data is nothing without context

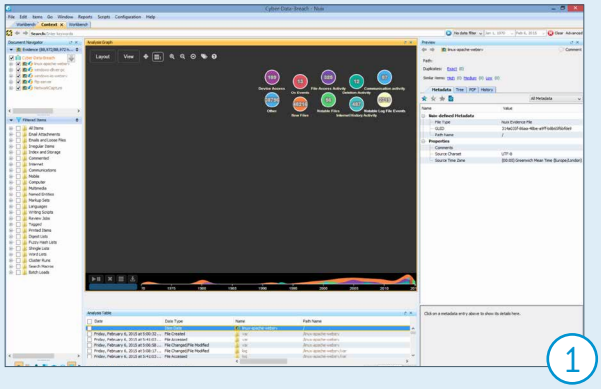
nuix INCIDENT RESPONSE

Nuix Incident Response reduces the gap between detection and remediation of data breaches. You can quickly discover the cause and scope of a breach, find out what happened next and plot an efficient route to resolution.

More than 90% of data breaches successfully compromise their targets within a few days[i] but such attacks typically take weeks to detect and a month or longer to resolve – and the longer they take, the more they cost.[ii]

A BREAKTHROUGH FOR INCIDENT RESPONDERS

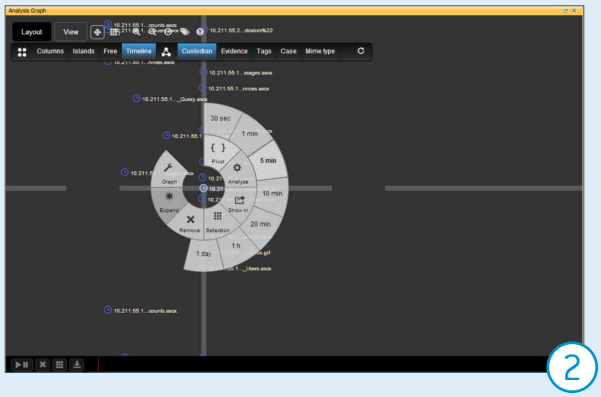
Nuix Incident Response guides incident responders toward the key evidence of internal or external breaches. You can capture data from hundreds of formats and use advanced investigative techniques to analyse, visualise and report on the evidence you uncover. Built-in intelligence from our cybersecurity experts accelerates your path to remediation and helps minimise the cost and damage your organisation incurs.



1. Applied intelligence

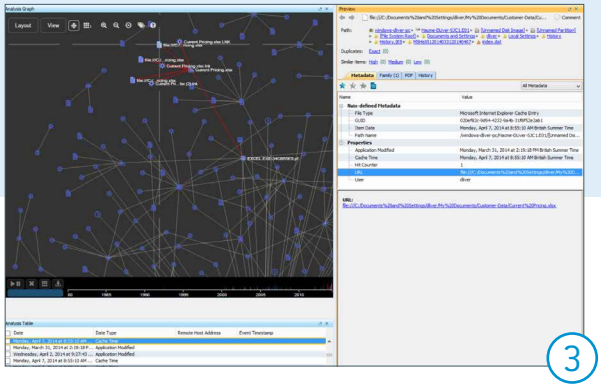
Nuix's powerful Context user interface is a fast and intuitive way to filter large numbers of items and allow the most interesting and relevant ones to float to the top. Its built-in intelligence automatically groups, shows relationships between and links highly relevant sets of items including:

- USB device access
- Internet history
- Deletion activity
- Notable files and log events.
- Operating system events
- File access activity
- Communication activity



2. Find a thread and pull it

Having identified an item of interest, incident responders can build a chronology of activity. The time serialisation table displays all date and time attributes associated with any file, allowing you to view relevant events in the order they happened, even across multiple evidence sources.



3. Examine links and relationships

Nuix Incident Response offers flexible ways to find links between items that share similar text, file system attributes, IP and email addresses and other connections across multiple evidence repositories, custodians and Nuix cases.

i Verizon 2015 Data Breach Investigations Report
ii Ponemon Institute 2013 Cost of Cyber Crime Study

nuix
Simple. Powerful. Precise.

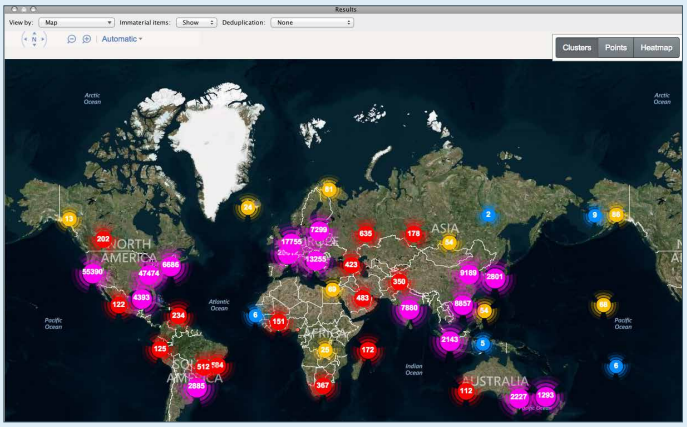
A FAST, HOLISTIC VIEW OF THE INCIDENT

Nuix analyses the complex data sources everyone else ignores because they are 'too hard'. These include:

- Live data including running processes, application handles and threads, services, drivers, network sessions, IP and MAC addresses, open ports, network routing tables, time zone and screen captures of running applications
- Network traffic PCAP files
- Log files and Logstash outputs
- Microsoft SQL Server and SQLite databases
- File system artefacts including deleted files, Windows jump lists and the Windows Prefetch folder
- Smart decoding and processing of Windows Registry artefacts including UserAssist, shim cache and ShellBags
- Enterprise repositories including file shares, Microsoft Exchange, Lotus Notes, Microsoft SharePoint, email archives and compliance storage systems
- Hard drives, virtual disks and forensic images
- Mobile device forensic containers
- Cloud services including Amazon S3 and Dropbox.

Log file, Logstash and geospatial analysis

Nuix natively analyses common log file formats including IIS and Apache web server, FTP and Windows Event logs. It can also handle hundreds more log file formats by ingesting Logstash outputs. You can use Logstash filters to enrich the content of log files, such as GeoIP filter to geo-locate IP addresses and generate item counts or heat maps.



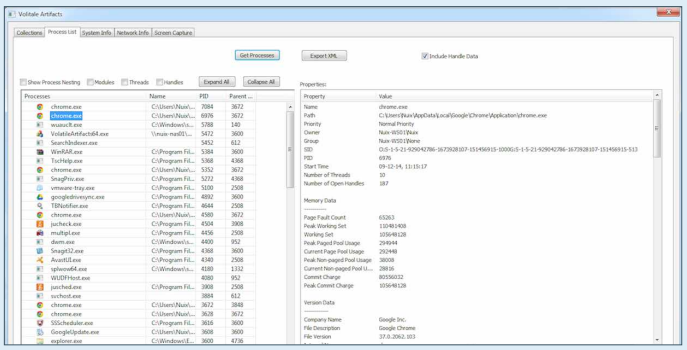
Generate item counts and heat maps from log file data.

Fuzzy hashing

You can use SSDeep 'fuzzy' hashes to identify near-duplicate executable files such as malware that modifies itself as it replicates over a network. Nuix Incident Response can also import SSDeep hash lists to leverage third-party intelligence feeds, and export hashes of newly identified malware.

Ruby, Python and ECMAScript scripting

Nuix can run scripts to control the conditions and parameters for Nuix Workers during processing and to conduct deeper analysis within the Context interface. For example, it can extract text from executables and compare them to YARA rules that could identify them as malicious, with immediate results.



Nuix's Collection technologies capture live data from systems across an entire network.

TO FIND OUT MORE VISIT

nuix.com/incident-response

ABOUT NUIX

Nuix enables people to make fact-based decisions from unstructured, semi-structured and structured data. The patented Nuix Engine makes small work of large and complex human-generated data sets. Organisations around the world turn to Nuix software when they need fast, accurate answers for digital investigation, cybersecurity, eDiscovery, information governance, email migration, privacy and more.

North America
USA: +1 877 470 6849
» Email: sales@nuix.com

EMEA
UK: +44 203 786 3160
» Web: nuix.com

APAC
Australia: +61 2 9280 0699
» Twitter: @nuix

nuix

CY1505US1