GFIRST

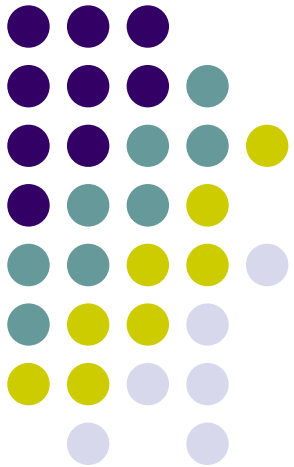
*Uniting the Cyber Response Community*

4th Annual GFIRST National Conference

June 1–6, 2008

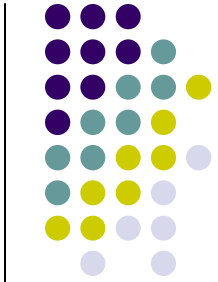
Caribe Royale Orlando | Orlando, Florida

# Incident Response Challenges in a Dynamic Threat Environment June 3, 2008



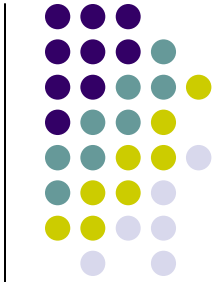
Jeanie M Larson, CISSP-ISSMP, CISM
Jeanie.Larson@hq.doe.gov

# Objectives



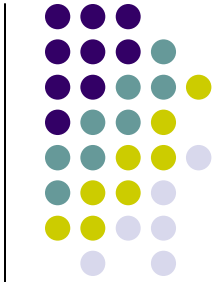
- Understanding some technical aspects of cyber attacks
- Understanding of the incident response challenges
- Capabilities organizations need to respond
- Incident Response Paradigm Shift
- Forensic analysis value in Incident Response
- Some effective mitigation strategies

# Setting the Stage



- Trends in cyber threat and economic espionage
- Threats increasing in complexity
- Traditional security infrastructure – no longer effective
- A well defined incident response capability is crucial to protecting information assets

# Economic and Industrial Espionage



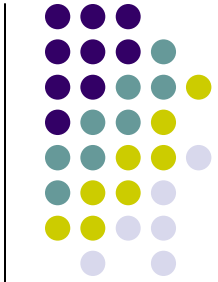
- According to the American Society for Industrial Security, economic and industrial espionage cost US businesses an estimated $59 billion in 2005.

- The Economic Espionage Act of 1996 permits legal action regarding “financial, business, scientific, engineering, technical and economic information,” if a company can demonstrate it has attempted to keep this information classified and protected.

- Most information reported as having been compromised was physically located in the U.S. when the compromise occurred, but foreign entities were the major beneficiaries.

- Information assets in all formats (paper, electronic, oral, prototypes, and models) are being targeted for possible compromise.

# More on Economic Espionage



February 8, 2008
**Trojan Dragon: China's Cyber Threat**
by **John J. Tkacik, Jr.**
*Backgrounder #2106*
America's counterintelligence czar, Dr. Joel F. Brenner, painted an alarming picture of economic espionage in 2006, albeit in the objective tones and neutral parlance of the intelligence community. He reported to Congress that "foreign collection efforts have hurt the United States in several ways": Foreign technology collection efforts have "eroded the US military advantage by enabling foreign militaries to acquire sophisticated capabilities that might otherwise have taken years to develop.""[M]assive" industrial espionage has "undercut the US economy by making it possible for foreign firms to gain a competitive economic edge over US companies."[1]

# Wake Up!

- Estonia (April 2007)

  The attacks, which started around April 27, have crippled Web sites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aarelaid, chief security officer for Estonia's Computer Emergency Response Team (CERT), on Thursday.

  Computerworld May 17, 2007


- Root Level Domain Name Servers (DNS) attacks (Feb 2007)
  - DDoS targeting primarily 2 of 13 servers – limited impact, but got attention because of potential
  - Oct 2002 – DDoS targeting all 13 root servers

# Increasing Attacks

**China is spying on UK business, warns MI5**
People's Liberation Army is conducting wholesale cyber espionage, says head of UK government security service
Tom Young, Computing, 30 Nov 2007


China denies claims of cyber warfare

**Estonia under cyber-attack**
Nato mobilises to deal with online threat
Iain Thomson, vnunet.com, 17 May 2007

**Cyber attacks from Chinese government offices**
A web site producing malicious material belongs to the government, claims software supplier
Tom Young, Computing, 03 Dec 2007

# Unprecedented…

From The Times

December 1, 2007

## MI5 alert on China's cyberspace spy threat

**Exclusive: director-general of MI5 sends letter to British companies warning systems are under attack from China**

Jonathan Evans sent a confidential letter to 300 chief executives and security chiefs at banks, accountants and legal firms

In an unprecedented alert, the Director-General of MI5 sent a confidential letter to 300 chief executives and security chiefs at banks, accountants and legal firms this week warning them that they were under attack from "Chinese state organisations". It is believed to be the first time that the Government has directly accused China of involvement in web-based espionage.

# Attacks Plague USG

Congressional testimony (April 19, 2007)

James Langevin, Chairman

Subcommittee on Emerging Threats, Cybersecurity, Science and Technology

"Let me be clear about the threat to our federal systems: I believe the infiltration by foreign nationals of federal government networks is one of the most critical issues confronting our nation. The acquisition of our government's information by outsiders undermines our strength as a nation. If sensitive information is stolen and absorbed by our enemies, we are strategically harmed".

- http://www.house.gov/list/speech/ri02_langevin/stmtcyber41907.html

# USG Response

- A series of recent events are having an impact on federal agencies…

FCW.COM STORY

**Einstein keeps an eye on agency networks**

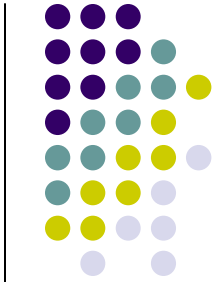
**Voluntary network gateway monitoring program gives DHS a big-picture view of federal cybersecurity**

By Jason Miller
Published on May 21, 2007

# Technical Aspects of Attacks

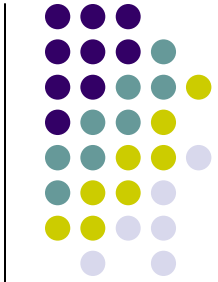
- Some of the Techniques, Tactics and Procedures (TTPs)

# Tactics, Techniques and Procedures (TTPs)



- Reconnaissance on target
  - Very sophisticated and very targeted
- Launch spearphishing (Email to targets)
  - Containing attachment with malicious code
  - URL Hyperlink directing to malicious site
- “Bait” frequently visited site for “drive by” infection

# TTPs - continued

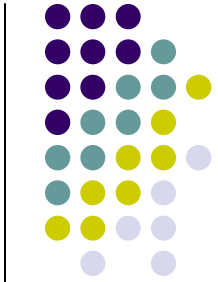


- User action (usually) required
  - User opens email
  - Clicks on attachment or link
  - Malicious code launches
- Malicious code
  - “Injects” into normal processes
  - Often involves downloader to download additional hacker tools
  - “Call Home” to attacker
  - Creates backdoor for command & control
  - Cleans up!

# TTPs - continued

- Trojan installed
  - Command and Control channel established
    - Controlled remotely by attacker
  - Trojan capabilities often include:
    - Data collection and export to remote attacker
    - Keystroke loggers
    - Sleep commands
    - Cleanup – making validation difficult
    - Registry settings
    - Privilege escalation

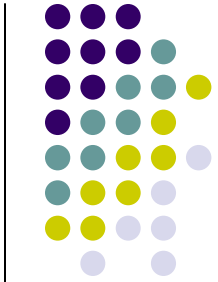
# Understanding Challenges



- No Silver Bullet

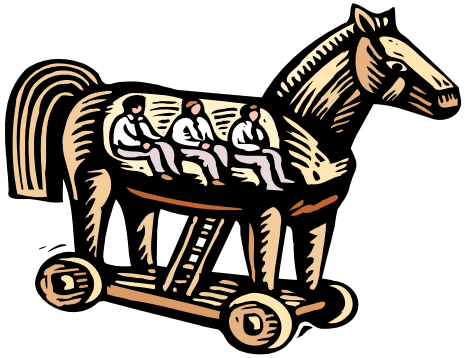
- Challenges in detecting, identifying, containing and recovering from sophisticated attacks

# Traditional Defenses Ineffective



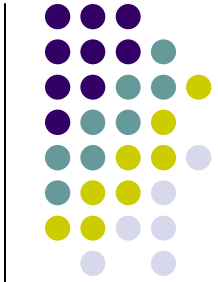
- Anti-virus, Firewall, Intrusion Detection/ Prevention
  - In many cases only 25% of malware variants detected by AV signatures
- Patching
  - Operating system
  - Application
- Current protection relies heavily on user computing habits
  - Email and web – the current primary vector for most attacks
- Perimeter protection model ineffective
- **Point:**
  - Even if you do everything “right”, you are susceptible to compromise.
  - There are no silver bullets!

# Identifying the Initial Vector



- How do you know?
  - Quiet, stealthy trojans
  - Often no indicators
- Most common attack vectors
  - Email
  - Web
- Diligence in monitoring for initial vector
  - Email

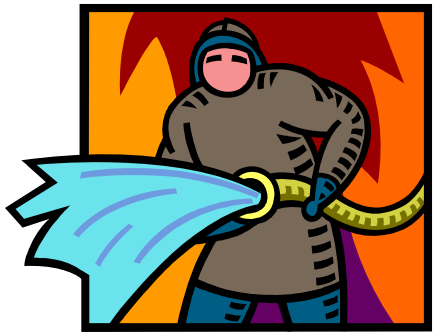
# Dynamic Network



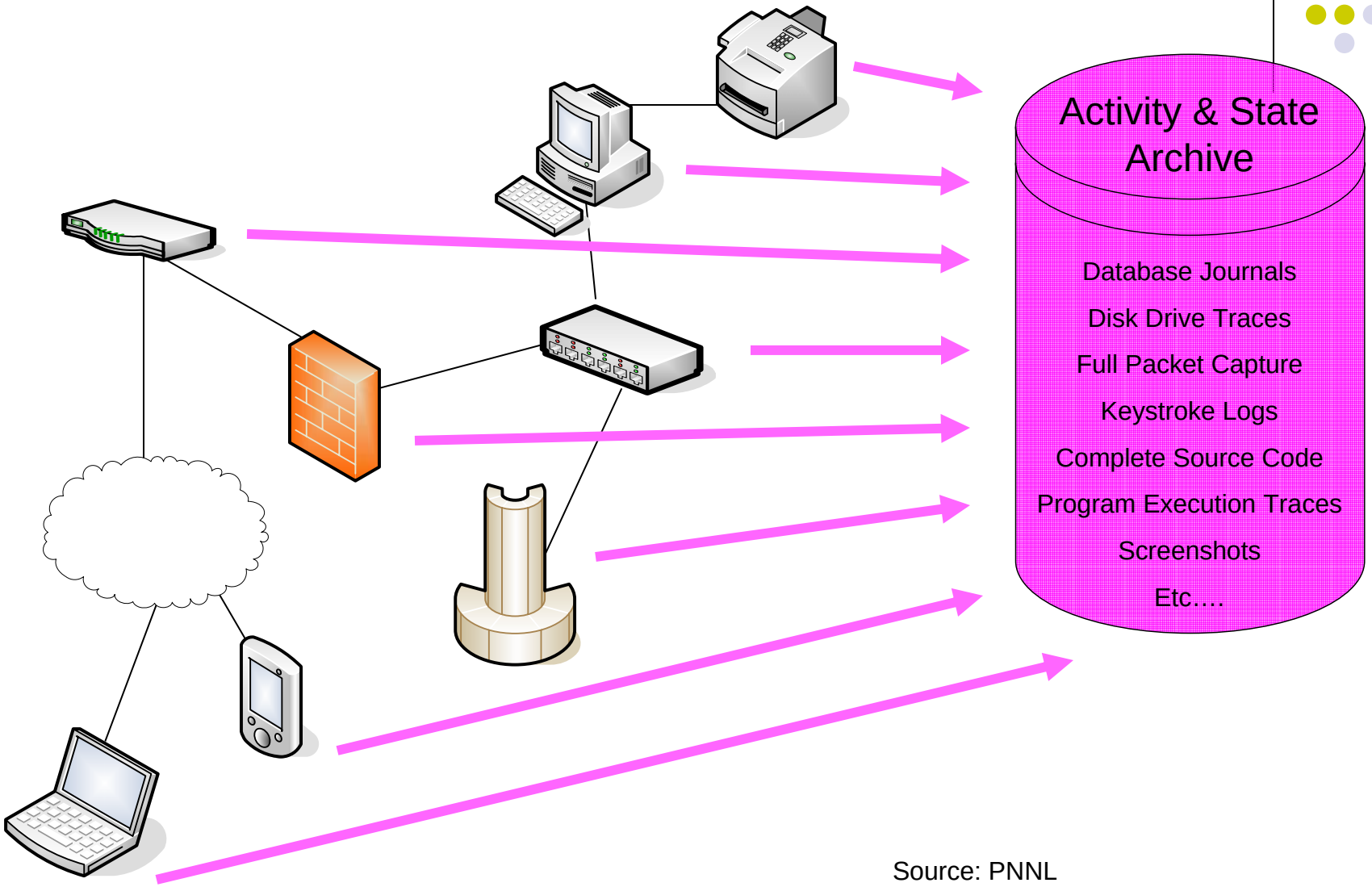
- Dynamic Nature
  - Use of dynamic DNS to convolute the source (timing)
  - Use of Domain names (and sub-domains)
  - Dynamic nature of web hosting makes investigations (especially after-the-fact reconstruction) difficult if not impossible
    - One IP address could host hundreds of domain names
    - Today that domain resolves to this IP, but at the time of the attack, it resolved to ???

# More Challenges…

- Information Sharing –
  - Who? / What? /How?
    - Share enough, but not too much
    - With whom?  Law Enforcement, Internal investigations
    - Classification issues
- Monitoring-In-Depth
  - Netflow – the 50,000 foot view
  - Locally managed NIDs
  - Log data crucial – DNS, web, PKI, host, Firewall, IDS/IPS
  - Full Packet? Absolutely REQUIRED if for damage assessment
- Incident Response
- Data Overload – how do you manage?
- Public Image – Perception is reality

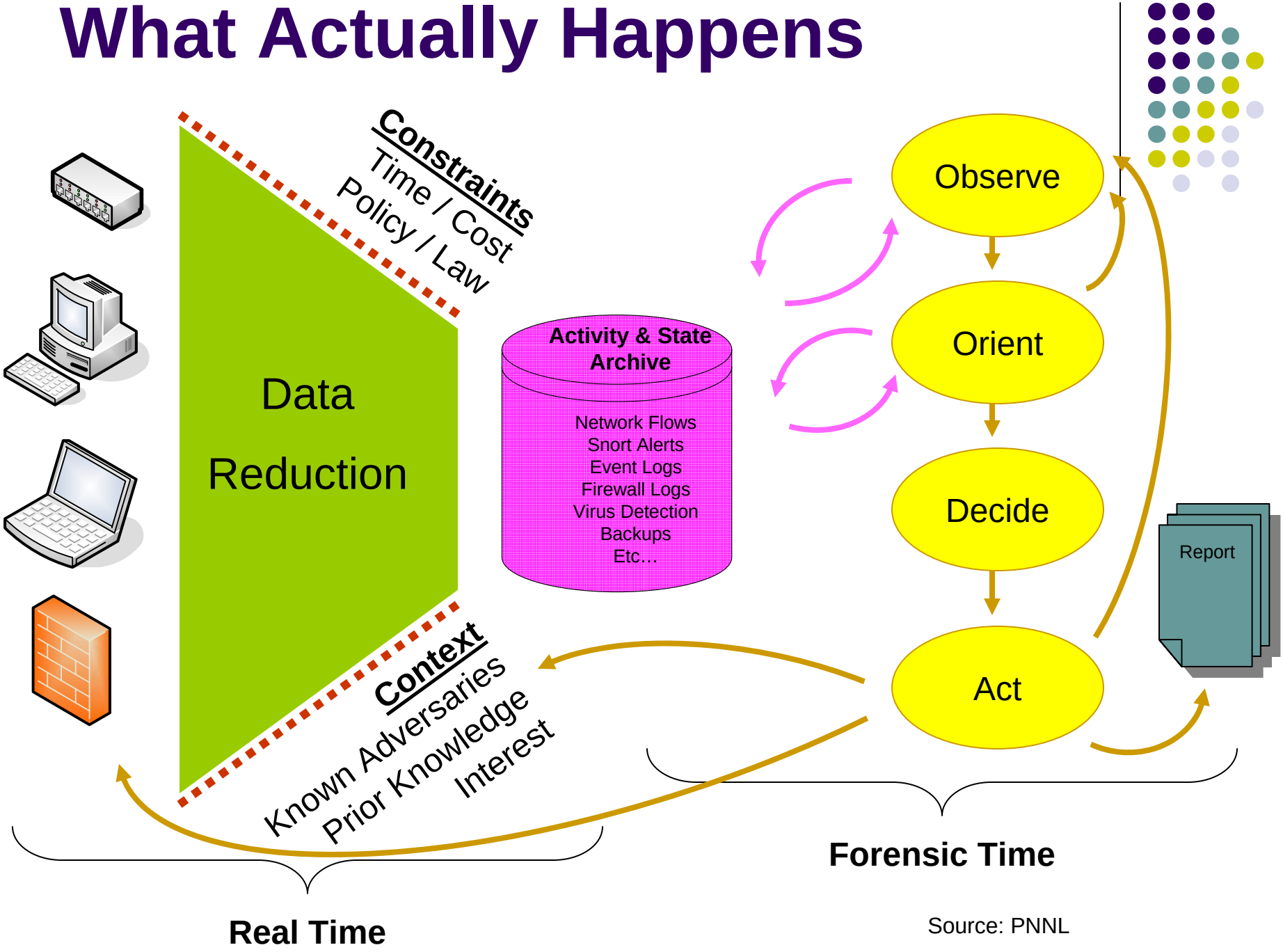


# Monitoring - The Platonic Ideal




Source: PNNL

# What Actually Happens



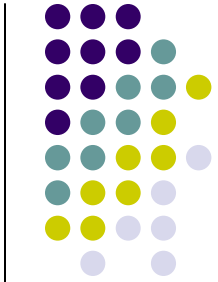

Source: PNNL

# Network Monitoring - Defense In-Depth

| Technology | Keeps | Discards | Misses |
|---|---|---|---|
| **Network Flow**<br>Cisco Netflow | Summary of packet headers including packet/byte counts | TCP/UDP Payload | Malicious network activity that goes to a legitimate service |
| **Signature-Based IDS**<br>Network Intrusion Detection | Alerts about network traffic that matches known malicious signature | Network traffic that does not match signature | Malicious network activity that's doesn't have a known signature |
| **Infrastructure Logs**<br>DNS, LDAP, PKI, Citrix, remote access, authentication servers, Firewall, Web, Active Directory | Name to number lookups and other transaction-oriented history | All traffic that isn't related to directory services | Malicious network activity that uses legitimate addresses or credentials |
| **Host Logs**<br>Event Logs (Windows), Syslog | Anomalous host service events | Network traffic that initiates an event; application behavior | Network or application attacks |
| **Application Logs**<br>Web, browser, database | Application activity (web pages served) | Non-application activity | Network or underlying operating system problems |

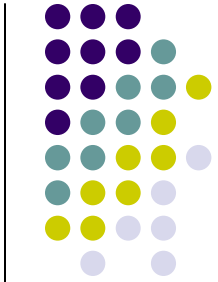
Source: PNNL

## Data Challenges



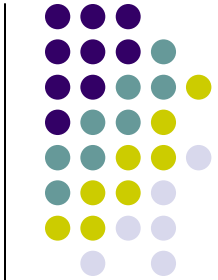
- Correlation
  - What Flows correlate with anomalous SYSLOG records?
  - Which application failures correlate with Snort Alerts?
- Retrospective Analysis:
  *Learn the IP used by an Adversary yesterday:*
  - Too late to deploy Snort rules to find yesterdays' traffic
  - Not too late to look at Flow records to find my potentially targeted systems, and then examine their logs in detail
- Data mining
  - Searching a DB for malicious activity
  - Storing, searching and reconstructing PCAP can be a problem

# Monitoring – The Bottom Line



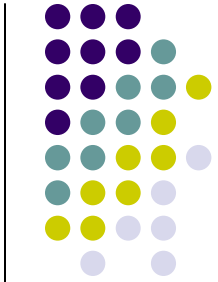
- No practical single solution can preserve enough information to handle any Adversary's activity.
- Every monitoring technology discards some data
- Context is crucial to select and preserve data of interest
- Mitigate the inevitable loss of useful data through correlation and inter-technology directed analysis, and by continuously updating the monitoring technology with newly acquired context.
- Diverse monitoring technologies assist the human cyber defender by providing complementary views into IT infrastructure activity.
  - But can be labor intenstive

# Information – Dichotomy



- Not Enough Information:
- Access to timely and actionable information
  - Analysis efforts and products
  - Indicator lists being published without context not useful to defenders (I got a “hit”, now what?)
  - De-confliction non-existent (or not accessible)
  - “Leaks” of information tip off attacker and sources “dry up”
    - Well intentioned, CSIRTs still poke, probe and prod the attacker resources!!
  - Over classification can impede information sharing needed for CND purposes
- Too Much Information:
  - Thousands of indicators – point of degradation in Intrusion Detection systems
    - Impossible to monitor everything forever
    - How to “age” or retire old signatures

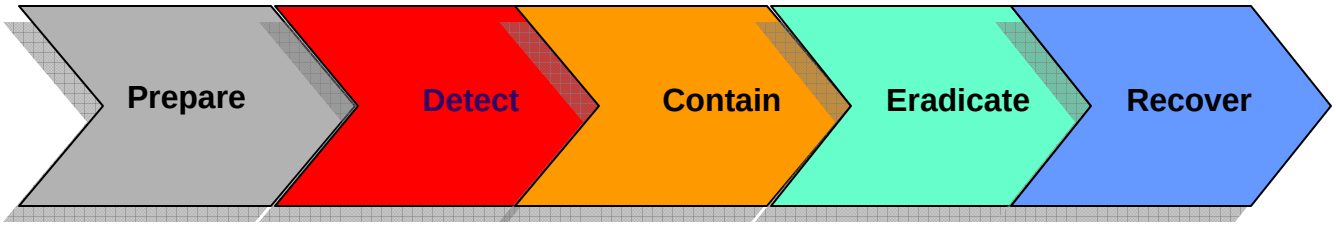
# Incident Management Paradigm Shift



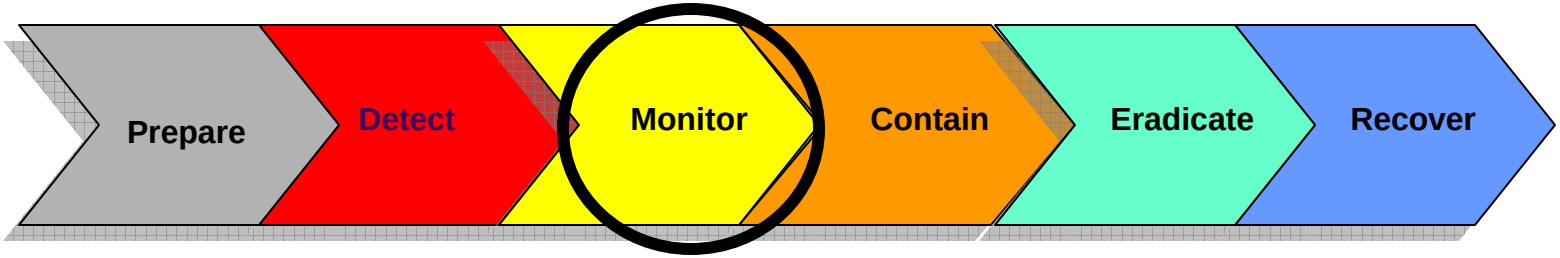
- Linear approach to Incident response no longer effective
  - Restoring to operation is not always the ultimate goal
    - Damage assessment
    - Information used from analysis could aid in identifying other malicious activity

# IM Paradigm Shift

Traditional Incident Management Paradigm

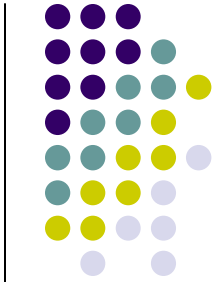



New Incident Management Paradigm




Sources:
NIST SP800-61 Computer Security Incident Handling Guide
CNSS National Information Assurance (IA) Approach to Incident Management

# Monitor or Shut down?



- Decision to monitor
  - Risk based
    - Involves key decision makers
  - Deploy full packet capture
  - Have a plan
    - What to do (who decides?)
    - Who to notify

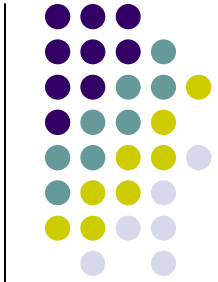
# Incident Capabilities

- To respond to sophisticated attacks, organizations need advanced capabilities

# Skills

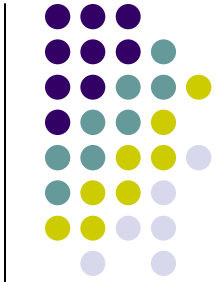
- Skilled incident responders (Tier 1-n)
- Skilled forensics staff
  - Network (pcap analysis)
  - Host (image)
  - Malware
    - Sandboxing
    - Reverse Engineering
- Programmers (strong math background)
  - Decrypting / Decoding
  - Scripting tools

# Capabilities



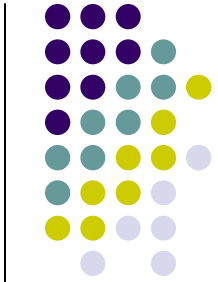
- Incident Response
  - Centralized / SOC
  - Centralized incident reporting
  - Centralized analysis
    - Value derived communicated across enterprise

# IR and Forensic Functions



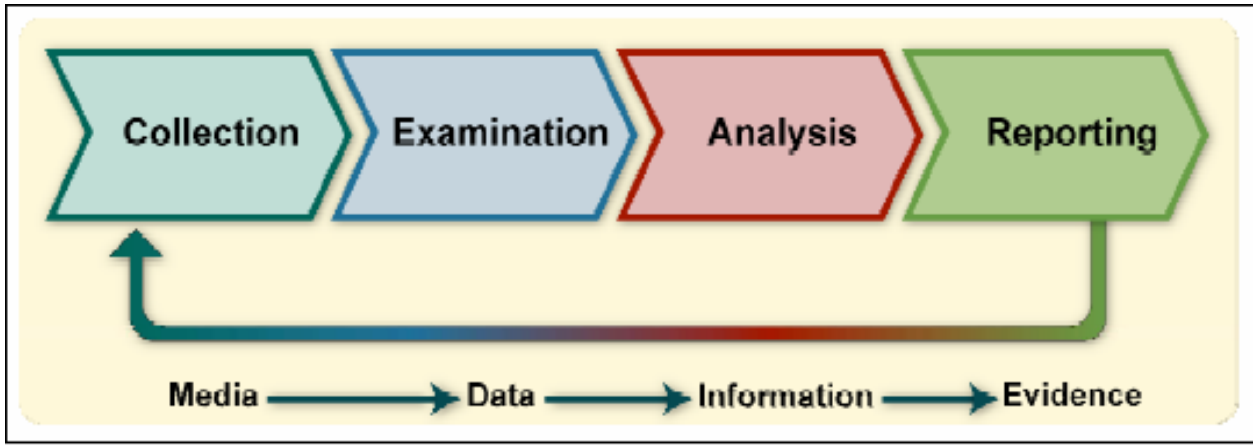
- Collection and preservation of evidence
- Initial vector analysis
  - Useful in identifying other attempts or compromises
- Forensic collection
  - Underlying infrastructure & policies crucial
- Correlation of events
  - Relies on historical data records and tools to correlate

# IR and Forensics Process

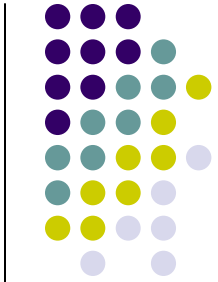


- Forensic reconstruction
  - Ability to reconstruct attack
    - Damage assessment
    - Threat and forensic analysis
      - Use results to improve security posture
  - DOCUMENT!
    - If you don’t document, all lessons learned are lost forever!

# Forensic Process

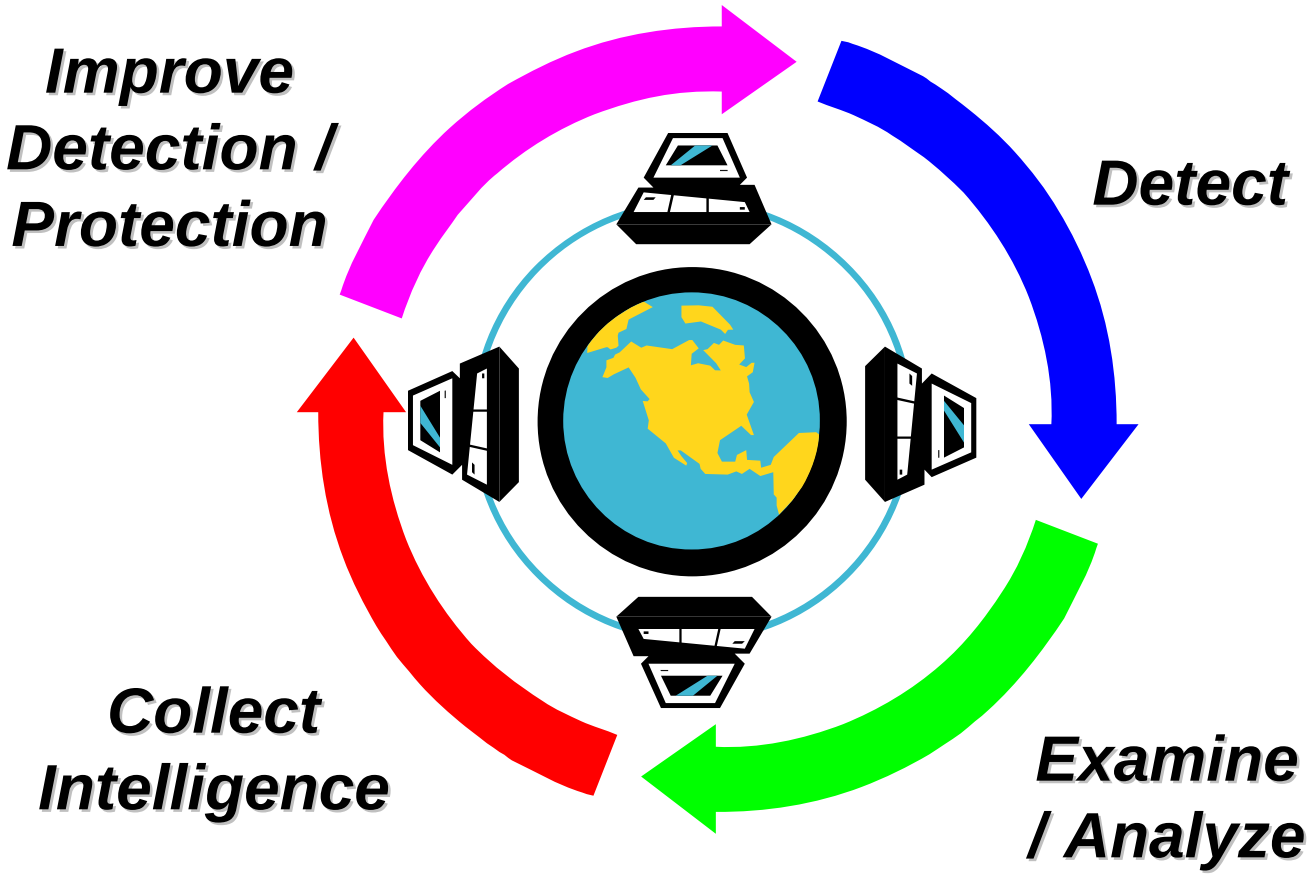


# Forensic Components



- Data Collection
  - Identify data sources
  - Acquire data
  - Legal considerations (Privacy Impact Assessment)
- Incident Response
  - Evidence Collection
  - Containment strategies
- Examination
  - Data reduction
  - Immediate value (indicators)
  - Correlation

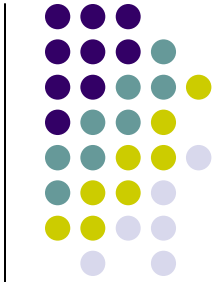
# Forensic Lifecycle



# Data Collection Requirements

- What do you need to perform forensic reconstruction of event?
- Host logs
- Server audit logs
  - Email gateway
  - DNS
  - HTTP (Web)
- Network Logs
  - Netflow (incident scoping)
  - Full packet capture of session
  - DNS, Firewall, Intrusion Detection, Web
- Decrypting/decoding tools

# Signatures



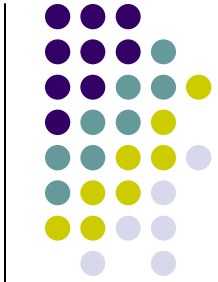
- Only good for known attacks
- Last count over 6,000 SNORT signatures
- Most sensors have degradation issues
- Where do you get your signatures?
- How do you evaluate their effectiveness?

# Damage Assessment - What happened?

- Damage Assessment (Has anyone done this?)
  - How did they get in?
    - Initial vector?
  - What did they take?
    - Full packet capture?
  - Impossible!
    - Unless you can reconstruct everything that occurred on your network, you can only guess
    - Requires:
      - Full packet capture (at least 6 months on hand)
      - Ability to develop decryption/decoding tools
      - Highly skilled analysts familiar with specific threats

# Other Issues

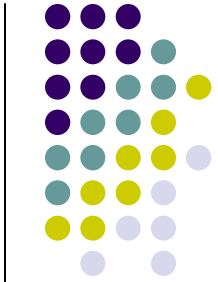
# Organizational & Governance Issues



- Incident likely to cross organizational boundaries

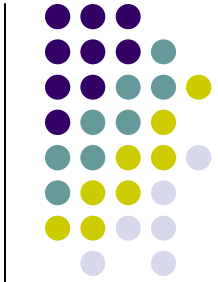
- Centralized forensics analysis benefits:
  - Centralized collection and examination of forensic evidence ensures “enterprise” view (scope)
  - Centralized forensics analysis enhances skills and eliminates stove pipe efforts

# Case Management



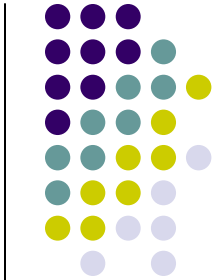
- Incident tracking
  - Tying pieces together – event correlation
- Data management
  - How/where to store:
    - Key Incident Indicators (IP addresses, domain names, file names/hashes)
    - Malware repository?
    - PCAP
    - Flow data
  - Data must be “usable” by analysts
    - Correlation with other events
    - Historical reconstruction

# Some Mitigation Strategies



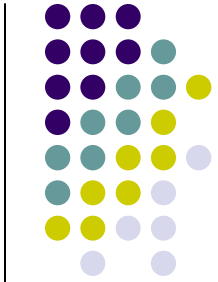
- Identify key corporate assets and perform risk assessments
- Classify assets, define data protection requirements and protect appropriately
- Educate users about phishing and reporting
  - End users are first line of defense!
- Establish Incident Response Capability with forensics analysis

# Technical Mitigation



- Implement Two-Factor authentication where ever possible
  - Remote access, system administrators
- Implement encryption - data at rest and data in transit
- Web application security testing crucial!
- Establish and implement requirements for forensics in your security infrastructure
- Architecture
  - Email – Sender Policy Framework
  - Full packet capture (damage assessment)
  - DNS
  - Web proxy
- Keep applications and operating systems patched!

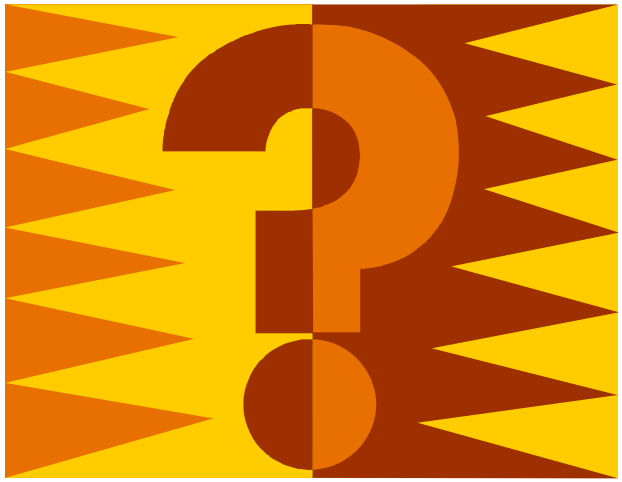
# Thoughts in Closing



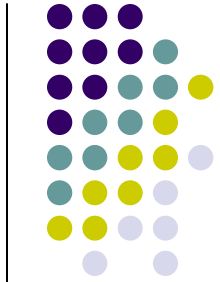
James Langevin:

"We don't know the scope of our networks. We don't know who's inside our networks. We don't know what information has been stolen. We need to get serious about this threat to our national security".

# Questions?



# Useful Resources



Antiphishing Working Group
http://www.antiphishing.org/index.html

Microsoft Phishing Filter http://www.microsoft.com/athome/security/online/phishing_filter.mspx

Guide to Integrating Forensic Techniques into Incident Response SP-800-86
http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Securing email client
http://www.malwarehelp.org/securing-your-e-mail-client-outlookexpress2.html

Email Sender Policy Framework
http://www.openspf.org/

Committee on National Security Systems
National Information Assurance (IA) Approach to Incident Management (IM)
http://www.cnss.gov/full-index.html

ICANN Report on root server attack:
http://www.securityfocus.com/brief/456

Information Asset Protection Guide
http://www.asisonline.org/guidelines/guidelinesinfoassetsfinal.pdf