Is Privileged User Monitoring Enough for the Mainframe?
Executive Summary

If an auditor asked your organization: “what kind of Security Monitoring do you have in place?” the answers might resemble:

“We have SIEM X, Y, Z... used by our SOC...”

• “We ingest operational and security logs and send them to Tool X...”

• “We have an Operations Center that watches our operations dashboards 24/7...”

While all the above are good things and, strictly speaking, might answer the monitoring question, they are lacking in completion from a security perspective. It is one thing to have monitoring to see or ingest data, but the real question is: is the data providing real security value?

For example, an organization might have SIEM X in their environment ingesting logs, but does it know what precisely to look for at a granular level to produce high fidelity alerts? This need is magnified with the mainframe, where security expertise is often lacking in enterprise environments.

Equally as important, does SIEM X take real-time action to mitigate potential threats? Can it read “between the lines” and identify anomalous patterns, security use cases, and suspicious activity on the mainframe?

Does Tool X enrich data so it provides real security value to human analysts? Sending a blob of data may qualify as monitoring, but do you have a method of parsing the data and adding custom fields from other data sources to provide intelligent security context?

Is it sustainable or effective to have a human supported, 24/7 operations center? Do your operators know what their baselines are and what suspicious activity looks like all the time, every time? Do they have an incident response plan in place?

These are just a few of the shortcomings of viewing security monitoring as a complete solution to securing your environment. Moreover, enterprises must have the tools to respond effectively in real-time. Simply put, security monitoring is not detection and response.
Privileged User Detection and Response with BMC AMI Security

On the mainframe, detecting and responding to suspicious activity of privileged users and services is essential to a hardened security posture. AMI Security enables security and operations teams to detect anomalous activity by privileged users across multiple areas and respond accordingly. Leveraging data enrichment and automation, AMI Security brings specific adversary tactics and techniques to the surface so your security team can focus on the threat events that matter most and rapidly mitigate them.

Detection within Unix System Services (USS)
AMI Security protects against privilege escalation attacks related to USS through the use of three unique checks.

First, AMI Security now checks whether the Unix User Identifier (UID) has changed to 0. In Unix, a UID of 0 indicates a “superuser” or a special user account used for system administration. Such accounts can take a multitude of sensitive actions, such as updating the External Security Manager (ESM) database.

Second, AMI Security also checks whether read access to the BPX.SUPERUSER facility has changed in the ESM. Using the BPX.SUPERUSER resource in the FACILITY class is another way for users to get authority to do most tasks that require superuser authority.

Third and for completion, AMI Security also goes through a series of checks to determine whether access to certain privileged functions has changed. Even if a user does not gain total superuser access via UID 0 or BPX.SUPERUSER, it is still possible that they may attempt to leverage certain privileged services. For enhanced coverage and detection capabilities, AMI Security checks for any change in access to select privileged services as well.

Thanks to USS privilege enrichment, security and operations teams can more effectively detect unusual privileged user activity, respond appropriately when privileges change and see suspicious activity in real-time.

Supervisor Calls (SVC) Screener
In addition to USS privilege enrichment, AMI Security detects suspicious access and dynamic changes to critical mainframe services known as Supervisor Calls (SVCs).

What is a Supervisor Call and why monitor them?
Supervisor calls are special instructions that allow programs, both authorized and unauthorized, to access Operating System (OS) services.

An inherent risk within SVCs is that if an attacker intercepts an SVC, they can leverage common storage on the mainframe to cause significant damage. Any user or program can access common storage and it is much easier to access than other sensitive areas of the mainframe.

Here’s an example. Let’s say a program loads a new program via an SVC. If an attacker inserts themselves in front so the program calls them first, they can use the authorized SVC to do anything they want. All of this is possible via common storage.
**Why are SVCs so important?**
SVCs, particularly ones that can be leveraged for nefarious purposes, can hide in plain sight. In fact, many are not used and only an attacker will know about them, such as those numbered between 200-255 which are “User SVCs” and not IBM defined.

Using a malicious SVC, any code can do anything it wants on the mainframe. The potential for damaging effects on the mainframe is endless. That’s why AMI Security now detects suspicious SVC activity in real-time to ensure your security operations have the tools, capabilities, and intelligence to mitigate this risk and, if needed, respond accordingly.

**How does AMI Security respond?**
With AMI Security, security and operations teams can take automated responses on the mainframe such as revoking TSO IDs and e-mailing the Security Operations Center (SOC) as soon as an alert is raised.

In addition, data sent from AMI Security enriched with User ID, Job ID, and other intelligence essential to an investigation by your SOC will be provided with further correlation in your preferred SIEM.

**What does the SVC Screener do?**
SVC Screener continually scans the SVC table in memory and reports any dynamic changes. It also checks the SVC type and compares it with where the actual call is in storage. The reason for this is that certain SVCs should only reside in more sensitive areas of the mainframe, not common storage.

For example, if SVC Screener detects SVC Type 1 in the nucleus, this is expected behavior. However, if it detects SVC Type 1 in common storage this is unexpected and is immediately flagged. Memory mismatches are also reported because this means an SVC was dynamically modified. A type mismatch can also flag a policy violation and create an alert for further investigation.

SVC Screener detects these changes as soon as they happen. Using these advanced detection techniques, AMI Security helps ensure you have the granular visibility and intelligence needed to generate high-fidelity alerts for investigation.
Go Beyond Monitoring

There is a difference between passive monitoring and active detection and response. The former requires no additional inputs or analysis and often produces raw data with minimal security value. Security teams need the context to accurately detect and respond to threats but not at the cost of alert noise or by manually connecting the dots between tools.

AMI Security goes beyond monitoring and alerts that can get lost in the noise of a growing number of security tools by providing intelligent detection and response for the mainframe. By providing data that is enriched with investigative indicators of compromise and tailored alerts, security teams get the context they need to respond to threat events involving privileged users.

Automated detection and response actions immediately halt and reverse malicious actions involving privileged user accounts until you can fully investigate them. A real-time integration with your SIEM helps your incident responders pivot to action and close the window of opportunity for attackers.

For more information
To learn more about how AMI Security stays on the cutting edge of innovation in mainframe detection and response, visit https://www.bmc.com/it-solutions/bmc-ami-mainframe-security.html