How to “Successfully” Start and Lead a Purple Team Program

Methods Means Metrics

to Improve

Prevention Detection Response

Presenter:

Micah VanFossen

Who Am I

- 5 years in Cybersecurity
- Data / SIEM Engineer
  - Focused on data analysis and visibility, CTI, detections, threat hunting
- SIII US Cyber Games program
- Blog focused on SecOps https://purplevan.substack.com/
- TID Ecosystem project https://start.me/p/X25q7l/threat-informed-defense-ecosystem
- Average meme creator and mildly skilled AI critic

H2L SOLUTIONS

US CYBER GAMES
TRAIN. COMPETE. WIN.

startme

Content

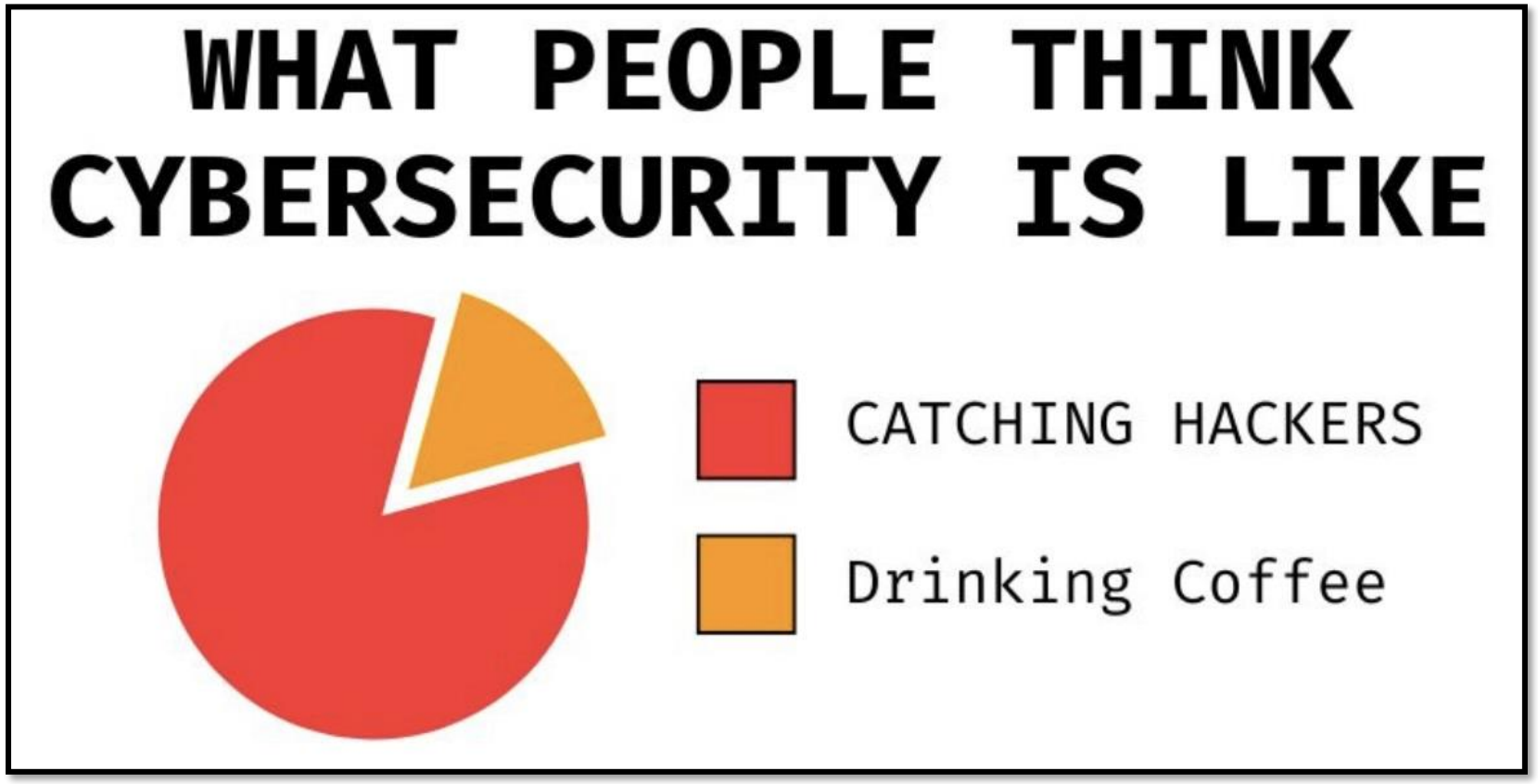
1. Why Purple Teams / Functions Are Needed
2. What Are They
3. How to Run a Purple Team Exercise
4. Maturity Levels of Purple Teams
5. Metrics to Measure Effectiveness / ROI

Why


!BREAKING NEWS!
EVERYTHING IS VULNERABLE,
AND ALL THE DATA IS BREACHED.
imgflip.com

We Walk a Lonely Road

Cyber defense is really **difficult…**

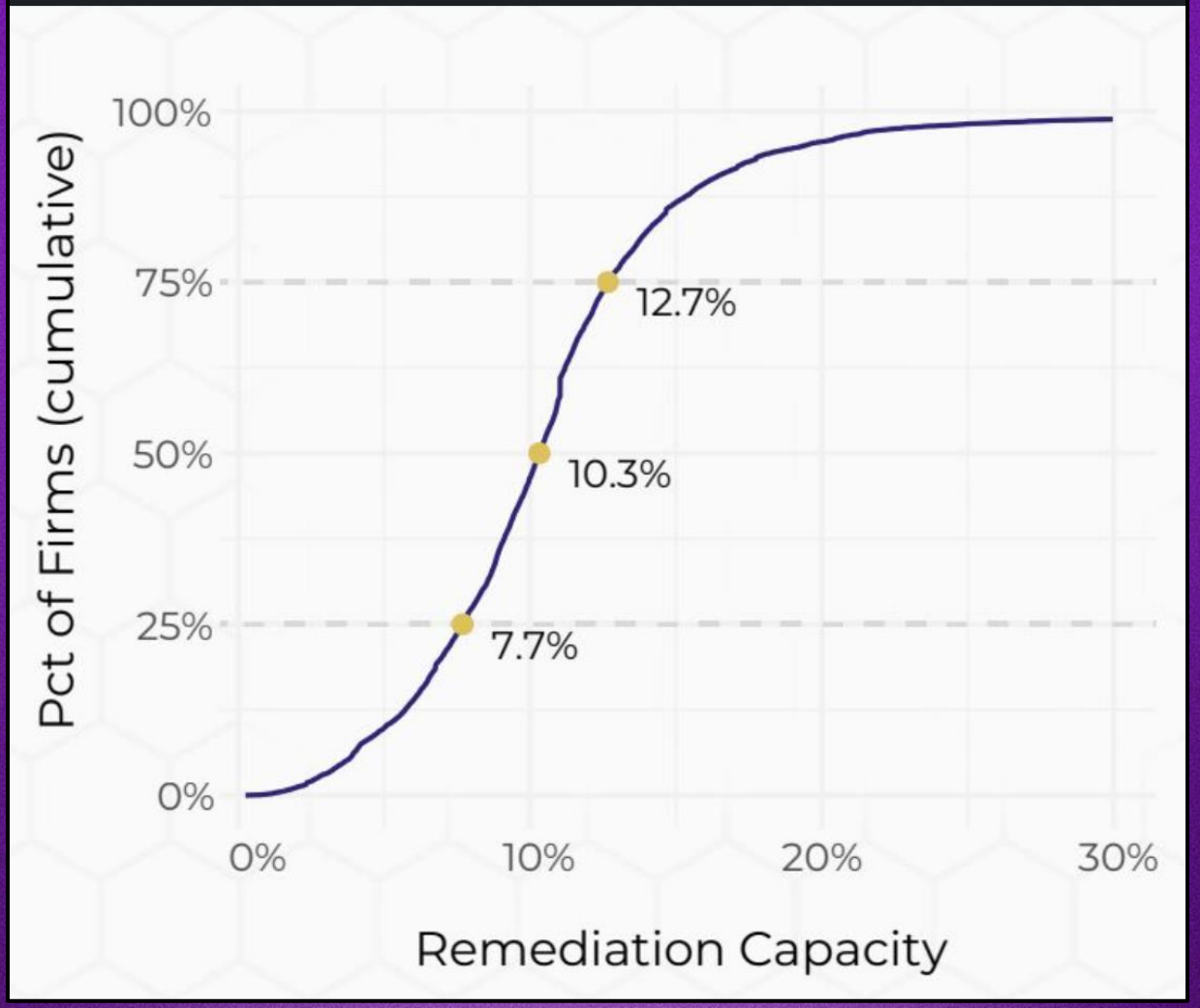


WHAT CYBERSECURITY IS ACTUALLY LIKE

- Security Awareness
- Patching
- Documentation
- Troubleshooting
- Unlocking accounts
- Meetings
- Compliance Assessments
- Incident Response
- Vendor Management
- Resetting Passwords

Spencer Alessi
Hacker | Pentester
Co-Host - Cyber Threat Perspective

*Graphic from the Security Scorecard / Cyentia Institute report "The Fast and the Frivolous" which shows the average percentage of vulnerabilities companies can fix each month (10.3% compared to the 58% most policies require).



https://library.cyentia.com/report/report_016087.html

Why Purple Team?

1. Stop impact with robust detection + rapid response
   - Deny easy attack vectors
   - Improve resilience
   - Inflict pain of change
2. Prioritization (patching, controls, time, $)
3. Gap identification
4. Train operators

Example: Vulnerability Prioritization

Patch all High & Critical (7.0 – 10.0) in 30 days?

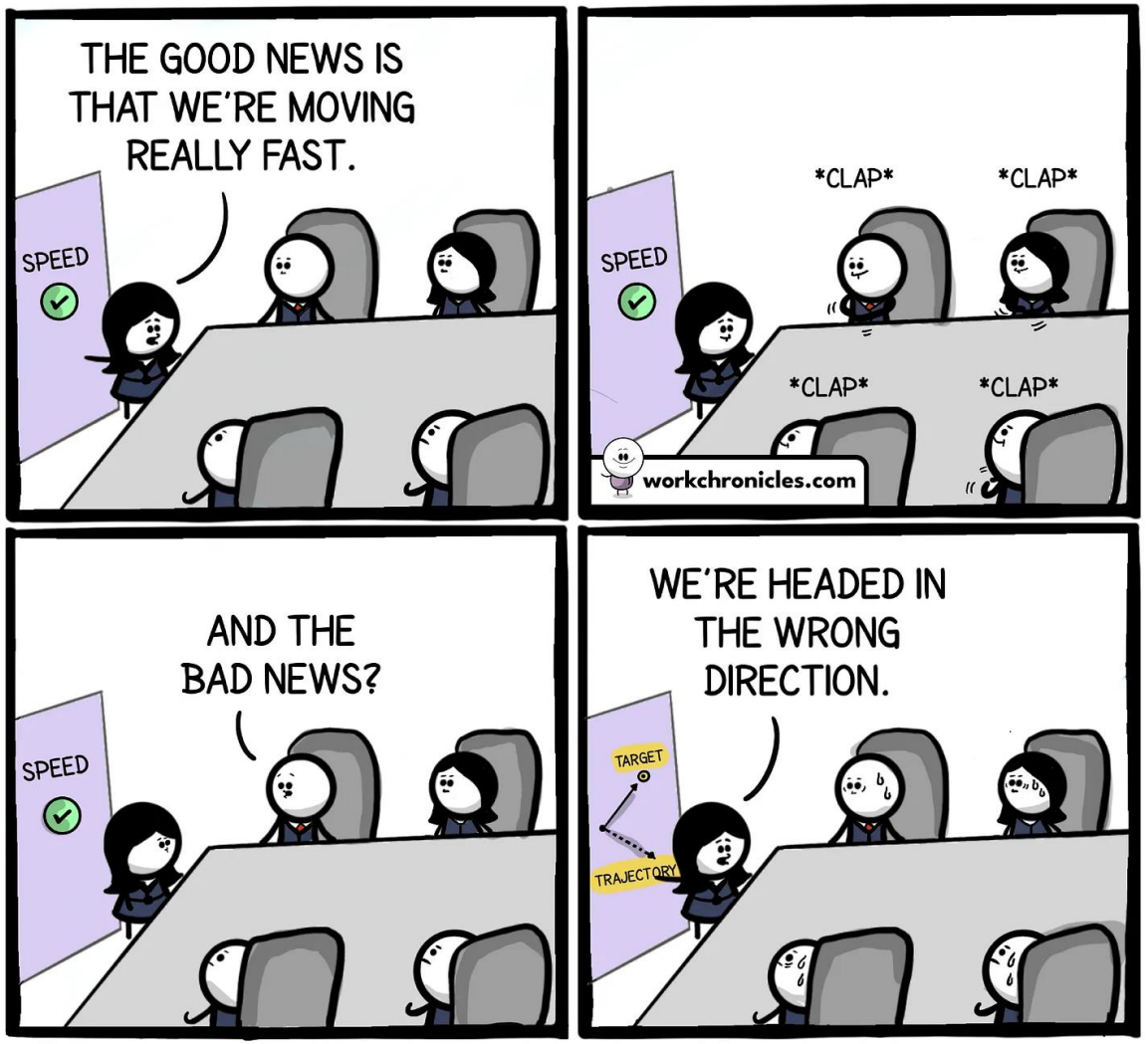
- 58% NVD - High or Critical
- Exploitable vulns get hit in hours
- CVE count is growing exponentially

Focus on Vulns that are:

- Being actively exploited in the wild, by actors known to target your org, industry, size
  - Likelihood and Impact of Exploitation
- Patch all others quarterly

Where's the Target?

- Our focus is misaligned
  - AI hype
  - Vendor FUD
  - Forgetting fundamentals
  - APTs!!!!



How Stop Bad Guys?

“When it comes to the HOW of so much adversary activity: focusing on exploiting vulnerable systems (and NOT with "zero days"), targeting users, buying access from infostealer networks, and similar… defenders have gone "all in" on advanced security mechanisms, while adversaries continue to thrive through subversion of security basic best practices.”

Joe Slowik MITRE ATT&CK Lead

https://www.linkedin.com/pulse/whats-old-new-again-joe-slowik-al2jc/

What Matters Most?

Survey for security executives…

“No competent person in security that I know - that is, working day-to-day cybersecurity as opposed to an institution dedicated to bleeding-edge research - cares about any of this. They're busy trying to work out if the firewalls are configured correctly, or if the organization is committing passwords to their repositories”

- Nihkil Suresh

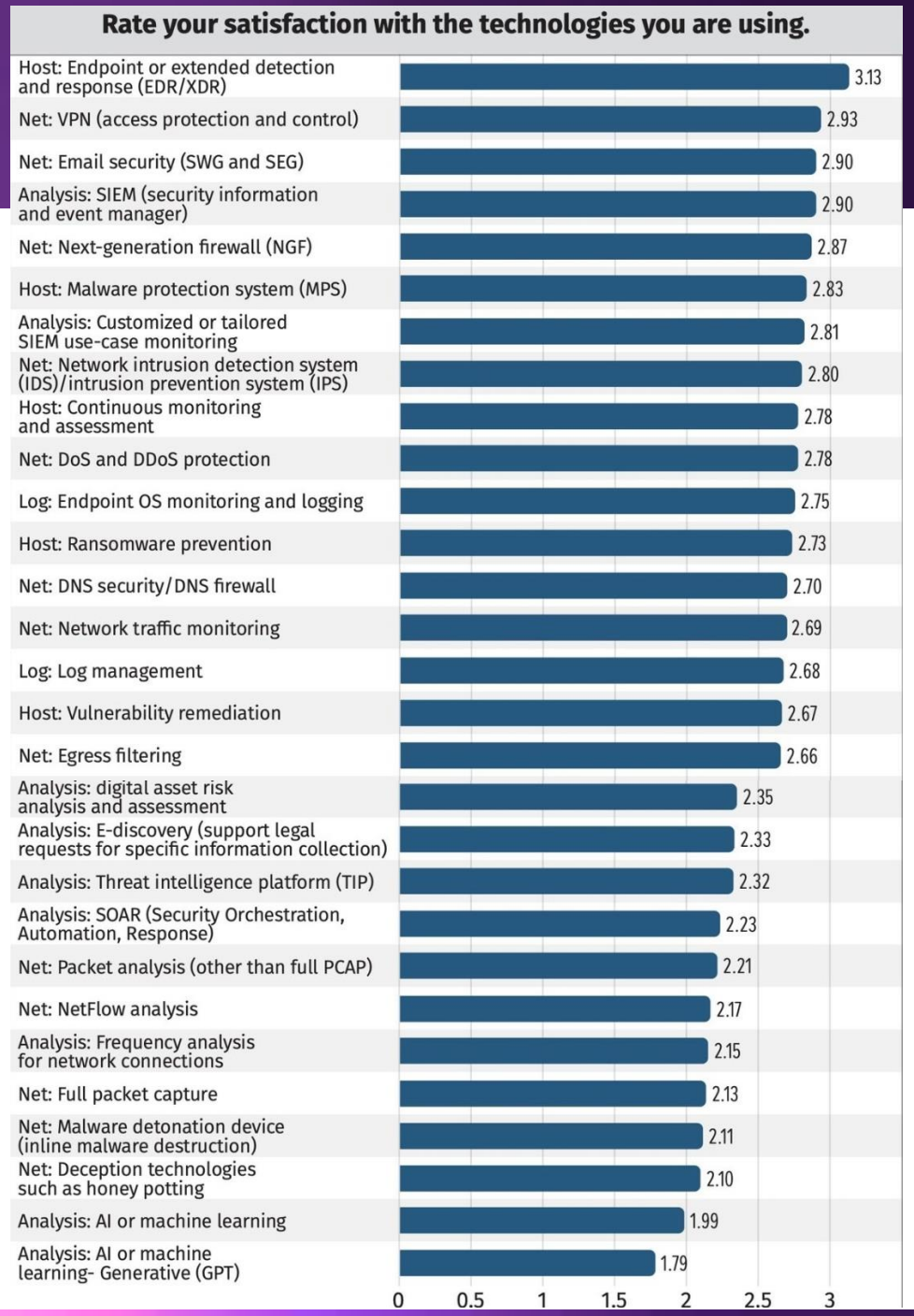
https://ludic.mataroa.blog/

AI To the Rescue?

Isn’t AI going to fix it…

SANS SOC Survey 2024 (different survey)

https://www.sans.org/white-papers/sans-2024-soc-survey-facing-top-challenges-security-operations/



What

Successful Programs = Leadership

- All successful programs start with leadership
- Set the
  - Culture
  - Mission
  - Vision
  - Resources

Culture – Who Are We?

Example - Multi-team group possessing various cybersecurity and organization specific skill sets working collectively

Seek integration & collaboration, not a siloed team

Mission – What Do We Do?

Example - Utilize continuous collaboration to test people, processes, and technology (controls) against relevant attack methods

Test to improve, not to shame or hand slap

Vision – Define OUR successful program?

Example - Improve organizational cyber defense resilience through gap identification and validated prevention, detection, and response

The more specific, the better the odds of reaching it

Resources – What is Needed?

- Examples
  - People (defenders, attackers, CTI, sysadmins, managers)
  - Visibility - Logs from endpoint / host, network, identity
  - Intel collection and operationalization
  - Defensive controls
  - Testing capability
- All about people, processes, data (not just technology)

People Matter

- Cyber has a fixation on tools, tech, and shiny new things
- The MOST important thing to a successful program is people
- “The secret to Special Forces is intensive, ceaseless, meticulous training and preparation. The quality of your operators matters far more than the equipment.” - Simon Jeffries, Ex-Special Forces
- Skills, training, and preparation is key
- People and processes will win out over time

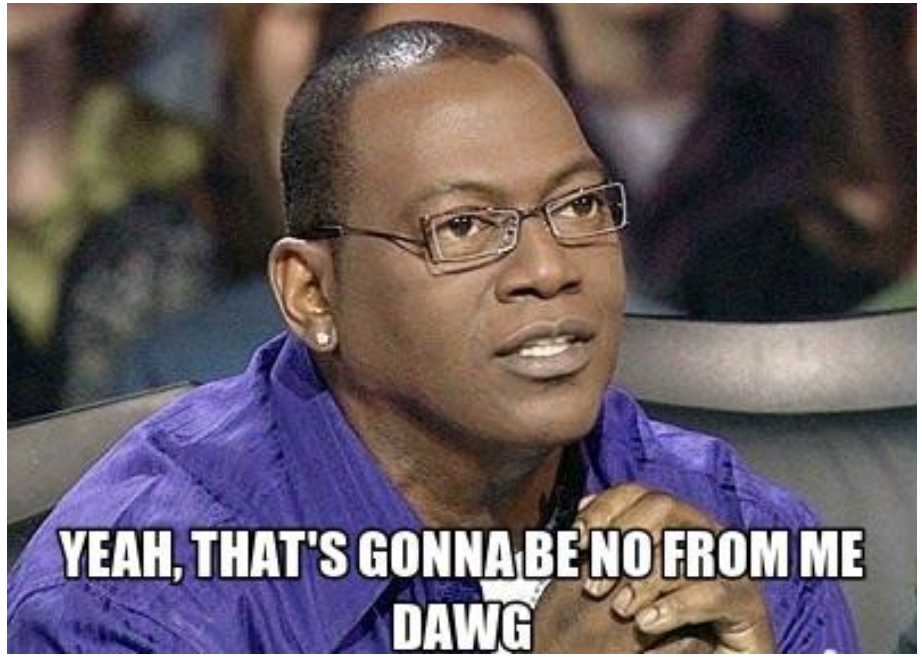
What is a Purple Team Program?

The collaboration of relevant multi-team members and skills working together that continuously test people, processes, and technology controls against relevant attack methods to improve organizational cyber defense resilience through gap identification and validated protection, detection, and response. This function is accomplished through utilization of people, environment visibility, intel, defensive controls and a testing capability.

Culture Mission Vision Resources

Poor Purple Teams

- A siloed group that functions alone
- Don’t track metrics
- Don’t provide actionable recommendations
- Just a vulnerability assessment
- Require internal red / CTI teams
- Require elite expertise of every cybersecurity domain



How

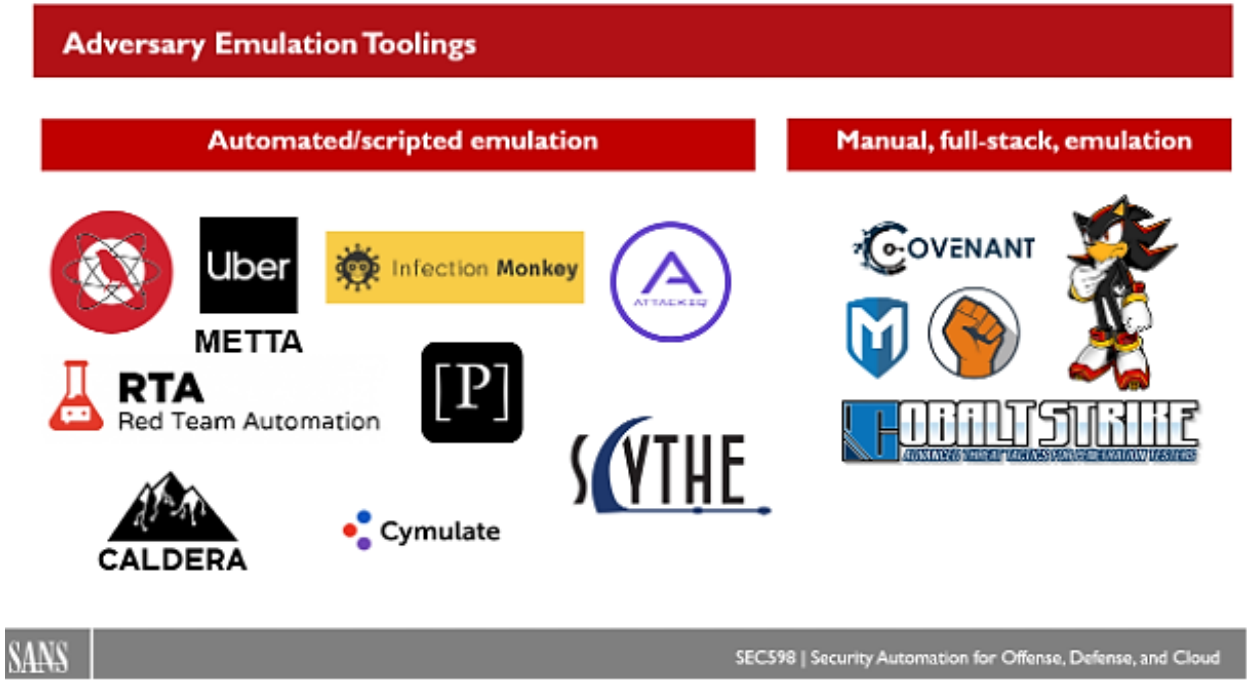
Prerequisites To Purple

Must have's

- **People** with dedicated functions for purple teaming
- Some Security / IT maturity
- Logs – SIEM / Query capability
- Detection (defend) capability – EDR/SIEM
- Testing (attack) capability – Manual or Automated
- Identified attack chain(s) or atomic TTPs

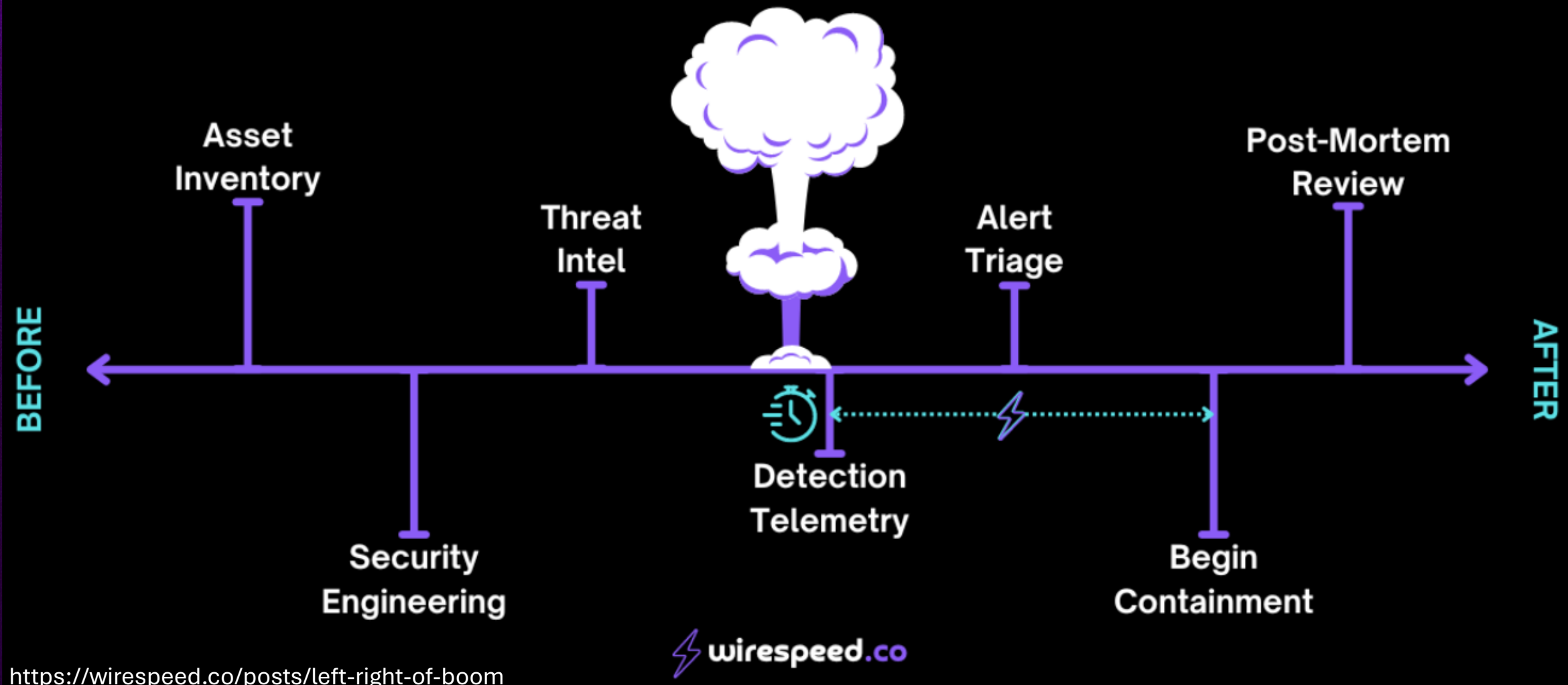
Nice to have's

- Threat Model
- Blue team workflows / SOPs
- Separate attack / defense teams



Jeroen Vandeleur: https://www.sans.org/blog/continuous-purple-teaming-practical-approach-strengthening-offensive-capabilities/

LEFT & RIGHT OF BOOM



https://wirespeed.co/posts/left-right-of-boom

Where We Are Headed

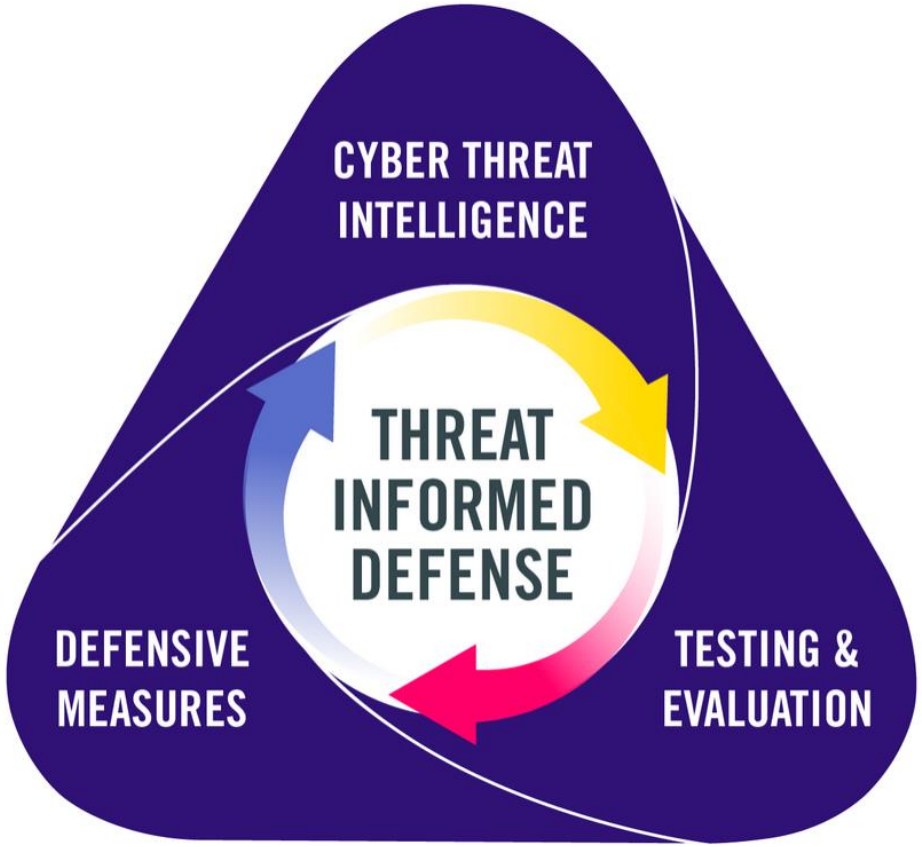
Threat Informed Defense - align defensive measures to real-world observations of adversary tradecraft

Cyber Threat Intel – Know the Adversary & Self

- Know the adversary, their objectives, behaviors, and their tactics/techniques/procedures (TTPs)
- Identify and prioritize most likely threats

- **Testing and Evaluation** – Learn and Improve
  - Assess defenses by emulating real adversary TTPs
  - Continuous validation of security controls with threat-led attack simulations of prioritized threats

- **Defense Measures** – Proactively Defend
  - Implement prevention, detection, and mitigation tailored to known threats based on data-driven analysis
  - Evolve defenses as environment and threats change



https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/threat-informed-defense/

Stages to TID

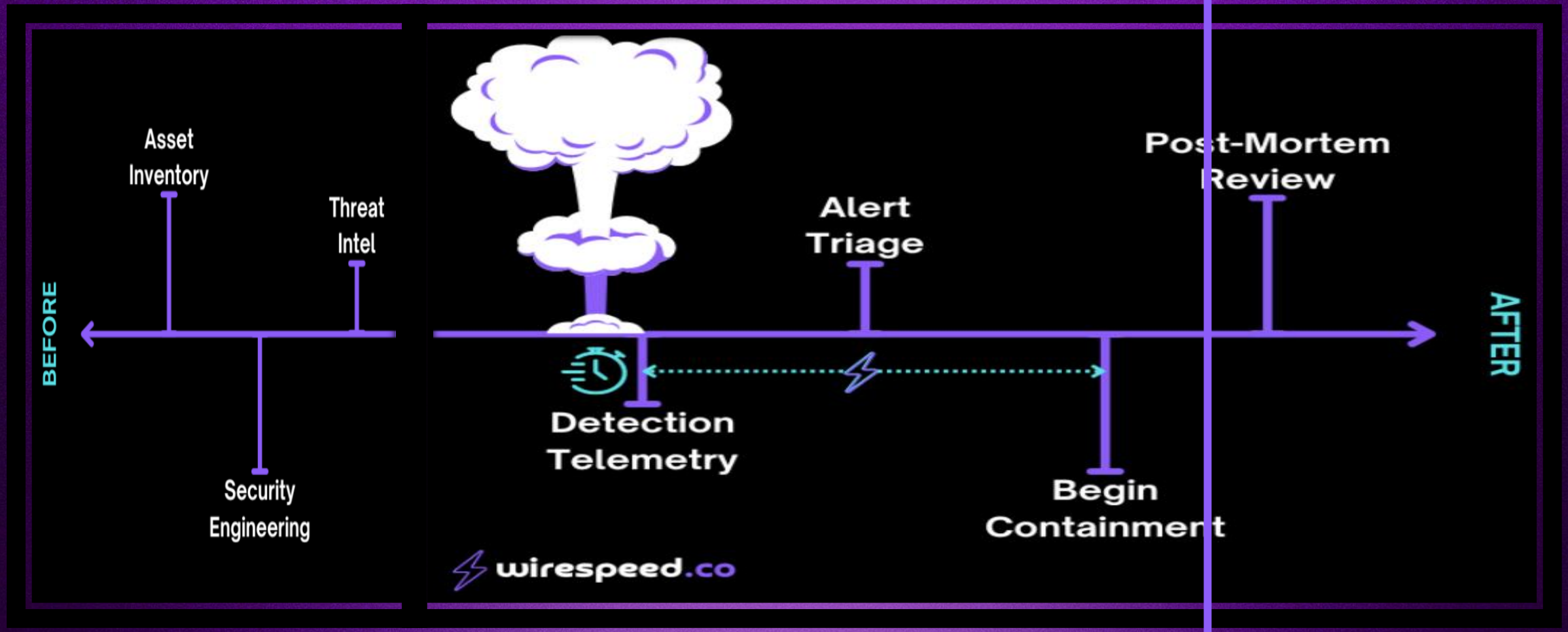
3. Threat-centric defenses: detection, triage, response

2. Threat-informed defenses: some prevention, etc

1. Threat-agnostic defenses / hygiene / “the basics” [no threat awareness]

https://medium.com/mitre-engenuity/threat-informed-defense-is-hard-so-we-are-still-not-doing-it-31ae7b68955f

Prevention - Time you can resist attack

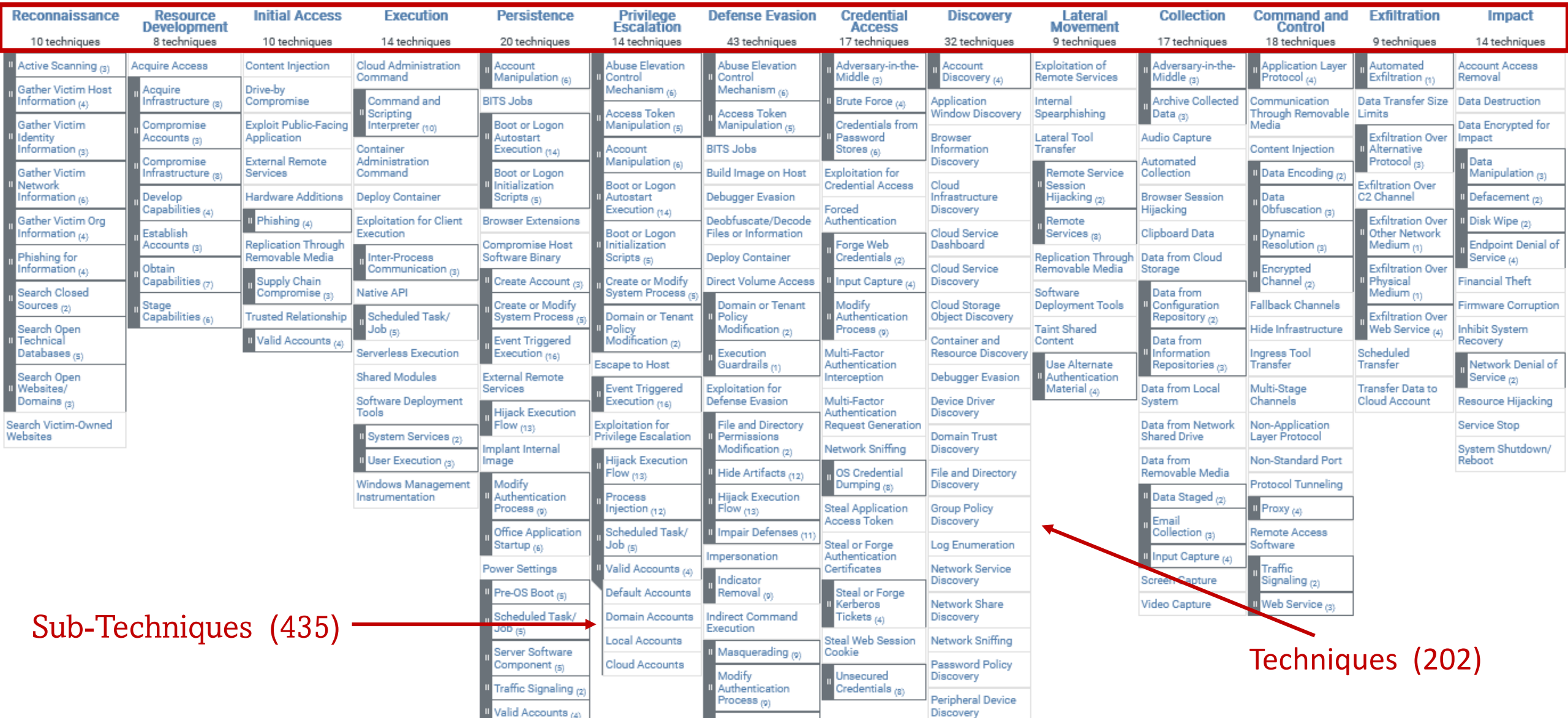


Detection

Response

ATT&CK Enterprise Matrix

Tactics (14)



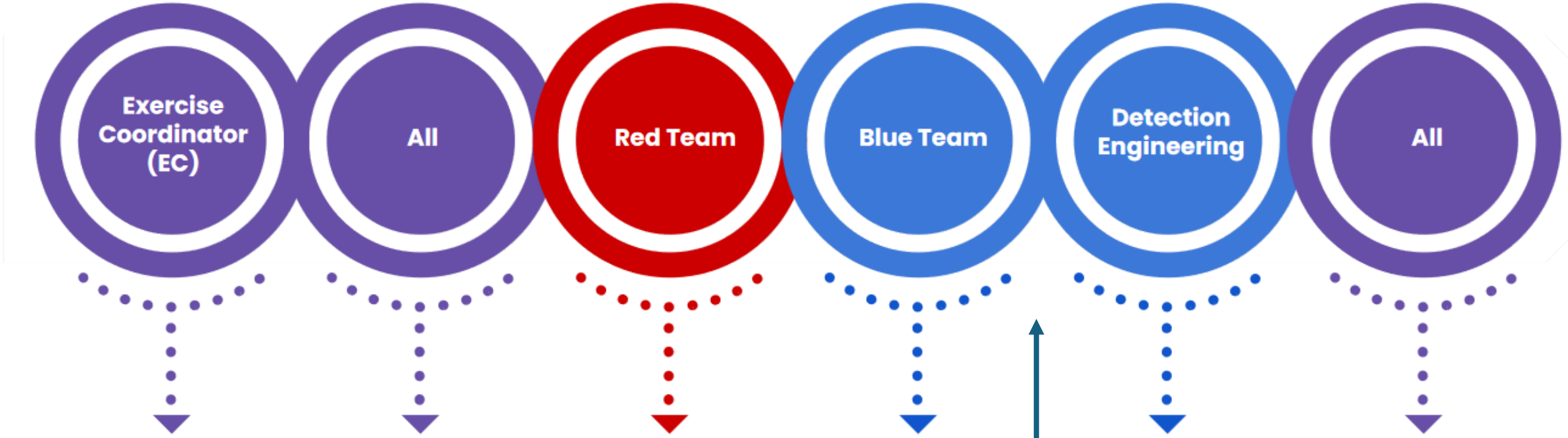
Sub-Techniques (435)

Techniques (202)

Purple Teaming – 1000 ft (CADD)

- CTI
  - Gather intel on something to test
- Attack
  - Emulate the TTP in your environment
- Detect
  - Review/add detections, reduce noise
- Defend
  - Implement/adjust defenses, harden systems, modify permissions, etc.

Purple Team Exercise – 2 right feet



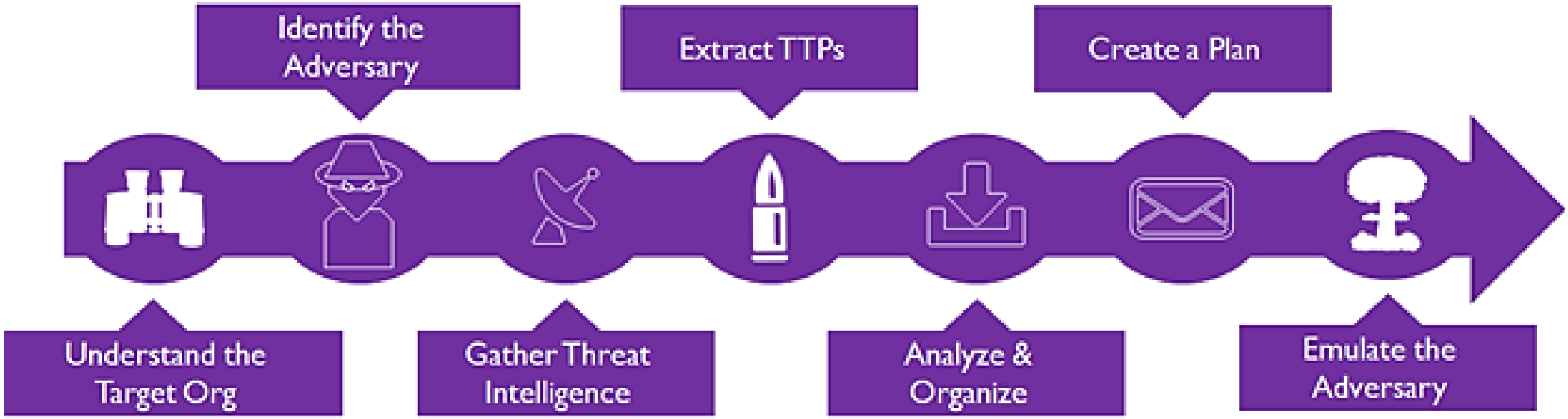
https://github.com/scythe-io/purple-team-exercise-framework/blob/master/PTEFv3.md

CTI – The “So What?”

Purpose: Utilize evidence-based knowledge, context, indicators, capabilities, and behaviors of a threat to assess how that may affect the organization

- “A Red Team can try thousands of methods to reach an objective, a Purple Team will focus on the methods, tradecraft, and TTPs that are most likely to impact the organization” – PTEF
- Goals:
  1. Collect data
  2. Conduct analysis
  3. Influence security decisions with data (now it’s “intel”)
  4. Disseminate proactive and actionable intelligence
  5. Don’t be a news/IOC feed

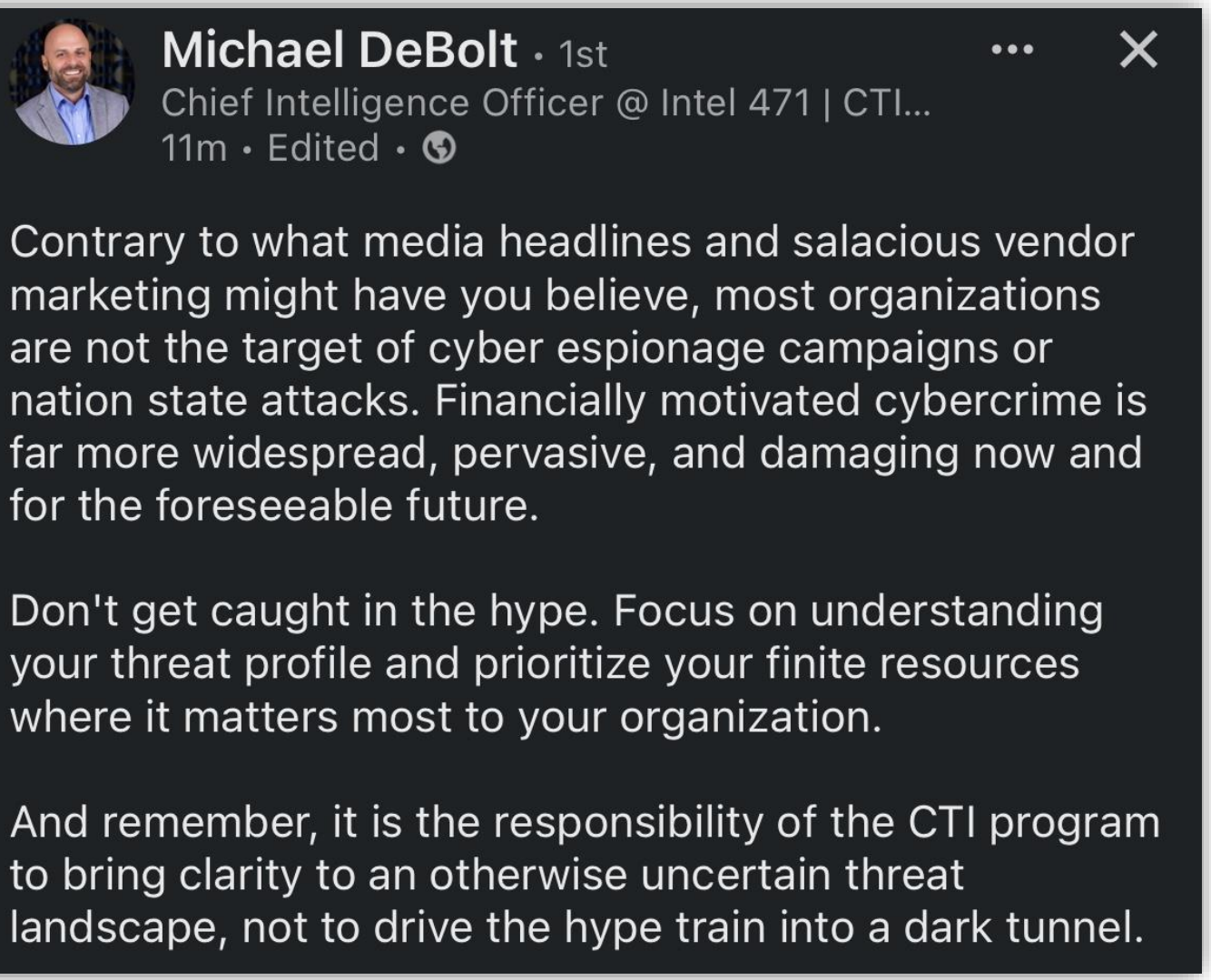
CTI/Testing Workflow



Katie Nickels and Cody Thomas presentation: "ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK"

Questions to Ask CTI

- What threat actors commonly target my industry or size? (Intent)
- What tactics, techniques, & procedures are used by these groups? (Capability)
- What are our business-critical functions, information, and systems that we must protect? (Crown Jewels)



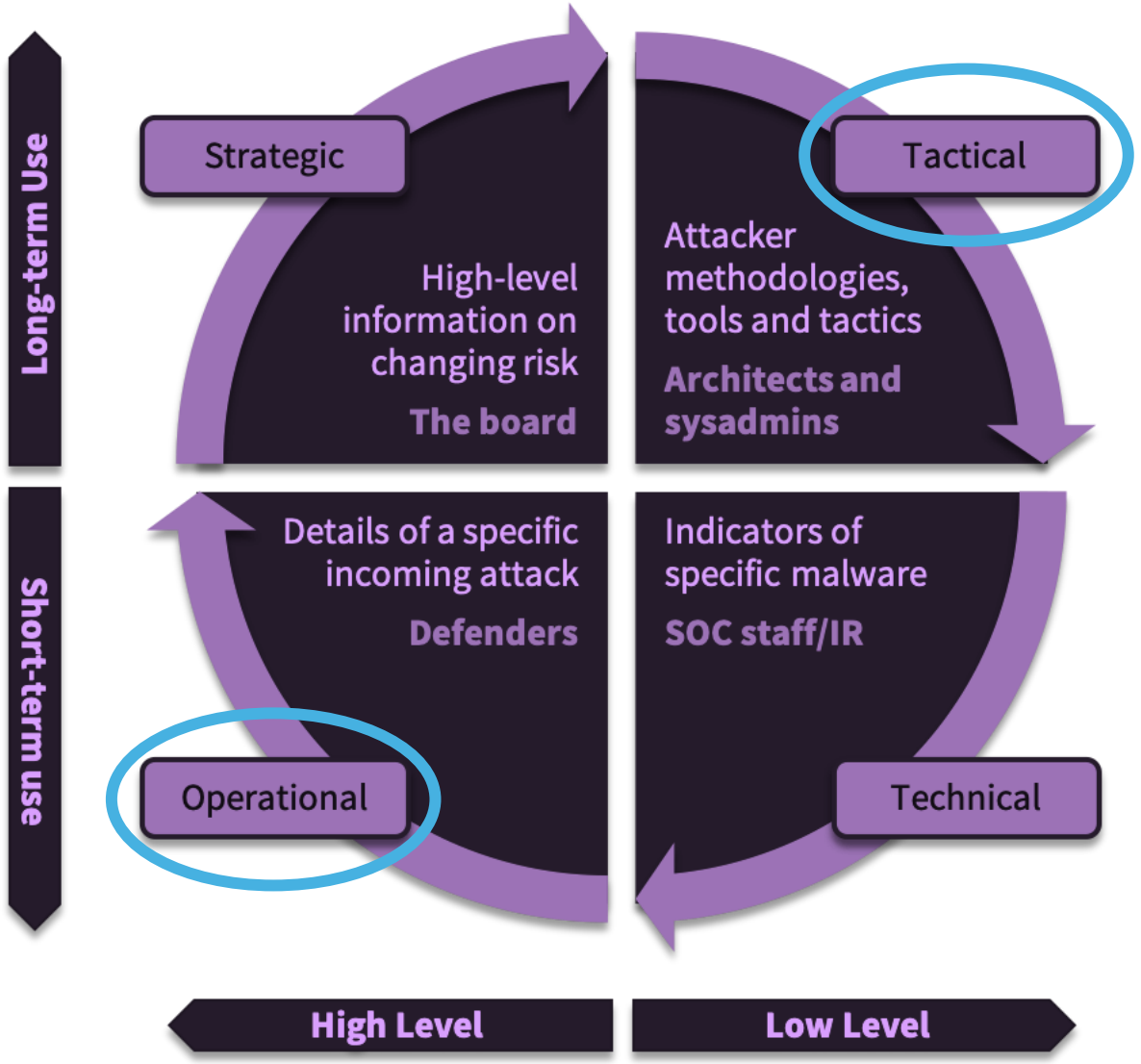
Michael DeBolt · 1st
Chief Intelligence Officer @ Intel 471 | CTI...
11m · Edited ·

Contrary to what media headlines and salacious vendor marketing might have you believe, most organizations are not the target of cyber espionage campaigns or nation state attacks. Financially motivated cybercrime is far more widespread, pervasive, and damaging now and for the foreseeable future.

Don't get caught in the hype. Focus on understanding your threat profile and prioritize your finite resources where it matters most to your organization.

And remember, it is the responsibility of the CTI program to bring clarity to an otherwise uncertain threat landscape, not to drive the hype train into a dark tunnel.

What CTI?



https://www.securnite.com/index.php/onepress_service/cyber-threat-intelligence/

Good CTI Resources

What?

- Threat Actor Reports
- DFIR / Campaign Reports
- Annual Trends
- Feedly, Start.me - RSS feeds

Storage – TIP

- OpenCTI FREE
- MISP FREE
- Flashpoint
- Recorded Future

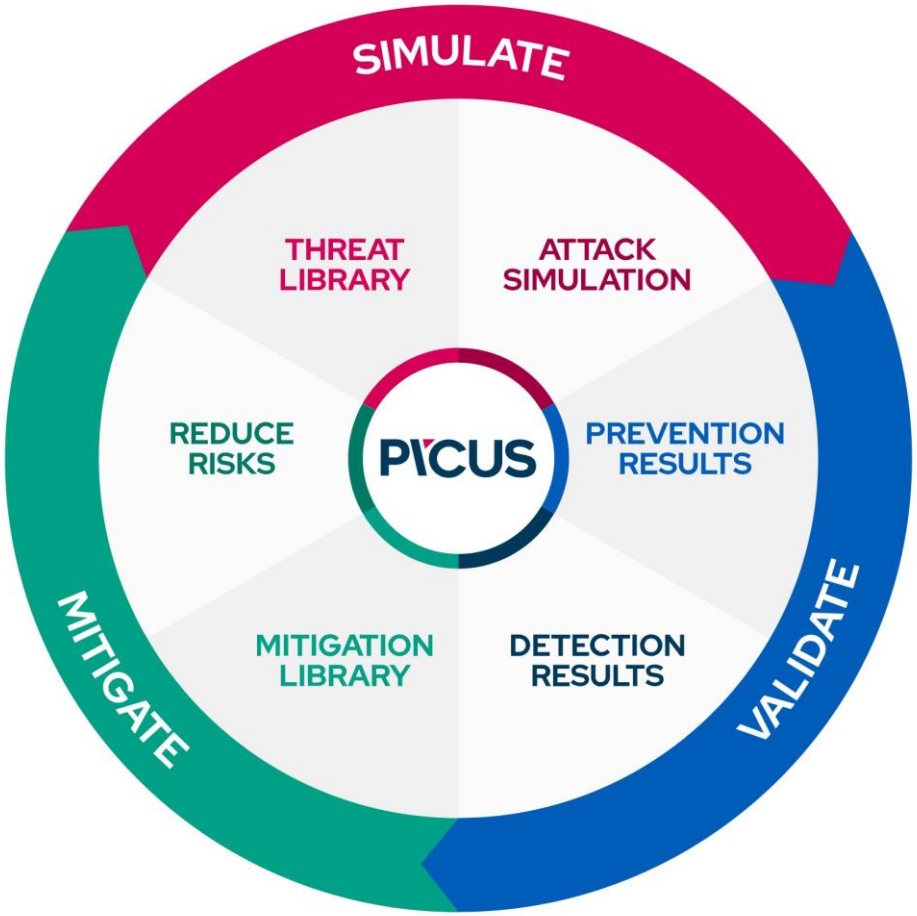
From FREE

- CISA / FBI / Joint Alerts/Advisories
- MITRE ATT&CK
- DFIR Report
- Palo Alto Unit 42
- TrustedSec
- Google T.A.G
- CrowdStrike
- Huntress
- Red Canary
- Recorded Future
- Intel 471
- Zero Fox

Testing/BAS – What Would Happen If?

Purpose - To simulate the behavior a threat would likely conduct in our environment to achieve objectives

- Attempt to emulate TTPs in each group:
  - Not prevented (otherwise it's already covered)
  - Logged / Visible (if not visible, can we add a source?)
  - Detected
  - Alerted



https://abes.com.br/en/clm-e-picus-analisam-as-cinco-principais-ciberameacas-que-surgiram-em-julho/

Testing/BAS Questions & Resources

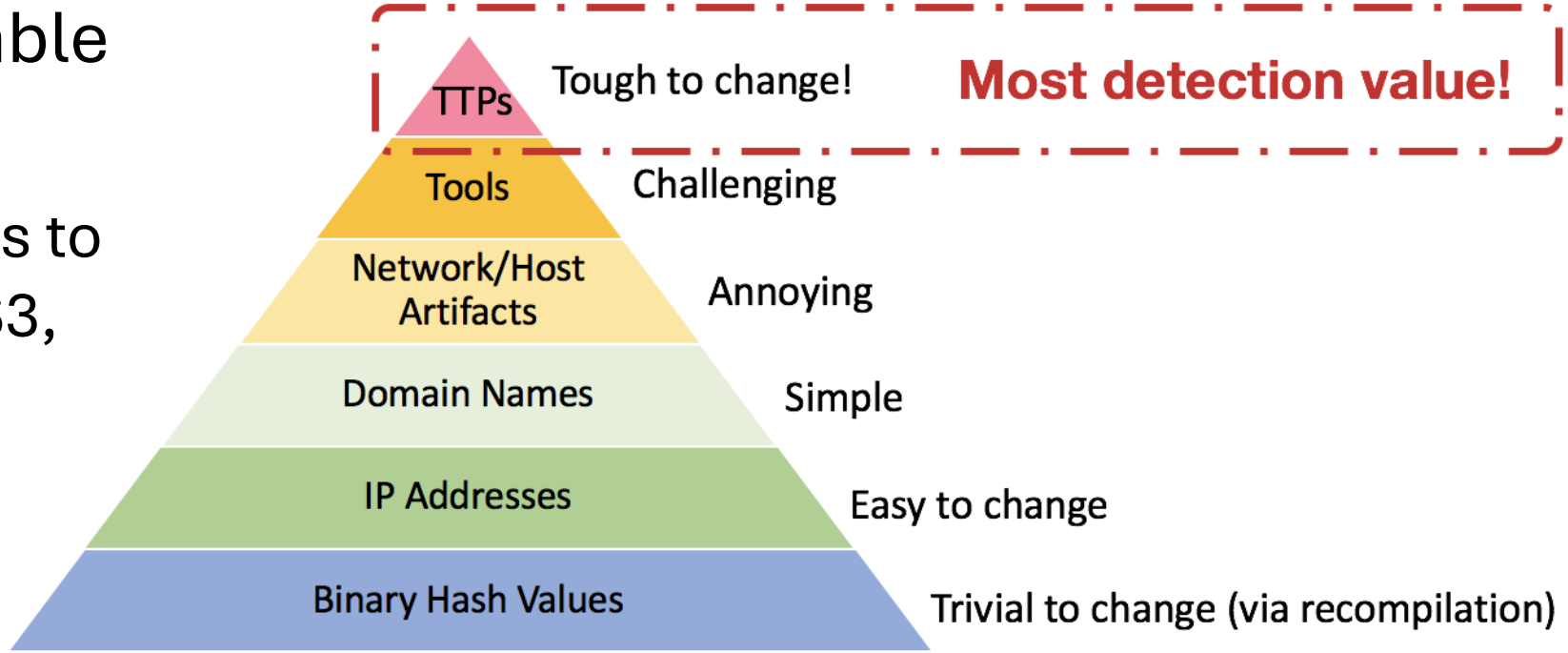
- What procedural variance could an adversary use to circumvent our detections?
- What detections work / have been validated?
- What controls do we currently have?
- Are we missing any test coverage?

- CALDERA FREE
- OpenBAS FREE
- Atomic Red Team FREE
- Stratus Red Team FREE
- C2 Matrix FREE
- Attack Range Splunk FREE
- AttackIQ
- SCYTHE
- Prelude
- Picus
- FourCore
- PlexTrac

Detection – I Spy With Log

Purpose - To detect suspicious events that may be indicative of malicious actors

- Detect *behaviors* with low variance
- Log forensic valuable items to SIEM
  - Send all other logs to cheap storage – S3, Azure Blob, etc



https://redcanary.com/blog/security-operations/detection-engineering/

David Bianco: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

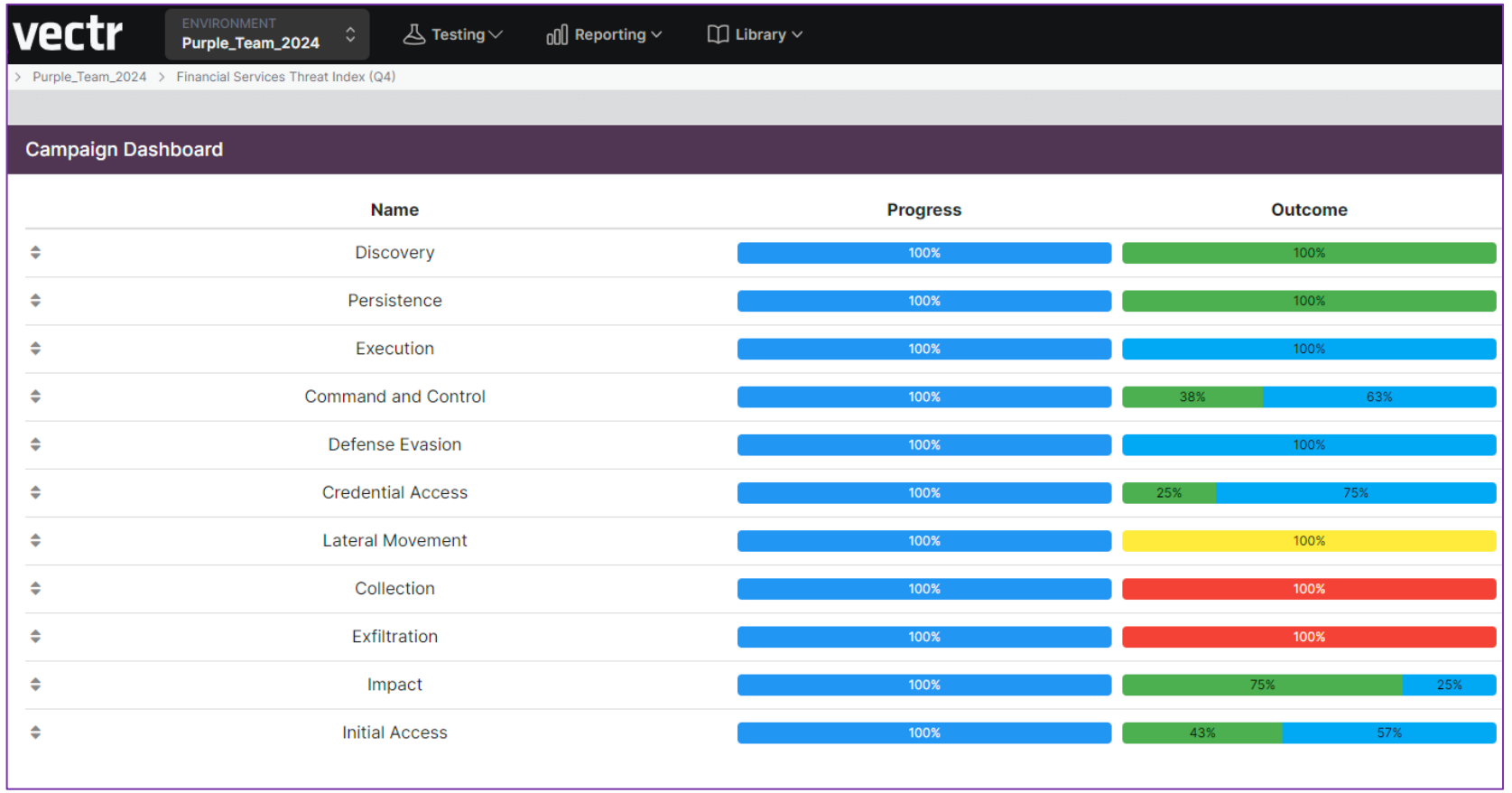
Detection Questions & Resources

- What log and telemetry data sources do we have?
- Are we lacking any visibility?
- What is the process for creating detections and/or alerts?
- Do we have visibility/logs for the TTPs conducted?
- Were there any alerts?
- What were the responses by the team?
- Were responses appropriate?

- SIGMA FREE
- LOLBAS FREE
- Chainsaw FREE
- DeTT&CT FREE
- Splunk Detections FREE
- Elastic Detections FREE
- SnapAttack FREE
- Impede FREE
- SOC Prime FREE
- TIDAL Cyber FREE

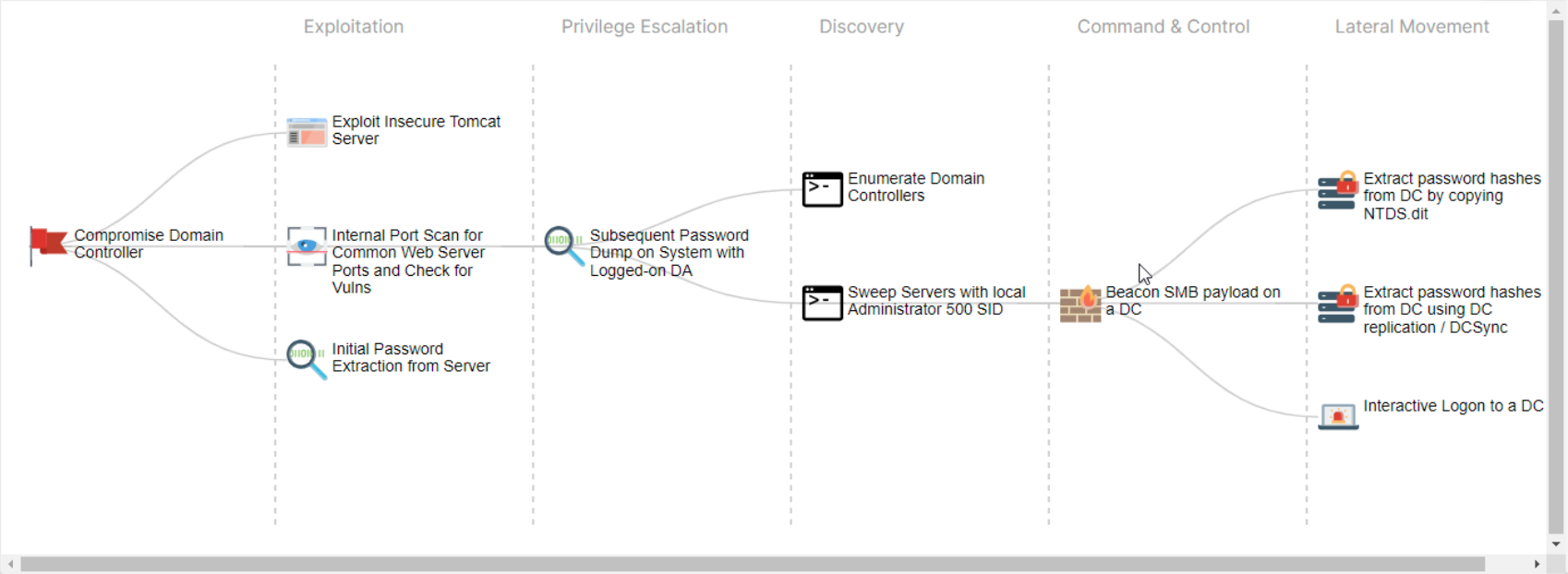
Purple Platform - Vectr

- Community and Enterprise
- Tracking of purple team and adversary testing program
- Measure threat resilience gaps and success
- View / compare assessment results
- Automated adversary simulation
- ATT&CK mapping
- https://vectr.io/



Compromise Domain Controller: Escalation Path

PNG



Timeline

01/05/2024 10:14:58
Internal Port Scan for Common Web Server Ports and Check for Vulns : status changed to Completed

01/05/2024 10:14:58
Exploit Insecure Tomcat Server : status changed to Completed

01/05/2024 10:14:58
Initial Password Extraction from Server : status changed to Completed

01/05/2024 10:14:58
Beacon SMB payload on a DC : status changed to Completed

01/05/2024 10:14:58
Enumerate Domain Controllers : status changed to Completed

01/05/2024 10:14:58
Subsequent Password Dump on System with

Test Cases

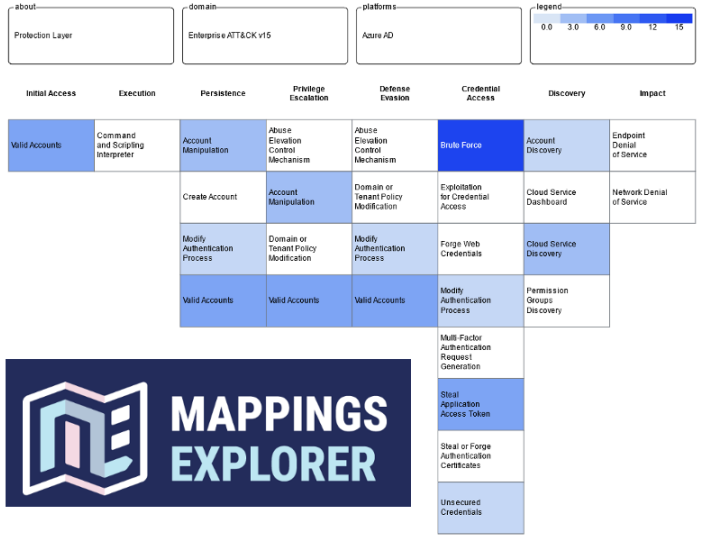
CAMPAIGN ACTIONS

Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	search ...	search ...	All	All	All	
Lateral Movement	Compromise a DC	Extract password hashes from DC by copying NTDS.dit	Completed	Not Alerted	Content Dev	
Discovery	Windows Domain Enumeration	Enumerate Domain Controllers	Completed	None	Content Dev	
Lateral Movement	Compromise a DC	Extract password hashes from DC using DC replication / DCSync	Completed	None	Engineering, Top Fix	
Exploitation	Web Server Compromise	Exploit Insecure Tomcat Server	Completed	None	Engineering, Top Fix	

ATT&CK Mapping

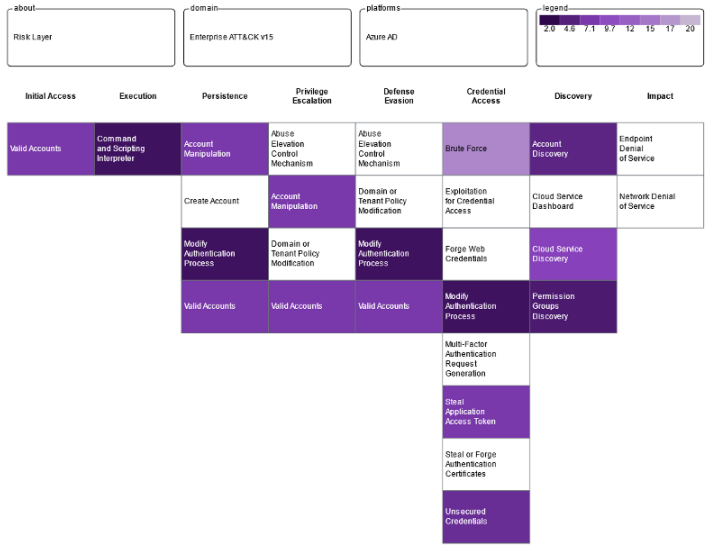
Threat

Defense



MAPPINGS EXPLORER

Risk



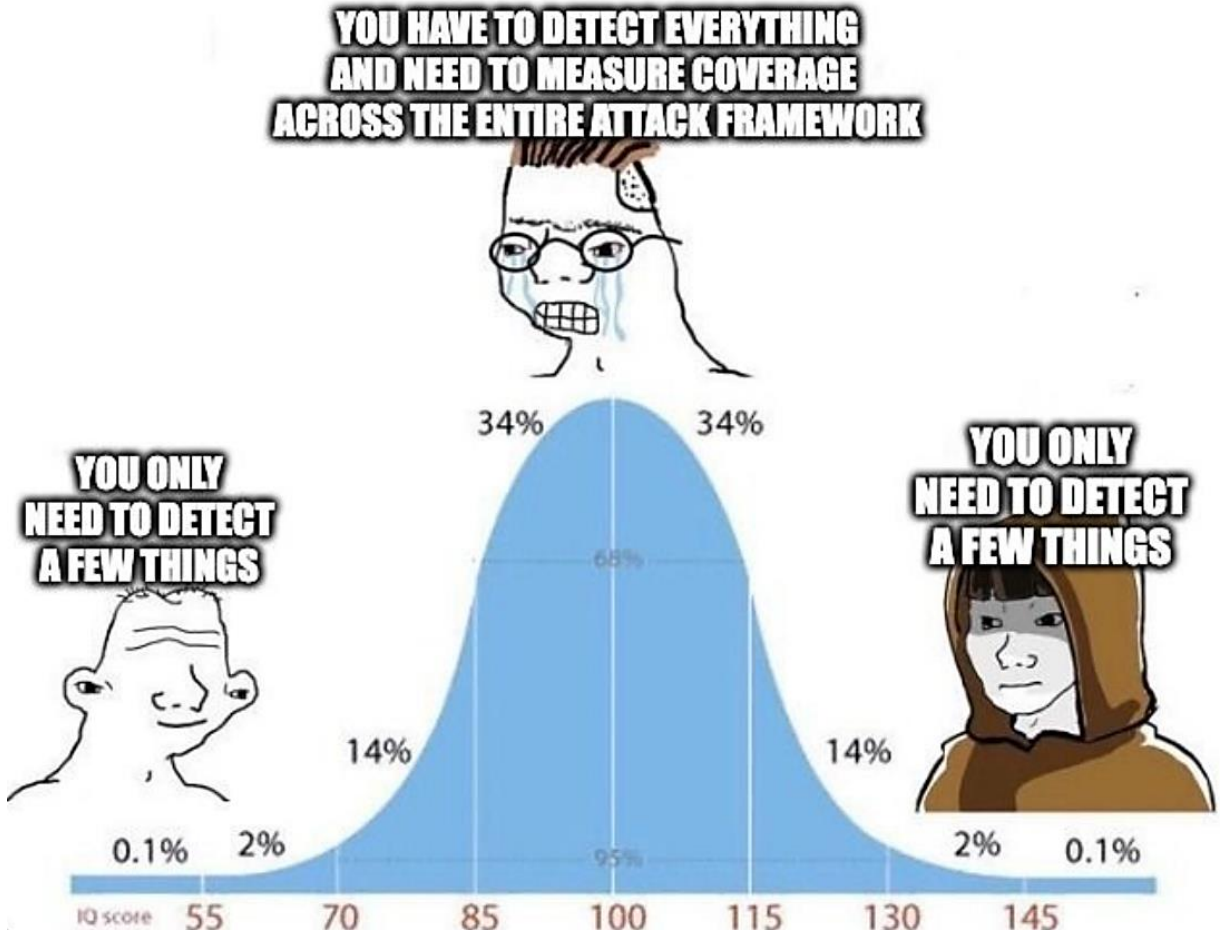
Mission Decomposition | System Decomposition | Vulnerability Identification | Cyber Threat Intelligence | **Defense & Risk Analysis** | **Mitigation & Remediation** | Monitoring Analysis & Evaluation

THREAT MODELING WITH ATT&CK

https://medium.com/mitre-engenuity/turn-your-threat-model-to-supermodel-with-att-ck-a6dfaa6787c2

ATT&CK Map the Right Way

- Detect important things
- Don’t play bingo with ATT&CK
  - You’ll never fully cover T1071.001 App Layer Protocol - Web Protocols
- Map to find holes and close clear visibility gaps, not to get all ‘green’ boxes

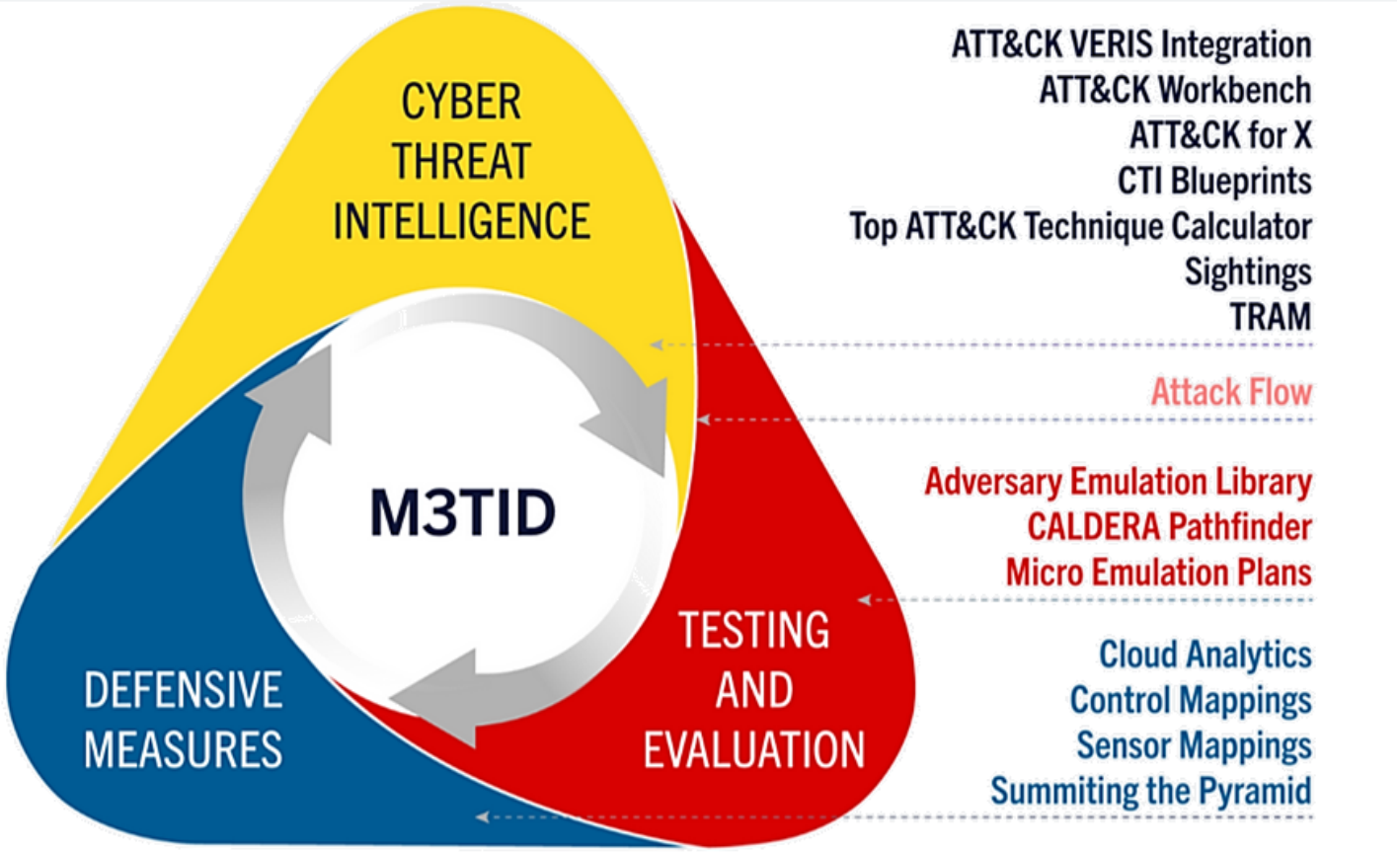


Josh Liburdi – Linkedin

Free CTID Tools

Tools that can assist: FREE

- ATT&CK Navigator
- Mappings Explorer
- Top ATT&CK Techniques Calculator
- CALDERA
- CTI Blueprints
- ATT&CK Workbench
- TRAM
- Micro Emulation Plans
- Technique Inference Engine
- Threat Model with ATT&CK



MITRE ENGENUITY | Center for Threat Informed Defense

Center for Threat Informed Defense projects: https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/

Learning Resources

- ATT&CK training FREE
- AttackIQ Academy FREE
- Picus Purple Academy FREE
- Antisyphon Training
- MAD ATT&CK Certifications
- Level Effect

Purple Maturity

Direction

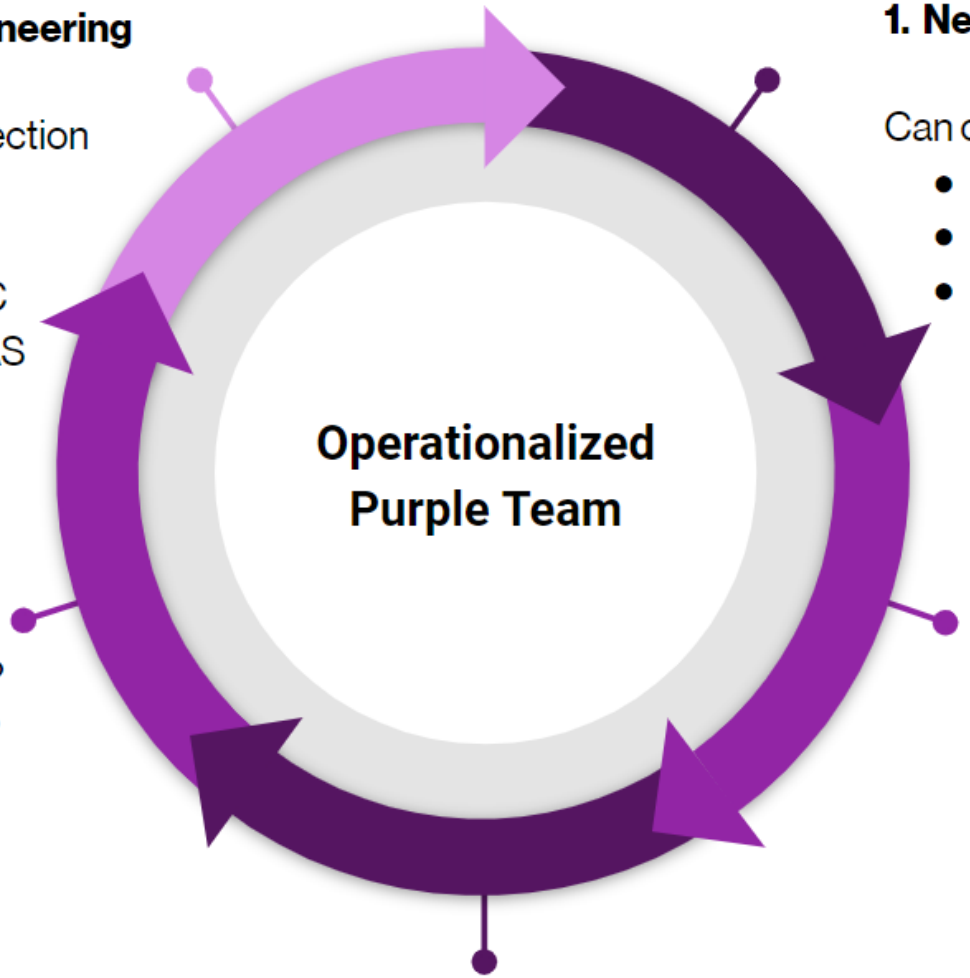
To get anywhere, you must first know where you are and decide where you want to be

Purple Team Maturity Levels

1. One Time Engagement
   - Give it a try one time
2. Ad-Hoc Exercises
   - Can perform this capability but takes time to spin up
   - Requires moving people or resources from other workflows
   - Varied success rates
3. Regular Exercises
   - Regularly meets the need based on current volume of having to deploy this capability
   - Success rate is a reasonable level
   - Not viewed as a strain on operations to deploy this capability
4. Continuous Purple Teaming
   - Operationalized effort, performs capability quite often or with near 100% success rates
   - Someone or something (tech) is designed to operate this workflow as a primary responsibility
   - The environment is set up so that using this capability is second nature

Bullets 2-4 maturity definitions from
Max Rogers Sr Director SOC @ Huntress

Purple Team Program



1. New Adversary Behavior/TTP

Can come from anyone:

- CTI
- Red Team
- Blue Team

2. Analyze & Organize

- Extract TTPs
- Were these already tested?
- Is there coverage?

3. Red Team Emulation

Do the TTPs work here?

4. Blue Team Result

- Was there an Alert?
- Is there Telemetry?
- Can we Threat Hunt?

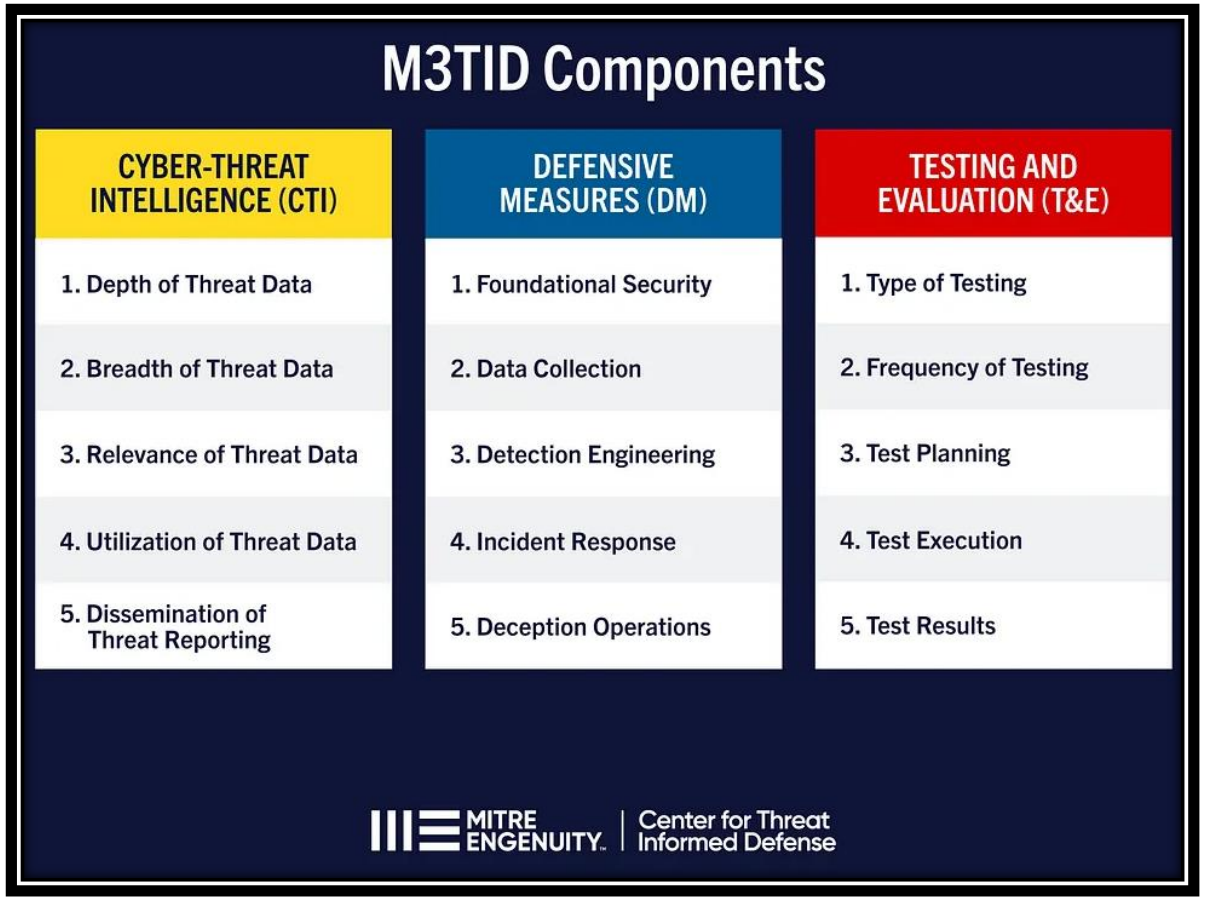
5. Detection Engineering

- Build Detection
- Deploy
- Tune
- Train SOC
- Add to BAS

https://github.com/scythe-io/purple-team-exercise-framework/blob/master/PTEFv3.md

Maturity Models / Frameworks

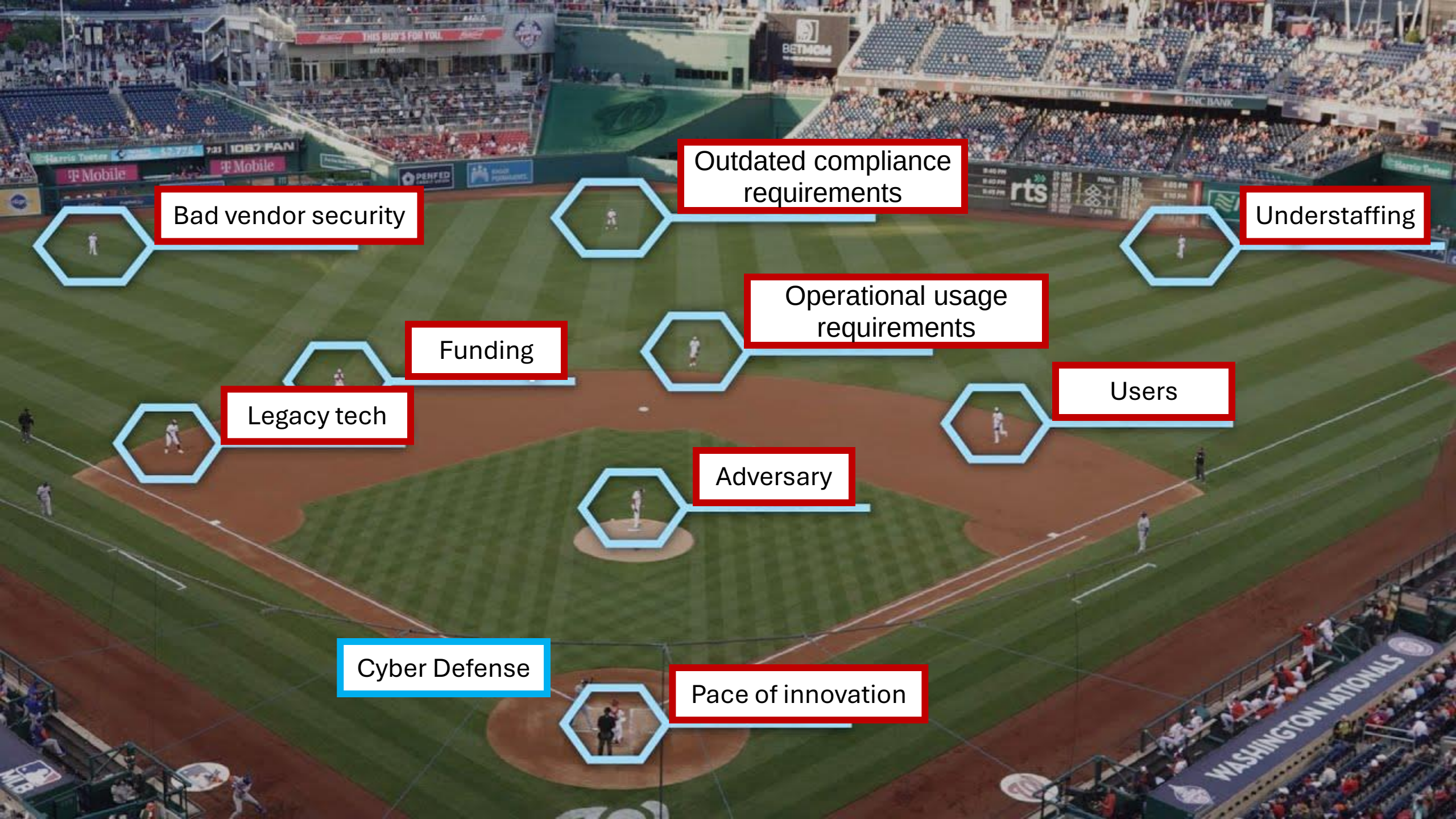
- MITRE CTID - Measure, Maximize, and Mature Threat-Informed Defense (M3TID)
- Cyber Threat Intelligence Capability Maturity Model (CTI-CMM)
- Mandiant - CTI Program Maturity Assessment
- SCYTHE - Purple Team Maturity Model (PTMM)
- Kyle Baily – DE Maturity Matrix
- Sqrrl - Hunt Maturity Model



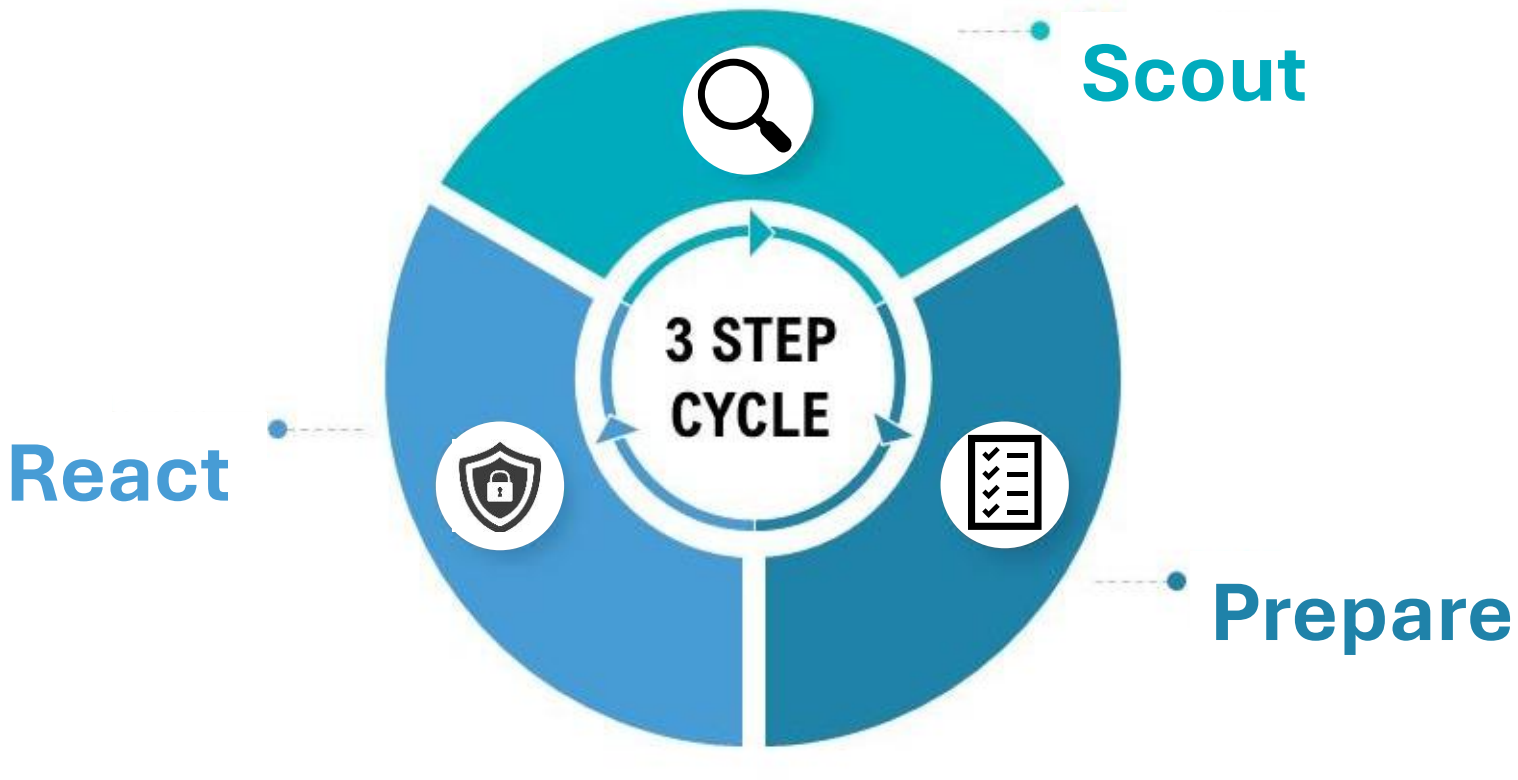
Classic Sports Analogy

Pitcher vs Batter

- This is the marquee matchup in baseball
- The pitcher knows what he will throw, and the batter must react to the pitch he receives
- In cybersecurity, we like to think of it as adversaries vs defenders


Bad vendor security
Outdated compliance requirements
Understaffing
Funding
Operational usage requirements
Legacy tech
Users
Adversary
Cyber Defense
Pace of innovation

Baseball – The Analytic Game

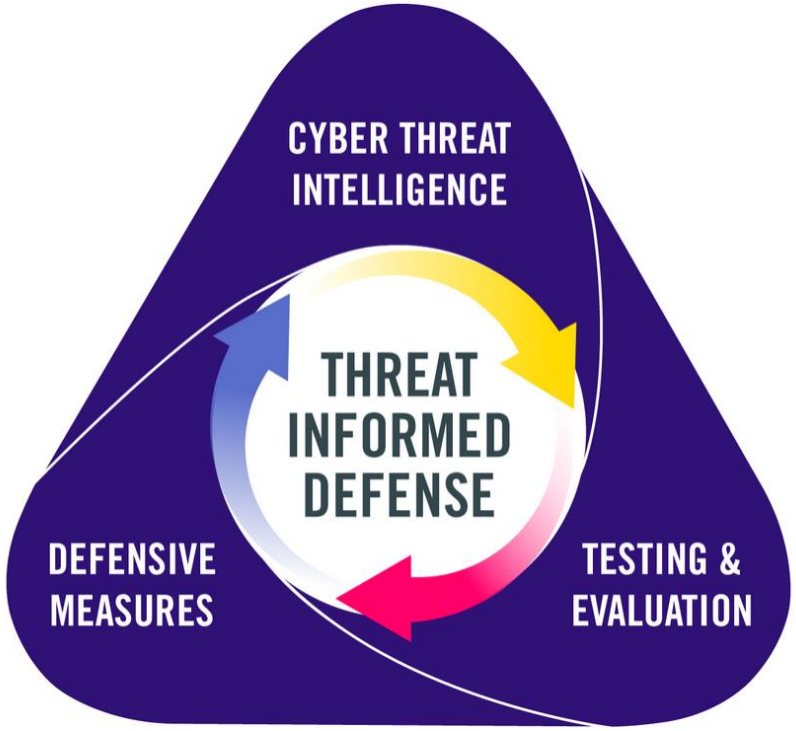


Look Familiar?

CTI
Scout

+ IR
React

DM + T&E
Prepare



Scout – Increase Odds of Success

Scout

Objective(s): Gather intelligence on threats / self.
Actions: Crown Jewel Analysis, Threat Model, baseline environment, analyze CTI.

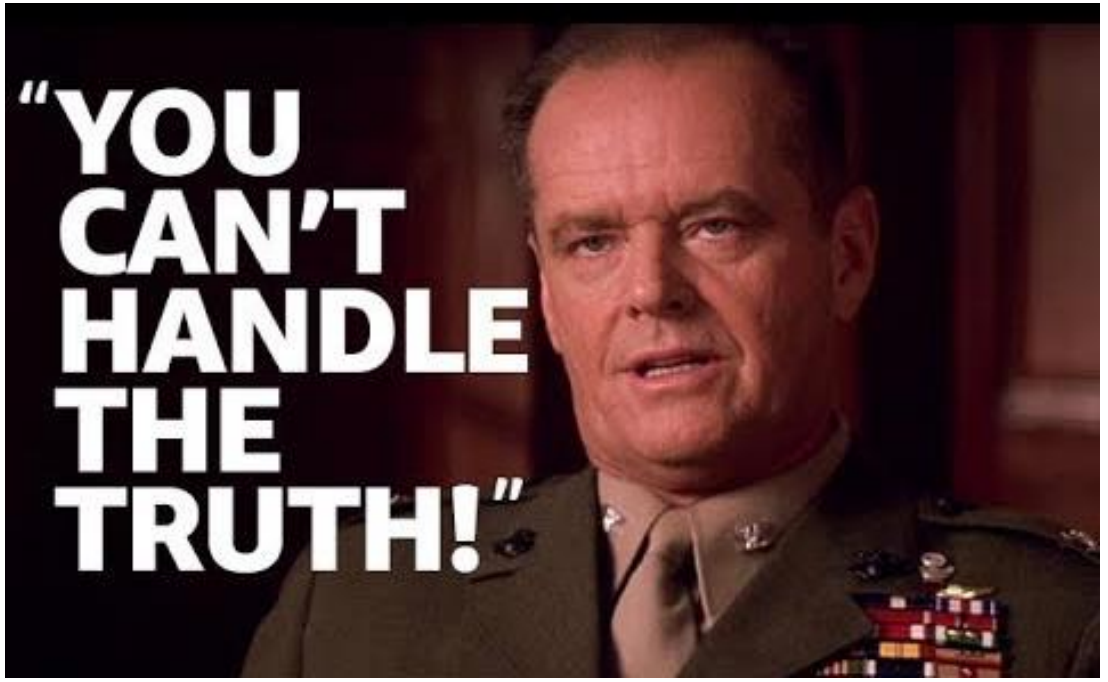
Prepare

React

Phase 1 – Scout

Answer questions

- Who are our top threats?
- What are these adversaries doing?
- How are they operating?
- What are their goals?
- What is our most important data, systems, and processes?
- How much should be spent on securing them?
- What is normal activity in our environment?



Cyber Defenders

Trying to look through petabytes of data for suspicious behaviors

Prepare – ⬆ Skills with Practice

Scout

Objective(s): Gather intelligence on threats / self.
Actions: Crown Jewel Analysis, Threat Model, baseline environment, analyze CTI.

React

Prepare

Objective(s): Act on intelligence, focus on prevention.
Actions: New controls, emulations, detections, test responses.

Phase 2 – Prepare

Answer more questions

- Can we detect adversary activity in our network?
- Do our preventative controls work?
- Did we validate with emulations?
- Is our intel useful?
- Are we missing visibility?
- Do we have processes/time to patch based on intel?
- Would we bring pain to adversaries?

React – Execute Under Pressure

Scout

Objective(s): Gather intelligence on threats / self.
Actions: Crown Jewel Analysis, Threat Model, baseline environment, analyze CTI.

React

Objective(s): Identification and quick response to threat events.
Actions: IR, tune detections, threat hunt.

Prepare

Objective(s): Act on intelligence, focus on prevention.
Actions: New controls, emulations, detections, test responses.

Hey guys,

I know this isn't really the place to ask for support, but I've got a weird log on my server.

Anyone able to help? Please see screenshot below.

Phase 3 – React

Answer all the questions

- How noisy are our detections?
- Can we react quickly to true positives?
- Can we spot abnormal activity?
- Do we collect the right data and look at what's happening in the environment?
- Is our 'normal' response time acceptable?
- Do we know what to do and who to call when we see something?

Improvement, Not Perfection

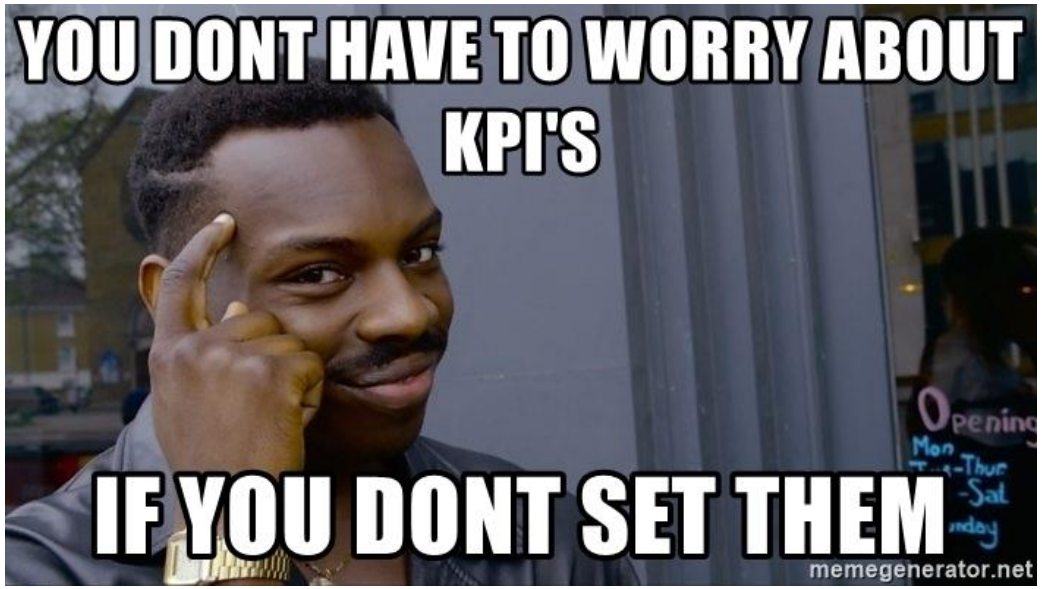
- Sometimes, as in baseball, you can do everything right and still not “win”
- Cyber defense = continual improvement
- Cyber defense != perfection

Metrics

Metrics, Fun!

- Cyber teams are historically bad at communicating value-add
  - Left behind teams that can clearly display metrics and proven value to C-Suite (marketing, product, etc)
- Goal - effectively demonstrate value of the security program and our efforts
- “Mature metrics are correlated with business goals, outcomes and enablement. You measure on performance & effectiveness.”

  - Gert-Jan Bruggink



Example TID Program Metrics

What is our high-level security status?

What timeframes are reporting on

What financial value does security bring?

How are the initiatives operating?

Where does security contribute to supporting business?

What do we track outside of the company

How does the company prepare, manage & control what is tracked outside & inside?

What manifests as incidents at the company

How well does the company Detect and Respond?

What do we track inside of the company

Full .xlsx download available on @gertjanbruggink GitHub

Example TID Program Metrics

Higher level status of the program

- Current Security Alert Level
- # of days without a major security incident
- # of days without a major security issue (near miss)

Filters

- Day vs day
- Day vs Month
- Day vs Year

Our value to the business

- Yearly Cost of Security program (USD, optionally year to year comparison)
- Yearly Average Total Cost saved (USD)

Key Change Activities

Strategic company Initiatives	Status	Progress
	Status	Progress
	Status	Progress
	Status	Progress

Regulatory Compliance

- Percentage Increase in Compliance with Industry Regulations
- % differences

Major threats tracked

- Total # of TI sources
- % changes in source
- Top 3-5 Notable Threat items (eg high media items)
- % of Successful Threat Intelligence Sharing Collaborations
- Total # of Threat Actors tracked
- Top 3 Threat Actors
- Top 5 most referenced MITRE ATT&CK Techniques

People Controls

- Percentage Changes in Security Awareness Training Completion
- Percentage Increase in Employee Reporting of Suspicious Activities
- Total # emails reported as malicious
- % emails reported actually malicious
- Total # other events reported as malicious
- % events reported actually malicious
- Employee Survey on Cybersecurity Awareness and Understanding

Total Number of Incidents, categorized per type

MTTD: Average vs Exercise

Average MTTD	% difference per filter
Exercise MTTD	% difference per filter

MTTR: Average vs Exercise

Average MTTR	% difference per filter
Exercise MTTR	% difference per filter

Major risks tracked

- Top 5 Risks, sorted based on Risk Appetite (e.g. above appetitive)
- Top High Risk Assets, sorted based on Criticality
- Top Risk items, with open decisions (e.g. using narrative format, ready for direct explanation)

Technical Controls

- Percentage of Critical Assets with Proactive Defense Measures
- Percentage Reduction in Vulnerability Resolution Time, vs Average
- Percentage Reduction in High-Risk Vulnerabilities

Review Those Slides (& logs)

1. Why Purple Teams / Functions Are Needed
   - Reduce Impact, Prioritization, Gap Identification, Train Assets, Inflict Pain
2. What Can Be Done
   - Develop a purple team function to enhance defenses with threat-informed defense
3. How to Run a Purple Team Exercise
   - CTI, Attack, Detect, Defend
   - CTI, BAS, Detection - resources and strategies
4. Maturity Levels of Purple Teams
   - One Time Engagement, Ad-Hoc Exercises, Regular Exercises, Continuous Purple Teaming
5. Metrics to Measure ROI

Questions?

Contact: Linkedin_micah-vanfossen/ or email available on request