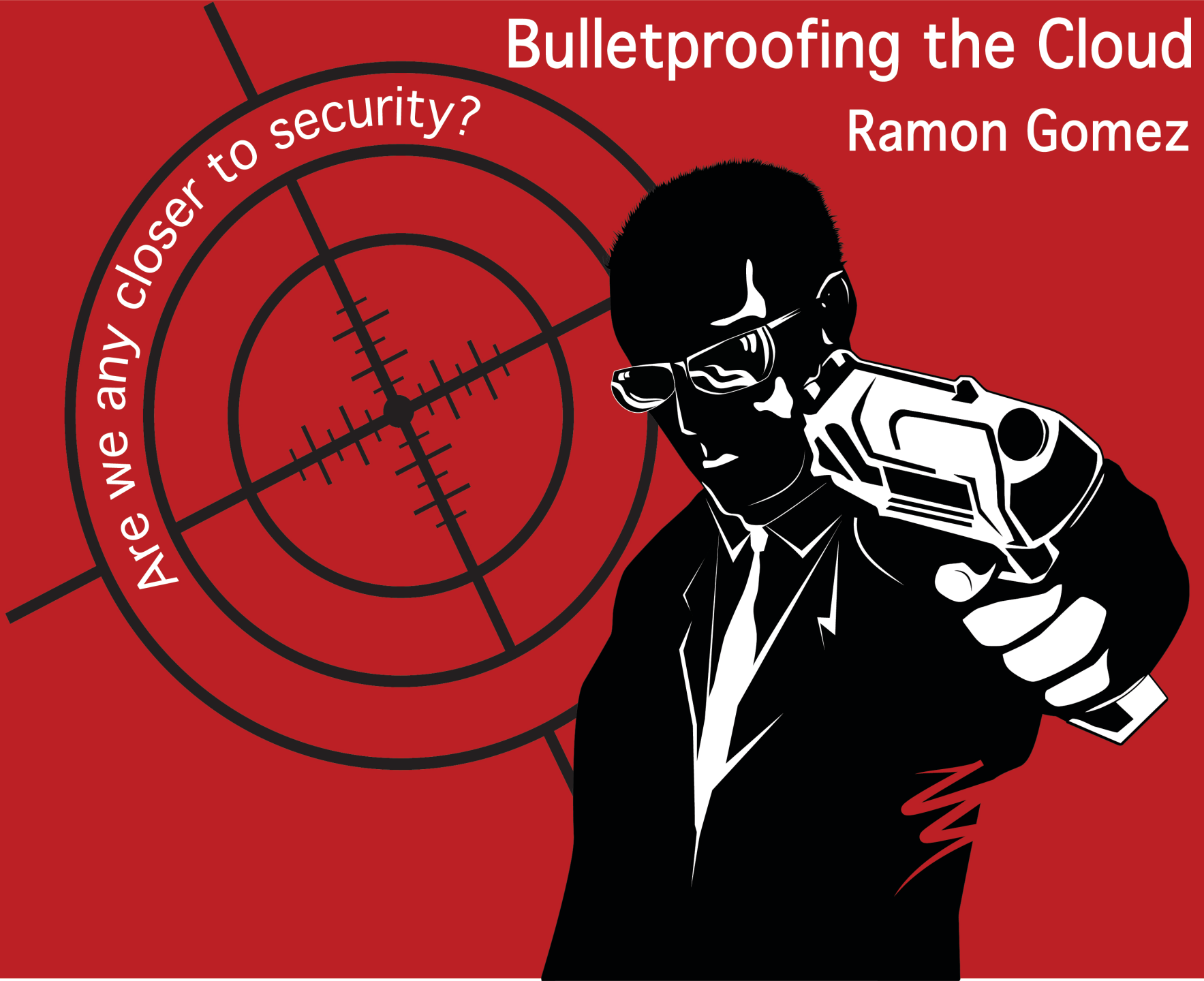
Bulletproofing the Cloud

Ramon Gomez



Who am I?

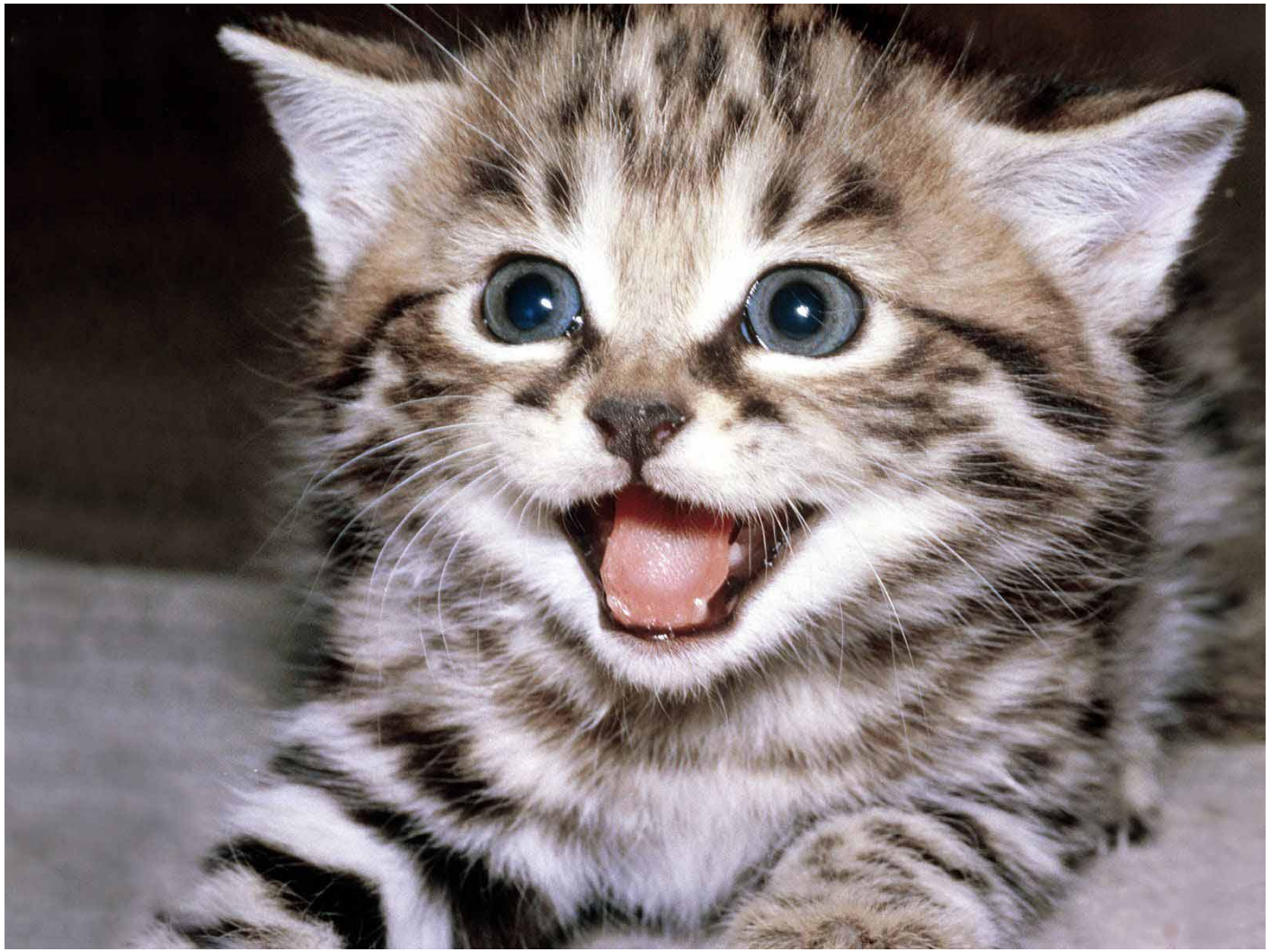
- 11 years in InfoSec with 5 years of hobby work prior to that
- Primary interests: penetration testing, intrusion detection, and log correlation
- Currently employed as an InfoSec generalist at a cloud provider
- Previously worked at several Fortune 100 companies
- blindedscience@gmail.com

What is this

What is the “Cloud?”

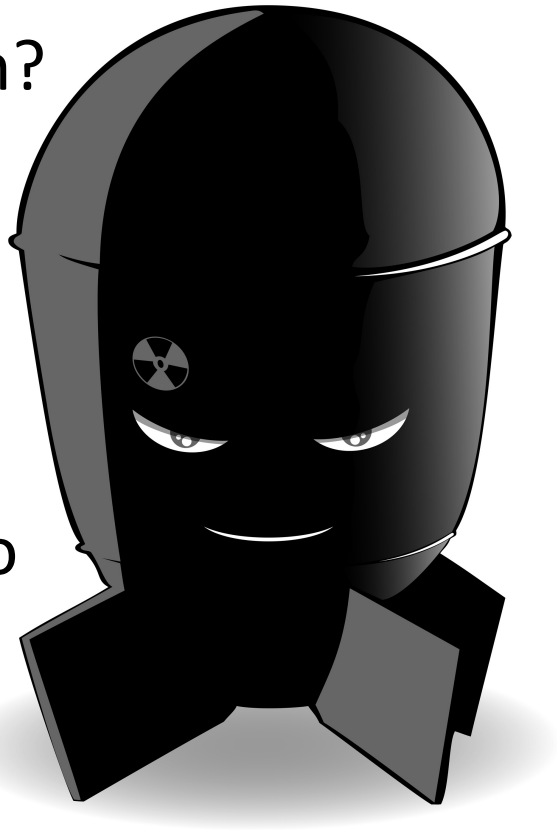
- Harnesses the massively scalable Internet infrastructure to provide multiple users with on-demand access to data, applications, and services
- Use of shared or virtualized resources to lower costs, reduce complexity, and increase flexibility
- For the purpose of this talk, we’re talking about IaaS or SaaS

This is a picture of a kitten



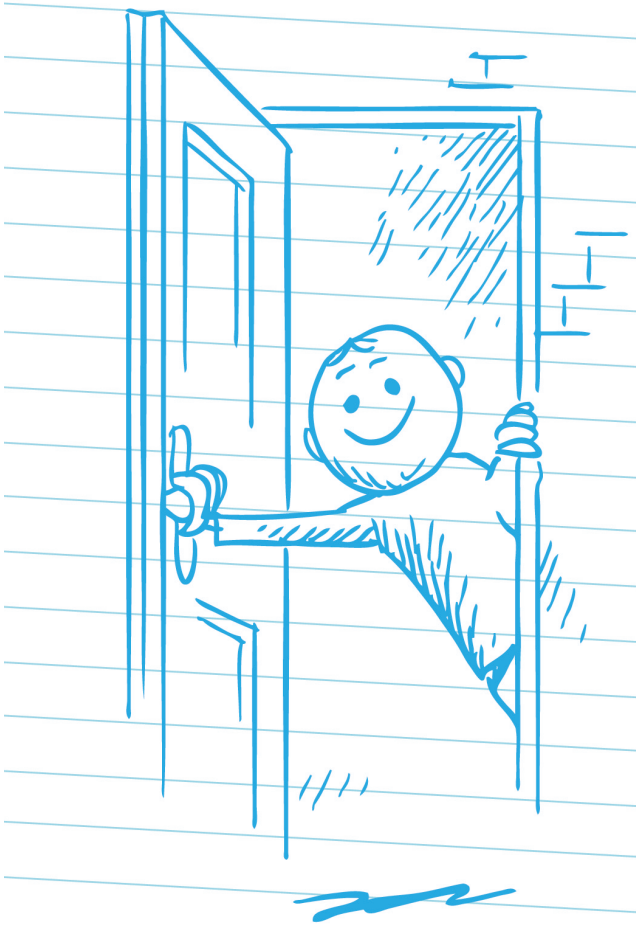
A Weapon of Mass Destruction?

- DefCon 17 – Clobbering the Cloud (SensePost)
- DefCon 18 – Cloud Computing: A Weapon of Mass Destruction? (Bryan/Anderson)
- Cloud providers essentially aren't doing much internal policing of their clients
- Unofficial policy: "As long as no complaints are received, nothing will be done"



Vulnerabilities of the Cloud

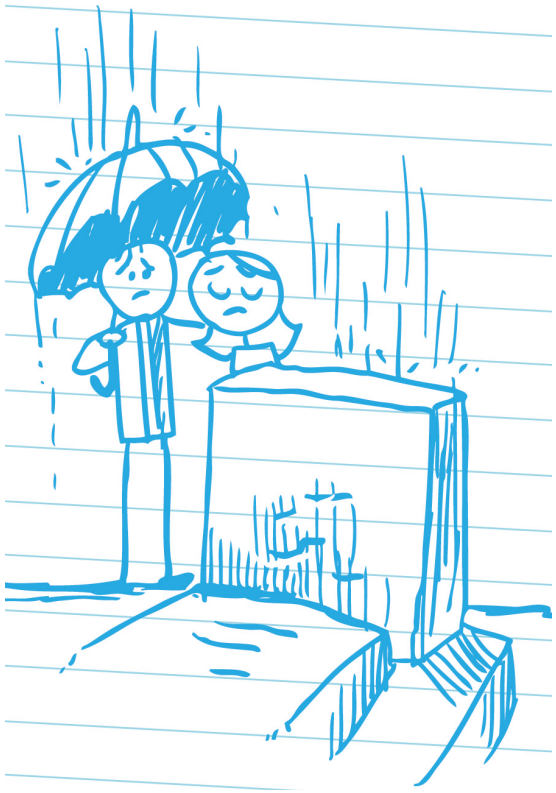
Easy Access



Anonymity/Fraud

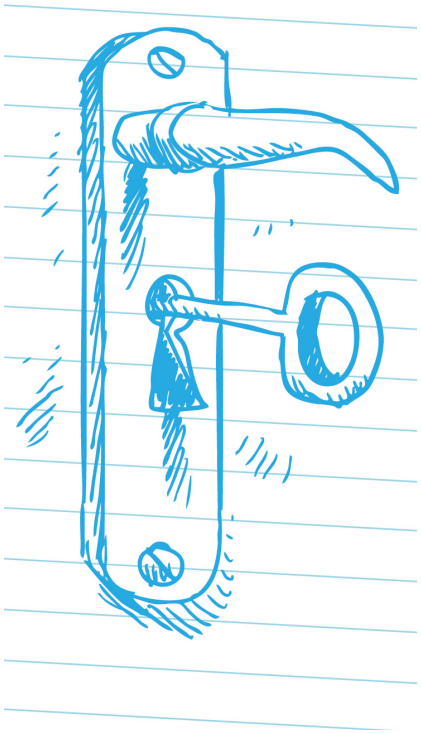
Contention for resources

Threats to the Cloud Provider



Infrastructure Damage

Fraudulent/
Nonpaying Clients



Proven inability
to address
security

Threats to the Client

One compromised client of a multi-tenant environment can affect others

Users can be unaware that their data is compromised

What are most cloud providers currently doing?

- Providers are treating cloud security as a traditional hosting environment
- Clients are given a virtual firewall with in-line IPS services
- Providers frequently offer Vulnerability Assessment for free
- Each client's virtual instance is independent
- Clients are "fending for themselves" with no coordinated enterprise security

Conventional Solution: IPS

- Very difficult for providers to offer prepackaged IPS that works for all clients and won't block legitimate traffic
- Information coming from an IPS is frequently incomplete (encryption, lack of end-point awareness)
- In-line IPS has to work at line speeds, so very complex correlations aren't possible

Conventional Solution: Traditional Design

- Focus on external threats
- Assume internal hosts are trusted
- Clients can't benefit from security data being generated by other clients

By the way, how's that working?

- I can't say for certain what the security posture is inside a company
- I can guess the nature of the security posture based on behaviors of their network and personnel
- Guesses are based on how frequently a particular host contacted my network, and how long it took for it to stop
- Data is from first six months of 2011

(AWS)

- There was a single recurring host from AWS. Given their size, that's probably a very good indicator

  Wed Apr 20 06:54:50 PDT 2011 FW Block: 122.248.246.104 Sweep

  Wed Apr 20 06:54:54 PDT 2011 Complaint: 122.248.246.104 abuse@amazonaws.com ec2-abuse@amazon.com email-abuse@amazon.com

  Wed Apr 20 21:34:48 PDT 2011 FW Block: 122.248.246.104 AdminProtocol

  Wed Apr 20 21:34:49 PDT 2011 Complaint: 122.248.246.104 abuse@amazonaws.com ec2-abuse@amazon.com email-abuse@amazon.com

- Based on this, Amazon's response time to complaints/incidents is at least 14.5 hours

Rackspace/Slicehost

- There were 10 recurring hosts from Rackspace. The worst:

Thu Mar 17 22:18:36 PDT 2011 FW Block: 184.106.187.15 Sweep

Thu Mar 17 22:18:37 PDT 2011 Complaint: 184.106.187.15 abuse@cloud-ips.com abuse@rackspace.com abuse@slicehost.com

Sat Mar 19 22:45:10 PDT 2011 FW Block: 184.106.187.15 Sweep

Sat Mar 19 22:45:11 PDT 2011 Complaint: 184.106.187.15 abuse@cloud-ips.com abuse@rackspace.com abuse@slicehost.com

- Based on this, complaint/incident response time from Rackspace is greater than 48 hours

Softlayer: Your World Wild Web provider!

SOFTLAYER®

- 5 recurring hosts from Softlayer; all spanned multiple days
- Softlayer **never** responds to complaints or incidents, or at the very least, response is measured in months

The Proof: Softlayer Data

Mon Feb 14 02:46:37 PST 2011 FW Block: 174.37.237.66 Sweep
Mon Feb 14 02:46:38 PST 2011 Complaint: 174.37.237.66 abuse@softlayer.com
Tue Apr 19 04:26:09 PDT 2011 FW Block: 174.37.237.66 Sweep
Tue Apr 19 04:26:11 PDT 2011 Complaint: 174.37.237.66 abuse@softlayer.com
Fri May 13 10:29:53 PDT 2011 FW Block: 174.37.237.66 Sweep
Fri May 13 10:29:53 PDT 2011 Complaint: 174.37.237.66 abuse@softlayer.com
Mon Jun 13 09:06:44 PDT 2011 FW Block: 174.37.237.66 Sweep
Mon Jun 13 09:06:45 PDT 2011 Complaint: 174.37.237.66 abuse@softlayer.com

Not as bad:

Thu Mar 10 18:02:58 PST 2011 FW Block: 174.37.255.47 AdminProtocol
Thu Mar 10 18:03:20 PDT 2011 Complaint: 174.37.255.47 abuse@softlayer.com
Fri Mar 18 23:21:20 PDT 2011 FW Block: 174.37.255.47 Sweep
Fri Mar 18 23:21:20 PDT 2011 Complaint: 174.37.255.47 abuse@softlayer.com
Sun Mar 20 03:41:04 PDT 2011 FW Block: 174.37.255.47 AdminProtocol
Sun Mar 20 03:41:05 PDT 2011 Complaint: 174.37.255.47 abuse@softlayer.com

Tighten it up

- Clients should have their own IDS/ firewall/etc, but…
- Hosts that are attacking multiple clients should be detected and shunned by the provider
- The provider should take steps to help their clients protect themselves
- The provider should also be looking for intentionally malicious clients

DANGER!

- Consolidating events from all client environments to look for enterprise-threatening external agents would improve things, but…
- The single largest unaddressed threat is the client networks

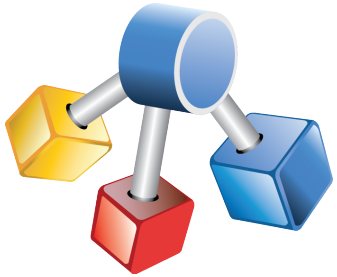
What Are Providers Dealing With?

- Frequent, rapid client changes
- Clients with a wide variety of services, users, and ways of utilizing resources
- Clients who are in an unknown state
- A need to be as close to 0% false positive as possible

What Stays the Same?

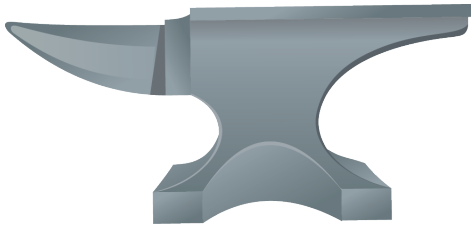
- In-line IPS, owned and controlled by the client
- Firewall, owned and controlled by the client
- Vulnerability Assessment (VA)
- Well-understood technologies that allow clients baseline control over their own networks within the cloud

What Are We Adding?



Netflow Analyzer

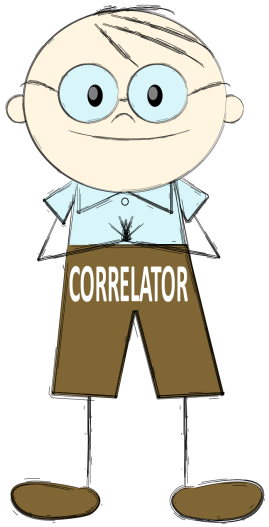
IDS



NAC

On-access misconfiguration detection

Log Consolidation



Event Correlation

Why Not OSSIM?

- http://alienvault.com/community
- OSSIM uses many of the same tools I'm suggesting
- It makes assumptions about the network it's placed into (tool/vendor lock-in)
- Correlation engine is not as flexible as SEC; regardless, has advantages

Netflow (nfdump)

- http://nfdump.sourceforge.net/
- Used to monitor for excessive, prolonged network utilization
- Can also trend network performance and flag suspicious spikes
- Data is sent from internal switches and other network devices for analysis
- Provides network server/service inventory data

Enterprise-Wide IDS (Snort)

- http://www.snort.org/
- Well-known, widely used
- Independent of clients; no client visibility
- Attached to network egress points
- No trusted networks: monitoring ALL traffic
- Provides network server/ service inventory data

NAC (PacketFence)

- http://www.packetfence.org/home.html
- Post-admission behavioral quarantining
- This system will take input from our other systems, and use it to make decisions to quarantine devices

Log Consolidation (syslog-ng)

- Well-known, widely used
- All infrastructure devices (servers, switches, IDS, etc) logging here

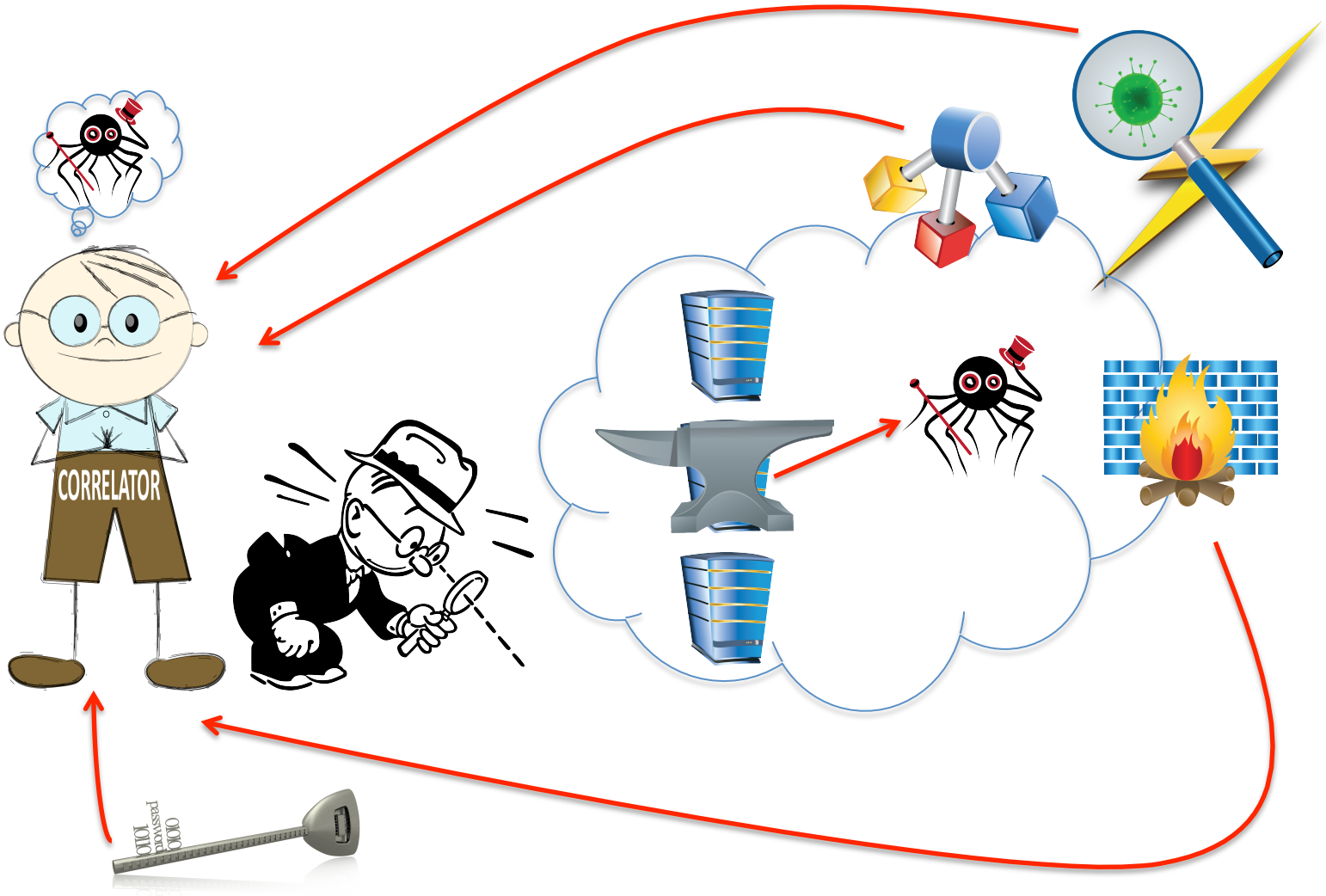
On-Access Misconfiguration Detection

- Medusa
  http://www.foofus.net/~jmk/medusa/medusa.html
- Metasploit
  http://www.metasploit.com/
- Nmap
  http://nmap.org/
- Others
- Tools called by correlation system to run basic misconfiguration checks of new services and servers

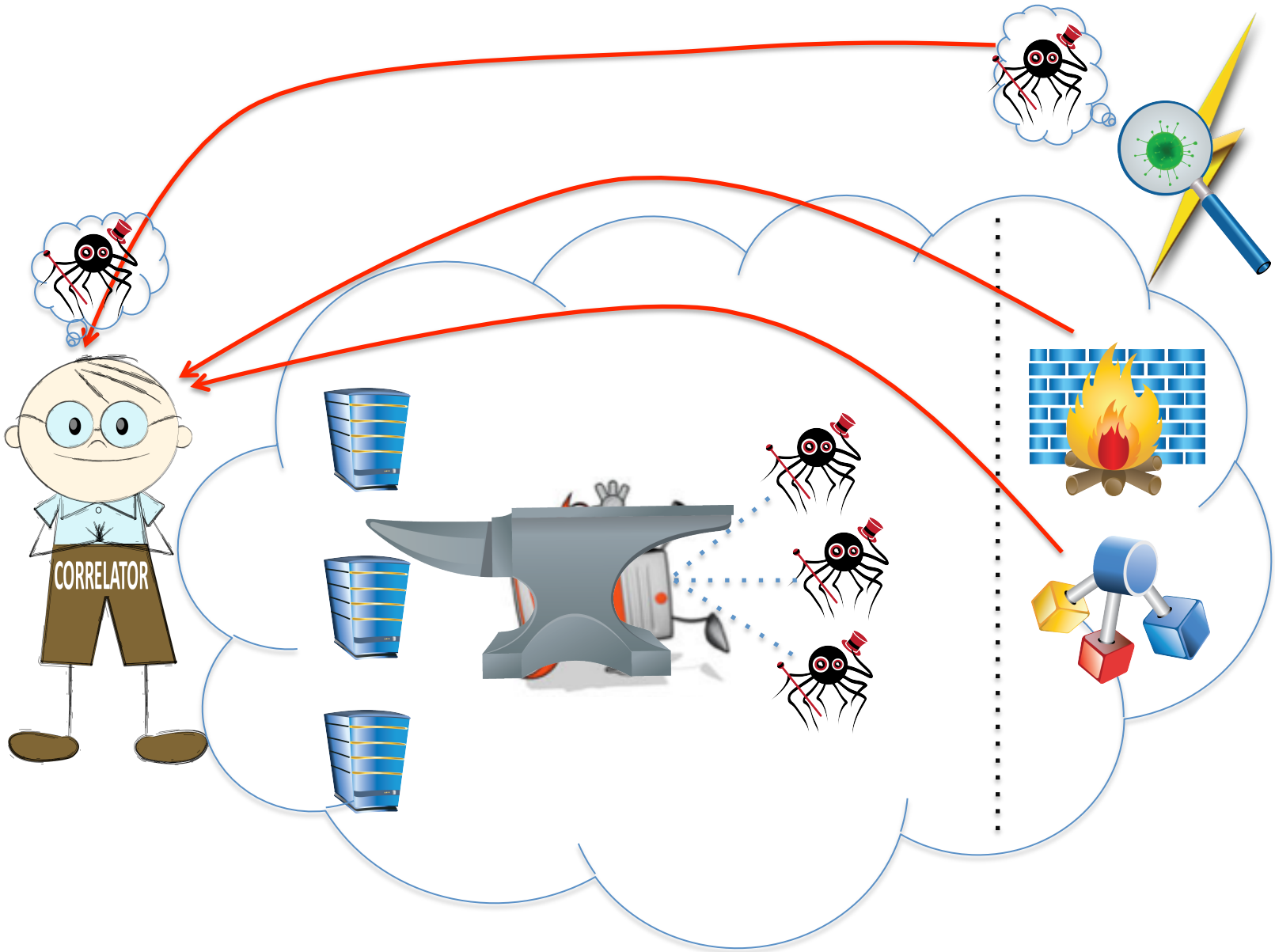
The “Magic”: Correlation (SEC)

- http://simple-evcorr.sourceforge.net/
- Keeps track of events from a variety of sources
- Isn’t in-line, makes it possible to make slow, well-informed decisions
- Coordinates all other components

How does this work?



Identifying Misbehaving Hosts



nfdump

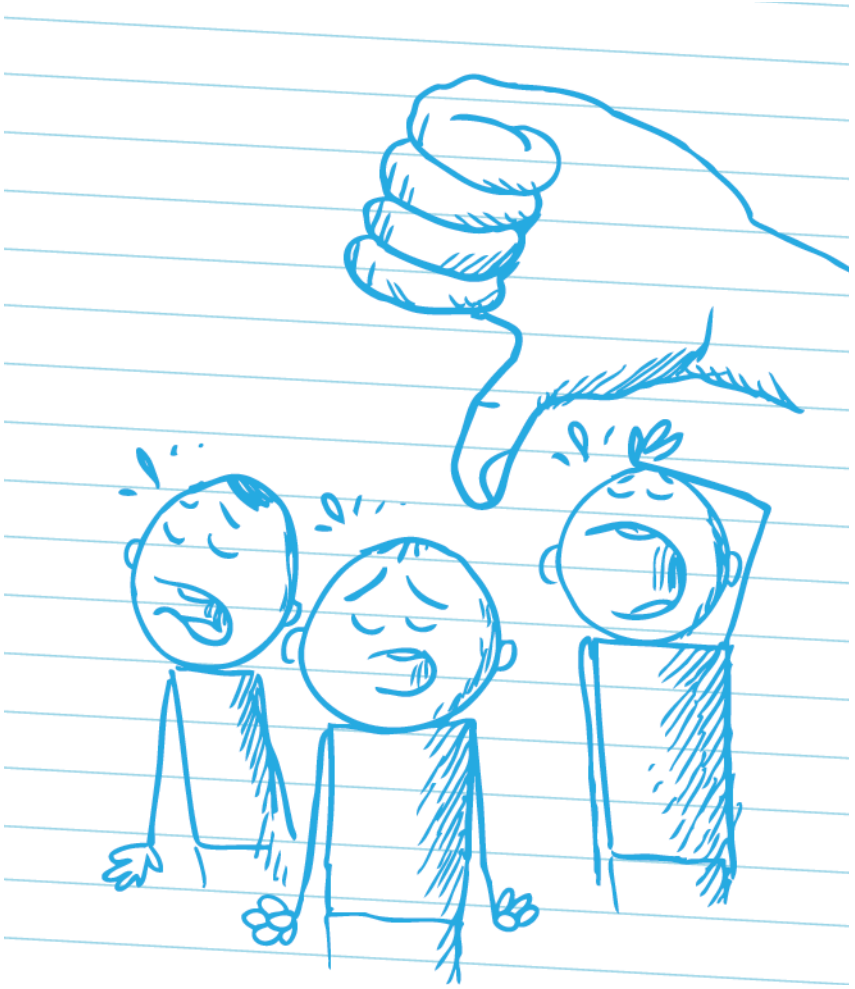
- Unusual traffic patterns alone don't dictate an incident
- nfdump data should be compared with IDS, firewall and other data to look for anomalies
- Example: Traffic peak, combined with ARP collision messages from switches → ARP Cache Overflow
- Example: Traffic peak, combined with many IRC events → Botnet Participation

Correlated IDS Logs

- Much better information, but limited to what we can see
- Example: Single event type enters server, replayed by server multiple times → Worm Infection
- Example: Server contacts successive servers using the same administrative protocol → Protocol Scanning

Limitations

- Err on the side of caution
- Reactive, so damage might already be done



Demonstration

Conclusion

- Cloud providers don't appear to be internally policing their clients' networks
- Reliable measures should be be taken to detect both malicious clients and compromised clients

Questions