PFP Cybersecurity Participates in ICS-CERT Joint Working Group

Experts Gathered this Week to Discuss Industrial Control System and Critical Infrastructure Cybersecurity Challenges

Vienna, VA - October 9, 2014 - PFP Cybersecurity, a threat detection technology company, announced today they were selected to participate in the Industrial Control Systems Joint Working Group (ICSJWG) meeting that took place this week in Idaho Falls, Idaho. The ICSJWG was established by the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to facilitate information sharing and reduce the risk to the nation's industrial control systems.

The meeting brings together asset owners and operators, government professionals, vendors, systems integrators and academic professionals to discuss the latest initiatives impacting critical infrastructure security and address the risk of threats and vulnerabilities to their systems.

Thurston Brooks, Vice President of Product Marketing at PFP Cybersecurity presented a demonstration on the "Cyber-Detection Gap" on Wednesday, October 8. His 45-minute demonstration showed a new approach to cybersecurity using independent, out-of-band analysis, which detects anomalies, malicious intrusions, and unauthorized modifications in hardware, BIOS, OS, and software by monitoring side-channel signals. He also showed that, by using the instantaneous power usage of a device, all active and dormant attacks can be detected.

"We are honored to have been selected through a very rigorous process to participate in this Fall's ICS-CERT working group," says Steven Chen, Founder and Chairman, PFP Cybersecurity. "Threats to industrial control and SCADA systems are real, and working with an elite group like this to address these challenges is a great way to make strides in protecting our critical infrastructure and other vital systems."

For more information, visit: https://ics-cert.us-cert.gov/ICSJWG-Fall-Meeting-agenda-Idaho-Falls.

About PFP Cybersecurity
Headquartered in Washington, D.C., PFP Cybersecurity provides a unique, anomaly-based cyber security threat detection technology that can find any cyber intrusion in any device, including active and dormant attacks. With its innovative P2Scan technology, PFP shortens the window of attack detection and compromise to milliseconds by monitoring for changes in electromagnetic frequencies and power supplies. This physics-based technology can be applied to detect advanced malware and sophisticated threats in critical cyber systems. It can also detect threats of hardware Trojans and counterfeits in the supply chain. For more information, please visit: www.pfpcyber.com

---

Media Contact:
Julia McGavran
Merritt Group
802.318.8109
mcgavran@merrittgrp.com