


Strengthen your vendor ecosystem through external threat detection and digital risk protection

 **High**

Vulnerability Exploit
CloudSecurity
CyberAttack
DataBreach
SupplyChainAttacks

GhostAction Supply Chain Attack Exposes GitHub Secrets

Created September 06, 2025 at 09:23 AM, last updated September 10, 2025 at 04:15 PM

Overview
What to do
1 IoC
7 TTPs
11 Sources






The GhostAction supply chain attack on GitHub exploited compromised GitHub Actions workflows to exfiltrate over 3,325 secrets, including tokens and passwords, affecting 327 users across 817 repositories. This attack highlights the critical need for securing CI/CD pipelines and monitoring for unauthorized changes.

Timeline 12 updates, 3 with relevant findings
Only updates to CVEs and IoCs are notified.

☒ Show only relevant findings

New last finding on 09/10/2025 at 04:15 PM

GhostAction attack update: Salesloft GitHub account compromised, impacting Cloudflare, Zscaler; new AI-based SIngularity attack identified. [Tecmundo](#)

 Malware: **Ghostaction, SIngularity**
 Target industry: **All**
 Target organization: **PyPI, npm, GitHub, Salesloft, Salesforce, Cloudflare, Zscaler, Palo Alto Networks, PagerDuty**
 The GhostAction attack was first detected on September 5, 2025, while the SIngularity malware activity was noted between August 26 and August 31, 2025.
 All impacted assets

Modern supply chains are highly interconnected. Vendors and partners often have privileged access to critical systems, making them prime targets for attackers.

With continuous monitoring, automated response workflows, and AI that prioritizes the most relevant threats, Axur strengthens resilience across the entire supply chain, ensuring your business remains prepared for the evolving external threat landscape.



Detect threats before they escalate into incidents



Accelerate response to vendor-related incidents



Ensure compliance while reducing operational risk

Why this matters for vendor risk

External monitoring

Continuously scans the surface, deep, and dark web for vendor mentions, phishing attempts, impersonations, and leaked credentials.

AI-powered intelligence

Automates up to 86% of threat management, prioritizing the most critical vulnerabilities in third-party systems and networks.

Brand protection

Protects your brand from misuse via compromised vendors, reducing reputational risk and strengthening customer trust across the ecosystem.

Third-party vendors often have access to sensitive systems or data. A breach in their environment can ripple through your entire supply chain. Axur's approach helps you with:

Automated response

Real-time alerts and takedown workflows neutralize risks quickly, seamlessly integrating with ServiceNow and Splunk for incident management.

API & Integrations

APIs, webhooks, and custom feeds connect Axur to your security stack, enabling tailored monitoring of vendors and automated workflows.

Threat Hunting

Proactively investigates third-party risks such as leaked credentials and malicious domains before they escalate into supply chain incidents.

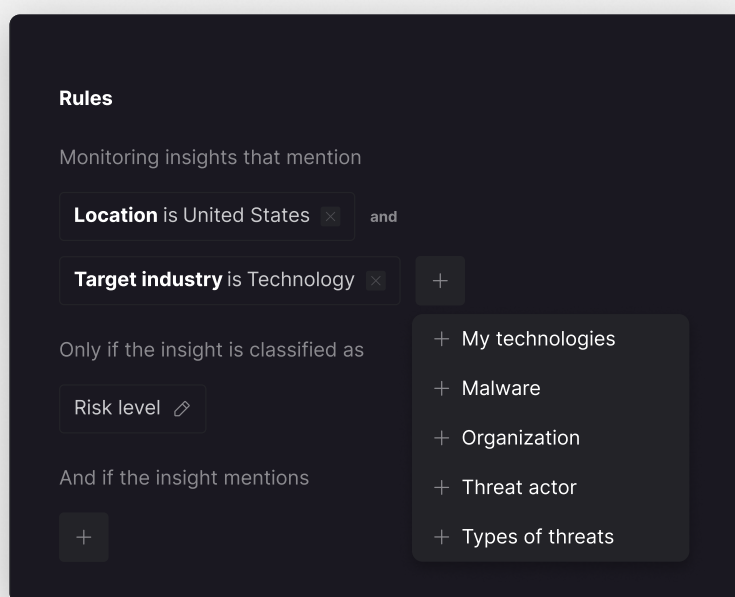
Extend your threat visibility with Axur AI-powered CTI

Third-party asset monitoring

Monitor sources for attacks affecting vendors, gaining early alerts on ransomware, cyber attacks or malware incidents that could impact your supply chain.

Vulnerabilities

Track CVEs and exploited flaws linked to third-party technologies and suppliers, helping you prioritize responses and reduce risks.



Stay ahead of third-party risks with Axur

GET A DEMO



Gartner Peer Insights 4.9 ★★★★★

Discover all our solutions at axur.com

///AXUR