Tech Tuesday Workshop Cobalt Strike Detection via Log Analysis

Tuesday, 11 May 2021 1:00PM EDT (11 May 2021 17:00 UTC)

Speaker: Chad Tilbury

Cobalt Strike has become the attack tool of choice among enlightened global threat actors, making an appearance in almost every recent major hack. Cobalt Strike is an extremely capable and stealthy tool suite, but log analysis can level the playing field, providing many opportunities for detection. This workshop will leverage data sourced from SANS FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics to provide insight into how Cobalt Strike operates and how to detect many of its characteristics via endpoint logs. Whether you are just starting out in threat hunting or a FOR508 alumni, there will be something for everyone in this new workshop!

Prerequisites: Participants will need a system running the Windows operating system to perform Windows event log analysis (virtual machines are okay).While logs will be provided in CSV format for attendees without access to Windows, your experience will be greatly diminished without native access to Windows logging libraries. Some familiarity with Windows event log is desirable.

System Requirements: Prior to the workshop, participants should prepare the following:

- A host or virtual machine running a Windows 64-bit operating system (Win7-Win10)
- Download and install Event Log Explorer 'https://eventlogxp.com/download.php
- Download and install Microsoft Sysinternals Sysmon: 'https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- Install a tool capable of viewing and filtering CSV files (this is particularly important for attendees who do not have a system running the Windows OS)

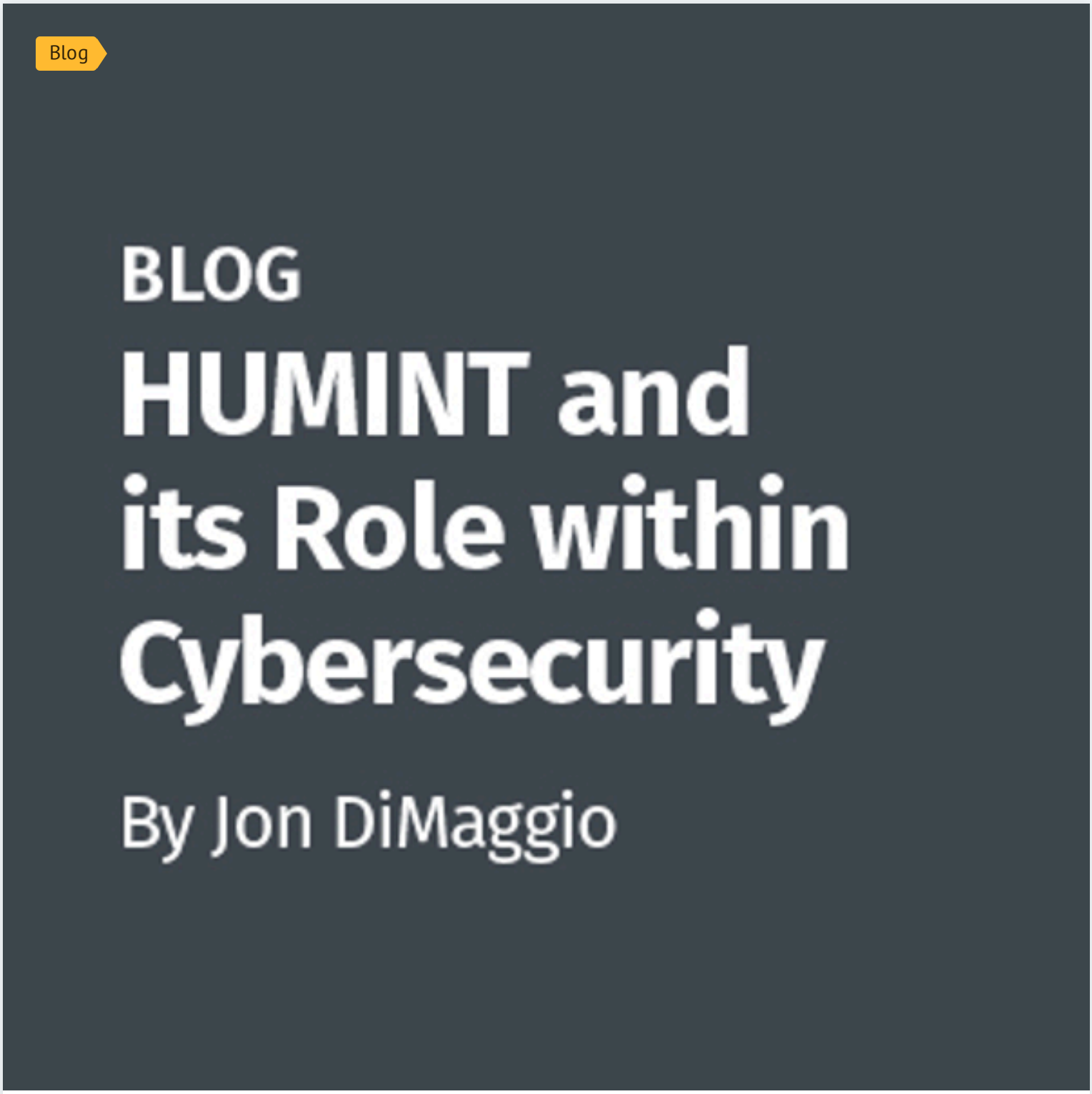
Lab materials should be downloaded here: https://sansurl.com/cobalt-strike-workshop-labs/

An optional final part of the workshop will include working with Cobalt Strike beacon malware. Examples will be given using SANS Linux-based SIFT virtual machine available here: https://digital-forensics.sans.org/community/downloads

***Please note:** Due to the nature of these workshops, many have a capacity limit, so to help us offer this opportunity to as many people as possible, we are asking that you please only register if you plan to attend live.

Login to Register

Related Content



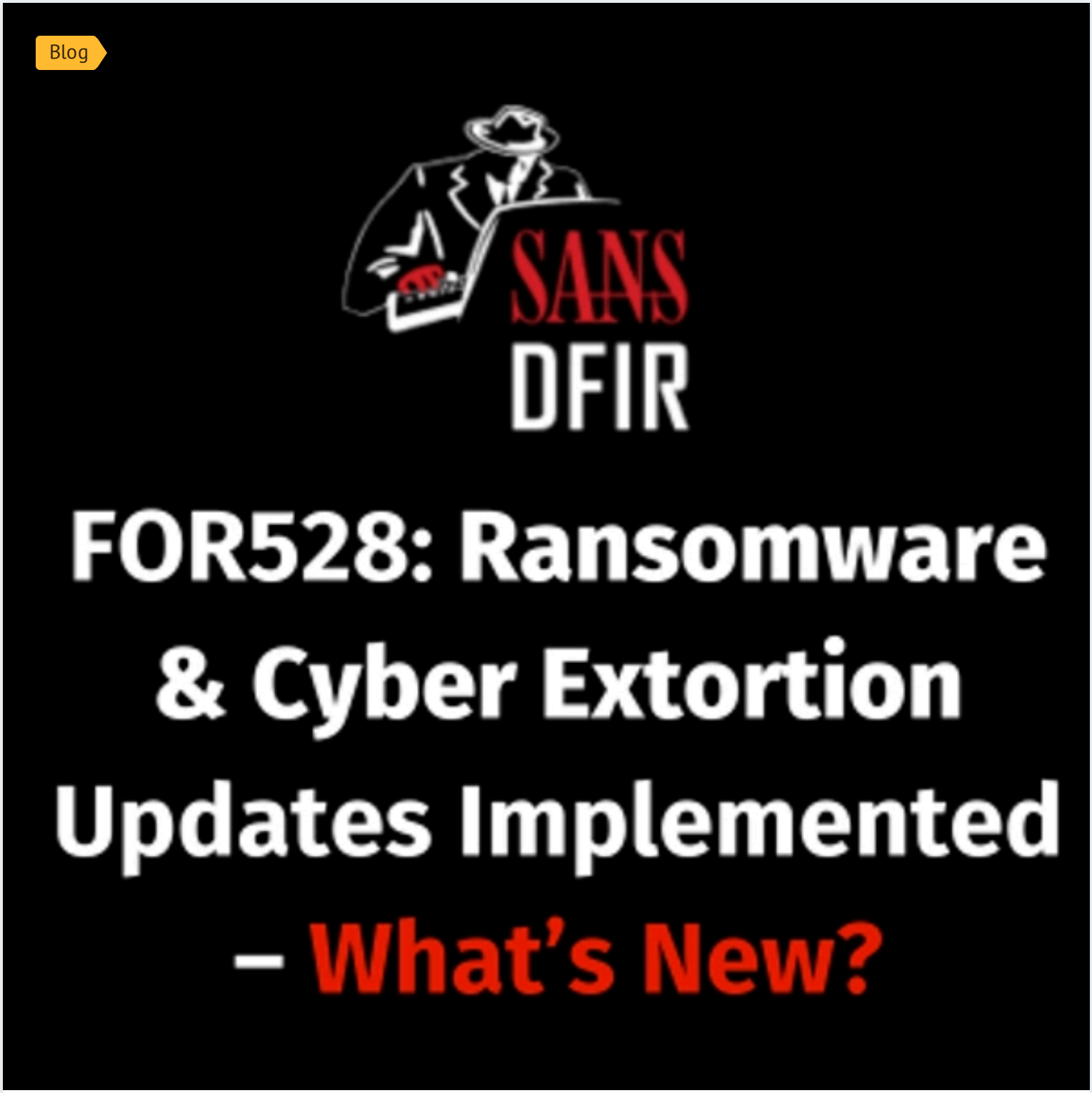
Digital Forensics, Incident Response & Threat Hunting · October 4, 2024

HUMINT and its Role within Cybersecurity

This blog explores HUMINT's role in cybersecurity, detailing its implementation, benefits, and potential risks.

Jon DiMaggio

→

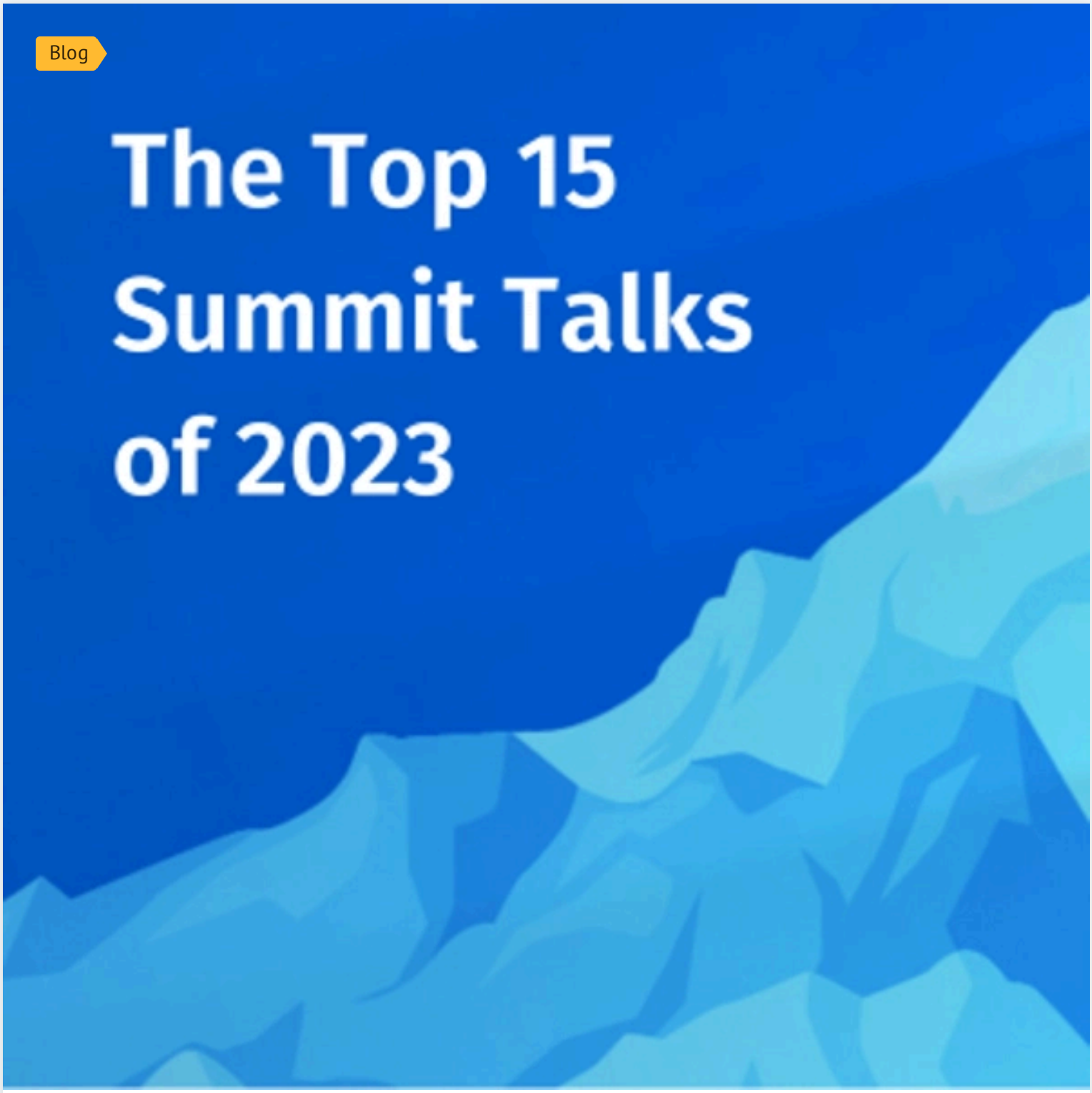


Digital Forensics, Incident Response & Threat Hunting · January 16, 2024

FOR528: Ransomware & Cyber Extortion Course Updates Implemented – What's New?

The recent FOR528 course better addresses the differences between ransomware and cyber extortion, and provides new hands-on labs and bonus content.

Ryan Chapman



Cybersecurity Insights, Digital Forensics, Incident Response & Threat Hunting, Cyber Defense, Cloud Security, Open-Source Intelligence (OSINT), Cybersecurity Leadership, Security Awareness, Artificial Intelligence (AI)

· December 18, 2023

Top 15 SANS Summit Talks of 2023

This year, SANS hosted 16 Summits with 209 talks. Here were the top-rated talks of the year.

Alison Kim

Subscribe