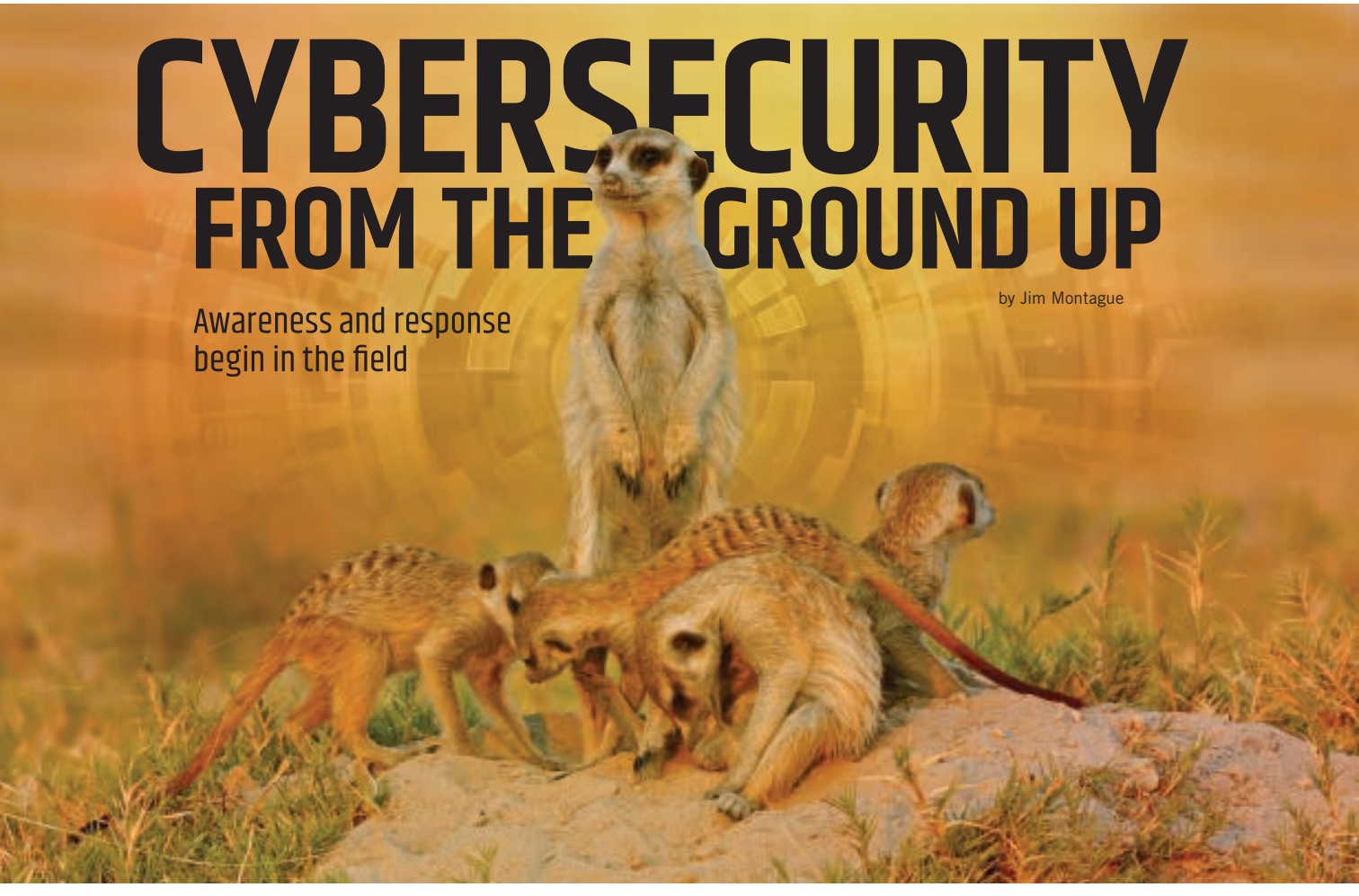
CYBERSECURITY FROM THE GROUND UP

Awareness and response begin in the field

by Jim Montague



JIM LaBonty speaks like the experienced, calm, matter-of-fact process engineering veteran he is, so it's unexpected to hear an edge of concern in his voice.

"The NotPetya malware and attack in 2017 took out Merck's production for two months and cost $870 million. In a brief to Pfizer's board, we estimated a similar incident would cost us $1.5 billion," says LaBonty, director of global technology and engineering at Pfizer (www.pfizer.com), who spoke at ARC Industry Forum 2019 (www.arcweb.com/events/arc-industry-forum-orlando-2019) in February in Orlando. "The financial impact is obvious, but there's more at stake.

"Pfizer delivers about 74 billion doses of medicine per year, and while it might seem like hospitals and pharmacies have months of medicines stored up, many only have a two-week supply, so an interruption in production could be catastrophic for much of the U.S. health care system."

This is why Pfizer needed to better secure its supply chain, starting with production and onward to providers and people. However, as usual, there were some obstacles. First, each of Pfizer's 60 plants worldwide has a unique combination of:

- Size, from small to extra large;
- Pharmaceutical types, including biopharmaceutical, chemical, vaccine, solids and sterile injectable;
- IT and automation technology (AT) team capability;
- OT technologies from different control suppliers and OEMs;
- Manufacturing local area network (MLAN) and control local area network (CLAN) from flat to comingled to separated; and
- Push or pull styles of technology integration.

"We're not invincible," explains LaBonty. "We had very poor visibility of our industrial control system (ICS) assets; 7,000 ICS information technology (IT) devices, including many that couldn't be patched anymore and many at end of life; 24/7 operations at 60 plants, making it difficult to schedule downtime for patching; and limited IT and operations technology (OT) governance that increases recovery times."

Downtime, maybe death

In the past, cyber attacks were more inconvenient than dangerous or life-threatening, but today's cyber attacks can quickly go from annoying to potentially injurious or even put lives at risk.

John Cusimano, vice president of industrial cybersecurity, aeSolutions (www.aesolns.com/industrial-cybersecurity), a consulting, engineering and CSIA-member system integrator in Greenville, S.C, agrees the most significant cybersecurity events recently were the Triton/Trisis safety system malware and the WannaCry and NotPetya ransomware attacks. "These events have shaken industry even more than Stuxnet," he says. "Triton/Trisis was especially alarming because of the potential impact to health and safety. It's raising awareness of the importance of security safety systems per the IEC 61511 and 62443 standards. People who believed their last-line-of-defense safety systems were untouchable have realized they're just as vulnerable."

To protect safety systems from these and other attacks and malware, Cusimano recommends users employ physical key switches to prevent changes to local devices. "I'm a big fan of key switches as a layer of protection for remote access and management of change. If remote access is required for troubleshooting, someone should still have to stand in front of a rack or cabinet to say when it's OK to allow remote access, and then turn it off later," says Cusimano. "Any process that's potentially unsafe should be monitored locally, and require someone to be there to provide ushered access."

Logical first steps

Most cybersecurity efforts begin with the defense-in-depth concept of deploying multiple layers of protection between plant-floor OT and business-level IT, and the Internet. This typically suggests users:

- Inventory existing devices and software;
- Perform a cybersecurity risk assessment that checks for vulnerabilities such as open network ports;
- Use passwords and other authentications;
- Segment production areas with Ethernet switches used as firewalls, especially from IT, business networks and the Internet;
- Monitor network traffic for anomalous behavior;
- Enable physical security measures onsite;
- Establish cybersecurity policies, procedures; and
- Train and retrain staff, contractors and clients.

The U.S. Dept. of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ics-cert.us-cert.gov) reports that a defense-in-depth strategy's elements should include a risk management program, cybersecurity architecture, physical security, industrial control system (ICS) network architecture, ICS network perimeter security, host security, security monitoring, vendor management and the human element.

Out in the field

Just as users must be sure their contractors and clients are protected—and not just themselves—they must also extend cybersecurity beyond—and below—their usual networks, especially to sensors, instruments and other plant-floor devices. If identifying and fixing cybersecurity vulnerabilities means pursuing them into the trenches, then it's not time to worry about getting dirty. The constant downpour of cyber probes, intrusions and attacks are only increasing, and just like a flood, are seeking entry at any vulnerable point. Fortunately, ground-level troubleshooting is one of the jobs that plant-floor personnel know and do best.

"Almost all cybersecurity, whether IT or OT, is based on network threat hunting and network anomaly detection. Control system users rely on information from OT networks. However, they typically lack expertise at the process sensor level, even though attacks can come from that source," says Joe Weiss, managing partner at Applied Control Solutions (ACS, realtimeacs.com) and producer of *Control*'s Unfettered blog (www.controlglobal.com/blogs/unfettered). "Some attacks can look like malfunctions, so even if a user's data appear to be secure, their system and equipment could still be corrupted. Many disasters have been caused by sensors and physical device failures. Process sensors have been hacked. Consequently, it's crucial to understand how these and other Level 0 components must secure their own ecosystems for any control system cybersecurity program to be effective. Unfortunately, no sensors to date have completed c

Seven cybersecurity commandments

Though every user, application and organization should be well aware of their primary cybersecurity tasks, they always bear repeating to get them fully instilled into an effective cybersecurity routine. They include but aren't limited to:

- Switch on passwords, enable other user and device authentications including two-factor when available, and enable basic anti-malware software.
- Isolate sensor, instrument, equipment, production and other operations technology (OT) networks from administrative, enterprise, corporate, Internet and other information technology (IT) networks with multiple managed Ethernet switches used as firewalls.
- Divide plant-floor operations into networks and sub-networks based on priority functions, criticality and safety with added firewalls.
- Establish publish-subscribe capabilities such as MQTT protocol and data diode that allow production to transmit data upwards, but don't allow incoming communications or software downloads.
- Collaborate with OT and IT to evaluate and select logical software patching policies.
- Educate, test, drill and retrain employees to follow security procedures, so they become habit and part of the organization's culture.
- Implement continuous and routine network network traffic evaluation using IT-based software that can find, separate, reject and mitigate non-baseline communications, activities, probes and intrusions.

Cogenerator cuts patch time

As the largest natural gas-fired, combined-cycle electricity and steam generating plant in the U.S., Midland Cogeneration Venture (MCV, midcogen.com) in Midland, Mich., has always taken cybersecurity seriously. Its 1,633-megawatt (MW) combined-cycle power plant produces up to 1.5 million pounds per hour of bulk process steam for nearby chemical companies. The plant runs 12 ABB GT11N gas turbines, 12 CE heat recovery steam generators, two GE condensing steam turbines, and one ABB Stahl noncondensing steam turbine.

Because of North American Electric Reliability Corp. (NERC) Critical Infrastructure Protection (CIP), Version 6, standards that went into effect in July 2016, MCV had to comply with CIP standard 2 through 11. This meant that a formal, documented process for patch management, configuration management, security event monitoring and more was needed. However, with only two staffers responsible for control systems on more than 12 operating units at MCV, meeting those obligations would be difficult. In fact, a cybersecurity program using homegrown tools and tracking sheets would require the two-person team to manually patch 70 control system-related workstations, which was unmanageable because this monthly task would actually take 45 days to complete. This initial plan also didn't include patching workstations on other plant networks or the team's responsibility to manage malware protection, annual vulnerability assessments, configuration management and daily distributed control system (DCS) operations.

"After reviewing several options, the most comprehensive cybersecurity proposal came from our DCS supplier, Emerson Automation Solutions (www.emerson.com), which already knew us, our plant and our systems well," says Scott Woodby, engineering manager, MCV. "Its customizable cybersecurity suite integrates hardware and virtualized software modules to provide security management functions, not only for Emerson's Ovation system, but also for controls from other suppliers."

As a result, Emerson's patch management module was installed to push patches out to Microsoft Windows workstations and servers once a month. A centralized, automated patch management process proved more manageable, taking about 7-11 days to complete—nearly 30 days faster than the previous manual process. Added cybersecurity modules were also deployed, including security incident and event management, backup and restore, configuration management and malware prevention.

After successful implementation of the cybersecurity modules, responsibilities of MCV's two-person team expanded beyond managing the security of the primary DCS system to include all plant networks and equipment affiliated with plant operations including turbines, CEMS and plant LAN assets—nearly doubling their scope of responsibility to 140 workstations and servers.

bersecurity testing, which is needed to monitor their raw signals in real time. Ironically, the serial-to-Ethernet filters used to move data up to Ethernet networks don't allow higher-frequency, raw data anymore, but this is what's needed for sensor-level forensics to monitor and plug these holes at the lowest levels."

Weiss adds that sensor-level cybersecurity and process safety can be improved by implementing an independent network for plant-floor devices that's not tied the usual Microsoft Windows, human-machine interface (HMI), and other Ethernet-based, IT-related networks compromised by Stuxnet and Triton. "It's important to do a cybersecurity risk assessment to understand critical processes and sensors, and determine what's needed. However, their relative criticality is in the eye of the beholder, so having a serial, I/O-Link or other hardwired network that's removed from the Windows and IT network can help an operation maintain its process view and control if and when the main network goes down," explains Weiss. "This really is back to the future because it's a lot like the redundant safety networks mission-critical processes used to avoid having a single point of failure. Luckily, installing a redundant network is easier and less costly now. For example, for a feedwater control or critical condensate application, all that a redundant network would need is less than 10 sensors to monitor critical measurements such as temperature, pressure, flow and valve position."

Evaluate and organize

To continue its mission as a trusted pharmaceutical provider, Pfizer launched its ICS Cybersecurity program in February 2018 to achieve control system hardening and rapid threat detection at its 60 plants. LaBonty reports its key objectives are:

- Mitigate unpatchable IT and OT assets and related risks;
- Gain rapid visibility of ICS threats and the ability to detect IT and OT malware;
- Update inventories daily of system assets and status of their vendors, models, operating systems, versions and firmware;
- Protect manufacturing platforms from intrusion and attacks by known and unknown malware;
- Limit paths and traffic to reach critical manufacturing systems via networks, USB or other means; and
- Make certain ICSs in the OT layer have no direct connections to or from the Internet.

"To make our assets and systems as secure as we can, we need close-in looks at them and their control systems layers," says LaBonty. "We also need daily updates about what assets we have because maybe next week a new suite is added, and an old one is swapped out. To be really protective, we can't work with old data. We could follow IT and patch like crazy to protect against attacks, but we asked if there was a better way, and I think we've got a solution. Still, we need to limit avenues to the factory floor, and limit data that gets down to the ICS to just what's needed to run and optimize the plant."

Beyond adopting more heads-up cybersecurity software, La-

Bonty reports Pfizer's ICS Cybersecurity program also aims to improve on the ISA99 cybersecurity standard's organizational layers with added network segmentation where needed, but also by combining OT and IT tools where useful.

"We learned to migrate what IT and OT each do well, but also segment them to narrow network paths and attack vectors to the few critical platforms for operating our systems. We use 10 to 20 firewall rules, not the hundreds or thousands that IT uses. We just say, 'This server can talk to that device,' and that's it."

The Pfizer cybersecurity program has seven workstreams:

- Global manufacturing security policy,
- Manufacturing security organization,
- Security awareness/training,
- Risk management
- Preventive and detective controls,
- Asset discovery and threat detection, and
- Vulnerability management.

Besides installing added firewalls, the program initiated pilot programs for passive network threat detection and asset discovery, OT hardening and whitelisting ICS OT assets, and USB device lockdowns and security, which will be full-scale programs that will be built and optimized during the next couple of years.

> "Just pick one. Waiting for nirvana and the perfect cybersecurity solution is waiting too long."

"We're working quickly and making progress, but people are the base. That's why our first four workstreams are organizational, and consist of training, developing a security champion matrix across all sites, connecting to our security operations center (SOC), and enabling policies and structures for cybersecurity governance," says LaBonty. "The last three workstreams are technical, where we focus on automating asset discovery and threat detection. I'm from the OT world, so I'd rather have a tool that identifies assets, so I don't have to walk around everywhere and can focus optimizing processes, instead of maintenance tasks like gathering, logging and keeping track of data.

"We'd also rather use tools for asset discovery, threat detection and vulnerability management, so we kicked the tires, and found out what worked well and what didn't. It helps that the suppliers that offer these tools are very good, so my best advice is just pick one, and work with them to secure your asset base. Waiting for nirvana and the perfect solution is waiting too long."

Take a page from IT

Though many OT folks view their IT counterparts with sometimes justified suspicion, IT has been dealing with malware, viruses, worms and other quickly evolving cybersecurity issues for more years than the manufacturing side—and offers many best practices OT can use. However, even though IT technologies, such as intrusion detection, are making big strides into OT, aeSolutions' Cusimano adds it's important to remember that OT networks have different needs and need to be “tuned” to their environment for maximum benefit. "For example, to help users get the most value from their ICS detection investments, we visit a site, make sure the system is properly installed, monitor its traffic and performance, and build dashboards and displays," explains Cusimano. "Users often recognize they're not getting the performance and value they expect, so aeSolutions can help them 'operationalize' their investment by, for example, making sure that alerts make sense to the operators."

Cusimano adds, in the swirl of rapid technological change around cybersecurity, it's also crucial to avoid installing the latest, shiny solution without addressing less exciting, underlying network and device vulnerabilities. "This is like installing a high-tech alarm system on a house with unlocked doors and windows," he adds. "These underlying issues usually include lack of network segmentation, weak access control, and lack of network and device hardening, such as switches that haven't disabled unused ports, installed the latest patches or are too easy to access. These tasks aren't so easy, and many users shy away, but they must be addressed."

Always, the human element

Of course, even if all the bases are covered—at all levels—with the latest cybersecurity solutions, they can't be effective if the people using them aren't made aware, thoroughly trained, and routinely practiced in cybersecurity best practices. Just as sensor-level cybersecurity must be understood and implemented, Weiss reports that laptops, tablet PCs, smart phones, calibrators and other portable/handheld devices are often taken inside firewalls, even though they're potentially cyber vulnerable and could transmit malware. Consequently, these devices also need to be secured before connecting them to sensor networks.

"Engineers and other users must be trained, so they can understand if a process is doing what's expected. If there's an upset, does it make sense? If not, they must be able to talk to their network people to see if anything funny is happening," says Weiss. "IT doesn't usually care if a motor has a problem. However, cybersecurity is also about better understanding operations and what's going on. That can't be done by keeping process engineers out of the picture. Policies and procedures can be drafted, but you must have control system expertise, not just cybersecurity, to make sure cybersecurity policies don't negatively impact control systems."

To help rally OT and IT together around cybersecurity, Weiss reports management must recognize it's a priority, establish procedures and governance, and dedicate resources. However, he adds, management must also clearly define who's in charge of control system cybersecurity devices and software. "Management has to tell engineering, 'This is your equipment and you're responsible for it.' Engineers don't usually attend cybersecurity meetings, but if a new device has been added to a turbine, then engineering needs to be involved. With the cybersecurity team telling engineering the cyber-implications of using new devices, this coordination can be started by bringing engineering and networking people together, and developing key performance indicators that demonstrate how they're working together."

Act and implement

Once its ICS Cybersecurity program was in place, LaBonty reports Pfizer segmented its IT and OT networks, separated its formerly joined MLAN and CLAN at its plants with firewalls, and restricted the avenues between them (Figure 1).

"We knew that we had to segment our IT and OT networks, so we went to the sites with the biggest supply chain or business risks, and tackled and completed their segmentation in about six months during 2018," says LaBonty. "Since we kicked off in 2Q18, our cybersecurity team has grown to about 60 people, and includes three Pfizer people, but mostly consul-

tants and vendors. Is this a highwire act? Yes, but we learned to play well, not get burned, trust that our suppliers will deliver, and improve our cybersecurity with minimal risk."

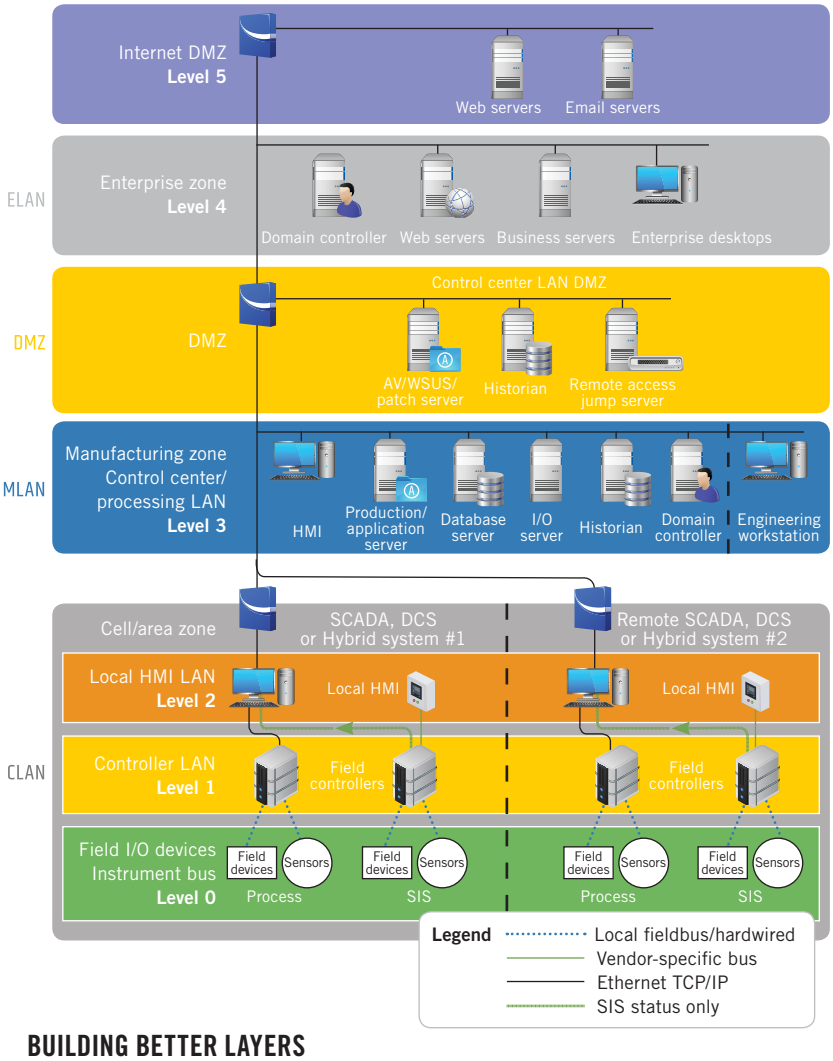
LaBonty adds a crucial aspect of Pfizer's threat-detection workstream in its ICS Cybersecurity program is passive detection that can view its operations and security measures in real time. "If you and your cybersecurity tools can see production and network traffic while they're happening, then you can be smarter, and know, respond and plan better. You can even let intruders and malware look around a bit, so you can see what they're after before they do anything bad."

Meanwhile, the program's second technical workstream, OT hardening and whitelisting ICS OT assets, relies on the fact that normal operations are relatively stable and don't change much. "Usually, what a controller talks to its devices about doesn't change, so if something starts talking against the baseline, then that's something to look at. Again, the key is making visible what's been invisible in OT. If you're going to invest in segmenting a network, then invest in one or more tools that will let you see it. IT has always been able to view it's network activity, but OT didn't have to as much because it didn't used to get attacked. Well, now we're front and center on the cybersecurity radar screen."

Finally, USB device lockdowns are the third technical workstream in Pfizer's ICS cybersecurity program because 90% of intrusions still come from the IT side to the controls side, according to LaBonty. "We still use some USBs with an added security layer, and this is because we allow zero communications and data to go though cellular modems," he added.

For example, on a representative aseptic production line, LaBonty showed that Pfizer can view ICS and IT assets discovered at the manufacturing executive system (MES), supervisory control and data acquisition (SCADA) and programmable logic controller, (PLC) and equipment levels, as well as communications and data flows. "Plus, we can filter our displays, so they only show OT activity," said LaBonty. "Previously, we'd have to find logical flow maps. Now, we can see what's talking to what, and when a new PLC is added or swapped, it's detected and displayed in two seconds, including a complete audit trail. If a device is added or a wire us changed, you know it.

"This is all a little bit Big Brother, but it's good because we can operate our plants well. Many users change their behavior and culture based on the possibility of being watched. If someone may see them, people will think before doing something, and that's good, too. Viewing our OT assets also gives us insights, instead of having to scramble to check and confirm what's happening. The tool also recommends what we should work on, and takes out 80% of our former effort, so we can spend that time optimizing our processes and saving money."



BUILDING BETTER LAYERS

Figure 1: One of the primary strategies Pfizer's ICS Cybersecurity program is using at its 60 different pharmaceutical plants is separating its formerly joined manufacturing local area network (MLAN) from its control local area network (CLAN) with firewalls, and limiting the networking paths between them, so that only authorized communications and essential data needed to run and optimize the plant are allowed through. Source: Pfizer

Still—watch the network

Once passwords are enabled and networks are segmented—and even though the device level must be addressed—the most pervasive cybersecurity procedure is still network monitoring, traffic analysis, and threat detection and response. For instance, the City of Raleigh, N.C., recently deployed Indegy's (www.indegy.com) Industrial Cybersecurity Suite in just a few days to its public utilities that provide water/wastewater and other services to 500,000 customers.

"One thing that was a real plus was the ability to query PLCs and get back information about what programming changes had been made to them, versioning information as changes were made that we didn't have in the past. Now we have a time stamp on when changes were made, and can determine who made them," says Steve Worley, SCADA security manager, City of Raleigh NC Municipal Government. "Other solutions do more passive monitoring, but Indegy does both the passive and active component that was a real value to us. We wanted to provide some accountability to our system integrator, who was making changes on a regular basis. We also needed to do some automated asset discovery, but it's a huge job to keep track of them, and so automation is key."

Worley adds that within minutes of installing and engaging its Indegy device, the utility was able to provide a huge amount of data on the network that would have taken weeks to collect by hand. "The automation provided asset names, IP and MAC addresses, and other things that were useful to us for network management, and didn't have to be gathered manually," says Worley. "We had it all on one screen on the Indegy console. Because some of the asset management is automated, I can spend less time on that and more time on looking at vulnerabilities and remediating them."

> "We only pause the kernel for a few microseconds, but this lets us see any bad code and kick it out."

Communicate, collaborate, trust

LaBonty adds Pfizer selected Rockwell Automation (www.rockwellautomation.com) as its global network services partner because of its global reach, experience and local country support. Services provided include design, global implementation, global logistics, PMO coordination, documentation, testing, local site training, and OT network services support.

"This gives us timely, effective communications, as well as closer partnerships and trust," says LaBonty. "Segmenting our IT and OT networks, adding cybersecurity infrastructure, and migrating assets down to the control system network layer clears up the mud on former IT vs. OT issues, and clarifies roles, scope and other broad areas, so we can make headway quickly. We're establishing separate global IT active directory (AD) domains and local manufacturing site OT layer AD domains, and adding tools to manage them that also set up account and audit trails."

"All of these asset discovery, threat detection and vulnerability management tools are important because many of Merck's assets were wiped out in two hours. If you don't have some cybersecurity protections in place, by the time you've figured out you have a problem, it will be too late, and you'll be toast."

In addition, Pfizer reports that it's been working with four-year-old Digital Immunity (www.digitalimmunity.com), which is a bioinformatics-based cybersecurity provider that develops in-memory, runtime security software. For instance, its DI Protect product runs in the kernel to harden operating systems and related applications to prevent malware attacks.

"We identify trusted operating systems and related applications on the Microsoft platform, and harden them," says John Murgo, CEO of Digital Immunity. "No other solution provides in-memory, runtime protection using bioinformatic DNA mapping. This means we can stop attacks without any pre-knowledge of the attack on operating systems and applications by building a shield around every process and binary. So far, we've detected 100% of exploits against vulnerabilities."

Murgo adds Digital Immunity can help resolve the traditional conflict when IT tries to apply software patches and OT refusing due to downtime and safety concerns. "We can help defer patching and protect un-patchable systems because our software is more active and uses a more deterministic approach to identify which ones and zeros are good or bad," explains Murgo. "For instance, many OT and IT applications and supply chains can't have downtime and they can't deploy antivirus software on the OT side because they can require shutting down production lines during operation. DI Protect is more lightweight and surgical because it runs in the kernel-level at Ring 0 of Windows, while most other software runs at Ring 3. This is really the only way to address this problem because it protects the memory where the code is executed by preventing executable payloads. For example, it would have been able to prevent the Triton/Trisis code from executing."

To protect process applications and their endpoints, DI Protect functions by verifying code loaded in memory, comparing it to each process "DNA map", and "walking the stack backwards" to check any executable code that's trying to run. "We only add a few microseconds of overhead, but this lets DI Protect see any bad code that's been injected, and kick it out," says Murgo. "This lets good processes and applications keep running by eliminating bad processes." ∞