



SURVIVAL GUIDE

FOR LEAN
TEAMS **USING**
SPLUNK



**How to reduce
alert fatigue,
improve visibility,
and stay sane—
without replacing
your tools**



About the Author



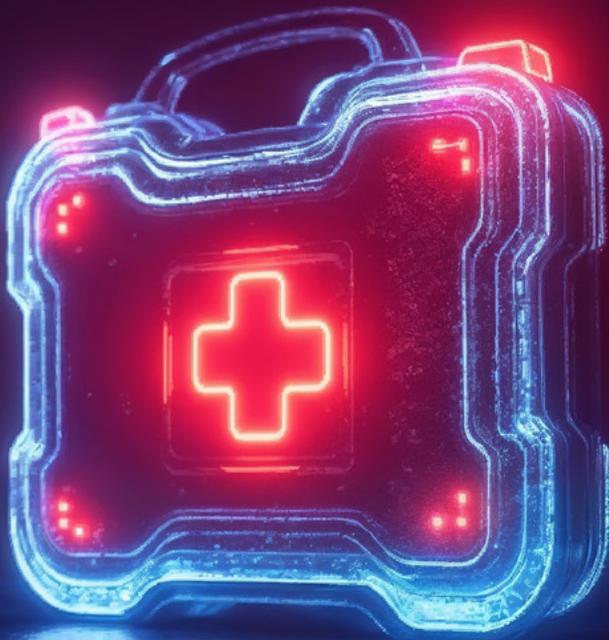
Carl Adasa

**VP, SOC Engineering and Managed Cyber Services
Deepwatch**

After 15+ years leading global SOCs for enterprise brands, I've seen how fast Splunk can become challenging to maintain peak optimization and innovation, especially when your team is lean. This guide distills lessons from hundreds of Splunk environments, dozens of burnouts, and the hard truth that detection isn't just about tools—it's about operational reality. This is what I wish someone had handed me when I first moved into leadership.

TABLE OF CONTENTS

INTRODUCTION	4
<hr/>	
THE HIDDEN COSTS OF RUNNING SPLUNK ALONE	5
<hr/>	
5 WARNING SIGNS YOU'RE DOING TOO MUCH WITH TOO LITTLE	6
<hr/>	
THE TUNING & HYGIENE CHECKLIST	7
<hr/>	
BONUS: FULL SPLUNK HEALTH CHECK DIAGNOSTIC	8
<hr/>	
WHAT GOOD LOOKS LIKE: A HEALTHY SPLUNK ENVIRONMENT	9
<hr/>	
SPLUNK HABITS THAT BURN-OUT SECURITY TEAMS	10
<hr/>	
WHAT TO SAY TO LEADERSHIP	11
<hr/>	
LIGHT ROI SNAPSHOT: TIME, TEAM, AND TOOLS	12
<hr/>	
YOUR NEXT STEP: THE HEALTH CHECK	13
<hr/>	

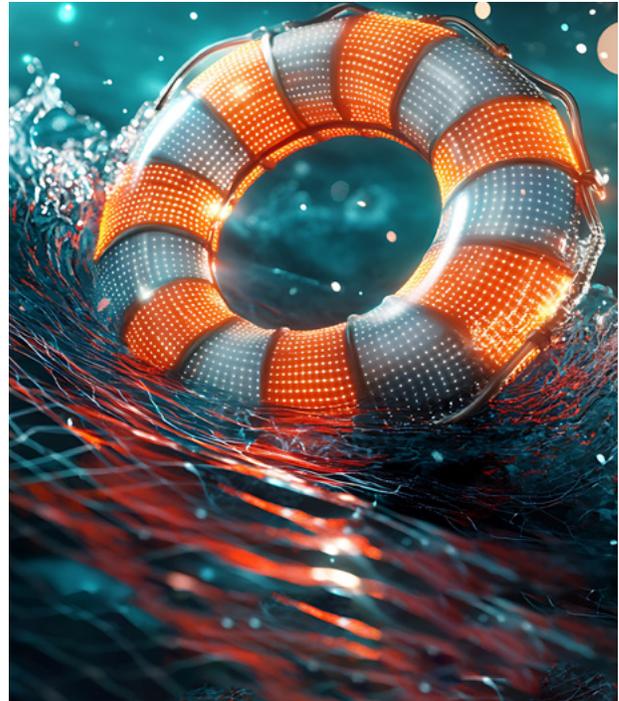
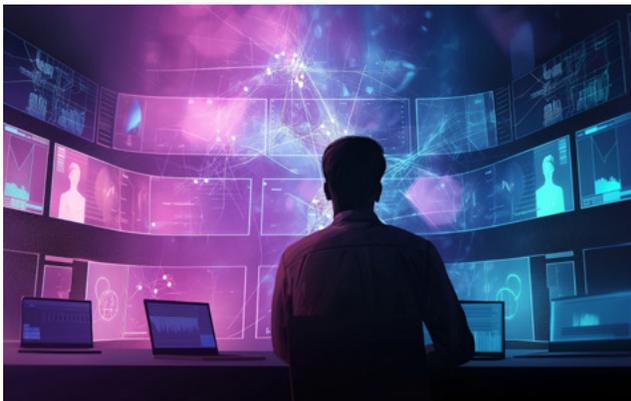


01

INTRODUCTION

▶ **Splunk is a powerful engine for detection and response, but when your team is lean, even the best tools can become unmanageable.** Over the years, I've worked with dozens of SOC teams who started with strong intent and a well-licensed platform, only to find themselves overwhelmed, under-resourced, and caught in a cycle of tuning, triage, and toil.

This guide is designed to break that cycle. Whether you're leading a small team or scaling detection maturity across the enterprise, this is a practical framework to identify friction points, restore operational clarity, and get the outcomes you originally invested in Splunk to achieve.

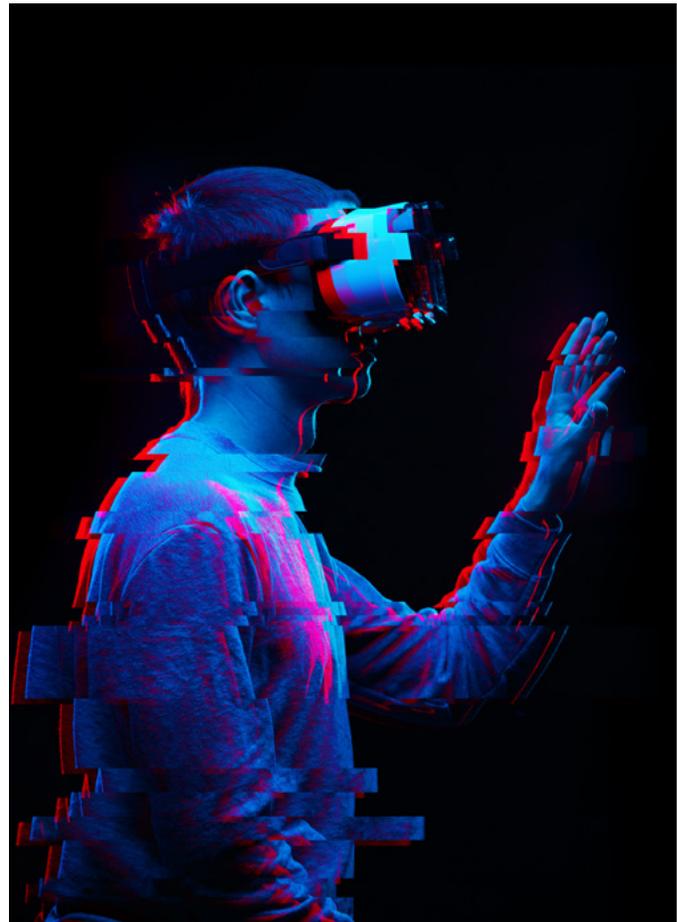


Too often, SOC teams invest in dashboards that create the illusion of visibility without improving outcomes. This guide doesn't promise silver bullets—it offers a grounded path based on hard-earned lessons to help your team refocus on what matters: signal clarity, faster response, and sustainable operations.

The Hidden Costs of Running Splunk Alone

Your Splunk license isn't the most expensive part of your SIEM. The real cost? The slow bleed of operational strain that few talk about. Let me paint the picture, not from a white paper, but from experience.

In one of my earlier roles, I oversaw global SOC operations responsible for the enterprise, cloud, and corporate infrastructure. Despite our maturity, Splunk alert volume regularly outpaced what our teams could handle. I remember a particularly sobering weekend when one of our regional SOCs nearly missed a brute-force credential attack because the team was manually triaging over 1,500 alerts. The incident turned into a multi-week investigation, costing significant cycles in incident response, engineering, and executive reporting. It was a turning point in how we thought about automation, correlation logic, and 24/7 support models.



HERE'S WHERE THE HIDDEN COSTS SHOW UP:

- **Alert Fatigue:** 73% of SOC teams report burnout due to excessive alert volume (Devo SOC Performance Report, 2024).
- **Data Chaos:** Duplicate logs, irrelevant events, and missing source types erode detection fidelity.
- **Missed Threats:** A recent study by ESG found that 60% of orgs had at least one incident in the past year that bypassed their SIEM.
- **Tool Sprawl:** Adding point solutions for enrichment or correlation leads to dashboard overload and integration debt.
- **Lost Time:** Your analysts spend more time on tool hygiene than threat hunting.

And then there's morale. In a world where AI deepfakes can trigger phishing campaigns within minutes, your team can't afford to waste hours every week cleaning up log clutter. It's not just inefficient—it's dangerous.



5 Warning Signs You're Doing Too Much with Too Little

1. Your team spends more time chasing alerts than investigating threats

When alert triage becomes your primary function, threat analysis suffers. This imbalance is often the first indicator that the SIEM is serving the data, not the mission.

2. You don't fully trust your telemetry

Whether it's missing logs, miscategorized events, or unexplained gaps in coverage, unreliable data erodes both detection fidelity and analyst confidence.

3. Dashboards are abundant—but underused

Over time, teams accumulate dashboards meant to show value. But if no one's using them daily, they're not aiding decisions—they're artifacts of past intentions.

4. There's no consistent 24/7 monitoring

Coverage gaps—whether due to headcount, burnout, or alert fatigue—are risk multipliers. Threats don't work 9-to-5, and neither should your detection strategy.

5. You've begun exploring outsourcing or MDR for relief

The search for MDR or co-managed services often starts when internal strain reaches a tipping point. That's not a failure. It's a recognition that capacity needs to scale faster than headcount.

.....

If these scenarios resonate, you're not alone. This isn't about blame—it's about identifying where strategic support can shift your team from survival to precision.. You're trying to run enterprise defense on startup resources. It's time to think about scaling your capacity, not just your tools.

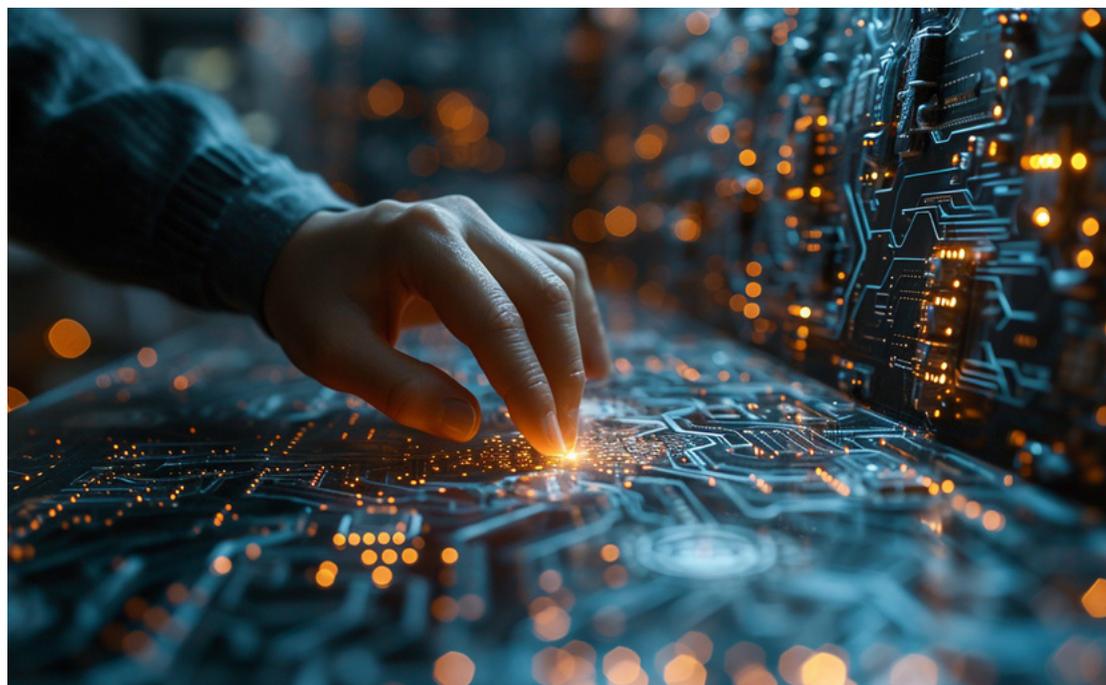
04

THE TUNING & HYGIENE CHECKLIST

Before jumping into the full diagnostic framework below, here are six quick checks that help identify whether your Splunk environment is quietly underperforming.

- ▶ **Log Source Normalization:** Are your logs deduplicated, normalized, and reliably parsed?
- ▶ **Detection Coverage:** Do your rules align with defined threat models like MITRE ATT&CK?
- ▶ **Alert Fidelity:** Are your alerts mostly actionable—or mostly noise?
- ▶ **24/7 Consistency:** Is your coverage model dependable after hours and across shifts?
- ▶ **Ingestion Hygiene:** Are you sending data that supports use cases—or just adding volume?
- ▶ **Rule Lifecycle:** When was the last time correlation logic was reviewed or retired?

If more than two of these are uncertain or untracked, it's worth moving on to the full diagnostic. That deeper review begins in the next section.



Bonus: FULL SPLUNK HEALTH CHECK DIAGNOSTIC

▶ If you want a broader look at Splunk performance, use the Deepwatch Splunk Health Check framework. **This quick diagnostic explores five key areas:**

✓ ALERT VOLUME & FATIGUE

- Are you receiving 50+ alerts per day, most of which go uninvestigated?
- Are analysts suppressing alerts to manage the noise?
- Do correlation rules overlap or trigger redundant alerts?
- Do alerts often require manual triage?
- Have you missed real incidents due to alert fatigue?

✓ TEAM CAPACITY & RESILIENCE

- Do you lack 24/7 coverage?
- Is burnout or turnover creeping in?
- Are engineers spending more time maintaining Splunk than defending systems?
- Are you missing a roadmap to reduce alert noise?

✓ DATA INGESTION & HYGIENE

- Are you ingesting logs “just in case” with no mapped use case?
- Do parsing errors show up in searches?
- Is ingestion volume growing without detection quality improvement?
- Is onboarding of new sources inconsistent?



✓ DETECTION LOGIC

- Are you overly reliant on vendor-provided rules?
- Are detections mapped to MITRE ATT&CK or threat models?
- Are low-severity alerts tuned or ignored?
- Do suppression rules evolve reactively?

✓ REPORTING & VISIBILITY

- Do your dashboards show alert counts—but not MTTR or asset coverage?
- Is reporting manual or hard to align with business value?

If you've checked multiple boxes across multiple sections: Your Splunk instance might be doing more harm than good. It doesn't mean you need to switch platforms—it means it's time to bring in help.



05 What Managed SIEM on Splunk Looks Like

When teams hit a breaking point with Splunk, the instinct is often to assume the platform itself is the problem. Some consider replacing it entirely, despite the cost, complexity, and disruption. Others look to throw more headcount at it or add yet another tool to band-aid the symptoms.

But in most of the environments I've seen, the issue isn't the technology. It's the lack of operational capacity, tuning discipline, and 24/7 consistency needed to make Splunk perform the way it should.

That's where Managed SIEM comes in. With the right partner, you don't need to replace Splunk. You need help making it sustainable.

Deepwatch can serve as an extension of your team to:

- Provide 24/7 monitoring, alert triage, and tuning
- Ensure log hygiene and enrichment are always current
- Detect threats faster with high-fidelity correlation
- Reduce alert volume without reducing visibility

BEFORE:

- 2 analysts covering business hours only
- 800+ daily alerts, mostly low-fidelity
- Manual triage with inconsistent processes
- No structured after-hours or weekend coverage
- Increasing backlog and missed detection SLAs

AFTER:

- Full 24/7 managed detection with automated triage
- 90%+ reduction in non-actionable alerts
- Defined alert routing and coverage handoffs
- Improved detection speed and response metrics (MTTD/MTTR)
- Operational stability, even with lean internal teams

▶ CUSTOMER SNAPSHOT

“Before Deepwatch, we were constantly reacting. After bringing them in, we finally felt like we had a handle on Splunk again.”

— SOC Director, Financial Services

06

What Good Looks Like: A Healthy Splunk Environment

If you're wondering what “healthy” actually looks like, here's a quick north star to aim for:

- ✓ Alerts mapped directly to business-critical use cases
- ✓ High-fidelity detection logic reviewed every 90 days
- ✓ 80%+ of alerts auto-triaged or suppressed
- ✓ Consistent 24/7 coverage across time zones
- ✓ Ingestion volumes mapped to actual use cases (not “just in case”)
- ✓ Dashboards focused on outcomes (MTTR, coverage, threat type)

This isn't a unicorn setup — it's what happens when your Splunk is tuned, curated, and supported.

Splunk Habits that Burn-Out Security Teams

- 1. Chasing Every Alert Like it's a Zero-Day**
Teams stuck in reactive mode treat every alert as urgent—burning out analysts and reducing time for actual threat hunting.
- 2. Letting Ingestion Grow Without Reviewing Use Cases**
It's common to ingest “just in case” logs, but without clear use case mapping, you're just increasing noise and cost.
- 3. Skipping Quarterly Rule Audits**
Correlation rules age quickly. What made sense six months ago might be generating nothing but false positives today.
- 4. Letting Stale Dashboards Pile Up**
A proliferation of unused dashboards often signals misalignment between what's being monitored and what matters.
- 5. Suppressing Alerts Just to Survive the Day**
Suppression becomes a coping mechanism, not a strategy. Over time, this masks systemic issues that need attention.

These aren't just inefficient habits—they're warning signs that your detection pipeline is over-extended. Reversing them doesn't require a platform change. It requires operational clarity, tuning discipline, and the right support model.

08

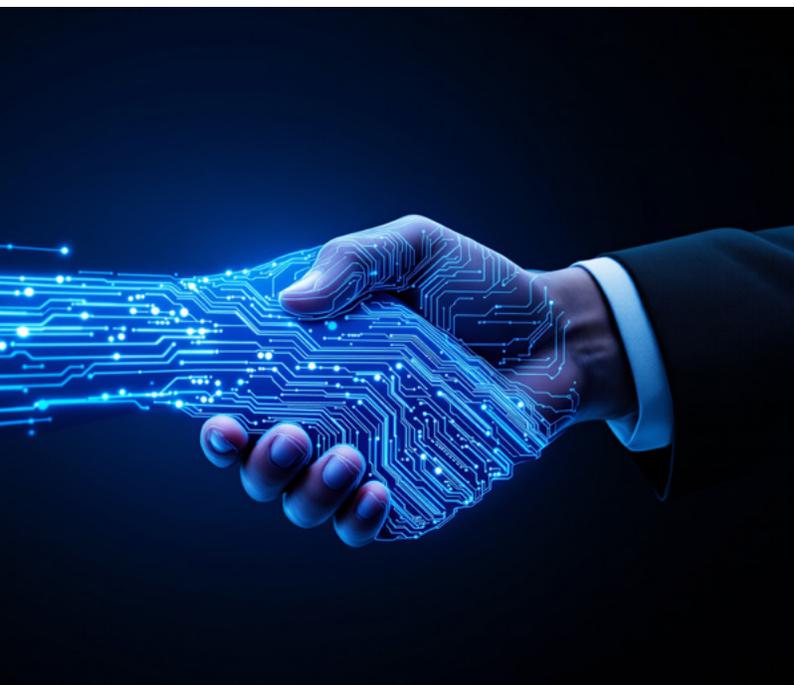
What to Say to Leadership

▶ When it's time to raise the flag internally, here's a three-sentence elevator pitch for execs:

“WE’RE NOT ASKING TO REPLACE TOOLS. WE’RE ASKING TO RESTORE TRUST IN WHAT WE ALREADY HAVE. A SPLUNK HEALTH CHECK GIVES US A CLEAR PATH TO REDUCE NOISE, RECLAIM TIME, AND PRIORITIZE REAL THREATS.”

This frames the issue in terms of ROI, efficiency, and business risk

— not just tech jargon.



09

Light ROI Snapshot: Time, Team, and Tools

▶ Here's how optimization pays off:

- Reducing 400 false positives/week = ~1 FTE/week reclaimed = ~\$120K/year in capacity
- Improved MTTD = reduced breach exposure = lower IR costs
- No new platform = no migration downtime or retraining cost

Even small wins in Splunk tuning have outsized impact on cost, stress, and visibility.

Your Next Step: The Health Check

“Every team deserves a SIEM that works for them—not the other way around.” — Carl Adasa

You don't have to overhaul your security strategy to get results. Start with a **Splunk Health Check**:

- We Assess Your Ingestion, Rules, Alerting Logic, And Gaps
- You get a No-BS Scorecard and Quick-Win Roadmap
- No Obligation, No Platform Switch

 [\[Book Your Splunk Health Check Now\]](#)



DEEPWATCH™

Deepwatch® is the leader in Precision MDR powered by AI and humans. We amplify human expertise with AI insights to reduce the risks that matter most to your business. Our protection is **proactive, preemptive and responsive**, tuned to your business, with no black boxes, and watched by experts **24/7/365**.

Learn more: www.deepwatch.com

Follow us:

[Blog](#) | [LinkedIn](#) | [Facebook](#)