

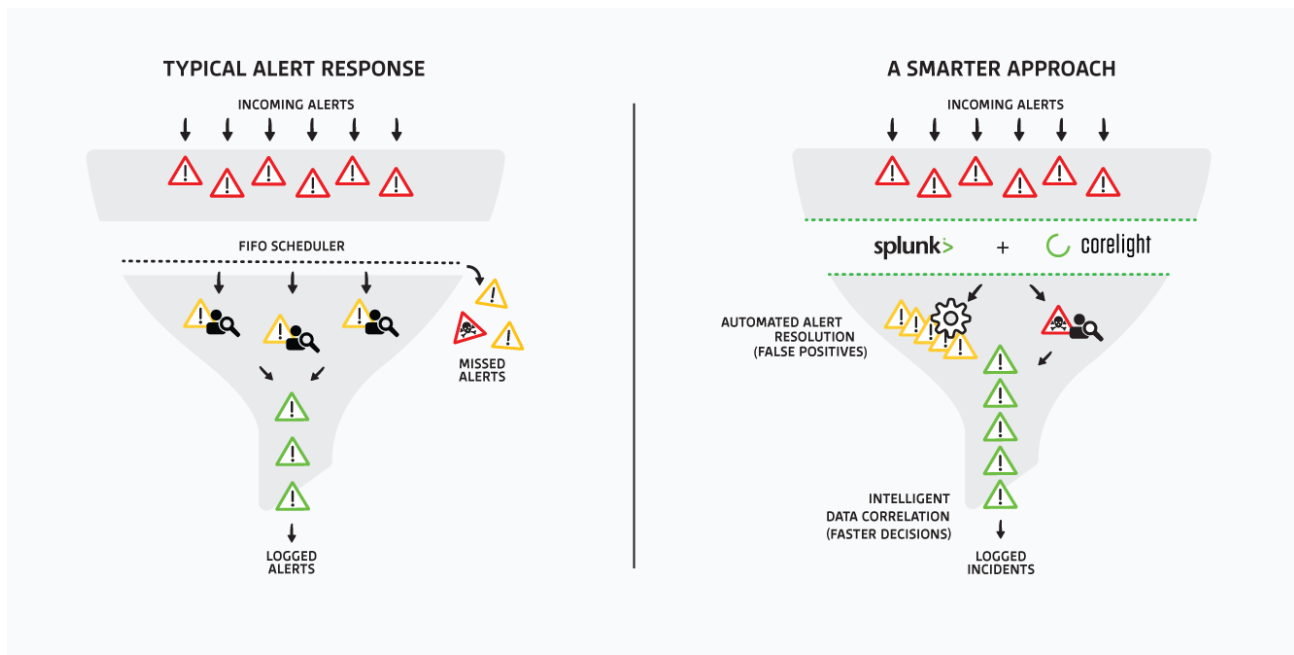
Joint Solution

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.

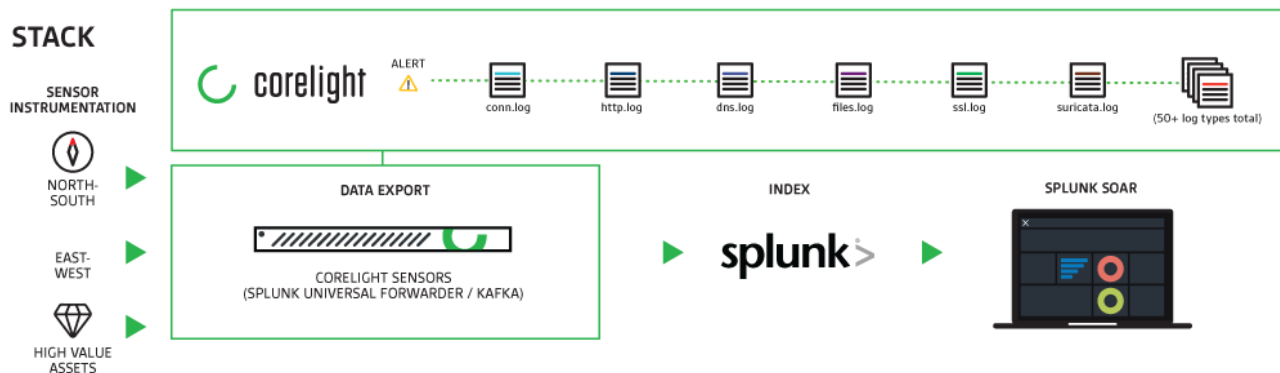
***Analysts can receive
2000–6000 alerts a day***

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.

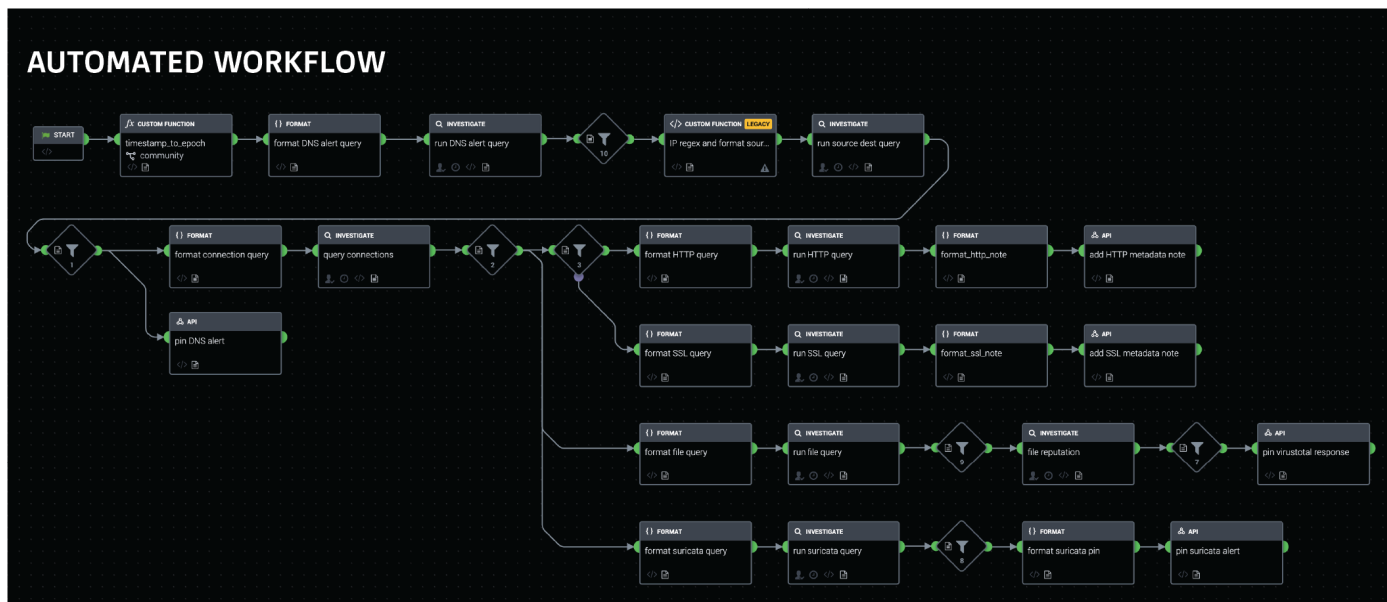
The answer to alert fatigue is as clear as its cause: reduce the number of alerts that analysts see, and cut time to resolution. Automation can do both.

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 precorellated, 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!



Field	Value
alert.action	allowed
alert.category	Generic Protocol Command Decode
alert.gid	1
alert.metadata	updated_at:2019_08_30 created_at:2015_10_26 former_category:DNS
alert.rev	6
alert.severity	3
alert.signature	ETPRO DNS SkullSecurity Encrypted Shell Possible Tunnel 2
alert.signature_id	2814578
community_id	1b214mdePmfV1visUNijTw6uPb+0=
dest_ip	34.215.241.13
dest_port	53
flow_id	2067524783758651
service	dns
src_ip	192.168.1128
src_port	62035

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:

automation 7 minutes ago

- investigate
- geolocate_ip_1
- ip_reputation_1
- whois_ip_1

automation 7 minutes ago

Event status updated to 'open' (id: 4)

admin a few seconds ago

- corelight_investigate_dns_alert
- run_dns_alert_query

Completed Total events: 24

Query: index=corelight sourcetype=corelight_dns C9Hg-kXgB6QWZKkg earliest=1598667100.35 latest=now() | table uid answer id orig_h roode_name

Command: search

Parse Only: False

Results

UID	ID.DNS.H	ROODE_NAME
C9Hg-kXgB6QWZKkg	192.168.137.63	NXDOMAIN
C9Hg-kXgB6QWZKkg	192.168.137.63	NXDOMAIN
C9Hg-kXgB6QWZKkg	192.168.137.63	NXDOMAIN

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.

Splunk Log Entry on 2020-08-28T19:26:51.959-07:00: source

Connection to Alerted DNS Address ["interbanx.co.id"]

File Downloads VT Hit ["547787fab0e9a791efbd1d813ba398bc7f0cc0d"]

Malware hash

Run Query Completed

1 action succeeded

APP RUN ID	ASSET	NAME	APP	STATUS
578	splunk-demo	run_HTTP_query	Splunk	Completed

Completed Total events: 1

Query: index=corelight sourcetype=corelight_http CN8U5jvm9lag0lp7 | table ts uid host uri method referer user_agent

Command: search

Parse Only: False

Info

Suspicious URL

Results

TS	UID	URI	HOST	METHOD
2020-08-28T02:26:51.959804Z	CN8U5jvm9lag0lp7	/license/lookup bin	[corelight-suricata-demo, interbanx.co.id]	GET

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

The screenshot displays the Splunk Cloud interface. At the top, the 'splunk> xmon' header is visible. The main content area is titled 'Run Query' and shows a completed action. Below this, a table of results is displayed, which is highlighted with a green border. The table contains three rows of data, each representing an alert. The columns are: TS, UID, ALERT REV, ID.Orig_H, ID.Orig_P, ID.Resp_H, ID.Resp_P, ALERT CATEGORY, ALERT SEVERITY, ALERT SIGNATURE, and ALERT SIGNATURE_ID. The first row shows an alert for 'ETPRO HUNTING' with a severity of 2. The second row shows an alert for 'ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download' with a severity of 2. The third row shows an alert for 'ET POLICY PE EXE or DLL Windows file download HTTP' with a severity of 1.

TS	UID	ALERT REV	ID.Orig_H	ID.Orig_P	ID.Resp_H	ID.Resp_P	ALERT CATEGORY	ALERT SEVERITY	ALERT SIGNATURE	ALERT SIGNATURE_ID
2020-08-29T02:26:51.960091Z	CN8U5jvm9iaqDp7	2	10.4.30.101	49175	202.169.44.149	80	Potentially Bad Traffic	2	ETPRO HUNTING Suspicious Request for bin with Terse Headers	2839621
2020-08-29T02:26:51.962654Z	CN8U5jvm9iaqDp7	3	10.4.30.101	49175	202.169.44.149	80	Potentially Bad Traffic	2	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download	2016538
2020-08-29T02:26:51.962654Z	CN8U5jvm9iaqDp7	4	10.4.30.101	49175	202.169.44.149	80	Potential Corporate Privacy Violation	1	ET POLICY PE EXE or DLL Windows file download HTTP	2018959

...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