CONTROLLING YOUR OWN BATTLESPACE

From Threat Response Teams

To Threat Intelligence Teams

Agenda

- Motivations
- The Intelligence Process
- The Cyber Kill Chain Approach
- Indicators of Compromise
- Information Sharing
- Takeaways

Today's Threat Landscape

Organized attackers

Increasing volume

Sophisticated

Remediation is broken

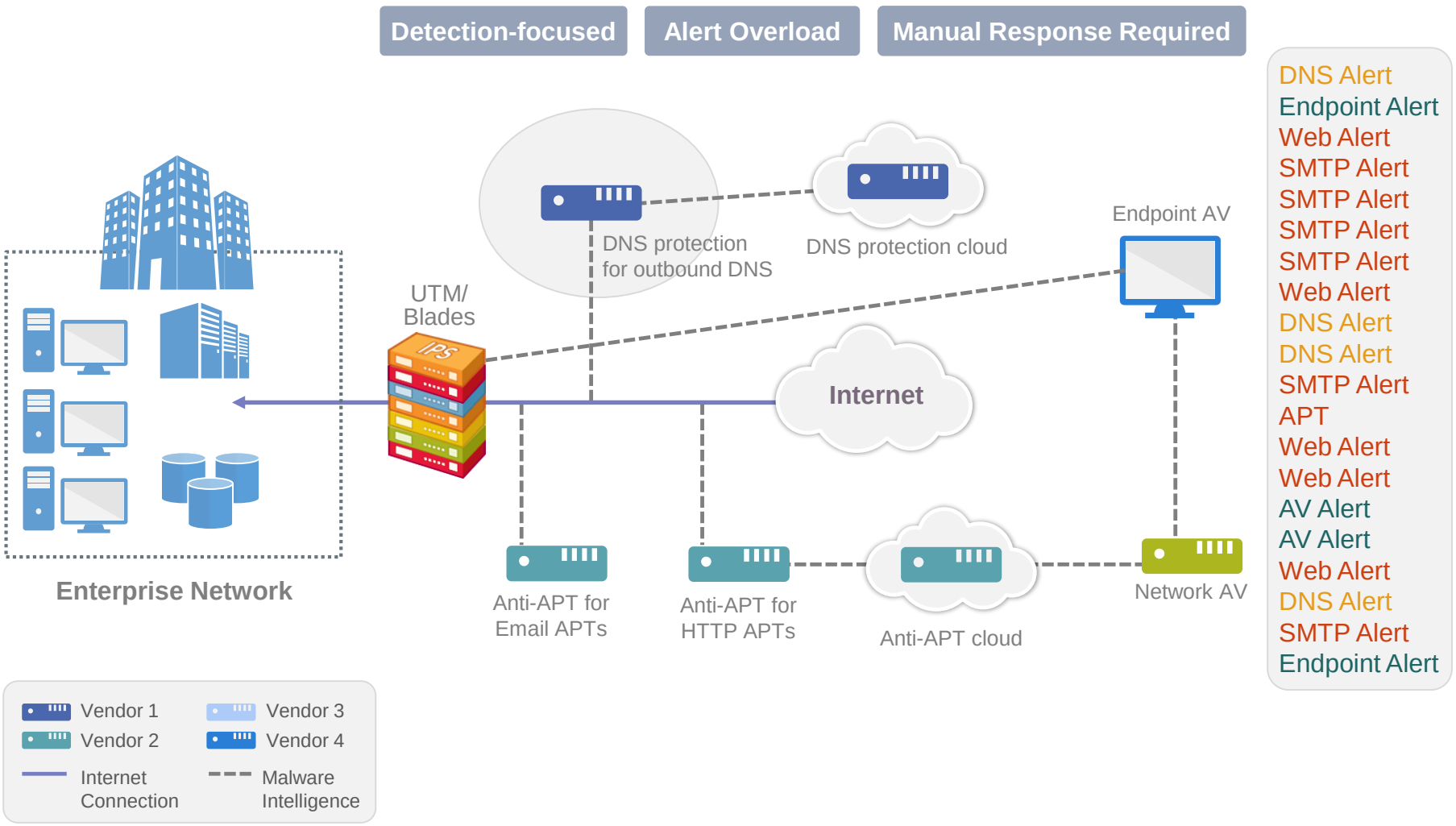
Must prevent attacks across perimeter, cloud and endpoint

Limited correlation across disjointed security technologies

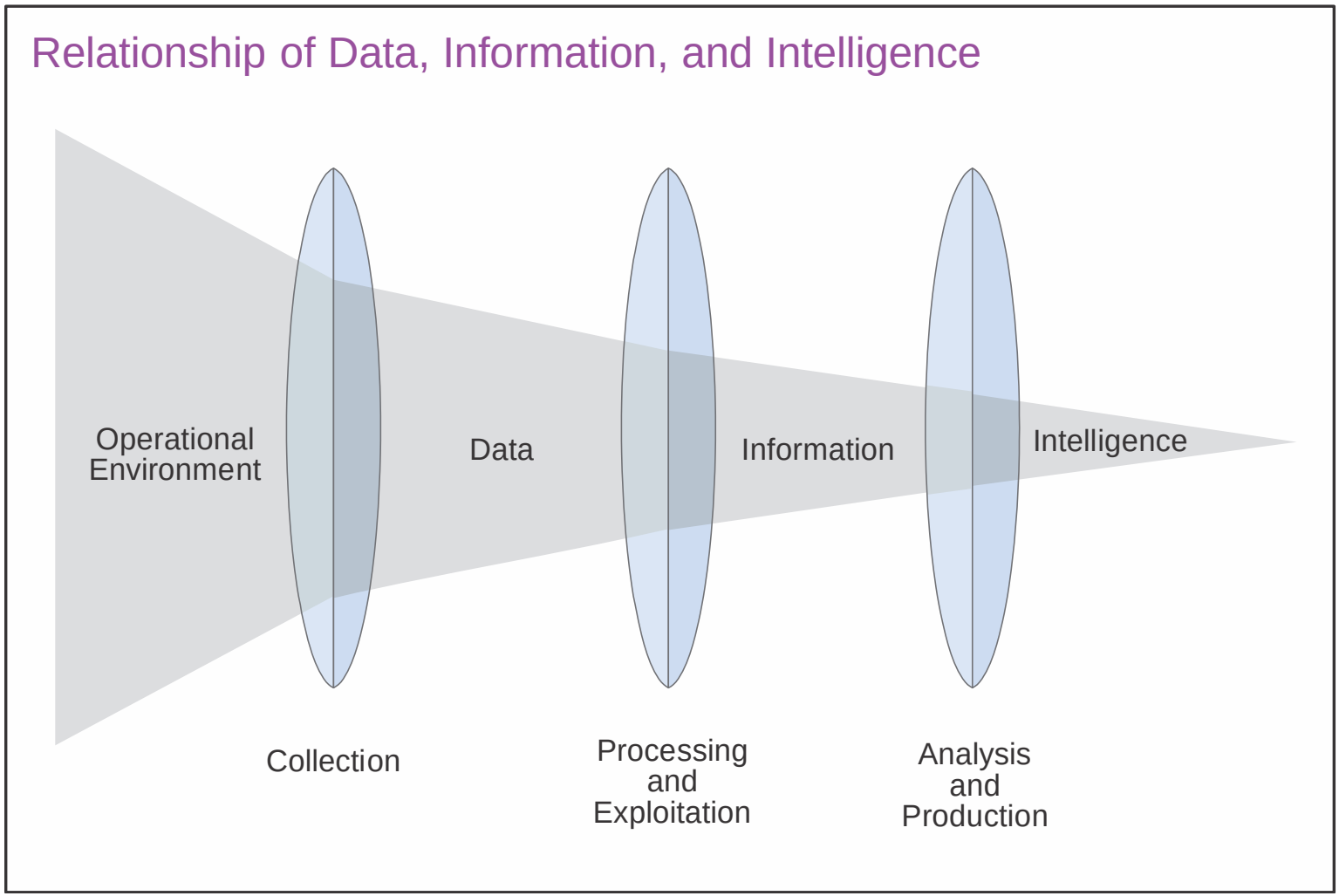
Limited security expertise

CSO challenges

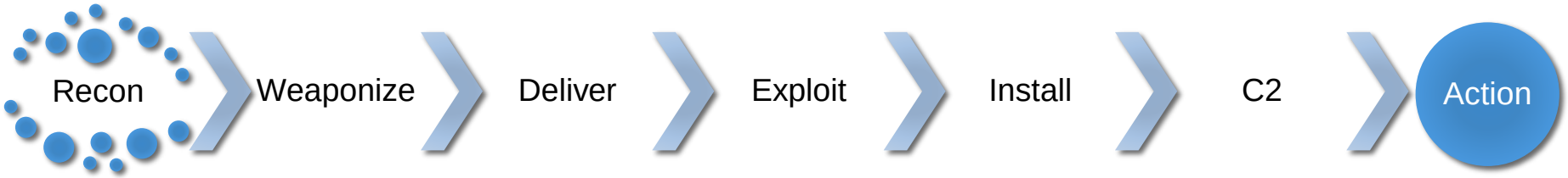
Information Overload



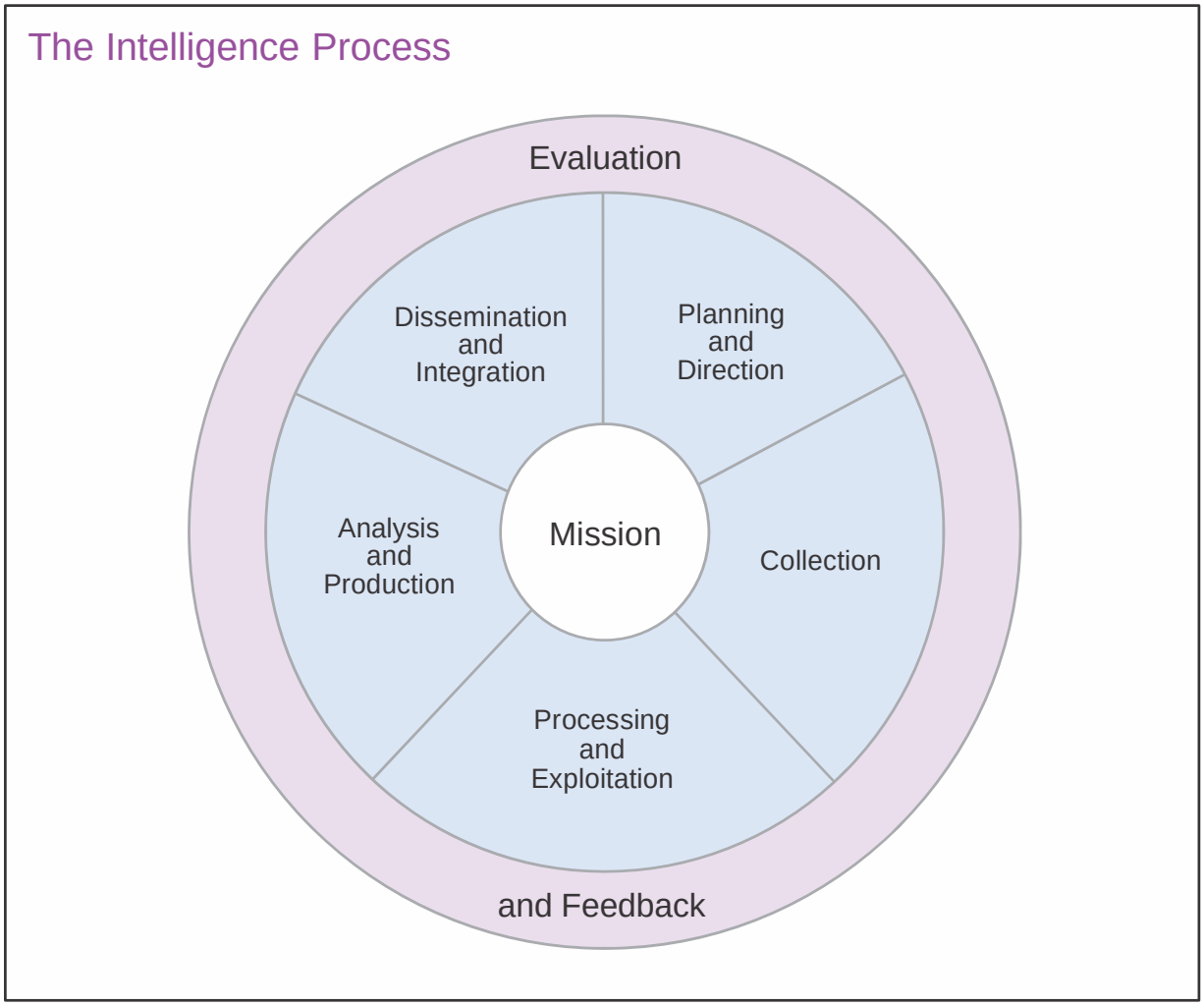
Cyber Kill Chain



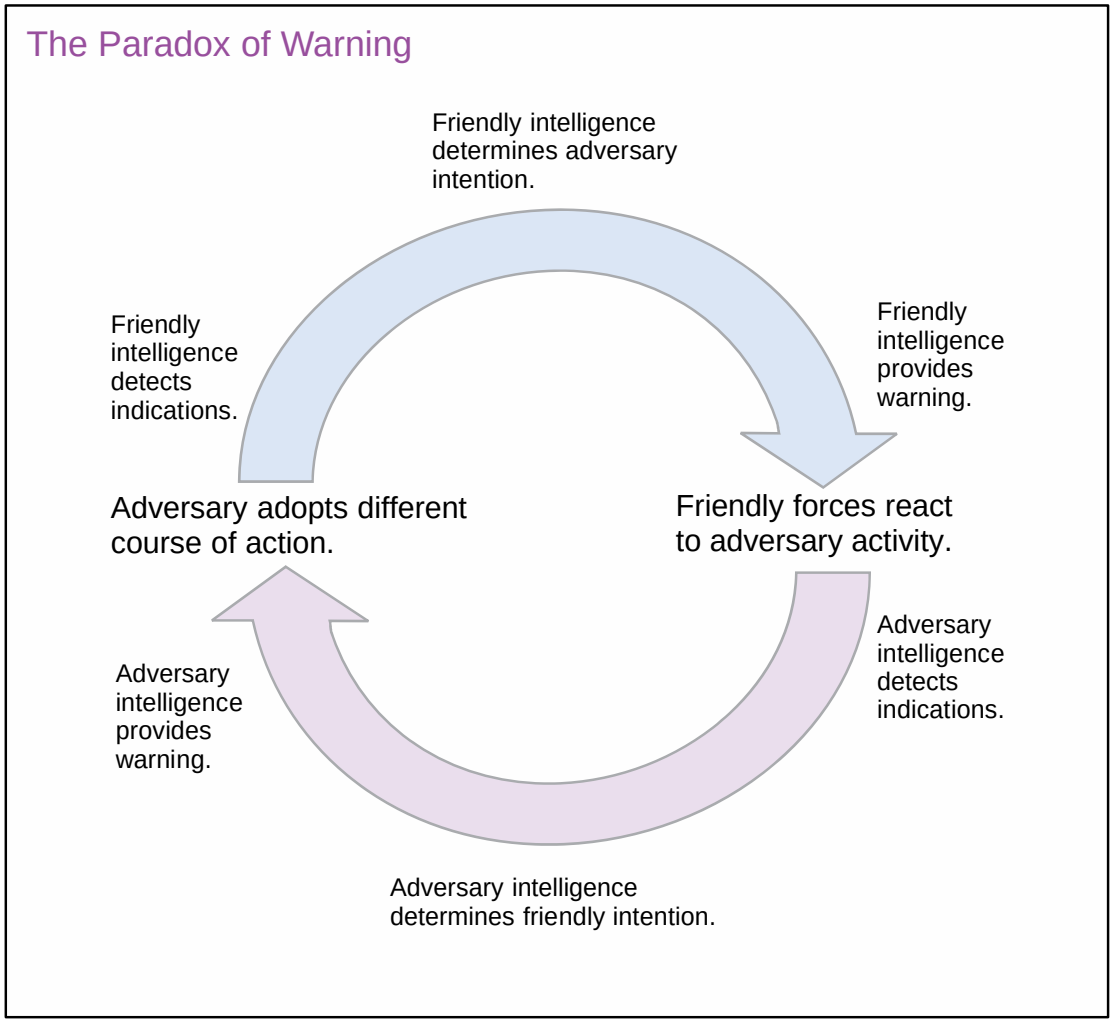
Cyber Kill Chain



The Intelligence Process



The Intelligence Process



Indicators of Compromise

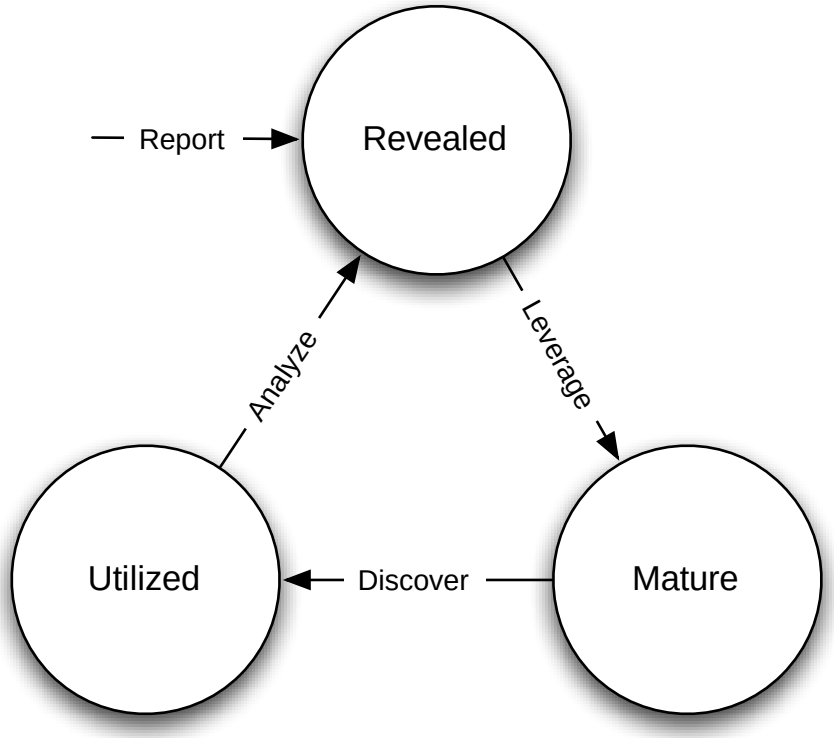
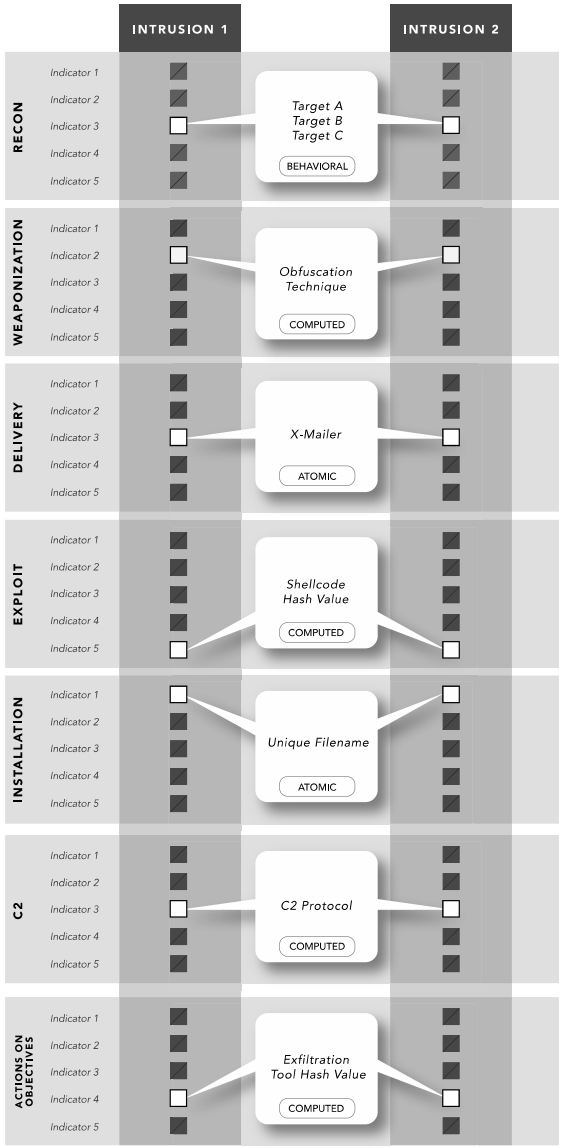


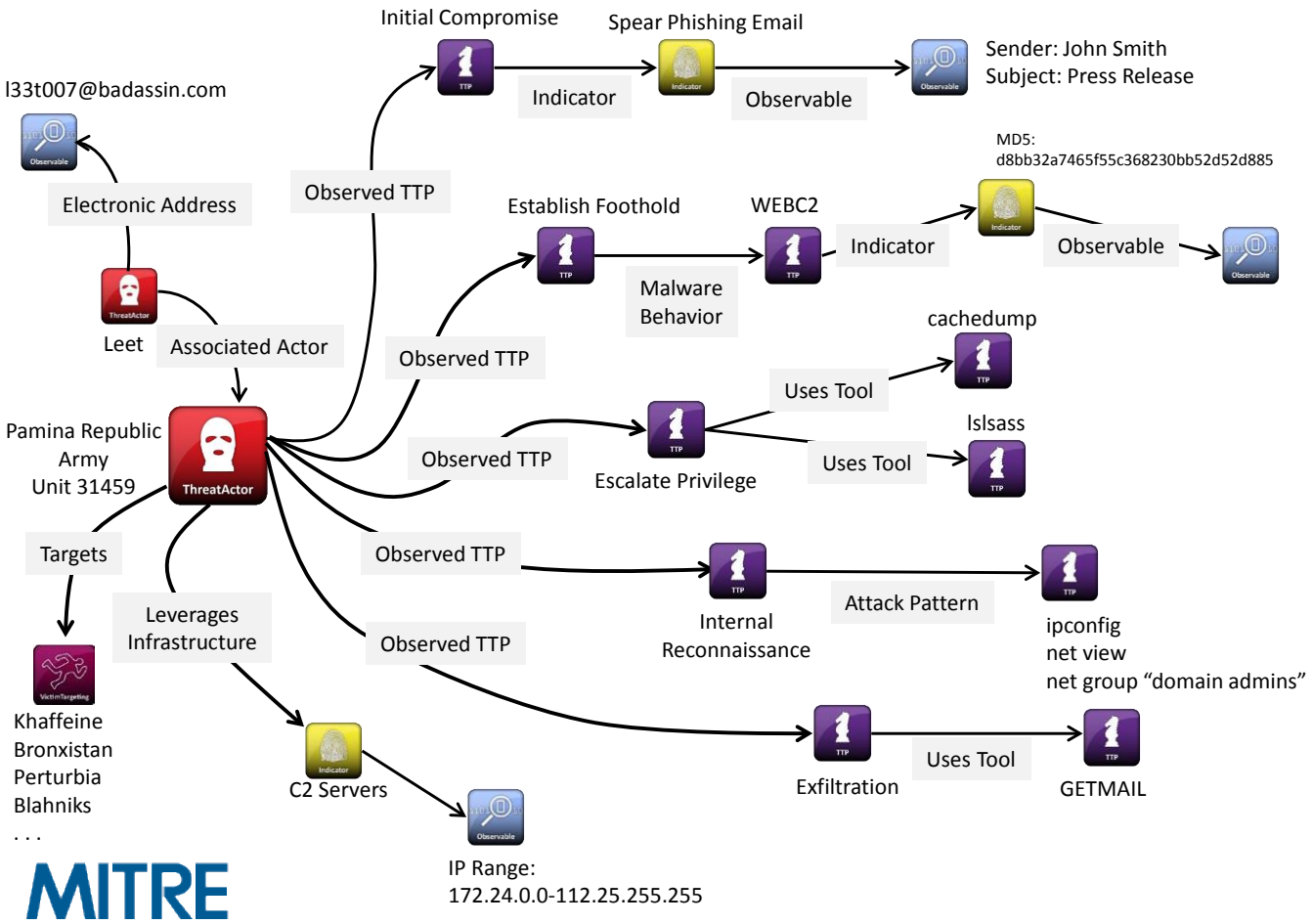
Figure 1: Indicator life cycle states and transitions

Indicators of Compromise



Information Sharing

Expressing Relationships in STIX



Information Sharing

FINANCIAL SERVICES ISAC

REN-ISAC

ES ISAC
Electricity Sector Information
Sharing Analysis Center

a division of cyber squared inc.
THREATCONNECT
Driven by community. Defined by intelligence.

NH-ISAC
National Health ISAC

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Takeaways

- Move onus of security ops from reactionary to proactive
  (Incident Response to Threat Intelligence)
- Place and tune your defensive sensors appropriately
  Use the intelligence feedback loop
- Don’t do it alone