BIZCOMMUNITY

A collaborative approach to cybersecurity in a converged IT/OT environment

By Antoine D'Haussy

16 Apr 2020

In industry, technical evolutions are transforming operations and driving innovation. And at the same time, devices, endpoints, and networks across both IT and OT environments are more connected than ever.

Antoine D'Haussy

In fact, Forrester research commissioned by Fortinet shows that 66% of industrial firms say their factories now run through IP-connected networks. But the road to the future is also filled with potential cybersecurity challenges – and these are only exacerbated by the longstanding divergence between IT and OT security teams.

For example, despite business environments being more connected than ever, IT and OT security teams still operate in silos – interacting, but falling shy of true integration. Historically, IT and OT have had very different security concerns; OT's domain generally wasn't a part of the connected IT world, thereby minimising the threats it faced.

But as OT operations become increasingly digitalised, their networks are being exposed to more cyber risk. In fact, almost three quarters (73%) of industrial firms believe that the attack surface of their IP-connected factory machines has expanded.

So, in a world where even a factory production line could now be controlled by malicious actors, cybersecurity is no longer just about protecting emails and users – it's also about keeping factories, production systems, processing plants, refineries, energy plants, transportation and delivery networks, and other essential infrastructures safely operating. To achieve this, a collaborative approach to security solutions and incident response is essential.

Benefits worth converging for

The business benefits of converging IT and OT are significant: 66% of firms agree that such collaboration can provide access to real-time data insights from manufacturing operations, while 59% believe it can create new business opportunities via increased insight into production data.

The security benefits of converging IT and OT strategies are also numerous. Forming effective processes, adopting specific, stringent industry standards, and delivering an orchestrated response is much easier with a consolidated group. It's not hard to see why 43% of industrial firms feel this convergence contributes to enhanced visibility that can enhance the mitigation of cybersecurity threats.

Convergence can create efficiencies, too. Threats identified by one team can be rapidly defended against by the other, stopping the spread of malicious intent and malware. And it's undoubtedly more convenient to only have one security system to pay for, configure, manage, and maintain – which is a more likely outcome when IT and OT security approaches are converged.

But the advantages don't end there. Merging these teams provides a ripe opportunity for cultural transformation, creating the ideal breeding ground for innovation as two sets of intelligent people collaborate to generate a truly robust and comprehensive security strategy.

Roadblocks ahead

There are, however, some serious difficulties in redressing this division – starting with the technical specificities of OT and IT. OT experiences a longer product lifecycle and has to grapple with a wide breadth of industrial protocols and environmental constraints due to the nature of the equipment used.

Implementing a specific architecture in-line with industry best practice standards is crucial to making sure OT teams are able to thrive in the new converged environment – and getting all of this in place can be time-consuming and complex.

Priorities are also different. IT networks prize confidentiality and data integrity over availability, while the nature of production lines and factory floors demands that availability and the security of personnel be at the top.

As a result of these inverted priorities and very different technologies, there are bound to be clashes when these two groups with differing viewpoints are brought together. People who work in these two teams tend to have different attitudes towards their lines of work.

OT workers are often more conservative, focusing on the process, output, safety, and availability. In contrast, those in IT are more likely to be early tech adopters, eager to embrace change, and very data-centric.

Blending these two groups together and establishing a harmonious workforce isn't easy, but it can be done if those involved are willing to embrace a new, third way of thinking.

Fusing IT and OT Teams

Anyone looking to kickstart this merger will need to sit down and apply their focus to planning strategic alignment on goals.

Driving cultural transformation will play a key role in the success of any convergence project, with strong leadership needed to ensure culture clashes are dissipated and neither party feels like an afterthought. Be aware that changes may cause friction – so explain what is being deployed and how it will affect the process to ensure that nobody feels left behind or confused by complicated terminology.

Care must also be taken to make technological adjustments to accommodate this merger, such as adopting security tools that cater to both IT and OT requirements. Collaborative tools such as SIEMs (Security Information and Event Management) and SOARs (Security Orchestration, Automation and Response) can help security teams manage and respond to threats at machine speed, rather than having to plough through log files and system reports manually, wasting time and leading to a bottleneck of issues to resolve.

It's not just the amount of new hardware that poses a risk to these newly converged teams – it's the nature of that hardware as well. The devices used by OT often present a set of unique security liabilities that IT teams may not have had to tackle before. Older systems that may have been in place for years not only have never been updated, they also monitor critical systems, such as thermostats and pressure valves, so they cannot ever be taken offline, even for patching. And ultra-sensitive systems designed for pristine environments can be affected simply by being scanned.

But as the network expands and becomes more connected, it's also increasingly important to keep tabs on what's going on – and increasingly difficult to stay on top of it all. OT threat reports by Fortinet indicate that threat actors target both IT and OT systems using the same malware, banking on the fact that OT systems often use older technology to ensure a higher success rate.

Dynamic, intelligent processing solutions like Next-Generation Firewalls, secure access, and Network Access Control, combined with OT-specific protocols, can be combined to create a zero-trust network access strategy to ensure accurate control of network traffic combined with high visibility across the new converged team's operations, allowing easy and centralized management of complex systems.

There's a wide range of additional tools available to give any team 360-degree protection from cyberattacks, from sandboxing to two-factor authentication. These are essential weapons against intrusions, such as automated malware that would be otherwise free to roam the expanded network in search of sensitive data to steal.

Do it Right – Do it Once

Adopting a 'safety first' stance may be more time-intensive, but rushing convergence will only lead to problems down the line. Making the effort to prioritise security at the start will ensure these new converged teams against future disasters without impacting end users. Looking at the bigger picture and embracing a structured and tightly integrated cybersecurity platform can also help reduce the inevitable complexity of the process, while continuously confirming that newly deployed systems are aligned with industry standards and frameworks.

With a combination of a converged vision and the right tools, any business or industry can reap the rewards of IT/OT convergence. It’s simply a matter of working together. It’s not always easy, but it is worth it.

ABOUT THE AUTHOR

Antoine D'Haussy, Director Business Development EMEA Operational Technology at Fortinet