The digital revolution is creating transformational business opportunities for midstream oil and gas companies that harness the power of the Internet of Things (IoT) and Big Data. However, to safely capitalize on the benefits afforded by connecting operational technology (OT) assets, pipeline operators must be prepared to operate in an environment where cyberattacks are all but inevitable.

While no industry today is safe from malicious cyber activity, pipelines represent an especially attractive target due to their interconnected and distributed nature, as well as the high-impact outcome that can arise from a successful attack.

In 2018, four American pipeline companies reported communications system interruptions after a cyberattack on a data network. While gas service was not interrupted, all four companies were forced to temporarily shut down communications with their customers.

For the owners and operators of the more than 2.7 million miles of pipelines across the nation, events like these highlight the vulnerabilities inherent in midstream infrastructure. While the impact in this incident was relatively minor, other utility and energy companies have not been so lucky. In fact, a number of cyberattacks have led to millions of dollars in losses and potentially devastating near-miss safety events due to such viruses and malware as WannaCry, Havex, BlackEnergy Trojan, etc.

Artificial intelligence and security analytics hold the keys to pipeline cybersecurity.
Cybersecurity challenges
Unlike most parts of the oil and gas value chain, pipelines represent the true convergence of information technology (IT) and OT, making cybersecurity critical to safe operation. However, the vast majority of midstream infrastructure in operation today was not designed with connectivity in mind. Digital capabilities have simply been bolted on top. This integration of the physical and digital worlds has made infrastructure more vulnerable to increasingly sophisticated cyberattacks.

Today, the core challenge for protecting connected midstream assets, such as compressor stations, is visibility.

Most companies are not aware of the threats that lie within their fleet, how vulnerable they are or what actions they should take to prevent attacks.

Operators cannot protect what they cannot see. Most companies are not aware of the threats that lie within their fleet, how vulnerable they are or what actions they should take to prevent attacks. One salient example occurred in the power sector in December 2015, when a cyberattack in Ukraine caused 225,000 homes to lose power in the middle of winter. For the first few hours, the utility operator did not know a cyberattack was occurring. The operator simply thought the control system was malfunctioning.

Digitalization, and more specifically, the application of security analytics and artificial intelligence (AI), hold the key to protecting midstream infrastructure from cyber threats. However, the energy industry has historically been unable to apply these tools to identify malicious threats within distributed OT systems. This is particularly the case with pipelines, where assets are spread over millions of square miles of remote terrain.

In this environment, it has traditionally been very difficult and cost-prohibitive to apply and scale the necessary analytics and cybersecurity solutions across networks.

Sprints and marathons
Overall, the challenge of identifying and defending against cyberattacks is both a sprint and a marathon. As we see more advanced threat scenarios, we also see advancements in the technologies needed to counter them, with data analytics and AI leading the way.

Armed with these tools, companies can “own their environment” by significantly improving detection when an operation system is being attacked and implementing effective measures to ensure safety and reduce overall risk.

Siemens recognized the growing need for a holistic cybersecurity solution that could address the unique challenges presented by distributed energy infrastructure. That is why we partnered with Chronicle, an Alphabet Inc. company, to apply the power of analytics and AI to secure pipeline networks. (Alphabet owns Google). Through a unified approach that will leverage Chronicle’s Backstory platform and Siemens’ strength in industrial cybersecurity, the combined offering gives energy customers unparalleled visibility across IT and OT so they can quickly detect and confidently act on threats.

This partnership between Siemens and Chronicle will help the industry securely and cost-effectively leverage the cloud to store and categorize data, while applying analytics, AI and machine learning to identify patterns, anomalies and cyber threats within OT systems.

Chronicle’s Backstory, which is a global security telemetry platform for investigation and threat hunting, will be the backbone of Siemens’ managed service for industrial cyber monitoring, in both hybrid and cloud environments.

Backstory is designed to collect, integrate and store petabytes of data. It can conduct forensic analysis and investigations of behavior so that security analysts can identify and understand unusual activity that might indicate an attack is, or even was, underway.

Through the integration of analytics from Backstory and Siemens-managed OT services, an analyst can trace activity from the OT network back to the IT network, identifying gaps and unpatched systems that represent pathways for an adversary to enter a network, establish control and lie dormant—waiting to take over and force a shutdown. This is achieved by enabling the following:

Enhanced Visibility—Visibility is grounded in developing a continuous situational awareness of what’s happening in the physical and digital worlds. To do this, a pipeline operator must consume several different types of data—and in unfathomable volumes. Being able to store this amount of information, let alone study it for those key links that may identify a cyberattack, was once nearly impossible. But with Backstory, it is now a reality.

For instance, in the Ukraine example previously referenced, the way to identify an attack or system malfunction would have been to analyze control system data and then correlate it with network data—something that wasn’t feasible because operators lacked visibility into all systems at once. But now, looking at the two systems, which were never designed to work together, we can understand that the system errors are the result of intentional malicious activity.

Context—The second key in thwarting a cyberattack is context. Even after detecting an attack, operators are still powerless to act because they cannot understand how the attack is impacting their systems or determine the attack’s reach or intent. This is where context matters.

A better way to think of this is pattern identification—how quickly and how accurately can we examine normal asset
behavior versus abnormal behavior. By identifying patterns in Backstory, Siemens’ security analysts can build an accurate picture of the environment so operators can act.

**Quick and Decisive Action**—With the insight provided by Backstory, Siemens’ OT specialists can then work with customers to take quick and decisive action to stop the cyberattack and mitigate impacts on infrastructure. In most cases, this will not mean shutting down the system. Rather, it is about working with the customers to develop options that balance operational, safety and security constraints. The ultimate objective is to initiate a proportional and appropriate response and to use insights to continuously harden systems and protect them from future attacks.

This integrated solution and first-of-its-kind OT-managed service from Siemens and Chronicle is a significant advance in raising the OT cyber defenses for pipelines. It leverages all that digitalization has to offer to unlock the value of security data—providing cyber protection across the entire midstream operating environment.

**Industry-government collaboration**

When it comes to cybersecurity in oil and gas, and particularly the midstream sector, the most important idea that companies must embrace going forward is that securing their environment is not something they can achieve on their own.

It will require collaboration between industry and government and a strengthening of trust in the digital world. To achieve this, Siemens initiated the world’s first-ever joint charter for cybersecurity—called the “Charter of Trust.”

The Charter of Trust points out 10 areas for action in cybersecurity where government and business must become equally active. It calls for establishing responsibility for cybersecurity at the highest levels of government and businesses and for introducing a dedicated ministry in government and a Chief Information Security Officer at companies.

It also calls for mandatory, independent certification for critical IoT applications. Above all, it aims to create an industrial environment in which cybersecurity is addressed proactively so that companies, including oil and gas operators, can realize the full potential of digital transformation.

The government must take a leadership role when it comes to the rules in cyberspace; however, private companies must take a risk-based approach to implement standards and share best practices in a trusted community.

**Air gapping**

OT cyberattacks against the oil and gas industry have risen from 5% to 30% in just a few short years. They range from disrupting SCADA and industrial control systems, causing outages and safety issues, to ransomware attacks, where systems are held hostage with threats to disrupt and destroy operating systems.

With more than 2.7 million miles of oil, gas and chemical pipelines crisscrossing the U.S. alone, intrusions into control systems could do more than disrupt deliveries. As a result, the primary challenge midstream operators face is securing a complex and open ecosystem without impacting profitability.

Given that the likelihood of being attacked in today’s environment is 100%, pipeline operators cannot wait any longer to address cybersecurity. Many mistakenly believe that the only way to protect their assets is to “air gap,” an absence of a direct or indirect connection between a computer and the Internet for security reasons.

Air gapping, however, focuses on minimizing connectivity, which prevents companies from reaping all the benefits that digitalization has to offer. It also limits visibility into the operating environment, which makes it all but impossible to recognize abnormalities and react when a cyberattack does inevitably occur.

**Inside threats**

Air gapping also doesn’t protect against inside threats, which often pose the greatest risk to critical operations.

In a recent survey conducted by Siemens and the Ponemon Institute of 377 oil and gas security professionals, 65% of respondents said that a negligent or careless insider was their top cybersecurity concern, while 15% said it was a malicious or criminal insider.

It is essential that midstream companies view cybersecurity not as a seatbelt or an airbag in the digital world, but rather as a crucial component to their success in the digital economy. Data and security analytics hold great promise in identifying and thwarting sophisticated machine speed attacks, which require immediate levels of response and pattern recognition.

This innovative OT-managed service from Siemens and Chronicle leverages analytics and AI to unlock the value of security data—providing cyber protection across the entire midstream operating environment.

*Leo Simonovich is vice president of industrial cybersecurity for Siemens.*