

# Fortalezca su ecosistema de proveedores con inteligencia de amenazas y protección contra riesgos digitales

🔥 High
Vulnerability Exploit
CloudSecurity
CyberAttack
DataBreach

## El ataque a la cadena de suministro de GhostAction expone los secretos de GitHub

Creado el 06 de Septiembre de 2025 a las 09:23, última actualización el 10 de Septiembre de 2025 a las 16:15

**Visión general**
Qué hacer
1 IoC
7 TTPs
11 Fuentes

---

El ataque a la cadena de suministro de GhostAction en GitHub aprovechó los flujos de trabajo comprometidos de GitHub Actions para filtrar más de 3.325 secretos, incluidos tokens y contraseñas, que afectaron a 327 usuarios en 817 repositorios. Este ataque pone de manifiesto la necesidad imperiosa de proteger las canalizaciones de CI/CD y supervisar los cambios no autorizados.

**Línea de tiempo** 12 actualizaciones, 3 con hallazgos relevantes

Solo se notifican actualizaciones sobre CVE e IOC.

Mostrar solo hallazgos relevantes

● Nuevo último hallazgo en 10/09/2025 a las 16:15

Actualización del ataque de GhostAction: la cuenta GitHub de

🛡️ Malware: **Ghostaction, S1ngularity**

🏢 Industria destinataria: **Todas**

🏢 Organización destinataria: **PyPI, npm, GitHub, Salesloft, Salesforce, Cloudflare, Zscaler, Palo Alto Networks, PagerDuty**

📅 El ataque GhostAction se detectó por primera vez el 5 de septiembre de 2025, mientras que la actividad del malware S1ngularity se observó entre el 26 y el 31 de agosto de 2025.

Las supply chains modernas son altamente interconectadas. Los proveedores y socios suelen tener acceso privilegiado a sistemas críticos, lo que los convierte en objetivos preferentes para los atacantes.

Con monitoreo continuo, flujos de respuesta automatizados e IA que prioriza las amenazas más relevantes, Axur refuerza la resiliencia en toda la supply chain, asegurando que su empresa esté siempre preparada frente a un panorama externo de amenazas en constante evolución.



Detecte amenazas antes de que se conviertan en incidentes



Responda más rápido a incidentes de proveedores



Asegure el cumplimiento y reduzca riesgos operativos

# Por qué esto importa para la seguridad

## Monitoreo externo

Explora de forma continua la surface, deep y dark web en busca de menciones a proveedores, intentos de phishing, suplantaciones y credenciales filtradas.

## Inteligência com IA

Automatiza hasta el 86% de la gestión de amenazas, priorizando las vulnerabilidades más críticas en sistemas y redes de terceros.

## Proteção de marca

Protege su marca frente al uso indebido a través de proveedores comprometidos, reduciendo el riesgo reputacional y fortaleciendo la confianza de los clientes en todo el ecosistema.

# Amplíe su visibilidad con el CTI de Axur potenciado por IA

## ➔ Monitoreo de activos de terceros

Monitoree fuentes de ataques que afectan a proveedores, recibiendo alertas tempranas sobre incidentes de ransomware, ciberataques o malware que pueden impactar su supply chain.

## ➔ Vulnerabilities

Haga un seguimiento de CVEs y fallas explotadas en tecnologías y proveedores externos, lo que le ayuda a priorizar respuestas y reducir riesgos.

Muchos terceros tienen acceso a sistemas o datos sensibles. Una brecha en su entorno puede impactar a toda su supply chain. El enfoque de Axur le ayuda con:

## Respuesta automatizada

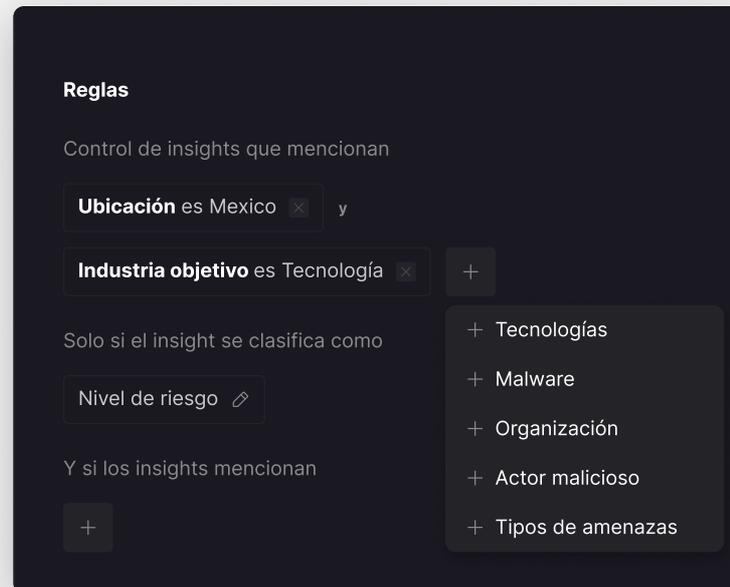
Alertas en tiempo real y flujos de takedown neutralizan riesgos rápidamente, integrándose de manera nativa con ServiceNow y Splunk para la gestión de incidentes.

## API & Integrações

APIs, webhooks y feeds personalizados conectan a Axur con su security stack, permitiendo un monitoreo adaptado de proveedores.

## Threat Hunting

Investiga proactivamente riesgos de terceros, como credenciales filtradas y dominios maliciosos, antes de que escalen a incidentes en la supply chain.



# Anticípese a los riesgos de terceros con Axur

AGENDE UNA DEMO



Gartner Peer Insights 4.9 ★★★★★