
nuix
Simple. Powerful. Precise.

The Good Shepherd Model for Cybersecurity

Minimizing the potential for, and damage suffered from, data breaches

Stuart Clarke
Director Cybersecurity & Investigation Services, Nuix

SESSION OUTLINE

- Perimeter Security Assessment
- Information Governance – importance of understanding the working environment
- Managing cyber risk with Information governance
- The ‘Good Shepherd’ Model – The how?
- Summary – Changing the mindset

- *'against a sufficiently skilled, funded, and motivated adversary, no network is secure.'* **Schneier, B.**
  - Malware marketplace
  - Spear phishing effective
  - Spoofed sites
  - Sponsorship

- However strong your perimeter – its easier to go around it
  - The attacker becomes the insider
    - Your perimeter has failed!

CYBER CRIME TIMELINE

1980s

- First viruses & Morris worm
- Cult of the Dead Cow forms
- First National Bank of Chicago victim of cyber theft

1990s

- Citibank loses $10 million
- 15 year old hacks US DOJ
- First MiTM attack
- Kevin Mitnick captured

2002-2005

- ILOVEYOU virus
- First teenage hacker sentenced
- DoS hits Yahoo, Amazon & CNN
- First large botnet - SoBig

2009

- TJ Maxx hacked (2007)
- Conflicker worm infects millions
- Government sites in Israel attacked

2010-2011

- Stuxnet worm
- Advanced mobile malware forms
- First Wikileaks posts
- Bank of America & SonyPS hacked

2012

- $45 millon stolen from ATMs
- LulzSec attack on mass
- Edward Snowden

2013

- Millions of stolen card numbers posted online
- Red October virus discovered

2014 Q1

- Bitcoins stolen
- 350 million account details released
- KT Corp breached
- 8 year attack concludes – 160 million accounts

2014 Q2-3

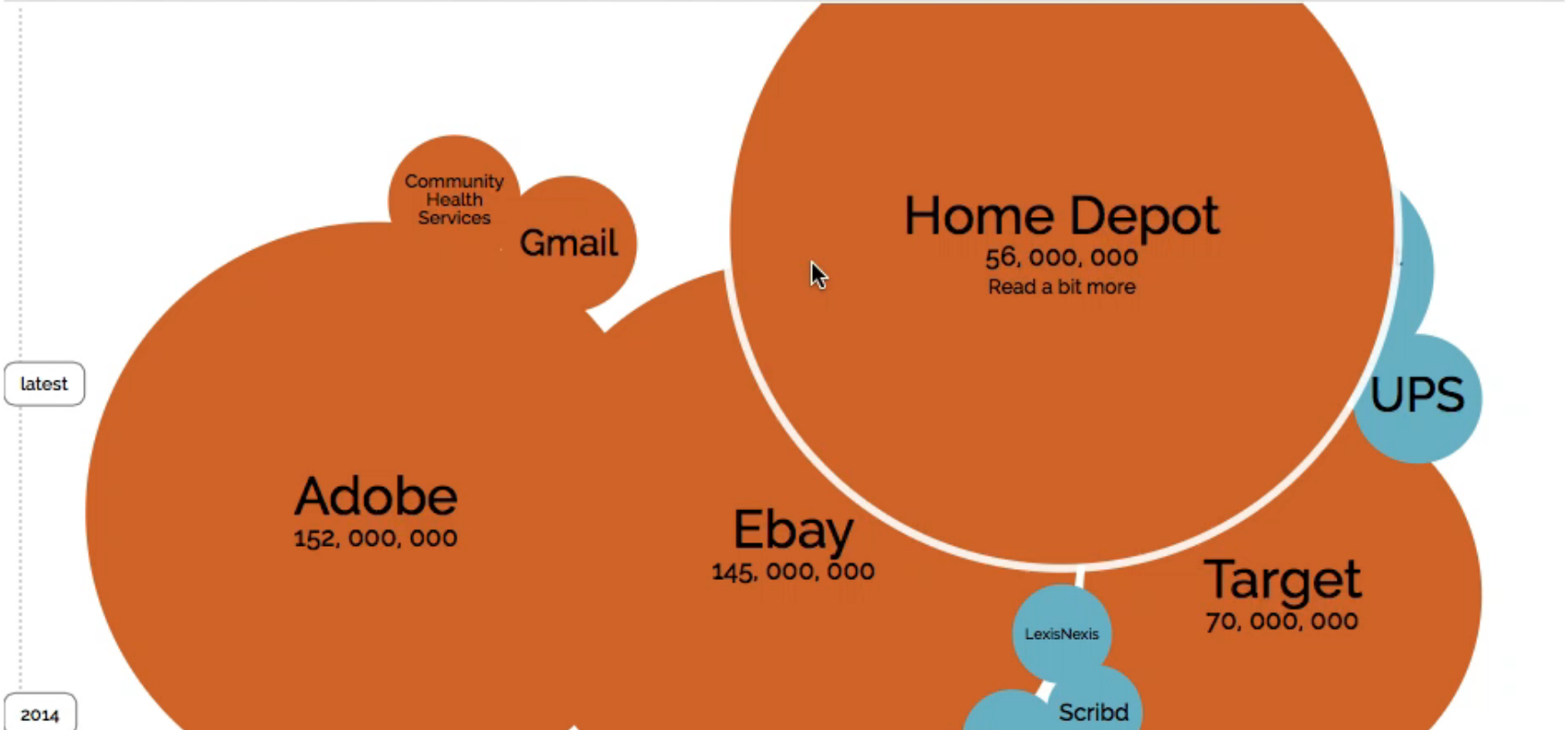
- Heartbleed bug found
- German ISP loses millions of account details
- Home Depot, Target & JP Morgan – hacked
- POS malware rises - Backoff

World's Biggest Data Breaches

Selected losses greater than 30,000 records

interesting story

YEAR | *BUBBLE COLOUR* YEAR | METHOD OF LEAK | *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



- Identify and understand
  - What type of data is it? How much of it is there?
- How old and who uses it?
  - Is it past the retention period? What is it used for?
- Where is it stored and who owns it?
- What is it worth to the company?
- What is it worth to some else?
- Security of data:
  - Confidentiality. Integrity. Availability.

"Gartner predicts that 40% of companies will combine their information governance and information security policies by 2017, there are a variety of lingering questions about how and why this might occur."

- Expose the gaps & minimizing cyber risk
  - Identify systems which contain high value data and minimum security environments
    - Improve effectiveness of cyber investigations
  - Identify gaps in policy & procedures that introduce risk
    - Cybersecurity & IG bring process, procedure and people together
- Ensure Business continuity
  - Time is money

- Create & update data retention and deletion policies.
- Identify R.O.T data
  - Shingling and near-duplicate analysis
  - Date and Time range searches
- Identify valuable data
  - Regular expression and named entities
  - Powerful index searching

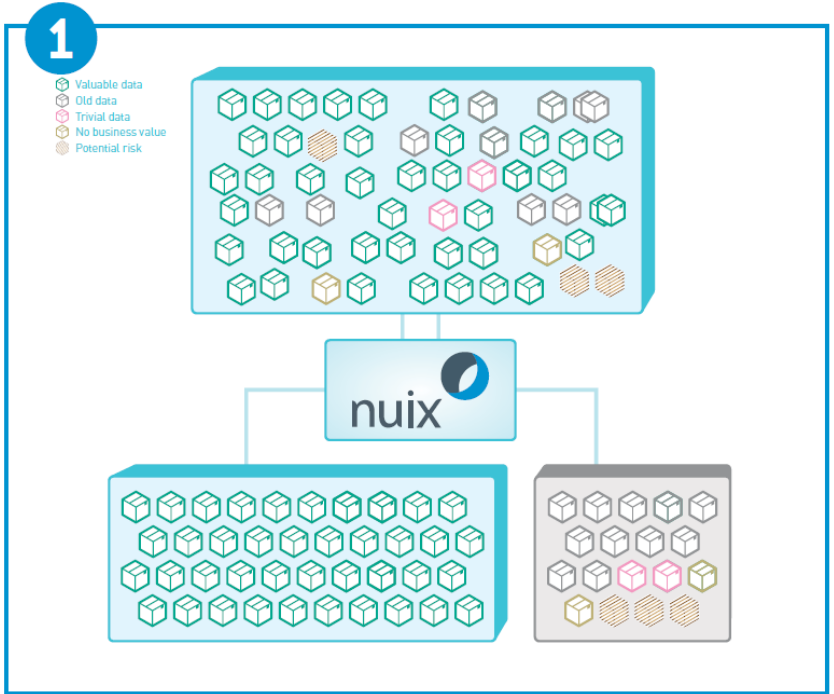


Fig 1: Deleting low-value data minimizes risk and reduces the scope of post-breach investigations.

- Identify what is valuable or sensitive
- Identify data in the wild
  - MD5 hashes
  - File types & file path
  - RegEx, Boolean, wild card, phase searching
- Tag responsive data
- Apply workflow to, move, contain it, and reduce risk

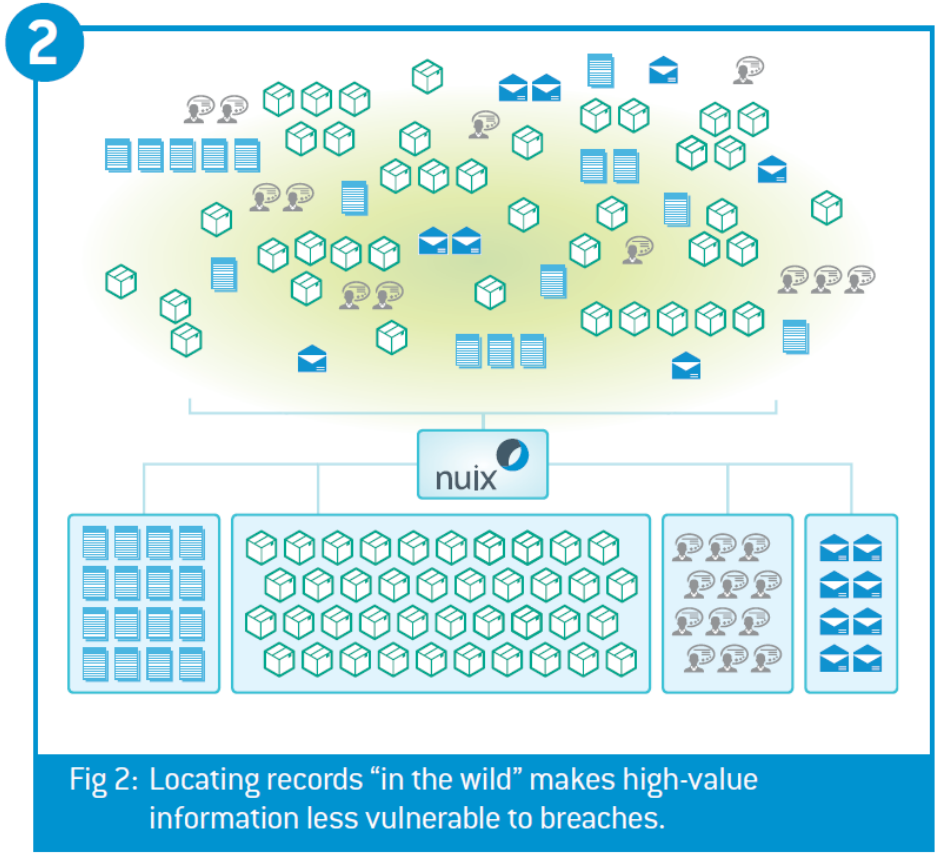


Fig 2: Locating records "in the wild" makes high-value information less vulnerable to breaches.

- Create hash-lists, word-list of sensitive files.
- Identify unprotected systems
- Identify known-sensitive files using hash and word lists
- Use shingling, topic modelling and named entities to identify unknown sensitive information

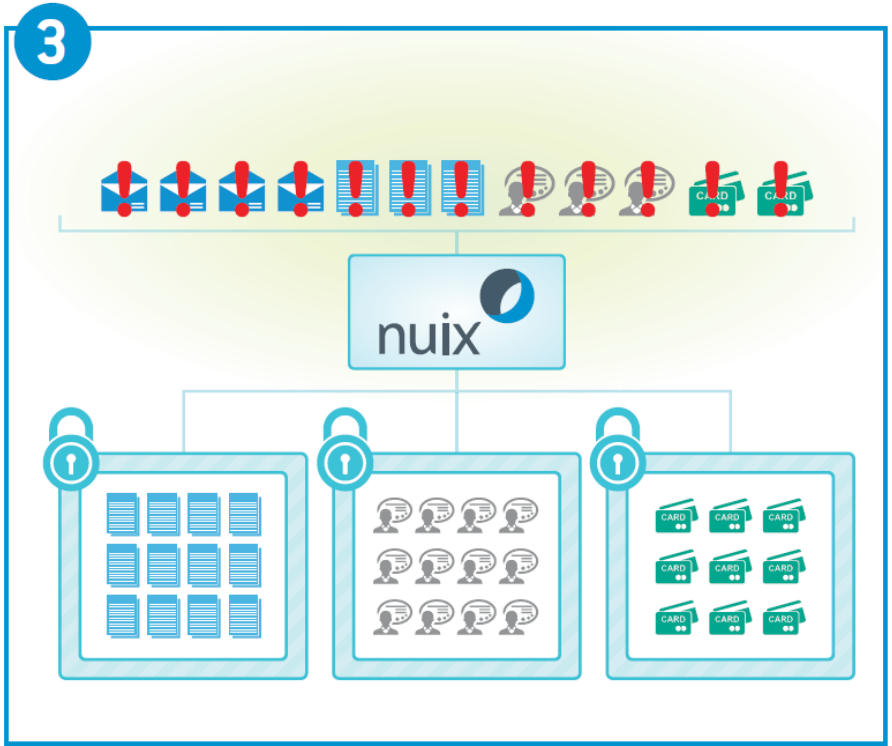


Fig 3: Keeping private, financial and health data within known, protected locations reduces business risks.

- Review current access control policies and ensure this is line with data retention and security policies

- Conduct regular access control assessment
  - Conduct access test to ensure theory matches reality
  - Ensure access rights are proportionate and accurate to job roles
  - Ensure access rights are in line with security policies

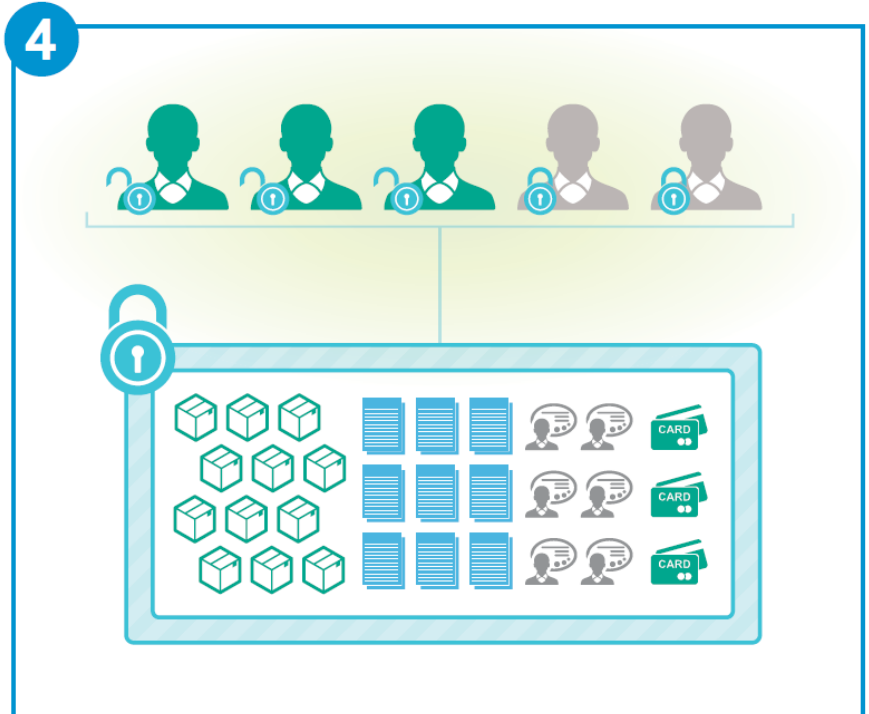
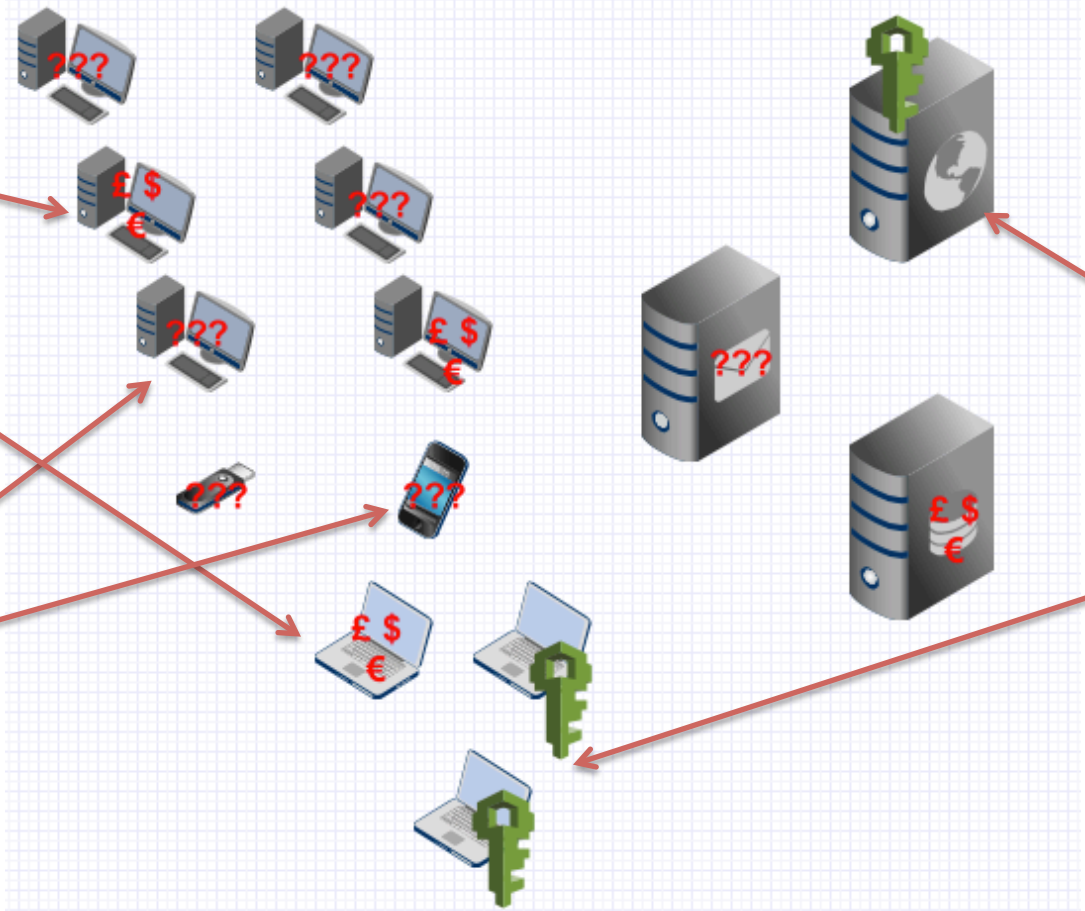


Fig 4: Regularly auditing access controls ensures security policy matches reality.

- **Effective decision making during a cyber incident**
  - Confidence in the working environment
- **Reduced response times in a breach**
  - Targeting and securing high value data first
- **Reduce the risk of the “inside attack” or accidental release of data**
  - Finding security gaps with access controls
  - Identifying, controlling and securing sensitive information
- **Save time and costs** by removing R.O.T data and reducing risk.

Known to contain sensitive data – **non-encrypted**!

Content unknown – **high risk**!

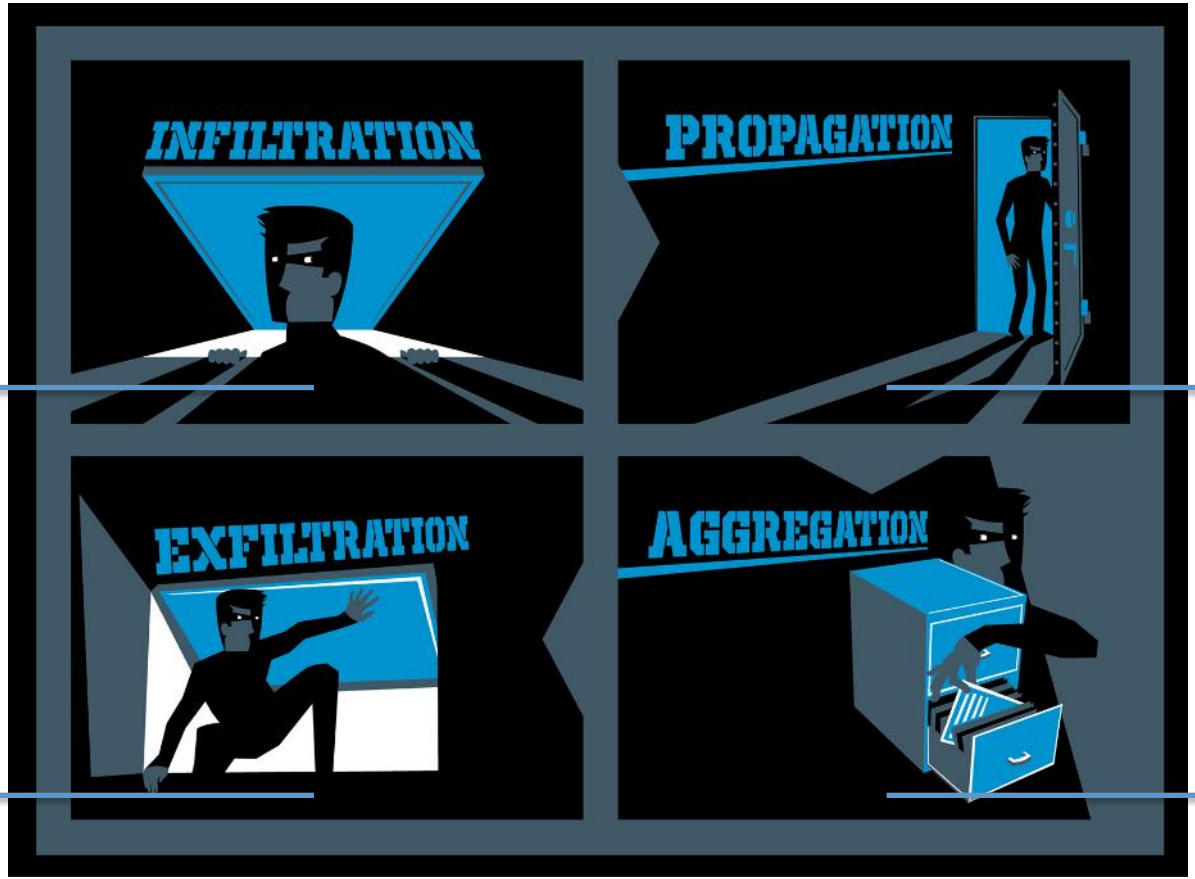


Known sensitive data – **encrypted**!

CYBERSECURITY BREACH QUADRILATERAL

Infiltration

Bad guy in…



Propagation

Bad guy move…

Exfiltration

Bad guy get away with stuff…

Aggregation

Bad guy take stuff…

nuix

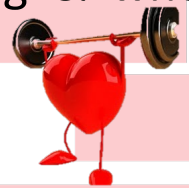
4 Pillars Of Data Breach Investigation

FOUNDATION

SOLID

Live Data

Understand the current health of the system, what is running & who is accessing it



Log Files

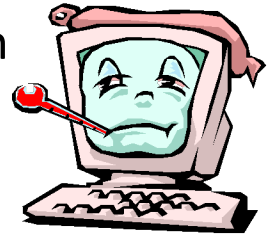
Review and search all/ any logs for records of malicious activity on the system

Databases

Understand your valuables! What, where, how much, level of protection!

Malware

Identify and understand the impact of malicious files/code on the system



- Extraordinarily capable software
- Infused with real world intelligence
- Dramatically impacts capability
- Collective expertise of SME's
- Know the crime, know the evidence
- Time to respond is greatly diminished
  - Reduction of impact on the business
  - Business resumption

NUIX GRADUATED RESPONSE

nuix

1. *IR Event Monitoring*
2. *Indicator of Compromise detected*

ESCALATION *(AUTOMATIC)*

3. *Yellow Alert Workflow Initiation*
4. *Additional data retrieved via Nuix API*
5. *Data submitted directly from Nuix to external tool via API for correlation*
6. *Additional Indicators of Compromise analysed*

7. *Orange Alert Workflow Initiation*
8. *Persistent Nuix Index of suspect endpoint captured*
9. *Authorised users are notified*
10. *Nuix Web Review of information from suspect endpoint available*

ESCALATION *(AUTOMATIC)*

ESCALATION *(MANUAL)*

11. *Full, bit level, forensic image of the suspect endpoint created*
12. *Analyst review of suspect endpoint initiated*
13. *Notable events and security indicators fed back into originating system*
14. *Suspect endpoint reimaged to last known good state*

Cases Admin Download Support Log Out: administrator

Enter a Nuix Query

Select a Dat

Export CSV

Visualize Results

Select or Create a Folder

Add Selected Add All

« ‹ 1 of 44132 › » Showing 1 - 50 of 2206591 Results. Viewed 8 of 2206

Kind	Name	File Type
	webserver.nuix-philly.com	Nuix Evidence File
	ftpserver.nuix-philly.com	Nuix Evidence File
	WEBSRV	Directory
	d-liver.nuix-philly.com	Nuix Evidence File
	DLiver	Directory
	ftp.suesuspect.me.uk.zip	Zip-Compressed File
	Hacme-DLiver-SJC1.E01.txt	Plain Text
	ftp.suesuspect.me.uk	Directory
	Hacme-DLiver-SJC1.E02	EnCase EWC Disk Image
	.listing	Plain Text
	Hacme-DLiver-SJC1.E03	EnCase EWC Disk Image
	actualspy.exe	Windows Executable
	Hacme-DLiver-SJC1.E04	EnCase EWC Disk Image
	Current Pricing.xlsx	Microsoft 2007 Excel Spreads
	Hacme-DLiver-SJC1.E05	EnCase EWC Disk Image

« ‹ 1 of 44132 › » Showing 1 - 50 of 2206591 Results. Viewed 8 of 2206

Engine Version: 5.3.36914 Web Review Version: 6.0.0.0-SNAPSH

Link Analysis: Breach_Demo

10.211.55.4:8380/nuix-wr/#analytics/popup/60c6d25b-0c76-ad5d-7eb6-ad4ce1205d71/Link Analysi...

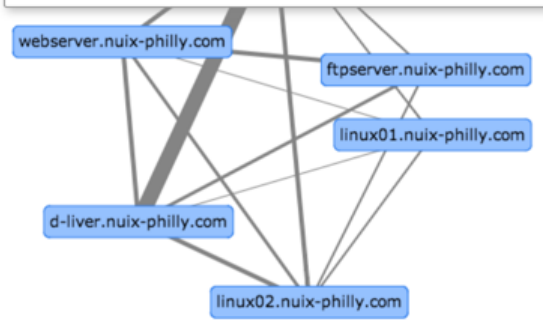
Visualization Options

+A -A AAA

d-liver.nuix-philly.com - live

3166 Common Attributes between **d-liver.nuix-philly.com** and **win-xp.nuix-philly.com**

entities:personal-id-num: 190 attributes in common
entities:credit-card-num: 21 attributes in common
entities:url: 2955 attributes in common



SESSION SUMMARY

- Big Data = New Investigation Approach
- Prevention Not Achievable
- Data at Rest Must Meet Data in Motion
- Automation & Intelligence Are Key
- Improving Your Workflow Will
  - Reduce the gap between intrusion & detection
  - Reduce the gap between detection & containment
  - Reduce the gap between containment & removal

Pick up a copy of our white paper, “A Good Shepherd Model for Cybersecurity”.

nuix

FIND OUT MORE:


twitter.com/nuix


facebook.com/nuixsoftware


linkedin.com/company/nuix


youtube.com/nuixsoftware


blog.nuix.com