WHITEPAPER

Protecting Software Intellectual Property and CI/CD Security with Xiid SealedTunnel

Introduction

In modern software development, Continuous Integration and Continuous Deployment (CI/CD) pipelines have become critical for achieving excellent code quality and efficient software delivery. However, these pipelines are also a prime target for cyber threats like credential theft, supply chain attacks, remote code execution, and unauthorized access. This can lead to potentially catastrophic loss of intellectual property and the compromise of customer assets downstream such as in the infamous Solarwinds breach.

Xiid's SealedTunnel™ is a robust solution that mitigates these threats by enabling secure transport and access without exposing sensitive intellectual property or CI/CD systems to the public internet.

CI/CD Security Challenges

Organizations face several security challenges in their CI/CD environments, such as:

Credential Exposure

API keys, tokens, and credentials in environment variables or accidentally committed to repositories may be vulnerable to leaks.

Unauthorized Access

CI/CD servers, repositories, and artifact storage systems are frequently targeted by attackers and may become compromised, leading to exfiltration of intellectual property and making it possible for code and artifacts to be tampered with.

Data in Transit Risks

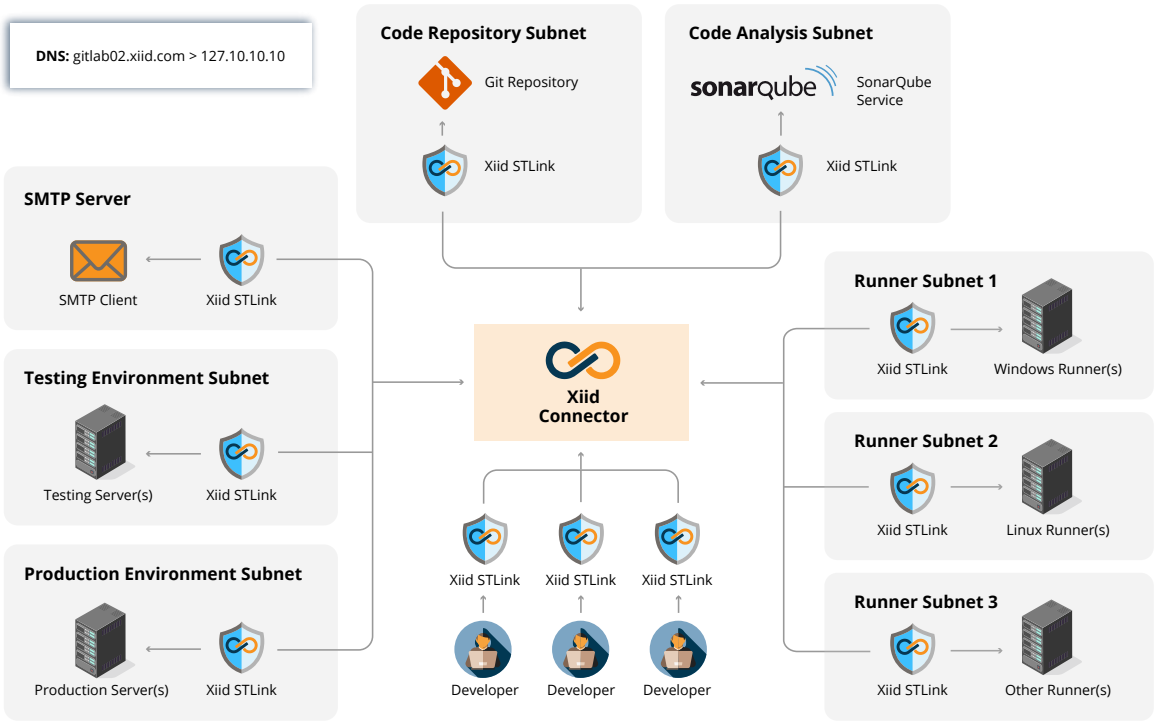
CI/CD systems frequently communicate with external services over the internet, increasing exposure to man-in-the-middle (MitM) attacks.

Source Control System Vulnerabilities

Systems such as GitLab often suffer from critical vulnerabilities and are not always patched or updated, leaving them open to exploitation for extended periods of time. These systems may themselves also be attached to other vulnerable systems such as SMTP.

Ultra-secure CI/CD with Xiid SealedTunnel™

No subnets or servers need any open inbound ports or public IP addresses.



Xiid SealedTunnel: A Secure CI/CD Solution

Xiid's SealedTunnel addresses these security concerns with Xiid's **Zero Knowledge Networking (ZKN)** technology which eliminates attack surface by allowing all inbound ports to be completely closed. SealedTunnel prevents tampering, decryption, or man-in-the-middle attacks with triple-encrypted, quantum-secure, process-to-process tunnels that make it easy to access and use CI/CD systems while preventing unauthorized access.

Key Features of SealedTunnel for CI/CD Security

Eliminates Credential Exposure
Since SealedTunnel takes CI/CD architecture "offline" by allowing all inbound traffic to be rejected, API keys, tokens, and environment variables are kept safe – even those committed by accident.

Exceeds Zero Trust Access Standards
SealedTunnel not only ensures that only authenticated and authorized sessions can access the CI/CD pipeline but also goes further by segmenting resources at the process level, eliminating the risk of lateral movement by attackers.

Mitigates Data in Transit Threats
The quantum-resistant, triple-encrypted communication channel ensures that sensitive data exchanged between CI/CD components is protected against eavesdropping and interception.

Ultra-Secure Code Repository Access
Xiid SealedTunnel eliminates inbound network access to the centralized code repository, making repositories impossible to reach by outside attackers but easy to access by authorized and authenticated staff.

Reduces or Eliminates Vulnerability Exploitation
As outside attackers can no longer address a potentially vulnerable CI/CD component, it may be exceedingly difficult or impossible for them to attempt an exploit.

Seamless Integration
Xiid SealedTunnel is designed to integrate with popular CI/CD platforms such as Jenkins, GitLab CI/CD, GitHub Actions, and CircleCI with few, if any, modifications.

USE CASE

Secure Code Analysis and Deployments with SealedTunnel

A software company using GitLab CI/CD can implement SealedTunnel in the following way:

PROTECT GITLAB RUNNERS

SealedTunnel secures GitLab Runners by allowing all inbound access to them to be rejected and enforcing quantum-secure access. This prevents unauthorized access or tampering.

SECURE API AND TOKEN ACCESS

By removing direct exposure to API keys, SealedTunnel ensures that credentials required for deployments and integrations remain inaccessible to external threats.

DEFEND AGAINST VULNERABILITIES

From SMTP to GitLab, removing the ability to directly address systems can make it nearly impossible for attackers to exploit active vulnerabilities, giving system administrators confidence in the integrity of CI/CD systems and more time to apply patches.

PREVENT CODE INJECTION ATTACKS

SealedTunnel eliminates malicious unauthorized access to GitLab and the possibility of communication being tampered with, preventing code from being injected into the GitLab repository, CI/CD pipeline configurations from being changed, and secrets from being modified or stolen.

SECURE CLOUD DEPLOYMENTS

When deploying applications to cloud environments, SealedTunnel ensures that all connections to production servers, databases, and services remain isolated and sealed from potential breaches.

Enhancing DevOps and SecOps with Xiid SealedTunnel

DevOps Security Benefits

Automated Secure Deployments

Xiid SealedTunnel ensures that CI/CD automation remains protected from unauthorized access and credential leaks.

Immutable Security Posture

DevOps teams can maintain security controls with SealedTunnel without affecting the speed and agility of development and deployment cycles.

Secure Code Repositories

SealedTunnel prevents unauthorized access to code repositories, ensuring that only authenticated users and processes interact with the codebase.

Secure Runner Access

DevOps CI/CD runner access can be restricted to authorized DevOps team members through SealedTunnel and be made impossible to access by unauthorized developers.

SecOps Security Benefits

Zero Trust Implementation

SealedTunnel enforces strict authentication, ensuring that only verified entities can interact with the CI/CD pipeline and centralized code repositories.

Continuous Security Monitoring

SealedTunnel integrates with security tools to detect and mitigate threats in real-time without exposing infrastructure.

Threat Isolation

SealedTunnel ensures that any potential breach is contained, preventing lateral movement within the network and safeguarding critical assets.

Conclusion

As CI/CD pipelines and source control solutions continue to be key attack vectors, organizations must adopt advanced security measures to protect their software supply chain. Xiid's SealedTunnel offers a Zero Knowledge approach to securing CI/CD environments by eliminating inbound access to resources, securing credentials, and ensuring tamper-free, safe software delivery.

By integrating SealedTunnel, organizations significantly enhance their CI/CD security posture while maintaining development efficiency. Furthermore, both DevOps and SecOps teams benefit from SealedTunnel's ability to safeguard the entire CI/CD ecosystem, making it an essential component in modern software development and security operations.