

Asia-Pacific ATT&CK Community Workshop
April 26, 2024

Changing the Game Through Global Collaboration

Jon Baker
Director, 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

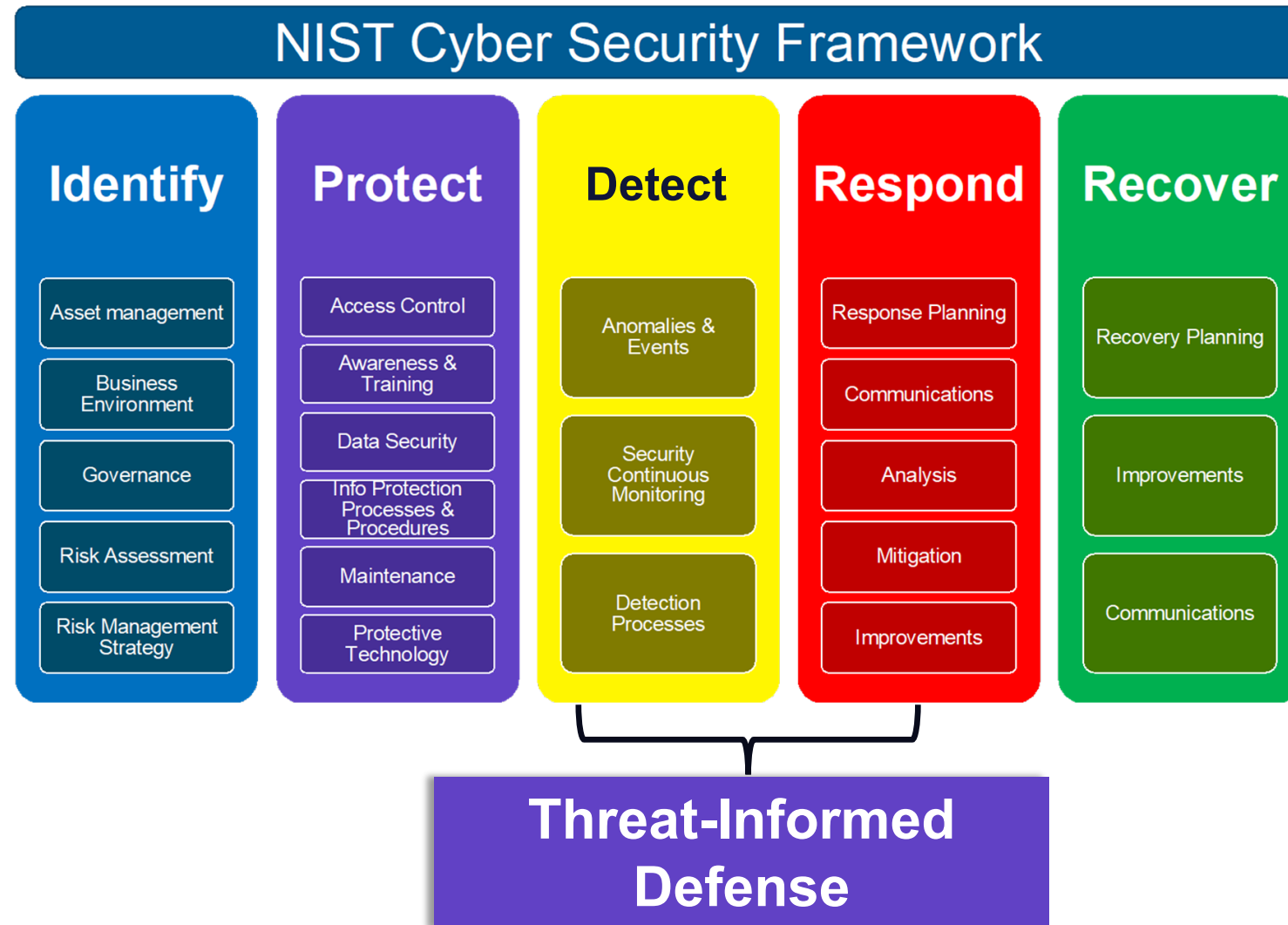
Working in the public interest to advance cybersecurity for all



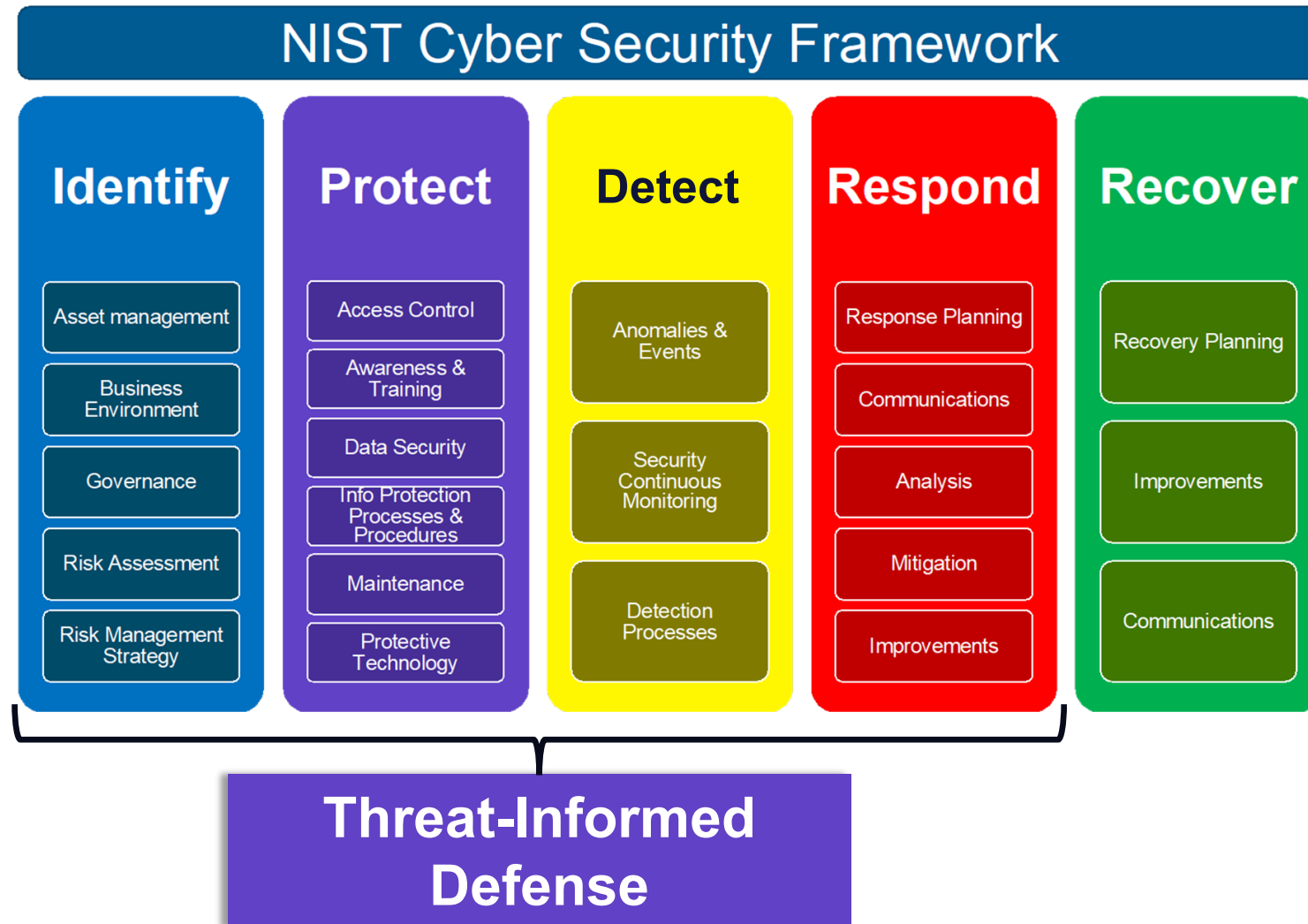
What is Threat-Informed Defense?

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

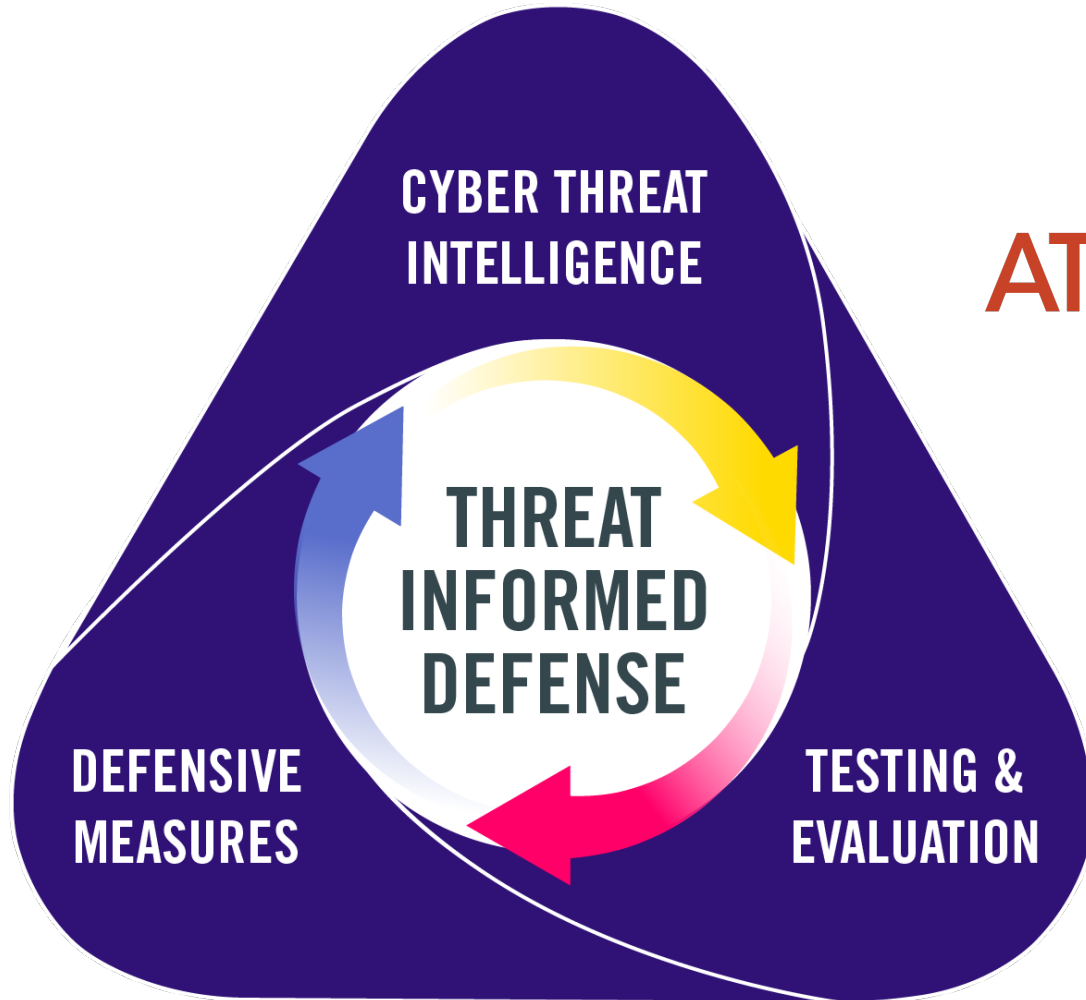
Where does it fit?



Where does it fit?



Threat-Informed Defense Cycle



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

Threat-informed defense is a continuous process.

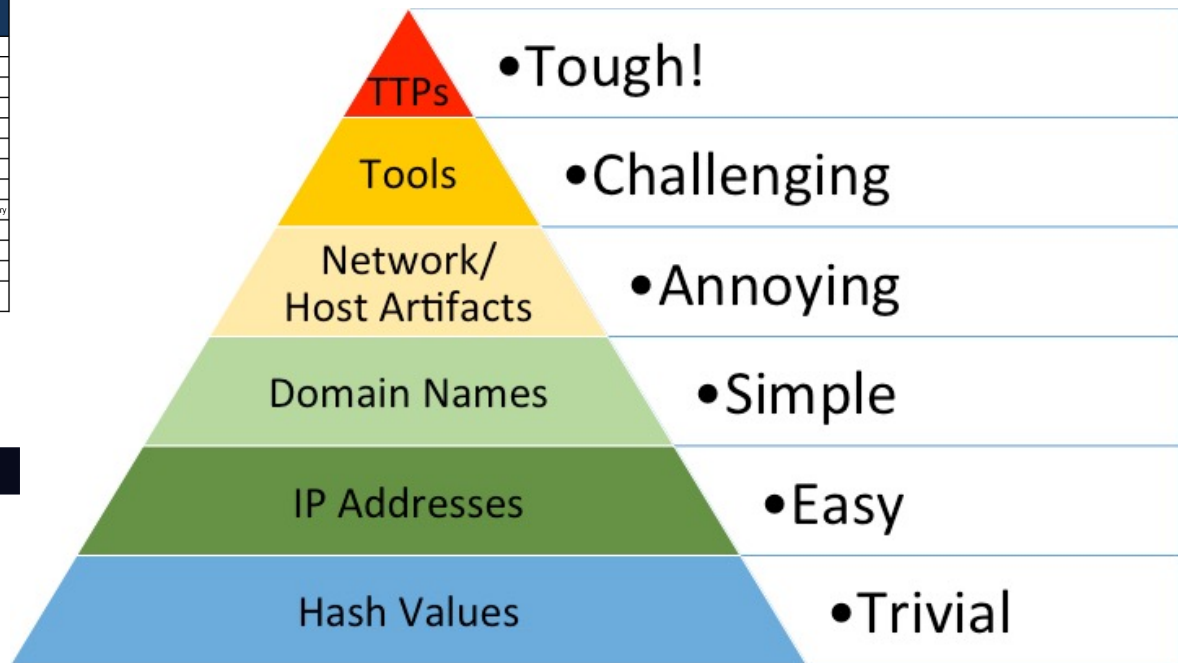
As our defenses improve, our environments change, and adversaries evolve, the cycle continues.

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 Credentials	Replicate/Remove/Supply	Supply	Domain Policy Modification	Container	Forge Web Credentials	Input Capture	Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe	
Search Closed Sources	Stage	Supply	Supply	Supply	Supply	Supply	Supply	Supply	Supply	Supply	Supply	Supply	
Search Open Technical Databases	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	Trusted Relationship	
Search Open Websites/Comments	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	
Search Victim-Owned Websites	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	Valid Accounts	

ATT&CK

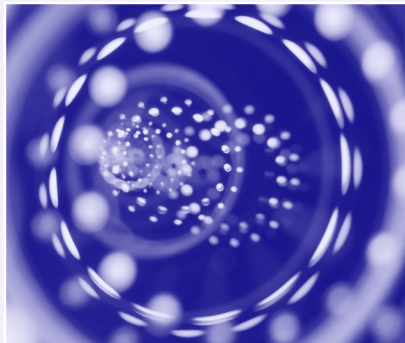
A community-driven knowledgebase of adversary TTPs



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

Threat- Informed Defense is...





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

How do we scale threat-informed defense?



The Center for Threat-Informed Defense conducts collaborative R&D projects that **improve cyber defense at scale**



+ **MITRE**
SOLVING PROBLEMS
FOR A SAFER WORLD™

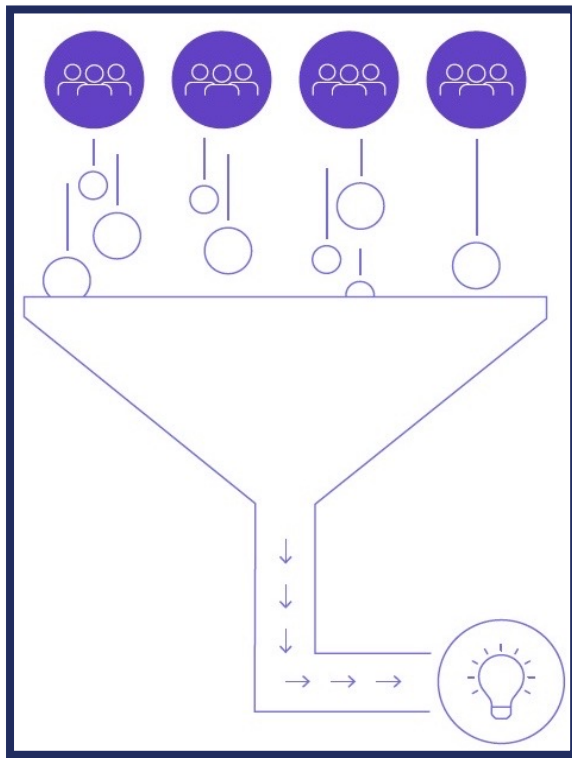
Membership is:

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

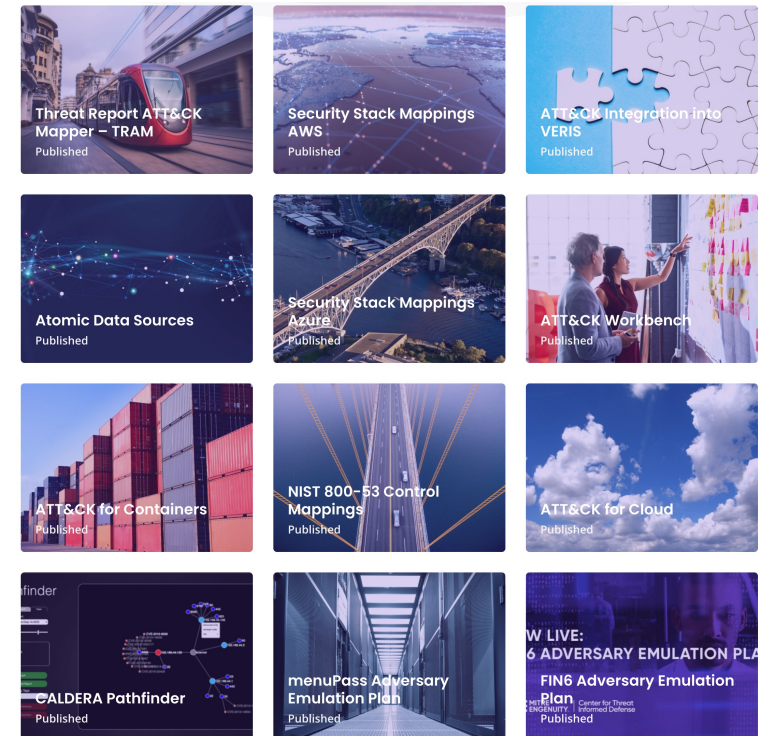
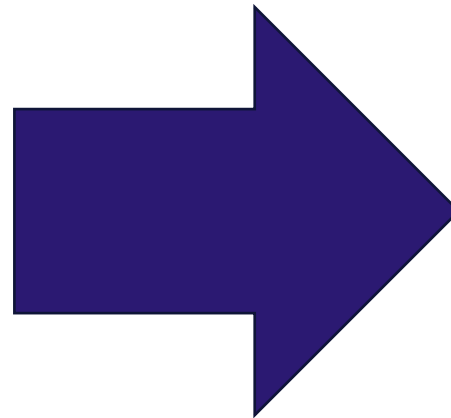
Mission: Advance the state of the art and the state of the practice in threat-informed defense globally.

**The cyber challenges
we face are larger than
any one organization**

A repeatable, scalable, approach to R&D built on member-powered collaboration



Systematically
identify challenges



Develop solutions
together

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

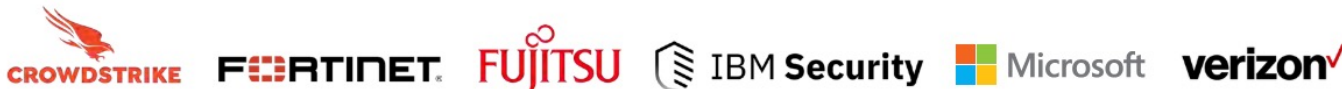
MITRE
ENGENUITY | Center for Threat
Informed Defense

PUBLISHED SEPTEMBER 2023

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.

PROJECT SPONSORS



Rapid Global Impact

“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 at a global consultancy



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

How do we scale threat-informed defense?

It takes community

Participants



Participants drive the R&D program with active engagement and funding

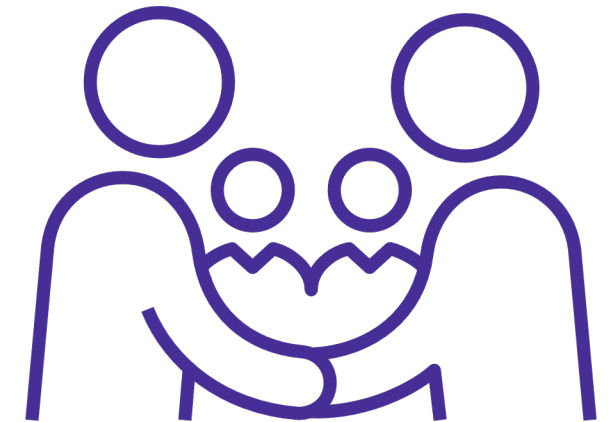
Benefactors



Enable the global community to advance public interest cybersecurity programs through charitable giving.

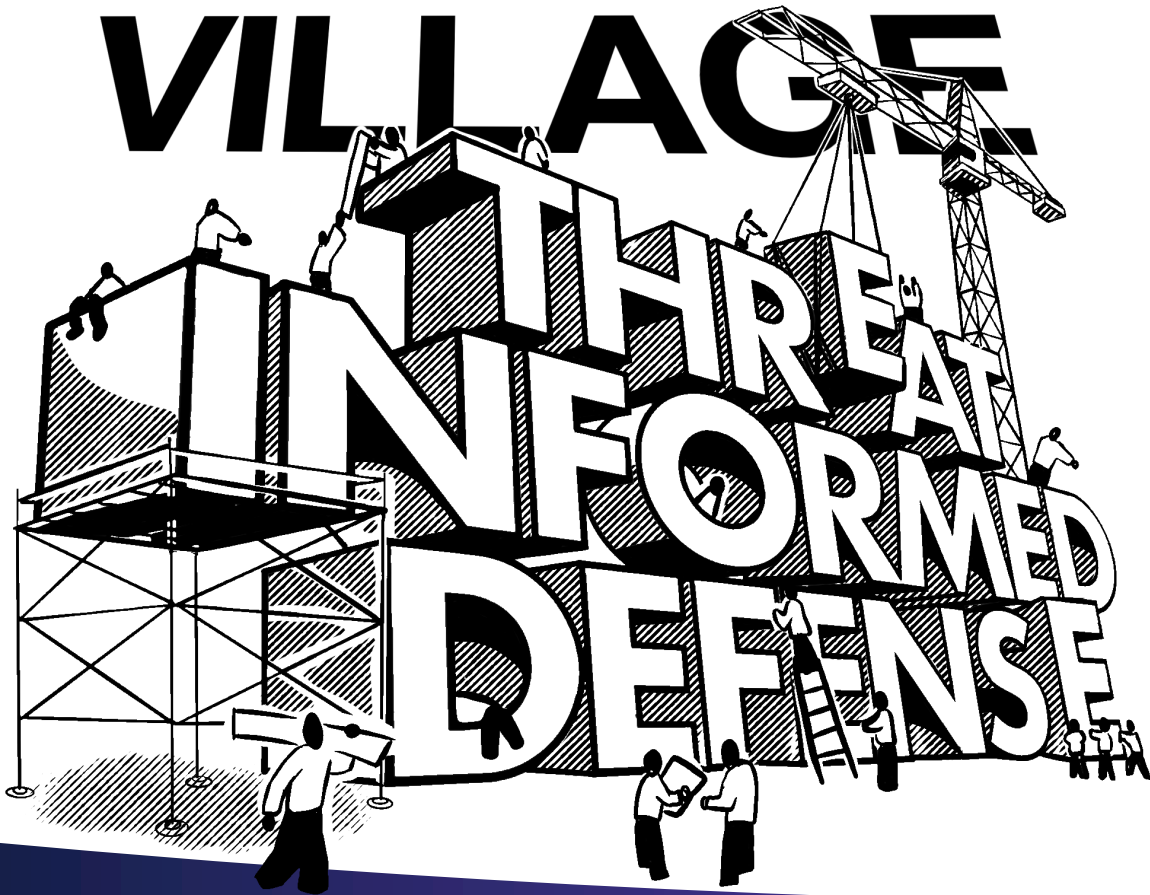
Benefactors support independent research in the public interest

Community



Global adoption leads to impact. Your use cases drive community-wide advancement

IT TAKES A VILLAGE



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>