Pipeline & Gas Journal
connecting you to the pipeline industry worldwide

PIPEDLINE INTEGRITY

Northeast Energy Outlook
Leak Detection
Drones
Corrosion

Gulf Energy
You Do Leak Detection, but Do You have Breach Detection?

By Paul Rostick, Chief Information Security Officer, aeSolutions

Pipeline leaks are bad for everyone. They can have catastrophic effects on the environment, on communities, and a company’s bottom line. Given a bad enough leak, you could lose your license to operate, lose a fortune in revenue, and even face jail time. No one wants leaks.

Pipeline companies invest considerable effort preventing, detecting, and responding to leak incidents, but are they investing enough effort preventing, detecting, and responding to cybersecurity incidents? Since, in principle, a cyber-incident could lead to a leak incident, companies should consider breach detection as part of their overall leak prevention program.

Tale of 2 Possible Scenarios

Bob is the multi-state district supervisor for the (fictional) Best Crude Transport LP (BCTL) and is responsible for over 1,000 miles of crude oil pipeline operations. Bob reviewed the day’s schedule. It called for a shipment of Permian crude to a large refinery in southern Texas. At the appropriate time, the control center initiated the refinery shipment by remotely opening the valves for Tank A123 and directing the crude into the designated pipeline segment. This was a routine operation that had been performed dozens of times without incident.

About midway through the shipment, Tyrone, the control operator, noticed that the dedicated leak detection system began alarming on a significant drop in flow-rate and pressure. After reviewing the alarms and quickly conferring with his control room manager, they determined that the source of the pressure drop seemed to be at or near the tank farm.

Using the emergency communications system, they contacted Bob, and Helen, the tank farm supervisor. Running out into the field, Helen saw a spray of crude shooting out of the manifold and shouted back to them “It’s a leak! Shut it down!” The control center immediately shut down the operation. According to protocol, Bob initiated a formal incident response.

Fortunately, because of the SIEM alarms, and Tom and Lisa’s quick reactions, the intruder was disconnected from the network and his fake super user accounts were deactivated. However, there is still more forensic work ahead to ensure that the attacker is permanently eradicated. Regarding how the intruder managed to infiltrate the SDADA network, early indications point to an engineer’s network credentials being compromised, probably through a phishing email attack, but investigations are ongoing.

Incident Parallels

Since both of these stories involve incidents, there are many obvious parallels, including the importance of dedicated, skilled and trained employees. But the most important parallels, for our purposes, are these two: quick detection and quick response.

Although the stories are dramatized accounts, they are not exaggerations. Pipeline spills, and SCADA network breaches, are quite real and there are many documented cases of both.

If you are a pipeline professional, the first of the two stories – leak detection and response – should sound pretty familiar. Rapid leak detection and response have become established competencies of the pipeline industry.

However, the second story – the SCADA breach detection and response – may sound unfamiliar. In my experience working with pipeline companies, it is rare to find a pipeline operations “breach detection program” on par with the leak detection program. This is unfortunate and dangerous, since we know that the bad-guys

You Do Leak Detection, but Do You have Breach Detection?
are increasingly targeting operational systems (like SCADA).

Therefore, the parallels between leak detection and breach detection reveal parallel requirements: the importance of dedicated, intelligent tools that automatically detect both physical and digital anomalies and generate alarms accordingly.

The parallels also reveal the importance of tools that enable quick analysis, accurate decisions, and appropriate actions, because they will significantly reduce the impact and severity of an incident – whether a crude oil spill or a SCADA network intruder (or both).

In both of these types of incidents, the overall detection, containment and response times are the difference between a minor incident and a catastrophe.

**Making Invisible Visible**

Pipelines are constructed of thick-walled heavy steel, and, for the most part, they’re buried underground. Yet, it’s imperative to know exactly what’s going on inside them at all times. But you can’t see inside the pipes, at least not directly. To see what’s going on, you need a proxy – something that can represent what’s going on in the darkness. You need a way to see what you can’t see.

For this reason, pipeline companies deploy a vast array of sensors placed strategically throughout the system that continuously collect real-time data about the activity occurring within the pipes. Some of the sensors monitor flowrates, while others monitor pressures or temperatures. An enormous stream of this telemetry data is fed through the SCADA network and into the control room. Some of it is displayed on the operator’s console screen. Meanwhile, behind the scenes, all of this data is being recorded in a “historian” database, in case we ever need to go back and review the causes of an event.

But, there’s something else behind the scenes watching all that sensor data – an intelligent leak detection system. The advantage of such a system is that it can hold a working model of the pipeline system and schedule, and then correlate all of the telemetry feeds into a real-time picture of the operating conditions throughout the pipeline. Because it’s a computer, it can ingest and observe far more data, far faster, and far better, than a human. But more than that, it can make intelligent inferences about its observations: “This seems OK, that seems normal … wait, that does not seem normal … better raise an alarm!”

Leak detection systems have been a godsend to pipeline operations, helping to significantly reduce the risk and impact of pipeline spills. But what if you could do exactly the same thing for cybersecurity? What if you could have a breach detection program?

**Seeing Through the Bits**

SCADA networks, from the outside, can seem analogous to pipes: conduits for information flows. Every moment, billions and billions of bits (digital 1’s and 0’s) are flying through the network, coming and going at unfathomable speeds. But in reality, it’s far more complicated than that.
Those billions of bits have no inherent meaning. They’re not smart, or helpful, and they’re neither good nor bad. To be meaningful and useful, they must be assembled and reassembled into hierarchies of meaning: bits assemble into frames, frames into packets, packets into segments, segments into sessions, and sessions into streams.

And those streams can be of near infinite variety. Some streams of bits are computer programs, some are files, some are emails, and some are commands. Some streams are destined for an operator’s workstation, some for the printer down the hall, some for the historian database, and some for the industrial controllers that open and close valves.

In a computer network, everything is context. (And if you’re wondering, the station PLC won’t be able to tell who sent the Modbus command either – it will happily close the valve regardless of the identity or intentions of the sender.)

What we need, then, is a digital breach detection program analogous to the physical pipeline’s leak detection program. This means we must deploy digital network breach sensors throughout the SCADA network. However, unlike the pipeline sensors which track product flows and pressures and temperatures, these digital sensors’ will capture network activities such as: user logins, program installs, file changes, account creations, protocols, machine-to-machine communications, and thousands of other potentially anomalous activities.

Essentially, you’re on perpetual lookout for an unknown number of invisible enemies potentially hiding inside every conceivable bit stream in your network. And just as the telemetry of automated leak detection is beyond human capacity, there is no human alive who can monitor a computer network’s billions of bit-streams per second.

**Conclusion**

The parallels between a leak detection program and a breach detection program are striking (Figure 1).

For example, pipeline companies invest considerable effort to prevent the occurrence of spills, yet, somewhat paradoxically, they behave as if they will have them – hence the focus, not only on protection, but on detection and response. They regularly and extensively drill on handling spills.

Interestingly, this is the exact model recommended for cybersecurity: Do everything you can to prevent breaches but act as if you will have them. Why? The truth is, breaches happen. And because they happen, detection-time and response-time mean the difference between a minor event and a catastrophe.

And finally, you’ll notice, (Figure 1), that the bad-guy is straddling both worlds. This is the reality of the pipeline business in the 21st century. Physical operations and digital operations are now so inexorably intertwined and interdependent, a risk to one is a risk to the other. And remember, your digital operations are under attack by a global enemy. A breach could lead to a spill, or worse, and is therefore just as dangerous and just as important to: identify, protect, detect and respond. P&GJ

**Author: Paul Rostick** is the chief information security officer (CISO) and industrial cybersecurity advisor for aeSolutions, a Greenville S.C. engineering firm that specializes in assisting companies manage their industrial cybersecurity risks. Prior to joining aeSolutions, Rostick, who has over 25 years’ experience in petrochemicals and pipelines, was the CISO and director of cybersecurity for Sunoco Logistics Partners.