Time	Session
08:00 – 08:30	**Partner Breakfast**
08:30 – 10:00	**Partner Academy**
09:30 – 10:15	**Registration & Breakfast**
10:30 – 10:35	**Welcome Address |** Steve Hamilton, VP, EMEA North
10:35 – 11:20	**Certainty in an Uncertain World |** Dan Streetman, CEO *A Government Organisation*
11:20 – 12:00	**Facilitating the Future: Customer Panel |** Hosted by Charles Ross, CCO *University of Manchester | Leeds & York Partnership NHS Foundation Trust | A pharmaceuticals Organisation*
12:00 – 13:00	**Lunch**

	Breakout Sessions		
13:00 – 13:45	Lab 1: How to Operate Tanium Like a Pro for Patching and Software Maintenance	Lab 2: Hidden Exposures: Unmasking Vulnerabilities & Software Ingredients with Tanium SBOM & Comply	Customer Stories | Hosted by Steve Hamilton *Weir Group | Electrolux | Dutch Government*
13:45 – 14:05			Proving Value with Tanium | Erik Gaston & Dan Jones
14:05 – 14:25			Tanium + ServiceNow | Vivek Bhandari *ServiceNow*

Time	Session
14:30 – 15:00	**Break**
15:00 – 16:05	**Tanium Innovation: The Future is Autonomous |** Matt Quinn, CTO, Harman Kaur, VP AI and Melissa Bischoping, Director of Endpoint Security Research
16:05 – 16:35	**Tanium + Microsoft |** Vivek Bhandari, VP Product Marketing *Avanade | NCC | Microsoft*
16:35 – 16:55	**The Future of the CISO |** Steve Murphy, EMEA VP *Unilever*
16:55 – 17:00	**Closing Remarks**
17:15	**Converge After Party |** Ham Yard Hotel

Labs Descriptions:

Lab 1: How to Operate Tanium Like a Pro for Patching and Software Maintenance:
In this lab you will learn how to take your Tanium operations for patching and 3rd party updates to the next level. This lab will focus on Tanium Patch, Deploy, and Comply being used in a stepped maturity program designed to move organizations towards a mature automated approach, maximizing control and effective use of manpower. *Pre-Req(s): None*

Lab 2: Hidden Exposures: Unmasking Vulnerabilities & Software Ingredients with Tanium SBOM & Comply:
In this lab you will learn best practices for efficiently scanning your enterprise for vulnerabilities. You will identify vulnerable libraries that you may not have known existed within products you commonly use. Once the systems are identified, you will apply updates to the affected products to remediate the vulnerabilities. Finally, you will use Asset and Reporting to showcase vulnerable versions and the remediation efforts you have completed. *Pre-Req(s): Working knowledge of Tanium functions. Understanding of vulnerability and Patch management concepts. Working knowledge of Tanium Patch and Deploy modules*