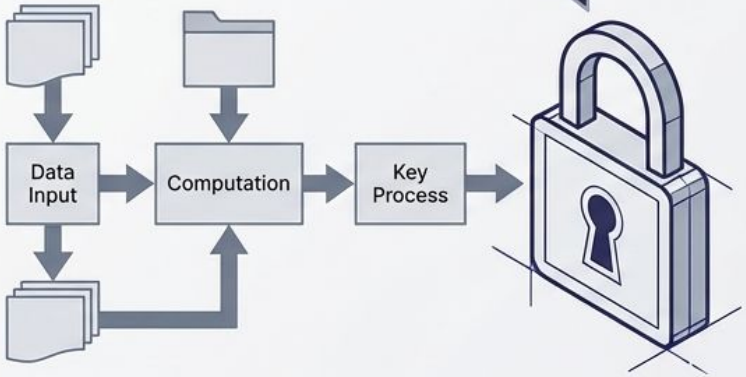

corelight
The Quantum Threat &
The Path to Crypto-Agility
Navigating Harvest Now, Decrypt Later and the
Mandate for Automated Cryptography Discovery
Vince Stoffer - Field CTO Corelight
NotebookLM

A Fundamental Leap in Computation

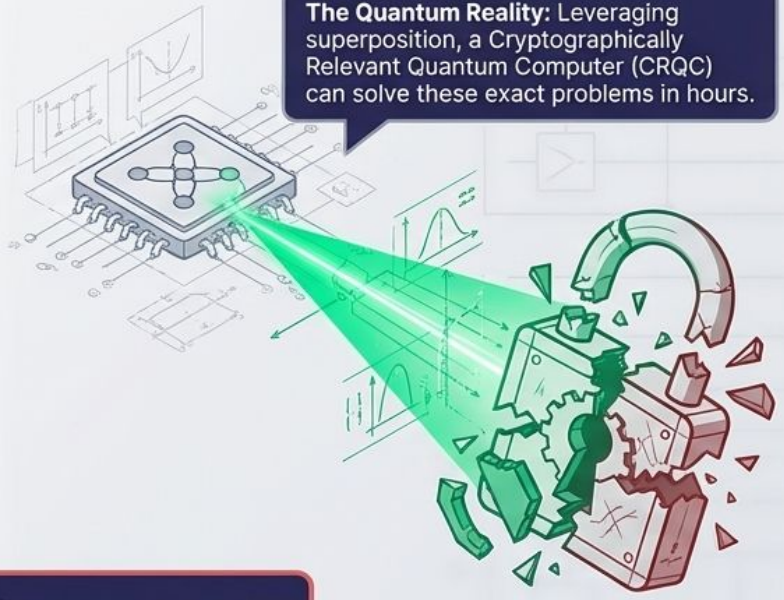
Classical Computing

The Classical Limit: Traditional encryption relies on mathematical problems (like integer factorization) that take classical supercomputers millennia to solve.



Quantum Computing

The Quantum Reality: Leveraging superposition, a Cryptographically Relevant Quantum Computer (CRQC) can solve these exact problems in hours.



The Threat: Shor's Algorithm completely breaks modern public-key cryptography.

The Cryptographic Fault Line

Classical Asymmetric (RSA, ECC, Diffie-Hellman)	Classical Symmetric (AES-128)	Post-Quantum Cryptography (Lattice-based ML-KEM / Hash-based LMS)
Underlying Math: Integer factorization / Discrete logarithms.	Underlying Math: Key length.	Underlying Math: Structured lattices / Cryptographic hash functions.
CRITICAL VULNERABILITY	MODERATE VULNERABILITY	SECURE
Broken entirely by Shor's Algorithm.	Grover's Algorithm halves key strength. Requires immediate upgrade to AES-256.	Immune to known quantum algorithms.

The Vulnerability Window is Already Open

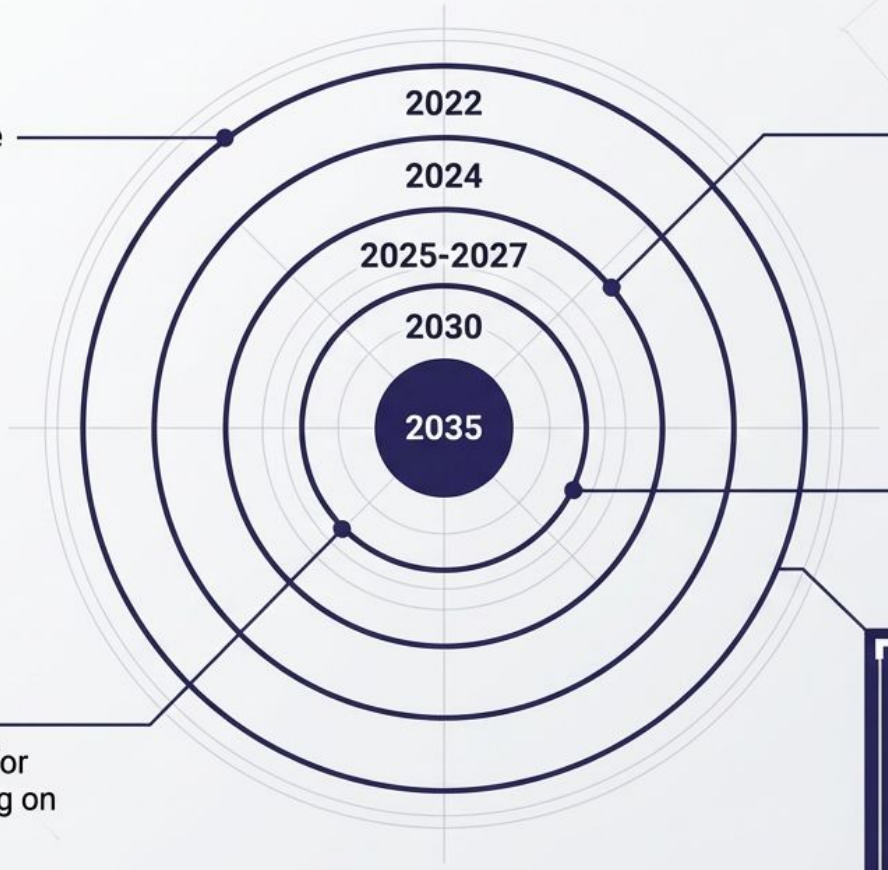
PQC Deployment Date = Q-Day minus Cover Time

The Threat to Longevity: Any data with a shelf-life extending beyond Q-Day (state secrets, intellectual property, health records) is already compromised if traveling over classical encryption.

The Mandate for Quantum-Resistance

2022 (NSM-10): White House directive requires federal agencies to inventory vulnerable systems.

2025-2027 (CNSA 2.0): Mandatory transition begins for software and firmware signing on National Security Systems.



2024 (NIST FIPS 203/204): Finalized Post-Quantum algorithms officially published.

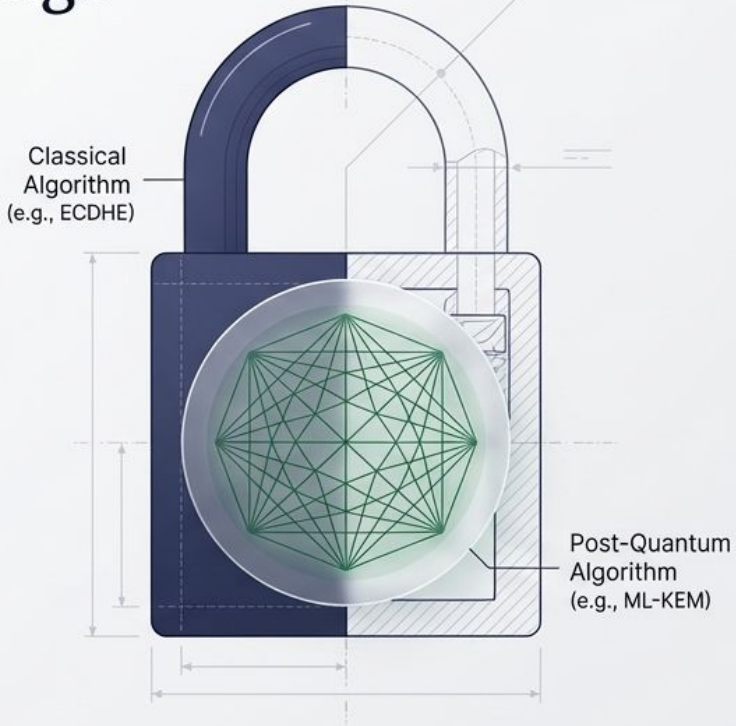
2030: Recommended full deprecation of RSA/ECC algorithms.

Financial Impact: The U.S. government estimates a $7.1 Billion transition cost for non-National Security Systems alone.

Bridging the Gap with Hybrid Key Exchange

The Strategy

Combine a traditional algorithm with a post-quantum algorithm within the same TLS 1.3 handshake.
An attacker must break both to access the payload.



The Outcome

Protects against HNDL attacks today, while hedging against any undiscovered mathematical flaws in newly standardized PQC algorithms.

You Cannot Protect What You Cannot See

The transition to Post-Quantum Cryptography is a massive inventory challenge. Before migrating to quantum-safe algorithms, an enterprise must answer one impossible question: Where exactly is RSA-2048 running in our network right now?

The Foundation of Crypto-Agility: The CBOM


```
{
   "CBOM_Inventory": [
      {  "Asset": "Server_Certificate_A",
         "Algorithm": "RSA-2048",
         "Key_Length": "256",
         "Status": "Deprecated",
         "Cipher_Suite": "TLS 1.2"
      },
      {  "Asset": "Encryption_Key_B",
         "Algorithm": "AES-GCM",
         "Key_Length": "256",
         "Cipher_Suite": "TLS 1.3"
      },
      {  "Asset": "Signing_Key_C",
         "Algorithm": "ECDSA_P256",
         "Key_Length": "256",
         "Cipher_Suite": "N/A"
      },
      {  "Asset": "Legacy_System_D",
         "Algorithm": "SHA-1",
         "Key_Length": "160",
         "Status": "Deprecated",
         "Cipher_Suite": "N/A" }
   ]
}
```


Definition

A Cryptographic Bill of Materials (CBOM) catalogs every cryptographic asset —algorithms, key lengths, certificates, and cipher suites—actively in use across the environment.

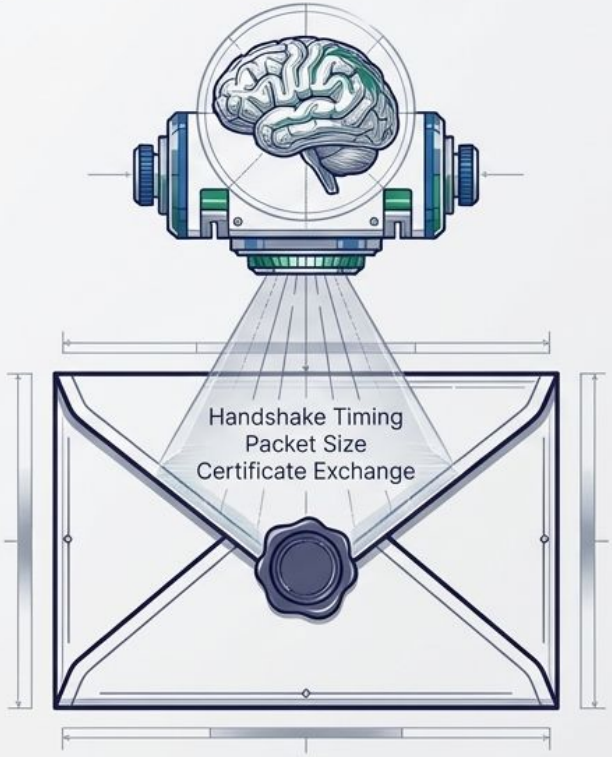
Purpose

A dynamic CBOM is the mandatory first step outlined by federal mandates (like NSM-10) to baseline current risk, identify deprecated algorithms, and prioritize the PQC migration.

Total Insight, Without the Overhead of Decryption

Mechanism

NDR platforms utilize Deep Packet Inspection (DPI) and Encrypted Traffic Analysis to scan the exterior of the connection (unencrypted metadata).



Result

Maps all RFC ciphers, elliptic curves, and certificates in real-time.

Achieves 100% cryptographic visibility.

Achieves 100% cryptographic visibility without breaking data privacy or impacting performance.

Building the Automated CBOM Pipeline

Gather

Passive collection of network and cloud traffic at scale.

Analyze

Extract SSL/TLS metadata, categorize services, and map cryptographic capabilities (DPI for PQC-enabled protocols).

Attribute

Correlate crypto data to specific applications, unmanaged devices, and users using entity profiling.

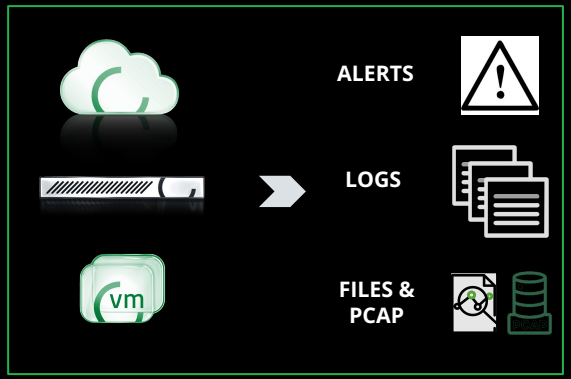
Drive

Export structured data to SIEM/Data Lakes to power continuous PQC Readiness Dashboards.

Corelight Open NDR | Powerful network data generation for ACDI

Gather
network and cloud traffic

Analyze
extract metadata categorize services, applications



Drive
workflows for cryptographic discovery + inventory

Your SIEM / DATA LAKE / XDR

- SSL/TLS, protocol metadata
- Inventory/ Compliance Dashboards
- Data Exploration

Corelight Investigator

- Alert Workflow
- Pre-canned dashboards
- Log search / storage

Deploy physical, virtual, software, cloud, at scale

Can operate fully air gapped

- DPI for PQC-enabled protocols
- Full metadata extraction for SSL/TLS
- Capture crypto capabilities exchange as well as chosen ciphers
- Maps all RFC ciphers/curves
- Powerful protocol, service, and application discovery
- Works across all ports (DPD)

- Flexible export for integration with existing SIEM/analytics workflows
- Compact data for long-term storage and inventory
- Easy to create dashboards and feed other inventory systems
- Unique connection identification to tie application/service to crypto data

Zeek | Powerful network data generation for ACDI

Gather
network traffic

Analyze
extract metadata
categorize services

Drive
workflows for cryptographic discovery + inventory

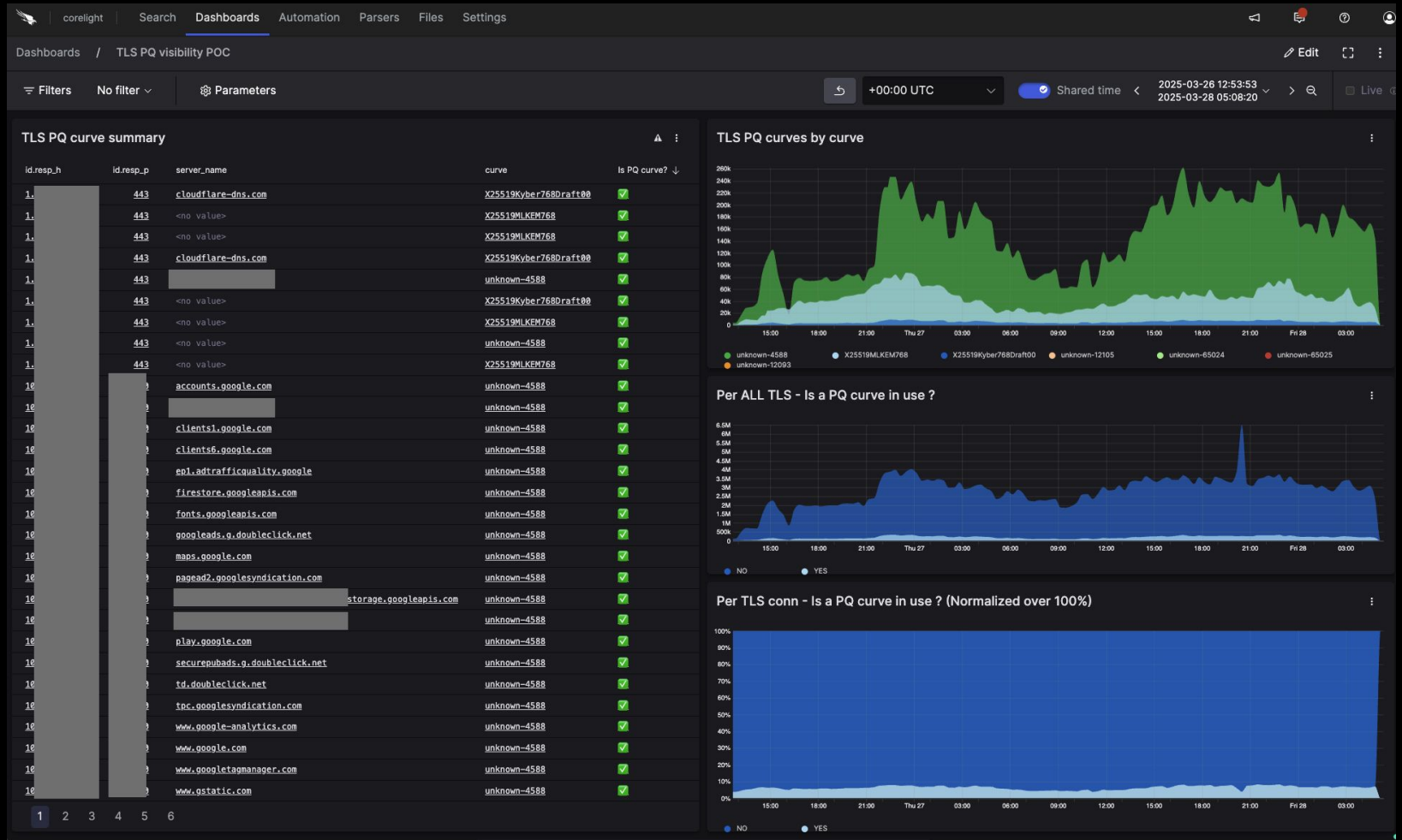
Deploy sensors

Can operate fully air gapped

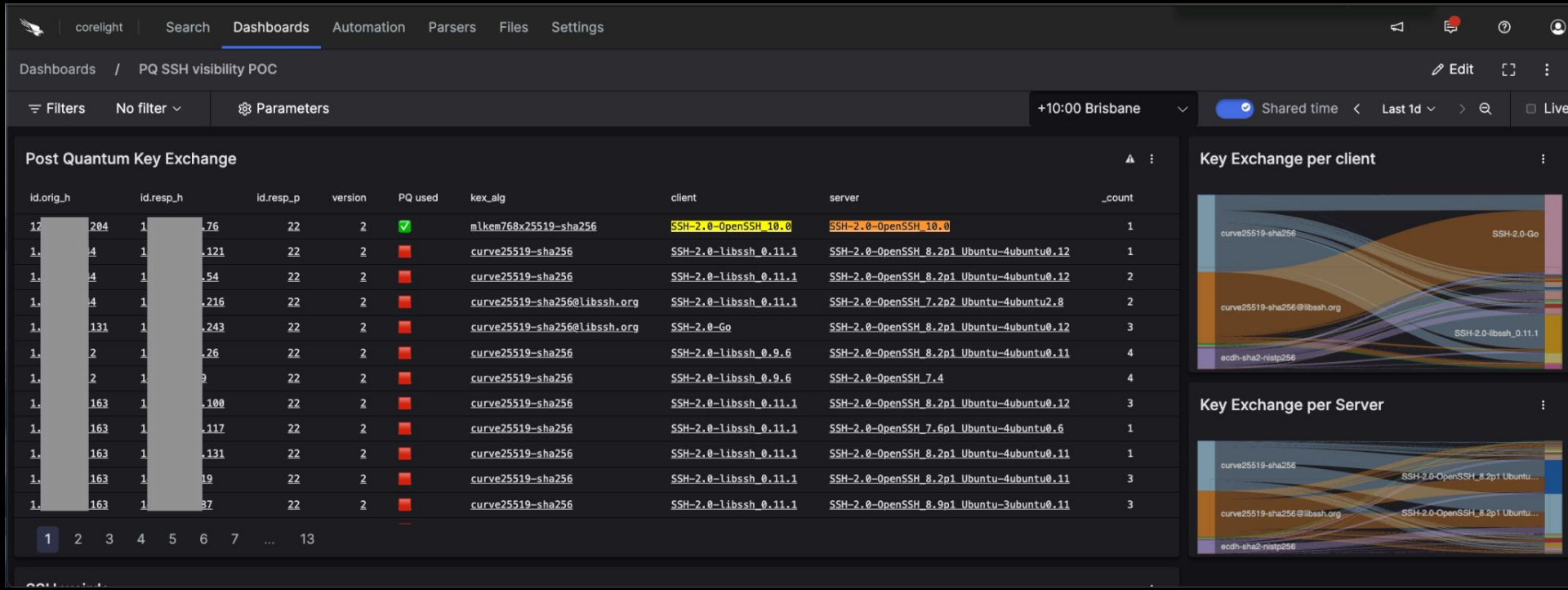
- DPI for PQC-enabled protocols
- Full metadata extraction for SSL/TLS
- Capture crypto capabilities exchange as well as chosen ciphers
- Maps all RFC ciphers/curves
- Powerful protocol, service, software discovery
- Works across all ports (DPD)

- JSON export for integration with existing SIEM/analytics workflows
- Compact data for long-term storage and inventory
- Easy to create dashboards and feed other inventory systems
- Unique connection identification to tie service to crypto data

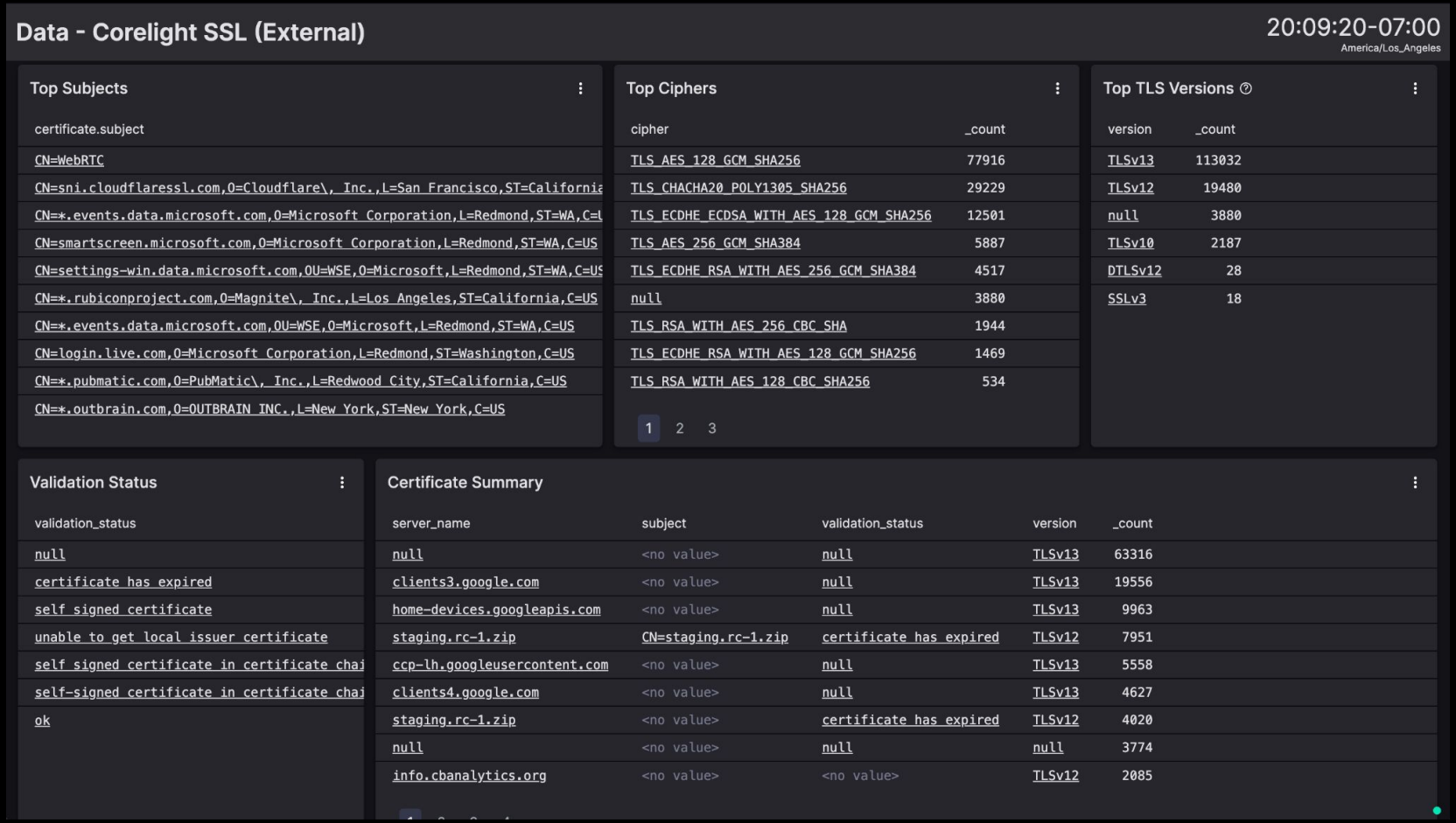
Dashboard example - PQC Inventory (live research data)



Dashboard example - SSH PQC Inventory



Dashboard example - SSL/TLS overview



Data - Corelight SSL (External)

20:09:20-07:00
America/Los_Angeles

Top Subjects

certificate.subject
CN=WebRTC
CN=sni.cloudflaressl.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California
CN=*.events.data.microsoft.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=U
CN=smartscreen.microsoft.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=US
CN=settings-win.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US
CN=*.rubiconproject.com,O=Magnite\, Inc.,L=Los Angeles,ST=California,C=US
CN=*.events.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US
CN=login.live.com,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US
CN=*.pubmatic.com,O=PubMatic\, Inc.,L=Redwood City,ST=California,C=US
CN=*.outbrain.com,O=OUTBRAIN INC.,L=New York,ST=New York,C=US

Top Ciphers

cipher	_count
TLS_AES_128_GCM_SHA256	77916
TLS_CHACHA20_POLY1305_SHA256	29229
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	12501
TLS_AES_256_GCM_SHA384	5887
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	4517
null	3880
TLS_RSA_WITH_AES_256_CBC_SHA	1944
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	1469
TLS_RSA_WITH_AES_128_CBC_SHA256	534

1 2 3

Top TLS Versions

version	_count
TLSv13	113032
TLSv12	19480
null	3880
TLSv10	2187
DTLSv12	28
SSLv3	18

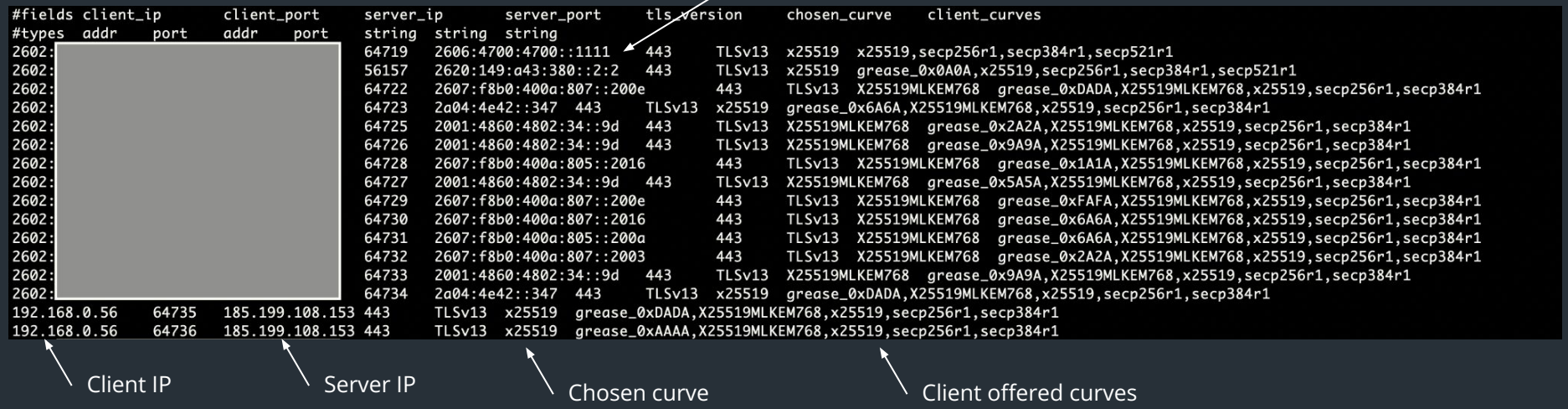
Validation Status

validation_status
null
certificate has expired
self signed certificate
unable to get local issuer certificate
self signed certificate in certificate chai
self-signed certificate in certificate chai
ok

Certificate Summary

server_name	subject	validation_status	version	_count
null	<no value>	null	TLSv13	63316
clients3.google.com	<no value>	null	TLSv13	19556
home-devices.googleapis.com	<no value>	null	TLSv13	9963
staging.rc-1.zip	CN=staging.rc-1.zip	certificate has expired	TLSv12	7951
ccp-lh.googleusercontent.com	<no value>	null	TLSv13	5558
clients4.google.com	<no value>	null	TLSv13	4627
staging.rc-1.zip	<no value>	certificate has expired	TLSv12	4020
null	<no value>	null	null	3774
info.cbanalytics.org	<no value>	<no value>	TLSv12	2085

Example PQC inventory log



- Flexible scripting allows creation of custom logs to handle crypto inventory. Example includes:
  - Summary of Client + Server IPs, TLS version, chosen crypto and client offers
    - policy/protocols/ssl/ssl-log-ext.zeek
  - Link to additional metadata and protocol logs for every connection
  - Optionally add JA3/JA3S/JA4 hashes

SSL/TLS log


```
{ [-]
   _path: ssl
   _system_name: sensor.cyberlab-20250110a-ngs.training.corelight.io
   _write_ts: 2025-01-10T23:55:06.679538Z
   cert_chain_fps: [ [+]
   ]
   cipher: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   client_cert_chain_fps: [ [+]
   ]
   curve: x25519
   established: true
   id.orig_h: 172.16.12.100
   id.orig_p: 9245
   id.resp_h: 192.0.0.3
   id.resp_p: 443
   issuer: CN=Kubernetes Ingress Controller Fake Certificate,O=Acme Co
   ja3: 8a9d5d0f12f7d43ee3af1c51d2998d99
   ja3s: 76c691f46143bf86e2d1bb73c6187767
   resumed: false
   ssl_history: CsxknGIi
   subject: CN=Kubernetes Ingress Controller Fake Certificate,O=Acme Co
   ts: 2025-01-10T23:55:06.666597Z
   uid: CahWeL1FNoar72GxQi
   validation_status: self signed certificate
   version: TLSv12
}
```


- Comprehensive logging for all SSL/TLS metadata including negotiated ciphers and curves, key lengths, and more
- Includes history field with full TLS transaction/negotiation details
- Out-of-band validation status included
- All RFC compliant PQC ciphers currently included, extensible to any ciphers

SSH log

```
#path   ssh
#open   2025-03-27-19-32-44
#fields id.orig_h       id.orig_p       id.resp_h       id.resp_p       client  cipher_alg      mac_alg compression_alg kex_alg host_key_alg
#types  addr    port    addr    port    string  string  string  string  string  string
192.168.0.11    40048   192.168.0.10    22      SSH-2.0-OpenSSH_9.9     chacha20-poly1305@openssh.com   umac-64-etm@openssh.com none    mlkem768x25519-sha256   ssh-ed25519
```

Client IP

Server IP

PQC algo

- Identification of the client and server version strings
- Identification of the encryption, signing (MAC), compression, key exchange and server host key algorithms
- Display of the server's key fingerprint for future correlation
- Optional logging of HASSH fingerprints for client and server (PQC ready)
- Extension of Crypto Inventory script can include additional SSH protocol specific details

x509 log

```
#fields ts      fingerprint     certificate.version     certificate.serial      certificate.subject     certificate.issuer      certificate.not_valid_before    certificate.not_valid_af
ter     certificate.key_alg     certificate.sig_alg     certificate.key_type    certificate.key_length  certificate.exponent    certificate.curve       san.dns san.uri san.email
san.ip  basic_constraints.ca    basic_constraints.path_len      host_cert       client_cert
#types  time    string  count   string  string  string  time    time    string  string  string  count   string  string  vector[string]  vector[string]  vector[string]  vector[addr]
bool    count   bool    bool
1743631602.941203       4b016e8ac76e528bfc4872bd0efcb09fb7b0cc5d4d0c0491a235bbfeb5a63e35        3       0C95469D0B3BFF3DF47B8E50D9B06E46        CN=*.dropbox.com,O=Dropbox\\, Inc,L=San
Francisco,ST=California,C=US    CN=DigiCert TLS RSA SHA256 2020 CA1,O=DigiCert Inc,C=US 1731398400.000000       1765267199.000000       rsaEncryption   sha256WithRSAEncryption rsa
2048    65537   -       *.dropbox.com,dropbox.com       -       -       -       F       -       T       F
1743631602.941203       52274c57ce4dee3b49db7a7ff708c040f771898b3be88725a86fb4430182fe14        3       06D8D904D5584346F68A2FA754227EC4        CN=DigiCert TLS RSA SHA256 2020 CA1,O=Di
giCert Inc,C=US CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US      1618383600.000000       1933916399.000000       rsaEncryption   sha256WithRSAEncryption rsa
2048    65537   -       -       -       -       -       T       0       F       F
```

- Full certificate information including fingerprint, certificate subject, issuer, validity dates, algorithms, key types + lengths, curves and subject alternative name information
- Use for application and cryptographic inventory and to correlate to established network connections

corelight

Connection (conn) log

#fields	ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration		orig_bytes		resp_bytes		conn_state		local_orig		missed_bytes	
#types	time	string	addr	port	addr	port	enum	string	interval	count	count	string	bool	count	string	count	count	count	count	set[string]		
1461774592.294620		CAeUis4fMjsN0mMpWk	192.168.4.139	51583	52.84.231.88	443	tcp	-	0.006677		0		0		RSTR	-	0	Fr	1	52	1
1461774592.957786		CImQp73RXHzX5KGBia	192.168.4.139	51712	198.207.200.82	443	tcp	-	4.172211		0		31		SF	-	0	dfAFa	3	156	3
1461774592.258279		C88GkF48IZNni148Ql	192.168.4.139	60222	192.150.186.8	53	udp	dns	0.001007		58		125		SF	-	0	Dd	1	86	1
1461774592.258322		CFUwWd2xQWttYBU4ne	192.168.4.139	52436	192.150.186.8	53	udp	dns	0.000962		51		302		SF	-	0	Dd	1	79	1
1461774592.258398		C33dTAvxwpOvZ0yO2	192.168.4.139	57796	192.150.186.8	53	udp	dns	0.001076		58		125		SF	-	0	Dd	1	86	1

Client IP

Server IP

Protocol, Service and application

connection details

- Basic connection metadata + protocol, service, and application information
- Use to generate inventory information using IP, port, service and other details
- Protocol and services are identified regardless of port based on dynamic protocol detection (DPD)
- Unique identifier (UID) ties to other logs including protocol specifics

Future needs from Zeek

- Improvements to identification (translation of numerical identifier to human readable name) of PQC cipher suites and curves
- Faster and/or dynamic input for PQC cipher suites and curves
- Exploration of additional log enhancements and additions to facilitate specific protocol requirements (i.e. what else can we find?)
- Exploration of TLS 1.3 / ECH implications on ACDI

Q & A