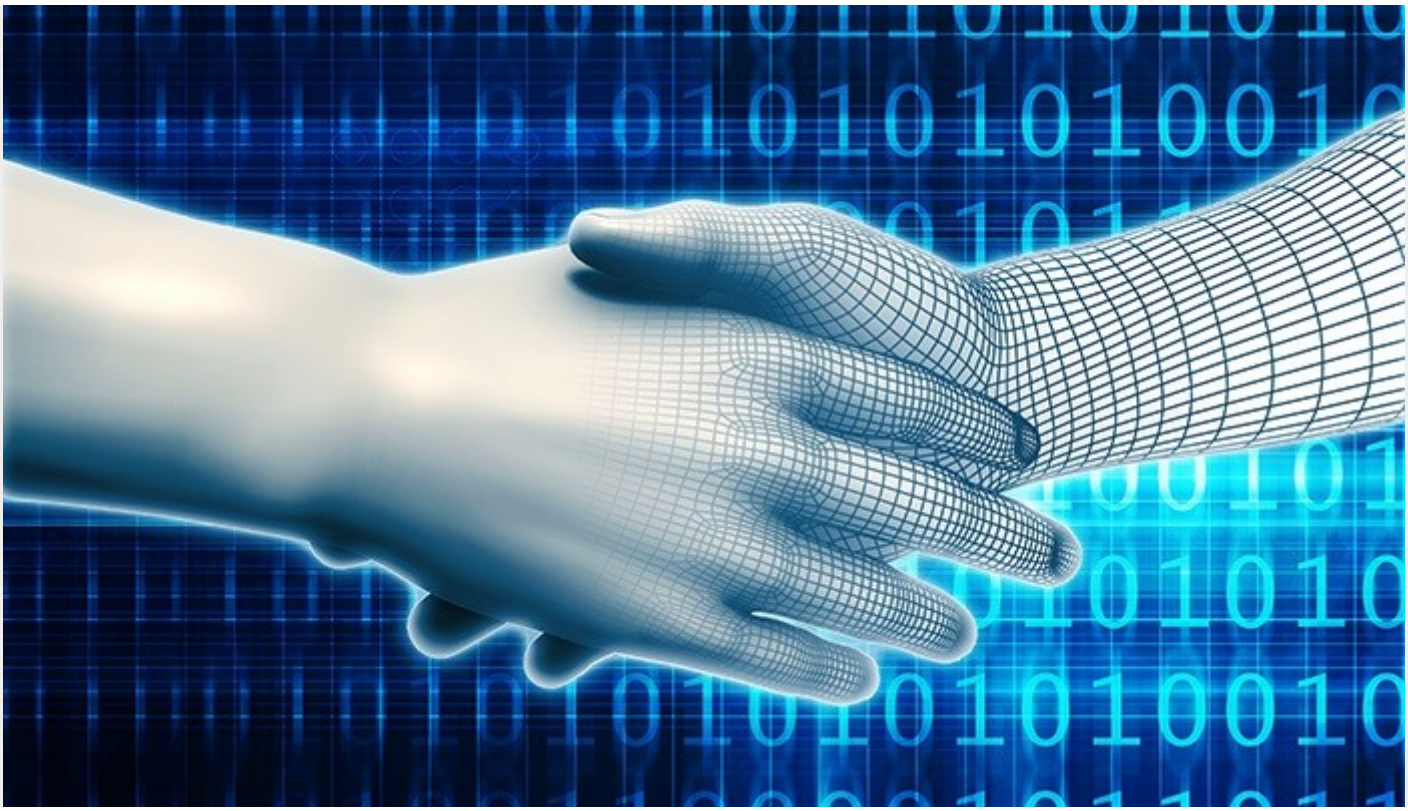
THE MAINFRAME SECURITY INTELLIGENCE GAP



If you have a mainframe, it is nearly guaranteed that you are a professional organization who handles extremely valuable data. This data may range from your customers' Personally Identifiable Information (PII), to financial transactions, or even your intellectual property.

Following industry standard best practices to protect your data, you have likely established a fully functioning Security Operations Center (SOC) complete with expert security analysts who monitor the enterprise through your Security Information and Event Management (SIEM). These security analysts are prepared to respond to security threats in real-time and bring your response rate to an attack down from months to hours. You feel protected. Are you?

Your security analysts responsible for defending your organization are only as good as two things:

1. The information they receive
2. Their training on how to handle that information

The Information in the SIEM

When was the last time your security architects analyzed the forwarders that feed your SIEM to ensure it has a complete picture? An effective SIEM will aggregate data across the breadth of your technology infrastructure. Everything from your firewalls, servers, and routers to your end point devices is responsible for forwarding relevant data to the SIEM. Any gap, or missing equipment,

leaves a glaring hole in the vision of your SOC which can be exploited by hackers, insider threats[1], or simply a poorly executed command by an employee.[2] Your SOC needs to have immediate access to all of your key infrastructure in order to have a timely and effective response to any incident.

Is your mainframe protected by the same level of best practices and automation as your distributed servers? Let's discuss the mainframe – the refrigerator sized computer that is the backbone of your entire enterprise. For the longest time, the mainframe was considered the pinnacle of secure computing which has enabled it to be fundamentally ignored by most security engineers who didn't understand it. While the mainframe is indeed a secure system, the threat landscape has developed to include nation state level resources put towards attacking civilian companies as an extension of their military and foreign policy.[3] As secure as the mainframe is, it is no match for capabilities of these advance persistent threats who are attacking systems as complex as off-the-grid nuclear power plants.[4] To protect your mainframe, and the capacity of your entire company, it is time to start treating the mainframe for what it is: just another computer on your network. This means that it is time to synchronize the mainframe's information and event logging into your SIEM in real time. Ask yourself, what would happen if your mainframe data was encrypted with ransomware?

The Mainframe Security Intelligence Gap

Let's assume that you are already on the foreword edge of security monitoring and you have worked with your mainframe and security engineers to integrate your mainframe information into your SIEM in real-time. Unfortunately, even with this, you may still be lacking the requisite knowledge and expertise to successfully use the information and react to it. It is vital to understand that data is not the end state, but the tool used to derive actionable intelligence.

With real-time monitoring your security analysts will be immediately notified of any alerts but how fast will they be able to use the data and react to an incident? If they have never touched a mainframe, and acronyms like RACF and ACF2 are foreign to them, then it is likely they will not be able to differentiate between a false positive and a devasting incident. By the time your organization realizes something has gone wrong it could cost you upwards of billions of dollars.[5]

So, who should own the responsibility of mainframe security? The answer is – it depends. Doctrinally, the role of securing the systems should fall on the SOC, but as Secretary of Defense James Mattis used to say, "doctrine is the last refuge of the unimaginative." Each organization needs to determine whether it is pragmatic for the SOC, who understands security, or the mainframe operations team, who understand their platform, that should own the role of monitoring and responding to security incidents on the mainframe. There is a strong debate for either method in the market right now. The part that isn't debatable, is that whoever owns the role needs to have it codified and then provided the resources to accomplish the mission successfully.

Training the Security Analysts

We often work with customers who have determined that the SOC will be responsible for defending the mainframes in addition to the other endpoints on the network. Most SOC security analysts will come from a background where they will be very comfortable in windows, linux, and routers which all use an entirely separate operating system than z/OS operating system designed by IBM.

Fortunately, this isn't an overwhelming gap as the foundational knowledge of security transcends all systems.

A CISO who prioritizes his analysts getting the requisite training, and providing the scenarios for them to practice, will find that the mainframe and its alerts will quickly become part of their battle rhythm. This ongoing training and education will enable the organization to have a truly defensible posture. To jumpstart this process, successful companies have generally conducted two actions:

1. Hired individuals with a mainframe background and interest in security. This new hire provided diversity of thought and experience to the security team to provide a holistic understanding.
2. Leveraged available training programs like Evil Mainframe[6] to receive a crash course on mainframe penetration testing by two of the world's leading mainframe hackers.

Whether your company choses to have centralized security in a SOC or have the mainframe operations team monitor for security issues BMC is here to help. BMC Automated Mainframe Intelligence (AMI) for Security packages the industry's leading mainframe hacking defense expertise into preconfigured alerts for your team to strengthen your security posture. If you are interested in learning more about how we can help integrate the mainframe into your SOC and provide true actionable security intelligence, start your easy trial at https://www.bmc.com/it-solutions/bmc-ami-mainframe-security.html.

[1] https://securityintelligence.com/these-5-types-of-insider-threats-could-lead-to-costly-data-breaches/

[2] https://www.geekwire.com/2017/amazon-explains-massive-aws-outage-says-employee-error-took-servers-offline-promises-changes/

[3] https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html?noredirect=on&utm_term=.cece25943963

[4] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[5] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[6] https://evilmainframe.com/