PITWALL

Security Stack Effectiveness Platform Overview

You built your security stack the right way.

You researched the options. You ran the POCs. You deployed each product correctly. Over and over again.

But over time, as the stack grew, something changed. Too many controls generating too much signal. Your team started chasing alerts that turned out to be nothing instead of working the investigations that actually mattered.

You looked at AI SOC agents. Maybe you deployed one. It helped. But in the back of your mind you know the underlying problem is still there.

You did not make wrong decisions. Your team is not missing anything.
You just need to see how the car is running.

Why This Is Happening

Stack Growth

Every new threat vector spawned a new product category. Every new category spawned a new vendor. A 100-control stack is now normal, not exceptional.

No Visibility

No product gives SOC teams real-time insight into how each control is actually performing. The stack is a black box between audits.

The Automation Gap

AI SOC agents automate alert triage. They do not fix the controls generating the alerts. You can automate chaos, but you cannot automate your way out of it.

The stack is underperforming. The analysts are burning out. And nobody has time to fix it.

PITWALL

Real-time visibility into how every control in your security stack is actually performing.

With the ability to fix what is not working **without adding headcount** or **touching your architecture.**

We do not replace anything in your stack. We make everything in it work better.

How Pitwall Works

01

Alert Tracking

Logs every alert from every control, from generation to resolution.

02

Performance Monitoring

Identifies which controls are operating outside accepted standards within the first week.

03

Auto-Diagnosis

Generates human-readable output explaining what is wrong and what configuration change will fix it.

04

Automated Remediation

SOC manager reviews the recommendation and applies the fix. Automated remediation available at Enterprise tier.

05

Continuous Learning

Learns the environment over time. Recommendations get sharper. The stack improves without dedicated audit cycles.

What Changes | SOC Manager

BEFORE

- Majority of shift spent on false positive triage
- No visibility into which controls are causing the noise
- Stack tuning deferred indefinitely — no time, no data
- Analyst burnout accelerating, turnover rising

AFTER

- Dashboard shows exactly which controls are underperforming
- Auto-diagnosis identifies root cause without manual investigation
- Configuration fixes applied in minutes, not quarters
- Analysts work real investigations. Burnout drops.

What Changes | CISO

BEFORE

- Board asks if the stack is working. No data to answer with.
- Budget renewal requires justification built on confidence, not evidence
- Post-incident questions about why controls did not catch it
- No continuous view of stack effectiveness between audits

AFTER

- Boardroom-ready report showing performance data for every assessed control
- Stack investment justified with specific metrics, not general assurance
- Configuration gaps diagnosed and documented before they become incidents
- Continuous monitoring replaces point-in-time audits

What Changes | Security Analyst

BEFORE

- Hours of each shift spent triaging alerts that resolve as false positives
- Real investigations backlogged while the queue keeps growing
- No visibility into why certain controls generate constant noise
- The work that matters keeps getting pushed

AFTER

- False positive volume drops. The queue becomes workable.
- Backlogged investigations get time again
- Noisy controls identified and fixed. Fewer ghosts to chase
- Spend the shift on work that actually matters

Early Adopter Result

45%

reduction in false positives within 30 days

That is not a product claim. It is what happens when a security team finally has the visibility to tune what they have already built.

Who Built It

JS

Joe Stack

Co-Founder and CEO

Former SOC analyst turned security architect. Over a decade building security stacks in finance and healthcare. Has lived through SIEM correlation rules that brought an entire SOC to its knees. Built Pitwall because he could not find a solution when he needed one.

BA

Bill Argentina

Co-Founder

Former CISO turned founder. Spent his career on the business side of security investment decisions. Knows what it feels like to sit in front of a board and try to justify a $40M security investment with no performance data to back it up. Built Pitwall to give CISOs the answer.

They did not build Pitwall because they studied the problem. They built it because they lived it.

The Pitwall Shakedown

The entire first half of the sales cycle is one ask: start the Shakedown.

14 days	Up to 20	None required	Zero obligation
Duration	Controls	Infrastructure changes	Commitment

How It Works

1. SOC Manager selects up to 20 controls and configures thresholds. Goes live with no infrastructure changes.
2. Pitwall monitors every alert for 14 days, identifies anomalies, and auto-diagnoses underperforming controls.
3. At day 14, Pitwall generates a boardroom-ready report showing exactly how the controls performed and what to fix.
4. SOC Manager and CISO review results together. The data makes the case.

One Ask

Run the Shakedown.

14 days. Up to 20 controls. No infrastructure changes. No obligation.

At the end you have data specific to your own environment. Your SOC Manager has a report to bring to the CISO. You have not committed to anything.

pitwall.io/shakedown
Start today. No procurement required.