### 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.
Case Study: Major federal security

DNS event flowchart without Corelight

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:
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.
Case Study: Major federal security

The flowchart below illustrates their new workflow with Corelight:

**DNS event flowchart with Corelight**
Case Study: Major federal security

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.

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