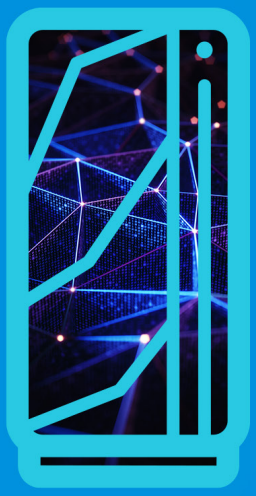
Connecting the Mainframe to Your XDR Strategy



THE EVOLUTION FROM EDR TO XDR

Endpoint Detection and Response (EDR) has been recognized as necessary but also incomplete as attacks on enterprises increasingly leverage less traditional endpoints like Internet of Things (IoT) devices and legacy or critical infrastructure systems. Security practitioners have realized that defending infrastructure and data from unauthorized access, privilege escalation and misuse are now a necessary component of threat detection and response causing many to look at adopting an Extended Detection and Response (XDR) strategy.

Definitions of what a successful XDR strategy should include vary but generally the idea is to protect across multiple systems, environments and vectors that attackers may leverage for an attack. The context gained from a broader view of threat events offers security analysts a stronger insights into attack methods in order to better hunt and remediate them.

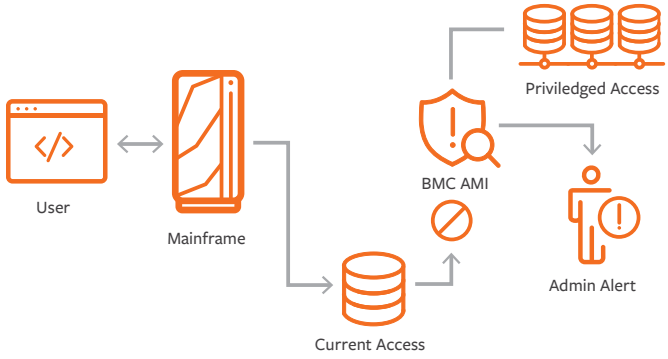
Critical systems no matter the level of native security they possess can (and have) been targeted and need to be secured and included as part of a complete XDR strategy. Mainframes although built with certain security capabilities are still just like any other computer in that they are susceptible to vulnerabilities, insider threats, configuration errors and credential theft leading to **breaches** and costly recovery.

THE SOLUTION – AUTOMATED DETECTION AND RESPONSE

Security expertise is in short supply and mainframe expertise is equally challenging. BMC AMI Security has decades of experience built-in and can automatically detect and respond to mainframe threat events and surface actionable insights to security responders in their Enterprise System Information and Event Management (SIEM) of choice.

USE CASE 1: HALTING PRIVILEGE ESCALATION

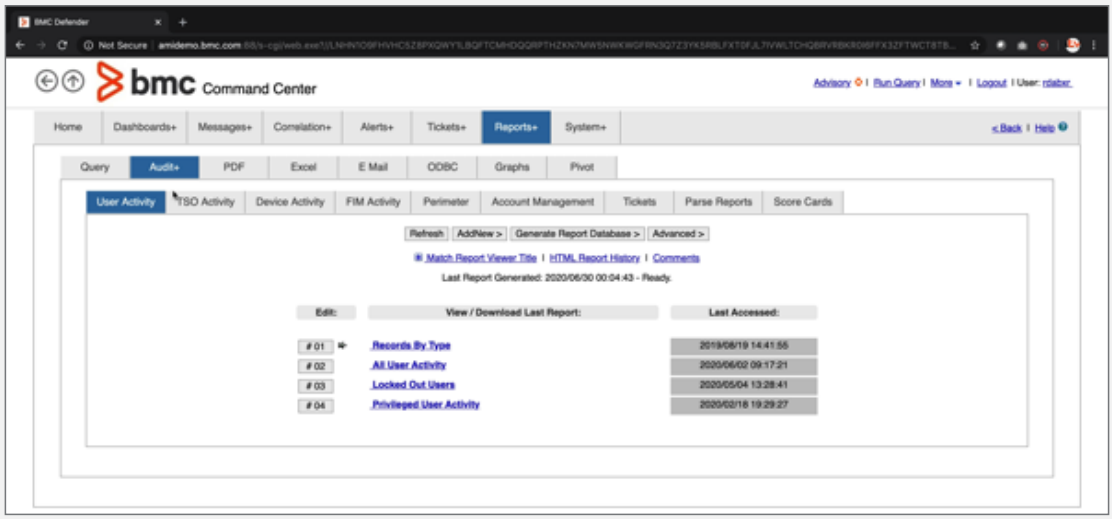
Suppose a member of your mainframe operations team falls victim to a social engineering attack or an insider decides to alter their privileges to access sensitive data. BMC AMI Security continuously monitors user privileges for changes like these and can automatically reverse a privilege escalation to cut off access and prevent malicious changes. A log of the actions taken including the user, system and connection details are captured as well for further investigation.



BMC AMI Security detects when attackers or malicious insiders attempt to escalate their privileges and automatically prevents access to protect your data.

USE CASE 2: AUTOMATIC AUDITING FOR INCIDENT RESPONSE

A successful threat investigation involves getting as much data as possible on threat events and the tactics used by attackers. Observing and recording them is key to correlating and establishing context in order to adapt your defenses and countermeasures. BMC AMI Security automatically detects when threat events occur on the mainframe but also begins creating an audit trail so incident responders have a detailed list to work from to perform investigations.



INTEGRATION – THE KEY TO XDR SUCCESS

One of the challenges of effective detection, response and investigation is the complexity introduced by a collection of security tools that each issue volumes of alerts and reports that analysts have to sift through. Manually correlating data and pivoting between consoles further complicates investigations giving attackers and extended window of opportunity. An effective XDR strategy should extend your existing security expertise and tools to address the mainframe. BMC AMI Security integrates with your Enterprise SIEM tool to bring indicators of compromise (IOC) and security events on mainframe systems to your incident investigation and response team. One of the largest libraries of IOCs and findings presented in common security terms help you leverage your existing team to investigate and remediate threats no matter their level of mainframe experience.

BMC AMI SECURITY – XDR FOR THE MAINFRAME

Obscurity doesn't ensure security. You need to know when threat events occur on critical systems like your mainframes to prevent malicious actions, data breaches and adhere to compliance mandates. With BMC AMI Security you can automatically protect, detect and remediate mainframe threats and ensure visibility for your security analysts to help inform a more effective XDR strategy.

FOR MORE INFORMATION

To speak with a BMC AMI Security Expert, please visit **bmc.com**

About BMC
From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent **www.bmc.com**

523423