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

Changing the Game Through Global Collaboration

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…

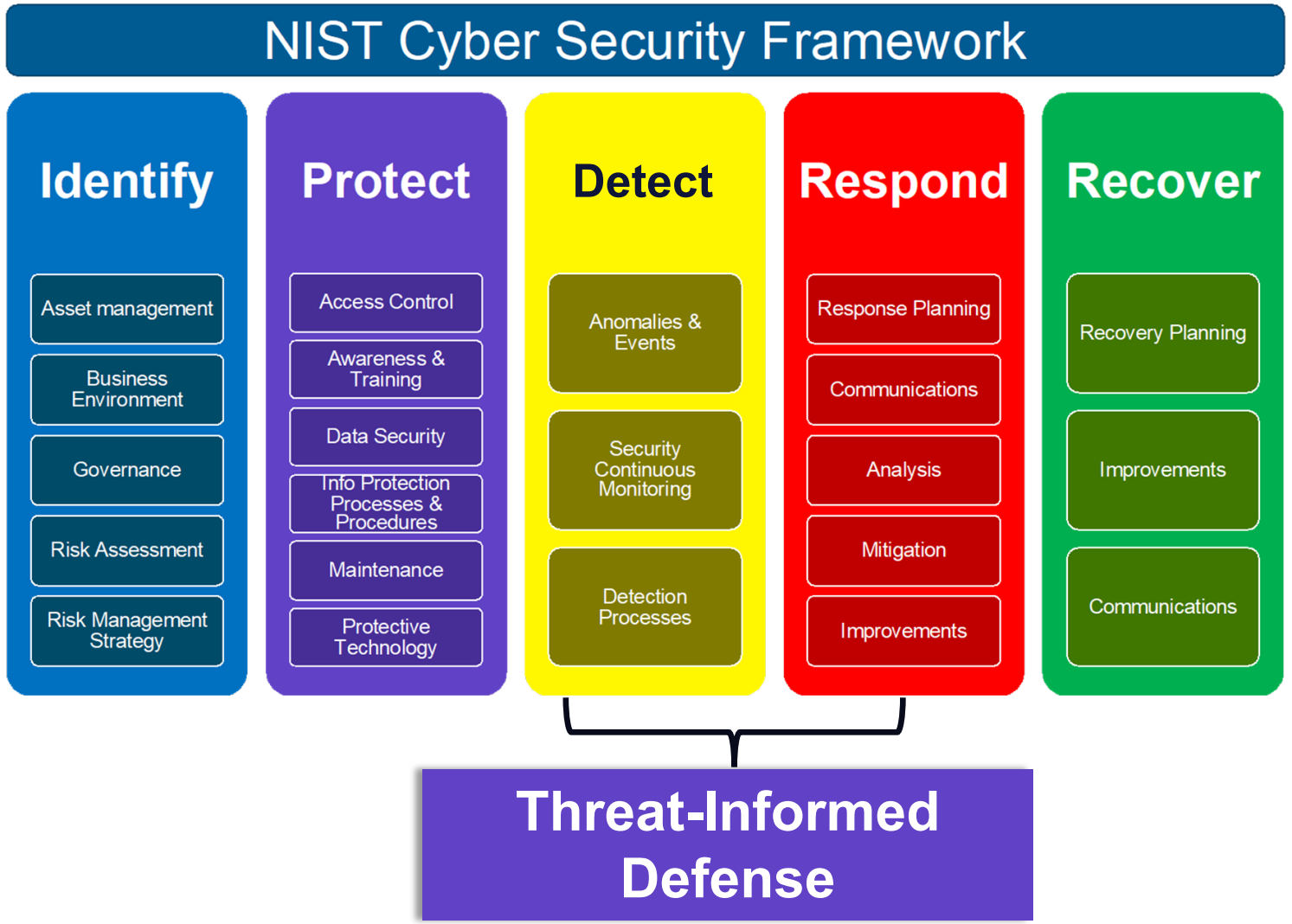
Started out as a software engineer

Working in the public interest to advance cybersecurity for all

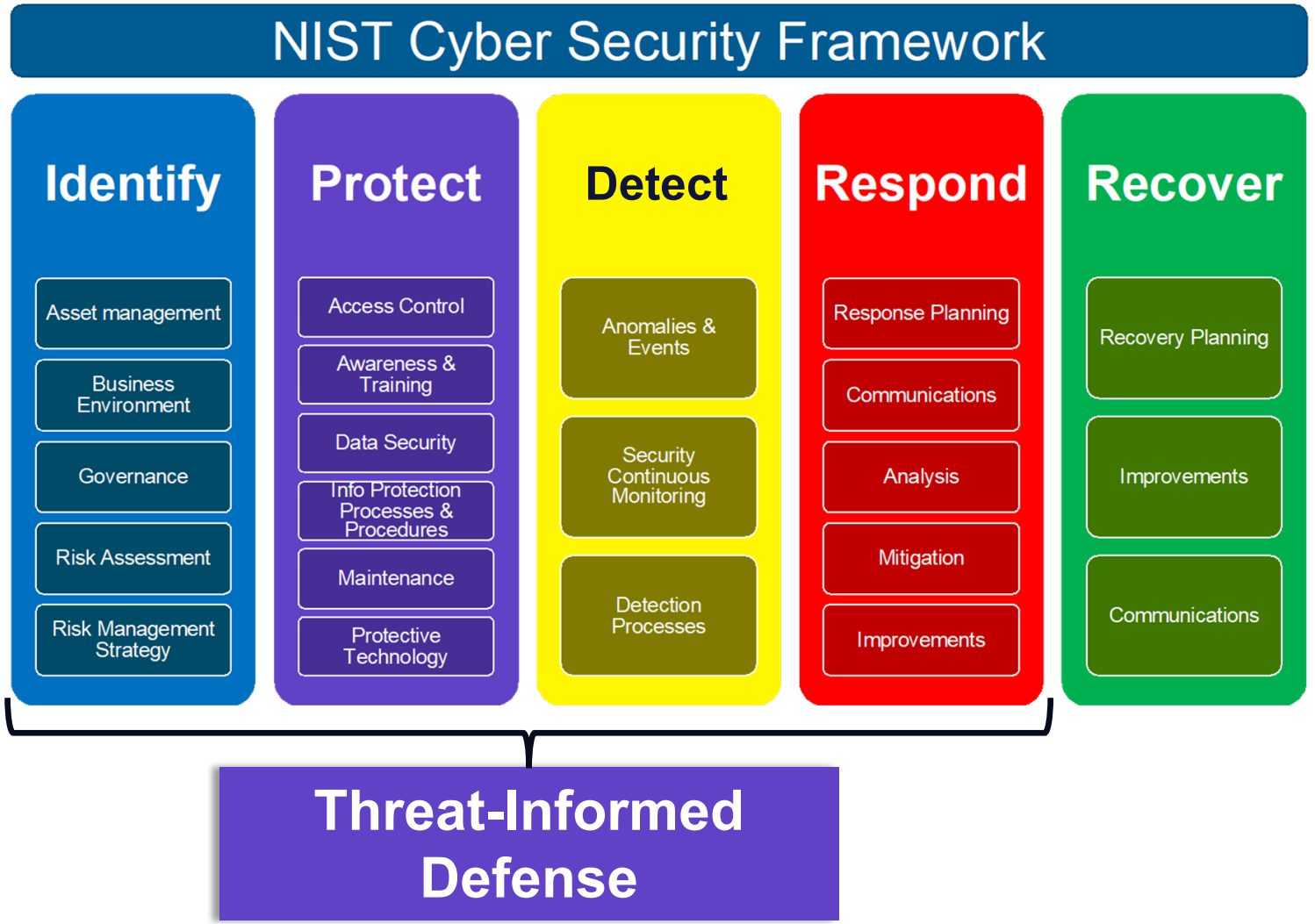
What is Threat-Informed Defense?

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

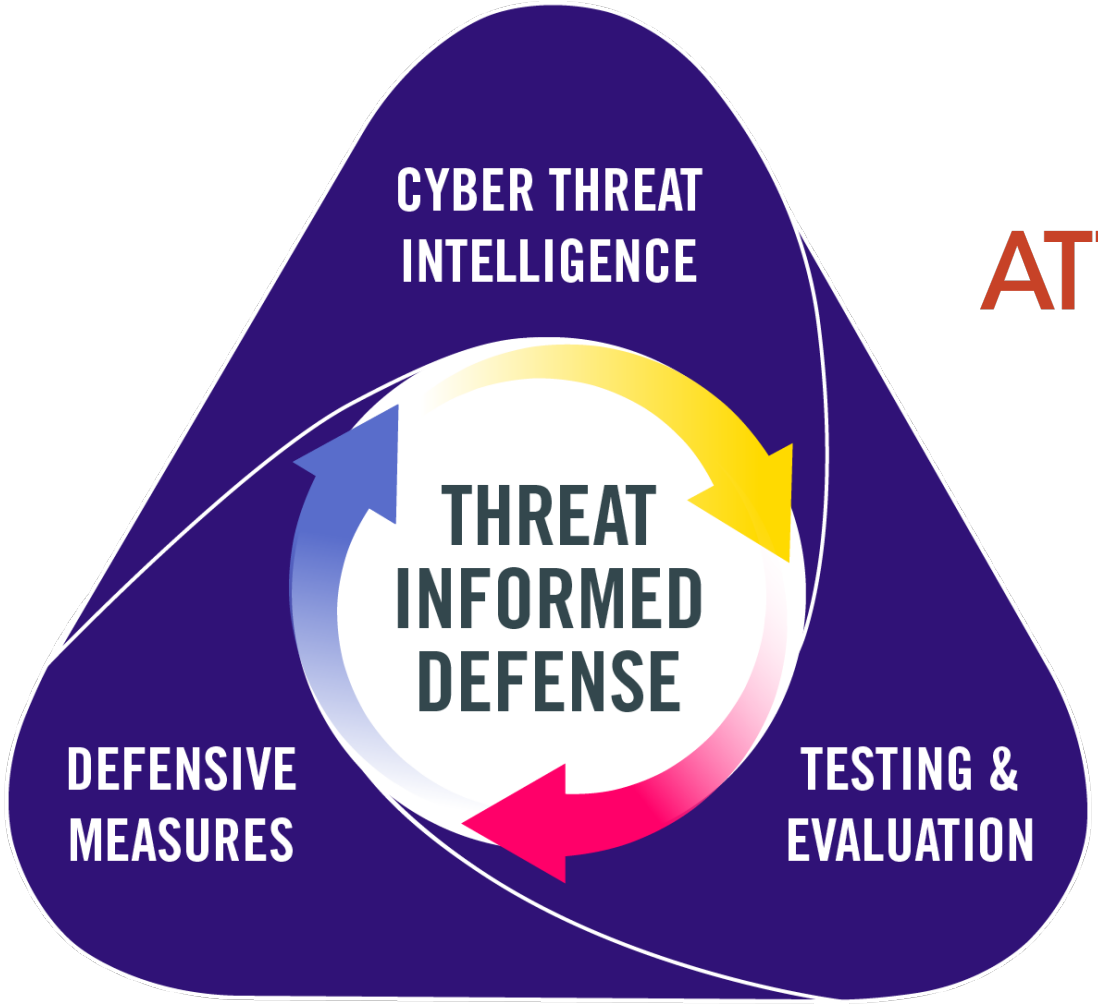
Where does it fit?



Where does it fit?



Threat-Informed Defense Cycle

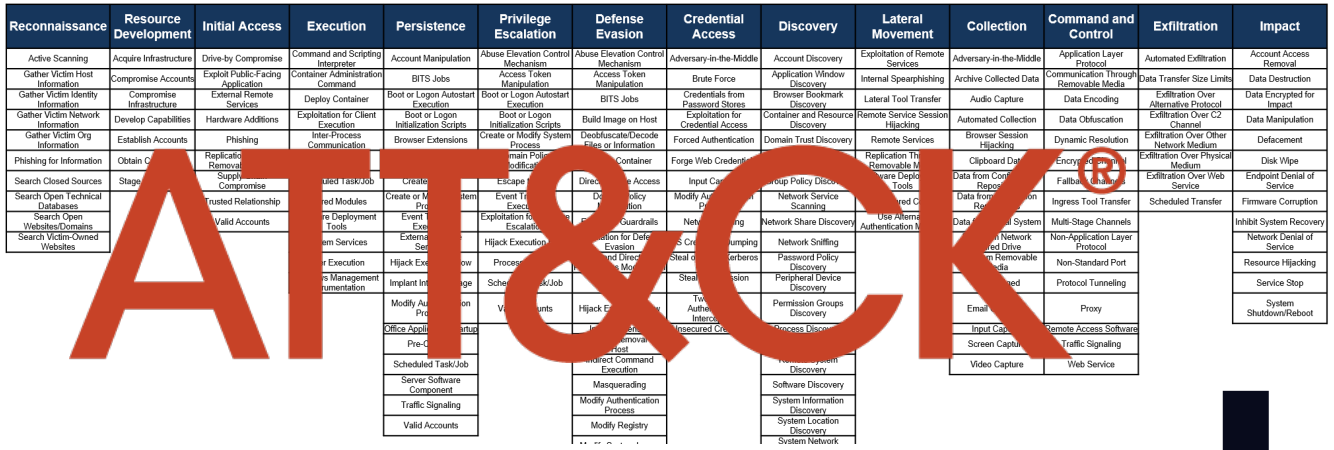


ATT&CK® is at the core of threat-informed defense

Threat-informed defense is a continuous process.

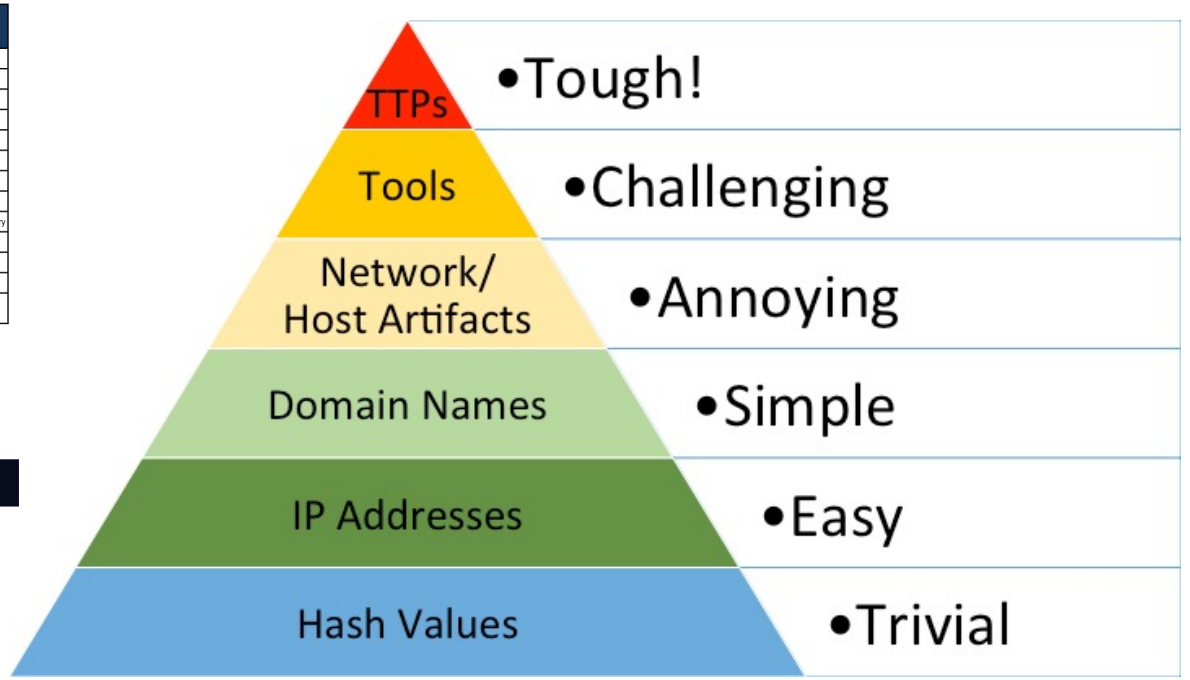
As our defenses improve, our environments change, and adversaries evolve, the cycle continues.

Increase the Cost for the Adversary



A community-driven knowledgebase of adversary TTPs

+

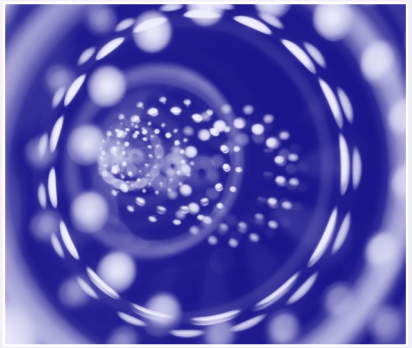


* Pyramid of Pain by David Bianco http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

MITRE ENGENUITY™ | Center for Threat Informed Defense

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

How do we scale threat-informed defense?

MITRE ENGENUITY | Center for 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

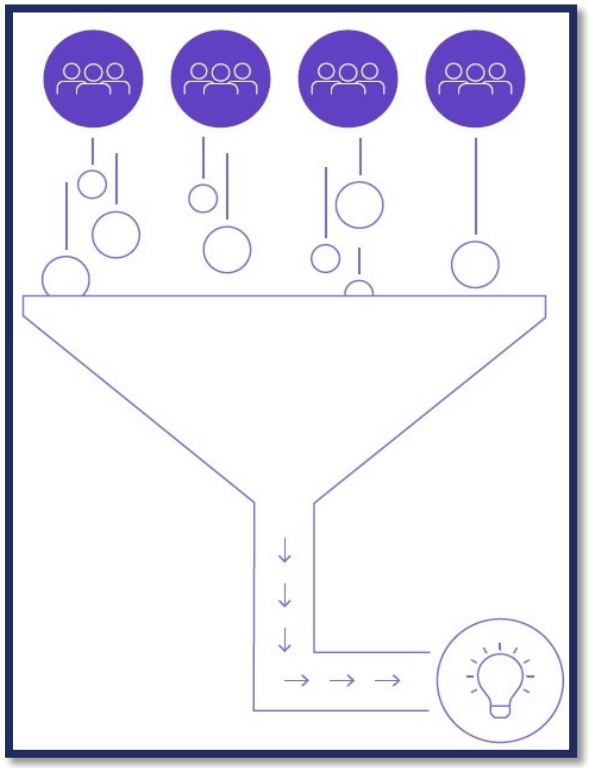
Mission: Advance the state of the art and the state of the practice in threat-informed defense globally.

MITRE ENGENUITY | Center for Threat Informed Defense

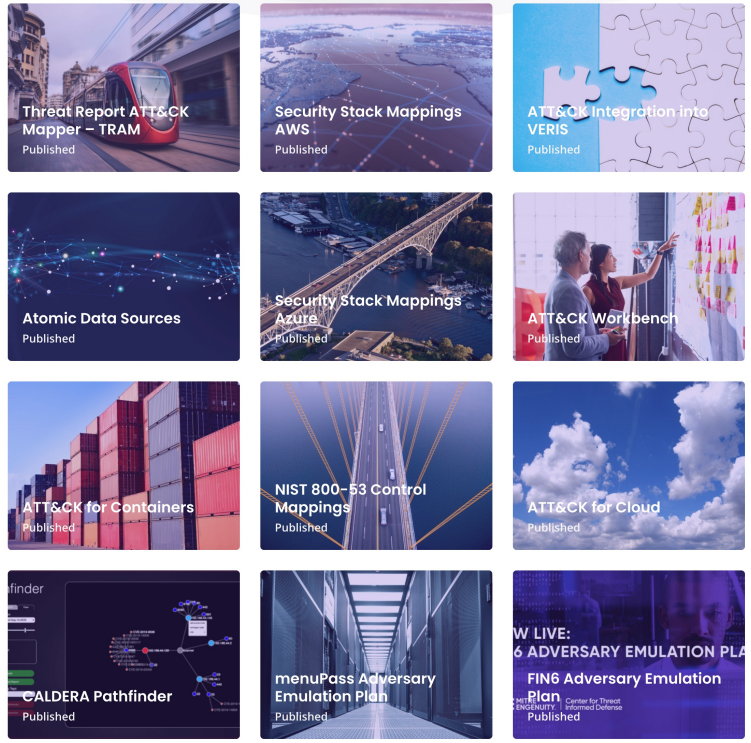
The cyber challenges we face are larger than any one organization

MITRE ENGENUITY | Center for Threat Informed Defense

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

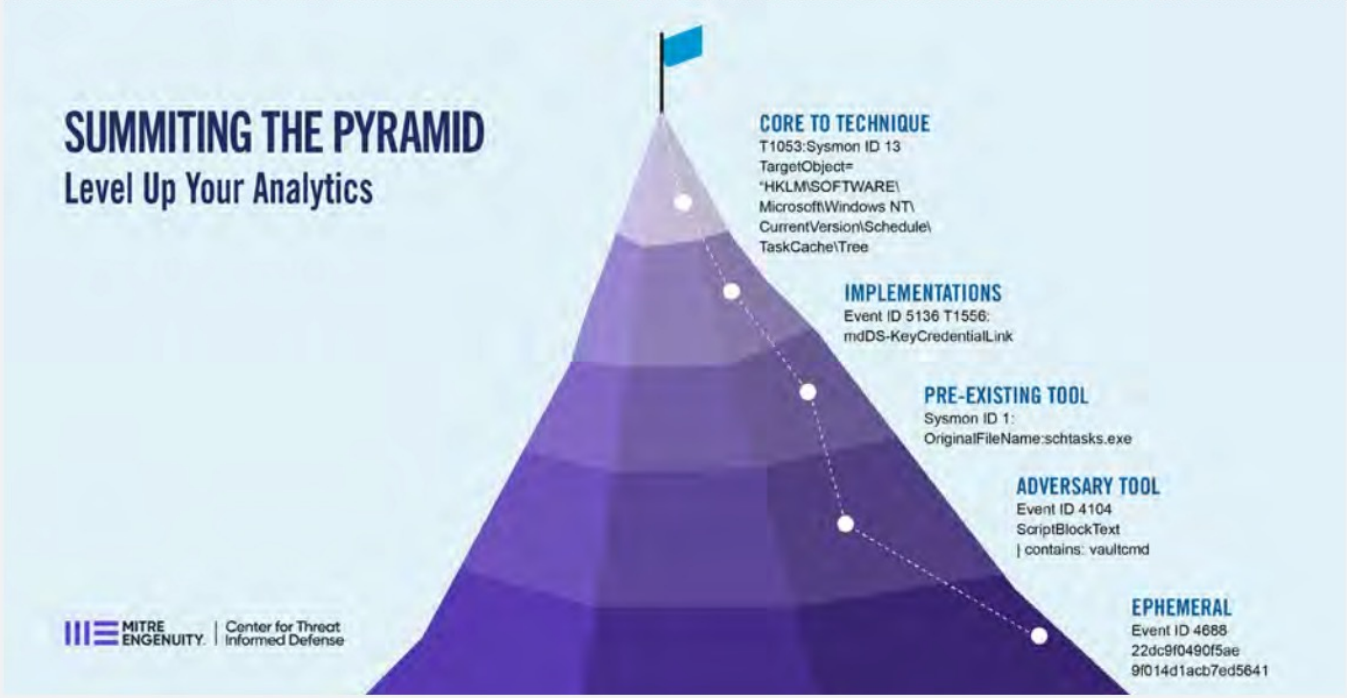


Systematically identify challenges



Develop solutions together

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

CROWDSTRIKE FORTINET FUJITSU IBM Security Microsoft verizon

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

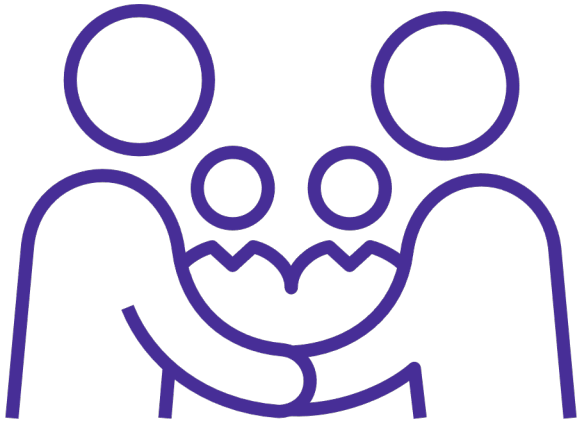
Benefactors

ACALVIO
COALFIRE
TIDAL CYBER
nviso
SQC PRIME
ZIMPERIUM

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

Benefactors support independent research in the public interest

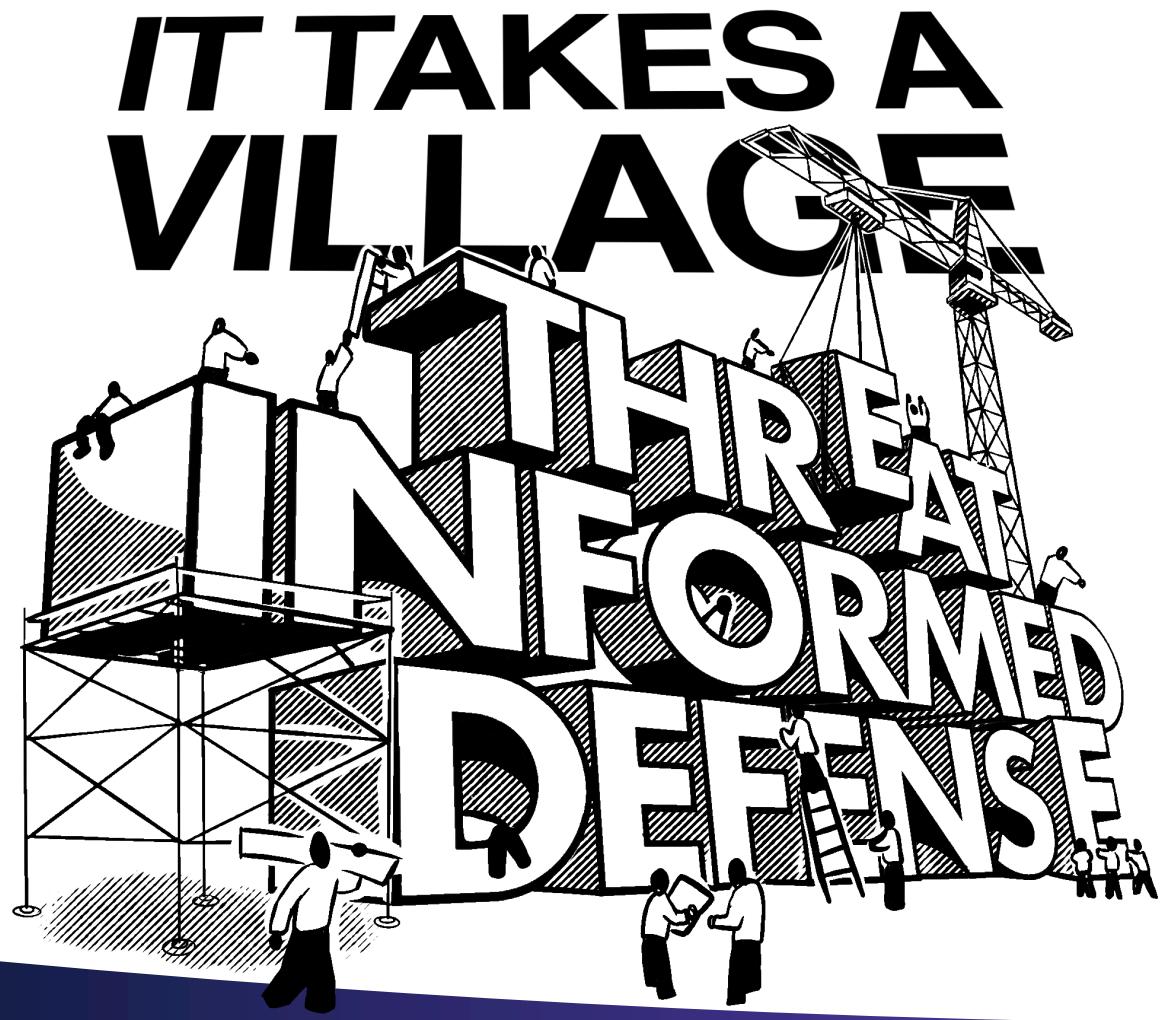
Community



MITR

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

MITRE ENGENUITY | Center for Threat Informed Defense



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