Challenge
A security team struggled with manual pulls of spotty data needed for investigations

Solution
Corelight delivered rich, readily-accessible network data to unlock automation.

Integrations
SIEM

Case Study

Federal SOC reduces response time by 75% via automation and DNS visibility

Background

A high-performing security operations team at a major government organization had automated many key workflows, but analysts still lost valuable time undertaking manual data source pivots and struggling to fill information gaps, especially concerning DNS traffic.

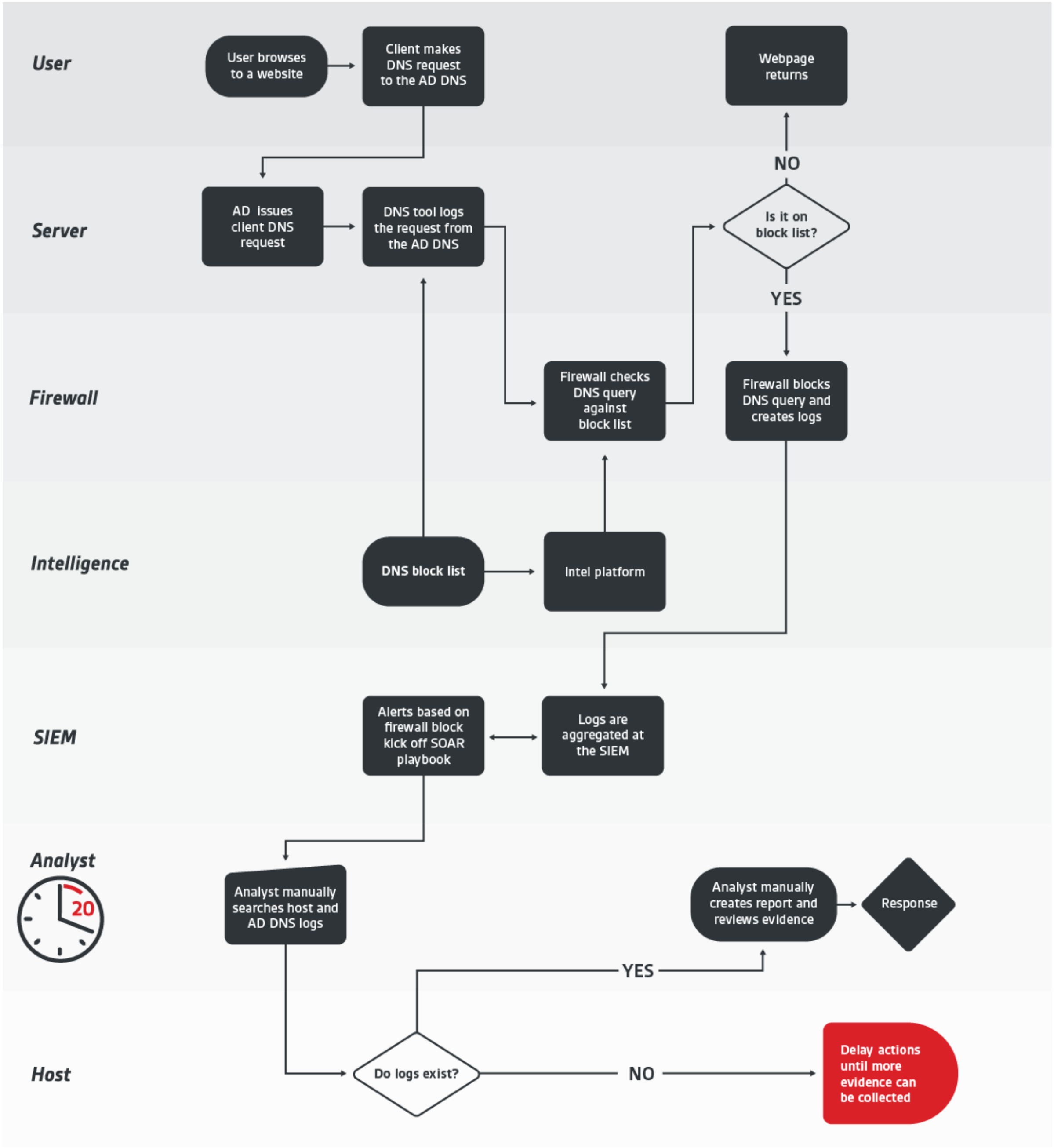
Challenges

Adversaries routinely try to hide their movements in the volume and noise of DNS traffic via techniques like DNS tunneling to communicate with c2 servers or exfiltrating data by embedding it in outbound DNS requests. Consequently, nearly every network event contains DNS forensic information in the documentation trail for security events or incidents. For example, verifying proper "Block List" operations requires analysts to confirm that perimeter security successfully blocked users who attempted to access unauthorized sites.

Associated name servers (e.g. BIND, Active Directory) make it difficult to retrieve short, real-time DNS transaction data since they generally "batch up" logs and summarize the data therein. This creates both a time lag and an information gap that forces analysts to manually search and cobble together other logs. This manual pivoting and data collection cost the team’s security analysts approximately 20 minutes per event. Additionally, DNS server records typically lack critical security detail, such as DNS query responses that could contain evidence of DNS tunnelling.

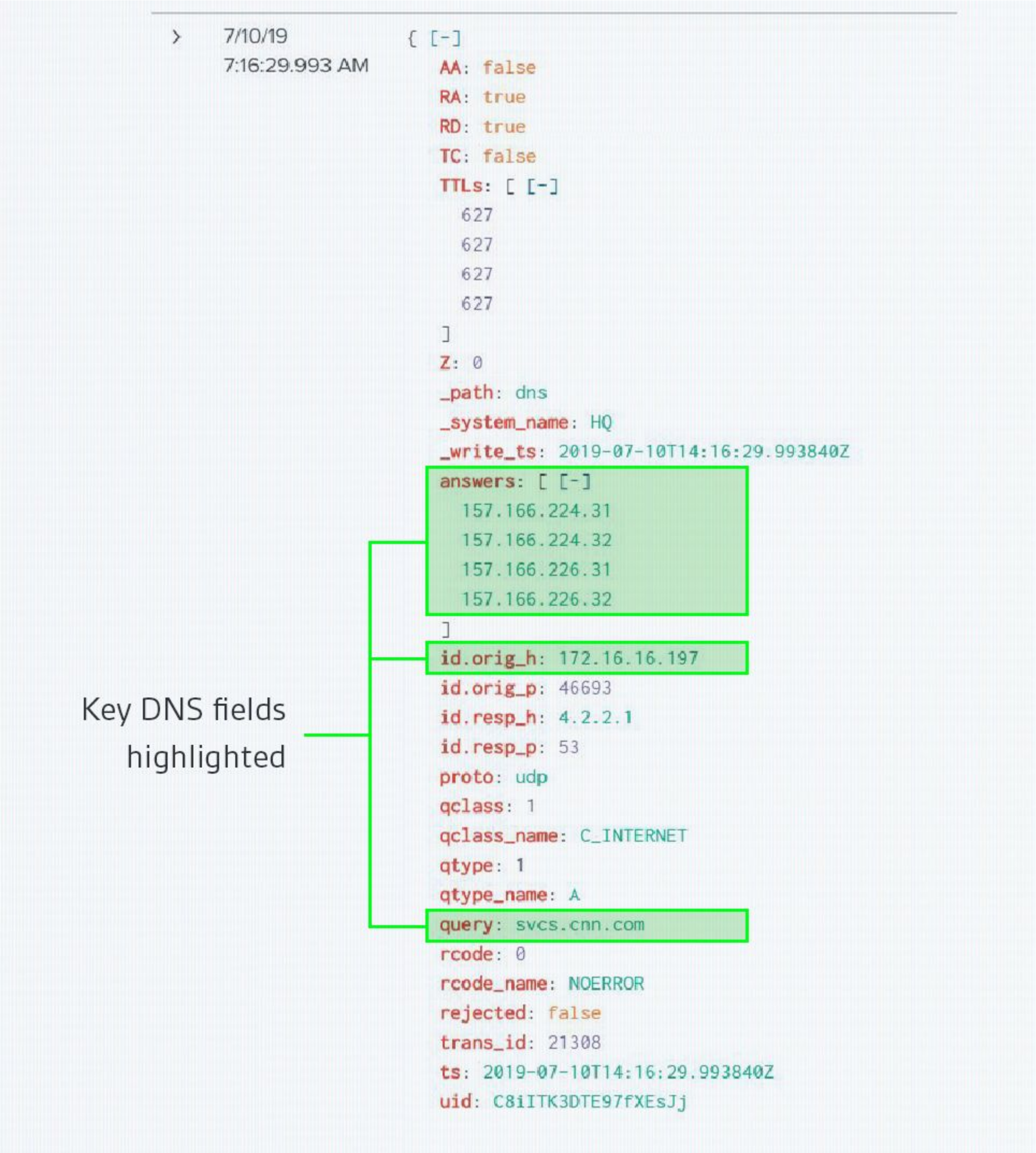
As the flowchart on the following page depicts, the team’s prevention and vulnerability scanning infrastructure was well-deployed, yet the aforementioned time lags and data gaps continued to persist.

DNS event flowchart without Corelight


User
User browses to a website
Client makes DNS request to the AD DNS
Webpage returns
NO
Server
AD issues client DNS request
DNS tool logs the request from the AD DNS
Is it on block list?
YES
Firewall
Firewall checks DNS query against block list
Firewall blocks DNS query and creates logs
Intelligence
DNS block list
Intel platform
SIEM
Alerts based on firewall block kick off SOAR playbook
Logs are aggregated at the SIEM
Analyst
20
Analyst manually searches host and AD DNS logs
Analyst manually creates report and reviews evidence
Response
YES
Host
Do logs exist?
NO
Delay actions until more evidence can be collected

Solution

The team decided to deploy and test a Corelight Sensor in the east-west traffic path between the AD servers and workstations. After reviewing Corelight's rich network logs in their SIEM they realized that virtually all of the user information they required for the event was already present in Corelight's DNS log, an example of which is shown with key DNS fields highlighted:



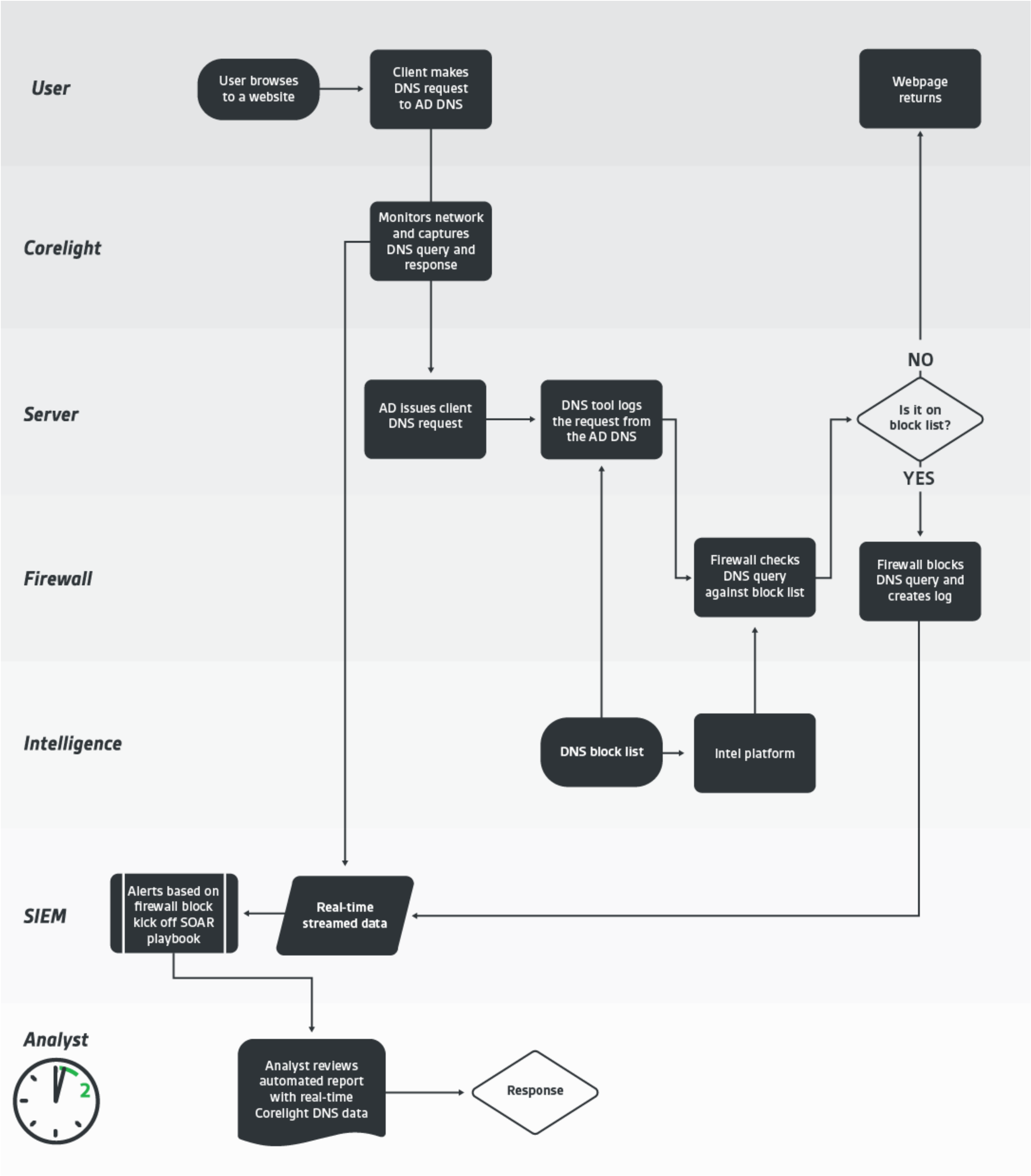
```
>   7/10/19              { [-]
    7:16:29.993 AM         AA: false
                           RA: true
                           RD: true
                           TC: false
                           TTLs: [ [-]
                             627
                             627
                             627
                             627
                           ]
                           Z: 0
                           _path: dns
                           _system_name: HQ
                           _write_ts: 2019-07-10T14:16:29.993840Z
                           answers: [ [-]
                             157.166.224.31
                             157.166.224.32
                             157.166.226.31
                             157.166.226.32
                           ]
                           id.orig_h: 172.16.16.197
                           id.orig_p: 46693
                           id.resp_h: 4.2.2.1
                           id.resp_p: 53
                           proto: udp
                           qclass: 1
                           qclass_name: C_INTERNET
                           qtype: 1
                           qtype_name: A
                           query: svcs.cnn.com
                           rcode: 0
                           rcode_name: NOERROR
                           rejected: false
                           trans_id: 21308
                           ts: 2019-07-10T14:16:29.993840Z
                           uid: C8iITK3DTE97fXEsJj
```

Key DNS fields highlighted

Armed with this new data and DNS visibility, the team quickly wrote a playbook consisting of SIEM queries that pulled recent traffic before/after the DNS request relevant to the host who triggered the alert and then enriched it with Corelight-derived user information. The result? A pre-populated event record that analysts could review to make an immediate decision and close-out, saving the team approximately 15 minutes per event, freeing up substantial team bandwidth to reinvest in higher-priority activities.

The flowchart below illustrates their new workflow with Corelight:

DNS event flowchart with Corelight


User
User browses to a website
Client makes DNS request to AD DNS
Webpage returns
Corelight
Monitors network and captures DNS query and response
NO
Server
AD issues client DNS request
DNS tool logs the request from the AD DNS
Is it on block list?
YES
Firewall
Firewall checks DNS query against block list
Firewall blocks DNS query and creates log
Intelligence
DNS block list
Intel platform
SIEM
Alerts based on firewall block kick off SOAR playbook
Real-time streamed data
Analyst
2
Analyst reviews automated report with real-time Corelight DNS data
Response

Results

This case study offers a prime example of the evolution to data-driven security models led by keen security practitioners like this federal team. Their ability to operationalize multiple data sources with orchestration and automation and accelerate mundane tasks allowed them to reclaim significant security team bandwidth and apply it to higher priority tasks. Corelight's DNS data helped them automate and reduce average response time by 75% and provides just one example of how their security stance is continually sustained and enhanced by the power and agility of the network data Corelight generates that covers dozens of protocols.

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