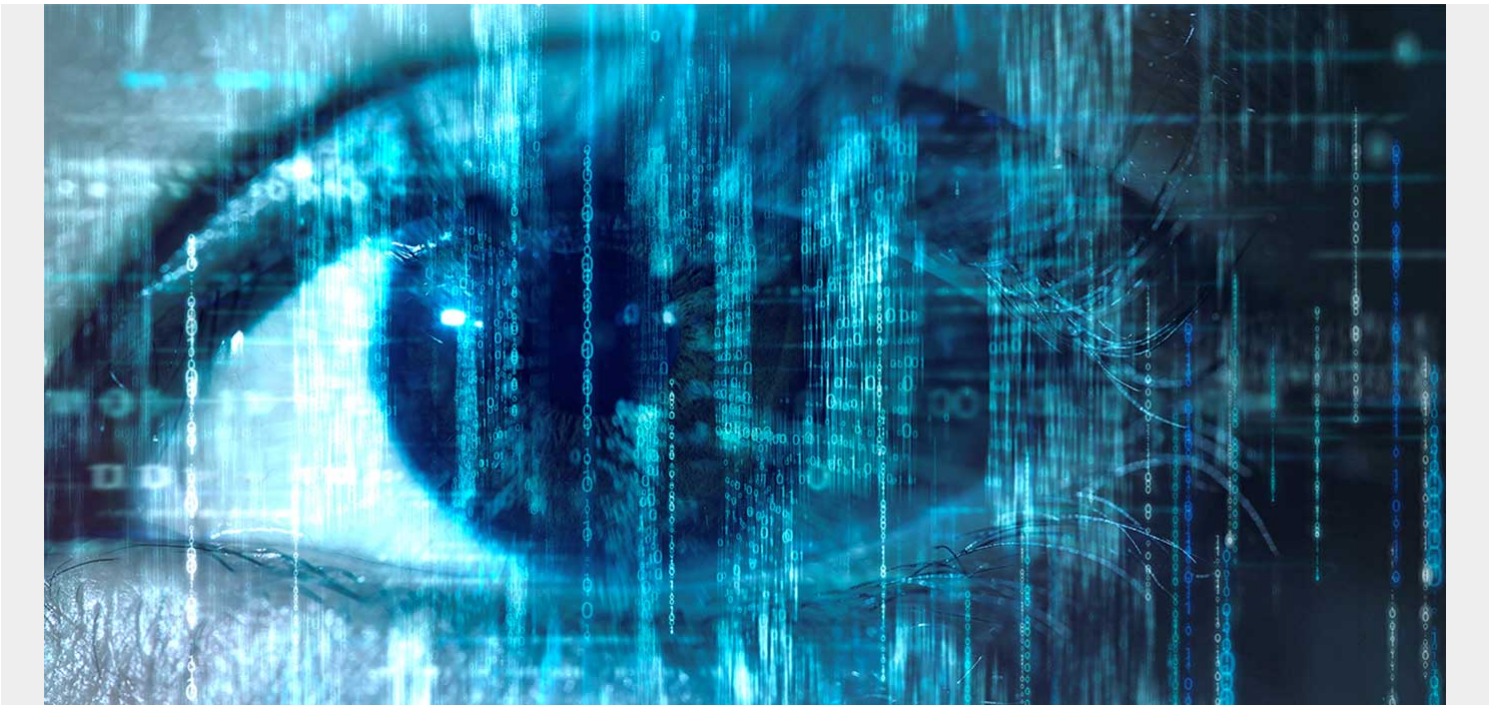
NEW PRIVILEGED USER MONITORING CAPABILITIES FOR THE MAINFRAME



Privileged users have access to the most sensitive areas of your mainframe environment. To keep them protected and help prevent credential theft or threats from a malicious insider, you need to go beyond monitoring solutions alone. BMC is excited to announce two new, innovative detection capabilities for BMC AMI Security that will enhance enterprises' ability to monitor, detect, and respond to threat activities involving privileged users: Unix System Services (USS) privilege enrichment and Supervisor Call (SVC) screener.

Unix System Services (USS) privilege enrichment

Ever wonder if there are new superusers in your Unix subsystem? What if a user suddenly became a superuser with keys to the kingdom and you weren't aware of it? If a tree falls and no one hears it, did it really produce a sound? (The answer is yes.)

From a security perspective, USS can be a valuable resource for attackers on the mainframe. While the intricacies of z/OS and its numerous applications might be foreign to an attacker, the Unix subsystem offers a familiar environment in which attackers can explore and experiment.

Security teams must maintain visibility into and situational awareness of changes in permissions and access. With the addition of USS privilege enrichment, BMC AMI Security now gives mainframe enterprises that visibility and situational awareness, including visibility into a key subset of privileged users. In addition, BMC AMI Security integrates with modern security information and event management (SIEM) solutions to ensure security teams can leverage this and other critical mainframe security intelligence within their respective analytics engines.

Supervisor Call (SVC) screener

In addition to privileged users, security teams must also have visibility into privileged "calls" on the mainframe. A call is simply the process of executing another predefined routine or set of instructions. Even without access to a privileged account, an adversary can intercept an authorized SVC and use it do anything they want on the mainframe. Thankfully, BMC AMI Security now checks for anomalous SVCs to ensure they are not misused, continually scanning the SVC table to ensure that SVCs are only present in sensitive areas of the mainframe and no other areas where an attacker could leverage them for nefarious purposes.

The features above are just two of many capabilities BMC AMI Security provides to detect and respond to threats on the mainframe. To learn more about how USS privilege enrichment and SVC screener work, read our new BMC whitepaper here. To learn more about how BMC AMI Security helps enterprises detect and respond to threats on the mainframe, watch this video.