DEEPWATCH™

Always Watching. Always Protecting.™

FROM NOISE TO CLARITY:

THE SECURITY LEADERS' PLAYBOOK FOR MAXIMIZING SPLUNK INVESTMENT

www.deepwatch.com

TABLE OF CONTENTS

01
INTRODUCTION: WHY THIS GUIDE EXISTS
- From Alert Fatigue to Executive Impact, Why Splunk Isn't the Problem — But Running It Alone Might Be

02
THE CHALLENGE: WHAT TODAY'S CISOS FACE WITH SPLUNK
- Tool Sprawl, Alert Volume, and Limited Resources
- The Tipping Point for MDR or Co-Managed Help

03
STRATEGY 1: TRANSLATE SPLUNK DATA INTO BUSINESS RISK
- Metrics That Matter to Executives
- Framing Cyber Risk in Business Terms

04
STRATEGY 2: FUTURE-PROOF YOUR DETECTION STACK WITHOUT RIPPING IT OUT
- Avoiding Costly Migrations
- Building on What Works

05
STRATEGY 3: SHIFT FROM PROACTIVE TO PREEMPTIVE SECURITY
- Continuous Exposure Management
- Testing Before an Adversary Does

06
STRATEGY 4: LAYER YOUR DEFENSE — USE SPLUNK AS YOUR INTEGRATION CORE
- Connecting the Dots Across Telemetry
- Using MDR to Unify Detection Signals

07
STRATEGY 5: MODERNIZE REPORTING WITH EXECUTIVE-GRADE METRICS
- From Volume to Value
- What Your Board Actually Cares About

08
STRATEGY 6: AUTOMATE WITHOUT LOSING VISIBILITY OR CONTROL
- The Right Way to Leverage SOAR
- Reducing Alert Fatigue With Intelligence-Driven Rules

09
STRATEGY 7: REDUCE ANALYST BURNOUT WITHOUT ADDING HEAD COUNT
- How Co-Managed Detection Offloads the Right Tasks
- Maintaining Team Health While Scaling Operations

10
STRATEGY 8: RUN A SPLUNK HEALTH CHECK — BEFORE IT BECOMES A LIABILITY
- Detection Coverage, Ingestion Hygiene, and Rule Performance
- Using the Deepwatch Diagnostic Framework

11
STRATEGY 9: USE MITRE ATT&CK AS A NORTH STAR — NOT JUST A CHECKBOX
- Aligning Rules to Real Threat Behavior
- Mapping and Measuring Coverage Over Time

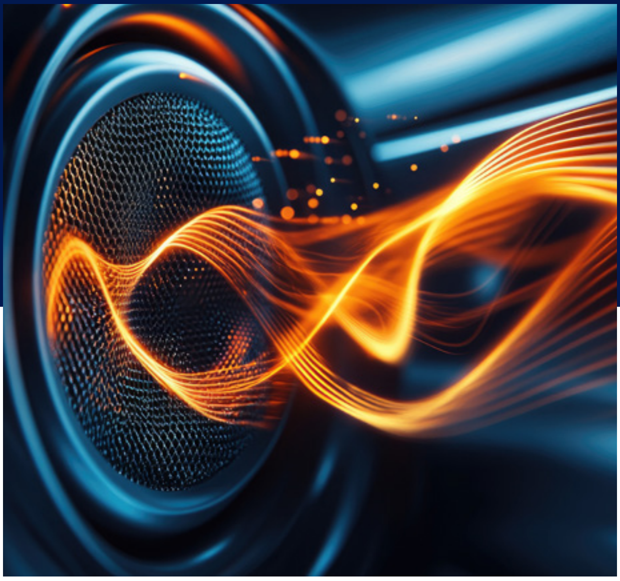
12
STRATEGY 10: TREAT MDR AS A STRATEGIC EXTENSION — NOT A VENDOR SWAP
- Partner Models vs. Outsourcing
- What Makes Co-Managed MDR Different

13
WHY DEEPWATCH: THE PARTNER BUILT FOR SPLUNK-POWERED SOCS
- 24/7 Response Without Losing Control
- Built-In Tuning, Customization, and Advisory

14
YOUR NEXT STEP: BOOK A SPLUNK OPTIMIZATION BRIEFING
- How to Assess Readiness and Fit
- What to Expect From a Health Check

INTRODUCTION

From Alert Fatigue to Executive Impact, Why Splunk Isn't the Problem — But Running It Alone Might Be



Splunk is one of the most powerful detection platforms in cybersecurity, but without the right operational model, even the best tools can become a burden. For many security leaders, managing Splunk often involves endless tuning, high ingestion costs, and triaging alerts well beyond business hours. While your team is capable, they are stretched thin. Your Security Information and Event Management (SIEM) system is robust, but overwhelming. Instead of focusing on strategic initiatives, your analysts find themselves in survival mode.

This guide is designed for you, the CISO managing a security program that relies on Splunk but struggles to turn its data into meaningful business impact.

You don't need a new platform; you need a smarter approach to leveraging the one you already have. This means shifting from simply reviewing alerts to implementing strategic threat reduction. This involves prioritizing decisions over dashboards and focusing on outcomes instead of just detection tools. In the following pages, you'll discover proven strategies to help you:

- Reclaim analyst time and reduce alert fatigue.
- Strengthen Splunk tuning and improve detection logic.
- Align security metrics with executive priorities.
- Extend coverage without increasing head count.
- Enhance visibility across your threat surface—not just in log volume.

This guide is not about changing your technology stack; it's about maximizing the value of what you already own and providing your team with the support they need to lead effectively.

THE CHALLENGE

TOOL SPRAWL, ALERT VOLUME, AND LIMITED RESOURCES—THE TIPPING POINT FOR MDR

CISOs today are not struggling because Splunk is ineffective; they are struggling because Splunk requires more time, more tuning, and more team capacity than most organizations can sustain. Security teams find themselves caught between urgent operational tasks and long-term maturity goals, with this tension heightened in Splunk-heavy environments.

Each week brings new detection use cases, while every quarter adds more logs, more cloud infrastructure, and increasing pressure to justify spending. You are running detection on a platform designed for scale but lack the necessary resources to match that scale.

HERE IS WHAT THIS TYPICALLY LOOKS LIKE:

01 **Alert fatigue is real.**

Even well-established Splunk setups generate excessive noise that overwhelms analysts in triage and forces them to suppress low-priority signals just to keep up.

02 **Tool sprawl slows you down.**

With various point products for EDR, identity, vulnerability management, and SaaS logs often integrating into Splunk, piecing together a coherent picture from these disparate sources becomes operationally exhausting.

03 **You are tuning rules after hours.**

Without enough staff to maintain 24/7 detection, your team is either stretched thin or making compromises that no CISO wants to acknowledge

04 **Ingestion cost versus value is unclear.**

While it is easy to add data, aligning that data with real business risk is more challenging.

Every Splunk-heavy security team eventually reaches a tipping point where operational demands overwhelm their capacity for detection and response. This can occur after missing a Service Level Agreement (SLA), when a high-priority alert is lost in the backlog, or when a senior analyst departs and there's no one to maintain their custom logic.

Co-managed support via an MDR solution enhances Splunk rather than replaces it. A strategic Managed Detection and Response partner introduces discipline, automation, and scalability, extending your detection capabilities while keeping your team in control. Making this transition sooner allows you to shift from reactive firefighting to achieving measurable resilience.

STRATEGY 1: TRANSLATE SPLUNK DATA INTO BUSINESS RISK

METRICS THAT MATTER TO EXECUTIVES, FRAMING CYBER RISK IN BUSINESS TERMS

Splunk excels at gathering and correlating security telemetry, but without context, the alerts it produces are merely noise to a business. CISOs who succeed in the boardroom understand that the sheer number of events investigated or rules triggered is far less convincing than demonstrating how these actions actually reduce an organization's risk exposure. Your executive colleagues (CFO, COO, and CEO) communicate in terms of business impact. They want answers to the following questions:

1. **What is at risk?** (Revenue, operations, brand trust)
2. **What has changed?** (Are we more or less exposed than last quarter?)
3. **What is the ROI?** (Are we improving in terms of speed and efficiency?)

To bridge this gap, it is important to translate Splunk's security data into metrics that executives understand. Consider the following:

- **Time to Contain (TTC):** The duration from threat detection to neutralization, quantified by reduced downtime or revenue at risk.
- **Critical Incident Exposure:** The number of high-impact threats detected and resolved prior to disrupting business operations.
- **Coverage of Crown Jewel Assets:** The percentage of mission-critical systems that are monitored and protected, aligned with business priorities.
- **Reduction in False Positives:** Gains in operational efficiency that translate into recovered analyst time and lower labor costs.

FRAMING THE CONVERSATION IN BUSINESS TERMS

- **Instead of saying:**
  "We reduced false positives by 30% in Splunk last quarter."
- **You could say:**
  "By reducing false positives by 30%, our analysts recovered the equivalent of 300 work hours, enabling us to investigate 40% more high-priority incidents without adding to head count."
- **Instead of saying:**
  "We are collecting more telemetry from our EDR and SaaS tools."
- **You could say:**
  "We have expanded Splunk coverage to include the systems that process 80% of our revenue transactions, ensuring faster detection of threats that could disrupt our core business."

When Splunk data is presented in this manner, security begins to shift from being perceived as a cost center to being viewed as a competitive advantage. This transformation allows the CISOs to move from merely justifying expenditures to actively shaping strategy.

STRATEGY 2: FUTURE-PROOF YOUR DETECTION STACK WITHOUT RIPPING IT OUT

AVOIDING COSTLY MIGRATIONS, BUILDING ON WHAT WORKS

Splunk is one of your largest investments in security technology, covering licensing, data ingestion, infrastructure, and the countless hours your team has dedicated to detection engineering. The quickest way to disrupt a security program's progress is to abandon that investment for the allure of a "shiny object" migration. Most Splunk customers do not face a technology problem; rather, they confront an operational issue. Future-proofing your detection stack means finding ways to extend its life, efficiency, and coverage without starting over. **This requires that you follow two principles:**

1. Avoid costly rip-and-replace cycles

Replacing Splunk means the following:

- Rebuilding years of correlation logic and dashboards.
- Retraining your analysts and engineers.
- Migrating terabytes of historical log data—often with format incompatibilities.
- Enduring 6–12 months of reduced visibility during the transition.

2. Build on what already works

Instead of replacing your SIEM, strengthen it with the following:

- **Optimized ingestion** — Drop irrelevant or duplicate logs; prioritize high-value telemetry aligned to use cases.
- **Detection tuning & enrichment** — Improve alert fidelity by combining Splunk rules with external threat intelligence and context from your EDR, IAM, and SaaS tools.
- **Co-managed MDR support** — Offload 24/7 monitoring, triage, and tuning to a trusted partner while retaining control of your platform.

PRO TIP: ***Treat your Splunk environment as a dynamic asset that evolves, not as a static system. Regular tuning cycles, content updates, and architecture reviews can significantly extend its useful life for years and prevent you from becoming dependent on an expensive migration project.***

STRATEGY 3:

SHIFT FROM PROACTIVE TO PREEMPTIVE SECURITY

CONTINUOUS EXPOSURE MANAGEMENT, TESTING BEFORE AN ADVERSARY DOES

For years, "proactive security" referred to identifying vulnerabilities before they could be exploited by attackers. However, in today's evolving threat landscape, proactive measures are no longer sufficient, as adversaries can act faster as adversaries can act faster than security teams that rely on quarterly patch cycles or annual penetration tests. The new standard is preemptive security: actively eliminating vulnerabilities before they can be weaponized.

Continuous Threat Exposure Management (CTEM) brings structure to this approach. CTEM programs do the following:

- Continuously identify exposures across on-prem, cloud, SaaS, and remote endpoints.
- Focus on prioritizing exposures according to the business context rather than solely relying on CVSS scores.
- Validate remediation through automated testing and attack simulation.

Splunk can play a central role in CTEM by ingesting, correlating, and reporting on exposure data from various tools, but it requires the appropriate operational framework:

- **Automated coverage checks** — Verify that high-value assets are continuously monitored and that new data sources are onboarded immediately.
- **MITRE ATT&CK alignment** — Ensure that detections map to known adversary behaviors and that coverage is validated regularly.
- **Simulated attack paths** — Use red team exercises or breach-and-attack simulation tools to test detection-and-response logic before attackers do.

PRO TIP: ***Collaborate with a co-managed MDR partner to test your detection logic. For instance, Deepwatch conducts simulated attack paths and validates Splunk rules, ensuring that critical threats are detected and escalated while minimizing false positives.***

BOTTOM LINE: Proactive security minimizes known risks, while preemptive security eliminates potential attack opportunities by addressing vulnerabilities before they can be exploited. In a Splunk-driven Security Operations Center (SOC), this approach involves creating a dynamic detection ecosystem that is consistently tested, refined, and validated on a daily basis rather than only following an incident.

STRATEGY 4: LAYER YOUR DEFENSE: USE SPLUNK AS YOUR INTEGRATION CORE

CONNECTING THE DOTS ACROSS TELEMETRY, USING MDR TO UNIFY DETECTION SIGNALS

Defense in depth is a well-established principle, but simply adding more tools doesn't ensure better security. Many enterprises now use various point products such as EDR for endpoints, IAM for identity management, cloud security tools, DLP, and vulnerability management. The real challenge is not acquiring these tools but ensuring they work together to provide actionable insights.

Splunk can serve as the integration core of this strategy by collecting and normalizing data from across your security and IT ecosystems. It applies correlation logic to detect threats that individual tools might overlook. However, without a clear strategy, this capability can become just another source of noise.

The Case for a Layered Splunk-Centric Architecture

A modern layered defense should have the following:

- Multiple security controls across domains — Endpoint, network, identity, application, and cloud.
- Telemetry correlation — Linking seemingly unrelated events (e.g., endpoint malware alerts + anomalous login) to reveal attack paths.
- Prioritized alerting — Using context from across layers to promote only the most critical threats for prioritized analyst review.

Splunk becomes the nervous system for this architecture:

- EDR + Splunk — Capture detailed endpoint activity, and enrich Splunk alerts with forensic context.
- IAM + Splunk — Detect credential abuse or privilege escalation in context with other suspicious activity.
- Cloud + Splunk — Identify misconfigurations or unusual API calls alongside related endpoint or network activity.

Why MDR Is the Glue That Makes It Work

Even with Splunk at the core, stitching layers together requires constant engineering and tuning. That's where co-managed MDR partners deliver value:

- Detection engineering across layers — Crafting correlation searches that tie together endpoint, identity, network, and cloud indicators.
- Noise reduction — Suppressing low-value alerts that slip in from multiple sources.
- Threat-informed prioritization — Escalating multi layer alerts that map to known adversary behaviors in MITRE ATT&CK framework.
- 24/7 cross-domain monitoring — Ensuring that critical detections are never missed, regardless of the data source.

PRO TIP: ***Refrain from viewing Splunk as just a SIEM. Instead, treat it as a comprehensive security data platform that integrates and correlates all layers of defense. MDR partners can leverage it to create a real-time threat detection engine rather than just a post-incident investigation tool.***

A layered defense without integration can lead to tool sprawl while integration without prioritization creates excessive noise. By using Splunk as the core for integration and ensuring that detection engineering encompasses every layer of your stack, you can transform fragmented security data into a cohesive and effective defense strategy.

STRATEGY 5: MODERNIZE REPORTING WITH EXECUTIVE-GRADE METRICS

FROM VOLUME TO VALUE, WHAT YOUR BOARD ACTUALLY CARES ABOUT

In many Splunk-driven SOCs, reporting often focuses on technical metrics such as the number of alerts processed, rules triggered, and logs ingested. While these metrics are valuable for internal operations, they do not effectively communicate the broader picture to executive audiences. The C-suite and board members are not interested in an overwhelming amount of numbers; instead, they seek a clear understanding of risk reduction and the overall impact on the business.

The challenge for CISOs is to translate the constant hum of Splunk activity into executive-grade insights that answer four core questions:

1. Are we more or less exposed than before?
2. Are we detecting and responding faster?
3. Are our investments delivering measurable security outcomes (security posture)?
4. Are we in compliance with regulatory requirements?

Shift from Technical Metrics to Business-Aligned KPIs

By modernizing your reporting, you shift from saying "We investigated 2,000 alerts last month" to a more impactful statement: "We prevented a critical outage that could have disrupted 80% of our revenue transactions."

Recommended Business-Aligned Metrics:

- **Mean Time to Detect (MTTD) & Mean Time to Contain (MTTC):** Demonstrate faster threat neutralization in terms of reduced downtime or loss avoidance.
- **Critical Incident Prevention Rate:** Highlight the percentage of high-priority threats stopped before they impacted operations.
- **Coverage of Crown Jewel Assets:** Show the percentage of critical systems continuously monitored by Splunk rules.
- **False Positive Reduction:** Translate reduced noise into regained analyst hours and cost savings.
- **Detection Coverage Mapped to MITRE ATT&CK framework:** Present maturity in terms of known adversary tactics covered.

Tell a Story, Not Just a Number

Boards remember narratives, not spreadsheets. Instead of simply presenting data points, convey the story of how your Splunk detections, tuning, and responses directly prevented a breach. For example, "Last quarter, we reduced our MTTD by 43%. This improvement allowed us to detect and contain a ransomware attempt targeting our ERP system before any data could be encrypted, ultimately preventing an estimated $2.5 million in downtime."

How MDR Partners Enhance Reporting

A co-managed MDR provider can transform reporting by doing the following:

- Correlating outcomes across data sources for a unified picture of detection performance.
- Providing quarterly risk trend analysis tied to business priorities.
- Delivering board-ready dashboards that cut technical jargon and focus on risk posture improvement.

PRO TIP: ***Ask your MDR partner to integrate reporting directly into your executive dashboards, with trend lines that map security investments to reduce business risk over time.***

The true value of Splunk lies not in the volume of alerts it processes but rather in the impact those alerts have on safeguarding your revenue, customers, and brand. By modernizing your reporting, you can not only demonstrate the return on investment (ROI) of security measures but also secure a prominent role in strategic decision-making.

STRATEGY 6: AUTOMATE WITHOUT LOSING VISIBILITY OR CONTROL

THE RIGHT WAY TO LEVERAGE SOC, REDUCING ALERT FATIGUE WITH INTELLIGENCE-DRIVEN RULES

Automation is one of the most powerful tools in a Splunk-driven SOC, yet it is often misunderstood. When implemented correctly, automation frees analysts from repetitive, low-value tasks and accelerates the process of containing threats. However, if implemented incorrectly, it can become a black box that reduces visibility, potentially allowing critical threats to go unnoticed.

For security leaders, the goal is not to automate everything but to automate intelligently. This involves developing workflows that minimize noise, handle routine containment, and enable analysts to concentrate on complex investigations, all while ensuring complete visibility into every step of the process.

The Case for Targeted Automation

Full automation without oversight is risky. But selective automation for high-confidence, well-understood scenarios is a force multiplier.

Start by automating the following:

- **Enrichment task**s — WHOIS lookups, geolocation checks, and threat intel queries for suspicious IPs or domains.
- **Low-risk containment actions** — Isolate a workstation with confirmed malware from the network.
- **Alert triage workflows** — Automatically close alerts that match known false positive patterns.
- **Notification and escalation** — Trigger Slack/Teams alerts or ticket creation when defined conditions are met.

This reduces the volume of manual touchpoints without removing analyst oversight.

SOAR + Splunk Enterprise = Speed + Clarity

Security Orchestration, Automation, and Response (SOAR) platforms integrated with Splunk allow you to accomplish the following:

- Trigger playbooks (workflows) directly from correlation searches.
- Document every automated action for auditability.
- Feed outcomes back into Splunk for continuous tuning.

For example, a Splunk rule detecting a suspicious login from a foreign country can automatically trigger a SOAR playbook that does the following:

- Pulls user context from IAM systems.
- Checks for recent MFA bypass attempts.
- Suspends the account if confidence is high.
- Notifies the analyst with a full chain-of-events log.

Maintaining Visibility and Control

Automation should never remove your ability to answer, "What just happened?" to preserve visibility, pay attention to the following:

- **Log every automated action in Splunk** so it's searchable alongside other security events.
- **Require human approval for destructive or high-impact actions** like mass account lockouts or system reboots.
- **Use a MDR partner to validate playbooks regularly,** ensuring they align with evolving threat behavior and business risk.

The MDR Advantage

A co-managed MDR provider can do the following:

- Help **design, test, and tune** Splunk-SOAR playbooks.
- Ensure automation **reduces false positives without reducing coverage.**
- Provide **24/7 oversight** so automation is monitored even outside business hours.

PRO TIP: ***Start small. Automate one or two high-confidence workflows, measure the impact, and expand only when you've confirmed both efficiency gains and visibility safeguards.***

Automation should enhance the speed of your SOC without sacrificing its visibility. In an environment powered by Splunk, the most effective SOC manager views automation as a precise tool. They use it to reduce noise, accelerate validated actions, and provide analysts with the time and focus to concentrate on the most important threats.

STRATEGY 7:

REDUCE ANALYST BURNOUT WITHOUT ADDING HEAD COUNT

HOW CO-MANAGED MDR OFFLOADS THE RIGHT TASKS, MAINTAINING TEAM HEALTH WHILE SCALING OPERATIONS

Alert fatigue is more than just a buzzword; it can be detrimental to your career. In SOCs that rely heavily on Splunk, analysts often encounter an overwhelming number of alerts, manual triage processes, and after-hours escalations. Over time, this situation results in slower investigations, missed detections, higher staff turnover, and a loss of valuable institutional knowledge. For SOC managers, replacing exhausted analysts is not only costly but also disruptive to operations.

The reality is that you cannot simply resolve this issue by hiring more staff. Skilled security professionals are rare, costly, and difficult to retain. Instead, the crucial approach is to optimize your team's workload. This involves offloading repetitive, low-value, or after-hours tasks so that analysts can concentrate on more complex, high-impact investigations.

Identifying the Burnout Triggers in Splunk Environments

Common burnout accelerators include the following:

- **High alert volume** with low fidelity, forcing analysts to sift through noise.
- **Lack of 24/7 coverage**, creating unsustainable on-call rotations.
- **Manual investigations** that could be automated or delegated.
- **Tool sprawl** requiring analysts to context switch across multiple consoles.

These problems extend beyond mere productivity; they fundamentally concern human sustainability.

How to Offload Without Losing Control

Co-managed MDR partnerships are designed for exactly this scenario. They can take over the following:

- **Initial triage and validation** of Splunk alerts, escalating only those that matter.
- **24/7 monitoring**, ensuring no alert backlog builds overnight or on weekends.
- **Detection tuning** to reduce false positives at the source.
- **Enrichment and correlation** to deliver ready-to-act incidents instead of raw alerts.

Your team retains control over the platform, rules, and incident response policies without the constant burden of processing every alert themselves.

Protecting Analyst Morale and Performance

Reducing burnout isn't just about taking work away—it's about making the work more meaningful:

- **Give analysts challenging investigations,** not repetitive triage.
- **Involve them in threat hunting and detection engineering,** where their skills make the biggest impact.
- **Rotate responsibilities** to break up monotony and spread expertise.
- **Track and celebrate wins,** such as high-impact incidents resolved or detection coverage improvements.

The MDR Impact on Burnout Reduction

With a capable MDR partner, organizations have reported the following:

- **90% reduction in false positive**s hitting analyst queues.
- **Fewer overnight and weekend callouts,** improving work–life balance.
- **Lower turnover,** preserving institutional knowledge, and detection expertise.
- **Higher job satisfaction,** as analysts spend more time on advanced work.

PRO TIP: ***Proactively measure burnout risk. If alert queues consistently exceed your team's daily investigative capacity, you are already on the path to losing talent, and it is time to bring in additional support.***

You don't have to sacrifice your team's well-being or increase your head count. By strategically offloading Splunk alert triage, tuning, and after-hours coverage to a trusted MDR partner, you can safeguard both your security posture and your team. This approach keeps your analysts engaged, effective, and prepared to address the most critical threats.

STRATEGY 8: RUN A SPLUNK HEALTH CHECK BEFORE IT BECOMES A LIABILITY

DETECTION COVERAGE, INGESTION HYGIENE, AND RULE PERFORMANCE; USING THE DEEPWATCH DIAGNOSTIC FRAMEWORK

Splunk's effectiveness relies heavily on the quality of the data you input, the rules you implement, and how well you maintain the system over time. Without regular assessments, even the most advanced Splunk environments can deteriorate into costly, noisy, and underperforming tools. This can lead to missed detection opportunities and overwhelm your analysts with unnecessary noise.

A **Splunk Health Check** serves as your early warning system. It ensures that your environment is properly configured for the threats that matter to you, that data ingestion is purposeful and cost-effective, and that correlation rules provide actionable alerts rather than unnecessary noise. Skipping this process can turn Splunk into a liability: you may end up paying for data ingestion that you don't utilize, miss important detections you assumed were covered, and lose confidence in your security metrics.

Key Areas Every Splunk Health Check Should Cover

1. **Detection Coverage**
   - Are your rules mapped to MITRE ATT&CK or other threat models?
   - Do you have coverage for your most critical assets and business processes?
   - Are there redundant or outdated rules that can be retired?
2. **Ingestion Hygiene**
   - Are you ingesting data "just in case" or mapped to specific use cases?
   - Are duplicate or irrelevant logs inflating your licensing costs?
   - Is parsing consistent, with minimal errors?
3. **Rule Performance**
   - What's your true vs. false positive rate?
   - Are suppression rules updated to match evolving patterns?
   - Are your correlation searches optimized for performance and accuracy?
4. **Operational Readiness**
   - Is your SOC able to investigate all high-priority alerts within SLA?
   - Are escalation workflows documented and tested?
   - Is 24/7 coverage in place, or do alerts age overnight?

Why CISOs Benefit from a Formalized Health Check

A formal Splunk Health Check is not just a technical exercise; it is a strategic one. The results should provide you with the following:

- **A prioritized list of gaps to close** (by risk level, not just technical category).
- **An ingestion cost-to-value map** showing where to cut waste.
- **A rule maturity roadmap** focusing on coverage that matters most to the business.
- **Metrics for executive reporting**, proving detection improvements over time.

The Deepwatch Diagnostic Framework

Deepwatch's Splunk Health Check uses a structured, CISO-friendly process:

- **Ingestion Review** — Align logs to use cases, drop the noise, and cut cost.
- **Detection Fidelity Analysis** — Identify the high-noise rules and tune them for precision.
- **Coverage Mapping** — Show exactly which MITRE ATT&CK tactics and critical assets are covered and which aren't.
- **Operational Readiness Audit** — Assess whether your SOC can handle current alert volume and SLAs.

PRO TIP: ***Schedule a Health Check quarterly. Threats evolve too quickly for a "set it and forget it" SIEM, and quarterly reviews ensure Splunk remains an asset, not an expense line you can't defend.***

A Splunk Health Check helps you distinguish between merely believing you're protected and actually knowing you are. It ensures that your detection stack remains efficient, relevant, and reliable. This way, when the board inquires if you can mitigate the most significant threats, you can respond confidently and with evidence.

STRATEGY 9: USE MITRE ATT&CK AS A NORTH STAR, NOT JUST A CHECKBOX

ALIGNING RULES TO REAL THREAT BEHAVIOR, MAPPING AND MEASURING COVERAGE OVER TIME

The MITRE ATT&CK framework has become the standard for describing adversary tactics, techniques, and procedures (TTPs). However, in many Splunk-driven SOCs, it is often treated merely as a compliance checkbox—an exercise completed once for a report and seldom revisited. This approach misses the main purpose of the framework.

The true value of MITRE lies not in simply stating, "We have guidelines for 40 techniques." Instead, it serves as a strategic framework that guides detection engineering, helps prioritize coverage for the most critical threats, and allows for measuring progress over time. In essence, MITRE should be viewed as your North Star for detection maturity, rather than just a static scorecard.

Why the MITRE ATT&CK Framework Should Drive Your Splunk Strategy

When aligned to MITRE, your Splunk detections can do the following:

- **Prioritize coverage where it counts** — Focus on techniques relevant to your industry, technology stack, and threat actors targeting you.
- **Identify gaps** — Clearly see where no current rule or correlation search addresses a given technique.
- **Avoid redundancy** — Reduce duplicate detections that add noise without adding value.
- **Show progress** — Track the growth of your coverage quarter-over-quarter in a way executives can visualize.

The Role of MDR in MITRE ATT&CK-Driven Detection

A co-managed MDR partner can accelerate your MITRE maturity by doing the following:

- Mapping your detections accurately to techniques and sub-techniques.
- Creating high-fidelity Splunk rules for high-priority techniques.
- Running regular simulations to validate coverage.
- Providing **executive-ready MITRE ATT&CK heat maps** to show progress and justify the budget.

Building MITRE into Your Detection Lifecycle

1. **Map current rules to MITRE**
   - Use Splunk Enterprise Security or a third-party mapping tool to align existing correlation searches to specific techniques.
   - Validate that mappings are accurate—not all detections claiming to cover a technique truly do.
2. **Prioritize Based on Threat Intel**
   - Cross-reference MITRE mappings with the TTPs used by known adversaries in your sector.
   - Focus on tuning and new content creation on these high-risk techniques first.
3. **Continuously Test and Validate**
   - Use breach-and-attack simulation tools to confirm Splunk rules detect the intended techniques.
   - Retire or improve detections that don't trigger reliably.
4. **Report in Business Terms**
   - Present coverage growth in a simple visual: "We increased the detection coverage of top 10 industry-relevant techniques from 60% to 85% in two quarters."
   - Link coverage improvements to risk reduction and faster response times.

PRO TIP: ***Targeting all MITRE techniques for 100% coverage is unrealistic and unnecessary. Instead, concentrate on the techniques most likely to affect your organization, ensuring they are detected with high accuracy.***

MITRE ATT&CK is not just a compliance framework. When used as your detection compass, it ensures that Splunk is precisely tuned to catch significant threats, demonstrates progress to stakeholders, and fosters continuous improvement in your SOC's effectiveness.

STRATEGY 10: TREAT MDR AS A STRATEGIC EXTENSION, NOT A VENDOR SWAP

PARTNER MODELS VS. OUTSOURCING, WHAT MAKES CO-MANAGED MDR DIFFERENT

Many CISOs worry that "outsourcing detection" means losing control over tools, processes, and visibility. Traditional MSSPs often heighten this concern by using their own environments and tools, offering little transparency about their detection methods and incident escalation. Consequently, organizations may end up in a transactional vendor relationship rather than a true partnership.

Modern MDR, particularly in a co-managed model, operates differently. The aim is not to replace your team or technology; rather, it is to integrate seamlessly with them. This approach provides additional scale, expertise, and 24/7 coverage while allowing you to retain the value of your existing investments in tools like Splunk EDR and vulnerability management.

From Vendor Swap to Force Multiplier

A strategic MDR extension should do the following:

- Operate leveraging your environment — using your Splunk instance, your rules, and your policies.
- Augment and enhance your team's capabilities — not replace them, but give them more bandwidth to focus on advanced investigations, threat hunting, and strategic security initiatives.
- Provide continuous tuning and detection engineering — so your Splunk rules evolve with the threat landscape, not just when something breaks.
- Offer full transparency — you see exactly what's being detected, how it's being triaged, and why it's being escalated.
- Enable preemptive security — with threat intel, threat hunting, and attack simulations to stop threats before they can be exploited.

Why Co-Managed MDR Works for Splunk

For Splunk-heavy SOCs, a co-managed MDR model offers unique advantages:

- No rip and replace — you keep your Splunk stack; the MDR team enhances it.
- Shared visibility — both your analysts and the MDR team operate from and have complete visibility into the same dashboards and alerts.
- Platform-specific expertise — the MDR provider has expertise in Splunk tuning, ingestion optimization, and correlation search engineering.
- 24/7 monitoring without 24/7 hiring — instantly extend coverage to nights, weekends, and holidays without expanding head count.

Signs You're Ready for MDR as an Extension of Your Team

Consider co-managed MDR if the following applies to you:

- Have a strong Splunk setup but limited after-hours coverage.
- Spend more time on alert triage than on actual investigations.
- Struggle to keep detection logic current with emerging threats.
- Need board-ready reporting but lack the cycles to produce it.

The Partnership Mindset

A true MDR extension should feel like an organic part of your SOC, not a separate black box service. This means the following:

- Regular joint reviews of detection coverage and operational metrics.
- Collaborative incident response playbook development.
- Open communication channels for quick context sharing during investigations.
- Strategic roadmapping sessions to align MDR capabilities with business goals.

PRO TIP: ***Evaluate MDR providers on their ability to operate in your environment and enhance your tools, not just on their marketing claims about speed or coverage. The best partner will measure success on the same terms you do—reduced risk, faster response, and making your team more efficient and productive.***

MDR is not meant to replace your SOC; rather, it aims to enhance its strength, speed, and resilience. In a co-managed model, your Splunk environment becomes a collaborative battleground. Your MDR provider acts as your frontline ally, and together, you can improve your security posture.

WHY DEEPWATCH: THE PARTNER PURPOSE-BUILT FOR SPLUNK-POWERED SOCS

24/7 RESPONSE WITHOUT LOSING CONTROL AND BUILT-IN TUNING, CUSTOMIZATION, AND ADVISORY

If Splunk is the backbone of your SOC, you need a partner who understands it deeply. Deepwatch enhances your detection capabilities without compromising your control over tools or strategy. We help security leaders operate Splunk at peak performance with precise detections, round-the-clock coverage, and a commitment to prioritizing your needs.

Unlike traditional MSSPs, we don't require you to change your SIEM or adopt our tools. We work within your Splunk environment to enhance your existing detections, ensuring your SOC never misses a high-fidelity alert. You retain ownership of your platform, data, and policies, while we provide the expertise and support to maintain optimal performance.

24/7 Response Without Losing Control

Deepwatch provides continuous monitoring, triage, and incident escalation directly in your Splunk workflows—without inserting a "black box" between you and your detections.

- **Always-on coverage** — Nights, weekends, and holidays are fully covered, with high-priority incidents escalated in real time.
- **Shared visibility** — You see exactly what we see, in your own Splunk dashboards and alerts.
- **Your policies, our execution** — We respond according to your defined workflows and escalation paths.

This model means your SOC is never blind, never idle, and never dependent on someone else's proprietary system for critical security data.

Built in Tuning, Customization, and Advisory

Splunk's power lies in its flexibility — but that flexibility requires constant care. Deepwatch handles the engineering heavy lifting so your team can focus on the big picture:

- **Precision tuning** — Continuous optimization of correlation searches to reduce false positives and surface high-value threats.
- **Detection engineering** — Development and refinement of rules mapped to MITRE ATT&CK and tailored to your threat profile.
- **Ingestion optimization** — Aligning data sources to defined use cases, cutting waste and costs.
- **Strategic advisory** — Regular reviews with a named detection engineer and CISO-level advisor to align security operations with evolving business priorities.

This combination of tactical support and strategic guidance keeps your Splunk stack lean, sharp, and aligned to your mission.

The Deepwatch Difference for Splunk-Powered SOCs

- **Co-managed approach** — We're an extension of your SOC, not a replacement.
- **Platform-first philosophy** — We build on the tools you've invested in, not ours.
- **Expert-led operations** — Every account is supported by seasoned detection engineers, threat hunters, and incident responders who live and breathe Splunk since 2017.
- **Business-aligned metrics** — We guarantee that reporting is tied to reduced risk and operational ROI.

PRO TIP: ***The best SOC not only detects threats faster but also improves continuously. With Deepwatch, Splunk is always evolving to address the challenges you will face tomorrow.***

YOUR NEXT STEP: BOOK A SPLUNK OPTIMIZATION BRIEFING

HOW TO ASSESS READINESS AND FIT, AND WHAT TO EXPECT FROM A HEALTH CHECK

If Splunk is central to your SOC but you suspect it could run leaner, faster, and with higher fidelity, a **Splunk Optimization Briefing** is your logical next move.

In this short, targeted session, we'll cover the following:

- Assess readiness and fit — Review your current Splunk setup, coverage model, and operational goals.
- Run a mini health check — Identify quick wins in ingestion hygiene, rule tuning, and detection coverage.
- Outline a path forward — Show how to reduce noise, improve visibility, and strengthen 24/7 response without replacing your stack.

RESULT: You'll walk away with a clear, actionable plan to get more value from the Splunk investment you already own — and a vision of what "optimized" really looks like.

BOOK A CALL

DEEPWATCH™

Always Watching. Always Protecting.™

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**