Secure IT - NYC
July 11, 2024

Measure, maximize, and mature your threat-informed defense

Jon Baker
Director, Center for Threat-Informed Defense

MITRE ENGENUITY | Center for Threat Informed Defense

About me

Co-founder & Director of the Center for Threat-Informed Defense

Formerly responsible MITRE's Cyber Threat Intel and Adversary Emulation work program

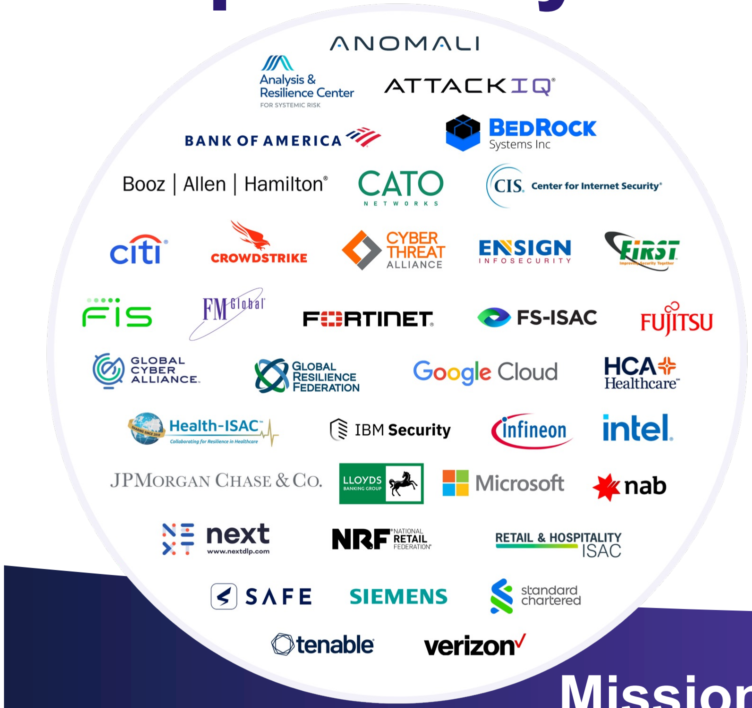
Led MITRE's security automation work – CVE, OVAL, CPE, MAEC, CAPEC…

Started out as a software engineer

Working in the public interest to advance cybersecurity for all

The Center for Threat-Informed Defense conducts collaborative R&D projects that

improve cyber defense at scale



+ MITRE

SOLVING PROBLEMS FOR A SAFER WORLD™

Membership is:

✓ Highly-sophisticated
✓ Global & cross-sector
✓ Non-governmental
✓ Committed to collaborative R&D in the public interest

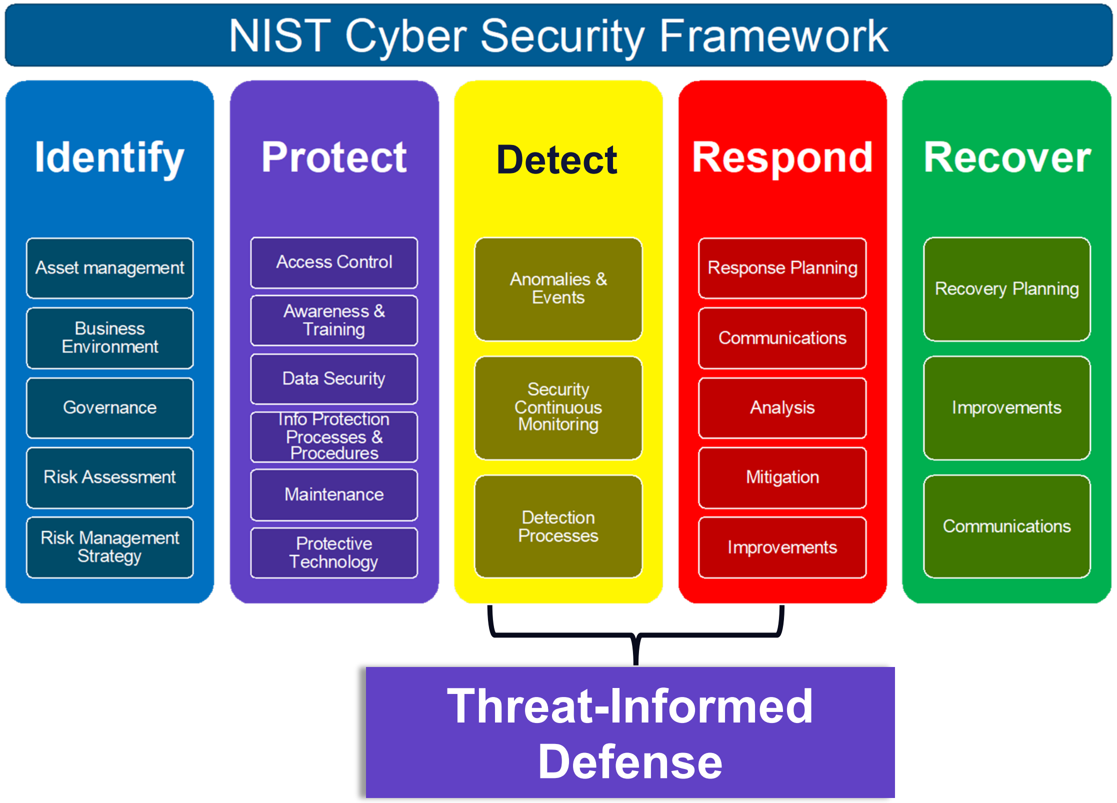
Mission: Advance the state of the art and the state of the practice in threat-informed defense globally.

MITRE ENGENUITY | Center for Threat Informed Defense

What is Threat-Informed Defense?

"The systematic application of a deep understanding of adversary tradecraft and technology to improve defenses."

Where does it fit?

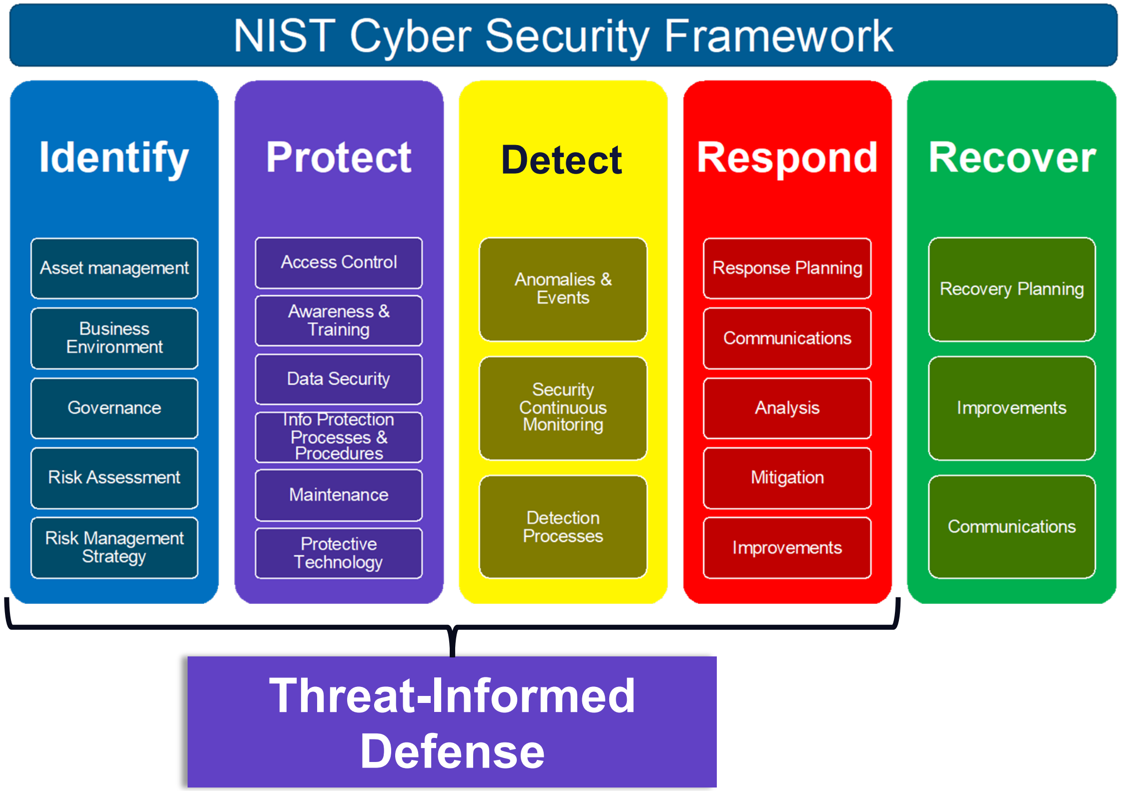


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Threat-Informed Defense

Where does it fit?

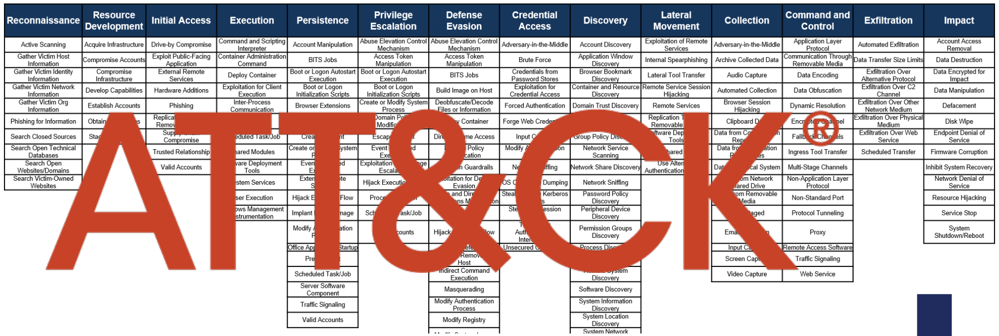


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Threat-Informed Defense

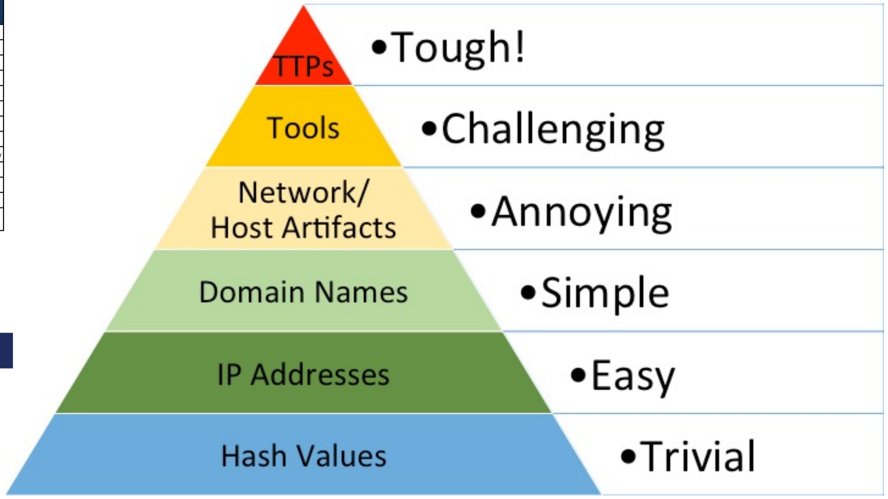
Increase the Cost for the Adversary



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Container and Resource Discovery	Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	[illegible]	[illegible]	Domain Policy Modification	Deploy Container	Forge Web Credentials	[illegible]	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Direct Volume Access	Input Capture	Group Policy Discovery	Software Deployment Tools	Data from Configuration Repository	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Technical Databases		Trusted Relationship	Shared Modules	Create or Modify System Process	Event Triggered Execution	Domain Policy Modification	Modify Authentication Process	Network Service Scanning	Taint Shared Content	Data from Information Repositories	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts	Software Deployment Tools	Event Triggered Execution	Exploitation for Privilege Escalation	Execution Guardrails	Network Sniffing	Network Share Discovery	Use Alternate Authentication Material	Data from Local System	Multi-Stage Channels		Inhibit System Recovery
Search Victim-Owned Websites			System Services	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping	Network Sniffing		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service
			User Execution	Hijack Execution Flow	Process Injection	File and Directory Permissions Modification	Steal or Forge Kerberos Tickets	Password Policy Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job	[illegible]	Steal Web Session Cookie	Peripheral Device Discovery		Data Staged	Protocol Tunneling		Service Stop
				Modify Authentication Process	Valid Accounts	Hijack Execution Flow	Two-Factor Authentication Interception	Permission Groups Discovery		Email Collection	Proxy		System Shutdown/Reboot
				Office Application Startup		Impair Defenses	Unsecured Credentials	Process Discovery		Input Capture	Remote Access Software		
				Pre-OS Boot		[illegible]		[illegible]		Screen Capture	Traffic Signaling		
				Scheduled Task/Job		Indirect Command Execution		Remote System Discovery		Video Capture	Web Service		
				Server Software Component		Masquerading		Software Discovery					
				Traffic Signaling		Modify Authentication Process		System Information Discovery					
				Valid Accounts		Modify Registry		System Location Discovery					
						[illegible]		System Network					

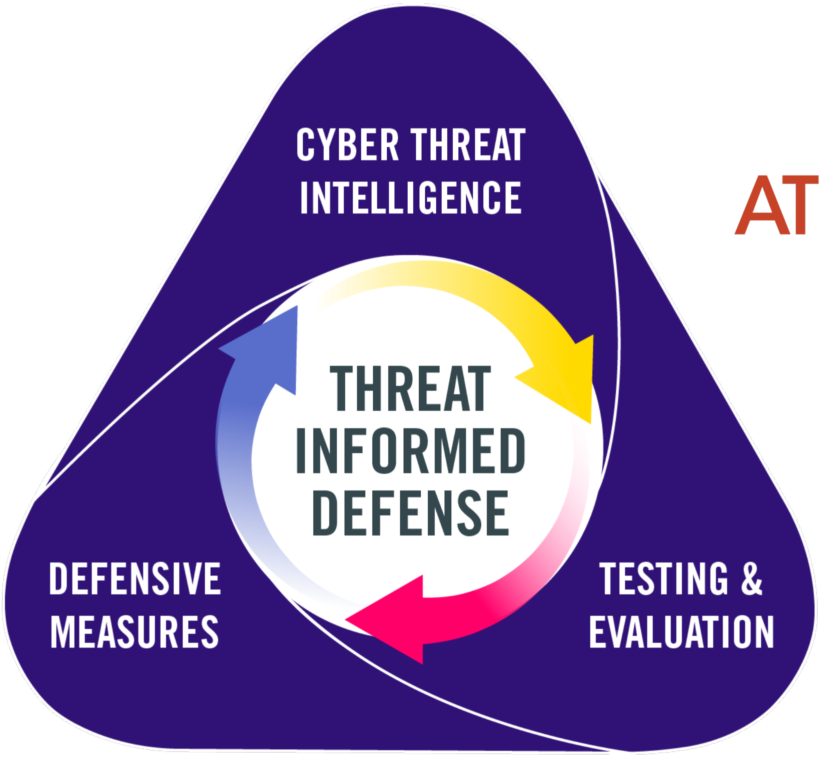
A community-driven knowledgebase of adversary TTPs

+



* Pyramid of Pain by David Bianco http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Threat-Informed Defense Cycle



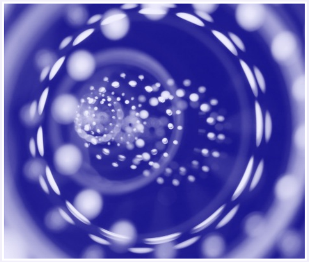
ATT&CK® is at the core of threat-informed defense

Threat-informed defense is a continuous process.

As our defenses improve, our environments change, and adversaries evolve, the cycle continues.

Threat-Informed Defense is…

MITRE ENGENUITY | Center for Threat Informed Defense



A lens, through which, you can understand your security posture

A way to think about your security architecture and operations

A way to prioritize your security strategy and investments

A way of assessing the effectiveness of your security investments

Thinking like an attacker

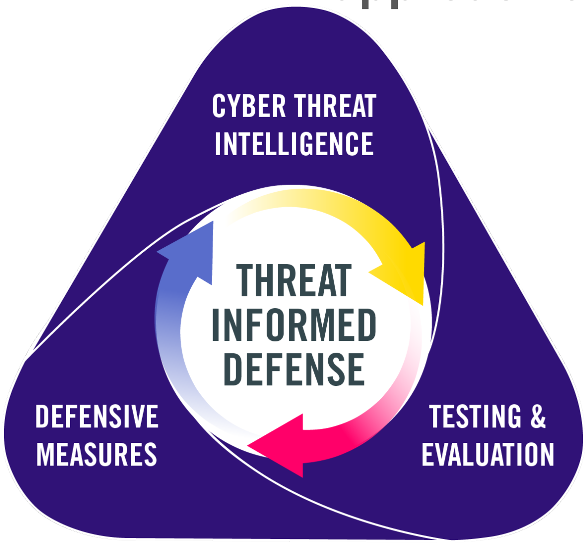
Make threat-informed defense actionable

How do I apply threat-informed defense?
What is good enough?
Where should I focus next?
Are we getting "better"?

MITRE ENGENUITY | Center for Threat Informed Defense

M3TID makes threat-informed defense actionable

Measure, Maximize, and Mature Threat-Informed Defense (M3TID) **leverages threat understanding to improve a security program** with an **actionable definition** of threat-informed defense, and a **formalized approach to measure** your threat-informed defense.



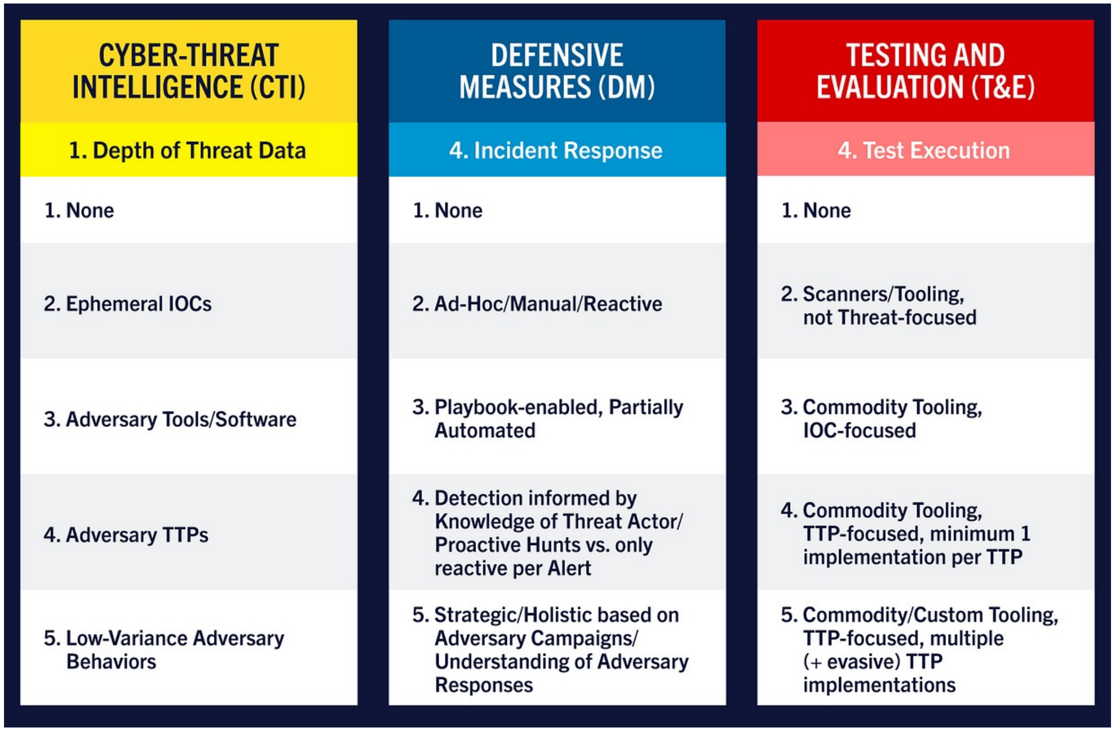
M3TID Components

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

M3TID expands the 3 dimensions of TID with 5 key components each.

MITRE ENGENUITY | Center for Threat Informed Defense

Define Maturity Levels



CYBER-THREAT INTELLIGENCE (CTI)	DEFENSIVE MEASURES (DM)	TESTING AND EVALUATION (T&E)
1. Depth of Threat Data	4. Incident Response	4. Test Execution
1. None	1. None	1. None
2. Ephemeral IOCs	2. Ad-Hoc/Manual/Reactive	2. Scanners/Tooling, not Threat-focused
3. Adversary Tools/Software	3. Playbook-enabled, Partially Automated	3. Commodity Tooling, IOC-focused
4. Adversary TTPs	4. Detection informed by Knowledge of Threat Actor/ Proactive Hunts vs. only reactive per Alert	4. Commodity Tooling, TTP-focused, minimum 1 implementation per TTP
5. Low-Variance Adversary Behaviors	5. Strategic/Holistic based on Adversary Campaigns/ Understanding of Adversary Responses	5. Commodity/Custom Tooling, TTP-focused, multiple (+ evasive) TTP implementations

For each component, there are 5 maturity levels

Measuring CTI Maturity

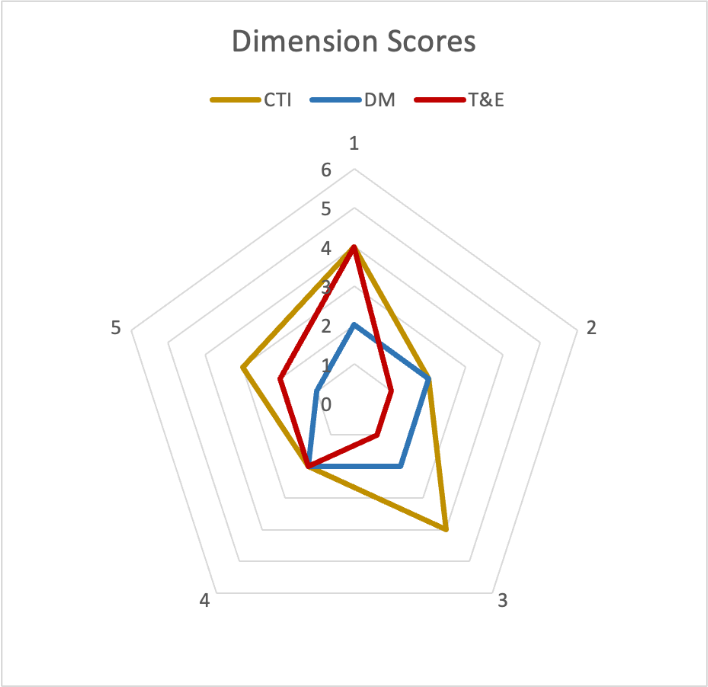
Cyber Threat Intelligence - Best Practices and Maturity Levels

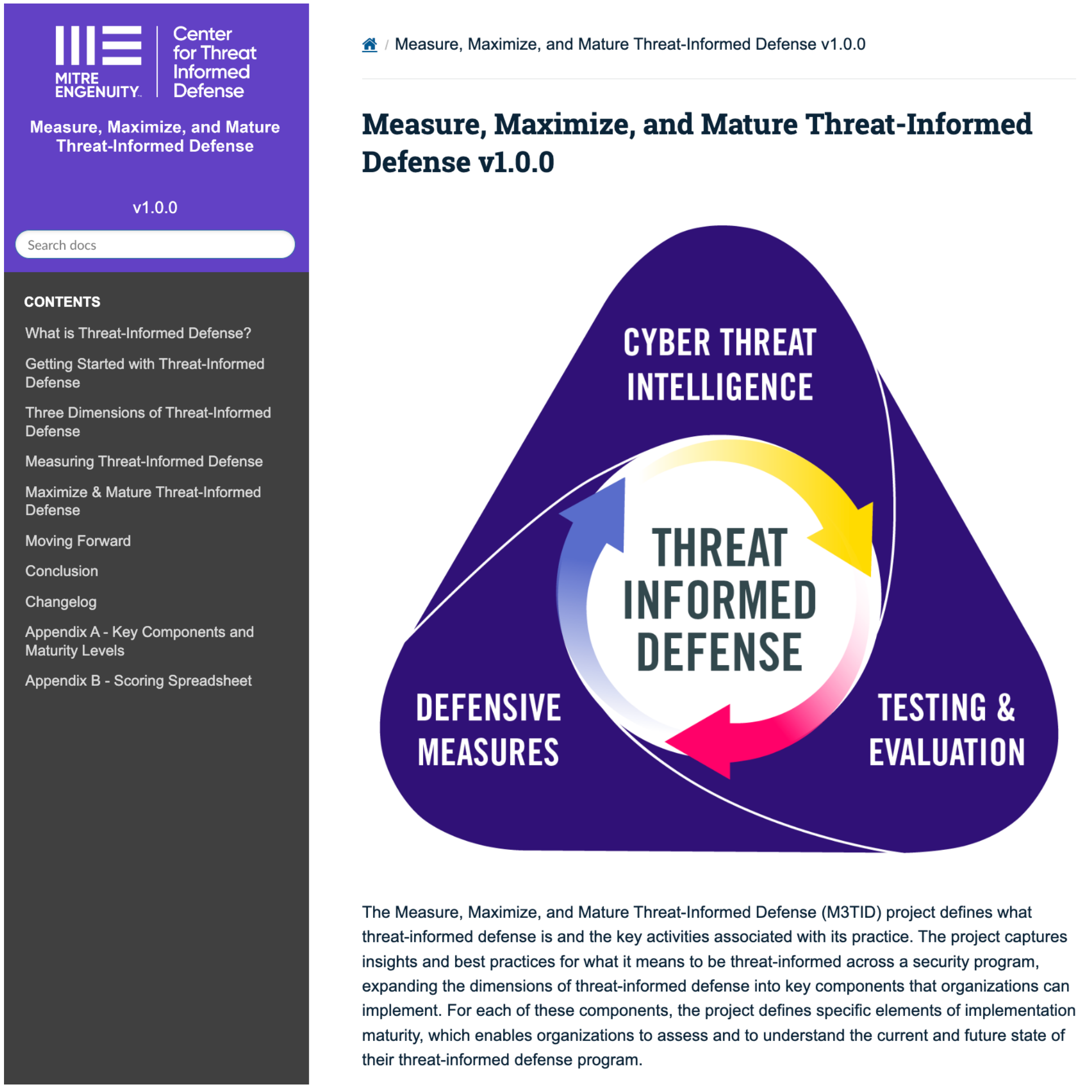
How well do you understand the Adversaries that may target your organization

		Components									
		I.1 - Depth of Threat Data		**I.2 - Breadth of Threat Information**		**I.3 - Relevance of Threat Data**		**I.4 - Utilization of Threat**		**I.5 - Dissemination of Threat Reporting**	
	Score Value	*What level of information (roughly relative to the Pyramid of Pain) is being used to track adversaries. [1]*	**Input Here**	*Complementary to the depth component score, roughly how many relevant Techniques are understood at that level of depth.*	**Input Here**	*Where is the threat information coming from and how timely is it*	**Input Here**	*How is the threat information being used by an organization*	**Input Here**	*What threat information is passed along within an organization [4]*	**Input Here**
Level 1	0	None	no	None	no	None	no	None	no	None	no
Level 2	1	Ephemeral IOCs: hashes, IPs, domains: data sources an adversary can change easily	yes	Single Technique	yes	Generic reports or freely available reporting	yes	Lightly / occasionally read	yes	Tactical reporting with highly perishable information (IOCs)	yes
Level 3	1	Tools / Software used by adversaries: tools or software which can be swapped or modified by an adversary to evade detection	yes	Multiple Techniques	yes	Internal reports	yes	Regularly ingested for analysis	yes	Tactical reporting focused on adversary behavior (TTPs)	no
Level 4	2	Techniques and Tactics used by adversaries: the techniques and behaviors that are harder to change for an adversary	yes	All top-priority Techniques relevant to the organization	no	Recent, in-depth reporting (often requires a subscription)	yes	Analyzed automatically [3] and/or by trained analysts	no	Operational reporting on pertinent security trends	yes
Level 5	2	Low-variance adversary behaviors and associated observables: specific actions most implementations of a technique must use so it is very difficult for an adversary to change or avoid	no	All Techniques relevant to the organization [2]	no	Customized briefings	no	Contextualized in disseminated reports for other internal stakeholders to operationalize	no	Strategic reporting on business impacts of security trends	no
CTI Total	3.0	Depth of Threat Data Total Score:	4	Breadth of Threat Information Total Score:	2	Relevance of Threat Data Total Score:	4	Utilization of Threat Information Total Score:	2	Dissemination of Threat Reporting Total Score:	3

Maturing Your Program

TID Dimension / Practice	*L2*	*L3*	*L4*	*L5*	*Maturity Score*
Overall TID Maturity (weighted)					**37%**
Cyber Threat Intelligence Maturity					3
I.1 - Depth of Threat Data	x	x	x		4
I.2 - Breadth of Threat Information	x	x			2
I.3 - Relevance of Threat Data	x	x	x		4
I.4 - Utilization of Threat Information	x	x			2
I.5 - Dissemination of Threat Reporting	x		x		3
Defensive Measures Maturity					1.8
D.1 - Foundational security	x	x			2
D.2 - Data Collection	x	x			2
D.3 - Detection Engineering	x	x			2
D.4 - Incident Response	x	x			2
D.5 - Deception Operations	x				1
Test & Evaluation Maturity					2
T.1 - Type of Testing	x	x		x	4
T.2 - Frequency of Testing	x				1
T.3 - Test Planning	x				1
T.4 - Test Execution	x	x			2
T.5 - Test Results	x	x			2




Center for Threat Informed Defense
MITRE ENGENUITY
Measure, Maximize, and Mature Threat-Informed Defense
v1.0.0
Search docs
CONTENTS
What is Threat-Informed Defense?
Getting Started with Threat-Informed Defense
Three Dimensions of Threat-Informed Defense
Measuring Threat-Informed Defense
Maximize & Mature Threat-Informed Defense
Moving Forward
Conclusion
Changelog
Appendix A - Key Components and Maturity Levels
Appendix B - Scoring Spreadsheet
/ Measure, Maximize, and Mature Threat-Informed Defense v1.0.0
CYBER THREAT INTELLIGENCE
THREAT INFORMED DEFENSE
DEFENSIVE MEASURES
TESTING & EVALUATION

Measure, Maximize, and Mature Threat-Informed Defense v1.0.0

The Measure, Maximize, and Mature Threat-Informed Defense (M3TID) project defines what threat-informed defense is and the key activities associated with its practice. The project captures insights and best practices for what it means to be threat-informed across a security program, expanding the dimensions of threat-informed defense into key components that organizations can implement. For each of these components, the project defines specific elements of implementation maturity, which enables organizations to assess and to understand the current and future state of their threat-informed defense program.

Mature your threat-informed defense

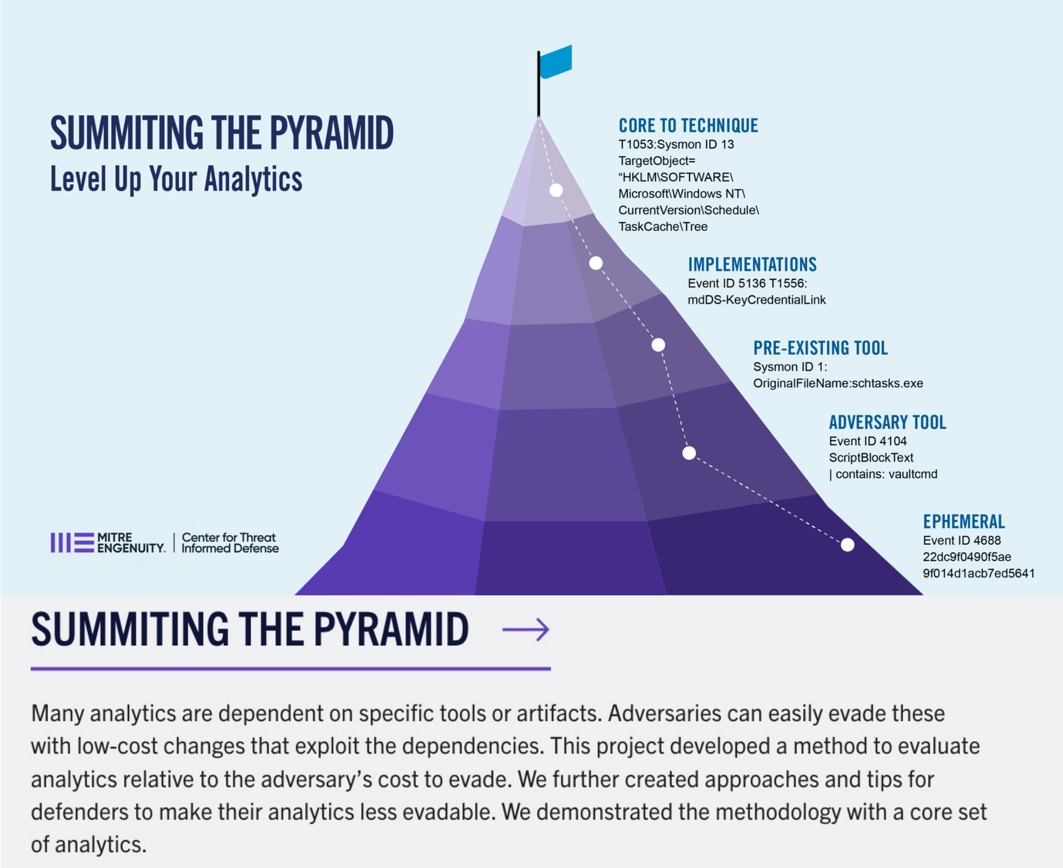
https://ctid.io/m3tid

MITRE ENGENUITY | Center for Threat Informed Defense

Applying Threat-Informed Defense

MITRE ENGENUITY | Center for Threat Informed Defense

Threat-Inform your Detection Engineering



SUMMITING THE PYRAMID

Level Up Your Analytics

CORE TO TECHNIQUE
T1053:Sysmon ID 13
TargetObject=
“HKLM\SOFTWARE\
Microsoft\Windows NT\
CurrentVersion\Schedule\
TaskCache\Tree

IMPLEMENTATIONS
Event ID 5136 T1556:
mdDS-KeyCredentialLink

PRE-EXISTING TOOL
Sysmon ID 1:
OriginalFileName:schtasks.exe

ADVERSARY TOOL
Event ID 4104
ScriptBlockText
| contains: vaultcmd

EPHEMERAL
Event ID 4688
22dc9f0490f5ae
9f014d1acb7ed5641

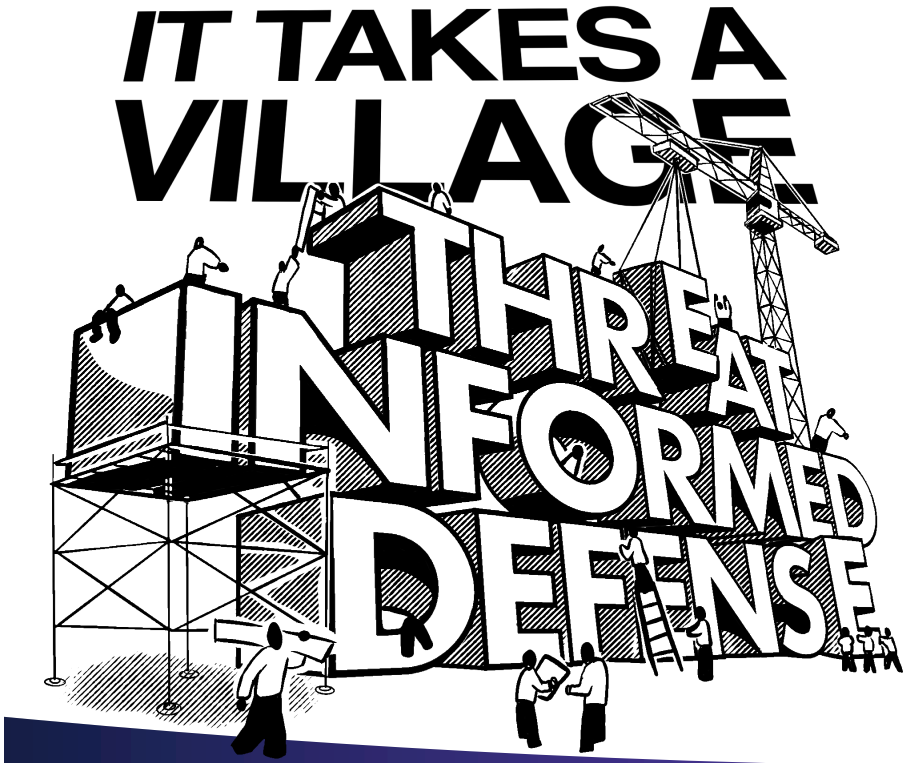
SUMMITING THE PYRAMID →

Many analytics are dependent on specific tools or artifacts. Adversaries can easily evade these with low-cost changes that exploit the dependencies. This project developed a method to evaluate analytics relative to the adversary’s cost to evade. We further created approaches and tips for defenders to make their analytics less evadable. We demonstrated the methodology with a core set of analytics.

“By scoring each threat detection rule, we gained a ***higher fidelity view of their security posture****. We determined that roughly* ***99.4% of their threat detection content was obsolete****, based on criteria such as analytic brittleness, current threat relevance and update frequency.*

In all my years of consulting, I have never witnessed a more catalyzed response—except in the case of a severe breach. ***This holistic, scientific method of threat detection analysis shocked them out of their lethargy*** *in ways their previous penetration tests never could.”* –
Summiting user from a global consultancy

https://ctid.io/summiting-the-pyramid



Join us and change the game!

Changing the game on the adversary requires a community-wide approach.

You play a critical role!

https://ctid.io/linkedin
https://ctid.io/get-involved

MITRE ENGENUITY | Center for Threat Informed Defense