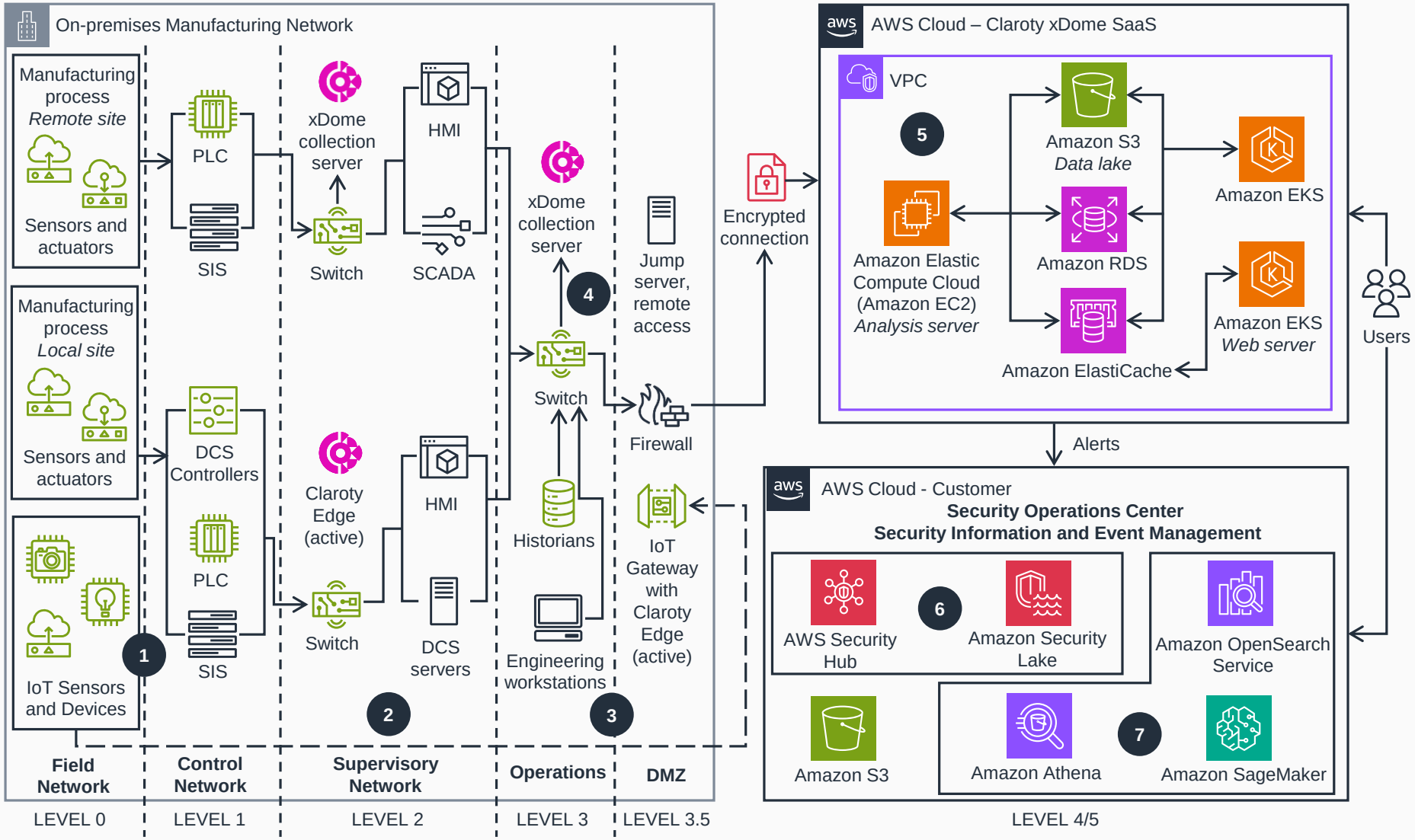
Guidance for Securing Operational Technology (OT) Assets using Claroty xDome on AWS

This architecture diagram shows how to protect OT infrastructure against security vulnerabilities. This slide details Steps 1-4.



1 In the Purdue Model, Level 0 refers to the physical process: sensors and actuators, field devices, solenoid valves, and motors. Level 1 consists of Programmable Logic Controllers (PLC), Distributed Control Systems (DCS) Controllers, and Safety Instrumented System (SIS) that interface with the electromechanical devices in Level 0 to provide basic control.

2 At Level 2, DCS Supervisory Control and Data Acquisition (SCADA) and human-machine interfaces (HMIs) provide control and monitoring of the manufacturing process. One or more Claroty xDome Collection servers can be installed to collect data from the control system network through a mirror port on an existing network switch that is on a network traffic access point (TAP). Claroty Edge can be deployed in order to actively discover devices.

3 Level 3 consists of historians, engineering workstations, and other systems that manage manufacturing operations. One Claroty xDome collection server collects data from the supervisory network through a mirror port on the core network. Level 3.5 denotes the demilitarized zone (DMZ) that separates the corporate network from the industrial control systems (ICS) environment. One or more IoT gateways that collect wireless sensor data from Level 0 resides behind the firewall.

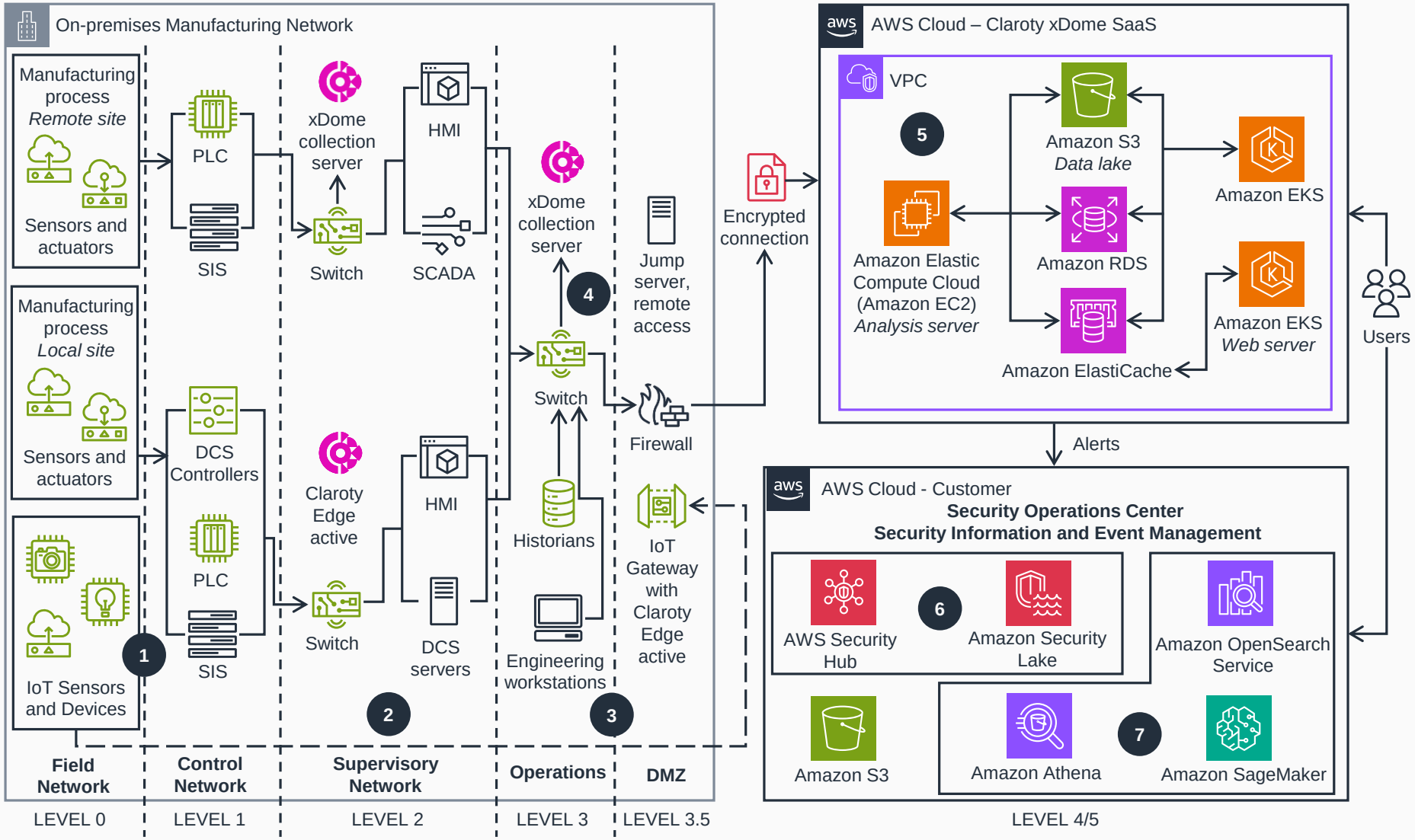
4 The xDome collection server converts network traffic into lightweight metadata, which is then forwarded to Claroty xDome software as a service (SaaS) for correlation and processing through an encrypted connection that supports TLS and IP Security (IPsec) protocols.

Reviewed for technical accuracy February 1, 2024

AWS Reference Architecture

Guidance for Securing Operational Technology (OT) Assets using Claroty xDome on AWS

This architecture diagram shows how to protect OT infrastructure against security vulnerabilities. This slide details Steps 5-7.



Reviewed for technical accuracy February 1, 2024

AWS Reference Architecture

5 The Claroty xDome analysis engine sits on the AWS Cloud, providing native, SaaS-delivered security with the latest protections and low total cost ownership (TCO) due to scalability and continuous updates. Each **Amazon Virtual Private Cloud (Amazon VPC)** can sit in a corresponding AWS Region to enable multi-site access. Claroty xDome uses **Amazon Elastic Kubernetes Service (Amazon EKS)** for performance efficiency, **Amazon Relational Database Service (Amazon RDS)** for disaster recovery, and **Amazon Simple Storage Service (Amazon S3)** to store backups. **Amazon ElastiCache** caches frequently accessed data and absorbs spikes in traffic.

6 Claroty xDome sends events and vulnerabilities to **AWS Security Hub** and natively sends events to **Amazon Security Lake** using the Open Cybersecurity Schema Framework (OCSF). These services can be a part of a comprehensive Security Operations Center and Security Information and Event Management workflow that consolidates OT and IIoT security event data and actions.

7 **Security Lake** can work with AWS Partner solutions in addition to automation and analytics services, such as **Amazon Athena**, **Amazon OpenSearch Service**, and **Amazon SageMaker** to gain additional insights on security events.