Microsoft

Azure Sentinel Level 400
Welcome!

Ofer Shezaf

Good morning

Introductions

Logistics

Goals

Agenda

Azure Sentinel level 400 training agenda

Modules:

1. Technical Overview
2. Use case / Business* discussion
3. Cloud architecture & MSSP support
4. On-prem collection architecture

Day 1

6. Writing rules
7. Playbooks
8. Hunting and Notebooks
9. A day in a SOC analyst's life

Day 2

Labs:

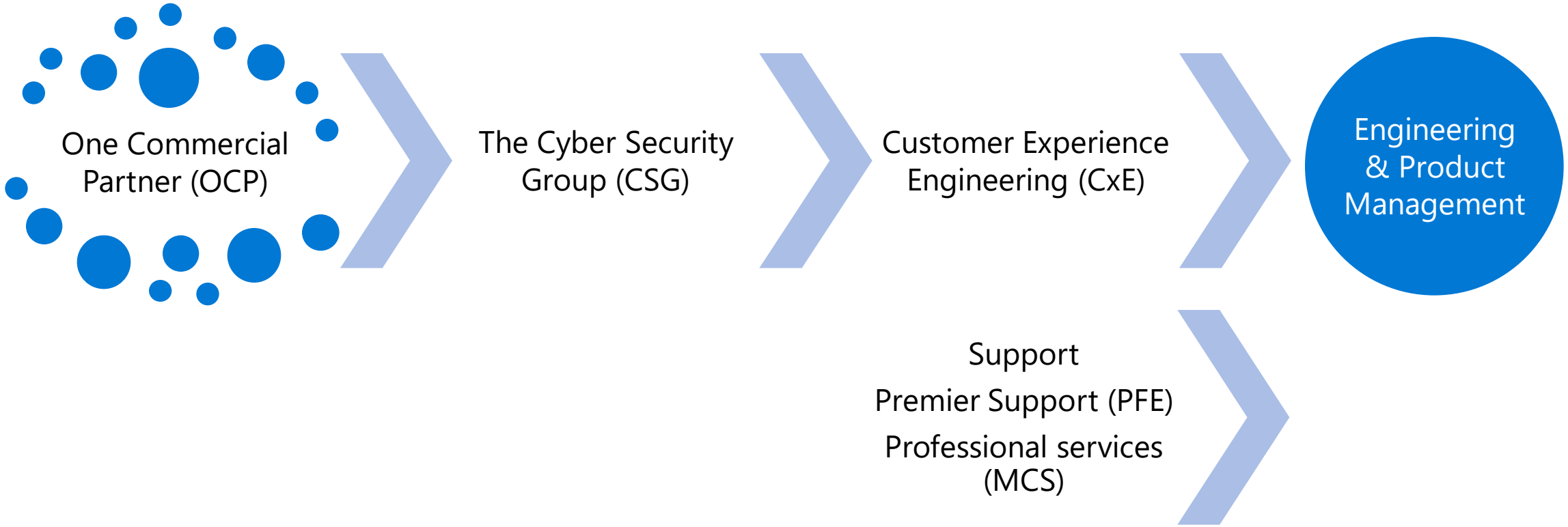
5. KQL Workshop — Day 1
10. Hands on Lab: Create alert rules, write playbooks, investigate, hunt — Day 2

*Use case for customers, Business for partners

The virtual version

Technical overview	MP4, YouTube, Deck
Cloud & on-prem architecture	MP4, YouTube, Deck
A day in a SOC life	MP4, YouTube, Deck
Deep dive into correlation rules	Deck, MP4, YouTube

Who is who?


One Commercial Partner (OCP)
The Cyber Security Group (CSG)
Customer Experience Engineering (CxE)
Engineering & Product Management
Support
Premier Support (PFE)
Professional services (MCS)

Resources

Learn:

- Partners Teams channel and e-mail distribution list
- Webinars, including many of the sessions in this course
- Tech Blogs

Discuss and contribute:

- Tech Community
- User Voice
- Github

Ask:

- AzureSentinel@microsoft.com