> How to be the Best Adversary Simulator

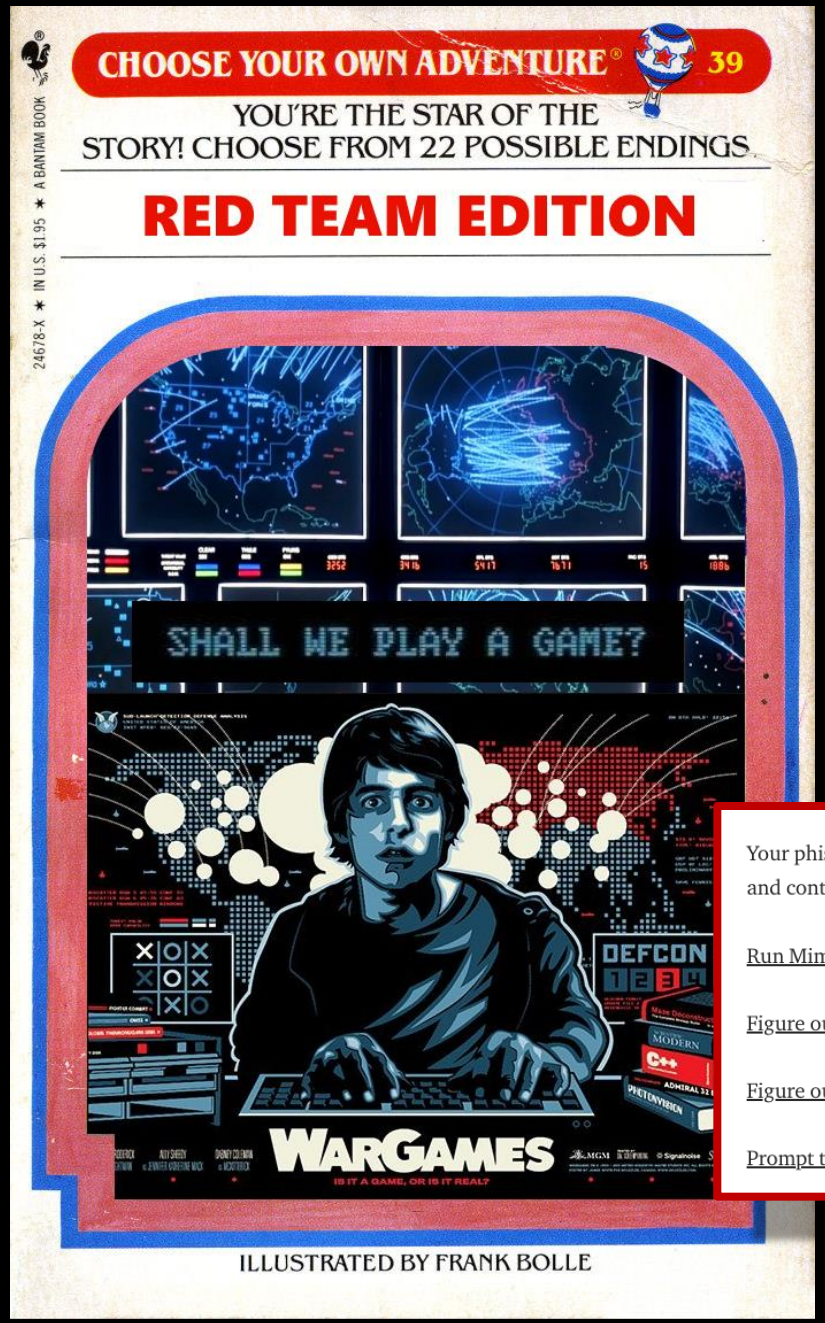
> Adversary Village
> DEF CON 30

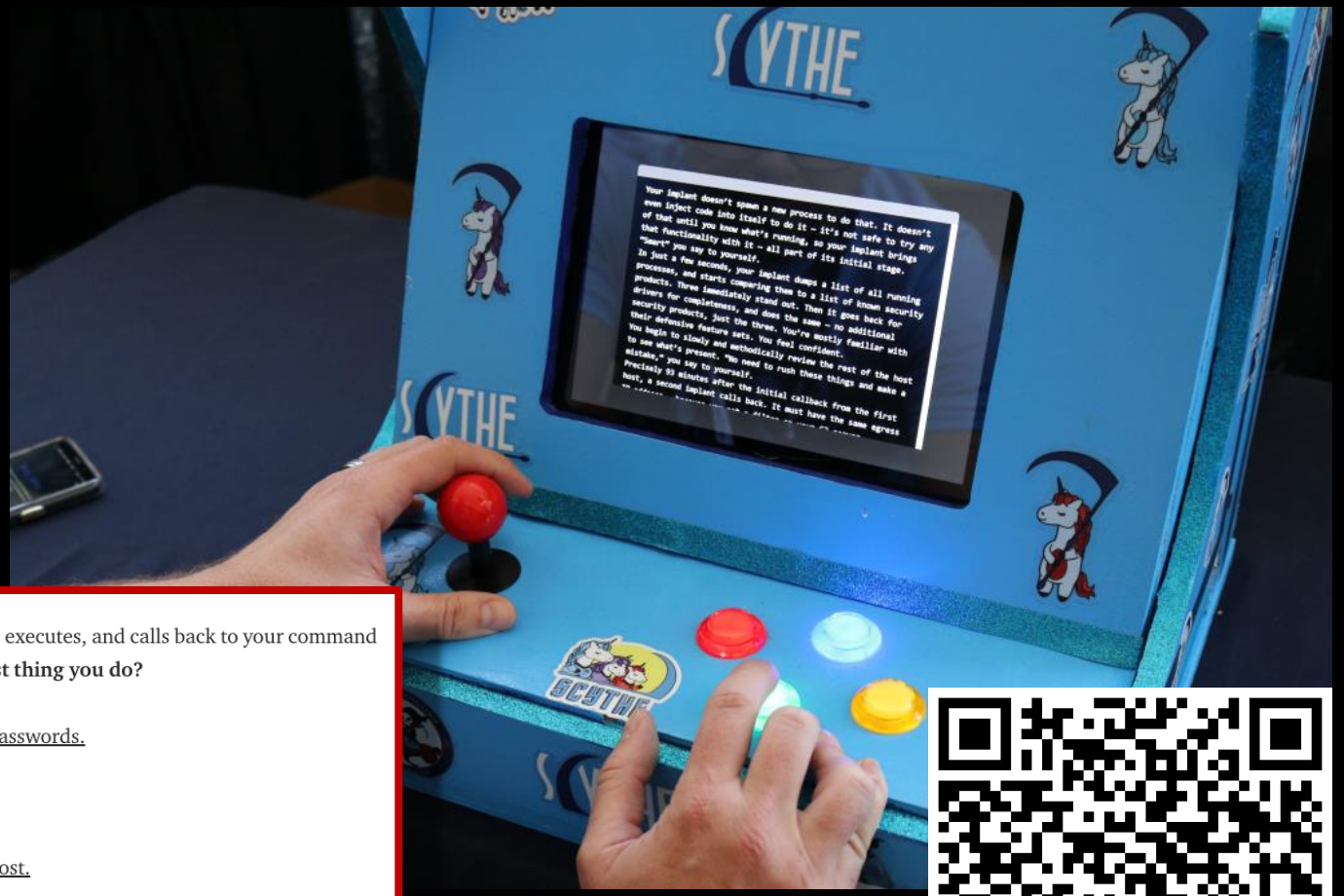
@malcomvetter

#about

- 20+ years tech/cyber
- built the red team program at Walmart (5 continents)
- CTO at Cyderes
- Head of Managed Services at Cyderes
- Advisor to Scythe
- Built/broke stuff
- Touched many $hot_stoves
- Have opinions
- Talked at {$places}

You might have seen this





Your phish payload lands on a host, executes, and calls back to your command and control server. **What is the first thing you do?**

Run Mimikatz to collect plaintext passwords.

Figure out where I am.

Figure out what's running on this host.

Prompt the user for their password.

(not an actual book)

https://malcomvetter.medium.com/

be the best adversary simulator

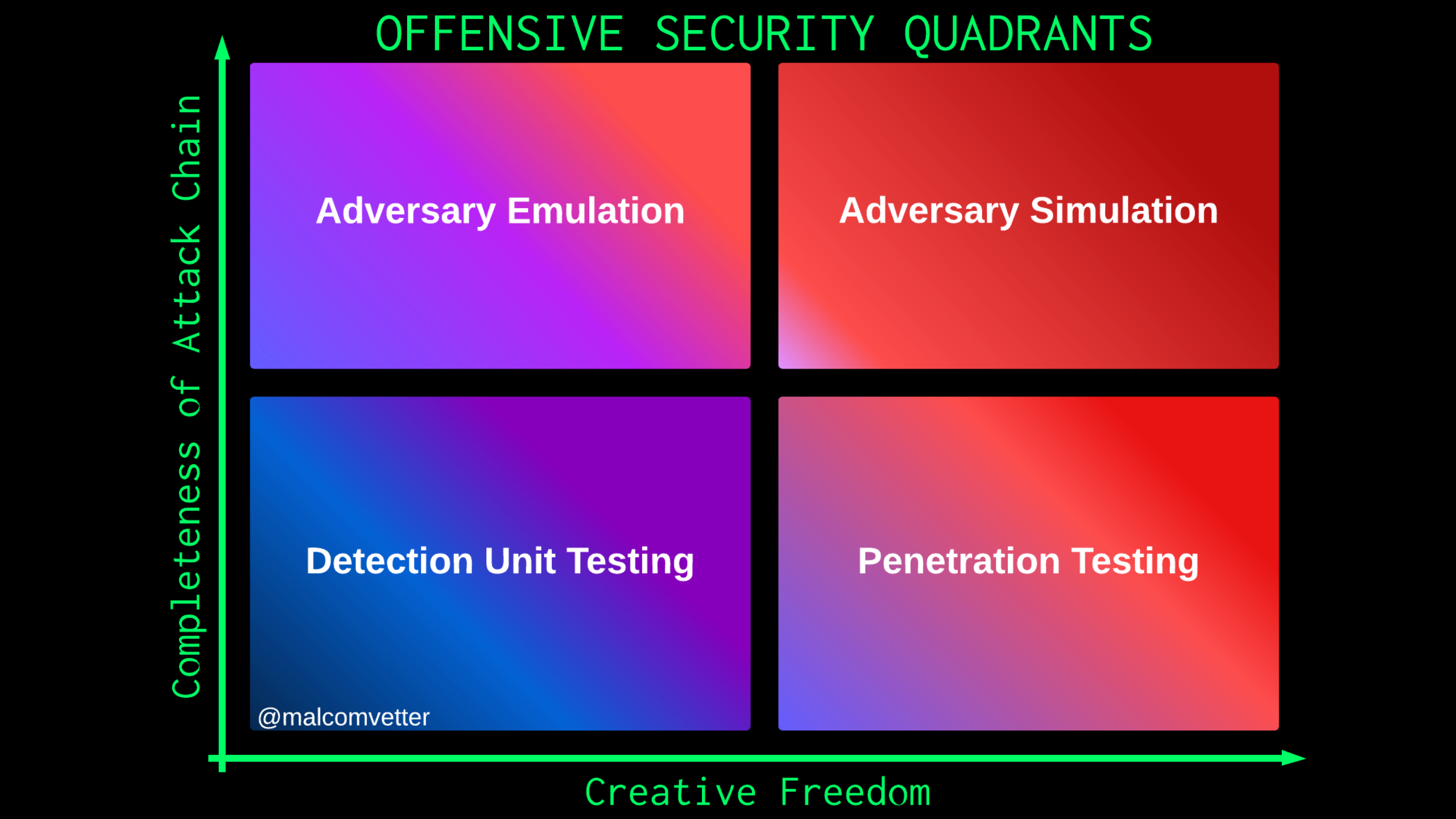
1. Know what adversary simulation truly is
2. Know your customers – yes, you have them
    1. Empathize them
    2. Downstream effects of your recommendations
3. Don’t fight the rat race
    1. Focus on your own self improvement
    2. Don’t compare to others
    3. Find value in your customers’ value
    4. Rear view mirror
4. Know yourself
    1. Find value outside of this space, or you’ll burn out
    2. Find challenging hobbies
5. Celebrate wins

1) Know what adversary simulation truly is

What does RED TEAM mean anymore?

What about ADVERSARY SIMULATION?

(Have we just given into the marketing?)


OFFENSIVE SECURITY QUADRANTS
Completeness of Attack Chain
Adversary Emulation
Adversary Simulation
Detection Unit Testing
Penetration Testing
@malcomvetter
Creative Freedom

Tim MalcomVetterTM
@malcomvetter

Pentest your prevention controls
Unit test your detection controls
Red Team your response processes

☝ Mixing the above comes with diminished results.

4:55 PM · Jan 13, 2020 · Twitter Web App

View Tweet analytics

83 Retweets **10** Quote Tweets **242** Likes

Tip

OFFENSIVE SECURITY QUADRANTS

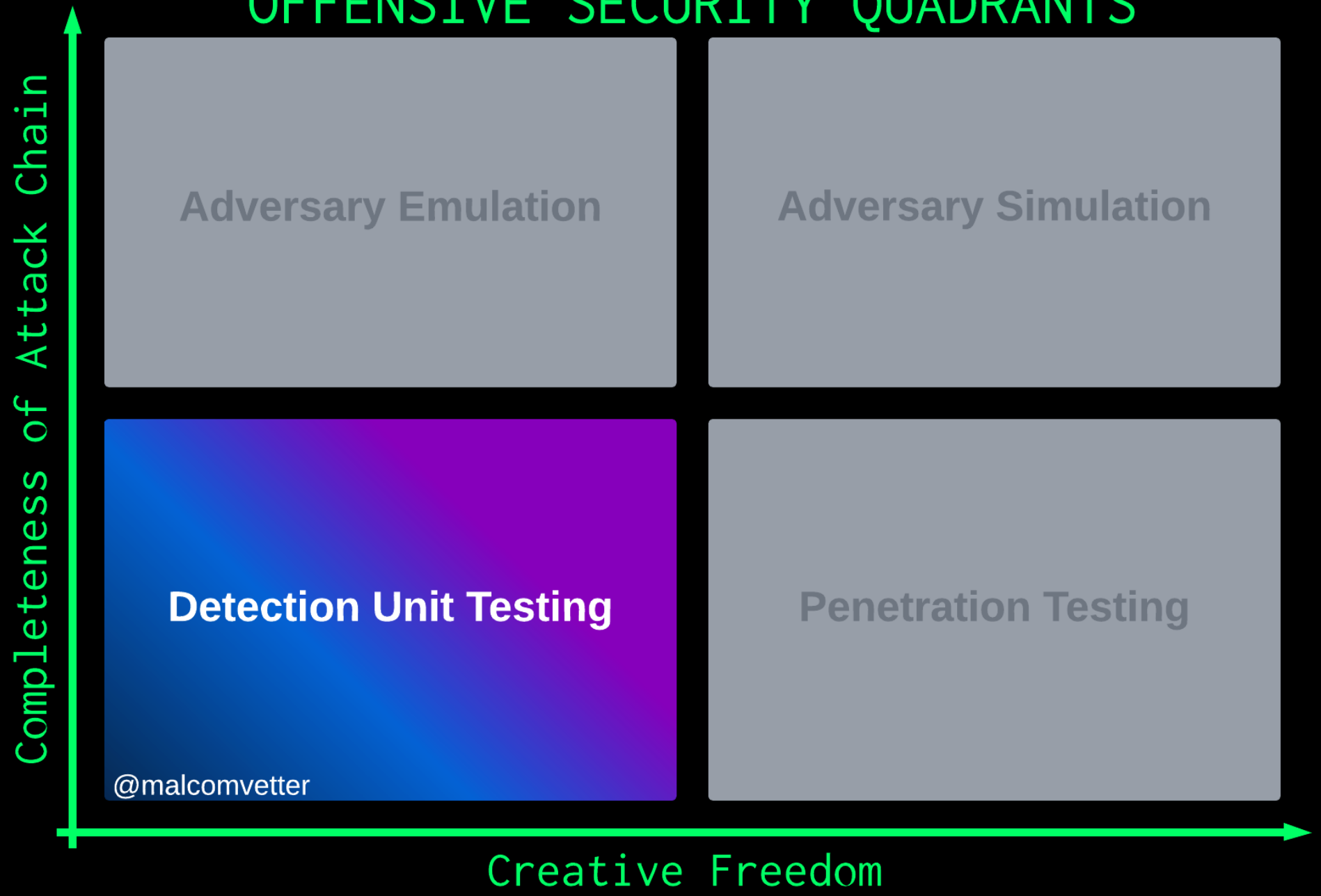
No Creativity, No Attack Chains.

Just TTP detection coverage.

The basics.

What every org should do before any of the other stuff.

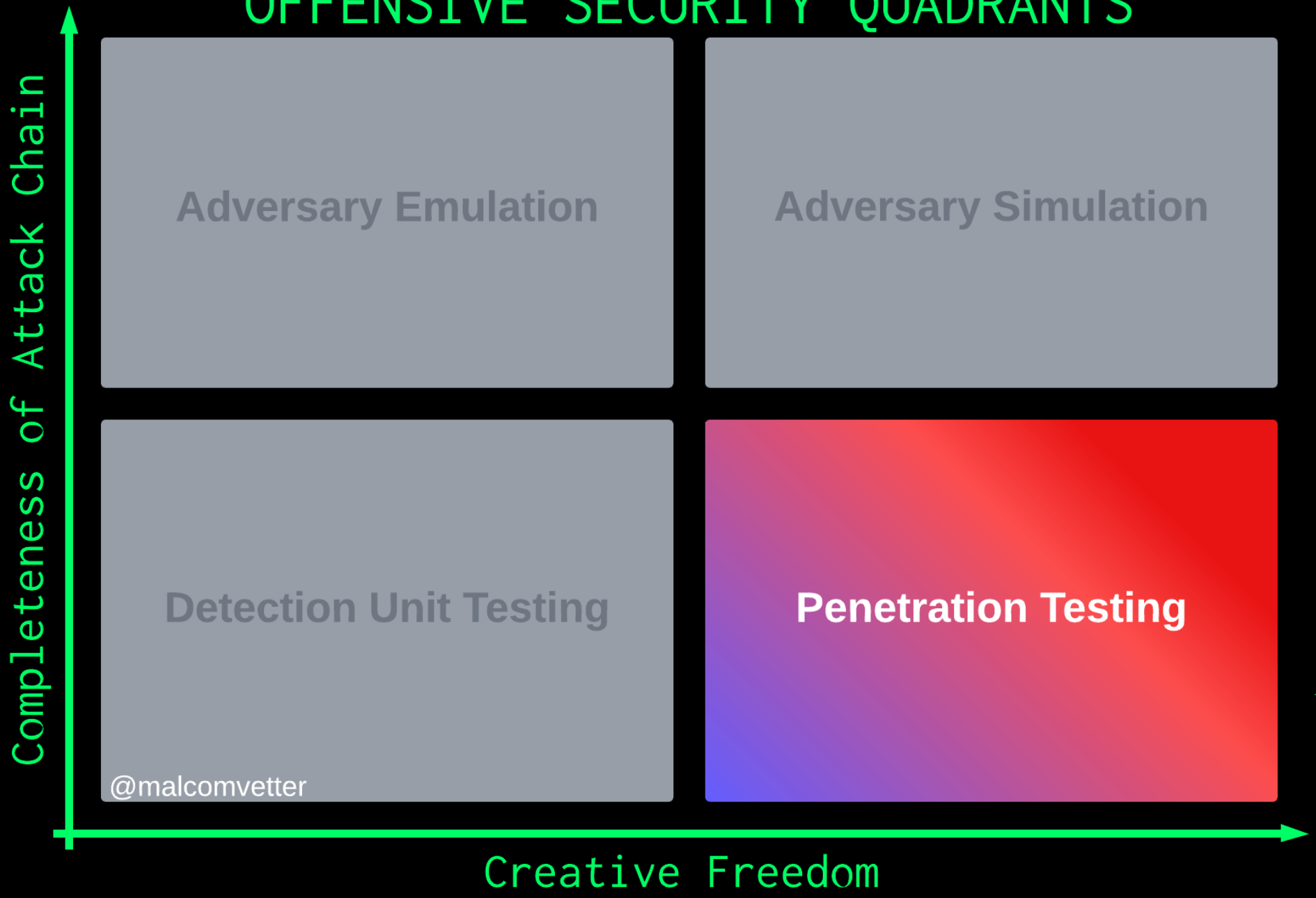
What most of us should be working on, Period.



Want to be a good ADVERSARY SIMULATOR?

Tell your { customers, org, CISO } they should unit test detections first.

OFFENSIVE SECURITY QUADRANTS



Maximum Creativity with Zero Attack Chain.

Find clever ways to exploit something, but no lateral movement and limited privesc.

Important work, but sometimes unrealistic.

"If I line all these items up in a once in a billion situation, I can pwn all the things."

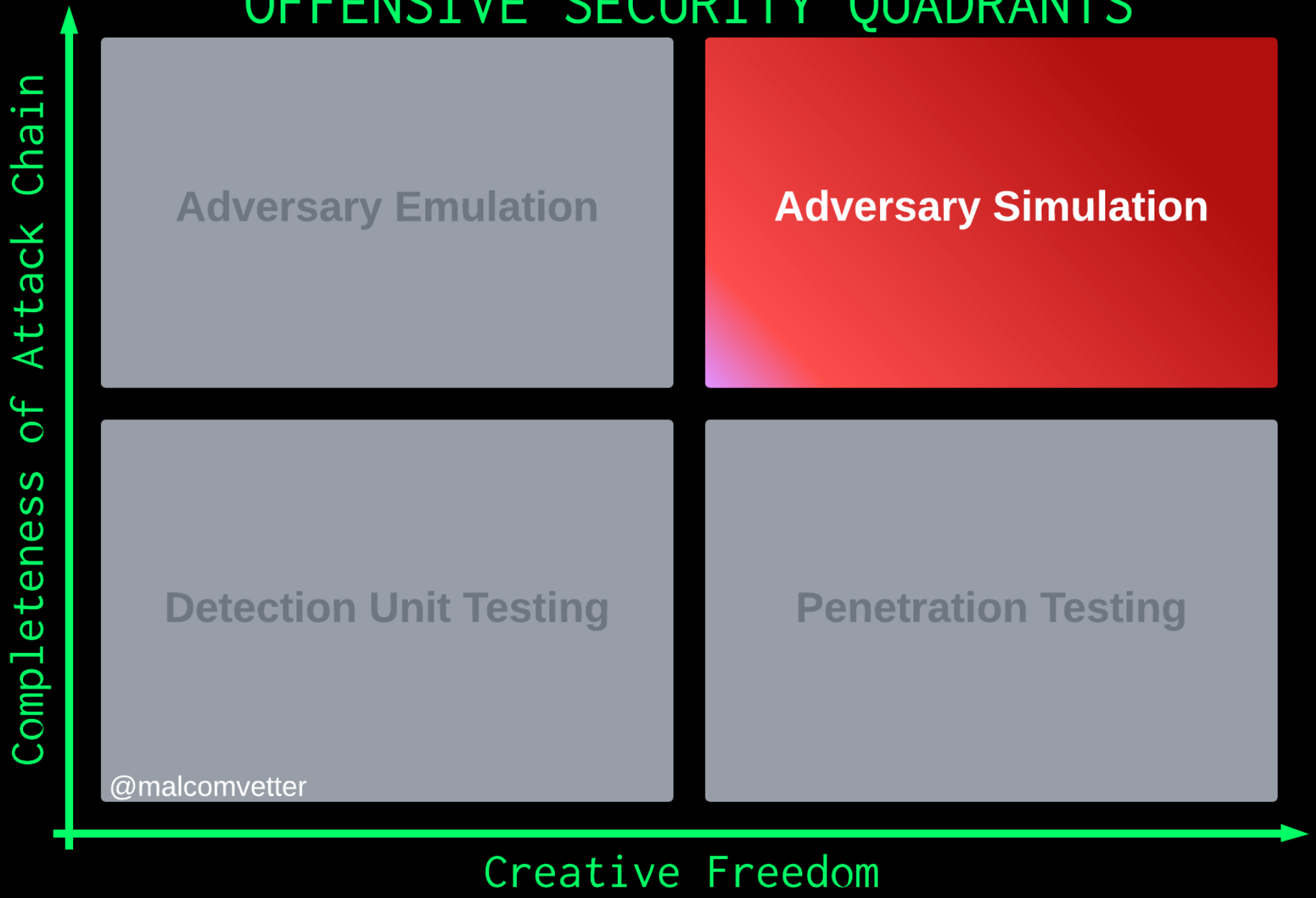

DANGER
MINES

Emulation: (computing definition) *reproduction of a function or action on a different computer or software system.* This is an older word used since before the 16th century English.

Simulation: *imitation of a situation or process; the action of pretending; the production of a computer model for the purpose of study or learning.* This is a newer word, first in widespread use during the mid 20th century.

False Flag: *a covert operation designed to deceive by creating the appearance of a particular party or group being responsible for the activity, disguising the true source of responsibility.*

OFFENSIVE SECURITY QUADRANTS



Maximum Creativity
+
Complete Attack Chains

What most OffSec people think of when they hear "Red Team"

What most lay people think of when they hear "penetration test"

Be like an adversary, don't be identical to a specific adversary.

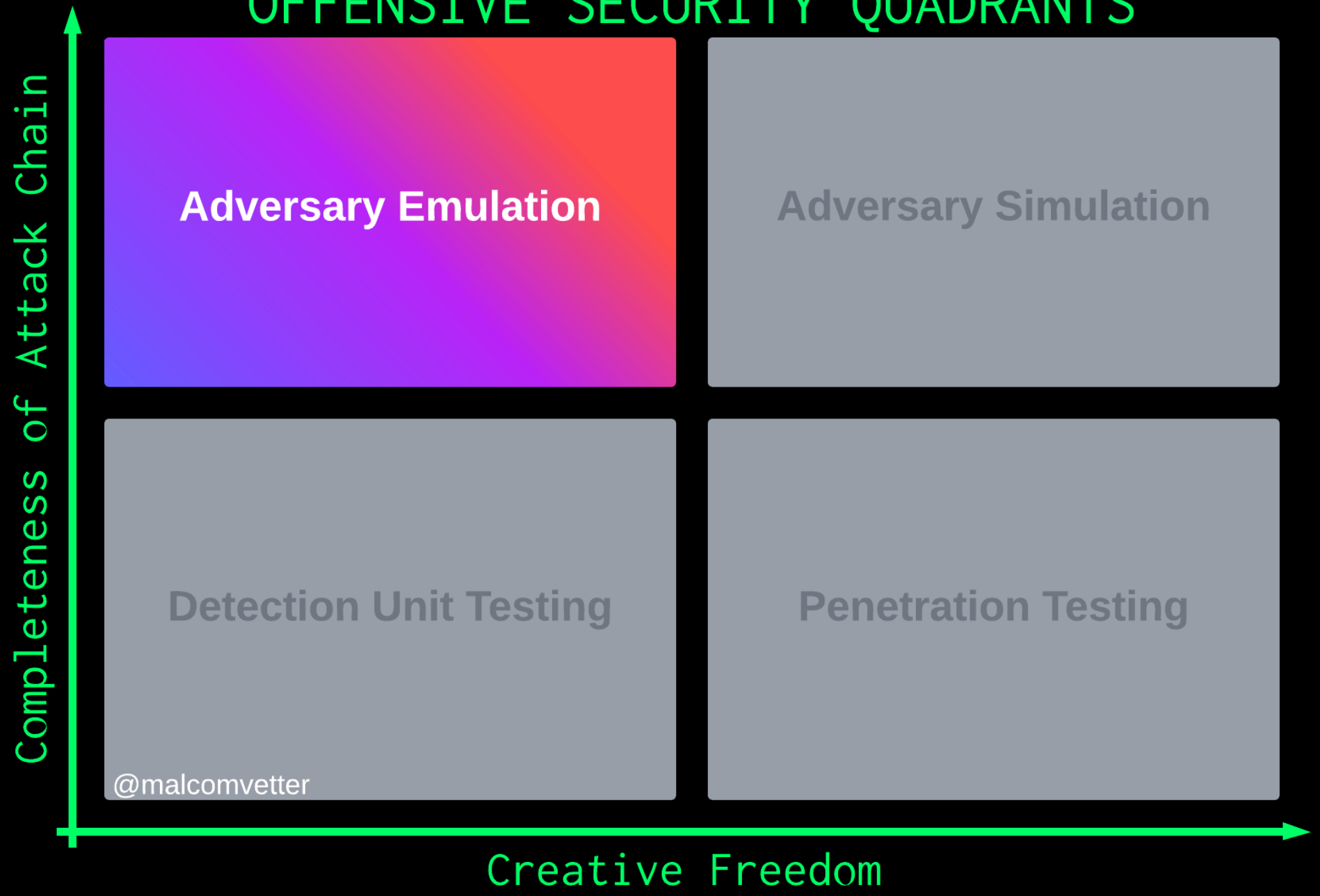
OFFENSIVE SECURITY QUADRANTS

No Creativity Allowed.

Execute what the threat actor executed, how the threat actor executed it.

Only as good as Threat Intelligence details.

But Johnny Q. CISO can tell the board "If APT99 hit us tomorrow with their techniques from 5 years ago, we'd be ready."



ADVERSARY EMULATION is a solution
in search of a problem.

Don’t do it.

2) Know who your customer is

Yes, you have customers.

```
customer = { paying_client, CISO, blue_team, etc. }
```

Empathize your customer.

What are they trying to accomplish?

How will your recommendations impact them?

Tim MalcomVetter™
@malcomvetter

I'm over here eating crow. Laugh at this with me, then realize your crow will come, too.

For all the times, as a red teamer/pentester when I wrote something dismissive like "just implement a detection for that" ...

1/

12:01 PM · Jun 28, 2022 · Twitter Web App

3) Don’t fight the rat race

Focus on your own self improvement

Don’t compare yourself to others

Some people have been doing this for DECADES at this point

Find value in your customers’ value

You can’t get where you’re going
looking in the rear-view mirror

I { made a tool, hacked a thing, got a job, etc. }

A word on tools …

“Nobody cares, work harder.”
- Cam Hanes

4) Know yourself

Find value outside of this space,
or you'll burn out.

Find something else to humble and challenge you.

5) Celebrate wins

```
wins = {
      protected a customer,
         improved security,
           made a new tool,
         caught a bad actor
}
```

Find balance

Now go do good things.