SANS SPONSORSHIP PROGRAMS

A SANS Whitepaper

A SANS 2020 Report | Measuring and Improving Cyber Defense Using the MITRE ATT&CK Framework

Author: John Hubbard | Date: July 2020

Multiple sessions at the 2019 SANS SOC summit highlighted that leading security operations teams have rapidly adopted the MITRE ATT&CK framework to help them identify and close gaps in cyber defense, increase the effectiveness of hunting processes, and decrease the time needed to efficiently respond to incidents.

Through the ATT&CK framework MITRE has generated a gold mine of information about the most important tactics and techniques used by attackers and how the blue team can detect and prevent these actions. Blocking atomic attack indicators such as domain names and IP addresses may work in the short term, but understanding the higher-level tactics in ATT&CK helps the blue team identify and anticipate attacker activity at a higher level of abstraction, slowing attackers down and giving defenders a fighting chance.

In this paper, SANS instructor and analyst John Hubbard will discuss the most important aspects of understanding and utilizing the ATT&CK framework including:

- MITRE ATT&CK matrix organization and the identified attacker post-exploitation tactics and techniques
- Understanding the details and layout of the ATT&CK matrix
- Basic security team requirements to enable effective use of ATT&CK
- Utilizing ATT&CK to identify and close gaps in organizational defenses
- Demonstrating objective improvement in blue team defensive capability when measuring against ATT&CK
- Avoiding common pitfalls and errors when using ATT&CK to measure cyber defense

Why Sponsor the SANS 2020 MITRE ATT&CK Framework Whitepaper

Lead Generation
300-lead guarantee with no cap.

Branding
Cobrand the 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.

About the Author

John Hubbard is a certified SANS instructor who authored the new SEC450: Blue Team Fundamentals: Security Operations and Analysis and co-authored SEC455: SIEM Design and Implementation. As an active security operations center lead and dedicated blue team member, he has firsthand knowledge of what it takes to defend an organization against advanced cyberattacks. John specializes in threat hunting, tactical SIEM design and optimization, and tailoring security operations to enable organizations to protect their most sensitive data.

Sponsorship Inclusions

Whitepaper	Sponsors will receive a draft of the paper for review and a final, branded whitepaper for their use.
Webcast	The whitepaper includes an associated webcast presented by the author. 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. ***Webcast Date: TBD August 2020***

Additional Sponsorship Opportunity

Associated Single-Sponsored Webcast	Sponsor your own webcast that aligns with the SANS 2020 MITRE ATT&CK framework whitepaper. Your webcast will be promoted by SANS. The sponsor will receive a minimum 200-lead guarantee with no cap and continued lead generation as a SANS archive webcast.

Lead Submission & Promotions

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 upon request.

Promotions

Whitepaper: Promotion of the SANS 2020 MITRE ATT&CK framework whitepaper will begin 6 weeks prior to the webcast.

Webcast: Promotion of the webcast will begin once the webcast has been scheduled. The webcast will be promoted via a weekly email blast to SANS opt-in audience, SANS e-newsletters and social media.

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