

Incident Response and Forensics

Every organisation has to deal with security incidents, however hard we work to minimise their likelihood and the impact. When a security incident arises you need to be able to respond to it swiftly and safely. MWR can work with you to pin point how, when and how the incident occurred and help you ensure that it does not happen again.



How do you currently identify and respond to a security breach?

Performing a detailed scoping and threat modeling exercise with your key employees can establish the scope and priorities of the investigation. This can identify not just the known incident, but any further threats from this or a related incident.



systems with various patching levels to ensure that the full extent of malware behaviour can be identified.

Do you fully understand the process of dealing with a cardholder data breach?

Experience with PCI DSS and QFI investigations means we can offer advice on the best possible outcome. Our report template utilises Visa Europe's Forensic Investigations template to ensure that all the information discovered is presented in a clear and logical format.



Do you have a safe way of investigating machines, preserving evidence and preventing further breaches?

MWR InfoSecurity have created a custom sandbox environment that allows the safe execution and analysis of malicious code and other software. This environment contains a number of operating



How do you distribute the findings of testing directly to the team responsible for implementing a resolution?

Our secure portal FastHold ensures a secure flow of sensitive information to authorised personnel only.

As an on-line merchant, our card payment processing systems are our lifeblood. When they were breached, MWR InfoSecurity were able to advise us on containing the breach; minimising the fines we faced.

*Head of IT,
Legal Sector*

The benefits of the **Incident Response and Forensics Service** and its integration with the **FastHold** platform include:

FastHold offers customisable reporting and management of user access

allowing you to control the level of access for users within your organisation. HTML reports allow you to drill down to the detail you require in order to investigate the incident without being overwhelmed. PDF reports also offer the flexibility for you to download and print the results as required.

The reports are clear and concise, allowing you to instantly identify areas of risk and the current state of the investigation. Reports are compliant with Visa Europe reporting standards for PCI DSS cardholder data breaches, ensuring that they are generated to an industry recognised standard.

Our Forensic Investigators are skilled researchers and penetration testers.

This means they are up to date with current threats and attack vectors, and perform attacks in realistic test cases, allowing them to quickly ascertain the cause and extent of real-life security breaches whether that is a malware outbreak, a malicious insider, or an opportunistic attack against your external infrastructure.

Upload key pieces of information safely and securely.

Our secure portal has been specifically designed to allow you to upload sensitive information. Investigations need not be delayed by time-

consuming journeys on and off site to collect printed documents.

Engaging an expert in incident handling will give you detailed advice on containing a security incident, swift analysis to determine the impact, and assurance that the cause of the incident has been eradicated.

The advantages go beyond the direct business benefits of preventing further breaches and information loss; working with MWR InfoSecurity will ensure that you are more secure following the breach and can be confident that a similar incident will not occur.

For information about the MWR InfoSecurity Incident Response and Forensics Service please see: <http://www.mwrinfosecurity.com/incident-response>



Contact us directly on: +44 (0) 1256 300920 for more information about how the service could benefit your organisation or to arrange a demonstration.