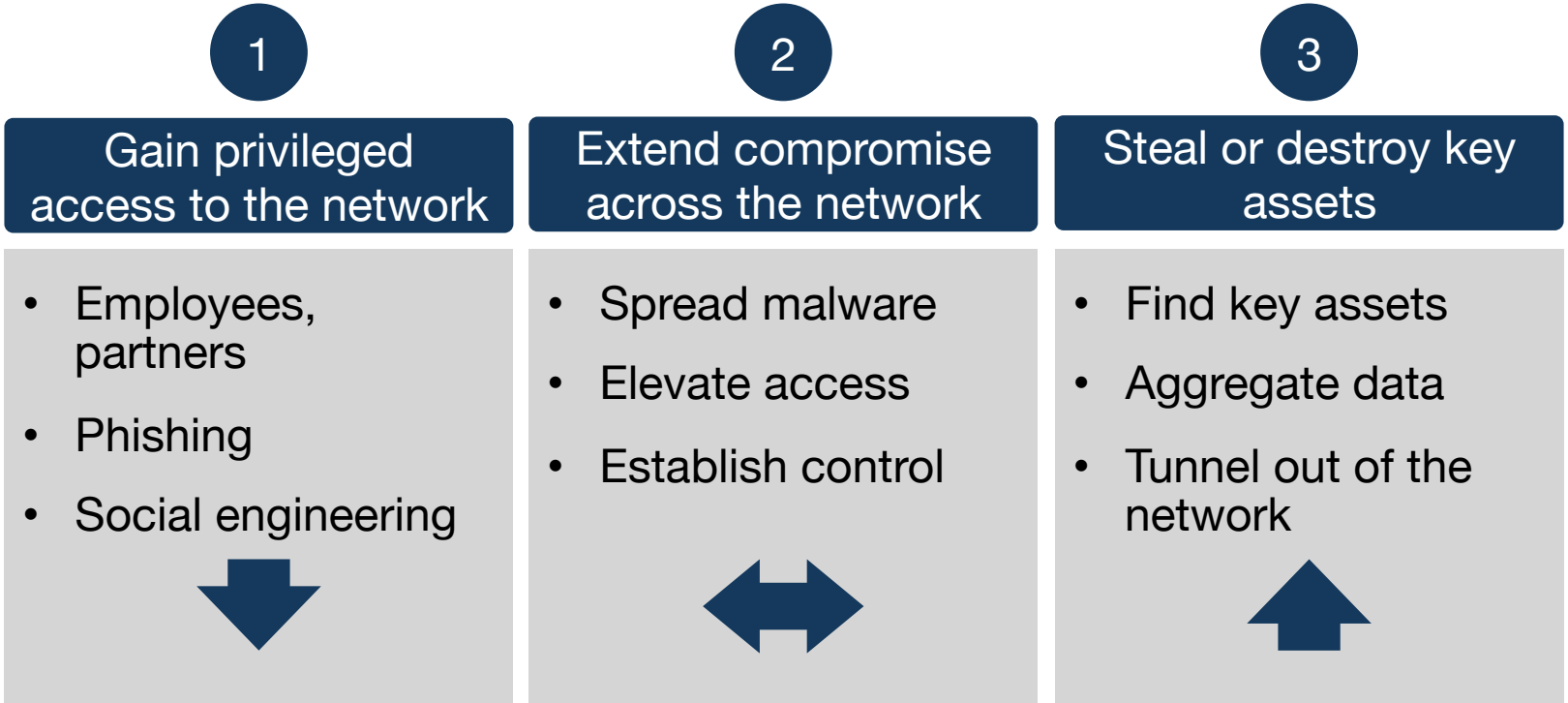
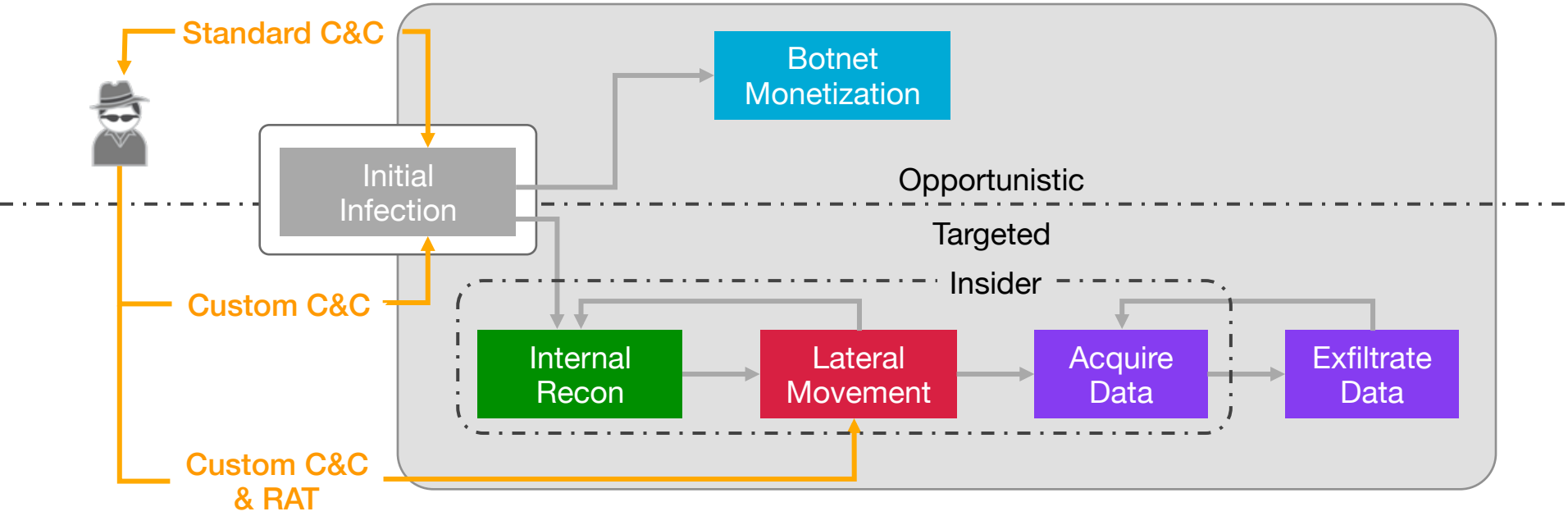
VECTRA

Automatically Detect Ongoing Cyber Attacks in Real Time

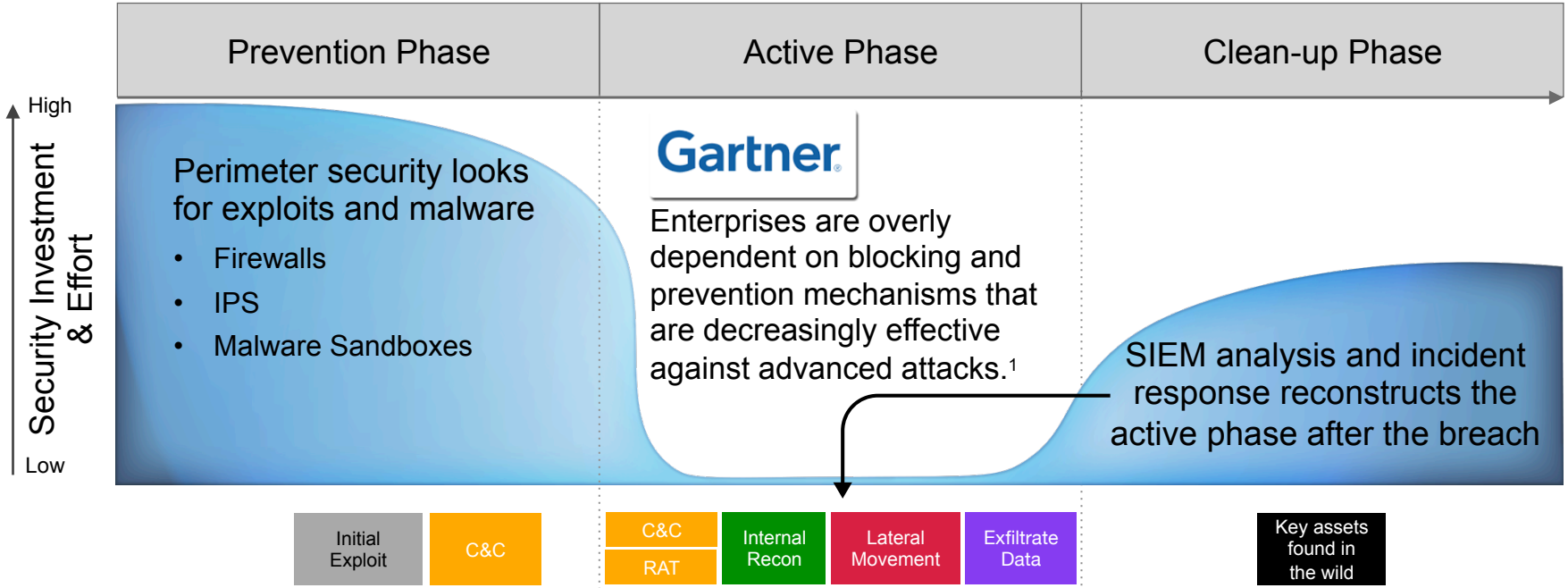
The cyber attacker blueprint



A closer look at modern cyber attacks



Perimeter security and SIEMs can't detect ongoing attacks



[1] Designing an Adaptive Security Architecture for Protection from Advanced Attacks, 12 February 2014, ID G00259490

How we automatically detect ongoing attacks in real time

- All packets
- N-S, E-W traffic
- Any OS, app, device

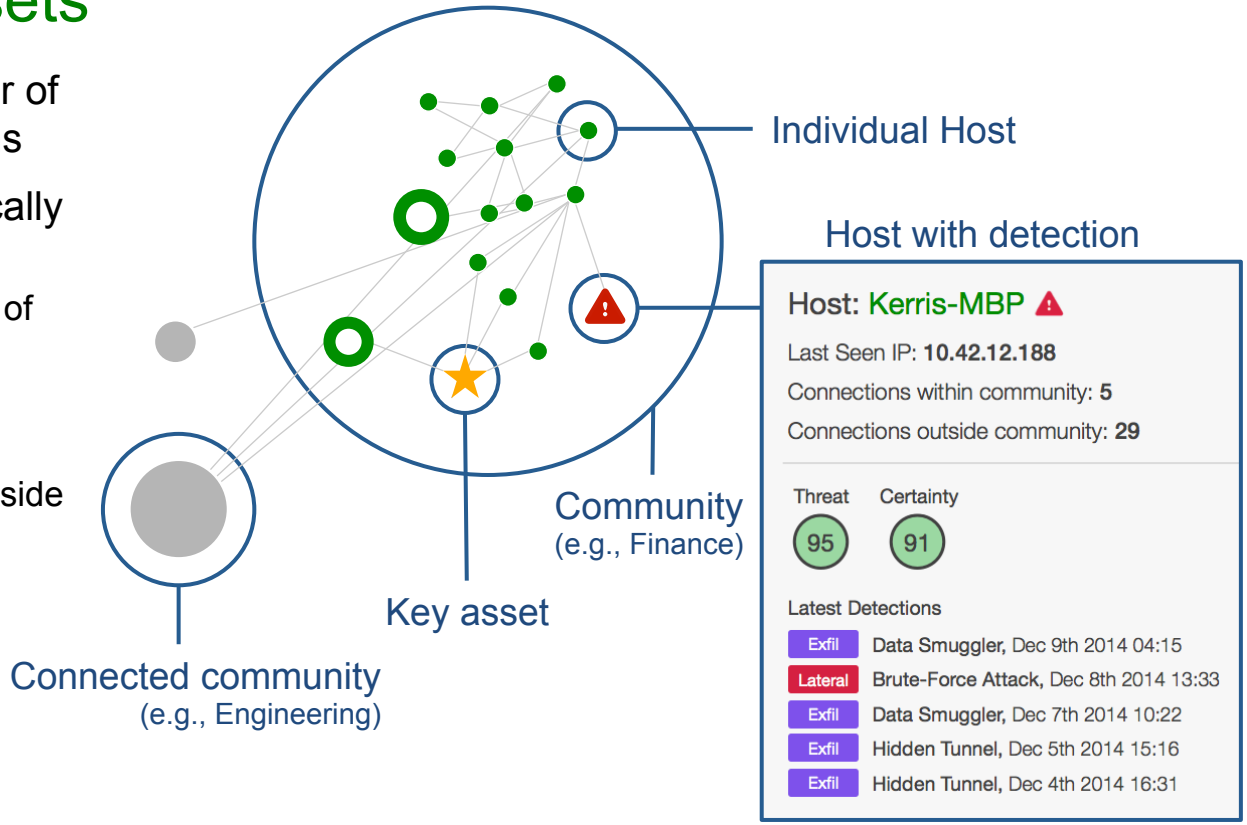
- Behavioral
- Machine learning
- Correlated over time

- No signatures
- No rules
- No configuration

- Prioritized by risk
- Correlated by host
- Insight into attack

Community Threat Analysis centers investigation on Insider Threat and Key Assets

- Puts key assets at the center of real-time threat investigations
- Communities built automatically based on network activity
  - Displays proximity and impact of threats to key assets
  - Dynamically shows the progression of an attack
  - Reveals devices operating outside their normal communities
- Enables faster, smarter decisions




VECTRA™
Security that thinks.™