Engineer

Proved the intrusion ban works every run

Proved the intrusion-banning path end to end on every hardening run by banning a reserved test address, reading the resulting kernel rule and unbanning in a guaranteed cleanup block, so a jail that stops working fails a run instead of reporting healthy.

September 2026

the ban path proved on every hardening run

Situation. The intrusion-banning service had already been caught banning a port the SSH daemon did not listen on. Fixing the port closed that instance. It did nothing about the reason the fault survived so long, which is that a ban path has no visible failure: the service runs, the jail is listed as active, and nothing anywhere says whether a ban ever reaches the kernel.

Task. The ban path had to be exercised on every converge, against the live rule set, rather than inferred from the service being up.

Action. The converge now bans an address from the block the standards reserve for documentation, reads back the resulting rule in the kernel's packet filter, and unbans it in a cleanup block that runs whether the check passed or failed. The reserved range is the load-bearing choice — the test address belongs to nobody, so a stray ban that outlives a failed run cannot lock out a real network. The kernel read-back is the other half: the service's own status output would report success for a ban that produced no rule, which is the exact failure being tested for. Alongside it, the ban mechanism is pinned rather than left to the service's detection, and the log source is set to detect because the operating system ships no traditional authentication log and the wrong choice fails silently by watching a file that never appears.

Result. A banning path that stops working now fails a converge instead of continuing to report healthy, which is the only property that mattered. It costs a few seconds on every run and it writes and withdraws a firewall rule

against production every time, which is a real intrusion into a live system and was accepted on the grounds that the alternative had already been demonstrated to be worse.

Bring this experience to your project

Use “Proved the intrusion ban works every run” as a starting point for a similar challenge in your organisation. The services behind this work are available for your project. Monitoring and alerts that speak up while a fault is still small, and the figures that show how often it stays that way.

Explore our services Get in touch →

Look behind the result

Read the situation, decisions and result in this example. We can discuss which parts transfer to your constraints and which need another approach. Proved the intrusion ban works every run — the ban path proved on every hardening run

Explore our services Get in touch →

Would you notice if a security control stopped working?

Talk through your project with the engineer responsible for delivery. We agree the scope, price basis and handover in writing before work begins.

Role context: Security Engineer. It draws on Infrastructure, Automation & CI/CD, Reliability & Backups, Linux & Servers, Security and Testing & QA. And while you are here, we are rather good at Site Reliability & Monitoring, System Administration, Security & Access Management and AI Agent Security.

Get in touch Explore our services

One piece of **a longer record** — and it is all on this site.

Every entry is written the same way: the situation, the task, what we did and what changed.

See the whole record

Define the improvement you need

Bring the deployment path, the operational risks and the people on call. We can scope a change with checks, a recovery route and clear ownership.

See what it costs Get in touch →

Would you notice if a security control stopped working?

Ask about the decisions behind “Proved the intrusion ban works every run”. You will speak with the people who can explain the work and assess your own project.

Explore our services

welcome@engineer.company +45 50 10 61 84 Copenhagen, Denmark

Take this page with you

Contact card

Carefully Crafted With Love by D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – present · Engineer ApS · All rights reserved.

Printed from https://engineer.company/portfolio/proved-the-intrusion-ban-works-every-run/