KLDiscovery

Cyber Incident Response

Addressing the Challenges of Cyber Incident Response Data Mining

Reports of data loss or exfiltration during cybersecurity attacks are increasing. Network infiltrations often go unnoticed while corporate or personally identifiable information/personal health information (PII/PHI) is compromised. This may include proprietary company information and private data such as names, addresses, ID numbers, bank details, or credit card information.

Data privacy and protection regimes such as GDPR, CCPA, and BIPA are serving as the foundation for a growing patchwork of regulatory constructs governing the protection of PII/PHI. For example, under GDPR, when PII/PHI is compromised, the EU data protection regulation requires the responsible entity to report the incident to supervisory authorities within 72 hours of being detected.

Many of these regulations also require a description of the PII/PHI impacted that indicates, where possible, the approximate number of data subjects, categories concerned, and affected records. Various jurisdictions in the United States and around the world have and continue to institute similar requirements.

KLDiscovery's Cyber Incident Response services leverage years of experience handling incident response matters, Canopy software purpose-built for data mining, and tailored workflows delivered by a dedicated team of incident response specialists.

The Problem

- Cybersecurity incident
- Large amounts of potentially impacted data
- Unknown impact
- Unquantified PII/PHI
- Limited resources to review affected data

Our technology enabled services and expertise solve the data-driven problems you face in the wake of a cybersecurity incident.

KLDiscovery's Solution

- Offer early insight on impacted PII/PHI to meet reporting and notification obligations
- Lead with AI/Machine Learning for increased speed and precision
- Be ready for any associated litigation or regulatory investigations

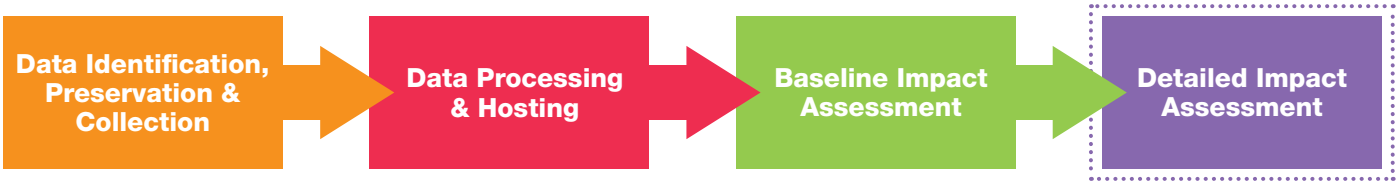
The use of purpose-built data mining software, Canopy, coupled with specialised, dedicated teams and tailored workflows, ensure the efficient identification and evaluation of data impacted during a cyber incident.

The first step in incident response is to determine which data has been compromised. Next, all PII/PHI must be processed and parsed for proper disclosure to the impacted entities and regulatory authorities.

Your organisation can rely on KLDiscovery whenever you need to:

- Leverage specialised teams, purpose-built technology, and tailored workflows for cyber incident response
- Quickly assess impacted entities and related data elements to offer early insight and regain control after an incident occurs
- Compile notification lists to contact entities potentially affected by a breach
- Lean on a partner with a steady and experienced hand at a moment of crisis with no limits on volume of data, global location, or data composition
- Conduct proactive evaluation of data protection measures to increase preparedness

We leverage intelligent, purpose-built data mining solutions to help locate, categorise, process, and review PII/PHI, enabling you to report impacted entities to supervisory authorities within the scope of mandatory reporting requirements. With an understanding of the fundamental differences between specialised cyber incident response and eDiscovery, we employ machine learning at every stage to deliver unmatched early insight and overall efficiency. Additionally, we use AI to address the most persistent challenges of data mining: lack of early insight on scope, handling of tabular data, and deduplication of impacted entities.



KLDiscovery supports your organisation with leading technology and specialised data mining services:

Technological expertise. Our specialised, dedicated Cyber Incident Response teams use battle-tested expertise, purpose-built technology, and tailored workflows to address the data mining challenges faced following a cybersecurity incident. We combine optionality in technology with years of experience focused on the task of identifying and linking impacted entities and data elements.

Proven methodologies. We have developed and refined customisable approaches to analyse impacted data. Our trusted review workflow and reporting methodologies have been adapted for a variety of industries, business units, and jurisdictions. With years of industry and issue-specific experience, we have the knowledge and ability to deliver the results you need.

Advanced analytics. Machine learning technology allows us to efficiently find PII/PHI buried in impacted data and link it to related entities.

Specialised data mining. Our dedicated Cyber Incident Response teams have years of experience leading incident response matters across industries. By leveraging purpose-built data mining software with tailored workflows, we reduce the cost of data mining matters while ensuring our clients are well positioned to meet reporting and notification obligations.

Multilingual capabilities. With reviews conducted in over 30 languages, and global operations and data management capabilities, we are ready to follow matters around the globe.

SLS KLD UK_Cyber Incident Response_Apr 2023

KLDiscovery
Nexus, 25 Farringdon Street
London, EC4A 4AB
+44 (0)20 7549 9600
www.kldiscovery.com/uk