MAGNET FORENSICS®

Saving Time during Incident Response

Memory Analysis with Volatility in Magnet AXIOM is Easier, Faster, and Comprehensive

THE CHALLENGE

RCB's team relied on open source tools for its memory analysis and other incident response processes. The tools were hard to install and configure, with many dozens of plugins and variations depending on which Windows version and service packs any given machine was running.

The team needed a more streamlined, less manual effort to perform forensics on key information, such as running parent and child processes, loaded DLLs, devices and their drivers, and other data stored only in memory. They also needed to be able to codify their processes to make it easier for the team to work from the same playbook.

COMPANY OVERVIEW

The seventh largest Oklahoma-owned bank by assets, RCB Bank serves more than 50 locations across Oklahoma and Kansas. Its in-house network security team comprises both junior- and senior-level information security professionals who handle all kinds of issues: from internal threats to the bank's intellectual property (IP), to external intrusions relying on malware.

> “I'm fairly impressed with Magnet AXIOM's memory dump analysis. I was particularly interested in the network connections and it presented it really well. Awesome tool for incident response!
>
> — Joe Sullivan, Network Security Team Lead, RCB Bank

HOW AXIOM HELPS

The answer: Magnet AXIOM, with the integrated Volatility Framework.

- Within AXIOM, Volatility can run multiple simultaneous processes—especially important capability during triage. Responders no longer need parse security account manager (SAM) or Registry hives, Most Recently Used (MRU) lists, event logs, or browser histories one by one.
- AXIOM's automatic parsing and clear artifact category display means it takes less time to determine whether a user opened a folder, copied a file, plugged in a USB drive, or other activity—and less time to train responders.
- Unlike command-line tools, AXIOMs saves time by automatically detecting a system's Windows version and service pack installations.
- AXIOM's user interface helps to set workflow boundaries. By contrast, open source command-line tools allow their users to "wander" through multiple ways to perform analysis. AXIOM helps them focus on the most necessary tasks.

Ultimately, AXIOM streamlines the RCB team's entire incident response process, making it easier to develop a playbook for how to dump memory, parse the data, and interpret the results. As a result, the team can more quickly deliver what's needed to make decisions.

AXIOM + Volatility

SEE AXIOM IN ACTION FOR YOURSELF

If you'd like to learn more about Magnet AXIOM and how it can help you run smoother investigations, visit magnetforensics.com/magnet-axiom. 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 version.

Learn more at magnetforensics.com

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

MAGNET FORENSICS®