

What's Next for Intrusion Detection and Prevention??

Marcus J. Ranum

CSO, Tenable Network Security, Inc.

<mjr@tenablesecurity.com>

Who?

- I am:
 - An early innovator in the firewall market
 - Former founder and CEO of Network Flight Recorder, Inc. - an early IDS start-up
 - Industry analyst
 - Consultant
 - CSO of Tenable (Vulnerability Management)

What?

- What to talk about:
 - The Past
 - The Present
 - The Future
 - How to get there

A Word About History

- When I say *X* is “first generation” I am speaking as a historian not a marketing person
 - In history “first generation” came before “second”
 - In marketing “first generation” is the obsolete stuff that the competition sells

1st Gen IDS

- Use system logs as data source
- Look for unusual behaviors and static patterns
 - I.e.: signatures and statistics

2nd Gen IDS

- Use packet data to generate virtual application streams
- Look for unusual behaviors and static patterns
 - I.e.: signatures and statistics

3rd Gen IDS

- Oops
 - There was none!
- Improvements in algorithms and signatures
 - Scoring-based anomaly detection systems (AKA: NBAD)

The Death of IDS

- Gartner “IDS is Dead”
 - Shotgun wedding between firewalls and IDS
 - ...and the bastard child “Intrusion Prevention” was born 6 months later!

What Happened?

- After “the death of IDS” IDS became a ***data source*** for other engines
 - IDS data used to control a firewall (I.e.: IPS)
 - IDS data used as input to SIM/SEM
 - IDS data modulated by inputs from vulnerability assessment tools

Where Are We Now?

- The *reasons* behind Gartner's "IDS is dead" quip were:
 - Too much data
 - Too many "false positives"
- Never mind the fact that, technically, they were *wrong*, customers shared that perception

First Response

- IDS data modulated by vulnerability assessment tools
 - Rewrite based on knowing if the target was vulnerable or not
- IDS data modulated by post-processing
 - Compact 1000 “CodeRed” alerts into 1 alert reading “1000 CodeRed attacks”

The Deeper Problems

- Signatures remain a reactive technique (network antivirus)
- Prevention only can be enabled on things you are *sure* are bad
 - Customers tend to only turn on signatures that clearly and 100% reliably match well-known attacks

Missing Data Sources

- IDS/IPS and firewalls interfere with the data flows
 - If the firewall blocks it according to policy then it never happens at all - ***and we can't find out if it would have been an attack or not***
 - This applies whether the IDS/IPS is inside or outside the firewall

Missing Data Sources

- One possible future option: instead of destroying connection complete it to a virtual target (I.e.: a honeypot)
- Merging honeypot data into IDS sensor data offers a greatly enhanced ability to identify scans and sweeps
 - But there's a “gotcha”

The “Gotcha”

- Nobody wants to care about attacks that didn't happen
 - (though we will find out later that they *should*)
- The new *next* focus of IDS/IPS is going to be insider threat/data leakage detection

The “Gotcha” - part 2

- Current IDS algorithms (signatures and data trend analysis) suck at detecting leakage; they are good for finding CodeRed but pattern-matches get too open when you’re looking for a SSN#
 - False positives will climb unbearably

Look for Shift to Positive Action

- NBAD is most likely to be the jumping off point for this
- Instead of identifying what SQL traffic that contains Slammer looks like, identify SQL traffic that looks like all the other SQL traffic that the site has already seen and handled

Technical Approaches

- Structural analysis - Learn the “shape” of data and look for new shapes
- NBS - Never Before Seen anomalies
- Behavior Failure Analysis - burglar alarms to detect 2nd order effects of attacks

Structural Analysis

- This is the NBAD approach applied to layer 7
- Example: look at SQL streams and “learn” the kinds of queries that normally happen against the database
 - Build a set of templates (anti-signatures, whitelists)
 - Match subsequent traffic against the whitelist

Structural Analysis

- Imagine a traffic structural analysis “Wizard”
 - It interacts with the network admin to build chains of virtual events into event clusters
 - It asks the admin “does this look normal?”
 - As answers come back it raises and lowers the normalness of various clusters
 - Add IDS input of detected known-bad events to pull down normalness of clusters

NBS

- For *any* type of data that does not fluctuate across a wide scope
 - Track instances
 - When an old instance is seen maybe keep a statistic
 - When a new instance is seen alert on it then update the “seen” database

Behavior Failure Analysis

- If something tries to connect to a system that does not exist
 - Let it connect to something (let's say a Windows box designated as a sacrifice)
 - Let it interact with that something
 - Fire alerts if the sacrifice system exhibits NBS behaviors (e.g: a new process starts that has never been started before, or a new file is accessed, or written, etc)

Crucial: Smart Interfaces

- Smart Interfaces ask a question and remember your answer:
 - 1st time: “do you want me to disable this yes/no?”
 - 2nd time: “do you want me to disable this yes/no? (default is what was picked last time)”
 - 3rd time: “do you *always* want me to disable this? yes/no/always ask”

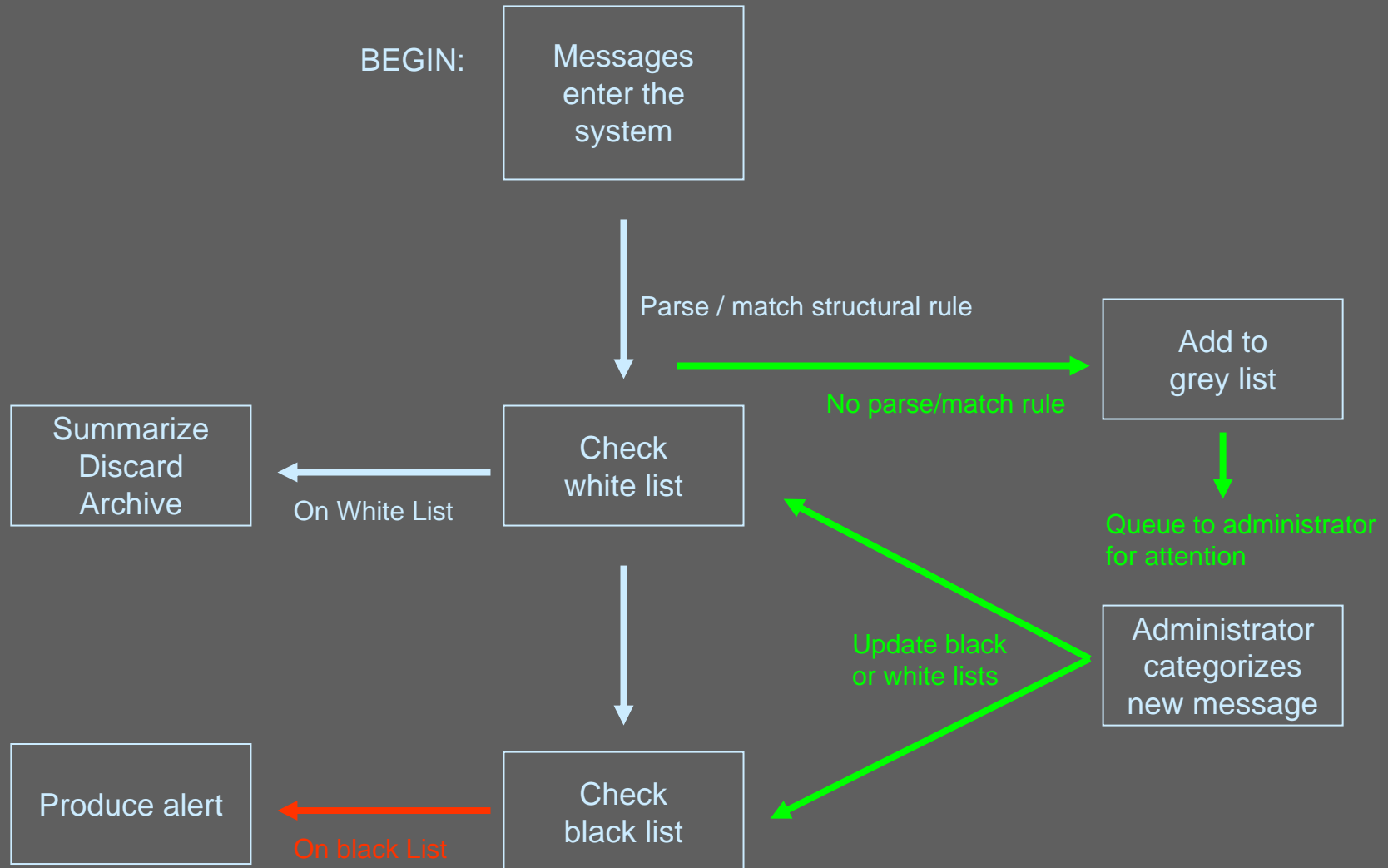
Crucial: Smart Interfaces

- Smart Interfaces extrapolate common groups of answers:
 - “I have noticed that every time I am 100% sure that traffic is an attack, you ask me to block it. Shall I always block *all* traffic that I am 100% sure is an attack?”
- This is *not* an AI problem, it’s a procedural process built by grouping rules and dependencies

Crucial: Smart Work-Flows

- Work-flows are how to build knowledge-bases automatically without AI
 - If you see something you've never seen before, ask someone what to do (obvious extension of a smart interface)
 - Incorporate management knowledge into the smart interface
 - “I've noticed that Ron cares about problems involving this machine and Marcus doesn't”

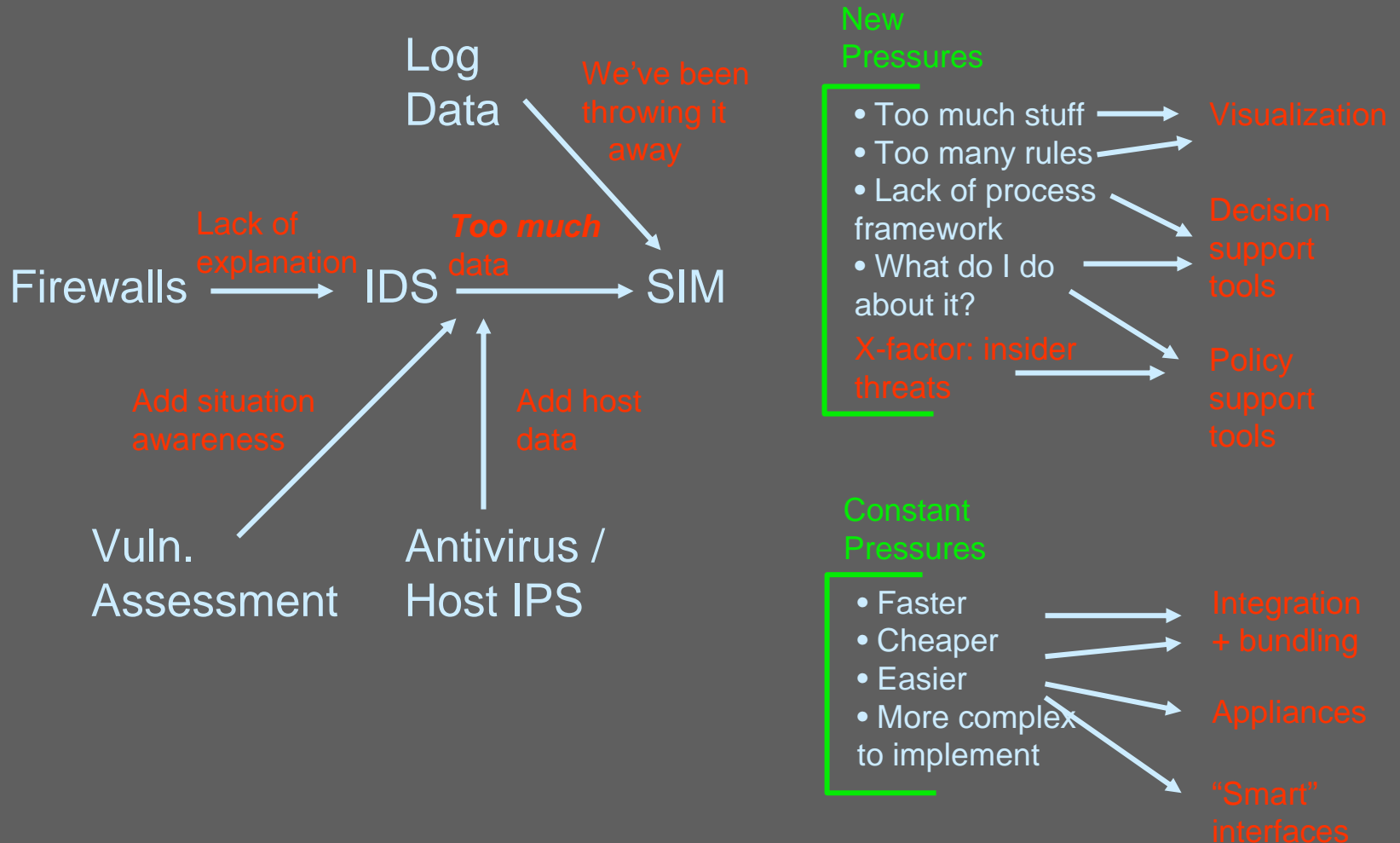
A Smart Work-Flow



A Smart Work-Flow V2.0

- Corporal: “Private - if you see an event that’s on the ‘escalate list’ - escalate it”
- Private: “OK”
- Corporal: “And if you see an even that’s on the ‘ignore list’ ignore it.”
- Private: “OK”
- Corporal: “If something comes in that’s not on either list, ask Sarge what list to add it to!”

Short/Near-term Roadmap



Evolution:

Input:

```
if(session is already established) {
    do intrusion detection on traffic
    if(intrusion detection finds something) {
        kill rest of session based on policy
        log alert
        log event
    }
    log event
    GOTO input;
}
if(session is not already established) {
    check firewall policy
    if(session not permitted) {
        if(honeypot intelligence desired) {
            while( session) {
                send traffic to honeypot
                collect attack information
                log event
                log alert
            }
        }
        kill rest of session based on policy
        log alert
        log event
    }
}
```

Summary:

- IDS/IPS is not dead; there is huge room for innovation remaining
- IDS is going to become an embedded producer/consumer of data
 - Everything should be thought of as part of a pipeline in which you do **not** own both ends
 - Winning technologies will be those that produce the best or consume the best