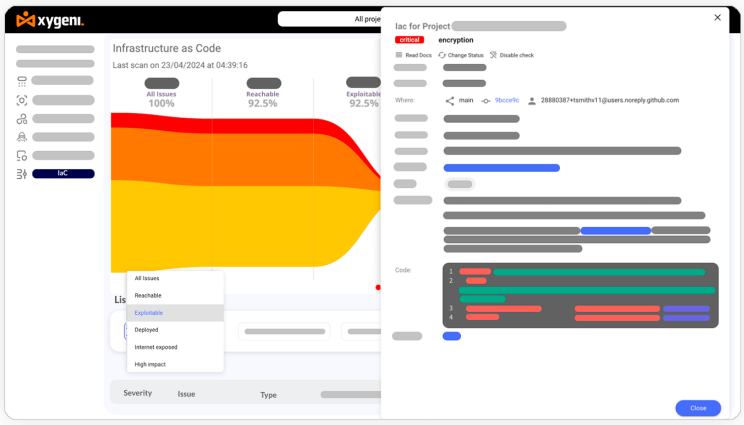
Infrastructure as Code

Solution Brief

Secure Your Infrastructure Automation with Precision

Maximize the reliability and security of your infrastructure as code processes. Our advanced IaC solution ensures that your automated configurations are not only efficient but protected against vulnerabilities from development to deployment.



About Company

Xygeni specializes in enhancing software development security and efficiency with our Application Security Posture Management (ASPM) platform. We offer complete control over application risks, a unified security view from code to cloud, and eliminate noise to prioritize risks effectively. Our advanced malware detection and early warning system makes Xygeni a leader in protecting applications from emerging threats, ensuring rapid and secure software delivery.

Securing your Infrastructure as Code (IaC) is essential in software development because misconfigurations and vulnerabilities can seriously harm your systems and give hackers opportunities to attack. Xygeni's IaC security tools help prevent these issues before they become problems, reducing the risk of data exposure and cutting down on expensive fixes. By integrating security early in the development process, Xygeni makes sure your cloud setups are secure and consistent, helping you meet compliance standards and minimize risks. Choose Xygeni to keep your delivery secure and smooth from start to finish.

Recent findings reveal significant security concerns in Infrastructure as Code (IaC) within software development and continuous delivery environments. **Nearly 200,000 IaC templates currently used in production are insecure, mainly due to misconfigurations.** Further compounding the issue, over 43% of cloud databases remain unencrypted, and only 60% of cloud storage services enable logging. These figures highlight the widespread security gaps in IaC implementations. This data underscores the urgent need for proactive security measures to mitigate risks and secure modern IT infrastructure effectively.

43% of cloud databases remain unencrypted

Infrastructure as Code

Solution Brief

Detect Any Cloud Misconfigurations:

Xygeni's platform efficiently identifies and mitigates cloud misconfigurations across various IaC templates, including Terraform, CloudFormation, and Azure Resource Manager (ARM), ensuring your cloud infrastructure is secured against common and complex vulnerabilities.

Integrated CI/CD Security and Adaptable Scanning:

Xygeni integrates seamlessly with your CI/CD pipelines, providing real-time alerts and halting problematic deployments. Here are several ways to incorporate Xygeni's IaC scanning capabilities:

Pre-Commit Hooks

Incorporate Xygeni's scanning as a pre-commit hook in Git to automatically check for IaC flaws before code is committed. This ensures that any potential issues are addressed at the earliest stage of development.

Example Git Pre-Commit Hook

```
#!/bin/bash
xygeni iac --scan --fail-on=high --format=text --output=scan_results.txt
if [ $? -ne 0 ]; then
  echo "IaC security issues detected. Commit aborted."
  cat scan_results.txt
  exit 1
fi
```

CI/CD Pipeline Integration

Integrate Xygeni scans into your CI/CD pipelines using popular CI tools like Jenkins, CircleCI, or GitHub Actions. Configure the scan to run at key stages, such as before a merge request is accepted or before deployment to production.

Example Git Pre-Commit Hook

```
#!/bin/bash
xygeni iac --scan --fail-on=high --format=text --output=scan_results.txt
if [ $? -ne 0 ]; then
  echo "IaC security issues detected. Commit aborted."
  cat scan_results.txt
  exit 1
fi
```

Automated Policy Enforcemen

Deploy extensive, predefined policies to automatically address major security challenges like infrastructure misconfigurations, container vulnerabilities, and exposed secrets, simplifying cloud security without additional effort.

Adaptable Scanning Capabilities

Xygeni's scanning tools are designed to adapt to various environments and configurations, allowing scans of both private and public registries, local file systems, and different container formats. This adaptability ensures comprehensive security coverage regardless of your infrastructure's complexity or scale.

Infrastructure as Code

Solution Brief

Comprehensive Support for Major Frameworks

- **Terraform:** We provide detectors for a wide range of resources across major cloud providers such as AWS, Azure, and Google Cloud, making it ideal for cloud-agnostic infrastructure setups.
- **CloudFormation:** Managed AWS service integration allows for detailed modeling and provisioning of AWS resources.
- **ARM and Bicep:** Tools for Azure resources, ranging from traditional ARM templates to the newer, more developer-friendly Bicep syntax.
- **Kubernetes:** Whether using basic Pods syntax or complex Helm charts, Xygeni ensures your Kubernetes deployments are secure.
- **Docker:** Our security extends to Docker environments, including Dockerfiles and docker-compose files that define services, networks, and volumes.

Comprehensive and Flexible Container Image Scanning

Xygeni enhances container security by detecting container image misconfigurations, vulnerabilities, and secrets. Xygeni can pull images from multiple sources for scanning:

- Local Docker Engine: Directly from the installed Docker engine.
- Containerd: Via the Containerd daemon or nerdctl.
- Podman: Using the Podman CLI.
- Remote OCI Registry: Directly from OCI-compliant registries or specified via tarball:<path> for local OCI format images.

Block IaC Misconfigurations Before Production

- By incorporating best practices and security guardrails directly into development workflows, Xygeni prevents noisy and redundant alerts, ensuring only relevant issues are flagged. This proactive approach blocks IaC misconfigurations before they reach production, maintaining the integrity and security of your deployments.

Context-Driven Security Insights

- By incorporating best practices and security guardrails directly into development workflows, Xygeni prevents noisy and redundant alerts, ensuring only relevant issues are flagged. This proactive approach blocks IaC misconfigurations before they reach production, maintaining the integrity and security of your deployments.

Prioritization and Remediation Guidance

- Simplify risk management by prioritizing significant IaC risks and providing detailed guidelines for remediation, reducing the time and effort needed to secure your infrastructure.

Infrastructure as Code

Solution Brief

Overview of Supported IaC Flaw Detectors

AWS CloudFormation

Specialized in analyzing CloudFormation templates for AWS, ensuring configurations like ALB security, AWS Lambda environments, and database settings adhere to best practices. Notable detectors include:

- Ensuring ALB uses HTTPS.
- Encryption enforcement on CloudTrail logs.
- Encryption checks on various AWS service deployments like EBS, S3, and RDS.

Ansible

Targets general security practices and specific AWS configurations within Ansible playbooks. Key focuses include:

- Enforcing non-deprecated modules.
- Ensuring encryption and proper versioning on S3 buckets.
- Validating security configurations in backup and recovery processes.

Azure Resource Manager (ARM) and Bicep

Covers Azure resource deployments with checks tailored to Azure's unique capabilities, including:

- Verification of secure transmission in Azure databases.
- Encryption validations for storage and database services.
- Network security checks for Azure Kubernetes services.

Kubernetes and Docker

Provides extensive coverage for containerized environments and orchestrations, ensuring:

- Secure Kubernetes deployments, including encryption and network policies.
- Dockerfile and docker-compose.yml analyses for secure container configurations.

Multi-Framework / AWS and Azure

- IAM configurations to prevent excessive permissions.
- Network security policies to safeguard cloud resources.

Book Your Demo Now - Transform Your Approach to Cybersecurity!