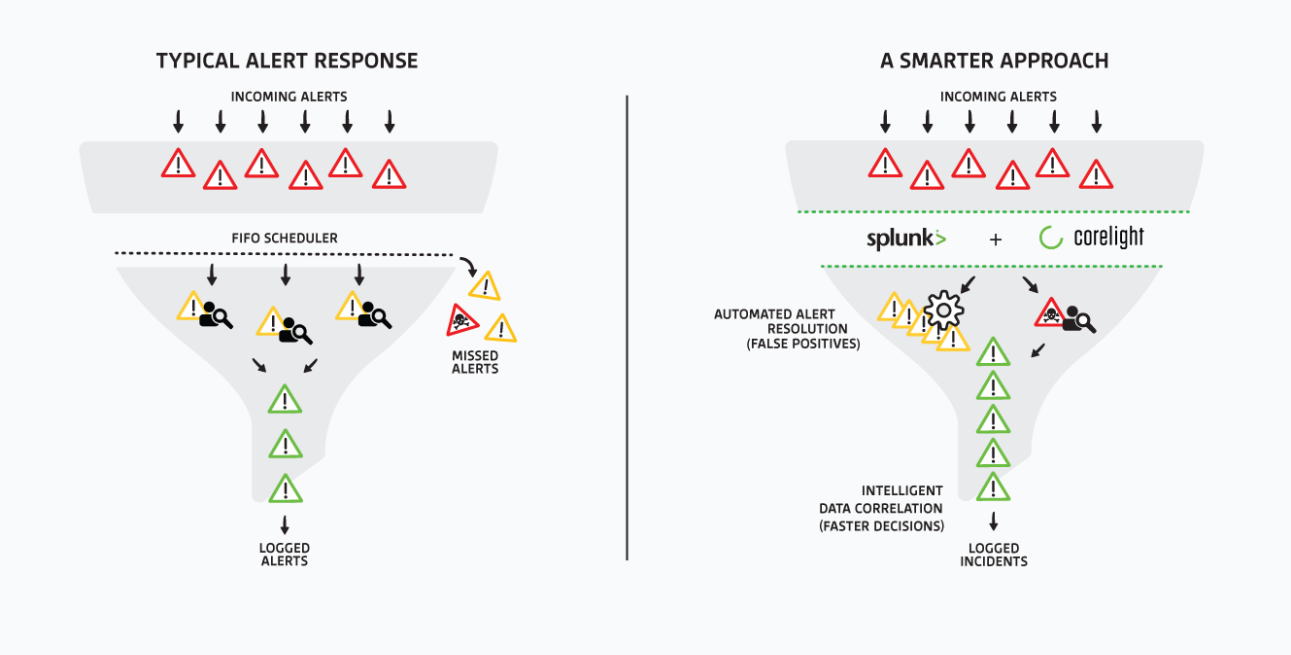
Joint Solution

Splunk® SOAR Playbooks

Expert-level impact from every analyst

Alert fatigue is one of the most devastating problems for SOCs today. Ever-increasing network alert volume combined with a chronically underfilled talent pool means that teams are stretched too thin, inviting breaches. Corelight and Splunk SOAR have an answer. Starting with extraordinary data, a powerful SOAR platform, and expert playbooks, you can cut down on alert noise and elevate the effectiveness of your entire SOC team.

The Corelight / Splunk SOAR solution:



Joint Solution: Corelight and Splunk SOAR

Splunk SOAR Playbooks from Corelight	• Eliminate 50% of alerts before they hit the human chain • Help each of your analysts become uniformly excellent • Develop your analysts so they can take on bigger challenges

The challenge: Alert fatigue

For such a thorny problem, it's actually easy to pinpoint the origin of alert fatigue. For years, cybersecurity has been captivated by trying to "find bad." While that makes intuitive sense, alerts necessitate review and disposition. This requires evidence, but what if that evidence isn't there, or it takes too long to find? The alert backlog grows, and the human chain will eventually break as analysts are forced to guess or even ignore alerts to clear their call screen.

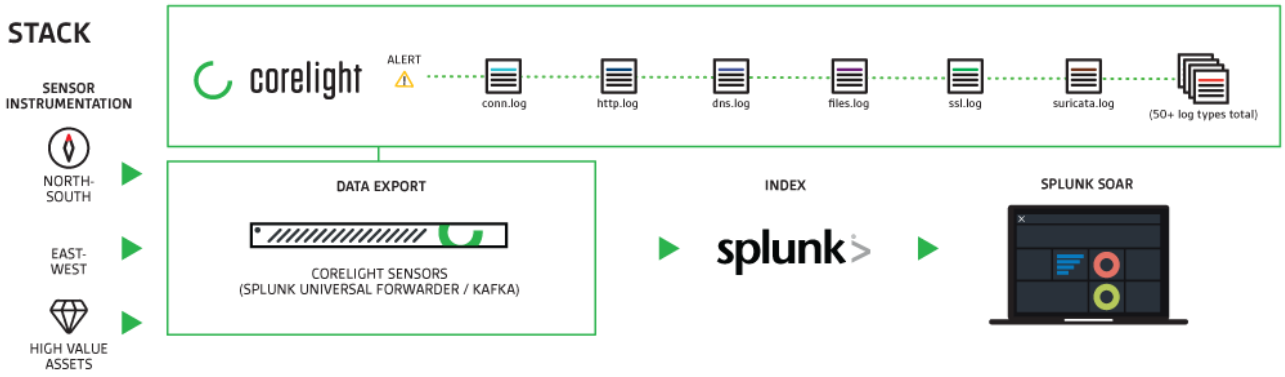
> ***Analysts can receive 2000–6000 alerts a day***

As alerts have multiplied, the number of people qualified to actually do something with them has dwindled. The result? The real work of network defense is interrupted, as mistakes or omissions now filter down to higher-level analysts. Better data, tools, and processes are needed.

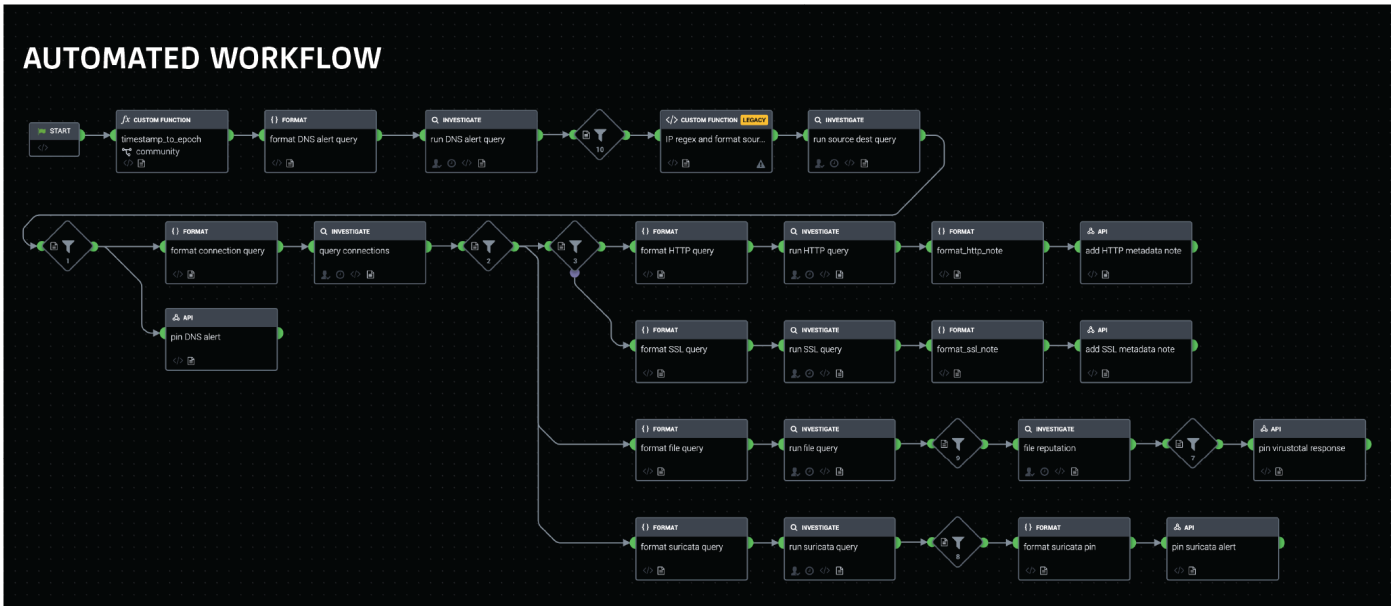
The answer to alert fatigue is as clear as its cause: reduce the number of alerts that analysts see, and cut time to resolution. Automation can do both.

A robust SOAR platform cuts through unimportant alerts, while at the same time improving decision quality across inconsistent analyst skill sets.

For SOAR to reach its true potential, however, you must replace a patchwork of non-standardized data sources with precorrellated, security-centric data:



How to transform your SOC with Splunk SOAR Playbooks from Corelight



1. Gather the right data to feed your SOAR playbook
Clear away legacy logging systems and start collecting normalized, security-centric Corelight data that contains critical information, and nothing else.

2. Automate away time-consuming, ultimately useless alerts
Start by using playbooks to screen out the obvious, like repetitive alerts that all point to the same event, or alerts that can't lead to an issue, such as DNS queries that don't have a response.

3. Deliver expertise to help analysts make great decisions fast
Our experts have vast experience in alert investigation, which they've translated into Corelight playbooks. Corelight pulls together relevant tradecraft and information needed for alert disposition.

4. Customize playbooks and fine tune alerts
With the time your team saves, they can improve playbooks and create new ones, or make detections more accurate.

> ***Help each of your analysts become uniformly excellent***

Gain and sustain advantage with Corelight + Splunk SOAR

True automation comes from pairing the right data with a versatile platform, and Corelight and Splunk SOAR both are world-class. Together, they can even gather all the evidence Tier 1s, 2s, and 3s need to make the right call.

What makes Corelight data different:

- Structured, security-centric data that's precorrelated for SOAR
- Built on Zeek®, the global standard for network monitoring for 25 years
- Rich, yet lightweight and storable to deliver great detail, indefinitely
- Easily replace legacy sources, overcoming political and technical hurdles
- Integrates seamlessly with all your existing technology and process

Fuse signal and evidence for precorrelations

Corelight makes next-level SOAR possible by integrating the open source powerhouses Zeek and Suricata. Because Suricata alerts are embedded directly into rich Zeek logs, it's far easier to make decisions and see patterns—it's fewer steps to the same finish line.

See how it works:

WATCH NOW!

Splunk SOAR, the world's most advanced automation platform:

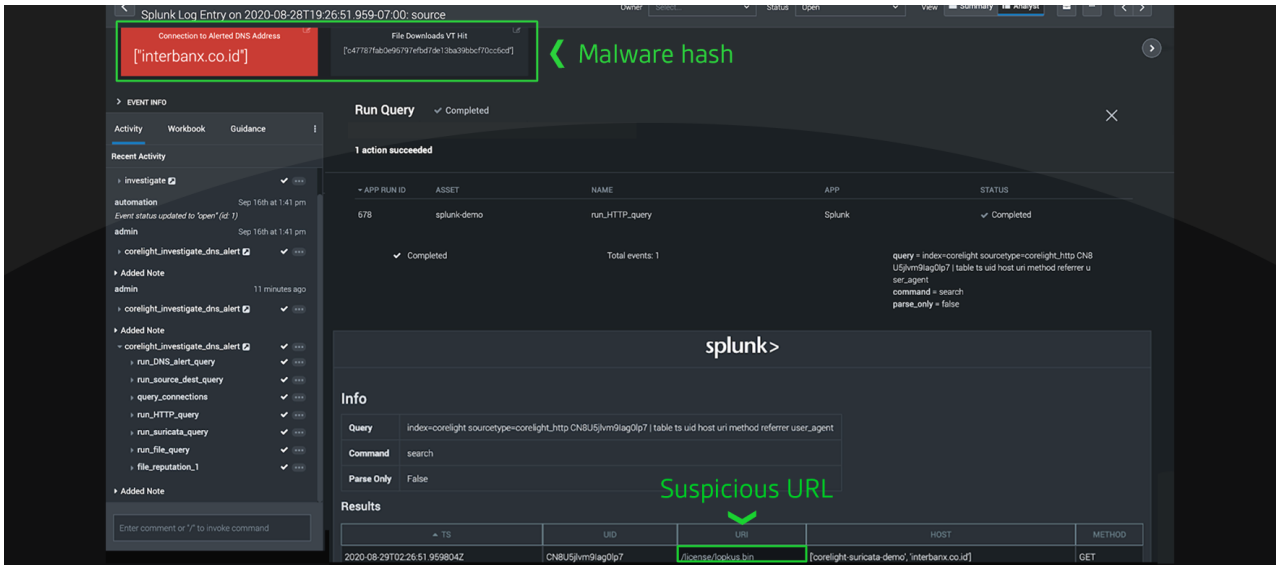
- Harness the full power of your existing security investments
- Execute actions in seconds, not hours
- Work smarter, respond faster, and strengthen your defenses

The power of SOAR playbooks, created by experts

Corelight + Splunk SOAR Playbooks make every analyst an expert. Created by elite cybersecurity practitioners, these playbooks dramatically reduce alert fatigue by leveraging years of tradecraft, exceptional data, and a powerful platform.

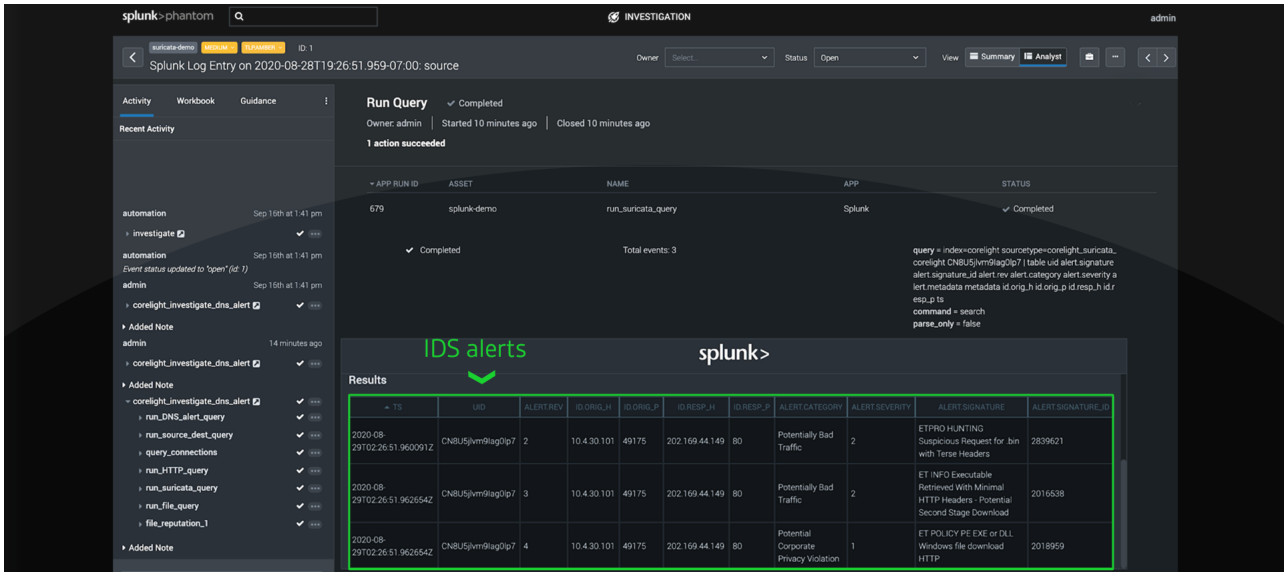
See what playbooks can do:

Weed out irrelevant alerts. *Often attackers try to compromise systems, but fail to do so. Above, a client tried to connect to a malicious site but it was offline. SOAR plus Corelight data helps analysts see when attacks go nowhere and focus on incidents that matter.*



Easily validate true incidents. *Successful attacks leave a trail of indicators—here a known malware hash, a suspicious URL…*

Joint Solution: Corelight and Splunk SOAR



...and here IDS alerts. Corelight evidence, presented by SOAR, speeds decision making and reduces attacker dwell time.

By combining the best network evidence available with playbooks written by seasoned practitioners, you can use Corelight and Splunk SOAR to dramatically reduce alert fatigue. But that's just the start. This approach can give you a lasting advantage in security, solving a host of problems by helping the people in your SOC reach their full potential. This is the promise of SOAR, delivered.

> ***Develop your analysts so they can take on bigger challenges***

What your people could be doing (instead of chasing dead-end alerts):

- Creating new playbooks to speed up IR
- Using rich data to hunt for new threats
- Tuning rulesets to make them more precise
- Looking for misconfigurations
- Training on new tools and techniques

Splunk is the world's first Data-to-Everything Platform. Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver. Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future. With more than 5,000 employees in 27 offices worldwide, we're focused on creating lasting data outcomes for our customers.

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.

All rights reserved. © Copyright 2022 Corelight, Inc.