EMA Blog: Avoiding Breaches by Using Security Analytics to Reduce Risk

SEPTEMBER 2018

The term "security analytics" can cover a broad range of analytics, from behavioral analytics and anomaly detection to predictive and threat analytics. All of them, however, have been created to reduce risk for the organization by spotting the problems faster to hopefully resolve them before damage is done. In this context, we will be discussing using analytics to proactively identify high-risk assets within the business infrastructure to reduce attack surfaces and ultimately, business risk.

EMA research called "*A Day in the Life of a Security Pro,*"which investigated issues encountered by security operations, identified a widening gap between security staff, assets, and vulnerabilities as companies get larger. The variance appears to grow nearly exponentially because employee count in security is linear while asset growth and vulnerabilities are closer to an exponential curve. Mid-sized organizations, having as few as 10 security personnel, had an average of just under 2,000 systems in place and just under 20,000 vulnerabilities. Enterprises of 5,000 to 10,00 people, having about 30 security people, had just under 13,000 systems in place, but the vulnerability gap got wider with nearly 131,000 vulnerabilities to manage. Very large enterprises of 10,000 to 20,000 people grew to about 100 security personnel, but their total vulnerability liability exceeded 1.3 million. Thus, although smaller companies have fewer security personnel, they manage proportionately fewer assets and associated vulnerabilities.

In addition, 74 percent of security teams identified that they were overwhelmed by the sheer volume of maintenance work assigned to them, and 79 percent said they were overwhelmed by the volume of threat alerts. To add to that, 79 percent of the respondents also said their organization's patching process was significantly manual.

What does all this mean for security analytics as it applies to avoiding breaches? "*A Day in the Life of a Security Pro*" also identified that the vulnerability pool for operating systems and common applications is expanding at an approximate average of 10 new vulnerabilities per system, per month. With the additional burden of new threats targeting custom applications and products, security and IT teams can't address all of them in a timely manner. This makes prioritization of the most potentially business-impacting vulnerabilities crucial for gaining optimal security with the available resources.

Just using the severity from the researchers and vulnerability management platforms is woefully insufficient to properly prioritize because those systems do not have enough information about the environment and business context of the asset and business impact if the vulnerability is exploited. Even the CVSS vulnerability scoring system cannot effectively address these variables because without the external sources, it does not have enough information.

New analytic approaches that use machine learning (ML) and artificial intelligence (AI) can make assessments based on model-driven experience that leverages large pools of collected information. These tools create better risk profiles for assets, changing the paradigm from whack-a-mole on vulnerabilities to a direct risk-based prioritization to first remediate or mitigate the assets that would have both the highest likelihood of being exploited and the greatest business impact should they be compromised.

Now, you can engage a self-learning system powered by ML and AI that continuously predicts the likelihood of a breach for every device, app, and user on your network across hundreds of attack vectors and can display to security a heat map of this information to aid in mitigation and prioritization. Now, security can show management data and progress based on risk, a language that the business executives have been speaking for years!

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

3710.091318