The Need for Intelligent Network Security:

Adapting IPS for today’s Threats

James Tucker
Security Engineer
Sourcefire Nordics

A Bit of History

- It started with passive IDS.
  - Burglar alarm for the network
- Classic IDS Has some key weaknesses
  - Too Many Alerts
  - False Positives!
  - Alert only
  - Can Create More work than problems it solves.
    - Hard Sell to Upper Management

IDS Is Dead!

- Gartner Article in 2003
- Pointed out some symptoms
- Pushed companies and vendors toward IPS
- Did not address the underlying problems with IPS
- With out good “D” it is impossible to have good Prevention.

SOURCEfire

Odds are Against the Defenders!

- Global Economy for Cybercrime
  - ▸ 80 Billion USD
- Malware created daily
  - ▸ 20,000 units
- Average number of 0-Days
  - ▸ 1 per month
- Average number of threats
  - ▸ **300** per month
- New Types of Targeted attacks

It’s not just the bad guys making it hard

- Mobile data
- Consumerisation of business IT
  - ► http://www.schneier.com/, 7th September
- Cloud Services
- Technology Overload

Employees are trying to do their jobs,
Businesses are trying to do much more with far less

The ‘new’ threat of 2010

- Advanced Persistent Threat:
  - Advanced: One Off, 0-day and custom attacks
  - Persistent: Attackers are mission orientated and not opportunistic. Unlike typical hackers, they have specific, often political goals.
  - Threat: A person, not a auto-rooter bot/software.

- COLD. HARD. REALITY.

So what else has changed

- The attacker
  - APT
- The “victim”
  - They’ve been given the tools of their own destruction.
- The attack vectors
  - Not only direct network-based attacks
  - It’s in the content

Addressing Todays Problems

- Event Analysis
  - Takes Time and Skill

- Tuning
  - Takes Time and Skill

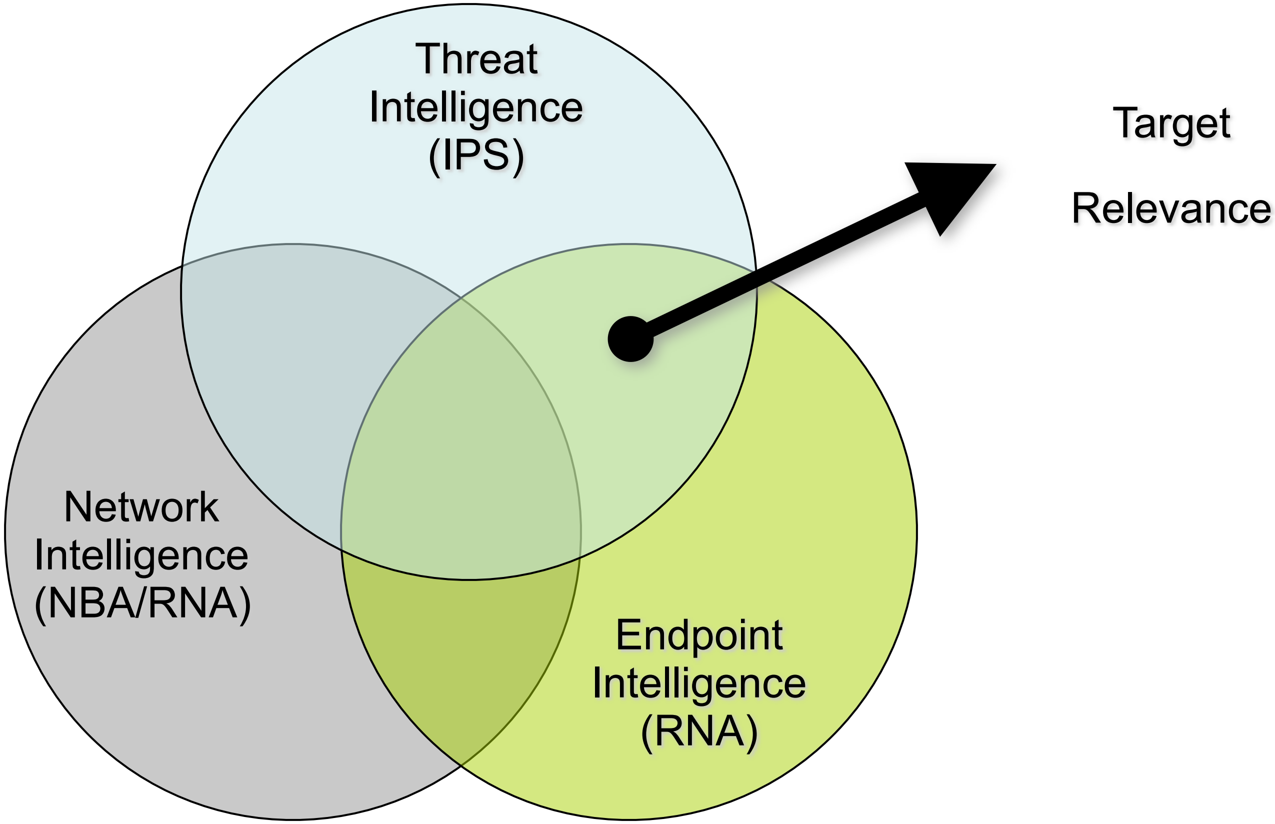
- The Right Strategy is based on *your* network.
  - It’s all about context

The Sourcefire Way

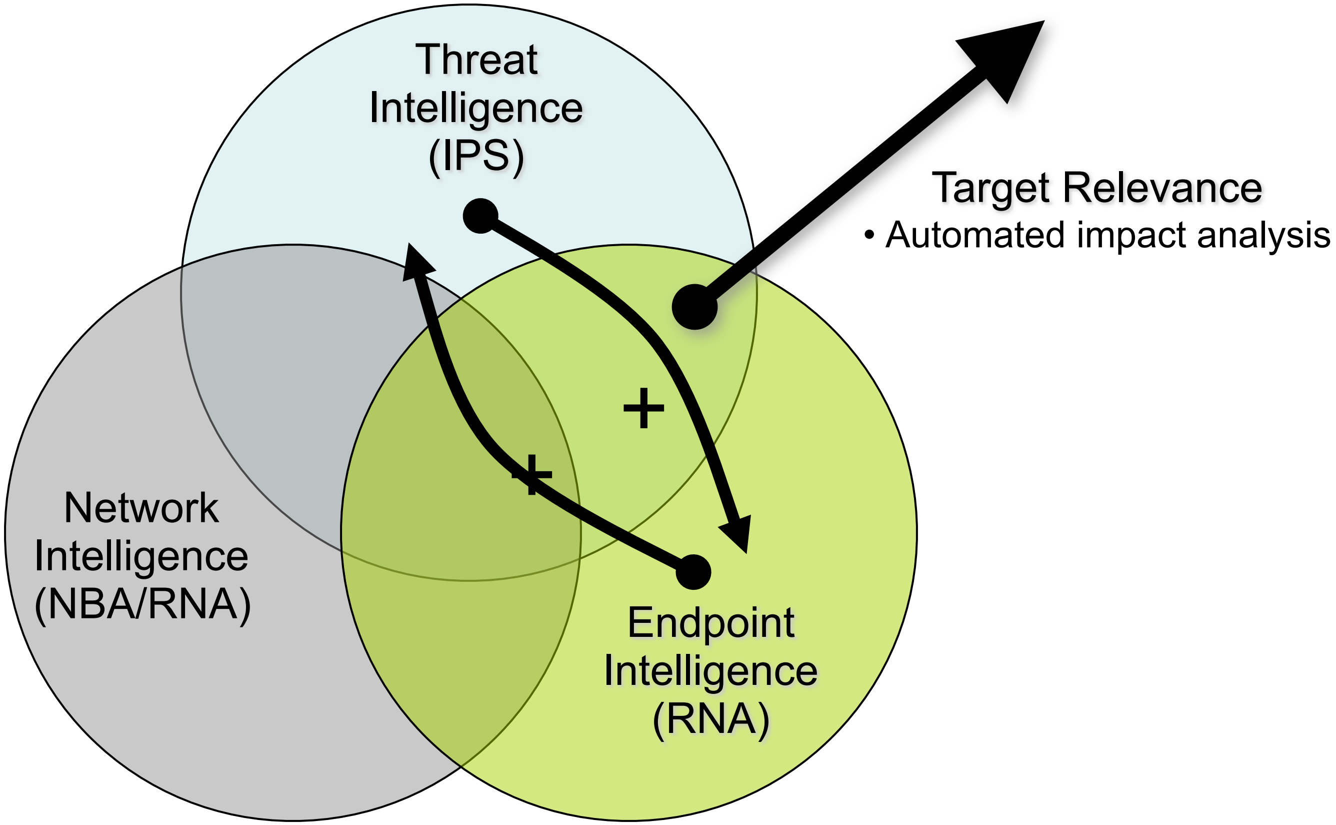
Sourcefire 3D Components

Component	Based on	Function
IPS	Snort	Intrusion detection and prevention
Real-time Network Awareness™	Passive network discovery	Network discovery, vulnerability mapping
Real-time User Awareness™	Wire-level UID capture and directory lookup	User name resolution to a security event
Sourcefire SSL Appliance™	Dedicated appliance	SSL inbound and outbound decryption for in-line and passive deployments
Defense Center™	Sourcefire analytical engine	Event correlation Compliance monitoring and enforcement.
Master Defense Center™	Defense Center	Correlate from multiple Defense Centers *(Only needed if your customer is LARGE)*

Event contextualization


Threat Intelligence (IPS)
Target
Relevance
Network Intelligence (NBA/RNA)
Endpoint Intelligence (RNA)

“Intelligence”



Threat Intelligence (IPS)

Network Intelligence (NBA/RNA)

Endpoint Intelligence (RNA)

+

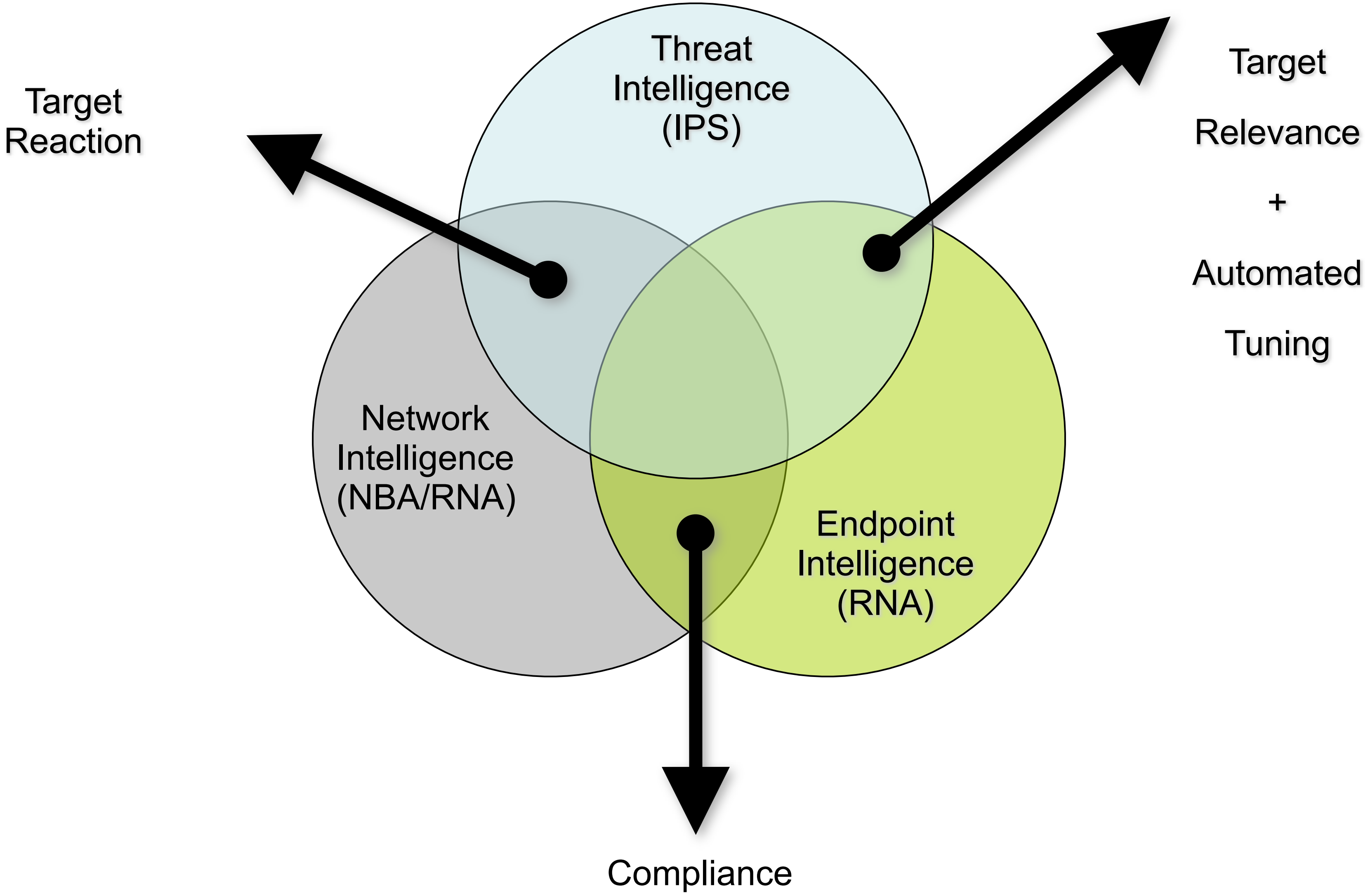
+

Target Relevance

- Automated impact analysis

Adaptive IPS (R3)

Putting it all together



Threat Intelligence (IPS)

Network Intelligence (NBA/RNA)

Endpoint Intelligence (RNA)

Target Reaction

Target

Relevance

+

Automated

Tuning

Compliance

Time is valuable

- Use context to
  - Automate event analysis
  - Automatically tune
  - Automatically defend
  - Eliminate false positives
  - Match policy with reality

- So what do we do with all this ‘extra’ time?
  - Flow Analysis
  - Business integration of Security Team

The Most Important Part

- The People in Your team
  - A tool is just a tool
  - Must *want* to protect the network
  - Balanced Business, Technical, and evil.

- The People You’re defending
  - Establish understanding
  - Avoiding the US VS THEM mentality.

Steps to Security.

- Step 1: IPS Must be part of a strategy
- Step 2: Find the right people
  - This is the most important success factor
- Step 3: Events must be analyzed
- Step 4: System must be tuned, regularly
  - You must know the network you are defending!

Then - See The Bigger Security Picture

- Flow analysis
  - The only way to detect many threats
    - Encrypted C&C networks
  - Misuse of resources
    - Bandwidth hogs
    - Data leakage
  - Find the root cause of the problem
  - Provides value to management

Business Integration

- Security needs to get out of the server room and into the meeting room.
  - Integrating security from the start of projects
  - Not be the guys who are tasked with “stopping packets”

- Assisting with Risk analysis
  - Key to a good security strategy.

Crystal ball gazing

- Automated IPS is a great tool.
- But It’s not everything
- What About
  - PDFs
  - Flash
  - ActiveX
  - A million unknown vectors?

- Near real time detection has to be next . . .

Tying it all together

- Use IPS when possible
- Automation will set you free
  - Automated rule tuning
  - Automated impact assessment
- Flow Data is the next logical frontier
- There are no “Magic Boxes” available
- Build a good team
- Near real time content inspection

Questions?

jtucker@sourcefire.com

http://www.sourcefire.com
http://vrt-sourcefire.blogspot.com/
http://labs.snort.org/razorback/