Tuskira

Meet Quell

Close the Zero-Day Exposure Window Before Exploitation

Quell is Tuskira's exposure-led zero-day defense capability that helps enterprises survive the period between disclosure and patch through continuous validation and compensating controls. Unlike traditional zero-day response that starts with the vulnerability, Quell starts with exposure: determining whether the vulnerability creates a reachable path to compromise in your environment. When a zero-day emerges, Quell identifies which exposures create a viable path to breach, validates whether existing controls would stop exploitation, and orchestrates the highest-leverage compensating control change through the tools you already own (EDR, firewall, IAM, WAF, SIEM), with analyst approval where policy requires.

> THE QUESTION MOST VULNERABILITY TOOLS NEVER ANSWER
>
> **Does my stack block this?**

WHY NOW

The Patch Window Has Collapsed

In the first month of Anthropic's Project Glasswing, a single Mythos-class AI model helped partners uncover more than 10,000 high- and critical-severity flaws in widely used code, with the disclosure-to-weaponization window now measured in minutes. Any defense that still depends on a patch cycle is already behind. What survives the window is not faster patching but faster mitigation through the controls you already run.

PROJECT GLASSWING, MONTH ONE

10,000+

High- & critical-severity flaws uncovered by a single AI model

DISCLOSURE → WEAPONIZATION

Weeks → Minutes

for AI-discovered exploits in the post-Mythos era

Market Alternative	Where They Stop	How Quell Is Different
Vulnerability scanners / VM tools	Rank CVEs by CVSS severity, with no view of what is reachable or whether existing controls would stop it.	**Scores each exposure by whether it opens a reachable path, whether existing controls would stop it, and which compensating control change closes the path.**
Exposure management tools	Score "behind existing controls" as a factor that reduces risk, without testing whether the control would stop this exploit.	**Tests every modeled attack path against the live state of your compensating controls, surfacing the silent bypasses any scoring model would miss.**
Threat intel & manual zero-day response	Produce indicators and advisories that teams operationalize by hand.	**Continuously converts live attack-path intelligence into compensating control changes that disrupt exploitation.**
Patch cycles & manual zero-day triage	Wait for a patch window, or assess scope by hand when a zero-day breaks.	**Hunts affected assets, pinpoints undefended exposure, and orchestrates the mitigating control change in hours.**

How Quell Converts Exposure Into Continuous Defense

1. **Unify Exposure Signals** — Normalize exposure, identity, cloud, endpoint & control telemetry into the Security Context Graph.
2. **Model Breachability** — Build a continuously updated digital twin of reachability and exploitability, grounded in business context.
3. **Identify Reachable Zero-Days** — Surface the disclosed zero-days that open a reachable path to compromise.
4. **Validate Defensive Gaps** — Test whether the controls you already run would stop exploitation, or are bypassed undetected.
5. **Deploy Compensating Controls** — Orchestrate the compensating control change that closes the path through existing controls, with analyst approval where policy requires. No patch required.
6. **Continuously Revalidate** — Confirm the exploit can no longer reach a target, not that a ticket was marked done.

Exposures & zero-days Quell defends against

Exposure / Scenario	Example	What Quell Determines	How Quell Mitigates It
Internet-exposed appliance zero-day	Edge VPN / appliance zero-day under active exploitation (e.g., Ivanti-class CVE)	Whether the appliance opens a reachable path to production, and whether WAF/EDR controls would block the exploit	**Orchestrates a virtual-patch / WAF rule and EDR block through existing controls in hours, before a patch exists.**
AI-discovered zero-day	Weaponized before patch guidance exists (a Mythos-class discovery)	Which assets run the affected component, and which are undefended versus already covered	**Orchestrates the compensating control change that closes the path before any patch guidance lands.**
Exploitable exposure behind a bypassed control	High-impact exposure on a host where the EDR policy is misconfigured or bypassed undetected	That the control would not stop exploitation: "covered on paper," breachable in practice	**Corrects the control gap and revalidates that exploitation is blocked.**
Identity-amplified attack path	Exploitable workload reachable via an over-privileged identity to crown-jewel data	That the exposure sits on a reachable path amplified by identity, not an isolated finding	**Closes the highest-leverage chokepoint (IAM policy or segmentation) that breaks propagation.**
Backlog at scale	Millions of raw findings ranked only by CVSS severity	The small subset that are publicly exposed, actively exploited, and reachable in your environment	**Focuses defense on actionable risk and tracks reduction with evidence over time.**

Reachable-path identification
Surface the zero-days that open a reachable path to compromise.

Compensating-control validation
Confirm whether the controls you run stop exploitation, or are bypassed undetected.

Zero Day Response in hours
Ingest the feed, hunt affected assets, pinpoint undefended exposure while others assess by hand.

Defensive chokepoints
Orchestrate the highest-leverage compensating control change that closes the most paths at once.

Zero-Day Response: Traditional vs. Quell

Traditional: Disclosure → Triage → Patch Cycle → Exposure Window

Quell: Disclosure → Reachability Analysis → Control Adaptation → Path Closed

>95%
De-prioritized as unreachable

99%
Reduction in breachable exposure

12.3M→0.46%
Raw findings cut to actionable risk (global financial services)

3 wks→30 min
Triage time in that same deployment

See Quell in Action

See which zero-days are reachable, whether the controls you already own would stop them, and which compensating control change closes the path before exploitation.

Request a Quell demo: tuskira.ai/demo | Lorin@tuskira.ai

Tuskira™
Full Stack Agentic SecOps