

# Fortaleça seu ecossistema de fornecedores com threat intelligence e proteção contra riscos digitais

High Vulnerability Exploit CloudSecurity CyberAttack DataBreach

## O ataque à cadeia de suprimentos do GhostAction expõe os segredos do GitHub

Criado em 06 de Setembro de 2025 às 09:23, última atualização em 10 de Setembro de 2025 às 16:15

Visão geral O que fazer 1 IoC 7 TTPs 11 Fontes

O ataque à cadeia de suprimentos do GhostAction no GitHub explorou fluxos de trabalho comprometidos do GitHub Actions para exfiltrar mais de 3.325 segredos, incluindo tokens e senhas, afetando 327 usuários em 817 repositórios. Esse ataque destaca a necessidade crítica de proteger os pipelines de CI/CD e monitorar alterações não autorizadas.

Malware: **Ghostaction, S1ngularity**

Indústria alvo: **Todos**

Organização alvo: **PyPI, npm, GitHub, Salesloft, Salesforce, Cloudflare, Zscaler, Palo Alto Networks, PagerDuty**

O ataque GhostAction foi detectado pela primeira vez em 5 de setembro de 2025, enquanto a atividade do malware S1ngularity foi observada entre 26 e 31 de agosto de 2025.

### Linha do tempo

12 atualizações, 3 com descobertas relevantes

Apenas atualizações em CVEs e IoCs serão notificadas.

Mostrar apenas descoberta relevantes

Nova última descoberta em 10/09/2025 às 16:15

Atualização do ataque GhostAction: conta do Salesloft GitHub comprometida, afetando Cloudflare, Zscaler; novo ataque

As supply chains modernas são altamente interconectadas. Fornecedores e parceiros frequentemente têm acesso privilegiado a sistemas críticos, tornando-se alvos preferenciais para atacantes.

Com monitoramento contínuo, fluxos de resposta automatizados e IA que prioriza as ameaças mais relevantes, a Axur fortalece a resiliência em toda a cadeia de fornecedores, garantindo que sua empresa esteja sempre preparada para o cenário em constante evolução de ameaças externas.



Detecte ameaças antes de virarem incidentes



Responda mais rápido a incidentes de supply chain



Assegure conformidade e reduza riscos associados

# Por que isso importa para a segurança

## Monitoramento externo

Faz varreduras contínuas na surface, deep e dark web em busca de menções a fornecedores, tentativas de phishing, fraudes e dados expostos.

## Inteligência com IA

Automatiza até 86% do gerenciamento de ameaças, priorizando as vulnerabilidades mais críticas em sistemas e redes de terceiros.

## Proteção de marca

Protege sua marca contra uso indevido por fornecedores comprometidos, reduzindo o risco reputacional e fortalecendo a confiança dos clientes em todo o ecossistema.

# Amplie sua visibilidade com o CTI da Axur, impulsionado por IA

## ➔ Monitoramento de ativos de terceiros

Monitore fontes de ataques que afetam terceiros, recebendo alertas antecipados sobre ransomware, ciberataques ou incidentes de malware que podem impactar sua cadeia de fornecedores.

## ➔ Vulnerabilidades

Acompanhe CVEs e falhas exploradas em tecnologias e fornecedores terceirizados, ajudando a priorizar respostas e reduzir riscos.

Muitos terceiros têm acesso a sistemas ou dados sensíveis. Uma falha no ambiente deles pode impactar todo seu ecossistema. A abordagem da Axur ajuda você com:

## Resposta automatizada

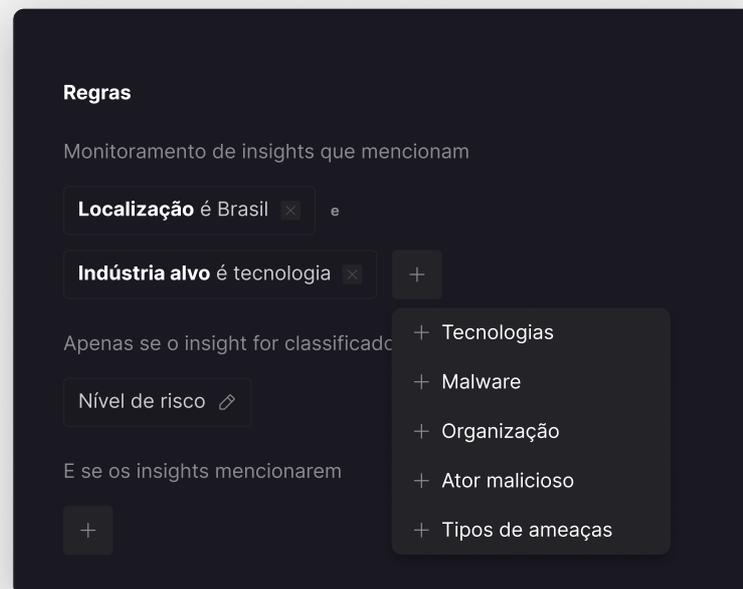
Alertas em tempo real e fluxos de takedown neutralizam riscos rapidamente, integrando-se de forma nativa ao ServiceNow e Splunk para gestão de incidentes.

## API & Integrações

APIs, webhooks e feeds conectam a Axur ao seu stack de segurança, permitindo monitoramento sob medida de fornecedores.

## Threat Hunting

Investiga proativamente riscos de terceiros, como credenciais vazadas e domínios maliciosos, antes que evoluam para incidentes na supply chain.



Esteja à frente dos riscos de terceiros com a Axur

AGENDE UMA DEMO



Gartner Peer Insights 4.9 ★★★★★

Descubra todas as nossas soluções em [axur.com](https://axur.com)

**AXUR**