



# Are You Still Fighting the Cyber War of 1995?



**Jeff Michael, Senior Systems Engineer, NetWitness Corporation,  
[Jeff.michael@netwitness.com](mailto:Jeff.michael@netwitness.com)**

- Observations on the current threat environment and what we can do to improve security during operations
- The need for network forensics and next generation monitoring and deeper inspection of network traffic
- Technology illustrations and specific cases
- Final thoughts and Q&A





---

## Observations on the Threat Environment



- People
  - Underestimate threat
  - Lack InfoSec knowledge and experience
- Process
  - Horrible IT metrics at best
  - Focus on compliance vs security
- Technology
  - Well suited to fight 1995's Cyber War
  - Deep holes in network visibility that must be addressed

- Electronic Criminal Groups: Rapidly Emerging Underground Industry (several examples of successful large scale operations)
  - Organization: High
  - Capability: High
  - Intent: High for financial gain, unknown otherwise
- Nation-Sponsored Activities: From Intelligence Gathering to Network-Centric Warfare
  - Organization: High
  - Capability: High
  - Intent: Connected to national policy



- (Chinese Information War: Theory and Practice / aka “Dragon Bytes”, Sandia, DoD, State Dept, DHS, Germany)

# Today's Threat Landscape... Easy Money



Quantity

<b>Price List: VISA, MasterCard USA (with cvv2 code)</b>		
количество	идентификация	цена в \$USD
5-50	есть в продаже	5.0
51-100	есть в продаже	4.5
101-500	есть в продаже	4.0
501-1000	есть в продаже	3.0
1001-5000	есть в продаже	2.0
более 10000	есть в продаже	пишите
Если Вам нужно более 10000 карт, свяжитесь с нами, для Вас будет отдельная скидка		

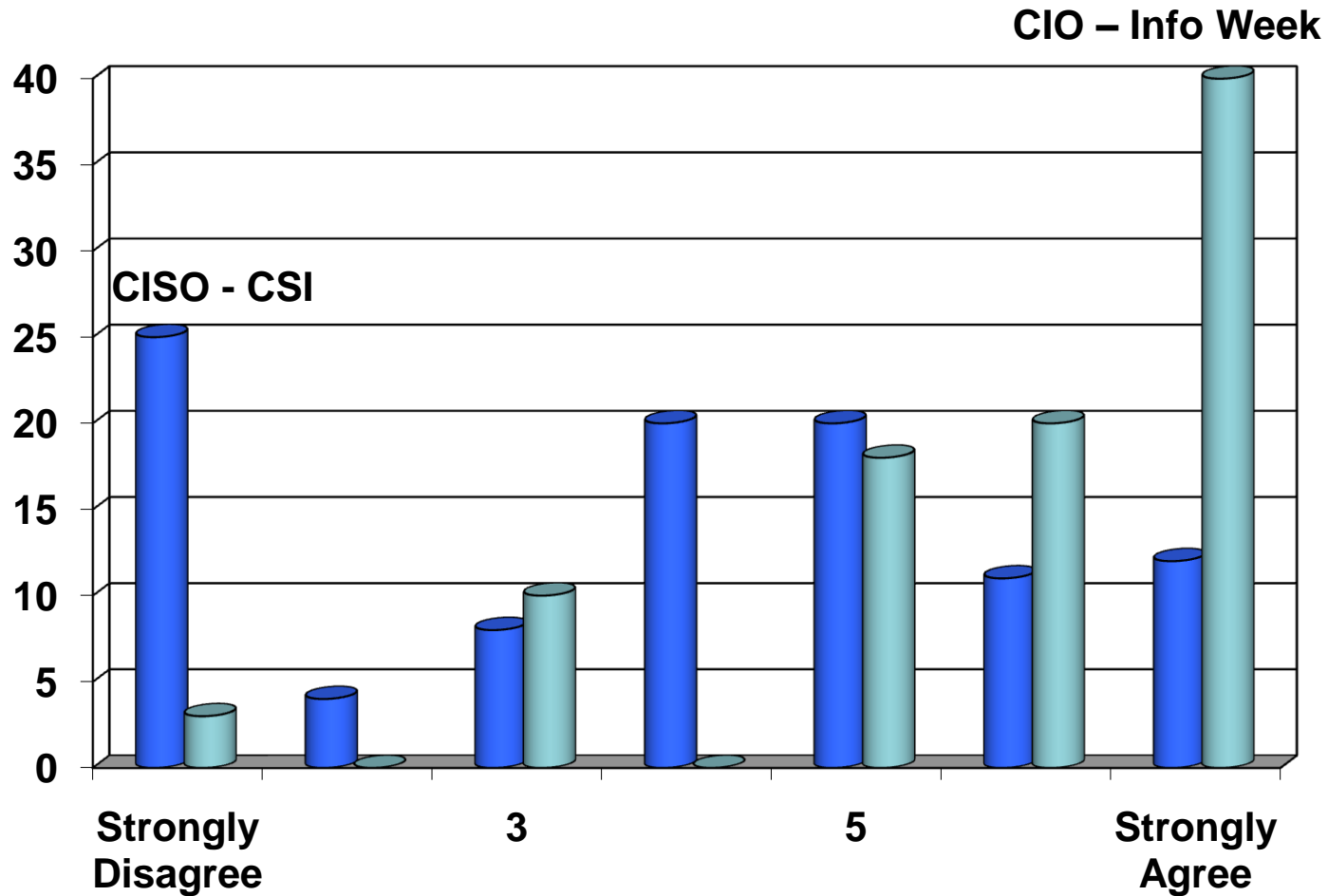
Price in \$USD

Call for Bulk Pricing

(Other providers sold separately)

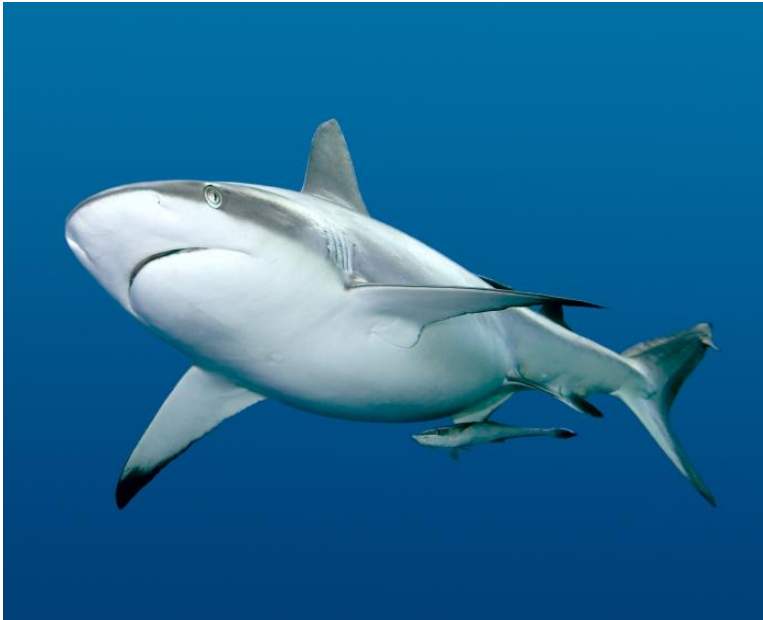
Source: iDEFENSE

# Underestimating the Threat: Has SOX Improved Our Security Posture?



Source: Pam Fusco

# Does Your Staff Have the Experience to Measure Threats?



VS.





Risk = Threats x  
Assets x  
Vulnerabilities





The good....

The bad & the ugly....



## Compliance vs. Security

# Advanced Threats Look Like...NORMAL



- Stealthy way in on any day
  - Spear Phishing email with new exploit in (office, adobe, etc...)
  - Webside malware with mobile code exploit (Java, JavaScript, ActiveX, etc...)....drive by or targeted
  - USB (drive, device, etc..)
- Persistence
  - Reboot: AV, Windows Update/Malware Removal and typical protections, Patch
  - DynDNS, peer/group architectures
- C&C and Exfiltration
  - Beaconing every xx, tunneling/encapsulation,
- Sleep well, Safely Protected by
  - AV, Vulnerability Scanners, IDS, Log Aggregators and SIEM, NetFlow, and now DLP





**Firewalls**

**IDS/IPS**

**Anomaly  
Detection**

**Content  
Monitoring**

**End-point  
protection**

- Unfortunately, “defense-in-depth” has been built upon a series of point solutions offering incomplete capabilities:
  - Signature based detection
  - Zone segmentation
  - Access controls
  - Packet filtering
  - Content monitoring
- This approach leaves many potential gaps in your network visibility, exploited by your top adversaries today:
  - Application attacks
  - Zero-day threats
  - Data loss events
  - Designer malware



TECH TRENDS: Wireless, Web 2.0, SOA, social networking, mobile computing, mobile code, XML, RFID

De-perimeterization /  
Connections to everyone

Transient user/partner base,  
globalization, digitization

- Security Infrastructures:
- No host trustworthiness for the foreseeable future
- Security is perimeter-based, external threat and network layer focused
- Largely signature-based/obsolete by definition against advanced threat
- Log and flow-based monitoring relies on the above (GIGO)
- Even the “silver bullets” are far from (consider authentication)
- Supply chain security issues

## The Bottom Line

- ALL THREATS ARE ALREADY ON THE INSIDE
- ALL EXPLOITS THAT MATTER ARE T MINUS 21 FROM ZERO-DAY
  - TRAFFIC LIGHTS OF RANDOMNESS

The End? Nah....





---

## The Need for Network Forensics

# What is Network Forensics?

---



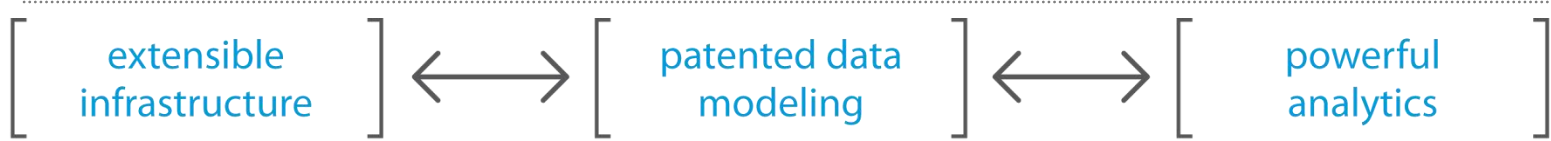
“Reconstruction of network events to provide definitive insight into actions and behavior.”



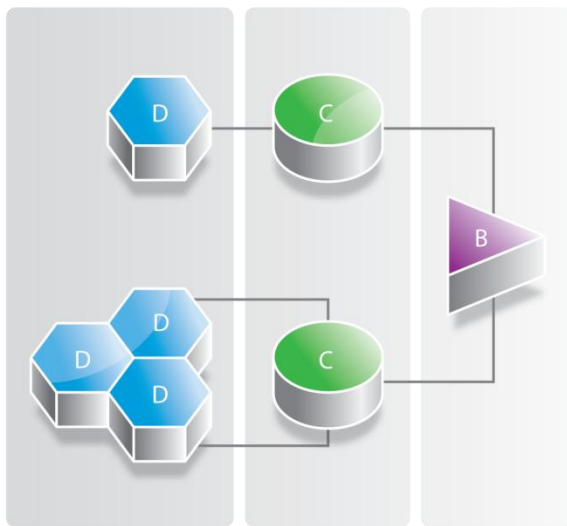
## **USE CASES:**

- **Continuous Augmented Awareness**
- **Incident Response and Post-Facto Investigatory Support**
- **Advanced Threat Intelligence**

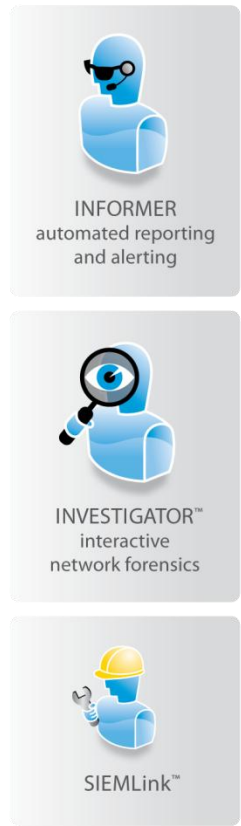
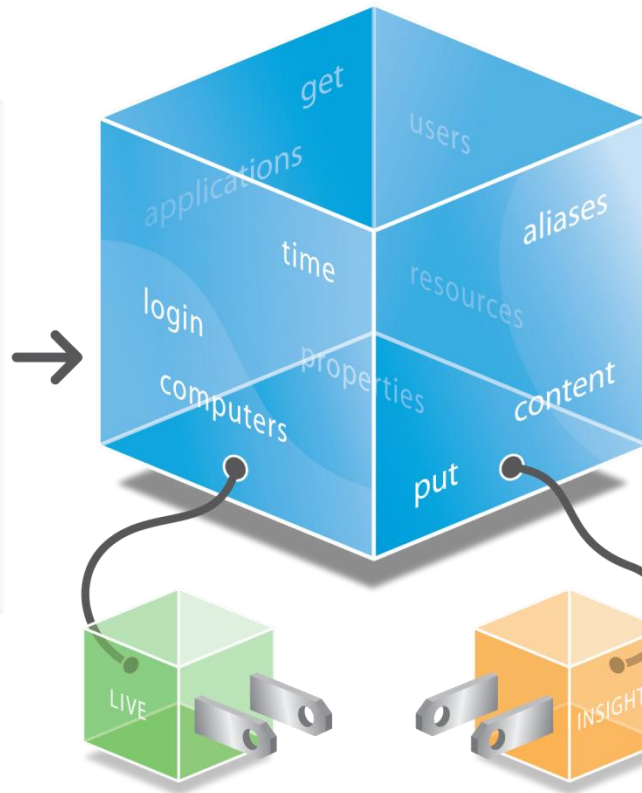
# How Does NextGen Work?



## NEXTGEN™ METADATA FRAMEWORK



DECODER → CONCENTRATOR → BROKER



- Enable your analysts to view network traffic as conversations instead of individual packets or groups of IP addresses
- Data reduction from a sea of full packet captures to organized metadata – orders of magnitude
- Render layer 7 protocols, e.g., Web-pages visited, reconstruct protocols such as email & chat
- Perform quick analysis & speed to findings and resolution
- Obtain total network knowledge and dramatically improved network visibility





- Why is our top destination today a foreign IP address with whom we never communicate?
  - Why is our top destination port 15347?
  - How can I be sure this SIEM event is a false positive?
- What is the magnitude of this incident?
  - What % of our employees are shopping for jobs or talking to competitors?
  - Who is using policy evasion technologies such as TOR, or PGP encryption?
  - What is the potential source of an attack or breach?
  - How is data leaving our organization?
  - Who is using Skype and other technologies to transfer files out of our network?



# Live Illustrations



---

## Final Thoughts and Conclusions

# Building Continuous Augmented Awareness Around Common Business Problems



- Data leakage
  - PII, SSN, DL, DoB, Address, etc.
  - Organization-specific content
- Compliance monitoring and measurement
  - GLBA, FISMA, HIPAA, PCI, SoX, etc.
- Counter-Intelligence
  - Outbound Network Activity
  - Inbound Network Activity
  - Top Email Competition Outbound
  - Top Email Competition Inbound
  - Email Outbound with Attachment
  - Email Outbound with Crypto
- Network Management
  - Top IPs Initiating DMZ Sessions
  - Top IP DNS Zone Transfer
  - Externally initiated streams
  - External Access Attempt to Internal Fileserver
  - Internal DNS Server Comm with External Hosts
  - Top FTP IP Destinations by Byte Count
  - Top FTP Users
  - Top FTP Files Deleted
  - Top FTP Files Up/Downloaded
  - Top Files FTP'd
  - Top FTP Passwords
  - Top FTP Files by Byte Count
  - Top IP Addresses by 'Anonymous' FTP



- MalCode / Hacker Related
  - BOTNet Activity
  - SQL Injection Scanner Executables
  - Malicious Email Attachments
  - Log "Hacking"
  - Root Access
  - password file access
  - Hacker research (URLs, hostname, newsgroups)
  - Hacker Application file Names
  - External to Internal Direct Jet
  - Username/login Buffer Overflow
  - QueryString Parameter Overflow
  - SQL Injection Scanner Executables
  - Unix commands in URL
- Web Browser as Attack Tool (phf Attack)
- IIS Buffer Overflow Attempt
- IRC Malicious Download
- IRC Malicious Open
- FTP Malicious Download
- FTP Malicious Upload
- Anomalous Activity
  - Top IP HTTP not over port 80
  - Top IP non-HTTP over port 80
  - Top IP non-FTP over port 21
  - Top IP non-SMTP over port 25
  - TOP IP non-DNS over Port 53
  - TOP IP SSH not over port 22
  - TOP IP SSL not over 443
  - Top IP non-SSL over 443



- System Administrative
  - Top Files Accessed
  - Top Files Printed
  - Administrative Accounts
  - Most Active Email
  - Most Active Logins
  - Most Active Logoffs
  - Failed Windows Login
  - Default Cisco Router Passwords
  - Top Database Users
  - SQL Query (meta count)
  - Database by Bandwidth
  - Top IP Running Oracle
  - Top IP Running MSSQL
  - Unencrypted DB Access
- I/T Asset Misuse
  - Gnutella/TOR/Tunneling
  - Clear-text passwords
  - Content Crypto
  - Unusual Services
  - Anonymizers
  - Yahoo Message Board Post
  - Google Message Board Post
  - Warez URL
  - Porn Sites
  - Auction Sites
  - Gambling Sites
  - Wireless Protocols
  - 2 MACS using 1 IP
  - Source Code
  - Job Searching
  - Google Searching

# Network Visibility Data Source Value Chain



Data Source	Description
IDS Software	Sometimes the first indicator of a problem, for known exploits. Can produce false positives and is signature based.
SEIM Software	Correlates IDS and other network and security event data and dramatically improves signal to noise ratio. Is valuable to the extent that data sources have useful information and are properly integrated.
Firewalls, Gateways, etc.	Overwhelming amounts of data with little context, but can be valuable when used within a SEIM and in conjunction with full packet capture and network forensics reviews.
NetFlow Monitoring	Network performance management and network behavioral anomaly detection (NBAD) tools. Indicators of changes in traffic flows within a given time slice.
Network Forensics	Collects the richest network data. Provides a deeper level of threat identification and analysis and traffic reconstruction.

- Advanced threats require a new approach to network monitoring and cyber threat analysis
  - Improved network visibility requires the use of network forensics, full packet capture, session analysis and both interactive and automated techniques
- Security programs can benefit significantly through:
    - Continuous augmented awareness
    - Improved incident responses through shortened time to problem recognition and resolution
    - Reduced impact and cost related to cyber incidents
    - Improved visibility into compliance with policy and governance objectives
    - More effective threat intelligence and investigations



# What Others are Saying About NetWitness



NetWitness was Selected to Network World 's "Top 10 Security Companies to Watch" in 2008



"[NetWitness] brings simplicity and order to the complex and sometimes confusing network activity...Verdict: Superb tool for capturing and analyzing network behavior"



"NetWitness NextGen is not a CMF, SIM, IDS or some other stand alone security technology – it is the next generation of enterprise security infrastructure and network monitoring."

-Michael Montecillo, Principal Analyst



Winner, 2008 and 2009 Best Products and Services Award, Network Products Guide



Winner, Top 5 Emerging Growth Companies for 2009

Top 50 Washington DC Area CEOs 2009



Winner, SC Magazine Awards, 2009 Best Computer Forensics Solution  
Finalist, Best Enterprise Security Solution



Winner, Red Herring 100 North America 2009



- 
- U.S. Federal Government
    - Department of Defense, National Security, Law Enforcement, Intelligence and Numerous Civilian Agencies
  - U.S. State and Local Government
  - Fortune 1000
    - Top 10 U.S. Financial Services
    - Critical Infrastructure: Utilities, Transportation and Telecommunications, Technology, Healthcare
    - Manufacturing, and Retail
    - Large Public and Private Universities
  - International
    - Used across Europe, South America, Asia, and the Middle East

## QUESTIONS?



---

### Next Steps:

- Download the freeware version of NetWitness Investigator:
  - <http://download.netwitness.com>
  - Online training is available!
- Watch our videos:
  - <http://www.youtube.com/netwitness>
- Follow us on Twitter:
  - <http://twitter.com/netwitness>
- For a copy of this presentation or for additional information, please email me:
  - [Jeff.michael@netwitness.com](mailto:Jeff.michael@netwitness.com)