Conferenza GARR 2026
La forma del cambiamento

Analisi del Traffico di Rete e Cryptographic Bill of Materials

ntop / Università di Pisa

Introduzione

Obiettivo Strategico

- Mitigare il rischio quantificando e stabilendo priorità per la migrazione verso sistemi Post-Quantum Ready (PQR).

Inventario della Crittografia "At Rest"

- Deployment di agent estremamente leggeri (lightweight) sugli end-point e sui server aziendali.
- Mappatura automatica di chiavi, certificati e algoritmi legacy memorizzati nei sistemi.

Analisi della Crittografia "In Transit"

- Implementazione di una sonda di rete passiva per il monitoraggio del traffico in tempo reale.
- Intercettazione dei protocolli di scambio chiavi e cifrari obsoleti vulnerabili agli attacchi quantistici.

Crittografia "At Rest": Architettura e Sfide Tecniche

Discovery e inventario OS-independent di asset crittografici.

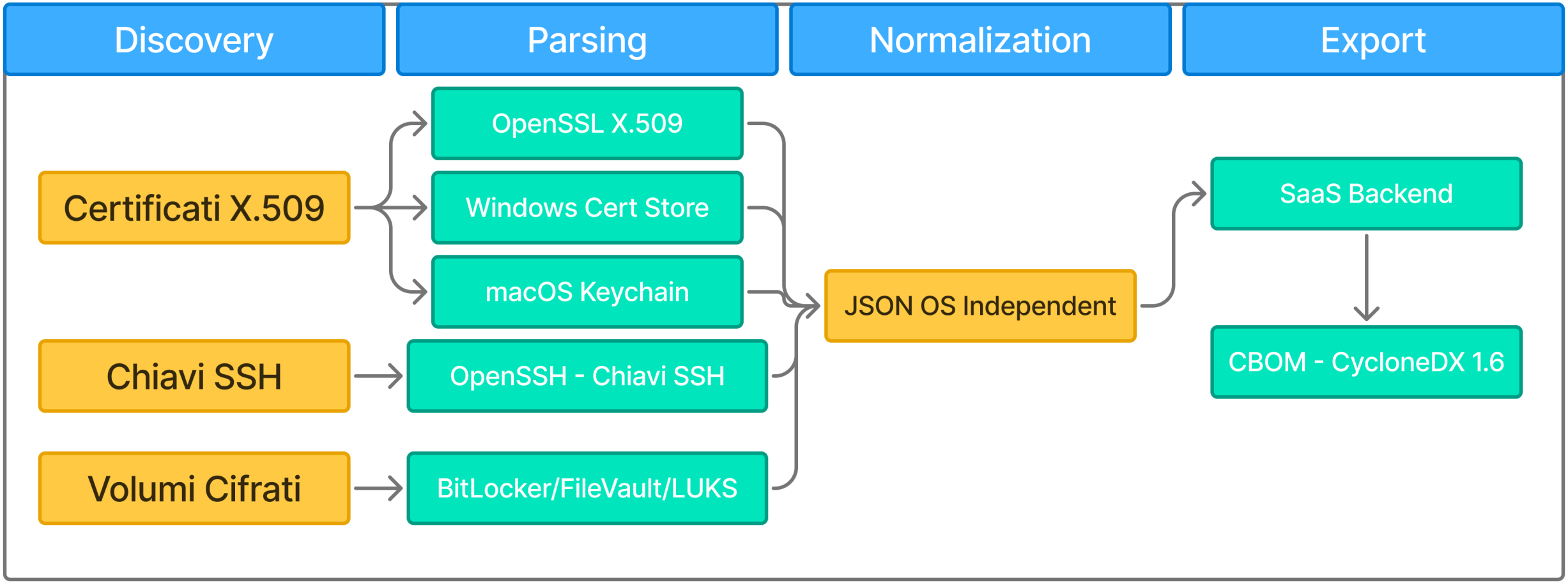
Problema

- Asset crittografici distribuiti su sistemi eterogenei.
- Visibilità frammentata.
- Filesystem e keystore nativi.
- Non esiste un modello semantico comune tra piattaforme.

Obiettivo

- Inventario OS independent, agent lightweight, output standardizzato.

Crittografia "At Rest": Pipeline



Crittografia "At Rest": Soluzione

CiperSight è un tool scritto in C++ che implementa un motore di normalizzazione per creare una rappresentazione intermedia e platform independent.

- Scanner platform specific: Linux FS, Windows cert store, macOS keychain
- Parser di informazioni crittografiche platform specific (native APIs).
- Normalizzazione in formato openSSL/SSH di cifrari, algoritmi, dimensione della chiave, volumi cifrati.
- Rappresentazione unificata JSON esportata al backend.

Crittografia "At Rest": CBOM (Cryptography Bill of Materials)

Perche' e' importante?

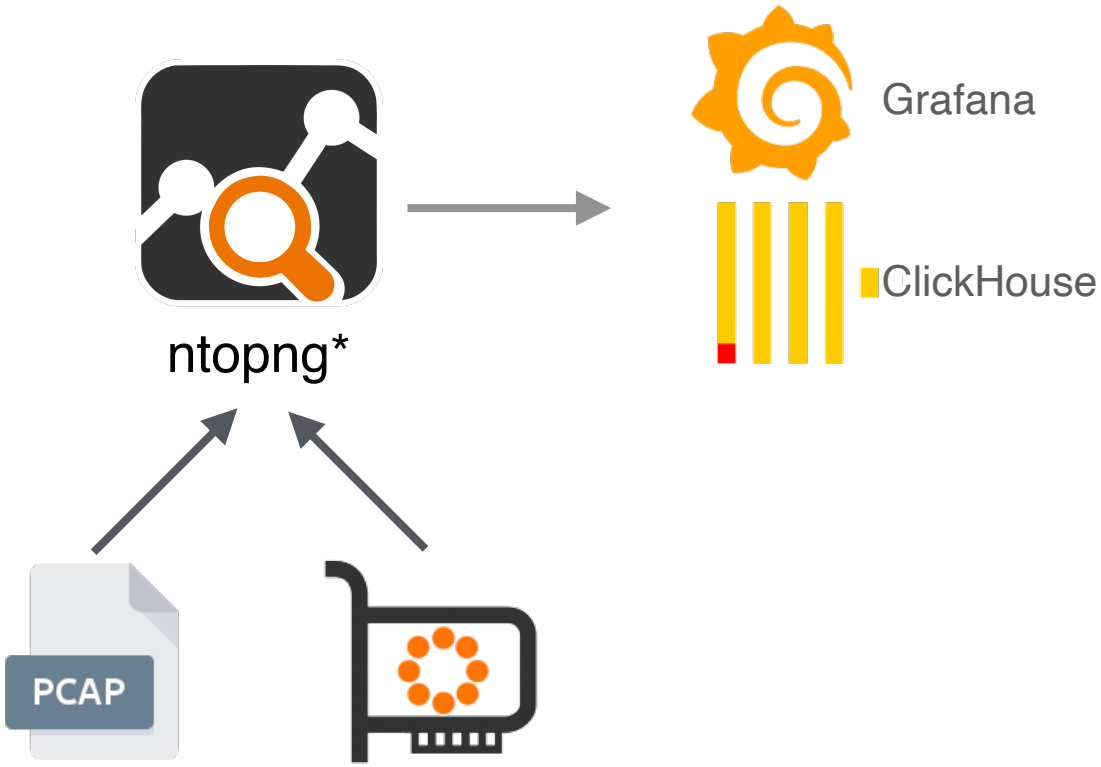
- Automazione di inventario e audit.
- Creazione policy.
- Creazione roadmap per migrazione.
- Quantificazione del rischio.
- Standard Cyclone DX 1.6.

Nell'esempio output di Qubitowl Continuum.


```
{
      "type": "cryptographic-asset",
      "name": "RSA Key: SHA256:uVnQoGNDm4pdw...",
      "bom-ref": "e12f1da1-33c6-44a4-af04-89ebf4a47ab7",
      "cryptoProperties": {
        "assetType": "related-crypto-material",
        "relatedCryptoMaterialProperties": {
          "type": "public-key",
          "format": "OpenSSH",
          "size": 3072,
          "algorithmRef": "algo-425d62dc-b253-416c-a53e-581e939642f8"
        }
      },
      "properties": [
        {
          "name": "pqc:key_type",
          "value": "ssh"
        },
        {
          "name": "pqc:discovery_source",
          "value": "cipher_sight"
        },
        {
          "name": "pqc:fingerprint",
          "value": "SHA256:uVnQoGNDm4pdwY7TJ983OcB7ixOuZ689UEgVuFmWylM"
        }
      ]
    }
```

Crittografia "In Transit": Pipeline

- Cattura del traffico di rete ed analisi tramite tecniche di Deep Packet Inspection (nDPI)*.
- Analisi di traffico criptato ed in particolare di SSH, TLS/QUIC e IPSEC.
- Estrazione di metadati (ciphers, certificati etc).
- Verifica dei dati per la conformità con il PQC.



* Open Source (https://github,com/ntop)

Crittografia "In Transit": Analisi Traffico

Issues	Description	Score	Info	Mitre Att&ck	Remediation	Actions
	Obsolete non-Post Quantum Ciphers nDPI	50	Obsolete non-PQC server	T1027 Defense Evasion		
	Remote Access ntopng	10	Remote Access	T1133 Initial Access		

CommunityId	1:LYlo0zm6hKOaxPucyupaQ0Scoy4=	
Actual / Peak / Average Throughput	170.51 bps — / 170.51 bps / 40.3 kbps	
HASSH	**Client:** D41D8CD98F00B204E9800998ECF8427E	**Server:** B12D2871A1189EFF20364CF5333619EE
SSH Signature	**Client:** SSH-2.0-OpenSSH_10.2	**Server:** SSH-2.0-OpenSSH_7.4p1 Raspbian-10+deb9u7

Referenze:

- https://github.com/ntop/
- https://www.qubitowl.com