INTEGRATING THE MAINFRAME WITH YOUR ITSM AND SOC

Bridging the gap between “legacy” (I prefer the term “time-honored,”which gives the mainframe the respect it has earned) systems and the enterprise was once considered an arduous task. It was the can kicked down the road, the last platform to integrate on the program manager’s schedule. With the array of solutions available on the market today, integrating the mainframe with your enterprise’s IT service management (ITSM) or security operations center (SOC) has never been simpler.

While this blog post could just as easily cover general mainframe enterprise integration, when it comes to security, the two main integration points are ITSM and the SOC. Many would argue a third, equally valid integration point would be the JML (joiners, movers, leavers) solution and they would be right. I will touch on it later.

Just in case ITSM and SOC are new terms to you, I’ll define them. ITSM is the practical implementation of the ITIL® framework. BMC and ServiceNow are two examples of ITSM solution vendors; a few practical examples might be the portal where you request your new laptop or raise a change for your weekend go-live. The SOC is a 24x7 staffed security function that detects and responds to cyberattacks in real time.

Maximize your mainframe

With 80 percent of enterprise data residing on mainframe, imagine all the insights that could be yielded by including the platform in the enterprise’s centrally driven processes. From benchmarking the number of major incidents that occur following changes to how often a security incident makes

its way to the SOC, there are a lot of business process that take a fork when it comes to the mainframe.

Currently, when we interact with our organization's ITSM and request an item from the catalog, we don't necessarily know which platform that request is for—we just request the application. There is no reason the mainframe cannot be maximized in this way. Platform-agnostic interfaces and standardized protocols are available for the mainframe and should be utilized. In essence, this can be summed up simply: If an integration is difficult or introduces toil, the chance of integration greatly decreases in favor of platforms that can be integrated.

ITSM

In principle, there are two ways the mainframe interacts with enterprise ITSM: as a request to the mainframe from ITSM or request to ITSM from the mainframe. Let's first look at the ITSM tool sending a request to the mainframe. To put this in perspective, I will make this use-case-based—a privileged access request.

The user logs on to the ITSM solution and chooses privileged access from the catalog. In the request form, their mainframe ID is automatically filled out by making a REST call to the privileged access management (PAM) solution. The projects they can request are also populated in a drop-down list generated as part of the same initial REST call. The user selects their project and enters an ITSM change reference. If the change reference is approved, the user's request can now be submitted. Upon managerial approval, the access will be granted through the ITSM tool based on the change window.

This example demonstrates a fully audited privileged access request linked to a change reference. Now, any actions executed on the mainframe side should also include the ITSM change reference for audit investigations or forensic analysis. Users only have to learn one system, which results in greater accuracy and less training overhead. The end-to-end auditing will also satisfy auditors in terms of controls.

The second use case is the mainframe sending a request to ITSM. There are events that happen on the mainframe that need to initiate a workflow, such as an alert to be investigated or a call to action. The use case to be highlighted here is suspicious behavior where it is known that no breach occurred. It should not be considered innocent behavior if a user tries to view a sensitive dataset but is denied. Automatically raising a ticket in ITSM from your real-time threat detection and alerting solution that notifies the security team to investigate is a sensible next action.

The third use case for ITSM and the mainframe is JML. Access can be requested as part of the catalog. There is therefore no reason, in theory, that the ITSM solution cannot make the call to take action on the JML request.

SOC

There are several major benefits to bringing your mainframe into scope of the enterprise SOC: comprehensive monitoring, early threat detection, improved incident response, better compliance, centralized management, and trend analysis.

There are two approaches to sending alerts to the SOC. The first is to send all security events and write indicators of compromise (IOCs) and indicators of attack (IOAs). The second is to use a product

with out-of-the-box intelligence and work with the mainframe security team to write any site-specific alerts. Any data sent to the SOC needs to be usable—for the mainframe, this often means record enhancement, i.e., an employee name or IP address—so it's vital to make sure SOC members have everything they need. Once alerts have already been sent to the SOC, the next step is making sure the SOC know what to do after they receive them. This can be anything from following a comprehensive playbook all the way to the on-call process for the mainframe security team.

Conclusion

Integrating the mainframe with enterprise ITSM and the SOC is a crucial step for any organization that has a mainframe, even if they're currently migrating away from it. Bridging this gap will deliver greater insights into the platform behind the organization's crucial workloads while improving compliance, reducing the risks associated with specific skills shortages, and bolstering the overall cybersecurity posture while reducing the attack surface.