IDC

Observability Case Study: Interview with the Chief Architect at a Water Supply Organization in Europe

ASSOCIATED WITH THE WHITE PAPER:

Network Intelligence and Insights: Driving Performance, Protection, and Productivity in Observability

AUTHORS:

Christopher Kissel

Mark Leary

Business Scenario

In Europe, a private agency maintains the safety and production of several thousand water treatment facilities. Each plant will have an operator and an engineer, but little other personnel. Self-evidently, the on-premises employees are concerned with testing the water at various stages of treatment for toxicity; making sure that the valves in the pumps are operating properly; and measuring tank and water transfer speeds.

The primary mechanisms that the water treatment agency deploys are devices using SCADA programmable logic controllers (PLC) with proprietary OS. Data from the devices, as well as inputs from the onsite operators and engineers, are collected by public cloud IaaS service providers through a dedicated, private VLAN and a private mobile network. For reasons of compliance and to satisfy regulators, adherence to several NIST 800-53 standards is observed and reported rigorously. **Read on...**

How Network and Security Operations (NOC/SOC) Are Managed

Interestingly, the company prefers to keep its NOC separated from its SOC; the water treatment company has a separate NOC and SOC that are several hundred kilometers a part. The NOC is in-house, but the SOC is outsourced.

For regulatory reasons and a certain amount of segmentation, resiliency, and redundancy, the NOC/SOC separation is deemed necessary. As expected, this approach is problematic. The Chief Architect has oversight over both the NOC and SOC. Alerts are generated by the NOC. Alerts are handled this way because the NOC has a better feeling for what is *"normal"* in the environment. Obviously, because contaminated water is a vital, public safety concern the NOC tends to over-generate alerts. Roughly 95% of alerts are noise. Additionally, the SOC has some OT experience but not a firm handle on specific problems related to water treatment, water storage, and water transfer. On the bright side, a digital twin is created for security enrichment and use case modeling.

Where Observability Fits In

The biggest problem the company has is understanding basic security hygiene. The NOC monitors for failed authentication attempts and has antimalware systems running. On a human level, engineers and operators are encouraged to sign in and stay with the dedicated networks (a small ask but as engineers transition to different facilities, their credentials and privileges can be lost).

Observability initiates the investigation process if there is an alert generated from an IDS/IPS system. Integration with Industry 4.0 SMART protocols and through SIEM and SOAR tools guide the SOC analyst. Pre-existing playbooks are deployed.

Worth noting, in facilities such as these, there may be any number of customer premises equipment (CPE) and even personal devices that double in use for business applications. These types of devices are connected to a Window/Linux/Apple OS and can become unmanaged. An observability platform would be able to detect if these devices were offline and could initiate a callback to reassociate devices with the network.

Opportunities to Enhance Operations with a Greater Commitment to Observability

As telemetry is collected, the session goes through SaaS applications into the private network via multi-protocol label switching (MPLS). The labeling system utilizes routing tables for the quickest delivery of packets for near real-time observation.

MPLS is expensive to deploy and what is gained in agility is potentially lost in security—MPLS is not encrypted (at least not the labeled part of the packet) and open-text is susceptible to visibility from the man-in-the-middle. However, observability means that all networking protocol sessions are monitored. An observability protocol can tell if a packet has been altered or if a given device is exhibiting C2C beaconing activity due to characteristics of a given session. The central strength of Gigamon is its ability to quickly associate the traffic observed with the type of device generating the telemetry and what the baseline performance expectations are in each application. If nothing else, the noisy alerts generated by the NOC could be resolved more quickly in the SOC.

Finally, the Chief Architect had doubts that current AI/ML models could add much to insights for his environment; in this particular case, the environment is literally and figuratively fluid. As water and chemicals are transferred through valves, it takes everything to make sure the operation is successful on the front end. Drinking water can only be safely transferred 50 miles and must be retested to see if there are additional treatments required. However, the same architect felt that a decade in the future the data collected in the valves and at capacitors could add a layer of safety that helps to supplement what is collected and tested manually.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200