RAPPORT DE SÉCURITÉ DEVSECOPS

Fichier analysé:	example_workflow.yml
Date d'analyse:	27/05/2025 à 16:17:11
Score de sécurité:	0/100 (CRITIQUE)
Niveau de risque:	CRITIQUE
Total anomalies:	53

RÉSUMÉ EXÉCUTIF

L'analyse du workflow GitHub Actions a révélé **53 anomalie(s)** de sécurité avec un score global de **0/100** (Grade: **CRITIQUE**). Le niveau de risque est évalué comme **CRITIQUE**. Les anomalies critiques (21) et de haute sévérité (23) nécessitent une attention immédiate.

Top 5 des Catégories Problématiques

Catégorie	Nombre d'anomalies
Outils Réseau Suspects	7
URLs Suspectes	7
Cryptominage	7
Secrets et Credentials	6
Commandes Système Dangereuses	5

ANOMALIES DÉTAILLÉES

■ *ANOMALIES CRITICAL*

Job	Step	Type	Détail	Recommandation
network_and_exfiltration	Data exfiltration attempt	Commande suspecte détectée	Pattern data_exfiltration trouvé dans la commande	CRITIQUE: Examiner ces commandes, possibl
network_and_exfiltration	Data exfiltration attempt	Commande suspecte détectée	Pattern data_exfiltration trouvé dans la commande	CRITIQUE: Examiner ces commandes, possibl
network_and_exfiltration	Data exfiltration attempt	Commande suspecte détectée	Pattern data_exfiltration trouvé dans la commande	CRITIQUE: Examiner ces commandes, possibl
network_and_exfiltration	Data exfiltration attempt	Commande suspecte détectée	Pattern data_exfiltration trouvé dans la commande	CRITIQUE: Examiner ces commandes, possibl
backdoors_and_persistence	Create backdoor user	Commande suspecte détectée	Pattern backdoors trouvé dans la commande	CRITIQUE: Commandes de backdoor détectée
backdoors_and_persistence	Install persistence mechanisms	Commande suspecte détectée	Pattern backdoors trouvé dans la commande	CRITIQUE: Commandes de backdoor détectée
backdoors_and_persistence	Install persistence mechanisms	Commande suspecte détectée	Pattern backdoors trouvé dans la commande	CRITIQUE: Commandes de backdoor détectée
backdoors_and_persistence	Install persistence mechanisms	Commande suspecte détectée	Pattern backdoors trouvé dans la commande	CRITIQUE: Commandes de backdoor détectée
crypto_mining	Download mining software	Commande suspecte détectée	Pattern crypto_mining trouvé dans la commande	CRITIQUE: Activité de cryptominage détectée,
crypto_mining	Configure mining	Commande suspecte détectée	Pattern secrets trouvé dans la commande	Utiliser GitHub Secrets pour stocker les informa
crypto_mining	Configure mining	Commande suspecte détectée	Pattern crypto_mining trouvé dans la commande	CRITIQUE: Activité de cryptominage détectée,
crypto_mining	Configure mining	Commande suspecte détectée	Pattern crypto_mining trouvé dans la commande	CRITIQUE: Activité de cryptominage détectée,
crypto_mining	Configure mining	Commande suspecte détectée	Pattern crypto_mining trouvé dans la commande	CRITIQUE: Activité de cryptominage détectée,
crypto_mining	Configure mining	Commande suspecte détectée	Pattern crypto_mining trouvé dans la commande	CRITIQUE: Activité de cryptominage détectée,
poor_secrets_management	JWT token exposure	Commande suspecte détectée	Pattern secrets trouvé dans la commande	Utiliser GitHub Secrets pour stocker les informa
poor_secrets_management	JWT token exposure	Commande suspecte détectée	Pattern secrets trouvé dans la commande	Utiliser GitHub Secrets pour stocker les informa
poor_secrets_management	JWT token exposure	Commande suspecte détectée	Pattern secrets trouvé dans la commande	Utiliser GitHub Secrets pour stocker les informa
poor_secrets_management	JWT token exposure	Commande suspecte détectée	Pattern crypto_mining trouvé dans la commande	CRITIQUE: Activité de cryptominage détectée,
poor_secrets_management	Private key exposure	Commande suspecte détectée	Pattern secrets trouvé dans la commande	Utiliser GitHub Secrets pour stocker les informa
poor_secrets_management	Private key exposure	Commande suspecte détectée	Pattern secrets trouvé dans la commande	Utiliser GitHub Secrets pour stocker les informa
poor_secrets_management	Private key exposure	Commande suspecte détectée	Pattern crypto_mining trouvé dans la commande	CRITIQUE: Activité de cryptominage détectée,

■ *ANOMALIES HIGH*

Job	Step	Type	Détail	Recommandation
dangerous_system_commands	Dangerous file operations	Commande suspecte détectée	Pattern dangerous_commands trouvé dans la commande	Éviter les commandes système dangereuses, u
dangerous_system_commands	Dangerous file operations	Commande suspecte détectée	Pattern dangerous_commands trouvé dans la commande	Éviter les commandes système dangereuses, u
dangerous_system_commands	Dangerous file operations	Commande suspecte détectée	Pattern dangerous_commands trouvé dans la commande	Éviter les commandes système dangereuses, u
dangerous_system_commands	System service manipulation	Commande suspecte détectée	Pattern dangerous_commands trouvé dans la commande	Éviter les commandes système dangereuses, u
dangerous_system_commands	System service manipulation	Commande suspecte détectée	Pattern dangerous_commands trouvé dans la commande	Éviter les commandes système dangereuses, u
network_and_exfiltration	Network reconnaissance	Commande suspecte détectée	Pattern network_tools trouvé dans la commande	Éviter les outils réseau non essentiels, utiliser d
network_and_exfiltration	Network reconnaissance	Commande suspecte détectée	Pattern network_tools trouvé dans la commande	Éviter les outils réseau non essentiels, utiliser d
network_and_exfiltration	Data exfiltration attempt	URL suspecte	URL suspecte: http://malicious-site.com/upload	Vérifier la légitimité de l'URL
network_and_exfiltration	Data exfiltration attempt	URL suspecte	URL suspecte: http://attacker.com/collect	Vérifier la légitimité de l'URL
network_and_exfiltration	Data exfiltration attempt	Domaine suspect	Domaine suspect détecté: pastebin.com	Vérifier la légitimité de pastebin.com

network_and_exfiltration	Download and execute script	Commande suspecte détectée	Pattern network_tools trouvé dans la commande	Éviter les outils réseau non essentiels, utiliser d
network_and_exfiltration	Download and execute script	URL suspecte	URL suspecte: http://malicious-domain.com/shell.sh	Vérifier la légitimité de l'URL
backdoors_and_persistence	Install persistence mechanism	Commande suspecte détectée	Pattern network_tools trouvé dans la commande	Éviter les outils réseau non essentiels, utiliser d
insecure_protocols	HTTP downloads	URL suspecte	URL suspecte: http://insecure-site.com/setup.tar.gz	Vérifier la légitimité de l'URL
insecure_protocols	HTTP downloads	URL suspecte	URL suspecte: http://192.168.1.50/malicious.sh	Vérifier la légitimité de l'URL
reconnaissance_and_exploitation	SQL injection testing	URL suspecte	URL suspecte: http://target.com/login.php	Vérifier la légitimité de l'URL
reconnaissance_and_exploitation	Network scanning	Commande suspecte détectée	Pattern network_tools trouvé dans la commande	Éviter les outils réseau non essentiels, utiliser d
suspicious_domains	Suspicious file sharing	Commande suspecte détectée	Pattern network_tools trouvé dans la commande	Éviter les outils réseau non essentiels, utiliser d
suspicious_domains	Suspicious file sharing	Domaine suspect	Domaine suspect détecté: transfer.sh	Vérifier la légitimité de transfer.sh
suspicious_domains	Suspicious file sharing	Domaine suspect	Domaine suspect détecté: pastebin.com	Vérifier la légitimité de pastebin.com
suspicious_domains	URL shorteners and trackers	Domaine suspect	Domaine suspect détecté: bit.ly	Vérifier la légitimité de bit.ly
suspicious_domains	URL shorteners and trackers	Domaine suspect	Domaine suspect détecté: tinyurl.com	Vérifier la légitimité de tinyurl.com
suspicious_domains	Crypto mining pools	Commande suspecte détectée	Pattern network_tools trouvé dans la commande	Éviter les outils réseau non essentiels, utiliser d

■ *ANOMALIES MEDIUM*

Job	Step	Type	Détail	Recommandation
network_and_exfiltration	Download and execute script	URL suspecte	URL suspecte: https://192.168.1.100/backdoor.py	Vérifier la légitimité de l'URL
third_party_actions	Use suspicious third-party action	Action tierce	Action tierce utilisée: suspicious-org/malicious-action@main	Vérifier la réputation et épingler la version
third_party_actions	Use suspicious third-party action	Version non épinglée	Action avec version flottante: suspicious-org/malicious-action@main	Épingler à une version ou un hash spécifique
third_party_actions	Use unversioned action	Version non épinglée	Action avec version flottante: actions/setup-node@latest	Épingler à une version ou un hash spécifique
third_party_actions	Use floating version	Action tierce	Action tierce utilisée: some-org/deploy-action@master	Vérifier la réputation et épingler la version
third_party_actions	Use floating version	Version non épinglée	Action avec version flottante: some-org/deploy-action@master	Épingler à une version ou un hash spécifique
reconnaissance_and_exploitation	Exploitation tools usage	Commande suspecte détectée	Pattern reconnaissance trouvé dans la commande	Limiter l'utilisation d'outils de reconnaissance à
reconnaissance_and_exploitation	SQL injection testing	Commande suspecte détectée	Pattern reconnaissance trouvé dans la commande	Limiter l'utilisation d'outils de reconnaissance à
reconnaissance_and_exploitation	Network scanning	Commande suspecte détectée	Pattern reconnaissance trouvé dans la commande	Limiter l'utilisation d'outils de reconnaissance à