IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Technology and Innovation

Why Digital Forensics and Incident Response Must Go Remote

Harsh Behl

Harsh Behl
Director of Product Management (DFIR)
Exterro

Biography

Harsh Behl is Director of Product Management (DFIR) Exterro (https:/www.exterro.com). He is responsible for overseeing the entire product lifecycle of Exterro's forensic products.

Prior to joining Exterro, Behl was on the front lines working as an evidence analyst and forensic investigator, forensic consultant, and a technical engineer. His hands-on experience and expertise provide a unique perspective that results in the development of products that are easy-to-use, intuitive, and practical.

Harsh brings a wealth of experience, knowledge and technical skill sets, steering the vision and execution of Exterro's marketing-leading Digital Forensics and Incident Response technologies.

Harsh shares his insights in Exterro company blogs at https://www.exterro.com/blog

Keywords Digital forensics, West Midlands Police, FTK Central, Cloud, DFIR, Evidence, Defensible
Paper type Research

Abstract

Corporate digital forensics are proving harder to carry out with a remote workforce. When performing a covert investigation, for instance, to detect if a user has been stealing intellectual property, it's no longer a case of physically borrowing that laptop. Security teams now need to obtain remote access to that device and to scan and image it. By centralizing the data, it can be analyzed by a designated expert or segmented and sent to multiple teams all of whom may also be working remotely. By as the author of this article explains, digital forensics is becoming increasingly more challenging.

Introduction

Up to 90%[1] of crime now features some element of digital evidence but discovering that information is becoming ever more challenging. There has been a proliferation in platforms, data formats and devices as we have become more dependent on technology, from our smartphones, to the Internet of Things (IoT) and the cloud, all of which has seen data become more disparate and dispersed.

It's a situation made yet more complex by the sudden shift in working patterns. The Enterprise DFIR Benchmarking Report 2022[2] found half of those businesses that

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

took part had a workforce that was over 50% remote while close to a third had a workforce who were 75% remote, revealing that working from home is here to stay. This rise in remote working has forced organizations to adapt their policies and technologies and that includes how they conduct digital investigations.

Investigations are carried out for a myriad of reasons, from ensuring regulatory compliance or data security to incident response. The latter usually concerns some element of breach and it's estimated that over a quarter of employees[3] steal intellectual property when leaving a company. Moreover, a recent study by PWC[4] found almost a third of fraud cases are carried out by an internal perpetrator. Should such a breach occur, the security team must be able to quickly, remotely, and at times covertly investigate matters.

Remote reconnaissance

It's common practice in such circumstances to carry out an audit of the device, usually by requesting it be handed in for a routine security check. However, remote working now makes it impossible to physically access the device, which means the investigating team need to obtain remote access to scan and image it. This requires access both on and off the corporate network so that data can be captured irrespective of whether the device is logged on to the VPN. Live data can then be captured directly at the endpoint the moment it connects to the internet, and should that connection be lost, the capture is paused and resumed when the connection is re-established.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

According to the DFIR report, organizations routinely investigate between 25-30 devices per month with some analyzing up to 350, making digital forensics and incident response (DFIR) time consuming and costly. Yet very few of these businesses had in place well defined, repeatable, managed, and optimized processes for handling remote digital forensics and incident response (DFIR). This suggests there's a real need to streamline and automate these workflows.

The automation of web-based review such as key word searching, tagging, and labelling was seen as a key objective by 40%, followed by endpoint collection and evidence processing by 20%, and then case creation and case management. But further advances in workflow automation are expected to help organizations adapt to the new normal of remote working. These include the use of machine learning to extract non-relevant data before assigning for review, integrated visualizations (including timelines, maps, charts and social communications analysis, along with image recognition), and cross-evidence insights that will flag possible causal connections.

The report found that most of the businesses that had a mainly remote workforce already had a Security Information and Event Management (SIEM) and/or Security Orchestration, Automation and Response (SOAR) solution in place but only 6% had integrated this with their DFIR solution. Doing so enables the business to capture and preserve evidence automatically on endpoints at the very moment that an intrusion or anomalous event occurs, which ensures evidence is collected 24/7.

The growing need for collaboration

Yet one of the biggest challenges of carrying out digital forensics and incident response with a remote workforce is in fact a people problem: the facilitation of cross-team collaboration. While the majority (77%) of those questioned reported occasionally or routinely collaborating on cases, 23% still work independently. Over half of the respondents said they have or would like the ability to share cases with reviewers outside their organization, such as legal counsel or third parties, indicating that technology supporting even broader collaboration would be welcome.

Such collaboration is likely to become more pressing as we go forward, given the shortage of skilled investigators, as this will allow the business to draw upon expertise from further afield. Centralizing the data will allow it to be analyzed by a designated expert or segmented and sent to multiple teams. Indeed, it's now becoming increasingly common for different departments across the business to get involved, with HR, compliance, and legal playing a more active role in data preservation, as well as collection and analysis as part of investigations.

However, involving these teams makes it even more vital that automated processes are in place to preserve the evidence correctly in the chain of custody. This is driving demand for integrated tools that enable and foster collaboration without requiring unnecessary data movement. The conventional approach sees data pass between platforms and tools, risking corruption or potential loss as well as elongating the time to resolution. In contrast, a single data store ensures that data doesn't have to move between separate, disparate platforms, and products, thereby minimizing risk to the chain of custody.

The move to take digital forensics remote is not just limited to the corporate sphere, however. The gathering of digital evidence is of course also key in law enforcement which is struggling to cope with a backlog of data. A recent report[5] by His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) revealed that more than 25,000 devices are still waiting to be processed and the report also flagged the need for a national lead/programme of improvement as well as the shortage of trained digital media investigators.

Police priorities

Law enforcement have three asks when it comes to Digital Forensics. To provide front line officers with the ability to review evidence, taking the pressure off investigators. To move from on premise to in the cloud with a secure defensible process. (There is no national blueprint on how to achieve this, leaving police forces to make the decision for themselves which has been daunting) – and finally, to automate as much of the workflow as possible and provide a scalable resource.

At the present time, forces are having to balance out the infrastructure, training, and cost of implementation against the advantages of transitioning to an automated suite. They recognize the value of being able to review their data from anywhere without the geographical constraints of getting data to the Digital Forensics Unit, can see the advantages of more powerful processing and moving from a CapEx to a subscription model but are unsure of how to do so.

The overarching concern has been how to store data in a legally defensible manner. But a testbed implementation has now paved the way in this regard. The West Midlands Police (WMP) has now rolled out a digital forensics solution in the cloud which sees FTK Central hosted over Microsoft Azure and its proved ground-breaking, significantly reducing the time and costs associated with reviewing evidence.

The project demonstrates the viability of a cloud-based solution but also the benefits of using a single platform. Up until recently, police forces have been using

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

five or six tools, but this makes it complicated for accreditation with the ISO 17025 standard that they are legally obliged to comply with. It's also harder for the reviewer, who will need to learn how to use a range of products, plus the force is also saddled with mounting software licensing costs. In contrast a single platform that can integrate with other software can cover all the standard operating procedures in ISO 17025 while providing efficiency gains, seeing the pendulum swing back in favour of an integrated workflow.

Alleviating the burden on investigators

The WMP project has revealed how bringing investigators into the workflow can relieve some of the burden that specialist investigators must bear. The front-line officers don't need to make determinations over the relevance of that data, as the software parses out that data and presents it to them to review but this does prevent investigators from becoming bogged down by data collection. If the review findings are brought into question, an investigator can then use their specialist skills to establish relevance, although this is rare as most digital evidence is accepted as fact by the defence or is met with a guilty plea at trial.

For police forces the journey from business case to implementation will undoubtedly be a long one. But the demand is now materializing from multiple directions, with enquiries coming from different elements of policing, investigators wanting immediate access to the data and specialists wanting to use their time in a targeted way. Many forces are bound by vendor agreements lasting three or four years with respect to ISO 17025 but as those contracts come up for renewal, we can expect these divisions to reconsider their options and to look to make a change, whether that be through automation, remote review or cloud hosting.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

What the experiences of those operating in the private and public sectors reveals is that DFIR is now on the cusp of substantial change. There's a real need to be able to collect, process and review digital evidence remotely, in near real-time, and using defensible processes. But this will also facilitate the kind of collaboration between teams necessary to expedite processing and drive down data backlogs, ultimately leading to speedier resolutions.

Reference

1 House of Lords (1 May 2019), Forensic science and the criminal justice system: a blueprint for change. House of Lords Science and Technology Select Committee. Available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldsctech/333/333.pdf

2 Exterro (2022), Enterprise DRIF Benchmarking Report. Exterro. Available at: https://exterro.com/resources/2022-enterprise-dfir-benchmarking-report

3 Biscom (16 April 2021), Enterprise Data Protection. Biscom. Available at: https://www.biscom.com/employee-departure-creates-gaping-security-hole-says-new-data/

4 PwC's Global Economic Crime and Fraud Survey 2022. PwC. Available at: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

5 An inspection into how well the police and other agencies use digital forensics in their investigations (1 December 2022). His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS). Available at: https://www.justiceinspectorates.gov.uk/hmicfrs/publications/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/