Time	Session		
08:00 - 10:00	**Registration & Breakfast**		
08:30 - 10:00	**Partner Academy**		
10:15 - 10:25	**Welcome:** CIONET & Tanium		
10:25 - 11:00	**CEO Welcome Keynote** "Certainty in Uncertain Times"		
11:00 - 11:45	**CIONET CIO/CISO Panel:** "Required Capabilities for complex Infrastructure Programs like ZERO TRUST" (CIONET, Siemens, N26, MTU Aero Engines)		
11:45 - 12:15	**CMO Keynote** "Confidence: Platform & a Path"		
12:15 - 12:40	**CTO Keynote** "The Future is the Autonomous Endpoint Roadmap Pt 1"		
12:40 - 14:00	**Lunch / CIONET Executive Lunch**		
	Breakout Sessions		
	Executive Track	**Technical Track (Labs)**	
14:00 - 14:30	**Industry Panel:** Simplify Complexity / Road to Automation	**Lab 1:** How to Operate Tanium Like a Pro for Patching and Software Maintenance	**Lab 2:** Hidden Exposures: Unmasking Vulnerabilities & Software Ingredients wit Tanium SBOM & Comply
14:30 - 15:00	**Power of Platforms:** ServiceNow & Tanium		
15:00 - 15:30	**Power of Platforms:** Microsoft & Tanium		
15:30 - 16:00	**Break**		
16:00 - 16:45	**CIONET CIO/CISO Panel:** Implementing GRC Automation - Beyond the Checkbox		
16:45 - 17:15	**Business Impact of Automation** | VP Global Executive Engagement		
17:15 - 17:45	**VP of AI Keynote:** "The Future is the Autonomous Endpoint Roadmap Pt 2"		
17:45 - 18:00	**Closing Remarks & Wrap-Up**		
18:00 - 20:00	**Evening Reception & Networking**		

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

*Agenda subject to change