RSAConference2018

Singapore | 25–27 July | Marina Bay Sands

#RSAC

SESSION ID: SEM-W01C

MACHINE VS. MACHINE: THE FUTURE OF HACKING

Adi Ashkenazy

VP Product
XM Cyber
@XM_Cyber

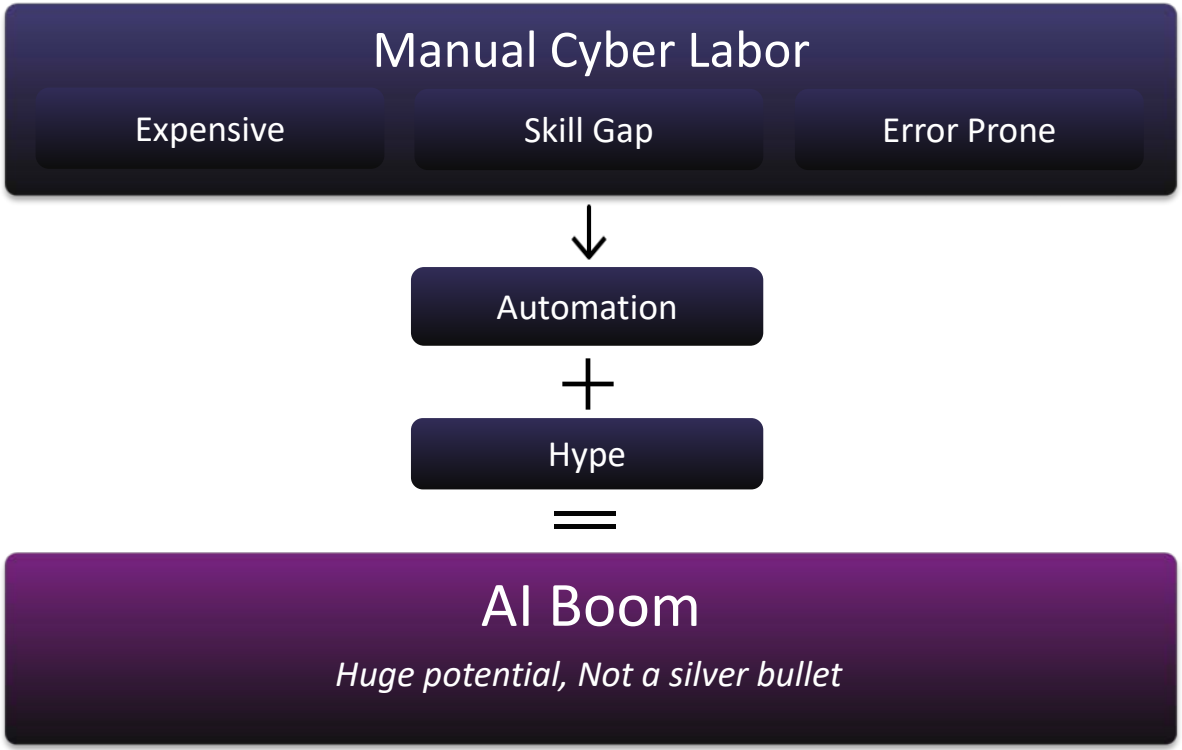
ABOUT ME

Led an offensive cyber unit
in government service

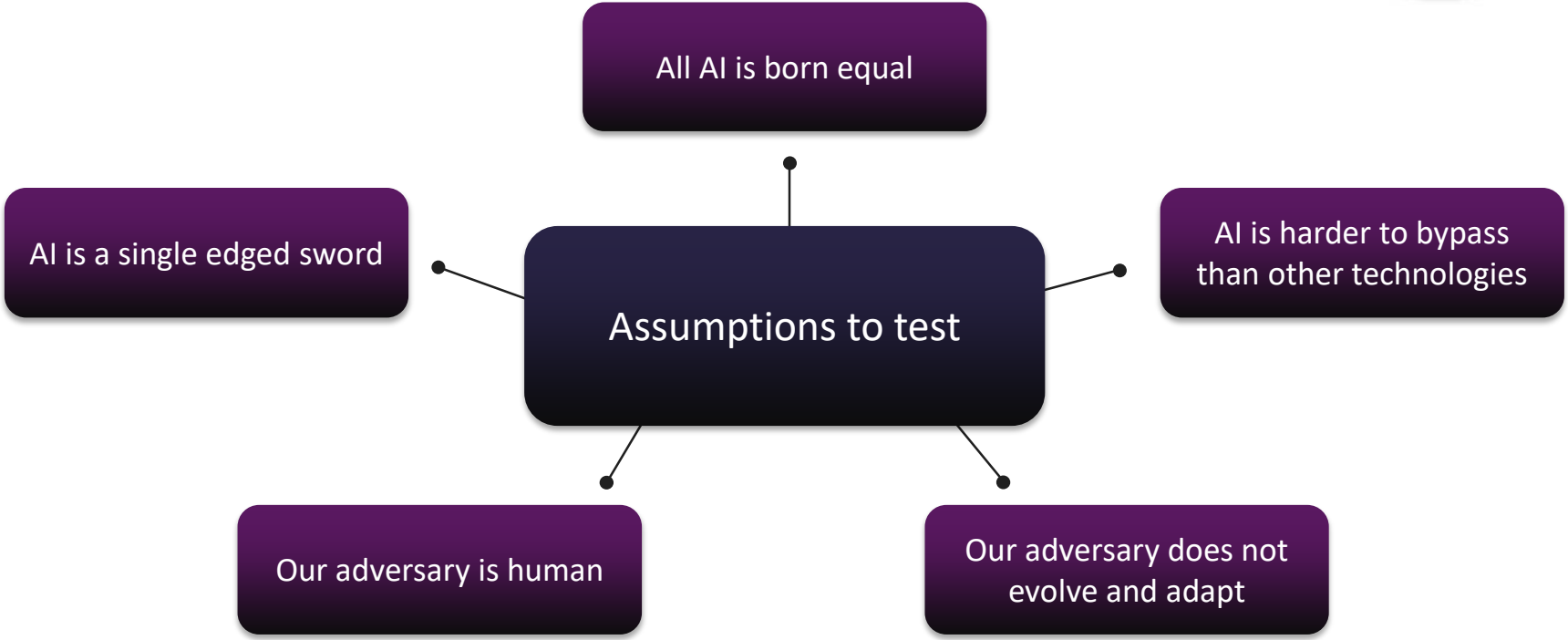
Have been designing and building an automated hacking machine as VP Product @ XM Cyber

A few disclaimers

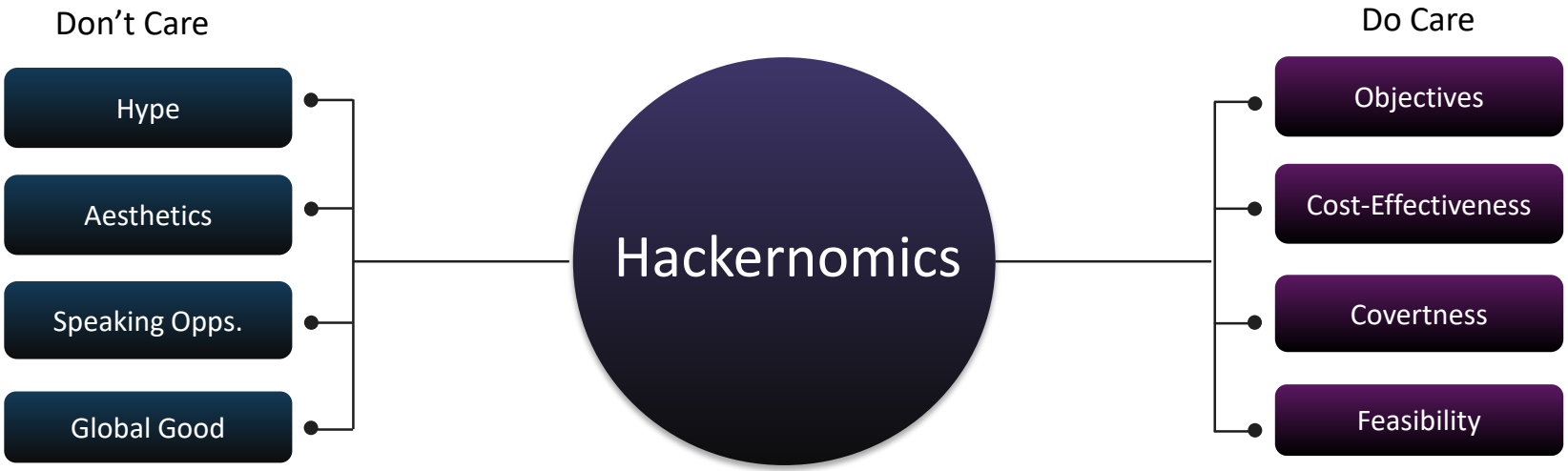
RISE OF THE (FRIENDLY) MACHINES



ASSUMPTIONS EVERYWHERE



AN OFFENSIVE CYBER APPROACH TO AI

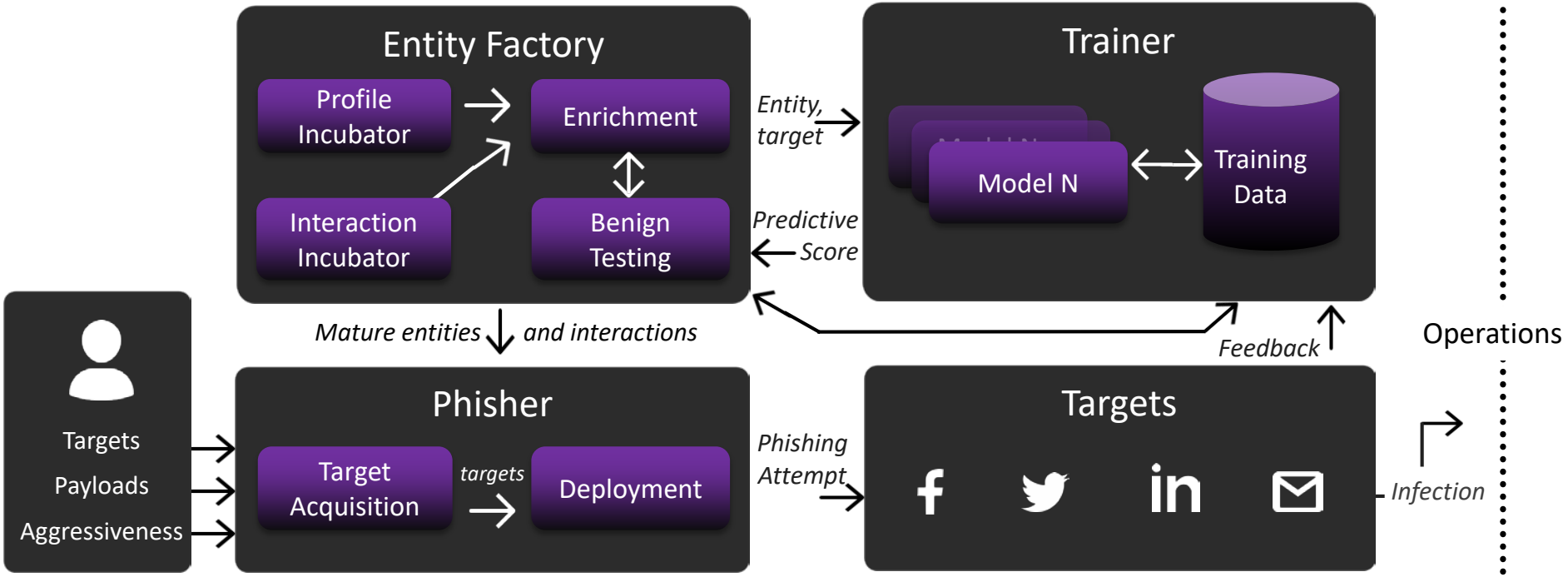


Let's build the machine together !

INITIAL BREACH

- Objectives: scale, targeting, avoid early detection
- Social engineering reigns supreme
- Direct exploits are commonly automated
- How can we cost-effectively use “AI”:
  - Train and enrich entities and interactions.
  - Machine vs. Machine expected - anti-phishing algorithms
  - Potentially phishing interactions for same target (watered down Turing test).

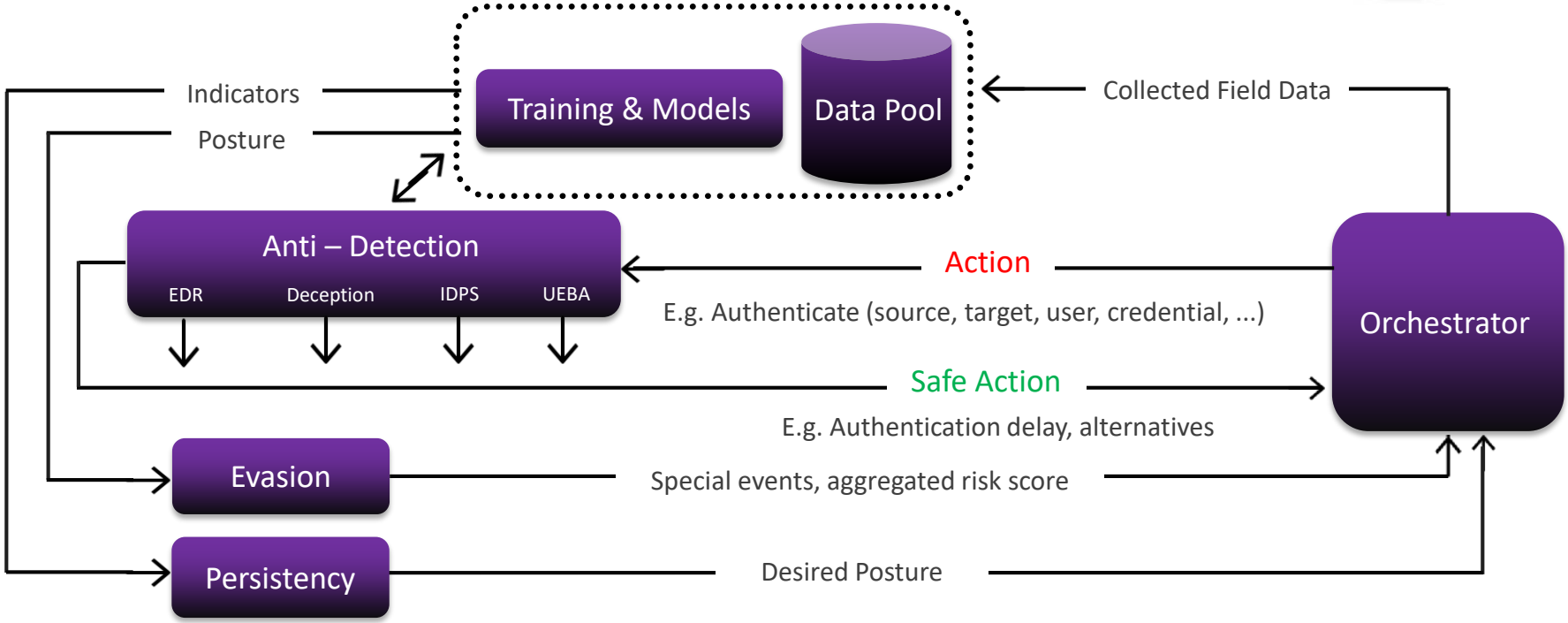
INITIAL BREACH – FLOW



SAFETY FIRST!

- Help our system make decisions based on risk appetite vs. aggressiveness over the lifetime of our activity.
  - Anti-Detection
  - Evasion
  - Persistency
- This is where we can test some of the silver bullet marketing…

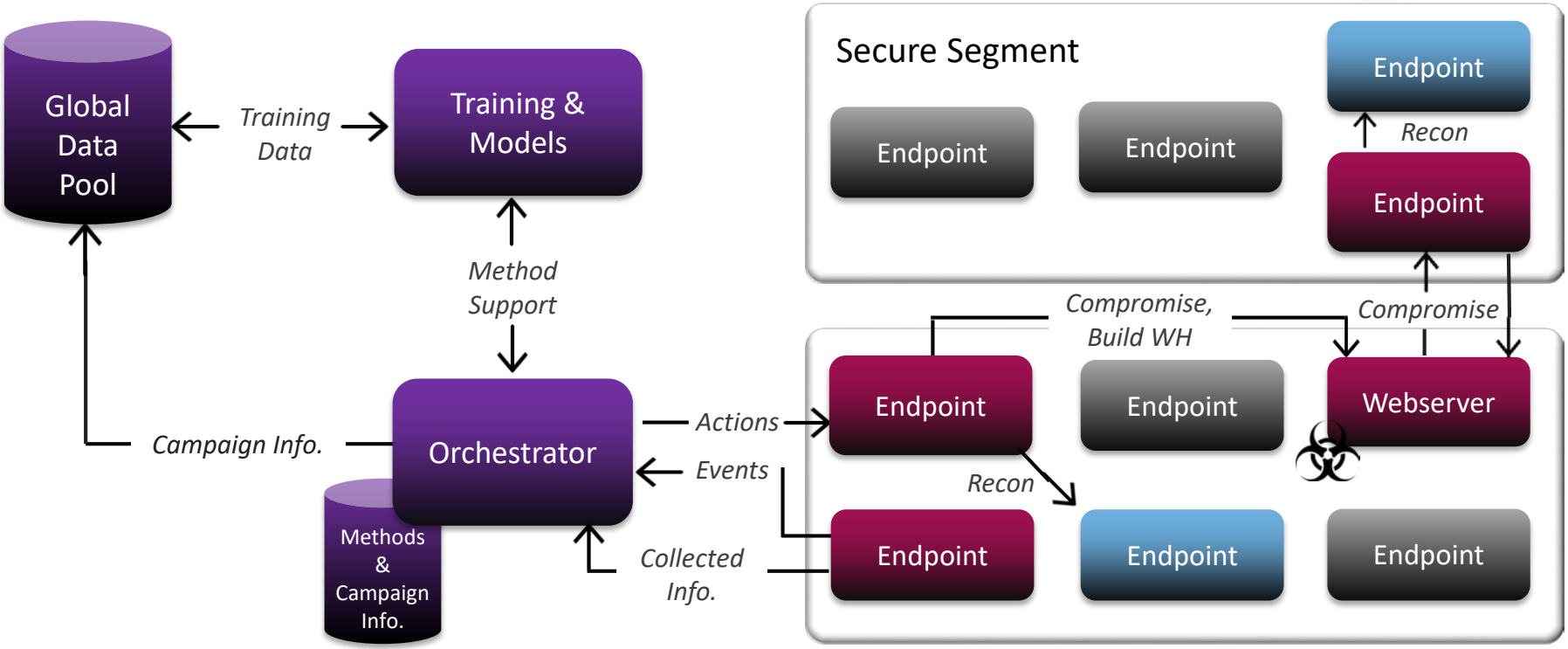
SAFETY FIRST! FLOW



LATERAL MOVEMENT

- Objectives
  - Network dominance
  - Asset centric - data, network, device.
- Single orchestrator entity controlling all activities:
  - Triggers request for information from compromised endpoints
  - Event driven state machine, controlling next action.
- Learning can be utilized across attacks to enhance (selected samples):
  - Target (next move) prioritization - identify high value targets, minimize steps.
  - Password guessing
  - Automated staging/multi-stage attacks - identify potential for watering holes, shared exe infection etc.

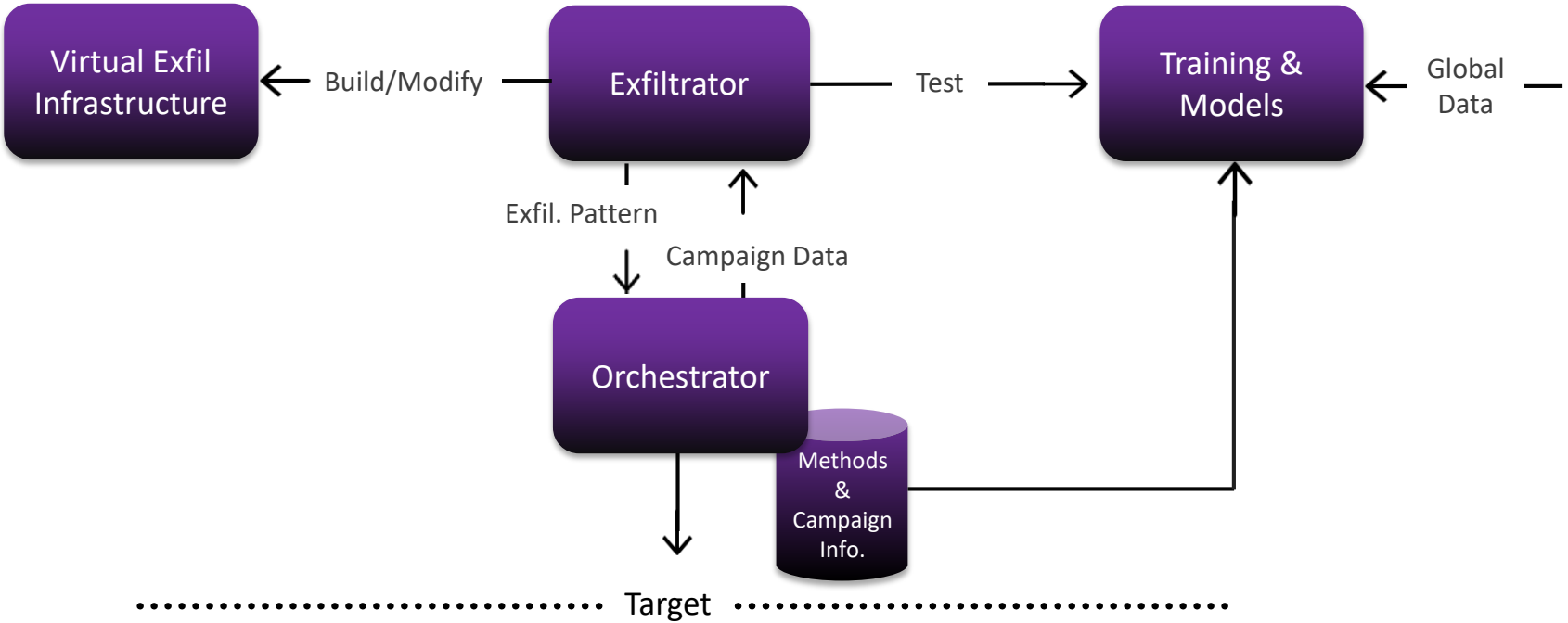
LATERAL MOVEMENT FLOW



EXFILTRATION

- Identify communication patterns
  - Protocol
  - Volume
  - Timing
  - Route
- Use default channel for minimal C2
- Set up and modify exfiltration infrastructure automatically as closest match (region, supplier, protocols etc.).

EXFILTRATION – FLOW



FINAL TAKEAWAYS

- Building an autonomous attacking machine is feasible with 2018 technology.
- Only questions are motivation and economic tipping point vs. manual labor, on a per module basis.
- Current autonomous defensive approach will need to evolve rapidly:
  - DO NOT assume static/human adversary
  - PRIORITIZE cross vendor cooperation and information sharing
  - INVEST in threat modelling and internal red teams

Thank you!

info@xmcyber.com