Know More With Sourcefire Intelligence

Defending Networks Without Borders

James Tucker
Security Engineer Nordics/Baltics

SOURCEfire

ENTERPRISE THREAT MANAGEMENT

Knowing Is Good

SOURCEfire
Security for the real world.

Not Knowing Can Make Headlines

Davidson Reports Data Breach Affecting 228,000 Clients

Lawsuit Filed Over **CardSystems** Data Breach

Hannaford Breach May Have Exposed Millions to Fraud

LexisNexis Warns 300,000 of Data Theft

WellCare Flubs Data Privacy for 10,000 Georgians

Commerce Bank Database Hacked

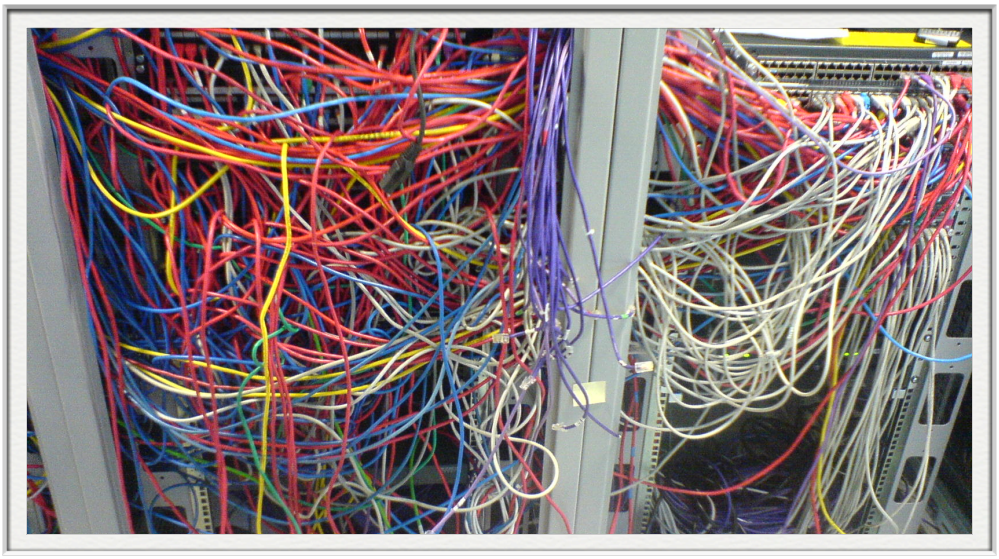
Advance Auto Data on 56,000 Customers Exposed

WellPoint Data Breach Affects 128,000 Clients

Hackers Tap **Western Union**; 20,000 Affected

Hacker Infiltrates **UCLA**, Data on 800,000 Stolen

Classic Network Security



- Flawed assumptions
- Narrow Solutions

Static Defenses Work

- The network is understood
- Threats are known or knowable

SOURCEfire
Security for the real world.

People Are Well Trained

- They are vigilant
- They are responsive
- They have the proper Time, Tools, and Training.

SOURCEfire
Security for the real world.

One Problem = one solution

- Stove-piped products
- Knowledge sharing an afterthought

SOURCEfire
Security for the real world.

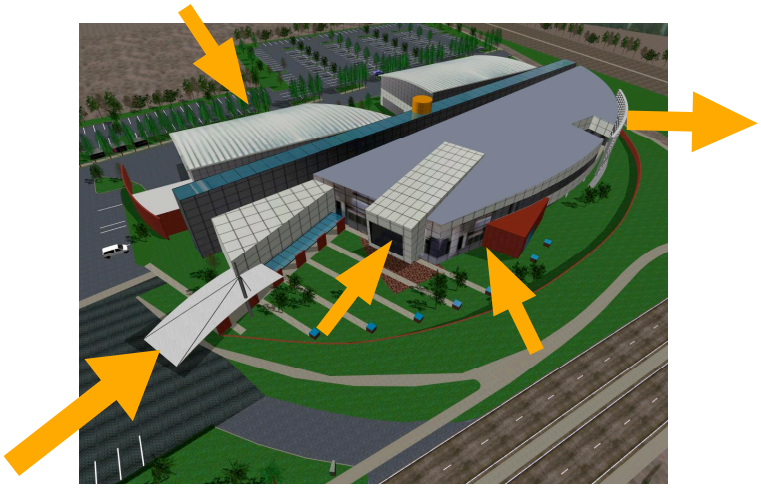
Security Events Must Have Context

-20°C, Tallinn

+20°C, London

SOURCEfire
Security for the real world.

Today's Threat Landscape



SOURCEfire
Security for the real world.

Sourcefire Intelligence Drives…

- Network Discovery
- Impact Assessment
- Automated IPS Tuning
- IT Policy Compliance
- Network Behavior Analysis
- User Identity Tracking

SOURCEfire
Security for the real world.

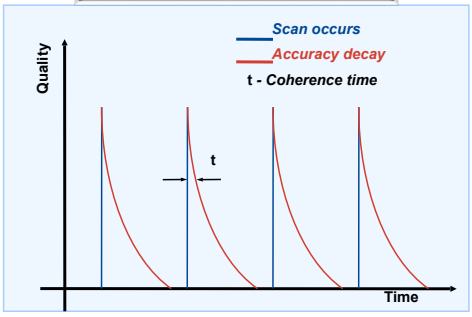
Key Sources of Sourcefire Network & User Intelligence

- Sourcefire RNA™
- Sourcefire RUA™
- Sourcefire NetFlow Analysis

SOURCEfire
Security for the real world.

Network Discovery - RNA

- Sourcefire RNA is Listening “all the time, in real time”
- You Know…
  - When a new host appears, whether physical or virtual
  - What OS and services it’s running (e.g., BitTorrent)
  - What ports are open
  - What protocols it’s using
  - What its potential vulnerabilities are



Impact Assessment

- Drastically reduce the number of “actionable” events through Impact Flag ratings

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 Later
- Impact Flags 3, 4 & 0 – Good to know

Network Behavior Analysis (NBA)

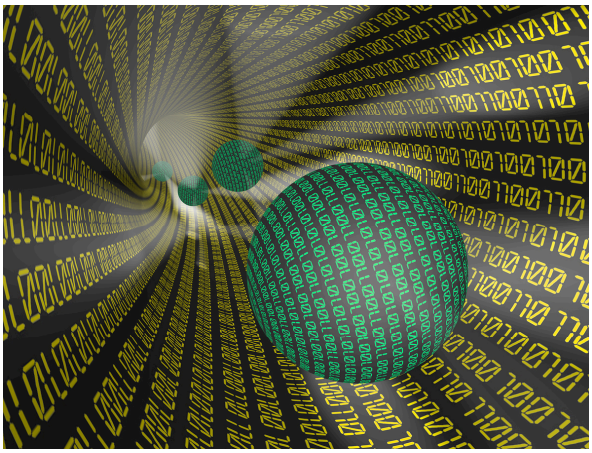
- The best network security strategy is one with layered defenses
  - Deterministic – IPS, Firewall, Ant-Virus, Anti-Spam
  - Non-Deterministic – NBA

“A $100,000 IPS can easily be defeated with a laptop and a good pair of sneakers.”

Martin Roesch
Sourcefire Founder & CTO

Network Behavioral Analysis

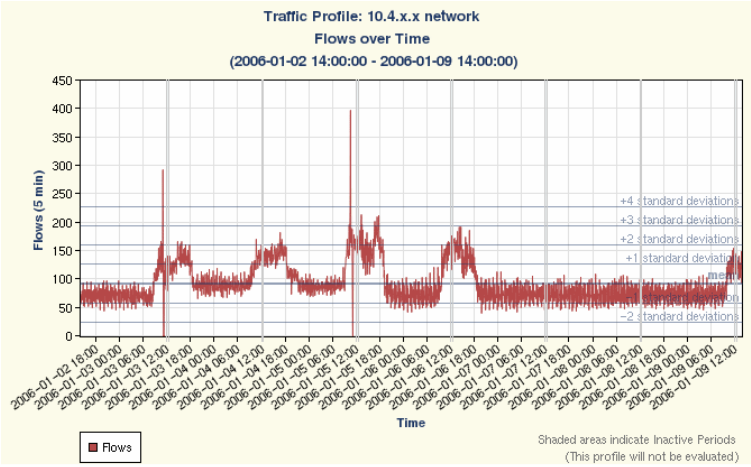
- Real-time monitoring of network behavior
- Statistical signal processing finds data in the noise.
- Monitors effect, not cause
- Sensitive to zero-day attacks



SOURCEfire
Security for the real world.

Key NBA Benefits

- Detect Internal Malware Before it Spreads
- Evaluate Bandwidth Provisioning
- Troubleshoot Network Outages & Degradations



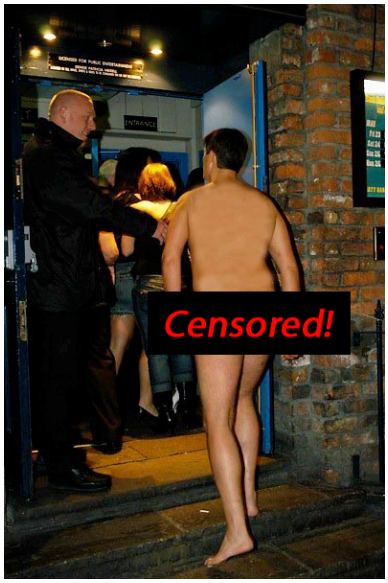
Real-time Network Access Control

- Actionable event triggers programmed response, e.g.
  - Limit offender's access to network
  - Update misconfigured or obsolete software
- Not just at time of entry to network

SOURCEfire
Security for the real world.

Access Control Explained

- How Typical NAC solutions Work:



SOURCEfire
Security for the real world.

Automated IPS Tuning

- How often does your network change?
- How often do you tune your IPS?
- Key “Adaptive IPS” capabilities include:
  - RNA Recommended Rules
  - Adaptive Traffic Profiles
  - Non-Standard Port Handling

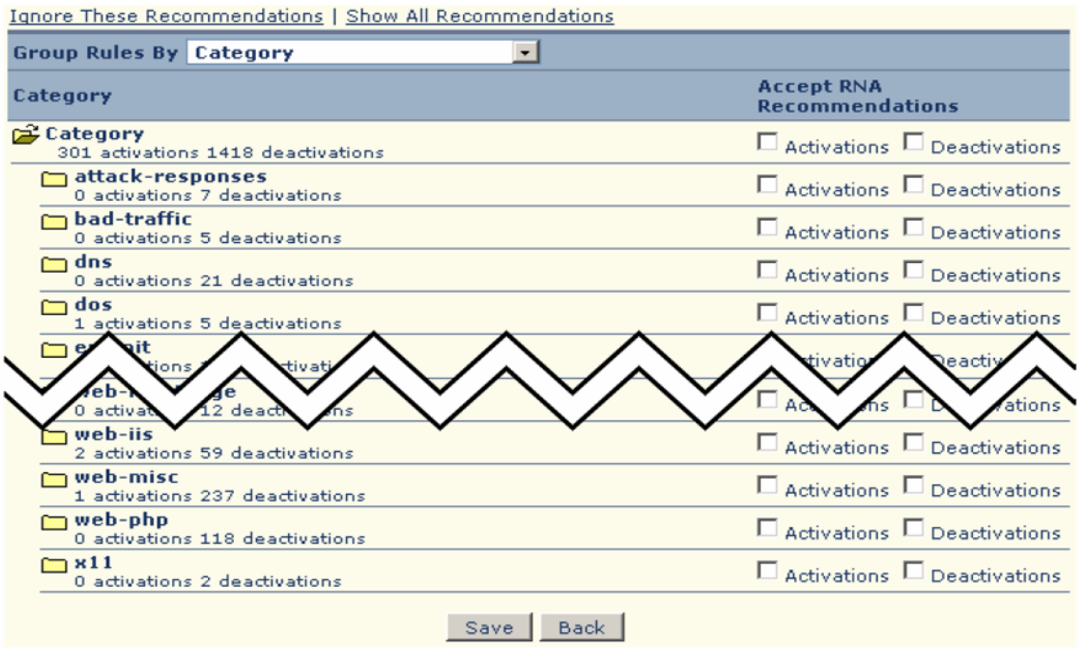
RNA-Recommended Rules

- **Benefits of RNA-Recommended Rules:**
  - ***Avoid missed attacks*** by recommending rules to turn on based on network services or assets in use
  - ***Increase performance and reduce false positives*** by recommending irrelevant rules to turn off
  - Ensure your IPS policy matches the network it’s deployed on
  - Periodically alert administrators to policy changes they need to consider

RNA-Recommended Rules

- Start with a default or existing rule configuration
  - Set of rules that are currently turned on
  - Sourcefire allows you to start with several default policies
    - Multiple default IPS policies
    - A single default IDS policy
- Give DC a network to “survey”
  - Assign it a network or detection engine to profile
  - Defense Center collects the network map/host profile information it has for that network
  - Notes which services and operating systems are being used on that network

RNA-Recommended Rules

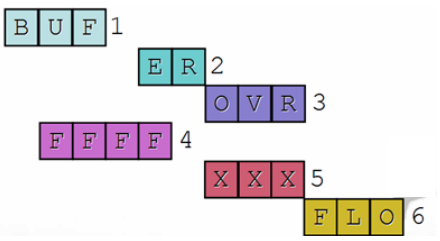


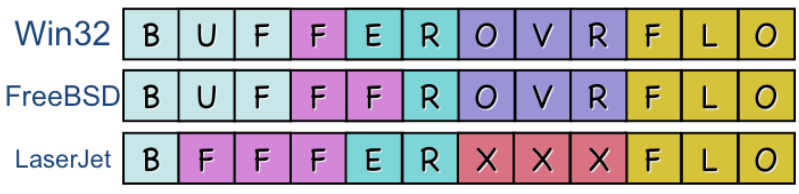
RNA-Recommended Rules

- Given this, the Defense Center recommends that you turn on or turn off a given set of rules
  - Turn on the rules that correspond to services and operating systems that are in my network (rules that are currently off)
  - Turn off the currently enabled rules that correspond to services and operating systems I don't have in my network
- Users are able to accept or reject the recommendations
- Can be configured to accept recommendations on a scheduled basis
- Periodically email the administrator a report of all the recommendations without accepting any recommendations

Adaptive Traffic Profiles

- Benefit of Adaptive Traffic Profiles:
  - Don't miss hacker attacks – Avoid a class of soon-to-be-common evasions – unlike any other IPS
  - Ensure the IPS sees traffic the same way the target machine of an attack would
- Different operating systems sometimes "see" the same traffic differently





Non-Standard Port Handling

- With 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.
- Net: administrator tuning effort reduced
- Support for this functionality is in 4.8

User Identity Tracking - RUA

- People Are the Perpetrators of Computer Crime
- Pairs an Active Directory or LDAP username with a host IP address
- Correlates usernames with security events so incidents can be resolved more quickly
- Click on username to reveal full name, telephone, email, and department
- Integrated into all Sourcefire 3D Sensors

Identify the "who" behind the "what" to resolve incidents quickly

The Compliance Challenge

An alphabet soup of regulation dealing with security, privacy, fraud and abuse concerns

- HIPAA – protection of patient information
- GLBA – protection of customer information
- SOX – accuracy and integrity of financial data
- PCI – protection of card holder account data
- FISMA – security of government information & systems
- BASEL II – capital, operational, & market risk

Impose implicit and explicit security requirements on organizations

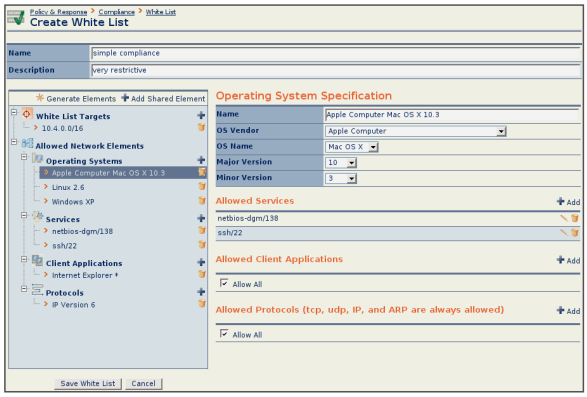
Compliance Made Easy

- How Does The 3d System address typical compliance controls?

Common Regulatory Requirements	Sourcefire Capability
Risk Assessment & Response	RNA Discovery and Defense Center Vulnerability Management
Identification of Security Threats and Incidents, including attack, malicious software, others	Intrusion Sensor, RNA Change Detection - new services, flows, etc.
Established procedures for responding to threats, intrusions	Defense Center Policy & Response 1-Click Compliance
Mitigate potential for damage, correct out-of-policy situations, notification to staff of incidents and/or actions taken	Defense Center - Alert, Block, Correct
Compliance reporting, forensic analysis, security policy improvements	Defense Center Database

One Click Compliance

- Users may set and enforce policies for endpoints, subnets, or networks with the Policy & Response engine
- Policy enforcement becomes highly automated and easy to maintain - compliance becomes real time
- Once defined, any change outside of policy would result in an array of possible corrective actions including:
  - Sending of an alert
  - Redirection of the asset into a “sandbox” or quarantined network
  - Blocking some or all traffic to or from the asset
  - Using patch management.



SOURCEfire
Security for the real world.

Benefits of Sourcefire Intelligence

Increases Security

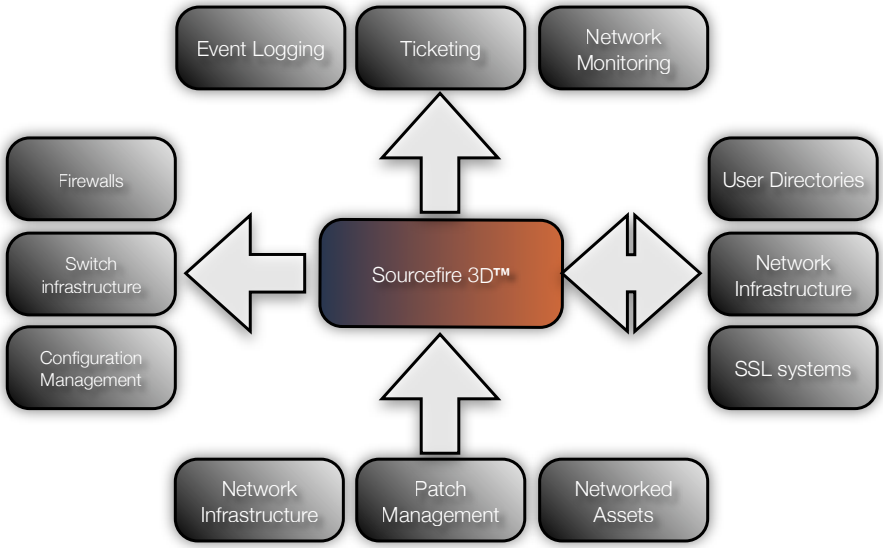
- You know what you’re protecting
- You know when your network changes
- You can detect exploits originating from inside and outside your network
- Your network is a safer place by monitoring and enforcing IT compliance policies

Saves Time & Money

- Your IPS is always “tuned”—even when your network changes
- You no longer have to sift through thousands of events to uncover what really matters
- You know who to call when a host is compromised

SOURCEfire
Security for the real world.

Unparalleled Integration with your infrastructure



SOURCEfire
Security for the real world.

Use Case I: MSSP

- Sourcefire IPS and RNA provide event reduction of 99:1
- MSP has visibility of customer assets
- Priority calls to customer unlikely to be false alarms

SOURCEfire
Security for the real world.

Use Case II: Large Bank

- Sourcefire IPS, RNA, RUA
- NBA to monitor for long-lived SSL sessions by traders
- Trader's 'hop' across machines - RUA identifies the event to the user

SOURCEfire
Security for the real world.

Use Case III: Hospital

- Sourcefire IPS and RNA
- Monitoring and drug delivery systems networked
- Scanning - 'a matter of life and death'
- Passive RNA gathers assets without risk to equipment

SOURCEfire
Security for the real world.

And Best Of All,
It Keeps You Out of the Headlines!

Questions?

SOURCEfire
Security for the real world.