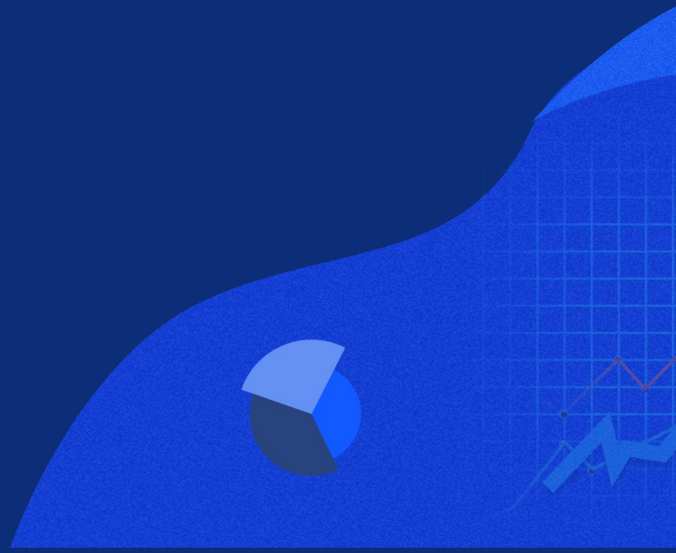
Zero-Days Without the Fire Drill

Adam Arellano
Field CTO @ Harness



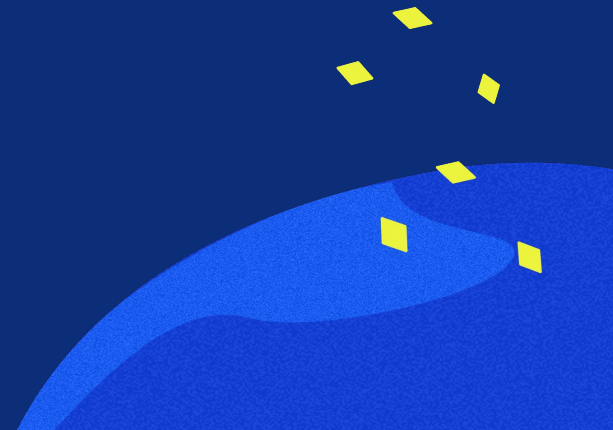
About Me

EngineeringX
Sponsored by harness

- Pacifist
- US Marine 2002-2016
- Company Commander
- Social Worker
- CTO/CISO(ish) MCRC
- FedRAMP @ Salesforce
- CISO(ish) @ Veritone
- CISO (fureal) @ Binti
- VP Enterprise Cyber PayPal
- Field CTO Traceable/Harness

Background

- Anthropic Mythos
- Project Glasswing



Recommendations

- Pre-position high-visibility incident response
- Plan for your dependencies and dependents
- Shared roadmap and accountability with Eng/Infra/Security
- Executive level awareness and accountability

Company

- Build with breach assumed
- Find bugs before you ship code
- Shorten patch/change cycles
- Plan for your dependencies and dependents
- Establish a surge defense capability
- Engineer and build for resilience and **simplicity**

Eng/Infra

- Leverage AI to do de-toil high calorie activities
- Automate technical incident response pipeline

Security

Company Level Actions

- Pre-position high-visibility incident response
  - Pre-approved and crafted messaging triggered by established conditions
- Plan for your dependencies and dependents
  - Know your software dependencies and who to contact in emergencies
  - Know who you need to contact should you have issues
- Shared roadmap and accountability with Eng/Infra/Security
  - These must be crafted jointly with clear responsibility per action item
- Executive level awareness and accountability
  - Preparations should be treated like new features
  - Customers may even be made aware of the uplift
  - Every executive and corresponding team will likely be affected/tasked

Engineering Specifc Actions

- Shorten patch/change cycles
  - Single most important metric, how quickly can you safely make changes
- Find bugs before you ship code
  - SAST, SCA, auto-pen test, prefer memory safe code lang, secure pipeline
- Build with breach assumed
  - Zero-trust, isolate services by identity, short lived tokens by default
- Plan for your dependencies and dependents
  - Same as the company task + technical work-arounds when your providers or you have issues
- Establish a surge defense capability
  - When faced with a severe or esp dangeroud situation, have a SWAT established with pre-approved authority, budget, and SOP across domains/teams and even outside help
- Engineer and build for resilience and **simplicity**
  - Audit your current code base and reduce dependencies, standardize on know good services andn libraries
  - **Reduce** and inventory what you expose

Security Specific Actions

- Leverage AI to do de-toil high calorie activities
  - Put a model in front of your alert queue and test it regularly
  - Triage and prioritization of scan findings
  - Ticket ops automation, etc.
- Automate technical incident response pipeline
  - Automate the bookkeeping around incidents, decisions should be made with assistance at most
  - Find places to leverage AI and accelerate the time between incident and resolution

Links and References

- https://www.anthropic.com/glasswing
- https://red.anthropic.com/2026/mythos-preview/ (bottom of page)
- https://claude.com/blog/preparing-your-security-program-for-ai-accelerated-offense
- https://www.leadershipincyber.com/blog/attack-surface-diet
-

EngineeringX
Sponsored by harness

Thank You