Automating Adaptive Adversaries

SCYTHE

Tim Schulz – Adversary Emulation Lead

SCYTHE

Sandia National Laboratories

MITRE

MITRE | ATT&CK®

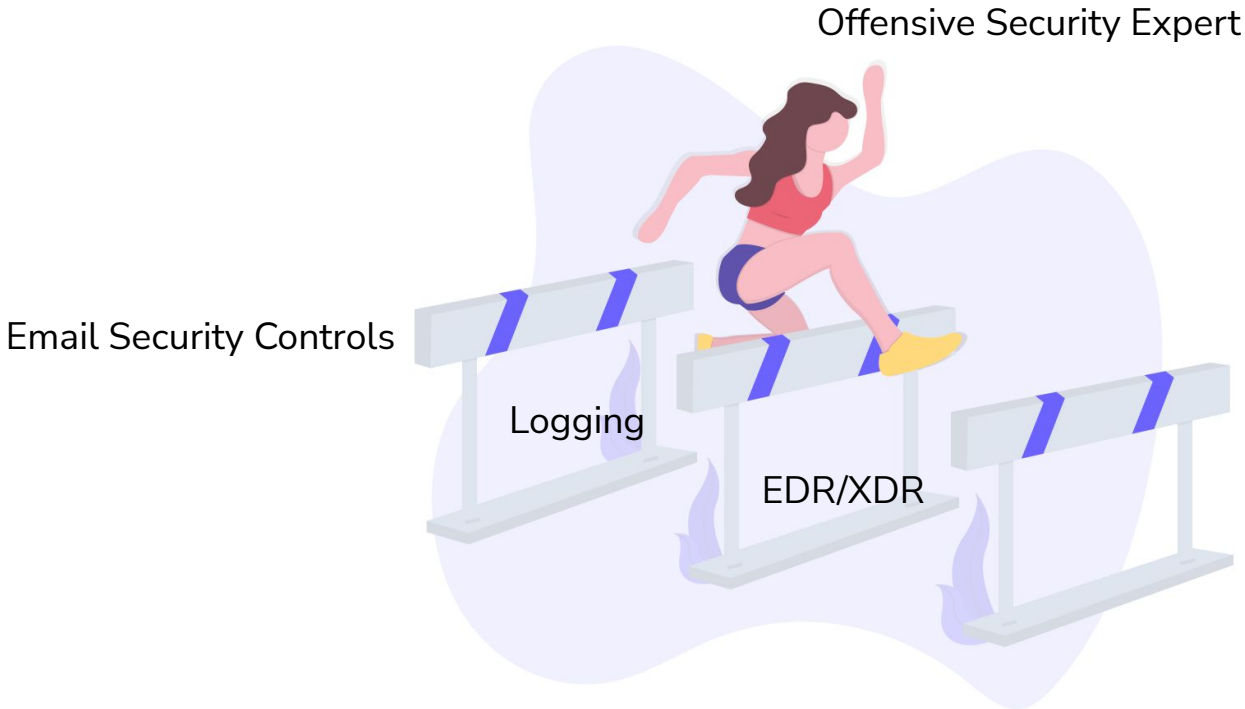
Setting the stage – who are we talking about?

Setting the stage – who are we talking about?

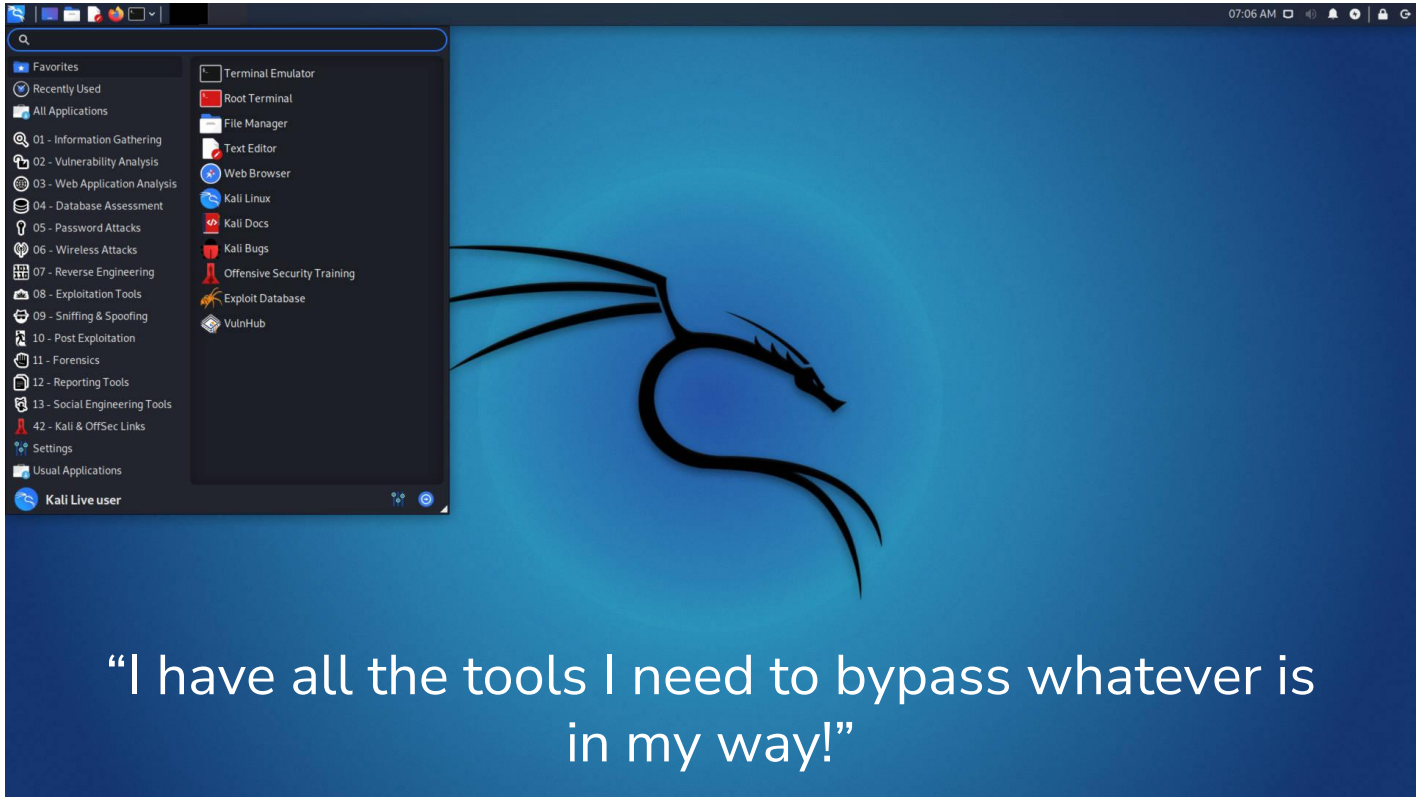
Word of the day

SCALE

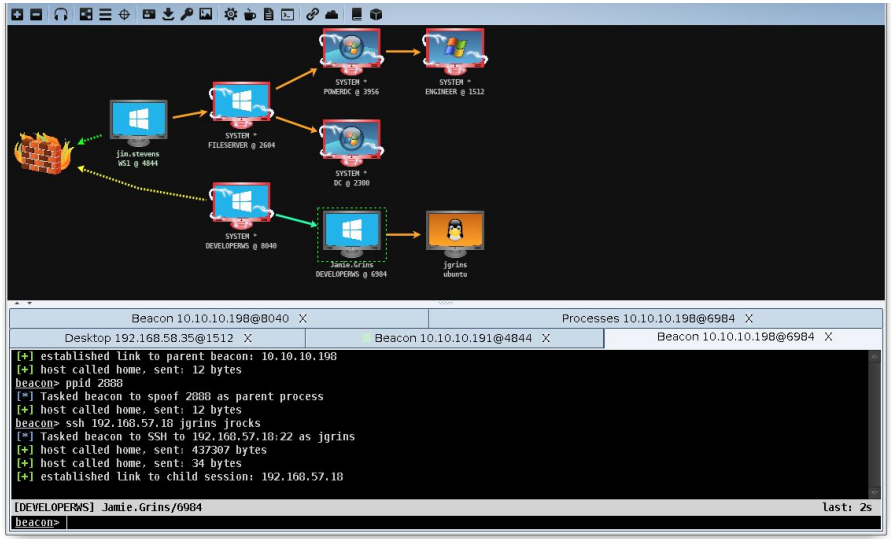
Am I adaptive?



How we gear up for emulating adversaries/security testing



How adversaries gear up for operations



I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue) ("mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

1.3 . **shell whoami** < ===== who am I

1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers

net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers

What is the difference?

What is the difference?

Capability

(and how it is viewed)

Scale and/or consistency

Automation is consistency at scale

Capability = Adaptability

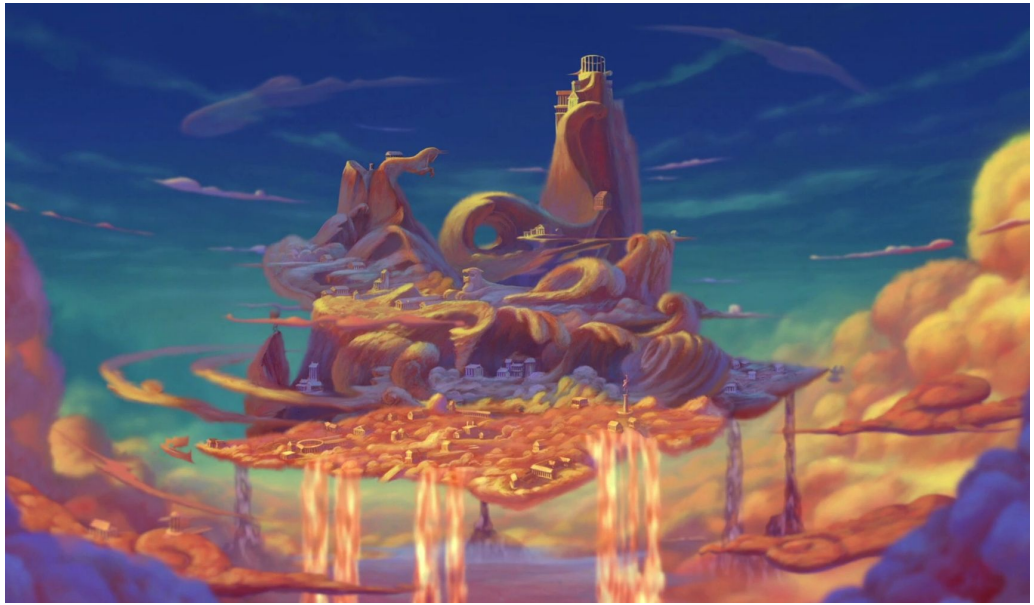
Automating ~~Adaptive~~ Capability of Adversaries

SCYTHE

Individual expertise does not scale

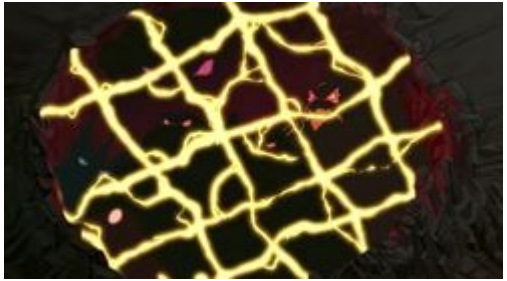
Case Study: Hades's Plan in Disney's Hercules

Scenario



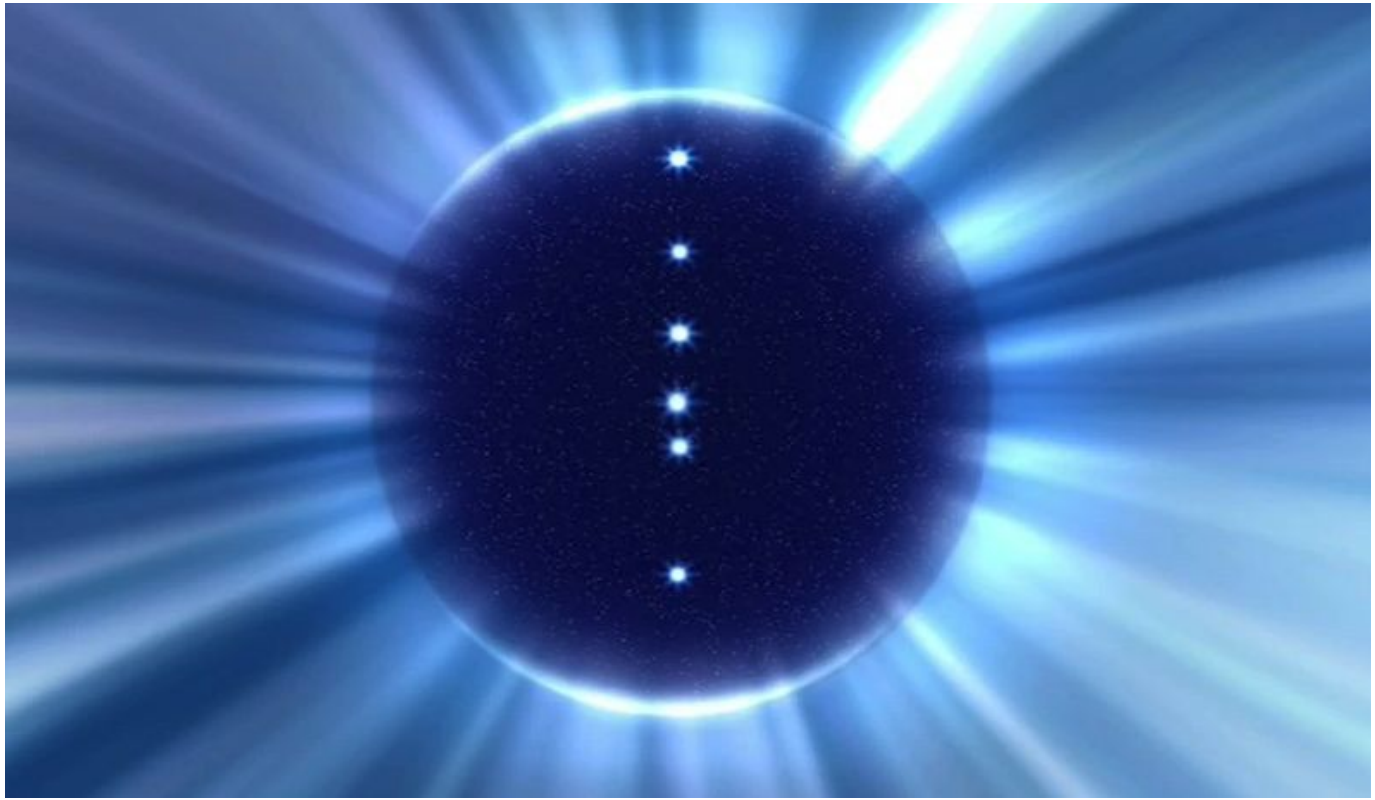
- **Target**: Mount Olympus
- **Challenge**: Lots of gods to beat

Titans (Red Team)



Slight Wrinkle:
They are locked up
(research)

Unleashing the titans....every 14 years?



Short Lived Success! (All the fates aligned)

Uh Oh

No more titans

Hades has to find a completely new plan

Analysis: Hades's Failure

- Attack vector didn’t scale
  - 4 Titans
- Capability extremely limited
  - No scale
  - Consistent but far apart

Measuring Capability

SCYTHE

Overall Concept comes from Wardley Maps

- Value Chain Mapping by Simon Wardley

Resources

- Free Book: https://medium.com/wardleymaps/on-being-lost-2ef5f05eb1ec
- (PDF download) https://learnwardleymapping.com/book/
- 13 minute video: https://www.youtube.com/watch?v=NnFeIt-uaEc
- 40 minute video: https://www.youtube.com/watch?v=L3wgzl2iUR4
- https://list.wardleymaps.com
- https://github.com/wardley-maps-community/awesome-wardley-maps

Measuring Capability

Genesis

- Everything starts as an idea
- Unproven
- “I wish I could fasten two things together”

Measuring Capability

Genesis → Custom

Idea takes hold - it has merit!

“Artisan fastener making”

Measuring Capability

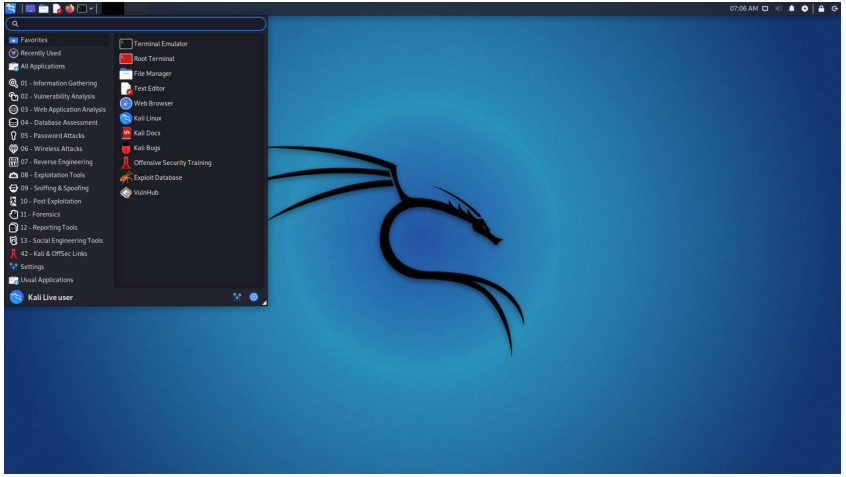
Genesis → Custom → Product

Cool – but what about cyber?

SCYTHE

Prepare to Dive!

Reframing the Challenge



VS

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue) ("mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

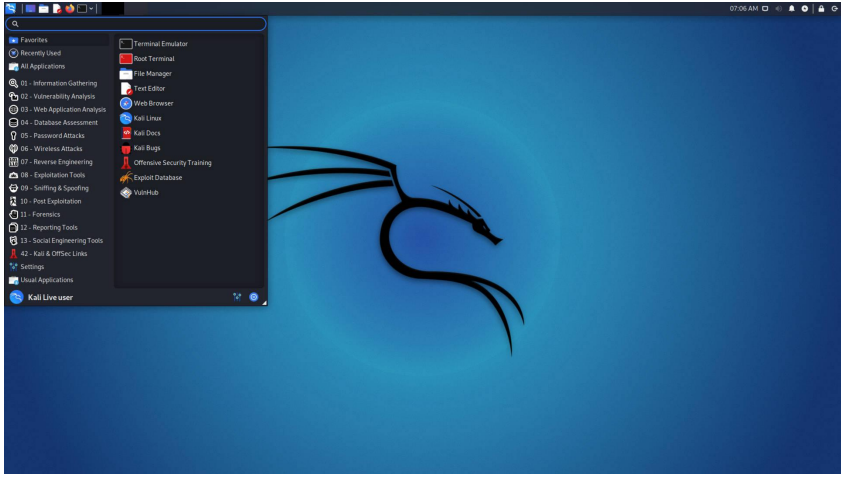
1.3 . **shell whoami** < ===== who am I

1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers
net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers

Reframing the Challenge



VS

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue) ("mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB

1.3 . **shell whoami** < ===== who am I

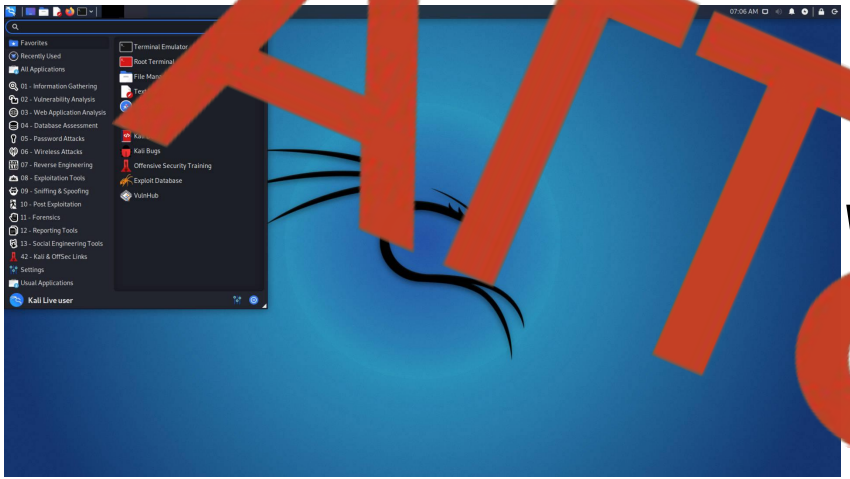
1.4 . **shell whoami / groups** -> my rights on the bot (if the bot came with a blue monik)

1.5 . 1 . **shell nltest / dclist:** <===== domain controllers
net dclist < ===== domain controllers

1.5 . 2 . **net domain_ controllers** < ===== this command will show the ip addresses of domain controllers

Genesis → Custom → Product

Reframing the Challenge



ATT&CK®

VS

I Tier . Increasing privileges and collecting information

1 . Initial exploration

1.1 . Search for company income

the company's website

on SITE + revenue (mycorporation.com + revenue) (

"mycor tion.com" "revenue")

check than 1 site, if possible

(owl anta, zoominfo, dnb, rocketrich)

2 . Defined by AB

. **shell whoami** who

. **groups** -> my rig the bot (if the bot came with a

)

. **shell est / dclist:** <===== in co lers

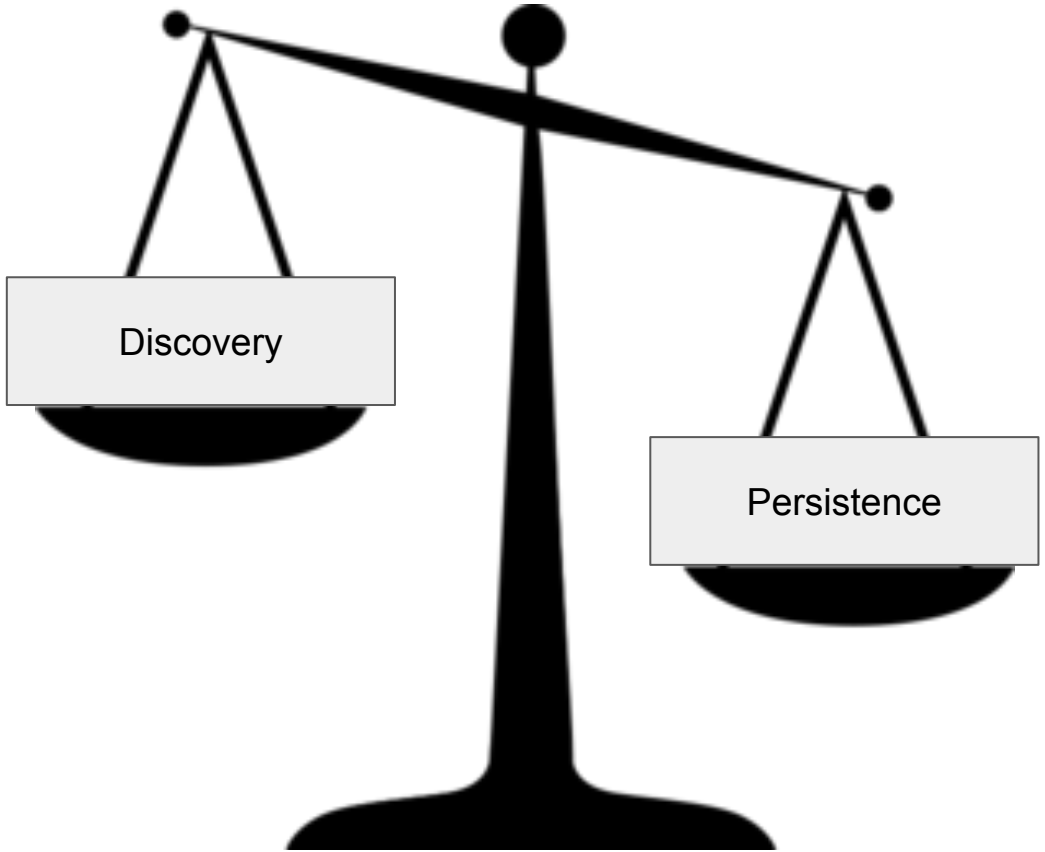
ist < = domain controllers

1.5 . **net ain_ controllers** < ===== th mmand wi the ip

addre of d controllers

Genesis → Custom → Prod ct

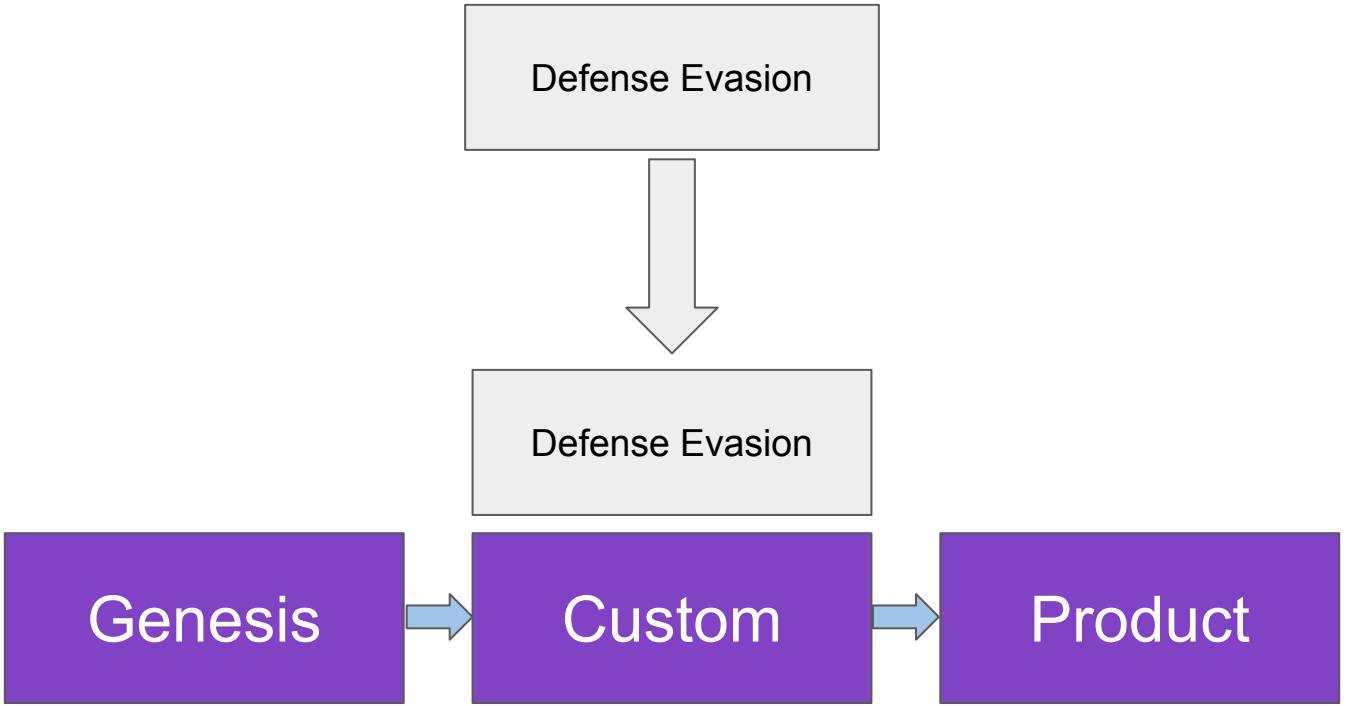
Not all TTPs are equal



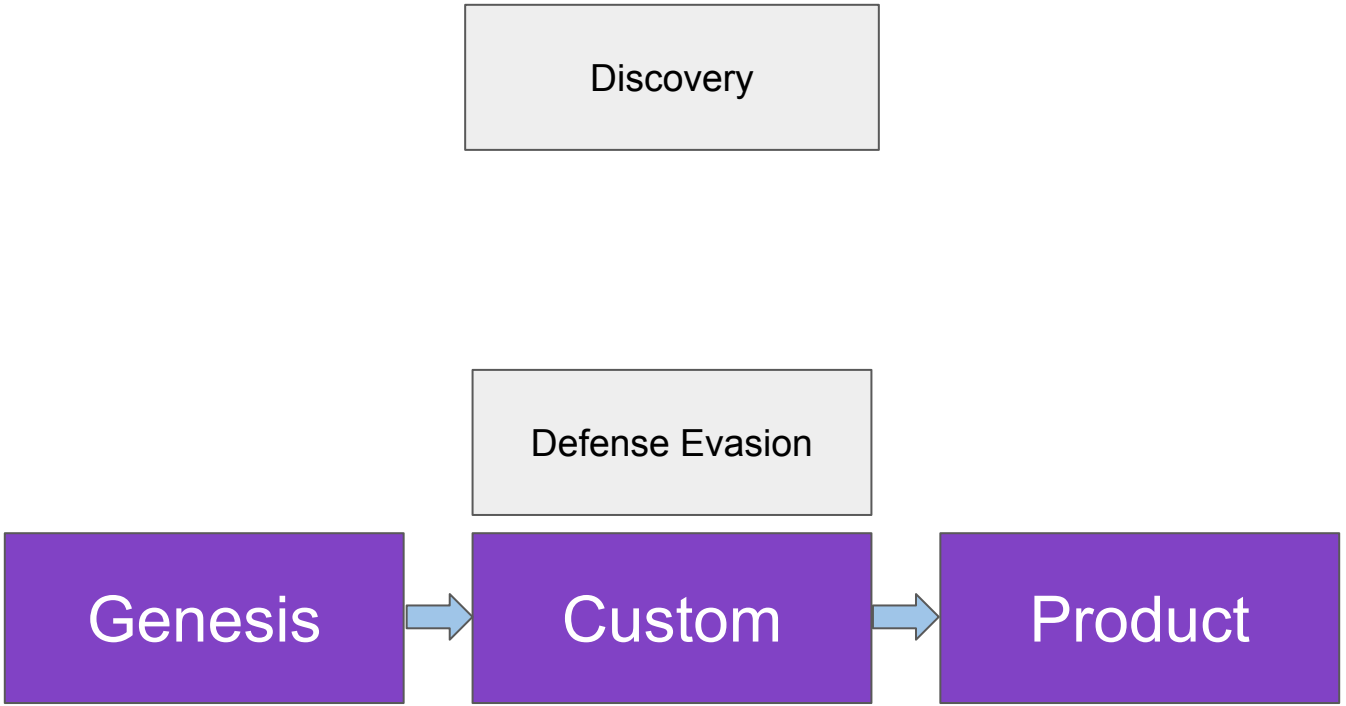
Measuring Capability: Tactics

Defense Evasion

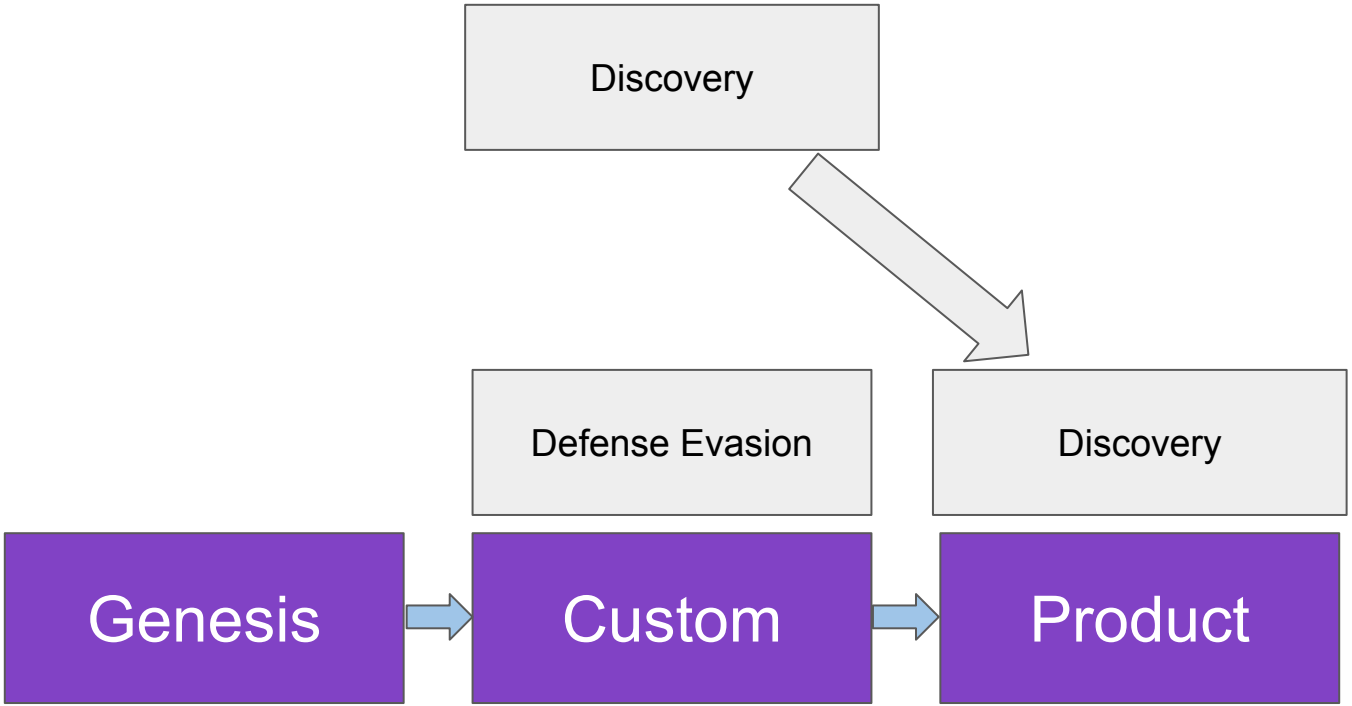
Measuring Capability: Tactics



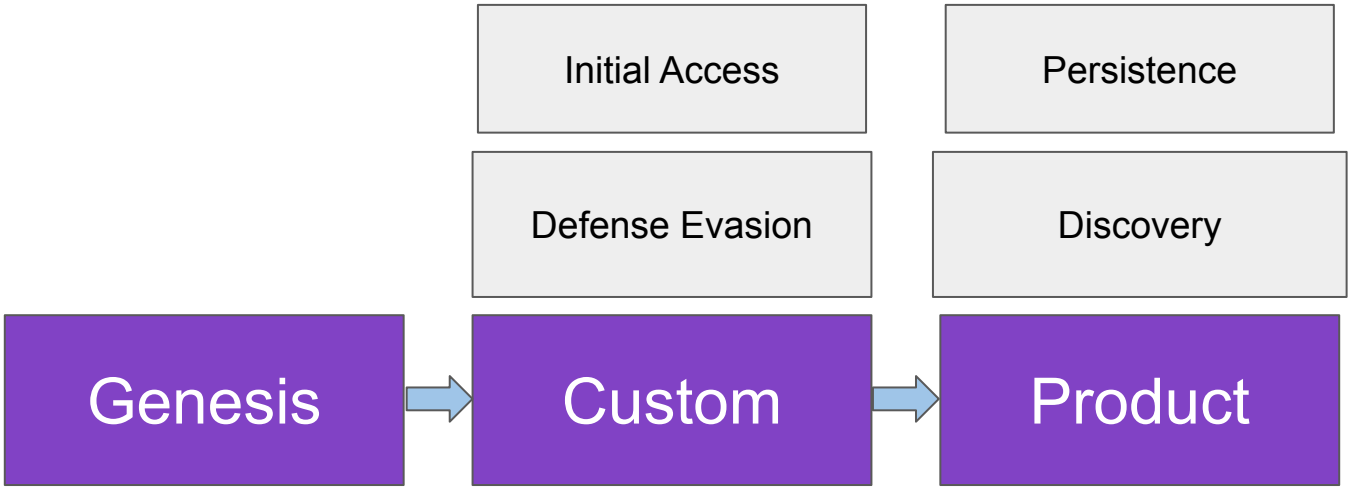
Measuring Capability: Tactics



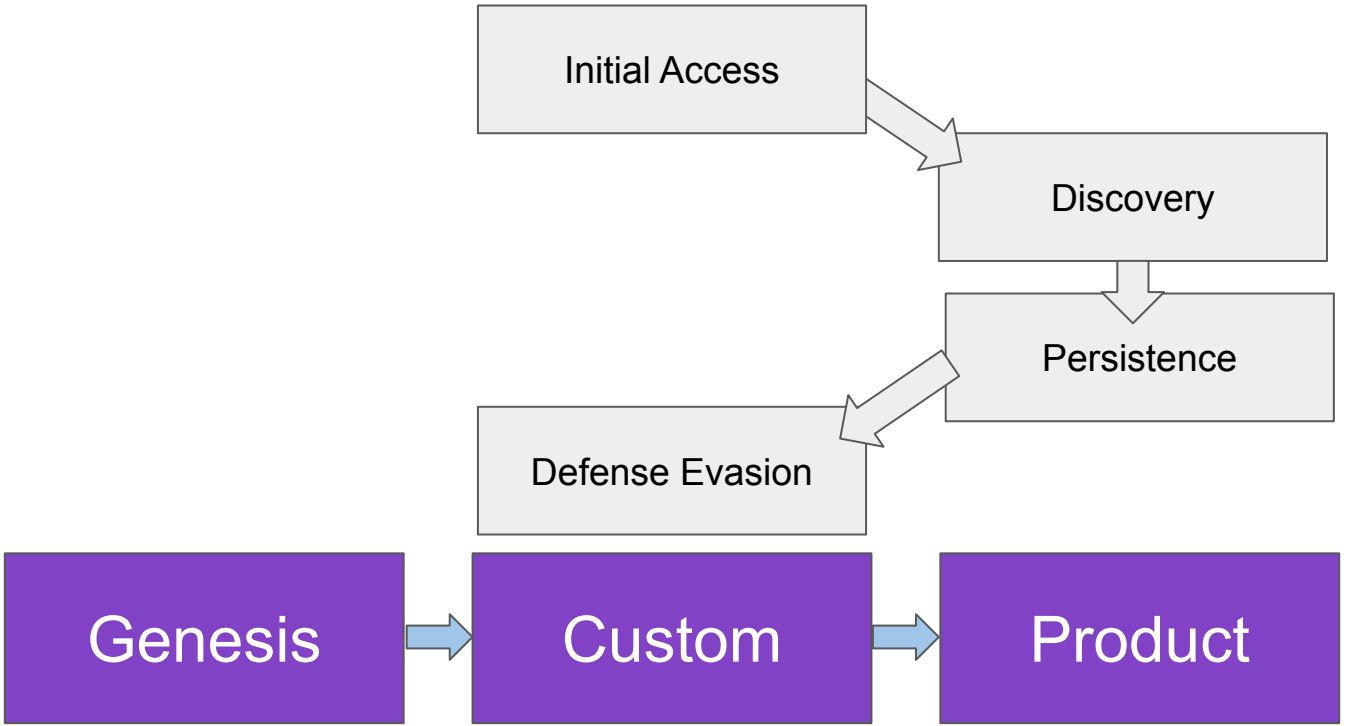
Measuring Capability: Tactics



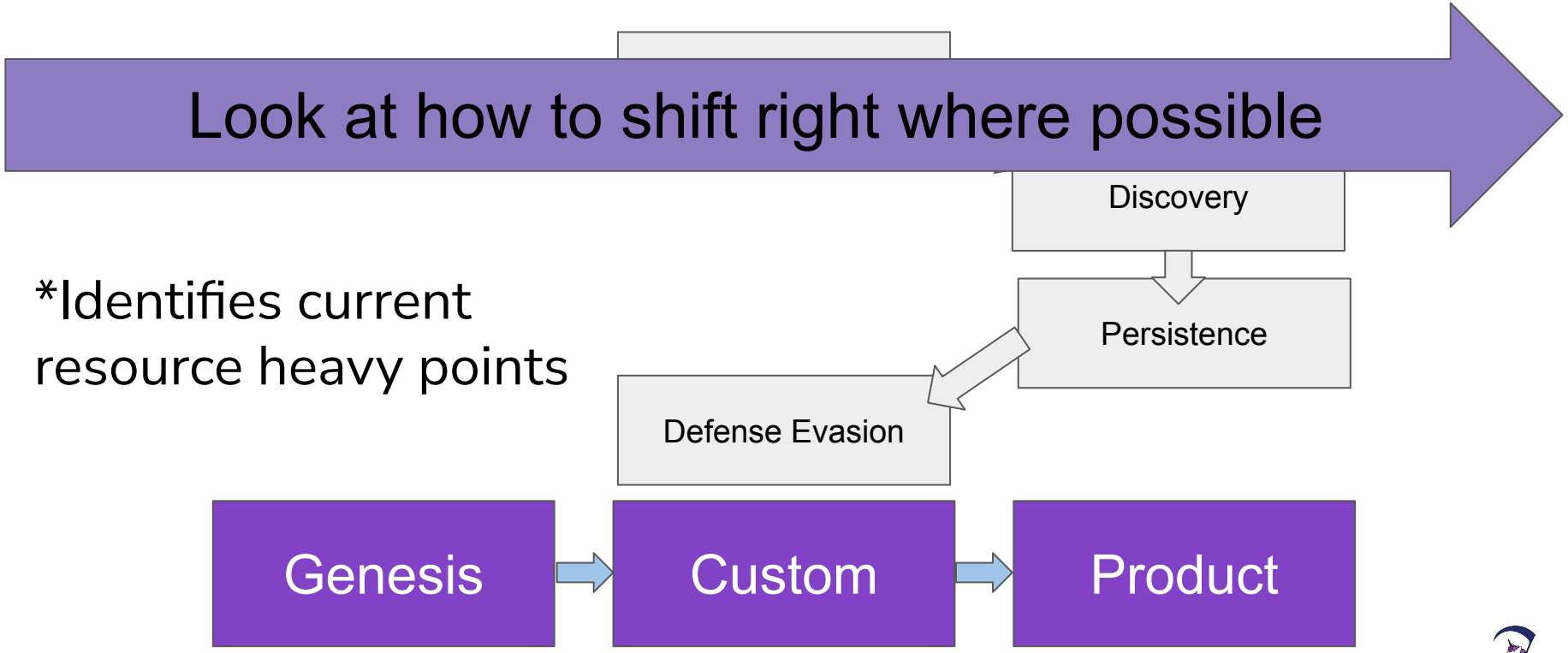
Measuring Capability: Tactics



Addressing Attack Chains

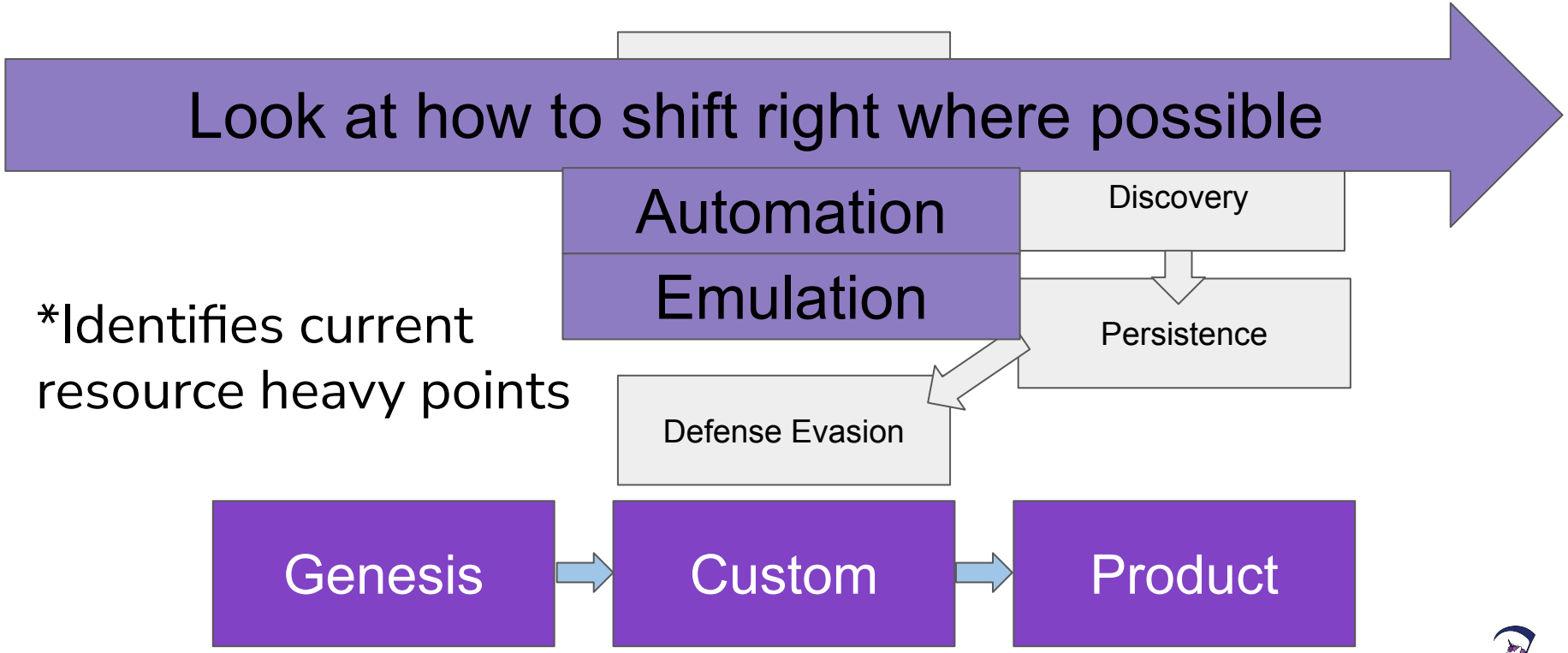


Addressing Attack Chains



*Identifies current resource heavy points

Addressing Attack Chains



*Identifies current resource heavy points

Strategies for Keeping Pace with Adversaries

SCYTHE

Strategies

Automation

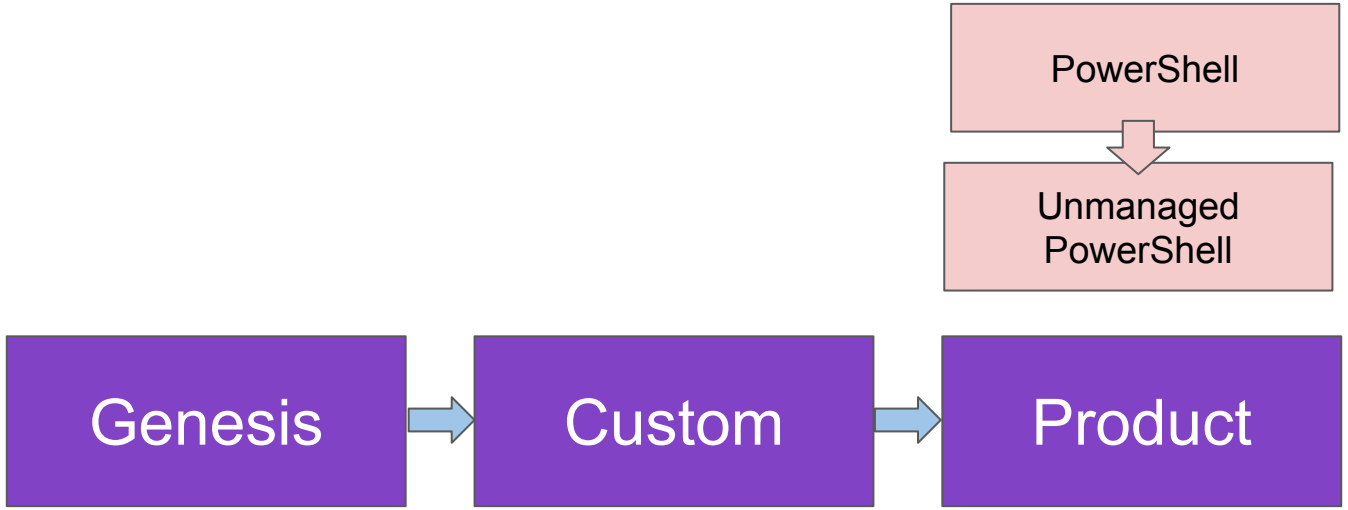
Emulation

Challenges of Automation

- Skillset differences for each phase
- Not all TTPs are scalable
- Not all TTPs are relevant

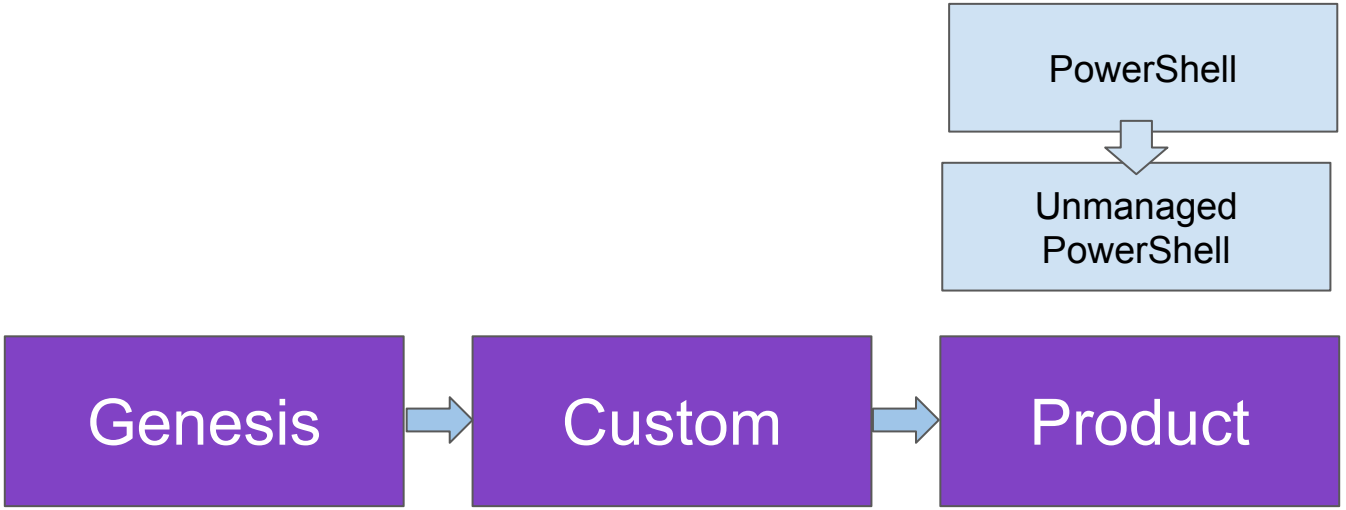
Adversary Capability Shift

Adversary switches to Unmanaged PowerShell (PowerPick)



Keeping Pace: Automation

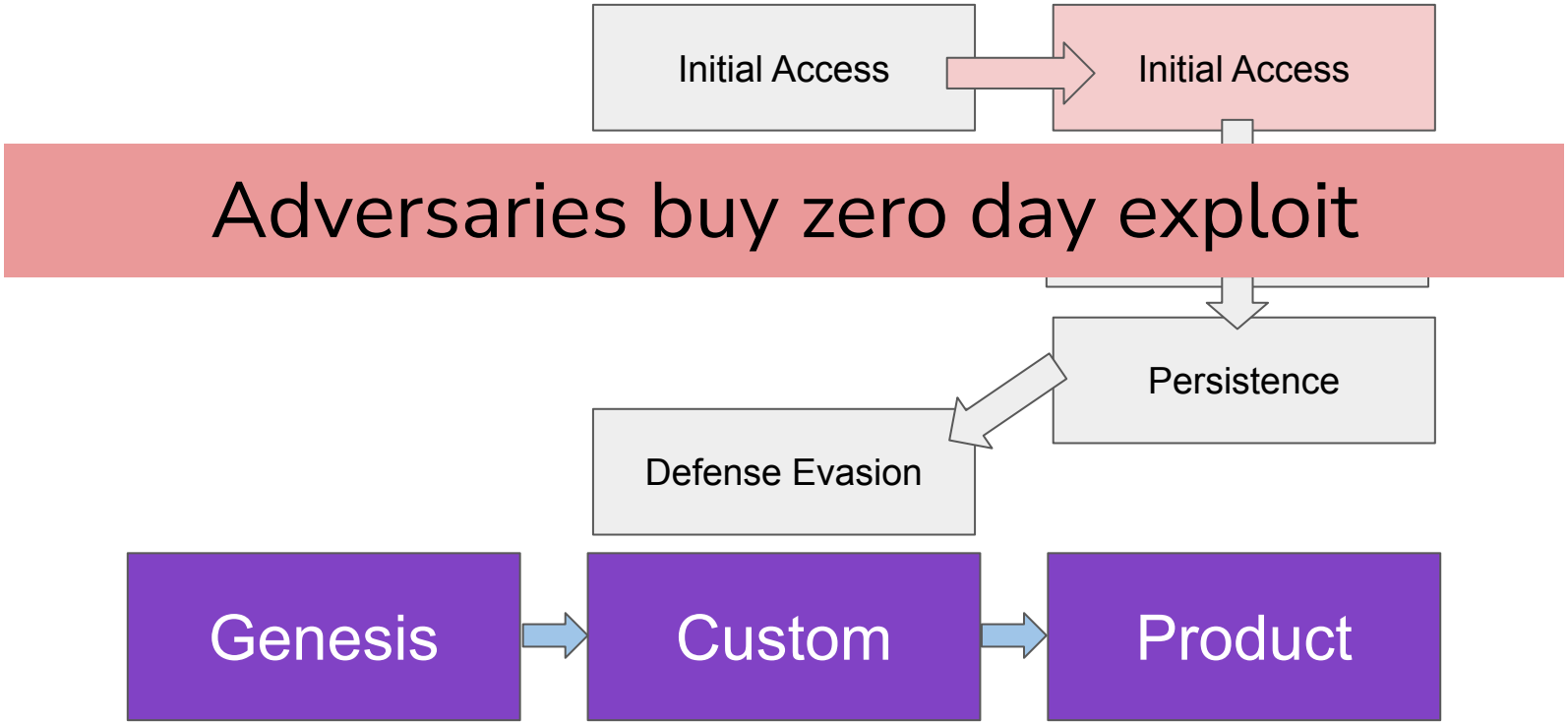
Swapping PowerShell tests to PowerPick tests to confirm detections



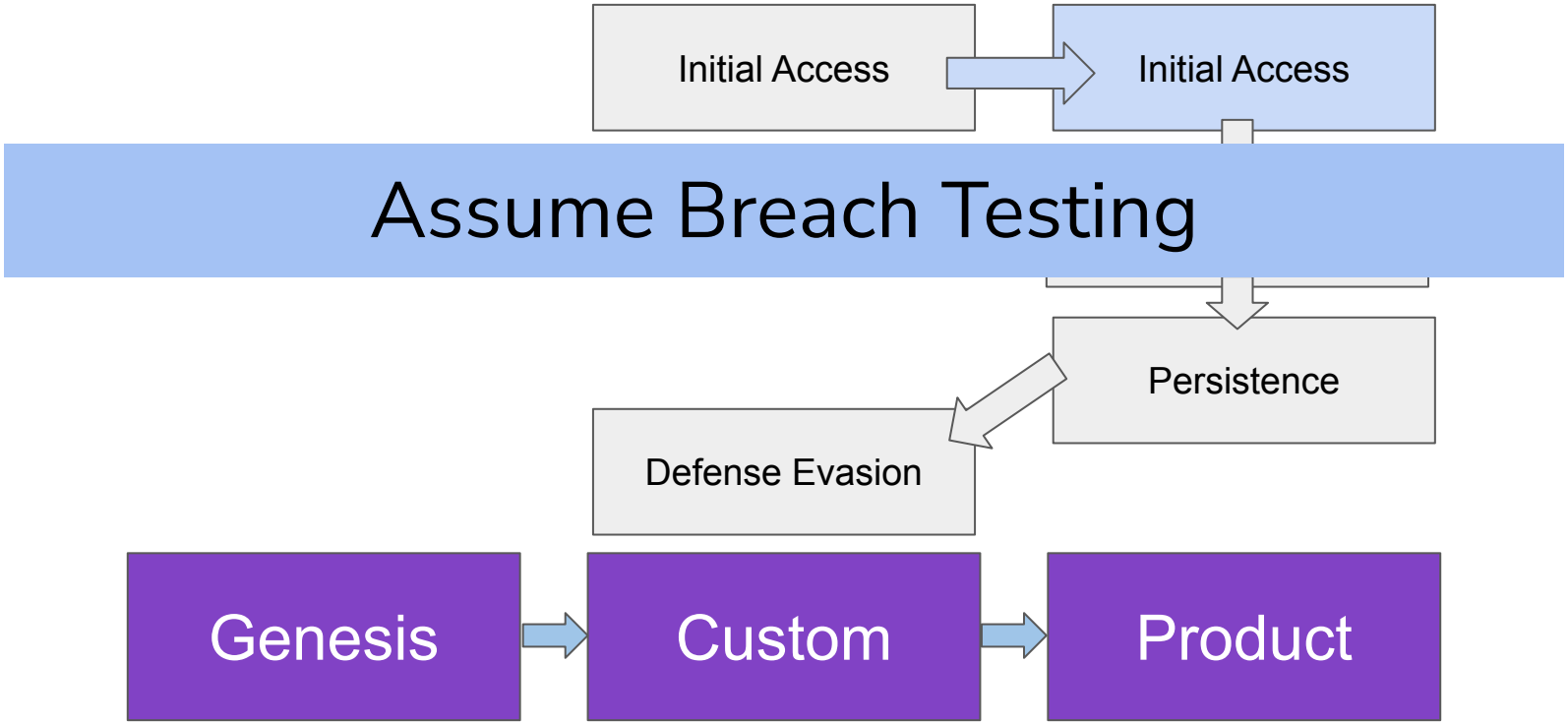
Challenges of Emulation

- Broader scope due to focus on behaviors
- Typically relied on individual expertise

Adversary Capability Shift



Keeping Pace: Emulation



Wrapping Up

Automating capabilities is as important as researching new techniques

Thanks for listening!

@teschulz

SCYTHE