Lets talk about Cybersecurity for the Manufacturing Sector: CS2AI Symposium Wednesday, May 25 1:00PM EST

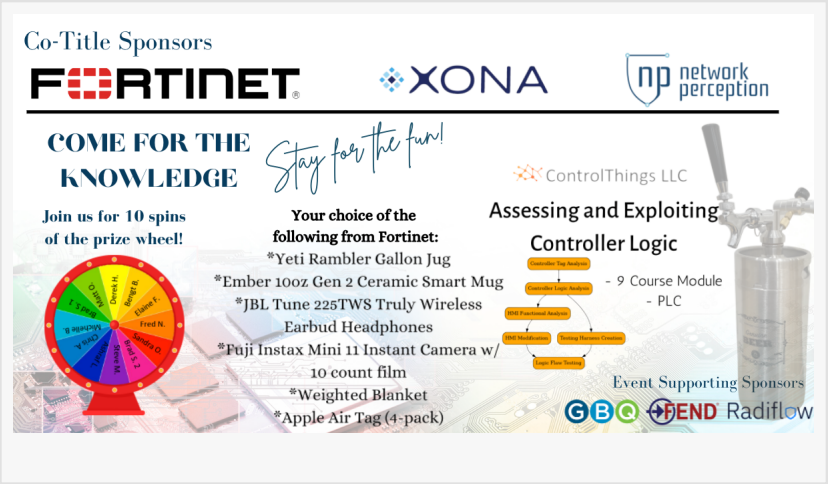
We invite you to join us for Part 1 of the Cybersecurity for Manufacturing Sector this Wednesday at 1 EST. This symposium is free and virtual.

ATLANTA, GA, UNITED STATES, May 23, 2022 /EINPresswire.com/ -- If you work in the manufacturing sector or have any interest in gaining more perspective on cyber security for the manufacturing sector, I invite you to join us on Wednesday, May 25th at 1pm Eastern for Part 1 of a (CS)²AI Online Symposium focused on Secure Control Systems for Smart Manufacturing. REGISTER HERE Part 2 event will be in Q3 with an end-user/asset owner perspective.

> Whatever metric one chooses to study, it is easy to see that the manufacturing sector is enormously critical to any high demand just-in-time economy."
>
> *Derek Harp, Chairman and Founder at CS2AI*

Whatever metric one chooses to study, it is easy to see that the manufacturing sector is enormously critical to any high demand just-in-time economy. In 2019, in the United States alone, more than 12 million workers were employed in manufacturing and produced more than $2.3 trillion of dollars of output.[1] Several manufacturing subsectors are noted to be growing particularly rapidly, notably pharmaceutical/medicine and aerospace products/parts.

At the same time, the manufacturing sector is getting "smarter" every day. Smart manufacturing is a very broad term with varied use, but generally refers to manufacturing which integrates digital information technologies to achieve high levels of operations insight, adaptability, and rapid responsiveness to changes in demand, supply chain, or other dynamic conditions. Do some of these awesome new business capabilities come with a dark side? Yes, they most certainly do!



Anyone following recent supply chain issues should be aware that manufacturing is a very frequently attacked sector, with IBM researchers finding that 23% of ransomware attacks targeted the manufacturing sector in the past year,[2] increasing several hundred percent over the previous year.[3] Reasons for this include financial motivations, with manufacturers counting high rates of fiscal impact during disruption and therefore strong incentives to take whatever steps promise rapid returns to normal operations (such as paying ransomware demands), and lower security profiles than other industries that have been forced to mature sooner.[4]

Ransomware attacks are not the only threat, of course, with phishing, business email compromise (BEC), and intellectual property theft on the rise as well, with BEC attacks four times as frequent as ransomware and hitting companies for as much as $60 million.[5]

Having such a large influence on any nation's economic health while also becoming increasingly more vulnerable brings important considerations to mind. We must better protect these important engines of commerce from intrusion, meddling and outright attack. It is certainly past time for manufacturing industry leaders to understand their risks and factor in the growing value (to various malicious 3rd parties) of causing disruption and/or stealing intellectual property. We must also not forget the disgruntled former employee too, who can in fact do $1.1M in damages from his home [6]

Though cyber security risks cannot be completely eliminated from any enterprise, there is low-hanging fruit in many low cyber security maturity manufacturing networks. There is prioritizable work to be done in most environments that can significantly reduce overall risk exposure to outside influence, reduce disruptive impacts, and speed recovery in the likely eventual event. If you want to gain some of those insights, please join me for Part I of a (CS)²AI Online Symposium focused on Secure Control Systems for Smart Manufacturing. This symposium will provide opportunities throughout the event to interact, ask questions, leverage the shared expertise of the (CS)²AI community and win some participation prizes?

On behalf of the (CS)²AI team, I also would like to take a moment to thank the staff of three of our Strategic Alliance Partners, Fortinet, XONA and Network Perception, who have collaborated with us to bring this two-part event together. Their thoughtful commitment to the event agenda (including locking in incredible speakers like Carlos-Raul Sanchez, Bill Moore, Robin Berthier and Paul Brownlee) and more to come in Part II in the series, has set us all up to walk away with new knowledge and actions that can be considered to mitigate risks associated with our smart

manufacturers. Thank you also to event supporting sponsors Radiflow, GBQ and Fend. A BIG Thank You to them and all the event speakers for taking time out of their busy schedules for our community.

Come for the knowledge - Stay for the fun!

Our adversaries discuss things and have even worked out ways to “trust” each other as incredible as that sounds. We must be better than that and why not have fun while we do it? The (CS)²AI prizes are awarded to event attendees that get involved in the event dialog. When you submit what we call a Quality Question during the event, you are more engaged, learn more and everyone benefits from it. You will also be entered to win 1 of 11 prize drawings valued at over $3000 total. We couldn’t offer free continuing education programs like this to the world without the generous support of this event's sponsoring partners. REGISTER NOW .

Sources:

[1] https://www.nam.org/state-manufacturing-data/2021-united-states-manufacturing-facts/

[2] https://www.tripwire.com/state-of-security/security-data-protection/manufacturing-was-the-top-industry-targeted-by-ransomware-last-year/

[3] https://www.xorlab.com/blog/how-ransomware-impact-manufacturing/

[4] https://www.radiflow.com/blog/why-cyberattacks-on-manufacturing-are-on-the-rise/

[5] https://resources.infosecinstitute.com/topic/the-state-of-bec-in-2021-and-beyond/

[6] https://www.theadvocate.com/baton_rouge/news/courts/article_7f6ea818-f488-11e6-bada-eb1757011f89.html

www.cs2ai.org

Trisha Harp
(CS)2AI
email us here
Visit us on social media:
LinkedIn

---

in today's world. Please see our Editorial Guidelines for more information.