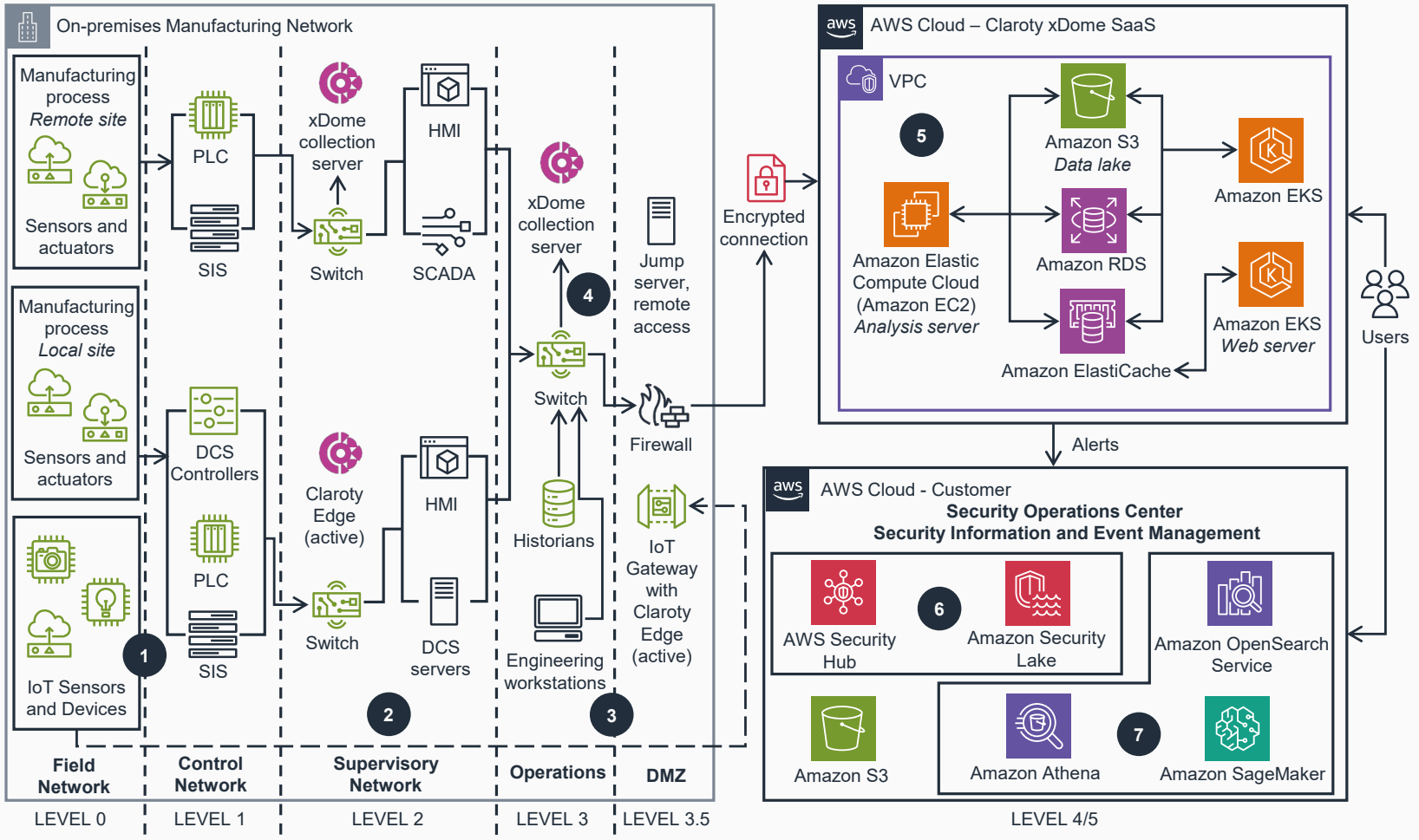
在 AWS 上使用 Claroty xDome 保护 OT 资产



1. 在 Purdue 模型中，第 0 级指的是物理过程：传感器和执行器、现场设备、电磁阀和电机。第 1 级由可编程逻辑控制器（PLC）、分布式控制系统（DCS）控制器和安全仪表系统（SIS）组成，它们与第 0 级中的机电设备进行接口交互，以提供基本控制。

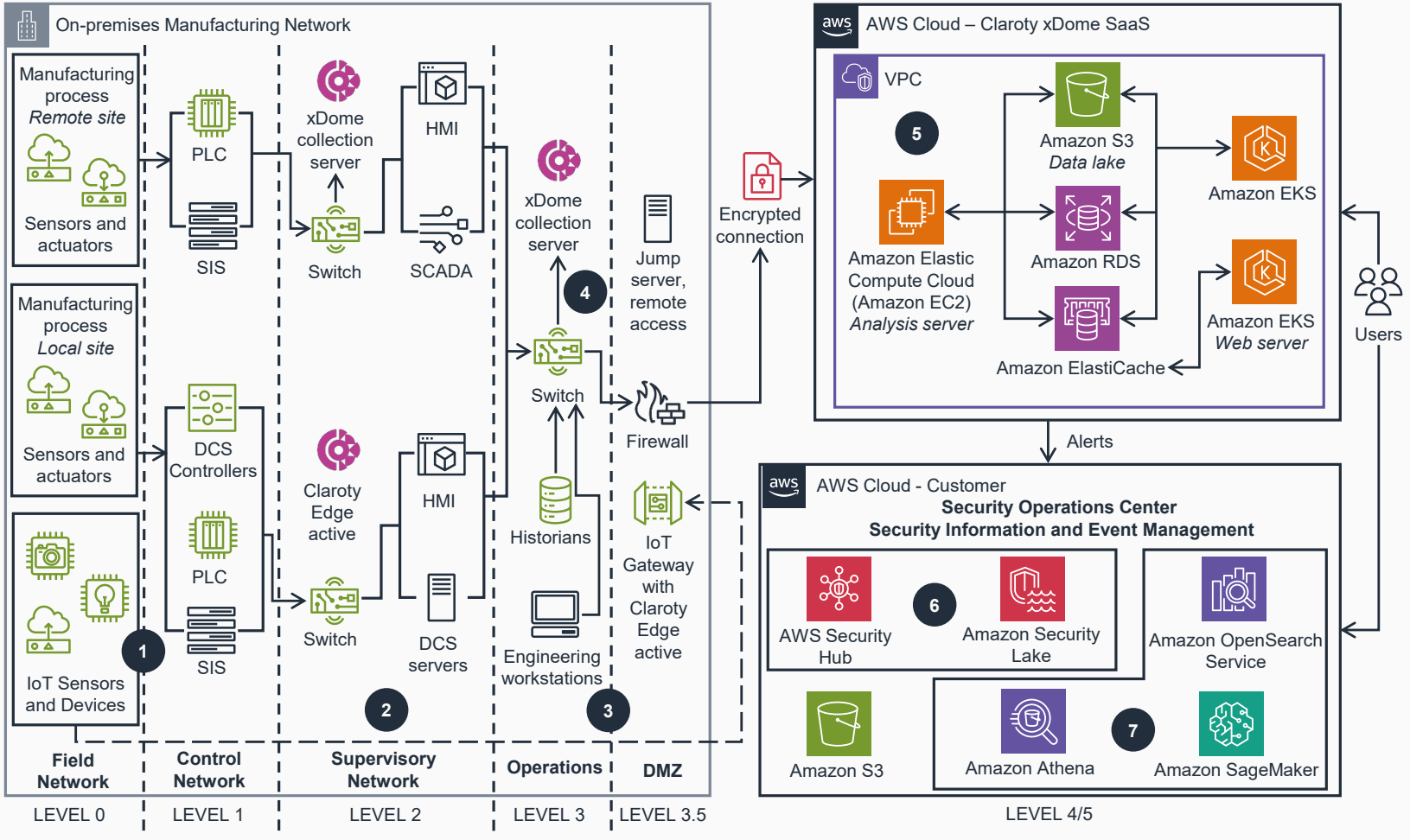
2. 在第 2 级，DCS 监控与数据采集（SCADA）系统、人机界面（HMI）对制造过程进行控制和监控。您可以安装一个或多个 Claroty xDome 收集服务器，通过网络流量接入点（TAP）上现有网络交换机的镜像端口从控制系统网络收集数据。要主动发现设备，可以部署 Claroty Edge。

3. 第 3 级包括历史记录器、工程工作站和其他管理制造运营的系统。一台 Claroty xDome 收集服务器将通过核心网络上的镜像端口从监控网络收集数据。
第 3.5 级表示将公司网络与工业控制系统（ICS）环境分隔开来的DMZ。一个或多个从第 0 级收集无线传感器数据的 IoT 网关位于防火墙后面。

4. xDome 收集服务器将网络流量转换为轻量级元数据，然后通过支持 TLS 和 IP 安全（IPsec）协议的加密连接将其转发到 Claroty xDome 软件即服务（SaaS），以进行关联和处理。

Reviewed for technical accuracy February 1, 2024

在 AWS 上使用 Claroty xDome 保护 OT 资产



5 Claroty xDome 分析引擎位于 AWS 云上，提供 SaaS 交付的原生安全性。 每个 Amazon Virtual Private Cloud（Amazon VPC）都可以位于相应的 AWS 区域中，以实现多站点访问。
Claroty xDome 使用 Amazon Elastic Kubernetes Service（Amazon EKS）来提高性能效率，使用 Amazon Relational Database Service（Amazon RDS）实现灾难恢复，使用 Amazon Simple Storage Service（Amazon S3）来存储备份。 Amazon ElastiCache 可缓存频繁访问的数据，并缓解流量高峰带来的压力。

6 Claroty xDome 向 AWS Security Hub 发送事件和漏洞，并使用开放网络安全架构框架（OCSF）直接从本地向 Amazon Security Lake 发送事件。 这些服务可以纳入综合安全运营中心和安全信息与事件管理工作流程（该工作流程整合了 OT 和 IIoT 安全事件数据和操作）。

7 除了自动化和分析服务（如 Amazon Athena、Amazon OpenSearch Service 和 Amazon SageMaker）外，Security Lake 还可采用 AWS 合作伙伴解决方案，获得有关安全事件的更多见解。

Reviewed for technical accuracy February 1, 2024