

Burns & McDonnell Unit Launches Proactive Cyberthreat Hunt and Respond Capability

The new capability is a major step forward in protecting critical infrastructure.

WASHINGTON, DC, UNITED STATES, February 23, 2023 /EINPresswire.com/ -- Everyone involved in computers is aware of information technology (IT), but fewer are aware of its industrial sisters, operational technology (OT) and industrial control systems (ICS).



1898 & Co. clients will get round-the-clock and all days of the year monitoring of every possible vulnerability on their systems, with a focus on the harder-to-detect intrusions on their OT and ICS."

Llewellyn King

These related systems play a vital role in everything that is made, calibrated, moved, transported and used in manufacturing or other automated processes — which can include oil rigs, refineries and electric utilities.

OT and ICS are as vulnerable to cyberattack as IT. But cyberattacks are often harder to detect on OT and ICS and require different mitigation.

Cyber-criminals are as likely to disturb a process as to shut it down. Consider a big dairy, where the attacker might interrupt the pasteurization process.

The United States, using the Stuxnet computer worm, launched an undetected attack on nuclear centrifuges in Iran in 2010. It frustrated Iranian engineers who couldn't figure out why they had lost control of their machines; why they were spinning at unplanned speeds and disrupting production.

In his latest article for Forbes, Llewellyn King, wrote that the consulting company [1898 & Co.](#) is taking a major step forward in protecting critical infrastructure. Under the rubric of "Managed Threat Protection and Response," the company, an arm of the engineering, construction and architecture firm [Burns & McDonnell](#), is offering "a proactive threat hunting and response capability," he wrote.

King described this new capability as "a one-stop shop" for cybersecurity, embracing threats to IT, OT and ICS. It is an addition to 1898 & Co.'s existing Managed Security Services solution, and will draw on the extensive experience of its parent company which has built a lot of the critical infrastructure, especially in the electric utility space.

The new capability will be housed in an operations center in Houston, close to many of their clients. King wrote, "1898 & Co. clients will get round-the-clock and all days of the year monitoring of every possible vulnerability on their systems, with a focus on the harder-to-detect intrusions on their operating technology (OT) to their Industrial Control Systems (ICS) that are a critical part of the infrastructure and which require special attention."

King noted that the response for an IT intrusion and an OT intrusion may not be the same; the former requiring immediate cut-off and the later, maybe, a more strategic response.

As Chris Underwood, 1898 & Co. vice president and general manager, said in the article, "Managing security for ICS and OT for security is a rare capability for one reason: Critical infrastructure is a highly complex environment.

"Our consultants live and breathe critical infrastructure. We've worked in the industry and for the industry, so we have a deep understanding of its challenges."

Llewellyn King
White House Media LLC
+1 202-441-2702
llewellynking1@gmail.com

Visit us on social media:

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/618679647>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.