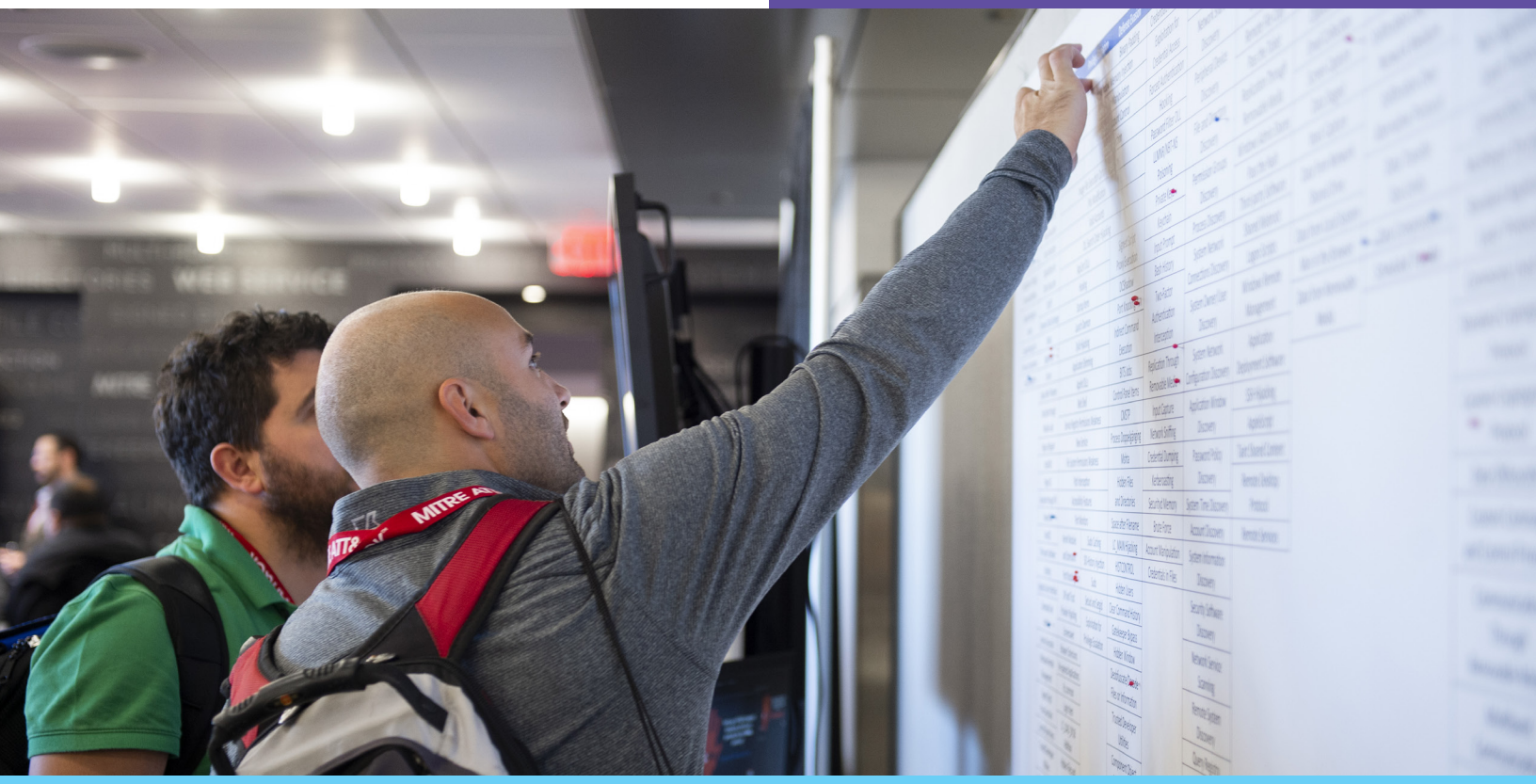
Shifting the Playing Field in Favor of Cyber Defenders

MITRE ENGENUITY™ | Center for Threat Informed Defense



Threat-informed defense is the systematic application of a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber attacks.

The Center for Threat-Informed Defense™ is a privately funded R&D organization focused on advancing the state of the art and the state of the practice in threat-informed defense. Together with the global private sector, the Center conducts applied research and advanced development to improve cyber defense at scale. And, since the Center operates for the public good, we freely share our research for the benefit of all.

Building on the foundation of MITRE ATT&CK

As a knowledge base for understanding adversary behavior and tradecraft, the MITRE ATT&CK™ framework is a critical foundation for threat-informed defense. Sophisticated security teams around the world use ATT&CK in their enterprise security operations and many cybersecurity vendors leverage ATT&CK in their products and services.

As a result, there is an ever-louder call for MITRE to expand upon ATT&CK and ensure that it remains open, free, and keeps pace with evolving threats. The Center brings together this robust and rapidly growing community to conduct research in support of ATT&CK and accelerate innovation in threat-informed defense.

Initial R&D Focus Areas

Advanced Global Understanding of Adversary Tradecraft

EXAMPLES

- Expand ATT&CK into new technology domains like cloud and ICS
- Identify a critical set of threat actor groups and systemically improve our ability to protect, detect, or respond to behaviors used by both groups

Measure Evolving Adversary Behavior

EXAMPLES

- Collect, analyze, and publish ATT&CK technique sightings
- Establish a most wanted list of adversary techniques

Enable Continuous Measurement of Our Defenses

EXAMPLES

- Mature and transition MITRE's current ATT&CK-based SOC assessment methodology to organizations who can deliver it at scale
- Develop, share, and automate adversary emulation playbooks

R&D results will be freely available to maximize public impact

Membership that leverages the diverse cyber community

The cyber challenges we face are bigger than any single organization, sector, or country. As a result, the Center is committed to bring together sophisticated and innovative security teams from leading organizations around the world, including:

- Global end-user and critical infrastructure companies
- Leading technology companies
- Cybersecurity-related non-profits including ISACs and ISAOs

Accelerating R&D in threat-informed defense

Center members are committed to relentlessly advance the ability to protect, detect, and respond to advanced adversaries through collaborative R&D. The Center will dramatically expand the global understanding of adversary behaviors, creating a scalable approach for identifying, conducting, and sharing public interest research.

MITRE Engenuity

Created by MITRE to respond to fast evolving public challenges, MITRE Engenuity is a foundation for public good. We work to drive impact on challenges that threaten a safer world.

MITRE ENGENUITY™
A Foundation for Public Good

For more information:
Richard Struse, Director
Center for Threat-Informed Defense
rstruse@mitre-engenuity.org