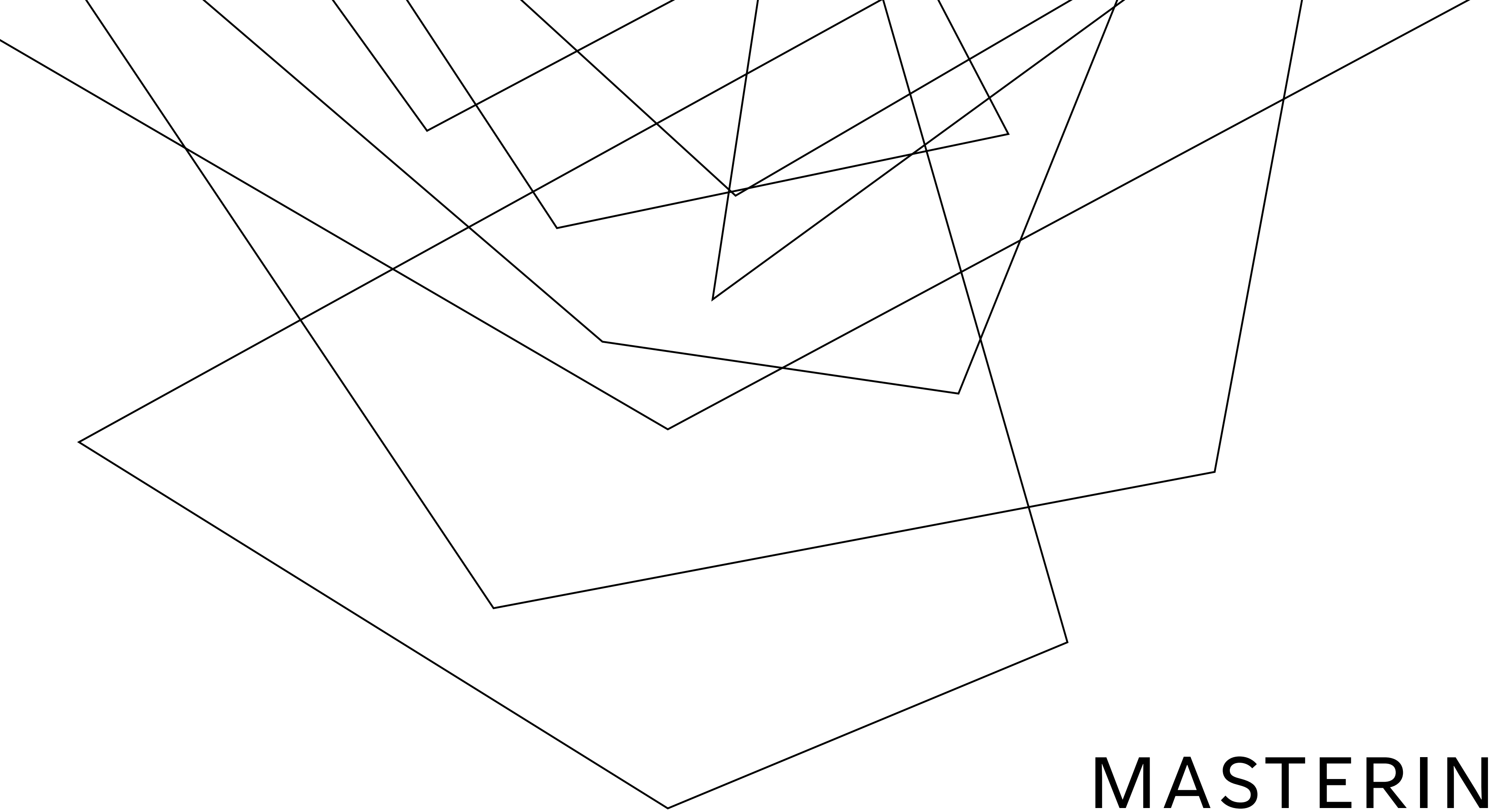


MASTERING THE (EXTRA)ORDINARY

A New Red Team Maturity Model

SPEAKERS AND PRIMARY CONTRIBUTORS

Garet Stroup

Director of Cyber Threat Simulation, Humana

Builder, Breaker, Automator of Things

Brent Harrell

Red Team Lead, Humana

Learner, Hole-Poker, Wielder of the Flame of Sarcasm

AGENDA

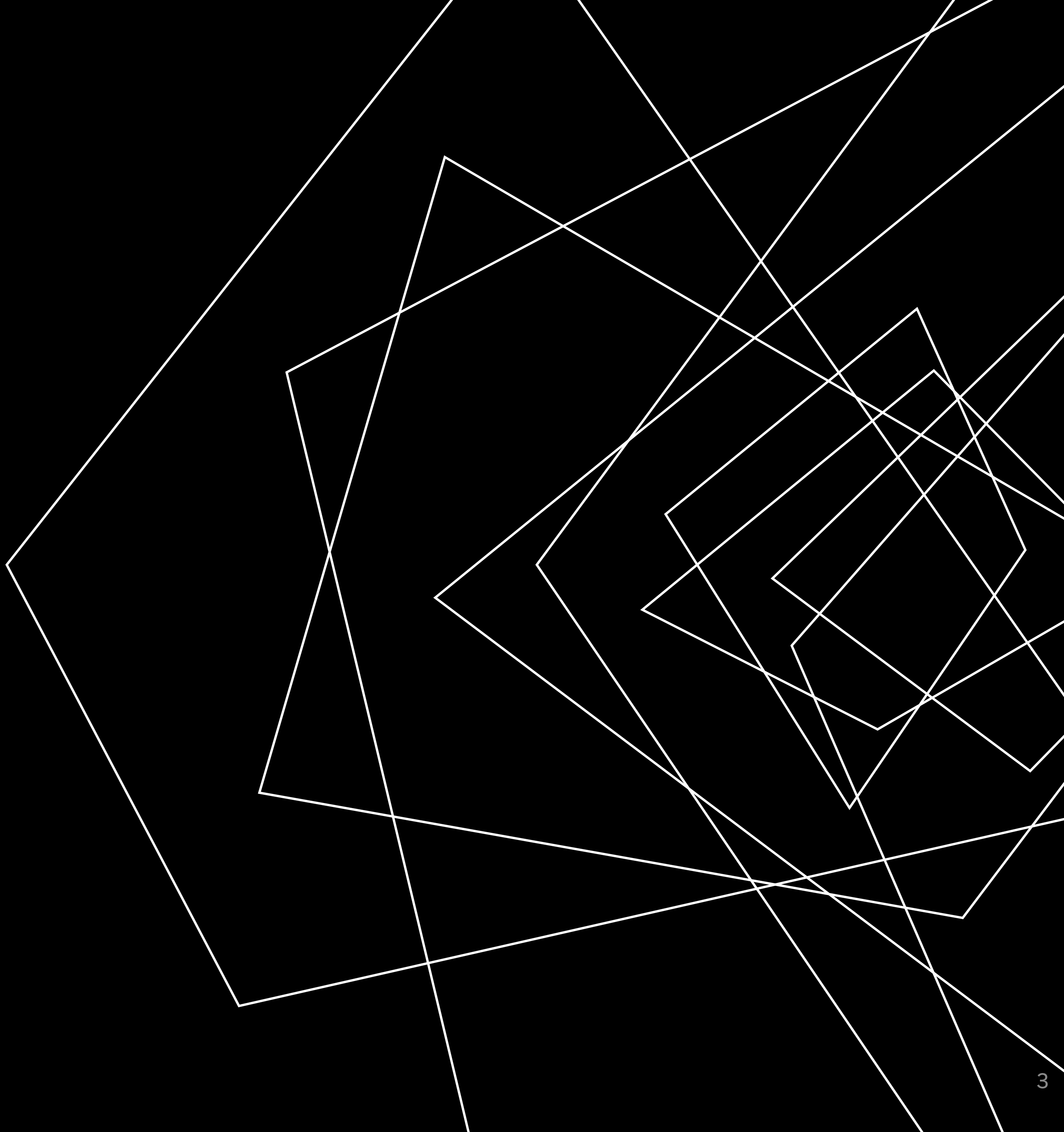
The Problem

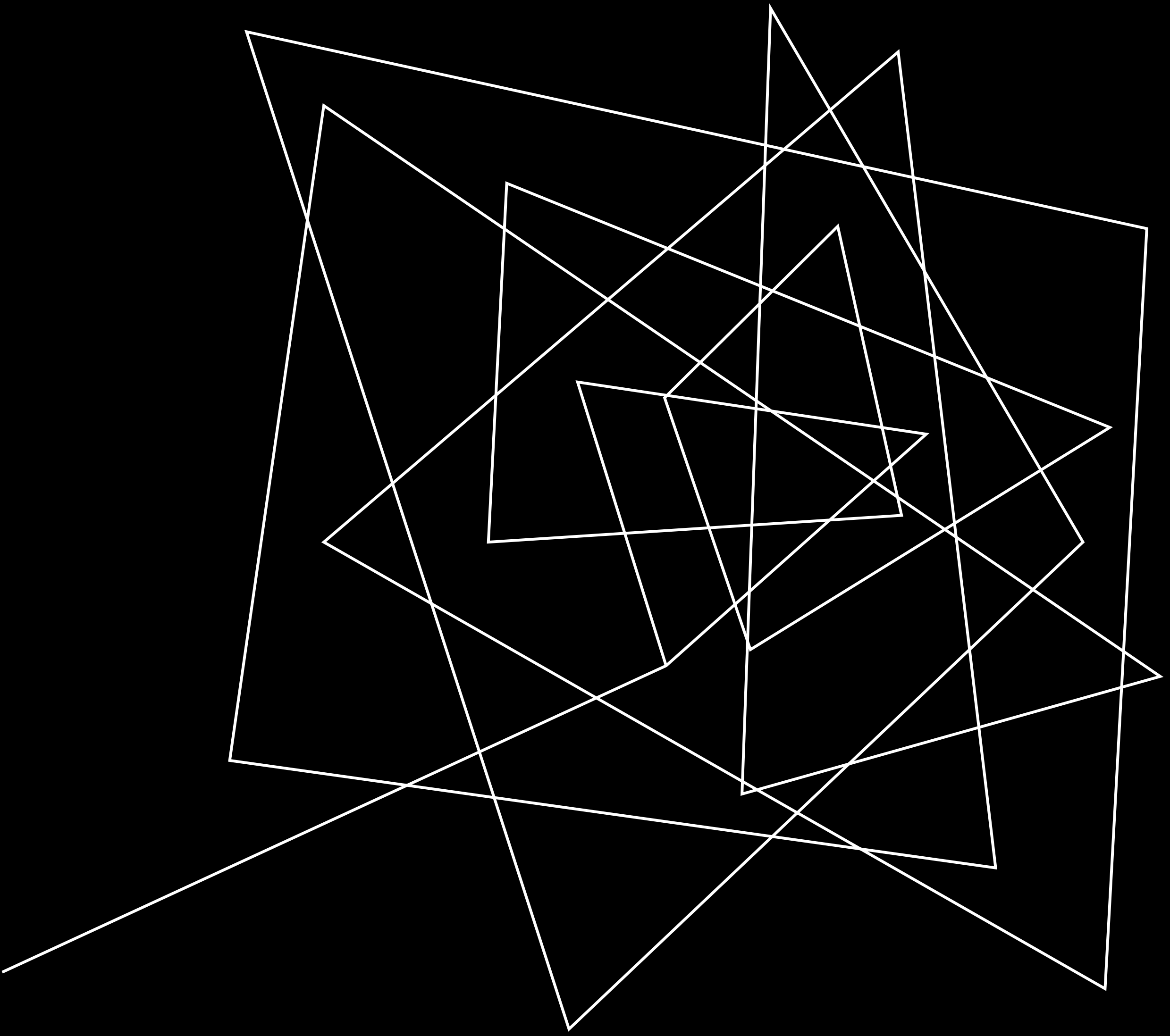
The Solution

Key CMM Elements

Implementation Notes

Wrap Up and Questions





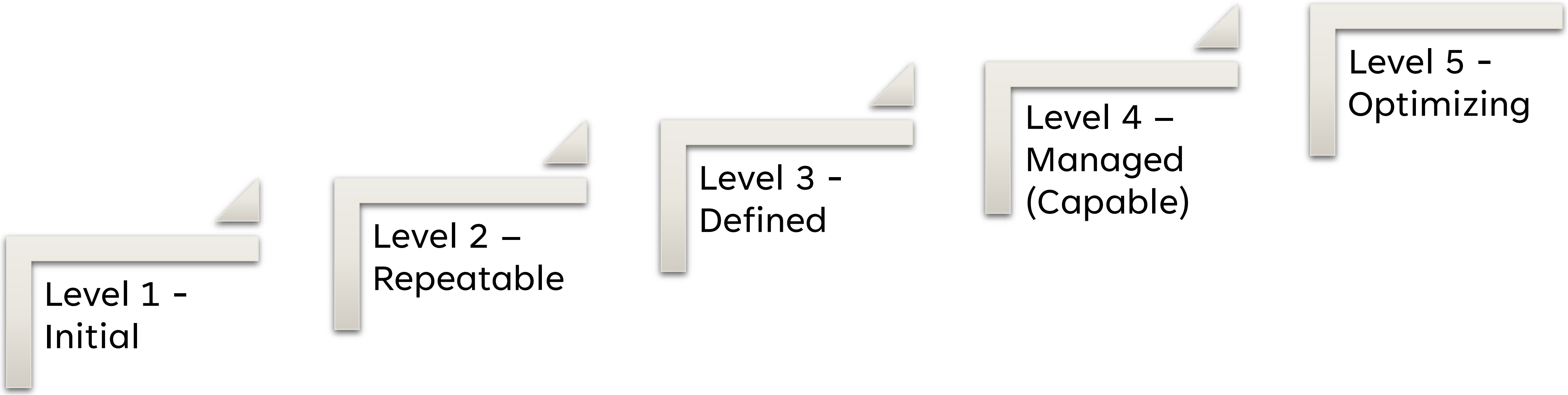
ΓΝΩΘΙ ΣΑΥΤΟΝ

… KNOW THYSELF

RED TEAMS INFORM AN ORGANIZATION’S UNDERSTANDING OF ITS RESILIENCY

HOW DO WE MEASURE, REPORT ON, AND PLAN FOR RED TEAM MATURITY TO IMPROVE THAT INFORMATION?

A QUICK CMM REVIEW



Level 1 - Initial

Level 2 – Repeatable

Level 3 - Defined

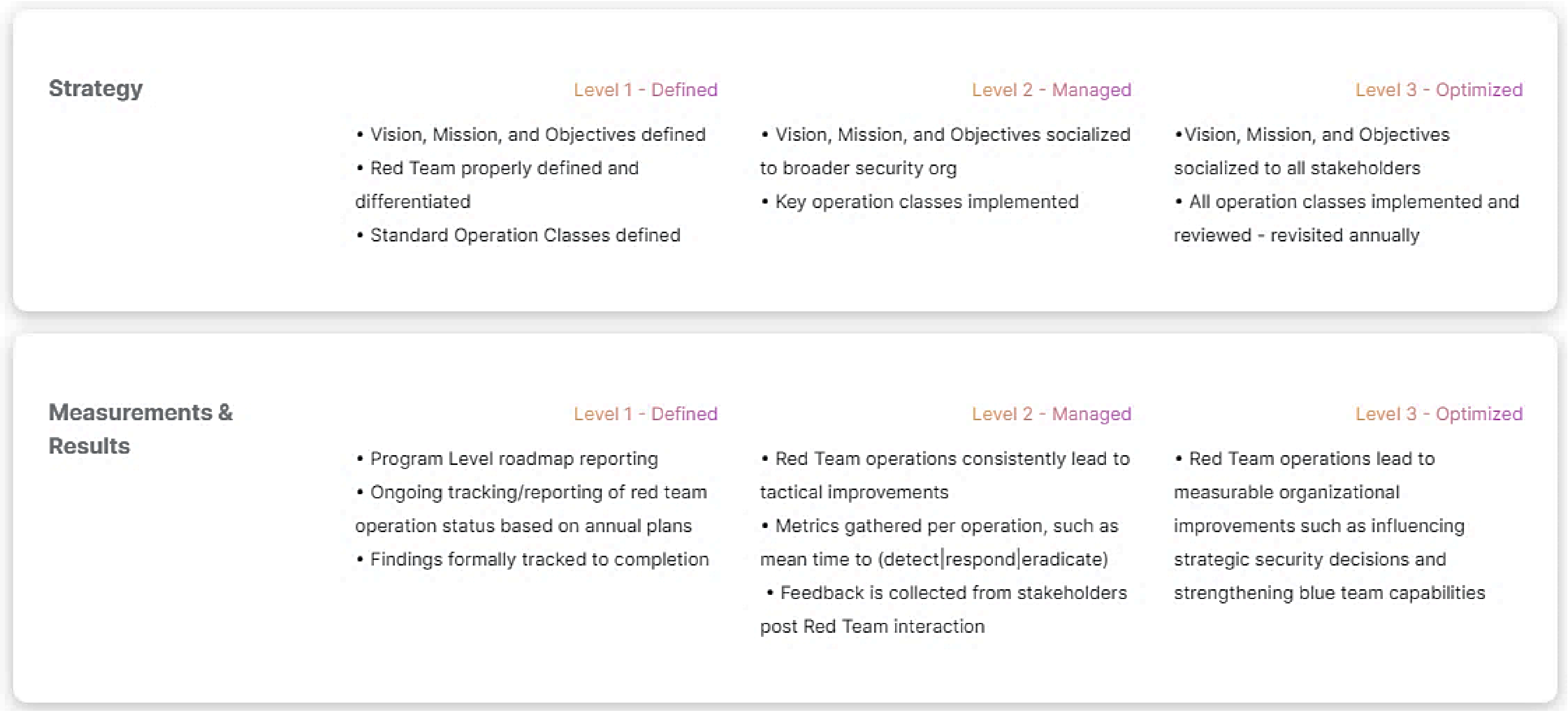
Level 4 – Managed (Capable)

Level 5 - Optimizing

- Levels provide behavioral examples
- Progression requires:
  - Meeting the prior level (and, typically, continuing that behavior)
  - Meeting all the described behavior in the new level

ORIGIN STORY

Program



Strategy	Level 1 - Defined	Level 2 - Managed	Level 3 - Optimized
	• Vision, Mission, and Objectives defined • Red Team properly defined and differentiated • Standard Operation Classes defined	• Vision, Mission, and Objectives socialized to broader security org • Key operation classes implemented	•Vision, Mission, and Objectives socialized to all stakeholders • All operation classes implemented and reviewed - revisited annually

Measurements & Results	Level 1 - Defined	Level 2 - Managed	Level 3 - Optimized
	• Program Level roadmap reporting • Ongoing tracking/reporting of red team operation status based on annual plans • Findings formally tracked to completion	• Red Team operations consistently lead to tactical improvements • Metrics gathered per operation, such as mean time to (detect|respond|eradicate) • Feedback is collected from stakeholders post Red Team interaction	• Red Team operations lead to measurable organizational improvements such as influencing strategic security decisions and strengthening blue team capabilities

Credit: Jordan Potti, Noah Potti, Trent Edgeworth; redteams.fyi

STRENGTHS AND GROWTH AREAS

> [I] decided to move to a more relaxed version given the ambiguity of our industry, and the additional complexity of the traditional CMM models.
>
> \- Jordan Potti, original author

Strengths

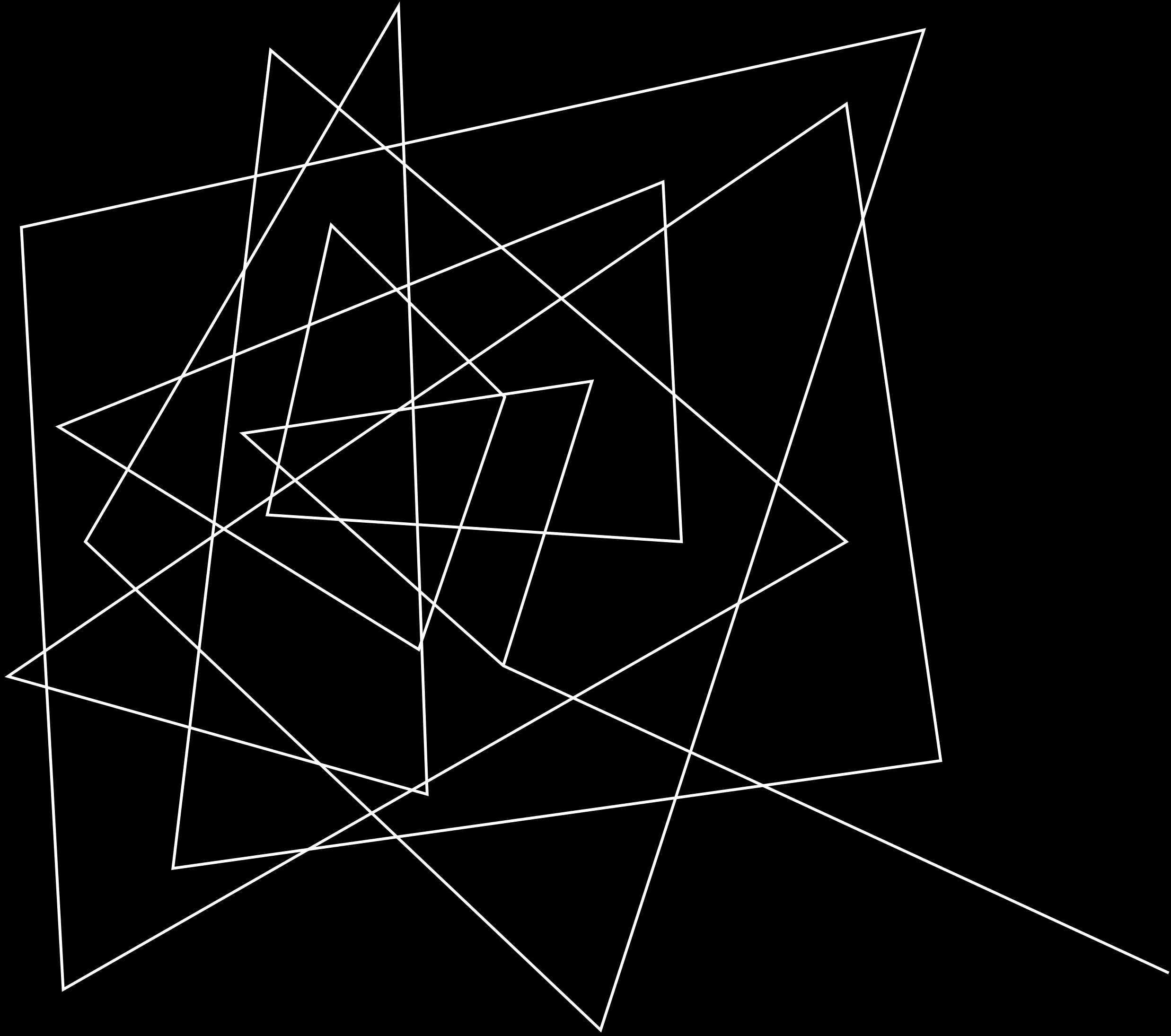
- Captured a lot of areas key to a mature Red Team
- Easily digested framework

Growth Areas

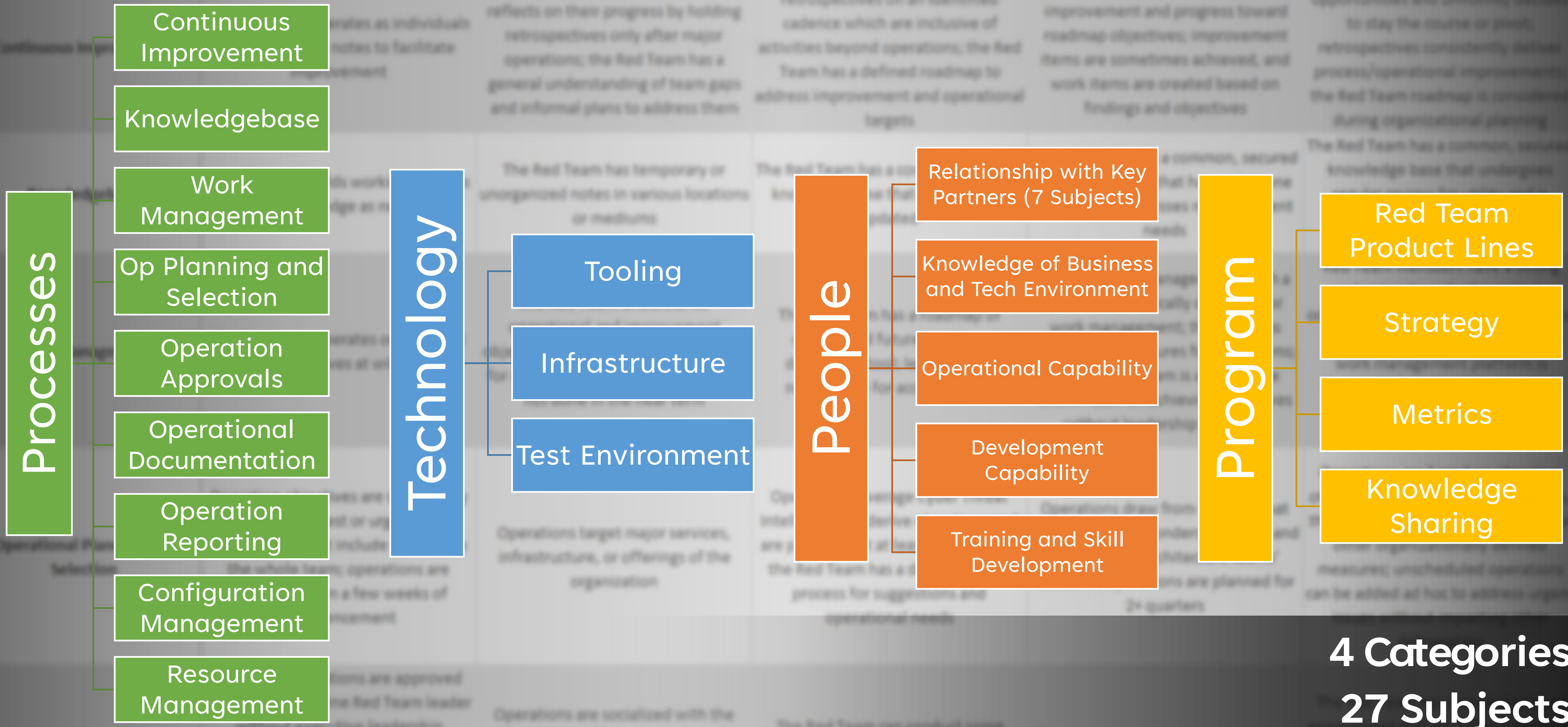
- Divergent format
- Subjects do not consistently track across levels

THE SOLUTION

A standardized Capability Maturity Model



THE REVISED MODEL



- Processes
  - Continuous Improvement
  - Knowledgebase
  - Work Management
  - Op Planning and Selection
  - Operation Approvals
  - Operational Documentation
  - Operation Reporting
  - Configuration Management
  - Resource Management
- Technology
  - Tooling
  - Infrastructure
  - Test Environment
- People
  - Relationship with Key Partners (7 Subjects)
  - Knowledge of Business and Tech Environment
  - Operational Capability
  - Development Capability
  - Training and Skill Development
- Program
  - Red Team Product Lines
  - Strategy
  - Metrics
  - Knowledge Sharing

4 Categories

27 Subjects

ADDRESSING EXISTING CHALLENGES

- Expanded from three levels to five to provide common scoring

- Aligned descriptors to language from other CMMs

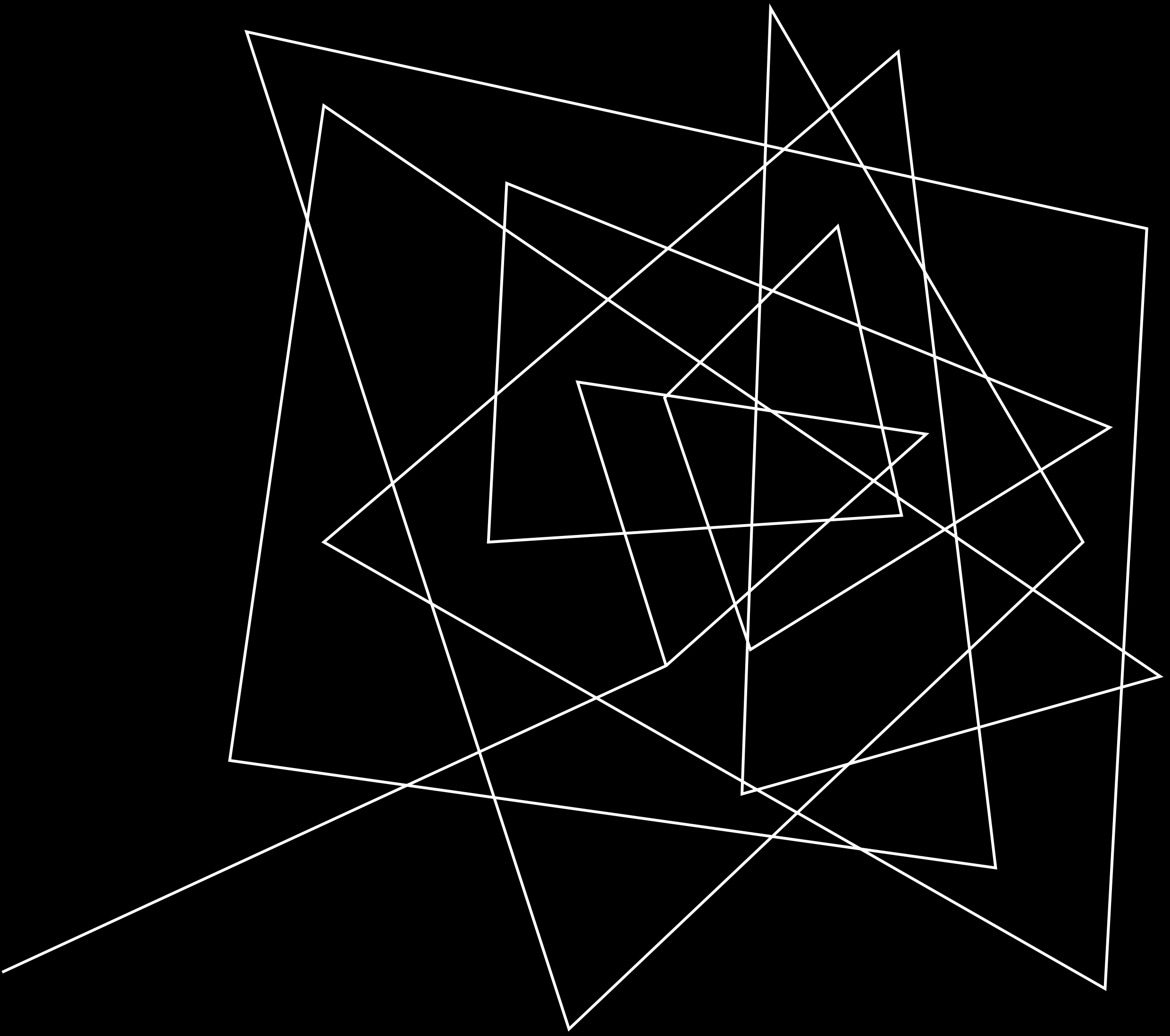
- Added new subjects to fill gaps left by simplification

THE NEW CHALLENGES WE FACED

- Existing level descriptors left gaps for Red Team-specific needs
  - Action: Added new descriptors that kept with the spirit of the originals

- “Additive” maturity does not work for all Red Team elements
  - Key offender: Technology subjects
  - Sliding-scale of maturity instead

- Keeping the subjects unique while not creating too many

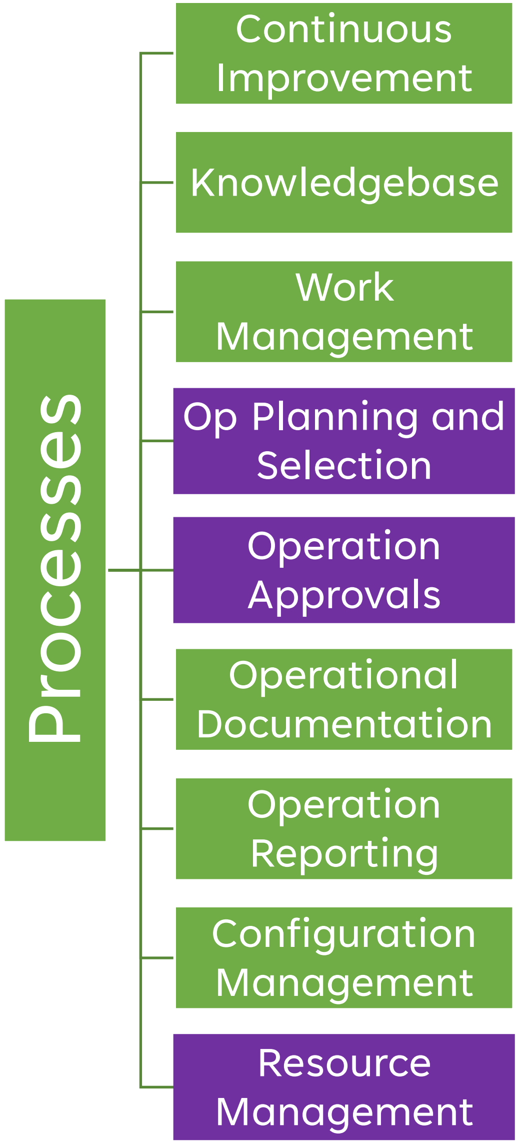


KEY CMM ELEMENTS

KEY ASSUMPTIONS AND GUIDELINES

- This CMM is predominantly for internal red teams
- The CMM presumes you have a staffed red team (not just a manager)
- Except for levels that describe a *negative*, teams must exhibit the preceding behavior before progressing
- If a team does not meet all the described behavior for a level, they cannot be at that level (including level 1)

PROCESSES



Processes

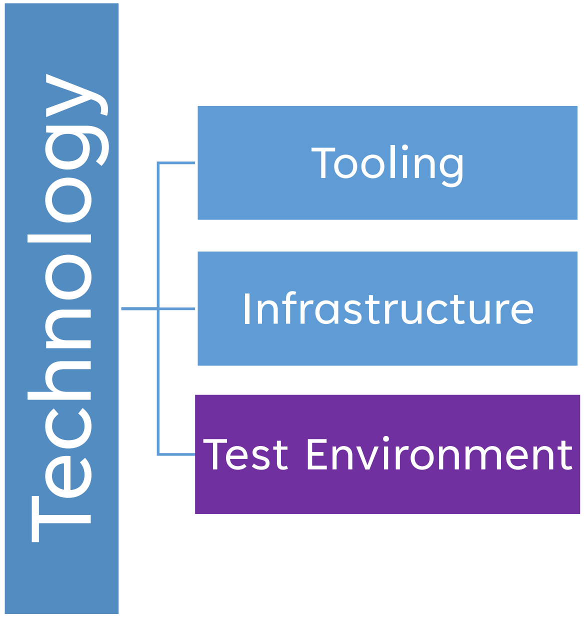
- Continuous Improvement
- Knowledgebase
- Work Management
- Op Planning and Selection
- Operation Approvals
- Operational Documentation
- Operation Reporting
- Configuration Management
- Resource Management

Key Notes – Processes

(Purple items denote areas with heightened leadership or organization interest – enabling or benefiting from Red Team maturity)

- Definition: Continuous Improvement - Red Team iterative improvement through planning and retrospection
- Definition: Work Management – Use of practices, like Agile, to guide efforts
- Note: Operational Approvals – Follows a forked path, either a bell-curve or linear downward slope ultimately leading to trust by leadership
- Definition: Resource Management – Accounts, licenses, or other non-personnel needs

TECHNOLOGY

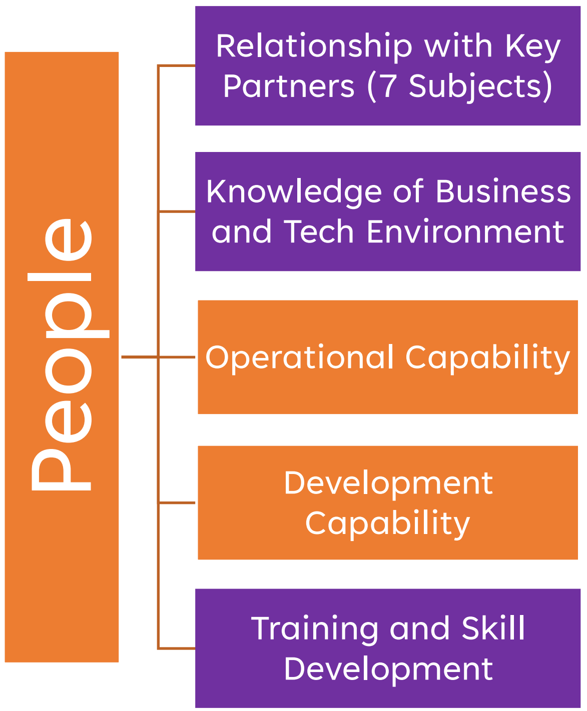


Key Notes – Technology

(Purple items denote areas with heightened leadership or organization interest – enabling or benefiting from Red Team maturity)

- Note: In general, this category follows more of a sliding scale of maturity rather than a layered approach
- Note: Key differentiators between levels are effectiveness of technology solutions and OPSEC considerations

PEOPLE



People

Relationship with Key Partners (7 Subjects)

Knowledge of Business and Tech Environment

Operational Capability

Development Capability

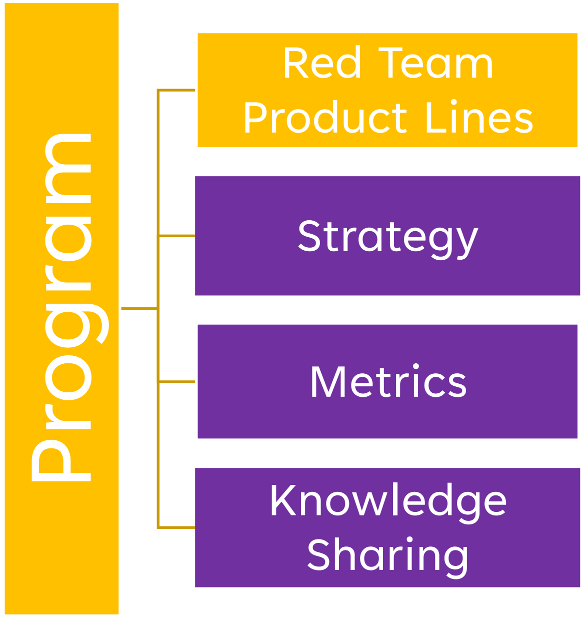
Training and Skill Development

Key Notes – People

(Purple items denote areas with heightened leadership or organization interest – enabling or benefiting from Red Team maturity)

- Note: The CMM contains 7 distinct subjects for partners like response teams, engineers, legal, and leadership
- Definition: Knowledge of Technical and Business Environment – The Red Team's awareness of key organization initiatives and technology stacks
- Note: To accurately simulate threats, the organization can support skill development with time and resources

PROGRAM



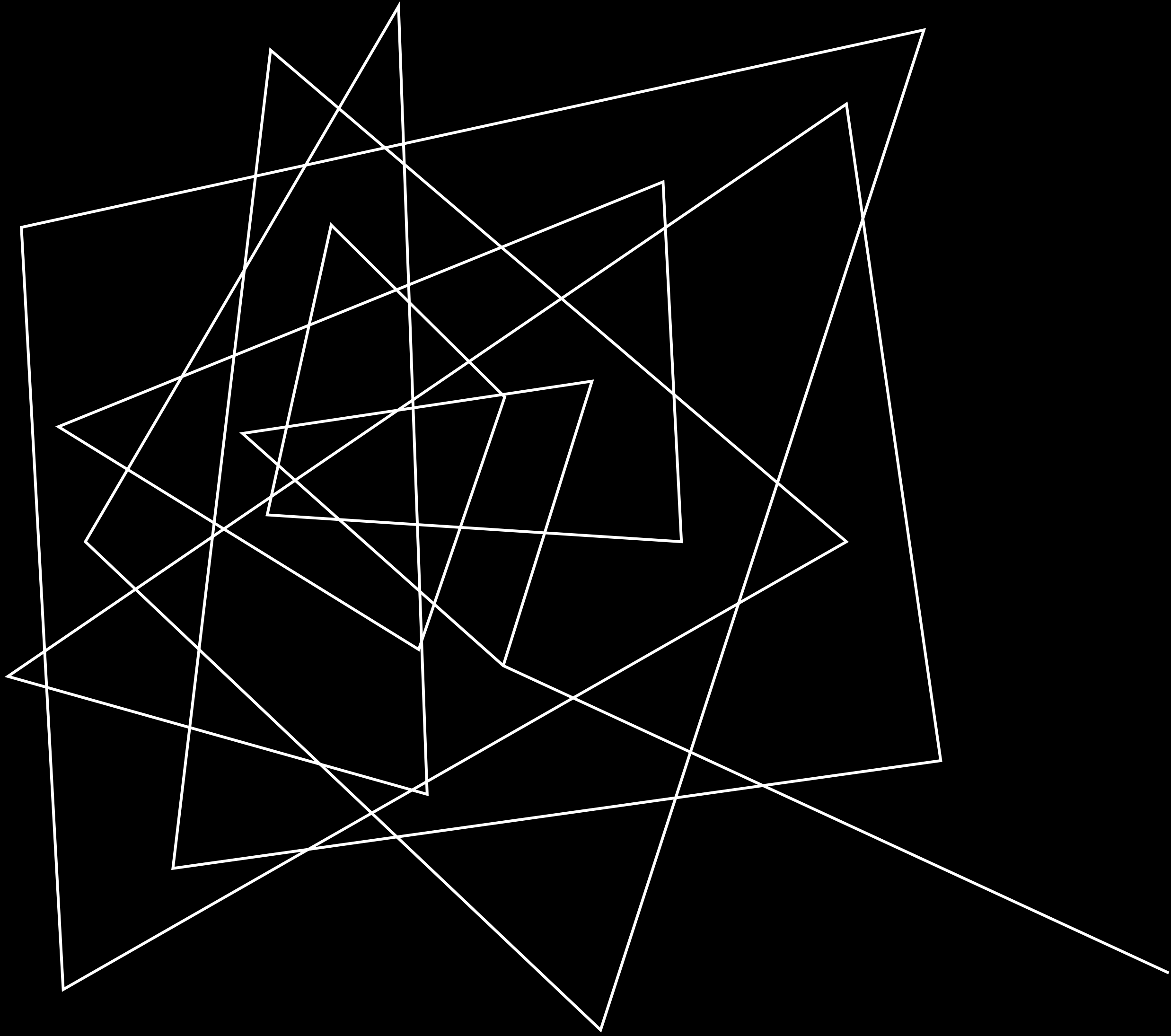
Key Notes – Program

(Purple items denote areas with heightened leadership or organization interest – enabling or benefiting from Red Team maturity)

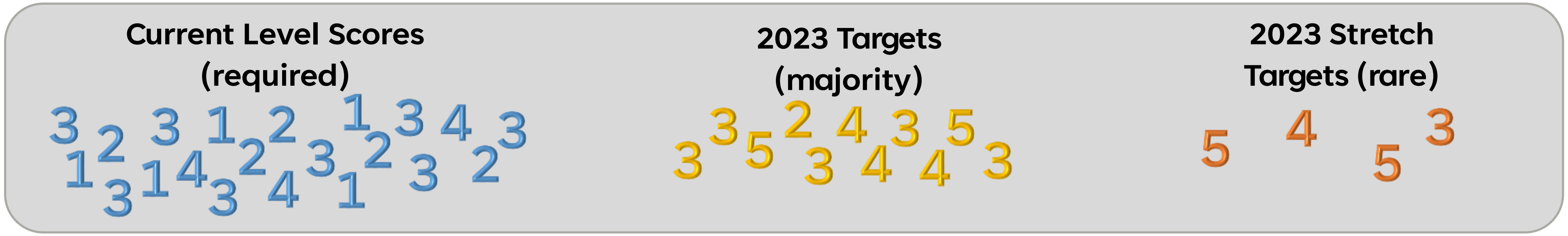
- Note: Organizational strategy guides Red Team operations; Red Team data can feed back into the organizational strategy
- Note: Level 4 typically entails metrics, but that does not apply to all the subjects in this CMM, leading to a category on metrics themselves
- Note: Information Security field relies on shared knowledge and resources to stay ahead; the Red Team should contribute

STORY TIME:

TALES FROM IMPLEMENTATION



Independent Team Scoring

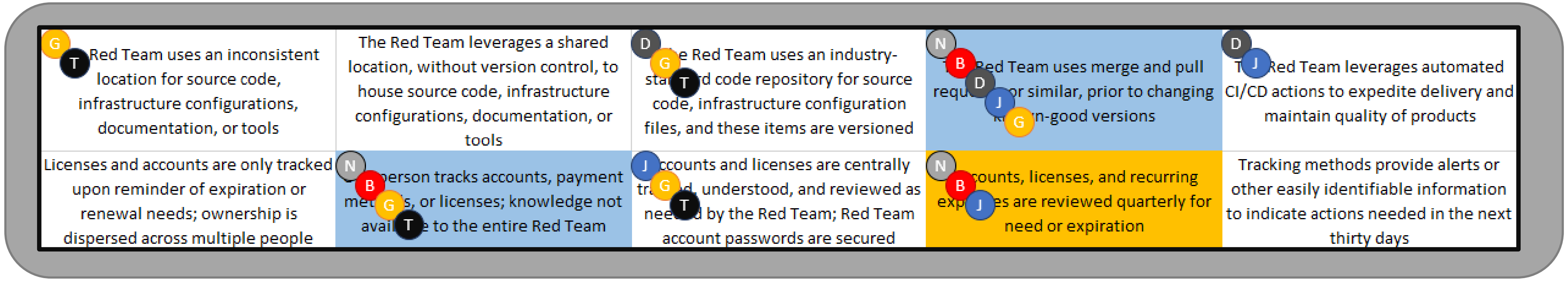


Current Level Scores (required)

2023 Targets (majority)

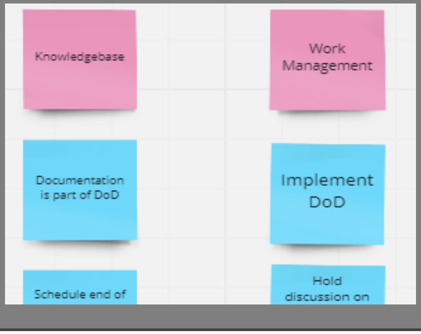
2023 Stretch Targets (rare)

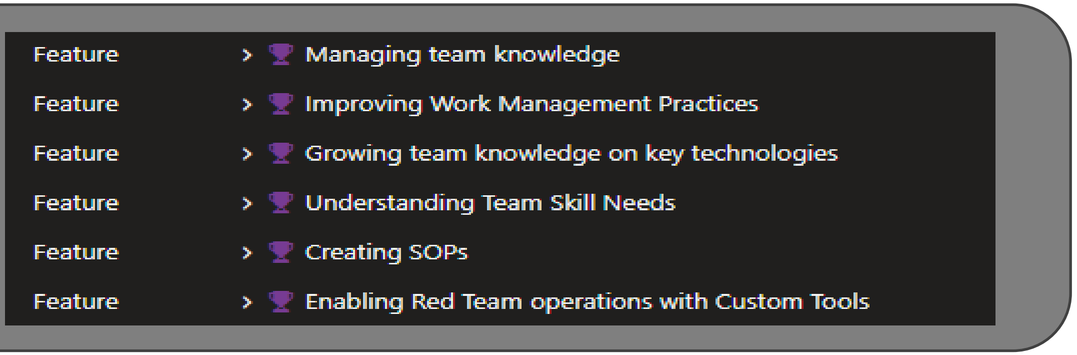
Delta Analysis and Friendly Arguing



G T Red Team uses an inconsistent location for source code, infrastructure configurations, documentation, or tools	The Red Team leverages a shared location, without version control, to house source code, infrastructure configurations, documentation, or tools	D G T e Red Team uses an industry-sta d code repository for source code, infrastructure configuration files, and these items are versioned	N B D J G T Red Team uses merge and pull requ or similar, prior to changing k n-good versions	D J T Red Team leverages automated CI/CD actions to expedite delivery and maintain quality of products
Licenses and accounts are only tracked upon reminder of expiration or renewal needs; ownership is dispersed across multiple people	N B G T erson tracks accounts, payment met s, or licenses; knowledge not avail e to the entire Red Team	J G T ccounts and licenses are centrally tr d, understood, and reviewed as nee d by the Red Team; Red Team account passwords are secured	N B J counts, licenses, and recurring exp es are reviewed quarterly for need or expiration	Tracking methods provide alerts or other easily identifiable information to indicate actions needed in the next thirty days

Build a Backlog





Feature > 🏆 Managing team knowledge

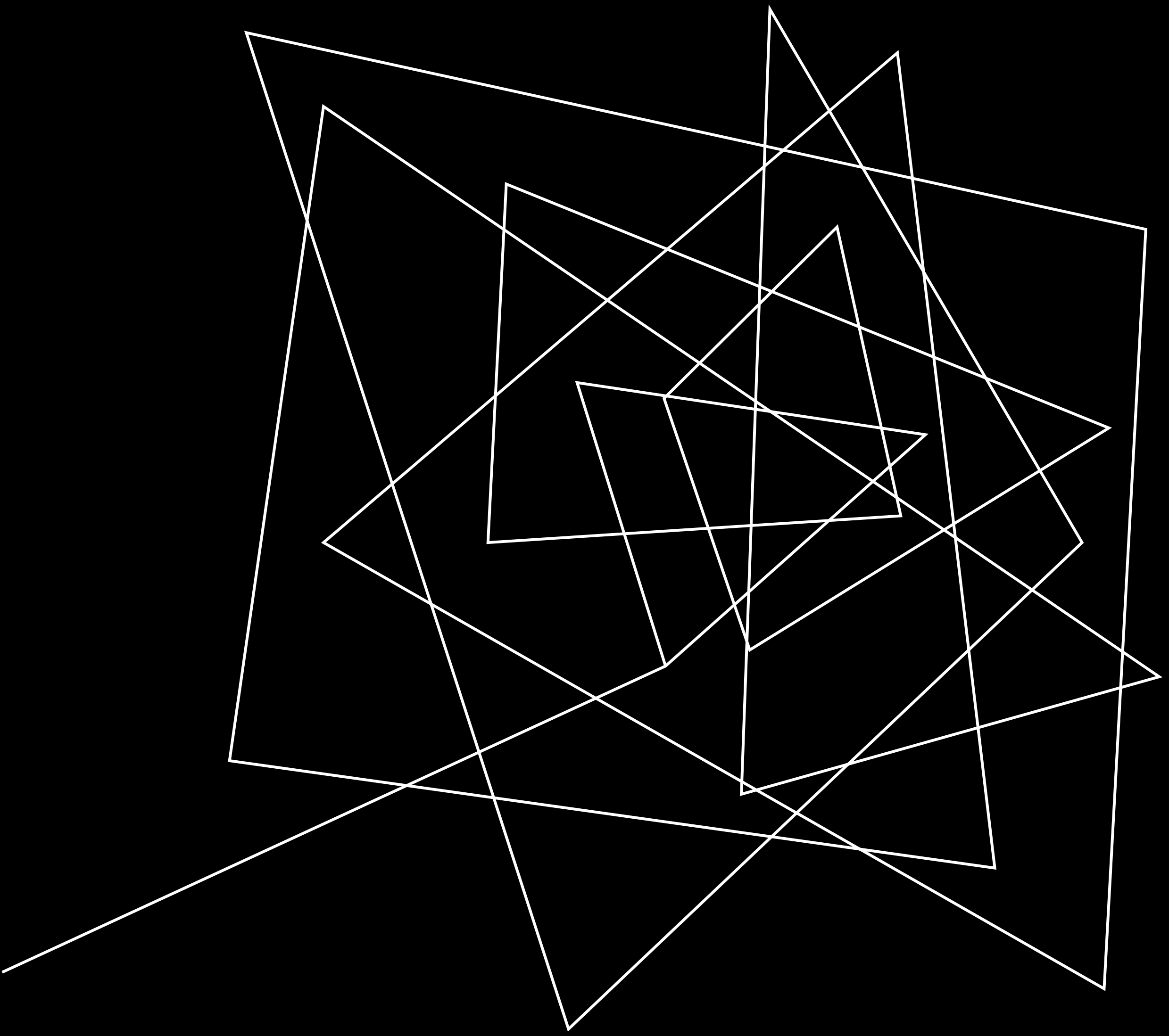
Feature > 🏆 Improving Work Management Practices

Feature > 🏆 Growing team knowledge on key technologies

Feature > 🏆 Understanding Team Skill Needs

Feature > 🏆 Creating SOPs

Feature > 🏆 Enabling Red Team operations with Custom Tools



SUMMARY AND THANKS

SUMMARY

New Resource — A new, community-owned Capability Maturity Model to plan for, and report on, Red Team maturity in a business-standard format

Where To Find It — The CMM can be found online at:

https://redteammaturity.com

How You Can Pitch In — We welcome contributions. Please view our GitHub page for guidance on submitting additions or modifications as well as to submit a change.

https://github.com/BCHarrell/redteamcmm

(also linked from the primary website)

WE WANT TO THANK THE FOLLOWING INDIVIDUALS FOR THEIR CONTRIBUTIONS TO THIS PROJECT AND ITS PREDECESSOR

NEW CONTRIBUTORS

Johann Rehberger

Red Team Director,
Electronic Arts

Andy Grant

Head of Offensive
Security, Zoom

Matthew Bjornstad

Principal Security
Engineer, Red Team,
Charter Communications

ORIGINAL CMM CONTRIBUTORS

Jordan Potti

Red Team Lead, Norton
Life Lock

Noah Potti

Senior Red Team
Operator, Bishop Fox

Trevin Edgeworth

Red Team Practice
Director, Bishop Fox

QUESTIONS?