Making Intrusion Event Analysis easy

June 3rd, 2009

SOURCEfire

ENTERPRISE THREAT MANAGEMENT

Agenda

- Adaptive IPS Today
- Adaptive IPS with RNA
- Competitive Comparisons
- Adaptive IPS Benefits

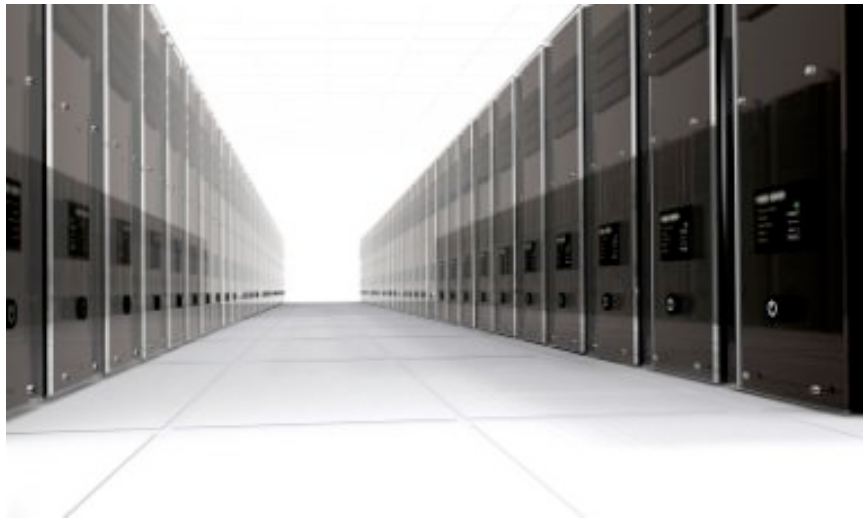
Adaptive IPS In-Depth

What is Adaptive IPS?

- Strategy for making the IPS:
  - Contextual
  - Self-tuning
  - Performance-efficient
  - More accurate and non-evadable
- Leverages network intelligence provided by RNA
- Benefits:
  - See only what's relevant
  - Handle more traffic faster
  - Put less effort into tuning
  - Avoid security evasions and detect traffic more accurately

Adaptive IPS Components

1. Impact Analysis
2. Automated IPS Tuning
3. Adaptive Traffic Profiles
4. Non-Standard Port Handling



SOURCEfire
Security for the real world.

1. Impact Analysis

- We know what this is! Impact Flags!

Impact Flag Rating	Target Network Monitored by RNA	Target Host Monitored by RNA	Exploit Matches Target OS and/or Service	Exploit Targets a Known Vulnerability
1	Yes	Yes	Yes	Yes
2	Yes	Yes	Yes	No
3	Yes	Yes	No	No
4	Yes	No	Unknown	Unknown
0	No	No	Unknown	Unknown

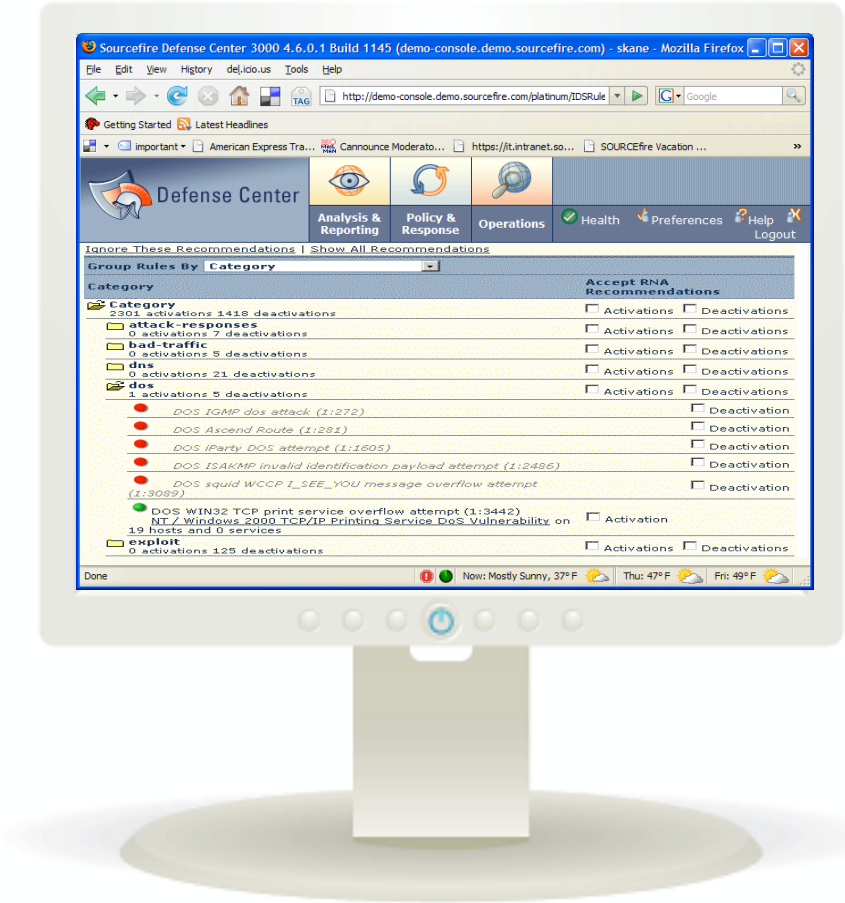
- Impact Flag 1 – Act immediately!
- Impact Flag 2 – Investigate
- Impact Flags 3, 4 & 0 – Good to know

2. Automated IPS Tuning

- We know this one, too!
- RNA Recommended Rules
  - RNA recommends Snort rules to enable based on the assets you're protecting
  - Maximizes network protection
  - Maximizes 3D Sensor resources

SOURCEfire
Security for the real world.

Let's See a Demo!



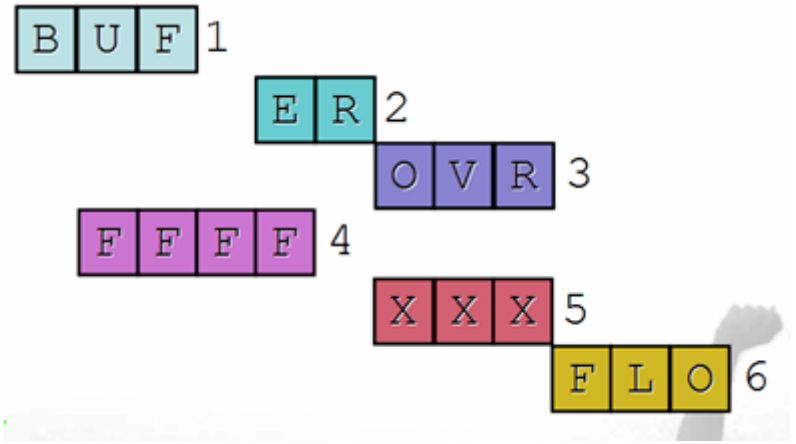
SOURCEfire
Security for the real world.

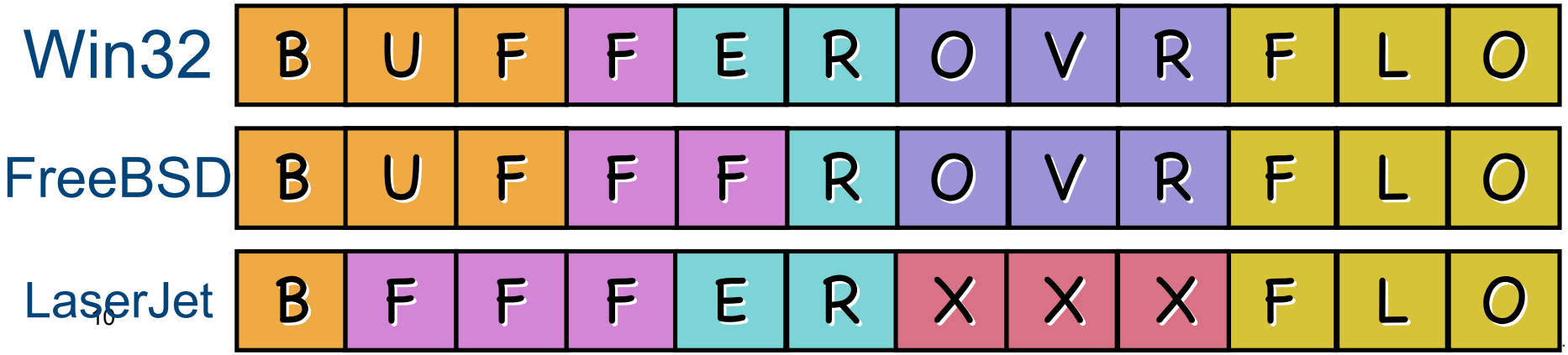
3. Adaptive Traffic Profiles

- Uses RNA network intelligence about the target host's operating system
- Models traffic the way that operating system would see it
- Other IPS products need to make assumptions about how to model traffic that are often wrong
- Avoids evasions

3. Adaptive Traffic Profiles, *cont.*

- Different operating systems sometimes “see” the same traffic differently
- If IPS and target see traffic differently, this can cause evasions
- Danger: IPS misses the attack but the target sees it





4. Non-Standard Port Handling

- IPS automatically applies appropriate rules to traffic on non-standard ports
- If HTTP is running on port 8080, RNA knows this. The Defense Center will instruct the IPS to apply HTTP rules to port 8080.
- Benefits:
  - Reduced manual administrator tuning
  - Maximized network protection

Adaptive IPS – Industry Comparison

Capability	SOURCEfire®	TippingPoint	Internet Security Systems	McAfee	Cisco	Juniper® Networks
Impact Analysis	✓		Limited	Limited		
Automated IPS Tuning	✓					
Adaptive Traffic Profiles	✓					
Non-Standard Port Handling	✓		✓	Limited		

Summary of Benefits

- Maximizes network protection
- Maximizes IPS performance
- Minimizes the quantity of actionable events
- Minimizes the need for manual IPS tuning
- Minimizes false positives
- Minimizes network security risks

SOURCEfire
Security for the real world.

Adaptive IPS Technology Brief

- Available now!

  http://www.sourcefire.com/resources/downloads/public/techbrief/SF_TB_AdaptiveIPS.pdf

SOURCEfire
Security for the real world.

Questions?