A SANS 2021 Survey
MITRE ATT&CK® for ICS Framework

Author: Mark Bristow | Date: August 2021

The MITRE ATT&CK® framework is one of the most comprehensive sets of attack tactics and techniques in use in the wild, and this revolutionary framework has recently been customized for the ICS space. This survey and analysis will inform the SANS audience on the adoptions and experiences of the recently released ATT&CK for ICS framework.

ATT&CK for ICS, much like ATT&CK for Enterprise, provides a structured framework for articulating adversary behaviors, tactics and techniques. The framework takes into consideration the unique characteristics of adversaries attempting to impact critical infrastructure operations such as physical impact, process exploitation, and denying or degrading response and restoration efforts. The framework helps organizations apply useful mitigations to frustrate adversary-desired outcomes while enabling defenders to track behaviors and more rapidly identify anomalous behavior.

The seven key questions SANS will examine in this report are:

- How are companies leveraging ATT&CK for ICS?
- How does ATT&CK for ICS help companies smartly apply resources to defend their control networks?
- How has ATT&CK for ICS helped to bolster network defensive postures?
- How has ATT&CK for ICS helped defenders to better understand what adversaries are using in the wild?
- How is ATT&CK for ICS different from other frameworks?
- What are the important use cases for ATT&CK for ICS?
- How are companies leveraging both ATT&CK for Enterprise and ATT&CK for ICS together?

Why Sponsor the SANS 2021 MITRE ATT&CK® Survey

Lead Generation
300-lead guarantee with no cap.

Branding
Cobrand the survey results whitepaper and webcast with SANS, the global leader in cybersecurity training, certification and research.

Thought Leadership
Collaborate with our best SANS authors who are at the forefront of the ever-changing war on cybersecurity.

Author

Mark Bristow is the Director for the Hunt and Incident Response Team (HIRT) at Department of Homeland Secuirty's Cybersecurity and Infrastructure Security Agency (CISA) where he leverages his expertise in incident response, industrial control systems, network monitoring and defense to support national security interests. Before ICS-CERT was integrated into HIRT, Mark was the Chief of ICS-CERT incident response. In Mark's sixteen-year security career he has also worked for CSRA and Securicon where he supported a variety of private and public sector clients.

Sponsorship Inclusions

	Gold	Platinum
Survey SANS will run a 20–25 questions survey for a minimum of 6 weeks. Sponsors will be informed of survey respondent counts. A SANS Analyst will develop a whitepaper based on the survey results. Sponsors will receive a draft of the paper and survey results for review and a final, branded survey results whitepaper for their use.	✓	✓
Survey Results Presentation Webcast The survey results will be presented by the survey author. The webcast will be branded with sponsor's logo. Sponsors will receive the webcast recording for their own promotions. Webcasts are archived for one year after the webcast date. Registrations may still be processed for archive viewing of the webcast. 300-lead guarantee with no cap. *Webcast Date: TBA*	✓	✓
Associated Panel Discussion Webcast The survey author will host a panel discussion with up to three sponsors discussing the SANS 2021 MITRE ATT&CK® Survey results. The webcast will be promoted by SANS. Sponsors will receive the webcast recording for their own promotions. 100-lead guarantee with no cap. *Limited to three sponsors* *Webcast Date: TBA*		✓

Additional Sponsorship Opportunities

Associated Single-Sponsored Webcast	Sponsor your own webcast that aligns with the SANS 2021 MITRE ATT&CK® Survey. The webcast will be promoted by SANS. 200-lead guarantee with no cap and continued lead generation as a SANS archive webcast.
Associated Paper or Product Review	Publish a custom paper based on a segment of the report that is of interest to you or a product review that calls on the report as an entry point to the review. This associated paper includes a webcast.
Associated Video	Have a SANS expert interview a representative of your company. The sponsor will receive a branded video(s) of the interview. The video will also be available on the SANS website for lead generation. SANS will organize all logistics.

Lead Submission

Promotions
Survey: Promotion for taking the survey will be promoted for 5-6 weeks through a weekly email blast to SANS opt-in audience, SANS e-newsletters and social media.

Webcasts: Promotion of the survey results presentation webcast and the panel discussion webcast will begin one week after the survey closes. The webcast will be promoted via a weekly email blast to SANS opt-in audience, SANS e-newsletters and social media.

Lead Submission
The initial installment of leads from the webcast will be provided within two business days of the live webcast. Additional leads will be provided on a regular basis for the first three months following the webcast. After three months, leads will be provided as requested.

To see additional SANS Surveys and Analyst Papers, **click here**.