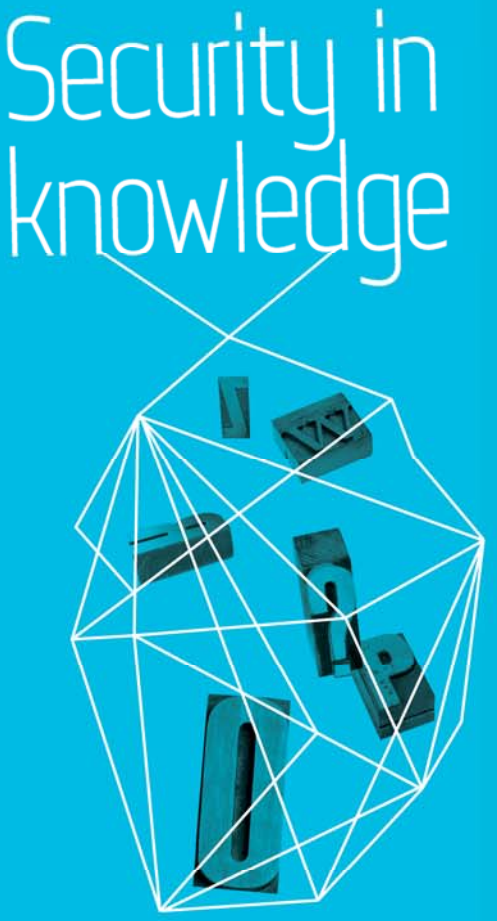
RSA CONFERENCE ASIA PACIFIC 2013



THREE ADVERSARIES – KNOW YOUR ENEMY

Paul Stamp
RSA

Session ID: CLE-W05
Session Classification: General Interest

Agenda

- The changing world
- Attackers and their motivation
- Characterizing attack probablility
- Defending against different adversaries

The changing world we live in

The "community" of attackers

Criminals

Petty criminals

Unsophisticated

Organized crime

Organized, sophisticated supply chains (PII, financial services, retail)

Nation state actors

PII, government, defense industrial base, IP rich organizations

Non-state actors

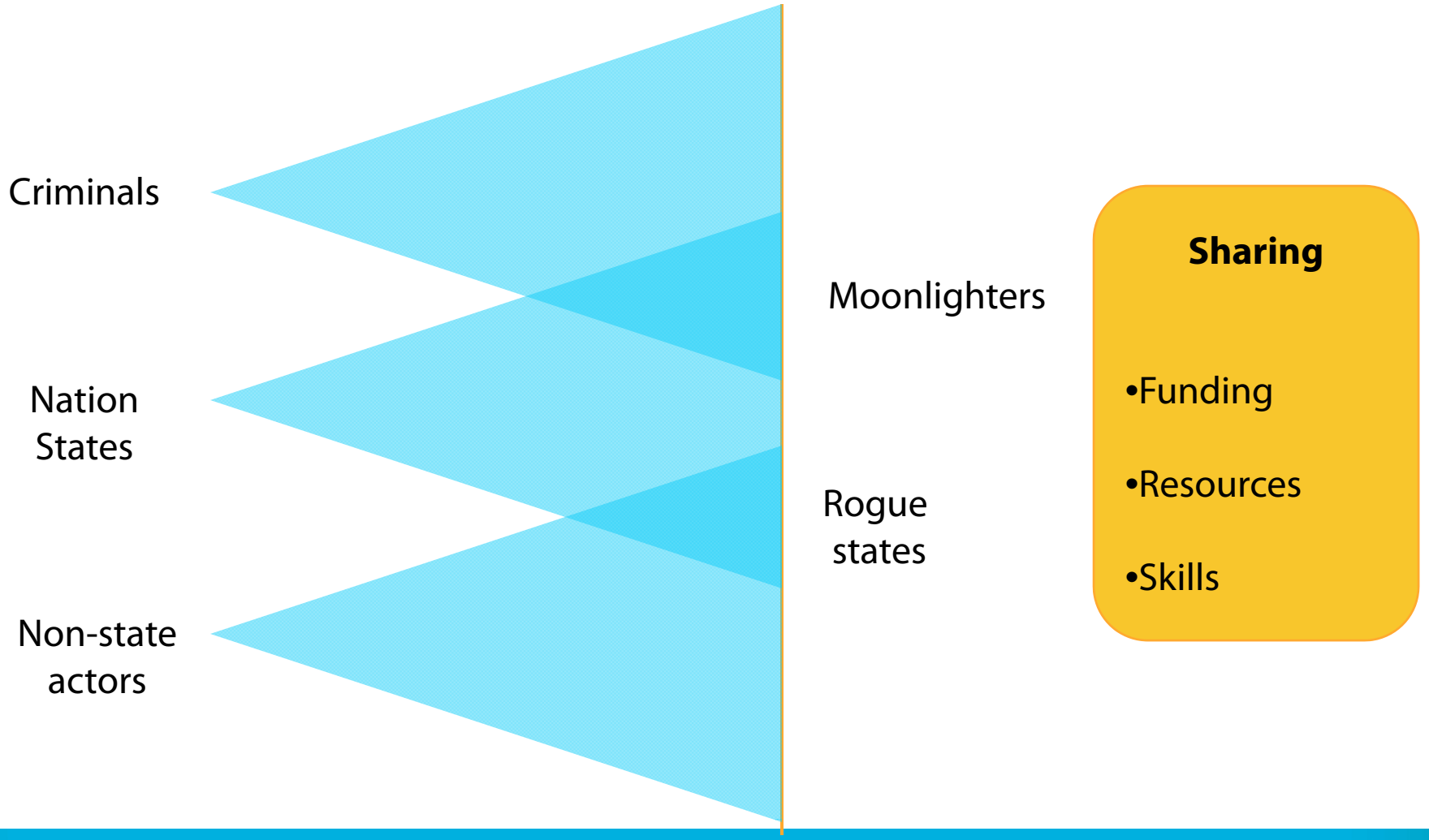
Terrorists

PII, Government, critical infrastructure

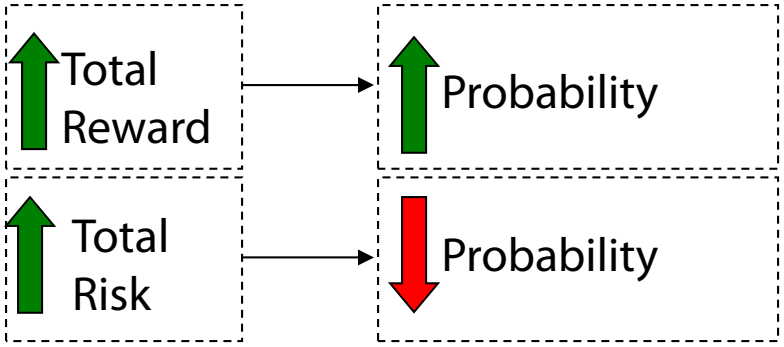
Anti-establishment vigilantes

"Hacktivists"
Targets of opportunity

When attackers converge?



The Law of Attack Probability



Therefore

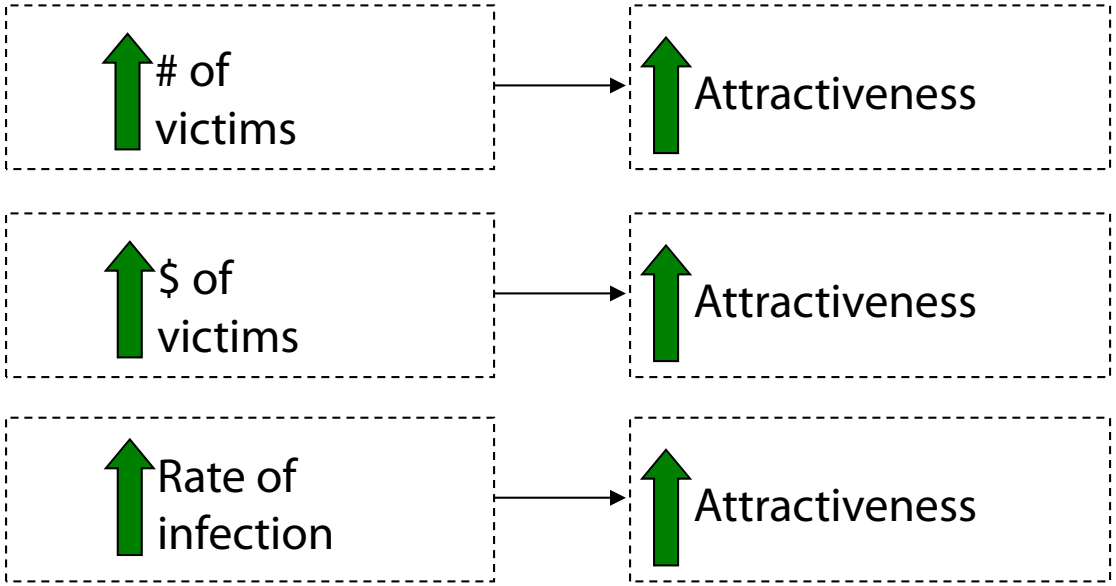
$$\text{Probability} \propto \frac{\text{Total Reward}}{\text{Total Risk}}$$

Or…

$$P_V \propto \frac{A_V}{D_V * R_V}$$

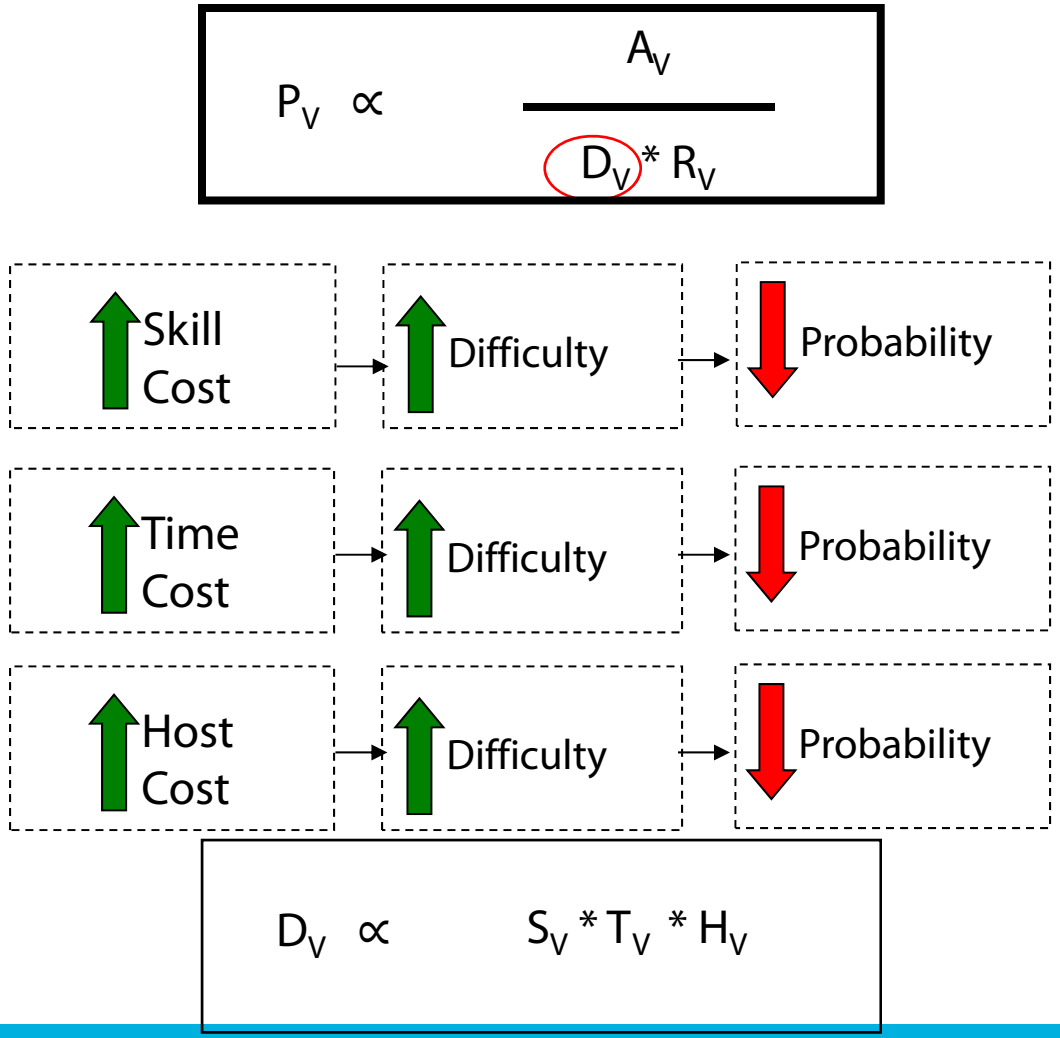
Target's Attractiveness

$$P_V \propto \frac{A_V}{D_V * R_V}$$



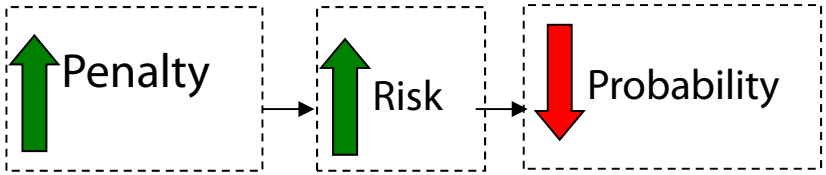
$$A_V \propto \#_V * V_V * R_V$$

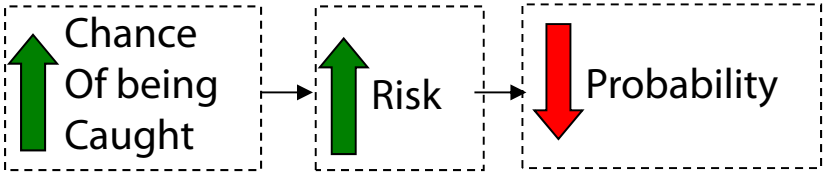
Difficulty (raw cost) of a Vector



"Risk" to the Attacker

$$P_V \propto \frac{A_V}{D_V * R_V}$$





$$R_V \propto P_V * \%C_V$$

As a defender…

- Do you have to be "Faster than the bear"…or faster than the next guy?

…it depends if the attacker is financially motivated or not

Defending against Cybercriminals

- Motivation
  - Financial all the way
  - Driven by a "profit per hack" metric
- Preferred Methods
  - Consumer targeted trojans, keyloggers etc.
  - "Supply chain" of off-the-shelf tools & infrastructure
- Decrease A_V
  - Reduce R_v by not storing required information
- Increase D_V
  - Make it too costly
  - Can often get this information anywhere
  - Be "faster than the next guy"

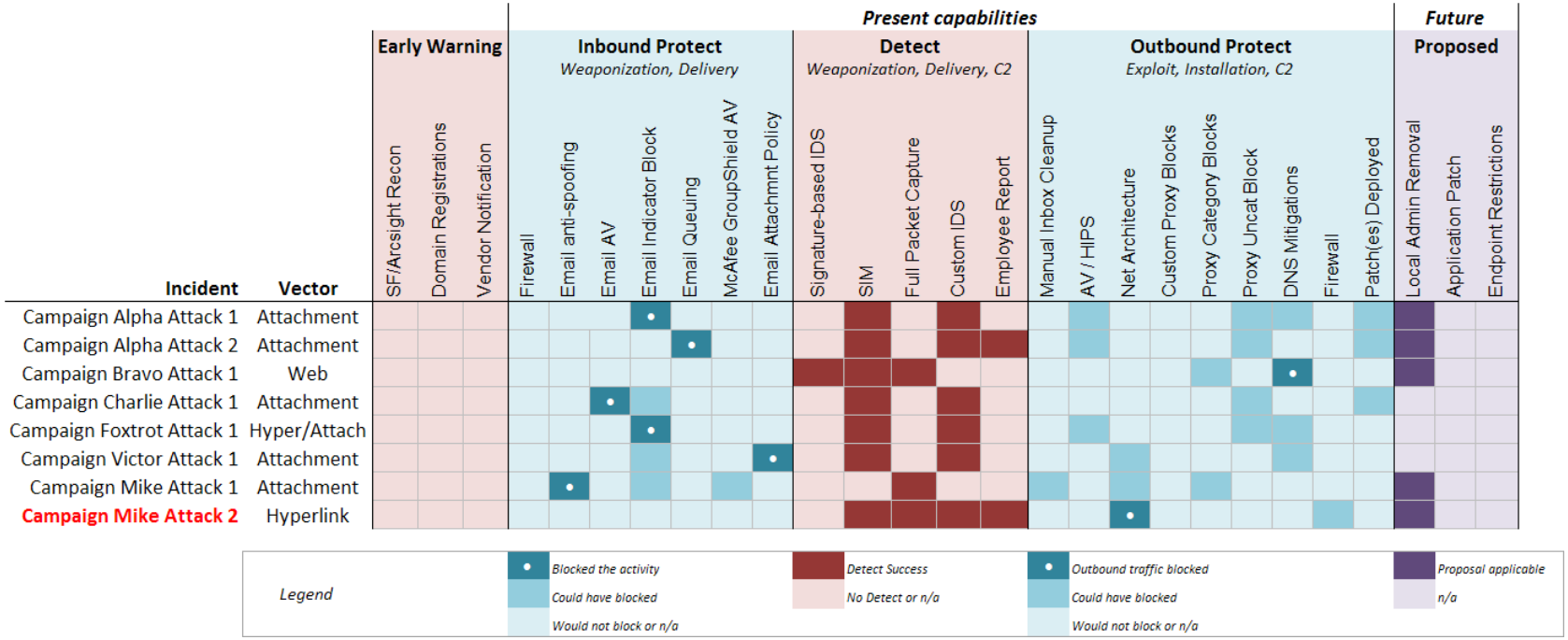
Defending against Nation States

- Motivation
  - IP theft
  - Disruption of critical activities
- Preferred Methods
  - Advanced Persistent Threats
  - Spear phishing of key employees
  - Custom malware
- Cant' do much about A_V
  - You are who you are
  - Useful to understand your targets
- Increase D_V
  - Introduce friction
  - "Keep the bear at bay"
- Increase R_V
  - Increase the chances of being caught
  - Establish relationship with

Defending against non-state actors

- Motivation
  - Increase cost of doing business
  - Cause embarrassment
- Preferred Methods
  - Heavy Social Engineering
  - Targeting online and Social Media presence
  - Botnet-based DDoS
- Be aware of business impact on A_V
  - Activities in social media
  - Make sure LoB is risk aware
- Increase D_V
  - Introduce friction e.g. DDoS protection, Social Media policies, awareness
  - “Keep the bear at bay”

The Sharp End: an illustration of defenses



Campaign Alpha Attack 1	Attachment	Email w/hostile attachment exhibiting known high-fidelity attributes
Campaign Alpha Attack 2	Attachment	Custom analysis reveals malicious content; email removed from queue before delivery
Campaign Bravo Attack 1	Web	New delivery vector, exploit for known backdoor. Mitigated due to leveraged intel on C2 infrastructure.
Campaign Charlie Attack 1	Attachment	COTS AV blocked delivery of actor bearing known-bad indicators.
Campaign Foxtrot Attack 1	Hyper/Attach	Email w/hostile hyperlink & attachment exhibiting known high-fidelity indicators.
Campaign Victor Attack 1	Attachment	Attempted delivery of malicious APT email not conforming to attachment whitelist policy.
Campaign Mike Attack 1	Attachment	Attempted spoof of target's boss by adversary mitigated by anti-spoofing mitigations at email gateway.
Campaign Mike Attack 2	Hyperlink	0day attachment delivered from another compromised subcontractor; compromised systems

Note / attribution:Similar content to this can be seen in Amin, Cloppert, Hutchins, Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Kill Chains, Proceedings of the 6th International Conference on Information Warfare, 2011

Organizations need

COMPREHENSIVE VISIBILITY

"Analyze everything that's happening in my infrastructure"

AGILE ANALYTICS

"Enable me to efficiently analyze and investigate potential threats"

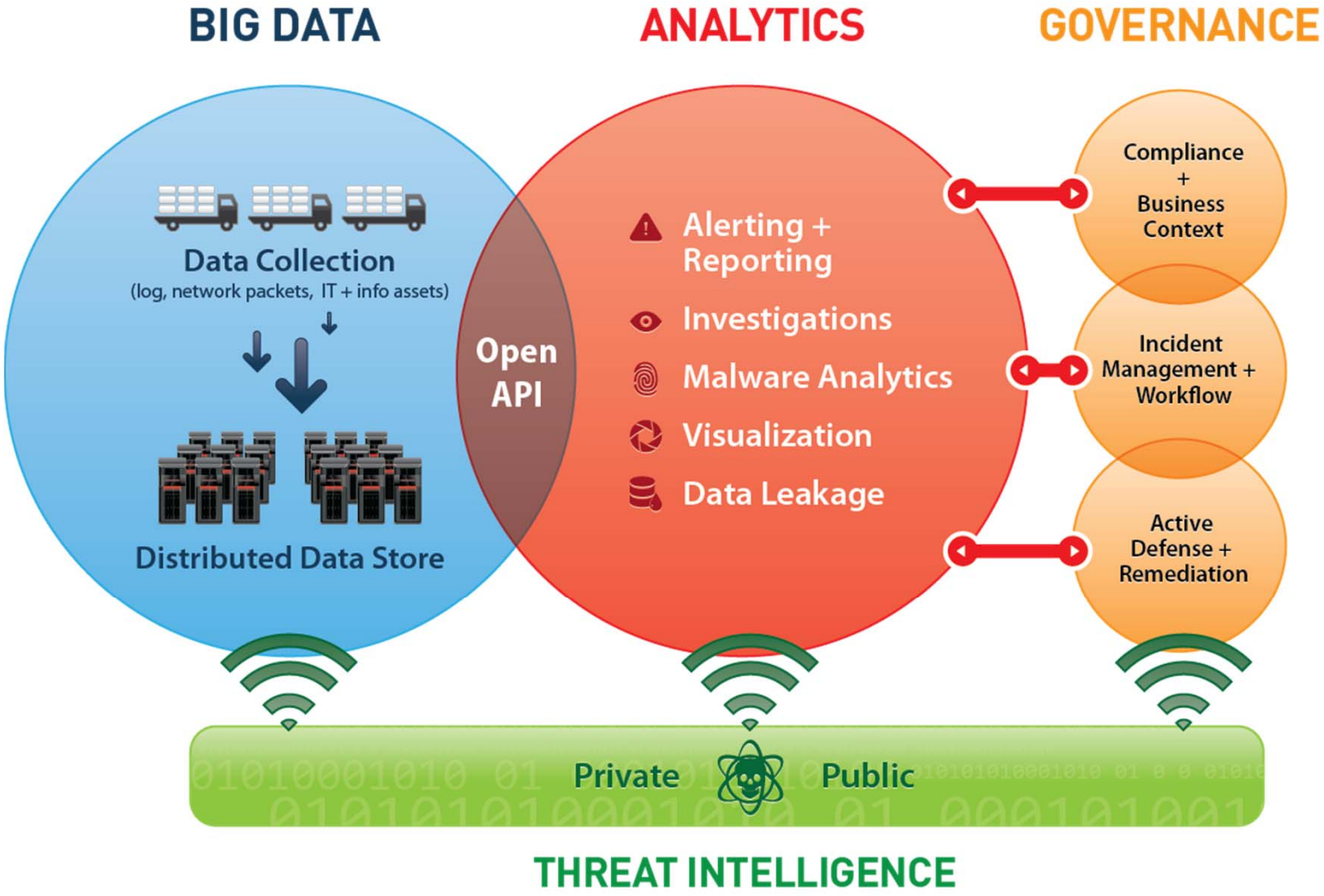
ACTIONABLE INTELLIGENCE

"Help me identify targets, threats & incidents"

OPTIMIZED INCIDENT MANAGEMENT

"Enable me to manage the incidents"

Defense Architecture



Forward-leaning Practices

- Intelligent tools and learning
- Education is key
- Think about security and vendor / service community for each of…
  - Device (new trust models needed)
  - Network
  - Data
  - Transactions
- Look to ecosystems for solutions
  - Products in combination
  - Talk to service providers: telcos, SaaS, etc.
- Information sharing is vital