What's Next from the Center for Threat-Informed Defense

Suneel Sundar, Director Research & Development

MITRE ENGENUITY | Center for Threat Informed Defense

Who is this guy?

Lead the R&D program in the Center for Threat-Informed Defense. Created and led MITRE early-career incubator Cyber New Professionals.

Founding member of CTI teams @ U.S. energy utility and Visa

Designed cryptographic algorithms @ NSA

Certified Iyengar yoga teacher since 2009

Suneel Sundar

Insider Threat TTP Knowledge Base

- 47 techniques and 29 sub-techniques
- 36 unique mitigations for these documented insider behaviors
- Observable Human Indicators - objective, quantifiable attributes of insiders that complement the cyber observables

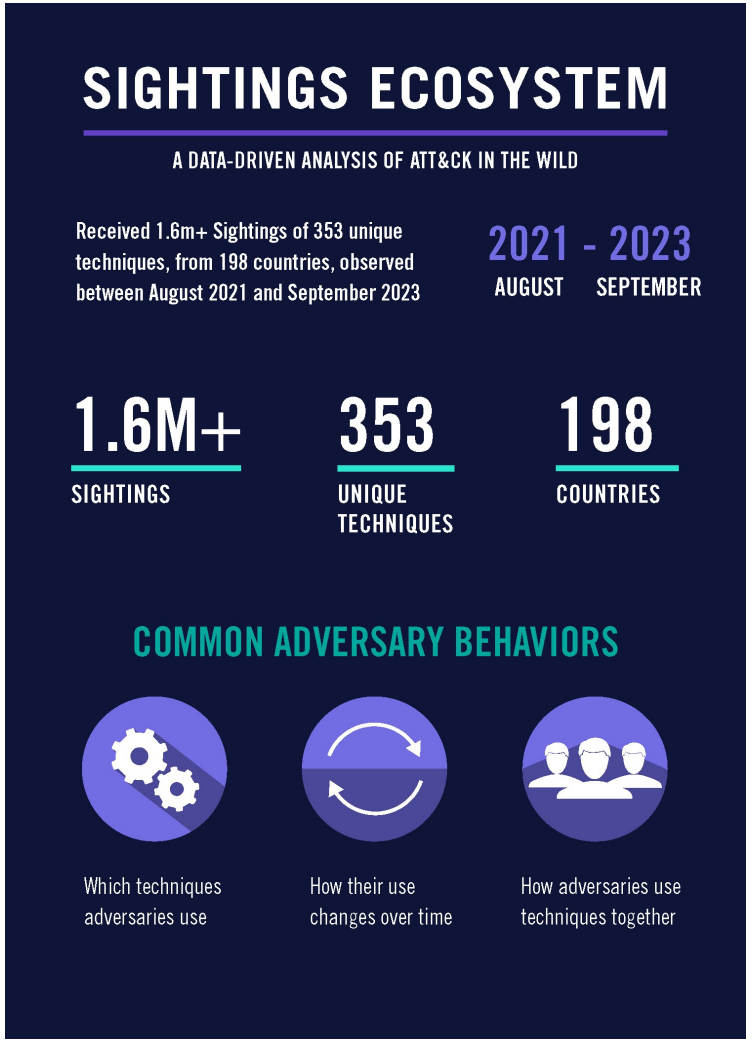
Cyber defenders across organizations will identify insider threat activity on IT systems and limit the damage

MITRE ENGENUITY | Center for Threat Informed Defense

Sightings Ecosystem

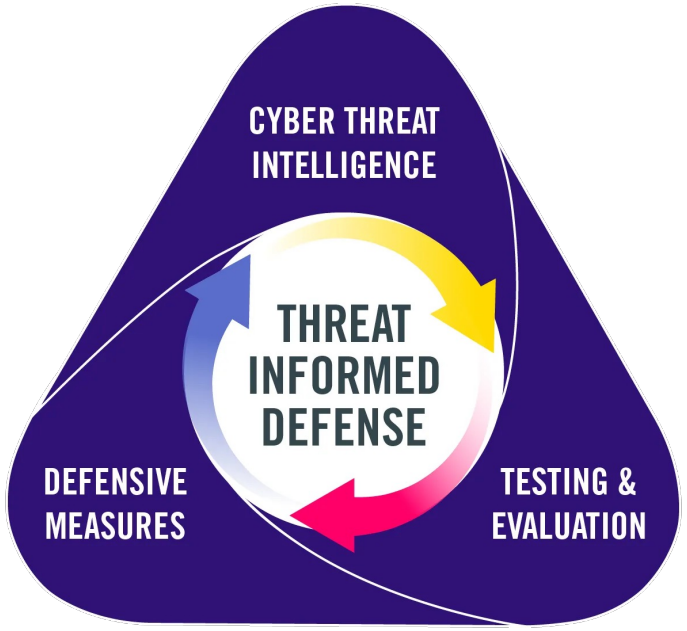
Voluntarily contributed observations of specific adversary TTPs (“sightings”) are anonymized and aggregated to produce insights into the most commonly used attacker techniques.

Threat activity across organizational, platform, vendor, and geographical boundaries



MITRE ENGENUITY | Center for Threat Informed Defense

Measure Maximize Mature Threat Informed Defense



M3TID Components

CYBER-THREAT INTELLIGENCE (CTI)	DEFENSIVE MEASURES (DM)	TESTING AND EVALUATION (T&E)
1. Depth of Threat Data	1. Foundational Security	1. Type of Testing
2. Breadth of Threat Data	2. Data Collection	2. Frequency of Testing
3. Relevance of Threat Data	3. Detection Engineering	3. Test Planning
4. Utilization of Threat Data	4. Incident Response	4. Test Execution
5. Dissemination of Threat Reporting	5. Deception Operations	5. Test Results

Actionable definition of threat-informed defense and its associated key activities, and a formalized approach to measure your threat-informed defense

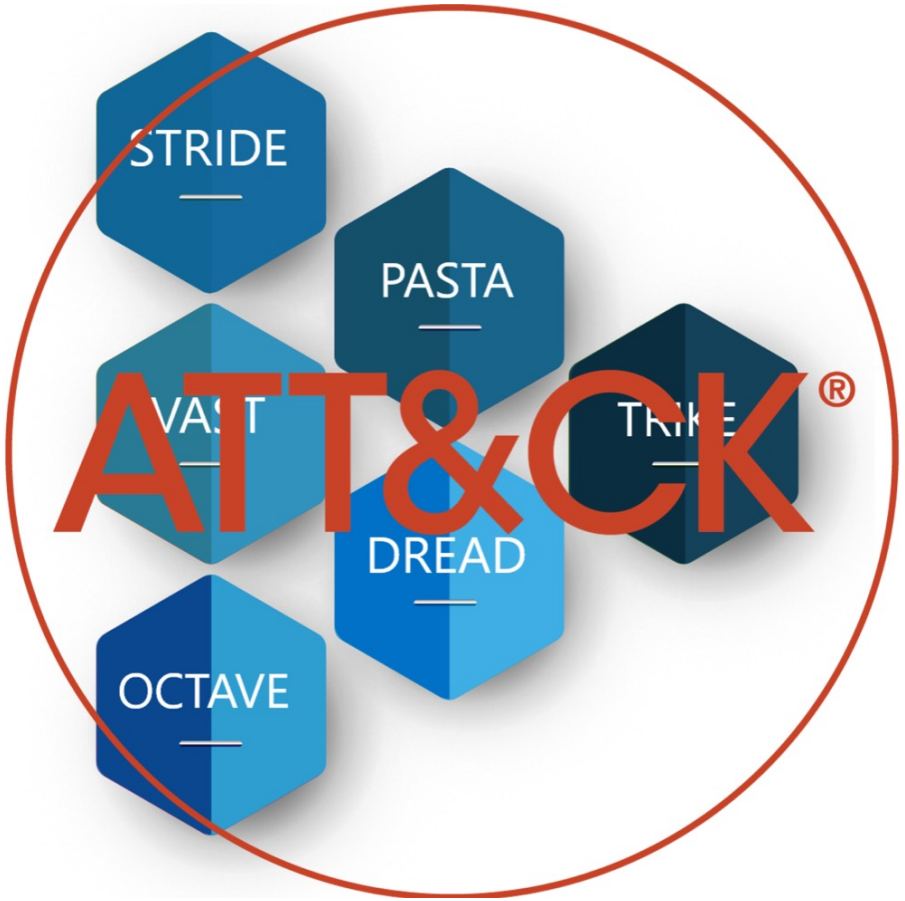
MITRE ENGENUITY | Center for Threat Informed Defense

And there is plenty more to come!

Threat Modeling with ATT&CK

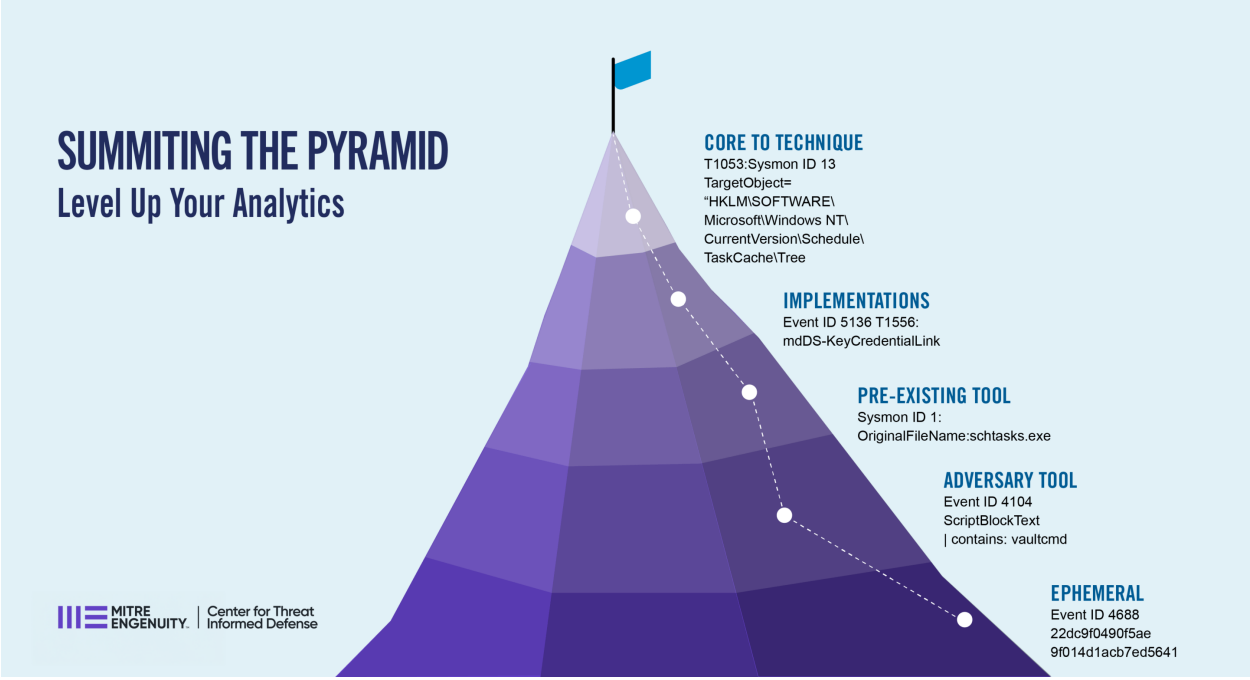
- Our partners across the security organization request guidance to to **identify relevant, impactful threat scenarios**.
- Develop an ATT&CK-compatible solution to enumerate threat scenarios for practitioners who are **developing systems or applications**.

Use the ATT&CK framework to prioritize relevant threat scenarios



Summiting the Pyramid V2

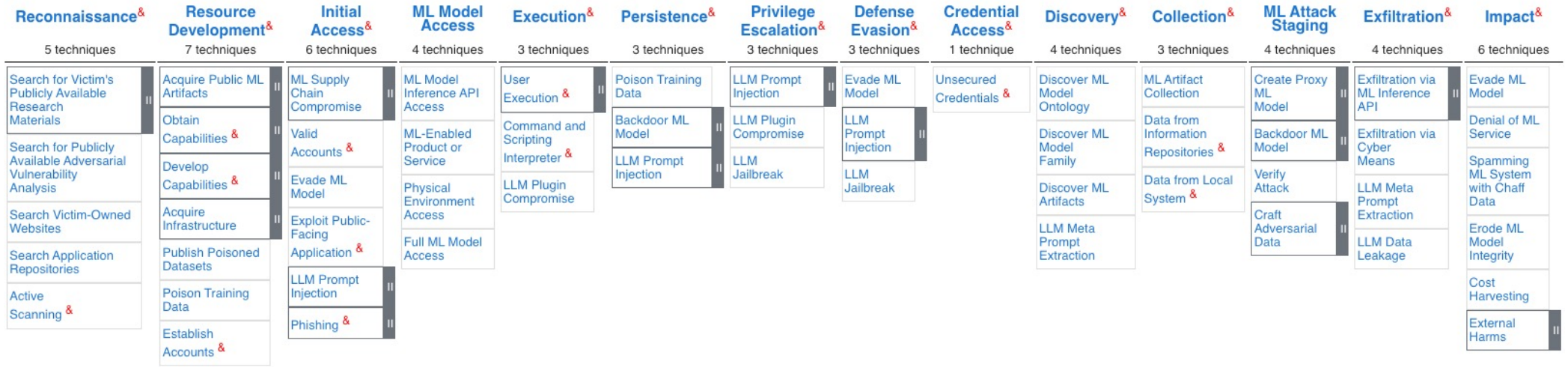
1. More **precise, less false-positive** prone analytics without sacrificing robustness.
2. Expand robustness to **network-focused data sources**.
3. Catalog and **score known data sources** for automated scoring.
4. Expand the number of **analytic and event observables**.



Unevadable analytics

MITRE ENGENUITY | Center for Threat Informed Defense

Secure AI



- Document new case studies that address the vulnerabilities of systems that incorporate **generative AI**.
- Keep the **ATLAS TTPs and ATT&CK TTPs** in sync.
- Strategies to **mitigate** relevant (high likelihood, high impact) threats to AI-enabled systems.
- Tools and playbooks to **emulate** threats to AI-enabled systems.

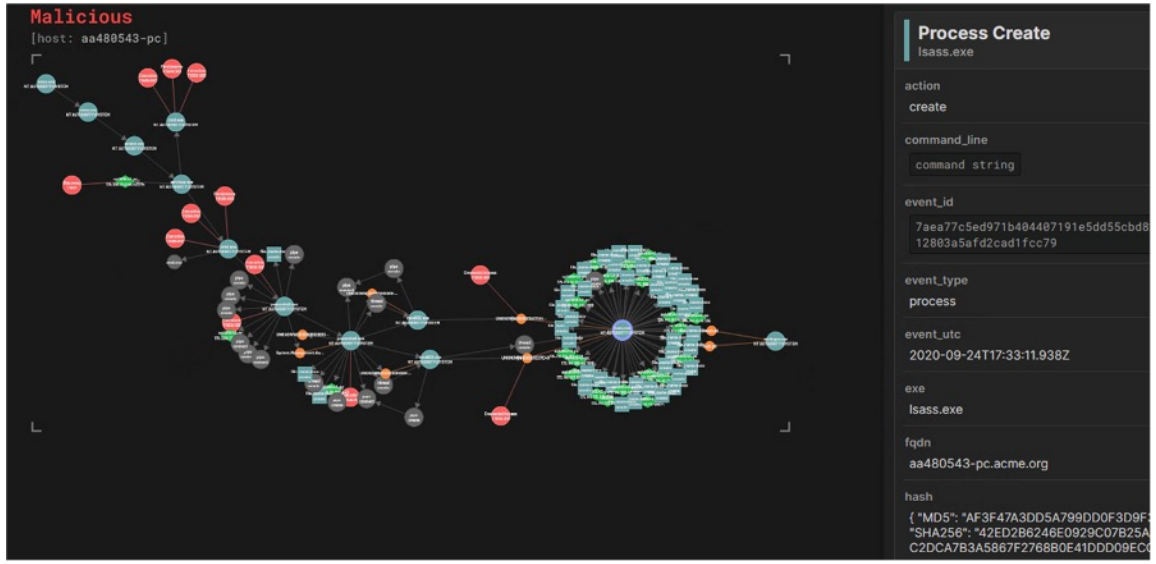
real-world threats through incident sharing

MITRE ENGENUITY | Center for Threat Informed Defense

Technique Inference Engine (TIE)

- Create a model usable by both human analysts and automation platforms to **investigate attack chains**.
- Given two or more observed techniques in sequence, TIE will **recommend a likely next technique** or previous technique.

Guide analysts, threat hunters, red teamers, investigators, and threat modelers from what technique is seen to what is not-yet-seen.



Security Capability Mappings

identify the potential **occurrence** of a (sub-) technique,

limit the **impact** of a (sub-)technique, or

provide **actions** to take for detected (sub-) technique.

Next up:

- *Prioritize Known Exploited Vulnerabilities* - bridge threat and vulnerability management by connecting **CVEs that are actively exploited** to the **impact of exploitation**
- Hardware-Enabled Defense

The defenses you need for the threats that you face

What About You?

Use this work

Share this work

Improve this work

Create more work