Get to SOAR Faster Guide

SOAR has incredible upside. Why has it belly flopped (so far)?

Data sources that are hard to use

If your data comes from a hodgepodge of sources, you're going to have a bad time. It needs to be available (not disabled for performance/political reasons) and ready for ingest (normalized and mapped properly) Otherwise it's garbage in, garbage out.

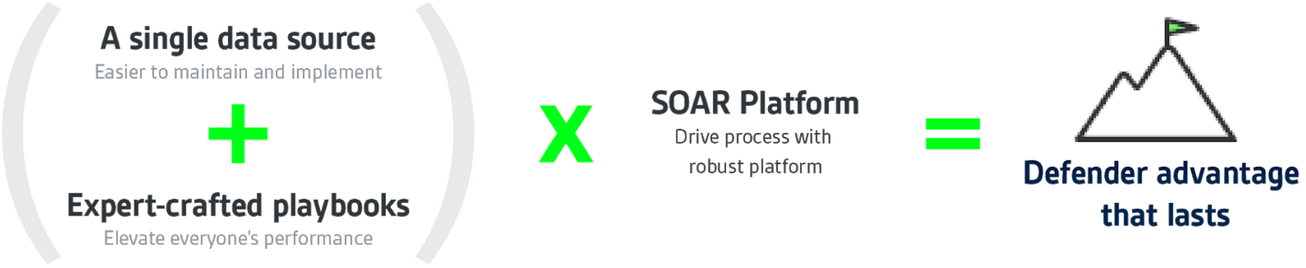
Data that wasn’t built for security

Most network data SOCs use comes from sources — like performance monitoring — that were created for a totally different purpose. This data isn’tcomprehensive or consistent enough to give you detailed evidence.

Playbooks that don’t do enough

Playbooks should automate entire core workflows, not just discrete tasks like threat intelligence lookups or firewall updates. Corelight's comprehensive data makes complex, end-to-end playbooks accessible for any SOC.

Formula for SOAR success



(A single data source

Easier to maintain and implement

+

Expert-crafted playbooks

Elevate everyone’s performance)

X

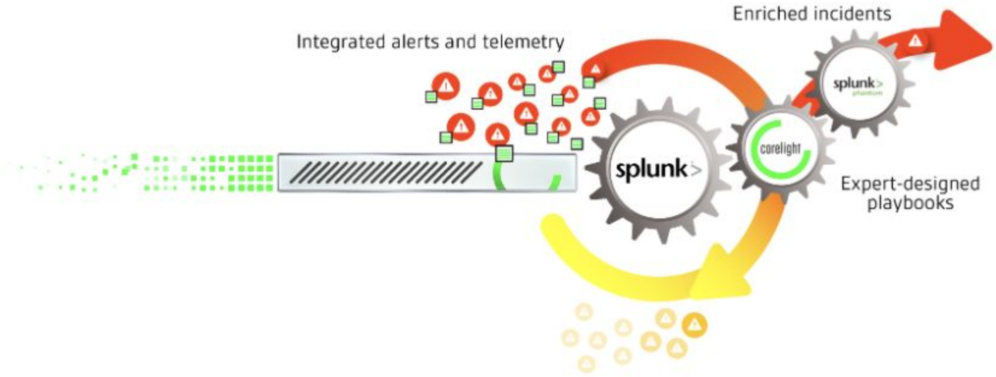
SOAR Platform

Drive process with robust platform

=

Defender advantage that lasts

How to make SOAR work, fast



To get automation's full benefits quickly, you need to pair the right data with expert playbooks on a versatile platform. This makes it easier to get SOAR up and running, and enables amazing abilities — like automatically gathering the evidence needed to make the right call.

Here's a step-by-step example on tackling alert fatigue:

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

2. Automate away time-consuming, ultimately pointless alerts
Start by screening out the obvious. For example, consolidate repetitive alerts that all point to the same event, or alerts that can't lead to an issue, like DNS queries without a response.

3. Package expertise to help your analysts overachieve
Analyst skill sets and familiarity with tools varies wildly. Give them expert playbooks to take the guesswork out of investigations. You'll get better quality and precision, while also training your team.

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

> ***"The most frequently cited barriers to excellence were lack of skilled staff (58%) and the absence of effective orchestration and automation (50%)."***
>
> *-SANS SOC survey**

The right tools make it all possible

A scalable, open, extensible SOAR platform

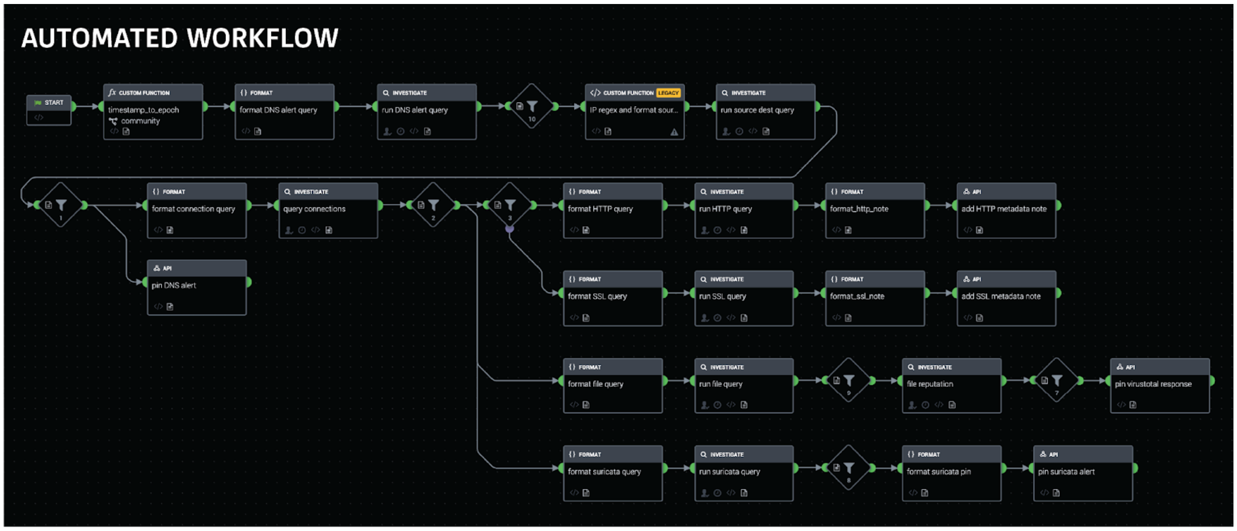
- Platforms like Splunk Phantom take action in seconds, not hours
- Harness the full power of your existing security investments
- Work smarter, respond faster, and strengthen your defenses

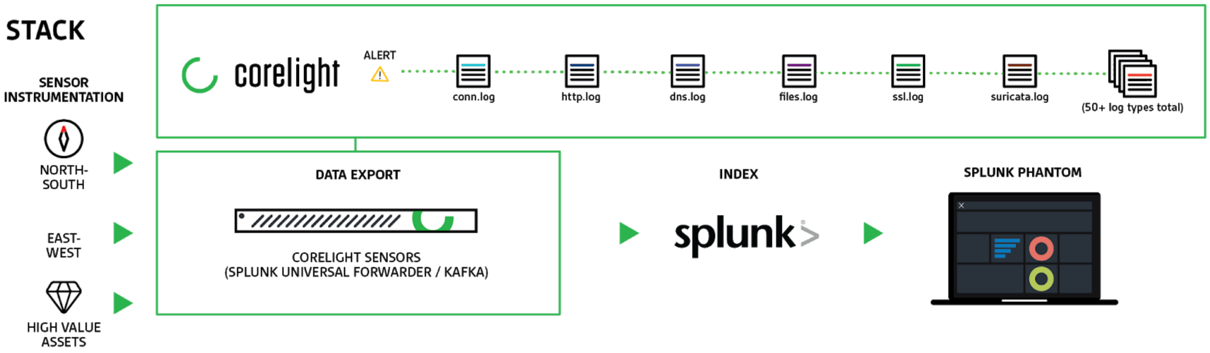
What makes Corelight data different

- 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

Playbooks created by experts, from Corelight

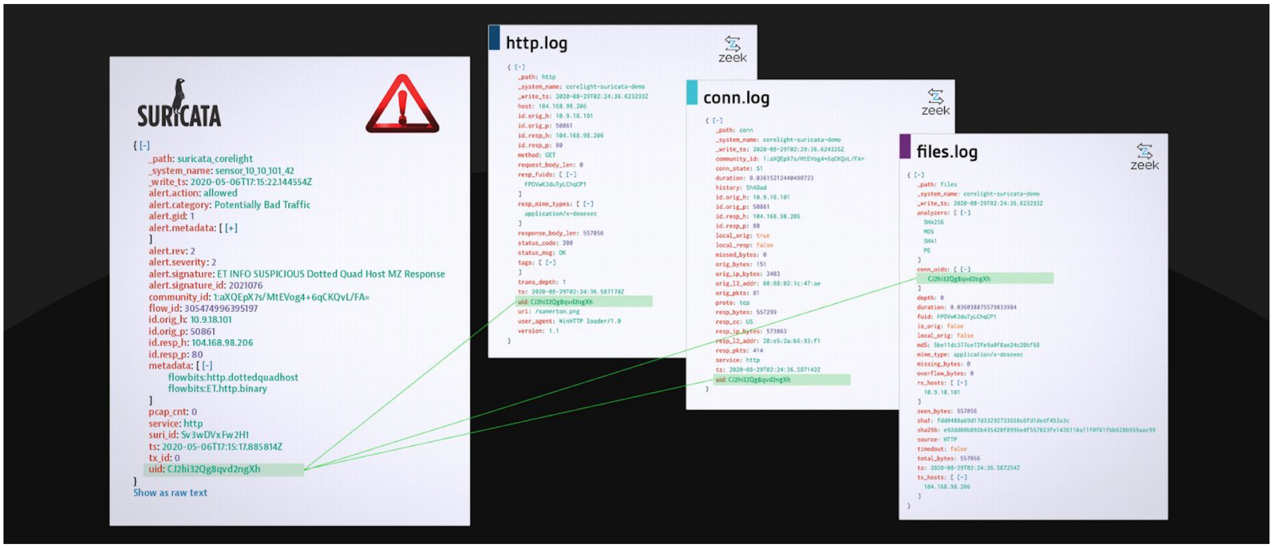
- Created by elite cybersecurity practitioners with deep experience
- Make every analyst perform better, and more consistently
- Leverages years of tradecraft to get the most out of your data and platform





Fuse signal and evidence for precorrelations

Corelight speeds up SOAR implementation by integrating the open source powerhouses Zeek and Suricata. Because alerts are embedded directly into rich logs, everything's faster down the line.



```
{ [-]
    _path: suricata_corelight
    _system_name: sensor_10_10_101_42
    _write_ts: 2020-05-06T17:15:22.144554Z
    alert.action: allowed
    alert.category: Potentially Bad Traffic
    alert.gid: 1
    alert.metadata: [ [+]
    ]
    alert.rev: 2
    alert.severity: 2
    alert.signature: ET INFO SUSPICIOUS Dotted Quad Host MZ Response
    alert.signature_id: 2021076
    community_id: 1:aXQEpX7s/MtEVog4+6qCKQvL/FA=
    flow_id: 305474996395197
    id.orig_h: 10.9.18.101
    id.orig_p: 50861
    id.resp_h: 104.168.98.206
    id.resp_p: 80
    metadata: [ [-]
        flowbits:http.dottedquadhost
        flowbits:ET.http.binary
    ]
    pcap_cnt: 0
    service: http
    suri_id: Sv3wDVxFw2H1
    ts: 2020-05-06T17:15:17.885814Z
    tx_id: 0
    uid: CJ2hi32Qg8qvd2ngXh
}
Show as raw text
```

```
{ [-]
  _path: http
  _system_name: corelight-suricata-demo
  _write_ts: 2020-08-29T02:24:36.623293Z
  host: 104.168.98.206
  id.orig_h: 10.9.18.101
  id.orig_p: 50861
  id.resp_h: 104.168.98.206
  id.resp_p: 80
  method: GET
  request_body_len: 0
  resp_fuids: [ [-]
    FPOVwK3duTyLChqCP1
  ]
  resp_mime_types: [ [-]
    application/x-dosexec
  ]
  response_body_len: 557056
  status_code: 200
  status_msg: OK
  tags: [ [-]
  ]
  trans_depth: 1
  ts: 2020-08-29T02:24:36.587178Z
  uid: CJ2hi32Qg8qvd2ngXh
  uri: /samerton.png
  user_agent: WinHTTP loader/1.0
  version: 1.1
}
```

```
{ [-]
  _path: conn
  _system_name: corelight-suricata-demo
  _write_ts: 2020-08-29T02:29:36.624325Z
  community_id: 1:aXQEpX7s/MtEVog4+6qCKQvL/FA=
  conn_state: S1
  duration: 0.03615212440490723
  history: ShADad
  id.orig_h: 10.9.18.101
  id.orig_p: 50861
  id.resp_h: 104.168.98.206
  id.resp_p: 80
  local_orig: true
  local_resp: false
  missed_bytes: 0
  orig_bytes: 151
  orig_ip_bytes: 3403
  orig_l2_addr: 00:08:02:1c:47:ae
  orig_pkts: 81
  proto: tcp
  resp_bytes: 557299
  resp_cc: US
  resp_ip_bytes: 573863
  resp_l2_addr: 20:e5:2a:b6:93:f1
  resp_pkts: 414
  service: http
  ts: 2020-08-29T02:24:36.587142Z
  uid: CJ2hi32Qg8qvd2ngXh
}
```

```
{ [-]
  _path: files
  _system_name: corelight-suricata-demo
  _write_ts: 2020-08-29T02:24:36.623293Z
  analyzers: [ [-]
    SHA256
    MD5
    SHA1
    PE
  ]
  conn_uids: [ [-]
    CJ2hi32Qg8qvd2ngXh
  ]
  depth: 0
  duration: 0.036038875579833984
  fuid: FPOVwK3duTyLChqCP1
  is_orig: false
  local_orig: false
  md5: 5be11dc377ce72fe9a0f8ae24c20bf68
  mime_type: application/x-dosexec
  missing_bytes: 0
  overflow_bytes: 0
  rx_hosts: [ [-]
    10.9.18.101
  ]
  seen_bytes: 557056
  sha1: fdd0480a69d17d33292733568c6fd1dedf453a3c
  sha256: e92dd00b092b435420f0996e4f557023fe1436110a11f0f61fbb628b959aac99
  source: HTTP
  timedout: false
  total_bytes: 557056
  ts: 2020-08-29T02:24:36.587254Z
  tx_hosts: [ [-]
    104.168.98.206
  ]
}
```

Investigate faster with alerts integrated into evidence. *Every Suricata alert contains its associated precorrelated Zeek data to bring foundational, standardized evidence all in one place, speeding investigations.*

[*] https://www.sans.org/reading-room/whitepapers/analyst/common-practices-security-operations-centers-results-2019-soc-survey-39060

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497