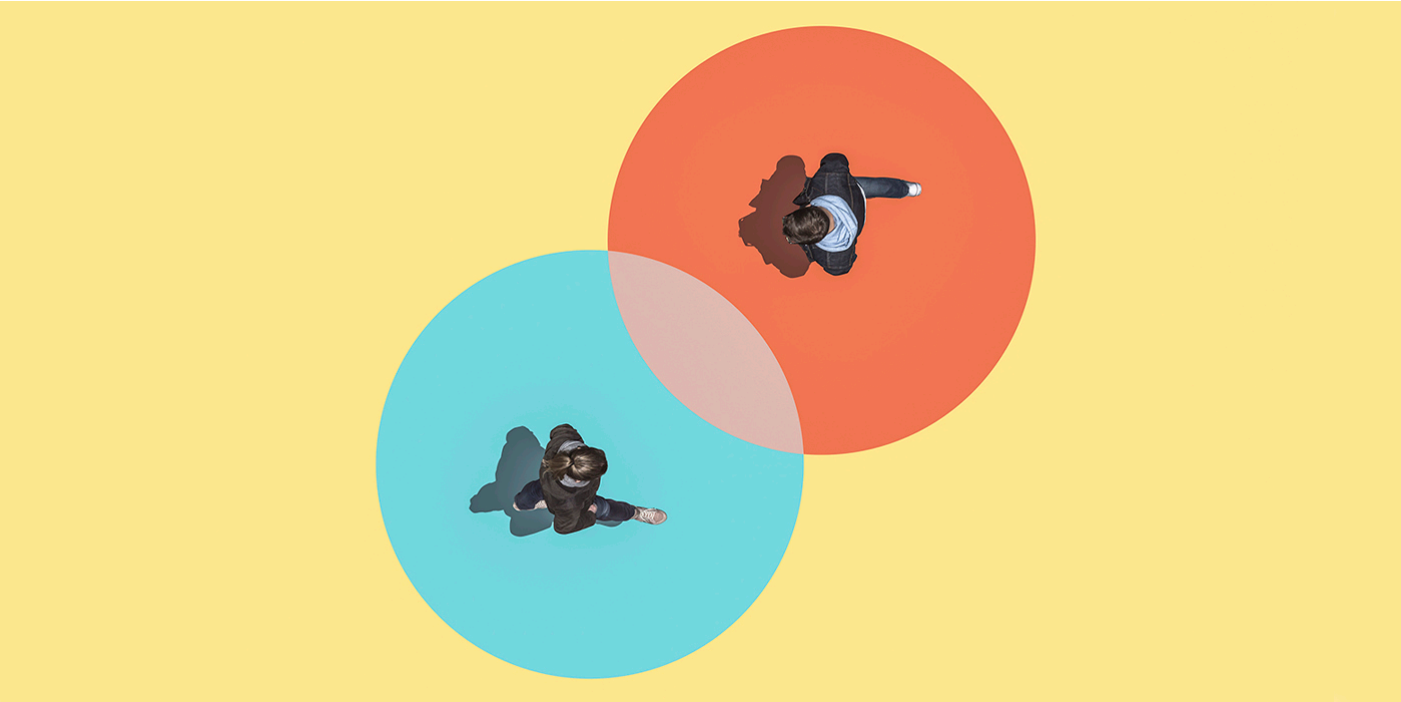
BETTER TOGETHER: APPLICATION AUDIT AND AMI SECURITY



One of BMC Software's most exciting announcements this year was the acquisition of Compuware, our largest purchase in our 40 years of serving the mainframe community. Compuware shares our fanatical belief in the longevity of the platform and now is part of our team for modernizing the 'backbone' of the IT enterprise. While Compuware has primarily focused on enabling application developers to adhere to the modern DevOps processes, one of their solutions provides detailed application and user behavior data that integrates directly into our AMI Security portfolio. This solution, Application Audit now works alongside AMI Security to enhance our ability to protect, detect, and respond to malicious threats on the mainframe.

What Is Application Audit?

Application Audit is a mainframe security solution that delivers deep insight into user behavior by capturing and analyzing start-to-finish user session activity. This provides not only file access that you would find in regular logs, but will show what data was viewed, by whom, and which applications were used to access it. This detailed data significantly increases the security teams ability to conduct User Entitiy Behavior Analytics (UEBA), support incident response, and fulfill compliance mandates regarding protection of sensitive data. It also has the ability to integrate the data directly into AMI Security where it can be consolidated alongside the data in AMI Defender for a single viewpoint for all security conerns on the mainframe. AMI Security is also specifically designed to display and integrate with AppAudit to support developing indicators of compromise and incident response following an alert.

Indicators of Compromise

AMI Security is the market leading solution for providing detection and response capabilities on the mainframe. Leveraging a real-time data stream mainframe logs and events, AMI Security is able to correlate actions together to build Indicators of Compromise as alerts for anomalous or malicious activity. Application Audit's detailed user behavior data is fully integrated in real-time which significantly enhances AMI Security's ability to perform UEBA to detect real-time threats and ultimately defend the platform.

Here is an example: One of the unique data points captured by Application Audit is the session keyboard commands, menu selections, and specific viewed data. When a malicious threat gains access to a system, the first thing they need to do is enumerate the environment to understand the specific logical partition, privileges, and available resources. This enumeration stage is often times automated in publically available scripts or follows a similar enough pattern that you could build correlation threads and alerts which would indicate that this is not normal user behavior. Now that the specific user activity is captured at this level with Application Audit, you can enhance your overall detection mechanisms to alert on a threat before they even begin to take malicious actions on the system.

Incident Response

Not only does Application Audit enable better detection capabilities, but the user data also significantly enhances the incident response team's ability to determine what the threat did on the mainframe. Since Application Audit captures the exact details for what the threat did, AMI Security can fully rebuild the 3270 screens to provide the security administrator the ability to see specifically what they were looking at, what data they were able to exfiltrate, and what data they were able to modify. The ability to graphically see all the threat's actions significantly decreases how long it would take to respond to the security incident and thus reduces the organization's total Mean Time To Respond (MTTR) which can be the difference between a minor breach and a catastrophic event.

Let's take a look at another example: Using AMI Security you get an alert that a specific user was able to escalate their privileges and now has special and operations privileges on the mainframe when they were not authorized. The incident response team takes the user ID and performs a query in AMI Security that has Application Audit data integrated and is able to see the specific information that the user was querying with their new privileges. You can immediately identify the RACF Database and encryption key datasets that the user opened and viewed so they could offline crack passwords for persistence and decrypt sensitive data. Since the incident response team was able to immediately identify the malicious activity, they were able to revoke the user's credentials and block them from accessing the mainframe through their initial point of entry while they changed the passwords, encryption keys, and responded to breach across the distributed portion of the enterprise.

Conclusion

BMC Software is dedicated to providing modern mainframe security software solutions that ultimately enable our clients to protect, detect, and respond to malicious threats. We could not be more excited to welcome the Compuware team into the BMC family and the Application Audit solution to the AMI Security portfolio. If you are interested in learning more about these solutions, or

simply discussing mainframe security, please feel free to reach me at Christopher_perry@bmc.com.

Compuware Acquisition PR

https://www.bmc.com/it-solutions/bmc-ami-mainframe-security.html

https://www.compuware.com/application-audit/

https://github.com/hacksomeheavymetal/zOS

https://www.bmc.com/blogs/top-10-privilege-escalation-hacks-for-the-mainframe/