The Case for Network Forensics

ISSA D.C. – Dec. 15, 2009

Peter Schlampp – VP, Product Management
Solera Networks

Obligatory Fear Mongering Intro

HIPAA, GLBA, Basel II, SOX, FISMA,
MiFID, GRC, FERPA, PCI, CALEA,
Insider-threats, Data-leakage,
Identity-theft, Gumblar/Conficker/Botnets,
Social network attacks, XSS, CSRF,
SQL-injection, DNS rebinding/poisoning,
TJX, Heartland Payment, IM/P2P leaks,
Mebroot/Torpig/Rootkits, HR-liability,
Exfiltration, Deperimeterization

No Shortage of “Anti-threat” Countermeasures

- Firewall, UTM, NG-FW
- IDS/IPS, Gateway Anti-Malware, Anti-Spam
- Host AV, Endpoint security, NAC
- 2FA, Strong Auth/Identity
- Content-filtering, WAF, DLP
- Honeypots, NBAD, Log analysis, SIEM

Since infinite resources cannot be allocated to countermeasures, the goal should be the mitigation of risk to an acceptable level

Yet you can only find what you're looking for

- **Risk** is the probability that some **threat** will exercise a certain **vulnerability** so as to negatively impact an **asset**
- Such events, or exploits, are only detectable by information security controls that have previously classified the events
- The occurrence and impact of an event *today* might not be known for weeks or months

Is it possible to unobtrusively and completely defend against the unknown, undetectable, and invisible?

Data Breach Investigations Report (June 2008)

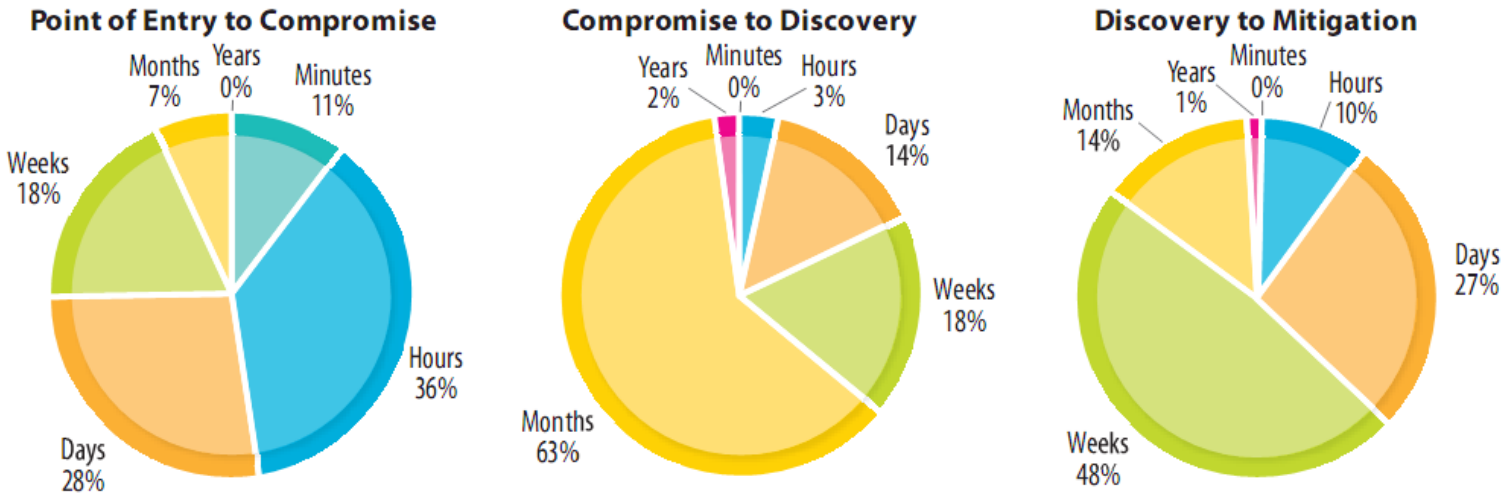


Figure 21. Data Breaches: A Time Span of Events

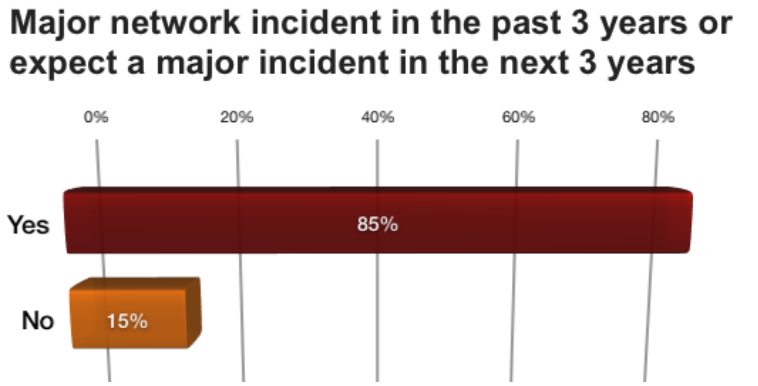
"… the main reason for this is that victims do not know how to respond. Many organizations—even those with full-time security resources—either have no incident response plan, or have never vetted it against real-world incident scenarios."

** http://www.verizonbusiness.com/resources/security/databreachreport.pdf*

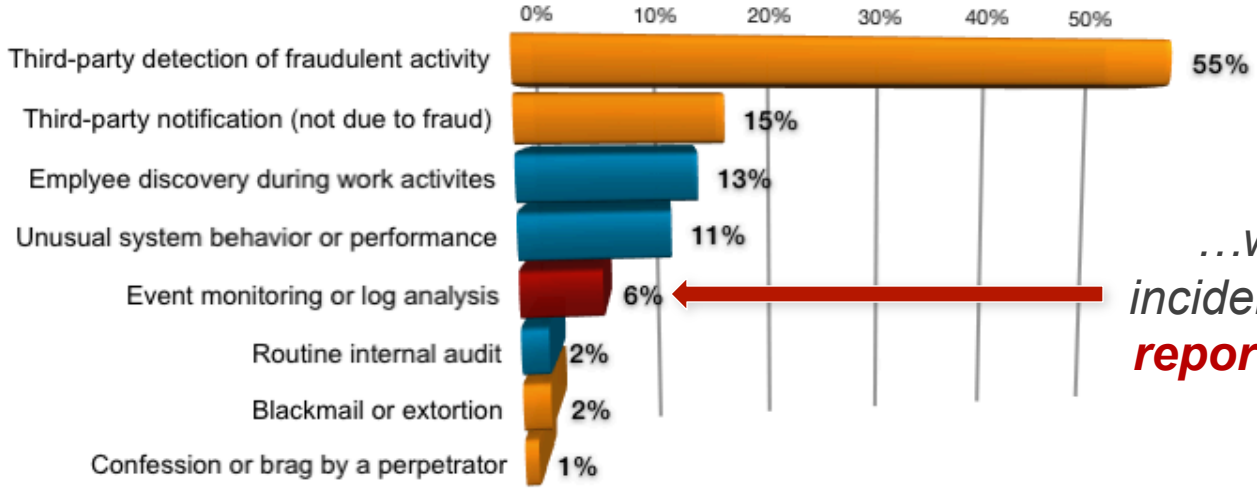
SOLERA NETWORKS

How will I know if I've been breached?

85% had a major network incident in the past 3 years or expect a major incident in the next 3 years…



Source: Trusted Strategies Network Forensics Survey, September 2009



Source: Verizon Business Report, 2008

…when network security incidents occur, ***existing tools report it only 6% of the time.***

SOLERA NETWORKS

“We need more humility”

- “The bad guys know all about the security methods employed in the industry. *We need more humility*.” - Robert Carr, Heartland Payment Systems CEO
- Why do we continue to have so much faith in tools that fail so frequently?
- **Hindsight bias** - our tendency to overestimate what we knew about a past event based on subsequent information
- This sense of being able to “predict” the past makes us more confident in our ability to predict the future

http://www.csoonline.com/article/print/499527

Experience Resists Transference

- “The audits done by our QSAs (Qualified Security Assessors) were of no value whatsoever” - Robert Carr, Heartland Payment Systems CEO
- It is difficult for us to understand risk based on the experience or of advice of others
- The worst of both worlds - we simultaneously underestimate and overestimate based on history

!= Security

http://www.csoonline.com/article/print/499527

SOLERA NETWORKS

“Invest in Preparedness, not in Prediction”*

- The probabilities of unknown or rare events aren't highly computable, but their consequences can be ascertained
- The occurrence of any event is rarely as important as the magnitude of its outcome
- Focusing on the prediction and prevention of past rare events can make us more vulnerable to future rare events
- Unknown events should be dealt with by preparing to deal with their *consequences*

From Nassim Taleb’s The Black Swan

Incident Response – the Basics

1. Contain the damage
2. Preserve/duplicate the compromised system's state
3. Contact law enforcement and legal agents
4. Restore operations of compromised system
5. **Determine incident cause**
6. Document incident and recovery details
7. Update control agents/implementation details accordingly
8. Update incident response plan, as needed

- Controls the indirect damage, such as injury to reputation, negative publicity, lost customer confidence, legal repercussions, and other fines or penalties
- Identifies and resolves the root causes of the incident, determines scope of impact, and helps prevent repeat occurrences

But the fact that it happened often implies that it was undetectable. How do you determine the cause of something after it already happened undetected?

NIST Special Publication 800-61 "Computer Security Incident Handling Guide" http://csrc.nist.gov/publications/nistpubs/

Surveillance is Vital to Physical Security

Why Not Network Security?

SOLERA NETWORKS

Introducing Network Forensics

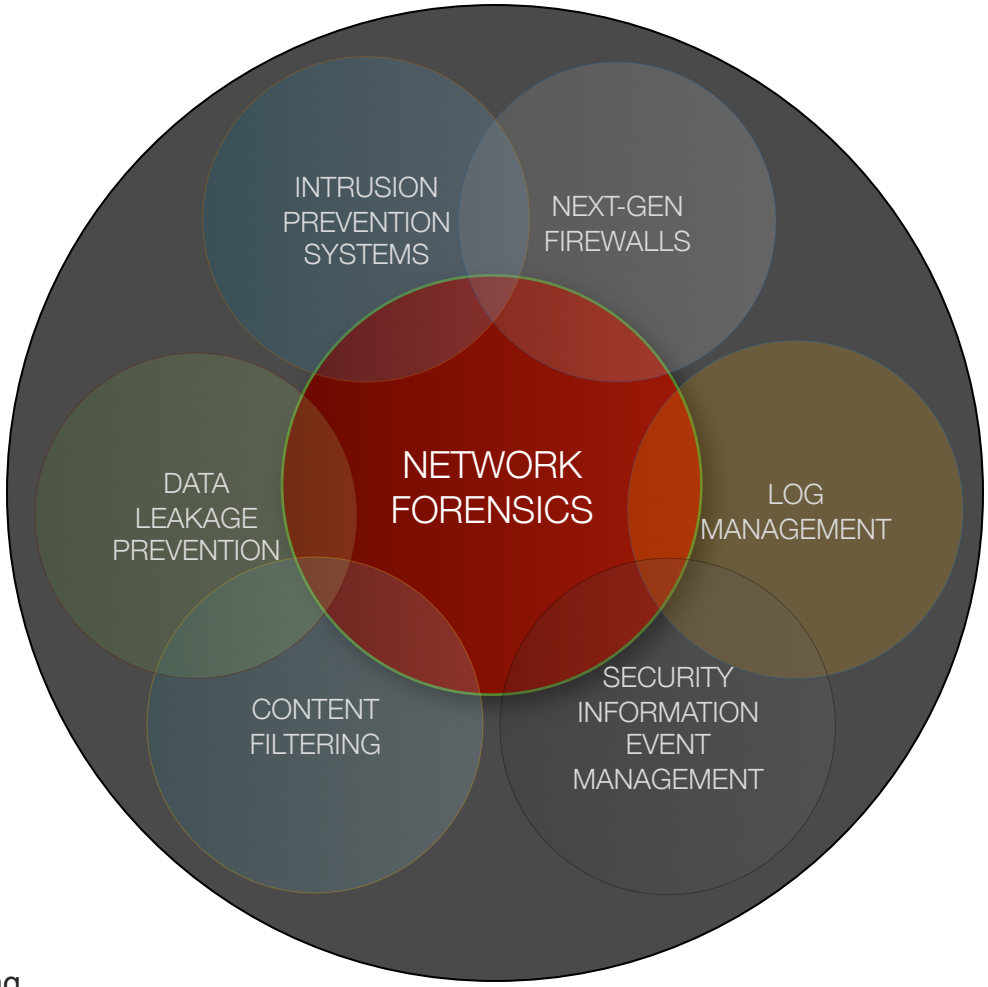
SOLERA NETWORKS

Network Security Landscape

Network Forensics uniquely **captures all data** crossing the network

It **fills an important gap** in today's network security landscape

It provides **full context** and **actionable evidence** to stop and remediate



"'**The fastest-growing area is network forensic software**… [it] doubled in value between 2007 and 2008…' He predicts that the market will jump another 50% by the end of this year."

-- *The Economist* quoting Gartner® Analyst John Pescatore

SOLERA NETWORKS

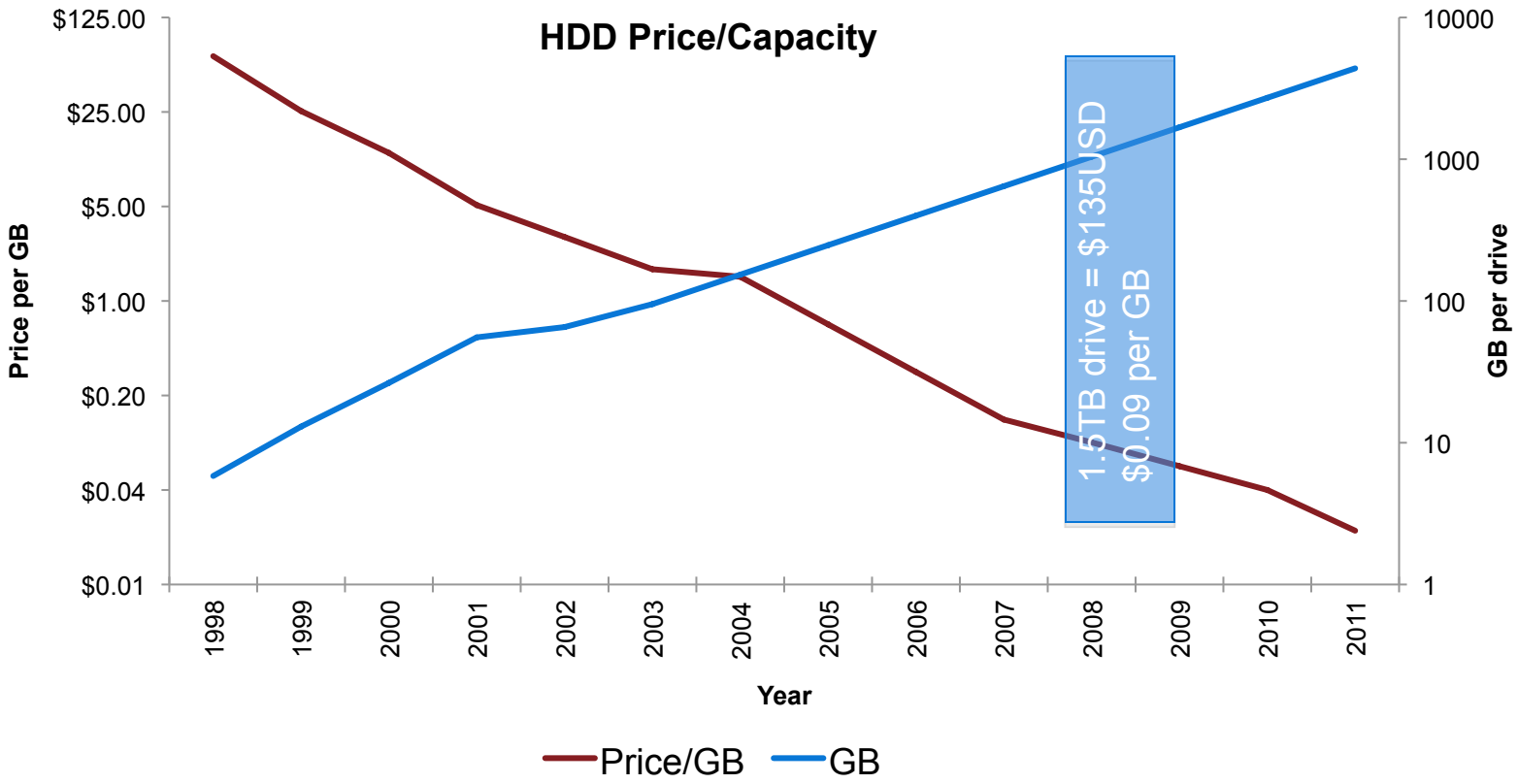
Network Forensics

- Previous attempts at network forensics rely on logs, IDS/IPS events, SIEM analysis, or subject-specific intercept
- To date, it has been infeasible to capture traffic at rates above Fast Ethernet because at those proportions:
  1. It's hard to pull the packets off the wire
  2. It's hard to lay them down on disk
  3. It's hard to visualize network traffic
  4. It's hard to find packets once they're there

Speed-Mbps	GB/Hour	TB/Hour	TB/Day
50	21.97	0.02	0.51
100 (FE)	43.95	0.04	1.03
500	219.73	0.21	5.15
1000 (GigE)	439.45	0.43	10.30
5000	2197.27	2.15	51.50
10000 (10GE)	4394.53	4.29	103.00

SOLERA NETWORKS

Storage Trends Enable Total Fidelity



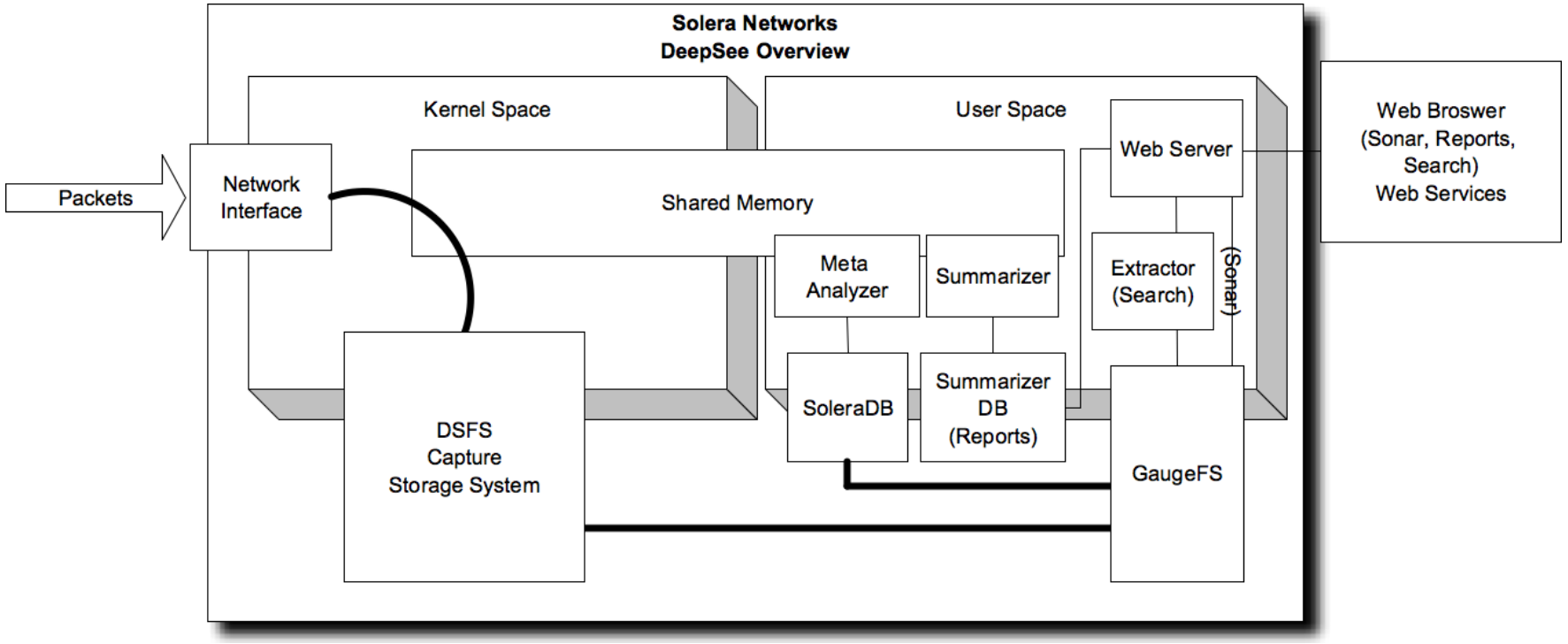
Sources: http://commons.wikimedia.org/wiki/Image:Hard_drive_capacity_over_time.png
http://www.alts.net/ns1625/winchest.html

SOLERA NETWORKS

The Needle in the Haystack

- So you've captured just over 3 days of traffic on your generally 1/3 utilized 10Gbps network:
  - That's about 100TB of data
  - For around 183 billion "average" sized packets (600 bytes)
  - At an average of 650,000 packets per second
- And now you want to find all the packets from IP address 71.213.89.177:
  - Do you read through 50 x 2TB or 50,000 x 2GB files?
  - Wouldn't it be helpful to have an index?
  - What database can handle 650,000 inserts per second?

More than a Collection of PCAPs



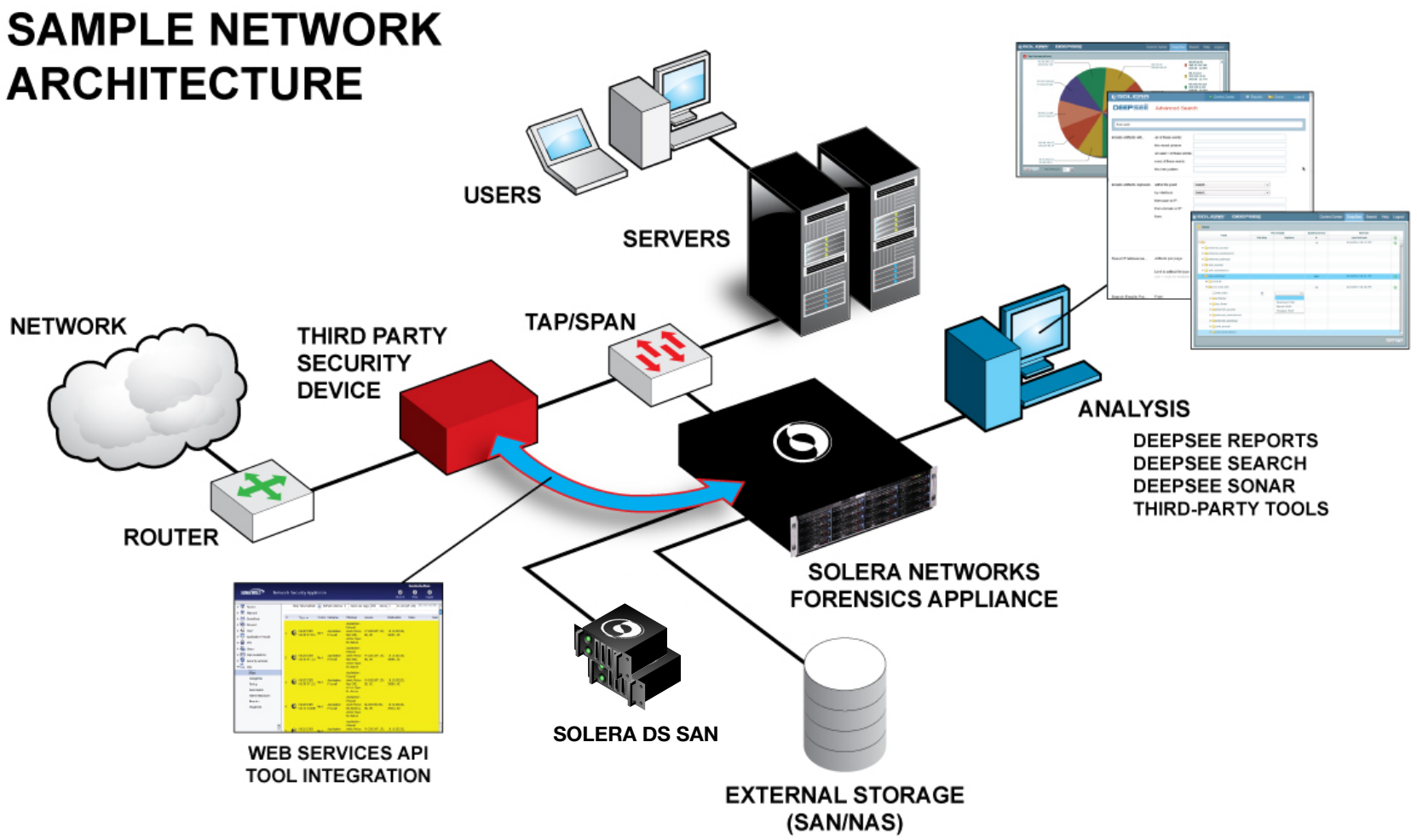
- Purpose-built DSFS packet-repository file system
- Packet-attribute specific database, scales with hardware
- Packet-centric virtual file system

A Better View into the Past – Instant Recall

ls -la /pfs/flows/ipv4_address/71.213.89.177

```
-r--r--r--  1 root root    0 2009-09-08 19:24 data.pcap
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ethernet_address
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ethernet_destination
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ethernet_protocol
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ethernet_source
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 interface
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ip_protocol
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ipv4_destination
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ipv4_source
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ipv6_address
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ipv6_destination
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 ipv6_source
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 packet_length
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 tcp_destination_port
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 tcp_port
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 tcp_source_port
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 udp_destination_port
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 udp_port
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 udp_source_port
dr-xr-xr-x  0 root root 4096 2009-09-08 19:24 vlan_id
```

Functional Deployment

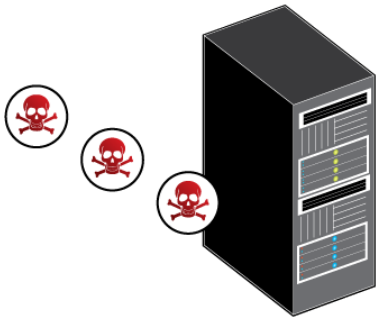


Collaboration

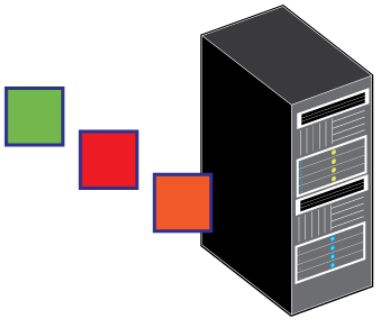
- There are many points of intelligence in our information systems
- However imperfect, their perspectives can serve as signals to larger events
- Simplifying the sharing and correlation of information can improve response
- Full contexts can be reconstructed from basic event descriptions

Negative Day Threat Detection

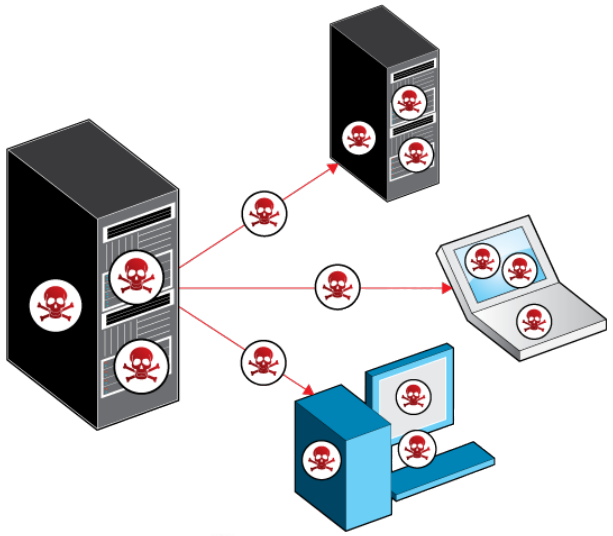
Malware Monday



Patch Tuesday

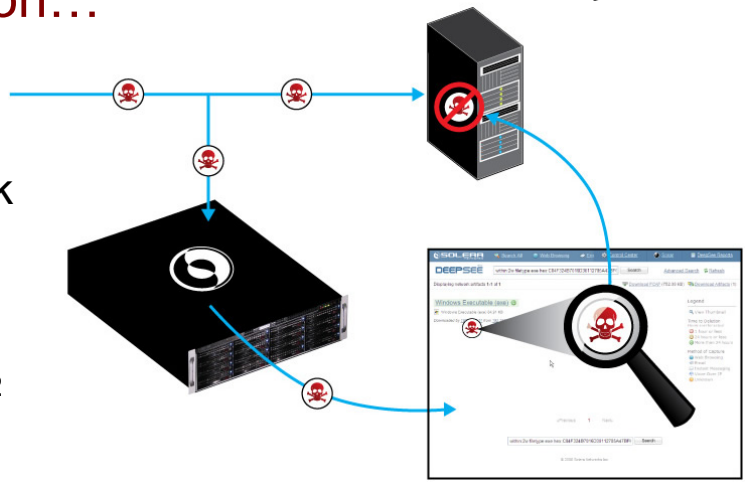


Wake-up Call Wednesday



Events can occur prior to remediation…

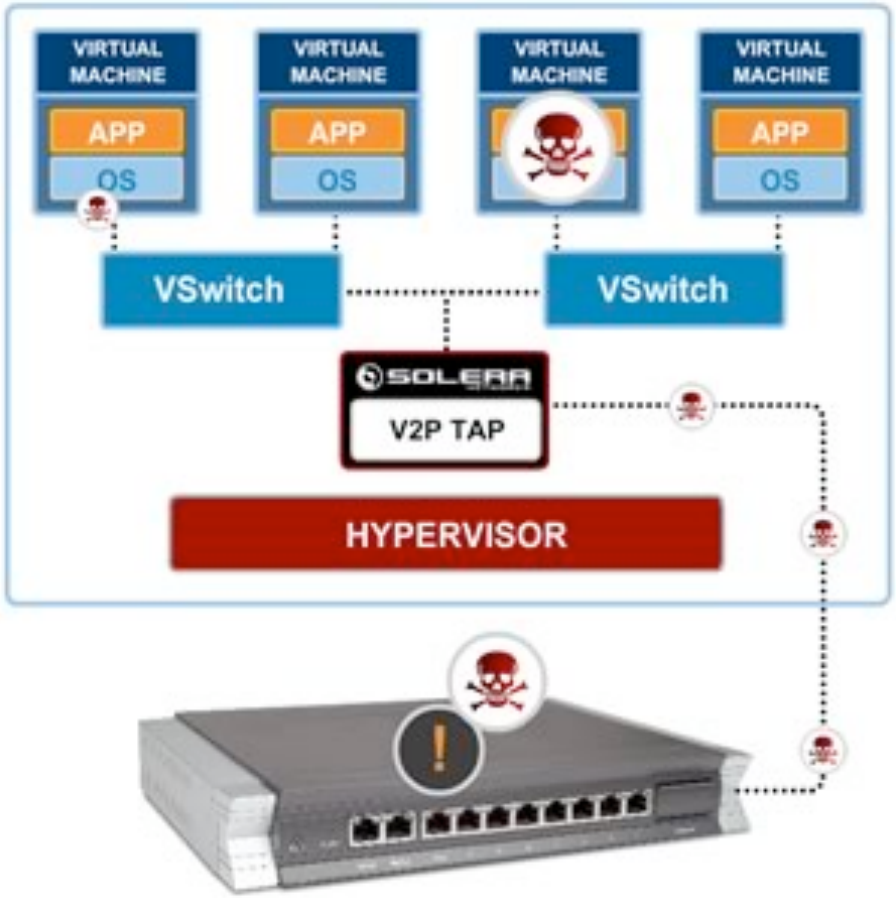
1. Microsoft released MS08-067 patch on October 23, 2008[1]
2. Evidence of exploits in the wild (dating back weeks) emerged shortly thereafter
3. Network memory allows a search for all executables containing hex-pattern: C84F324B7016D30112785A47BF6EE188[2]



1. http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
2. http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067?rev=1.8;content-type=text%2Fplain

SOLERA NETWORKS

Spanning the Virtual to the Physical



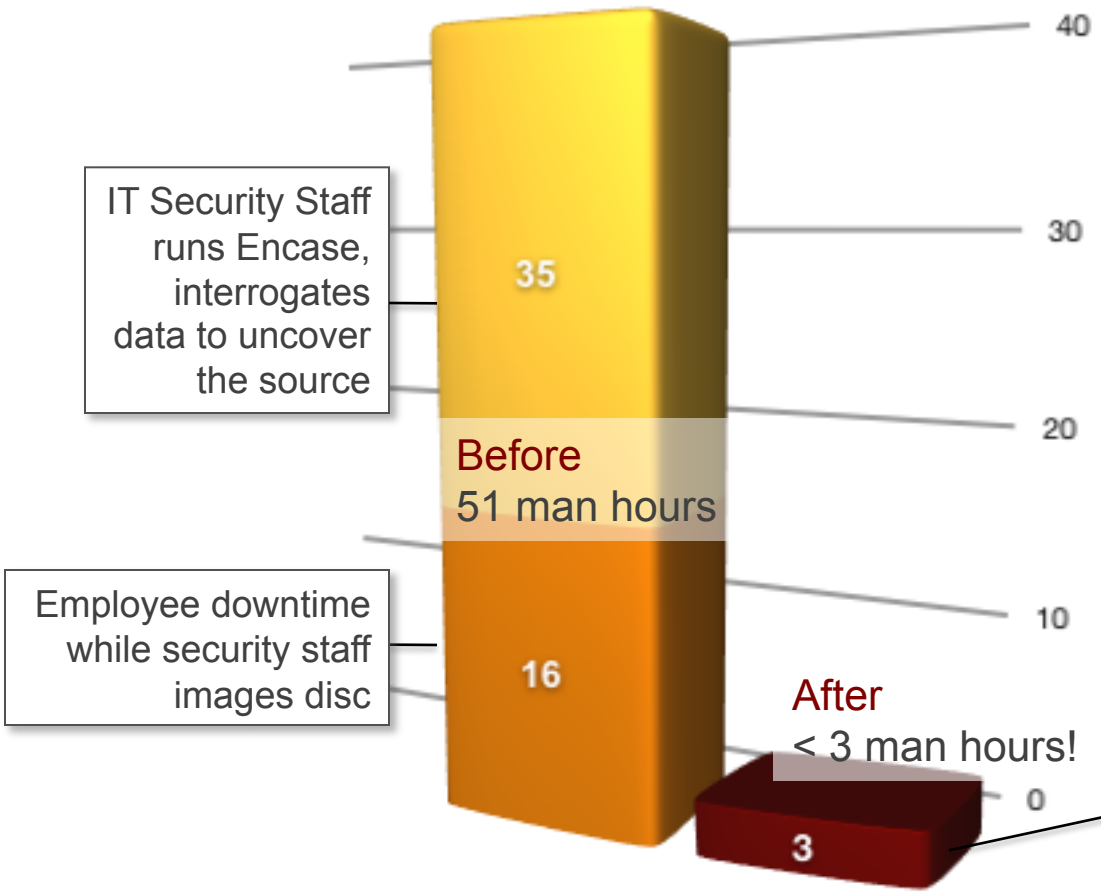
- V2P Tap sits passively off the vswitch
- Regenerates traffic outside the physical host to any security tool
- Complete visibility into intra-VM traffic

- Use existing tools from physical network
- Leverage current methods, processes, and IT professionals

SOLERA NETWORKS

Save Time/Money and Eliminate Risk

Network forensics doesn't need to be a costly and difficult process



Finding the source of a security event:

- Eliminate employee downtime
- Reduce exposure to further risk
- < 3 hours vs. 51 hours

Source: Pacific Northwest National Lab (PNNL)

SOLERA NETWORKS

Q&A

THANK YOU

pschlampp@soleranetworks,com