

STAR Webcast: Making sense of SolarWinds through the lens of MITRE ATT&CK(R)

Published: 2021-03-08 · Archived: 2026-04-05 14:42:10 UTC

Almost two months have passed since we first learned about the supply chain compromise of SolarWinds, and the community is still struggling to make sense of all of it. Enter MITRE ATT&CK. The speakers from the ATT&CK team will walk through how to use the framework to better organize what we know about the multitude of techniques from SolarWinds and related compromises. They will discuss both techniques that were previously known as well as those they recently added to ATT&CK in order to help attendees understand what actions they can take to better defend their networks. **DOWNLOAD SLIDES BY REGISTERING HERE:**

<https://www.sans.org/webcasts/star-we...> Speaker Bios
Katie Nickels [@likethecoins](#) is the Principal Intelligence Analyst for Red Canary. She has worked on cyber threat intelligence (CTI), network defense, and incident response for nearly a decade for the U.S. Department of Defense (DoD), MITRE, Raytheon, and ManTech. She also serves as an instructor for the SANS FOR578: Cyber Threat Intelligence course, enabling her to share her passion for CTI more broadly. Katie hosts SANS Threat Analysis Rundown (STAR), a popular monthly webcast series that discusses the current threat landscape and cyber threats. She is also the Program Manager at Cyberjutsu Girls Academy (CGA), a program for teenage girls that seeks to inspire exploration and learning in cybersecurity and STEM.
Jen Burns [@snarejen](#) is a Lead Cybersecurity Engineer at MITRE and the ATT&CK for Cloud Lead. She is also a red team lead and developer for ATT&CK Evaluations, combining her offensive security skills and software engineering background. Before switching to a career in tech, Jen worked as a percussionist and music educator throughout the country. She holds an MS in Information Security from Carnegie Mellon University, a BS in Computer Science from Oregon State University, and a BA in Music from the University of Texas at Arlington.
Adam Pennington [@_whatshisface](#) leads ATT&CK at The MITRE Corporation and collected much of the intelligence leveraged in creating ATT&CKs initial techniques. He has spent much of his 12 years with MITRE studying and preaching the use of deception for intelligence gathering. Prior to joining MITRE, Adam was a researcher at Carnegie Mellon's Parallel Data Lab and earned his BS and MS degrees in Computer Science and Electrical and Computer Engineering as well as the 2017 Alumni Service Award from Carnegie Mellon University. Adam has presented and published in a number of venues including FIRST CTI, USENIX Security, and ACM Transactions on Information and System Security.

STAR Webcasts with Katie Nickels

av SANS Digital Forensics and Incident Response

Source: <https://www.youtube.com/watch?v=LA-XE5Jy2kU>