



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

Suneel Sundar, Director Research & Development

# Who is this guy?

**MITRE**

**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

TA0043 Reconnaissance 2 techniques	TA0042 Resource Development 3 techniques	TA0001 Initial Access 3 techniques	TA0002 Execution 1 techniques	TA0003 Persistence 5 techniques	TA0004 Privilege Escalation 2 techniques	TA0005 Defense Evasion 6 techniques	TA0006 Credential Access 2 techniques	TA0007 Discovery 3 techniques	TA0008 Lateral Movement 2 techniques	TA0009 Collection 8 techniques	TA0011 Command and Control 1 techniques	TA0010 Exfiltration 5 techniques	TA0040 Impact 6 techniques
T1595 Active Scanning (1/1) T1595.001 Scanning IP Blocks T1589 Gather Victim Identity Information (1/1)	T1650 Acquire Access T1585 Establish Accounts (1/1) T1588 Obtain Capabilities (1/1) T1588.002 Tool	T1133 External Remote Services T1199 Trusted Relationship T1078 Valid Accounts (2/2) T1078.004 Cloud Accounts T1078.002 Domain Accounts	T1106 Native API	T1098 Account Manipulation (1/1) T1098.005 Device Registration T1136 Create Account (1/1) T1136.001 Local Account T1546 Event Triggered Execution (1/1) T1546.003 Windows Management Instrumentation Event Subscription T1133 External Remote Services T1078 Valid Accounts (2/2) T1078.004 Cloud Accounts T1078.002 Domain Accounts	T1548 Abuse Elevation Control Mechanism (1/1) T1546 Event Triggered Execution (1/1) T1546.003 Windows Management Instrumentation Event Subscription	T1548 Abuse Elevation Control Mechanism (1/1) T1562 Impair Defenses (2/2) T1562.001 Disable or Modify Tools T1562.011 Spoof Security Alerting T1070 Indicator Removal (2/2) T1070.001 Clear Windows Event Logs T1070.004 File Deletion T1036 Masquerading (1/1) T1027 Obfuscated Files or Information (1/1) T1078 Valid Accounts (3/3) T1078.004 Cloud Accounts T1078.001 Default Accounts T1078.002 Domain Accounts	T1555 Credentials from Password Stores (1/1) T1555.005 Password Managers T1552 Unsecured Credentials (1/1) T1552.008 Chat Messages	T1046 Network Service Discovery T1135 Network Share Discovery T1016 System Network Configuration Discovery (1/1) T1016.001 Internet Connection Discovery	T1210 Exploitation of Remote Services T1021 Remote Services (2/2) T1021.001 Remote Desktop Protocol T1021.004 SSH	T1560 Archive Collected Data (1/1) T1560.001 Archive via Utility T1119 Automated Collection T1213 Data from Information Repositories (2/2) T1213.003 Code Repositories T1213.002 Sharepoint T1005 Data from Local System T1039 Data from Network Shared Drive T1074 Data Staged (1/1) T1074.001 Local Data Staging T1114 Email Collection (1/1) T1114.001 Local Email Collection T1113 Screen Capture	T1219 Remote Access Software	T1048 Exfiltration Over Alternative Protocol (2/2) T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol T1011 Exfiltration Over Other Network Medium (1/1) T1011.001 Exfiltration Over Bluetooth T1052 Exfiltration Over Physical Medium (1/1) T1052.001 Exfiltration over USB T1567 Exfiltration Over Web Service (1/1) T1567.002 Exfiltration to Cloud Storage T1537 Transfer Data to Cloud Account	T1485 Data Destruction T1565 Data Manipulation (1/1) T1565.001 Stored Data Manipulation T1561 Disk Wipe (1/1) T1561.001 Disk Content Wipe T1657 Financial Theft T1496 Resource Hijacking T1529 System Shutdown/Reboot

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

# 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**

## SIGHTINGS ECOSYSTEM

A DATA-DRIVEN ANALYSIS OF ATT&CK IN THE WILD

Received 1.6m+ Sightings of 353 unique techniques, from 198 countries, observed between August 2021 and September 2023

**2021 - 2023**  
AUGUST SEPTEMBER

**1.6M+**  
SIGHTINGS

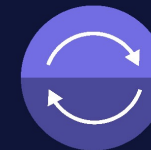
**353**  
UNIQUE  
TECHNIQUES

**198**  
COUNTRIES

### COMMON ADVERSARY BEHAVIORS



Which techniques adversaries use



How their use changes over time



How adversaries use techniques together



# 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**



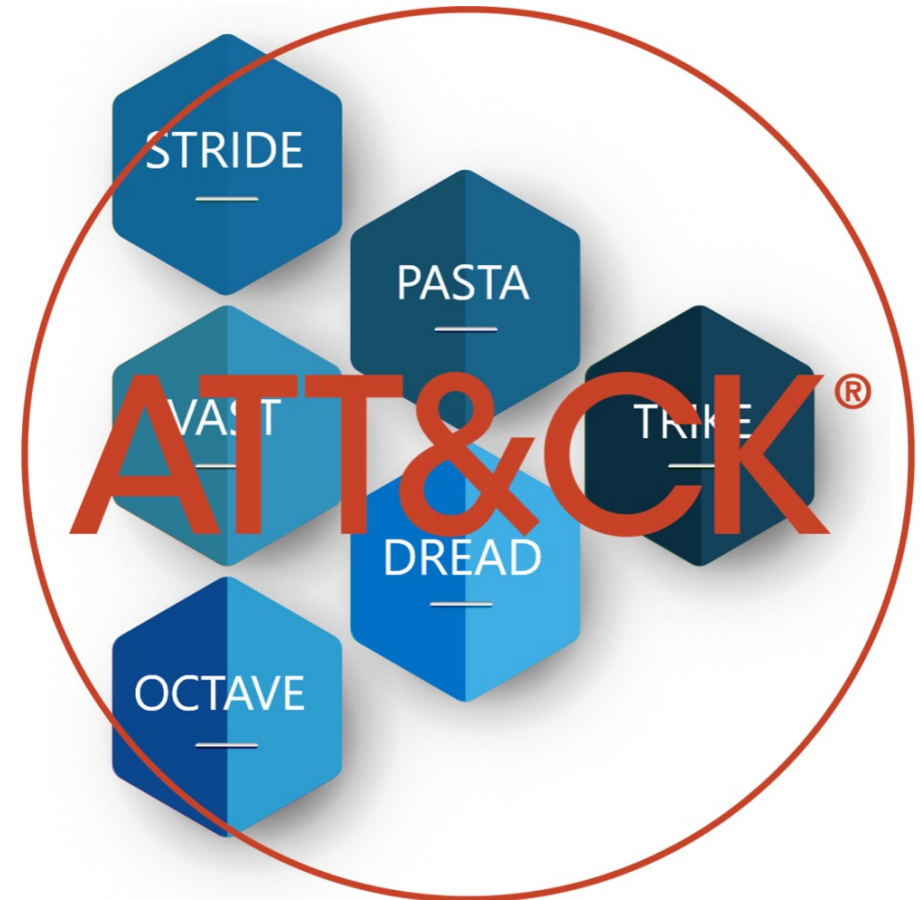
**And there is plenty more to come!**



# Threat Modeling with ATT&CK

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

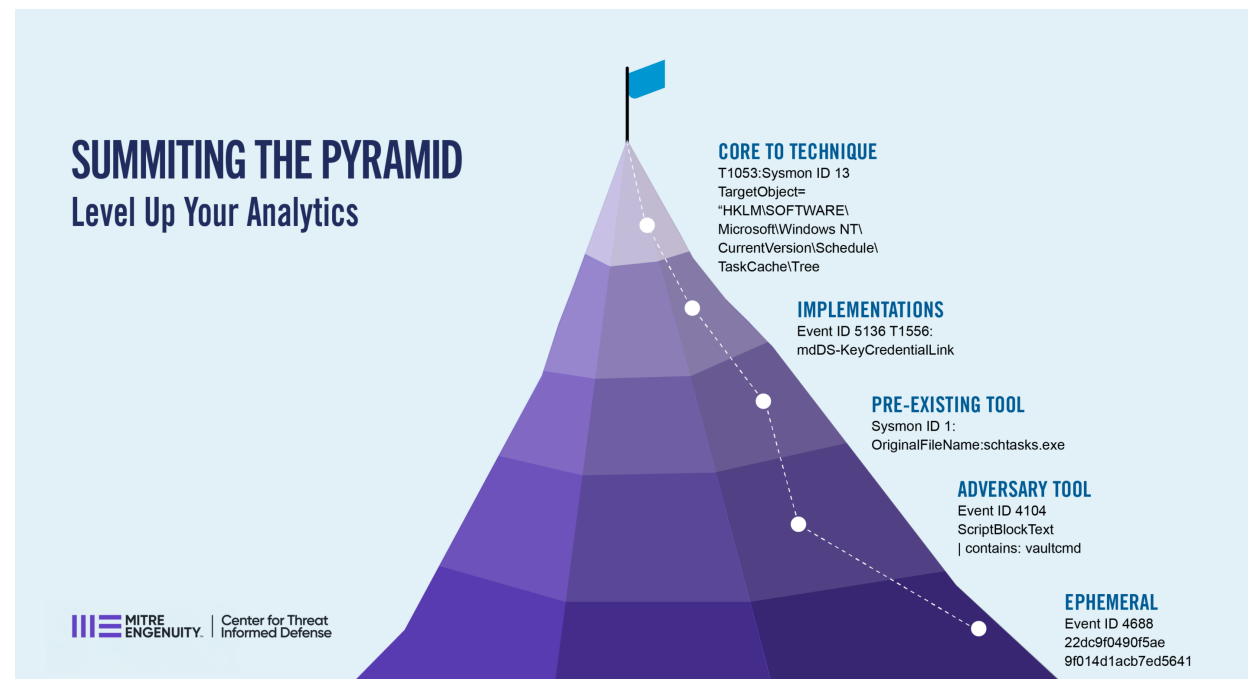
**Use the ATT&CK framework to prioritize relevant threat scenarios**



# 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**





# Secure AI

Reconnaissance&	Resource Development&	Initial Access&	ML Model Access	Execution&	Persistence&	Privilege Escalation&	Defense Evasion&	Credential Access&	Discovery&	Collection&	ML Attack Staging	Exfiltration&	Impact&
5 techniques	7 techniques	6 techniques	4 techniques	3 techniques	3 techniques	3 techniques	3 techniques	1 technique	4 techniques	3 techniques	4 techniques	4 techniques	6 techniques
Search for Victim's Publicly Available Research Materials	Acquire Public ML Artifacts	ML Supply Chain Compromise	ML Model Inference API Access	User Execution &	Poison Training Data	LLM Prompt Injection	Evade ML Model	Unsecured Credentials &	Discover ML Model Ontology	ML Artifact Collection	Create Proxy ML Model	Exfiltration via ML Inference API	Evade ML Model
Search for Publicly Available Adversarial Vulnerability Analysis	Obtain Capabilities &	Valid Accounts &	ML-Enabled Product or Service	Command and Scripting Interpreter &	Backdoor ML Model	LLM Plugin Compromise	LLM Prompt Injection		Discover ML Model Family	Data from Information Repositories &	Backdoor ML Model	Exfiltration via Cyber Means	Denial of ML Service
Search Victim-Owned Websites	Develop Capabilities &	Evade ML Model	Physical Environment Access	LLM Plugin Compromise	LLM Prompt Injection	LLM Jailbreak	LLM Jailbreak		Discover ML Artifacts	Data from Local System &	Verify Attack	LLM Meta Prompt Extraction	Spamming ML System with Chaff Data
Search Application Repositories	Acquire Infrastructure	Exploit Public-Facing Application &	Full ML Model Access						LLM Meta Prompt Extraction		Craft Adversarial Data	LLM Data Leakage	Erode ML Model Integrity
Active Scanning &	Publish Poisoned Datasets	LLM Prompt Injection											Cost Harvesting
	Poison Training Data	Phishing &											External Harms
	Establish Accounts &												

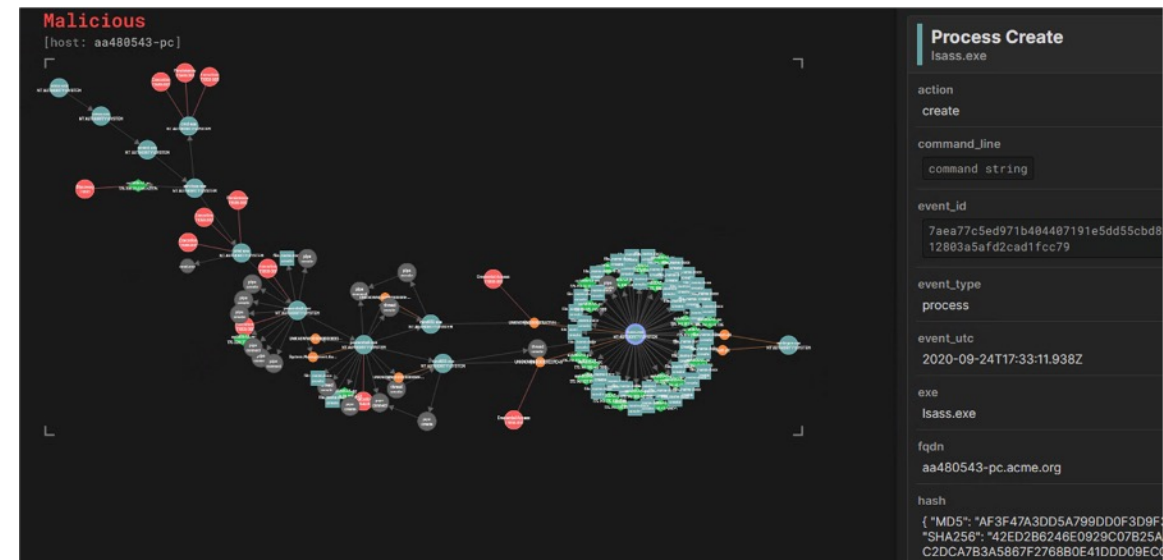
- Document new case studies that address the vulnerabilities of systems that incorporate **generative AI**.
- Keep the **ATLAS TTPs** and **ATT&CK TTPs** in sync.
- Strategies to **mitigate** relevant (high likelihood, high impact) threats to AI-enabled systems.
- Tools and playbooks to **emulate** threats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

real-world threats through incident sharing

# 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**