Cyber Encounter Workshop Agenda

8:30 – 8:45	Welcome: CyberSecurity and CEROC
8:45 – 9:15	Keynote
9:15 – 9:30	*Break (Laptops ready and power up)*
9:30 – 12:00	**Inside Tips and Key Tools** – participants will follow along on their laptops 1. Virtualization – a key tool for cybersecurity competitions because VMware solves all IT concerns and it's a requirement for many competitions like CyberPatriot or the Maryland Cyber Challenge. We will walk through how to properly configure and use this amazing tool and look at virtualization alternatives like Cyber Range hosting. 2. Web Vulnerability challenges – besides View Source, what are the other approaches and tools to solve these puzzles. 3. Wireshark – forensics questions often include a network packet capture file (pcap) to investigate. Wireshark is used by professionals, it's an excellent addition to cyber classroom labs – and it's not hard to learn!
12 – 12:30	*Lunch*

	Teachers	Students
12:30 – 2:00	• Making the technology work to support your teams – hardware needs and what to tell the IT department to get their help.	• CTF Scavenger Hunt competition – students work in teams to solve a series of cybersecurity puzzles. Fastest teams to the solution win prizes!

	• <u>Pop-Up challenges</u> and solution walkthrough solutions coming from CyberStart – schedule and how to use leading up to the competition • <u>CTF Scavenger Hunt challenge</u> – solve as a group and learn ways to how to give hints, not answers, while helping students in competitions	• Brainstorming session – what are ways to recruit students at your school for cyber competitions? How to reach the "non-technical" students?
2:00 – 2:30	Award Prizes - Distribute Swag – Wrap Up	