No More Noise

Make Your SOC Your Sanctum

No More Noise!

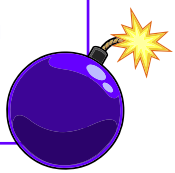
For cybersecurity pros, the cry of NO MORE NOISE reflects deep frustration.

It means there are too many alerts, not enough context, too much busywork, too many duplicates, too many false positives, and not enough time to focus on important tasks.

Alert overwhelm plagues nearly every SOC, affecting everything it touches. Major incidents slip by undetected, poor decisions are made in haste, employees burn out and leave, critical tasks get delayed, and costs skyrocket. All caused by noise.

Organizations need a way to turn the **noise down** so they can turn the **security up.**

Truth Bomb #1: According to a study by Enterprise Strategy Group, 75% of companies spend **as much time investigating false positives** as they do real incidents. Let that sink in.

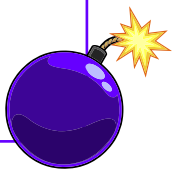


Why Hasn't it Been Solved?

Noise is the biggest problem in cybersecurity, and it's been left to fester by vendors who would rather focus on easier problems. And it's not just us saying that. Some vendors are on the record saying that noise reduction is too hard!

Security automation was supposed to get rid of noise, but most tools have come up short. Automating with a SIEM is too complex and costly. XDR was promising, but never lived up to the hype. Legacy SOAR struggles to scale reliably, isn't engineered to reduce noise, and most vendors got acquired and stopped innovating. Look under the mask of newer workflow automation products and you'll find legacy SOAR by other names, still prone to slowdowns and crashes that leave you wondering what you missed while they weren't ingesting alerts.

Truth Bomb #2: According to the 2023 State of Threat Detection Research Report, **67% of alerts go uninvestigated** because security teams don't have enough time. Hopefully there isn't anything important in there!



You can't eliminate noise without automating false positive dismissal and doing that safely requires high confidence. This is where it gets difficult, because achieving high confidence in your automated alert triage requires massive processing power. A high-confidence playbook might involve up to 100 automated enrichment and correlation actions. Many organizations process 100,000 alerts per day, so that adds up to 10 million actions being executed at high speed, every single day. Most tools cannot handle that scale.

Noise-Down Automation

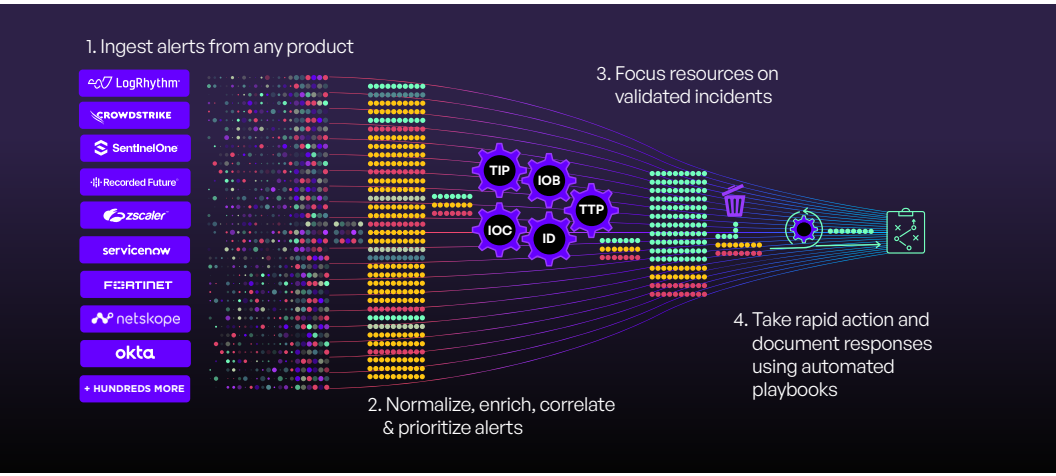
We aren't afraid of a challenge, so we're taking this one head on. D3's Smart SOAR actually turns down the noise—and it does it at scale.

We guarantee our clients an alert reduction of at least 91%. Some clients—like master MSSP High Wire Networks, which serves more than 25,000 end-customers through its channel program of MSSPs—have achieved 99% reduction or more.

We call it Noise-Down Automation. Here's how we do it:

High-Performance Integrations

Unlike vendors that rely on users and community groups to script integrations, D3 builds and maintains all integrations in-house. When you use a Smart SOAR integration, you know it was thoroughly researched, tested, and coded by our expert team. Because we're truly vendor-agnostic, you can integrate the entirety of any stack to ingest your alerts, cut out the noise, and orchestrate response.



The Event Pipeline

Unlike legacy SOAR products that just automate at the incident level, Smart SOAR has alert-level automation that gives you the confidence to filter out noise. The Event Pipeline normalizes, deduplicates, groups, correlates, and triages alerts to enable automated escalation or dismissal.

Powerful Workflow Engine

Noise-Down Automation requires workflows that are fast and reliable. Smart SOAR playbooks are not reliant on Python scripts, instead providing hundreds of prebuilt, drag-and-drop utility commands that execute faster and don't break down. Advanced capabilities like looping, parallel tasks, and scheduled automations work behind the scenes to pull off complicated processes while keeping the user experience simple.

Limitless Scale

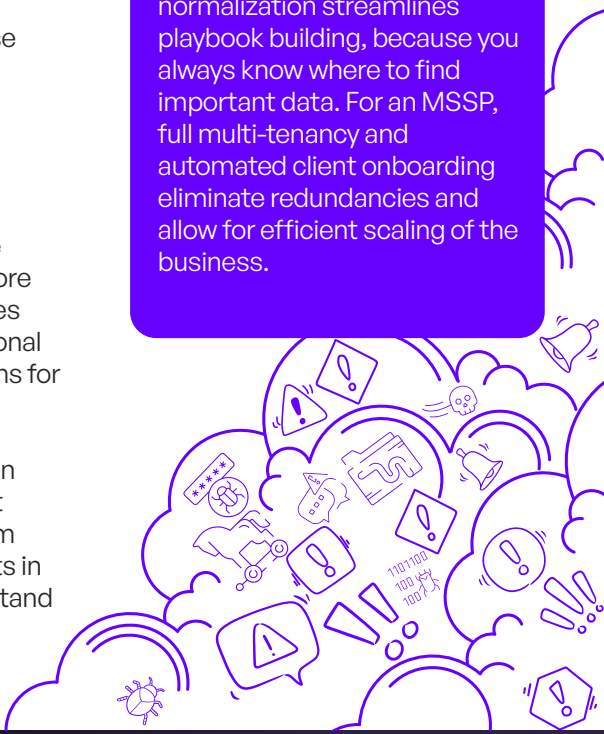
Smart SOAR is built to meet the requirements of the world's most targeted organizations and we have the results to prove it. Using cloud auto-scaling to dynamically allocate resources, we currently process up to 150,000 alerts per day, per customer. By the end of 2024, our capacity will be over one million alerts per day. Even the biggest enterprises and MSSPs can feed every alert into Smart SOAR for automated noise reduction.

Security Expertise

The implementation of your automation solution needs to be optimized, or it will just cause more noise. If that optimization requires expensive consultants, professional services, and trawling user forums for answers, it's going to require resources that busy SOC teams don't have. D3 is laser-focused on SOAR, so your dedicated project managers and 24/7 support team aren't generalists, they're experts in security automation that understand your deployment inside and out.

Ease of Use

Legacy SOAR has a reputation for being hard to use. Smart SOAR turns that on its head with features that remove noise from your day-to-day tasks. Everything you need for an investigation is extracted, enriched, and displayed on a single screen. Alert normalization streamlines playbook building, because you always know where to find important data. For an MSSP, full multi-tenancy and automated client onboarding eliminate redundancies and allow for efficient scaling of the business.



The Benefits of Turning Down the Noise

Noise Down, **Security** Up

- More time to spend on real threats
- 100% alert coverage
- Bandwidth for proactive tasks like threat hunting

Noise Down, **Confidence** Up

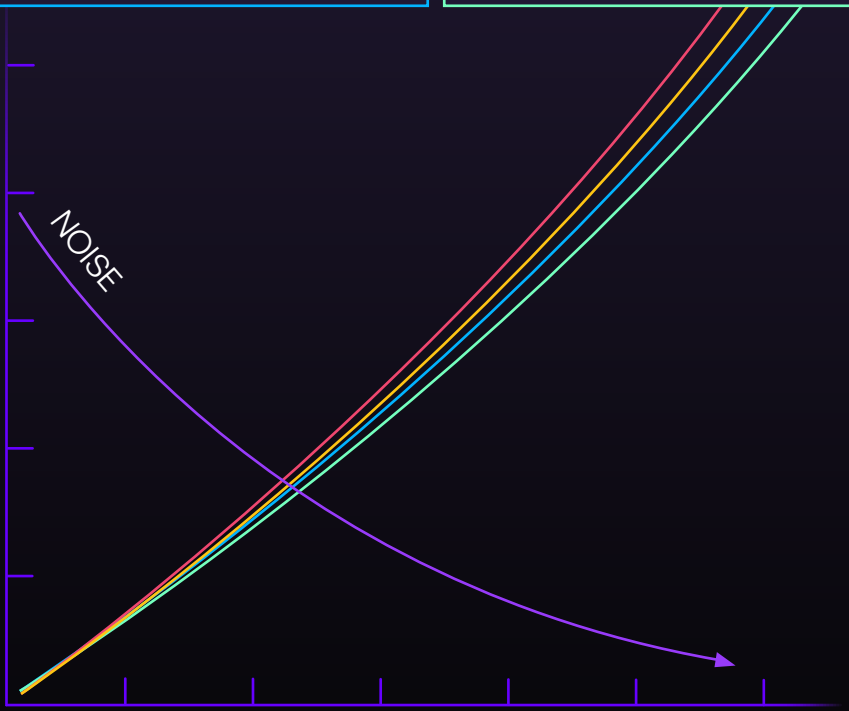
- Low-fidelity alerts are replaced with high-fidelity incidents
- Security teams can act with conviction
- A single pane of glass for comprehensive alert incident data

Noise Down, **Talent** Up

- Reduced burnout, which means less turnover
- Analysts can focus on interesting tasks that leverage their expertise
- No more wasting talented employees on repetitive busywork

Noise Down, **ROI** Up

- The resource-drain of handling false positives is eliminated
- More value from existing tool investments
- Less turnover means less resources committed to hiring and training

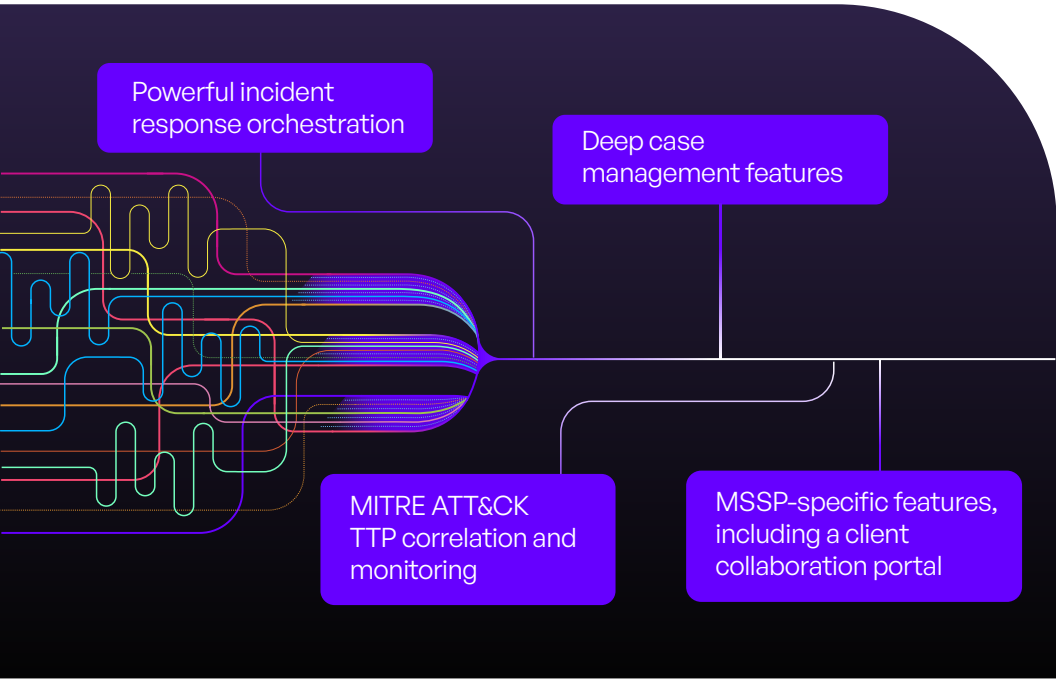


D3

It's Time for Smart SOAR

Legacy SOAR may have failed to live up to its promise, but SOAR still has an important role to play. That's why security teams are choosing Smart SOAR: the only automation tool that lets you **turn down the noise.**

But that's not all it does. Smart SOAR is a true, end-to-end security operations solution, with features we haven't covered here, including:



Truth Bomb #3: More than 73% of new D3 customers are **replacing a legacy SOAR platform.**

Visit **D3Security.com** to learn more about how Noise-Down Automation can help you tackle your biggest security challenges.

1-800-608-0081

sales@D3Security.com