LEVERAGING AUTOMATION TO BRIDGE THE CYBERSECURITY SKILLS GAP AND SECURE YOUR MAINFRAME DATA

The skyrocketing number of cyberattacks deserves the media attention it garners. 2018 saw a 350% increase in ransomware attacks, a 70% increase in spear-phishing attempts, and a 250% increase in business email compromise (BEC) attacks—alarming figures that rightfully have CxOs worried. Despite the fact that security was deemed the top investment priority by CIOs in 2019, 65% of security professionals nonetheless should expect to cope with a major breach in 2020.

Data Security: A Frightening Future

A large part of the reason for this less-than-rosy outlook stems from the cybersecurity skills shortage. As the amount of cybercrime increases and armies of cut-rate hackers are empowered with sophisticated Malware as a Service (MaaS) weapons, the number of able-bodied defenders has failed to keep pace with the looming threat. The latest figures from (ISC) report more than 4 million unfilled cybersecurity positions around the globe—an increase of more than a million over the previous year. It's no wonder more than two-thirds of security professionals believe that the skills shortage is impeding defense efforts, and 36% of organizations cite the lack of available cybersecurity talent as their primary concern in the workplace.

So, what's to be done? Universities and school systems aren't going to be able to train the next generation of cybersecurity talent quickly enough to meet the overwhelming demand, and in areas such as mainframe cybersecurity, experienced professionals are retiring faster than they can be

replaced. The skills gap is currently being addressed by the software vendor community. But if you are going to effectively close this security gap, you must pick the right vendor who can deliver the right solution with automation.

Arming Security Teams with Software and Automation

In an environment where organizations struggle to fill critical cybersecurity vacancies, it's clear that adding additional analysts to your ranks is all but impossible. Instead, forward-thinking companies must turn to automated security solutions that amplify the efforts of your current employees, giving each one the capabilities of many.

BMC AMI Security was specifically designed with mainframe data protection and automation in mind. It's powered by a best-in-class event management system that allows you to see mainframe and distributed security events correlated alongside one another in real time to reveal anomalous activity indicative of cyber threat. Going through this amount of event log data would take an army of security personnel countless days or even weeks to find anomalous activity, but the automation within BMC AMI Security works in step with your Security Information & Event Management (SIEM) system or Security Ops Center (SOC) looking for cyber threat triggers. Data security personnel are notified through multiple channels (SMS text, email, support desk trigger, etc.) to investigate, or other automated remediation events can take place within your systems to stem the bleeding.

BMC AMI Security uses a lightweight software agent installed on each logical partition (LPAR) that works with the Server Message Facility (SMF) to enrich mainframe events with critical security information. It then formats them for ingestion with leading enterprise analytics engines. The agent operates with extremely low resource utilization and the event messages leave the LPAR ready-formatted for your SIEM or SOC. The result is cross-platform event correlation in your security software system of record for up-to-the-second alerts on cyber threat.

To learn more about how BMC AMI Security is automating your mainframe defense and empowering your valuable cybersecurity personnel, please visit our product page or reach out to your BMC solutions expert today.