

Addressing the Big 3: Cyber Security, Fraud and Compliance

The cyber threat landscape has changed substantially over the last 18 months. A mature cybercrime economy and supply chain have emerged virtually overnight. This ever-expanding supply chain acts as a force multiplier for online crime, hactivism and cyber terrorism. And to make matters worse, the pace of innovation among these bad actors is far outpacing the evolution of the technologies designed to defend against them. As a result, most organizations have come to realize that it is really a matter of When, not If, they'll be breached, if it hasn't already happened and they just don't know it.

A recent Gartner study highlights that advanced targeted attacks make prevention-centric strategies obsolete and that investment in information security needs to shift substantially. The report specifically projects that spending on monitoring, detection and response technologies will grow to 60% of information security spending by 2020, up from less than 10% today.

The latest Verizon Data Breach Report shows that 76% of all breaches reported involved the use of weak or stolen credentials. That means that someone was pretending to be someone they're not. Almost invariably, the imposter, once into the network, will behave very differently than the authorized user whose credentials they're exploiting. Today, most organizations don't know what 'normal' looks like for their employees and authorized users. Therefore, they're unable to detect when abnormal activity occurs. That's where LogRhythm comes in.

Our credit union customers are using our out-of-the-box behavioral analytics capabilities to automate the discovery of what normal is on their networks. They then use our behavioral whitelisting feature coupled with our advanced analytics engine to monitor for and alert on exceptions to that baseline. There are also specific scenarios that credit unions know to be indicative of fraud, but they lack the ability to monitor for and detect when these scenarios occur. One of our customers uses LogRhythm to overcome this challenge by monitoring their online banking servers to detect when multiple withdrawals are made from a single account from multiple locations within a short period of time.

Our highly intuitive interface makes creating custom rules, like the one described above, a snap. Additionally, our customers find that our deep well of out-of-the-box rules for detecting a myriad of other concerning activities such as compromised credentials, zero-day malware and abuse of privileged user accounts to help accelerate the time-to-value for their LogRhythm deployment. And LogRhythm's SmartResponse™ feature enables customers to automate remediation when concerning activities are discovered, thereby reducing the credit union's time to respond to those activities and minimizing the burden of such a response on their IT staff.

As for compliance, the volume of mandates and changes to existing regulations seem to be keeping pace with the rate of innovation of the bad actors they're designed to address. LogRhythm's compliance automation suites, available to all customers, provide a foundation for continuous and automated compliance assurance. Our LogRhythm's Labs team of security and compliance experts provides embedded compliance expertise via prebuilt reports, alerts, alarms and analytic rule sets, so that credit union staffs don't need to become compliance experts themselves. One customer put it this way "Once we showed our examiners how LogRhythm provides us with continuous visibility to our compliance state, we sailed through our audit."

Mike Reagan
Chief Marketing Officer



Mike Reagan has over 27 years of experience in information security, data protection and network management. He has been a

featured presenter on leading information security topics such as incidence response, data leak prevention (DLP), insider threat detection, and critical infrastructure protection for organizations including ISSA, SANS, ISACA and InfraGard. Mr. Reagan is currently the chief marketing officer for LogRhythm, Inc. LogRhythm is the largest and fastest growing independent security intelligence company in the world. The company's patented and award-winning Security Intelligence Platform, unifying SIEM, log management, file integrity monitoring, network forensics and host forensics, empowers organizations around the globe to detect breaches and the most sophisticated cyber threats of today, faster and with greater accuracy than ever before.

Contact Info

www.logrhythm.com