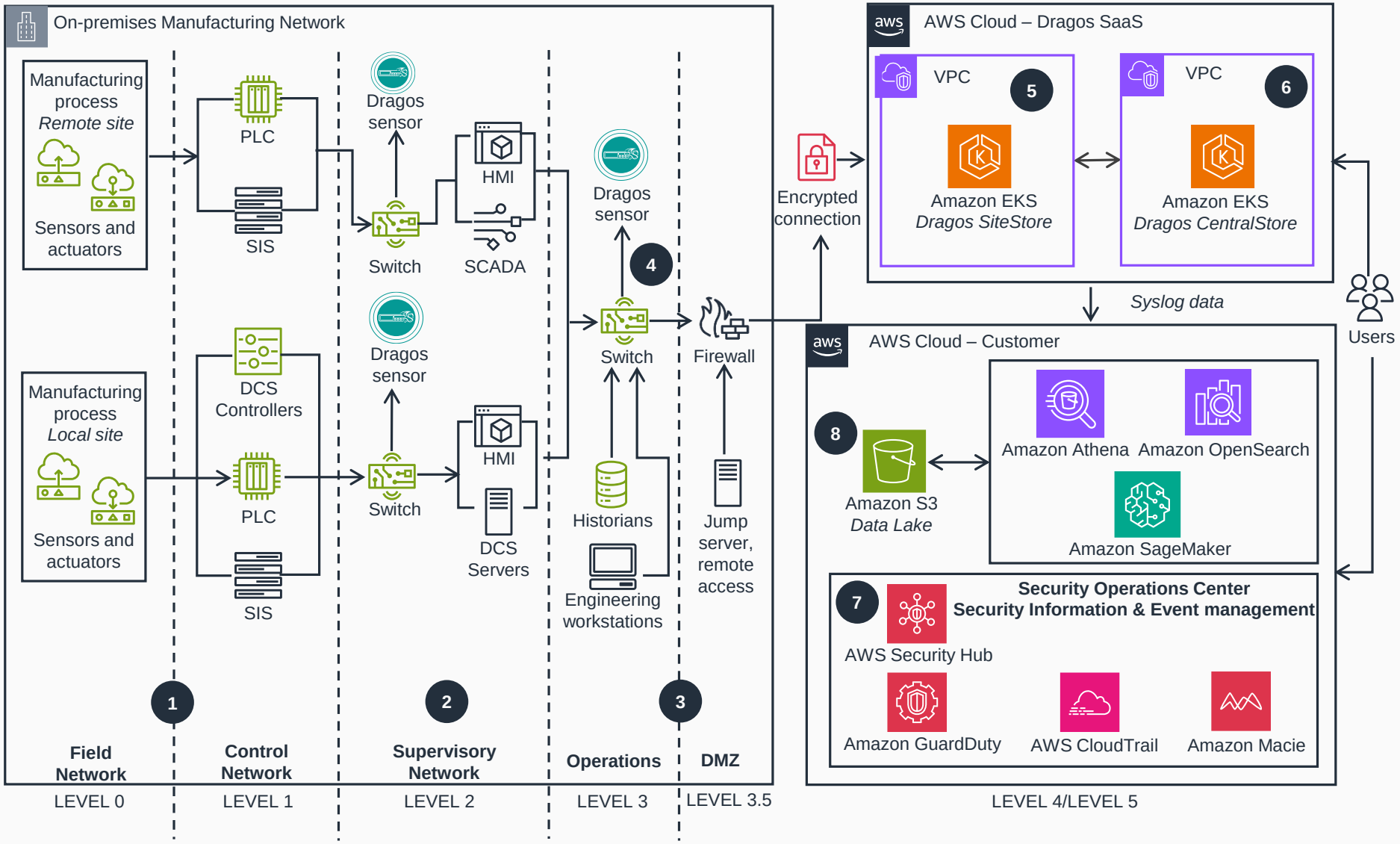
Guidance for Securing Operational Technology (OT) Assets with Dragos on AWS

This architecture diagram shows how to use the cybersecurity platform Dragos to secure operational technology (OT) assets at various manufacturing sites. This slide outlines steps 1-4; for details on steps 5-8, go to the next slide.



1 In the Purdue model for industrial control system (ICS) security, Level 0 refers to the physical process: sensors and actuators, field devices, solenoid valves, and motors. For basic control, Level 1 consists of programmable logic controllers (PLC), distributed control systems (DCS), and safety instrumented systems (SIS) that interface with the electromechanical devices in Level 0.

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 Dragos sensors collect data from the control system network through a mirror port on an existing network switch on a network traffic access point (TAP).

3 Level 3 consists of historians, engineering workstations, and other systems that manage manufacturing operations. One or more Dragos sensors collect data from the supervisory network through a mirror port on an existing network switch or network TAP. Level 3.5 denotes the demilitarized zone (DMZ) that separates the corporate network from the industrial control systems (ICS) environment.

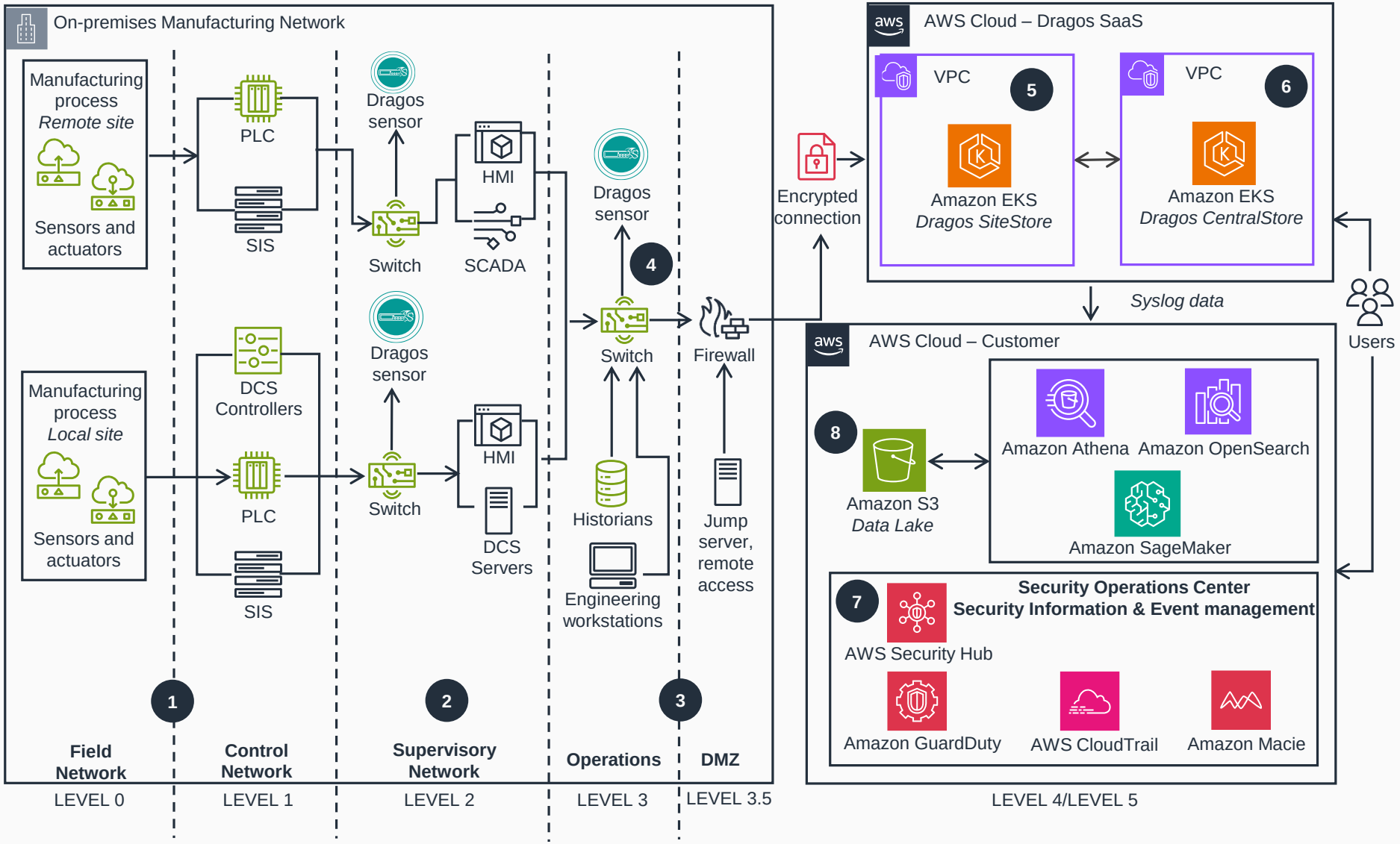
4 The Dragos sensor converts network traffic into lightweight metadata, which is then forwarded to Dragos SiteStore for correlation and processing through an encrypted connection that supports TLS and Internet Protocol Security (IPSec) protocols.

Reviewed for technical accuracy January 30, 2024

AWS Reference Architecture

Guidance for Securing Operational Technology (OT) Assets with Dragos on AWS

This slide outlines steps 5-8.



5 Dragos SiteStore, hosted on **Amazon Elastic Kubernetes Service** (Amazon EKS), serves as the management and reporting console for the Dragos sensor data. To enable multi-site operational technology (OT) access, this can reside in a separate virtual private cloud (VPC). Dragos SiteStore can also be deployed on-premises depending on your needs.

6 Dragos CentralStore, residing on **Amazon EKS**, provides enterprise-scale, multi-site OT visibility, detection, and response. Dragos CentralStore can also be deployed on-premises depending on your needs.

7 The OT security event data from SiteStore and CentralStore is sent to a security incident and event management system (SIEM) or a security operations center (SOC) that features **AWS Security Hub**, **Amazon GuardDuty**, **Amazon Macie**, and **AWS CloudTrail**, among other services. Considerations for the security operations center in the cloud provides more context for a SOC function when you operate in the cloud.

8 Syslog data associated with OT security events can be stored in an **Amazon Simple Storage Service** (Amazon S3) data lake. The data can be analyzed using **Amazon Athena**, **Amazon OpenSearch Service**, and **Amazon SageMaker**. This data can also be combined with IT security data to provide a centralized view of all OT and IT security events to enable alerting and automatic remediation.

Reviewed for technical accuracy January 30, 2024

AWS Reference Architecture