resillion

Quality: Engineered. Tested. Assured.

Datasheet

Digital Forensics

commissum ▸▸ resillion

Widespread use of technology increases your organisation's risk of attack, creating new opportunities to exploit and disrupt your daily operations.

Poor procedures and controls often lead to destroyed or impaired evidence, impeding an investigation and negatively impact the outcome. A digital forensic investigation conducted by our experts eliminates the risk of this happening.

The Solution

Using industry leading, technlogy, hardware, and accomplished forensic specials, Resillion retrieves all relevant information, potentially discovering further evidence, from your devices, ensuring that it's neither tampered with nor destroyed.

The evidence is then analysed, giving you a holistic view into the incident. Due to the complexity of the data involved, our experts plan and structure the investigation to produce results that are of a court-approved standard.

As the UK's largest full service cyber and forensics specialists, we have a wealth of experience in dealing with a variety of HR, legal and cyber incidents, offering impartial and constructive advice on how to handle an investigation.

Forensic Readiness

Being able to retrieve data exactly when you need it is imperative in a successful investigation outcome, as well as avoiding reputational damage or regulatory fines.

Forensic investigation is usually reactive, taking place after an incident has occurred. A lack of experience in sourcing, processing or handling digital data can prove detrimental in an incident. Forensic Readiness planning ensures that your organisation is prepared and knows what to do before an incident occurs.

This includes implementing evidence generators to capture any unwanted activities and that evidence is correctly preserved to assist the investigation and robustly support any legal requirements.

A forensic readiness plan is a key strategic tool to minimise any disruption to your operations in an incident and plays an important part in the incident response process. Without an effective plan, your response to an incident is severely limited.

Prepare your organisation for any incident and have the confidence that you act swiftly, and carefully, to reduce negative impact and losses.

All methodologies and practices are in line with those set by the Forensic Science Regulator. Commissum Associates is an UKAS 17025 accredited digital forensics laboratory No. 24471. Discuss more about our accreditations by getting in touch with us today.

Attacks Investigated

- Extortion, fraud, phishing attempts
- Malicious hacking (network attacks/intrusion)
- Illicit distribution
- Insider activity
- Malware analysis (including ransomware)
- Unauthorised access

Effects Investigated

- Stolen or leaked data
- Intercepted communications
- Data alteration or destruction
- Damaged reputation
- Fraud
- Digital vandalism

Computer and Mobile Forensics

Digital evidence both manages the impact of significant business risks and supports a legal defence, but only if it is handled appropriately. Digital data is ubiquitous, with large amounts of unseen data retained within the device that can determine the outcome of an investigation.

Forensic investigations are best left to the experts, knowing exactly what to do and at the right time – correct retrieval and preservation of the data is essential to retain the integrity of the evidence. Close collaboration between you and our UKAS 17025 accredited lab (Commissum Associates Limited) ensures that detection, protection and prevention of incidents is reduced, allowing you to continue operating as usual, increasing your resilience to threats.

Resillion is highly experienced in working on a multitude of sensitive matters, helping clients to mitigate risk and respond quickly to any incident. Our experts investigate and analyse data found on your electronic devices, to discover and recover evidence that is vital to your investigation. This includes any data that has been deliberately hidden, disguised, or destroyed, in a wide variety of devices.

Device Types for Investigation

- Computers/laptops
- Computer peripherals including USB sticks, CD/DVD/Bluray discs, memory cards
- Mobile phones
- SIM cards
- External hard drives
- Servers
- Digital cameras
- International devices
- Tablets
- PDAs
- Satellite navigation tools
- MP3/MP4 devices
- Drones
- CCTV
- Games consoles
- Locked devices
- Damaged devices - with certain repairs available in our lab

Key Evidence Types

Mobile examinations yield a wide variety of information, including:

- Contacts
- Call logs
- Messages (SMS, MMS, emails & bluetooth)
- Third-party messaging apps such as WhatsApp and Snapchat
- Social networking apps like Facebook, X, Tumblr, Instagram
- Internet browsing and web cookies
- Photos, videos, and sound recordings
- GPS and geo-tagging location information
- Internet and web browsing history
- Documents downloaded from the internet or transferred from other devices
- Organiser information
- Deleted data

All evidence, statements, and technical reports are appropriate for use in court. Resillion's commitment to quality and high standards has allowed us to achieve UKAS 17025 accreditation, and we adhere to the latest statutory FSR codes of practice.