# 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

		_			1
Job	Step	Туре	Détail	Recommandation	ļ
network_and_exfilt	ration att	e <b>©pt</b> mmande suspecte détecte	ePattern data_exfiltration trouvé dans la	c@Riffa@de: Examiner ces commandes	possik
network_and_exfilt	ra <b>Det</b> a exfiltration at	e <b>ւմpt</b> mmande suspecte détecte	ePattern data_exfiltration trouvé dans la	contracte: Examiner ces commandes	possib
network_and_exfilt	ration att	e <b>ւմpt</b> mmande suspecte détecte	ePattern data_exfiltration trouvé dans la	contractue: Examiner ces commandes	possib
network_and_exfilt	ration att	e <b>ւմpt</b> mmande suspecte détecte	ePattern data_exfiltration trouvé dans la	continuous: Examiner ces commandes	possib
backdoors_and_pe	r <b>sûstearte</b> ebackdoor u	s&ommande suspecte détect	ePattern backdoors trouvé dans la comr	naû <b>Re</b> TIQUE: Commandes de backdoor	détecté
backdoors_and_pe	r <b>sissterilcp</b> ersistence	m <b>echamisno</b> se suspecte détecto	ePattern backdoors trouvé dans la comr	na <b>ଉୟ•</b> TIQUE: Commandes de backdoor	détecté
backdoors_and_pe	r <b>sisterice</b> ersistence	m <b>echamisno</b> s suspecte détecto	ePattern backdoors trouvé dans la comr	naû <b>Re</b> TIQUE: Commandes de backdoor	détecté
backdoors_and_pe	r <b>sissterilcp</b> ersistence	m <b>echamisno</b> se suspecte détecto	ePattern backdoors trouvé dans la comr	na <b>ଉୟ</b> •TIQUE: Commandes de backdoor	détecté
crypto_mining	Download mining s	ofDwarmande suspecte détect	ePattern crypto_mining trouvé dans la c	on <b>մ RaTit@</b> UE: Activité de cryptominage d	étectée
crypto_mining	Configure mining	Commande suspecte détecte	ePattern secrets trouvé dans la commar	deltiliser GitHub Secrets pour stocker les	inform
crypto_mining	Configure mining	Commande suspecte détecte	ePattern crypto_mining trouvé dans la c	on Ratiko UE: Activité de cryptominage d	étectée
crypto_mining	Configure mining	Commande suspecte détecte	ePattern crypto_mining trouvé dans la c	on <b>RaTik@</b> UE: Activité de cryptominage d	étectée
crypto_mining	Configure mining	Commande suspecte détecte	ePattern crypto_mining trouvé dans la c	on@Rant@UE: Activité de cryptominage d	étectée
crypto_mining	Configure mining	Commande suspecte détecte	ePattern crypto_mining trouvé dans la c	on@Rant@UE: Activité de cryptominage d	étectée
poor_secrets_man	a <b>glennietu</b> ken exposu	reCommande suspecte détecte	ePattern secrets trouvé dans la commar	deltiliser GitHub Secrets pour stocker les	inform
poor_secrets_man	a <b>glennietu</b> ken exposu	reCommande suspecte détecte	ePattern secrets trouvé dans la commar	deltiliser GitHub Secrets pour stocker les	inform
poor_secrets_man	a <b>glennietu</b> ken exposu	reCommande suspecte détecte	ePattern secrets trouvé dans la commar	deltiliser GitHub Secrets pour stocker les	inform
poor_secrets_man	agleMiTetotken exposu	reCommande suspecte détecte	ePattern crypto_mining trouvé dans la c	on <b>ាកងកែលេ</b> UE: Activité de cryptominage d	étectée
poor_secrets_man	а <b>фтімен</b> ы key exposu	r€ommande suspecte détecte	ePattern secrets trouvé dans la commar	deltiliser GitHub Secrets pour stocker les	inform
poor_secrets_man	a <b>⊕rinete</b> t key exposu	r€ommande suspecte détecte	ePattern secrets trouvé dans la commar	deltiliser GitHub Secrets pour stocker les	inform
poor_secrets_man	a <b>g⊕rinæte</b> t key exposu	r€ommande suspecte détecte	ePattern crypto_mining trouvé dans la c	on@RaTit@UE: Activité de cryptominage d	étectée

### **■** ANOMALIES HIGH

Job	Step	Туре	Détail	Recommandation	
dangerous_system	_Comgenods file ope	rationsmande suspecte détecte	ePattern dangerous_commands trouvé	da <mark>Ésiterdesnowmoha</mark> ndes système dangereus	es,
dangerous_system	_Comgenods file ope	rationsmande suspecte détecte	ePattern dangerous_commands trouvé	da <mark>Ésiterdesnowmoha</mark> ndes système dangereus	es,
dangerous_system	_Cangerods file ope	rationsmande suspecte détecte	ePattern dangerous_commands trouvé	da <mark>lbsiterdesnowmohandes système danger</mark> eus	es,
dangerous_system	_ <b>6cystemansder</b> vice ma	nipalatinande suspecte détecte	ePattern dangerous_commands trouvé	da <mark>lbsiterdesnowmohandes système danger</mark> eus	es,
dangerous_system	_ <b>6cystemansder</b> vice ma	nipalatinande suspecte détecte	ePattern dangerous_commands trouvé	da <mark>lbsiterdesnowmohandes système danger</mark> eus	es,
network_and_exfilt	ratietwork reconnais	saccommande suspecte détecte	ePattern network_tools trouvé dans la co	ntimiaendles outils réseau non essentiels, utili	ser
network_and_exfilt	ratietwork reconnais	saccommande suspecte détecte	ePattern network_tools trouvé dans la co	ntimiaendles outils réseau non essentiels, utili	ser
network_and_exfilt	ration att	entd PatL suspecte	URL suspecte: http://malicious-site.com	n/u\particle de l'URL	
network_and_exfilt	ration att	entd PatL suspecte	URL suspecte: http://attacker.com/colle	ctVérifier la légitimité de l'URL	
network_and_exfilt	ration att	eliptmaine suspect	Domaine suspect détecté: pastebin.com	n Vérifier la légitimité de pastebin.com	

network_and_exfil ratiownload and executes income suspected electric electric relationship and executes income suspected electric electric relationship and executes income suspected electric electric relationship and executes income suspected electric relationship and executes income suspected electric relationship and executes income suspected electric relationship and executes in the commitment of the c						-
backdoors_and_persistence mechanisms suspecte détecte ePattern network_tools trouvé dans la confirmiseules outils réseau non essentiels, utiliser insecure_protocols HTTP downloads URL suspecte URL suspecte: http://insecure-site.com/sivisifice/datagisonité de l'URL insecure_protocols HTTP downloads URL suspecte URL suspecte: http://laget.com/login.ph/Vérifier la légitimité de l'URL reconnaissance_ands@xplojestion testingURL suspecte URL suspecte: http://target.com/login.ph/Vérifier la légitimité de l'URL reconnaissance_ands@xplojestion testingURL suspecte détecteePattern network_tools trouvé dans la confirmiseulles outils réseau non essentiels, suspicious_domainsSuspicious file sharingpmaine suspect détecteePattern network_tools trouvé dans la confirmiseulles outils réseau non essentiels, utiliser suspicious_domainsSuspicious file sharingpmaine suspect Domaine suspect détecté: transfer.sh Vérifier la légitimité de transfer.sh suspicious_domainsSuspicious file sharingpmaine suspect Domaine suspect détecté: pastebin.com Vérifier la légitimité de pastebin.com suspicious_domainsURL shorteners ar dibrardeine suspect Domaine suspect détecté: bit.ly Vérifier la légitimité de tinyurl.com	network_and_exfil	ratiownload and exe	cu <b>Cersunspiraleususprept</b> e détecte	ePattern network_tools trouvé dans la c	ontinitaendles outils réseau non essentiels,	utiliser
insecure_protocols HTTP downloads URL suspecte URL suspecte: http://insecure-site.com/se/resifice/lda/egitismité de l'URL insecure_protocols HTTP downloads URL suspecte URL suspecte: http://192.168.1.50/malicit/resifice/lda/egitismité de l'URL reconnaissance_and_exploijteation testingURL suspecte URL suspecte: http://target.com/login.ph/e/rifier la légitimité de l'URL reconnaissance_and_exploijteation testingURL suspecte URL suspecte: http://target.com/login.ph/e/rifier la légitimité de l'URL reconnaissance_and_exploijteation testingURL suspecte détecteePattern network_tools trouvé dans la confirmitaenclies outils réseau non essentiels, utiliser suspicious_domainsSuspicious file sharingumaine suspect Domaine suspect détecté: transfer.sh Vérifier la légitimité de transfer.sh suspicious_domainsSuspicious file sharingumaine suspect Domaine suspect détecté: pastebin.com Vérifier la légitimité de pastebin.com suspicious_domainsURL shorteners and @marckeinse suspect Domaine suspect détecté: bit.ly Vérifier la légitimité de bit.ly suspicious_domainsURL shorteners and @marckeinse suspect Domaine suspect détecté: tinyurl.com Vérifier la légitimité de tinyurl.com	network_and_exfile	ratiownload and exe	cululeR Leusupsipie cutse script	URL suspecte: http://malicious-domain	conférifietala. Ségitimité de l'URL	
insecure_protocols HTTP downloads URL suspecte URL suspecte: http://192.168.1.50/malicit/desifiparylla-aérigistimité de l'URL reconnaissance_and_exploiteation testingURL suspecte URL suspecte: http://target.com/login.php/erifier la légitimité de l'URL reconnaissance_and_exploiteation testingURL suspecte détecteePattern network_tools trouvé dans la confirmitaencles outils réseau non essentiels, utiliser suspicious_domainsSuspicious file sharin@pmande suspecte détecteePattern network_tools trouvé dans la confirmitaencles outils réseau non essentiels, utiliser suspicious_domainsSuspicious file sharin@pmaine suspect  Domaine suspect détecté: transfer.sh  Vérifier la légitimité de transfer.sh suspicious_domainsSuspicious file sharin@pmaine suspect  Domaine suspect détecté: pastebin.com Vérifier la légitimité de pastebin.com suspicious_domainsURL shorteners ar dibrancleins suspect  Domaine suspect détecté: bit.ly  Vérifier la légitimité de bit.ly suspicious_domainsURL shorteners ar dibrancleins suspect  Domaine suspect détecté: tinyurl.com  Vérifier la légitimité de tinyurl.com	backdoors_and_pe	r <b>sinatalice</b> ersistence	m <b>echamisno</b> se suspecte détecte	ePattern network_tools trouvé dans la c	ontinialendles outils réseau non essentiels,	utiliser
reconnaissance_a nd @kpliojteation testingURL suspecte  URL suspecte: http://target.com/login.phi/erifier la légitimité de l'URL  reconnaissance_a nd let provide le suspecte détecte e Pattern network_tools trouvé dans la confinite des outils réseau non essentiels, utiliser suspicious_domain sSuspicious file shari @pmmande suspecte détecte e Pattern network_tools trouvé dans la confinite des outils réseau non essentiels, utiliser suspicious_domain sSuspicious file shari @pmaine suspect  Domaine suspect détecté: transfer.sh  Vérifier la légitimité de transfer.sh  suspicious_domain sSuspicious file shari @pmaine suspect  Domaine suspect détecté: pastebin.com Vérifier la légitimité de pastebin.com  suspicious_domain sURL shorteners ar di @pacteine suspect  Domaine suspect détecté: bit.ly  Vérifier la légitimité de bit.ly  suspicious_domain sURL shorteners ar di @pacteine suspect  Domaine suspect détecté: tinyurl.com  Vérifier la légitimité de tinyurl.com	insecure_protocols	HTTP downloads	URL suspecte	URL suspecte: http://insecure-site.com	/s&/réssifiee-lelaléegijsiomité de l'URL	
reconnaissance_and_ewptorkasticamning Commande suspecte détecteePattern network_tools trouvé dans la continuite de soutils réseau non essentiels, utiliser suspicious_domain sSuspicious file sharin@pmaine suspect détecteePattern network_tools trouvé dans la continuite de transfer.sh utiliser suspicious_domain sSuspicious file sharin@pmaine suspect Domaine suspect détecté: transfer.sh Vérifier la légitimité de transfer.sh suspicious_domain sSuspicious file sharin@pmaine suspect Domaine suspect détecté: pastebin.com Vérifier la légitimité de pastebin.com suspicious_domain sURL shorteners ar dibrarckeinse suspect Domaine suspect détecté: bit.ly Vérifier la légitimité de bit.ly suspicious_domain sURL shorteners ar dibrarckeinse suspect Domaine suspect détecté: tinyurl.com Vérifier la légitimité de tinyurl.com	insecure_protocols	HTTP downloads	URL suspecte	URL suspecte: http://192.168.1.50/mal	cit/ésifiæryllæægstimité de l'URL	
suspicious_domainsSuspicious file sharin@pmmande suspecte détecteePattern network_tools trouvé dans la continuide de transfer.sh suspicious_domainsSuspicious file sharin@pmaine suspect Domaine suspect détecté: transfer.sh Vérifier la légitimité de transfer.sh suspicious_domainsSuspicious file sharin@pmaine suspect Domaine suspect détecté: pastebin.com Vérifier la légitimité de pastebin.com suspicious_domainsURL shorteners ar ditransferse suspect Domaine suspect détecté: bit.ly Vérifier la légitimité de bit.ly suspicious_domainsURL shorteners ar ditransferse suspect Domaine suspect détecté: tinyurl.com Vérifier la légitimité de tinyurl.com	reconnaissance_a	nc <u>S</u> @kpilojieatiiom testi	ngURL suspecte	URL suspecte: http://target.com/login.p	hp/érifier la légitimité de l'URL	
suspicious_domainsSuspicious file sharin@pmaine suspect  Domaine suspect détecté: transfer.sh  Vérifier la légitimité de transfer.sh  suspicious_domainsSuspicious file sharin@pmaine suspect  Domaine suspect détecté: pastebin.com Vérifier la légitimité de pastebin.com  suspicious_domainsURL shorteners ar dibrarckeinse suspect  Domaine suspect détecté: bit.ly  Vérifier la légitimité de bit.ly  suspicious_domainsURL shorteners ar dibrarckeinse suspect  Domaine suspect détecté: tinyurl.com  Vérifier la légitimité de tinyurl.com	reconnaissance_a	nd <u>N</u> etwpoorktasticamning	Commande suspecte détecte	ePattern network_tools trouvé dans la c	ntimitandes outils réseau non essentiels,	utiliser
suspicious_domainsURL shorteners ar dibrarckeinse suspect  Domaine suspect détecté: pastebin.com Vérifier la légitimité de pastebin.com  Vérifier la légitimité de pastebin.com  Domaine suspect détecté: bit.ly  Vérifier la légitimité de bit.ly  Suspicious_domainsURL shorteners ar dibrarckeinse suspect  Domaine suspect détecté: tinyurl.com  Vérifier la légitimité de tinyurl.com	suspicious_domaii	sSuspicious file sha	rit@mmande suspecte détecte	ePattern network_tools trouvé dans la c	ontimiaendes outils réseau non essentiels,	utiliser
suspicious_domainsURL shorteners ar dibrarckeinse suspect Domaine suspect détecté: bit.ly Vérifier la légitimité de bit.ly suspicious_domainsURL shorteners ar dibrarckeinse suspect Domaine suspect détecté: tinyurl.com Vérifier la légitimité de tinyurl.com	suspicious_domaii	sSuspicious file sha	rin@pmaine suspect	Domaine suspect détecté: transfer.sh	Vérifier la légitimité de transfer.sh	
suspicious_domainsURL shorteners ar dibrarckeinse suspect Domaine suspect détecté: tinyurl.com Vérifier la légitimité de tinyurl.com	suspicious_domaii	sSuspicious file sha	rin@pmaine suspect	Domaine suspect détecté: pastebin.com	n Vérifier la légitimité de pastebin.com	
	suspicious_domaii	sURL shorteners ar	d Drandkeinse suspect	Domaine suspect détecté: bit.ly	Vérifier la légitimité de bit.ly	
suspicious_domainsCrypto mining poo s Commande suspecte détecteePattern network_tools trouvé dans la continuidement outils réseau non essentiels, utiliser	suspicious_domaii	sURL shorteners ar	d Drandkeinse suspect	Domaine suspect détecté: tinyurl.com	Vérifier la légitimité de tinyurl.com	
	suspicious_domaii	sCrypto mining poo	s Commande suspecte détecte	ePattern network_tools trouvé dans la c	on trivitale des outils réseau non essentiels,	utiliser

### **■** ANOMALIES MEDIUM

Job	Step	Туре	Détail	Recommandation	
network_and_exfile	ratiownload and exe	ecululeRsusupsipiecuse script	URL suspecte: https://192.168.1.100/ba	ac <b>kéditiepl</b> a légitimité de l'URL	
third_party_actions	S Use suspicious thir	d-Apatitynalistice	Action tierce utilisée: suspicious-org/ma	alibléruiseadaioné@untaation et épingler la versor	nc
third_party_actions	Use suspicious thi	ird- <b>√cansijoaotion</b> épinglée	Action avec version flottante: suspiciou	u <mark>s-Époj/ng kelicảo wuse</mark> avo <del>tios i</del> w@no a ion hash spé <mark>c</mark> ifi	ifique
third_party_actions	Use unversioned a	actioersion non épinglée	Action avec version flottante: actions/s/	etu <del>lipinoglar@latest</del> version ou un hash spé <b>c</b> ifi	ifique
third_party_actions	s Use floating version	n Action tierce	Action tierce utilisée: some-org/deploy-	-actiénit@mlasteprutation et épingler la vers or	nc
third_party_actions	Use floating versio	on Version non épinglée	Action avec version flottante: some-org	g/d <b>éplog+actionn@manstion</b> ou un hash spé <b>c</b> ifi	ifique
reconnaissance_a	nd <u>Sexplibitatiols</u> usaç	eCommande suspecte détecte	ePattern reconnaissance trouvé dans la	a couinmitandetilisation d'outils de reconnaissa	ance
reconnaissance_a	nd <u>S@kpilojiteetiion</u> testi	ngCommande suspecte détecté	ePattern reconnaissance trouvé dans la	a couinmitandetilisation d'outils de reconnaissa	ance
reconnaissance_a	nd <u>N</u> etwpoorktasticamning	Commande suspecte détecte	ePattern reconnaissance trouvé dans la	a committendetilisation d'outils de reconnaissa	ance