

How One Government Security Team Substantially Reduced Response Time by Automating Event-Handling with Corelight's rich, real-time DNS visibility

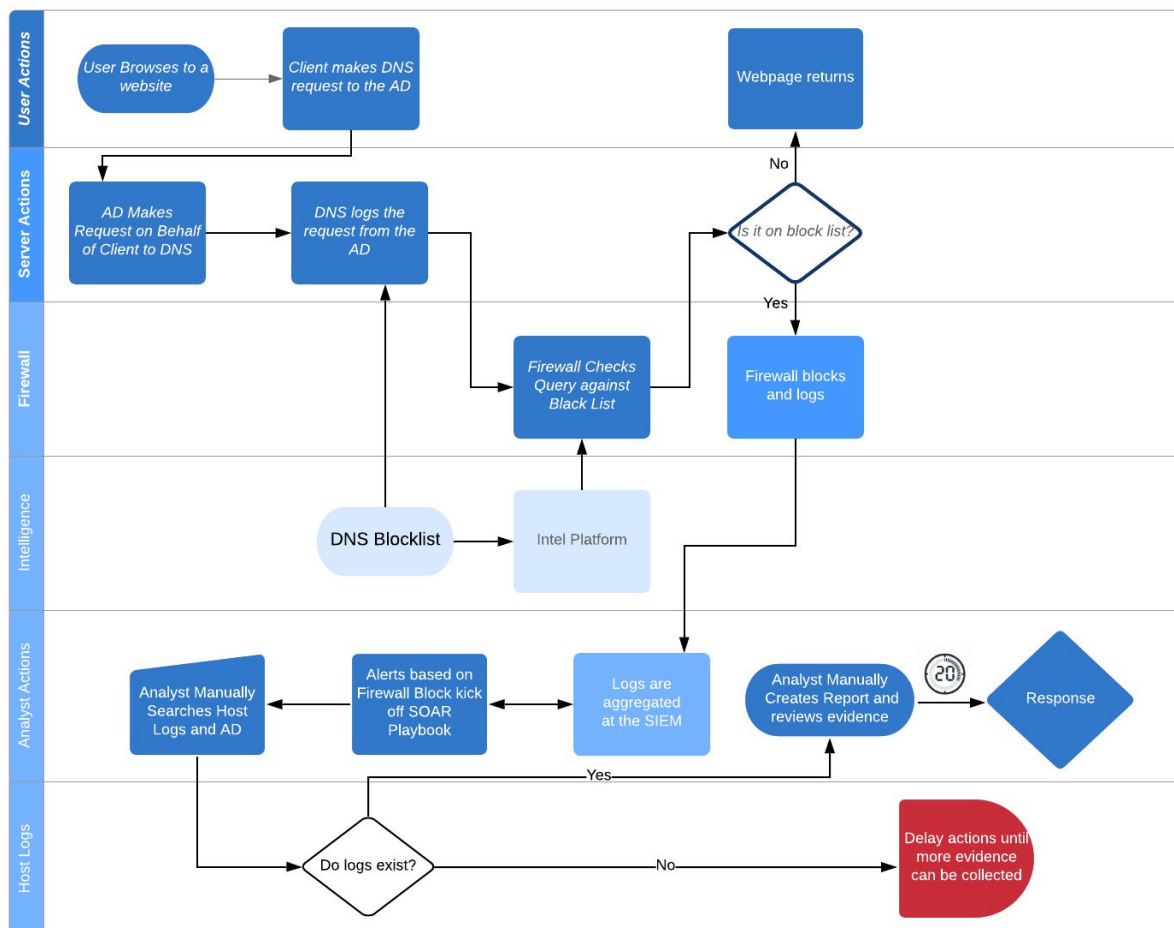
One of the most difficult applications to manage in any network is Domain Name Service (DNS) given its constant and ubiquitous use. Adversaries take advantage of this situation and regularly try to hide their movements in the volume and noise of DNS traffic, using DNS tunneling to communicate with c2 servers or even exfiltrate data by embedding it in outbound DNS requests. As a result, nearly every network event contains DNS forensic information as part of its documentation trail for security events or incidents. For example, verifying proper "Block List" operations requires analysts to confirm that users who attempted to access unauthorized sites were actually prevented by perimeter security.

Retrieving short, real-time DNS transaction data is further complicated by the fact that the associated name servers (i.e., BIND, Active Directory) generally "batch up" logs while often simultaneously summarizing information therein. This creates both a time lag and an information gap that forces analysts to manually search and cobble together other logs. This unnecessary pivoting incurs a cost on the analyst time: approximately 20 minutes wasted per event collecting the needed data. DNS server records themselves also typically lack critical security detail, such as DNS query responses that could contain evidence of DNS tunnelling, for example.

This particular use case around DNS visibility had always been a challenge at particular government organization before they became a Corelight customer. This organization is home to a small yet high-performing Security Operations team that has automated the maintenance of threat intelligence feeds.

As the flowchart on the following page depicts, their prevention and vulnerability scanning infrastructure was well-deployed, yet the time and data gaps mentioned above continued to drive analysts to manual methods.

DNS Event Flowchart without Corelight



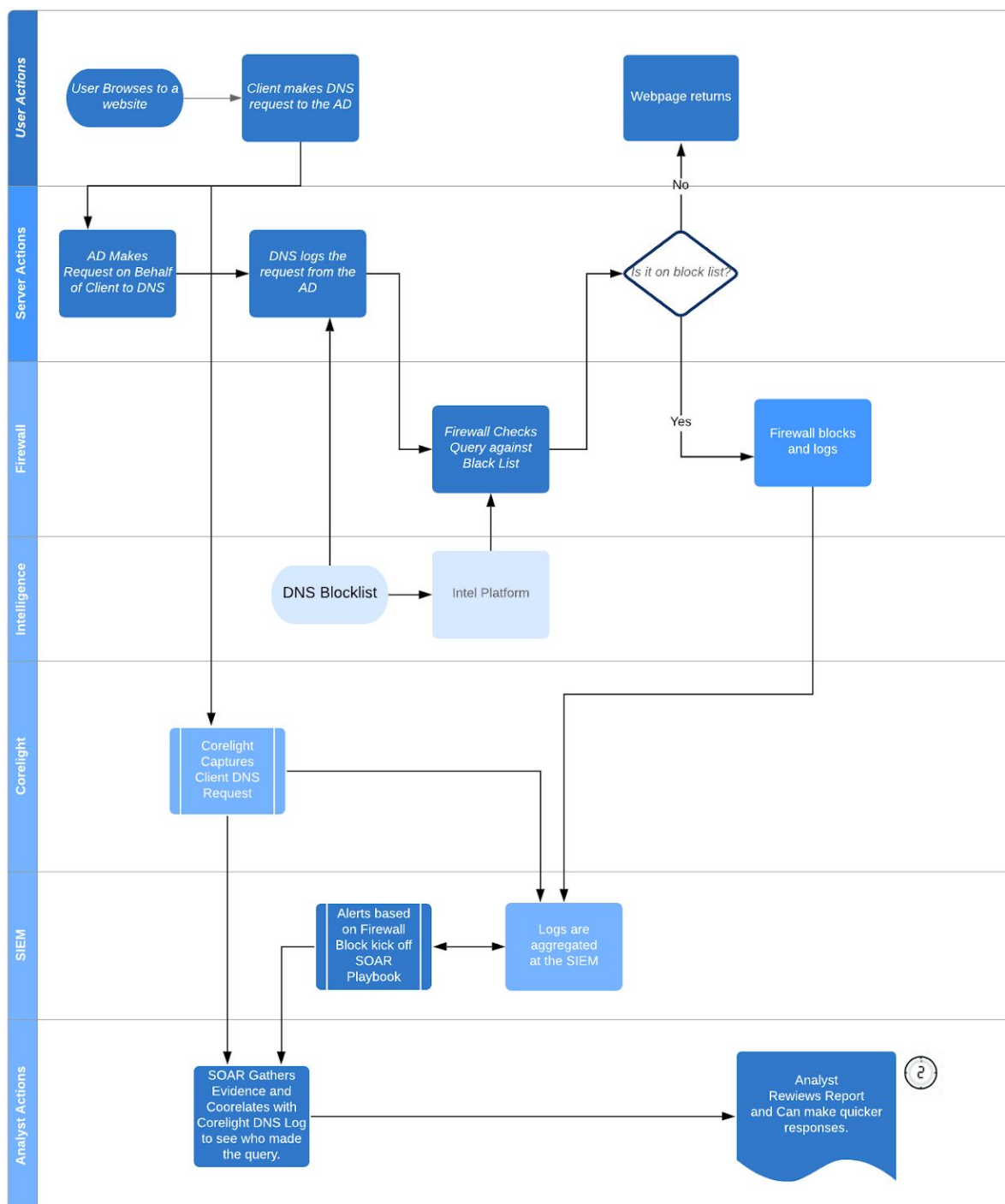
The team decided to deploy and test a Corelight Sensor in the east-west traffic path (i.e., between the AD servers and workstation VLANs) and after reviewing Corelight's logs in their SIEM they realized that virtually all of the user information they required for the event was already present in Corelight's DNS log, an example of which is shown on the following page with those 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
```

Armed with this new data and DNS visibility, the team quickly wrote a playbook consisting of SIEM queries which pulled recent traffic before/after the DNS request relevant to the host who triggered the alert and enriched it with Corelight-derived user information. The result was 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, which has freed up substantial team bandwidth to work on higher-priority activities.

The updated flowchart below illustrates their new workflow with Corelight:

DNS Event Flowchart with Corelight





This use case is an example of the evolution to data-driven security models that's being led by keen security practitioners such as the team at this government organization. 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. This is but one example of how their security stance is continually sustained and enhanced by the power and agility of insightful network data generated by Corelight.