Evidence Management

Ensuring video evidence integrity and admissibility

What classifies as video evidence?
The term 'video evidence' refers to any digital video images that may be utilized for organizational, legal, or criminal investigations. The specific type of investigation will impact on the level and complexity of operating procedures necessary for handling footage. For the purpose of this tech note, the information provided relates primarily to evidence for legal or criminal proceedings.

The evidence life-cycle: end-to-end data integrity
The stringent nature of audit trail requirements, coupled with the growing complexity and volume of data captured as evidence for investigation and/or prosecution purposes, means that many organizations are utilizing automated capabilities – often fulfilled by incident management functionality within their surveillance command and control platform – to meet admissibility requirements.

There are several technical mechanisms and capabilities that surveillance operatives should employ to guarantee video is securely handled at every stage in the evidence management journey.

SYNECTICS

Camera placement
Though not technically a surveillance command and control feature, it is important that cameras are placed in a pre-qualified, audited location, to ensure that each unit effectively gathers the maximum amount of information possible from its specific scene of coverage. This helps establish an efficient audit trail foundation from the very start of the evidential process.

Live evidence capture
Operators monitoring live incidents should consider real-time incident management functionality to trigger automated evidence management protocols. This functionality locks the camera control to ensure the operator monitoring the event can track and capture uninterrupted footage. Therefore all video footage, connected data, and actions taken, e.g. any manual control of cameras or event escalation and notifications, are securely logged in a repository*, establishing a firm audit trail.

*sometimes referred to as an evidence locker or secure evidence server

Supervisory review
Many command and control solutions also have built-in supervisory review functionality which permits the tracking of a particular event to be scrutinized, i.e. which cameras were used to view an incident, how and when they were moved, the sequence of camera switching, and which control room operator was controlling them at that time. This provides an additional level of procedural validation.

Evidence locker
A dedicated evidence locker – a robust server specifically configured to handle and store video evidence – should be utilized as a central point for evidence management. Providing a full managerial audit trail, all usage is logged onto a database. For future authentication purposes, a unique hash code is created (using a Secure Hash Algorithm – SHA-2 is the widely accepted standard) for the video footage. To date, there are no incidents of this particular hashing algorithm having ever been successfully compromised.

Automated redaction
Data protection requirements coupled with best practice evidence management means that surveillance operators should consider solutions such as automated redaction which, for example, can be used to blur faces or identifying markers (such as house numbers) unrelated to the incident that the evidence is required to support.

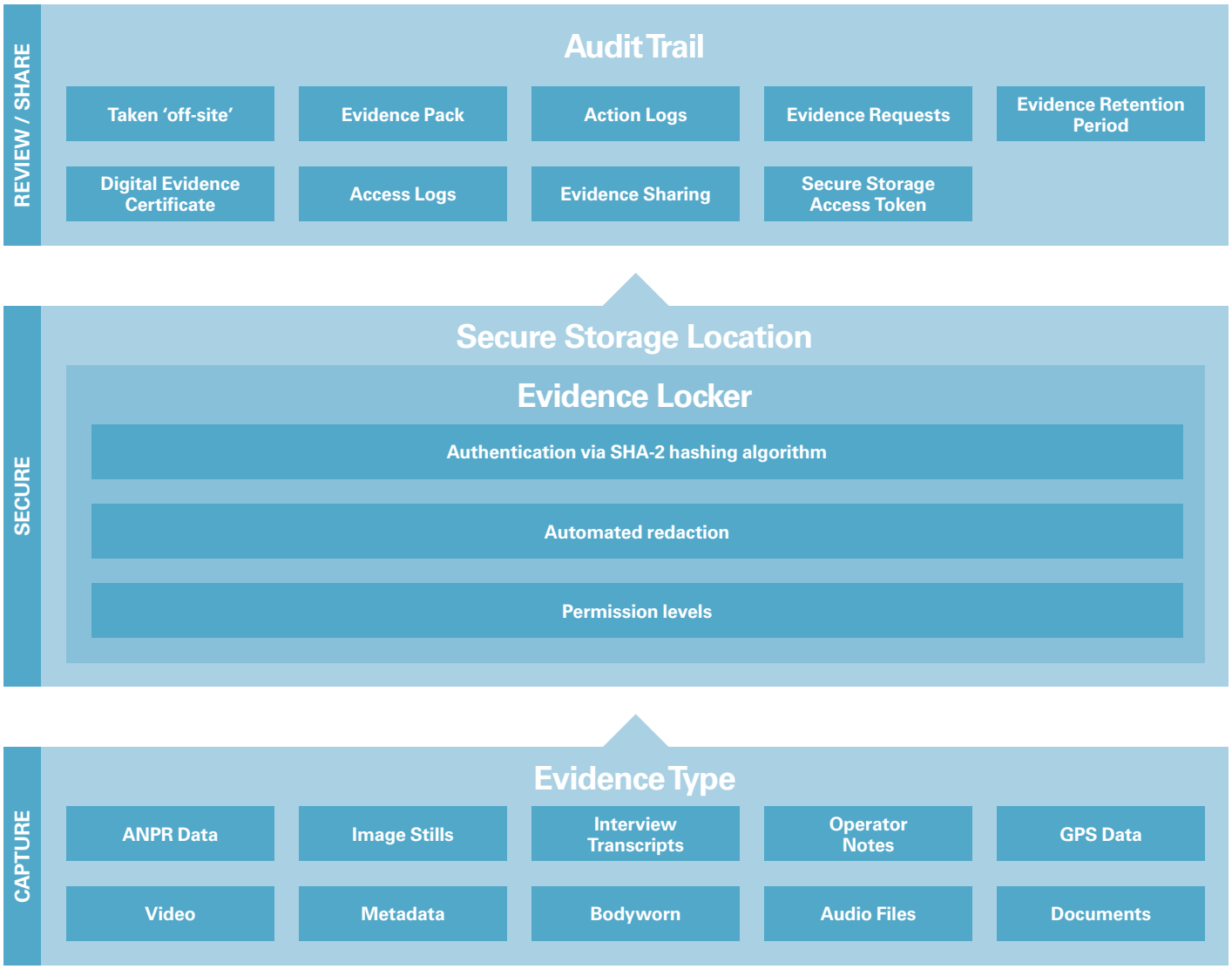
Sharing evidence
If video evidence is required to be taken off-site or downloaded by law enforcement, the system saves the video clip and evidence's hashing code, logged and detailed in the form of a 'Digital Evidence Certificate' to prove its legitimacy.

'Taken off-site' refers to evidence files being physically burned to CD/DVD, a USB or hard disk drive, and collected by a police officer or an authorized third party. In this instance, an evidence pack should be created which supplements the files with details regarding the request and removal, such as police officer's details, time of request, the reason for evidence, etc. The physical media should also be password protected. In the UK, there are Home Office guidelines for collection and transportation of physical media, for example regarding adequate packaging and labeling.

'Downloaded' refers to evidence files transferred electronically. Here, any individual requesting evidence should complete and submit a digital request for authentication. If the request is deemed legitimate, operators can issue a secure storage access token – a password and time-protected code to view the evidence remotely. Further codes can be issued which control and log any additional actions such as downloads. This is the fundamental process behind remote evidence access systems.

Maintaining end-to-end data integrity requires additional physical and procedural security measures.

Digital Evidence Management Framework



Evidence server location

Organizations have two main choices when it comes to where to store evidence; a networked secure location, typically on the premises, or a secure cloud location off-site. Deciding factors should take into account the sensitivity of the information held and with whom the information might need to be shared.

If the evidence is networked on the premises, then distribution and accessibility becomes more difficult as the third parties also need to be networked. If this is the case, appropriate levels of network security need to be in place to guard against wider unauthorized access. With a secure cloud location, it does not matter where the person who needs to access the information is based, and access is automatically restricted to the evidence required using the secure access token mechanism.

With either option, permission levels can be set to control how the evidence is used e.g. purely available to view, view and add data, or available to copy. It is also important to note that whichever option is chosen, the data owner will always retain the original information on its system.

Storage efficiency

Surveillance system operators frequently required to gather and handle evidence also might consider solutions relating to maximizing storage efficiency including, for example, options such as Time Lapse Later (TLL) recording technology. This enables high-quality footage to be captured at the very start of the recording process i.e. when it is liable to contain the most evidential value. Only later,

after an x-hour period is time-lapsing introduced; the frame rate of the stored digital video evidence is automatically reduced for the remaining x days – thereby decreasing the storage capacity required for its retention. Any footage containing valuable information is retained at the highest rate possible.

Physical and procedural security

It is important to remember that maintaining end-to-end data integrity also necessitates additional physical and procedural security measures. For example, the secure evidence server location should always be access controlled and have appropriate physical security measures in place as part of that access process (barriers, biometrics, CCTV).

Another vital step for evidence protection is to carry out employee background checks and make sure that IT policies and information management systems are both up-to-date and comply with industry standards (for example ISO 27001) in terms of legal, physical, and technical controls for identifying and managing risk. This should include regular assessments of authorized personnel to ensure that any changes in circumstances e.g. transfers, departures, are reflected in clearance/access levels.

Other types of evidence

While video evidence remains a vital component for surveillance-based evidence management systems, it is not the only form of data that can, and should, be handled appropriately.

The nature of advanced integrated surveillance solutions means multiple 'file types' can be handled, ensuring that evidence can be captured and collated from a broad range of disparate sources. Common forms of digital evidence other than video footage (from fixed or mobile solutions) may include: ANPR data, image stills, surveillance operator notes, interview transcripts or other form of documentation, and audio files (for example incident reports).

What are the quality specifications for video to be admissible?

Though higher resolution footage, for example from HD/megapixel cameras, may result in clearer images which make identifying and verifying unlawful activity easier, there are no specific image quality requirements for video to be considered admissible.

Admissibility in the UK is based on being able to demonstrate the security and integrity of footage from camera to court of law. It is important to follow the procedural framework outlined in the CAST (Centre for Applied Science & Technology) guidelines on the Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems.

Guidance to be aware of

Admissibility also relates to public surveillance being operated and managed in line with wider regulatory demands and operational codes. Those responsible for operating surveillance systems must comply with requirements under laws and codes including the EU's current Data Protection Directive.

In Europe, the upcoming GDPR (General Data Protection Regulation)* will have an impact on how evidence is captured and stored.

Outside of regulatory demands, the most important thing is simply to stay current with evolving surveillance capabilities, as best practice procedures for evidence management will evolve to reflect them.

*May 2018

Synectics
sales@synecticsglobal.com
synecticsglobal.com

Literature Reference: EVIDENCEMGMT-TN/0218/A4 Iss 1