MAGNET FORENSICS

CUSTOMER CASE STUDY

Using Magnet AXIOM in Corporate Security Incident Response and Investigations

Fast Processing Speed and Artifact Access Improves Time to Resolution

THE ISSUES

- Staying informed on new and updated apps and artifacts
- Finding and analyzing all relevant data quickly in the time immediately following breach detection
- Supporting both red-team and blue-team security assessment efforts with solid digital forensic analysis
- Delivering results to stakeholders in a timely fashion

MAGNET FORENSICS TOOLS

- Focusing on artifacts first, finding new artifacts even when investigators may not be aware of their presence
- Allowing investigators to triage quickly, then dig as deeply as necessary to identify and verify digital evidence
- Clear, concise reporting that provides stakeholders with only the most important details needed for decision-making

Name: Chris Brinkworth

State: Minnesota, U.S.

Investigation Type: Computer & Mobile

"Since making AXIOM their go-to disk forensics tool, Brinkworth estimates that AXIOM has cut his team's evidence examination response time by at least half."

BACKGROUND

As data breaches become ever more commonplace, the pressure to detect, respond to, contain, and remediate intrusions remains high. Companies need a strong, tested infrastructure that can withstand repeated and creative attacks, and the ability to respond immediately.

Enterprise Knowledge Partners, LLC, a Minneapolis (Minnesota, USA)-based consulting firm, offers these three main practice areas: enterprise information technology architecture, cybersecurity assessments, and e-discovery and digital forensics. In addition to serving clients directly, they also partner strategically to deliver services as a third party.

Chris Brinkworth, director of forensics and e-discovery, describes how his team's practice area supports and informs the others. Their deep understanding of data storage and data volumes enables them to lend necessary insights to the enterprise architecture team, while their expertise in data parsing is a critical part of the red-team and blue-team exercises involved in security assessments.

Magnet AXIOM has grown to be a linchpin for all these services. "We use it to triage standard forensic files for our public and private client base," Brinkworth says.

"AXIOM is also part of the core toolset for our incident response units, where it allows those teams to offset historically slow and tedious examinations with radically faster turnaround and provide a deeper understanding of breach impact at end points much faster than ever before."

IMPROVED CASE TURNAROUND TIME AND ACCURACY

Before AXIOM, Brinkworth imaged systems using a file system-focused digital forensics tool, together with manual processes and scripts. "This took hours, even with keyword searches," he says. AXIOM's artifacts-focused approach, and its processing speed, offers what he considers a "federated" search through the Windows registry hives, event logs, and various artifacts.

"[The other tool] could look through those as well, but it was not as clean nor presented as clearly as AXIOM does," he says. Since making AXIOM their go-to disk forensics tool, Brinkworth estimates that AXIOM has cut his team's evidence examination response time by at least half.

Since making AXIOM their go-to disk forensics tool, Brinkworth estimates that AXIOM has cut his team's evidence examination response time by at least half.

All this is partly a matter of AXIOM's processing speed, but also its capabilities. "I look at the Master File Table first, so often I don't have to go through an entire terabyte of unallocated space," Brinkworth explains. This can be valuable whether the image is the result of a remote acquisition, or disk backups.

Another valuable AXIOM feature: its filters. "We can create an artifact profile for a given advanced persistent threat where we know its hallmarks," says Brinkworth, "and then run that profile against each of the systems we've imaged to show which ones are impacted by that threat actor."

Once they've identified the affected systems, the team then uses AXIOM to validate the artifact profile(s) within the file system—a feature that Brinkworth says "catapults AXIOM past [other tools] in terms of utility."

This has been instrumental in making a critical operational shift: from providing services on the fly, to operating through a central lab in a hub-and-spoke model. Previously, the team imaged systems as part of blue-team defensive efforts to conduct post-mortem analysis following vulnerability tests. This took cycles out of the team's other work, however. Now, the central lab takes its direction from investigators onsite, spending an estimated 60 percent of its time on casework versus about 40 percent on incident response.

In fact, says Brinkworth, AXIOM's performance is an endorsement in and of itself. "Our partner firms ask how we turn our files around so fast with the results we yield, and I share our experience with AXIOM with them," Brinkworth explains. "Recently, I hadn't spoken to one of them in a few months and in that time they had purchased and implemented AXIOM in their own labs."

For consultants, this can be a critical marketing point: the ability to position their services as "built to run faster." Indeed, says Brinkworth, it's possible for him to turn around seven to ten two-terabyte hard disks in as little as two days.

AXIOM IN ACTION: SPEED AND RESULTS

This doesn't just pay off in terms of turnaround. It also pays off in results. Brinkworth offers a number of examples in which AXIOM retrieved unknown artifacts or those which are typically difficult to find, including more evidence from deleted or unallocated space.

"[In] one case, it allowed me to triage evidence quickly and implement an examination protocol specific to the matter," he says. "This had a scope of nearly a dozen devices. I was able to quickly isolate key artifacts, generate a report and prepare for testimony within two weeks."

THE VALUE OF AN INTEGRATED DIGITAL FORENSICS SOLUTION

The ability to process multiple images at the same time, as well as to perform mobile and computer examinations in one tool, are also key features because of the need for memory and binary analysis. "Mobile is a growing segment of ours," Brinkworth explains. "We send devices to a clean room for chipoff analysis, but when we get the binary back, we run it through AXIOM." Between AXIOM's emphasis on artifacts, its filters, and its breadth, Brinkworth estimates he and his team have reduced their use of other tools by approximately 70 percent.

In a recent employment case, Brinkworth used Magnet IEF to work out a chronology of the activity on an employee's system. That activity included both remote access, and use of a web browser in private mode. "People think you can't see their use of webmail in a browser's private mode, but in that case, we were able to see them sending proprietary email using their webmail," he explains.

In another case, AXIOM worked out another chronology of shellbags that showed a defendant had not only deleted files that were protected by a legal hold, but had also formatted his PC to hide the activity.

AXIOM has even worked in unexpected and unintended ways. Over one summer weekend, while processing nearly a dozen hard disk images, Brinkworth noticed an AXIOM feature he'd never seen before: "luring content." A new feature of AXIOM, Magnet.AI, had flagged content that was not directly related to a matter—and which was significant enough report to law enforcement.

Brinkworth says that features like this offer an additional level of thoroughness that clients, not only in the private sector but also in the public sector, may find valuable. That makes AXIOM's reporting the third pillar in its importance to Brinkworth's team.

"Forensic reports can take forever," he says, "but AXIOM makes it easy for us to create a two- to three-page brief that covers the nuts and bolts of a case: your hypothesis, the evidence to support or disprove it, the methods you use, and the relevant artifact categories. That gives the client what they need to know to make decisions."

Sometimes, those decisions involve whether to move forward with a trial. "We don't go to court often," says Brinkworth, noting that his clients settle out of court about twice as often as they end up at trial —largely for employment-related issues, such as intellectual property theft. Still, in those cases that do go to court, AXIOM proves invaluable on the stand.

SEE MAGNET AXIOM IN ACTION FOR YOURSELF

If you'd like to learn more about Magnet AXIOM and how it can help find evidence you may be missing with other solutions, visit magnetaxiom.com. While you're there, you can learn more about the product, request an in-depth personal demo from an AXIOM expert, and request a free 30-day trial.

Learn more at magnetforensics.com

For more information call us at 1-844-638-7884
or email sales@magnetforensics.com

MAGNET FORENSICS®