Session	Time	Topic			
General Sessions All attendees	8:00 – 9:00 a.m.	Networking Breakfast and Registration			
	9:00 – 9:05 a.m.	**Welcome | Rob Dao, VP of Federal**			
	9:05 – 9:45 a.m.	**Keynote | Mr. Chris Cleary – Dept. of Navy Chief Cyber Advisor** Secure, Survive, and Strike: How The Navy's Cyberspace Superiority Vision can offer guidance for other defense and civilian departments			
	9:45 – 10:25 a.m.	**Fireside Chat| ServiceNow + Tanium | Jonathan Alboum and Matt Marsden** What we don't know *can* hurt us: How the definition of visibility has changed, and why most organizations don't have it.			
	10:25 – 10:40 a.m.	**Networking break**			
	10:40 – 11:20 a.m.	**Fireside Chat | Harman Kaur, Chief of Staff and Renata Spinks, USMC** Breaking Down Barriers in Cyber: Lessons learned from challenging the gender and structural status quo			
	11:20 – 12:10 p.m.	**Fireside Chat| Microsoft + Tanium**			
	12:10 – 12:15 p.m.	**Closing Remarks and House Keeping | Rob Dao, VP of Federal**			
	12:15 – 1:15 p.m.	Lunch			
Role Specific Breakout Sessions		Breakout Session	Breakout Session	Hands On Lab	Hands on Lab
	1:15 -2:00 p.m.	Next-level visibility and control with ServiceNow and Tanium integrated workflows	A strategic Look at network risk and identifying patterns for detection and response	Vulnerability and Patching Lab	Better Together with Microsoft on a Security Level Lab
	2:00 – 2:15 p.m.	Break	Break		
	2:15 – 3:00 p.m.	Tanium + Microsoft: Get more out of your G5 license with real-time threat data and precise patching	"Reducing the Fog of War by Increasing Cybersecurity Readiness"		
Happy Hour All attendees	3:00 – 5:00 p.m.	Networking and Happy Hour Barrel and Bushel			

Better Together with Microsoft on a Security Level	Vulnerability and Patching
In this session, students will be afforded the opportunity to leverage Microsoft Defender to generate alerts in Tanium Threat Response. From there, we will dig deeper, integrating with Microsoft Sentinel to further investigate, remediate, and take action on the endpoint. Pre-Reqs: A security mindset would be helpful, but all practitioners are welcome	In this lab, attendees will be given an overview into the entire life cycle of vulnerability management. In part 1, we will review best practices for configuring Vulnerability scans in Tanium Comply, including scan frequency and low resource configurations. In part 2, we will look at an automated patching strategy that allows for a W0-W4 monthly patching cadence and makes handling patching exceptions exceptionally easy. Lastly, in part 3, we will walk through configuring KPI reports to show vulnerability posture and patching efficacy using Tanium Data. Products: Comply, Patch, Tanium Reporting Service