Final thoughts from Chris Crowley @CCrowMontance

Carson:
. Measure not just the breadth of your log collection, but the depth
. Unit test your SIEM rules / use cases
. Track your SIEM use case analyst quality
. Analyst baseball card

Shelly & Brett
. Establish Trust and protect it
. Scribe to collect and report: but everyone is repsonsible for taking notes!

Alissa
. Insight into the state of your potential hires. Go read what they are saying about their prospects.
. Chaos is not for everyone
. Bad apples spread bacteria
. Let Alissa talk to your SOC analysts! Figure out the problems and address them.

SOC Survey
. Hard to collect data, and we don't have a defined data set, but here are the highlights for this year's survey.
. Tune in for the webcasts and download the paper.

CompariSIEM
. tools matter, but making the most of the tool is the path to success

FOOD, not FUD
. Framework of 5 items to provide Factual, Objective, Optimized Data

Sun or Stars
. Challenges are abundant, few organizations are thinking about striving for what's best for the long term

Hacking your SOEL:
. Move the activity to the front of the response activity

All about your Assets:
. Identify tools that contain the information you need, and figure out how to connect those tools together

The Healthy SOC: A Case Study:
. I'm going to ask you next year to come give a presentation about how you moved from where you are today to what you are next year. Will we be impressed? ;)

-=-=-=-=-=- ~Day 2~ -=-=-=-=-=-

What the CISO Really Wants
. Have an in person conversation once a month with no computers, no technology, where you listen to understand

Building the SecOps Use Case:
. Develop the program for building and assessing use cases, starting with business use

Back to Basics: System Integrity
. Integrity Monitoring is important for identifying change

TTP Zero:
. Normalize the data to constrained conecpts to effectively and consistenly deliver the message on security operations

Technical to Managerial positions:
. It's a different skillset, you probably can't be both

Threat Hunting Tour de Force
. Start with ad hoc techniques then migrate them into procedures

Burning Down the Haystack
. operational tasks should be operational, identify pain points and fix them

Most Dangerous Game:
. Assess if you have full coverage using ATT&CK