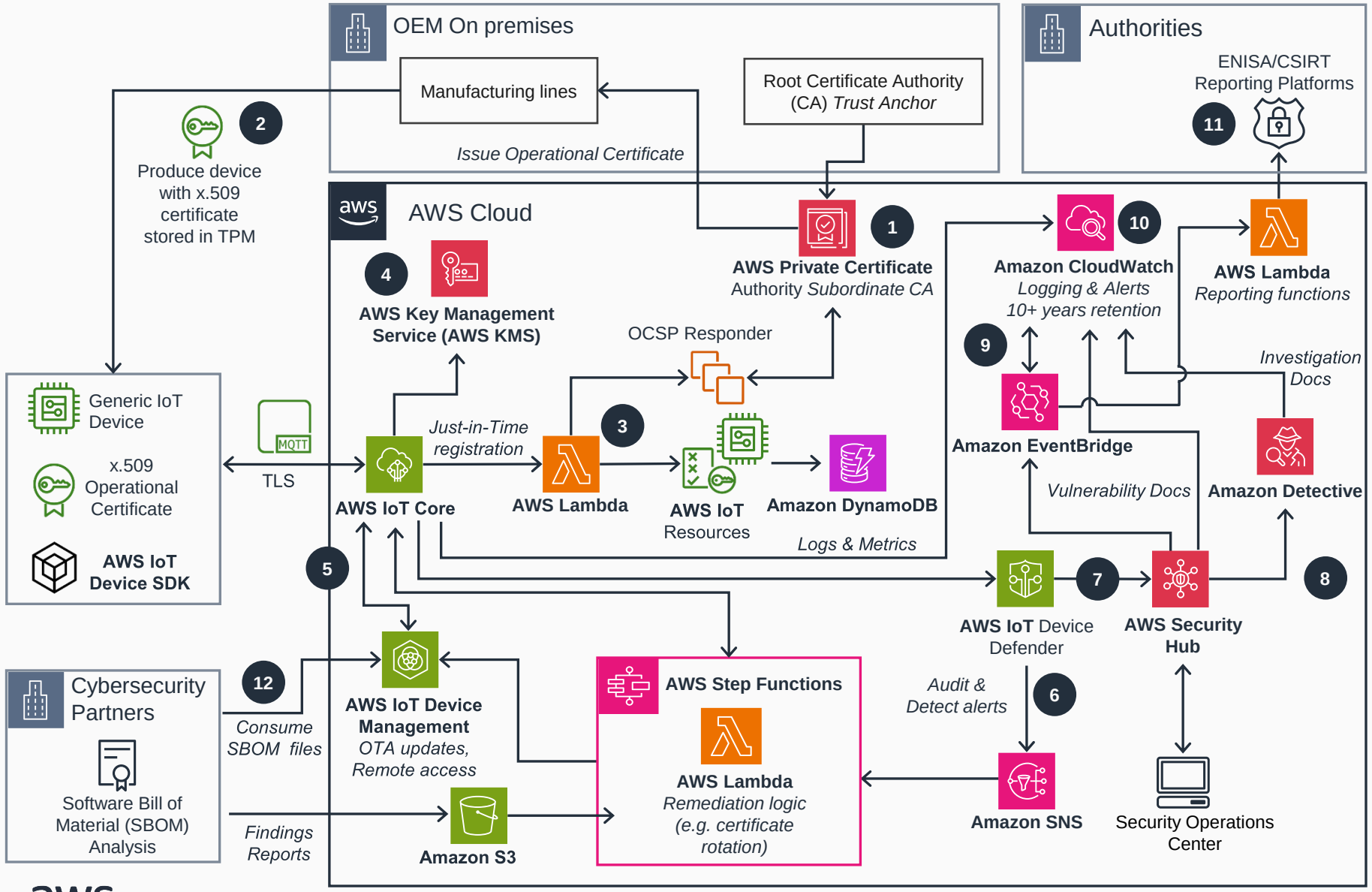
Guidance for EU Cyber Resilience Act on AWS

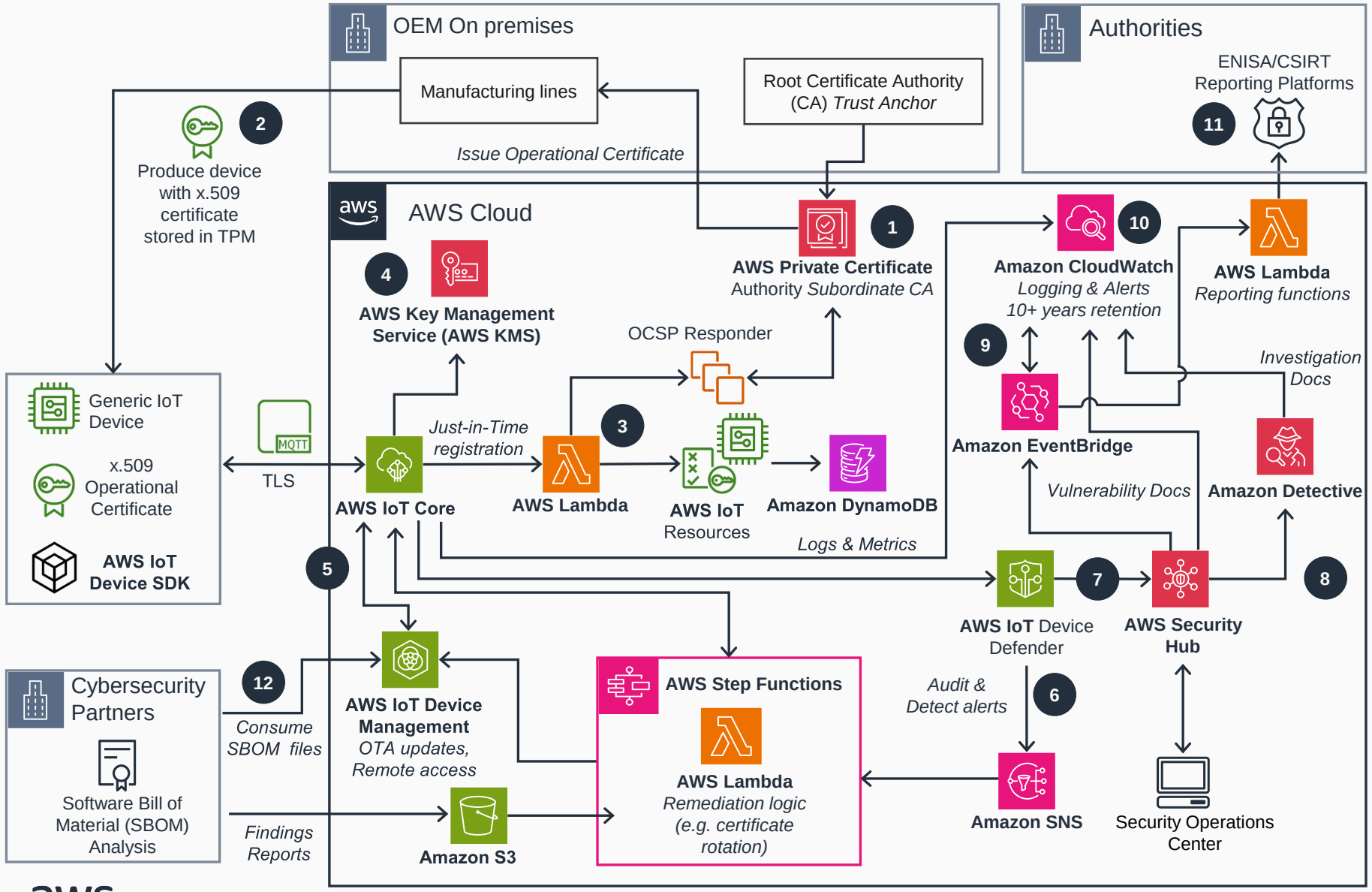


1. A subordinate CA is created in **AWS Private Certificate Authority (PCA)** with a certificate issued and signed by the offline Root CA.
2. IoT devices are provisioned with x.509 operational certificates from **AWS PCA** during manufacturing, securely storing them in their Trusted Platform Module (TPM).
3. On first connection with an unregistered certificate, an **AWS IoT Core Rule** invokes a **AWS Lambda** function that queries **Amazon DynamoDB**, validates the certificate via **AWS PCA** OCSP, creates IoT Thing and Policy resources, activates the certificate, enabling the device to establish MQTT connectivity.
4. Server-side encryption at rest, managed by **AWS Key Management Service (KMS)**, is enabled across all services.
5. **AWS IoT Device Management** can manage the device lifecycle through the required 5-year minimum support period. This includes maintaining device security through secure over-the-air (OTA) updates with signed firmware with **AWS IoT Jobs** and **Fleet Indexing,** and tracking software states to maintain version control with **AWS IoT Software Package Catalog**.
6. **AWS IoT Device Defender** publishes findings from both audit checks and anomaly detection (authorization failures, traffic patterns) to **Amazon SNS**, triggering **AWS Step Functions** workflows. For certificate findings, the workflow orchestrates rotation via **AWS IoT Jobs**, where devices generate CSRs, receive **AWS PCA**-signed certificates, and confirm installation before old certificate revocation.

Reviewed for technical accuracy March 22, 2026

AWS Reference Architecture

Guidance for EU Cyber Resilience Act on AWS



7 The findings from **AWS IoT Device Defender** are also sent to **AWS Security Hub** which can be consumed from a **Security Operations Center (SOC).**

8 **AWS Security Hub** feeds vulnerability data to **Amazon Detective**, enabling automated threat investigation and forensic analysis of security incidents.

9 **Amazon CloudWatch** alerts propagate to **Amazon EventBridge**, enabling the triggering of **AWS Step Functions** workflows for remediation.

10 **Amazon Cloud Watch** consolidates all security documentation events, vulnerabilities, incidents, and investigations—into a unified compliance repository with 10+ year retention for EU CRA auditing.

11 **Amazon EventBridge** with **AWS Lambda** functions reports severe cybersecurity incidents and actively exploited vulnerabilities to ENISA/CSIRT through the EU's designated single reporting platform.

Cybersecurity partners analyze SBOM files stored in **AWS IoT Device Management**, identify vulnerabilities, and securely deliver detailed reports to authorized **Amazon S3** buckets.

Reviewed for technical accuracy March 22, 2026

AWS Reference Architecture