Why your red team should not be special

Well it should be special but not *that* special

@isaiahsarju

Me

- Security consultant, co-owner Revis Solutions
- Red teamer
- Teacher
- Anti: nihilism, security theater, wasted time
- Pro: risk based security
- Loves islay whiskey

Why you should have a red team

- It’s not for everyone
- Need more than a pentest
- Challenge SOC/blue team
- Fine tune processes, decrease response time
- There are APTs in your threat model
- Justify security decisions with evidence

Red teams want to be special

- Dislike using corporate.*
- Manage own infrastructure
- Avoid oversight/accountability
- Believe they are un-hackable
- Think rules don’t apply to them

Scare Stories

- Naughty AWS Activity
- Lazy P3nt35t3r5
- What’s yours?

Why your red team should not be special

- Shadow IT
- Hackers can get hacked
- Lack of empathy

Red team maturity model

✓ What testing is right for us?

⚠ What should drive testing?

Organizational preparedness?

Threats in threat model?

Shadow IT

- This happens when red teams manage their own infrastructure
- Testing infrastructure
- Configuration drift
- Red teams aren’t IT departments
- Red teams can’t
  - Test
  - And help with remediation
  - And hone skills
  - And build new infrastructure
  - And maintain infrastructure
  - And do security monitoring
  - And …

Hackers can get hacked

- This happens because hackers ≠ good defenders
- Are they testing or are they hacked?
- Mentality

Lack of empathy

- This happens because hackers can be condescending
- “Just do ______”
- Corporate assets are cumbersome
- Balance security with usability
- Don’t understand how hard processes are to follow
- Red teams need to take their own medicine

What’s NOT the answer?

- “Here’s a laptop just like everyone else. Go forth and test”
- Give them a nice MacBook and say “show me me your worst”
- Ugh. Security is expensive. Goat sacrifices and crossed fingers are cheaper

A good approach

General

- Have red teams lead by example
- Plan for exceptions
- Keep data on "internal" infrastructure
- Allow current risk owners to keep owning risk

Technical

- Institute principle of least common mechanism
- Mediate data transfer
- Apply principle of least privilege policies

A good outcome

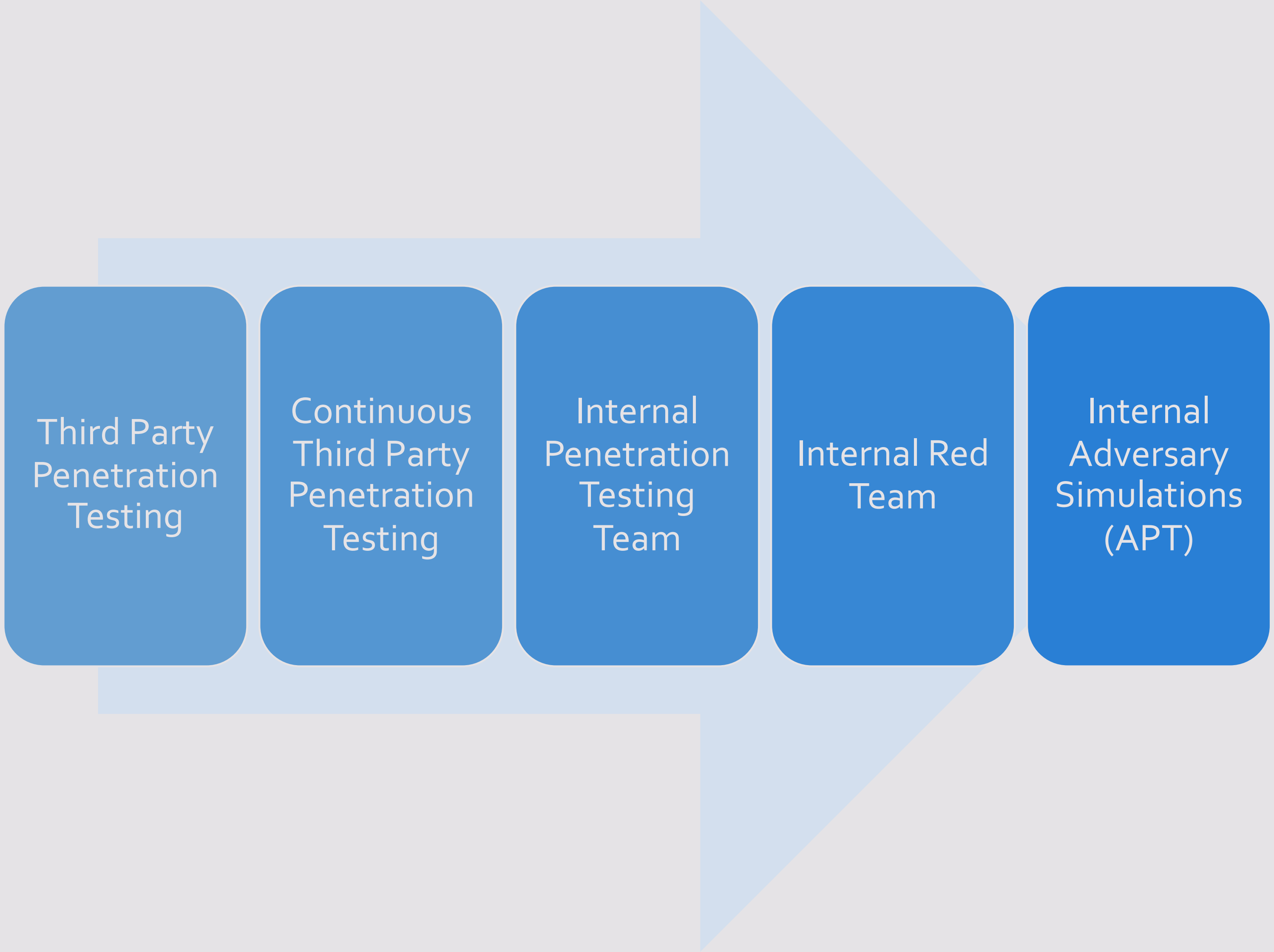
General

- Understand infrastructure/policies/procedures
- Grow together as a red/blue team
- Offload risk to current risk owners
- Build relationships that are necessary down the road

Technical

- Implement defense-in-depth
- Log, monitor, and differentiate between activity
- Allow red team to focus on what they do best

Red team maturity model



Third Party Penetration Testing

Continuous Third Party Penetration Testing

Internal Penetration Testing Team

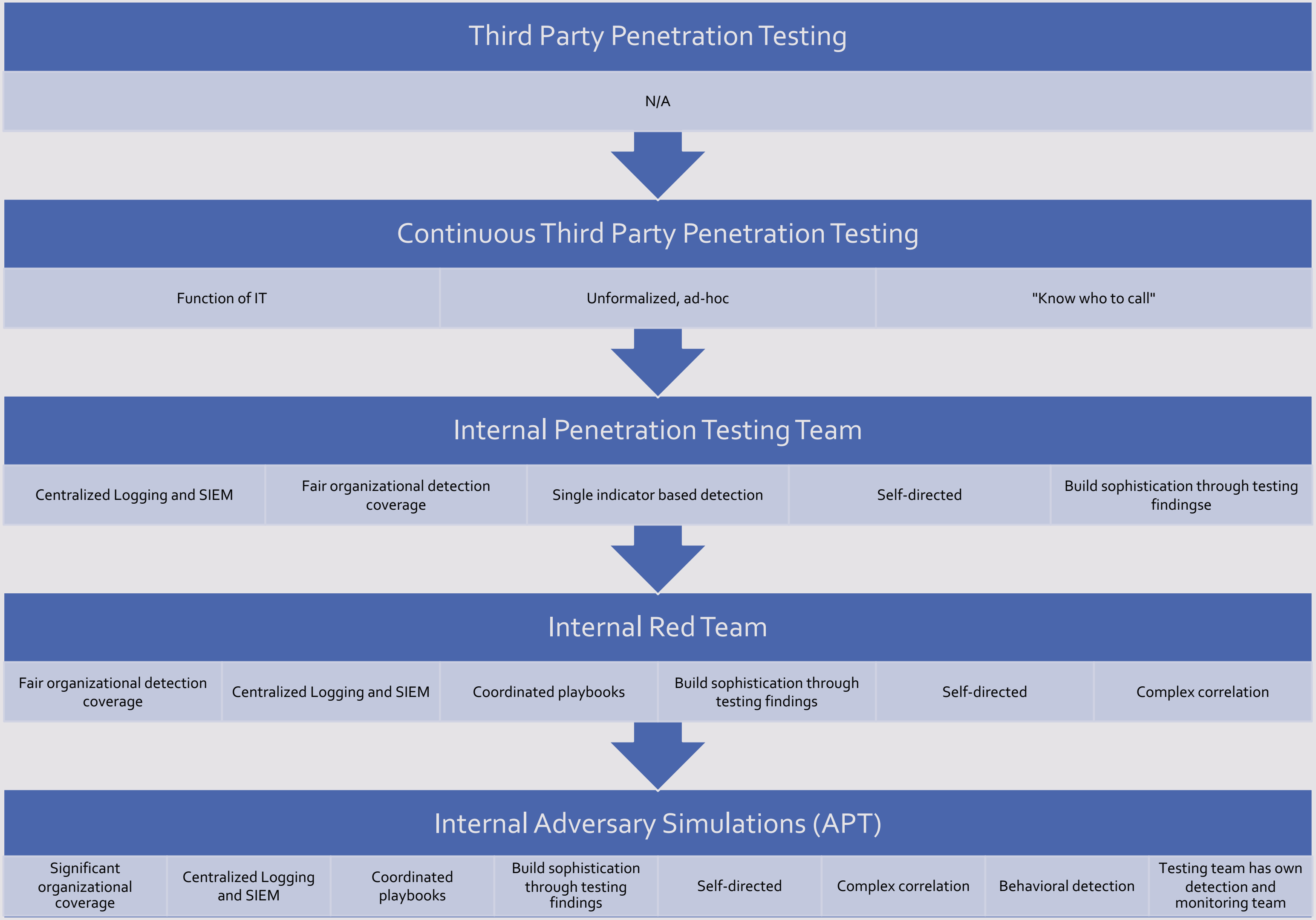
Internal Red Team

Internal Adversary Simulations (APT)

Red team maturity model indicators

- Infrastructure
- Organizational posture
- IT support capabilities
- IR capabilities
- Threat Intel
- Operator skill sets
- SOC capabilities
- Types of testing

RTMM SOC capabilities



Third Party Penetration Testing

N/A

Continuous Third Party Penetration Testing

- Function of IT
- Unformalized, ad-hoc
- "Know who to call"

Internal Penetration Testing Team

- Centralized Logging and SIEM
- Fair organizational detection coverage
- Single indicator based detection
- Self-directed
- Build sophistication through testing findingse

Internal Red Team

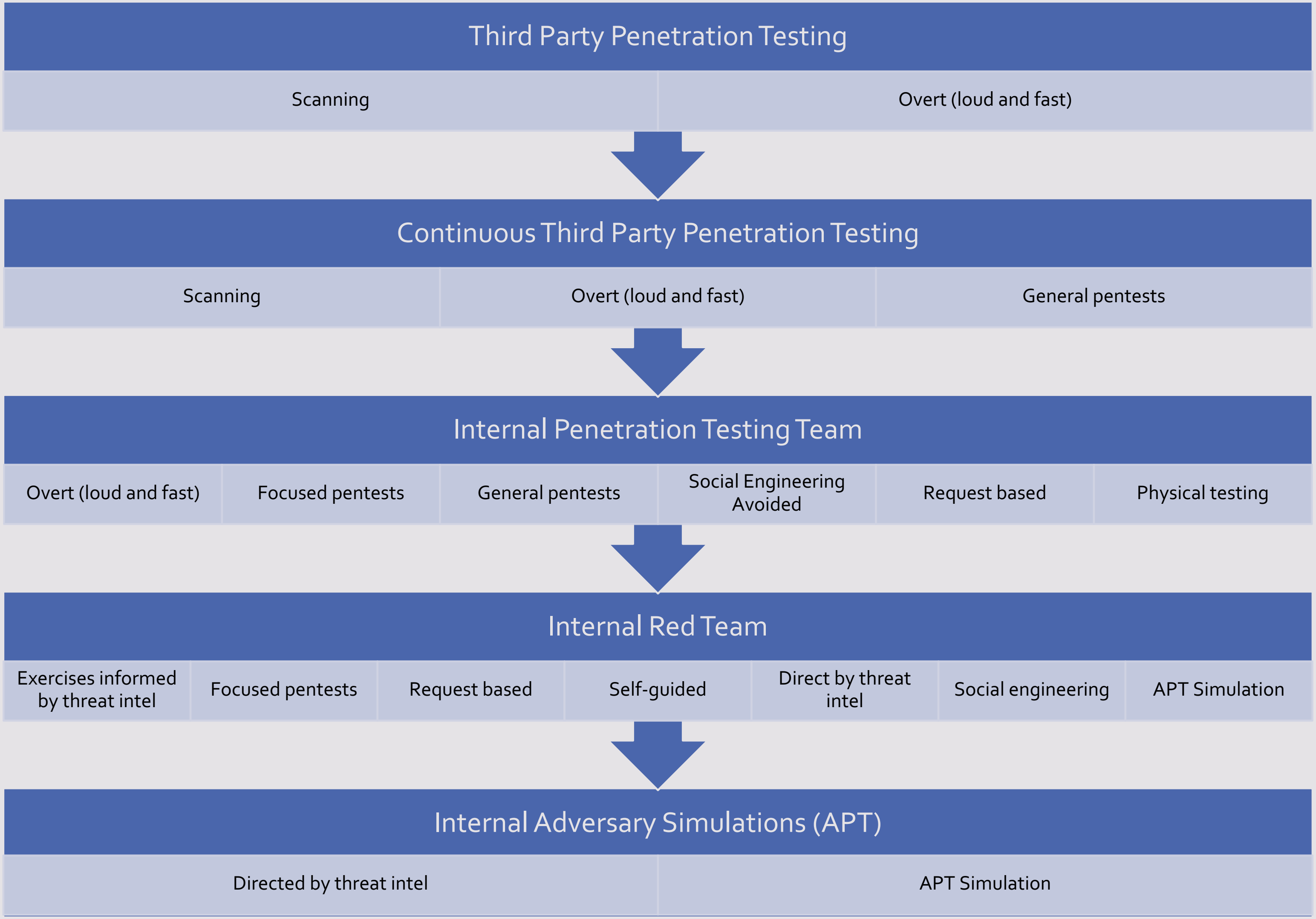
- Fair organizational detection coverage
- Centralized Logging and SIEM
- Coordinated playbooks
- Build sophistication through testing findings
- Self-directed
- Complex correlation

Internal Adversary Simulations (APT)

- Significant organizational coverage
- Centralized Logging and SIEM
- Coordinated playbooks
- Build sophistication through testing findings
- Self-directed
- Complex correlation
- Behavioral detection
- Testing team has own detection and monitoring team

@isaiahsarju

RTMM types of testing



Third Party Penetration Testing

Scanning | Overt (loud and fast)

Continuous Third Party Penetration Testing

Scanning | Overt (loud and fast) | General pentests

Internal Penetration Testing Team

Overt (loud and fast) | Focused pentests | General pentests | Social Engineering Avoided | Request based | Physical testing

Internal Red Team

Exercises informed by threat intel | Focused pentests | Request based | Self-guided | Direct by threat intel | Social engineering | APT Simulation

Internal Adversary Simulations (APT)

Directed by threat intel | APT Simulation

Why tie RTMM to staff preparedness vs actual threats?

Folks

Aren’t

Ready

Wrap this up

- May be unpopular. Especially with operators
- Red teams need to take a dose their own medicine
- Red teams can lead by example and build positive relationships
- Future Research: “Map” RTMM to ATT&CK

Info

- @isaiahsarju all over The Internet
- https://github.com/isaiahsarju/presentations

Questions?