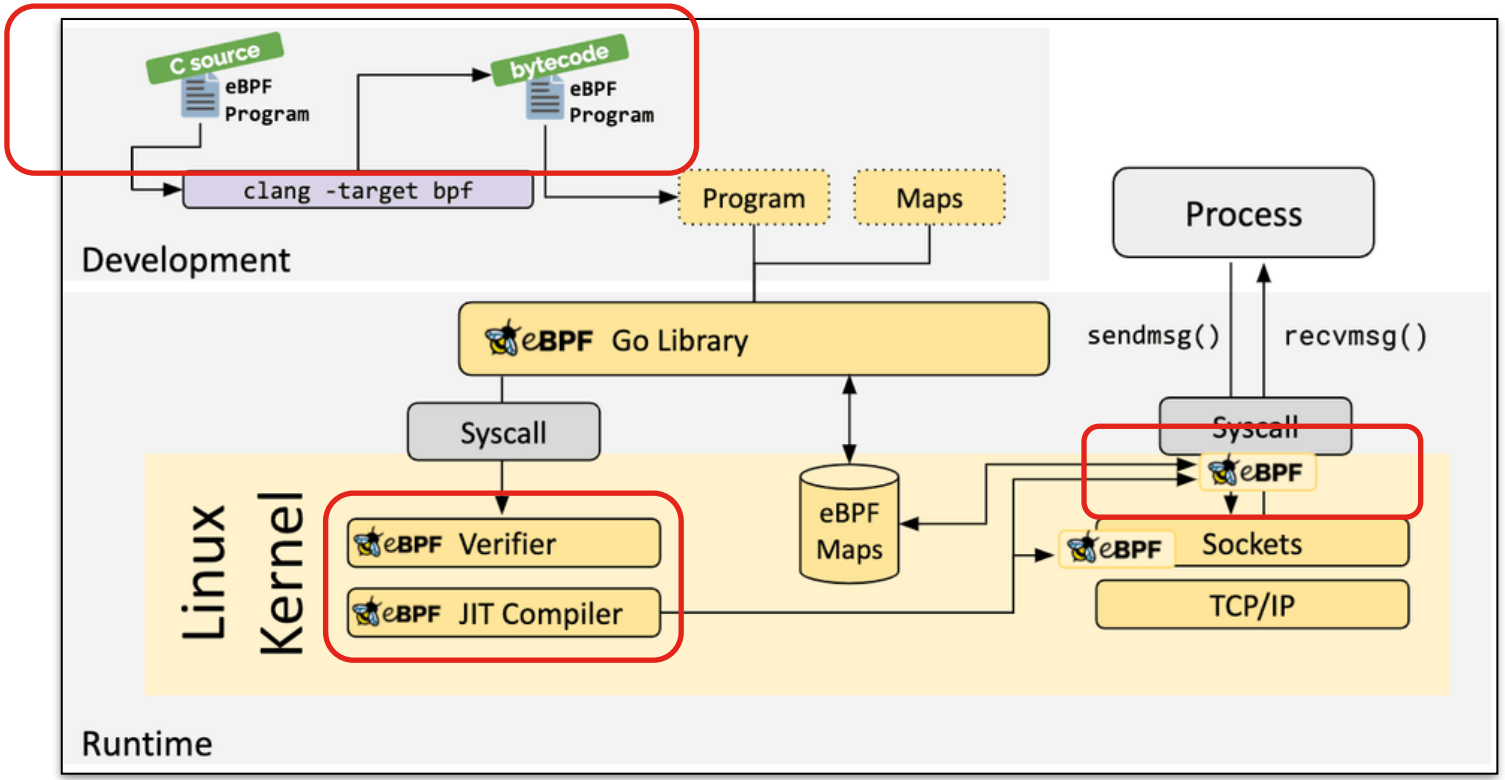
eBPF – Modular Kernel Extensions

- eBPF is a revolutionary technology invented by Isovalent (now part of Cisco) that can run sandboxed programs in the Linux kernel
- it is used to safely and efficiently extend the capabilities of the kernel without requiring to change kernel source code or load kernel modules
- BPF originally stood for Berkeley Packet Filter, but now that eBPF (extended BPF) can do so much more than packet filtering, the acronym no longer makes sense



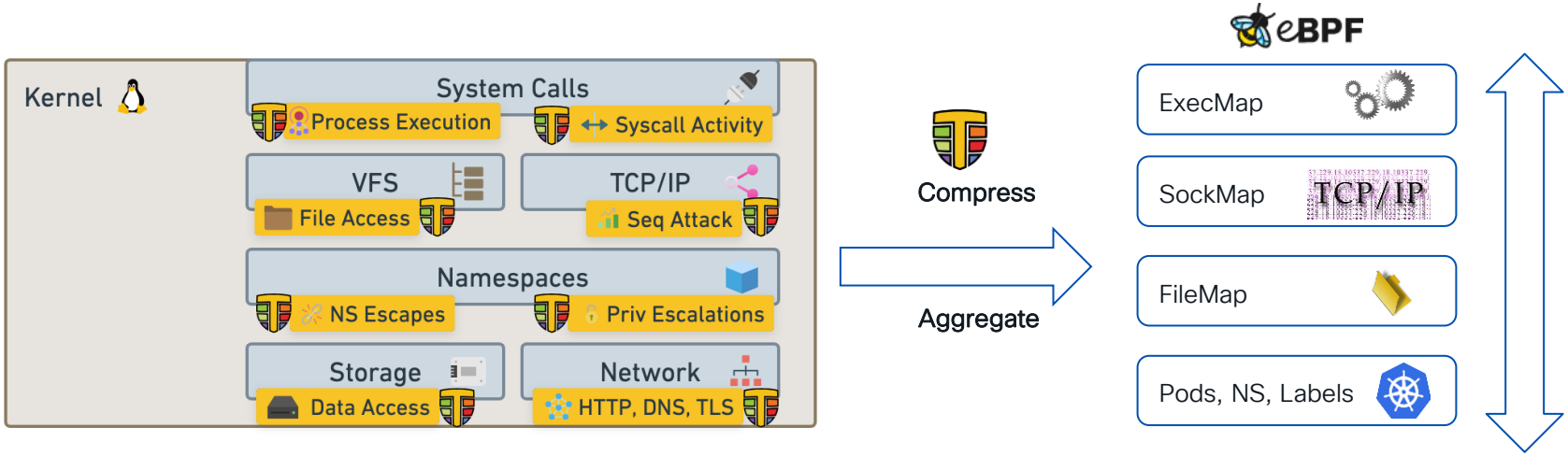

```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

        bpf_get_current_comm(&event.comm, sizeof(event.comm));
        comm_events.perf_submit(ctx, &event, sizeof(event));

        return 0;
}
```

eBPF – Kernel extension with guard rails



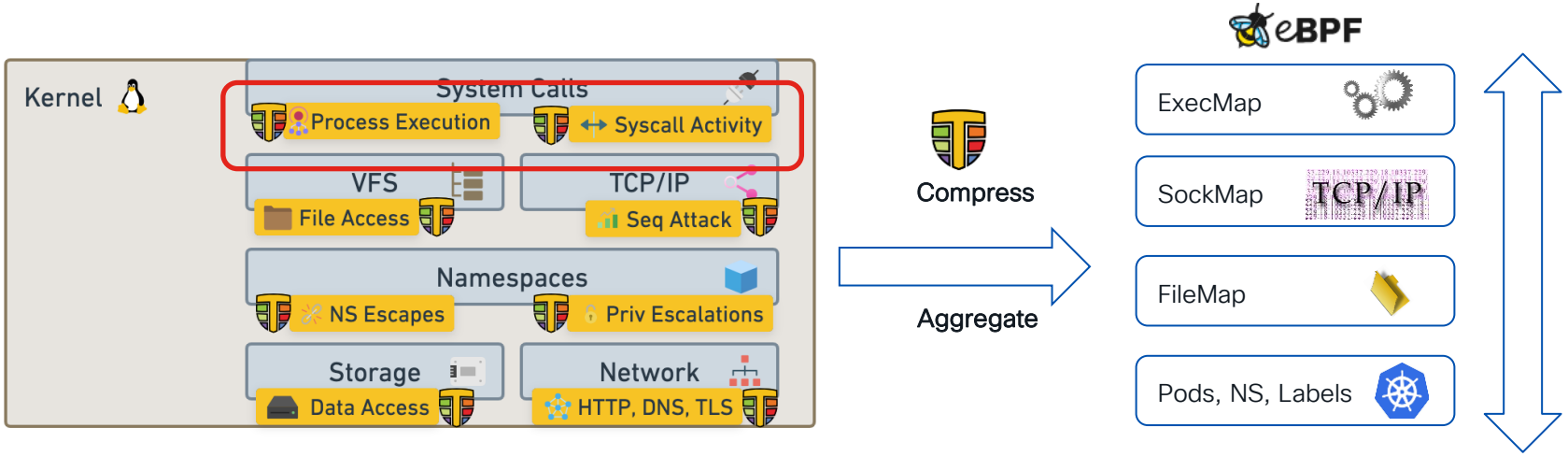
Principles for eBPF-based

In-Kernel-State is powerful for context and avoiding races



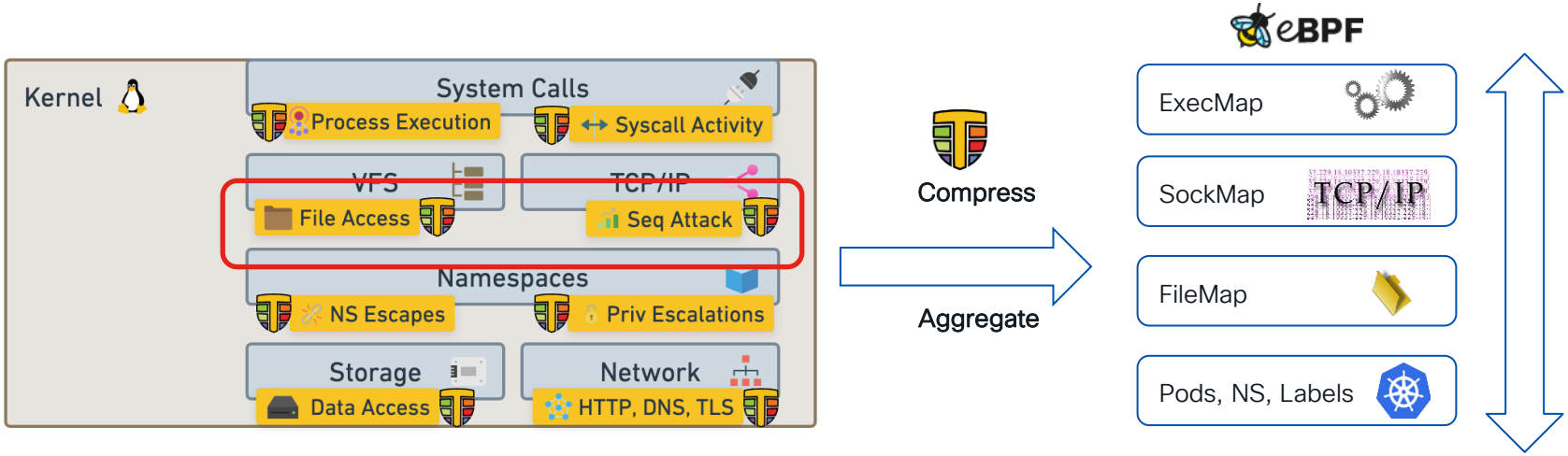
Principles for eBPF-based

In-Kernel-State is powerful for context and avoiding races



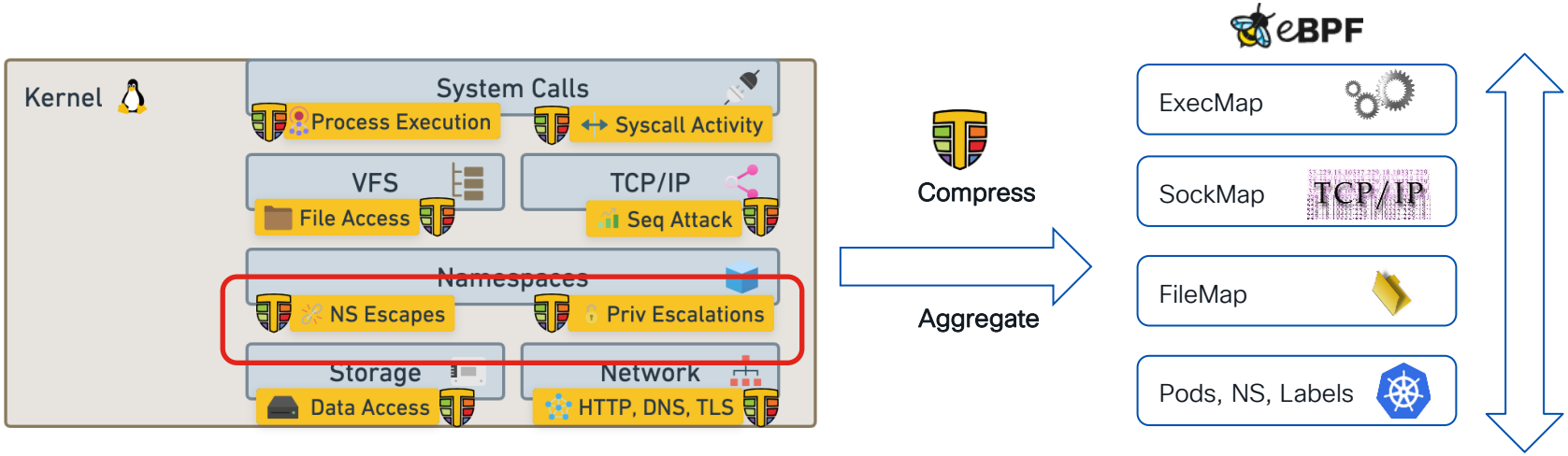
Principles for eBPF-based

In-Kernel-State is powerful for context and avoiding races



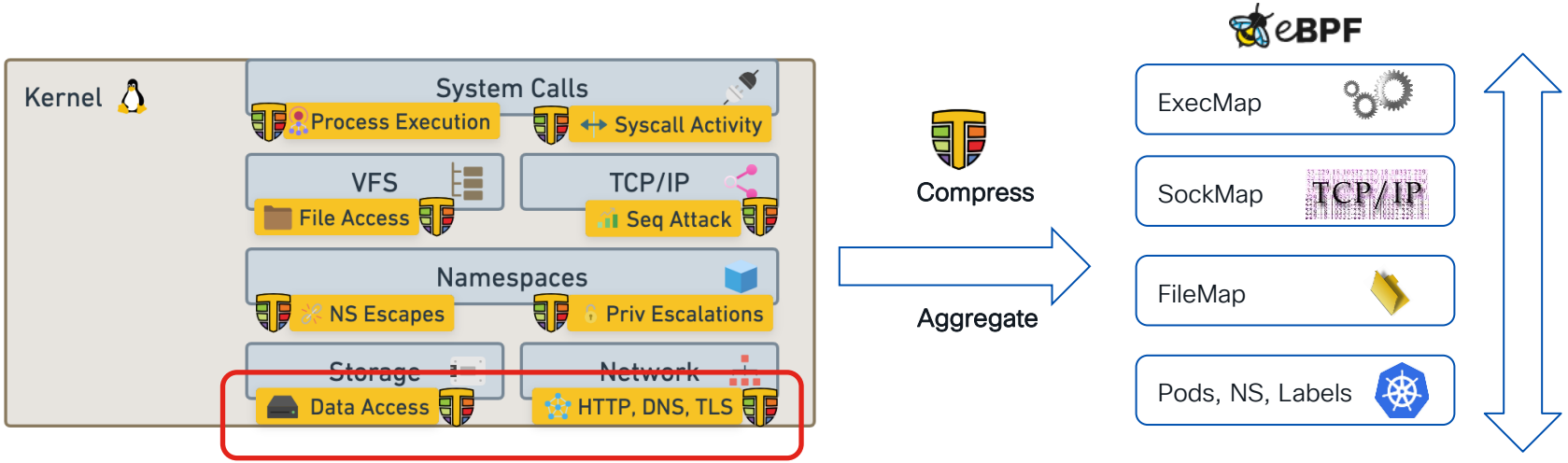
Principles for eBPF-based

In-Kernel-State is powerful for context and avoiding races



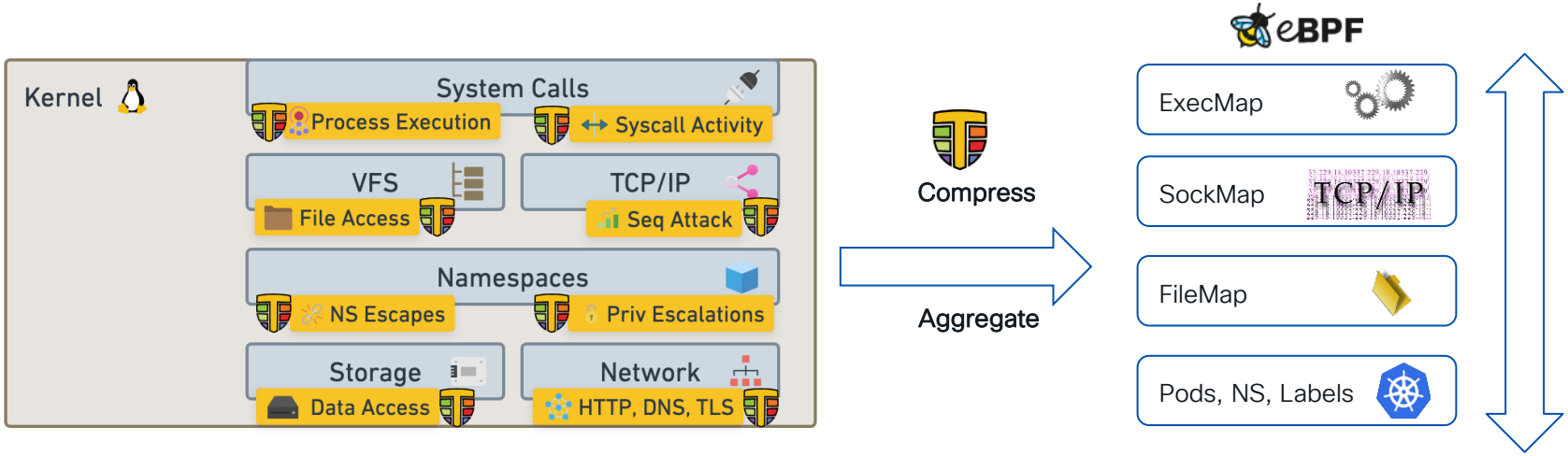
Principles for eBPF-based

In-Kernel-State is powerful for context and avoiding races



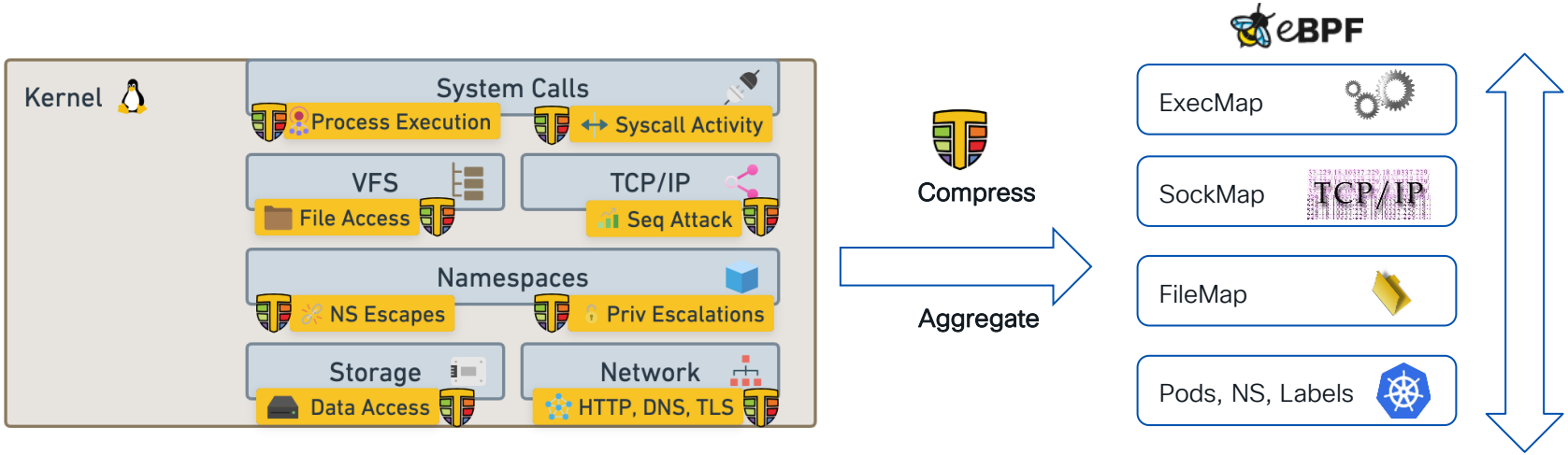
Principles for eBPF-based

In-Kernel-State is powerful for context and avoiding races

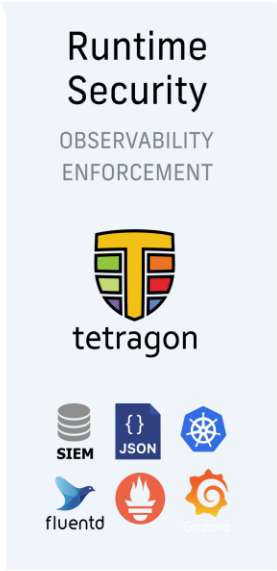


Principles for eBPF-based

In-Kernel-State is powerful for context and avoiding races



Isovalent Suite of eBPF Open Source Solutions



Isovalent Suite of eBPF Open Source Solutions

Service Mesh

RESILIENCE AUTHENTICATION TRAFFIC MANAGEMENT

cilium Service Mesh

Ingress Gateway API spiffe

Observability

METRICS TRACING SERVICE MAP LOGS

cilium Hubble

SIEM JSON fluentd Grafana OpenTelemetry

Networking

ENCRYPTION LOAD-BALANCING NETWORK POLICY NETWORKING

cilium CNI

IPsec
Wireguard

Kubernetes
DSR • Maglev

DNS • L7
L3/L4

IPv4 • IPv6 • Overlay • BGP
Egress Gateway • Multi-Cluster

Runtime Security

OBSERVABILITY
ENFORCEMENT

tetragon

SIEM JSON fluentd Grafana

Kubernetes Container VM Metal

aws Google Cloud Azure Alibaba Cloud Red Hat OpenShift vmware

Tetragon Overview

Tetragon

Open Source

- Apache 2.0 (userspace) & GNU GPL (eBPF)
- Part of CNCF as a subproject of Cilium

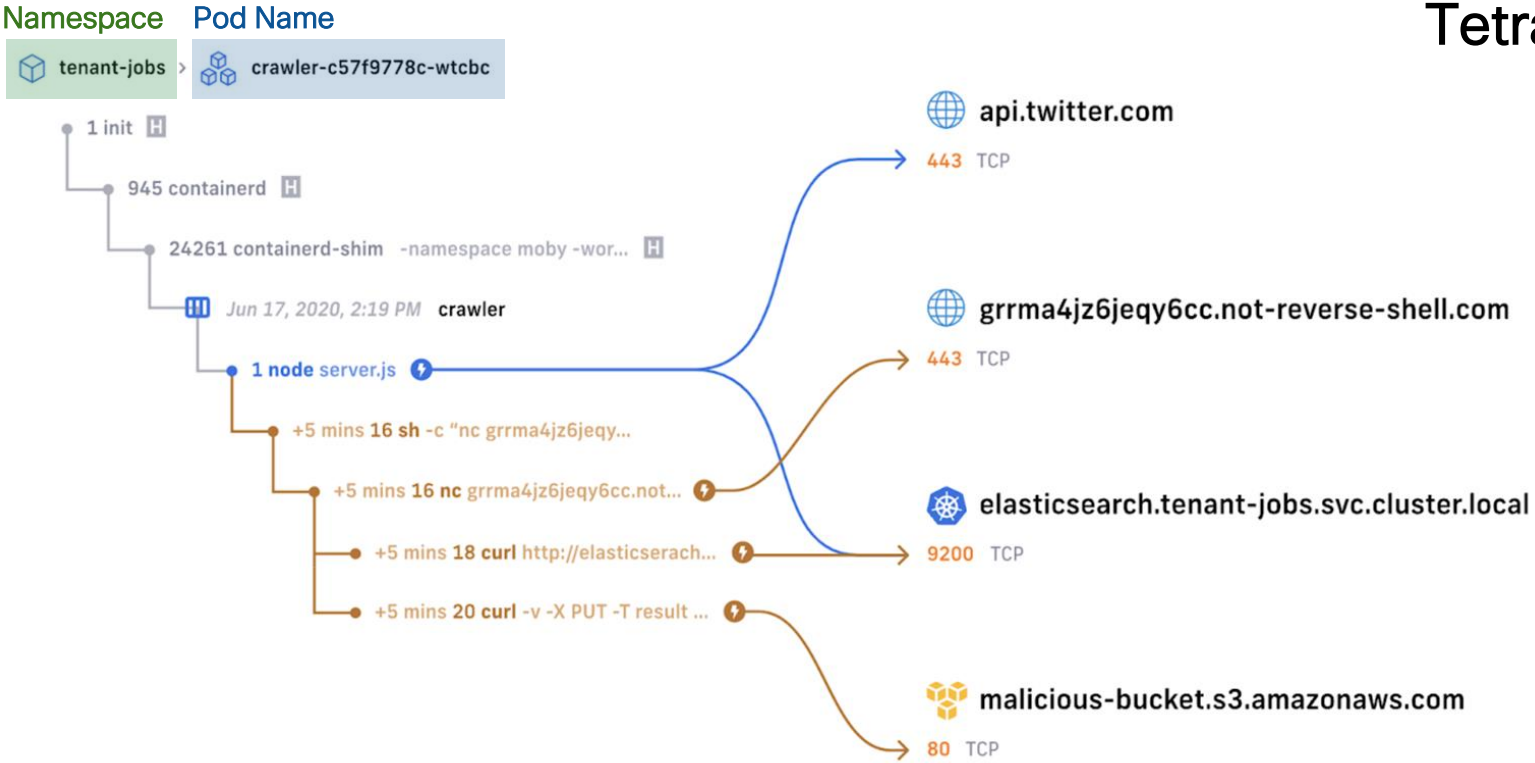
eBPF-based

- Generic low level process events
- In-kernel filtering and enforcement

Kubernetes-native

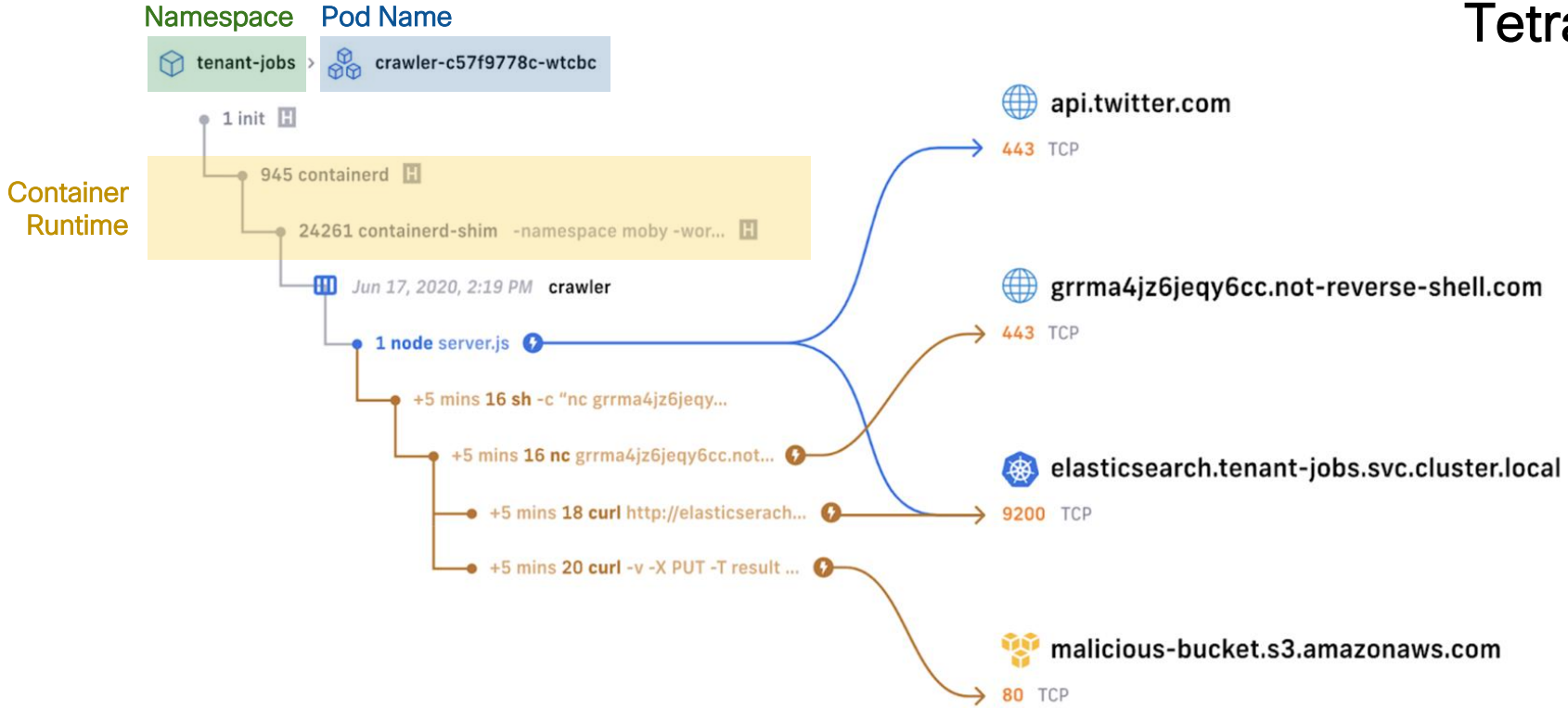
- Kubernetes metadata in events
- Configuration via custom resources

Let’s Deep Dive into a Kubernetes Pod



Tetragon

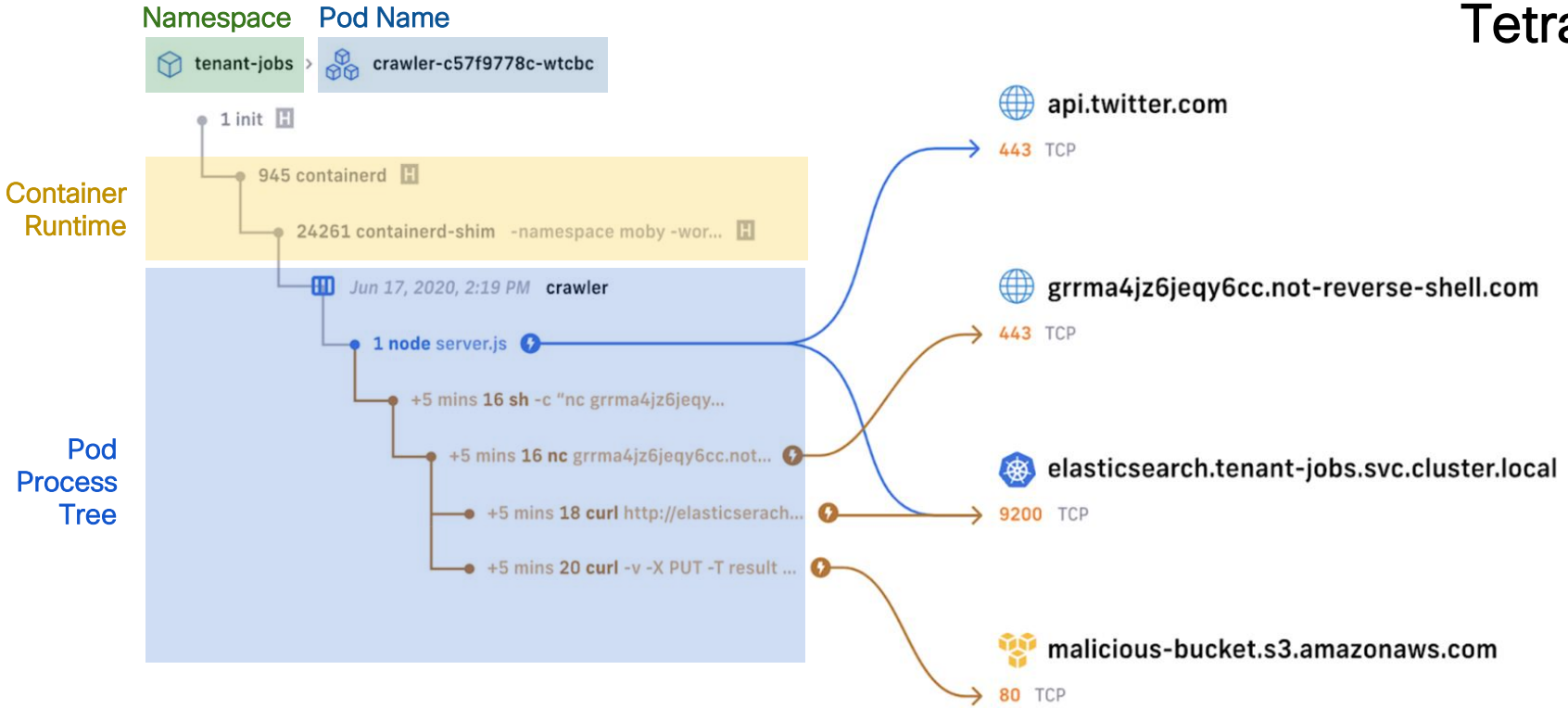
Let's Deep Dive into a Kubernetes Pod



Tetragon

Let's Deep Dive into a Kubernetes Pod

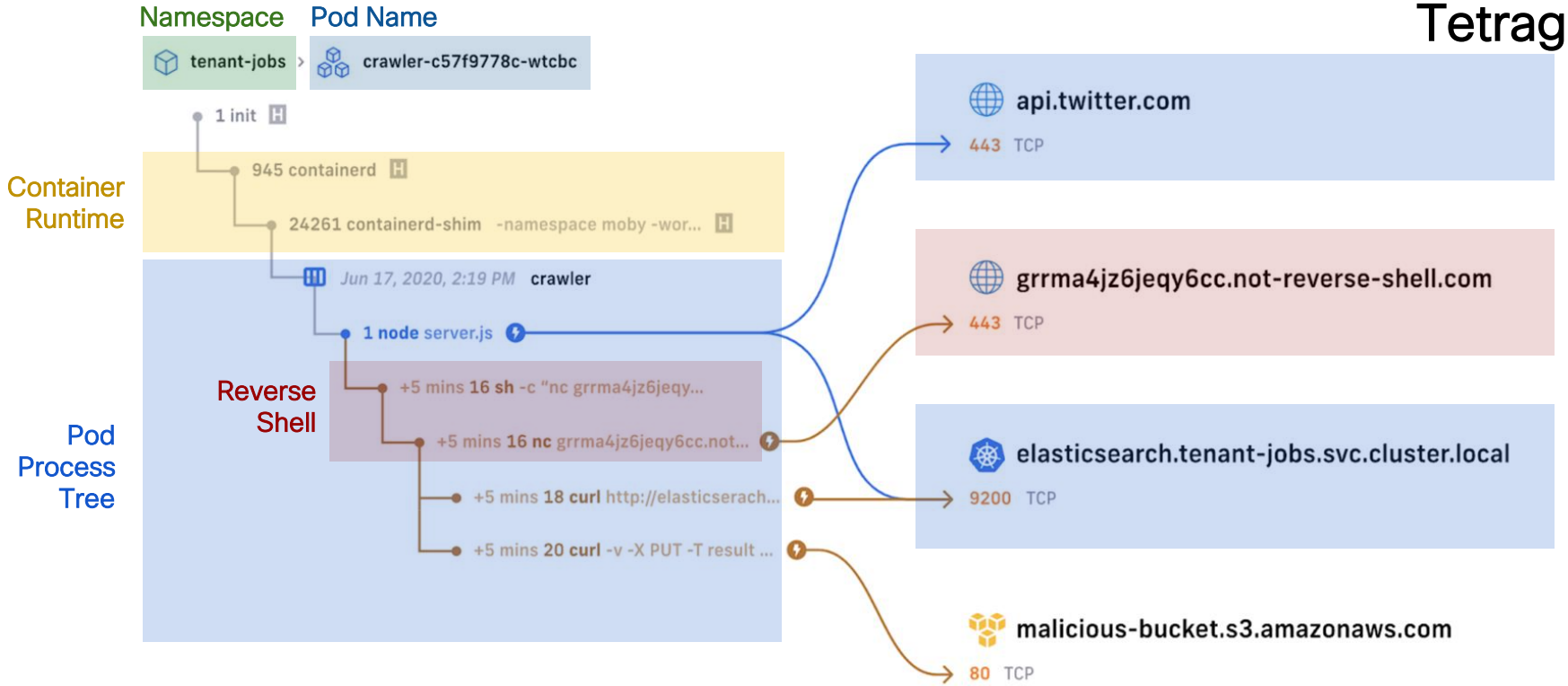
Tetragon



Let's Deep Dive into a Kubernetes Pod

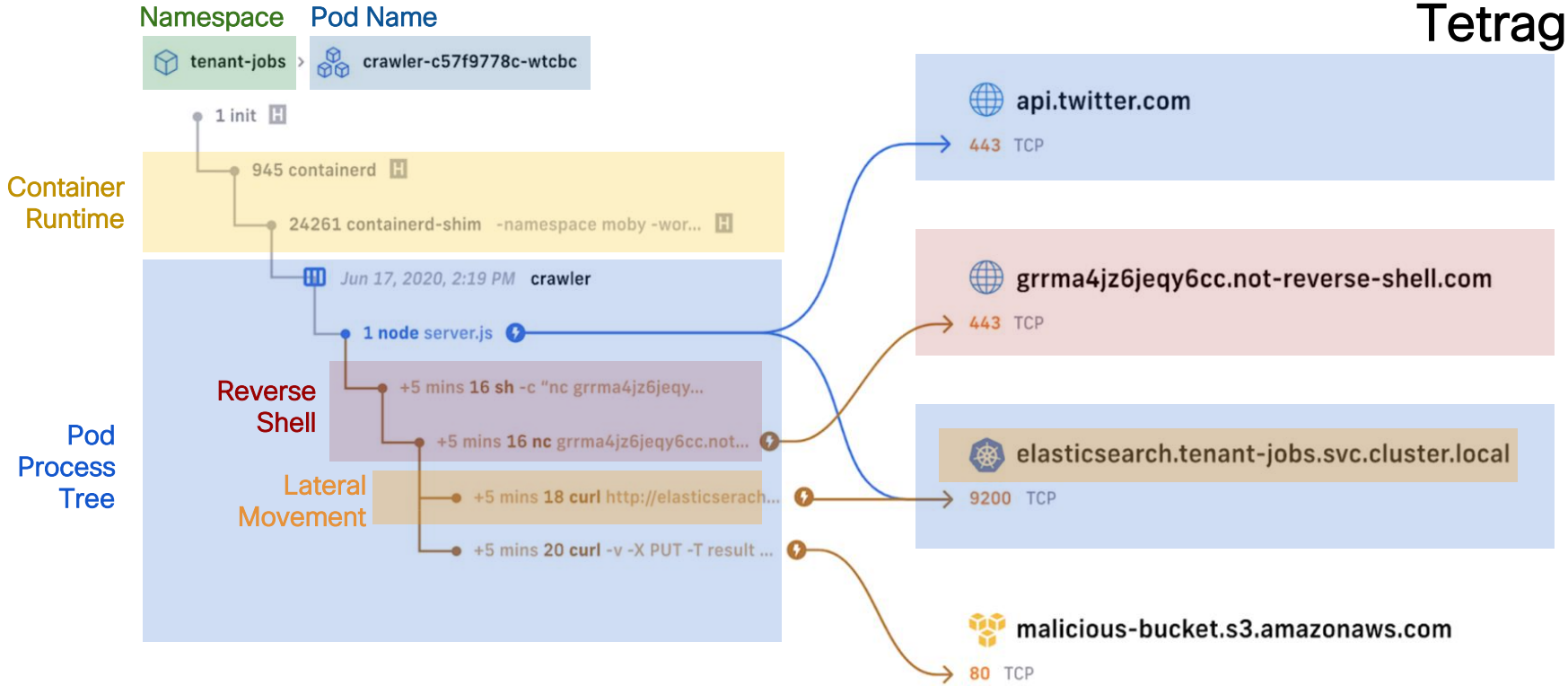
Tetragon

Let's Deep Dive into a Kubernetes Pod



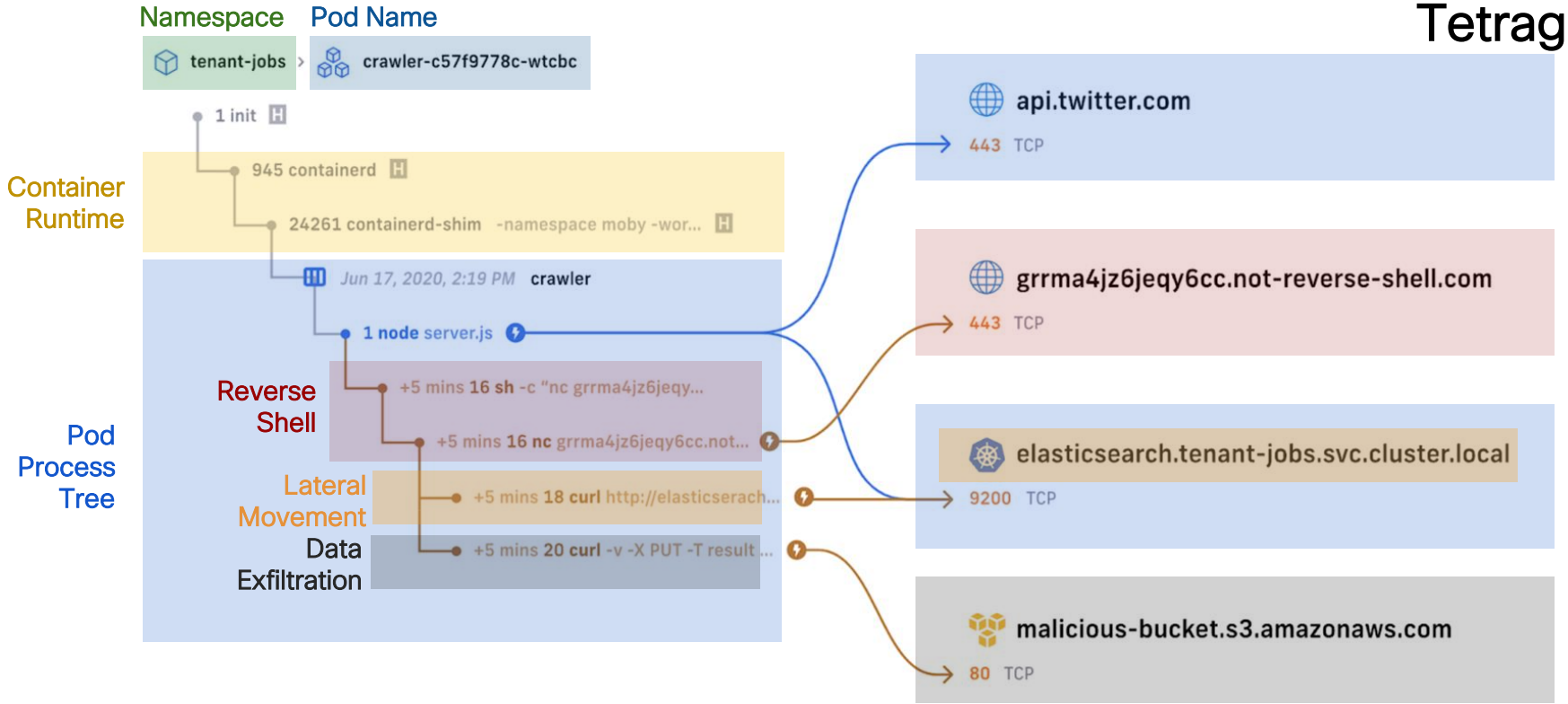
Tetragon

Let's Deep Dive into a Kubernetes Pod



Tetragon

Let's Deep Dive into a Kubernetes Pod



Tetragon

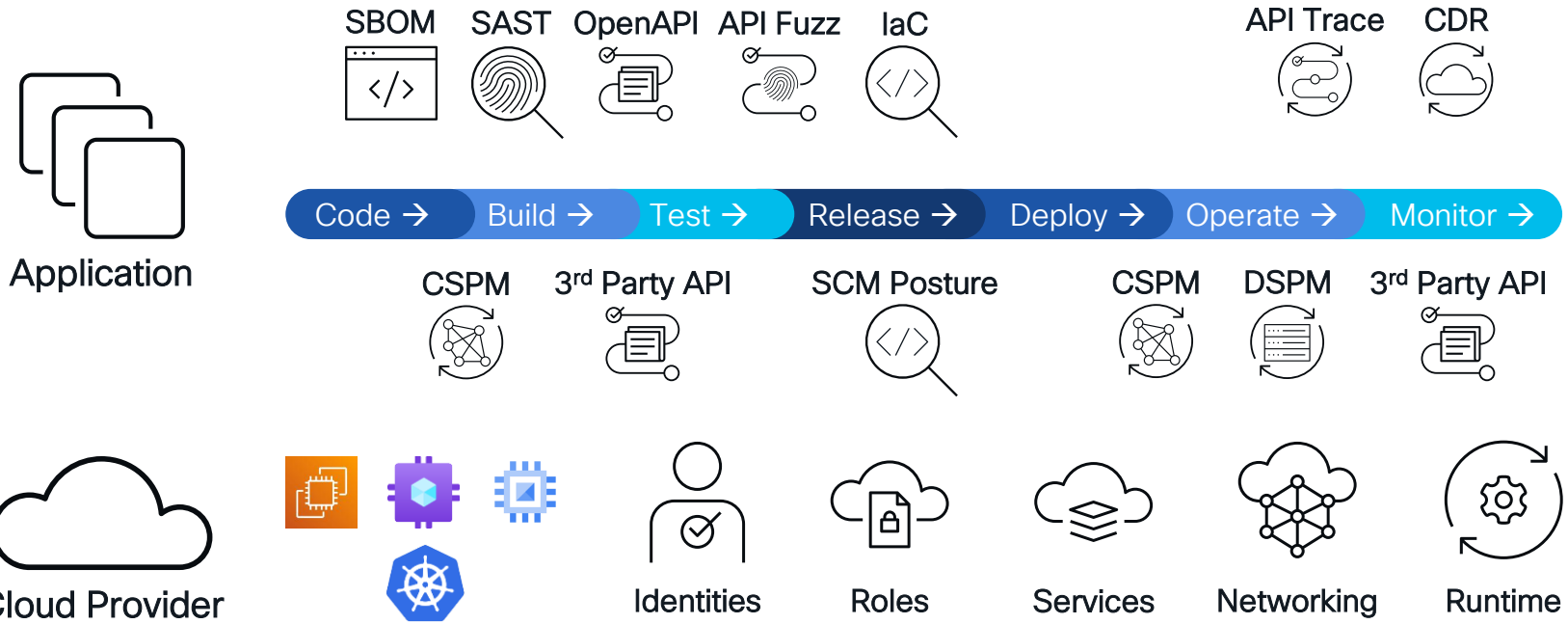
Realtime Security

Instrument your Kubernetes cluster to observe in real time potential threats to your applications. Leverage eBPF based policies to prevent known bad behaviors.

Tetragon eBPF-based Security

- Transparent suspicious activity detection
- Native Kubernetes policy enforcement

Cloud Native Application Stack



Summary

Final Thoughts

- Open source software and technologies form the foundation of Cloud Native Applications, both in their development as well as their lifecycle management (pipeline)
- Application and cloud security open source projects provide clean, simple interfaces to assess the security risks in your cloud environments.
- The key to cloud native security is prevention and automation so leveraging native pipeline capabilities provides immense value with only minor investments.

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me on LinkedIn

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

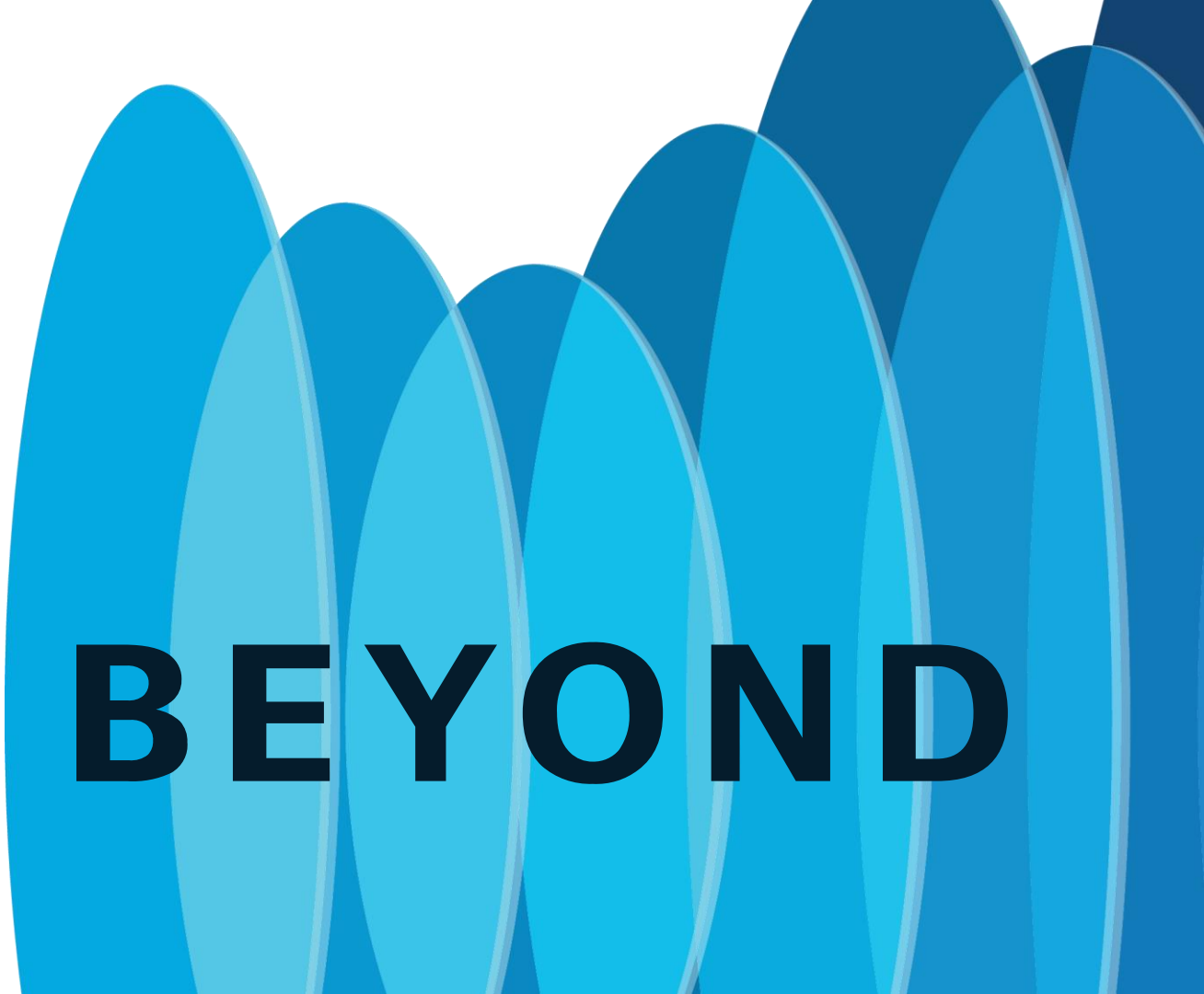
The Internet of Agents is here

Want to learn more about
Outshift and Internet of Agents?

Thank you

cisco Live!

cisco Live!



GO BEYOND